2018 TAG CYBER SECURITY ANNUAL

VOLUME 1

OUTLOOK FOR FIFTY CYBER SECURITY CONTROLS

Expert Advisory Research

Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber

September 2018

Design – TAG Cyber LLC
Finance – M&T Bank
Administration – navitend
Research – TAG Cyber LLC
Lead Author – Dr. Edward G. Amoroso
Researchers – Liam Baglivo, Matt Amoroso, Miles McDonald
Facilities – WeWork, NYC

TAG Cyber LLC
P.O. Box 260, Sparta, New Jersey 07871

Security experts and practitioners must recognize that best practices, technologies, and information about the cyber security industry and its participants will always be changing. Such experts and practitioners must therefore rely on their experience, expertise, and knowledge with respect to interpretation and application of the opinions, information, advice, and recommendations contained and described herein.

Neither the author of this document nor TAG Cyber LLC assume any liability for any injury and/or damage to persons or organizations as a matter of products liability, negligence or otherwise, or from any use or operation of any products, vendors, methods, instructions, recommendations, or ideas contained in any aspect of the 2018 TAG Cyber Security Annual volumes.

The opinions, information, advice, and recommendations expressed in this publication are not representations of fact, and are subject to change without notice. TAG Cyber LLC reserves the right to change its policies or explanations of its policies at any time without notice.

September 7, 2017

To the Reader:

This *2018 TAG Cyber Security Annual – Volume 1: Outlook for Fifty Cyber Security Controls* is a companion guide to the report of similar name issued last year. I will admit that it was tempting to take last year's report and tweak a few words, add some new descriptions, and maybe draw a couple of fresh diagrams – and call the result a *new report*. Luckily, that lazy option passed, and instead, I spent an hour of each day for the past six months writing a new book. So, if you thought you'd get off easy, then forget it: *You have some reading to do*.

This new volume complements two other new volumes issued as part of the TAG Cyber Security Annual series and available to you as free PDF downloads at https://www.tag-cyber.com/. I suppose one could debate whether our TAG Cyber material is useful, but there is full consensus that our material is *voluminous*. As always, we offer our reports at a whopping price of *free*, but I suspect that if we ever decide to sell these massive volumes, we will set pricing based on dollars-per-pound.

The process used to create this volume had much in common with last year's approach. The most obvious similarity is that I once again received a lot of help. Like last year, I carefully selected and reached out to a select group of cyber security technology vendors – most of them new this year – and asked that they invest the time, energy, and resources to help me learn their specialty. These wonderful *Distinguished Vendors* are listed on the next page – and I hope you'll reach out and learn from them as well. Your time will be well spent.

Also, like last year, I spent hours and hours and hours (and more hours) with enterprise security professionals and Chief Information Security Officers (CISOs) from every sector in business and government. I invited them to dinners, I cajoled them into weekly discussion sessions, and I cornered them at every conference. I think some now head the other way when they see me approaching. But this is necessary, because cyber security only comes into focus with many different perspectives. Even within the same company, I often hear different answers to the same question. So, there are no shortcuts.

An awesome new input this year was the group of *paying customers* (yes, that's right) for which my growing TAG Cyber team – Liam Baglivo, Matt Amoroso, and Miles McDonald – provided cyber security consulting. To respect their privacy, I won't name the companies here, but they provided amazing insights into current views on best practices in cyber defense. These clients included two banks, a software company, a government support team, a tech company, a non-profit, and a medical device company. Assisting on their projects was enormously helpful in the creation of this volume.

My annual caveat on bias must start with AT&T, where I served for thirty-one incredible years. I continue to believe that the expert team there is doing groundbreaking work in software defined networking under John Donovan, and it is ridiculous for me to try to appear unbiased. My comments on managed security services offer a glowing vision of self-provisioned, virtualized security via cloud and SDN, and if that appears to align with AT&T's approach – well, then I admit the alignment. I spent years helping to design that work, so I cannot untangle myself.

I have, however, carefully removed myself this year from all major boards. I loved my year with M&T Bank as an Independent Director on their Corporate Board, but the relationship has been redesigned as senior consultative. That is one fine group of people up in Buffalo, and I hope you use their banking services. I also stepped down from the NSA Advisory Board so that I could write openly, publish more freely, and devote the proper amount of time required for this research. That government board included an awesome group of amazing volunteers and civil servants – and I wish each of them well.

My academic affiliations remain intact, albeit perhaps more intense. I continue to teach two courses per year in a massive lecture hall to about two-hundred graduate students at the Stevens Institute of Technology annually. I've also accepted a position as a Research Professor at NYU, where I focus on cooperative learning, government-funded research, and cyber awareness events for executives. Finally, I continue to serve as a Senior Advisor to the Applied Physics Lab at Johns Hopkins University, where I support a group of ridiculously smart technologists.

Anyway, enough about me: It's time that you dive into this *2018 TAG Cyber Security Annual: Volume 1 – Outlook for Fifty Cyber Security Controls*. As you read the book, my advice is to use the Feynman self-summarization technique to absorb the material using a sharpened Ticonderoga, a fresh lined pad, and an open mind. I hope this book is useful to you.

Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber LLC
Fulton Street Station on Broadway

2018 TAG Cyber Distinguished Vendors

Each of the vendors listed below invested their valuable time, resources, and money in the development of the volume you have in your hands. They were carefully hand-selected based on the uniqueness, importance, and relevance of their offering to Chief Information Security Officer (CISO) teams from the nearly 1500 vendors we cover each year. I would list them all as co-authors if that was feasible – but of course, it is not. Instead, they are listed below alphabetically, with a brief note of thanks for their unique insight, friendship, and support of the global cyber security industry. It goes without saying that any unexpected errors in this volume, or recommendations that might ultimately prove incorrect, are entirely my fault – not theirs. Here is the list, with a word or two about their fine leaders:

4iQ – I loved working with the 4iQ team this year, including Monica Pal and Julio Casal. The digital risk monitoring and identity threat intelligence services they provide represent one of the most important contributions in our cyber security industry.
Agari – It was a delight working again with Pat Peterson and the new Agari CEO Ravi Khatod. The Agari team helped me understand email security perhaps better than any other group – and I am so appreciative of their assistance.
AlienVault – Roger Thornton is such a wonderful technologist, always available to expertly help explain some aspect of advanced cyber security. My thanks go to Roger and the entire AlienVault team for their partnership with TAG Cyber.
Appthority – Domingo Guerra was generous with his time helping to explain how app risk can be extended to holistic mobility management. Paul Stich, as always, continues to be such a wonderful contributor to our cyber security industry.
Arbor Networks – Brian McCann and his team continue to do such a great job reducing DDOS risk and helping to assure business communications. The Arbor team is first class and always great hosts for visits to Boston.
Ataata – It was a delight getting to know Michael Madon, CEO of Ataata, and to immerse in his original and amazing content. His fine subscription-based content offering provides an accurate glimpse into the future of security awareness.
AT&T – The security community at my former employer has been so incredibly helpful to the TAG Cyber team in areas such as MSS, SDN, NFV, and evolving threat. The Government Solutions team has also been a delight to work with this year!
Attivo Networks – Tushar Kothari and his capable team continue to improve and advance the state of the art in modern cyber deception for the enterprise. His support and friendship are so appreciated by the TAG Cyber team.
Bayshore Networks – Francis Cianfrocca is one of my favorite industry partners. His enthusiasm, knowledge, and good humor are such wonderful assets to the IoT/OT/ICS industry. Thank you – Francis, for our many detailed discussions!
Blackridge – When John Hayes and Mike Miracle explained first packet authentication to me, I was totally blown away by the concept. This is a fine group with deep technical expertise and experience – and I am so grateful for their help this year.
Bromium - Simon Crosby is one of the great pioneers in the use of virtualization technology to protect endpoint resources. He's been willing to assist the TAG Cyber team from the beginning and it's an honor to be associated with his fine company.
Capsule8 – John Viega and Dino Dai Zovi are two awesome technologists with enough experience and expertise between them to populate five companies. It was hard not to play favorites with such an incredible Linux security start-up from Brooklyn.
CIX Software – Sameer Malhotra is a friend and Jersey neighbor, and his people have been so generous explaining their area and helping me to understand the best way to protect software applications. I am so grateful to the team.
CloudPassage – Carson Sweet's concept for cloud security aligns tightly with my own thinking, so it was natural for me to gravitate in that direction for assistance. Every time I chat with Carson and the CloudPassage team, I learn something useful.
Contrast Security – It was such an amazing privilege to get to know Jeff Williams and the Contrast Security team. They have amazing credentials and they really know what they are doing. I am so grateful for their valuable time and partnership.
CrowdStrike – George Kurtz, Dmitri Alperovitch, and Shawn Henry might be one of the strongest executive technical management teams in cyber security today – or possibly ever. I appreciate their friendship and on-going support.
Cyber adAPT – Kirsten Bay was so generous with her time (including a day spent at NYU in Brooklyn for my students). She is one of the fine leaders in our industry, and I so appreciate her team's partnership this year with TAG Cyber.
Cyber Ark – The CyberArk team was so generous with their time this year, helping me to understand one of the most neglected aspects of cyber security – namely, privileged account management. Thanks to the fine team for their wonderful support.
Cybereason – I was so pleased to see Sam Curry recently join Cybereason, just making an excellent cyber security company that much better. I've learned so much from the Cybereason team on vital topics including the best ways to avoid ransomware.
Cylance – I am grateful to Stuart McClure and Malcolm Harkins for their continued support of TAG Cyber. Without their kind assistance explaining advanced algorithms, machine learning, and artificial intelligence, this report would not exist.
Cytegic – It was wonderful getting to know Elon Kaplan, a man with an eclectic background including an advanced degree in organizational psychology. His team's platform approach to risk management is a great contribution to our industry.
Cyxtera – I've been friends with David Keasey, Leo Taddeo, and other members of the Cyxtera team for years, and I consider their new company one of the bright spots in our industry with a world-class approach to software defined perimeters.
Deep Instinct – Few people understand machine learning, artificial intelligence, and deep learning one-tenth as well as Eli David understands, explains, and applies the technology to cyber security. I appreciate all his team does for our industry!
Digital Defense – I was so pleased to see Larry Hurtado and his team apply their years of experience and expertise to a new world-class platform for enterprise vulnerability management. I appreciate his team's continued support!

E8 Security – Industry veteran Matt Jones and his fine technical and marketing teams at E8 Security are so knowledgeable on behavioral intelligence and analytics, and they were amazingly supportive of TAG Cyber this year.
Fireglass – I enjoyed getting to know Guy Guzner and his team at Fireglass and it was wonderful to see the Symantec acquisition. Isolation is such a powerful technique for preventing malware and it was exciting to learn from the experts!
Fortinet – Ken Xie is one of the finest and most capable CEOs in our industry. We all owe much to Ken, Michael Xie, and the rest of the Fortinet team for their clear vision and strong contributions to cyber security protection of our global infrastructure.
Global Data Sentinel – The Global Data Sentinel team might be one of the most experienced groups I've encountered in my cyber analysis work. I enjoyed my interactions with Alf Poor, John Galinski, and the rest of the management team.
Guidance Software – Patrick Dennis and his team offered wonderful insights into the synergies between cyber investigative support and endpoint security. Anthony Di Bello was particularly helpful to this report. Thanks to the team!
IronNet Cybersecurity – Every time I visit the IronNet team in Maryland under the direction of retired General Keith Alexander, I return with such a renewed sense of pride at the fine people and technology the company exemplifies for our industry.
Javelin Networks – It was thrilling to learn the Javelin approach to Active Directory security, which I believe is perhaps the most neglected aspect of IT operations protection. Roi Abutbul and his team were so kind to explain their technology in detail.
Lookout – Mobile security is one of the most important aspects of the CISO portfolio, and Lookout has been a great leader in this area from the inception. I am in debt to Jim Dolce and his team for this on-going support of our work at TAG Cyber.
Lumeta – Reggie Best has always been willing to sit down and explain the fine work his team does at Lumeta. Sanjay Raja, more recently, has been a great partner. I'm so proud to continue working with such an awesome team!
Menlo Security – I so enjoyed working closely with the Menlo Security team this year, including Poornima DeBolle, who is such a fine technologist. I find isolation to be one of the bright spots in our industry, one I hope all CISOs will adopt more readily.
NIKSUN – I consider Parag Pruthi to be not only a great contributor and representative of our industry, but also an inspiration for his vision of how cyber protections must evolve. The NIKSUN story is a great one, and I am so appreciative of all they do.
Panaseer – It was such a pleasure making friends with the Panaseer folks from the UK. They were so kind with their time and energy, spending multiple hours with me explaining their approach to advanced enterprise risk management.
Ping Identity – Like last year, Ping was so generous to help me in one of the most complex aspects of cyber security. Patrick Harding spent time with me in New York, providing deep insights into modern IAM. Thanks to the Ping team!
Prevalent – It was great making friends this year with the Prevalent team, my New Jersey neighbors. Jonathan Dambrot is a true expert when it comes to managing risk in third parties, which may be the highest contributor to enterprise attacks today.
Prevoty – I rarely use the phrase "read deal" when referencing a technology and management team, but the Prevoty group is just that. Kunal Anand is a true rising star in our industry, and I love getting together with him to learn about software security!
RiskIQ – Lou Manusos has been so generous with his time this year (including braving the Brooklyn subway system for our meetings). The work at RiskIQ is world-class, and digital threat management has become essential for every CISO team.
RiskSense – I was so impressed this year with Srinivas Mukkamala and his fine team at RiskSense. I learned so much this year from the RiskSense group on automating risk management into a world-class platform. Thanks to the team for their support!
Securonix – Sachin Nayyar has assembled one of the finest teams in the cyber security industry. I learned so much this year from Securonix about advanced analytics, with the bonus that they understand IAM-based analysis as well as anyone!
SertintyOne – The SertintyONE team is as capable, helpful, and knowledgeable as any I've encountered in our entire industry. Greg Taylor sets a mood in that company that serves as a model for all of us – and I am so appreciative of their great support.
Skycure – I've had the great pleasure to be friends with Adi Sharabani, and consider him one of the leading experts in our field. I was so pleased to see the acquisition this year, and believe the Skycure solution will continue to grow in its effectiveness.
Skyhigh Networks – Rajiv Gupta is one of the most capable CEOs in our business. Every time he and I sit down, I come away with twenty pages of notes. My sincere appreciation to Rajiv and the Skyhigh team for all their support to TAG Cyber!
Skyport – It is such a delight to run into truly novel solutions in our industry, and so, it was thrilling to learn about the Skyport technology from Michael Beesley. I loved digging into and learning the details of hyper secured infrastructure this year!
Sqrrl – The Sqrrl team is capable, energetic, and gifted in their understanding of how best to support the cyber hunter working with data in a SOC focused on UEBA and other indicators. I am so grateful for all the time they spent with me this year!
Symantec – I don't think I can say enough about how much I value my friendship with Greg Clark, Hugh Thompson, and the Symantec team. I doubt you could ever find a more capable and knowledgeable executive team. I appreciate their support!
Synack – The Synack team has been so helpful to me over the past two years, helping me see the future of vulnerability discovery using vetted teams of experts. Aisling MacRunnels went way beyond the call of duty with her advice and assistance!
TenFour – Bruce Flitcroft is one of the most energetic CEOs in the business and it was exciting to have a font row seat as he rebranded his fine company to TenFour this year. His utility model has powerful implications for security at the network level.
Tripwire – It is such a privilege to have the assistance this year of such a capable team from the iconic Tripwire brand! I love their focus on a return to the fundamentals and I loved working with them on how their solutions can assist the CISO.
TruSTAR – I've been friends with Paul Kurtz for years, and I can attest to his personal convictions around the importance of threat information and intelligence sharing. He and his team are assets to our industry and I appreciate their fine support.
vArmour – Tim Eades and his team at vArmour, including Marc Woolward and Mark Weatherford, were so generous with their person time this year. They are always willing to sit down face-to-face and help me learn more about virtualized security.

Vectra Networks – The application of machine learning and AI to cyber security is a great bright spot in our industry, and Vectra does it as well as anyone. I appreciate their time and assistance to TAG Cyber, and I learned so much from their fine team!
VMWare – Alex Tosheff is a rising star in cyber security, and he helped me understand the role that virtual operating systems and infrastructure will play in next generation cyber protection. It was such a delight to work with the VMWare team!
Waterfall Security – It is impossible to spend time with Lior Frenkel from Waterfall and not come away excited and invigorated to meet the growing challenges of protecting industrial control systems. Keep up the great work, Lior and team!
ZeroFox – The wonderful team at ZeroFox under James Foster was generous with their time and assistance to TAG Cyber, helping us better understand the best way to address social and digital risks. Thanks to the ZeroFox team!

2018 TAG Cyber Security Annual

Volume 1: Outlook for Fifty Cyber Security Controls

Prepared by the TAG Cyber Security Analysts
Team Lead: Dr. Edward G. Amoroso

Introduction

To assist the enterprise cyber security team in the reduction of risk, TAG Cyber has identified and published fifty controls that must be addressed in any effective organizational protection program. These controls are depicted using a tabular diagram that many users have come to refer to as the *periodic table* of cyber security controls:

Perimeter Controls	Network Controls	Endpoint Controls	Governance Controls	Data Controls	Industry Controls
1 Intrusion Detect/Prevent	9 CA/PKI Solutions	17 Anti-Malware Tools	26 Brand Protection	35 Application Security	43 Industry Analysis
2 Data Leakage Prevention	10 Cloud Security	18 Endpoint Security	27 Bug Bounty Support	36 Content Protection	44 Information Assurance
3 Firewall Platform	11 DDOS Security	19 HW/Embedded Security	28 Cyber Insurance	37 Data Destruction	45 Managed Security Svcs
4 Network Access Control	12 Email Security	20 ICS/IoT Security	29 GRC Platform	38 Data Encryption	46 Security Consulting
5 Unified Threat Management	13 Infrastructure Security	21 Mainframe Security	30 Incident Response	39 Digital Forensics	47 Security Recruiting
6 Web Application Firewall	14 Network Monitoring	22 Mobile Security	31 Penetration Testing	40 Identity and Access Mgmt	48 Security R&D
7 Web Fraud Prevention	15 Secure File Sharing	23 Password/ Privilege Mgmt	32 Security Analytics	41 PCI-DSS/ Compliance	49 Training/ Awareness
8 Web Security Gateway	16 VPN/ Secure Access	24 Two-Factor Authentication	33 SIEM Platform	42 Vulnerability Management	50 VAR Security Solns
		25 Voice Security	34 Threat Intelligence		

Figure i. TAG Cyber Periodic Table of Fifty Cyber Security Controls

The fifty controls are introduced and explained in Volume 1 of the *2017 TAG Cyber Security Annual*, along with detailed cross-reference listings of world-class cyber security vendors supporting each control. Readers are advised to take some time to review that volume to build familiarity with the TAG Cyber approach. It is available to you as a free PDF download at https://www.tag-cyber.com/.

The purpose of this volume is to provide a detailed 2018 outlook on each of the fifty controls for both enterprise practitioners and cyber security vendors. Each of the fifty control outlooks was developed to help security teams optimize their programs. Many wonderful frameworks exist that provide tips and guidance for existing programs, but the TAG Cyber controls match up with the specific, day-to-day, practical issues that arise for enterprise security organizations.

The outlooks in this volume were written under the assumption that the enterprise security team is unsatisfied with the effectiveness of their existing approach. We have tried to capture a

general view of how most teams are either planning, or should plan, a comprehensive improvement of their cyber security ecosystem. This general view is best captured by its simple moniker: *Explode*, *Offload*, and *Reload*.

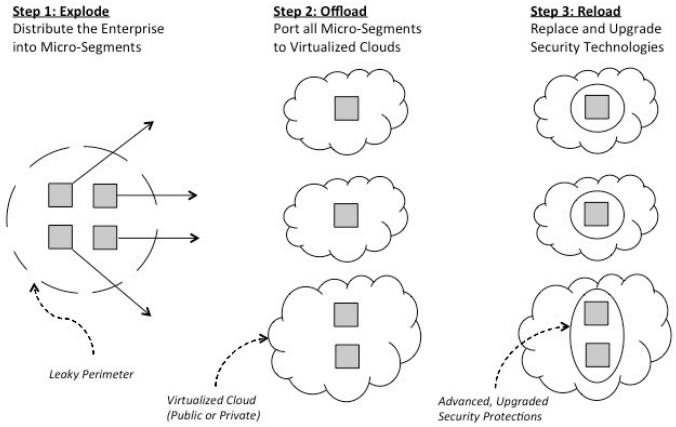

Figure ii. Explode, Offload, and Reload Methodology

By *explode*, we imply that every enterprise security team must immediately break-up and distribute the existing flat perimeter-protected network. By *offload*, we imply that every enterprise security team must then virtualize the result distributed workloads into a service provider-supported cloud and network infrastructure. By *reload*, we imply that the resultant new set-up must then be protected with the best new security solutions available.

Readers must understand that our outlooks are useless to any security practitioner, technology developer, compliance auditor, or other cyber industry professional who does not buy into the TAG Cyber methodology. Each of the outlooks assesses appropriateness and readiness of a given control to support distribution, virtualization, and protection upgrade in the context of the evolving enterprise. If you love perimeters and mainframes, then this book is not for you.

The sections below follow directly from the periodic table of controls. Each section briefly introduces the associated control, and then offers an outlook based on our methodology. Specific guidance is offered for enterprise security professionals and cyber security technology providers. This guide can be read stand-alone, or can be used as a companion document to the original TAG Cyber Security Annual. Vendor listings for each control area have been updated for 2018.

Control 1: Intrusion Detection and Prevention Systems

Intrusion detection and prevention systems (IDPS) are cyber security functional controls that are designed to detect and mitigate cyber attacks. Such functionality is sufficiently broad and general to complicate an easy definition of this control. This was not always the case, of course, since early intrusion detection systems (IDS) involved sensors in networks and hosts that

collected indicators for correlative processing. Defining IDS was simple then. Today, enterprise security teams should view modern IDPS as consisting of three fundamental approaches:

- *Traditional IDPS*: Traditional IDPS network and host appliances, now mostly virtual, collect signature-based indicators and provide optional mitigation.
- *Advanced IDPS*: Advanced IDPS use clever methods such as virtualized detonation to identify serious and subtle conditions such as advanced persistent threats.
- *Deception-Based IDPS*: Deception-based IDPS demonstrate great promise in using creative lures, traps, and honey to detect and ultimately mitigate threats.

The techniques used in these IDPS categories increasingly rely on the use of machine learning, deep learning, and artificial intelligence. While these methods are well-established means for applying heuristic mathematical reasoning to computing problems, their proper application in cyber security products is non-trivial. Some solutions appear to do this well, whereas others might be using the terms to advance marketing goals.

General Outlook

The general outlook for IDPS involves transition from a stand-alone function in 1998 to increased use as a function integrated into other security components. IDPS has also undergone transition from a more generalized attack detection function to one that involves more domain-specific capability. First generation IDPS from 1998 to 2007 was characterized by early introduction of host-based intrusion detection systems (HIDS) and network-based intrusion detection systems, both offered as hardware appliances using general intrusion signatures. Second generation IDPS from 2007 to 2016 was characterized by integration with next-generation firewalls (NGFW), early introduction of behavioral detection algorithms, early use of simple deception technology, and the beginnings of virtualization for cloud workloads. Third generation IDPS, which begins in 2016 and can be predicted accurately through 2025 will involve heavy implementation in Internet of Things (IoT), mobile and cloud infrastructure, generally as lighter, virtualized appliances, running in cloud operating systems with software defined network (SDN) support, and more effective use of deception.

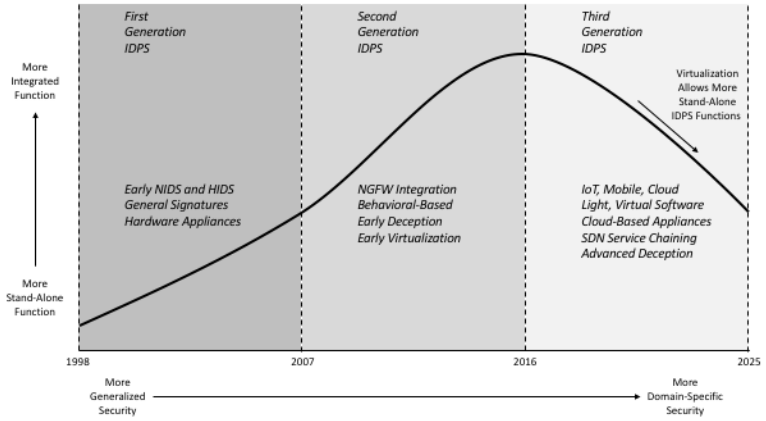

Figure 1. 2018 Intrusion Detection and Prevention System Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, given the rather clear momentum transition that is on-going today. The visual drop-off in the graphic showing transition back to more stand-alone functions should not be viewed as a negative trend, but rather as a more appropriate means for delivery of attack detection functions using specific virtual appliances. Stand-alone processing lends more naturally to virtual service chains and to the development of flexible, defense-in-depth cloud security gauntlets found in microsegments and cloud access security architectures.

Advice for Enterprise Security Teams

Enterprise security teams are advised to *diligently ensure full and proper coverage* in all three areas of IDPS, including traditional (signature), advanced (virtual, behavioral), and deception-based, since each area offers unique and necessary protections. Domain-specific environments such as industrial control will benefit from the additional domain options for IDPS, especially where more standard industrial control protocols such as Modbus and CANbus are being used. IDPS functionality must be connected to reasonable back-end support infrastructure for threat analysis, even if this requires partnership with a suitable managed security service (MSS) provider.

Advice for Security Technology Vendors

IDPS security technology vendors should recognize that the generic functions they previously supported will continue to become commoditized. In its place, domain-specific, stand-alone, virtualized IDPS capability using advanced algorithms will generate sales. Vendors should differentiate their IDPS products based on specific, targeted capabilities, because IDPS functionality will become sufficiently ubiquitous that general, signature-based functions detecting well-known attacks will go the way of calculators and flashlights. That is, they will become virtualized and integrated into other components. Deception will continue to grow in relevance and the best vendors will learn to deal with specific business characteristics to ensure target believability.

List of Support Vendors

Alcalvio – Through acquisition of Shadow Networks, Alcalvio creates virtual networks where programmers can simulate attacks.
AlienVault – AlienVault is a SIEM vendor that includes IPS security functions in its crowd-sourced cyber security capabilities.
Attivo Networks – Attivo Networks provides customers with deception-based attack detection and prevention capabilities.
Bricata – Bricata offers high performance intrusion prevention that operates at line speed with a large network.
BluVector – BluVector provides advanced threat detection solutions including a capability based on artificial intelligence.
Check Point Software – Check Point Software offers solutions with IPS as an integrated features or stand-alone capability.
Cisco – Cisco's intrusion detection products helped to establish the enterprise IPS market in the mid-1990's.
Core Security – Core Security provides an advanced platform for real time network data collection and security analytics.
Cymmetria – Cymmetria offers deception-based computing to detecting advanced cyber security threats.
DB Networks – DB Networks provides continuous monitoring and attack detection for database infrastructure.
Deep Instinct – Deep Instinct employs deep learning to detect advanced real time APT in endpoints, servers, and mobiles.
Endian – Endian provides a wide range of UTM, firewall, VPN, and related solutions, many with integrated IPS capability.
enSilo – enSilo provides advanced data exfiltration detection solutions for enterprise customers experiencing a breach.
Extreme Networks – Extreme Networks offers an IPS based on its Enterasys acquisition years ago.
FireEye – FireEye provides APT detection and prevention through data collection and virtual detonation of suspicious payloads.
Fortinet – Fortinet offers the Fortinet Intrusion Prevention System with the ability to customize signatures.

HPE – The Tipping Point product, acquired by HPE, was one of the earliest intrusion prevention systems in our industry.
Huawei – Huawei is a major Chinese technology and network provider that includes IPS solutions for enterprise.
IBM – Solution provider IBM offers its Security Network Intrusion Prevention system appliances powered by X-Force R&D.
Idappcon – Idappcon offers in-line network intrusion detection solutions with the ability to write Snort-based security rules.
Illusive – Illusive provides IDS utilizing deception based on the experience of the principals working in Israel's elite Unit 8200.
Intrusion – Intrusion has been offering a range of IDS and IPS solutions since 2000.
IronNet Cybersecurity – IronNet is a network monitoring and security analytics firm providing state-of-the-art attack detection.
Javelin Networks – The company uses deception to provide advanced Active Directory protection for enterprise.
LightCyber – LightCyber supports advanced behavioral attack detection through its Magna platform.
MetaFlows – MetaFlows has developed intrusion prevention technology based on in-line Snort operation.
Intel – McAfee, previously Intel, offers intrusion prevention system products with signature and signature-less inspection.
Niara – Niara provides a security analytics platform that supports forensics and basic real time attack detection capabilities.
NIKSUN – NIKSUN can support packet capture and analysis at extremely high network capacity rates.
NSFOCUS – NSFOCUS includes intrusion prevention capabilities in its anti-DDOS product and service suite.
Onapsis – Onapsis provides automated security assessment and attack detection services for SAP.
Palo Alto Networks –Palo Alto Networks provides a range of embedded, integrated support for IPS in its security products.
PrivacyWare – PrivacyWare offers advanced intrusion prevention and Web application security software for Microsoft IIS.
Radware – The DefensePro Network Intrusion Prevention is integrated with DDOS and SSL-based attack protection.
Reversing Labs – Reversing Labs provides automated support for detecting malware in files, web, and email.
Seculert – Seculert provides a virtual, cloud-based platform that is accessible to the enterprise via APIs.
Securonix – Securonix provides a platform for collecting and analyzing cyber security intelligence for threat detection.
Snort – Snort consists of free intrusion detection software used in academic, research, and innovative environments.
SS8 – SS8 extends its expertise in law enforcement data collection and into support for modern IPS based on deep inspection.
Symantec – Symantec offers mature network-based IPS protection solutions as part of its wide range of security offerings.
TrapX Security– TrapX provide cyber attack detection through camouflaged malware traps and deceptive computing.
TrustedMetrics – TrustedMetrics offers an intrusion detection system with advanced threat and malware detection.
TrustWave – The well-known solution provider includes IPS capabilities in its range of IT security offerings for enterprise.
Vectra Networks – Vectra provides advanced, real time, AI-based continuous monitoring of networks.
Veedog – The Veedog solution offers malware prevention that sandboxes suspicious files and screens them for problems.
Webroot CyberFlow Analytics – Webroot acquired the CFA advanced breach detection product for enterprise customers.

Control 2: Data Leakage Prevention Systems

Data leakage prevention (DLP) systems are cyber security functional controls that are designed to detect both accidental and malicious release of proprietary or sensitive information to any unauthorized entity. When such operation involves inadvertent, accidental data leakage, DLP systems exist on the margins of security and information technology (IT). Increasingly, however, DLP systems are expected to detect malicious activity involving the exfiltration of data to external sources. These are tough marching orders for any security component. Today, enterprise security teams should view DLP as consisting of two main technical approaches:

- *Endpoint DLP* – Functionality is embedded in endpoints such as PCs, mobiles, and even cloud workloads to detect and optionally block sensitive information transfer across networks, USB connections, and other means.
- *Gateway DLP* – Functionality is embedded in gateways, both logical and physical, to detect and optionally block information transfer. Gateways are becoming increasingly virtual, and have expanded to include adjacent mechanisms such as application programming interfaces (APIs) between software processes.

The techniques used in DLP started with simple pattern matching on a few phrases such as 'proprietary' or 'confidential' that each organization would use to detect data leakage. This method quickly expanded to include matching on numeric patterns, sometimes using regular expression definition. The goal, obviously, was to detect credit card numbers and US social security numbers being sent inappropriately. Such techniques have been complicated by encryption and complex architectural set-ups with third-parties, hybrid clouds, and mobile devices. Hence, the modern DLP vendor will take a more holistic approach to detecting leakage, often combining traditional means with the use of behavioral analytics, machine learning, and other advanced predictive algorithms.

General Outlook

The general outlook for DLP involves transition from an observational, reactive solution to one that uses behavioral methods to prevent leakage. Architectural positioning will shift from centralized gateways and endpoints to a more distributed hybrid deployment focused on cloud workload data leakage. First generation DLP from 1998 to 2007 was characterized by phrase-matching methods on endpoints and networks to detect non-malicious information transfer. Second generation DLP systems from 2007 to 2016 began to incorporate more advanced algorithms, including machine learning and regular expression parsing, to detect more subtle leaks. Third generation DLP, beginning in 2016 and advancing to 2025, should be expected to continue their algorithmic improvement using machine learning to proactively prevent advanced, subtle data leakage attempts from virtualized computing structures such as hybrid cloud workloads. As perimeter gateways dissolve and as physical PC and mobile endpoints become software-defined, behavioral determination of data leakage will become fully virtual.

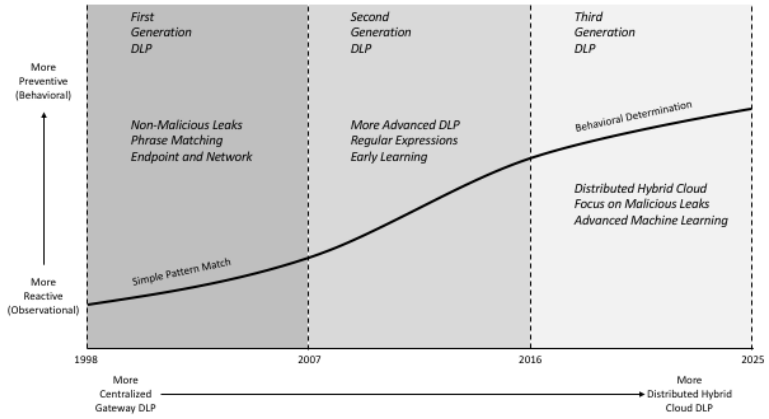

Figure 2. 2018 Data Leakage Prevention System Outlook

The TAG Cyber degree of confidence in this predictive outlook is high given the clear momentum views that have been established in the DLP market over the past two decades. The suggestion that physical endpoint PC and mobile devices will become software-defined (like your calculator and flashlight) can be jarring to some observers, but should be nonetheless expected, given the predictable pattern for how technology progresses.

Advice for Enterprise Security Teams

Enterprise security teams are advised to focus their efforts in three areas: First, they must revisit and improve on data classification definitions across the enterprise. This task is always done poorly, including in multilevel security environments in government, and this is unfortunate, because proper DLP is not possible without proper definitions. Second, they must optimize existing DLP deployments that are likely to be scattered across gateways and endpoints. For most companies, this is a mess, and it will continue to be for some time. Third, and this is the good news, enterprise teams should begin reviewing and testing the use of DLP in cloud microsegments, cloud access security broker (CASB) tools, software defined network (SDN) applications, and other virtualized computing entities. This is the future of DLP, as a powerful embedded capability, so it's time now to begin learning how to orchestrate such collective data leakage processing.

Advice for Security Technology Vendors

DLP security technology vendors should recognize that the generic functions they previously supported, especially for non-malicious pattern matching, will continue to become highly commoditized. In its place, domain-specific, stand-alone, virtualized DLP capability using advanced algorithms will become the norm. It will be challenging for DLP vendors to orchestrate dynamic policy changes, build a distributed snapshot of leakage risk, and prevent advanced attacks across multiple cloud workloads. DLP vendors who ignore this obvious shift to hybrid-cloud based, SDN-orchestrated virtualization will become extinct in the next decade.

List of Support Vendors

Absolute Software – Through its acquisition of Palisade Systems, the company offers enterprise DLP solutions.
Axway – Axway provides secure file transfer and email security solutions including support for DLP.
BHC Laboratory – BHC is a cyber security consulting and training firm in Estonia that includes a range of DLP products.
Boole Server – Boole Server is an Italian encryption software firm that includes DLP for advanced data protection.
CA Technologies – CA offers enterprise cyber security capabilities including data leakage prevention.
CenterTools – The German company offers IT security and data protection tools including DriveLock software for DLP.
Check Point Software – Check Point offers DLP solutions for on-premise or virtual deployment.
CipherCloud – CipherCloud supports DLP-based cyber security compliance solutions for public, hybrid, and private clouds.
Cisco – The company offers the Cisco IronPort product for high performance protection of email and Web data.
Comodo – Security firm Comodo acquired the MyDLP data loss prevention software solution.
CoSoSys – CoSoSys includes data loss prevention functionality as part of its endpoint security offerings for enterprise.
DataLocker – Kansas-based DataLocker includes a USB-based DLP protection solution with digital rights management.
Deep-Secure – Deep-Secure provides next-generation content inspection for its firewall and related enterprise products.
DeviceLock – DeviceLock offers the DeviceLock DLP solution for protecting personal and business data.
Digital Guardian –Digital Guardian offers next-generation DLP to control data, enforce egress policies, and more.
Fidelis CyberSecurity – Fidelis is a leader in providing cyber security solutions including support for enterprise DLP.
Forcepoint – The Forcepoint security offerings include a DLP Module in its TRITON APX product.
Fortinet – Advanced data leakage prevention functionality for the enterprise can be configured using the FortiGate product.
GajShield – The GajShield next-generation firewall appliances include advanced data leakage prevention functionality.
GroundLabs – The Enterprise Recon solution from Singapore-based vendor includes sensitive data discovery and management.
GFI Software – GFI Software provides a range of advanced data leakage protection and data awareness for portable devices.
GTB Technologies – The California-based firm offers enterprise data loss prevention and cyber security solutions.
HPE – The HP Enterprise Atalla information protection and control solution includes data leakage protection functionality.
IBM – Global technology firm IBM offers data loss prevention products as part of its Data Security suite of solutions.
InfoWatch – Russian firm InfoWatch offers customers the Traffic Monitor Enterprise integrated data loss prevention system.
Intellinx – Intellinx offers an advanced data leakage prevention solution as part of its overall set of enterprise products.
JIRANSOFT – JIRANSOFT provides a range of SaaS-based data leakage prevention solutions for the modern enterprise.

McAfee – Recently spun off from Intel, McAfee continues as a leader in enterprise cyber security including DLP.
Microsoft – Microsoft includes a range of advanced data loss prevention as part of its suite of solutions including Office 365.
Mimecast – UK-based firm Mimecast provides data loss prevention for email to support governance, risk, and compliance.
Minereye – This Israeli start-up security company applies machine-learning controls to protect companies from data loss.
Intelisecure – Through acquisition of Pentura in 2015, Intelisecure now provides a managed data leakage prevention service.
Proofpoint – Proofpoint includes high-quality, advanced DLP functionality in its advanced email security filtering technology.
RSA – The cyber security pioneering company includes data loss prevention in its cyber security suite of enterprise solutions.
RUAG – RUAG provides a DLP Product for the enterprise that is referred to as Adaptive Data Loss Prevention.
SilverSky – Now part of BAE Systems, SilverSky offers email data leakage prevention solutions for enterprise customers.
Skyhigh – Skyhigh offers a cloud-based security solution, including data leakage prevention for enterprise.
Sophos – Sophos includes advanced data loss prevention capabilities in its suite of cyber security protection solutions.
Somansa – The company, located in the US and Mexico, offers DLP for network, email, and other enterprise systems.
Spambrella – Spambrella offers cloud-based data loss prevention solutions for customers as part of its email filtering service.
Symantec – The cyber security firm includes a data loss prevention in its overall cyber security suite of enterprise solutions.
TrendMicro – TrendMicro includes data loss prevention in its extensive cyber security suite.
Trustwave – Trustwave offers advanced data loss prevention solutions through its acquisition of Vericept in 2009.
Zecurion – Zecurion provides mobile data loss prevention solutions for enterprise that address BYOD initiatives.
ZixCorp – ZixCorp integrates its email encryption product with data loss prevention features.

Control 3: Firewall Platform

Firewall platforms separate networks, or other computing environments, to enforce a desired security policy. Most firewall platforms reside on gateways between networks, but some reside on endpoints to enforce more local policies. Firewall platform operation is defined by a set of rules, usually administered using vendor-provided tools. Note that we reference firewalls as platforms here to highlight the integrated set of capabilities found in most modern firewalls. Readers already know that firewall technology continues to win the award for most explanatory taxonomies – with some pointing to two main categories of firewalls, some pointing to three main categories, some pointing to five, and on and on. Our view is that the enterprise security team will want to differentiate firewall platforms based on the following seven criteria:

- *Stateless Packet Filter* – These are simple firewall components, often implemented in routers, that provide enterprise security teams with filtering that can be deployed quickly and at low cost.
- *Stateful Application Gateway* – These are more complex firewall products that include application-level functionality such as proxies and that are also simple to deploy, and at relatively low cost.
- *Next-Generation Platform* – These are more modern and powerful firewall platforms with an impressive set of integrated security capabilities and features, especially at the application level.
- *Shared Network-Based Platform* – This is a firewall platform that resides in a network, usually as part of a multi-customer, shared managed service from a security solution provider.
- *Virtual Appliance* – This is a firewall policy enforcement capability that has been virtualized to run in a cloud operating system often as part of a micro-segmented architecture.

- *Firewall Platform Support Tools* – These are firewall support capabilities, usually focused on assisting firewall administrators with their growing number of rule sets and policy management obligations.

Note that endpoint firewalls require different management, and are best viewed separately as part of a protection solution for PCs, servers, mobiles, IoT devices, and the like. It goes without saying that firewalls will continue to serve as the backbone for most enterprise security architectures. To illustrate, just ask any Chief Information Security Officer to sketch their architecture on a white board, and they will start drawing firewalls and networks. This implies that regardless of whether the firewall platform is stateless or stateful, packet-level or circuit-based, simple gateway or complex next generation platform, locally-managed or service provider controlled, or physical or virtualized – the firewall will remain at the center of every enterprise security solution for the foreseeable future.

General Outlook

The general outlook for firewall platforms involves transition from hardware appliances to more virtual solutions, and the single gateway nature of most older enterprise networks will continue to evolve to distributed, cloud-based systems with multiple workloads requiring firewall protection. First generation firewalls from 1998 to 2007 combined a basic five-tuple packet filtering methodology with early proxy functions into a simple gateway solution. The capacity requirements for such firewalls certainly expanded during this period, but remained modest by today's standards. Second generation firewalls from 2007 to 2016 included the massive growth of next-generation firewall solutions with the ability to dynamically learn how applications worked. During the period, however, the complexity of the perimeter approach produced spectacular collapses for most enterprise security teams, and the firewall gateway could not keep up with the expanded number of rules, features, and gateways. It also did not help that capacity needs grew considerably during this unfortunate period. Third generation firewalls, from 2016 to 2025, have the obligation to fix the problem of non-working perimeters. They will do this by embracing distribution, virtualization, and simplification. Expect to see simpler virtual firewall capabilities that self-tailor to the needs of a specific cloud workload. Expect to see virtual firewall capabilities that can work in the difficult terrain of IoT and industrial control processing. Also expect to see a massive increase in distributed firewall deployments into micro-segmented environments on cloud operating systems such as OpenStack. In addition, as large network gateways are distributed and virtualized, the capacity needs for enterprise firewalls, which began modestly and then expanded during the second generation, will now become reduced once again to more modest sizes – although the aggregate capacity in a typical enterprise will become much greater.

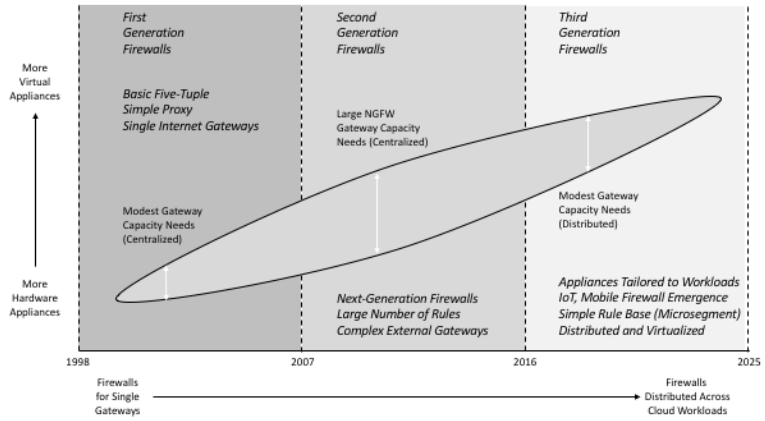

Figure 3. 2018 Firewall Platform Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, but the powerful firewall industry might not enjoy all aspects of this evolution. Existing firewall hardware might continue to amortize on the organization's capital books for years into the future, and teams might be hesitant to immediately replace them. Despite this, the obvious collapse of the enterprise perimeter in every size network will drive distribution, virtualization, and simplification faster than anyone might currently expect.

Advice for Enterprise Security Teams

Enterprise security teams are advised to take as much time as possible this year to *learn* the various options that are available for firewall platform protection as the perimeter network evolves. Basic understanding of five-tuple technology is insufficient in the coming years to deal with the myriad of decisions that will be required to optimize firewall platform selection, installation, and management, especially for next-generation solutions. This is a difficult time for enterprise teams with a dissolving perimeter, so it is time to study, learn, and absorb everything available regarding firewall platform technology. Teams should also take time to understand evolving options from service providers for network-based and cloud-resident virtual firewall capabilities.

Advice for Security Technology Vendors

IDPS security technology vendors should recognize that the perimeter is melting quickly, and with this change will come greater demand for distributed, virtual firewall solutions. Vendors are warned that the history of technology teaches us that these changes sometimes come in a choppy manner, rather than as a smooth transition. Traditional hardware products that reside on a perimeter might be paying the bills for vendors today, but this can change in a heartbeat – so firewall platform vendors must be careful not to wait too long before rethinking their technology approach. The next decade will demand simpler, domain-specific firewall tools that are light, virtual, and distributed. Vendors who miss this transition will suffer the consequences.

List of Support Vendors

AlgoSec – AlgoSec provides advanced tools for supporting enterprise firewall policy management and operations.

Barracuda Networks – Barracuda provides tools for firewall policy management and operations in the enterprise.
Blackridge – The company's first packet authentication provides advanced network access control for enterprise.
Calyptix Security – The Calyptix team offers the AccessEnforcer firewall as part of its unified threat management solution.
Check Point Software – Check Point Software was the first major firewall vendor and remains a force in the firewall market.
Cisco – Cisco complements their offerings with a firewall product for premise and network.
Clavister – The Clavister team provides software and appliance-format firewall and VPN solutions for business.
Comodo – Comodo includes a free firewall for download, which focuses on PC security protections.
Deep-Secure – Deep-Secure is a UK-based company providing cyber security solutions ranging from DLP to firewalls.
Dell – Dell offers the SonicWall firewall solution, which integrates hardware, software, and services into a common platform.
Endian – Endian provides a unified threat management (UTM) solution that includes enterprise firewall capabilities.
F5 – F5 is a successful network solutions provider with an extensive range of security capabilities including firewall solutions.
Forcepoint – In 2015, Raytheon acquired and spun off the former Websense, as part of Forcepoint.
Fortinet – Fortinet offers a security fabric of premise and network-based firewall and related enterprise security products.
GajShield – GajShield provides next-generation firewall capability with data leakage prevention and cloud security support.
gateprotect – Now a part of Rohde & Schwarz, gateprotect offers a range of next-generation firewall and UTM products.
Hillstone Networks – Hillstone Networks provides next generation firewall capabilities with integrated behavioral analytics.
Huawei – Huawei is a Chinese company that provides high quality firewall appliances including high performance options.
Juniper – Network solution provider Juniper offers traditional and next-generation firewall solutions for the enterprise.
Kerio – The Kerio team, now a part of GFI Software, offers a personal firewall and firewall functionality in its UTM solution.
ManageEngine – The ManageEngine team offers a suite of enterprise network security products including firewalls.
NetAgent – Japanese firm NetAgent provides a wide range of effective firewall solutions for use in the modern enterprise.
Palo Alto Networks – Palo Alto Networks offers solutions for application-aware firewall and endpoint security.
Sangfor – The Sangfor team offers a next generation firewall solution with effective support for SSL/VPN applications.
SmoothWall – The free firewall solution SmoothWall is available for download and use in protecting an enterprise network.
Sophos – Sophos provides a range of network security solutions, some based on the Astaro and Cyberoam acquisitions.
Tufin – Tufin provides a security policy orchestration to help firewall administrators ensure an optimal firewall rule set.
vArmour – vArmour offers a distributed, virtualized firewall for data centers and enterprise with orchestration.
VenusTech – Chinese firm, VenusTech, offers network security solutions for enterprise including firewalls.
WatchGuard – WatchGuard provides a unified threat management (UTM) platform with firewall capability.

Control 4: Network Access Control

Network Access Control (NAC) consists of security mechanisms designed to protect a local area network from malware or other infections that might result from allowing connectivity by an insecure device. NAC security mechanisms include the following three categories of protection functionality:

- *Pre-Connectivity Protections* – This involves any pre-testing, analysis, inventory, patching, scanning, or other checks that help determine security suitability of a given device for connectivity to the local area network.
- *Quarantine Processing* – This involves any intermediate testing, analysis, mitigation, patching, or other quarantine-based protections that are designed to improve device integrity before connectivity is allowed.
- *Post-Connectivity Protections* – This involves any post-connectivity updates, mitigations, scans, patches, or other enhancements that are designed to reduce malware risk after a device has been permitted to connect to a local area network.

NAC developed at the intersection of flat, perimeter protected enterprise networks with unmanaged, non-company-controlled device access. The valid concern was that by allowing untrustworthy devices to connect to a local area network, the result might be immediate and

comprehensive lateral propagation of malware to all other connected devices and systems. This approach, memorialized in standards such as IEEE 802.11, had immediate challenges, including the practical problem of PC scanning taking much longer to complete than any user would be reasonably expected to wait for network entry. More recently, with the dissolution of the perimeter, and the advance of cloud-based mobile device usage, the NAC challenge has shifted to the virtual hybrid cloud infrastructure. That is, the desire remains that devices cannot introduce malware to the virtualized organizational network. For this reason, basic entry and admission conditions continue to be an important requirement.

General Outlook

The general outlook for network access control involves transition from more manual detection and quarantine functions to highly automated capabilities that perform similar functions more rapidly and efficiently. Traditional LAN-based NAC for PCs using hardware-based controls will shift toward virtualized, hybrid cloud access with support for PCs, tablets, mobiles, and other devices. First generation NAC from 1998 to 2007 was characterized by simple PC policy controls to detect basic patching and vulnerability conditions before entry would be permitted. Many failed projects ensued because the NAC goal was so clear, but implementation was so much more complex. Some organizations even tried to provide NAC using inventories of media access control (MAC) addresses, but this approach never caught on more generally. Second generation NAC involved improved policy controls with self-assisted remediation in quarantines. NAC solutions began to recognize the shift to cloud and increased use of mobile devices in the enterprise. Third generation NAC, starting in 2016 and evolving to 2025, will experience a total dissolution from the enterprise, and an almost total virtualization to cloud. Quarantines will benefit from the virtualization, and simpler cloud workloads will be easier to analyze from an integrity perspective. The shift to cloud will bring all hardware-based NAC solutions for physical LANs to a close, but will open many new opportunities for virtualized NAC controls, including dynamically created quarantines that can learn the situation and adjust processing to its unique characteristics.

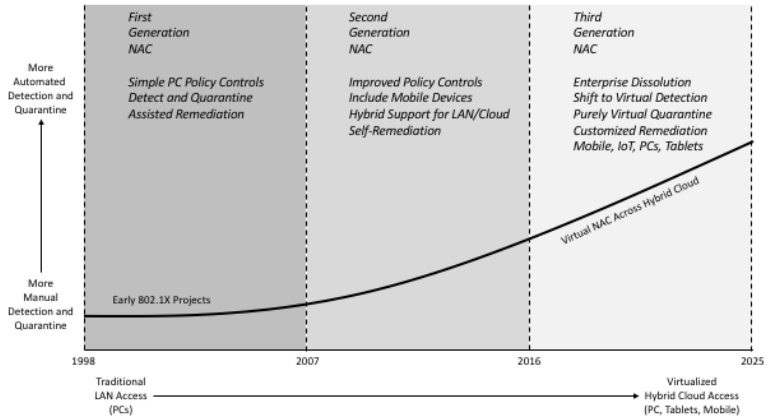

Figure 4. 2018 Network Access Control Outlook

The TAG Cyber degree of confidence in this predictive outlook is moderately high, with the only hesitation here being the unpredictable nature of the cloud marketplace. NAC-like capabilities might become embedded into the identity and access management for cloud services, which would result in a greatly reduced opportunities for pure virtual NAC solutions. NAC technology has been tough for analysts to call in the past, so this one remains a bit uncertain.

Advice for Enterprise Security Teams

Enterprise security teams are advised to follow two paths in the coming years: First, they must not neglect the importance of NAC-based policy enforcement for unmanaged devices if they continue to operate a perimeter-based local area network. It would be easy to forget that amidst all the talk about cloud services, day-to-day enterprise network security must continue to operate. Second, they must also begin to plan for new implementations of NAC policy in the presence of virtualization and distributed XaaS usage. Discussions with NAC vendors should always include discussion of this rapidly approaching reality.

Advice for Security Technology Vendors

NAC security technology vendors should recognize that their existing local area network-based hardware solutions will not be viable for more than a few additional years. This is not bad news, because the intensity of NAC policy will not only remain in the enterprise, but with hybrid cloud, NAC objectives might intensify. This will require that product solutions adjust to the new architecture, perhaps with closer relationships formed with mobile security, cloud security, and remote access solution providers.

List of Support Vendors

Aruba Networks – Aruba Networks, now part of HP, provides the ClearPass Policy Manager NAC solution for the enterprise.
Auconet – San Francisco-based Auconet includes a network access control solution for enterprise customers.
Avaya –Telecommunications vendor Avaya provides a range of network access control solutions for the enterprise.
Bradford Networks – Bradford Networks provides a NAC solution for the enterprise called Network Sentry/NAC.
Cisco – Cisco embeds NAC functionality into its LAN solutions for enterprise via the Cisco NAC Appliance.
Endian – The Italian firewall and IPS vendor includes NAC solutions as part of its enterprise offering.
Extreme Networks – Extreme Networks offers NAC as part of its networking and security product.
ForeScout – California-based ForeScout provides a NAC solution called ForeScout CounterACT for the enterprise.
Great Bay Software – Great Bay Software provides a range of network access control solutions for enterprise.
Impulse – Impulse provides the SafeConnect network access control solution for the enterprise.
InfoExpress – InfoExpress provides a unique peer-to-peer network access control solution for mobile devices and laptops.
Juniper – Juniper embeds NAC into its EX Series Ethernet Switch product.
Macmon – The small company, headquartered in Berlin, provides full IEEE 802.1x NAC solutions.
PacketFence – PacketFence provides a network access control solution for its enterprise customers.
Portnox – The Israeli company provides its Portnox NAC network access control solution for the enterprise.
Pulse Secure – Pulse Secure is a spin-ff of Juniper and provides a mobility and BYOD-supporting NAC solution for enterprise.
SnoopWall – SnoopWall acquired the NetBeat network access control solution for the enterprise from Hexis in 2014.
StillSecure – StillSecure provides the Safe Access network access control solution for the enterprise.
TrustWave – Security service provider TrustWave provides a managed network access control solution for the enterprise.
United Security Providers –The Swiss company offers a variety of network access control solutions.
ViaScope – Located in South Korea, ViaScope offers integrated IP address management, DHCP, and NAC solutions.

Control 5: Unified Threat Management

Unified Threat Management (UTM) integrates common security gateways functions such as firewall, intrusion detection and prevention, data leakage prevention, and antivirus filtering into a common appliance product. Small and mid-sized business (SMB) organizations have tended to prefer the use of UTM solutions because of their management convenience and relatively low cost. Some UTM solutions offer more fine-grained user-level identity-based protection than the less effective source IP address-based granularity of a traditional five-tuple firewall. An additional advantage of UTM solutions is that they support a wide range of comprehensive visibility, auditing, reporting requirements, as regulatory creep continues to drive additional security compliance obligations down into SMB organizations.

General Outlook

The general outlook for unified threat management involves transition from uneven deployment and coverage across SMB organizations to much more comprehensive deployment and coverage, although in a more virtualized manner. A corresponding trend, however, is that these SMB buyers will be moving their centralized enterprise LANs to more distributed hybrid cloud set-ups, which will require considerable adjustment to the packaging, installation, design, and operation of UTM solutions. First generation UTMs from 1998 to 2007 involved basic hardware-oriented, integrated gateway functionality that saved rack space and power. Second generation UTM solutions from 2007 to 2016 continued to add integrated options to the hardware appliance, and continued to be an excellent maintenance and low cost options for many groups. Third generation UTM, from 2016 to 2015, will experience dramatic changes – perhaps as much as any cyber security solution on the marketplace. SMB organizations are embracing cloud faster than any other buying segment – hence, they will have less need for UTM gateway hardware, but much more need for integrated security functionality to support perimeter-less, software-based hybrid cloud architectures.

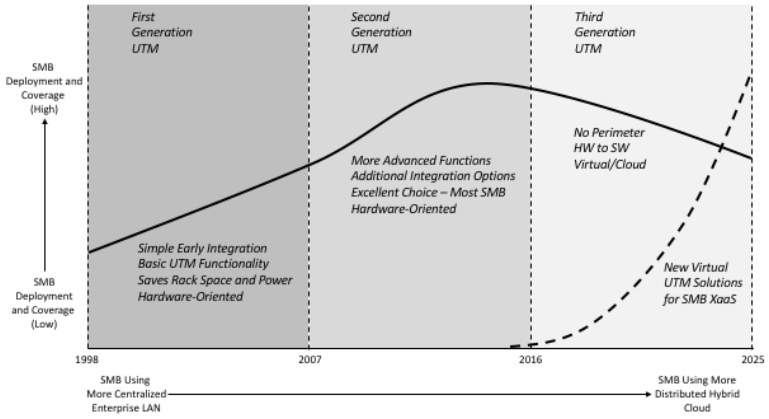

Figure 5. 2018 Unified Threat Management Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since evidence of SMB adoption in cloud is clear and significant. Since so many different security solution providers

have their eye on this space, however, it is not clear that all UTM solution providers will proactively adjust their strategy to deal with the new SMB arrangement.

Advice for Enterprise Security Teams

Enterprise security teams, especially in SMB markets, who enjoy their existing UTM should work with their vendor to identify a cloud strategy. Virtualizing an existing UTM is harder than it sounds, simply because UTM hardware platforms were designed to bring many functions together into a single, physical point. Distributed cloud virtualization, in contrast, is designed to do just the opposite. UTM users and buyers should thus consider options in adjacent markets such as cloud access security broker (CASB).

Advice for Security Technology Vendors

Unified threat management security technology vendors should recognize that the SMB market has already shifted dramatically to cloud. Any UTM vendor that has not already proactively adjusted its strategy to deal with this shift is probably too late to make sufficient changes now. Certainly, a physical appliance-based enterprise gateway market will remain for some users, and UTM vendors might have the option of charging premiums, as is often seen for stubborn users of legacy technology. But the real growth will come in cloud – and that is not up for much reasonable debate.

List of Support Vendors

Barracuda Networks – Barracuda Networks provides its X-series UTM solution as part of its firewall product portfolio.
Calyptix Security – Calyptix Security offers a unified threat management solution focused on small and medium sized business.
Check Point Software – Check Point includes a mature and advanced UTM product offering.
Cisco – Cisco offers all-in-one UTM security solution for SMB desiring simple management with accurate threat intelligence.
Dell – Dell includes a unified threat management offering for its customers under their SonicWall brand.
Endian – Endian offers an open source, unified threat management solution with firewall and IoT security.
Fortinet – Fortinet includes an extensive range of firewall and gateway security solutions in their UTM offering.
gateprotect – gateprotect is a German company that offers unified threat management and next-generation firewall solutions.
GuardSite – GuardSite provides UTM, SSL-VPN, and firewall solutions under the WatchGuard brand.
Juniper – Juniper's SRX series is among the highest rated UTM solutions for capacity and throughput.
Kerio – The company, part of the GFI Software family, offers its Kerio Control NG Series UTM solution for enterprise.
NetPilot – NetPilot is a UK-based company offering a UTM solution with content filtering and secure cloud connectivity.
MyDigitalShield – MDS is a security-as-a-service provider with a unified threat management offering.
SecPoint – Located in Denmark, SecPoint offers a cloud protector UTM solution for enterprise.
Sophos – Sophos markets a UTM solution for small and medium sized business based on Cyberoam acquisition.
Topsec Science – Topsec Science is a Chinese company offering a range of information security solutions including UTM.
TrustWave – TrustWave includes unified threat management in its comprehensive solution offerings.
VenusTech – Beijing-based company, VenusTech, offers network security solutions including UTM.
WatchGuard – WatchGuard provides a UTM appliance including anti-Spam, malware detection, and intrusion prevention.

Control 6: Web Application Firewall

Web application firewall (WAF) solutions protect HTTP applications from cyber attacks including well-known methods such as SQL injection and cross-site scripting, as well as new zero-day exploits that might generate more subtle indicators. WAF tools typically protect servers in a familiar reverse-proxy arrangement. As the security industry has progressed in recent years, WAFs operate adjacent to similar functions including intrusion detection and prevention tools

and web security tools. WAFs, to date, have been primarily packaged as hardware appliances or server plugins, but the goal to virtualize into cloud operating systems is increasing. WAFs require an understanding of the applications being protected, and this can result in tailoring for the specific application protocol being used.

General Outlook

The general outlook for web application firewalls involves transition from hardware appliances to virtualized cloud capabilities. Since WAFs operate at the application layer, they are more intimately connected to the associated software development lifecycle. Correspondingly, WAFs have had to adjust from more traditional software lifecycles with less frequent changes to more modern Dev/Ops lifecycles which involve frequent application changes, sometimes on a daily or even hourly basis. First generation WAFs from 1998 to 2007 involved hardware appliances that were designed to handle common attacks based on a small set of signatures. Second generation WAFs from 2007 to 2016 were characterized by an improved set of attack signatures, including some zero-day exploit detection. During this period, WAFs experienced the first hybrid cloud applications requiring protection, which changed how the WAF reverse proxies had to be deployed. Third-generation WAFs from 2016 to 2025 should expect to see a much larger set of signatures and behavioral processing solutions. The transition to hybrid cloud will require WAFs to virtualize into cloud or SDN infrastructure. The complete adoption of Dev/Ops will result in WAF developers and maintainers to have to deal with high rates of application changes.

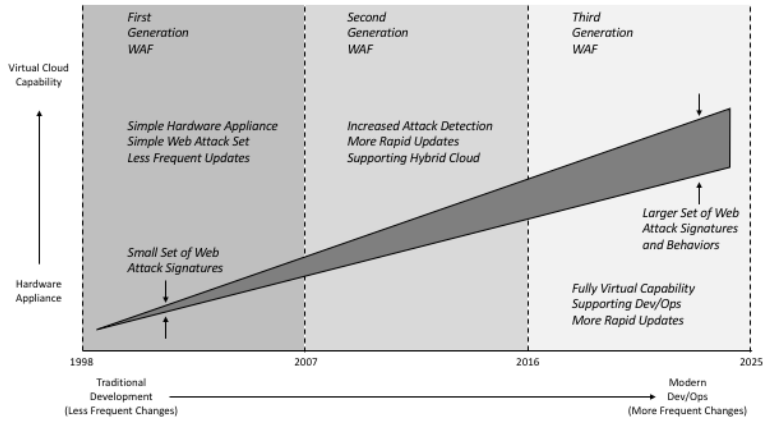

Figure 6. 2018 Web Application Firewall Outlook

The TAG Cyber degree of confidence in this predictive outlook is moderately high, based on a clear momentum view, but slightly couched by the less predictable nature of software application evolution. The adjacency of so many comparable security solutions will also put pressure on WAFs to differentiate their value, versus similar functions in related products.

Advice for Enterprise Security Teams

Enterprise security teams are advised to work with their existing or planned WAF vendor to discuss how application-specific protections might evolve with inevitable changes in how applications will be delivered to the enterprise in the next few years. Support for data center virtualization, cloud hosting, and mobile device access must be central to the planning discussion. A challenge for security teams is that HTTP protection capability will be available in so many more products than previously. CASB, micro-segmented security, distributed firewalls, and other tools will include web security protocol solutions.

Advice for Security Technology Vendors

WAF security technology vendors should recognize that the traditional arrangement of placing a WAF appliance in the reverse-proxy stream for enterprise applications will give way to cloud-hosted applications accessed via bring-your-own-device (BYOD) mobiles. Perhaps more importantly, however, WAF solutions will require support for rapid Dev/Ops changes to applications at a frequency previously considered impossible. This will require that vendors integrate their tool with Dev/Ops lifecycle management capabilities such as configuration and version control tools.

List of Support Vendors

Ad Novum – Switzerland-based Ad Novum provides nevisProxy reverse proxy and WAF solutions.
Akamai – Akamai offers its customers the Kona web application firewall, which provides always on, scalable protection.
Alert Logic – Alert Logic offers customers a managed Security-as-a-Service web application firewall.
Applicure – Applicure offers customers the dotDefender enterprise-class web application firewall solution.
A10 Networks – San Jose-based A10 Networks provides its Thunder TPD web application security product line.
BAE Systems – Through their acquisition of SilverSky, BAE provides a WAF solution as part of its cloud security services.
Barracuda Networks – Barracuda Networks offers WAF product solutions for small, medium, and large-scale applications.
Bee Ware – Bee Ware makes web application security solutions for customers on Amazon Web Services.
BinarySEC – BinarySEC offers the EasyWAF web application firewall solution for protection, acceleration, and statistics.
Brocade – The technology company from San Jose offers Brocade Virtual web application firewall solution.
Citrix – The well-known cloud virtualization company offers its Citrix NetScaler AppFirewall solution for customers.
CloudFlare – CloudFlare's wWAF includes features such as a strong default rule set and customized Layer 7 defense.
ControlScan – ControlScan includes a WAF solution as part of its MSS and DDOS security services for SMBs.
DBAPP Security – Web application security firm DBAPP Security offers customers the DAS-WAF solution.
Dell – Dell provides its extensive customer base an advanced web application firewall called SonicWall.
DenyAll – DenyAll is a French security vendor offering a WAF appliance as part of its next-generation web security solutions.
Ergon – Swiss company, Ergon, provides customers with an enterprise web security solution called Airlock WAF.
F5 – F5 provides its BIG-IP family of solutions including a WAF designed for white and black listing.
5nine Software – The small company offers the 5nine WAF with Microsoft server integration and support for Hyper-V.
Fortinet – As part of its product line, Fortinet offers enterprise customers the FortiWeb WAF solution.
Forum Systems – Forum Systems provides an API gateway across web applications, services, and infrastructure.
Imperva – Imperva offers customers a range of advanced web application firewall solutions including SecureSphere.
KEMP Technologies – KEMP integrates web application firewall functions with load balancing offers.
NinjaFirewall – Embedded in WordPress and applicable to PHP, the Ninja Firewall is essentially a web application firewall.
NSFOCUS – NSFOCUS offers a WAF with coordinated blacklist and whitelist capabilities as part of its DDOS security offering.
Penta Security – Korean firm, Penta Security, offers a web application firewall product called WAPPLES.
Port80 Software – Port80 Software includes the ServerDefender VP host-based web application security solution.
Positive Technologies – Positive Technologies focuses on retail POS and includes security and WAF capabilities for its customers.
PrivacyWare – PrivacyWare offers web application firewall and intrusion prevention software for Microsoft IIS.
Qrator Labs – Qrator Labs is a Russian firm that provides the Wallarm WAF solutions over the Qrator.
Qualys – The well-known cyber security company Qualys includes a next-generation cloud-based WAF solution.
Radware – Tech firm, Radware, offers enterprise customers the AppWall web application firewall.
Riverbed – Riverbed provides tools for web caching and optimization of traffic with WAF capability embedded.
Shaka Technologies – Shaka Technologies includes the Ishlangu web application firewall product.
SiteLock – Arizona-based SiteLock offers enterprise its customers the TrueShield web application firewall.

Sophos – Sophos includes enterprise WAF solutions as part of the Cyberoam and Astaro acquisitions.
Sucuri – The small company located in Delaware provides its CloudProxy web application firewall solution.
Sungard – Sungard includes managed web application firewall solutions as part of its availability services for business.
Symantec – Symantec includes web application firewall capability as an integrated component of its suite of offerings.
TrustWave – TrustWave provides a web application firewall appliance for real time continuous security protection.
United Security Providers – United Security Providers includes the USP Secure Entry Server for web security.
Wallarm – Located in Russia, Wallarm offers a web application solution for defending web front-ends and APIs.
Zscaler – The web security firm includes cloud-based next-generation firewall capability including WAF.
Zenedge – Zenedge markets a WAF capability embedded in the ZenEdge DDOS protection solution.

Control 7: Web Fraud Prevention

Web Fraud Prevention involves security techniques that reduce the risk of online account exploitation once the user credentials for an account have been stolen. In such cases, authentication is no longer relevant, so advanced behavioral methods must be used to determine if a malicious fraudster has control of an account and is attempting to commit theft. Some web fraud prevention methods try to proactively avoid malicious activity, whereas others try to minimize losses after the fraud has already commenced. Most products in this area rely on heuristics as hints, such as unusual web page traversal, that fraud is underway. This is a powerful technique, because it combines observational techniques with experience-based heuristics for how websites are usually attacked by fraudsters.

General Outlook

The general outlook for web fraud prevention involves transition from reactive signatures for simple eCommerce to more preventive solutions based on diverse, behavioral attributes. Web fraud prevention platforms are also moving from centralized gateway deployments to distributed set-ups across hybrid cloud architecture. First generation web fraud prevention solutions from 1998 to 2007 involved focus on simple account takeover for eCommerce websites. Second generation web fraud prevention from 2007 to 2016 involved more end-to-end focus, including early behavioral analysis, for a wider range of sites including banking. Third generation web fraud prevention from 2016 to 2025 should expect more support for virtualized account usage, with advanced analytics and more proactive focus on preventing takeover fraud before it commences.

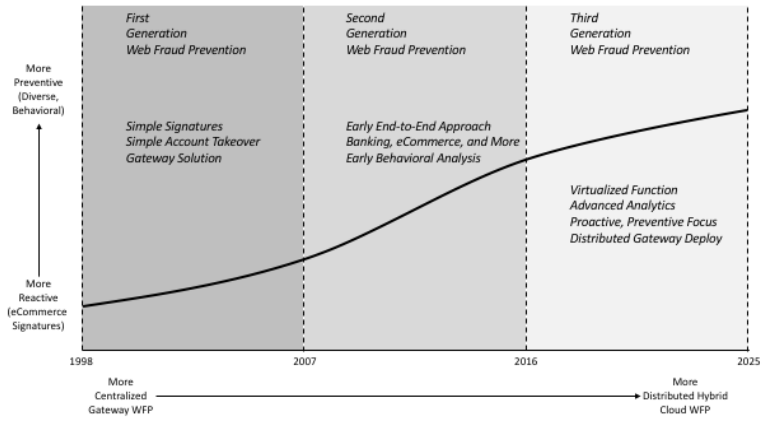

Figure 7. 2018 Web Fraud Prevention Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, given the clear momentum views of how fraud has progressed for online websites. The wild card is that fraudsters have always been amongst the most clever and difficult to predict group of malicious actors, so third generation predictions must take this into account.

Advice for Enterprise Security Teams

Enterprise security teams are advised to ensure that any online systems that might be targeted for account takeover have sufficient web fraud prevention coverage. This is an area that has been commonly neglected by enterprise security teams who have often been poorly integrated with company eCommerce and related digital objectives. This functionality should be a requirement for XaaS applications that might be susceptible to fraud, so contracts for cloud application hosting providers should be designed accordingly.

Advice for Security Technology Vendors

Web fraud prevention security technology vendors should recognize that enterprise security teams have not typically considered this functionality as a primary component in their solution space. This complicates the sales process since year-over-year planning budget may not be available for web fraud prevention. Vendors would be wise to target the application virtualization process to cloud as a vehicle for defining security team buying habits in this area.

List of Support Vendors

Accertify – Accertify is a provider of fraud prevention, chargeback management, and payment gateway products and services.
Agari – Agari's DMARC protections are an important component of reducing fraud across email and domain usage.
Agilence – New Jersey-based Agilence provides exception-based reporting for retail payment fraud prevention.
Caveon – Caveon offers digital forensics and security audit services to prevent test fraud in schools.
CyberSource – CyberSource offers online payment fraud management across multiple channels and devices.
Cyxtera – Through its legacy Easy Solutions, Cyxtera offers an end-to-end total solution for dealing with web fraud.
Feedzai – The machine learning platform from Feedzai focuses on fraud and risk from a cloud-hosted or on-site deployment.
F5 – The F5 Web Fraud Protection solution detects potential fraudulent activity and secures transactions.
Forter – New York-based Forter provides so-called frictionless fraud prevention for online retail systems.
41st Parameter – The company, now part of Experian, offers global fraud management solutions for financial institutions
First Cyber Security – The company offers independent verification of website authenticity to reduce fraud risk.

FraudCracker – FraudCracker provides a platform for reducing fraud risk through anonymous employee reporting.
Guardian Analytics – Guardian Analytics provides behavior-based fraud detection software and services.
IBM – IBM offers the IBM Security Trusteer fraud prevention solution for advanced malware and on-line fraud detection.
iovation – The company offers device-based solutions for authentication and fraud prevention.
Imperva – The company offers threat intelligence and fraud prevention as part of its Web application security solution.
Intellinx – Intellinx supports enterprise fraud management through data collection and analysis.
Kaspersky – Kaspersky Fraud Prevention for Endpoint (KES) is designed to prevent security incidents and fraudulent activity.
Kount – Kount is an Idaho-based firm that provides anti-fraud solutions for e-commerce merchants.
MaxMind – MaxMind offers IP intelligence and online fraud prevention tools that leverage Geolocation.
MicroFocus – MicroFocus offers a range of enterprise security products including fraud and misuse management.
Network Kinetix – Network Kinetix offers business assurance and anti-fraud solutions for carriers to improve revenue assurance.
NoFraud – NoFraud provides e-commerce risk management through transaction analysis to determine pass and fail decisions.
NuData – Canadian firm NuData offers a behavioral analytics platform for reducing the risk of on-line fraud.
Pindrop Security – Pindrop Security provides solutions for detecting ad preventing phone scams and fraud in call centers.
RSA – The well know security firm offers web fraud prevention through an appliance solution.
Signifyd – The company focuses on e-commerce fraud prevention and chargeback.
ThreatMetrix – ThreatMetrix refers to itself as a Digital Identity Company, which emphasizes the important role of identity.
Trustev – The company, part of TransUnion, offers on-line fraud prevention based on contextual pattern matching.
VU Security – VU Security focuses on intelligent transaction analysis for behavior-based fraud detection.
Webroot – Internet security firm Webroot provides advanced online fraud prevention for PCs and mobile devices.
Whiteops – Whiteops provides a solution for preventing botnet fraud in on-line advertising.

Control 8: Web Security Gateway

Web Security Gateway solutions protect an enterprise from malware that might originate on an infected or compromised website. This is typically accomplished using forward proxies that protect endpoints, reverse proxies that protect servers, and threat feeds that provide up-to-date lists of URLs for filtering. Increasingly, web security gateways focus on application-specific controls to reduce security threats. Web security gateways are also involved in the enforcement of acceptable-use policies for enterprise employee browsing. Performance issues have traditionally been a concern when web security gateways are deployed, which helps explain why many of the more successful vendors trace their involvement in this area to web acceleration solutions. It is worth mentioning that web security gateways represent one of the first protection solutions where a live threat feed is used by enterprise teams to accepts and allow remote reconfiguration of a device. While this is generally low risk for URL feeds, this is nevertheless a profound shift from localized control of all reconfigurations toward acceptance of live updates from trusted partners.

General Outlook

The general outlook for web security gateways involves transition from more signature-based URL lists as the basis for proxy functionality to an increasing reliance on behavioral profiles to detect potential malware downloads from infected sites. Web security gateways are moving from centralized hardware appliance deployments to more distributed, hybrid cloud proxy software. First generation web security gateways from 1998 to 2007 involved simple URL proxies implemented as hardware with feed updates from the vendor. Second generation web security gateways from 2007 to 2016 include improved cloud-based threat intelligence from vendors with early attention to expanded anti-malware capability using advanced algorithms. Third generation web security gateways from 2016 to 2025 will be fully virtualized with

advanced analytics and support for distributed gateways across cloud infrastructure. One should expect their associated threat feeds to improve in the coming generation as well.

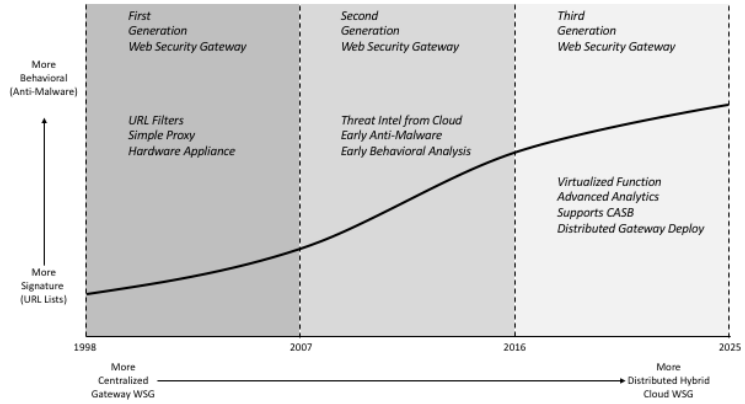

Figure 8. 2018 Web Security Gateway Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, given the fact that virtualization has already been a major factor in web security gateway design. Collision with other security solutions in cloud will produce challenges for vendors in this area.

Advice for Enterprise Security Teams

Enterprise security teams are advised to work with their existing proxy vendor on a plan to cover the inevitable progression to hybrid and full cloud architectures. The challenge will be determining how to deal with the collision that occurs with related cloud security functions such as CASB which are offered separately or as an integrated protection from the cloud application vendor. Traditional web security gateway solution providers have the advantage of the best available URL feeds with mature infrastructure for delivery and update. Enterprise teams should not delay analysis here, as cloud protections will fundamentally shift the required proxy arrangement from gateway appliances to software running on cloud operating systems.

Advice for Security Technology Vendors

Web security gateway technology vendors should recognize that any hardware acceleration or appliance performance advantages will dissolve quickly with the dissolution of the perimeter. The most successful web security gateway vendors will fully embrace distributed virtualization, even using that arrangement to improve the vantage point for detecting web infections and malware. The most successful web security gateway providers will also continue to improve their URL lists into comprehensive, world-class threat feeds for enterprise customers. For some buyers, the threat feeds might be as valuable as the platform.

List of Support Vendors

Acunetix – Vulnerability management company Acunetix includes advanced solutions for website security.
Banff Cyber – Singapore-based Banff Cyber focuses on prevention of web defacement in their products.
Barracuda Networks – The company offers the Barracuda Web Filter, which is a comprehensive web security gateway.
BeyondTrust – BeyondTrust includes the Retina Web Security Scanner for protection of web applications.

BinarySEC – The French company provides a managed security solution for reducing the risk of website attacks.
Bloxx – The Bloxx Secure Web Gateway, now part of Akamai, focuses on so-called *zero-second* protection for users.
CA Technologies – CA offers the Web Services Security platform (formerly CA SiteMinder Web Services Security).
Celestix – The CelestixEdge platform includes a range of advanced web application proxy capabilities.
Check Point Software – The company includes web security in its portfolio of cyber security products and services.
Cisco – Cisco's Web Security Appliance, Cloud Web Security, and Cloud Access Security support web security protection.
Clearswift – Now part of RUAG, the UK-based Clearswift SECURE Web Gateway focuses on Internet communications.
CloudFlare – CloudFlare, based in San Francisco, provides acceleration, domain, and security services for websites.
ContentKeeper – ContentKeeper, headquartered in Australia, provides web threat protection and web filtering.
CronLab –United Kingdom-based CronLab provides an Integrated Web Filter solution for business customers.
DeepNines – The Dallas-based company provides a unified security gateway solution for enterprise.
Distil – Located in Arlington, the company protects websites from botnet attacks and data mining.
EdgeWave – EdgeWave provides cloud-based remote web filtering services via an appliance solution.
FireEye – FireEye offers an industry-leading web and network security solution for detecting and preventing APT attacks.
Fireglass – Now part of Symantec, the company offers browser isolation technology to stop advanced malware.
First Cyber Security – The UK firm includes web security in its portfolio of anti-fraud and cyber security solutions.
Forcepoint – Forcepoint offers an integrated portfolio of web security solutions.
Fortinet – Fortinet includes web security gateway functionality in its extensive security product line.
GFI Software – Located in Luxembourg, GFI's WebMonitor product helps control web activity and avoid web-based threats.
iboss – The iboss Cloud Secure Web Gateway Platform offers a range of web security capabilities.
Imperium – Now part of Google, the group provides automated tools for removing malware from websites.
Imperva – Imperva includes a range of web security protections in its WAF and DDOS offerings for enterprise customers.
Ingenico – Ingenico offers an XML-based cryptographic hardware security module for Web applications.
Litous – Located in Iceland, Litous provides a range of web security products including the Malware Spider.
McAfee – Industry-leading McAfee offers customers the McAfee Web Gateway solution for analyzing web traffic.
Menlo Security – The start-up led by Amir Ben-Efraim includes web security in its unique isolation technology.
Netsparker – Netsparker, located in the UK, offers a Web application and vulnerability scanning solution.
Optenet – Optenet, now part of Allot Communications, provides customers with its multi-tenant Secure Web Gateway product.
Panda Security – Headquartered in Spain, Panda Security offers the GateDefender solution for web browsing security.
Penta Security – Located in Seoul, Penta offers its customers web security capabilities in its offerings.
Port80 Software – The San Diego-based company provides web security in its range of WAF and application security solutions.
PortSwigger – PortSwigger markets a range of testing tools and solutions for web application security.
Sangfor – Sangfor provides its advanced Internet Access Management gateway for securing web traffic.
Shaka Technologies – The UK firm includes web security in its load balancing, acceleration, and related functions.
Shape Security – Shape Security provides protection of web content from automated attacks such as botnets.
SiteLock – Located in Florida, SiteLock provides WAF and web security capabilities for customers.
Smoothwall – Originating in the UK, Smoothwall provides content-aware web security filtering and gateway functions.
Sophos – The Sophos Cloud Web Gateway offers secure web gateway functionality for enterprise.
Spikes Security – Los Gatos-based Spikes Security, now part of Aurionpro includes web security in its isolation technology.
Sucuri – Sucuri offers a range of web security capabilities to complement its WAF and DDOS protections.
Symantec – The Symantec Web Gateway offers content filtering and related data loss protections.
Tinfoil Security – Tinfoil Security provides both web security and vulnerability management solutions.
Total Defense – The company merged with Untangle to provide security for Internet browsing and application protection.
Trend Micro – The Trend Micro InterScan Web Security Virtual Appliance provides web security functionality.
Trusted Knight – Trusted Knight, through its acquisition of Sentrix, offers web security through its Infinite solution.
TrustWave – TrustWave includes web security gateway functionality tracing back to its M86 Security acquisition in 2012.
Webroot – The California-based company includes web security in its portfolio of endpoint and Internet security solutions.
WebTitan – The company offers the WebTitan Gateway, which includes content filtering and related security controls.
WhiteHat Security – The Santa Clara-based firm provides WhiteHat Sentinel for continuous security assessment of websites.
Zscaler – Well-known security firm Zscaler offers cloud-based web security gateways across its global infrastructure.

Control 9: CA/PKI Solutions

Certification Authority/Public Key Infrastructure (CA/PKI) Solutions consist of infrastructure-level controls based on public key cryptography that support strong authentication, encryption,

and integrity requirements using data structures known as public key certificates. Public key technology has been in existence for many decades, and has never realized its original promise as a direct revenue producer. Instead, public key technology has assumed a background role helping to secure various elements of personal, enterprise, website, network, and Internet infrastructure. The coverage has been spotty to date, with, for example, strong support for website security via the secure sockets layer (SSL) protocol, but weak support across organizational domains for email. The most substantive categories (not a complete list) of present and future CA/PKI business solutions are as follows:

- *CA/PKI Support for Websites* – Running https on your website requires that you obtain and use a certificate from a CA, and this is often your web hosting provider, especially if you run a small, modest site requiring low assurance.
- *CA/PKI Support for Networks* – Operating most network equipment such as routers at the infrastructure level requires the use of certificates for secure usage, and the attendant tasks such as key management are often done directly using tools from the equipment vendor.
- *CA/PKI Support for Authentication* – Certificates can be issued and used to identify devices, such as mobiles, often as a second or third factor, with handling supported by IT systems such as mobile device management (MDM).
- *Protection of Keys and Certificates* – Some select cyber security companies offer customers advanced protection solutions for managing and securing the keys and certificates that underlie CA/PKI offerings.
- *Future CA/PKI Support for IoT* – As computing moves to more automated interactions in the IoT, industrial control, machine-to-machine (M2M), and operations technology (OT) realms, CA/PKI solutions should play a vital, growing role.

As future applications move to IoT, M2M, and OT/IT orientation, the security support of CA/PKI solutions will be a good match. This may represent the direct revenue opportunity that companies in this area have been searching for during the past decades – but the jury is still out.

General Outlook

The general outlook for CA/PKI solutions involves transition from ad hoc operations and assurance (ranging from low to high) to much more systematic and improved operations and assurance, where more users pay attention to the assurance model driving CA operations. This will be true because more engineers will drive CA decisions for IoT and M2M versus browser users checking assurance levels before visiting an eCommerce site. First-generation CA/PKI from 1998 to 2007 involved the simplest support for SSL running on browsers and websites with poor attention to assurance models for binding public keys to certificates. Second generation CA/PKI from 2007 to 2016 included more applications for CA/PKI including use in mobile authentication with MDM. An explosion of CAs emerged during this period with users often confused about which ones are acceptable (most smaller site owners opted to just work with their service provider). Third-generation CA/PKI solutions from 2016 to 2025 should expect to see dramatic expansion to mobile and IoT, with more emphasis on assurance and protection

of keys and certificates. During this generation, the gradual increase in application options for CA/PKI will become clearer, as CA/PKI supports a truly varied mix of user and infrastructure applications across the Internet, critical infrastructure, enterprise, and personal/home use environment.

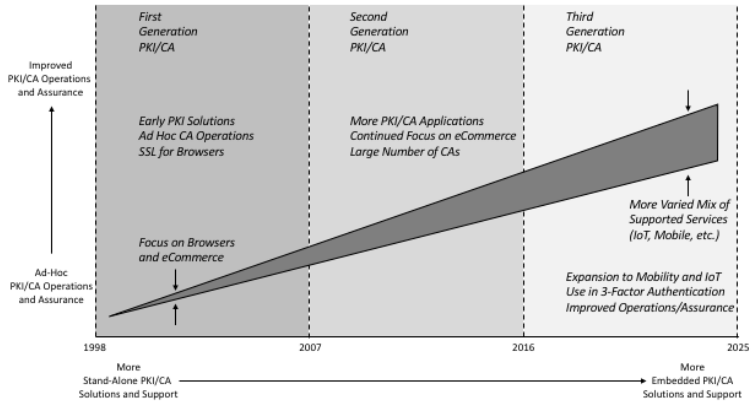

Figure 9. 2018 CA/PKI Solutions Outlook

The TAG Cyber degree of confidence in this predictive outlook is moderate, only because predicting CA/PKI technology and usage trends has been so hazardous (and mostly wrong) in the past. Our predictions are thus offered with the full recognition that virtually no pundit, observer, or analyst has been reliably correct about PKI for decades. We hope to be the first here.

Advice for Enterprise Security Teams
Enterprise security teams are advised to reassess their relationship with certification authorities and PKI solutions providers to determine readiness for the shift to cloud services, virtualization, and SDN infrastructure. Team are advised to consolidate their CA/PKI relationships to a high-quality vendor with support for high assurance public key binding procedures. Many companies might be astounded to find that they are buying certificates from multiple (perhaps even dozens) of different CAs. This is a bad approach given the fundamental role CA/PKI will play in IoT and other M2M applications. Now is the time to select good partners – and to not forget that protection of keys and certificates in an important and highly neglected function.

Advice for Security Technology Vendors
Web security gateway technology vendors should recognize that sloppy operational procedures and questionable assurance practices will not be acceptable as fewer buyers (service providers) deal with CA and PKI solution providers for more customers moving to shared IT and cloud services. We believe that excellent prospects lay ahead for the best CA/PKI solution providers, simply because this technology is so well-suited to the technology future that lies on the immediate horizon. Vendors would be well-served to optimize their solutions now, and to revisit customers who might not have purchased solutions in the past. Architectures are changing, so PKI is becoming more highly relevant to the resulting distributed, virtualized

systems. Buyers will thus be likely to select a fresh set of CA and PKI solution partners in the coming years.

List of Support Vendors
ACCV – Agencia de Tecnologia y Certificacion Electronica is a Spanish public entity providing CA/PKI services.
Buypass – Buypass is a European firm that offers certificates to secure electronic communications and other applications.
Camerfirma – Camerfirma provides electronic security services including PKI and authentication across Spain.
Certicom – Now part of Blackberry, Certicom is a Canadian group that owns Elliptic Curve cryptography.
Certified Security Solutions – The professional services firm in Ohio supports projects involving identity, access, and PKI.
CertiPath – Virginia-based CertiPath offers a PKI-based trust framework and set of identity services.
certSIGN – certSIGN is a UTI company providing a range of PKI and certification services in Romania.
Chunghwa Telecom – The Taiwanese company provides public certification authority services for SSL and other applications.
CNNIC – CNNIC is a Chinese CA that had some bumpy interactions with Google and other browser vendors in 2015.
Comodo – Comodo provides a full range of SSL certification solutions for small, medium, and large customers.
Cryptomathic – The French firm specializes in data encryption and CA/PKI technologies and services.
CV Cryptovision – CV Cryptovision is a German company focusing on data encryption and CA/PKI solutions.
Deutsche Telekom – The German telecommunications company offers certification authority and PKI services.
DigiCert – DigiCert provides high assurance, low-priced SSL certificates along with code signing and other PKI services.
E-Güven – Turkey-based E-Güven provides a range of certification authority and PKI-based services.
Entrust Datacard – Entrust provides CA and PKI services supporting ten million identity and payment credentials issues daily.
E-Tugra – Turkey-based E-Tugra is certification authority and PKI solution provider supporting SSL and related services.
Gemalto – Gemalto has expanded its cyber security offerings to include authentication in areas closely connected to PKI.
GeoTrust – GeoTrust provides for online customer security with SSL and code signing certificates.
GlobalSign – GlobalSign offers its customers a full range of personal, SSL, and code signing certificates.
GoDaddy Group – The major domain services and hosting provider issues certificates as part of its service.
Hongkong Post – Hongkong Post issues e-Cert certificates with digital signature support from the Hongkong Post CA.
IdenTrust SSL – IdenTrust SSL, now part of HID Global, provides a range of standard and multi-domain SSL certificates.
Izenpe – Izenpe is a Spanish X.509 certificate authority and PKI services organization owned by the Basque government.
Japanese GPKI – This Japanese Government PKI group provides various certification authority and PKI services.
Logius – Logius is a government service in Netherlands offering CA/PKI support.
Microsec – Microsec is the largest Hungarian certification authority and PKI supplier of electronic signatures.
NetLock – NetLock is a Hungarian solutions provider offering digital signature, SSL, and related PKI services.
Network Solutions – Network Solutions is a Web hosting provider offers certificates as part of its services.
OpenTrust – OpenTrust supports enterprise and citizen trusted identities with CA/PKI-based solutions.
PrimeKey – PrimeKey is a Swedish company that offers open source PKI-based products and services.
QualitySSL – QualitySSL offers customers a full range of high assurance 256-bit encrypted SSL certificates.
Secom Trust – Secom Trust is a Japanese security company offering various certification authority and PKI services.
Qualys – Qualys provides an SSL server test function for public Web servers to increase assurance.
QuoVadis – QuoVadis provides managed PKI services to assist with deployment of digital certificates.
SafeCipher – SafeCipher offers a range of security consulting services including PKI solutions, PCI services, and encryption.
SK ID Solutions AS – The Estonian PKI/CA services company provides Certification Centre services.
StartCom – StartCom is an Israeli firm supporting a range of SSL and related PKI services for the enterprise.
SwissSign – SwissSign is a Swiss company providing customers with certificates and related PKI services.
Symantec – The large cyber security provider offers industry-leading certificates and CA/PKI services including managed PKI.
Thales e-Security – The Thales Group is a French multinational offering security solutions including CA/PKI.
TrustWave – TrustWave offers certificate lifecycle management solutions for enterprise customers.
Turktrust – Turktrust is a Turkish firm in Mozilla's root program supporting e-signature, PKI-related R&D, and SSL applications.
TWCA – TWCA is a Taiwanese firm offering certificate services, SSL, PKI software, and certificate hardware.
Unizeto Technologies – Unizeto technologies is a Polish firm providing certification authority and PKI solutions.
Venafi – Venafi provides a unique set of enterprise cryptographic key and certificate security solutions.
WISeKey – WISeKey supports communications and data security with personal, corporate, and server SSL digital certificates.
WolfSSL – Located in Washington State, WolfSSL offers an embedded SSL library for devices and IoT.

Control 10: Cloud Security

Cloud Security consist of the myriad of emerging security functional, procedural, and policy-based controls required to minimize the risks associated with cloud services used by individuals and enterprise. Businesses require cloud security risk reductions as they transition from perimeter-based networks to hybrid use of as-a-service capabilities in shared cloud infrastructure. Vendor offerings in cloud security play an important role in the overall protection solution for both individuals and enterprise. Specifically designating the precise categories of cloud security is challenging, because virtually all cyber security products and services are being adjusted to this new approach. Threat intelligence and isolated endpoint security, for example, have become intimately connected to cloud for their operation. Nevertheless, we can offer a simple three-element taxonomy to help enterprise security teams differentiate between newly emerging approaches that are designed to protect cloud-resident assets:

- *Virtual Cloud Workload Protections* – Virtual cloud workload protections reside in close logical proximity to the cloud assets being protected. Such an approach includes the familiar microsegment solutions that bind security functions into the cloud operating system or container that supports run-time execution of the cloud applications being protected. Cloud workload protections can include compliance, scanning, firewall, attack detection, and other functions that might be arranged into a run-time gauntlet for cloud applications embedded in a service provider cloud, cloud operating system, or other run-time construct.
- *Cloud Access Security Brokers* – CASB solutions reside in the network path between users and cloud workloads to functionally mediate security policy rules put in place by workload owners. CASBs have the flexibility to house compliance, identity, access, firewall, attack detection, and many other solutions given their vantage point in the network path. Most products have focused their initial efforts, however, on offering network and security visibility to security teams about usage patterns of public cloud from the enterprise perimeter.
- *Software-Defined Network Security* – The transition from physical network services in data centers, LANs, and WANs to their virtualized, software-based equivalent has the effect of essentially turning our landline and mobile network infrastructure into an enormous cloud, with all the attendant advantages and challenges. Security solutions to protecting SDN and associated network function virtualization (NFV) are still in their infancy, but enterprise security teams should be aware of this new protection method. Architecturally, SDN includes a control-level function with an application programming interface for add-on capabilities such as security analytics and identity management to be included natively in the usage paths for technology such as 4G/LTE and emerging 5G mobile networks.
- *Cloud Isolated Security Tasking* – The use of cloud as a means for isolating security tasks from users includes new capabilities such as virtual detonation testing of potential malware in the cloud, or virtual isolation of end-user browsing to prevent dangerous scripts and background site execution from reaching endpoints. These solutions are characterized by their deliberate use of cloud as a functional means to isolate and separate potentially dangerous functionality from protected user assets.

The use of cloud will soon become sufficiently embedded in every individual and enterprise approach to computing that this category of security control will become fully subsumed by other control areas. Reference to cloud security will likely shift into the same category as references to system security or network security. For now, however, we choose to include this as a separate category to highlight the ongoing transition.

General Outlook

The general outlook for cloud security involves transition from zero use of cloud security solutions to high usage across all enterprise hybrid cloud architectures. This follows the growing shift in belief that cloud is no longer a problem, but is rather an important part of the solution to reducing the risk of advanced cyber threats. First generation cloud security from 1998 to 2007 (and the term was barely used in the early part of that period) included some focus on compliance and data encryption for shared IT services. Second generation cloud security from 2007 to 2016 saw the emergence of early CASB and microsegment solutions with greatly improved encryption support and even some service-level agreements (SLAs) from cloud providers in security. While SDN and NFV emerged during this period, associated security applications barely registered for users. Third generation cloud security from 2016 to 2025 should expect to experience massive growth in CASB solutions, microsegment solutions adjacent to the workload, and containerized security for virtual applications. In addition, isolated tasking, especially for browsers will be more common, as well as continued improvement in the practical use of encryption for cloud-stored data. The emergence of SDN and NFV-based security solutions as applications bound to the API of data center and ISP-hosted SDN controllers will become a powerful new option for enterprise security teams who desire flexible security solutions in their mobile networks. Enterprise buyers will become savvier about the specifics of cloud security SLAs, especially in regulated environments where such due diligence will become a stricter requirement. Expect cloud security providers, as well as ISPs offering SDN, to make it easier for buyers to point-and-click on security tools in a virtualized marketplace, thus transforming the security provisioning experience for users and enterprise customers.

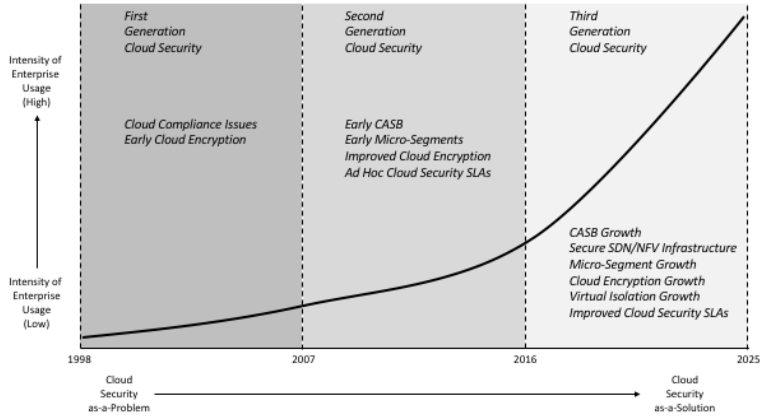

Figure 10. 2018 Cloud Security Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, given the growth that has already occurred in this area, combined with the obvious advantages cloud, SDN, and NFV usage offer CIOs and IT operations teams. Even if you removed all the security advantages of these technologies, the transition to virtualized shared IT and network services would proceed on a purely cost reductive basis.

Advice for Enterprise Security Teams

Enterprise security teams are advised to ensure that they have sufficient team strength focused in this area. While it might be tempting to just assume that all aspects of cyber security are moving to cloud and that everyone must become an expert here, there are clearly specific capabilities such as CASB, microsegments, and SDN that require focused study, learning, testing, and expertise. Enterprise security teams should also be laying the groundwork with executives and board members to help them overcome previously-held beliefs that compliance would be a roadblock in the progression to cloud. This is especially intense for regulated environments, such as banking, where these negative views are still strong. It will be time in 2018 for larger companies who have been testing cloud security in their innovation centers to move this technology to the mainstream with live deployments for production infrastructure.

Advice for Security Technology Vendors

Cloud security vendors should recognize that the competition will be fierce as the previously separate category of "cloud security" begins to collapse into the entire category of "cyber security." Every cyber security vendor in the business has already begun referring to itself as a cloud security provider, so differentiating your solution will only become more challenging. The good news, however, is that as the march to virtualized cloud services accelerates, the overall pie becomes so much larger that slicing it up amongst more vendor participants should still result in substantive growth for everyone offering a reasonable solution. Focus on simplicity, elegance of design, minimization of code, and streamlined deployment via SDN. It will be the simpler tools that are easier to use and understand that should move the front of the pack.

List of Support Vendors

Alert Logic – The Houston-based firm offers security services such as IPS and log management from the cloud via SaaS delivery.
Amazon Web Services – AWS integrates virtualized cloud capability with embedded or overlay virtual security services.
Armor – Rebranded from its original name as FireHost, the company offers secure cloud hosting.
Avanon – Avanon provides cloud access security with DLP, scanning, sanitization, and other features.
Big Switch Networks – Big Switch is an SDN solution provider with support for in-line security services.
Bitglass – Bitglass provides cloud access security broker services to support mobile access to cloud applications.
Blue Data – The small stealth start-up provides a range of secure, big data cloud solutions for enterprise.
Boxcryptor – Boxcryptor, located in Germany, offers encryption software products to secure files stored in public clouds.
Bracket Computing – Bracket focuses on secure information for multiple clouds with embedded security.
Buddha Labs – Buddha Labs is a consulting firm that makes available a pre-hardened secure Amazon Machine Image.
Cyxtera – Cyxtera's Catbird group focuses on cloud security microsegment capabilities with VMware and OpenStack.
Cato Networks – The Israeli firm provides cloud-based secure networking solutions for enterprise.
CipherCloud – CipherCloud, supports enterprise cloud security solutions for monitoring and encryption.
CipherGraph – Cipher Graph, located in California, provides a range of secure, cloud-based VPN access.
Citrix – Citrix is a pioneer in virtual computing, and offers a range platform services including security support for its customers.
Cisco – The company acquired Neohapsis, which offers a range of cloud security and compliance professional services.

CloudLink – Previously Afore Solutions, the Canadian company offers encryption for cloud applications and systems.
CloudLock – CloudLock is a Massachusetts-based company offering cloud access security broker and cyber security-as-a service.
CloudPassage – CloudPassage Halo provides innovative cloud compliance, security visibility, and vulnerability management.
Digital Guardian – The company provides a range of cloud security solutions via its acquisition of Armor 5.
Dome9 – Located in Israel, Dome9 offers a security and compliance solution for public and private cloud services.
Evident.io – Evident.io provides a continuous cyber security platform for Amazon Web Services customers.
F5 – F5 includes cloud security solutions in its extensive range of network and security products and services.
Forum Systems – Forum Systems provides API security management in support of cloud and enterprise systems.
FireLayers – FireLayers, now part of Proofpoint, extends the perimeter to allow access to cloud-resident apps.
5nine Software – The Illinois-based company provides cloud and virtualization management solutions and security applications.
FlawCheck – Now part of Tenable Network Security, FlawCheck offers malware protection for virtual Linux containers.
Fortinet – The company has an extensive range of security products and services including solutions for cloud security.
Forum Systems – Forum Systems provides proxy solutions for cloud storage in its suite of API and cloud gateway products.
GajShield – The Indian firm includes a range of cloud security support with its firewall and DLP offerings.
GuardiCore – Israeli start-up GuardiCore offers real time threat detection and mitigation via SDN.
HyTrust – HyTrust offers a range of cloud and virtual security management solutions for the enterprise.
IBM – IBM supports cloud security requirements through intelligence, access management, and other product features.
Illumio – Illumio, located in Sunnyvale, offers a range of dynamic virtual and cloud workload security protections.
Imperva – Imperva offers cloud broker solutions, and makes SecureSphere available for AWS customers.
IronSDN – The small company offers a unique security functional protection solution for integration with SDN infrastructure.
Juniper – The company has a portfolio of network and security products supporting SDN, cloud, and virtual networking.
Managed Methods – The Boulder-based company offers a range of cloud monitoring and cloud access security solutions.
Microsoft – Microsoft integrates cloud access security brokers services through its Adallom acquisition.
nCrypted Cloud – Located in Massachusetts, nCrypted Cloud supports secure cloud collaboration and secure file sharing.
Nakina Systems – Now part of Nokia, Nakina Sytems provides a suite of network integrity and security solutions for SDN.
Netskope – Netskope provides cloud access security broker services via the Netskope Active Platform.
Netwrix – Located in Irvine, Netwrix offers a range of solutions for auditing hybrid cloud environments.
Palerra – Palerra enables cloud security automation with threat detection and incident response support.
PerfectCloud – PerfectCloud is a Canadian firm supporting a range of security protections for cloud.
Porticor – The small company, now part of Intuit, provides cloud security and data encryption.
PrivateCore – PrivateCore, acquired by Facebook, offers virtual solutions for trusted execution of software in the cloud.
Protectwise – The Denver firm offers cloud security through network capture, forensics, and analysis.
Protegrity – Protegrity provides a range of Big Data and cloud security solutions including encryption.
Rackspace – Rackspace integrates security protections into its suite of cloud computing solutions.
SAP – The German firm includes security and data protection solutions for customers using its products in the cloud.
Seculert – Located in Menlo Park, Seculert provides a virtual, cloud-based platform accessible to enterprise.
SilverSky – Now part of BAE Systems, SilverSky offers a range of advanced cloud security capabilities.
Skyhigh Networks – The Cupertino-based firm offers a solution for security management of cloud access by the enterprise.
Symantec – The security firm includes cloud security solutions in its extensive range of products and services for the enterprise.
Threat Stack – The Boston-based company provides continuous security monitoring for elastic infrastructure.
Trend Micro – Trend Micro offers Secure Cloud to protect data in virtualized cloud environments.
Twistlock – Located in San Francisco, Twistlock offers vulnerability detection and related protections for virtual containers.
vArmour – vArmour's distributed perimeter solution provides an effective means for virtualizing the enterprise edge.
Vaultive – Vaultive provides cloud and SaaS application data encryption solutions via network-level proxy.
Vidder – Vidder provides software defined perimeter security, which can be integrated with cloud architectures.
VMware – VMware offers a cloud platform on which to integrate security solutions.
Zscaler – Zscaler's Web security solutions are well positioned to support security protections of cloud-based computing.
Zentera – The San Jose-based firm offers an overlay virtual network to connect the enterprise to cloud services securely.

Control 11: DDOS Security

Distributed Denial of Service (DDOS) Security consists of the functional and procedural measures required to prevent malicious attacks that utilize voluminous traffic, requests, or data from distributed sources to overwhelm a target's ability to function. Most DDOS attacks involve using malware to transform unwitting computers into so-called bots that are participants in a

botnet controlled by other computers (command and control nodes) that are also unwittingly infected with malware. Human botnet operators control the issuance of commands from the command and control nodes to the bots that result in floods of attack traffic being aimed at a victim. Since DDOS attacks often involve amplification and reflection, protocols and services on the Internet that support both capabilities are often implicated as participants in an attack. Existing protection techniques for securing infrastructure from DDOS attacks fall into the following categories:

- *Network Attack Monitoring* – This involves network-resident platforms that collect data and determine whether attack spikes warrant attention based on determined thresholds established from profiles of normal behavior.
- *Layer 3 Packet Scrubbing* – This is the traditional human-controlled (with automated assistance) diversion of malicious, voluminous traffic to special scrubbing systems that try to filter out bad packets while maintaining session integrity.
- *Layer 7 Application Filtering* – This is the extension of DDOS attack from packet floods to more intense overwhelming of applications via logical usage of the application from what might appear to be a normal user.

In addition to these familiar techniques, DDOS security has also included special group takedowns of botnets, administrative agreement to remove easily amplified services, and other ad hoc measures by volunteers and willing corporate participants. Since DDOS attackers do not follow conventional rules, we should never claim certainty in any predictions about threat, but it seems likely that DDOS attacks will gravitate toward mobility, IoT, virtualization, and cloud. With attack sizes now in the multiple 100 Gbps range, many observers expect to see an attack reach 1 Tbps, most likely from an IoT-infected botnet. ISP peering capacity, which hovers in the 1 Tbps range, will provide a natural ceiling on attack sizes.

General Outlook

The general outlook for DDOS security involves transition from low deployment rates across business to high deployment, as businesses of all sizes gear up to prevent incoming DDOS attacks. With this increased deployment will come the increasing obligation to move from simple attack detection and prevention based on obvious indicators to the mitigation of DDOS attacks with subtle early indicators. First generation DDOS security from 1998 to 2007 involved simple flood defenses using basic guard technology in the single Mbps range. Second generation DDOS security from 2007 to 2016 involved higher volume attack detection, including early layer 7 attacks in the tens to now hundreds of Gbps range. Third generation DDOS security will have to deal with attacks in the Tbps range using advanced mobile and IoT botnets. Security solutions will have to rely on the use of virtualization to expand absorption capability dynamically as application-level attacks progress.

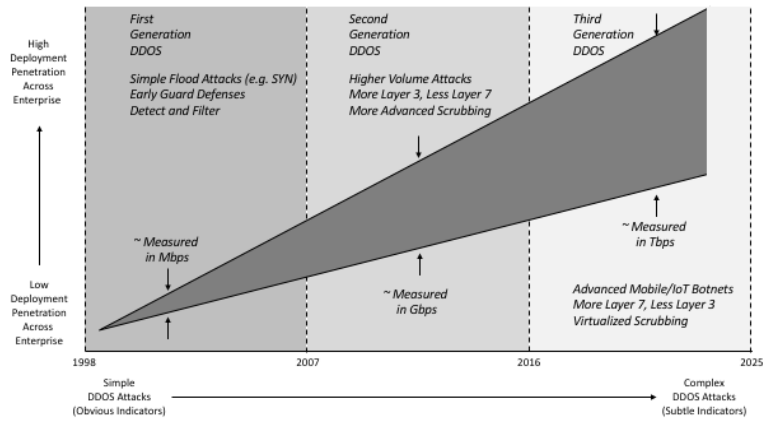

Figure 11. 2018 DDOS Security Outlook

The TAG Cyber degree of confidence in this predictive outlook is moderate, because cyber attack volumes are so hard to predict reliably. We can say with confidence, however, that DDOS attacks are unlikely to go away soon, and that they will get smarter, bigger, and more dangerous in the coming years. Defensive measures will have a hard time keeping up.

Advice for Enterprise Security Teams

Enterprise security teams are advised to take an accurate inventory of their existing DDOS security coverage at both Layer 3 and 7 with their existing service provider or vendor. Most organizations should not be building their own DDOS defenses, but should rather be obtaining advanced services from a provider such as their ISP or MSP. An important question to ask your provider is how they would deal with catastrophic conditions in which multiple major, concurrent attacks to multiple customers would be handled. There are no regulations in any country about maintaining minimum levels of sufficient processing capability in case of disasters. Now is the time to begin discussions with your provider about extending protections into cloud, IoT, and mobile infrastructures. Enterprise teams should also be developing resiliency plans to ensure proper operational mission support in the presence of successful DDOS attacks.

Advice for Security Technology Vendors

DDOS security vendors should be rethinking their future solutions in the context of distributed, virtualized enterprise customers using cloud services. This begs significantly different DDOS protections than the perimeter-protected gateways of the past two decades. Vendors should also recognize that the progression of attack size from botnets from Mbps to Gbps to Tbps will not continue indefinitely (there is no Moore's Law for DDOS attack size from botnets). Instead, vendors should expect to see targeted attacks that focus application-level energy on a victim, rather than a continuance of large DDOS attacks that use volume to overwhelm infrastructure. In addition, IoT-generated DDOS traffic will be one of the largest attack trends in cyber security in the coming years. Vendors with the ability to reduce IoT attack risk will see considerable

success. This might require some domain knowledge for certain types of IoT devices, particularly in the industrial control OT ecosystem.

List of Support Vendors
Akamai – Through its Prolexic acquisition Akamai provides a carrier-independent DDOS filtering service for enterprise.
Arbor Networks – Arbor Networks, acquired by NetScout, provides an advanced DDOS detection and mitigation platform.
A10 Networks – San Jose-based A10 Networks is an application delivery network provider, which includes DDOS services.
AT&T – AT&T provides world-class DDOS mitigation services for managed Internet enterprise customers.
Bell Canada – Bell Canada provides DDOS mitigation services for managed Internet enterprise customers.
BT – BT provides a range of DDOS mitigation services for managed Internet enterprise customers.
Black Lotus – Newly acquired by Level 3, Black Lotus offers enterprise customers DDOS security capabilities.
CloudFlare – CloudFlare is an application and content delivery network provider including DDOS services.
Corero – Corero, located in the UK, is a network security services company that includes a line of DDOS defense solutions.
Crypteia Networks – Crypteia is a threat intelligence and MSS provider in Greece that includes DDOS prevention services.
DOSarrest – The Canadian firm offers a range of cloud-based Website defense solutions for DDOS attacks.
F5 – F5 offers the Silverline DDOS defensive product for enterprise based on its acquisition of defense.net.
Fortinet– Fortinet provides a DDOS technology solution for carriers and large enterprise.
Huawei– Huawei provides a DDOS platform for carriers and large enterprise.
Imperva – The Web security, cyber security, and database security company includes DDOS solutions.
Link11 – German CDN and hosting firm, Link11, offers a range of DDOS protection services for customers.
Neustar – The Virginia-based company offers infrastructure security solutions including DDOS protection.
NexusGuard – San Francisco-based NexusGuard provides a range of DDOS detection and mitigation services for enterprise.
NSFOCUS – Chinese company, NSFOCUS, offers DDOS mitigation solutions in conjunction with its WAF and IPS solutions.
Qrator Labs – The Russian firm provides network-based solutions for DDOS attacks to the enterprise.
Radware – Radware provides an advanced DDOS platform for carriers and large enterprise including layer seven capabilities.
RioRey – RioRey provides a high performance DDOS platform for carriers and large enterprise.
SecurityDAM – SecurityDAM, headquartered in Tel Aviv, focuses on DDOS for use by MSSPs.
Sentrix – Now part of Trusted Knight, Sentrix offers cloud-based Web application security and DDOS protection.
Shape Security – Shape Security offers detection of automated attacks such as botnets aimed a Websites.
Sharktech – Las Vegas-based Sharktech offers a gateway solution for protecting enterprise networks from DDOS.
Staminus – Now part of StackPath, Staminus offers hybrid DDOS protection and mitigation services.
Sucuri – Sucuri provides various Website protections against malware and denial of service attacks.
Verisign – Verisign provides DDOS filtering service for enterprise.
Verizon – Verizon provides advanced DDOS detection and mitigation services for its managed Internet enterprise customers.
Zenedge – Zenedge offers a range of DDOS protection capabilities embedded in its Web application firewall.

Control 12: Email Security

Email Security consists of the functional mechanisms required to prevent email content or payloads from infecting recipients with malware, and to support properties such as confidentiality, digital signatures, sender authentication, and integrity control using cryptographic controls. Surprisingly, email security has experienced relatively fewer innovations in the past decade, particularly in cross-domain encryption support. That is, two individuals from different companies are just as unlikely to have the facility to mutually encrypt or authenticate email as they were ten years ago. Recent filtering advances for email content and attachments have taken advantage of virtualized computing and advanced algorithms. For enterprise users, email security includes controls in the following areas:

- *Email Encryption* – This includes the algorithmic and key management functions necessary to encrypt email from third-party prying eyes who might be eavesdropping on the Internet.

- *Digitally Signed Email* – This includes the cryptographic and key management support required for senders to digitally sign email and for recipients to validate such reported identities.
- *Email Fraud Prevention* – This includes the infrastructure-level controls required to logically connect reported sender identities to reported addresses for associated mail servers.
- *Email Content and Attachment Filtering* – This is the advanced security functionality required at gateways and elsewhere to detect and filter malicious content or attachments in email.

These functions are typically provided by different vendors, which complicates the creation of a robust end-to-end security architecture for email. A major risk for any provider of email security is the relatively blasé approach most millennials take to the use of email for communication – with most opting for more immediate forms of communication including texting and social posts.

General Outlook

The general outlook for email security involves transition from the prior focus on dealing with minor threats with low intensity attacks such as basic phishing to the greater challenge of dealing with much higher intensity threats such as (ahem) not-so-basic phishing. The transition also involves a shift from lightly deployed security filters, with light attention to standards such as DMARC, to much more extensive use of these malware tools and security standards. First generation email security from 1998 to 2007 involved the most basic email anti-virus software running on corporate gateways. These tools were largely ineffective in detecting most types of malware. Almost no one was using data encryption tools for email during that period, except for enterprise solutions running within large companies for inter-employee email security. Second generation email security extended to more advanced filters at increasingly distributed gateways. Data encryption and digital signature use in business and personal email remained light during this period. Third generation email security from 2016 to 2025 should expect to see more intense phishing challenges being dealt with effectively by better email controls that use machine learning and that support virtualized email in the cloud. During this period, business use of email will also experience a significant shift downward, being replaced by other forms of more immediate communication preferred by current Millennials including texting, collaboration tools, and social posting. The result of improved security with reduced emphasis on email in personal and business use will be an astounding reduction in the email threat. Phishing will become less intense, since users will be much more astute about what they click on, and virtual computing and isolated browsing will contribute to a lessening of overall cyber risk.

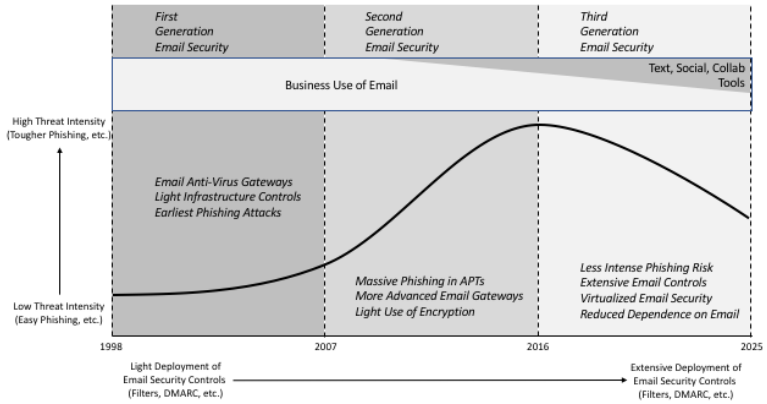

Figure 12. 2018 Email Security Outlook

The TAG Cyber degree of confidence in this outlook is moderate, since the threat intensity is being (boldly) predicted here to lessen, which is always a tenuous statement in any aspect of cyber security. Nevertheless, we see real improvements in security in this area, and that will be good news for anyone in business or using email on the Internet.

Advice for Enterprise Security Teams

Enterprise security teams are advised to continue along the path of performing security awareness to reduce the risk of users clicking on attachments, running AI and machine learning technology in email filtering solutions, and deploying standards-based solutions such as DMARC to reduce risk as well. If you are not using a DMARC-based solution to protect your email today, then it's time today to rectify that gap. The use of encryption and digital signatures in email will likely never reach the level of SSL use with web services, but enterprise teams should nevertheless consider secure means for file transfer, probably using cloud, to supplant insecure file transfer using unencrypted email. Security teams should expect and welcome the transition from heavy email use to texting, social media, and collaboration platform usage.

Advice for Security Technology Vendors

Email security technology vendors should recognize that the use of email will shrink in business and personal use in the coming years. This is a fact that is disputed with peril. Vendors should optimize their positioning with enterprise for the foreseeable future, perhaps with longer term contracts to lock in business. Better algorithms and technology to detect malware in payloads will continue to be an important differentiator. Secure email solutions will be supplanted by increased use of secure cloud services, collaboration tools, and private texting. Keep in mind that business communications will never cease – they will simply shift in how the task is accomplished.

List of Support Vendors

Agari – Agari provides email security infrastructure monitoring including DKIM and SPF-based misuse and fraud analysis.
AppRiver – AppRiver is a cloud-based secure email hosting with Spam and virus protection capability.
AT&T – AT&T offers network-based email security filtering and policy enforcement through technology partnership.
Barracuda Networks – Barracuda provides a range of products and services for email Spam and virus filtering.

Cisco – Cisco provides a standard email security platform and service features.
Clearswift – Now part of RUAG, the Clearswift Secure Email Gateway includes security protections for email.
Comodo – Comodo includes a free Email security solution, an anti-Spam gateway, and encryption/authentication support.
Dell – The Dell SonicWALL solution includes advanced anti-Spam and additional features to secure email.
EdgeWave – EdgeWave offers cloud-based secure email hosting with Spam and virus protection capability.
FireEye – FireEye provides an APT-detection platform for addressing email Spam and filtering malware.
Forcepoint – The TRITON AP-EMAIL provides secure email gateway features for this Raytheon Websense combination.
Fortinet – Fortinet provides an integrated platform solution for addressing email Spam and filtering malware.
GFI Software – GFI offers a range of cloud-based secure email hosting with Spam and virus protection capability.
Google – The popular Gmail provider includes a range of security features including OpenPGP for encryption.
HPE – The Voltage solution from HPE offers a range of email encryption capabilities for enterprise.
Microsoft – Microsoft supports a range of security options for email with Outlook and Exchange offering.
Mimecast – Mimecast offers cloud-based secure email hosting with Spam and virus protection capability.
OPSWAT – OPSWAT includes email security with the Metascan mail agent, which detects malware and email-borne threats.
Proofpoint – Proofpoint's email security product platform provides malware detection and removal for email with quarantine.
ReturnPath– ReturnPath email security infrastructure services including DKIM and SPF-based misuse and fraud monitoring.
SilverSky (BAE) – SilverSky offers a portfolio of secure email communication, collaboration, and infrastructure services.
Sophos – Recently acquiring Cyberoam, Sophos offers secure email gateway with DLP, threat detection, and anti-Spam.
Symantec – Symantec includes range of secure email features including end-to-end encryption.
TargetProof – The TargetProof solution focuses on fraud prevention for email, Web, and user authentication.
ThreatTrack Security – ThreatTrack includes advanced threat detection for email in its anti-malware solution.
TrendMicro – TrendMicro offers policy-based encryption capability for enterprise and consumer email.
TrustWave – The TrustWave Secure Email Gateway includes the standard set of secure email features for the enterprise.
Verizon – Verizon offers a network-based email security filtering and policy enforcement service.
WatchGuard Technologies – WatchGuard provides a secure email and Web gateway as part of its UTM and firewall offerings.
ZixCorp – ZixCorp offers secure email solutions including encryption for companies and individuals.

Control 13: Infrastructure Security

Infrastructure security includes the functional and procedural controls that are used primarily by governments and service providers to reduce cyber security risk in large-scale shared infrastructure including the public Internet. CISO teams rarely have much control over these types of protections, but are deeply affected by the degree to which they are properly attended. The primary traditional focus areas for infrastructure security have been domain name system (DNS) and border gateway protocol (BGP) protections and security system overlays. Technical solutions have tended to utilize public key infrastructure (PKI) to harden systems and protocols against known attacks. More recent attention to global cyber norms across governments and large providers has complemented these functional measures to deal with the increasing risk of large-scale attacks that cascade across the Internet. Service providers have been building private infrastructure protections based on secure peer-to-peer gateways between virtual private networks (VPNs) and cloud infrastructure. This reduces dependency on public networks such as the Internet. SDN-based virtualized networks offer increased security flexibility at the infrastructure level by minimizing the hardware base to a small trusted core and by supporting the ability to dynamically service-chain virtual security functionality via application interfaces on SDN controllers. Future infrastructure security risk is highly uncertain and could easily follow paths of roughly equal probability toward increased, continued, or reduced risk (obviously, a tautology). While it is never fashionable for analysts to flip a coin in making an assessment, the future of infrastructure security for systems such as DNS and BGP is impossible to predict. If a massive, large-scale attack should occur, for example, then regulatory

controls in these areas could complicate matters considerably. This is an area of great risk for enterprise security teams.

General Outlook

The general outlook for infrastructure security involves transition from lower intensity infrastructure security incidents such as minor routing problems or DNS amplification for DDOS to potentially more intense attacks at the infrastructure level, potentially resulting in life-critical or catastrophic consequences. This increase in intensity will result in an increase in emphasis across the community – albeit with few practical strategies that can be taken by the typical enterprise team. First generation infrastructure security from 1998 to 2007 was characterized by early recognition of the risks associated with DNS and BGP. Efforts to use PKI to secure both protocols were essentially failures during this period due to lackadaisical adoption by governments and service providers. Second generation infrastructure security from 2007 to 2016 saw more of the same – with DNS and BGP risk growing, and the associated risk mitigations showing negligible improvement or adoption rates. Third generation infrastructure security from 2016 to 2025 is impossible to predict, except to acknowledge that two of the three scenarios do not include greater risk. That is, ISP initiatives in peering security, SDN and NFV underlying base design, increased shift to mobility, and deeper use of virtualization could result in lower risk, or at least continued levels of risk. The possibility does exist, however, that some malicious group might finally use infrastructure weaknesses to cause a truly catastrophic event.

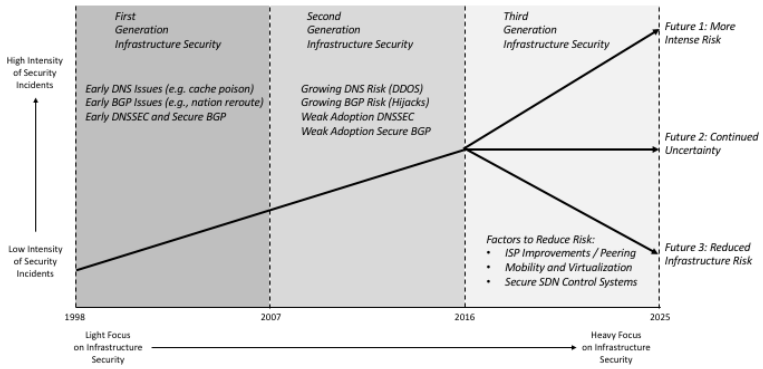

Figure 13. 2018 Infrastructure Security Outlook

The TAG Cyber degree of confidence in this predictive outlook is low to moderate. Certainly, it is a tautology to say that things will get better unless they do not. That said, our confidence is low regarding prediction of which of the three possible futures will be achieved for infrastructure security. Most cyber security experts would likely share this pessimistic view of infrastructure security moving into the next generation.

Advice for Enterprise Security Teams

Enterprise security teams are advised to put pressure on their service providers and government leaders to maintain focus in this area. We should encourage service providers, for

example, to follow emerging cyber norms that minimize the deployment of services and protocols that can be amplified for DDOS purposes. We should also encourage governments to be thoughtful in response to the growing intensity of infrastructure attacks. Poorly conceived or rushed legislation is likely to occur if large-scale routing, naming, or other infrastructure attacks should occur. Expect DNS and BGP weaknesses to remain largely unsolved security risks across the globe.

Advice for Security Technology Vendors

Infrastructure security vendors – and this is a difficult category to define – should recognize that they play a dual role in the coming decade for modern society: Certainly, they have their baseline objective as vendors to provide financial returns for their shareholders and investors. They also, however, carry the burden to help service providers and governments avoid catastrophic infrastructure attacks that could have serious consequences for global society. Educating customers about the risks of infrastructure attacks is the best vendor strategy one might conceive, because awareness of the possible threats in this area will not only be good for business, but will help decision makers select the most secure and reasonable paths forward.

List of Support Vendors

Agari – Agari supports email security at the infrastructure level through DKIM and SFP monitoring and controls.
Akamai – Akamai offers CDN-based controls and DDOS protection at the infrastructure and global network level.
AlphaGuardian – AlphaGuardian supports data center infrastructure protections for servers and telecommunications.
Amazon Web Services – AWS ensures proper infrastructure controls into and out of their virtual services.
AT&T – Global Tier 1 ISPs like AT&T play a key role in protecting infrastructure for enterprise networks.
Box – Box includes services to ensure infrastructure controls into and out of their services as well as for virtual services.
BT – Global Tier 1 ISPs such as BT play a key role in protecting infrastructure for enterprise networks.
CloudFlare – CloudFlare offers CDN, optimization, DDOS, and DNS infrastructure security solutions.
Deutsche Telekom – Global Tier 1 ISPs such as Deutsche Telekom play a role in protecting enterprise networks.
DomainTools – DomainTools provides domain, network, and monitoring tools for look-up, research, and investigation.
Dropbox – Dropbox includes infrastructure security controls into and out of their cloud-based storage services.
Farsight Security – Farsight Security provides threat intelligence feeds from real time passive DNS solutions.
Google – Google ensures infrastructure controls into and out of the Google cloud.
IBM – IBM focuses on ensuring proper infrastructure controls into and out of the IBM cloud as well as for virtual services.
Infoblox – Infoblox offers a range of secure DNS, network services, and network automation services.
Microsoft – Microsoft provides infrastructure controls into and out of the Azure cloud as well as for virtual services.
Neustar – Telephony provider Neustar offers a range of infrastructure security solutions including focus on DDOS and DNS.
NCC Group – NCC includes domain support through the high assurance ".trust" solution for reduced network risk.
Nominum – Nominum supports a range of DNS network infrastructure and cyber security analytics.
Norse – Norse provides active monitoring of network and BGP-related telemetry and security metrics.
NTT – Global Tier 1 ISPs such as NTT play a key role in protecting infrastructure for enterprise networks.
OpenDNS – The San Francisco-based firm offers cloud delivered network security through enhanced DNS protection.
ReturnPath – ReturnPath offers a range of infrastructure-level email and related security services.
Schneider Electric – The company (APC) provides solutions for data center and infrastructure management.
ThousandEyes – ThousandEyes monitors BGP routing, paths, and VOIP for improved trouble-shooting and protection.
Tufin – The Israeli company offers firewall policy orchestration for enterprise infrastructure.
Verisign – Verisign provides infrastructure services including domain services, DDOS, and related controls.
Verizon – Global Tier 1 ISPs such as Verizon play a key role in protecting infrastructure for enterprise networks.

Control 14: Network Monitoring

Network monitoring for cyber security consists of the advanced tools and associated processes required to capture network data, usually at high capacity, for the purposes of retention, aggregation, correlation, analysis, and ultimately action. Motivations for network monitoring range from advanced persistent threat (APT) avoidance to lawful intercept by service providers. Network monitoring tools have differentiated in the past purely on their ability to expand to growing bandwidth. More recently, the differentiation points have evolved to include the ability to perform advanced analysis at line speed, as well as to reliably connect data feeds gathered from a large group of distributed nodes. Small and mid-sized businesses (SMB) have tended to not utilize network monitoring tools directly, but with the progression to shared IT services in cloud, a much wider swath of users is likely to emerge. Virtualization clearly changes the nature of many network monitoring solutions, shifting from IP connections between computers to application programming interfaces (APIs) between processes. This lowers the requirements for a network monitoring tool to handle individual capacity from the expected Tbps range for ISPs to something considerably lower for cloud workload collection and processing.

General Outlook

The general outlook for network monitoring involves transition from low collection and processing capabilities to much higher functionality in both areas. In addition, network monitoring for cyber security is moving from more stand-alone centralized monitoring to more distributed aggregate monitoring of hybrid infrastructure. First generation network monitoring from 1998 to 2007 involved hardware appliances performing basic capture at logical chokepoint gateways. Second generation network monitoring from 2007 to 2016 involved increased capacity with advanced analytics at line speed. This second generation also included early support for hybrid cloud architecture. Third generation network monitoring for cyber security from 2016 to 2025 should expect to see two branches of operational support emerge. ISPs will continue to need massive capacity support reaching into the Tbps range with full line speed analytics. Most enterprises, however, will follow a different path with more distributed workloads requiring monitoring, as well as embedded monitoring in microsegments that must be aggregated into a common view.

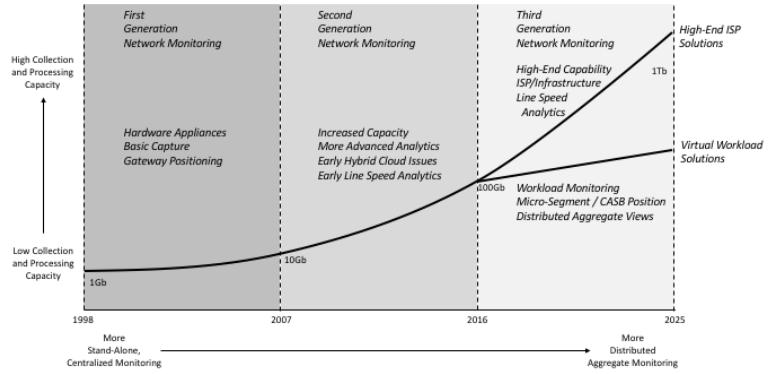

Figure 14. 2018 Network Monitoring Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, given the obvious trends in ISP and enterprise networking. Advances in analytics have tracked growth in capacity closely, and this is likely to continue for the next decade.

Advice for Enterprise Security Teams

Enterprise security teams are advised to consider network monitoring solutions if they have not already. Integrating advanced network capture and analytics into the enterprise security architecture is a powerful enhancement, and more teams should consider this option in the coming years. ISPs should continue to work with network monitoring vendors, and should demand not only line speed analytics for massive pipes, but also support for SDN and NFV initiatives that will require analytics as SDN applications between virtual workloads.

Advice for Security Technology Vendors

Network monitoring vendors should recognize that the previous capacity support race will be replaced by ISPs and enterprise looking more for network monitoring partners that can flexibly support virtual and hybrid architectures. There will remain a niche market that demands the more powerful hardware support, but a much larger market will emerge, especially in the enterprise, that will prefer virtualized appliances in cloud operating systems or SDNs.

List of Support Vendors

Allot Communications – Allot Communications provides network monitoring optimization, monetization, and security solutions.
APCON – Oregon-based APCON offers network monitoring and optimization solutions for data centers.
Arbor Networks – Arbor offers a platform for monitoring network traffic volume and conditions related to DDOS.
AT&T – As AT&T virtualizes its network, unique opportunities arise for SDN-based network monitoring solutions for security.
Attivo Networks – Attivo Networks provides deception-based attack detection and prevention for network monitoring.
Symantec – Through acquisition of Blue Coat, Symantec supports proxy, network analysis, and related network monitoring.
BluVector – The McLean-based firm offers an advanced threat detection and network monitoring platform.
Bradford Networks – Bradford Networks integrates NAC with live network connections views.
Cisco – The acquisition of Lancope introduces the StealthWatch network security analytics tool into the Cisco suite.
Sophos – Via acquisition of CyberFlow Analytics, Sophos obtained security analytics for network security anomaly detection.
Fidelis – The Fidelis XPS system analyzes network traffic to detect tools and tactics of advanced attackers.
FireEye – FireEye provides solutions for detection of advanced attacks using the signature-less MVX engine.
Flowmon – Located in the Czech Republic, Flowmon offers network monitoring and security solutions.
FlowTraq – FlowTraq provides network flow analysis, monitoring, and anomaly detection to support network forensics.
Gigamon – The Gigamon platform supports forensics, visibility into encryption, and threat detection.
GreeNet Information Service – Headquartered in China, GreeNet offers traffic inspection for network monitoring and security.
Intel Security (McAfee) – The McAfee Advanced Threat Defense solution detects stealthy attacks and generates intelligence.
IronNet Cybersecurity – IronNet offers advanced network analytic tools that monitor packets at very high line speeds.
Juniper – The Juniper Security Intelligence Center is integrated into the SRX Series Gateways to support network security.
ManageEngine – ManageEngine supports network behavior anomaly detection through network security management.
Napatech – Napatech, located in Denmark, supports capturing, processing, and monitoring of traffic for real time visibility.
NIKSUN – NIKSUN includes capability in their product to manage capture and analysis at very high network capacity rates.
Novetta Solutions – Novetta provides an advanced network security analytics platform that delivers actionable insights.
PacketSled – PacketSled offers a next-generation network security tool for providing continuous monitoring.
Plixer – Located in Maine, Plixer provides solutions for NetFlow capture, deep packet inspection, and log data replication.
Qosmos – The French firm, Qosmos, offers a platform for collecting network traffic for management and security.
RISC Networks – The Cloudscape solution from RISC Networks offers IT and network security analytics.
RSA – RSA Security Analytics supports enterprise and network security monitoring and attack detection.
Savvius – California-based Savvius offers a range of network monitoring and security solution software.
SolarWinds – In addition to performance, application, and database monitoring, SolarWinds offers IT security solutions.
Trisul Networks – Trisul offers a range of multi-layer streaming network analytics tools for customers.
Verizon – Verizon's network infrastructure virtualization supports SDN-based network monitoring for security.

Zscaler – Zscaler provides Web security based on an extensive network of gateway proxy solutions.

Control 15: Secure File Sharing

Secure file sharing involves the platforms and tools required for different entities to send, receive, and use files without introducing threats such as unauthorized disclosure or modification. Most secure file sharing mechanisms to date have been encryption-based, often integrated with email, and this remains an important underlying technology. Some secure file sharing is purely end-to-end and over-the-top with respect to the underlying network. Other means involve intermediaries that utilize secure network protocols such as secure sockets layer (SSL) to ensure mutual secrecy. The major trend in secure file sharing is public cloud usage with mobile device access. This is a tidal wave hitting this aspect of cyber security, and any vendor supporting secure file sharing must include a clear strategy for co-existence with cloud. Another major trend involves secure machine-to-machine sharing in IoT environments, perhaps the modern equivalent of traditional electronic data interchange (EDI) systems.

General Outlook

The general outlook for secure file sharing involves transition from light, exception-based use of secure file sharing tools to heavier, perhaps even routine use of secure sharing methods. This increase tracks the increased distribution of workers which changes collaboration and sharing from local area network-based trust to remote sharing. Secure file sharing tools are also undergoing a dramatic transition from more stand-alone products in the enterprise to solutions that will be embedded in public cloud and XaaS offerings. First generation secure file sharing from 1998 to 2007 involved encryption and some use of underlying secure protocols to patch together solutions for people to share files securely, but usually only as exceptions to the norm. Second generation secure file sharing from 2007 to 2016 increase capability, including easier crypto tools, and introduced early support for hybrid cloud. Third-generation secure file sharing, from 2016 to 2025, should expect to experience a cloud dominant architecture with embedded sharing capabilities. The good news is that exception-based secure sharing will be replaced with default secure options.

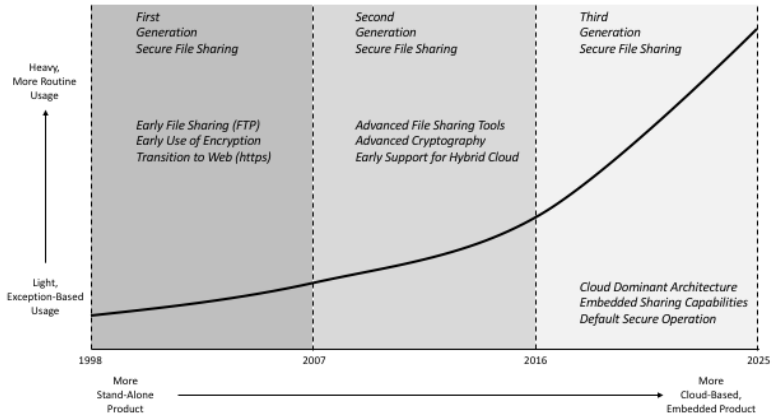

Figure 15. 2018 Secure File Sharing Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, as the transition to cloud is already well underway – even for current buyers of secure file sharing technology. Nevertheless, there is still much to do across cloud infrastructure for most Internet users to properly address threats. Consider, for example, how you might share sensitive information with a business partner today. You might attach the file to an email, and perhaps password protect it. Similarly, you might drop the file into a cloud service such as Box and maybe text over a password. These are weak methods that will undoubtedly improve, and the collision with the existing secure file sharing solution marketplace will occur quickly.

Advice for Enterprise Security Teams

Enterprise security teams are advised to take a complete and accurate inventory of current file sharing methods across the business. Most will find a varying, perhaps ad hoc range of different approaches, with poor correlation to actual business risk. Now is the time to fix this, since the secure file sharing solutions available in cloud-based, XaaS will be excellent. Existing secure file sharing vendors will also step up their game and improve their methods considerably to hopefully ward off the threat of cloud sharing. This is an excellent time for CISO teams to investigate and plan better approaches in this area.

Advice for Security Technology Vendors

Secure file sharing vendors should recognize that the cloud represents an existential threat to their business if they do not currently include a clear roadmap to mobility-enabled, cloud accessible sharing services. The good news is that the entire ecosystem around secure file sharing will grow dramatically, so it is a great time to be a capable vendor in this area. Stubborn vendors who expect buyers to use proprietary OTT solutions, however, might find that their growth becomes stymied in this coming decade, so heed our warning now: Begin to virtualize your secure file sharing solutions into the cloud today, if you have not already.

List of Support Vendors

Accellion – Accellion provides range of secure file sharing capabilities for its enterprise customers.
Amazon Web Services (AWS) – AWS offers support for enterprise and individual file sharing and collaboration capabilities.
ANX – Southfield-based ANX, recently acquired by OpenText, offers managed compliance and collaboration solutions.
Apple (iTunes) – Apple device and content services on iTunes includes support for file sharing and collaboration.
Authentica Solutions – Authentica supports data management solutions for a common data store across educational districts.
Autotask – Through acquisition of Soonr, Autotask provides a cloud-based secure file sharing solution for enterprise.
AvePoint – AvePoint specializes in security and compliance of Microsoft enterprise solutions including SharePoint.
Axway – Axway provides range of secure file sharing capabilities for enterprise customers including support for cloud APIs.
Biscom – Biscom provides a range of support for secure file transfer of large and confidential files.
Blackberry – The acquisition of Watchdox provides Blackberry with an excellent secure file sharing solution.
Boldon James – Boldon James offers data encryption and classification in support of file protection via sharing.
Box – Box cloud storage services include a range of world-class support for file sharing and collaboration.
Brainloop – Brainloop, located in Germany, provides secure collaboration and control with external partners.
Cisco – Through acquisition of Pawaa, Cisco offers secure on-premise, encrypted file sharing capabilities.
Citrix – The virtualization company located in Florida and California offers sharing via its workspace-as-a-service solutions.
Cloak Labs – Cloak Labs provides end-to-end encryption of application data from the enterprise to partners.
Comilion – Integrated into Dell-EMC, Comilion provides a range of decentralized solutions for secure collaboration and sharing.
Content Raven – Content Raven provides cloud-based solutions for protecting the distribution of files.
Covata – Australian firm Covata offers customers with encryption-based secure file sharing solutions.

Covertix – Covertix provides a range of encryption rights managed file security protection solutions.
Deep-Secure – Deep-Secure provides a cyber security guard solution for organizations to securely share information.
Dell-EMC – Through Syncplicity, EMC provides various means for securely sharing and syncing files for business.
Egress Software Technologies – Egress offers managed file transfer with encryption and other security features.
Exostar – Herndon-based Exostar includes secure collaboration along with identity and secure chain management products.
FinalCode – San Jose-based FinalCode offers a range of solutions for secure file sharing in the enterprise.
GFI Software – Through acquisition of Kerio, GFI Software offers UTM and secure collaboration solutions for the enterprise.
Globalscape – San Antonio-based Globalscape offers a range of secure file transfer and secure information exchange solutions.
Google – Cloud and computing services from Google include support for enterprise and individual file sharing and collaboration.
Hightail – Formerly YouSendIt, Hightail provides secure file sharing services for small business and consumer applications.
HoGo – New Hampshire-based HoGo offers DRM-based protection for sharing enterprise documents.
HPE/Voltage – The acquisition of Voltage by HPE obtained encryption capability with advanced secure file sharing support.
Huddle – Huddle provides an offering that supports secure team collaboration services in the cloud.
IBM – Cloud services from IBM include support for enterprise and individual file sharing and collaboration.
Ipswitch – Massachusetts-based Ipswitch includes secure, automated, managed file transfer and secure FTP solutions.
IRM Secure – IRM Secure provides security for data usage control, information rights management, and secure outsourcing.
JIRANSOFT – The Los Altos-based firm provides an advanced SaaS platform for secure storage and control.
JSCAPE – JSCAPE provides an advanced Web-based solution for monitoring secure file transfer applications.
LeapFILE – LeapFILE offers business secure file transfer services via Web application or desktop client.
Linoma Software – Linoma offers a range of cyber security solutions including secure file transfer.
Microsoft – Microsoft supports enterprise hosted file collaboration with SharePoint and Azure collaboration offerings.
Mimecast – Mimecast, located in the UK, provides email cloud services support security, archiving, and collaboration.
MobileIron – Through acquisition of Averail in 2014, MobileIron secures content on mobile devices.
NC4 – Through acquisition of Soltra, NC4 supports open, automated intelligence with Soltra Edge.
nCrypted Cloud – nCrypted Cloud offers encryption-based data security solutions for sharing files in the cloud.
NEXOR – UK-based NEXOR offers security solutions for information exchange and information assurance.
Nexsan – Nexsan offers a solution called Transporter that enables business and government to own and control information
Owl Computing Technologies – Owl offers an advanced data diode for cross-domain secure data transfer.
Safe-T – Israeli firm Safe-T offers solutions for managing secure data exchange between business, people, and applications.
Seclore – Seclore is an Indian firm that provides customers with a range of secure file sharing services.
SecSign – SecSign Technologies provides two-factor authentication, encryption, and related file sharing capabilities.
Securitinet – The small firm provides a range of cloud-based cyber security solutions for businesses with critical data.
Senditonthenet – Senditonthenet is a free and secure file transfer and sharing service available on the Internet.
SendSafely – New York firm, SendSafely, offers secure file transfer across a zero-knowledge platform with encryption.
SendThisFile – SendThisFile, located in Kansas, offers products for secure file transfer.
ShareVault – ShareVault provides range of secure file sharing capabilities with emphasis on Microsoft SharePoint.
SmartFile – SmartFile offers a range of secure file sharing services and FTP hosting for business customers.
SmartVault – SmartVault is an on-line document storage and secure file sharing capability for business.
Softlock – Softlock offers a Secure Data Exchange solution for secure document and file exchange.
STEALTH Software – Located in Luxembourg, STEALTH Software offers security protections for SharePoint and .NET applications.
Surevine – The UK-based Surevine provides a secure collaboration solution for the enterprise.
TeraDact – The Minnesota-based company offers secure information management and sharing solutions.
Terbium Labs – The small company offers fingerprinting solution that can detect stolen intellectual property.
Thru Inc. – Thru Inc. offers an enterprise file sync and sharing service with cloud storage and secure managed transfer.
TITUS – TITUS, located in Canada, offers a range of secure file sharing and leakage protection solutions.
Tresys – The Tresys secure transfer product offers deep content inspection and related security features.
TruSTAR – TruSTAR provides an anonymous means for sharing of threat and vulnerability information with a community.
Varonis – The New York-based Varonis offers solutions for data governance via file sync and share.
Vaultize – Vaultize supports enterprise secure file sharing through a range of DRM support capabilities.
Vera – Vera, located in Palo Alto, offers a solution for securing data and files with enterprise protections.
Votiro – The Israel-based company offers various data security solutions including sanitization tools.
Workshare – The UK-based Workshare offers secure file sharing and document collaboration tools.

Control 16: VPN/Secure Access

Virtual private network (VPN)/secure access solutions allow remote entities to securely share and communicate across an insecure network such as the Internet, public or home WiFi, or broadband mobile. Most VPN/secure access tools are designed for remote teleworkers to access an enterprise securely through a gateway established at the perimeter DMZ. This capability evolved from an exceptional use-case (e.g., work closure due to weather) to the normal everyday case (e.g., people working 24/7 including from home, airports, and Starbucks). Everyone knows that the enterprise perimeter is dissolving in lieu of mobility-enabled, public cloud services, so the corresponding concept of a VPN for secure remote access will shift dramatically. This is not necessarily bad news for vendors, because the need secure communications over insecure media will remain, and perhaps grow. In fact, the physical perimeter gateway will give way to a distributed, virtual secure access capability that will define the virtual edge of the new enterprise. VPN/secure access solution providers are well-positioned to take advantage of this evolution to grow their business. They should use this positioning to help move organizations to stronger forms of two or three-factor authentication in the process.

General Outlook

The general outlook for VPN/secure access involves transition from weak authentication to stronger authentication for services that shift from enterprise-focused remote access to mobility and cloud-focused virtual access. First generation VPN/secure access solutions from 1998 to 2007 supported early telework by employees and third-parties using passwords and sometimes tokens for 2FA. Second generation VPN/secure access solutions from 2007 to 2016 saw greatly increased telework with massive growth in third-party access requirements. Authentication improved during this period with most enterprise security teams demanding 2FA. Third generation VPN/secure access solutions from 2016 to 2025 should expect to see total perimeter dissolution in lieu of mobile access to virtualized services in hybrid cloud arrangements. Stronger forms of 3FA will emerge, perhaps using hardware-based credentials exported from trusted execution environments.

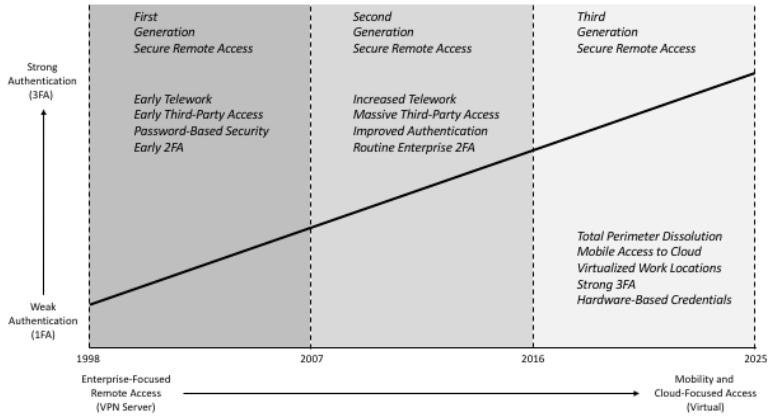

Figure 16. 2018 VPN/Secure Access Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, given the clear direction of perimeter and cloud networking. Readers are advised that VPN solutions from ISPs for site-to-site communications over networks such as multi-protocol label switching (MPLS) are different from remote access VPN solutions. MPLS is not a security protocol since labels are not robust. This does not preclude MPLS services from being secure, of course, but a business VPN is optimized to flexible operations rather than cyber security from label separation. Readers should also note that we include many lighter, free options for VPN/remote access in our analysis, simply because these solutions – often not viewed as enterprise-grade – can be enhanced to meet business requirements. Buyers and vendors are advised to keep an eye on these solution providers, because the savvier solution offerings will find a market in some cloud-positioned enterprise buyers in the coming years.

Advice for Enterprise Security Teams

Enterprise security teams are advised to begin planning for support of more flexible, hybrid cloud focused secure remote access for employees and third-parties. Where previously, for example, remote access into the VPN gateway was a mandate for any outsourced contract, the new approach will involve shared workloads in mutually accessible cloud services that no longer enjoy trusted adjacency to other enterprise resources. This is bad news for APT actors, but excellent news for security teams. The shift to 3FA is advised as part of this transition, with biometrics on the mobile device (e.g., thumb), underlying certificate exchange using mobile device management, and a user-managed password process as good options. Adaptive platforms will help to fine-tune this to the remote access risk situation for a given access request. This is a big shift from existing approaches, so enterprise teams should begin their study, testing, and vendor interviews now.

Advice for Security Technology Vendors

VPN/secure access vendors should recognize that they have the bad news/good news scenario of a dramatically melting existing perimeter-base being replaced with a massive new opportunity to support virtual remote access to cloud-based workloads over insecure networks. Vendors who recognize this incredible opportunity to become a new primary control for virtual enterprise will thrive. Stubborn vendors who continue to push VPN gateway hardware appliances for DMZ usage will see free fall in revenue in the coming years. Vendors must also accept that the next generation employee and partner will use a mobile device for most applications. PCs will not go away, but security solutions should be designed mobile-first, and PC-second.

List of Support Vendors

AirVPN – AirVPN provides a VPN based on OpenVPN and operated through community involvement.
AnchorFree – Mountain View-based AnchorFree provides VPN solutions for secure Web browsing.
Anonymizer – San Diego-based Anonymizer provides a personal VPN service for private Internet access.
AT&T – The carrier can design remote access solutions for business customers with support for two-factor authentication.
Barracuda Networks – Barracuda offers an SSL VPN client-less solution for secure access via a Web browser.
Bomgar – Bomgar offers secure remote access through firewalls without the need for a separate VPN.
Celestix – Fremont-based Celestix provides secure remote access connectivity to cloud and distributed offices.
CipherGraph – The Pleasanton firm offers a range of secure cloud-based VPN solutions for its customers.
Cisco – Cisco provides its AnyConnect Secure Mobility Client for “per app” VPN support and secure endpoint.

Clavister – Headquartered in Sweden, Clavister provides a range of network security solutions including VPN.
CyberGhost – CyberGhost provides downloadable software in support of on-line secure browsing to avoid behavior tracking.
Cyxtera – Cryptzone, part of Cyxtera, offers a gateway solution for secure access to the enterprise.
F-Secure – F-Secure offers the Freedome VPN solution for Windows, OS X, iOS, and enterprise business.
Hideman – Hideman allows unblocking of Websites, hiding IP addresses, and removal of surfing limits.
Huawei – The large Chinese networking firm offers a range of network security products including support for remote access.
IBM – IBM offers its customers the IBM Mobile Connect, a fully featured wireless virtual private network.
IPVanish – IPVanish offers a solution that hides IP addresses during surfing and other online resources.
Juniper – The large networking firm offers a range of network security products including support for remote access.
NordVPN – NordVPN offers an application for anonymous surfing with no customer usage logging policy.
Private Internet Access – Private Internet Access offers high-speed anonymous VPN services for Internet access.
PureVPN – PureVPN delivers a fast VPN service with flexible support for online privacy and security.
OpenVPN Technologies – OpenVPN Technologies provides an open VPN solution deployable as software or appliance.
Pulse Secure – Pulse Secure offers access control, SSL VPN, and mobile device security solutions for the enterprise.
SecureLink – The Austin-based company offers its SecureLink remote support network for secure remote access by third parties.
Soha Systems – Now a part of Akamai, Soha Systems provides a secure access solution for third parties and employees.
Spotflux – Spotflux offers a secure, managed connection to the Internet for mobile devices and desktops.
SSH – The Finland-based firm offers SSH key management, privileged access control, and identity solutions.
TorGuard – The TorGuard product includes a range of anonymous VPN services in support of end user security and privacy.
Tunnelbear – Tunnelbear offers a mobile VPN solution that is designed to unblock and secure websites.
Uniken – Located in Florida, Uniken offers a range of secure virtual private networking solutions.
Verizon – Verizon offers remote access service solutions for business customers with support for strong authentication.
VyprVPN – VyprVPN offers a secure VPN that executes on Windows, Mac, and other compute platforms.
ZenMate – The German company offers a privacy and security-enhanced browser for virtual networking.

Control 17: Anti-Malware Tools

Anti-malware tools are designed to prevent, detect, and mitigate malware on computers. Early anti-virus software emerged over two decades ago to address the growing problem of Trojan horse software in early PCs. This evolved gradually into today's complex protection systems that use the best available static and dynamic computing analytics to reduce the risk of potentially malicious software on computers. The pure use of signatures to detect malware has been largely discredited, but the best vendors have been careful not to toss the baby with the bathwater. Signature-based solutions remain useful, albeit in the context of powerful behavioral analytics that detect and prevent the presence of malware through observational heuristics in real or virtual computing environments. The expansion of anti-malware to mobility has already occurred, but the next big frontier is the myriad of IoT and ICS devices that possess unique, often proprietary run-time systems into which malware could be introduced. While such systems often do not scale sufficiently to support generalized commercial anti-malware development, their frequently critical mission could easily justify the work to develop a specific attack.

General Outlook

The general outlook for anti-malware tools involves transition from signature-based anti-virus software to advanced use of behavioral analytics to address malware. This transition also involves gradual shift from software for PCs and servers to capabilities focused on mitigating malware from entering virtualized workloads. First generation anti-malware tools from 1998 to 2007 involves significant growth of deployment for pure signature-based software on PCs to chase (unsuccessfully) the growth of nasty variants. Second generation anti-malware tools from

2007 to 2016 saw a depressed market with buyers dissatisfied with the results, which allowed offensive actors to easily evade defenses. Some early behavioral analytic tools emerged in this area, but not enough to slow down a massive depression in this area of cyber security for both home and business use. Any PC or server administrator during this period would likely explain that their antivirus software does not work, and this had dire business consequences for some of the larger players in this area. McAfee, for example, experienced bumpy times during this second-generation period as part of (and then no longer part of) Intel and as part of (and then sometimes no longer part of) the enterprise architecture. (The good news is that McAfee remains capable and well-managed, and will experience success ahead.) Third generation anti-malware tools from 2016 to 2025 should expect to see a considerable resurgence in use due to greatly improved analytics and even signatures. Techniques that will contribute to the growth renaissance of anti-malware in the coming period will include cloud-based threat intelligence and dramatically increased use of automation in the form of machine learning. This should help drive anti-malware tools back into the growth column in the coming decade, and this is good news for the industry.

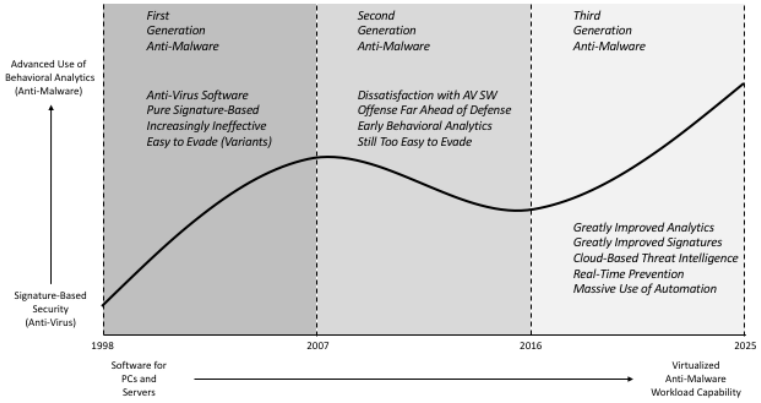

Figure 17. 2018 Anti-Malware Tool Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since the resurgence of anti-malware has already begun to occur. The drive to new types of protection targets is also quite likely since IoT, industrial control systems, and cloud workloads will all need some form of malware protections.

Advice for Enterprise Security Teams

Enterprise security teams are advised to perform a thorough reassessment of capabilities in this market, and should be certain to include the traditional anti-virus vendors in their work. The old vendors you threw out a couple of years ago, might be doing work that is similar to the new ones you brought in. This does not imply shortcomings in the newer vendors – quite the contrary. Instead, this entire field is getting better, and buyers should make certain to take full advantage. A big challenge is that the endpoint security and anti-malware markets have largely merged, which is a huge mistake for vendors. Detecting, preventing, and mitigating malware is

more general than endpoints, and will be needed soon for cloud workload protection. This could turn out to be the biggest anti-malware market ever.

Advice for Security Technology Vendors

Anti-malware vendors should immediately separate their endpoint security and anti-malware business focus. Both are valid, but the concerns are different. Excellent anti-malware capability should generalize to cloud workloads, containers, industrial devices, servers, virtual machines, and even larger entities such as clouds and networks. The introduction of SDN and NFV will offer a huge new opportunity to extend anti-malware solutions to data center controllers, WAN components, and network devices, all of which are being redefined as software. Vendors are also advised to integrate the best available techniques including both static and dynamic, local and cloud, and compile-time and real-time protections.

List of Support Vendors

Advanced System Care – Advanced System Care offers PC tools for protection, optimization, and other functions.
Agnitum – Agnitum offers its Outpost Security Suite with PC anti-virus and Internet security tools.
AhnLab – AhnLab is a South Korean firm that offers V3 Internet security tools for business endpoint protection.
Antiy Labs – The Chinese company offers an advanced anti-virus SDK engine and anti-virus service.
AppGuard – Blue Ridge Networks offers its AppGuard anti-malware and associated Internet security tools.
Ashampoo – Ashampoo offers customers a standard set of PC anti-virus and Internet security tools.
Avast – Czech Republic-based Avast offers standard free and upgraded PC and mobile anti-virus and Internet security tools.
AV-Europe – The Netherlands-based firm distributes various security products including anti-virus and Internet security.
AVG – Netherlands-based firm, AVG, offers free and upgraded PC anti-virus and Internet security tools.
Avira – German firm Avira offers a range of free and upgraded PC anti-virus and Internet security tools.
Bitdefender – Bitdefender, headquartered in Romania, offers a range of standard PC anti-virus and Internet security products.
BullGuard – The UK-based firm offers the standard set of PC anti-virus and Internet security tools.
ClamXav – ClamXav offers Apple customers with a suite of Mac-based anti-virus and Internet security tools.
Comodo – Comodo offers the standard set of free, downloadable PC anti-virus and Internet security tools.
CrowdStrike – CrowdStrike includes anti-malware solutions in its extensive range of cyber security and response solutions.
Cylance – Cylance uses advanced machine learning and AI to detect malware in computing endpoints.
Dr. Web Ltd. – Dr. Web Ltd. is a well-known Russian anti-virus and Internet security firm offering a wide range of solutions.
Emsisoft – Emsisoft, headquartered in Austria, offers its customer a suite of anti-malware and Internet security tools.
eScan – eScan offers its customers a standard set of PC anti-virus and associated Internet security tools.
ESET – ESET is a well-known global cyber security company that offers range of PC anti-virus and Internet security tools.
FireEye – FireEye helped invent the run-time virtual detection of malware through safe detonation.
FixMeStick – FixMeStick is a virus removal device to clean infections from user personal computers.
Fortinet – Fortinet includes free PC anti-virus and Internet security tools in its FortiClient offering.
F-Secure – F-Secure, located in Finland, offers online PC scanning and security tools for home and business use.
G Data – German company G Data offers customer a standard set of PC anti-virus and Internet security tools.
GFI Software – The Luxembourg-based firm provides a range of IT security products and services.
Google – The VirusTotal free resource from Google allows researchers to help identify and understand their malware.
Hitman Pro – Hitman Pro from SurfRight in the Netherlands offers standard set of PC anti-virus and Internet security tools.
Humming Heads – Located in Japan, Humming Heads provides anti-virus and Internet security products.
Ikarus Security Software – The Austrian firm offers a range of virus prevention tools for mobility and cloud.
INCA Internet – The South Korean firm provides a range of PC security solutions including anti-virus.
Intego – Intego offers a range of PC anti-virus and associated Internet security tools for Apple Mac users.
IObit – IObit offers a range of Apple Mac performance and security tools including anti-virus software.
Kaspersky – The firm offers standard set of PC anti-virus and Internet security tools for home and business.
Kromtech – Kromtech offers standard set of Mac anti-virus and Internet security tools for Apple customers.
Lavasoft – Lavasoft offers a free Ad-Aware product that includes the standard set of PC anti-virus and Internet security tools.
Malwarebytes – Malwarebytes provides advanced anti-malware detection algorithms in its security offering.
McAfee – McAfee continues to provide world-class capability for enterprise anti-malware controlled by its ePolicy Orchestrator.
Microsoft – Microsoft Security Essentials includes the standard set of PC anti-virus and Internet security tools.
Network Intercept – The Los Angeles-based firm offers anti-malware and keystroke encryption for PCs and Macs

Norman Security – The Norman Security Suite includes the standard set of PC anti-virus and Internet security tools.
Panda – Spanish firm Panda offers customers a standard set of PC anti-virus and Internet security tools.
Qihoo 360 Technology – The Chinese company's product Qihoo 360 includes PC anti-virus and Internet security tools.
Quick Heal – Quick Heal offers the standard set of PC, Mac, and Mobile anti-virus and Internet security tools.
SecureIT – Security Coverage offers the standard set of PC anti-virus and Internet security tools to customers.
Sophos – Sophos offers PC anti-virus and Internet security tools for business customers, including its SurfRIght solution.
SUPERAntiSpyware – The company offers Roboscan, Spybot, and SUPERAntiSpyware anti-virus and Internet security tools.
Symantec – Symantec provides endpoint anti-malware detection solutions based on the famous Norton anti-virus suite.
ThirtySeven4 – ThirtySeven4 offers PC anti-virus and Internet security tools for schools, universities, business, and home.
ThreatTrack Security – ThreatTrack offers customers the standard set of PC anti-virus and Internet security tools.
Topsec Science – The Chinese company offers anti-malware tools as part of its suite of security products.
Total Defense – Located in New York State, Total Defense offers anti-malware solutions for PCs and mobiles.
Trend Micro – Trend Micro offers a full range of advanced PC anti-virus and Internet security tools.
TrustGo – TrustGo, part of Baidu, offers customers a full set of mobile anti-virus and Internet security tools.
Trustlook – Headquartered in San Jose, Trustlook offers a range of anti-virus and anti-spyware solutions.
TrustPort – TrustPort from the Czech Republic offers a range of anti-malware security tools for home and enterprise.
Valt.X – Valt.X offers its customers a range of advanced, non-signature-based anti-malware tools.
VoodooShield – The company offers the VoodooShield suite of anti-virus and Internet security tools.
Webroot – Webroot, headquartered in Colorado, offers standard set of PC and Mac anti-virus and Internet security tools.
ZoneAlarm – ZoneAlarm includes PC anti-virus and Internet security tools in its range of solution offerings.

Control 18: Endpoint Security

Endpoint security is a crowded place in our cyber security market, and perhaps for good reason. Since all personal and business computing usage begins with a PC, tablet, or mobile, the endpoint provides an intimate environment for vendors to offer *visible* cyber security support. Human beings can *see* and *directly experience* endpoint security controls, and this creates an irresistible urge for vendors to develop solutions in that area. The range of endpoint security solutions spans widely from remaining anti-virus solutions to advanced modern container protections. The space also includes a wide range of algorithmic protections from simple signatures to advanced artificial intelligence, so it is often difficult to place these solutions in the same category. Even the enterprise management of endpoint security solutions ranges from proprietary tools with their own console to advanced product suites with APIs that allow for comprehensive integration into an existing enterprise environment. The common theme for all endpoint security, however, will be near-term consolidation – and this includes for more advanced endpoints such as IoT devices, ICS components, and virtual machines. The market is too scattered and buyers remain confused about what to buy, what to ignore, what to replace, what works, what doesn't, and on and on. Sharing your favorite endpoint security solution with friends over a beer in 2017 and 2018 has become bizarrely like sharing your favorite Wall Street stock. This will dissolve in the coming years as endpoint security solutions consolidate into cleaner, simpler tools that lightly embed into a range of physical and virtual endpoints with little regard for the ergonomics of the endpoint usage.

General Outlook

The general outlook for endpoint security involves transition from simple security software to comprehensive, integrated security solutions. The focus will also shift from PCs to a wide range of PCs, servers, mobile, IoT devices, industrial control systems, virtual machines, and on and on. First generation endpoint security from 1998 to 2007 involved mostly anti-virus software,

simple encryption tools, and early data leakage prevention (DLP) tools to address the light security threat of simple viruses. Second generation endpoint security from 2007 to 2016 saw the introduction of more behavioral security solutions to address a more intense threat. Containerized endpoint protection became a new type of security solution during this era, and techniques such as cloud-based endpoint security support emerged. Third generation endpoint security from 2016 to 2025 will see more types of protection solutions, including isolated browsing, while also experiencing massive consolidation of techniques into common suites for endpoints. These new, combined solutions will be fully integrated into cloud support and will take full advantage of virtualization techniques.

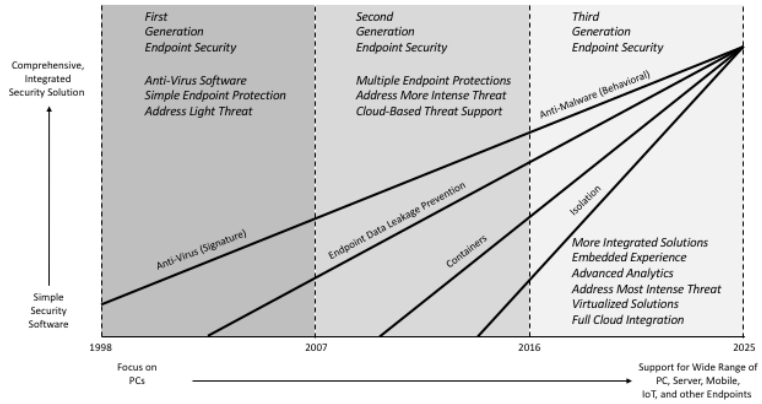

Figure 18. 2018 Endpoint Security Outlook

The TAG Cyber degree of confidence in this predictive outlook is moderate, because there are so many moving parts involved in this aspect of cyber security. Endpoint devices continue to experience innovation, for example, with some types such as home gaming systems and set-top-boxes, having highly unpredictable futures. One would expect to see, however, generic hardware with the ability to virtualize operation to whatever is desired. This implies that in the future, your router, gaming system, and irrigation control will probably all run virtually in a common cloud operating system installed on the same hardware.

Advice for Enterprise Security Teams

Enterprise security teams should follow two tracks in their endpoint security programs. The first track should be focused on optimizing near-term security solutions for their PCs and mobiles. Emphasis here should be on the accuracy and effectiveness of the security algorithms (probably machine learning and artificial intelligence-based), as well as the ease of IT management for the security solution. The second track, however, should carefully consider longer-term issues such as consolidating seemingly disparate endpoint solutions such as behavioral analytics, endpoint data leakage prevention (DLP), and cloud isolation of browsing. This second track should be approached as an R&D activity, and the best CISO teams will create small testbeds to evaluate integrated solutions for early adoption. Endpoint security is a mature enough market that early adopters of integrated protection suite will not have to deal with high levels of risk. The

integration should be relatively smooth, which implies that in the next decade, most enterprise users will see shifts and changes in their endpoint security protection. Stay tuned.

Advice for Security Technology Vendors

Endpoint security solution vendors must learn immediately to integrate their products and services into the evolving enterprise. This implies a strict focus on open interfaces, platforms, and tools. Proprietary *anything* in the coming years for endpoint security will create barriers for CISO teams to purchase and use the product. *Open* will be the best approach. Vendors are also advised to form alliances with complementary solution providers in the same endpoint security category. AI-based security tool providers might, for example, form alliances with cloud isolation vendors; similarly, containerized security providers might form business alliances with DLP providers; secure encryption-based endpoint solution providers might form alliances with hardware-assisted endpoint protection providers; and so on. This will provide momentum for architectural consolidation and will help endpoint security vendors learn to integrate with diverse computing ecosystems.

List of Support Vendors

Absolute Software – Canadian firm Absolute Software provides endpoint security and management solutions.
Arkoon – Arkoon merged with Netasq resulting in the Stormshield network and endpoint security protection solutions.
Atomicorp – The Virginia firm offers advanced security protections for Linux and Windows servers.
AT&T – Service providers such as AT&T manage mobile endpoints with advanced support for enhanced security.
Authentic8 – Authentic8 provides secure, authenticated access to Web apps through an isolated securely contained browser.
Autonomic Software – Autonomic provides endpoint management and security plug-ins integrated with McAfee's ePO.
Avecto – Avecto combines privilege management, application control, and sandboxing to provide endpoint security.
Avira– German anti-virus and Internet security provider includes range of endpoint security protections.
Barkly – Boston-based Barkly offers endpoint security that collects real time data to prevent malware attacks.
Beachhead – Beachhead provides subscription services to secure and manage mobile and PC devices.
Black Duck Software – The Burlington-based company offers a range of appliance and container security.
BlueRISC – Located in Massachusetts, BlueRISC provides hardware-assisted endpoint protection.
Bromium – Bromium provides endpoint security protection products that make use of a hardware assisted security container.
BUFFERZONE – Israeli firm BUFFERZONE provides an endpoint container security solution for enterprise.
Capsule8 – The start-up company offers advanced cyber security protections for Linux systems.
Carbon Black – The corporate merger of Bit9 with Carbon Black combined threat strength with endpoint capability.
CenterTools – The DriveLock solution from German firm CenterTools includes DLP and encryption.
Check Point Software – Check Point includes endpoint security solutions such as disk encryption for PCs.
Code42 – Minneapolis-based Code42 provides a range of secure data protection solutions for endpoint backup.
Confer – The Waltham-based company offers an endpoint senor that provides early warnings of malware.
CoSoSys – CoSoSys provides DLP, device control, and mobile device management with emphasis on endpoint security.
CounterTack – The Waltham-based company provides an endpoint protection solution for active retaliation.
CrowdStrike – CrowdStrike offers its advanced threat intelligence-based endpoint protection solution via its Falcon platform.
CyberArk – The acquisition of Cybertinel introduced signature-less endpoint security to the CyberArk offer set.
Cybereason – Cybereason combines endpoint security with enhanced analysis tools to reduce the risk of attacks.
Cylance – Cylance offers an advanced endpoint threat detection product using innovative malware detection algorithms.
Cynet – Cynet collects indicators and supports enterprise analysis for detection and mitigation of threat.
Deep Instinct – The San Francisco-based firm provides intrusion detection solutions for endpoints.
Dell – Tech company Dell offers endpoint encryption, endpoint management, and compliance solutions.
DeviceLock – Located in San Ramon, DeviceLock offers a range of endpoint device and port controls.
Digital Guardian – Digital Guardian provides an endpoint security product for data leakage and advanced threat prevention.
Druva – Sunnyvale-based company, Druva, offers endpoint security solutions to support data governance.
Dtex Systems – Dtex Systems focuses on insider threat protection using security analytics with behavioral pattern detection.
ESET – Traditional anti-virus and Internet security provider ESET includes range of endpoint security protections.
FireEye – The firm offers endpoint security protections to complement its virtual malware detection and response capability.
Fireglass – The company, now part of Symantec, offers browser isolation technology for endpoints.

Fortinet – Fortinet includes the advanced FortiClient endpoint security solution for its business customers.
Great Bay Software – The Minnesota-based firm offers endpoint security solutions for discovery and management of threats.
Guidance Software –The Encase Analytics product from Guidance Software includes EnCase Endpoint Security
Heat Software – Heat Software provides a range of unified endpoint management tools including security.
Impulse Point – Impulse Point focuses on network access policy enforcement and endpoint security.
McAfee – McAfee combines traditional endpoint security with popular ePO distribution system for enterprise.
Intelligent ID – The Ohio-based firm provides an advanced endpoint monitoring and protection solution.
InterGuard – Located in Westport, InterGuard offers employee-monitoring UBA solutions for the endpoint.
iScan Online – The Plano firm offers a range of endpoint scanning and vulnerability detection products.
itWatch – The German firm provides a suite of IT security products including endpoint protection.
Kaspersky – Russian anti-virus and Internet security provider Kaspersky includes a range of endpoint security protections.
Light Point Security – Light Point offers a virtual machine-based browsing solution to contain malware.
Lumension – Endpoint software and management company Lumension offers a range of data protection solutions.
Malwarebytes – Malwarebytes offers anti-malware and complementary endpoint security protections in their offering.
Menlo Security – Menlo Security provides agentless endpoint Web protections through on-premise or cloud based isolation.
NPCore – Located in Seoul, NPCore offers customers a suite of network and endpoint security products.
nTrepid – The Herndon-based company offers a fully-managed virtual machine-based VDI solution for enterprise.
Outlier Security – The Nevada firm provides agentless cyber security solutions for endpoint analytics.
Palo Alto Networks – Palo Alto Networks provides an advanced endpoint protection solution called Traps.
Panda – Spanish security provider Panda includes a range of endpoint security protections for Windows, Mac, and Android.
PFP Cybersecurity – PFP provides embedded integrity verification technology for industrial control and other endpoint devices.
Promisec – The company provides an agentless cloud-based or on-premise solution for securing endpoints.
Quarri Technologies – Quarri includes a range of data protection and armored browsing solutions for endpoint control.
Red Canary – The Denver-based firm offers managed endpoint security protections to detect advanced threats.
Safetica – Czech firm Safetica offers its customers with a range of endpoint security with DLP capabilities.
SentinelOne – SentinelOne is a start-up that provides next-generation endpoint protection products using predictive inspection.
SertintyONE – The Nashville-based company provides SmartDATA, which complements endpoint security solutions directly.
Sirrix AG Security Technologies – Located in Germany, the company offers endpoint security and trusted VPN solutions.
SkyRecon – SkyRecon's endpoint protection platform called StormShield offering suite of security features.
Sophos – Through acquisition of Invincea, Sophos obtained an advanced endpoint security container solution.
Spirion – New York-based Identity Finder searches computers including endpoints for sensitive information.
Symantec – Symantec includes endpoint security that will become integrated with the Blue Coat portfolio.
Tanium – Tanium provides ultra-fast endpoint scanning, analysis, and discovery through efficient queries.
ThreatTrack – GFI spin-off ThreatTrack includes a range of APT detection and prevention solutions for networks and endpoints.
Trend Micro – Traditional AV provider Trend Micro includes a range of endpoint security protections.
Trusted Knight – The company provides browser security protections including keystroke logging prevention.
Trustpipe – Trustpipe offers customers with an advanced endpoint security analytics and protection solution.
Wave – Wave provides the Safend Protector for endpoints, which uses encryption to safeguard data.
Webroot – Webroot offers endpoint anti-malware solutions with related Internet security controls.
Ziften – Austin-based Ziften offers advanced endpoint security solutions with enterprise security analytics support.

Control 19: Hardware/Embedded Security

The use of hardware and embedded security for cyber protection involves reliance on physical componentry to reduce risk, increase trust, and prevent malicious attacks to computing and networking systems. Reliance on hardware and embedded security has experienced clear reduction in emphasis during the past two decades as software and virtualized controls have taken over much of the responsibility for cyber protection. This has caused considerable debate, especially with respect to the use of hardware and embedded security to maintain protection in rapid, real-time contexts that require high performance. Network monitoring tools for large networks, for example, continue to rely on good hardware to keep up with capacity requirements. Nevertheless, the trend has been clear, especially as larger network gateways and systems are being distributed and virtualized. That said, a renaissance in

hardware and embedded security is occurring, albeit from different areas of cyber than the construction of hardware appliances for performance. Instead, a renewed emphasis on hardware and embedded security is occurring in IoT and ICS protection, as well as in the underlying trusted base required to support high assurance computing. These trends will introduce a fresh new emphasis on hardware and embedded security with recognition in the community that not everything can be totally virtualized. At some point, more tangible, physical controls play an important role in the cascading of trust from underlying platforms all the way up to application requirements such as authentication and access control.

General Outlook

The general outlook for hardware/embedded security involves transition from high emphasis, down to much lower emphasis, but then turning back up toward higher emphasis, albeit in different areas than then original focus. Specifically, the change will occur from using hardware to deal with increasing capacity needs to using hardware for increased assurance and trust, especially in IoT and ICS security. First generation hardware/embedded security from 1998 to 2007 involved hardware appliances as the platform base for most security tools, especially in environments where network and computing capacity growth was an issue. Second generation hardware/embedded security from 2007 to 2016 involved a clear shift to virtual appliance as network segmentation and virtualization began to accelerate in distributed environments. Such distribution tended to split the capacity requirements, as in micro-segmentation. Third generation hardware/embedded security from 2016 to 2025 should expect to see a major resurgence in emphasis as the need for underlying trusted hardware base computing will grow. A renewed focus on underlying assurance for applications such as trusted identity federation from hardware to application will also occur. Clearly, embedded security for IoT and ICS devices and systems will grow substantially during this period.

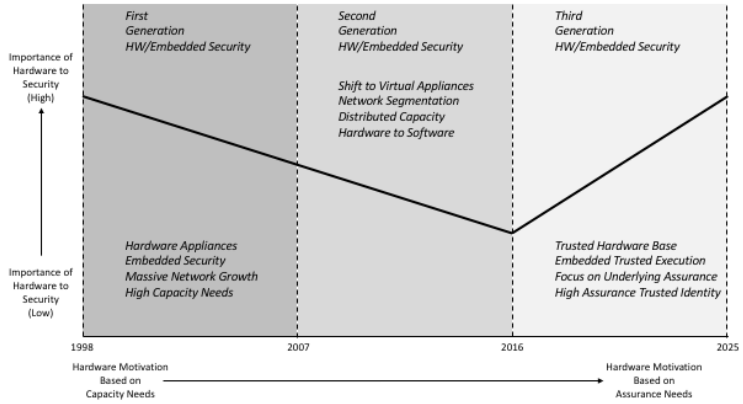

Figure 19. 2018 Hardware/Embedded Security Outlook

The TAG Cyber degree of confidence in this predictive outlook is moderate to high, given the clear increase in emphasis on IoT and ICS security across the entire community. Using trusted execution environments (TEE) as the basis for high assurance identity cascade and federation is an awesome idea, but its adoption remains somewhat to be determined.

Advice for Enterprise Security Teams

Enterprise teams are advised to continue to push security vendors to software-define and virtualize their underlying platforms, especially in the data center and WAN. Concurrently, however, they should begin to demand hardware-based, underlying trusted execution support for their applications both in the enterprise and across hybrid cloud environments. This is not an easy request to meet for most public cloud services such as in AWS or Azure. Nevertheless, the need to plant high assurance and trust in the underlying hardware, regardless of the computing environment, will grow. The approach for mobiles is slightly simpler, since TEE functionality exists in virtually all mobiles. The trick in the next decade is for enterprise security teams to begin using this high assurance computing. Obviously, if an enterprise team works in an IoT and ICS-rich environment, then the emphasis on hardware and embedded security will continue to increase, so little additional advice is required here to drive home that point.

Advice for Security Technology Vendors

Advice for vendors regarding hardware and embedded security really depends on their situation. For most vendors, the continued push to virtualize and software-define their platforms remains an important concern. This will neither shift nor slow down. Your customer demand virtualized capability and you will need to deliver in this manner or risk going out of business. That said, any opportunity to embed a cascading trust federation path from the underlying hardware up to the application will be well-received, especially for mobile. Vendors should take the time to review any opportunities to integrate with underlying TEE functionality, perhaps to support high assurance identity management. For vendors in IoT and ICS security, the emphasis on embedded security will grow, as will all other aspects of protection in these areas. Future directions might sort themselves out, but for now, the idea of embedding security into IoT or ICS devices and systems at the hardware level will be a valid and growing technique.

List of Support Vendors

Allegro Software – Allegro makes software for manufacturers to enable machines to embed onto the Internet.
BlueRISC – Massachusetts-based BlueRISC offers hardware-assisted endpoint security with anti-tamper features.
Device Authority – D-Factor is an authentication engine that supports trust for IoT applications.
Gemalto – Gemalto provides a range of digital security solutions including SIM card, NFC, and other embedded applications.
HID Global – The company provides devices that manufacture smart cards and other hardware identifiers and tags.
Icon Labs – Icon Labs provides embedded protection for IoT devices that connect via Modbus protocol.
Ingenico – The French firm provides retail secure payment and protection solutions for merchants.
Inside Secure – Inside Security provides embedded security solutions for mobile, content protection, secure access, and IoT.
Intel – Platform provider Intel embeds security into its underlying trusted execution processing and architecture.
Lynx Software – Lynx focuses on protecting real time embedded operating systems from malware.
NagraID – Located in Switzerland, NagraID makes high-end smart cards for identity applications.
Oberthur Technologies – The firm includes embedded digital security for transactions and other financial applications.
PFP Cybersecurity – PFP develops physics-based endpoint security with processor power consumption protections for IoT.
Rivetz – Steven Sprague's company Rivetz provides and support underlying trusted execution for mobiles.
Secure-IC – Secure-IC offers a range of sustainable embedded technologies that support threat protection.
Sequitur Labs – Sequitur focuses on hardware and embedded security for a range of advanced device management functions.
Skyport Systems – Founded by Stefan Dycherhoff, Skyport provides solutions for hardware and embedded security in servers.
Sypris – The Louisville-based firm offers trusted hardware manufacturing with focus on cyber security.
Tactical Network Solutions – The company provides digital forensics and analysis of memory and firmware.
Trustonic – Trustonic develops a secure environment that executes within smart connected products and devices.
Ultra Electronics AEP Networks – Ultra provides hardware security modules and cryptographic hardware support.

Watchdata – Located in India, Watchdata offers SIM cards for mobile with capability to support mobile payment.

Control 20: ICS/IoT Security

Cyber security solutions for Industrial Control System (ICS) and Internet of Things (IoT) infrastructure and applications involves the functional, procedural, and policy-based protections required to avoid malicious threats to these critically important capabilities. Both ICS and IoT infrastructure involves the hardware, electronics, control systems, software, and networks that manage, monitor, or control tangible, physical processes and devices. These tangible elements that comprise ICS and IoT range from components in major operations such as business factories and nuclear power plants to more whimsical devices such as kitchen appliances and home video recorders. The common element is that the associated controls range from analog or digital signaling at the hardware level all the way up to advanced software controls over IP networks. The cyber security implications of all this infrastructure are enormous and have been neglected, which makes this aspect of our industry appear much like the entire industry looked in the early 1990's. That is, ICS and IoT security are still being explored by both offense and defense. Some frameworks have emerged such as the Purdue Model that help explain the range of SCADA options, but this is still a green field for most cyber security vendors. Expect this area to take more shape in 2018 and to begin to blossom into one of the most vital aspects of cyber security in the coming decade. Virtually every aspect of the best available protections – ranging from risk analysis, to GRC tools, to 2FA, to advanced machine learning – will have to be recast in the context of ICS and IoT. This will create massive growth opportunities for vendors, but also big redesign efforts for purveyors of industrial and IoT systems.

General Outlook

The general outlook for ICS and IoT security involves transition from early stand-alone, hardware-based ICS and IoT systems to more virtual, cloud-based protections for ICS and IoT systems. This will be complemented by transition from the myriad of special, proprietary, non-standard protocols and systems being used to operate and security ICS and IoT infrastructure, to more open, standards-based ICS and IoT protections. New solutions such as unidirectional gateways will become more common in industrial environments. These trends track on-going shifts in the larger industry, so this should come as no surprise to any observer. The underlying trend during this shift from first to third-generation ICS and IoT security involves growth from tens of millions of deployed devices to tens of billions of deployed devices.

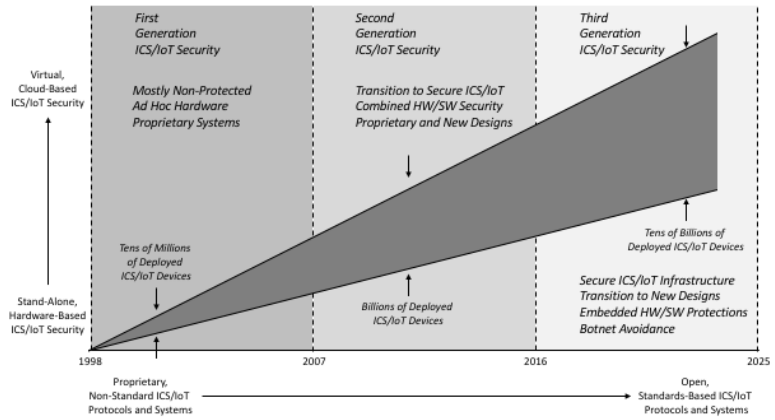

Figure 20. 2018 ICS and IoT Security Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since the transition has already begun for this massive increase in size, scope, and relevance of ICS and IoT. The shift to open, standard-based technology is slightly less certain since effective standards for securing industrial and IoT devices and infrastructure have not emerged to date.

Advice for Enterprise Security Teams

Enterprise security teams working in ICS and IoT environments must deal with the growing number of security vendors offering solutions in this area. 2018 is likely an excellent time to spend considerable time absorbing and learning the best available approaches from the most capable vendors. Many enterprise security teams will have to create sub-groups or identify individuals to specialize in this complex area. This will be more intense, obviously, for organizations that deal specifically with industrial or IoT devices – and this includes car companies, telecommunications companies, power plants, defense industry participants, and any associated government agencies.

Advice for Security Technology Vendors

ICS and IoT vendors are advised to carefully examine trends in the IT security space for major hints as to the types of controls that will be needed in the corresponding OT security space. This will lead to an ICS/IoT global offering roadmap that should mirror – albeit perhaps somewhat time-lagged – the deployment of new technologies such as machine learning, adaptive authentication, and automated SOC controls. The vendor space in ICS/IoT will no doubt become quite crowded in the coming years, and real vendors offering real solutions will have to work extra hard to differentiate themselves from more conventional cyber security vendors who decide to add “ICS and IoT security” to their marketing materials.

List of Support Vendors

Allegro Software – The Massachusetts-based firm offers ICS/IoT security solutions for embedded devices.
AT&T – AT&T integrates ICS/IoT product technology into its emerging SDN infrastructure.
Bayshore Networks – Bayshore Networks provides an appliance for securing ICS and Industrial Internet.
Berkana Resources – Berkana is a SCADA integrator offering SCADA security, compliance, and audit services.
Covisint – Covisint has expanded to secure IoT, supply chain, and identity and access management.

CyberX – CyberX provides security solutions for protecting industrial Internet from malicious attacks.
Digital Bond – Digital Bond provides professional services with emphasis on SCADA and ICS security.
Enet 1 Group – Enet 1 Group provides security services in SCADA, critical infrastructure, and mobility.
FireEye – FireEye includes a range of ICS security support as part of its extensive APT protection portfolio.
Fortinet – Fortinet includes ICS security support as part of its larger firewall and gateway security portfolio.
IBM – IBM includes a range of security product solutions for companies in the ICS and IoT space.
Icon Labs – The Iowa-based firm provides security solutions for IoT via portable software for embedded devices.
Indegy – Indegy provides security solutions for protecting industrial Internet from malicious attacks.
Inductive Automation – Inductive Automation provides a Web-based and cross platform solution for SCADA.
Innominate – German firm Innominate provides industrial, machinery, and related ICS security solutions.
IOActive – IOActive is a consulting firm with expertise in hardware and ICS systems including security protection.
Mocana – Mocana provides a mobile application security platform with support for embedded IoT devices.
MSI – ICS security solutions from MSI include protections embedded in the lower analog and digital layers.
NexDefense – NexDefense is an expert resource on cyber security protections for automation and ICS systems.
PFP Cybersecurity – The Virginia-based firm offers embedded integrity verification tools for IoT and other devices.
Radware – Radware's range of cyber security products include industrial control security protections.
Red Tiger Security – Red Tiger is a Houston-based consulting company with expertise in industrial security.
Rubicon Labs – Rubicon Labs provides a secure communications and key management solution for cloud and IoT.
SCADAhacker – SCADAhacker provides a range of training and consulting services for SCADA protection.
SecureRF – Located in Connecticut, SecureRF offers security solutions for wireless systems including NFC and IoT.
Securicon – The Virginia-based firm offers a range of security solutions for SCADA and process control.
SecurityMatters – Located in the Netherlands, Security Matters offers a platform for security protection of SCADA.
Siemens – The firm offers solutions for energy, automation, and other sectors with ICS security challenges.
Sophos – Sophos provides the Cyberoam network security appliances with support for ICS/IoT systems.
Synopsis – With the acquisition of Codenomicon, the company from Finland can test ICS/IoT devices and applications.
Tenable – Cyber security firm Tenable markets a range of offerings applicable to ICS/IoT applications.
ThetaRay – ThetaRay provides solutions for detecting threats in critical infrastructure and industrial systems.
Tofino Security – Tofino, a division of Belden, includes a security appliance for industrial network security.
Waterfall – The Israel-based firm provides advanced unidirectional gateway network security solutions for industrial control.
WISeKey – WISeKey provides security, authentication, and identity management solutions for mobility and IoT.
Wurldtech – Wurldtech is a GE company focusing on cyber security solutions for operational technology.

Control 21: Mainframe Security

Mainframe security involves the system administrative protection of traditional mainframe computers, operating systems, applications, and data sets from a variety of cyber attacks. This is the single, most mature aspect of information security, spanning five decades, but has the dubious distinction of being perhaps the least well-understood aspect of modern cyber protection in large companies and government agencies that still include mainframes. It is beyond the scope of this report to provide a tutorial on mainframe security, and 99% of readers would skip the narrative anyway due to boredom; but it is important to recognize that the skillset required to protect mainframes is dying off – *literally*. If you run mainframes, then the likelihood is high that your entire RACF or ACF2 protection team is long past retirement age and you are begging them not to leave. This is a grave risk to companies in this situation and must not be ignored. Since it is unlikely that your new-hire from Stanford will enjoy accepting a role running z/OS access controls, you can either accelerate moving mainframe apps to more modern virtual infrastructure, or you can select a good vendor partner to help you with your mature, mainframe infrastructure.

General Outlook

The general outlook for mainframe security involves transition from moderate percentages of infrastructure security including mainframes to a very low percentage including this type of computing. During the same period, the cost of mainframe security consulting and services has begun to increase, simply because the capability is becoming scarce. First generation mainframe security from 1998 to 2007 involved financial systems with heavy legacy back office systems running on mainframes with traditional protection tools. Second generation mainframe security from 2007 to 2016 saw most mainframes retired, leaving legacy systems with the requirement that they be protected as part of a dying art. Third generation mainframe security from 2016 to 2025 should expect to see rare legacy systems in stubborn environments remain with fewer tools and resources supported by a select group of specialized vendors offering professional services.

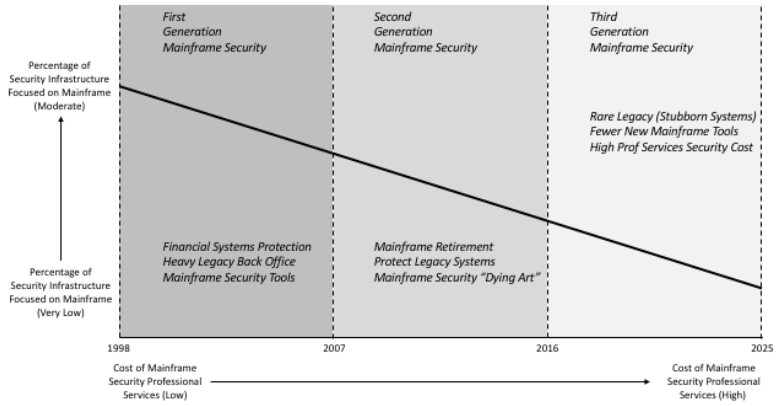

Figure 21. 2018 Mainframe Security Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, and the transition to higher cost professional services is already well-underway. Any CISO team that includes mainframes in its suite needs to focus immediately on this risk.

Advice for Enterprise Security Teams

Enterprise teams that include mainframes need to establish a plan for support that at least matches estimates for how long those systems will remain in operation. If the mainframe security team is beyond retirement age, then a human resource management plan is required to maintain support. If a vendor is in place or desired, then now is a good time to lock in a long-term deal. Regarding threats, I am willing to admit that I cannot think of a major malicious mainframe hack that has had significant business consequences for anyone in the past couple of decades. (Maybe we should all be moving everything back to mainframes.)

Advice for Security Technology Vendors

If you are in the mainframe security business, then you already know the good news/bad news situation. You customer base is dwindling, but the stubborn companies that love their mainframes and want to continue using them will remain excellent customers paying fair or even dear prices for your suite of solutions. Training newly-hired youngsters to be part of

mainframe security professional services offers can be a challenge, but when a twenty-two-year-old sees the money that can be made by learning ACF2 in detail, this challenge can sometimes be overcome.

List of Support Vendors
ASPG – ASPG is a Florida-based mainframe software company with a suite of products including security.
Atsec – Atsec is a security consulting firm that provides penetration testing services for mainframes.
CA Technologies – CA provides mainframe security governance, access management, and data protection.
Correlog – Correlog provides log management and SIEM functions, including support for mainframes.
Enforcive – Enforcive supports mainframe deployments and compliance programs for IBM z Security.
Ensono – Formerly Acxiom IT, Ensono provides hybrid IT services including support for mainframe.
IBM – The IBM company has been synonymous with the protection of mainframe products and services for many decades.
Imperva – Imperva acquired Tomium, which provides a mainframe security solution for continuous auditing.
Infosec Inc. – Infosec Inc. provides professional services specifically in mainframe, including security.
Interskill – Interskill provides mainframe training with catalog of IBM mainframe and security courses.
PKWare – PKWare offers a range of software solutions for mainframe including PKZIP and encryption.
Raz-Lee – The New York State-based firm offers audit, monitoring, and related compliance solutions for mainframe.
Safestone – Part of HelpSystems, Safestone provides customers with a range of IBM server security products.
Sea – Software Engineering of America provides data center solutions including for mainframe and security.
Software Diversified Services – SDS supports z/OS mainframe software with range of products and solutions.
Treehouse Software – Treehouse Software offers data integration and related solutions for mainframe.
Vanguard – Vanguard provides a range of IBM mainframe solutions including security protections.
Xbridge – Xbridge provides data discovery solutions with coverage for z Systems maintenance and security.

Control 22: Mobile Security

Mobile security involves cyber security controls in the ecosystem supporting the use of mobile devices, applications, and infrastructure. The evolution of this protection discipline lagged the development of early mobile services, simply because the earliest devices were not perceived to require any security at all. (Everyone seems to remember what they were doing on 9/11, so think back to the clunky mobile device you might have been carrying around on that terrible day. It probably had spotty coverage and no device security.) Not until Blackberry pioneered the concept of a secure enterprise server did the community begin to even consider the possibility that cyber risk was an issue. Fast forward to today, and the security challenge now will be to consolidate the myriad of different protections that scatter across mobile device, mobile app, enterprise mobility management, and mobile carrier infrastructure. Cloud-based virtualization support will be the common denominator in most of this consolidation so that protections can be selected largely independent of your physical device choices. Nevertheless, device-focused security will continue to be an important aspect of the mobile industry as the threat progresses. Expect also to see carriers offer much higher levels of security option in their 5G deployments. As a summary of components, below is a list of the major mobile security solution areas that will consolidate in the next decade:

- *Mobile Carrier Security Controls* – These protections will become software-defined in 5G infrastructure deployments.
- *Mobile Endpoint Security Software* – This software will become (surprisingly) less device dependent and more cloud controlled.

- *Mobile Device Management Tools* – These tools will embed into hybrid cloud enterprise IT orchestration systems.
- *Mobile App Risk Management* – This capability will improve and become a naturally-embedded aspect of all mobile app store and mobile app hosting systems.

Such consolidation around cloud and software-defined themes is good news, because it will counter the growing mobile threat across the globe. Expect to see some more serious mobile threat campaigns in the coming years. Hopefully, our improved mobility security systems and tools will be sufficient to keep us protected.

General Outlook

The general outlook for mobile security involves transition from weak mobile device infrastructure and protection to much stronger solutions for mobility security. This will track transition from the mobile as a complement to the traditional PC/LAN enterprise infrastructure to the mobile device as the essential basis for a virtualized hybrid cloud enterprise infrastructure. First generation mobility security from 1998 to 2007 involved weak carrier controls such as one-way tower authentication (in 2G services), weak encryption controls, and virtually non-existent local WiFi controls as it become more popular during this era. Second generation mobility security from 2007 to 2016 saw a plethora of new solution areas from vendors including mobile endpoint security tools, mobile device management (MDM) systems for security, and mobile app risk management suites. Third generation mobility security from 2016 to 2025 should expect to see consolidation of these capabilities with more advanced techniques such as machine learning embedded in the algorithms. Mobile app risk management will see increased focus, as well SDN-enablement of the underlying security infrastructure. Improved mobile device patching and configuration management will follow increased compliance pressure for companies.

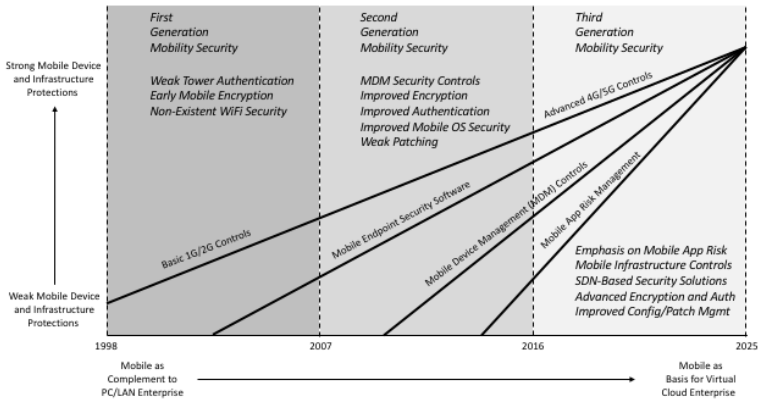

Figure 22. 2018 Mobile Security Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since mobile trends have been relatively easy to spot and track. SDN enablement with cloud support is the easiest trend to spot, and the flexibility of network function virtualization will allow designers to be more

creative in this mobile security space. One wild card that is especially intense for mobile security is that if a major mobile attack cascades across a large portion of global infrastructure, then the impact on the market, regulatory environment, and buyers is hard to predict. If anything, the focus on mobile security would become more intense, with compliance programs rapidly appended to include more stringent requirements.

Advice for Enterprise Security Teams

Current enterprise security team emphasis on mobile security varies considerably – and the variance does not seem to track any rational boundaries. For example, it would be easy to conclude that larger companies have greater emphasis, whereas smaller organizations do not, but this correlation is not crisp. Rather, what we see today is the usual sort of scattered emphasis one finds in a new discipline. Consider, for example, the use of mobile app risk management, an approach that is easy to deploy and sensible to incorporate. Use of this method across enterprise seems arbitrary with too many teams viewing this as a future consideration. My advice for enterprise teams is to step up to the plate now on mobile security with strong policy requirements, mandatory controls, and a three-year plan that takes advantage of emerging consolidation (or at least integration) of mobile device security, infrastructure controls, MDM, and mobile app risk solutions. This is no longer the security emphasis of the future: It must be a major security emphasis of the present. If you wait too long, then you might be explaining to your board these coming years why your team was caught flat-footed by a serious mobile attack that might have been prevented.

Advice for Security Technology Vendors

Analysts have been largely in agreement that growth will continue in the intensity of mobile threats, as well as our collective dependency on mobile in all personal and business affairs. These two conditions provide the perfect recipe for trouble, because corresponding emphasis on mobile security solutions – especially for personal use – is not increasing in any commensurate manner. Vendors must therefore focus on three agenda items: First, they must continue to educate the public and businesses to the growing risk. This should be done in a calm, matter-of-fact manner, because the potential use-cases speak for themselves. Unavailability of your mobile due to a massive malware worm hitting Android devices would be a catastrophe for anyone affected. Second, they must continue to focus on deployment and usage simplification. The easier it is for a given mobile security tool to be purchased and installed, the better. Third, all mobile security vendors must focus on consolidation through partnership, merger, or just integration testing. This is especially recommended for large mobile ISPs with emerging API-based SDN platforms. Creating an integrated suite of mobile security solutions centered on the carrier's SDN controller northbound application interface is an approach that will help everyone avoid mobile threats.

List of Support Vendors

Active Mobile Security – Active Mobile Security provides a mobile security solution for data separation and malware protection.
AdaptiveMobile – Adaptive Mobile provides mobile threat intelligence, protection, and infrastructure protection.
AirPatrol – AirPatrol supports location-based content delivery and security management for WiFi and mobile devices.
Apple – The mobile device provider includes novel security features in iTunes, iOS, and across the Apple mobile ecosystem.
Appthority – Appthority offers enterprise mobile app security analysis to support data loss and privacy risks.

Arxan – Arxan protects mobile, desktop, embedded, and server applications including a mobile app assessment.
AT&T – AT&T offers advanced options, increasingly based on SDN, for their enterprise customers in mobile security and MDM.
Avast – Acquisition of Remotium provides Avast with a range of secure mobile enterprise solutions.
AVG – AVG offers anti-virus and optimization for endpoints including Android mobiles and tablets.
BETTER – BETTER supports detection and prevention of mobile attacks to Android and iOS.
Bitdefender – Bitdefender provides a range of endpoint security protections include support for mobile.
Blackberry – Blackberry offers a wide range of secure mobility and mobile device management solutions.
Box – Box provides mobile security by supporting extending content securely across all mobile devices.
BullGuard – Anti-virus protections for endpoints from BullGuard include support for Android security.
Check Point Software – Acquisition of Lacoon brings Check Point a mobile threat prevention solution.
Cyber adAPT – Cyber adAPT offers a unique integration of cyber attack prevention with mobile threat avoidance.
eAgency – eAgency is a provider of mobile security products for consumers, business, and carriers.
ESET – Anti-virus and security protection for endpoints from ESET includes advanced protection support for Android.
F-Secure – F-Secure anti-virus and security solutions include support for smartphones and tablets.
Google – Google includes many useful cyber security features in the OS and supporting ecosystem.
Huawei – The large Chinese technology company offers a range of security products including mobile security.
IBM – The IBM MaaS360 enterprise MDM solution includes mobile security capabilities.
Icon Labs – Headquartered in Iowa, Icon Labs provides embedded device security, including support for mobile.
IntegriCell – Washington-based IntegriCell, led by industry expert Aaron Turner, provides a range of mobile security solutions.
ITADSecurity – ITADSecurity offers a range of security risk intelligence solutions for mobile devices.
Kaprica Security – Kaprica Security offers penetration testing services with emphasis on mobile security.
Kaspersky – Kaspersky offers mobile device protection including password manager, safe browsing, and QR scanning.
Lookout – Lookout provides advanced anti-malware software tools for protection of mobile devices, data, and apps.
McAfee – McAfee offers customers its Mobile Security solution for Android and iOS mobile devices.
MobileIron – MobileIron offers MDM security capabilities such as certificate exchange for multi-factor authentication.
Mocana – Mocana provides mobile security threat containment through software application wrapping.
mSignia – Irvine-based mSignia offers technology to support strong authentication and fraud prevention on mobile apps.
NowSecure – Illinois-based NowSecure provides mobile security and privacy for Android smart phones and tablets.
NQ Mobile – Anti-virus protection from NQ Mobile is designed for Android and Windows devices.
Nubo – Nubo provides protection for BYOD remote enterprise secure workspace for mobile devices.
Omlis – UK-based firm Omlis supports a range of mobile payment solutions with support for cyber security.
Phone Warrior – Phone Warrior supports Spam call blocking, text blocking, and Caller ID functions for mobile.
Pradeo – Located in France, Pradeo offers a suite of mobile application security testing tools and APIs.
Proofpoint – Through acquisition of Marble, ProofPoint offers mobile application security based on cloud threat intelligence.
Protected Mobility – Protected Mobility, headquartered in Virginia, offers solutions for mobile app security.
Pulse Secure – Pulse Secure, a Juniper spin-off, offers a range of SSL VPN and mobile device security.
Rapid7 – Rapid7 acquired Mobilisafe in 2012, which provided them with advanced capability in mobile security.
Samsung – Samsung offers the Knox suite of mobile enterprise security solutions for device protection and management.
SAP – SAP Mobile Secure provides a software-as-a-service capability to manage mobile protection.
Sequitur Labs – The small company in Washington State offers mobile security application development tools.
Skycure – Skycure, led by Adi Sharabani, offers a range of advanced mobile intrusion detection and prevention solutions.
SnoopWall – SnoopWall offers a range of malware detection solutions for tablets and mobile devices.
Sophos – Sophos Mobile Security provides customers with advanced security protection for Android devices.
Symantec – Symantec provides MDM and mobile security solutions for enterprise and consumers.
TekTrak – TekTrak offers a range of mobile application security products for Android mobile devices.
Trend Micro – Trend Micro offers security protection for Android including mobile device management.
TrustGo – Part of Baidu, TrustGo offers mobile security solutions for app scanning and other features.
Trustlook – San Jose-based Trustlook offers anti-virus, anti-Spyware, and other security capabilities for Android devices.
Verizon – Verizon offers a range of protection options for their enterprise customers in mobile security and MDM.
V-Key – Redwood City-based V-Key employs intrusion prevention protection for mobile applications.
VMware – VMware offers a range of mobile virtualization and application wrapping for cyber security.
Webroot – Webroot offers customers its SecureAnywhere Mobile solutions for Android smart phones.
Workspot – Workspot offers a secure virtual desktop solution for the enterprise with cloud support.
Zimperium – Zimperium offers enterprise mobile security solutions supporting enterprise BYOD initiatives.

Control 23: Password/Privilege Management

Password and privilege management involves the people, processes, and tools required to properly control and protect passwords and privileged accounts in an enterprise. IT, network, and application teams recognized years ago that enterprise identification and authentication required more focused attention in two areas: Passwords were being poorly selected and routinely mishandled by virtually all users, and privileged account neglect had particularly significant consequences for any enterprise. As such, tools emerged to improve both areas, and have grown in use over the past two decades. Even with advances in multi-factor, adaptive authentication, the use of password and privilege management tools will continue to grow in the coming years. This is an enterprise control where the risk equation works out quite well; that is, modest investment produces great benefit. The only reason these tools have not grown more rapidly is that decisions for password and privilege management are often made in the organizational seams between security and IT teams. Vendors in this area are often unsure who their customer really is, in an enterprise. This has slowed the growth of proper infrastructure solutions in these areas.

General Outlook

The general outlook for password and privilege management involves transition from simple administrative controls such as password stuffers to more advanced analytic tools that will take advantage of behavior algorithms to improve usability and accuracy. Password and privilege management tools, including password vaults, will move from stand-alone tools to more embedded capabilities in the systems that comprise hybrid cloud-based virtual infrastructure. First generation password and privilege management tools from 1998 to 2007 involved the simplest password managers, mostly for PCs with non-privilege focus to combat weak threats. Second generation password and privilege management tools from 2007 to 2016 saw much improved tools, increasing used to handle 2FA. Enterprise focus on protecting privileged accounts grew during this period, to address many privilege weaknesses that stemmed from ignorance and basic system administrative neglect. Third generation password and privilege management tools from 2016 to 2025 should expect to see massive transition to MFA which will require more advanced, embedded controls. Machine learning and analytics will help this area of enterprise cyber security deal with more advanced threats.

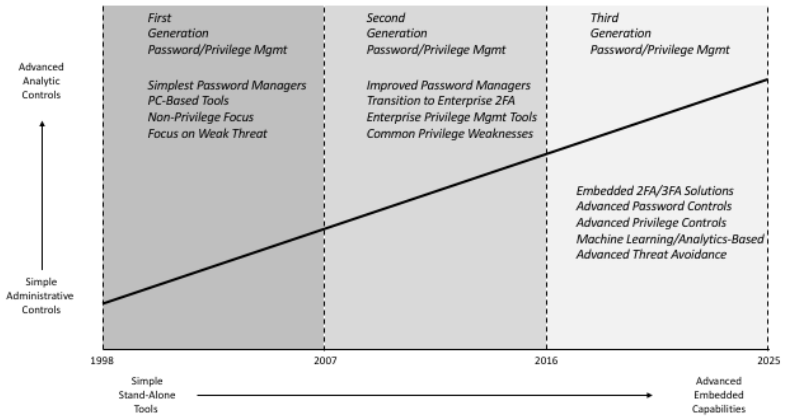

Figure 23. 2018 Password/Privilege Management Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since the growth of password and privilege management tools and systems has been steady. Passwords will not go away in personal and enterprise use, but will rather see complement by 2FA and adaptive authentication. Growth will continue steady over the coming decade.

Advice for Enterprise Security Teams

Chances are that your team is doing a much better job today managing user passwords than you did a decade ago. Chances are also, however, that you could stand to improve your management of privileged accounts. Too many privileged access use-cases do not include sufficient mandatory control of proof tokens in proper vaults with centralized oversight. APTs often take advantage of this enterprise system administrative weakness to build power during lateral traversal inside a perimeter. Security teams are thus advised to first take inventory of their privileged accounts, which by the way, is often the most difficult aspect of proper protection. Sufficient diversity of vendors exists today to build out improved solutions for securing privileges, so there are no longer the types of supply chain issues that existed in this area when it first emerged.

Advice for Security Technology Vendors

Vendors providing security management support for password and privileged accounts should keep at it, because tangible benefits and growth have occurred in the past decade. Since the organizational seams between IT and security will continue, you must step up your education and awareness programs, because not all IT decision-makers understand the tools you offer. Virtualization and shift to hybrid cloud will only increase the need to centralize control of distributed account management across heterogeneous as-a-service capabilities. Expect to see continued growth, but you will need to expect some native capabilities emerge from cloud and SDN providers. This might be a good opportunity for IP licensing or partnership.

List of Support Vendors

AgileBits – Canadian company AgileBits offers the 1Password solution for personal and enterprise use.
Animabilis Software – Animabilis offers a full-featured password storage and management solution for enterprise.
Avatier – The global firm offers password management as part of its identity and access management suite.
Avecto – Avecto combines privilege management, application control, and sandboxing to provide endpoint security.
BeyondTrust – BeyondTrust provides password, privileged account, and vulnerability management solutions.
Bitium – Santa Monica-based Bitium provides password, user, and identity management solutions.
CA – CA offers the Privileged Access Manager product for fine-grained user access controls in the enterprise.
CyberArk – CyberArk provides privileged account management and security solutions for the enterprise.
Dashlane – Dashlane offers the Dashlane Password Manager and Secure Digital Wallet products.
DataViz – DataViz includes a product called PasswordPLUS for organizing passwords across iOS, Android, Mac, and Windows.
Dell – Dell provides a range of privileged account management solutions for Unix, Windows, and other environments.
Fischer International – Fischer offers a range of password, privilege, and identity management solutions.
Fox-T – Mountain View-based Fox-T offers access management and password/privilege management solutions.
Hitachi-ID – Hitachi-ID includes privileged access management in its identity management and access governance solutions.
IBM – IBM includes privileged identity management in its suite of identity and access management solutions.
KeePass – KeePass is an open source password manager that might be considered for use in the enterprise.
Keeper Security – Keeper Security includes a password manager capability and secure digital vault.
Lamantine Software – Lamantine Software develops a password manager and form filler called Sticky Password.
LastPass – LastPass offers a password manager, auto form filler, random password generator, and secure digital wallet.

Lieberman Software – Lieberman Software supports identity, passwords, and privilege management.
ManageEngine – ManageEngine includes privileged password management and self-service password management solutions.
mSeven Software – mSeven Software provides a password manager for Mac and Windows users.
MyLOK+ – MyLOK+ offers its customers a secure password manager and data storage capability.
NetWrix – NetWrix offers IT security and auditing solutions for protecting systems and applications across IT infrastructure.
OneID – Redwood City-based OneID offers identity, access, password, and privilege management.
Oracle – Oracle offers password and privileged identity management functions in its identity and access management solutions.
OrangeCat Software – Orange Cat Software offers a password keeper product solution for its customers.
Osirium – UK-based Osirium offers identity, access, password, and privilege management solutions.
Password Genie – Password Genie is a data protection and password security solution for Windows, Mac, Android, and iOS.
RoboForm – RoboForm provides its customers with an advanced password management capability.
SplashID – SplashID supports management of passwords for iPhone Android, Windows, and Mac.
Symantec – Symantec includes identity access manager capability in its information protection suite.
Thycotic – Thycotic offers complete privileged account management solution for enterprise IT administrators.
Wallix – Wallix provides SSO, password management, privileged user management, and related functions.

Control 24: Two-Factor Authentication

Two-factor authentication (2FA) solutions provide increased assurance in the validation of reported identities. Generally, 2FA is used to enhance the security of remote or on-line service access from users who had previously just supplied passwords to prove their identities. To reduce the likelihood of malicious spoofing or fraud, a second (or third) diverse factor is added to increase the difficulty of an attacker guessing, stealing, or deriving access to a target system or account. Popular 2FA methods include hardware or software tokens, public key certificates, biometric identifiers, and text exchange of codes with known mobile devices. Enterprise security teams commonly include 2FA as an assurance requirement for external access to shared services, so the progression to hybrid cloud will naturally cause increased deployment of this technology. Consumers are likely to remain skeptical of 2FA, however, for the foreseeable future in their access to social media, Internet email, and other on-line services. Eventually, the use of contextual, adaptive authentication will dominate, based on behavioral analytics and situational characteristics including location and observed ergonomics; but this might take a bit longer than most expect, simply because old habits die hard. Expect passwords, plus a simple second factor to remain the baseline 2FA choice for several years, after which the technology will become more streamlined. One new aspect of 2FA that should emerge in the coming decade involves the greater use of trusted execution environment (TEE)-hosted identities that are cascaded directly to applications without interaction with the operating system. This results in a super high assurance authentication process that result in the actual device becoming a trusted proof factor. Issuance of known devices, for example, that are provisioned with highly assured cryptographic identities allows for secure public cloud access without a perimeter.

General Outlook

The general outlook for two-factor authentication involves transition from a simple, add-on second factor to adaptive, contextual authentication – albeit over a slower than expected period. This is complemented, however, by a transition from low use of 2FA in the late 1990's to more intense use of the technology across all types and sizes of enterprise in the coming decade. First generation 2FA from 1998 to 2007 involved hand-held tokens (mostly from RSA)

used in larger enterprise and government organizations, but with almost no use by consumers. Second generation 2FA from 2007 to 2016 involved the addition of some new types of 2FA tokens including biometrics and certificates, as well as software tokens. Early adaptive and contextual authentication solutions emerged during this period. Third generation 2FA from 2016 to 2025 should expect to see the gradual transition to 3FA, but when the transition does occur, it will be heavy. That is because once adaptive authentication solutions become super easy to use, every enterprise and even every consumer will become heavily vested in the technology. Expect the transition to be slow in coming, but rapid once it does come. Also expect to see TEE-based authentication solutions turn mobile devices and even PCs into token authenticators themselves with trust coming from high assurance provisioning of cryptographic identities. Mobile service providers will naturally gravitate toward this type of business.

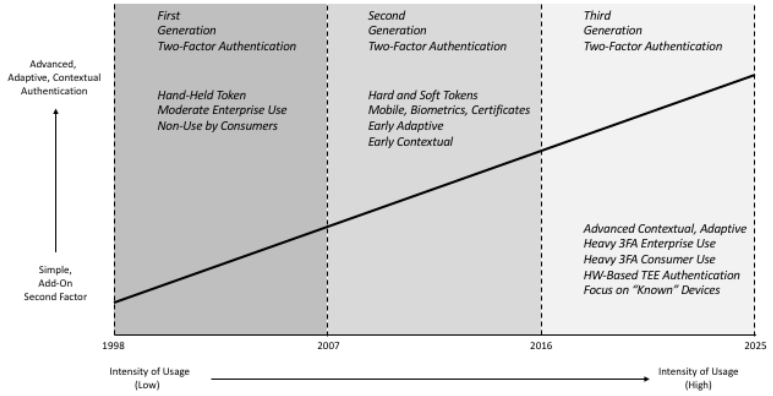

Figure 24. 2018 Two-Factor Authentication Outlook

The TAG Cyber degree of confidence in this predictive outlook is moderately high, given the pattern that has been established for early 2FA adoption by a wider segment of business. Confidence levels are not high, however, simply because predicting user preferences in this area can be hazardous. For example, PKI-based usage predictions for consumers made twenty years ago with high confidence, never came true.

Advice for Enterprise Security Teams

Enterprise teams should already be using 2FA for remote access, as well as access to shared services in public clouds. If they are not, and this might be more common for smaller companies, then it is time now to make the transition. Start by writing "should" requirements for user access to anything of value, and eventually transition to "must" requirements. Selection of second factors should be consistent with the local culture and environment. Mobile devices are generally ubiquitous in business settings, so text-based exchange of mobile codes is a natural method. In environments, where endpoints are issued by the IT or OT administration team, the provisioning of an underlying certificate, enabled with a device biometric might be the preferred approach.

Advice for Security Technology Vendors

Companies providing 2FA solutions are in an excellent position to experience continued growth for many years. The challenge is that eventually, the issuance of identity proof will become embedded in the behavioral analytic process, so that could spell trouble for existing solutions. Widespread adoption of adaptive and contextual methods remains hard to forecast, and some aggressive vendors trying to innovate in this area have seen their early solutions fizzle. This is a natural artifact of any transitioning new technology, and it highlights the importance of perfect timing in the introduction of a change in commonly used computing methods. My advice would be to maintain good programs of R&D in adaptive solutions, but to remain pragmatic about revenue opportunities in the near term. Once it becomes clear that 2FA solutions are truly becoming more embedded into contextual analytics, the more attentive vendors should be ready to make the transition, albeit in the role of follower (which might be better anyway).

List of Support Vendors
Authentify – Authentify, part of Early Warning, offers phone-based multi-factor out-of-band authentication (OOBA) solutions.
AuthLite – Located in Springfield, AuthLite offers two-factor authentication using a USB key and password.
AuthRocket – Colorado-based AuthRocket provides a user management API to support authentication as a service.
Authy – Authy provides a two-factor authentication smartphone application for individuals and business.
Auth0 – Auth0 supports software developers with SSO, token, and related products for integration into apps and APIs.
Behaviosec – Swedish firm Behaviosec provides a biometric authentication solution based on behavioral attributes.
BI2 Technologies – Biometric intelligence and identification technologies firm BI2 technologies is based in Massachusetts.
Blackridge – The company utilizes first packet authentication to enforce strong network access control policy.
CA – CA offers strong authentication services embedded in its range of identity and access management solutions.
Celestix – Fremont-based Celestix provides unified remote access to any application on any device using single sign-on.
MIRACL – The company provides a two-factor encryption and authentication solution, as well as a cryptographic SDK.
Collective Software – Collective Software provides the AuthLite two-factor authentication system.
Comda – The Israeli firm offers a range of IT security products including biometric authentication.
Crossmatch – Crossmatch offers its DigitalPersona Altus solution for biometric identity verification and enrollment.
Cyxtera – Cyxtera's Easy Solutions includes mobile and strong authentication in its suite of anti-fraud solutions.
Daon – Daon is a biometrics identity management company with an underlying Biometric Trust Infrastructure.
Deepnet Security – Deepnet, located in the UK, offers an authentication platform using multifactor and biometric solutions.
Delfigo – Delfigo develops a range of identity-based strong authentication services for customers.
Delta ID – The California-based firm provides the DeltaID iris recognition solution for strong authentication.
Device Authority – The D-FACTOR authentication engine delivers connected devices for IoT applications.
DirectRM – Located in California, DirectRM provides strong authentication and access management solutions supporting BYOD.
Duo Security – Duo Security provides two-factor authentication solutions with emphasis on endpoint visibility protection.
DynamiCode – Located in Hong Kong, DynamiCode offers strong authentication and secure mobile POS solutions.
ECKey – The Pennsylvania-based firm offers solutions for turning Bluetooth smartphones into access control components.
ElevenPaths – The Madrid-based company provides a range of security products including authentication.
Entersekt – Located in South Africa, Entersekt provides interactive authentication and encryption solutions.
Entrust – Entrust provides identity and authentication technologies using mobile, certificates, and other technologies.
FEITIAN Technologies – The Chinese firm offers a range of IT security solutions including authentication.
Gemalto – Gemalto provides digital security solutions ranging from biometrics to SIM card and NFC security.
HID Global – HID Global includes access control and secure identity solutions including smart cards and readers.
Hoyos Labs – Hoyos Labs offers a range of mobile biometric solutions for strong two-factor authentication.
ID Control – Located in the Netherlands, ID Control provides a range of strong authentication solutions.
Idevity – Idevity supports smart card and identity use with visualization apps for mobile and related products and services.
ImageWare – ImageWare provides biometric solutions to support authentication and identity management.
Imprivata – Massachusetts-based Imprivata focuses on single sign-on, authentication, and related solutions for health care.
Iovation – Located in Portland, iovation supports on-line fraud prevention based on strong device authentication.
i-Sprint Innovations – Located in Singapore, the company supports identity, credential, and access management solutions.
Keypasco – Swedish firm Keypasco offers secure authentication, multi-factor, and device authentication.
Mi-Token – Mi-Token develops a range of two-factor authentication solutions based on soft tokens.
mSIGNIA – mSIGNIA provides mobile authentication enhanced with biometric device recognition.
Nok Nok Labs – The firm provides a streamlined strong authentication protocol based on Fast Identity Online (FIDO).

Nymi – Nymi enables secure, continuous authentication through a wearable, multi-factor biometric device.
OneLogin – OneLogin offers cloud-based IAM with secure access to cloud applications from mobile devices.
OnWire – OnWire includes a FedRAMP, multi-factor authentication platform with cloud based IAM.
PointSharp – The PointSharp mobile app provides authentication via software-based one-time password token.
Protectimus – UK-based firm Protectimus offers customers a range of two-factor authentication solutions.
RSA – RSA offers one-time password token solutions that are in use around the world.
Ingenico – Ingenico's SafeNet provides enterprise authentication as part of its suite of security solutions.
Salesforce Identity – Salesforce Identity provides federated identity services.
Seamoon – Chinese company Seamoon provides a one-time password authentication solution for its customers.
SecSign – Located in Nevada, SecSign provides two-factor authentication, encryption, and related capabilities.
Secure Access Technologies – Secure Access Technologies provides mobile authentication via the SAT Mobile ID solution.
SecureAuth – SecureAuth supports two-factor authentication and SSO for enterprise applications.
SecurEnvoy – UK-based SecurEnvoy offers mobile phone-based tokenless two-factor authentication.
SecureKey – SecureKey, located in Canada, supports identity and authentication needs for online consumer services.
SecurePush – Israeli firm, Secure Push, offers its customers a strong multi-factor authentication platform.
SecuTech – Canadian firm SecuTech offers the UniKey and UniToken solutions for USB-based plug-and-play authentication.
Socure – Based in New York, Socure provides social biometric solutions for identity verification.
Sonavation – Sonavation is a biometrics firm supporting identity authentication and other security solutions.
SSH – Headquartered in Finland, SSH provides SSH key management, access, and authentication support.
StrikeForce Technologies – Headquartered in New Jersey, StrikeForce provides out-of-band authentication.
SurePassID – SurePassID supports next-generation identity and access management with FIDO authentication and secure IoT.
Swivel Secure – UK-based Swivel Secure provides strong authentication for cloud, Web, VPN, and desktop.
Syferlock – Connecticut-based Syferlock offers a range of token-less solutions for multi-factor authentication.
Symantec – Symantec provides cloud-based validation and ID protection services for secure multi-factor authentication.
Synaptics – Synaptics supports high-end technology in the touch sensing and display integration area.
TeleSign – The California-based company offers a range of mobile identity and authentication solutions.
Transmit Security – The company, run by Rakesh Loonkar, offers a range of programmable biometric solutions.
TRUSTID – Located in Oregon, TRUSTID offers customers a range of automatic caller identity validation capabilities.
Twilio – Twilio provides a range of messaging, voice, and authentication APIs for customer applications.
2FA – The Austin-based company offers customers a range of two-factor authentication solutions.
Usher – Usher provides biometric, location-based authentication solutions for business and individuals.
Vasco – Illinois-based Vasco provides solutions for strong authentication, digital signature, and identity management.
Vir-Sec – The Florida-based firm provides a range of multi-factor authentication access to applications.
VU Security – Headquartered in Argentina, VU Security offers two-factor authentication solutions.
WWPass – WWPass provides strong two-factor authentication solutions using cryptography techniques.
Yubico – The Swedish firm provides an advanced, open source, USB authentication solution for platforms.

Control 25: Voice Security

Voice security consists of special encryption-based protections that address secrecy and authentication weaknesses in mobile voice and text conversations. Most voice security solutions are designed as end-to-end software apps, evolved from many previous hardware products, that operate over-the-top on user mobiles. Key management solutions have improved to the point where end users generally must do little more than download the app and participate in groups of other users with the app. A major use-case that motivates deployment of voice security solutions involves executives and others who must travel to regions of the globe where the underlying mobility infrastructure might be less trustworthy or robust. Voice security solutions must deal with the challenge of generally lesser recognition among consumer and business users of the secrecy threats that exist for mobile voice and text communications. This is exacerbated by the common practice of authenticating Internet transactions with texts, which implies much higher levels of security. While this might be

somewhat true, voice and text traffic is now digital, so the likelihood of malicious eavesdropping is growing. Luckily, voice security solution quality is now excellent.

General Outlook

The general outlook for voice security involves an increase in intensity of the disclosure threat, along with the obvious transition from heavy landline voice to heavy mobile 4G/5G communications in the coming years. First generation voice security solutions from 1998 to 2007 involved early transition to mobile with weak encryption solutions from many carriers. Most of the voice security issues for mobile involved cell cloning, and the only real encryption tools were used in government and the military. Second generation voice security from 2007 to 2016 involved an increased disclosure threat, such as SS7 weaknesses, through rapid growth of smart phones. The recognition of this growing disclosure threat, especially for travelers, remained weak, however. Encryption improved considerably during this period, especially from mobile carriers. Third generation voice security from 2016 to 2025 should expect more intense disclosure issues, routine voice communication leaks to places like WikiLeaks, stronger encryption, and more routine use of higher quality solutions.

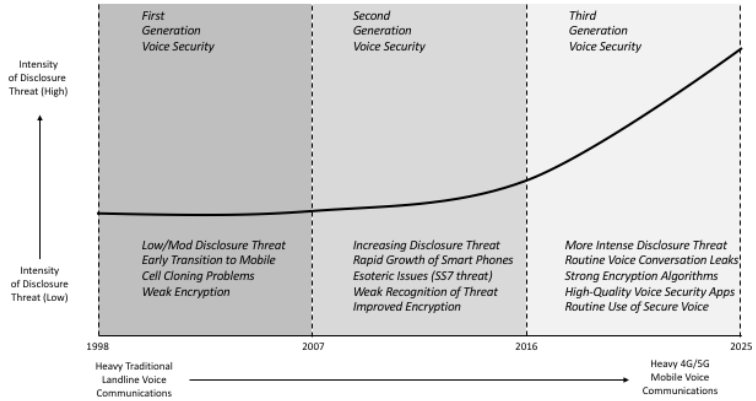

Figure 25. 2018 Voice Security Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, but additional work is required to help business users understand the potential threat. If some prominent business or government executives see their voice communications posted to WikiLeaks, then the use of voice security tools will most certainly grow quickly. Few compliance frameworks include voice security as a requirement, and the likelihood that this will change is moderate, since most regulatory and audit teams will tend to carry over previous requirements into any new framework updates.

Advice for Enterprise Security Teams

If your executives travel, then they should be using encryption-based security apps for their mobile voice and text communications. The cost is low, the administration is low, and the benefits are considerable, especially in global regions where the voice infrastructure is less trustworthy. To extend the use of voice security across the entire employee base is surprisingly

simple and low cost, so this is one of those unusual areas of cyber security where active adoption is a no-brainer. Nevertheless, voice security use at scale is remarkably low, so go figure. My advice is to give this control a fresh look in the coming years – and if some company watches its sensitive merger talks or confidential earnings discussions posted to WikiLeaks, then you will be ready to address the risk.

Advice for Security Technology Vendors

Most voice security solution vendors have been hard at work improving the secrecy, key management, usability, and quality of their products during the past years. My advice is to focus on education and awareness, producing good content for potential buyers to understand how much better voice security quality and usability have become. Many personal and enterprise buyers continue to think that voice security is for government spooks and conspiracy kooks, so this will require some doing. Keep at it – and the dividends will come during the next few years.

List of Support Vendors

AEP (Ultra Electronics) – The UK-based firm provides HSMs for data and voice security protection.
AT&T – The ISP/MSP will design a secure voice solution that can integrate with managed security and threat intelligence.
Cellcrypt – Cellcrypt provides a range of voice security solutions with encryption and related protections.
CellTrust – The company provides a secure voice and messaging security gateway and aggregation solution.
CoverMe – CoverMe is a free download for Android and Apple to encrypt mobile communications.
Enigmedia – Headquartered in Spain, Enigmedia provides solutions for secure voice and telepresence.
General Dynamics – General Dynamics offers Sectera Wireless GSM phone for secure communications.
Koolspan – Koolspan offers solutions for voice, texting, and messaging security for enterprise and mobile voice platforms.
Nuance – The firm provides a range of advanced knowledge-based and voice biometric solutions.
Ostel – The Jitsi app from Ostel offers encrypted, open source tools resulting in secure voice comparable to Skype.
Phone Warrior – Phone Warrior supports Spam call blocking, text blocking, and Caller ID functions for mobile.
Pryvate – Pryvate offers encryption products for secure voice, video, IM, and related communications.
RedPhone – RedPhone is a free, open source, secure voice application for Android created by Whisper Systems.
SecureGSM – Australian-firm SecureGSM provides a range of mobile communication security solutions.
SecureLogix – SecureLogix offers secure telephony infrastructure controls for service providers and enterprise.
Secure Mobile – The division of SiRRAN Communications offers encryption-based security solutions for mobile.
Silent Circle – Silent Circle provides encryption designed by Phil Zimmerman with high levels of privacy protection for users.
Simlar – Simlar is a German-developed app for security mobile with support for Apple and Android.
Sophos – The well-known security firm offers its SafeGuard encrypted voice security solution for customers.
T-Systems – The large technology and information assurance company offers a voice encryption application.
Twilio – Twilio offers a range of voice and messaging secure infrastructure protection solutions for customers.
Verizon – The large mobile carrier offers secure voice solutions through a business partnership with Cellcrypt.
VIPole – VIPole is a secure messaging application developed in the United Kingdom for secure business communications.
Voice Security Systems – The California-based company offers technology solutions for voice security protection.
Whatsapp – Whatsapp is an application claiming a billion users with embedded cryptographic protections for privacy.
ZoIPer – ZoIPer is a SIP softphone product with a range of advanced encryption-based security features.

Control 26: Brand Protection

The area of brand protection involves techniques to monitor and mitigate digital risks from social networks, websites, email, and on-line services that can adversely affect the reputation, integrity, and public view of a company's assets. The primary umbrella asset for an organization is its brand, but more specific components at risk of digital spoofing, tampering, fraudulent use,

and misrepresentation include corporate domains, websites, e-commerce sites, certificates, and other designations that would be purported to have been created with the full authority of the organization. This is a new area of cyber security, one that is undergoing transition from teams of human investigators trolling and scraping websites in search of keywords, to more automated platforms that use advanced analytics to detect, learn, and mitigate any identified brand issues. Vendors differentiate today based on a combination of their team experiences and platform features, so buyers will generally have to examine both. Most CISOs have traditionally not been involved in this aspect of cyber security to date, so the possibility exists that public relations or marketing teams might have already been buying adjacent capabilities.

General Outlook

The general outlook for brand protection involves transition from simple search methods such as screen scraping to more advanced *digital risk monitoring* including the use of data analytics. The transition of buyer focus for this type of protection is also shifting from marketing and brand management teams to expanded involvement of enterprise security team buyers. First generation brand protection from 1998 to 2007 involved simple data collection from the Internet with some early Dark Web investigation. Techniques involved screen scraping and the focus was on very basic brand protection. Second generation brand protection from 2007 to 2016 involved expended data collection and navigation across the Internet and Dark Web in search of brand fraud and misrepresentation. Early risk analytics emerged during this period which allowed for more serious threat to be monitored and even mitigated. Third generation brand protection from 2016 to 2025 should expect to see a more comprehensive, Big Data analytic-based approach to digital risk monitoring and mitigation. All-source investigation will power these methods which will provide stronger brand protection and identification of much more serious threats to brand, domain, and reputation.

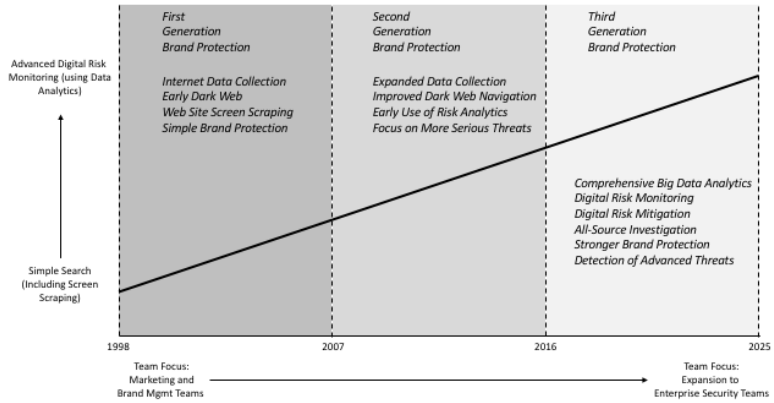

Figure 26. 2018 Brand Protection Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since this risk has become so much more prominent. One could argue that the Russian hacking of the US elections in 2016, for example, involved large-scale brand and reputation tampering against one of the political parties in the United States, and that this attack might have been addressed by a

national program of digital risk monitoring and brand protection. Gradual recognition of this fact will tend to highlight the importance and practical application of these new protection measures.

Advice for Enterprise Security Teams

Enterprise security teams should educate themselves immediately about the value of digital risk monitoring and brand protection. Many excellent new vendors have emerged that can be interviewed, tested, and partnered with to create a new program, where one previously did not exist. Platform solutions are now more professional (less emphasis on site scraping) with advanced analytics that can learn to recognize potential digital risks to organizational assets. Check around the company to make sure your marketing or public relations teams have not already engaged similar capabilities for adjacent purposes. This would not be bad news, by the way, but rather would provide a natural partner for sharing costs and expending existing contracts and relationships.

Advice for Security Technology Vendors

If you are providing digital risk monitoring and brand protection solutions, then you already know that this is a massively growing aspect of cyber security – especially since the election tampering of 2016 in the United States. Maintain your focus on automation, because as customer lists grow, the ability for human analysts to scale their support will diminish quickly. This is an important fact to share with your sales and marketing teams because their presentations still tout the backgrounds and capabilities of your human analysis teams. This will cause suspicion amongst buyers who know that human investigation only works when the client base is small.

List of Support Vendors

Agari – Agari's provides advanced brand protection enhancement via DMARC solutions for email fraud.
Bouju – Located in Los Angeles, Bouju offers a range of brand protection solutions via data collection and analysis.
Brady Brand Protection – Part of Brady Corporation, the company provides product authentication labels.
Brandle – Brandle offers its customers a range of social media security and brand protection solutions.
Brandma – Chinese brand protection firm Brandma works closely with top-level domain registrars.
BrandProtect – Canadian firm BrandProtect offers customers a range of brand protection services.
Brandshield – Brandshield supports a range of technology methods to monitor and protect brands online.
BrandVerity – BrandVerity provides brand protection and monitoring services for search, Website content, and coupon codes.
Channel IQ – Chicago-based Channel IQ offers business pricing, media, and brand monitoring services.
CitizenHawk – CitizenHawk is a provider of advanced online reputation and brand protection services.
DomainTools – DomainTools provides domain, network, and monitoring tools for research and threat intelligence.
First Cyber Security – The UK firm provides reputational analysis of website authenticity for reducing fraud.
4iQ – The company scans surface, deep, and dark web source to detect evidence of brand-based fraud and misuse.
Identify – Identify provides brand protection to help businesses with online trademark infringements.
MarkMonitor – Obtained by Thomson Reuters, MarkMonitor offers solutions for protecting organizational brands.
Microtrace – Microtrace offers security solutions for brand protection, anti-counterfeiting, and product authorization.
NetNames – NetNames provides domain registration, brand management, name alerts, and consulting services.
OpSec Security – OpSec Security supports anti-counterfeiting, brand protection, supply chain security, and Internet monitoring.
Original1 – Original 1 offers its customers a Security-as-a-Service solution for brand protection.
One World Labs – Owl uses advanced Dark Net threat intelligence to understand risks and protect brands.
Reputation.com – Located in Redwood City, Reputation.com offers brand and personal reputation protection services.
ReturnPath – ReturnPath offers a range of anti-fraud and brand protection solutions for the enterprise.
RiskIQ – RiskIQ uses advanced, intelligence driven techniques to scan the open web for evidence of abuse.
SecureMySocial – The New York-based firm focuses on detection of social media activity that could be considered abusive.

Sproxil – Sproxil provides a consumer SMS and app product verification service to reduce counterfeit risk.
Stealthmark – Recently acquired by Wellness Center, Stealthmark offers product authorization solutions.
The Media Trust Company – The company provides media security scanning for Websites, advertisements, and mobile.
YellowBP – YellowBP provides a wide range of brand protection and anti-counterfeiting solutions.
Your Internet Defender – Your Internet Defender provides a service for managing online reputation.
ZeroFox – Baltimore-based ZeroFox offers a range of social medial risk management and cyber security solutions.

Control 27: Bug Bounty Support

Bug Bounty support involves in-house and third-party infrastructure set-up to accept vulnerability information from external researchers for review and potential reimbursement. This infrastructure consists of staff, policies, procedures, tools, incident response measures, and financial payment systems. Larger companies often set this up themselves, but increasingly, this is performed in conjunction with a vendor product, platform, or service offering. Vendors provide an important layer of coordination and even protection between researchers and (ahem) hackers, and the enterprise security team staff. Vendors also provide platforms, coordinated communities of testers, and payment methods that greatly simplify the process of paying external hackers to test externally visible systems in an enterprise. It appears inevitable that even much smaller companies will begin using this process, simply because it offers a cost-effective means for detecting certain errors without much required set-up. The most common mistake made in a bug bounty program involve misinterpreting quiet periods with security, and busy periods with insecurity. Instead, bug bounty programs, like penetration testing, provide a reasonably dependable means for showing the presence of errors, but never their absence.

General Outlook
The general outlook for bug bounty support involves transition from early bug bounties with purely reactive response solutions to bug bounties focused more on preventing problems. This transition also includes simple reimbursement for reported bugs to more comprehensive, relationship-oriented programs between enterprise teams and security researchers. First generation bug bounty programs from 1998 to 2007 involved early adopters dealing with occasional, exceptional reports, with non-uniform means for reimbursement. Second generation bug bounty programs from 2007 to 2016 involved more creative solutions from vendors, with more comprehensive adoption, and more uniform approaches to important tasks such as researcher compensation. Third generation bug bounty programs from 2016 to 2025 should expect to see full coverage across the entire industry focusing more on early indicators to prevent rather than just react to issues. Increased vetting will improve relationships between enterprise teams and researchers, which will introduce better means for compensation. A wider range of vendor services will also emerge to support bug bounties in more specific and niche areas such as ICS and IoT.

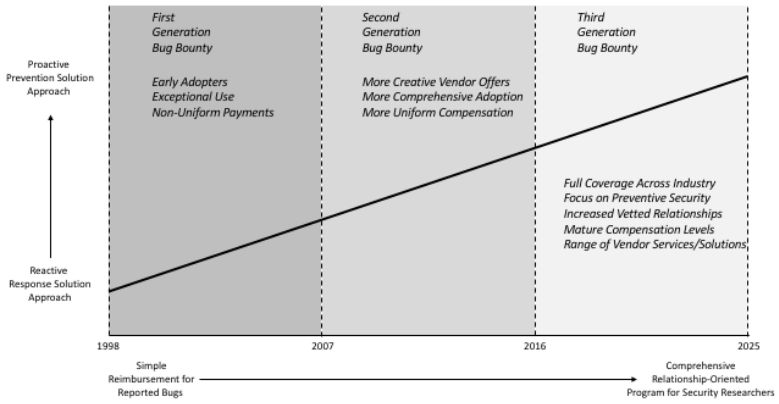

Figure 27. 2018 Bug Bounty Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, and it is difficult to find many downsides in bug bounty provision for both enterprise and vendors. Both will see a growing ecosystem in the coming decade, and soon, the use of bug bounties will be as common as penetration testing and other familiar means for detecting vulnerabilities.

Advice for Enterprise Security Teams

If you do not have a bug bounty or crowd sourced vulnerability discovery solution today, then get one. Researchers and hackers are generally willing to follow your defined procedures if they discover an issue in one of your Internet-visible systems or services. If you do not publish any procedures, however, then their response will be ad hoc. Enterprise buyers should be careful to check with their bug bounty solution provider to make sure that ad hoc reporting from unknown researchers is covered in the ecosystem. Some bug bounty solution providers offer excellent, vetted research teams that attack your services and provide amazing value; but these services do not address the problem of stray hackers stumbling onto an issue on your site. You'll need to do an end-to-end assessment to make sure you have bug bounty support and well-defined procedures for anyone not part of a defined bug bounty community.

Advice for Security Technology Vendors

Times should be good for bug bounty providers in the coming decade, especially down-market for SMB customers. Despite the relatively small number of vendors supporting bug bounty today, more competition will emerge in this area due to relatively low barriers to entry, so finding a unique value proposition is essential. A creative option for some providers might involve viewing discovered vulnerabilities as items of value, from which markets might emerge. Just as trading occurs for commodities and securities, the possibility emerges that trading might occur for discovered vulnerabilities. While the idea of trading vulnerabilities might not sound appealing, it is an example of the type of out-of-the-box thinking that will be required for bug bounty teams to differentiate in the coming years.

List of Support Vendors

BugBountyHQ – BugBountyHQ provides a platform and resources in support of Bug Bounty programs.
BugCrowd – BugCrowd offers a crowd-sourced approach to vulnerability discovery.

Cobalt – Originally called CrowdCurity, Cobalt involves teams of crowd sourced security researchers.
HackerOne – HackerOne offers a security-as-a-service (SaaS) platform for operating a corporate bug bounty program.
Hacking Team – The Italian firm (controversially) sells offensive intrusion and surveillance capabilities to governments.
Mitnick Security – The professional services firm operated by Kevin Mitnick includes a zero-day exploit exchange.
Offensive Security – Penetration test training firm Offensive Security operates a bug bounty program.
Synack – Synack provides an advanced intelligence platform for bug bounty support with actionable intelligence.
Zerodium – Zerodium offers an exploit acquisition platform focused on paying rewards for high consequence vulnerabilities.

Control 28: Cyber Insurance

Cyber insurance involves transferring aspects of cyber risk from enterprise teams to insurance companies. Despite considerable activity in the past decade, this remains a weakly understood aspect of cyber security management. The most uncertain aspect of cyber insurance involves the proper level of insurance for an enterprise, and how much that level of risk transfer should cost in terms of premiums. Simple back-of-the-envelope calculations help CISO teams determine if a given deal is reasonable. For instance, if it costs a large bank $5M per year in premiums to obtain $500M in insurance, then this is likely a good deal simply because twenty years of premiums amount to $100M in payout – and the potential for a $500M cyber loss increases every day. Changing these terms to $5M annual premiums for $50M in cyber risk transfer might be a less attractive deal. You get the idea. Here are some issues that remain somewhat in flux in this important area of cyber security:

- *Human Initiated Risk* – Humans cause the cyber risks being transferred, rather than Acts of God like floods and storms. This difference affects the nature of probability analysis and makes it harder for insurance companies to develop predictive models of occurrence.
- *Pre-Existing Risks* – Every company has pre-existing risks, simply because all software and complex systems include bugs. This complicates re-existing analysis and might lead to discrepancies once a claim is filed.
- *Government Fines* – Whether or not insurance covers government fines is a point of debate, and should be an important factor for any regulated company considering purchase of an insurance policy.
- *Vetting and Due Diligence* – The process of performing vetted due diligence for a potential buyer could involve large numbers of underwriters who need detailed information about a buyer's security program. CISOs should not provide such data to people they do not know.

Despite these challenges, cyber insurance will continue to evolve into a vitally important aspect of the cyber security equation for all sizes and shapes of enterprise.

General Outlook
The general outlook for cyber insurance involves transition from a highly varying set of different coverage levels and premiums to a converged and more uniform set of offerings. In addition, a transition is on-going from ad hoc buyer decisions about whether to purchase policies, to more

mature best practices for cyber insurance risk transfer. First generation cyber insurance from 1998 to 2007 involved the earliest insurance offerings purchased by early adopters with unclear risk bases and equations. Adoption of cyber insurance during this period was low. Second generation cyber insurance from 2007 to 2016 involved a greatly expanded marketplace with more uniform and understandable coverage and premiums. Executives and boards also became more familiar and comfortable with cyber insurance as a viable risk transfer option. Third generation cyber insurance from 2016 to 2025 should expect to see essentially full coverage across the entire buying industry, perhaps excluding smaller companies in the SMB segment. Cyber insurance will become an effective risk management tool with expanded options. CISO expertise will be used to help improve the financial equations to determine proper risk coverage.

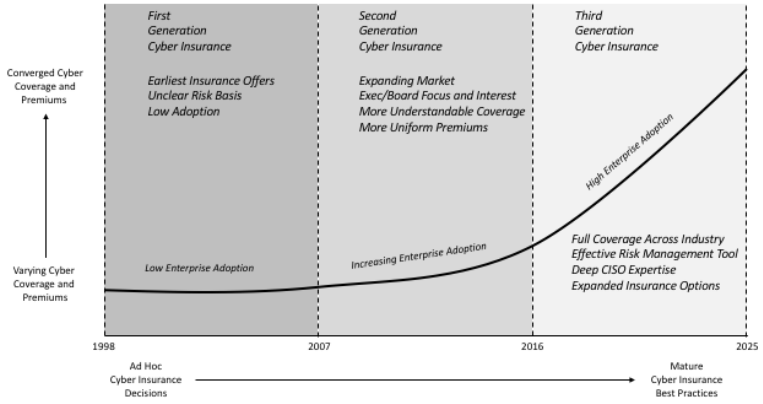

Figure 28. 2018 Cyber Insurance Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, and the expansion in this industry is already occurring. Most insurance companies view cyber products as one of their most promising areas of future growth and the brokers and agents are all gearing up to provide expanded support as well.

Advice for Enterprise Security Teams

If you work in a larger company, then your board has probably already begun to probe about cyber insurance – that is, if you don't already own a policy. Boards typically have a poor understanding of true cyber risk, so you will have to help them understand the nature of consequence after an attack. Be mindful of the challenges of due diligence, because insurance underwriters will want to know every sensitive detail about your program. One aspect of the cyber insurance procurement process that makes the product irresistible for most CISOs is that enterprise security budgets are rarely on the hook for the insurance purchase. What this implies is that additional risk management is offered to the security team without impacting their capital, headcount, or operating expense – simply because finance teams usually cover insurance purchases. This makes cyber insurance a must-do for most security teams, especially in larger companies.

Advice for Security Technology Vendors

Insurance companies offering cyber risk transfer products for enterprise must be careful to maintain solid quantitative models of likelihood and consequence of covered attacks. This is a wonderful growth area, but it also comes fraught with unusually high risk of massively cascaded attacks that could cut through swaths of industry in a matter of minutes. The potential for the cyber equivalent of a 2008 AIG-like event, where insufficient capital exists to cover all the claims after a massive global breach, must be modeled and factored into premiums and reserve. Brokers and agents, on the other hand, should expect to see mostly upside here with a greater market of buyers. All purveyors of cyber insurance should seek creative differentiators such as partnerships and discounts from the best available security vendors.

List of Support Vendors

AIG – AIG is a large insurance company that is now offering cyber insurance policies to companies.
BCS Insurance Company – BCS includes Cyber and Privacy Loss Protection insurance that covers fines and coverage to $30M.
Chubb – Chubb recently acquired by the ACE Group, that offers a range of cyber insurance policy offerings.
CoverWallet – CoverWallet is an insurance manager, with an on-line platform that provides broker services.
ECBM – Located in Pennsylvania, ECBM is a broker that provides cyber insurance consulting and brokerage services.
IDT911 – IDT911 is a broker providing cyber insurance products and concierge professional services.
Insureon – Insureon is a broker that will connect small businesses with an appropriate agent for commercial insurance.
Integrated Coverage Group – Integrated Coverage Group is an independent insurance agent supporting cyber insurance plans.
Locke Lord – Locke Lord is a large legal firm with expertise and experience in the insurance industry.
Lockton – Lockton is an insurance brokerage that writes policies for cyber risk management to augment data backup.
Philadelphia Insurance Company – Philadelphia Insurance Company markets a Cyber Security Liability program.
John Reed Stark Consulting – John Reed Stark Consulting provides independent consulting for cyber insurance.
TechInsurance – TechInsurance is a broker that offers business customer support for buying cyber insurance.
Travelers – Travelers offers cyber insurance policies for public entities, technology companies, and small businesses.
XL Catlin Group – XL Catlin Group offers policies that cover reasonable customized costs after a breach.
Zurich – Zurich offers comprehensive data breach insurance protection and data management solutions.

Control 29: GRC Platform

Governance, Risk, and Compliance (GRC) platforms support embedded initiatives within an organization to identify, control, and manage risks, and to ensure the highest levels of integrity for all facets of the organizational mission. Despite this stiff definition, GRC tools are a welcome addition to the enterprise security team's arsenal, simply because they provide support for three challenging goals: First, they use automation to ease the compliance task for any required frameworks such as PCI and NIST. Second, they support broad governance in an umbrella manner to help prioritize heterogeneous risk across all facets of a business. Third, they support a methodology that embeds GRC data collection and mitigation directly into business unit processes, rather than as a traditional overlay. Surprisingly, most CISO teams are still just learning to fully utilize the power of GRC platforms – some even using the workflow capability for adjacent needs such as incident response handling and support. More companies in the SMB category are beginning to find GRC platforms useful as well, with cloud-based SaaS offerings emerging to support this need. GRC platforms are a bright spot in the cyber security vendor ecosystem, because they support the noble goals of simplifying paperwork, compliance reporting, and management interaction – all of which free up cyber security staff to focus on more important operational tasks.

General Outlook

The general outlook for GRC platforms involves transition from stand-alone enterprise hosted systems to virtualized, hybrid cloud-hosted capabilities in an as-a-service mode. This transition also includes a shift from traditional non-embedded compliance overlays to GRC solutions that are fully-embedded into business unit workflow. First generation GRC platforms from 1998 to 2007 involved early risk management features that tracked basic compliance using simple work governance processes. Many security teams first became aware of GRC during this period, but many did not purchase platform support, opting to use Microsoft Excel and manual procedures. Second generation GRC platforms from 2007 to 2016 saw an expansion of automated support in the enterprise, with early embedded hooks into business units for GRC data collection. More extensive risk management tasks could thus be performed based on multiple different compliance frameworks. During this period, GRC platform truly became part of the cyber security lexicon. Third generation GRC platforms from 2016 to 2025 should expect to see a heavy transition to cloud services, with virtualized functions for lighter, as-a-service usage. GRC hooks will drive deeper into business unit processes, perhaps following the business into the cloud. GRC platform support will become a more common element of smaller cyber security team architectures, especially in businesses with more compliance requirements. This includes small regional banks and financial institutions, as well as any smaller businesses providing parts or component solutions to larger organizations with demanding compliance needs. The push to cascade GRC and compliance framework support from larger business contexts down to all smaller third-parties will drive the GRC platform business to higher levels of usage and revenue growth.

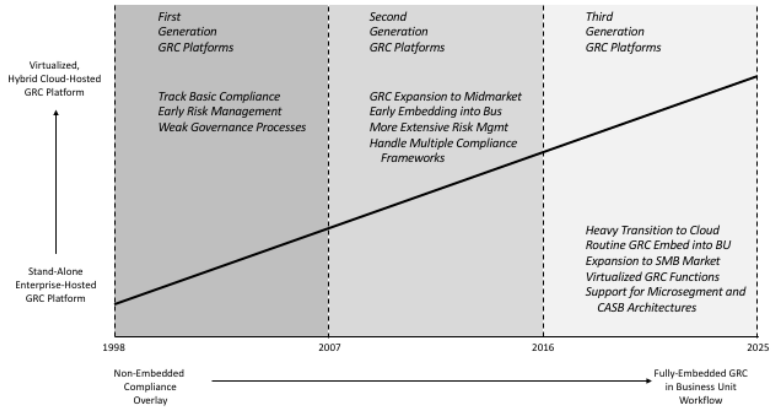

Figure 29. 2018 GRC Platforms Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since the likelihood of compliance needs being driven to a larger percentage of the SMB and hybrid cloud-based ecosystem has already begun. It seems obvious that the need to automate compliance will grow, so the prediction that GRC platform usage will increase, virtualize, and become more embedded should not be viewed as controversial.

Advice for Enterprise Security Teams

All enterprise security teams by now should be using some sort of GRC platform to support compliance and risk activities. Larger teams have already experienced the obvious benefits, and now smaller teams should expect to see risk management and compliance improvements through automation, especially if they find a good SaaS partner at a low cost. Just about every buyer at some point will be exposed to a marketing or sale presentation on a powerful GRC tool from one of the industry-leading platform providers. For smaller teams with lighter budgets, consider these powerful tools aspirational, and take solace in the fact that administration, configuration, and set-up activities for these tools are non-trivial. Smaller teams should stick to lighter, cloud-based platforms – albeit with more modest features.

Advice for Security Technology Vendors

Two challenges exist for GRC platform vendors: First, apart from a couple of massive, industry leading offers, there is a long tail of solution providers in this area. As a result, differentiation becomes difficult. Perhaps the best advice is to use professional services and concierge treatment for customers to create a more unique value proposition. Second, the enterprise is shifting rapidly from perimeter-based enterprise to a more heterogeneous collection of hybrid cloud services from many different service and application providers. The GRC ecosystem and challenge will thus shift from embedded collection to a federated sharing model, where companies will demand GRC integration from third parties. The best GRC platform solutions will include connectors, interfaces, and APIs to ease this task of creating a GRC program from many different constituent business units, partners, suppliers, and even customers.

List of Support Vendors

ACL – Vancouver firm ACL offers products and services focused on governance, risk, and compliance.
Active Risk – Active Risk provides an advanced platform solution called Active Risk Manager for enterprise risk management.
Alert Enterprise – Alert Enterprise, provides a next-generation governance, risk, and compliance solution for enterprise.
Allgress – Allgress provides a governance, risk, and compliance solution with emphasis on business risk intelligence.
ARAMA TECH – Located in Denmark, ARAMA TECH offers a governance, risk, and compliance solution for enterprise.
Aruvio – Aruvio provides a suite of advanced continuous governance, risk, and compliance solutions.
Audit Square – Audit Square provides audit and configuration assessment tools for Windows.
AvePoint – Jersey City firm AvePoint offers a range of governance, risk, and compliance solutions.
Bitcrack – South African consulting firm Bitcrack offers services related to governance, risk, and compliance.
Blue Lance – Houston-based Blue Lance provides enterprise solutions for governance, risk, and compliance.
Brinqa – Austin firm Brinqa offers an integrated GRC platform for analysis of business compliance and risk.
BWise – NASDAQ firm BWise provides an advanced governance, risk, and compliance solution for enterprise.
Cisco – Cisco offers a governance, risk, and compliance security assessment service for its enterprise customers.
CMT – CMT provides a comprehensive portfolio of security, compliance, and related solutions for business.
Coalfire – Coalfire provides advisory professional services on governance, risk, and compliance issues.
CompliancePoint – The company performs GRC assessments and audits with emphasis on call and contact centers.
Compliance 360 – Alpharetta firm Compliance 360 provides an advanced GRC solution for enterprise.
ControlPanelGRC – ControlPanelGRC offers an advanced governance, risk, and compliance solution for SAP.
Convercent – Convercent provides an ethics and compliance software solution for enterprise customers.
CriticalWatch – Critical Watch, part of Alert Logic, provides security risk, vulnerability, and compliance platforms.
Cura Software – Singapore firm Cura Software offers global customers an advanced GRC solution for enterprise.
Cytegic – The company offers an advanced, automated risk management platform for enterprise.
Deloitte – Deloitte provides professional services related to governance, risk, and compliance issues.
Delta Risk – San Antonio-based Delta Risk provides strategic advice and expert consulting in GRC.
Elemental – Las Vegas-based Elemental provides GRC management solutions for enterprise customers.
EMC/RSA – RSA offers the industry-leading Archer platform, which includes all baseline and advanced GRC functions.
Enablon – Enablon includes an advanced governance, risk, and compliance solution for enterprise.

EY – Global consulting firm EY acquired Integrc and offers governance, risk, and compliance services for SAP users.
FairWarning – FairWarning provides enterprise security and compliance integration across the enterprise.
Fastpath – GRC Studio from Fastpath is an integrated governance, risk, and compliance tool for enterprise.
The GRC Group – The GRC Group is a member organization with resources supporting GRC programs.
GRC 20/20 Research – GRC 20/20 Research offers governance, risk, and compliance advisory services with advice for buyers.
High Water Advisors – Consulting firm High Water Advisors offers governance, risk, and compliance advisory services.
IBM – IBM's OpenPages offers an advanced governance, risk, and compliance solution for its customers.
InfoDefense – The InfoDefense platform includes support for governance, risk, and compliance, as well as IAM and DLP.
IntelleSecure – IntelleSecure is an Indian firm that provides governance, risk, and compliance training.
KPMG – KPMG provides professional services supporting governance, risk, and compliance issues.
Leviathan Security Group – Seattle-based Leviathan offers information security and GRC consulting.
LockPath – The Keylight platform from LockPath is an advanced governance, risk, and compliance solution for enterprise.
LogicManager – Boston-based firm LogicManager provides an advanced enterprise risk management solution.
Mega – Mega develops tools to support governance, risk, and compliance solution for enterprise.
Metacompliance – Metacompliance provides a range of products and services supporting governance, risk, and compliance.
MetricStream – MetricStream provides an advanced governance, risk, and compliance solution for enterprise.
Modulo – Modulo is a New Jersey-based firm that provides governance, risk, and compliance services.
Mycroft – Now part of EY, Mycroft includes governance, risk, and compliance consulting services in its IAM suite.
Namtek – Bedford-based Namtek offers a governance, risk, and compliance professional services practice.
Navex Global – Navex Global provides software, content, and services to support governance, risk, and compliance.
Nettitude – Nettitude includes consulting services for governance, risk, and compliance solutions in the enterprise.
NextLabs – NextLabs data protection and IAM platforms support governance, risk, and compliance.
OCEG – OCEG is a non-profit group supporting governance, risk, and compliance best practices and solutions.
Oracle – Oracle provides the Fusion governance, risk, and compliance solution for enterprise customers.
Paladion – The Risq Vu platform from Paladion is an advanced GRC tool supporting workflow and audit management.
Panaseer – Panaseer offers a platform for intelligence on a network including cyber security threat identification.
Pervade Software – Pervade Software, headquartered in the UK, offers security compliance monitoring solutions.
Picus Security – Located in Turkey, Picus Security provides solutions for compliance monitoring and assessment.
Prevalent – The New Jersey-based firm offers a wide range of GRC consulting services and advanced platform solutions.
Protiviti – Protiviti offers its Governance Portal to support governance, risk, and compliance within enterprise.
PwC – PwC provides consulting services in support of advanced governance, risk, and compliance.
Resolver – Canadian firm Resolver offers customized governance, risk, and compliance solutions in the cloud.
RiskLens – RiskLens offers an advanced platform and methodology for estimating enterprise security risk.
RiskVision – Sunnyvale firm RiskVision (formerly Agiliance) offers an integrated GRC solution for the enterprise.
Rofori – Manassas-based Rofori offers a capability for managing cyber risks consistent with the NIST Framework.
Rsam – Rsam provides an integrated GRC platform with vendor risk management and capability to build custom apps.
RSD – RSD offers range of information governance services in support of governance, risk, and compliance.
RSM – Former McGladrey, RSM offers its customers advanced governance, risk, and compliance services.
Quad Metrics – Ann Arbor-based Quad Metrics offers advanced tools for estimating enterprise risk.
SaaSAssurance – Irish firm SaaSAssurance offers a compliance platform for managing GRC in enterprise.
SAI Global – SAI Global provides SaaS-based, advanced governance, risk, and compliance solution for enterprise.
SAP – SAP provides an integrated set of governance, risk, and compliance features for SAP users.
SAS – The SAS Enterprise platform automates the range of governance, risk, and compliance functions.
Saviynt – Los Angeles-based Saviynt provides an advanced cloud access governance solution for enterprise.
SDG – TruOps is an advanced governance, risk, and compliance solution for enterprise customers.
Secure Digital Solutions – The Minnesota-based firm offers a range of GRC consulting services for customers.
Security Weaver – Located in The Netherlands, Security Weaver offers GRC solutions for SAP users.
SecZetta – SecZetta provides a range of consulting services supporting governance, risk, and compliance.
SignaCert – SignaCert, located in Texas, offers product solutions for automated continuous compliance monitoring.
Software AG – The ARIS platform from Software AG supports governance, risk, and compliance solutions.
STEALTHbits – The New Jersey-based firm provides a range of data access governance solutions for enterprise.
Symantec – Symantec offers solutions for continuous monitoring of infrastructure for compliance and audit.
Templar Shield – Templar Shield provides a range of GRC security consulting, managed security, and recruiting services.
Tevora – Tevora supports a range of enterprise risk management solutions using its HydraRisk Model.
ThomsonReuters – The Enterprise Risk Manager from Thomson Reuters is an advanced GRC platform.
Titania – UK-based Titania provides audit compliance tools for enterprise devices, servers, and workstations.
TraceSecurity – TraceSecurity offers the Trace CSO governance, risk, and compliance solution for enterprise.
TrustWave – TrustWave GRC is an advanced governance, risk, and compliance solution for enterprise.

Turnkey Consulting – Turnkey Consulting offers SAP GRC Consulting services for enterprise customers.
Veris Group – Information assurance provider Veris Group includes GRC-related support for government customers.
VivoSecurity – VivoSecurity, located in Los Altos, provides a range of automated risk calculation solutions.
Winterhawk Consulting – Winterhawk Consulting offers range of governance, risk, and compliance services for enterprise.

Control 30: Incident Response

As its name implies, *incident response* involves the people, processes, and technology required for an organization to deal with on-going or completed cyber attacks. Traditionally, incident response involved cleaning-up a cyber mess after it had occurred, but more recently, advanced persistent threats have led to greater focus in the incident response process on detecting attacks while they are on-going. This might seem like a more proactive stance, but the reality is that most cyber exploit activity is just lasting longer. Incident response began decades ago with interested parties – usually security and system administrators – agreeing informally to a set of helpful procedures, contact and conference bridge numbers, and case documentation methods for dealing with the growing number of attacks that were occurring. Thus, unlike many other types of cyber security defense, incident response grew organically from the people who were doing the work. Increasingly, incident response is dependent on automated workflow, and vendors have stepped up to the task of creating intelligent, incident-aware automation that helps move the response activity along more rapidly and effectively. One would expect that this automation will eventually move most of the human involvement out of the way, so that virtualized incident response functionality will be used proactively to deal with a real-time stream of indicators. In this sense, one can see incident response begin to collide with live attack detection – which is a competitive situation few might have predicted in the past.

General Outlook
The general outlook for incident response involves transition from reactive response in the presence of clear evidence of attacks with few false positive cases, to more proactive focus on early indicators, which could increase false positive situations. If the incident response function is virtual and automated, then false positives become largely irrelevant. First generation incident response from 1998 to 2007 involved ad hoc coalitions of IT and security professionals using manual processes to handle cases. There was either poor or non-existent testing of incident response, but some of the more visionary teams began to focus on automating workflow. Second generation incident response from 2007 to 2016 involved improved automation from better defined teams using more advanced metrics in a proactive manner. During this period, incident response established itself as a mandatory component of every CISO team's arsenal. Automated incident response platforms also became, during this period, more popular vendor solution offerings. Third generation incident response from 2016 to 2025 should expect to see a heavy introduction of automation, with integration into security operation center (SOC) workflow. Incident response activities will have to expand during this coming period to handle more third-party cases, as well as cloud and SaaS infrastructure. The emergence of hunt teams in SOCs provides a natural point of great coordination with existing or new incident response teams, simply because the groups have overlapping charters with respect to on-going organization cyber incidents.

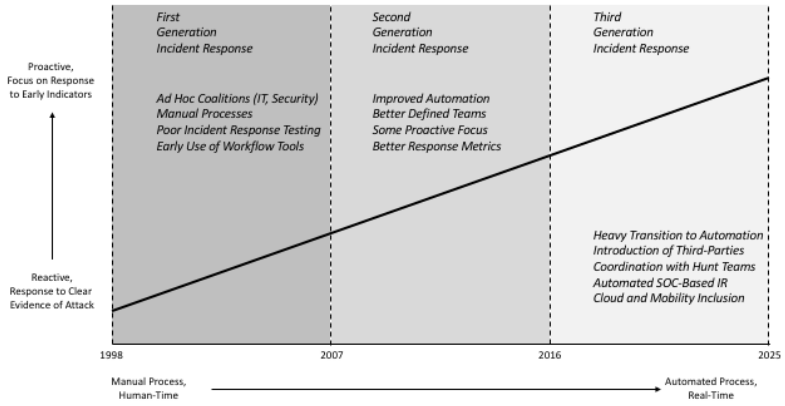

Figure 30. 2018 Incident Response Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since the growth and progression of incident response from its organic roots to its automated future has gone just about as everyone would have expected. The trend to third-parties, cloud, and SOC coordination with hunt teams seems just as obvious.

Advice for Enterprise Security Teams

Every enterprise and IT security team can improve its incident response procedures simply because human coordination is involved, and that is never perfect. Smaller teams should focus more on the basics, whereas larger teams should have an eye to automated workflow management. Every size team should be examining the impact on incident response methods of greater hybrid cloud usage of SaaS services with growing dependence on third-parties. This will tend to increase the complexity and reduce the cycle times for most incident response tasks. Newer incident response platforms should include APIs and federation support so that two organizations working together might coordinate their respective automation during a joint incident.

Advice for Security Technology Vendors

The focus for incident response platforms should be in two primary areas: First, vendors must optimize the workflow automation in their tools, because that will increasingly become the primary differentiator. Embedding analytics and smart algorithms into incident response tools will be welcome, but this will not be the primary criterion for buyers. Second, incident response vendors must ensure the highest level of open interfaces in their products, because buyers are going to start demanding that all support players in an ecosystem connect their incident response automation together during a case. In an SDN context, one could imagine seeing dynamic service chaining of different company's incident response applications being done through some ISP carrier's northbound SDN controller interface. This is advanced stuff, but it seems perfectly feasible given current technology.

List of Support Vendors

AccessData – AccessData provides data forensics products and services for cyber security including incident response.
Arctic Wolf Networks – Arctic Wolf Networks provides security-as-a-service cloud-based SIEM with incident response.
CounterTack – CounterTack focuses on endpoint security with the potential for active retaliation to on-going attacks.
CrowdStrike – CrowdStrike offers expert incident responders as a professional service for the enterprise.
CyberSponse – CyberSponse provides a collaboration platform for supporting security incident response.
Cyfir – Cyfir provides an enterprise forensics suite to support computer and network investigations and incident response.
D3 Security – D3 Security provides an advanced platform for incident management and response software.
Emagined Security – Emagined Security provides professional consulting services for information security and compliance.
Enclave Forensics – Enclave Forensics provides incident response and digital forensic services for enterprise customers.
Fast Orientation – Fast Orientation provides software that allows IT organizations to explore IT events in real time.
FireEye – FireEye includes the industry-leading Mandiant platform and process for supporting incident response.
4Discovery – 4Discovery provides digital forensics including mobile, remote collection, computer analysis, and reporting.
Guidance Software – Leading digital forensics firm Guidance Software support incident response activities in the enterprise.
IBM – IBM now provides the Resilient platform for incident response.
ID Experts – ID Experts provides a SaaS platform for aggregating breach details during response.
Intel – Intel provides security consulting services that include support for incident response.
ISARR – ISARR provides a Web-based platform for managing risk, resilience, response, and security intelligence.
Kroll – Kroll offers a range of cyber and physical investigatory services that are useful during incident handling and response.
K2 Intelligence – K2 Intelligence support investigations and response before, during, and after a breach.
Larson – Larson Security provides cyber security services including digital forensics and incident response.
LIFARS - LIFARS provides cyber security, digital forensics, and incident response support and services
Maddrix – Maddrix provides incident response professional services including remediation and threat intelligence.
Modulo – Modulo offers a platform that is used frequently to automate workflow management during response.
Palerra – Palerra provides a SaaS platform for threat, analytics, and incident response in public cloud offerings.
Praetorian – Praetorian provides professional services in support of enterprise incident response.
Reversing Labs – Reversing Labs offers advanced threat protection and analytics with support for incident response.
Roka Security – Roka Security provides a range of security consulting services including support for incident response.
RSA – Many enterprise teams use the RSA Archer GRC platform to automate workflow for incident response.
SecureState – SecureState is a global management-consulting firm focused on information security and incident response.
Security Management Partners – Security Management Partners provides security and IT assurance-consulting services.
Stroz Friedberg – Stroz Friedberg, now part of Aon, offers professional services after a breach requiring investigative response.
Swimlane – Swimlane offers a range of enterprise support for the incident response and handling process.
Sword & Shield – Sword & Shield provides a range of managed and professional cyber security services.
Syncurity – Syncurity provides advanced incident response solutions for enterprise breach remediation.
Thales Group – The Thales Group offers a range of cyber and data security solutions.
Vijilan Security – Vijilan offers a range of managed security services including monitoring and incident response.
Xyone – Xyone provides security consulting including penetration testing, compliance, incident response, and training.

Control 31: Penetration Testing

Penetration testing involves the deliberate use of hacking techniques under controlled conditions to demonstrate the presence of specific, targeted vulnerabilities in some application, system, network, or infrastructure. Many security managers mistakenly try to demonstrate the absence of vulnerabilities through penetration testing, but this cannot be done. Software lacks a continuity theorem which would enable testing of a range of values and then concluding that interim values follow a continuous shape. Instead, software testing can produce unpredictable and ad hoc results, so this means that all forms of testing, including penetration testing, play a different role than in traditional analog systems. Penetration testing can be accomplished in the following ways:

- *In-House Staff* – Larger companies often hire so-called white hat hackers to penetration test their systems. This may not be optimal for smaller companies because the

mischievous skills required to probe and hack systems often do not easily extrapolate to other required security activities such as compliance.

- *External Consultants* – Consultants and penetration testing professional services abound in the industry, so this is an easy task to hire out. Companies need to determine whether to deal with multiple testers, or to build a relationship with one testing group for repeat work.
- *Unknown Researchers* – Penetration testing by external researchers who have not been specifically engaged to probe for problems is adjacent to the bug bounties provided by companies.

The use of penetration testing has increasingly relied on automation, and it is possible that bot-controlled penetration testing will become a more popular technique. The danger of such automated probing is that it could lead to disaster if not properly controlled. The Nachi worm of 2003, for example, was presumably probing for security problems to fix, when it spun out of control and brought down massive portions of the Internet.

General Outlook

The general outlook for penetration testing involves transition from broad, general penetration tests to more focused, domain-specific tests in areas such as virtual systems, IoT, mobility, and industrial control. Transition is also on-going from mostly ad hoc manual penetration tests by experts to automated, platform assisted testing that can be done by staff with less expertise. First generation penetration testing from 1998 to 2007 involved a wide range of capabilities using mostly ad hoc hacking methods with little commonality and uneven cost and pricing structures. Second generation penetration testing from 2007 to 2016 involved improved testing tools with more professional engagements. The discipline emerged during this era as a legitimate aspect of the cyber security profession with increased commonality of approach. Third generation penetration testing from 2016 to 2025 should expect more domain-specificity and embedded functionality. One irony is that whereas penetration testing automation will reduce the expertise requirements for testers, the requirement for more domain knowledge might increase the demand for experts with specific knowledge and background in a target area. Penetration testing platforms will likely also virtualize to cloud operating systems so that embedded tools exist to support test engagements.

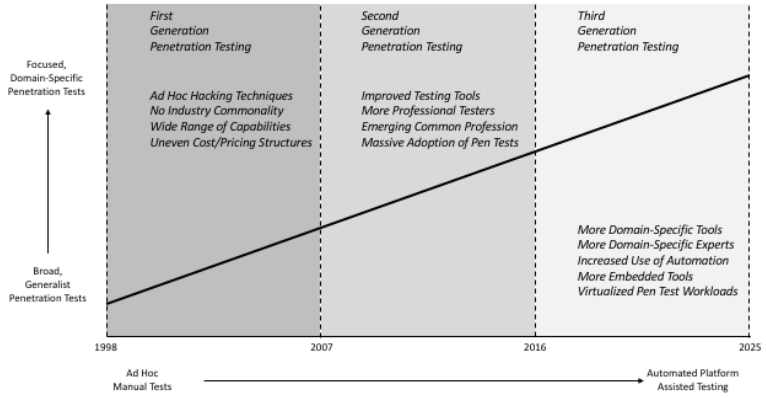

Figure 31. 2018 Penetration Testing Outlook

The TAG Cyber degree of confidence in this predictive outlook is moderate to high, since considerable misunderstanding exists in the marketplace around the benefits of penetration testing. So many boards and C-suite members have such a deep lack of knowledge and understanding in this area that it might skew the progression of this discipline.

Advice for Enterprise Security Teams

CISO teams must be clear on this: If the plan is to use penetration testing to identify and remove vulnerabilities, then plan on emptying out the budget in record time. This is an ineffective method for operating a cyber security program and is perpetuated by rookies who do not know better. CISOs instead must be fully aware of the many amazing benefits of penetration testing for demonstrating the presence of flaws. A favorite technique involves running penetration tests on the finance team in advance of budget time. Show the CFO a long list of serious vulnerabilities in the financial infrastructure and this will have deep influence on funding.

Advice for Security Technology Vendors

Vendors should focus on four initiatives to be more successful in penetration testing during the coming decade: First, they should continue to develop technical skills, because with automation, greater competition will emerge from testers with weak backgrounds. Second, they should select, develop, and integrate the best possible automated suites into their engagements. Hacking suites trace their lineage back to tools such as SATAN and Metasploit, and the usefulness of automation has never waned. Vendors should thus pay close attention to research tools from open source and academic communities for ideas and available software. Third, penetration testing teams should select good areas for domain-specific focus, with IoT, ICS, cloud, and mobility as excellent candidate choices. Finally, penetration test team management should try to build deeper relationships with select clients. The old shotgun method of having different client every week produces weaker results for the buyer than a partnership with a great penetration test team.

List of Support Vendors

ACROS Security – ACROS is a small, family-owned Slovenia penetration testing and research company.
AppSec Labs – Israeli application security expert group AppSec Labs has emphasis on testing mobile apps.
Atsec – Atsec is a security test and evaluation group with a mainframe penetration testing service.
AT&T – AT&T offers a range of penetration testing solutions through on-staff and outsourced groups.
Atredis Partners – Atredis is a small expert team of penetration testers with presence at conferences such as Black Hat.
Aura Information Security – Part of Kordia, Aura provides information security and penetration testing.
Auxilio – The California-based company offers security risk, compliance, and penetration testing services.
AVeS – Located in Johannesburg, Aves provides a range of IT consulting and penetration testing services.
Avnet – Israel-based Avnet provides security consulting and penetration testing with focus on securing databases.
BINAR10 – Peru-based BINAR10 provides a range of ethical hacking and related cyber security services.
Bishop Fox – Phoenix-based Bishop Fox offers security consulting and penetration testing services.
Bitcrack – Located in South Africa, Bitcrack offers security consulting, GRC, and penetration testing.
Bitshield – Located in the Philippines, Bitshield provides security consulting and penetration testing services.
Buddha Labs – The Encino-based firm offers IT security and testing services for clouds including AWS.
BugSec – Located in Israel, BugSec offers clients various penetration testing and security consulting services.

Carve Systems – Carve provides full-stack penetration testing services for IoT devices and other targets.
Coalfire Labs – Coalfire Labs offers audit, risk, penetration, and scanning services across the US and UK.
Comodo – Penetration testing is done by Comodo Dragon Labs, which includes staff around the world.
Content Security – Content Security, located in Australia, offers security consulting and testing services.
Core Security – Core Security offers the Core Impact Pro penetration testing platform for networks, endpoints, and Web.
Cyber Alpha Security BV – Located in The Netherlands, Cyber Alpha Security offers consulting and testing services.
Cyber Defense Labs – Cyber Defense Labs provides security consulting and penetration testing solutions.
Cyberis – San Antonio-based Cyberis provides security consulting and penetration testing solutions.
Dell SecureWorks – Penetration testing is offered as part of the SecureWorks Testing and Assessments Services.
Depth Security – Kansas City-based Depth Security provides security consulting and penetration testing solutions.
Fortego – Maryland-based Fortego provides network operations, reverse engineering, and other advanced cyber test services.
FRSecure – FRSecure offers penetration testing as part of its suite of security consulting services.
GoSecure – Canadian firm GoSecure provides security consulting and penetration testing solutions.
Grid32 Security – Newark-based Grid32 Security provides penetration testing and vulnerability assessment.
Hacking Team – Hacking Team provides offensive attack tools and surveillance capability for law enforcement and government.
HackLabs – Security consulting firm HackLabs specializes in penetration testing and ethical hacking.
Halock Security Labs – Halock Security Labs provides security consulting and penetration testing solutions.
Hedgehog – The UK-based consulting firm provides a range of penetration testing and security research services.
High-Tech Bridge – Located in Switzerland, High-Tech Bridge provides security consulting and penetration testing solutions.
Immunity – Florida-based Immunity provides security consulting and penetration testing solutions.
InGuardians – Washington-based InGuardians provides security consulting, audit, and penetration testing solutions.
ITsec Security Services – ITsec Security Services provides security consulting and penetration testing solutions.
Ixia – The California-based firm focuses on security and penetration testing solutions for enterprise.
Kaprica – Reston-based Kaprica provides security consulting and penetration testing solutions with emphasis on mobile.
Kernel – Located in Colorado Kernel provides security consulting and penetration testing solutions.
KoreLogic – KoreLogic provides security consulting, application security assessment, and penetration testing solutions.
Kroll – Kroll is an experienced security firm that includes penetration testing as part of their consulting offer.
Krypsys – UK-based Krypsys provides a range of security consulting and penetration testing solutions.
Kyrus – Located in Virginia, Kyrus focuses on reverse engineering, security research, and related testing.
Lancera Security – Lancera is a Utah-based security firm that includes penetration testing as an offer.
Layer Seven Security – Security services group Layer Seven, part of CA, focuses on offering SAP penetration testing.
LBMC Security & Risk Services – LBMC has an information security team with penetration testing capability.
Logically Secure – UK-based Logically Secure provides security consulting and penetration testing solutions.
Lunarline – Virginia-based information assurance firm Lunarline offers penetration testing services.
Maven Security – Maven Security provides a suite of cyber security consulting and testing services.
Meta Intelligence – Virginia-based Meta Intelligence offers risk management and penetration testing.
Mitnick Security – Mitnick security is the security consulting and penetration testing firm of well-known hacker Kevin Mitnick.
NCC Group – The company offers a range of testing services from deep technical investigations to higher-level assessments.
Netragard – Penetration testing firm Netragard made news by terminating their exploit acquisition program in 2015.
Nettitude – Nettitude provides penetration testing, risk management, and related cyber security services.
NetSPI – Information security and risk consulting company NetSPI includes a penetration testing capability.
nGuard – Charlotte-based cyber security consulting firm nGuard includes penetration testing services.
Nisos Group – Nisos Group focused on penetration and stress testing to detect advanced threats.
Offensive Security – Offensive Security is a group of expert hackers running a range of penetration testing courses.
Oneconsult AG – Swiss security consulting firm Oneconsult AG offers a range of penetration testing.
Parameter Security – Missouri-based Parameter Security provides security consulting and penetration testing solutions.
Pen Test Partners – UK-based Pen Test Partners provides penetration testing services for mobile, SCADA, and applications.
Pentura – Part of InteliSecure, Pentura offers security consulting and penetration testing services.
PivotPoint Security – PivotPoint Security provides information assurance including penetration testing and ethical hacking.
Portcullis – UK-based Portcullis provides a range of security consulting and penetration testing solutions.
Praetorian – Consulting and penetration testing services are available from Austin-based Praetorian.
Provensec – Provensec makes available cyber security and penetration testing focused on mid-sized business needs.
Pwnie Express – Boston-based Pwnie Express provides security consulting, asset discovery, and penetration testing solutions.
Rapid7 – Rapid7 offers scanning and penetration testing based on the work of H.D. Moore, inventor of Metasploit.
Reaction Information Security – Reaction Information Security provides security consulting and penetration testing solutions.
Rhino Security Labs – Rhino Security Labs includes network and Web penetration, mobile app, and secure code reviews.
Riscure – Located in The Netherlands, Riscure is a global security test laboratory focused on side channel analysis.
RiskSense – RiskSense provides a vulnerability management platform along with a range of security services.

Root9b – The New York-based company provides advanced cyber security consulting, testing, and training services.
SafeBreach – California-based SafeBreach provides a platform for breach execution on a target system.
SAINT – SAINT offers a range of penetration testing through the SAINTexploit scanning platform.
SECFORCE – UK-based SECFORCE offers a range of security consulting and penetration testing services.
Secure Anchor – Virginia-based Secure Anchor offers a range of security consulting and penetration testing services.
Secure Ideas – Florida-based Secure Ideas offers a range of security consulting and penetration testing services.
Security Art – Security Art provides a range of cyber security consulting services including red team exercises.
Security Audit Systems – UK firm Security Audit Systems offers a range of Website penetration testing services.
SecurityMetrics – SecurityMetrics offers PCI and HIPAA compliance services including scanning and penetration testing.
Sense of Security – Located in Australia, Sense of Security offers a range of security consulting and penetration testing services.
Synack – Synack offers continuous Bug bounty exploitation from a vetted team of crowd-sourced experts.
Syndis – Iceland-based Syndis offers a range of security consulting and penetration testing services.
Synopsys – The company offers a suite products and services focused on vulnerability testing.
TBG Security – TBG Security provides security consulting to assist with compliance in HIPAA, PCI, and related frameworks.
TechGuard Security – TechGuard offers security consulting and penetration testing for commercial and government customers.
Threat Intelligence – Australian firm Threat Intelligence provides managed threat intelligence including penetration testing.
Topgallant Partners – Topgallant Partners offers a range of security consulting, assessment, and penetration testing services.
Trail of Bits – New York-based Trail of Bits provides a range of expert research, training, and testing services.
Trojan Horse Security – Trojan Horse Security offers a range of security consulting and penetration testing services.
TrustedSec – Located in Ohio, TrustedSec offers a range of security consulting and penetration testing services.
Trustwave – Trustwave makes available cyber security consulting and PCI DSS QSA services including penetration testing.
2-Sec – 2-sec provides a range of security consulting offers including penetration testing and PCI DSS services.
ValueMentor – ValueMentor Consulting provides information security including assessments and penetration testing.
Veracode – Veracode is an application security firm that includes a range of penetration testing services.
Verizon – Verizon offers a range of penetration testing solutions through on-staff and outsourced groups.
vThreat – Herndon-based vThreat offers test and simulation platform support capabilities for cyber security functions.
Xyone – UK-based Xyone offers security consulting and penetration testing solutions for enterprise.
Yarix – Italian firm Yarix offers security consulting and penetration testing services for customers.

Control 32: Security Analytics

Security analytics involves advanced techniques, tools, and algorithms – often based on machine learning, deep learning, and artificial intelligence – that provide either stand-alone, embedded, or add-on functionality to detect evidence of security compromise in large volumes of data. Security analytics can be performed on data that is either stored at rest or collected in motion, perhaps even at line speed on a massive network. This is a capability that can be obtained by security teams in a variety of different ways, because virtually every security product and service includes some sort of security analytic function. The sweet spot for this advanced capability, however, involves platforms with tools for sifting through data in large stores, usually Hadoop-based, to pull indicator needles from metadata haystacks. Considerable cross-over exists in this area of enterprise cyber security with SIEM processing, and many of the vendors marketing themselves as security analytics providers use a SIEM as their platform base. Additional cross-over exists with network monitoring vendors who apply advanced analytics to their network packet and metadata capture engines. Even endpoint solutions include considerable cross-over since most security solutions for users and entities are now based on behavioral analytics. Fewer vendors than one would expect focus on pure licensing of their security analytics capability, especially user-behavioral, to turbo-charge solutions from other vendors. This is unfortunate, and one might expect that licensing deals will increase as the competition between security analytic platform vendors heightens.

General Outlook

The general outlook for security analytics involves transition from centralized, stand-alone analytic tools to distributed, platform-enabled capabilities embedded in cloud workloads. This transition also involves shift from simple data correlation methods to much more advanced algorithms based on machine learning, deep learning, and artificial intelligence. First generation security analytics from 1998 to 2007 involved simple correlation tools for SIEMs using small data sets to detect indicators after an attack. Second generation security analytics from 2007 to 2016 involved the introduction of more advanced, heuristic Big Data analytics, often based on Hadoop, in support of the SOC hunter. Third generation security analytics from 2016 to 2025 should expect to see massively distributed analytics coordinating advanced algorithmic processing across cloud workloads. Machine learning and artificial intelligence methods will be used to generate more proactive intelligence before an attack can produce consequences.

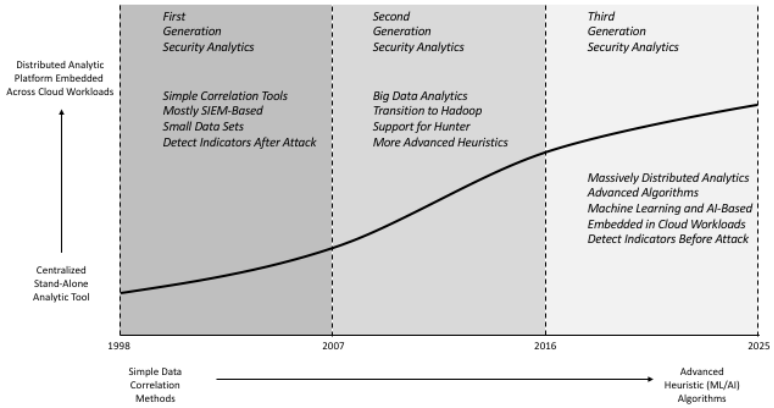

Figure 32. 2018 Security Analytics Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, because we have already seen significant growth in security analytics and our view is that consolidation and (in some cases) reality will set in, and the growth will settle down slightly to something more linear and sustainable.

Advice for Enterprise Security Teams

Enterprise security teams are advised to demand to understand the underlying mathematics of a given security analytics platform, and should demand full transparency in any human-assisted activity for machine learning and artificial intelligence tools. Since most of the products that your team will purchase in the coming years will include security analytics, the challenge of integrating all this distributed processing into something meaningful will become a new challenge. Ask your SIEM, network monitoring, log management, and endpoint solution providers to explain how such integration might be achieved. Since the steep growth in this area, especially for machine learning, will likely wane slightly in the next decade, it might be good to avoid long term contracts to take advantage of better deals that could emerge amidst greater competition.

Advice for Security Technology Vendors

Despite this being a promising aspect of cyber security technology, the business of being in security analytics might see some storm clouds ahead. This is a crowded field, with many different cyber security vendors claiming to be enabled with advanced analytics (even if they are not). Our advice here is to focus in two areas: First, any vendor with truly amazing analytic algorithms that really do work will be successful no matter the future circumstances. So, if you are the real deal, then keep it up. Second, our advice is to fully explore all possible usage opportunities for your technology, including add-on, embedded, and stand-alone. Licensing options may be the most attractive option for many vendors, especially in light of future needs in cloud, SDN, NFV, and virtual data centers.

List of Support Vendors

Attivo Networks – Attivo Networks provides deception-based attack detection and prevention including advanced analytics.
AxonAI – Virginia-based AxonAI provides a range of AI-based swam technology for anomaly detection.
Balabit – Located in Budapest, Balabit provides real time intelligence based network security analytics.
Bay Dynamics – Bay Dynamics offers customers its Risk Fabric predictive security analytics platform.
Brinqa – Located in Austin, Brinqa provides an integrated GRC platform that includes extensive security analytic support.
Context Relevant – Context Relevant provides state-of-the-art predictive data analysis tools for enterprise cyber security.
Cylance – Cylance offers artificial intelligence-based analysis tools to detect threats on endpoints.
Cymmetria – Cymmetria provides a range of cyber security analytic-based intrusion detection solutions.
Cynet – Based in New York, Cynet offers advanced enterprise analytic support for detecting cyber threats.
Cyphort – Cyphort supports the "single pane of glass" approach to enterprise analytics.
Darktrace – Darktrace offers a platform that supports so-called Enterprise Immune System technology for advanced analytics.
Dataguise – Fremont-based Dataguise offers advanced solutions for Big Data analysis security processing.
Dtex Systems – Dtex Systems focuses on insider threat protection using security analytics with behavioral pattern detection.
E8 Security - E8 security provides a security behavioral intelligence platform to support detection of threats in the enterprise.
Encode – Encode provides a security analytics and response orchestration platform for the enterprise.
Endgame – Virginia-based Endgame provides cyber security support for threat and vulnerability detection.
eSentire – eSentire offers an active threat protection solution with continuous monitoring service.
Exabeam - Exabeam provides user behavioral analytic intelligence from SIEM and log management data.
FileTrek – Known as Interset, the company provides endpoint behavioral analytics for enterprise.
FireEye – The popular FireEye platform includes advanced support for enterprise security analytics.
Flowtraq – Flowtraq provides an advanced capability for advanced analysis of network flow data.
Forcepoint – Forcepoint offers content security, analytics, cloud security, firewall, and Web security for the enterprise.
Fortscale – Fortscale provides user behavioral analytics solutions for enterprise security threat detection.
Guardian Analytics – Mountain View-based Guardian Analytics provides behavioral analytic solutions for detecting fraud.
GuruCul – GuruCul supports identity-based behavioral analytics to support cyber risk intelligence.
Hawk Network Defense – Hawk Network Defense provides analytics for enterprise, service providers, and SIEM enrichment.
Haystax Technology – Haystax Technology provides security intelligence and real-tome situation awareness solutions.
HPE – One of the industry-leading SIEM solutions, ArcSite from HPE, offers a range of security analytics functions.
IBM – IBM includes an extensive range of security analytic solutions as part of its cyber security product offerings.
IKANOW - IKANOW provides Big Data analytic solutions to reduce the risk of breaches and APT attacks.
Informatica - Informatica provides Big Data solutions including a data security offering focused on critical data intelligence.
InterGuard - InterGuard provides employee-monitoring software that records and controls PC activity for loss and misuse.
Jask – San Francisco-based Jask provides an artificial intelligence-based platform for security analytics.
KEYW – KEYW provides the Hexis enterprise security analytics solution with data analysis and SIEM functions.
Lastline – Lastline provides malware detection and threat analysis for enterprise as a hosted or on-premise solution.
LightCyber – Located in Israel, LightCyber provides advanced breach detection with emphasis on APT.
Morphick – Morphick provides security analytic tools for advanced threat detection and response.
Niara – Niara offers an integrated platform for performing analytics and forensics on enterprise data.
NIKSUN – Princeton-based NIKSUN provides network performance monitoring and security surveillance solutions.
Noragh Analytics – Noragh's TAC supports enterprise investigation and analysis of large volumes of information.
Novetta – Novetta provides an advanced analytics platform for detecting threat and potential fraud in the enterprise.
Nuix - Nuix provides investigation, information governance, eDiscovery, and cyber security solutions for enterprise.
ObserveIT – ObserveIT provides a software solution for user activity monitoring based on tailored analytics and forensics.

Outlier Security – Outlier Security provides agentless cyber security analytics as a service for endpoints.
Palantir – Palantir provides real time data fusion and intelligence platform solutions for enterprise and other applications.
Panaseer – Panaseer offers a platform for intelligence on a network including cyber security threat identification.
Pixlcloud – Pixlcloud supports Big Data analytics and visualization in the enterprise with training offers for analysts.
Red Lambda – Red Lambda provides a Big Data security platform that supports correlation, reporting, and automation.
RedOwl – RedOwl supports behavioral analytics for information security and enterprise compliance.
Reversing Labs – Reversing Labs provides a platform for threat protection and analytics with support for incident response.
Risk I/O – Rebranded as Kenna in 2015, the company provides a risk intelligence and vulnerability management platform.
RiskLens – RiskLens uses advanced analytics to optimize insurance and manage cyber security risk in the enterprise.
RSA – The industry-leading security division of EMC has expanded its focus on enterprise security analytics support.
SAS – Advanced analytics from SAS supports business intelligence and predictive analysis for enterprise.
Savvius – Savvius provides advanced network monitoring and security analytics software for enterprise.
Secnology – Secnology provides a wide range of SIEM, log management, and enterprise security analytics capabilities.
Secure Decisions – Secure Decisions provides security visualization for analysis of software, networks, and other systems.
SecurityDo – SecurityDo provides a product called Fluency that provides breach detection and response capabilities.
Sophos – Sophos combines endpoint security protection with enhanced analysis tools based on Cybereason acquisition.
SpectorSoft – SpectorSoft provides monitoring software to detect insider threats, employee fraud, and data breaches.
Splunk – Splunk offers a platform for intelligence on a network including cyber security threat identification.
Sqrrl – Sqrrl's Linked Data Analysis supports enterprise security analysis and monitoring of collected data.
SS8 – SS8 provides advanced enterprise communication security through analysis, correlation, and forensics.
Sumo Logic – Redwood City-based Sumo Logic provides advanced continuous log management and security analytics.
SurfWatch Labs – SurfWatch Labs provides a risk analytic platform API for translating data to intelligence.
Tanium – Tanium provides high performance, real time endpoint protection through data collection and threat analysis.
ThetaRay – ThetaRay offers enterprise cyber security analytics support for industrial sector customers.
ThreatStream – Redwood City-based ThreatStream offers a threat intelligence platform for supporting security data analytics.
ThreatTrack Security – ThreatTrack Security provides a sandbox-based solution to detect suspicious or malicious behavior.
TIBCO – TIBCO provides a range of business intelligence and infrastructure solutions, including data security.
Trustpipe – Trustpipe offers endpoint security via network traffic scans and analysis using an attack taxonomy.
21CT – 21CT provides a behavioral analytic fraud detection solution that supports enterprise investigations.
Verint – Verint provides analytic hardware and software for security, business intelligence, and surveillance industries.
Webroot – Having acquired CyberFlow Analytics, Webroot now provides network monitoring and security analytics.
Yaana – Yanna includes advanced cyber security analytics in its suite of Big Data solutions for enterprise.
Yaxa – Yaxa provides an insider threat protection solution based on user behavioral analytics for enterprise.
Zettaset – Zettaset provides solutions for securing Hadoop and orchestrating enterprise security analytics.

Control 33: SIEM Platform

Security Information Event Management (SIEM) platforms collect and process audit trails, activity logs, security alarms, telemetry, metadata, and other historical or observational data from a variety of different applications, systems, and networks in an enterprise. For a SIEM to operate properly, connectors and interfaces are required to ensure translated flow from the system of interest to the SIEM database. Eventually, better standards will emerge for how SIEMs integrate into an ecosystem, but for now, vendors differentiate based on how easily a customer can collect and process data. The processing part of a SIEM ranges from basic correlative analysis resulting in an activity dashboard with alarms, to machine learning-based heuristic analysis based on behaviors, profiles, and rudimentary artificial intelligence. (Many experienced SIEM operators prefer the simpler tools.) Adjacent solutions also exist to enhance the overall SIEM processing through improved log monitoring or domain-specific pre-processing of collected alarms. LAN-hosted SIEMs will naturally migrate to distributed, virtualization in hybrid cloud environments, so expect to see new points of marketing differentiation from this segment. This virtualization will assist down-market SMB organizations to become more active

SIEM users, a point that is becoming inevitable anyway, as third-party risk management programs impose SIEM solutions as part of imposed compliance requirements.

General Outlook

The general outlook for SIEM Platform solutions involves transition from usage mostly from larger organizations to expanded use by a larger number of organizations including from the SMB segment. This transition also includes a shift from centralized, LAN-based SIEM deployments to more distributed, hybrid-cloud hosted SIEM solutions that collect data from virtual workloads. First generation SIEM platforms from 1998 to 2007 involved the earliest tools with simple relational databases collecting firewall and IDS alarms. The actions resulting from these early SIEMS were typically uneven, with most SIEM buyers expressing disappointment at their investment. Second generation SIEM platforms from 2007 to 2016 involved more features, support for larger data sets (including netflow collection), and the earliest support for virtual cloud infrastructure. SIEM buyers were mostly satisfied with their investments during this period, and most compliance initiatives began to reference use of these tools as requirements. Third generation SIEMs from 2016 to 2025 should expect to see a reduction in LAN-hosted SIEMS as the perimeter implodes, but this will be replaced with expended virtual SIEMs deployed to hybrid cloud. Third-party risk requirements imposed on SMB organizations will drive this virtual growth, and the native capabilities will improve with machine learning, deep learning, and artificial intelligence.

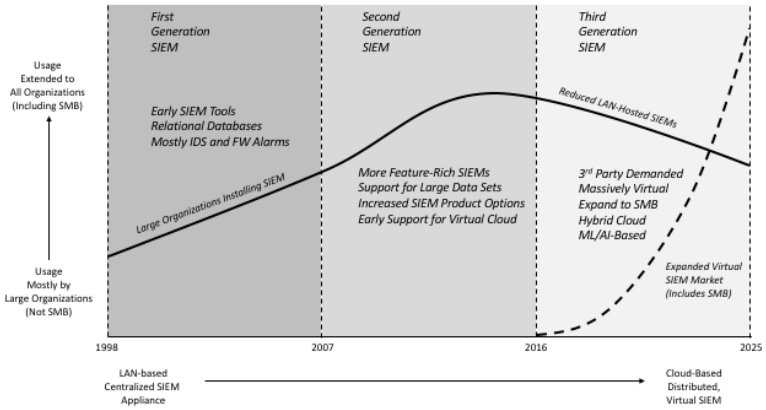

Figure 33. 2018 SIEM Platform Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since the market for SIEM platforms will continue to expand through compliance frameworks, virtual options for SMB, and better processing. This is a bright spot in cyber security and expect SIEMS to include better connectors for incident response workflow.

Advice for Enterprise Security Teams

Enterprise teams not currently using a SIEM should jump immediately to a virtual solution with an as-a-service, mobile device-accessible dashboard for rendering analysis output from data collected from cloud workloads. Teams with a LAN-hosted SIEM need to work with their vendor

to determine the best path forward for collecting data from heterogeneous distributed cloud components. This path should be something more elegant than just shoveling the cloud workload data back into the enterprise through open ports on gateway firewalls. Compliance framework writers are correct to include SIEMs in their functional requirements, and SMBs should no longer flinch when they see this as a mandatory expectation when they support a larger customer.

Advice for Security Technology Vendors

Expanding to virtual, cloud-based SIEM solutions is the obvious play here. The growth in that segment will be exponential, and the down-market options to SMB are exciting. Vendors should be careful not to overplay the advanced machine learning and artificial intelligence aspect, simply because most experienced SIEM operations teams understand that basic correlation, simple event count histograms, and clear comparison of one-thing-with-another are perfectly fine for detecting trends. Complex mathematical analysis will be useless if operations teams have no clue what a Bayesian distribution means. Our advice here is to keep it clean, elegant, and simple, especially on dashboards.

List of Support Vendors

Alert Logic – Alert Logic provides a managed, cloud-based security information and event management solution for enterprise.
AlienVault – AlienVault offers a unified SIEM platform for enterprise and SMB customers with open source threat feeds.
Arctic Wolf Networks – Arctic Wolf Networks provides managed security information and event management.
Assuria – UK-based Assuria sells a cloud-ready security information and event management platform for enterprise.
A3Sec – Spanish company A3Sec has a relationship with AlienVault and focuses on SIEM products and services.
BlackStratus – BlackStratus, formerly NetForensics, offers managed SIEM products and solutions for the enterprise.
Correlog – Correlog provides a security information event management component that operates in a mainframe environment.
EMC/RSA – RSA offers the enVision security information event management solution for enterprise.
EventSentry – EventSentry provides a platform for event log monitoring and related real time enterprise security functions.
EventTracker – EventTracker provides advanced SIEM-as-a-Service solution for enterprise customers.
Extreme Networks – Extreme Networks offers its Extreme SIEM based on the Enterasys acquisition.
Fortinet – Fortinet offers a security information and event management platform called FortiSIEM for enterprise customers.
GFI Software - GFI Software offers email security services, event management, and managed anti-virus.
HPE – HPE offers the industry-leading ArcSight platform, which includes all baseline and advanced SIEM functions.
Huntsman – Huntsman offers the advanced Tier-3 security incident and event management capability.
IBM – IBM offers enterprise customers the QRadar SIEM Q1 through its acquisition and integration of Q1 Labs.
Juniper – The Juniper JSA3800 appliance provides both enterprise security analytics and SIEM-like functions.
KEYW – KEYW acquired Sensage in 2012 and offers advanced log and event management solution.
LOGbinder – LOGbinder provides tools to connect security intelligence to enterprise SIEM with focus on Microsoft products.
Logentries – Logentries provides a feature-rich, low-cost security information event management product.
Loggly – Loggly offers an advanced security and event log management solution for enterprise customers.
LogRhythm – LogRhythm supports SIEM, log management, and network analytics in its enterprise platform.
ManageEngine – ManageEngine provides the real time EventLog Analyzer, which includes SIEM functionality.
McAfee – SIEM solutions from McAfee include advanced capabilities for enterprise and SMB customers.
Papertrail – Papertrail is an event viewer and log management application available as virtual solution.
Prism Microsystems – Prism offers advanced SIEM, IT security, compliance, and log management tools.
SolarWinds – Austin-based SolarWinds offers a SIEM, log, and event management solution on a single virtual appliance.
Splunk – Splunk offers a set of collection, correlation, and analysis tools for log and enterprise data security investigation.
Sumo Logic – Sumo Logic provides secure, cloud-based log monitoring, management, and analytics.
Stackify – Stackify offers a developer-centric solution that integrates application log management with Dev Ops.
Symantec – Symantec maintains support for existing SIEM customers through 2017 as it moves focus to other areas.
Tenable – Tenable offers an advanced security information event management solution for enterprise and SMB.
TIBCO – TIBCO offers an advanced security information event management solution for enterprise.
Tripwire – Tripwire offers a Log Center enterprise solution that includes advanced SIEM functionality.
Trusted Metrics – Trusted Metrics offers a cloud-based security information and event management solution.

Trustwave – Trustwave offers a range of security information event management solutions for enterprise.

Control 34: Threat Intelligence

Threat intelligence services consist of real-time information feeds for enterprise security teams from human and automated sources on the background, details, specifics, and consequences of present and future cyber risks, threats, vulnerabilities, and attacks. Threat intelligence services often include recommended actions, but most enterprise security teams tailor their response to reported threat issues based on local conditions. Most threat intelligence services were created based on the experience and expertise their founders – often former government intelligence officers. Increasingly, modern threat intelligence feeds are more centered on technology-based collection, aggregation, and presentation to customers using well-defined application and network exchange protocols. Note that *threat* intelligence is a superset of *cyber* threat intelligence, and this is a useful distinction for security operations staff. When performing all-source correlative analysis of cyber events and indicators, it is often useful to fold non-cyber threat intelligence into the analysis. This can include geo-political issues, natural disasters, criminal action, military maneuvers, and so on. Standards for threat intelligence automation are emerging, but accepting external information as the basis for automated system administrative actions is still in its infancy in terms of general enterprise adoption and comfort.

General Outlook

The general outlook for threat intelligence solutions involves transition from human time usage to real-time, automated use. In addition, threat intelligence is undergoing transition from simple threat intelligence sources such as vulnerability from reports from a vendor to all-source threat intelligence feeds from a variety of integrated origination points. First generation threat intelligence services from 1998 to 2007 consisted of basic information pulled from the earliest use of Dark Web, but with light integration into business response activity. Second generation threat intelligence services from 2007 to 2016 began to see more extensive use by CISO teams, simply because the threat information improved in terms of accuracy, relevance, and even tailoring to the enterprise buyer's needs. Third generation threat intelligence services from 2016 to 2025 should expect to see more automated feeds, increased real-time usage and application, more actionable data, and greater focus on domain-specific intelligence, especially for IoT and ICS.

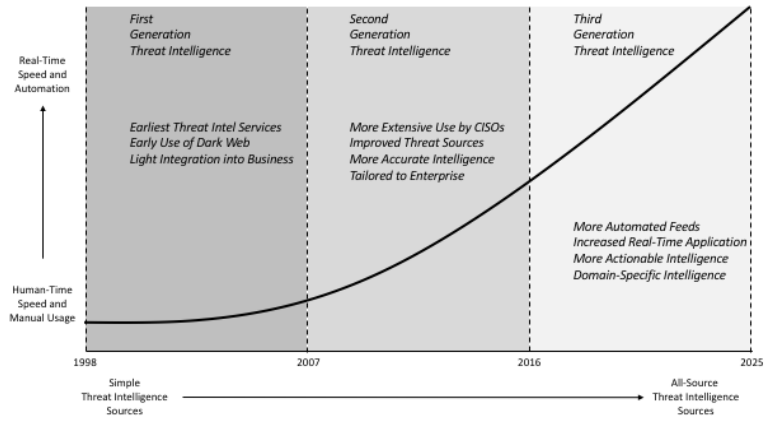

Figure 34. 2018 Threat Intelligence Outlook

The TAG Cyber degree of confidence in this predictive outlook is moderate, since threat intelligence is now so readily available as a component of virtually every cyber security product and service in the market. The barrier to entry for threat intelligence services is incredibly low, despite what your vendor brags about the backgrounds of their principals as former officials in the national intelligence service of their home country.

Advice for Enterprise Security Teams

Enterprise teams must learn to ingest threat intelligence for their cyber security programs in much the same way as automobiles must be designed to ingest gasoline, oil, and other fluids for proper operation. Security operations centers and hunt teams already know the value of threat intelligence, as do any gateway administrators accepting live URL feeds to keep the bored accountants in the Finance Department off porn sites. The real challenge for enterprise teams is whether they are willing to take the full leap into automated collection and rapid, automatic mitigation based on ingested data. The key attribute here is trust, and the question emerges whether sufficient confidence exists in a threat feed to allow machine-controlled reconfiguration of some system to occur. My advice is to proceed forward, albeit with sufficient caution to avoid rash integration of potentially buggy feeds degrading the corporate gateway.

Advice for Security Technology Vendors

Threat intelligence is a growing aspect of cyber security – no doubt. But the competition here is fierce with low barriers to entry and disintermediation with vendors skipping the threat intelligence feed integration step by just powering a feed themselves. Open source threat intelligence should be a less intense threat to business, simply because the signal-to-noise ratio in such feeds is suspect. The advice here is to focus on an elegant platform with simple operation, and clean, understandable interfaces. Furthermore, compliance with standards such as Structured Threat Information Expression (STIX), Cyber Observable Expression (CybOX), and Trusted Automation Exchange of Indicator Information (TAXII) are a must, as automated threat feed integration, federation, and sharing will increase in the coming years.

List of Support Vendors

AlienVault – AlienVault includes the Open Threat Exchange crowd-sourced threat intelligence in its security offerings.
AT&T – AT&T is the first ISP in the world to provide threat information via its virtualized SDN core.
BAE Systems – BAE Systems provides an advanced threat intelligence management and analytics platform.
Blueliv – The company provides an end-to-end cloud-based cyber threat intelligence solution.
Booz Allen Hamilton – BAH provides its Cber4Sight Threat Intelligence offering for the enterprise.
Centripetal Networks – Centripetal Networks provides a real-time network protection solution.
Confer – Confer provides a sensor that connects an enterprise to a cyber threat prevention network
Check Point Software – Check Point Software markets the ThreatCloud IntelliStore threat intelligence platform.
Corax Cyber Security – Corax Cyber Security provides security threat management and intelligence services.
CrowdStrike – CrowdStrike bases its endpoint solution on its cloud-based Intelligence Exchange (CSIX) program.
Crypteia Networks – Crypteia Networks provides threat intelligence and related security services in Eastern Europe and EMEA.
CyberInt – CyberInt provides intelligence, monitoring, and consulting focused on information security and cyber warfare.
CyberUnited – CyberUnited offers threat intelligence, analytics, and machine learning to detect malicious insider behavior.
Cyren – CYREN provides an advanced cloud-based platform that makes threat data available to endpoints.
Dell – Dell powers its solutions with threat intelligence from the Counter Threat Unit research team.
Digital Shadows – Digital Shadows offers cyber situational awareness solutions to protect against attacks.
Disrupt6 – Disrupt6 provides threat intelligence based on a subscription feed or via a deployed sensor network.
Distil Networks – Distil Networks protects Websites from botnets, scraping, and data mining with advanced threat intelligence.
DomainTools – DomainTools provides domain, network, and monitoring tools for look-up, investigation, and threat intelligence.
EclecticIQ – EclecticIQ, formerly Intelworks, provides a range of cyber threat intelligence management solutions.
Farsight Security – Farsight Security provides threat intelligence feeds from real time passive DNS solutions.
FireEye – Through acquisition, FireEye has emerged as one of the industry leaders in providing advanced threat intelligence.
Flashpoint – Flashpoint provides cyber ad physical threat intelligence services from the Deep and Dark Web.
Haystax Technology - Haystax provides actionable security intelligence and real time situational awareness.
Hold Security – Hold Security provides consulting services and threat intelligence for business clients.
HPE – HPE Threat Central includes actionable threat analysis and intelligence from HPE's cloud-based sharing platform.
IBM – The IBM Security X-Force Threat Intelligence supports IBM platforms with threat data.
Infoblox – Based on acquisition of IID, Infoblox offers a range of advanced threat intelligence services.
McAfee – The company offers the Global Threat Intelligence (GTI) situational awareness service.
Lookingglass – Lookingglass supports threat intelligence management supporting security operations and real time decisions.
Maddrix – Maddrix provides incident response professional services including remediation and threat intelligence.
PhishMe – PhishMe supplies threat management solutions to support their anti-phishing mission.
Meta Intelligence – Meta Intelligence provides intelligence-based services, cyber risk management, and penetration testing.
NC4 – NC4 supports disseminating information related to cyber threats, physical safety, crime, and incident management.
Noragh Analytics – Noragh Analytics offers a data analysis and decision framework for applications including cyber security.
Norse – Norse includes capability to report on live network protocol activity such as Border Gateway Protocol.
One World Labs – One World Labs provides threat intelligence and related services with emphasis on brand protection.
OWL Cybersecurity – OWL Cyber security offers a Dark Net threat intelligence platform.
Pierce Global Threat Intelligence – Pierce Global Threat Intelligence (GTI) provides ranked threat intelligence.
Recorded Future – Recorded Future provides real time threat intelligence to defend an organization.
RSA – RSA FirstWatch involves advanced threat intelligence and security analytics focused on sophisticated threat management.
Security-Database – Security-Database monitors and provides dashboard summaries of vulnerabilities for a variety of products.
Security Tracker – The organization provides free and premium security threat and vulnerability advisory information.
SenseCy – SenseCy's advanced cyber intelligence provides specific threat information for various sectors.
Silobreaker – Silobreaker provides an app for security professionals to keep track of open source data from the Web.
Spamhaus – Spamhaus is a non-profit focused on tracking Spammers and supporting anti-Spam activities across the world.
SurfWatch – SurfWatch Labs offers advanced, comprehensive cyber threat intelligence solutions.
Symantec – Symantec offers DeepSight Intelligence with actionable strategic and technical cyber information.
Taia Global – Taia Global provides a counter-intelligence service that works with a SIEM to provide real time information.
Team Cymru – Team Cymru provides actionable data with the intelligence required to protect an organization.
ThreatConnect – ThreatConnect offers a threat intelligence platform that empowers organizations to aggregate information.
Threat Intelligence – Threat Intelligence provides managed threat intelligence services including penetration testing.
ThreatQuotient – ThreatQuotient (ThreatQ) supports management of internal and external threat intelligence.
ThreatStream – ThreatStream offers enterprise class threat intelligence based on data collection, prioritization, and analytics.
Tripwire – Tripwire provides a range of advanced enterprise threat and vulnerability intelligence services.
TruSTAR – TruSTAR provides an anonymous means for sharing of threat and vulnerability information with a community.
Verisign – Verisign includes expert cyber threat intelligence services for global enterprise clients.
Wapack Labs – Wapack Labs provides cyber threat analysis, security research, and intelligence services.

Webroot – The Webroot BrightCloud Threat Intelligence Services includes IP reputation services.

Control 35: Application Security

Application security involves a variety of static and dynamic methods used to reduce cyber risk in enterprise software applications. Techniques for application security span a broad range of emphasis including focus on software process enhancements, static code improvements, and run-time operating system environmental controls. Because the work activities involved in each of these approaches vary so widely – from software methodology reviews to autonomous run-time learning – it is difficult for many CISO teams to get their arms around this aspect of their enterprise protection responsibility. Code scanning tools have traditionally been the primary focus, but advances in the ability of software to self-protect using advanced heuristic means make this aspect of application security highly promising. To help keep track of the various possibilities, here is a list of current techniques typically associated with application security:

- *Software Process Reviews* – This method follows the presumption that it is easier to predict software issues by looking at how you develop software than by looking at the actual code you produce.
- *Software Framework Compliance* – Various best practice frameworks for application software such as OWASP can be helpful to developers in reducing cyber risk through common sense Dev/Ops approaches.
- *Application Security Scans* – This method involves running automated scans of executables and source code to identify evidence of possible vulnerabilities or exploitable weaknesses.
- *Application Code Reviews* – This involves the tedious process of peer-review by human beings of developed code. Most developers will explain that nothing replaces the value of expert review.
- *Run-Time Security Controls* – Embedded software that exports run-time telemetry or that imposes controls on behavior from application executable is becoming more commonly used in enterprise application hosting.
- *Advanced Self-Protection* – The technique of autonomous, self-protection is an exciting premise for improving application security during run-time.

Since all these methods contribute to the same goal of improving security of software applications in the enterprise, expect to see convergence of solutions in the marketplace, even in the face of significant differences in how CISO teams carry out the respective activities.

General Outlook

The general outlook for application security involves transition from manual, mostly ad hoc application security reviews to automated, intelligent, self-learning application security controls. This transition also involves shift from application as a minor (or even missing) component of most security teams to an essential, highlighted component of every CISO program in every sector. First generation application security from 1998 to 2007 involved ad

hoc functions, mostly scanning, with early process maturity work. Second generation application security from 2007 to 2016 involved a more complex mix of solutions as application became perceived as a greater security risk. CISOs applied more focus in this area during this period. Third generation application security from 2016 to 2025 should expect to see greater convergence of solutions, across the board, with an even heavier focus from CISO teams. Funding for application security is likely to become more routine with year-over-year budget positioning making the functions less ad hoc and more predictable.

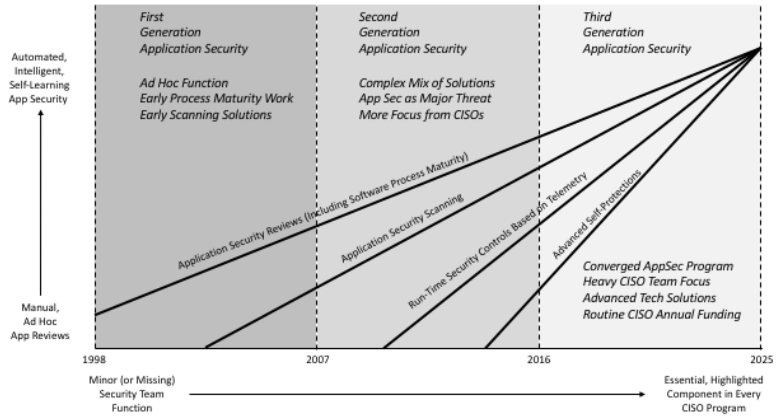

Figure 35. 2018 Application Security Outlook

The TAG Cyber degree of confidence in this predictive outlook is moderate, only because there are so many moving parts here. Application security could easily be argued as the least well-developed aspect of enterprise security programs. If you were to ask a group of typical CISOs what concerns them the most, for example, application security would be a popular answer.

Advice for Enterprise Security Teams

If you are part of an enterprise security team and you are feeling somewhat confused about application security, then you are not alone. Take some time this year to focus on learning about the different dimensions of application security, especially areas that you might be less familiar with as a team. Many enterprise teams have little understanding, for example, of software security maturity models, so perhaps spending some time in this area would be well spent. Similarly, many enterprise teams may have never considered the use of a run-time security control such as a RASP tool in their application hosting environment. This would thus be a good area to spend some time. In advance of the coming convergence in application security, the advice here is to focus on learning new methods, deploying proof-of-concept engagements, and creating new relationships with diverse vendors. Expect to see considerable merger and acquisition activity in this area in the coming decade.

Advice for Security Technology Vendors

The good news for application security vendors is that every CISO will agree that this is a huge risk area and that improved solutions are required. Such common and uniform recognition will go a long way to driving new business. The bad news, however, is that you are dealing with a

confused and partitioned customer market. One challenge is that no one in a typical enterprise has any idea who owns running applications: It might be the developers; it might be the hosting tea; it might be the sponsoring business unit; it might be the community of users; and on and on. So, when a security team wants to improve the protection profile for an application, it's often unclear what steps need to be done – or even who to work with inside the enterprise. This can be frustrating for application security sales teams. The advice here is to remain patient and focus on helping everyone understand the mechanics of how your solutions works. Even if you cannot solve the enterprise confusion around who owns given applications, you can at least ensure that your own solution is not contributing to the complexity.

List of Support Vendors
Appthority – Appthority offers a unique solution for risk-scoring applications based on security factors.
AppSec Labs – AppSec Labs provides research and tool development for mobile application security.
Arxan – Arxan provides run-time protection for applications on mobile, desktop, embedded, and servers.
Aspect Security – Aspect Security provides training, software testing and analysis, and security consulting.
Beyond Security – Beyond Security offers automated security testing for networks, software, and Web applications.
Black Duck Software – The company provides app security, container security, and compliance for open source.
Bluebox – Bluebox offers advanced mobile app security and management solutions to protect data.
Capstone Security – Capstone Security offers services in application security, regulatory compliance, and security assessments.
Checkmarx – Checkmarx provides a range of static code analysis tools in support of application security.
CIX Software – CIX Software is working specifically in RASP with principals from the financial industry.
Code DX – Code Dx provides tools for static software testing of applications.
Content Security – Content Security provides a software solution for security testing Web applications.
Contrast Security – Contrast Security secures applications from zero day vulnerabilities via interactive security testing.
Coverity – Coverity provides a range of advanced software application testing tools for static analysis.
Cybera – Cybera provides a secure application defined network platform for enterprise applications.
Cyxtera – Cryptzone, part of Cyxtera, offers secure access, content encryption, and related security solutions.
DBAPPSecurity – DBAPPSecurity provides Web application and database security technology solutions.
Denim Group – Denim Group provides secure software, including app development, assessment, training, and consulting.
D-Risq – D-Risq provides automated formal analysis tools to improve the correctness of software.
ERPScan – ERPScan offers a suite of SAP security products and services for enterprise customers.
F5 – F5 supports network security and optimizing application delivery network capabilities.
Fortego – Fortego provides computer network operations development, reverse engineering, and security analysis.
Fortinet – Fortinet offers its flagship next-generation firewall with VPN integration and support for application security.
GreenSQL – GreenSQL provides database application security for data masking, compliance, and database threat protection.
Groundworks Technologies – The company provides engineering services including embedded device security.
HPE – HPE offers the WebInspect dynamic analysis security-testing tool for vulnerability discovery in Web applications.
IBM – IBM offers in its security suite the AppScan tool, which tests Web and mobile applications for vulnerabilities.
Include Security – Include Security offers information and application security assessment, advisory, and consulting services.
Indusface – Indusface offers a suite of Web application firewall (WAF), and Web and mobile application testing products.
Klocwork – Klocwork provides advanced secure code analysis tools for software and application security.
Lancera Security – Lancera Security offers penetration testing and secure application development.
Layer Seven Security – Layer Seven Security offers SAP security services including app security and penetration testing.
Lookout – Lookout offers a range of mobile and application security solutions for personal and enterprise use.
Marble Security – Marble, acquired by ProofPoint in 2015, provides a mobile app security based on threat intelligence.
Metaforic – The company provides technology for software developers to ensure that their code is self-defending.
Minded Security – Minded Security provides software security consulting as well as application security testing tools.
Mocana – Mocana provides a mobile appl security platform with support for embedded devices in the Internet of Things.
N-Stalker – N-Stalker provides a Web app security scanner to support the web development lifecycle.
Onapsis – Onapsis supports advanced protection of SAP applications and processes from vulnerabilities.
Parasoft – Parasoft offers virtualization, API testing, and development testing software solutions.
Penta Security – Penta Security offers Web application security, database security, and single sign-on solutions.
Port80 Software – Port80 Software provides Web application security and performance focused on Microsoft IIS.
PortSwigger – PortSwigger offers the Burp Suite Web application security testing software solution.
Pradeo – Pradeo provides an advanced suite of mobile application security testing tools and APIs.

Prevoty – Prevoty offers an advanced, dynamic run-time application security solution for the enterprise.
Protected Mobility – Protected Mobility offers solutions for mobile app security including a secure SMS service.
Quotium – Now part of Synopsis, Quotium provides an automated continuous, application security testing solution.
Radware – Radware offers application delivery and load balancing, web application firewall, and other areas.
Rapid7 – Rapid7 provides vulnerability management, penetration testing, and application monitoring security solutions.
SafeBreach - The SafeBreach platform executes breach methods on a target system to identify potential weaknesses.
Saviynt - Saviynt provides cloud access governance and intelligence for data protection, privacy, and regulatory requirements.
Security Innovation – Security Innovation provides app security awareness training and related products and services.
Sentrix – Sentrix provides cloud-based Web application security and DDOS solutions for the enterprise.
Sonatype – Sonatype provides open source dev/ops tools including Nexus firewall for software development organizations.
Synopsys – Synopsys provides a range of application security protections from several recent acquisitions.
Trend Micro – TrendMicro provides a range of enterprise and cloud security solutions that are applicable to application security.
TrulyProtect – TrulyProtect provides an encryption-based software data security solution.
TrustWave – TrustWave provides solutions based on the acquisition of Application Security Inc. in 2013.
Veracode – Veracode offers enterprise, Web, and mobile application security solutions to detect weaknesses.
Virsec – Virsec provides next-generation data breach protection for applications including virtual patching.
Virtual Forge – Virtual Forge offers a range of advanced security solutions for SAP application users.
Waratek – Waratek provides application security through runtime application self-protection for Java as well as containers.
White Cloud Security – White Cloud Security provides blocking of untrusted application executables and scripted malware.
whiteCryption – whiteCryption provides code integrity protection for apps, as well as a white-box cryptography library.
WhiteHat Security – WhiteHat Security supports discovery and continuous scanning of Web applications.

Control 36: Content Protection

Content Protection involves the establishment and management of digital rights for owned, created intellectual property. The emphasis here is less on protection of digital rights for pure entertainment such as movies, video, music, and books – although much of the discussion here certainly applies. Instead, however, our emphasis is on the use of familiar techniques such as digital rights management (DRM) to protect conventional business assets such as files, databases, records, and other information. Almost all DRM solutions, which generally use cryptographic controls and administrative software to enforce owner-defined policies for digital property, have underperformed to date for a variety of reasons. One reason is the complexity of operating the underlying PKI services; another is relative unpopularity of digital rights, especially in entertainment; a third is the clumsy approach to private readers and other client software sometimes used to contain content; and we could go on. As a result, the view here is that enterprise DRM solutions will not grow, although some stubborn users will continue to run stand-alone systems. Instead, however, a new content protection industry will emerge in the cloud, where embedded cryptographic controls will allow users to host their intellectual property in the cloud and to specify exactly the controls required for users. Anyone who has ever published a book on Amazon.com or placed music on iTunes knows exactly how this works, and the extrapolation to enterprise IP is obvious. The difference is that instead of using a credit card to purchase an eBook from the cloud – which we all do often, you would use a credential to download a shared business document. Our commentary here is largely predictive and observational, since we have not seen as much vendor activity here as we would expect.

General Outlook
The general outlook for content protection solutions involves transition from weak, ineffective stand-alone enterprise DRM systems that are hosted inside a perimeter LAN to cloud-hosted

content protection systems that are embedded into SaaS infrastructure. First generation content protection from 1998 to 2007 involved early enterprise DRM solutions that were complex and that led to many failed projects. (OK, maybe not all were failed, but next time you are with some more senior CISOs, ask about their enterprise DRM efforts during that period and 90% of them will be happy to share their prior challenges.) Second generation content protection from 2007 to 2016 involved a clear reduction in emphasis on enterprise DRM, amidst a clear rise in content risk. So much intellectual property was stolen by nation-state actors during this period, for example, that some observers would call this period as having experienced the largest shift of intellectual property (from owner to cyber thief) in the history of the world. Some visionary CISOs began to explore use of cloud to protect content, but it never reached much critical mass. Third generation content protection from 2016 to 2025 should expect to see familiar techniques such as embedded rights in cloud-hosted content to be used more extensively in the enterprise to protect shared data. It's almost comical that during enterprise security team discussions about how to deal with this "frustrating problem of protecting our IP," that during the meeting break, attendees will download a song from iTunes or a book from Amazon. The obvious design extrapolation will become more noticed during the next decade and cloud-hosted content protection in the enterprise will grow exponentially.

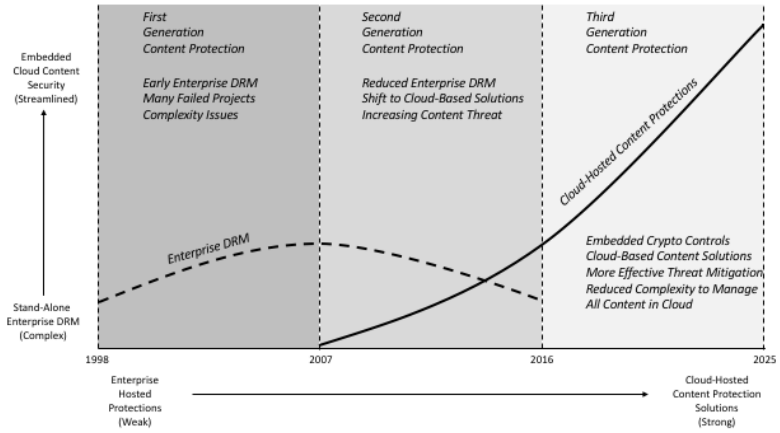

Figure 36. 2018 Content Protection Outlook

The TAG Cyber degree of confidence in this predictive outlook is moderate, because we are being predictive here about a complex area. Only minor evidence exists that embedded DRM solutions in the cloud will catch on at-scale across enterprise sectors. Time will tell, but we are hopeful.

Advice for Enterprise Security Teams

If you are new to content protection and DRM, then you are not alone. Most CISOs do not have experts on staff who understand this technology, and their predecessors may have warned about avoiding complex enterprise DRM solutions with their private client readers and complicated PKI underbellies. Most current document protection deployments tend to be small and isolated, with a plethora of tiny vendors supporting handfuls of clients. The problem is that

enterprise content and IP are being ripped off at ridiculous high rates across entire industrial sectors, so CISO teams would be wise to begin exploring protection options with small document protection vendors, and with the larger cloud and SaaS providers. You will find that most of the more successful cloud service providers will be happy to discuss DRM-like capabilities with you.

Advice for Security Technology Vendors

The embedded use of cloud-based content protection to offer virtualized DRM solutions for enterprise is a major business opportunity with massive growth opportunities and exponential revenue growth potential. It is therefore curious that this is not a bigger component of the cyber security vendor landscape. Cloud service providers should be marketing virtual DRM to enterprise buyers. The advice here is to learn from the existing consumer DRM solutions from Apple, Amazon, and the like. The use of TPM-based TEE on mobile and PC devices could also be used to federate credentials from the user domain up to the embedded DRM domain where IP is stored.

List of Support Vendors

Adhaero – Adhaero Doc supports encryption and control of Microsoft Office and Outlook documents throughout the lifecycle.
aegisDRM – G-Tech offers aegisDRM product that supports security control for Microsoft Word and other Office products.
Amazon Web Services (AWS) – Amazon offers DRM options for content users as well as for AWS infrastructure services.
Apple – Apple supports DRM for its range of devices, computers, systems, applications, and support.
Appligent – Appligent supports a range of enterprise DRM protections for protecting PDF documents.
Araloc – Araloc offers secure content management, distribution, and file sharing.
Armjisoft – Armjisoft provides DRM solutions for license protection, watermarking, and related protections.
Artistscope Copysafe – Artists Copysafe offers a web plugin to protect media from unauthorized copy.
Arxan – Arxan provides two-tiered software-based application and key protection for digital media.
Axinom – Axinom offers a multi-DRM service supporting Microsoft PlayReady, Apple FairPlay, and Google Widevine.
Aspack – Aspack provides its ASProtect solution for software protection with crypto registration keys.
Bisantyum – Toronto firm Bisantyum offers distributed DRM management using block chain technology.
ContentGuard – ContentGuard provides DRM-based content management technology solutions.
Content Raven – Content Raven provides cloud-based solutions for protecting the distribution of files.
CryptKey – CryptKey provides a range of software licensing and software copy protection options.
Defective By Design – Defective By Design is an organization that supports opposition to DRM.
docTrackr – docTrackr, from Intralinks, controls security in Gmail extensions and web apps for API-based and custom solutions.
Dubset – Dubset offers secure distribution solutions for artists, labels, and producers.
DRM NZ – DRM NZ provides advanced DRM support services for content creators, managers, and owners.
EditionGuard – EditionGuard consists of a secure eBook distribution platform with selling tools and DRM.
EMMS – Emacs Multimedia System supports multimedia files in Emacs using external players.
EZDRM – EZDRM provides an advanced digital rights management solution to protect digital media.
Fadel – Fadel supports the management of intellectual property via digital asset rights in the cloud.
Fasoo – Fasoo supports continuous encryption, permission control, and enterprise DRM solutions.
FileOpen – FileOpen consists of an Adobe Acrobat plugin that ensures that digital publications are not redistributed.
FinalCode – FinalCode provides an encryption-based solution for secure file sharing in enterprise.
Foxit – Foxit offers its customers a range of advanced secure PDF protection solutions including readers.
Gemalto – Through acquisition of SafeNet, the company includes DRM in their range of content protection offerings.
GiantSteps – Management consultancy GiantSteps focuses on protection for the content industries.
GigaTrust – GigaTrust offers its customers a range of pervasive content management security solutions.
Google – Google includes Widevine DRM protections in its device, application, system, and content ecosystem.
Haihaisoft – Haihaisoft offers the DRM-X digital rights management solution to protect digital content products.
HoGo – HoGo provides a digital rights management (DRM)-based solution for protecting and sharing documents.
Inside Secure – Inside Secure provides embedded security for mobile payment, content protection, secure access, and IoT.
InterTrust – InterTrust Technologies invents, develops and licenses software and technologies in crypto and DRM.
Identify3D – Identify3D provides IP protection, quality assurance, and data security through all phases of digital manufacturing.

Link Data Security – Link Data Security provides advanced copy protection for CDs, DVDs, USB, and Web.
Liquid Machines – Liquid Machines develops enterprise rights management software to protect corporate assets.
Locklizard – Locklizard provides DRM software for complete document security and copy protection.
Lockstream – Lockstream offers advanced DRM solutions for ringtones, music, and mobile games.
Microsoft – Microsoft provides software, electronics, and PC services including IT security and content protection.
NextLabs – NextLabs supports a wide range of enterprise digital rights management security solutions.
OpenText – OpenText provides a content management platform for cloud, Oracle, Microsoft, and other software suites.
Rchive – Rchive consists of a copyright protection system for securely sharing, tracking, and revoking access to screenplays.
Rightsline – Rightsline provides DRM for tracking contract and royalty rights with emphasis on media and entertainment.
Sansa – Sansa provides embedded security for device content protection, platforms, and chip manufacturers supporting IoT.
SecureMedia – SecureMedia provides a security system for encrypted distribution of digital content.
Sealedmedia – Sealedmedia offers a range of digital rights management software solutions for customers.
Sofpro – Sofpro offers software copy protection and licensing solutions for Windows and .NET framework applications.
Softwarekey – Softwarekey supplies Protection PLUS software licensing and server licensing automation technology.
Source3 – Source3 provides an advanced software platform for licensing and distribution of 3D content.
Terbium Labs – Terbium Labs provides a fingerprinting solution that can detect stolen intellectual property.
Trend Micro – Trend Micro describes its endpoint and related security solutions as content security.
Valve – Valve develops Steam, a DRM-free solution for games. Their algorithms only protect titles that do not include a 3.
Vaultize – Vaultize supports enterprise secure file sharing solutions through its DRM security support.
X-Formation – X-Formation offers a wide range of software license management solutions in its suite.
Vitrium – Vitrium provides document security and digital rights management protection for PDF files.
Watchful Software – Watchful Software provides DRM-based data security solutions for enterprise customers.

Control 37: Data Destruction

Data destruction involves the policies, procedures, tools, and technology used to securely delete information and dispose of equipment. Amazingly, despite the most intense intellectual property theft in the history of the world during this past decade, enterprise security teams still pay insufficient attention to this critically important function. Data destruction should be addressed from three perspectives:

- *Destruction of Unneeded Stored Data* – Employees should only save data that is absolutely required for their job function. Massive distributed stores of old information across all the PCs in the company is a huge risk that can be easily avoided by informing employees of suitable criteria and procedures for removal.
- *Secure Delete Function for Critical Data* – When critical data is simply deleted on a PC, even the most novice IT professional knows that it can be recovered with readily available tools. This can be avoided through proper use of secure delete functions.
- *Proper Decommission of Unneeded Equipment* – When equipment is decommissioned from a company, the task is usually handled by a low-level IT employee who might have zero connection to the enterprise security team, and who might be following ad hoc procedures. This is obviously a large risk that is easily avoided.

It is surprising that this aspect of data handling has received so little attention to date in enterprise, but the good news is that virtual cloud services and infrastructure will begin more aggressively offering secure deletion functions for stored data and even computing infrastructure. This will grow significantly as criteria requirements frameworks begin to demand this capability, especially for anything critical, sensitive, or significant. Good standard for media

sanitization do exist including NIST 800-88 and DoD 5220-22, but the typical CISO will not even recognize these designations.

General Outlook

The general outlook for data destruction solutions involves transition from ad hoc IT control of this function to mandatory control of data destruction and media sanitization by security teams. First generation data destruction methods from 1998 to 2007 involved ad hoc coverage with parking lot dumpsters in heavy use for most companies, which led to the emergence of dumpster diving as a popular hack during this period. Second generation data destruction methods from 2007 to 2016 saw continued weak focus by enterprise security teams characterized by (I hate to say this but) neglect by CISOs. Few CISOs, for example, every bothered during this period to challenge records information management (RIM) policies developed by corporate lawyers that turned employees into pack rats saving everything on their PCs. Third generation data destruction from 2016 to 2025 should expect to see a massive growth in cloud-hosted solutions for media sanitization, secure delete, and proper decommission of virtual servers and equipment.

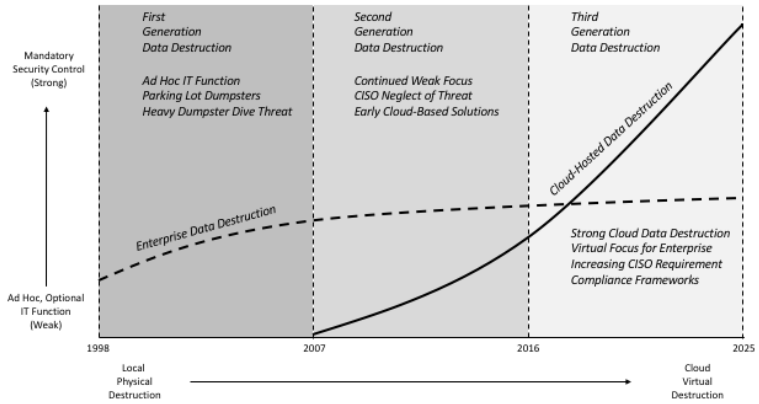

Figure 37. 2018 Data Destruction Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since the threat is significant and virtual solutions are not only easy to implement, but will be readily adopted by enterprise teams.

Advice for Enterprise Security Teams

The advice here is to an inventory today of your processes in this area. If a low-level IT staff member performed the decommission, then do whatever is necessary to either gain control of the function or write mandatory requirements for how the task is performed. The NIST 800-88 standard should help you. You should also immediately review your RIM policies to see if employees might be encouraged or required to get rid of anything they don't need. Do the math: If ten thousand employees remove a GB of unneeded data, you're just removed 10 TB of information that hackers can no longer steal.

Advice for Security Technology Vendors

The existing market will continue to operate within the enterprise with small to negligible growth. Lots of tiny local vendors driving trucks to corporate parking lots for periodic disposal will continue to be popular, albeit offering insecure services. The big trend is for cloud providers to include secure deletion, media sanitization, and secure decommissioning of virtual servers and infrastructure as an option for customers. Some of the larger providers mention secure data erasure today in passing, but few use this as a marketing differentiator. The advice here is to highlight the function wherever you can, and market it as an add-on capability for users who need more protection (and this should be everyone).

List of Support Vendors

All Green – All Green provides secure and certified data destruction and on-site hard drive shredding services.
Altep – El Paso-based Altep provides forensics and data destruction with a consulting practice focused on cyber security.
Applied Magnetics Lab – Applied Magnetics Lab manufactures military security and data destruction equipment.
Brass Valley – Brass Valley is a comprehensive IT solutions and services firm with solutions for data destruction.
Corporate Business Services – Corporate Business Services provides hard drive shredding and related services.
CloudBlue – CloudBlue provides IT asset disposition, on-site data destruction, and IT lifecycle support.
Data Destruction – Data destruction offers hard drive shredding, paper shredding, and electronic recycling.
Data Devices International – DDI provides secure data destruction, degaussing, and hardware destruction services.
Data Killers – Data Killers includes a range of on-site shredding and degaussing solutions for tapes and hard drives.
Data Security Inc. – Data Security supports securely erasing and destroying data stored on hardware media.
4Secure – 4Secure provides security consulting and training for clients across Europe.
4thbin – 4thbin provides a range of certified and secure data destruction services for customers in New York.
Garner Products – Garner Products includes professional data destruction for high security wiping.
Guardian Data Destruction – Guardian Data Destruction specializes in on-site data destruction.
Heshengda Information Security – HSD manufactures information destruction devices including degaussers.
IntelliShred – New Jersey firm, IntelliShred, offers a wide range of on-site document shredding services.
Iron Mountain – Iron Mountain is an industry-leading information disposal, destruction, and management firm.
Kroll Ontrack – Kroll Ontrack includes a range of recovery, restoration, collection, review, discovery, and erasure services.
LSoft – Canadian firm LSoft provides a suite of advanced tools for data recovery, security, and backup.
Nexcut – Nexcut provides its enterprise customers with hard drive and digital media shredding services.
Phiston – Phiston offers a range of high security data destruction solutions including hard drive destruction.
ProShred Security – ProShred Security provides on-site shredding solutions for customers in the New York area.
ProTek Recycling – ProTek Recycling offers hard drive and data destruction including desktops, laptops, and servers.
Rockland IT Solutions – Rockland IT Solutions provides data destruction, data erasure, and document shredding.
Seagate – Seagate is a major American storage company offering a range of business products and services.
Secudrive – Secudrive provides USB data leakage prevention and advanced data security solutions including disk erasure.
Securis – Securis provides a range of IT asset recycling and data destruction services for businesses.
Shred-it – Shred-it offers a wide range of hard drive destruction services for obsolete data storage.
Sims – Sims offers customers several on-site data destruction services for magnetic and solid state devices.
Solstice Technologies – Solstice Technologies supports degaussing of USB, SD card, flash, and other media.
Systems Maintenance Services – Systems Maintenance Services includes IT asset disposition as part of its range of services.
TBS Industries – TBS Industries is a full-service computer recycling company supporting data destruction.
TechFusion – TechFusion offers data forensics and eDiscovery services including erasure verification and evidence preservation.
Verity Systems – Verity Systems is a manufacturer of magnetic media bulk erasers for data destruction.
Whitaker Brothers – Whitaker Brothers supplies paper shredders, folder, and other business equipment.
White Canyon – White Canyon offers advanced solutions for wiping hard drives and recovering files.
Wise Data Recovery – Wise Data Recovery offers a range of freeware for recovering deleted files.
World Data Products – World Data Products delivers refurbished equipment based on sales of used hardware.
ZLOOP – ZLOOP offers a range of data destruction and hardware recycling products and services.

Control 38: Data Encryption

Data encryption involves advanced technology, organized into a collection of algorithms, protocols, and supporting infrastructure, designed to protect information from unauthorized disclosure either during movement or at rest. Many use-options exist for this familiar and important security technology: Data encryption solutions can be packaged as stand-alone products, embedded features, or licensed software. They can be designed using proprietary algorithms (to take advantage of the attendant secrecy of design) or using standard, publicly available algorithms (to avoid the weaknesses of security-through-obscurity). They can be embedded in protocols that are designed specifically for a local or proprietary application, or they can be integrated into standard, massive-use protocols such as SSL or HTTPS. They can be weak, in the sense that either domain size or algorithm complexity are sub-optimal (as with obfuscation tools), or they can be strong enough to withstand the cryptanalytic techniques of nation-states (not an easy task). They can also be expensive to purchase and use, or they can be freely available toolkits that you can use with no restrictions. Years ago, the country of origin was a huge issue in data encryption, to the point where export issues became part of the computer security lexicon. Today, that issue, while still not completely non-existent, is certainly less of a pressing issue. The bottom line is that buyers will need to navigate the options listed above – not to mention the added dimension of picking an encryption vendor. This may be the most traditional and well-known aspect of our industry, but it remains one of the more difficult to properly deploy. One area where this difficulty will wane somewhat in the coming years involves protection of keys and certificates, if only because with virtualized computing in hybrid cloud, more of this critically important task will be outsourced to a third-party. Today, few buyers deploy proper protections of their keys and certificates. In the coming years, everyone will, given the relatively streamlined infrastructure required to support.

General Outlook

The general outlook for data encryption solutions involves transition from ad hoc, optional key management solution deployed in an uneven manner across our industry to required, standard key management, perhaps with hardware assisted protection using tools such as hardware security modules (HSMs) in trusted execution environments (TEE). The transition also involves a shift from ad hoc use of stand-alone data encryption tools to more smoothly embedded encryption functionality into virtualized hybrid cloud infrastructure. Databases, for example, are moving from enterprise-hosted systems to virtualized cloud-resident services; this enables embedded encryption and key protection options. First generation data encryption from 1998 to 2007 involved early software encryption with clumsy key management and poorly protected certificates. HTTPS usage grew during this period, which for many security experts, was the first introduction to PKI. Second generation data encryption from 2007 to 2016 saw continued growth of data encryption solutions with slightly improved key management techniques. HTTPS usage on the web grew dramatically for web-based e-commerce, but data encryption tool usage was massively scattered. Third generation data encryption from 2016 to 2025 should expect to see continued linear growth, but key and certification protection solutions will grow dramatically. During the coming decade, encryption solutions will become more embedded, simpler to manage, more dependent on hardware-based protection, and focused on encrypting cloud workloads. More as-a-service solutions, including database in the cloud, will include

embedded advanced encryption and supporting key management. This is good news for our industry.

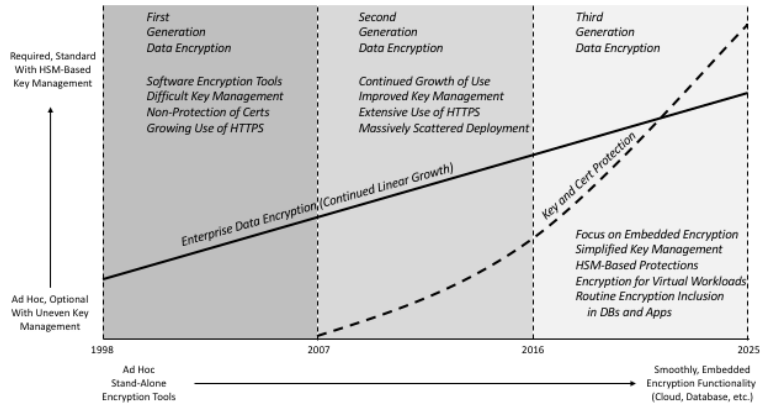

Figure 38. 2018 Data Encryption Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since data encryption will remains a core control, and virtualization will make the ever-nagging challenges of PKI, key management, and certificate handling much easier. This trend has already begun.

Advice for Enterprise Security Teams

The advice here for enterprise security teams is to remain committed to strong data encryption as a primary control, but begin to plan for more streamlined infrastructure as cloud services offer attendant encryption features. Spend less time debating key size, and more time figuring out how to federate and integrate different PKI solutions from cloud providers. Standards groups will emerge, like the FIDO Alliance, for how this can be accomplished. Write requirements this year that demand world-class encryption options from cloud providers, and look closely at vendors who offer excellent overlay solutions for encrypting your virtual data. These vendors have improved quite a bit in recent years.

Advice for Security Technology Vendors

This is a good time to be in the encryption business, but expect challenges from two different angles. First, you must expect the big infrastructure providers such as Tier 1 ISPs with SDN-based infrastructure and cloud service providers with virtualized capability to include embedded encryption into their offers. These large companies will have strong value propositions, so smaller encryption vendors should work hard to develop partnerships. Second, the use of encryption is becoming so commonly embedded in every aspect of computing that the integration and federation of different solutions will become as important as the strength of the cryptography and protocols. Make sure your alliances are strong and that your key management infrastructure plays nicely in the enterprise.

List of Support Vendors

Absio – Absio supports securely storing and sharing email messages externally, while maintaining control of its use.
AgileBits – AgileBits provides a range of security applications for password protection and file encryption.

Alertsec – Alertsec offers a Web-based service to deploy and administer Pointsec disk encryption software on PCs.
Boldon James – UK-based Boldon James provides data classification, secure messaging, and a range of related security products.
Boole Server – Italian vendor Boole Server provides data security and DLP through its encryption and support for sharing.
Boxcryptor – Boxcryptor provides file encryption tools for use with public cloud services such as Dropbox and Google Drive.
CA Technologies – The large software and technology company includes data encryption solutions for its customers.
CENTRI – Seattle-based CENTRI provides an advanced encryption-based solution for data protection.
Certes – Certes Networks provides software-defined, encryption-based security for enterprise applications.
Certicom – Now part of Blackberry, Certicom provides a range of cryptographic solutions using elliptic curve cryptography (ECC).
CertiVox – Now known as MIRACL, the company offers open source, distributed security and encryption solutions.
CheckPoint Software – CheckPoint provides a range of data encryption solutions based on its Pointsec acquisition.
CipherCloud – CipherCloud provides cloud security monitoring, encryption, and key management solutions.
Cisco – Through acquisition of Pawaa, Cisco offers secure on-premise, encrypted file sharing capabilities.
CloakLabs –The company provides end-to-end encryption of application data from the enterprise to partners.
CloudLink – Previously Afore Solutions, the company provides data security and encryption management products.
CORISECIO – CORISECIO provides a wide range of data encryption solutions for Microsoft SharePoint.
Cryptography Research – Part of Rambus, Cryptography Research licenses crypto solutions for semiconductor chips.
Cryptomathic – Cryptomathic provides security solutions for eBanking, PKI, ID, and ePassport.
Cypherix – Cypherix markets drag-and-drop personal data encryption software and network security tools.
DataLocker – Kansas-based DataLocker includes USB-based DLP protection solutions with digital rights management.
east-tec – Located in Romania, east-tec offers encryption-based products including secure erasure and other means.
Echoworx – Echoworx offers advanced email and desktop encryption products to secure data at rest.
EgoSecure – EgoSecure provides data protection solutions based on encryption, control, filtering, and management.
Encryptics – Encryptics provides a data privacy and protection software platform including encryption.
Entrust – Entrust provides a suite of authentication, identity, PKI, certificate, and mobile security solutions.
Fasoo – Fasoo offers a wide range of continuous data encryption, document security, and DRM solutions.
Futurex – Futurex offers a range of data encryption solutions include hardware security modules.
Gazzang – Now part of Cloudera, Gazzang offers data encryption solutions for Big Data deployments.
Gemalto – Through acquisition of SafeNet, the company provides authentication and encryption technologies.
GigaTrust – GigaTrust provides enterprise rights management built on Microsoft's Rights Management Services.
Global Data Sentinel – The company provides an advanced data security solution for the enterprise.
Guardtime – Guardtime provides keyless signature infrastructure that enables data integrity through block chain.
HPE – The acquisition of Voltage provided HPE with strong capability in data and email encryption marketplace.
InfoAssure – InfoAssure supports protecting assets through cryptography and content-based access controls.
InterCrypto – Seattle-based InterCrypto provides data encryption tools for files, disks, and media.
InterTrust – InterTrust Technologies invents, develops and licenses software and technologies in DRM and crypto.
Ionic Security – Ionic Security provides a cloud security platform focused on data protection, single sign-on, and analytics.
Krimmeni Technologies – Krimmeni Technologies provides secure communications and key management for cloud.
Linoma Software – Linoma Software focuses on data security solutions including encryption, backup, and secure file transfer.
Network Intercept – Network Intercept provides security and keystroke encryption products for PCs, Macs, and mobiles.
Penta Security – Penta Security offers web application security, database security, encryption, and single sign-on solutions.
PKWare – PKWare provides a data encryption solution for securing data files at rest and in transit.
Porticor – Porticor provides cloud security, encryption, and key management for public and private clouds such as AWS.
Protegrity – Protegrity markets comprehensive data security including tokenization, encryption, and policy enforcement.
Quintessence Labs – Quintessence Labs develops security for cryptographic purposes including quantum key cryptography.
RSA – This name is synonymous with public key encryption, but the company also focuses on other aspects of cyber security.
SafeLogic – SafeLogic supports integration of Suite B and FIPS 140-2 validated encryption into mobile devices.
Secure Channels – Secure Channels provides a range of data encryption solutions for various types of systems and applications.
Senetas – Australian firm Senetas provides defense-grade encryption solutions for government and commercial customers.
Sophos – The UK-based security firm offers encryption solutions, including full disk encryption, for its customers.
StrongAuth – StrongAuth offers encryption, tokenization, and key management for compliance and security.
Symantec – The large technology and cyber security company includes data encryption solutions for its customers.
TecSec – TecSec provides information assurance for access control enforced through encryption and key management.
Trustifier – Trustifier provides kernel-level security protections including mandatory access controls for UNIX systems.
Vaultive – Vaultive encrypts Microsoft Office 365 documents and other SaaS applications in cloud.
Venafi – Venafi secures the keys and certificates required for secure storage and communications.
Virgil Security – Virgil Security provides developers with advanced cryptographic software and services.
Vormetric – Vormetric deploys high performance data encryption for cloud, Big data, and other enterprise applications.
Wave – Massachusetts-based Wave provides a range of data security solutions for the endpoint including a virtual smart card.

whiteCryption – whiteCryption provides code integrity protection for apps, as well as a white-box cryptography library.
WinMagic – WinMagic provides full-disk encryption software to protect sensitive information on desktops and laptops.
WolfSSL – WolfSSL offers its customers an advanced and extensive SSL/TLS library for software developers.
Zettaset – Zettaset develops enterprise class data protection and encryption for Hadoop and other Big Data databases.
Zixcorp – ZixCorp provides a range of email encryption, BYOD, and DLP solutions for enterprise customers.

Control 39: Digital Forensics

Digital Forensics involves the people, processes, and tools required to investigate computing hardware and software artifacts to answer questions about prior improper or malicious use, and to perform data or system recovery tasks after damage may have been caused by a crime or other integrity-degrading action. Digital forensics traditionally was a human task with weak tools, but is evolving toward a more automated task with powerful tools. This unique branch of forensic science has a range of motivations to include investigation of a breach to recovering systems that were innocently damaged. (Emphasis in this report is primarily on malicious scenarios.) The biggest change in recent years that will intensify in the next decade is that digital forensics for enterprise must be increasingly performed on data that is under someone else's control – usually a cloud provider or third-party company. This change in control complicates the digital forensic task in both legal and technical manners, with the technical issues stemming from the diversity of infrastructure that must be addressed by the forensic investigator. This is not a big problem if standard, well-known technologies are being used; but it is an enormous task when proprietary systems must be analyzed. An added problem is that virtually everything is being encrypted, so any key management or algorithmic protections must be unraveled as part of the task. This was always true, but it has intensified. Law enforcement issues tend to weave into the digital forensic industry, simply because government investigators are large influencers in the technology direction of vendors in this segment. Many former law enforcers have tended to become successful digital forensic consultants to industry.

General Outlook

The general outlook for digital forensics solutions involves transition from data and systems being analyzed under local enterprise control to ones scattered across virtualized cloud workloads under the control of an external entity. An additional transition is occurring from digital forensics as an isolated task by a human expert under controlled conditions to one that integrates with the modern notion of SOC-based hunt team, usually focused on proactive investigation. This transition from reactive to proactive investigation is a good idea, because it allows digital forensics to be used to detect indications of malicious activity in advance of more serious consequence. First generation digital forensics from 1998 to 2007 involved rudimentary tools, heavily influenced by law enforcement with uneven adoption in all but the largest enterprise. Digital forensics was a unique skill during this era and 100% of the activity was performed after something bad had happened – often with the goal of recovering some damaged hard drive or computer. Second generation digital forensics from 2007 to 2016 involved more widespread adoption of the task, with law enforcement still dominating the skillset. Increased enterprise adoption during this era led to better forensic tools and early proactive focus. Third generation digital forensics from 2016 to 2025 should expect to see more

integrated digital forensic platforms with increased focus on investigative activity for data or systems no longer under direct enterprise control. Heavy emphasis will emerge for cloud-stored data, and the digital forensic task will integrate with SOC processes and hunt teams who tend to have a more proactive goal.

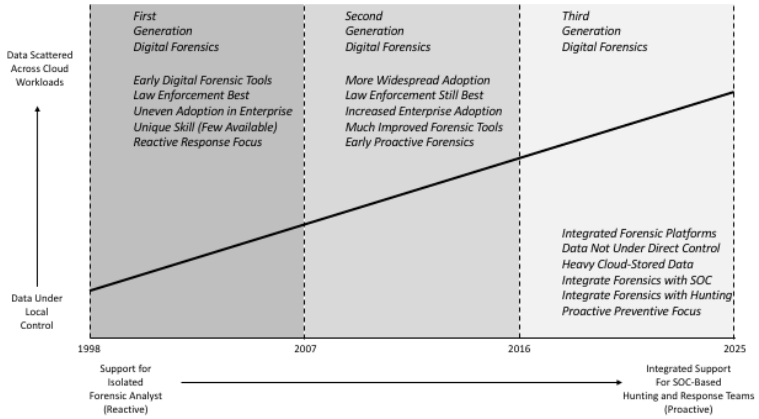

Figure 39. 2018 Digital Forensics Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since the likelihood that most enterprise data will migrate away from local control is almost 100%. This does not change the ultimate responsibility for the business assets of an enterprise, because outsourcing or offloading storage or processing does not shift ownership, unless a special contractual situation is established.

Advice for Enterprise Security Teams

If you are part of a large team, then you already have a well-developed digital forensic team, and you already know that your tools are becoming more powerful. What you may be just realizing is the degree to which your present and future data is migrating to distributed, virtualized systems scattered across hybrid cloud infrastructure. This will require some adjustment. If you are a smaller team, then the extent of digital forensics might be the desire to recover damaged devices or perform more isolated forensic tasks on mobile devices. Such emphasis on mobile device forensics is also something that requires attention, but most vendors offer effective solutions in this area, so this should not be much of a challenge. The biggest management challenge is whether to hire and manage local digital forensic experts or to outsource to expert consultants. The good news is that many former law enforcement experts with digital forensic skills are available for hire as consultants.

Advice for Security Technology Vendors

Digital forensics vendors are expanding their focus, so if you sell tools or services in this area, be so-warned. The most common expansion is from platforms that allow investigators to perform digital forensic surgery on some device to full endpoint security solutions that are more forensic and virtualization-friendly. The consulting business here must target solutions for hybrid cloud, with enterprise buyers wondering how to achieve forensic goals when the data to be

investigated or the machines to be analyzed are virtual and under someone else's control. International support is also a common requirement, so it helps to be a geo-political expert if you are performing digital forensic consulting for large multinational customers. The nagging concern for all digital forensic vendors is that the low barrier to entry continues to result in a huge number of small, medium, and large vendors offering solutions in this area. Expect to see consolidation, but it is still relatively easy to get into this business as a consultant. One additional major issue for digital forensic vendors is the heavy focus so many solution providers have on legal support. This is adjacent to the cyber security issue, so we do not maintain much focus on legal eDiscovery in this report; but most vendors cross over between cyber and legal, which is why the list of support vendors below includes many firms who sell to law firms.

List of Support Vendors
ACE Data Group – Philadelphia firm ACE Data Group provides data recovery and forensics services.
AccessData – AccessData is an expert provider of eDiscovery, computer, and mobile device forensics.
AC-Forensics – Kentucky firm AC-Forensics provides a range of data recovery and forensics services.
Advanced Discovery – New York-based Advanced Discovery supports legal eDiscovery for its customers.
Altep – Altep offers certified data forensic investigators, emergency response technicians, and data privacy consultants.
Asgard Group - Asgard Group provides wireless RF and comm security for counterintelligence and cyber investigations.
ASR – ASR provides expert technical support in digital forensics for customers with Linux-based systems.
Atlantic Data Forensics – Atlantic Data Forensics offers digital forensics, eDiscovery, and witness services.
Axiom – Axiom provides a range of forensic accounting, investigative, and expert witness services.
Azorian Cyber Security – Azorian Cyber Security provides a range of cyber security services for enterprise customers.
Barrister Digital – Barrister Digital offers a range of litigation and digital discovery support services.
Belkasoft – Belkasoft develops the its Evidence Center for enterprise digital forensic investigative support.
BIA – BIA offers expert digital forensics, eDiscovery, and witness services for enterprise customers.
Binary Intelligence – Binary Intelligence specializes in forensics of computers, cell phones, and chips.
BitSec Global Forensics – Maine-based BitSec Global Forensics provides computer forensic support.
Burgess Forensics – Santa Monica-based Burgess Forensics offers digital forensics, eDiscovery, and witness services.
Caveon – Caveon includes a range of data forensics solutions in its suite of fraud testing and investigative services.
CBL Data Recovery – CBL Data recovery provides a range of data recovery capabilities for failed hard drives.
Cellebrite – Cellebrite offers mobile forensics for analysis and extraction supporting law enforcement and military users.
Crane Engineering – Crane Engineering includes data forensics in its suite of technical and engineering consulting services.
Cyber Diligence – Cyber Diligence provides professional services to combat and investigate digital crimes.
CyberEvidence – CyberEvidence trains computer investigators in art of data recovery and analysis of evidence.
Cyfir – Cyfir provides its enterprise customers with an advanced digital forensics platform to support investigation.
Data Recovery Labs – Florida-based Data Recovery Labs specializes in expert data recovery for clients.
Data Forensics Group – Data Forensics Group supports data acquisition, data recovery, forensics analysis, and eDiscovery.
Datarecovery.com – Datarecovery.com supports a range of expert data recovery services for customers.
Data Rescue Labs – Canadian company provides data and system recovery solutions for mobiles and computers.
DataTriage Technologies – DataTriage Technologies offers computer forensics, recovery, and eDiscovery capabilities.
Data Triangle – Data Triangle offers computer forensics, recovery, and eDiscovery capabilities for litigation support.
Deedoc Consulting – Small Raleigh computer repair company Deedoc Consulting offers recovery services.
D4 eDiscovery – Rochester-based D4 eDiscovery includes a range of managed eDiscovery services.
Digital Detective Group (BLADE) – UK firm Digital Detective Group develops digital forensic software.
Discovia – Discovia delivers a range of managed eDiscovery services to companies and law firms.
Disklabs – Disklabs is a provider of computer forensic services for legal firms, law enforcement, and enterprise groups.
DisputeSoft – DisputeSoft provides advanced litigation support and expert testimony in New York.
Drivesavers – Data recovery firm Drivesavers support recovery for hard drives, RAID, SSDs, and phones.
D3 Forensics – Located in Asia, D3 Forensics provides a range of data forensics and litigation support.
DTI – DTI supports a range of expert legal eDiscovery professional services for enterprise customers.
Eco Data Recovery – Florida-based Eco Data Recovery offers a range of data and system recovery services.
e-fense – Colorado firm e-fense provides its customer with the Helix platform for digital forensic analysis.
Elcomsoft – Russian company Elcomsoft focuses on password and system recovery software solutions.
Elite Forensics Investigators – Elite Forensics Investigators supports digital forensics and paper discovery.
Enclave Forensics – Enclave Forensics offers expert incident response and digital forensic services.

Epiq Systems – Epiq Systems is a public company that supports technology services for the legal profession.
Expert Data Forensics – Small Nevada-based Expert Data Forensics supports recovery and forensics.
Flashback Data – Flashback Data offers a range of data recovery and computer forensics for hard drives.
Forensic Data Services – Forensic Data Services offers computer forensics, recovery, and eDiscovery capabilities.
Forensic Risk Alliance – FRA is a security consultancy that provides expertise in electronic forensic tasks.
Forensic Strategy Services – Forensic Strategy Services supports collection and preparation of evidence for legal proof.
4Discovery – 4Discovery offers computer forensics, computer security, and incident response solutions.
FireEye – Through its Mandiant unit, FireEye offers incident response and network analysis to support forensics.
FTI – Global business advisory firm FTI includes a range of digital forensics services for the enterprise.
Fulcrum Data Forensics – UK firm Fulcrum Data Forensics offers computer forensics, recovery, and eDiscovery capabilities.
G-C Partners – G-C Partners offers computer forensics, expert testimony, and eDiscovery capabilities.
GetData Forensics – GetData Forensics supports a range of data recovery, email recovery, and file repair tasks.
Global CompuSearch LLC – Global CompuSearch supports computer forensics, computer security, and incident response.
Global Digital Forensics – Global Digital Forensics supports data forensic investigations including eDiscovery.
Group-IB – Group-IB provides customer with a range of expert data forensic and investigative capabilities.
Guidance Software – Guidance Software is an industry-leading provider of the Encase forensic and analytic solution.
Hacking Team – Italian firm Hacking Team provides digital forensics and investigative tools for offense.
Hawaii Data Forensics – Hawaii Data Forensics specializes in investigations of computer forensics and network intrusion.
Helios Data Forensics – Helios Data Forensics offers computer forensics, computer security, and incident response.
ID Experts – ID Experts supports recovery services including identity theft protection and credit monitoring.
Iris Data Services – Iris Data Services provides a range of managed eDiscovery services for customers.
kCura – kCura develops advanced eDiscovery software for electronic evidence collection by customers.
Kessler International – Kessler offers forensic accounting, IP investigations, digital forensics, and investigative services
Kroll – Kroll provides a team of computer forensics experts to assist in digital evidence collection and analysis.
K2 Intelligence – K2 Intelligence is an investigative and risk analytics consultancy founded by Jeremy and Jules Kroll.
Larson Security – Larson Security provides cyber security services including digital forensics and incident response.
Lighthouse eDiscovery – Seattle-based firm Lighthouse eDiscovery supports legal eDiscovery for clients.
LIFARS – New York City firm LIFARS provides a range of data forensic and investigative capabilities.
Magnet Forensics – Magnet Forensics offers computer forensic and investigative tools for examiners.
Microforensics – Microforensics offers computer forensics, computer security, and incident response.
Northeast Ohio Forensic Data Recovery – Northeast Ohio Forensic Data Recovery supports digital forensics and litigation.
NowSecure – NowSecure includes digital forensics in its advanced suite of mobile security capabilities.
NTI Associates – NTI Associates offers computer forensics, computer security, and incident response supporting litigation.
Nuix – Nuix offers search, investigative, and information management analytics capabilities supporting digital forensics.
NuVida – The company offers a range of consultation, digital forensics, litigation, and expert witness services.
Oneconsult AG – Oneconsult AG provides data forensic and investigative capabilities along with its testing and auditing suite.
Optimo IT – Optimo IT includes legal support services in its range of technology consultation services.
OSForensics – OSForensics offers a range of forensic solution supporting discovery and extraction
The Oxman Group – Dallas-based Oxman Group includes data forensic and investigative capabilities in its response offering.
Paraben – Paraben provides a range of mobile data forensic and investigative capabilities for customers.
Parameter Security – Parameter provides pen testing, audit, and digital forensics specializing in the financial industry.
Peak Forensics – Peak Forensics offers computer forensics, eDiscovery, and expert witness services.
PwC Forensics – Consulting group PwC Forensics includes support for digital forensics dispute and related services.
Responsive Data Solutions – Responsive Data Solutions provides electronic discovery services and software for law firms.
St. Johns Data Consulting – St. Johns Data Consulting offers digital forensics, consulting, and expert witness in Jacksonville area.
Stroz Freidberg – Now part of Aon, Stroz Freidberg offers computer forensics, investigations, and expert witness.
Sylint – Sylint provides expert services in the areas of data forensics, eDiscovery, and compliance.
Symantec – Symantec supports a wide range of digital forensics capabilities across its product and service suite.
Tactical Network Solutions – Tactical Network Solutions supports a range of digital forensic solutions.
TCS Forensics – Western Canada firm TCS Forensics supports eDiscovery, forensics, and risk management.
TechFusion – TechFusion is a certified expert computer forensics firm located in Boston, Massachusetts.
Thumbtack – Thumbtack provides a range of data recovery and digital forensics services for customers.
Tri-State Data Recovery and Forensics – Tri-State Data Recovery and Forensics provides RAID and hard drive recovery.
UnitedLex – UnitedLex provides legal and business services that integrate consulting and technology.
US Data Forensics – US Data Forensics provides computer forensic examination, fraud investigations, and litigation support.
Wetstone – Wetstone, now part of Allen, offers a suite of forensic tools including WiFi Investigator and StegoHunt.
X-Ways Software Technologies AG – X-Ways provides hex file, disk, and RAM editor for data recovery and computer forensics.

Control 40: Identity and Access Management

Identity and Access Management (IAM) involves the people, processes, tools, infrastructure, and interfaces required to control the provisioning, maintenance, and operation of user identities and the associated set of authorizations required to enforce access policies in an enterprise. The case can be made that IAM is the most complex and challenging component of most enterprise security team responsibilities. Challenges include the following:

- *User Management* – IAM infrastructure must handle the day-to-day provisioning, maintenance, and help desk needs of users who might have serious deficiencies in their understanding of access and authorization policies.
- *System Interfaces* – IAM infrastructure must include connectors and interfaces to the systems and applications that require authorization policy. Human Resources (HR) systems are typical such applications.
- *Policy Complexity* – IAM policy can be complex and driven by unique organizational structure and asset protection needs. This often leads to highly customized IAM controls.
- *Approval Workflow* – The day-to-day authorization requirements for a typical IAM system will include workflow support including email approvals by supervisors for requested accesses.
- *Control Obligation* – IAM is increasingly challenged with the task of being primary control for many security requirements frameworks, supplanting the perimeter firewall with this assignment.
- *Performance Requirements* – Larger IAM installations supporting many users performing time-sensitive transactions, such as new product launches, will need to be particularly attentive to performance requirements.
- *Audit Responsibility* – Any IAM professional will attest that enterprise audits almost always have IAM infrastructure controls in their cross-hairs.

In addition to the above familiar challenges for IAM, the current issue involves transition from enterprise-hosted IAM with links to local applications and systems such as Active Directory to distributed, virtualized hybrid cloud environments that might require extensive federation of credentials and single sign-on (SSO) across heterogeneous environments. This is complex and evolving. An additional challenge, as if there weren't enough already, is the organizational debate that is so common regarding whether IAM should be managed by security teams or IT operations teams. The inevitable tug-of-wars that result will not make it any easier to manage IAM infrastructure in 2018 and beyond.

General Outlook

The general outlook for identity and access management solutions involves transition from centralized IAM deployment on an enterprise LAN to a distributed IAM configuration supporting hybrid cloud services. IAM infrastructure is also moving from highly complex,

difficult to administer services to greatly simplified services that are much easier to administer. First generation IAM infrastructure from 1998 to 2007 were enterprise hosted, highly complex, and generally tangled up in compliance issues that required a variety of complicated changes to support. IT team almost always had sole responsibility for IAM during this period. Second generation IAM infrastructure from 2007 to 2016 included early support for cloud, but continued complexity and compliance issues. IAM solutions during this era began to address IoT and M2M infrastructure, and began to evolve toward enterprise security team responsibility. Third generation IAM infrastructure from 2016 to 2025 should expect to see a transition to distributed, virtualized support embedded across hybrid cloud services and integrated into CASBs and microsegments. Introduction of strong identity credential federation originating in TEE-based computing will be another major advance.

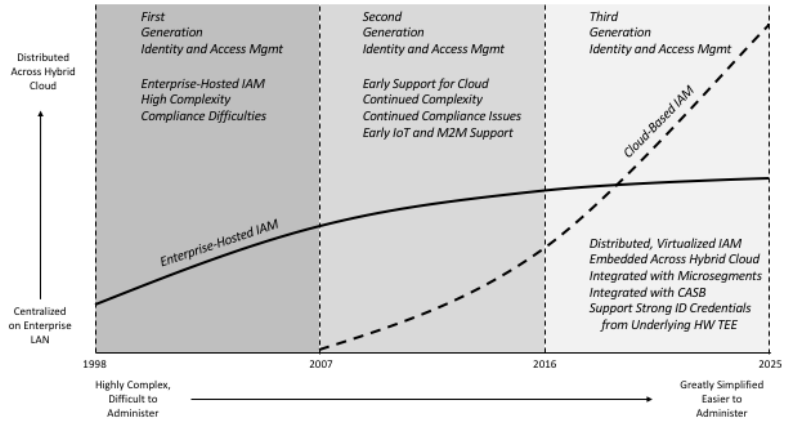

Figure 40. 2018 Identity and Access Management Outlook

The TAG Cyber degree of confidence in this predictive outlook is moderate, only because IAM has been such a messy aspect of enterprise security to date, and is thus difficult to predict. The biggest challenge to proper evolution to cloud for IAM is that so many important support systems such as Active Directory remain on the enterprise LAN. This results in IAM services constantly reaching back onto the enterprise LAN for information required to properly manage IAM and authorization workflow. As these support services migrate to cloud – as with Microsoft virtualizing Active Directory to cloud infrastructure, this effect will wane.

Advice for Enterprise Security Teams

So many different local issues will tend to exist across aspects of the IAM spectrum that it is especially hard to give broad, general advice to enterprise teams about this area. One common suggestion is to work hard for clarity of IAM responsibility with IT operations staff. Too often, confusion around IAM responsibility results in weak action, and this can be fatal for companies moving to hybrid cloud. In addition, enterprise teams should demand roadmaps from their existing IAM vendors on how the transition to mobility-enabled cloud services can be handled. New entrants in the CASB and cloud security space can offer IAM services, so competition will emerge from these previously non-existent vendors. If there is one rallying cry for enterprise teams regarding IAM over the next decade, it would be to *reduce complexity*. More is less in

IAM, and new features are less attractive then streamlined operation. Pay special attention to complex federation schemes that some vendors will offer across heterogeneous cloud services, resulting in a weird pass-the-buck arrangement for identities.

Advice for Security Technology Vendors

IAM vendors range from small consultants to monster-sized companies offering full-featured enterprise solutions. In all cases, however, the transition to mobility-enabled hybrid cloud will change the nature of IAM solution offerings. It thus stands to reason that you will need to develop a migration plan to support virtual data center and SDN-hosted infrastructure, including public cloud. You will resist this transition at your peril, and excuses such as Active Directory and legacy HR applications remaining inside the perimeter will not serve you well in the long run. Commit to cloud immediately. In addition, the advice offered above to enterprise teams to seek less complex solutions for IAM extends to vendors as well. More features are less impressive than streamlined, simplified management and operation. Less really is more in IAM, and the best vendors will internalize this into their designs.

List of Support Vendors

Aegis Identity – Aegis Identity offers an identity management solution focused on the education market.
Alert Enterprise – Alert Enterprise provides infrastructure protection through GRC management and monitoring
Amazon Web Services – AWS includes IAM capability for securely controlling access to its cloud services and resources.
Atos – Atos offers the DirX portfolio of advanced identity and access management product solutions.
Aujas Networks – Aujas Networks provides security solutions in vulnerability management, data protection, and IAM.
Auth0 – Auth0 provides a product that allows developers to add identity federation to their apps.
Avatier – Avatier automates IT operations and compliance of user provisioning, access management, and related functions.
Avecto – Avecto focuses on providing Windows-based privilege management for desktops and servers.
Axiomatics – Axiomatics supports attribute-based access control and dynamic authorization based on XACML 3.0.
BeyondTrust – BeyondTrust supports privilege and identity management for servers and other IT software.
Bitium – Bitium provides a cloud-based platform for managing passwords, users, and SaaS application access.
CA – CA offers its Identity Suite, Privileged Access Manager, Identity Manager, and Identity Governance solutions.
Centrify – Centrify offers an identity and cloud management platform supporting Identity-as-a-Service solutions.
Certified Security Solutions (CSS) – Certified provides solutions in the areas of PKI, encryption, and identity for IoT
Coreblox – Coreblox is a premier provider of identity and access management for enterprise, federation, and cloud.
Core Security – Formerly Courion, Core supports IAM with self-service password management and automated access reviews.
Covisint – Originally focused on connected vehicle, Covisint has expanded to secure IoT, supply chain, and IAM.
Cross Match Technologies – Cross Match technologies provides IAM and biometric identity verification solutions.
CyberArk – CyberArk focuses on locking down privileged accounts to reduce security risk and advanced persistent threats.
Daon – Daon offers platforms, tools, and apps focused on identity assurance and biometrics.
Deep Identity – Located in Singapore, India, and the UK, Deep Identity supports identity and data governance.
Deepnet Security – Deepnet Security provides multi-factor authentication and identity and access management solutions.
Dell Software – Dell provides a suite of identity governance, access management, and privileged management for enterprise.
DirectRM – DirectRM provides strong authentication and access management solutions supporting BYOD.
Ellucian – Ellucian provides range of education industry software with identity and access management consulting services.
Equifax – Equifax supports credit reporting via identity assurance for personal, small business, and larger business applications.
Evidian – Evidian supports IAM for single sign-on, user provisioning, and related functions for enterprise and cloud.
Exostar – Exostar offers a range of identity and access management and cloud collaboration solutions.
Experian – Experian supports identity and credit access, as well as related data management solutions.
Fischer International – Fischer offers IAM software for outsourced and on premise environments for higher education.
ForgeRock – ForgeRock provides identity and access management for cloud, mobile, and enterprise.
FoxT – FoxT provides a suite of network security and access management solutions for the enterprise.
Gluu – Gluu provides an open source or on demand, standards-based identity and access management capability for enterprise.
Google – Google offers identity services that federate Google login to other cloud identity and access apps and services.
HID Global – HID Global provides identity and access solutions including smart cards, readers, RFID tags, and software.
Hitachi-ID – Hitachi-IS provides identity and access management including support for governance and password management.

HPE – HPE offers its Cloud Identity Service supporting secure identity and access management for the Helion Public Cloud.
IBM – IBM offers capabilities based on early acquisition of Tivoli for identity and access management.
Identacor – Identacor enables secure, one-click access to corporate applications via SaaS identity management and SSO.
Identia – Identia provides next-generation identity and access focused on cloud use and integrated with PKI technologies.
Identicard – The company manufactures ID, access, and security cards and accessories in support of IAM.
Identigral – Identigral offers consulting services and solutions for clients working on identity and access management.
Identiv – Identiv offers a range of identity solutions supporting premises access, data access, and credential management.
Identropy – Identropy provides a range of information, resources, and services in support of IAM.
i-Sprint Innovations – i-Sprint Innovations provides identity, credential, and access management solutions.
iWelcome – iWelcome supports identity and access management for European government applications.
Jericho Systems – Jericho Systems provides support for access management with emphasis on XACML implementation.
Lieberman Security – Lieberman includes a range of products related to identity, passwords, and privilege management.
Mycroft – Now part of EY, Mycroft provides a range of managed and professional services in IAM.
NetIQ – NetIQ, offered by MicroFocus, includes full-featured IAM and security management solutions.
NextLabs – In addition to data and rights security, NextLabs offers XACAML policy server solutions.
neXus Group – neXus Group supports identity management, certificate and key management, and authentication.
9Star – The company offers customers its Elastic SSO software solution for federated access technology.
Okta – Okta offers customers a cloud-based solution for identity and access management services.
OnWire – OnWire includes a FedRAMP, multi-factor authentication platform with cloud based IAM.
Omada – Omada offers solutions for identity management, governance, compliance, and user provisioning.
OneID – OneID focuses on the management of on-line identities without the need for passwords.
OneLogin – OneLogin supports cloud-based IAM with secure access to cloud applications from mobile devices.
Oracle – Oracle provides a full featured, industry-leading capability with large and small customers.
Osirium – Osirium provides privileged user account management and protection solutions for the enterprise.
PerfectCloud – PerfectCloud offers range of cloud security solutions including SmartSignin with SSO and federated IAM.
Ping Identity – Ping Identity supports enterprise identity and access management for internal and SaaS applications.
Protected Networks – Protected Networks is a German company that provides server access rights management solutions.
Radiant Logic – Radiant Logic supports identity, federation, and directory services through virtualization and cloud.
RSA – RSA offers a range of IAM solutions building on the Aveksa acquisition and the industry-leading RSA token for 2FA.
Sailpoint – Sailpoint offers on-premise and cloud-based identity and access management platform.
Salesforce Identity – Salesforce Identity includes extensive IAM functions to provide SaaS protections for Salesforce.
Saviynt – Saviynt provides cloud access governance and intelligence for data protection, privacy, and regulatory requirements.
SecureAuth – SecureAuth provides an IAM solution supporting SSO and 2FA for mobile, web, and cloud applications.
SecureKey – SecureKey offers identity and authentication solutions for online consumer service providers.
SecZetta – SecZetta provides services specializing in IAM implementation and privileged account management.
Simeio – The company offers the Simeio Identity Orchestrator platform and Identity Intelligence Center solution.
Soffid – Soffid offers an open-source identity and access management solution with support for SSO.
Stormpath – Stormpath provides a user management API that allows developers to integrate authentication for users and roles.
SurePassID – SurePassID provides cloud-based identity and access management for mobile and hybrid cloud use.
Syntegrity – Syntegrity provides security products and services including support for identity and access management.
Tools4Ever – Tools4Ever offers identity governance and administrative tools and enterprise solutions.
Transunion – Transunion provides fraud, identity, and credit-related services. Transunion acquired Trustev in 2015.
2Keys – 2Keys provides managed and professional services with emphasis on user authentication and identity attributes.
UnboundID – UnboundID offers identity and preference management through the UnboundID platform.
White Cloud Security – 2Keys provides managed and professional services for user authentication and identity attributes.

Control 41: Security Compliance

Security compliance involves the lifecycle activities required to provide sufficient evidence that an organization meets the requirements of a desired control framework. In industry, the dominant such framework to date has been the Payment Card Industry (PCI) Data Security Standard (DSS) which supports merchants around the world who are handling credit cards. Many other frameworks exist – in fact, the situation has grown almost absurd with the enormity of security compliance obligations for organizations of every size and scope, and in

every sector. PCI DSS is highlighted here simply because such a large professional service industry exists for Qualified Security Assessors (GSAs) who are certified to be sufficiently competent to work with clients. But the reality is that this industry is burgeoning to the point where enterprise cyber security teams in sectors such as banking might direct roughly 75% of their time, energy, and budget to compliance activities. Perversely, this obsession is often driven less by any sincere desire for security program quality, and more by the need to avoid repercussions by financial regulators or other large organizations such as credit card companies. Most business being done by security vendors in this area focuses on professional services, but adjacencies with GRC platforms are obvious. The advice from many pundits (including here) has been an urgent plea for more streamlined security compliance requirements in cyber, with local selection of one good framework that could support a single, properly done compliance assessment. Federation or export of those results should be sufficient. Nevertheless, the global industry appears to be headed in the other direction, which is excellent news for compliance consultants, but terrible news for CISOs. The next decade is as impossible to predict as an election, but we will be optimistic here – and will maintain the hope that the needs of the working enterprise security practitioner will prevail, and that compliance will become a saner activity in the coming decade. Such sanity would involve doing compliance properly once – *even in the face of many more compliance frameworks*, and using the results to support a wider variety of needs by business partners and regulators. The result would be a gradually improving quality of security compliance over the next decade, with the rate of improvements growing at a faster clip than has been seen to date. Improved automation support will contribute to this acceleration of quality as well – and that is good news for CISO teams.

General Outlook

The general outlook for security compliance solution offerings, especially in support of PCI DSS, involves transition from a small number of frameworks in the late 90's to the inevitable continued growth in the number of applicable compliance frameworks. The hope, however, is that even with this increased number of frameworks – new ones emerging, for example, in various US States – that CISO teams will be able to select and choose the correct ones and federate the results to different contexts. Transition will also continue from mostly manual, overlay processes for compliance to automated and embedded compliance programs. First generation security compliance programs from 1998 to 2007 were used as penalties by regulators. Most manual processes were used with lots of paperwork to support a growing number of frameworks. The quality of compliance programs remained low during this period. Second generation security compliance programs from 2007 to 2016 improved somewhat as GRC automation streamlined what was still too much paperwork. Regulators continued to use compliance as the basis for penalty and the number of frameworks continued to grow. The best effect during this period was the growing recognition that compliance and security were different objectives. Third generation security compliance from 2016 to 2025 should expect to see an accelerated rate of quality improvement for compliance with better automation and fewer applicable frameworks (note that *applicable* is different than *available*.) During this period, everyone will come to recognize compliance as clearly separate from security, and this

will result in much improved interpretation of results and less reactionary management plans, especially from Boards.

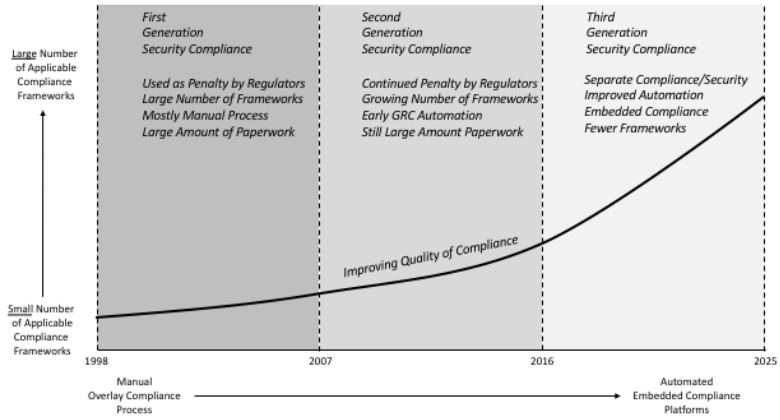

Figure 41. 2018 Security Compliance Outlook

The TAG Cyber degree of confidence in this predictive outlook is moderate, because compliance involves politics and power, neither of which are easy for gearhead cyber security analysts to factor into their predictions. Suffice it to say, we choose to be positive and to predict improved compliance quality, regardless of how this might be achieved in practice.

Advice for Enterprise Security Teams

Enterprise security teams are typically frustrated when it comes to compliance programs – albeit with a caveat: Some larger teams have seen internal groups and staff members grow comfortable with their compliance jobs. Some have spent nearly their entire professional career, perhaps over decades, working in security compliance. This leads to complacency and the common belief that what is familiar and normal is also optimal – which is sad, because the time and effort spent to date on compliance has had little impact on the security of our industry. Virtually all retail companies hacked in the past decade were PCI DSS compliant. The only reason the rate of security hacking has waned is that the functional weakness of unencrypted card swipe machines was replaced with better protection at the retail counter. CISOs thus should focus on three things: (1) Coach your teams to do great compliance, but to remain skeptical that this should be so dominant in your budget and attention planning; (2) Drive to the highest levels of automation possible to streamline gap analysis and to minimize the awful paperwork so typical of compliance work; and (3) Develop good relationships with world-class compliance consultants who can help bridge the gap between different frameworks.

Advice for Security Technology Vendors

If you sell solutions in this area – and we differentiate here with GRC platforms, which are considered a separate control area, then you are more than likely selling professional services to your clients. The good news is that business will continue to grow for you, but the warning here is that customers will demand that you speak multiple compliance languages. They are

going to be looking more and more for consultants that can help them establish PCI DSS, while at the same time helping them deal with customers who want better NIST Framework dependency. These are easy cross-overs for consultants, so this should not be a big deal. The competition is fierce in compliance consulting, so don't expect your small consultancy to develop into the next Deloitte unless you come up with a major break-through in automation support. Perhaps deep learning tools for compliance would be something to look at (and we are only partially kidding here).

List of Support Vendors
Above Security – Above Security includes PCI DSS and compliance consulting in its managed security and audit offerings.
ANX – ANX is a global provider of managed payment, compliance, and security services for customers.
AT&T – AT&T includes a wide range of expert compliance and PCI DSS QSA support in it global consulting offering.
Ather Technology – Trading as Cianna Technologies, Ather is the only PCI DSS registered in the Kingdom of Saudi Arabia.
Attack Research – Attack Research is a PCI-QSA certified consulting group located in Los Alamos.
Avnet – Avnet is a professional consulting firm in Israel includes range of compliance and PCI services.
BAE Systems – BAE acquired SilverSky, which offers a managed, GSA-approved PCI compliance solution.
Bell Canada – Bell Canada includes a range of security compliance and PCI consulting as part of its services.
Blackfoot – Blackfoot is a UK firm offering a wide range of PCI and compliance consulting services.
Cadence Group – Cadence Group is an advisory and compliance consulting firm offers support for PCI and other frameworks.
Cadre Information Security – Cadre Information Security consulting firm in Cincinnati provides compliance and PCI assessments.
The CISO Group – The CISO group offers information security consulting with an emphasis on PCI DSS compliance issues.
Clone – Clone Systems is an MSSP that focuses on continuous monitoring, secure cloud, security scanning, and consulting.
CNS Group – UK consulting firm CNS Group offers information assurance, IT security and compliance solutions.
Coalfire – Coalfire provides cyber risk management and compliance services for enterprise and government organizations.
Compass IT Compliance – Compass provides IT compliance, security, and audit professional services.
CompliancePoint – A PossibleNOW Company, CompliancePoint offers information security consulting.
Comsec Consulting – Comsec Consulting offers services with emphasis on risk management and compliance.
Content Security – Content Security includes a range of PCI DSS consulting in its professional service suite.
Contextual Security – Contextual Security offers IT security services including PCI and HIPAA consulting.
Continuum Security Solutions – Information security firm Continuum is engaged in compliance, assessments, and governance.
ControlCase – ControlCase is an information technology, GRC, managed compliance software, and services company.
ControlGap – ControlGap is an approved Canadian QSA company for PCI DSS security compliance.
ControlScan – ControlScan provides a wide range of PCI compliance and self-assessment services.
CrimsonSecurity – CrimsonSecurity includes compliance services for PCI DSS, ISO 27002, NIST 800-53, GLBA, and HIPAA.
Crossbow Labs – Crossbow Labs provides enterprise-consulting services for PCI DSS security compliance.
Cybercom Group – Cybercom Group is a Swedish consulting firm that includes compliance services.
Dara Security – Dara is a security firm of advisors and ethical hackers with experience in PCI DSS and other standards.
Deloitte – Deloitte serves as an approved Qualified Security Assessor (QSA) for its global enterprise clients.
Dimension Data – Dimension Data is a New Zealand group supporting PCI based on its Security Assessment acquisition.
DirectDefense – DirectDefense offers a range of security consulting services including compliance and PCI DSS.
ECSC – UK firm ECSC offers managed solutions for customers including PCI services and consultancy.
Enterprise Risk Management – Security consulting firm Enterprise Risk Management includes compliance management services.
Espion – Based in Dublin, Espion provides a range of security consulting and PCI DSS professional services.
Galix Networking – South African information security firm Galix Networking includes PCI compliance in its specialties.
Geobridge – Geobridge focuses on security, compliance, and payment services, which is fundamental to the PCI DSS process.
Grant Thornton – Accounting firm Grant Thornton includes a range of enterprise PCI DSS QSA consulting services.
GRC 360 – GRC 360 is a consultancy with PCI DSS capability operating in the Middle East region and UK.
Ground Labs – Ground Labs provides security and auditing software in support of PCI DSS compliance.
GRSee Consulting – GRSee Consulting is an Israeli consulting firm that includes PCI DSS assessments.
Halock Security Labs – Halock Security Labs includes compliance services along with penetration testing and risk assessment.
The Herjavec Group – The Herjavec group offers QSA services and PCI-compliant managed services.
IBM – IBM's global enterprise consultants are available to support PCI DSS assessments for customers.
Intersec Worldwide – Newport Beach firm Intersec Worldwide specializes in PCI compliance professional services.
IRM – IRM is a UK-based firm that provides a range of security consulting services including PCI DSS.
KPMG – KPMG includes PCI compliance and QSA consulting services in their professional service offerings.
Lazarus Alliance – Arizona firm Lazarus Alliance provides security, risk management, audit, and compliance.

Megaplan-IT – Megaplan-IT offers a PCI consultancy, including an on-site pre-PCI gap assessment service.
Nettitude – Nettitude offers penetration testing, risk management, and PCI consultancy services.
NetWorks Group – NetWorks group includes compliance services for PCI, HIPAA, and other frameworks.
nGuard – nGuard is a security consulting and testing vendor that also serves as a PCI QSA vendor.
Novacoast – Novacoast includes compliance services for PCI, FISMA, HIPAA, and other frameworks.
NTT Communications – NTT Com Security includes PCI DSS in its range of consulting and managed security services.
NTT Security – Operating in Ireland and Italy, NTT Security offers the ZeroRisk PCI portal for PCI compliance.
Optiv – Security solutions provider Optiv includes PCI support as part of its professional services.
Orange Consulting – Orange Consulting includes focus on governance, risk, and compliance assessments.
Paladion – Information risk management firm Paladion offers professional services including compliance.
Panacea Infosec – Indian firm Panacea Infosec provides information security services including PCI DSS certification.
Parameter Security – Parameter security includes compliance audits in its range of professional services.
Pentest Partners Compliance – Pentest Partners Compliance offers QSA and PCI forensics services.
Pondurance – Pondurance is an information security firm that includes security compliance services.
Praetorian – Praetorian offers customers a range of risk consulting and compliance advisory services.
Protiviti – Protiviti provides customers with PCI planning, readiness, and compliance capabilities.
PwC – PwC includes PCI professional services in its suite of global technology and consultation offerings.
RavenEye – RavenEye provides security consulting including ethical hacking, PCI DSS QSA services, and penetration testing.
Redhawk Network Security – Redhawk Network Security specializes in information security with PCI QSA services.
RedIsland – UK-based consulting firm RedIsland offers information security and governance with PCI.
SecureState – SecureState includes compliance in its suite of information security professional services.
SecurityMetrics – SecurityMetrics provides PCI DSS, HIPAA, and data security compliance assessments.
Security Risk Advisors – Security Risk Advisors includes compliance in its suite of information security consulting.
Sera-Brynn – Sera-Brynn serves as a PCI QSA and includes compliance in its suite of information security services.
SISA – SISA is a payments security specialist firm located in India with professional service capability in PCI DSS.
Solutionary – Part of NTT Group, Solutionary includes cyber security compliance consulting services.
Stickman Consulting – Stickman Consulting includes compliance, penetration testing, and information security services.
Sunera – Sunera addresses HIPAA and other compliance suites in its suite of information security consulting.
Sword & Shield – Sword & Shield includes PCI assessments in its suite of security professional services.
Sylint – Sylint offers customers a range of customized services for PCI, HIPAA, NIST, and ISO compliance and audit.
Sysnet – Sysnet provides a wide range of PCI, cyber security, and compliance solutions for business.
TBG Security – TBG Security provides security consulting for compliance in HIPAA, PCI, and related frameworks.
Tevora – Tevora provides security consulting, risk management, and compliance solutions for enterprise customers.
True Digital Security – True Digital provides network security, app security, and compliance/audit services for customers.
TrustedSec – Information security consulting firm TrustedSec, located in Ohio, offers PCI QSA services.
Trustwave – Part of Singtel, Trustwave offers PCI DSS professional services.
Truvantis – Truvantis offers a range of authorized PCI QSA services as part of its professional services suite.
2-sec – 2-sec provides a range of security consulting offers including penetration testing and PCI DSS services.
Veris Group – Veris Group serves as a PCI QSA for customers as part of its GRC assessment and advisory services.
Verizon – Verizon includes compliance in its suite of managed and information security consulting services.
Westnet Consulting Services – Westnet Consulting Services offers IT network security, compliance, and PCI QSA services.

Control 42: Vulnerability Management

Vulnerability management involves the processes, tools, and platforms involved in maintaining an accurate inventory and awareness of current and potential security weaknesses in an enterprise. Such weaknesses can include unpatched systems, known (but unfixed) vulnerabilities, and unknown (but suspected) exploitable holes. An irony is that although vulnerability management has been a component of every enterprise security team program for decades, it remains one of the more poorly understood and weakly attended to aspects of modern cyber security. One reason for this is the strong dependency of vulnerability management on accurate IT system inventories, which most security professionals have come to recognize as typically lacking. Good news in vulnerability management involves recent

advances in automated platforms that ingest live data, pull feeds from IT systems, and combine collected information into live, situationally-aware views of the enterprise. Such automation is clearly the future of vulnerability management, and cloud-based threat intelligence plays a strong, complementary role. Regardless of the size of a given enterprise, this function is essential to stopping cyber attacks, and vendors working in vulnerability management should expect considerable growth in sectors such as SMB that have traditionally not paid enough attention in this area.

General Outlook

The general outlook for vulnerability management solutions involves transition from isolated early focus on software patching to more comprehensive focus on a full range of exploitable vulnerabilities. This transition also has involved the shift from simple manual tools to intelligent automated platforms. First generation vulnerability management from 1998 to 2007 involved early patch management tools powered by weak intelligence coming mostly from the local enterprise. Second generation vulnerability management from 2007 to 2016 improved its focus to a more comprehensive view, using cloud-based intelligence to improve the process. Hybrid cloud and third-party risk emerged as clear components of vulnerability management programs, but the work remained mostly non-real-time during this period. Third generation vulnerability management from 2016 to 2025 should expect to see an even broader focus area of applicable exploits and weaknesses to manage, powered by live threat feeds from all-source intelligence services. Automation will introduce learning algorithms to improve support for risk mitigation from these platforms.

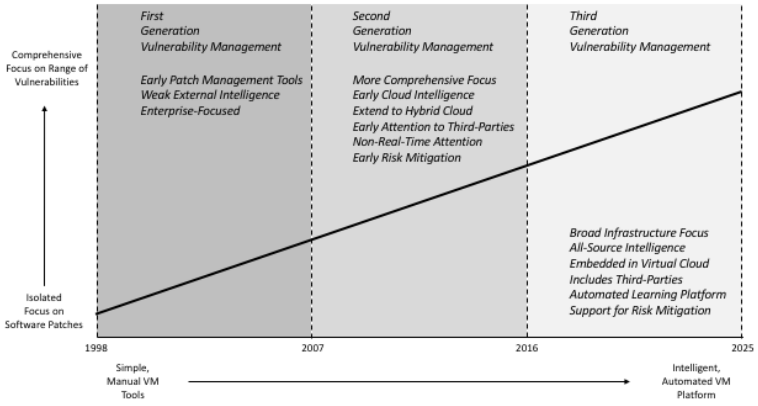

Figure 42. 2018 Vulnerability Management Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since this is a well-understand capability – albeit under-attended in too many environments. The clear shift to automation is excellent news since the biggest challenge to managing vulnerabilities has always been trying to keep track of everything relevant. (Computers and software have always been better than people at doing those sorts of tasks.)

Advice for Enterprise Security Teams

Enterprise teams should be working hard on integrating an automated vulnerability management platform into their emerging hybrid cloud environment. Increasingly, relevant vulnerabilities will emerge in systems managed by third parties and service providers, so federation support and API-connectivity of vulnerability management platforms will be something to include in RFPs. Don't expect software quality to improve soon enough to reach bug-free code in your lifetime. Dev/Ops and related processes are designed to compensate for rushed software lifecycles, rather than fix them – so you should expect a healthy barrage of continued software-based bugs that need to be patched, mitigated, and eventually removed. Vulnerability management teams will remain busy in the coming years, so make sure to account for this in headcount and budget planning.

Advice for Security Technology Vendors

Expect lots of growth in market need for automated vulnerability management support in enterprise, but also expect to see adjacent security tools such as SIEMs increasingly covering this function. So, the competition for vulnerability management functional support will increase. Also, the large cloud and service providers will almost certainly embed more extensive vulnerability management tools into their offerings, so this could have the effect of disintermediating security vendors from any hybrid cloud architecture. Vendors should be discussing partnership opportunities with the larger providers in advance of this inevitable shift. As discussed above, automation is the most essential component of vulnerability management, and with this comes the obligation of API support, code quality, and flexible licensing.

List of Support Vendors

Acunetix – Acunetix provides a vulnerability management solution for Websites and Web applications.
Allgress – Allgress provides solutions focused on governance, risk, and compliance (GRC) and vulnerability management.
Audit Square – Audit Square provides a Microsoft Windows security, configuration, and audit tools for desktops and servers.
Aujas Networks – Aujas Networks provides solutions in vulnerability management, data protection, and IAM.
Beyond Security – Beyond Security offers the AVDS automated security test suite for detecting weaknesses.
Buguroo Offensive Security – Buguroo offers a range of platforms and solutions including vulnerability management.
Contrast Security – Contrast Security provides continuous application to detect vulnerabilities and ensure compliance.
Core Security – Core Security provides a solution for consolidating and prioritizing vulnerability data.
Defence Intelligence – Defence Intelligence (Defintel) provides advanced malware solutions for customers.
Detectify – Detectify performs Web vulnerability scans through cloud-based tools that audit site security.
Digital Defense – The company supports vulnerability management via a world-class automated platform.
ElevenPaths – ElevenPaths provides a range of security solutions including authentication and vulnerability detection.
enSilo – enSilo provides data exfiltration detection solutions for enterprise customers experiencing a breach.
eSentire – eSentire provides security threat protection solutions including scanning, log centralization, and traffic capture.
Firebind – Firebind provides a passive, continuous network security and performance-monitoring tool.
FireMon – FireMon provides ntelligence capabilities for enterprise, government, and service providers.
GamaSec – GamaSec provides malware detection and Web vulnerability solutions via the GamaScan platform.
Grendel-Scan – Grendel-Scan offers an open-source downloadable tool for supporting automated testing.
GroundLabs – GroundLabs provides software tools for sensitive data discovery to support compliance and avoid breaches.
HPE – HPE offers dynamic analysis security for vulnerability discovery and management in Web applications.
IBM – IBM offers the AppScan tool, which tests Web and mobile applications for vulnerabilities.
Indusface – Indusface supports security testing of Web, applications, mobile, and enterprise software.
Infocyte – Infocyte provides a solution that scans networks for evidence of exploitable vulnerabilities.
Intel – Intel continues to support existing customer base with legacy scanning solutions as they approach end-of-life.
ISARR – ISARR provides a Web-based platform for managing risk, resilience, response, and security intelligence.
iScan Online – iScan Online scans and detects vulnerabilities on enterprise endpoint and mobile devices.
ITrust – Luxembourg-based information security company ITrust offers an online multi-anti-virus scanner platform.
Kenna – Formerly known as Risk I/O, the company provides a risk intelligence and vulnerability management platform.

Lumension – Lumension supports patching, vulnerability management, and application whitelisting.
Lumeta – Lumeta supports a combination of vulnerability discovery methods with visualization.
Lunarline – Lunarline offers cyber security and vulnerability management including SOC operation, pen testing, and privacy.
Mavituna Security – Mavituna Security offers the Netsparker tool for automatically detecting vulnerabilities and security flaws.
The Media Trust Company – The company provides media security scanning for Websites, advertisements, and mobile.
MileScan – MileScan provides an intelligent scanner that simulates hacker attacks and identifies security risks.
MyAppSecurity – MyAppSecurity provides risk management solutions for designers and developers via threat modeling tools.
NETpeas – NETpeas provides SaaS support with a payment front-end to security solutions including vulnerability management.
Nikto – Nikto consists of an open source Web scanner for detecting security vulnerabilities in servers.
NopSec – Nopsec provides unified vulnerability risk management solution collects and manages scanning output.
NRI Secure – NRI Secure offers customers the automated GR360 Website security scanning solution.
N-Stalker – N-Stalker provides a Web-application security scanner that includes a free downloadable edition.
Onapsis – Onapsis provides a behavioral-based approach to detecting anomalies with emphasis on SAP.
OPSWAT – OPSWAT provides IT security products that protect devices, and track data flows via malware scanning.
Orvant – Orvant uses multiple proprietary and open source scanning tools to detect vulnerabilities.
Outpost24 – Outlier Security provides agentless cyber security analytics as a service for endpoints.
Pwnie Express – Pwnie Express provides a range of penetration testing, security testing, asset discovery, and vulnerability.
Qualys – Qualys provides a vulnerability management platform with the original virtualized, cloud-based solution.
Rapid7 – Rapid7 offers AppSpider and integrates hacking talent on the team with its products and services.
RiskIQ – RiskIQ scans the Web to ensure security outside the firewall-protected enterprise, including on-line advertisements.
RiskSense – RiskSense provides a vulnerability management platform along with a range of security services.
SAINT – SAINT offers a range of vulnerability management, penetration testing, and compliance solutions.
SAVANTURE – SAVANTURE provides MSS and consulting including SIEM, log management, and vulnerability management.
SecludIT – SecludIT provides continuous vulnerability detection and management solutions for enterprise.
SecPoint – SecPoint provides IT security products including a vulnerability scanner, UTM firewall, and Web scanner.
Secunia – Now part of Flexera, the company provides a vulnerability management platform for enterprise.
Security Scorecard – Security Scorecard provides a threat management for collecting security-related information.
Shavlik – Shavlik provides patch management solutions for operating systems, virtual systems, and applications.
6Scan – 6Scan provides automated vulnerability detection and mitigation of malware on Websites.
Skybox – Skybox collects data from all network devices and systems and creates a model for analysis and response.
SolarWinds – In addition to performance, application, and database monitoring, SolarWinds offers IT security and compliance.
Solutionary (NTT) – Solutionary, an NTT Company, provides MSS and consulting using its cloud-based ActiveGuard platform.
Sucuri – Sucuri provides protection solutions for Websites, malware removal, and network asset security.
Symantec – Symantec offers customers the Control Compliance Suite vulnerability management solution.
TaaSera – TaaSera build runtime behavior detection solutions to proactively identify vulnerabilities.
Tenable – Tenable provides the Nessus vulnerability scanner for advanced detection of weaknesses.
Tinfoil Security – Tinfoil Security offers a developer-friendly service for scanning a website to detect vulnerabilities.
Tripwire – One of the original security companies in the scanning business, Tripwire offers WebApp360 for the enterprise.
TrustWave – TrustWave offers a behavior-based scanning technology acquired via Cenzic in 2014.

Control 43: Industry Analysis

Industry analysis involves research from third party expert analysts that provides technical and marketing support for the selection of vendor tools and security architectural decisions. Surprisingly, this important aspect of every CISO team's day-to-day work is never included in any security framework – probably because most frameworks are not developed by present or former CISOs! By way of analogy, imagine a framework for financial services that did not include the important task of reading and internalizing research on the economy, business conditions, and geopolitical factors. Leaving this type of industry analytic support from a cyber security framework is just as consequential. The bad news here is that most industry analysis on cyber security is terrible. Quadrants and waves from the larger analyst companies are pure pay-for-play activities, and leave out smaller companies (or ones that will not pay). Magazine and

Internet articles are bumpy and uneven in quality, and sometimes have so many advertising pop-ups that it's impossible to think straight while reading. With the TAG Cyber Security Annual, which you are reading now, the goal was to democratize great industrial research so that everyone has access to the best guidance. Larger companies can hire consultants, but that involves only a very few organizations. The trend here, one hopes, is that excellent, open-source, readily available research on the cyber security industry will be available to every organization in the world. This report, hopefully, will spur that trend.

General Outlook

The general outlook for industry analysis solutions in cyber security involves transition from weak recognition of quadrants and waves in the late 90's, through a period that involved significant growth in these review structures, but now to a coming period where such dependency will wane considerably. The transition also involved a shift from inexperienced general analysts to more experienced analysts with domain expertise. First generation industry analysis for cyber security from 1998 to 2007 involved early magazine articles, pay-for-play quadrants and waves, resulting in lower quality analysis and guidance than was needed. Most people during this time learned instead from books, talks, and courses. Second generation industry analysis in 2007 to 2016 involved a dramatic growth in the availability of bumpy information on the web, and massive growth in influence of pay-for-play quadrants and waves. Much available information during this period was just terrible and inaccurate. In fact, the perimeter model was spurred along by analysts during this period that did not understand the power of distributed systems, virtualization, and SDN. Third generation industry analysis from 2016 to 2025 should expect to see more professional analysis from domain experts with less focus on quadrants and waves. More honest, democratized cyber security analysis will be made available from experts for all to use.

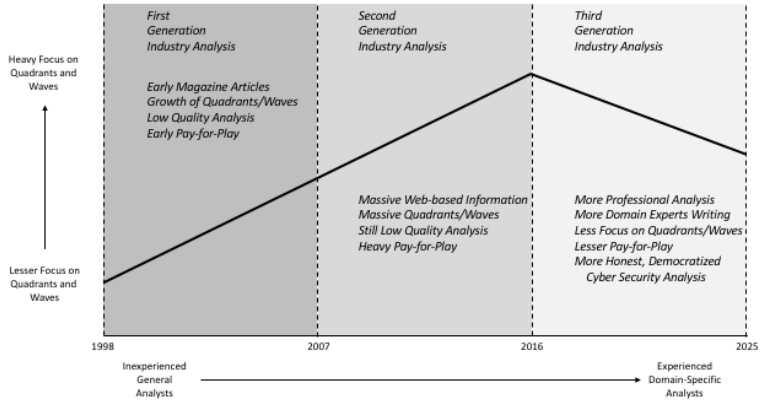

Figure 43. 2018 Industry Analysis Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, especially since our own involvement at TAG Cyber will hopefully spur this trend along. Strong opposition from a couple of large analyst companies will push back heavily on the idea of freely available research, but

the wave (ahem) will be too strong to stop. In the coming years, democratized analysis will be the norm.

Advice for Enterprise Security Teams
The advice here is to be careful what you read and absorb. Stick with sources you know and materials that are developed from a point of view that is consistent with your own view of the industry. For example, vendor material is often helpful in establishing the specifics of their design – and they are in the best position to provide that data. If you are buying a SIEM, for example, then demand good design descriptions of that product. But the idea that your SIEM provider should offer guidance on the day-to-day needs of the CISO seems silly; that is not what they do, and you'll get a jaded view. Academia is increasingly providing excellent materials for learning, and this should be used to develop an understanding of the underlying fundamentals like cryptography and virtualization. Government think-tanks have also been good, and the Department of Homeland Security has developed some excellent materials. This is good news. Enterprise security teams should be especially careful in what they absorb – and this is particularly important for SMB companies. We must all agree to *not* pay attention any more to quadrants and waves. They damage our industry.

Advice for Security Technology Vendors
If you are in the business of providing industry analysis for cyber security and you are reading this report now, then my suspicion is that you do not like my work much at all. The advice here is to adjust your model: Vendors should not pay a small fortune to be listed in the top right of some quadrant. That business model will wane. The competition will be open source, freely available material from domain experts. Adjust.

List of Support Vendors
CSIS – CSIS is a think tank and policy research institution with respected and experienced experts.
Cybersecurity Ventures – Cybersecurity Ventures provides a market report, including the Cybersecurity 500 list.
451 Alliance – 451 Alliance offers research reporting on the technology, telecommunications, and security industries.
Forrester – Forrester provides the Forrester Wave, including aspects of cyber security.
Gartner – Gartner provides the Magic Quadrant, including aspects of cyber security.
HfS Research – HfS Research offers reports and research that focus on the as-a-service market in technology and business.
HMG Strategy – HMG Strategy sponsors seminars, industry reports, and learning events for security teams.
IDC – IDC includes expert analysts who provide research, commentary, and analysis on technology, including cyber security.
Light Reading – The team of analysts, writers, and experts at Light Reading provide reporting to the cyber security community.
Markets and Markets – Markets and Markets sells its Cyber Security Market Global Forecast as a download on the Internet.
Radicati – The Radicati Group is a technology market research firm that publishes a market quadrant report on cyber security.
Securosis – Securosis is an independent research and advisory firm offering insights into Web 2.0, APT, and security investment.
TAG Cyber LLC – TAG Cyber provides the 2017 TAG Cyber Security Annual as a free, open source reference guide to CISO teams.
TechSci Research – TechSci Research is an independent research firm that offers a wide assortment of market research.

Control 44: Information Assurance

Information assurance is a designation used to describe a special type of security service that was developed primarily to deal with Federal government cyber risk challenges. The term was invented as the logical (and more positive) counter to *information warfare*, which became a

popular reference to offensive action against nations in the early 2000's. Today, information assurance is also used to reference government-related origin of services that are made available to generally larger commercial buyers. Large system integrators with defense solution businesses are the most likely to have an information assurance offering. Usually, such offerings involve threat intelligence, integrated protection architecture, security operations and fusion centers, and real-time situational awareness – all common in an effective national cyber defense. The commercialization of information assurance is a welcome trend since civil defense of critical infrastructure is performed by commercial groups, and they can all benefit from the discipline and real-time posture orientation of government defenders.

General Outlook

The general outlook for information assurance solutions involves transition from pure government focus to a combined focus of both government and commercial concerns and risk. The transition also involves shift from simple, reactive cyber defense programs and tools to comprehensive and integrated cyber security solutions that are more proactive. First generation information assurance from 1998 to 2007 involved early intrusion detection tool orientation by large integrators as the primary government response to information warfare. Second generation information assurance from 2007 to 2016 involved early security operations centers being developed with some commercial influence and expended use beyond simple IDS, if only to address the much more serious risk of advance persistent threats. It is worth mentioning that the APT actors were much more successful than the APT defenders during the era, so the combined solutions had the right idea, but largely did not work. Third generation information assurance solutions from 2016 to 2025 should expect to see full government and commercial integration, with an expanded range of proactive offerings. Market collision with managed security service providers will be obvious, as buyers might have trouble differentiating the two solution types. In general, though, a more intense approach to real-time cyber security from groups with their heritage in Federal government defense will be a good influence on the overall cyber security community and should thus be welcomed.

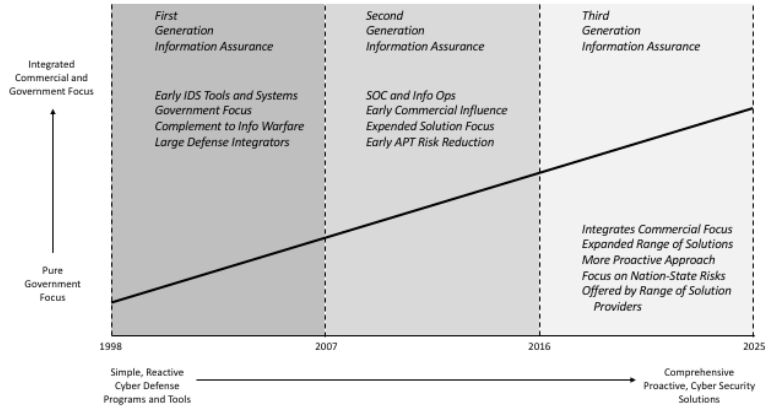

Figure 44. 2018 Information Assurance Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since recognition that cyber security of critical infrastructure is basically national civil defense. Several large integrators in many countries (US and Israel are the leaders) have already spun off units that focus on information assurance solutions for commercial buyers. As alluded to above, this is a welcome trend.

Advice for Enterprise Security Teams

If you are a larger enterprise security team, then you've probably already been approached by a defense integrator offering their information assurance services. If you have not already engaged, it might be worth revisiting these services, because the rigor and intensity that come from their legacy are worth integrating into your own solution approach. Cyber security is civil defense, so we all might as well begin learning from those who've been protecting national assets for the longest time. If you are a smaller enterprise security team, then keep an eye on this market for information assurance solutions targeting SMB-type budgets. This is not a big trend to date, simply because information assurance teams sell large projects to government, so they naturally gravitate toward commercial buyers who can swallow a large effort.

Advice for Security Technology Vendors

Information assurance vendors are almost always patriots who have experience defending their nation from cyber risk. When you engage with them, their initial marketing instinct is to tell you about their loyal service as warriors. This is to be expected, but you'll need to scratch deeper to see if they are the real deal. They will need to include a reasonable, well-designed collection of enhancements to their service to deal with the day-to-day needs of a commercial organization. Industry runs differently than government, so information assurance vendors are wise to recognize this fact and adjust. Partnering with an experienced commercial team might be the best approach. Moving down-market to SMB might be shocking when you see the tiny size of monthly invoices, so be careful before you commit to such action.

List of Support Vendors

Accenture – Accenture provides global professional services, consulting, and outsourced services, including cyber security.
Airbus Defence/Space – Airbus is a large aerospace company that includes a wide range of information assurance solutions.
AirPatrol – AirPatrol, part of Sysorex, provides platforms for enterprise delivery of software and wireless protection.
Applied Physics Lab – The non-profit group, affiliated with Johns Hopkins, provides IA services to the Federal Government.
ApplyLogic – McLean-based ApplyLogic specializes in cyber security and information assurance solutions.
Assevero – Assevero is a unique virtual company offering information assurance services to the government.
AssurIT – AssurIT is an information technology (IT) services and solutions provider that specializes in cyber security.
AT&T – AT&T includes a Government Solutions unit that provides information assurance and cyber security.
Axxum Technologies – Axxum Technologies is a minority and woman owned firm providing IT security and IA solutions.
BAE – BAE is a large British aerospace company that includes a range of information assurance solutions.
Boeing – Large American aerospace company Boeing includes a range of information assurance solutions.
Booz Allen Hamilton – Traditional professional services company BAH offers information assurance capabilities to its clients.
CACI – CCI is a defense contractor that provides a variety of technology and information assurance solutions.
Carahsoft – Carahsoft provides value added solutions including security and information assurance for the Federal Government.
CGI – CGI provides global IT consulting, systems integration, and outsourcing, including a practice in cyber security.
CSC – CSC is a traditional technology and professional services company that offers information assurance capabilities.
C3IA – UK-based small enterprise firm C3IA specializes in security solutions for defence applications.
Cyber Defense Agency – Sami Saydjari's consulting firm includes information assurance for government.
CyberDefenses – Consulting firm CyberDefenses includes a range of information assurance capabilities.
Cyber Net Force Technologies – CNF provides operations and engineering solutions for network defense and attack detection.

CyberPoint International – Consulting firm CyberPoint International includes a range of information assurance capabilities.
Cybersalus – Cybersalus is a consulting firm in Reston that includes a range of information assurance capabilities.
Chertoff Group – Michael Chertoff's consulting firm includes a range of information assurance capabilities.
CSRA – CSRA formed from (CSGov and SRA) provides a variety of technology and information assurance solutions.
Cyberbit – Spun off from Elbit, the Israeli company provides a range of information assurance solutions for commercial buyers.
Decisive Analytics – Decision Analytics is an employee-owned engineering firm offering information assurance capabilities.
Delta Risk – Delta Risk is a consulting firm that includes a range of information assurance capabilities.
EmeSec – Consulting firm EmeSec includes a range of information assurance capabilities for government customers.
EWA-Canada – Canadian consulting firm EWA-Canada includes a range of information assurance capabilities.
Fidelis Cybersecurity – Fidelis Cyber security provides information assurance for enterprise customers.
4Secure – Data diode firm 4Secure offers information assurance-related solution for UK-based customers.
General Dynamics – Defense contractor General Dynamics provides technology and information assurance solutions.
Good Harbor – Richard Clarke's consulting firm includes a range of information assurance capabilities.
Harris – Defense contractor Harris provides a variety of technology and information assurance solutions.
Hex Security – Hex Security provides information assurance consultation toward both strategic and compliance objectives.
IBM – IBM is a large technology and professional services company that offers information assurance capabilities.
InfoDefense – InfoDefense provides security consultation focused on compliance, information assurance, and response.
Information Assurance Solutions – Information Assurance Solutions is a consultancy providing information assurance solutions.
KEYW – HexisCyber, formed by KEYW through acquisition of Sensage, provides information assurance solutions.
Kroll – Kroll provides investigations, risk, and cyber security consulting services for business clients.
Leidos – Leidos offers solutions in national security, health, and engineering including cyber security.
Lockheed Martin – Lockheed Martin provides a portfolio of information assurance solutions including support for ECS.
Lunarline – Arlington-based firm Lunarline offers products and services with information assurance capabilities.
Magal S3– Defense contractor MagalS3 provides a variety of technology and information assurance solutions.
Mandalorian Security – Mandalorian Security provides information assurance services in EMEA and Asia Pacific.
ManTech – Mantech includes a range of information assurance capabilities, including active gateway traffic analysis.
Merlin International – Merlin International is a provider of IT and cyber security solutions for Federal Government.
MITRE – MITRE is a Federally-funded Research and Development Center with strong information assurance capabilities.
NCC Group – NCC Group offers security testing and information assurance including escrow, consulting, and domain services.
Netwar Defense – Netwar Defense is an SBA provider in Maryland of IT and cyber security solutions for Federal Government.
Network Security Systems Plus – Network Security Systems Plus provides information assurance focused on Government.
Newberry Group – Newberry Group is a provider of IT and cyber security solutions for Federal Government.
NEXOR – NEXOR provides security solutions for information exchange and information assurance.
NJVC – Virginia-based NJVC is a provider of IT and cyber security solutions for Federal Government.
Northrop Grumman – Defense contractor Northrup Grumman provides technology and information assurance solutions.
Northstar Group – Northstar Group is a provider of IT and cyber security solutions for Federal Government.
Patriot – Patriot provides information assurance solutions including infrastructure protection and mobile security solutions.
PivotPoint Security – PivotPoint Security provides information assurance including penetration testing and ethical hacking.
QinetiQ – British defense contractor QinetiQ provides a variety of technology and information assurance solutions.
Raytheon – Defense contractor Raytheon provides a variety of technology and information assurance solutions.
Referentia – Referentia provides information assurance and managed solutions with emphasis on government customers.
Renaissance Systems – RSI supports information assurance, cloud integration, network design, and other services.
SAIC – Defense contractor SAIC provides a variety of technology and information assurance solutions.
SecureNation – SecureNation provides IT security and information assurance through partnerships with technology vendors.
SecureWorx – SecureWorx provides secure data centre solutions for Australian government customers.
Sotera Defense Solutions – Defense contractor Sotera provides a variety of technology and information assurance solutions.
SphereCom – SphereCom provides a variety of technology and information assurance solutions.
Strategic Cyber Solutions – Strategic Cyber Solutions provides US Government with cyber intelligence and cloud data analytics.
Swain Techs – Swain Techs provides engineering, managed services, and information assurance consulting services.
Tangible Security – Tangible Security provides security consulting including assessments and virtual CISO for government.
TASC – Defense contractor TASC provides a variety of technology and information assurance solutions.
TDI – Security consulting firm TDI provides a variety of technology and information assurance solutions.
TechGuard Security – IT services firm TechGuard provides a variety of technology and information assurance solutions.
TecSec – TecSec provides information assurance for access control enforced through encryption and key management.
Telos – Cyber security solutions and secure mobility firm Telos offers information assurance solutions.
Templar Shield – Templar Shield provides a range of security consulting, managed security, and recruiting services.
Tenacity Solutions – Reston-based IT services firm Tenacity Solutions offers information assurance solutions.
Thales – The Thales Group is a French multinational defense and space contractor that offers cyber security solutions.

Unisys – Unisys is a technology company that includes cyber security solutions for enterprise customers and government.
Van Dyke Technology Group – Van Dyke Technology Group is a consulting firm that offers information assurance solutions.
VariQ – VariQ is a Washington-based IT and cyber security consulting firm that offers information assurance solutions.
Vencore Labs – Formerly known as ACS, this division of Vencore focuses on R&D projects including information assurance.
Veris Group – Veris Group provides information assurance consulting with emphasis on Federal Government customers.
Verizon – Verizon includes information assurance solutions for Federal Government customers in its portfolio.
Vistronix – Vistronix specializes in Big Data analysis solutions including a specialized focus on cyberspace and SIGINT operations.
Widepoint – Widepoint provides cyber security services for enterprise and government with emphasis on identity management.
ZRA – Lee Zeichner's consulting firm includes information assurance services for Federal Government and commercial clients.

Control 45: Managed Security Services

Managed security services (MSS) involve the staff, tools, resources, capabilities, and supporting infrastructure required for a solution vendor to accept outsourced responsibilities for designated, day-to-day cyber protection functionality for a customer. MSS began with remote management of firewalls, and has since burgeoned into a multibillion-dollar industry with a wide range of solutions offered to customers. The canonical set-up involves a business making the decision that the administration, care, operation, and response functions for a subset of its security infrastructure would be better served by an external MSS entity. Deciding which subset to outsource to an MSS is largely ad hoc decision, driven as much by what is being offered by managed providers as by any logical analysis of insourcing versus outsourcing. The good news is that cloud-based architectures and distributed, virtualized systems will change all of this, simply because *computing* and *networking* are moving toward an outsource model. Such transition is accelerated by the Internet service providers who are developing and now offering software defined network (SDN) services, which lend well to service chaining of virtual security appliance functionality. The result is that MSS will shift from traditional hardware management to a virtualized operation embedded in hybrid cloud architectures and powered by SDN services. This will advantage the larger cloud, Internet, and mobile service providers since they will possess the underlying infrastructure, and layering security capabilities as add-ons should be straightforward. Expect to be pointing and clicking soon on an ISP or cloud service provider's portal as the new provisioning mechanism for obtaining a managed security solution.

General Outlook

The general outlook for managed security services involves transition from hardware deployed manually to a customer DMZ for remote management to virtualized infrastructure with self-supported automation. The transition will also involve a shift from early, reactive up-down management of devices to modern, situationally aware and virtually controlled software deployment. First generation MSS from 1998 to 2007 involved early IDS and firewall management services, performed remotely from a physical center to the customer perimeter with human MSS analysts trying to make sense of the security alarm and logs (and mostly failing). Second generation MSS from 2007 to 2016 involved continued attempts to improve first generation services, but never fully realizing the goal of remote perimeter protection for one main reason: Perimeters don't work. MSS teams tried hard during this period to automate their services toward more real-time focus, and they deserve credit for improving their ability to stop attacks more proactively. During the latter portion of this period, early hybrid cloud

architectures with reduce emphasis on hardware began to influence MSS design. The gradual dissolution of the perimeter became evident during this period as well. Third generation MSS from 2016 to 2025 will experience two dramatically different shifts. First, the traditional hardware-based management of perimeter devices will finally sunset. MSS teams who stubbornly hold onto revenue from managed firewall deals signed a decade earlier will come to regret this decision. Second, virtualized MSS solutions built on SDN infrastructure will see massive, exponential growth. With this virtualization will come the real-time, automated control of virtual workloads in the cloud that MSS teams were trying so hard to achieve with hardware-based manual configurations. Expect to see integration of these virtual MSS solutions with cloud-based security such as micro-segmentation and CASBs.

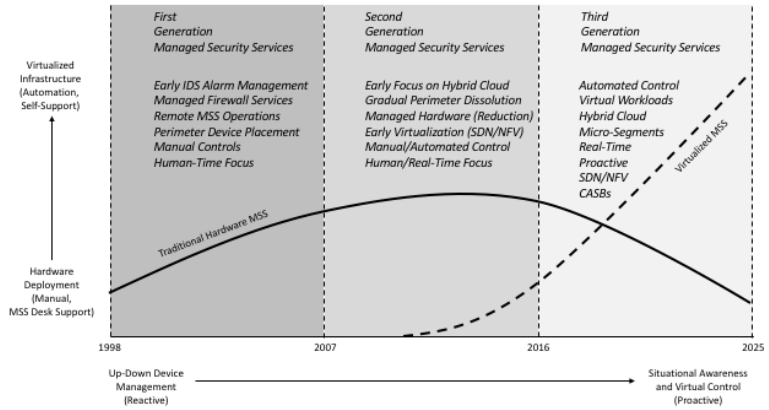

Figure 45. 2018 Managed Security Services Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, because the underlying investments in cloud and SDN from the large provides is well-underway. This provides an attractive base on which virtual security can be deployed for MSS solutions. It is possible that most security capabilities in future virtual enterprise networks will be deployed via portal and controlled by automated MSS tools from your cloud or service provider. This will have substantive implications on how future security capabilities are delivered to customers.

Advice for Enterprise Security Teams

This is a good time to take inventory with your IT and network partners of your transition progress toward a distributed, virtualized infrastructure. Assuming this is underway – and if you've moved some functions to cloud, then it is underway – then you should be developing a security architecture roadmap for such shift. MSS providers are potentially excellent partners to help you achieve this objective. Sit down with your ISP and cloud service providers and ask them to educate your team on how future virtualized MSS will work. You will find that some powerful capabilities are available *today*. Regarding existing perimeter MSS deals, my advice is to either plan to transition from your existing perimeter, or (if you are stubborn) at least negotiate a better deal than you have now. Expect prices for perimeter hardware management to increase as fewer companies choose this option, so you might as well lock in a good deal if you expect to remain on this Titanic deck for several more years.

Advice for Security Technology Vendors

If you provide MSS solutions today, then you have the unenviable problem of old revenue from a hardware base that will be soon replaced with new revenue from a software base. Whether the former is larger or smaller than the latter will be based on how cleverly you navigate this shift. The truth is that larger providers, especially ISPs, have a huge advantage with their existing infrastructure. It is tempting to say that light, virtual capabilities might allow smaller, more nimble operators to get into the MSS industry – and some of this is true. But the ability to provision security appliances into the northbound interface of ISP SDN controllers, for example, seems the simplest, easiest way to offer full MSS. Cloud providers also have a huge advantage with their ability to lightly deploy security appliances into local run-time environments that can be managed with automated tools. Creative entrepreneurs interested in MSS solutions would be advised to focus on great technology and advanced solutions, and to perhaps consider partnering with the ISPs and cloud providers. If there is any silver lining for the smaller vendors, it is that the ISPs and cloud providers will remain open and eager to embed, integrate, and acquire clever technology from more nimble start-ups. So, there is certainly room for new MSS offerings to find a way to thrive and grow.

List of Support Vendors

Above Security – Above Security delivers managed and IT security services including NIDS, HIDS, and log analysis.
Accenture – Accenture Operations offers managed cyber defense, managed identity, and managed compliance.
Alert Enterprise – Alert Enterprise provides infrastructure protection through GRC management and continuous monitoring.
Alert Logic – Alert Logic offers 24 by 7 monitoring and a research team as part of its managed cloud security services.
Allstream – Allstream offers a range of voice, IP, and unified communications, including managed security services.
Arcon – Brazilian firm, Arcon, is a managed security services provider serving enterprise customers in Latin America.
AT&T – AT&T provides managed security including network-based and SDN-resident protections for business and government.
Aura Information Security – Aura Information Security offers security consulting and managed security services in New Zealand.
BAE Systems – BAE Systems provides cloud-based enterprise managed security services including secure, hosted email.
Bell Canada – Bell Canada markets managed network protection services for Web, email, DDOS, and identity.
BinarySEC – French firm BinarySEC, provides a managed security solution to reduce the threat of attacks to Websites.
BT – BT Managed security includes DDOS, cloud, firewall, and event monitoring.
CenturyLink – CenturyLink Business provides managed firewall services and more comprehensive email and URL security.
China Telecom – China Telecom is a state-owned provider of phone, Internet, mobile, and managed security.
Clone – Clone Systems is an MSSP offering continuous monitoring, secure cloud, scanning, and security consulting.
ControlScan – ControlScan provides a range of managed security services and compliance support solutions.
CSC – CSC supports managed security services for data center, endpoint, network, and apps.
Cyber Engineering Services – Cyber Engineering Services provides managed data protection services for SMB
DarkMatter – DarkMatter offers professional and managed security services and solutions in Abu Dhabi.
Datapipe – Datapipe offers managed, hosting, and cloud services, including managed security, compliance, and resale services.
Deloitte – Deloitte focuses on audit, finance, tax, and consulting, including risk and compliance services, as well as MSS
Deutsche Telecom – Deutsche Telekom offers a range of managed and network-based security services.
DMX Technologies - In addition to media, ICT, and mobile SaaS, Hong Kong-based DMX offers MSS and consulting.
Earthlink – Earthlink provides Internet services including security services for residential and business customers in the US.
EWA-Canada – EWA-Canada provides information assurance in Canada including managed security services.
Foreground Security – Foreground Security, now part of Raytheon, provides virtual SOC, MSS, and threat intelligence.
GBprotect – GBprotect is an MSSP offering security operations and applications management as well as consulting.
The Herjavec Group – The Herjavec Group specializes in network security managed services and consulting.
IBM – IBM offers a range of MSS accessible to customers through a common Security Operations Portal.
Igloo Security – Igloo is a Korean company that provides managed security services including SIEM management.
Kernel – Kernel provides managed and network security as well as penetration testing and security audit.
Level 3 – Colorado-based telecommunications firm Level 3 offers a range of traditional managed security services.
Masergy – Plano-based Masergy provides a range of enterprise networking solutions including advanced managed security.

MegaPath – MegaPath provides voice, data, and broadband telecommunications including managed security services.
My Digital Shield – My Digital Shield provides network security services for small and medium-sized business market.
Netsurion – Netsurion provides managed security services, mobile access, and compliance solutions for enterprise customers.
NTT Communications – Japanese telecommunications firm NTT Communications provides a range of managed security services.
Orange Business Services – Headquartered in France, Orange Business Services includes a managed security service offering.
Paladion – Located in India, Paladion offers MSS and a range of risk management-based consulting services.
Proficio – Proficio offers advanced cloud-based managed security services with SIEM and SOC-as-a-service.
Quadrant Information Security – Quadrant provides security consulting, MSS, and enterprise security management.
Rook Security – Rook Security provides advisory services, managed security services, and solution integration.
SAVANTURE – SAVANTURE provides MSS and consulting including SIEM, vulnerability management, and authentication.
SecureWorks – SecureWorks, which has been in the MSS business since 1999, bases its services on its Counter Threat Platform.
Security on Demand – San Diego-based Security on Demand offers managed security solutions for enterprise and cloud.
Sentor – The company provides IT security including network protection, log management, and vulnerability monitoring.
Solutionary – Nebraska-based Solutionary operates as a separate subsidiary of NTT, offering managed security services.
Sword & Shield – Sword & Shield provides a range of managed and professional cyber security services.
Symantec – Symantec includes a range of managed security services in its extensive security portfolio.
TaTa Communications – TaTa is an outsourcing and technology firm that includes managed security services.
Tech Mahindra – Tech Mahindra is an outsourcing and services company that includes an information security services practice.
Telefonica – Telefonica is a Spanish telecommunications company that includes a managed security services offering.
TELUS – TELUS is a global telecommunications company in Canada that offers a range of managed security services.
TrustWave – TrustWave is a security compliance firm that includes managed security services including support for SMB.
2Keys – 2Keys provides a range of managed and professional services with user authentication and identity attributes.
Verizon – Large US-based telecommunications firm Verizon includes a traditional range of managed security services offers.
Vigilant – Vigilant provides cyber security services including managed network security, managed endpoint, and consulting.
Vijilan Security – Vijilan offers a range of managed security services including monitoring and incident response.
Wipro – Outsourcing and technology firm Wipro includes a wide range of managed security services.
XO Communications – XO Communications is a telecommunications firm that offers a range of managed security services.

Control 46: Security Consulting

Security consulting involves professional services delivered from experts to enterprise customers who require guidance, assistance, advice, or staffing of their cyber protection-related work activities. Security consulting services are delivered in as many ways as consultants and potential customers can invent, so there are no truly complete taxonomies to capture all forms of these tailored engagements. If, for example, you have some special skill in cyber security and someone is willing to pay for it, then you can serve as a security consultant. Similarly, even if you have weak cyber security skills, but you can compensate by being helpful, organized, and cheap, then you can also be a security consultant. It is a wide-open field, which is good news for budding consultants, but terrible news for the buying enterprise. One broad view of the security consulting industry might be depicted as follows:

- *High-Level Executive Advice* – This is delivered by the most distinguished experts to senior leadership and usually involves advice and guidance on the business implications of cyber risk. Risk presentations to boards or strategic security plans for CEOs are example deliverable in this category.
- *Mid-Level Strategic Delivery* – This involves project work by experts for enterprise security teams with specific needs in some aspect of their day-to-day cyber security work. Writing security policy requirements or reviewing GRC plans are example deliverables in this category.

- *Low-Level Tactical Support* – This involves temporary or day-to-day cyber security support from available staff to augment existing project teams and deliver some tactical result. Providing staff to perform a tedious inventory task or to augment a CISO team with entry-level workers are example deliverables in this category.

Security consulting will grow steadily in the coming years with more intense recognition of risk, so that is good news for the industry. The growth should be spread evenly amongst larger consulting teams who will benefit from Boards and C-suite attention, and smaller consulting teams who will benefit from SMB needs in this area. Domain expertise will also command a premium in the coming years.

General Outlook

The general outlook for security consulting solutions involves transition from mostly generalized, high-level consultants with broad skill sets to the availability of more domain-knowledgeable consultants who can help clients deal with security requirements in IoT, ICS, mobility, cloud, Dev/Ops, and other domain-specific areas. First generation security consulting from 1998 to 2007 involved simple, basic assessments such as scans and tests from a variety of available sources including (sadly) many non-experts offering weak advice that was consistent with no best practice standards. Second generation security consulting from 2007 to 2016 involved improved assessments of higher quality focused on discovering and making visible security issues. Advice during this period was much better as experts emerged in the field, but no common generally-accepted best standards for consulting services emerged other than those driven by frameworks such as PCI DSS or NIST. Third generation security consulting from 2016 to 2025 will see much improved services with domain expertise available in cloud, mobile, and virtual infrastructure. More experts will be available, and hopefully, more professional standards and generally accepted practices will emerge.

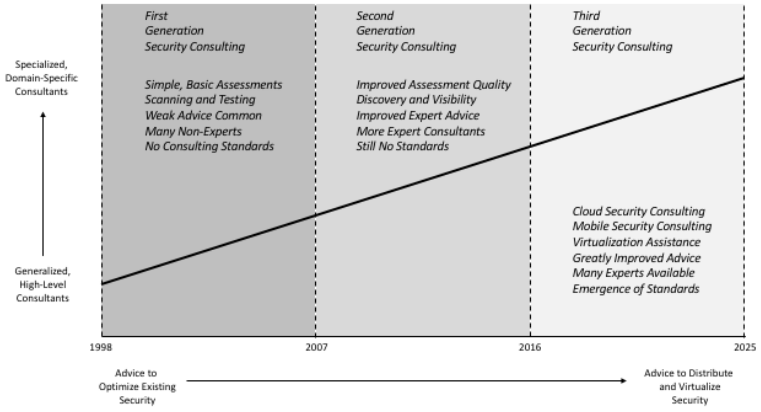

Figure 46. 2018 Security Consulting Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since the expectation here is just a continuation of what's been an on-going trend now for years: Namely, a gradual

increase in the quality and domain-specificity of consulting from a growing number of available experts.

Advice for Enterprise Security Teams

The advice here is to select your security consultants carefully, since relevant experience, domain expertise, and high integrity are the most important, yet difficult to determine, characteristics of a good consultant. Ask around before engaging any consultant. Hundreds of millions of dollars are wasted every year on consultants who have no idea what they are doing, and might be training their team on your nickel. It is also difficult to grade any company on their consulting prowess, because you could be assigned a weak rookie from a great firm or an experienced veteran from a tiny boutique start-up. Hire the consultant, if possible, rather than the firm – and you'll end up with the best results.

Advice for Security Technology Vendors

Increasingly, the non-technical attribute of having high integrity is more valuable in consulting than any other personal characteristic. What this means is that in hiring, training, or coaching your consultants, focus on developing strong character, honesty, and dependability more than anything else. You'll find that technical cyber skills will be in much greater supply in the coming years (contrary to all the published reports on the Internet about gaps in skills). You will have thus have less trouble than you have now in finding good consultants for your team. What this means is that *integrity* will be the main differentiator in establishing a successful consulting team. Establish a reputation as an honest firm that offers good services delivered on time at reasonable prices – and you will be a top cyber security consulting house. And yes, I know this is general advice, but security consulting is a new sector and the charlatans still lurk.

List of Support Vendors

ABR-PROM – ABR-PROM provides value added reseller (VAR) security solutions and IT outsourcing to customers in Poland.
Accellis Technology Group – The Cleveland-based firm offers managed IT, legal consulting, and cyber security/compliance.
Accenture – Accenture provides global professional services, consulting, and outsourced services, including cyber security.
ACROS Security – ACROS Security is a Slovenian provider of penetration testing and security, assessment, and research services.
Advent IM – Located in the UK, Advent IM offers a range of cyber and physical security consulting services.
Anchor Technologies – Business management consulting firm Anchor Technologies is located in Annapolis.
ANX – ANX provides managed compliance and collaboration services including PCI DSS compliance and secure connectivity.
Aon – Aon provides risk management and insurance, including cyber. Aon recently acquired Stroz Freidberg.
Ascentor – UK-based Ascentor offers its customers a range of information risk management consulting services.
Assure Technical – Assure Technical provides cyber and physical security consulting services including training.
Assuria – Assuria provides security solutions and managed SIEM supporting security operations and enterprise security needs.
AsTech Consulting – AsTech provides security consulting in discovery, remediation, software development, and training.
Atredis Partners – Atredis Partners provides software security research, embedded security, and penetration testing services.
Atsec – Austin-based atsec provides a range of laboratory and consulting services in information security.
AT&T – Large telecommunications firm AT&T includes a team of expert security consultants to complement MSS offering.
Attack Research – Attack Research provides a range of security consulting, assessment, and training services.
Aujas Networks – Aujas Networks provides risk and vulnerability management, data protection, and IAM services.
Aura Information Security – Aura Information Security, part of Kordia, offers security consulting and MSS.
Aurora Information Security & Risk – Aurora provides a range of security consulting solutions for enterprise customers.
AVeS – AVeS provides a range of IT consulting focused on digital information and information security.
Avnet – Avnet provides security consulting services with emphasis on helping companies secure their databases.
Axis Technology – Security consulting firm Axis technology focuses on governance, entitlement, and business risk.
Axxum Technologies – Axxum Technologies is an IT security services and solutions company focused on government customers.
Azorian – Azorian Cyber Security provides a range of cyber security services for enterprise customers.

Bambenek – Illinois-based Bambenek offers a range of cyber security investigations and consulting services.
Banff Cyber – Banff Cyber provides a solution for Web defacement along with complementary security consulting offers.
BDO Consulting – Accounting and tax firm BDO Consulting includes information security and compliance services.
BHC Laboratory – BHC Laboratory provides independent security consultation and advice for business customers.
BH Consulting – Ireland-based BH Consulting offers a range of information security consulting services.
Bishop Fox – Bishop Fox provides cyber security consulting, assessment, and testing services to enterprise customers.
Bitcrack – Bitcrack provides a range of security consulting services for business customers including penetration testing.
Bitshield Security – Bitshield security provides IT security consulting and training for customers in the Philippines.
BitSight – BitSight provides a security posture assessment and rating for organizations based on their visible behavior.
Blackfoot – Blackfoot provides a range of security consultants including risk, PCI, security awareness, and other areas.
Booz Allen Hamilton – Technology services and consulting firm BAH includes cyber security and information assurance.
BugSec – Located in Israel, BugSec offers a range of cyber and information security technical services.
Burns and McDonnell – Burns and McDonnell supports engineering services including integrated security.
Caliber Security Partners – Caliber Security Partners provides security technical and strategic staffing services.
Capstone Security – Capstone Security offers services in application security, regulatory compliance, and security assessments.
Carve Systems – Carve Systems provides security consulting and penetration testing services for IoT devices.
Certified Security Solutions – CSS provides security solutions in PKI, encryption, and identity, with emphasis on securing IoT.
CGI – CGI provides global IT consulting, systems integration, and outsourcing, including a practice in cyber security.
Chertoff Group – Michael Chertoff's consulting and advisory services firm offers high end services including advice on M&A.
Cigital – Cigital provides consulting in application and software security design, development, and maintenance.
Cirosec – cirosec provides security consulting and information security support for enterprise customers in Germany.
The CISO Group – The CISO group offers information security consulting with an emphasis on PCI DSS compliance issues.
CMT – CMT, now DataEndure, provides security, compliance, and archiving for protecting business sensitive information.
Coblue – Coblue offers a security benchmark platform that allows organizations to assess security posture.
Comda – Comda provides IT security services including biometrics, access control, consulting, and VAR integration.
CompliancePoint – CompliancePoint provides a range of compliance assessments, consulting, and managed IT.
Comsec Consulting – Comsec Consulting provides a range of security professional services for business customers.
Content Security – Content Security provides security consulting and professional services for enterprise customers.
ContextIS – Context, part of Babcock, provides security consulting and professional services for business clients.
Contextual Security Solutions – Contextual Security Solutions provides IT security and compliance consulting.
CriticalStart – CriticalStart provides information security services as well as resale of select security products.
CryptoNet – CryptoNet includes security consulting solutions for Italian customers.
CSC – Technology services and outsourcing solutions firm CSC includes a range of cyber security offerings.
Cyber Alpha Security BV – Cyber Alpha Security provides a range of security consulting services including ethical hacking.
Cyber Defense Agency – Sami Saydjari's consulting firm Cyber Defense Agency offers a range of security professional services.
Cyber Defense Labs – Cyber Defense Labs offers vulnerability assessments, penetration testing, and cyber forensics.
CyberInt – CyberInt supports intelligence, monitoring, and consulting focused on information security and cyber warfare.
Cyberis – Cyberis provides information security, risk management, and assurance consulting services and solutions.
CyberPoint International – CyberPoint International provides security services and information assurance.
Cyber Security Agency – The Cyber Security Agency offers security consultants with ethical hacking experience.
Cyber Shield Consulting – Information technology firm Cyber Shield Consulting offers cyber security consulting.
DarkMatter – DarkMatter provides a range of professional and managed security services and solutions.
Datashield – Datashield provides security consulting and managed services with emphasis on RSA/EMC products.
Day Zero Security – Day Zero Security provides security services ranging from residential users to police services.
Déjà vu Security – Déjà vu Security provides information security research and consulting services for enterprise customers.
Deloitte – Deloitte includes cyber security offerings such as PCI DSS pre-audits.
Delta Risk – Delta Risk provides strategic advice, consulting, and risk management to government and business clients.
Delphiis – Delphiis provides an application and services suite for enterprise, including risk management as a service.
Depth Security – Depth Security provides penetration testing, Web application security, and network access control.
Deutsche Telecom – Deutsche Telekom offers a range of managed and network-based security services.
Digital Defense – Digital Defense Inc. (DDI) provides managed and SaaS risk assessment, as well as security consulting.
Digivera – Digivera provides information security, managed services, and technology consulting services.
DMX Technologies – In addition to digital media, ICT, and mobile, DMX offers security consulting services.
Emagined Security – Emagined Security provides professional consulting services for information security and compliance.
Enet 1 Group – Enet 1 Group provides security services in the areas of SCADA and critical infrastructure, and mobility.
Enterprise Risk Management – Enterprise Risk Management provides security consulting and training services.
Espion – Espion provides security consulting services including information governance, forensics and eDiscovery, training.
EWA-Canada – EWA-Canada provides information assurance in Canada including risk management and security services.

EY – EY includes a range of cyber security, audit, and cyber advisory services for clients. EY acquired Mycroft in 2015.
Fortalice – Fortego provides security consultation and training services for business and government.
4Secure – 4Secure provides security consulting and training services to corporate and public sector clients across Europe. T
FoxIT – Fox-IT combines human intelligence with technology to provide security solutions and training for customers.
FRSecure – Cyber security consulting firm FRSecure specializes in compliance, standards, and regulatory solutions.
FTI Consulting – FTI is a global business advisory company with a practice in forensic consulting and eDiscovery services.
Galois – Expert team Galois uses mathematics and computer science to solve problems in technology and cyber security.
General Dynamics – General Dynamics is a defense contractor with cyber security and information assurance capability.
Global Cyber Risk – Global Cyber Risk (GCR) provides advisory to business and government in privacy and security.
Good Harbor – Richard Clarke's consulting and advisory firm Good Harbor offers higher end services including M&A.
GoSecure – Canadian firm GoSecure provides a range of security consulting and managed security services.
Grant Thornton – Large accounting firm Grant Thornton offers professional services including cyber and compliance.
Guidepost Solutions – Guidepost Solutions provides consulting services including investigation, compliance, and monitoring.
Halock Security Labs – Halock Security Labs provides security consulting including penetration testing and assessment.
H-Bar Cyber Solutions – H-Bar Cyber Solutions provides security consulting, compliance, and security training services.
The Herjavec Group – The Herjavec Group specializes in network security managed services and consulting.
Hex Security – Hex Security provides security consultation services toward both strategic and compliance objectives.
Hold Security – Hold Security provides consulting services and threat intelligence for business clients.
IBM – IBM offers cyber security consulting solutions in its suite of products and services.
Imagine Cyber Security – Information security assessments are available from Imagine Cyber Security, founded in 2014.
Immunity – Florida-based Immunity provides security consulting services including assessments and penetration testing.
Include Security – Include Security offers information and application security assessment, advisory, and consulting services.
InfoDefense – InfoDefense provides security consultation in regulatory compliance, information assurance, and response.
InfoGuard – InfoGuard provides ICT security products, professional services, and managed security for business customers.
infoLock – infoLock provides information security consulting, integration, and value added resale (VAR) services.
Infosys – Infosys provides IT consulting, technology and outsourcing services including a range of information security solutions.
InfoWatch – InfoWatch includes international companies, InfoWatch, Kribrum, EgoSecure, and Appercut.
InGuardians – InGuardians is a security consultancy offering audit, penetration testing, and related services.
Intellect Security – Intellect Security provides data security and encryption for enterprise and cloud using a network of partners.
Interhack – Interhack provides a range of computer-related professional services with emphasis on security assessments.
Intrinium – Intrinium offers a range of cyber security consulting and managed security services.
IOActive – Research group IOActive focuses on offering services related to hardware, software, and systems security.
IPV Security – IPV Security provides security consulting services focused on compliance, monitoring, management, and audit.
IRM – IRM is a UK-based firm offering a range of security consulting and risk management services.
ITsec Security Services – ITsec Security Services provides IT security-related consultation services in the Netherlands.
IT Security Experts – IT Security Experts is a UK-based security consulting organization focused on audits and training.
Jacadis – Ohio-based Jacadis provides a range of cyber security consulting services to business clients.
justASC – justASC provides security consulting focused on threat management, secure architecture and incident response.
Kindus – Kindus is an information security and services consulting firm located in the United Kingdom.
KLC Consulting – KLC Consultants offers security assessments, third-party risk management, and security engineering.
Knox Corps – The Knox Corps provides consulting solutions with emphasis on regulatory compliance.
KoreLogic – KoreLogic provides penetration testing, application security assessment, and threat modeling.
KPMG – KPMG provides a wide range of professional services to business clients, including information security.
Kroll – Kroll offers a range of information, physical, and investigative security professional services.
K2 Intelligence – K2 Intelligence provides investigative, integrity, and analytic consulting including forensics.
Larson Security – Larson Security provides cyber security services including digital forensics and incident response.
LBMC – LBMC Information Security offers a range of security consulting services including penetration testing.
Leidos – Formerly part of SAIC, Leidos offers a range of information assurance and cyber security services.
Leviathan Security Group – Leviathan Security Group is an information security and risk management consulting firm.
London Cyber Security (LCS) – Cyber security consultancy firm London Cyber Security serves global insurance markets.
Mandalorian Security – Mandalorian provides information assurance and advisory services in EMEA and Asia Pacific.
Marsh – Marsh provides insurance products and related professional services including several cyber security offerings.
Maven Security – Maven Security provides security consulting services including Web and network security assessments.
McKinsey – McKinsey offers technology and business advisory services including enterprise and IT security risk consulting.
Minded Security – Minded Security provides software security consulting as well as application security testing tools.
MindPoint – Virginia-based MindPoint offers a range of information security consulting and engineering services.
MKA – MKA provides security consulting services including SOC and vSOC capabilities for public and private sector customers.
Navixia – Navixia provides a range of security technical and advisory services including audit and training.

NCC Group – NCC Group is the parent company of several cyber security firms including iSec Partners.
NetSPI – NetSPI provides security professional services and penetration testing for its customers.
nGuard – nGuard provides a range of professional services including penetration testing and security assessment.
Nisos Group – Nisos Group provides penetration testing, risk advisory, and cyber security consulting services.
Northcross Group – Northcross Group provides management and technology consulting including cyber security.
NTT Security – NTT Security provides PCI QSA services, secure software consulting, and compliance support.
NuHarbor – NuHarbor is a cyber and information security consulting services firm located in Burlington, Vermont.
Obsidian Analysis – Obsidian provides management consulting and professional services in homeland security and intelligence.
One World Labs – One World Labs provides threat intelligence and related security services with emphasis on brand protection.
Optimal Risk Management – Optimal provides risk and security consulting services for business and government clients.
Optiv – Value added reseller security solutions provider Optiv includes security advisory consulting services.
Orange – Orange Business Services is a global integrator of communications solutions including cyber security services.
The Oxman Group – The Oxman Group provides cyber security management consulting and data forensics.
PA Consulting – London firm PA Consulting specializes in consulting, technology, and innovation.
Paladion – Risk advisory and consulting firm Paladion provides integrated SOC management, risk, and compliance.
Palo Alto Networks – Consulting from PAN include training, testing, proof of concept testing, and configuration audits.
Parameter Security – Parameter Security is a technical security audit and ethical hacking firm specializing in financial services.
PatchAdvisor – PatchAdvisor provides security consulting services, including penetration testing, to enterprise customers.
Patriot Technologies – Frederick-based Patriot Technologies provides information and network security services.
Pentura – Pentura, now part of InteliSecure, provides penetration testing, managed services, and GRC services.
Phirelight – Phirelight offers a suite of IT security consulting and cyber security protection solutions.
Phish Labs – Phish Labs provides a range of security services focused on detecting and preventing phishing-related threats.
Phoenix Data Security – Phoenix Data Security provides security consulting services with focus on data loss prevention.
PivotPoint Security – PivotPoint Security provides security consulting services including penetration testing and ethical hacking.
Portcullis – Portcullis security consulting services including penetration testing and threat analysis-based response.
Praetorian – Praetorian offers security consulting services focused on applications, mobile, and network.
Prevalent – Prevalent provides security consulting solutions including compliance and third-party vendor risk management.
ProactiveRisk – ProactiveRisk provides cyber security services including security testing and response planning.
ProfitStars – ProfitStars provides professional services including information security and risk management consulting.
Protiviti – Protiviti provides business consulting services included GRC, audit, and risk management.
Provensec – Provensec provides security consulting and penetration testing services for mid-sized businesses.
PUNCH – PUNCH is a boutique cyber consulting firm offering security analytic support for threat management.
PwC – PwC is a multinational professional services company that includes a cyber security consulting offering.
Quadrant Information Security – Quadrant provides security consulting, managed security, and security management.
RANE – RANE connects subject matter experts, including in cyber security, with subscribers requiring assistance.
RavenEye – RavenEye provides security consulting including ethical hacking, PCI DSS QSA services, and penetration testing.
Razorpoint Security Technologies – Razorpoint provides security consulting, professional, and managed services.
Reaction Information Security – Reaction provides security consulting services with emphasis on penetration testing.
Redspin – Redspin, now part of Auxilio, provides penetration testing, application security, and audit services.
Red Tiger Security – Red Tiger Security offers security consulting and training services with emphasis on ICS/SCADA security.
ReliaQuest – ReliaQuest offers a range of security consulting services focused on assessment, protection, and management.
Rhino Security Labs – Rhino Security Labs provides security consulting services including penetration testing.
Ridge Global – Ridge Global provides security professional services including cyber insurance protection for business.
Risk-Based Security – Risk Based Security provides vulnerability intelligence, training, and cyber risk analytics.
RiskSense – RiskSense provides a vulnerability management platform along with a range of security services.
Rofori – Rofori provides a capability for managing cyber risk consistent with the NIST Cybersecurity Framework.
Roka Security – Roka Security provides network reviews, vulnerability assessments, and support for incident response.
Rook Security – Rook Security is a security and advisory consulting firm with managed security services and solution integration.
Root9b – root9b provides advanced cyber security training and consulting along with regulatory risk mitigation services.
SafeCipher – SafeCipher offers a range of security consulting services including PKI solutions, PCI services, and encryption.
Sage Data – Consulting firm Sage Data offers its nDiscovery Log Analysis service for enterprise customers.
sandSecurity – sandSecurity offers a range of security consulting services including assessments and risk mitigation.
Seccuris – Seccuris, now part of Above Security, provides consulting, MSS, and security educational services.
Secure Anchor – Secure Anchor provides vulnerability assessment, penetration testing, and forensics.
Secure Digital Solutions – Secure Digital Solutions provides a range of IT security and GRC consulting services
Secure Ideas – Secure Ideas provides a range of security consulting solutions including penetration testing.
SecureState – Consulting firm SecureState specializes in compliance, information security, and incident/breaches.
SecureWorx – SecureWorx provides security consulting solutions with emphasis on the Australian Government.

Securicon – Securicon provides security solutions including assessments of SCADA, process control, and other areas.
Security Art – Security Art provides a range of cyber security consulting services including red team exercises.
Security Audit Systems – Security Audit Systems provides a range of security consulting services including penetration testing.
Security Compass – Security Compass provides application security assessment and secure development advisory.
Security Management Partners – Security Management Partners provides security and IT assurance-consulting services.
SecurityMetrics – SecurityMetrics provides PCI DSS, HIPAA, and data security compliance assessments.
Security Risk Solutions – Security Risk Solutions provides information security and compliance consulting services.
Secur1ty – Secur1ty provides a social platform for connecting customers with security experts on demand.
Sense of Security – Information security services provider Sense of Security is located in Australia.
Sentor – Sentor provides IT security services including network protection, log management, and vulnerability monitoring.
Sera-Brynn – Sera-Brynn provides PCI DSS QSA services as well as security risk management consulting.
7Safe – 7Safe provides information security consulting, penetration testing, training, and related services.
Singular Security – Singular Security provides a range of risk analysis, vulnerability assessment, and cyber security services.
Spohn – Spohn offers security audit and assessment services in addition to telecommunications and training.
Spyders – Spyders is a Canadian firm providing IT and network security consulting and advisory services.
Stealth Entry – Stealth Entry offers an experienced cyber security and network assessment team in Columbus, Ohio.
Stickman Consulting – Stickman Consulting is a security consulting firm that specializes in PCI DSS compliance.
STI Group – STI Group provides a range of strategic and tactical information security services for clients.
Stratum Security – Washington-based Stratum offers a range of information security consulting services.
Stroz Friedberg – Now part of Aon, Stroz Freidberg provides investigation and response-based consultation services.
S21sec – S21sec is a multinational firm that provides a range of cyber security services and technology across many industries.
Sunera – Sunera provides IT and risk advisory, information security, and corporate/regulatory governance consulting services.
Sword & Shield – Sword & Shield provides a range of managed and professional cyber security services.
Symosis – Symosis supports secure apps, mobile, and cloud platforms through assessments, gap analysis, and due diligence.
Syndis – Syndis is a security think tank offering a range of cyber security services including penetration testing.
Synercomm – Synercomm is an IT, mobility, infrastructure, audit, testing, and security consulting firm.
SystemExperts – SystemExperts is a boutique provider of IT compliance and security consulting services.
TAG Cyber – The TAG Cyber team provides expert consulting, assessment, and training in cyber security.
Taino Consulting Group – Boston-based firm Taino Consulting Group specializes in security risk management.
Tangible Security – Tangible provides security consulting including assessments and virtual CISO for government.
TBG Security – TBG Security provides security consulting to assist with compliance in HIPAA, PCI, and related frameworks.
TDI – TDI provides a range of security technology, policy compliance, and audit consulting services.
Tech Mahindra – Large Indian outsourcing and technology firm Tech Mahindra includes cyber security consulting.
Telos – Telos provides a range of cyber security, secure mobility, and identity management solutions.
Templar Shield – Templar Shield provides a range of security consulting, managed security, and recruiting services.
Tevora – Tevora provides security consulting, risk management, and compliance solutions for enterprise customers.
360CyberSecure – Texas-based 360Secure provides a range of security consulting and assessment services.
Tiger Security – Tiger Security provides security consulting services including offensive, investigation, and intelligence.
Tiro Security – Tiro Security provides staffing and consulting services with emphasis on security assessments and virtual CISO.
Topgallant Partners – Topgallant Partners provides security consulting services including assessment, audit, and risk analysis.
Torus Technologies – Torus Technologies provides valued added resale security including consulting offerings.
Trojan Horse Security – Trojan Horse Security provides penetration testing and compliance assessments.
TruSec Consulting – TruSec provides security consulting services including IT compliance assurance and IT risk management.
TrustedSec – TrustedSec provides a range of security consulting services including penetration testing.
TrustWave – Cyber security firm TrustWave includes PCI DSS, managed security, and security consulting.
TSG Solutions – TSG Solutions offers infrastructure security and technology solutions including risk management.
TwelveDot – TwelveDot provides a range of security consulting with emphasis on mobile and cloud.
2B Secure – 2B Secure provides a range of value added reseller solutions in information security.
2-sec – 2-sec provides a range of security consulting offers including penetration testing and PCI DSS services.
Urbane Security – Urbane Security provides information security consulting services.
ValueMentor Consulting – ValueMentor Consulting provides security consulting including compliance and assessments.
VariQ – Security consulting company VariQ covers IT, cyber security, and software development.
Varutra – Varutra offers a range of information security consulting and training services for enterprise customers.
Veris Group – Cyber security company Veris Group offers a range of cyber security consulting services.
Verizon – Verizon offers cyber security consulting as part of its portfolio for enterprise.
Vigilant – Vigilant provides security services including managed network security, managed endpoint, and consulting.
VigiTrust – VigiTrust provides security training, compliance readiness, GRC, and related security professional services.
Voodoo Security – Voodoo offers security-related professional services for enterprise and security technology vendors.

Wipro – Wipro provides IT services, consulting, and outsourcing, including a practice in IT security services.
Wizlynx Group – Wizlynx Group provides a range of IT security services based on its Information Security Competence Center.
Xyone – Xyone provides security consulting including penetration testing, compliance, incident response, and training.
Yarix – Yarix provides security consulting services including penetration testing, forensic analysis, and audit.

Control 47: Security Recruiting

Security recruiting involves the on-going attention and focus required by enterprise security managers to properly nurture, improve, and *grow* their present and future staff, often with the assistance of third-party executive search specialists. Since enterprise security is such a growing field, much of this recruiting function involves finding the best qualified candidates to fill essential roles – which admittedly can be a rewarding and even exciting activity. Too many CISOs do not take the time to nurture trusted relationships with executive search firms, and this leads to rushed engagements when external search assistance is required. As the CISO position continues to evolve to a fully-recognized executive appointment, one can only hope that more attention is placed in this area. Search firms also bear some of the responsibility for less than stellar relationships with CISOs to date. Not recognizing the unique aspects of the CISO role, many search firms thrust general solutions to staffing problems at the security team, only to produce confusion and distrust. The coming years, we must hope, will bring a new set of closer, more trusted relationships between search firms and security executives. It is worth noting that this trust is in everyone's interest as CISOs seek to staff their local teams – or alternatively, seek to find their own potential new opportunities.

General Outlook
The general outlook for security recruiting solutions involves transition from isolated focus on job search opportunities to a more holistic focus on career management for CISOs and their teams. The transition also involves a shift from transactional retained search to a more relationship-based partnership over a longer period. First generation security recruiting from 1998 to 207 involved a headhunter mentality with a buckshot approach to finding candidates, often with high fees being paid by all participants. Second generation security recruiting from 2007 to 2016 involved increased partnership between search firms and more informed CISO buyers doing a better job working with search firms. During this period, the rate of executive moves at the CISO level reached fever pitch, especially in financial services, where CISOs seemed to shift jobs every few months (perhaps for more money). Also during this period, many new college hires were made based on the graduate's ability to perform cyber security chores. Third generation security recruiting from 2016 to 2025 is likely to continue the trend toward a more professional approach, based on relationships and holistic career management. The range of search, recruit, and hire options will increase, and more executive search firms will move in the direction of using search as a free, loss-leader toward more potentially lucrative consulting engagements.

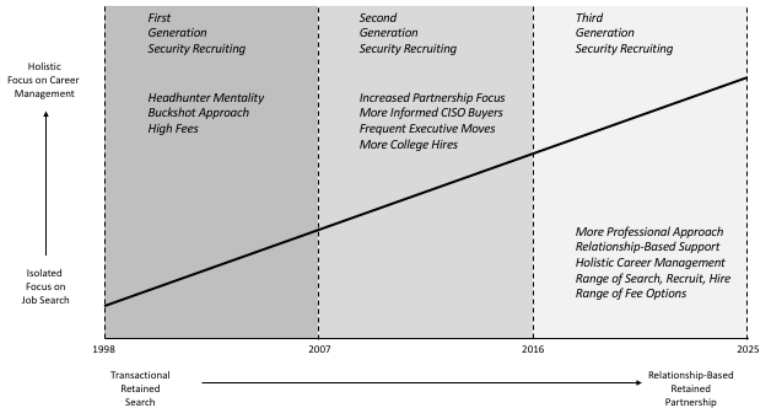

Figure 47. 2018 Security Recruiting Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since recruiting and search firms are already moving in the direction of more extensive consultative roles with their business clients. Also expect to see a burgeoning of virtual CISOs who help clients get their programs up and running, sometimes helping to select and hire a more permanent enterprise security management team.

Advice for Enterprise Security Teams

This advice is mostly for CISOs: Take a moment to reflect on all those email offers you get each day from executive search firms suggesting that you get together to meet. If you are like your CISO peers, then you delete these offers from your in-box, perhaps grimacing in anger as you do so. As painful as this might seem, especially if you are a typically introverted CISO, you should *take* some of these calls and set up some of these appointments. Building a relationship with a solid, trustworthy executive search firm will pay dividends in the future, and will future proof you from that awful feeling when a new project pops up that requires ten new staff immediately, or when you need a new incident response manager yesterday. You should also take the time to be less introverted and try to attend more dinners, cocktail parties, and other events with your peers. These activities extend your reach and will help you identify great candidates when the need arises.

Advice for Security Technology Vendors

If you are an executive search firm, then retained search remains the staple of your revenue stream – and this is fine for the foreseeable future. But you should open yourself to the possibility that your services are better viewed as *consulting*, and that you have a unique vantage point to help decision makers with business issues well beyond the recruiting of new managers or staff. Focus on building relationships with CISOs and their reports, and try to extend your range of professional services beyond retained search, because if you do not, then the enormous numbers of security consultants out peddling their wares might do precisely that to you.

List of Support Vendors

Acumin – Acumin is part of Red Snapper Group with executive search reach across the UK (headquartered), Europe, and the US.
Alliance Resource Network – Alliance has offices in NY/NJ with focus on broad set of C-suite positions including cyber security.
Alta Associates – Boutique search agency Alta Associates focuses on information security, risk management, GRC, and privacy.
Ashton Search Group – Ashton Search Group offers engineering and technical recruiting including cyber security.
Assevero – Assevero offers a range of cyber security services for business customers including security recruiting.
Barclay-Simpson – Search firm Barclay-Simpson, located in the UK, specializes in IT security and audit positions.
BeecherMadden – UK-based BeecherMadden is a search and selection business providing corporate positions including cyber.
Benchmark Executive Search – Benchmark includes a practice in cyber security and secure communications.
Blackmere Consulting – Blackmere offers specialized recruiting services with a focus on information security and enterprise risk.
Brandon Becker – Brandon Becker focuses on placement in networking, cloud, security, and virtualization.
Bridgen Group – Executive search firm Bridgen Group specializes in senior to C-level positions and cyber response.
Caliber Security Partners – Caliber provides security technical and advisory services, as well as staffing, for enterprise.
Cyber Search West – Cyber Search West is a search firm specializing in the managed security services sector.
Cyber Security Recruiters – Cyber Security Recruiters performs recruiting for security professionals from CISO to analyst.
CyberSN – Boutique recruiting company CyberSN specializes in cyber security talent in companies around the world.
Cyber 360 Solutions – Cyber 360 Solutions provides information security search and recruiting services.
Direct Recruiters – Recruiting firm Direct Recruiters has many areas of staff specialization including an IT Security practice.
Egon Zehnder – Major global executive search firm Egon Zehnder focuses on C-suite and board level positions.
ExecRank – ExecRank provides an on-line marketplace for executive and board search and connections.
First Arrow Executive Search – First Arrow Executive Search focuses on the intelligence, DoD, and Federal marketplace.
Glenmont Group – Glenmont Group offers executive search with emphasis on legal and litigation support positions.
Robert Half – Robert Half offers staffing focused in accounting, technology & IT, administrative, creative, and legal.
Hammer Consulting – Hammer Consulting focuses on staffing positions related to sales teams for technology companies.
Heidrick & Struggles –Heidrick & Struggles focuses on executive and senior leadership positions including CISO and CSO.
Intelligent Executive Search – Intelligent Executive Search provides executive career development portal services.
Korn Ferry – Major executive search firm Korn Ferry has expertise in finance, industrial, technology, and life sciences.
Kreamer Search Partners – Kreamer Search Partners is a search firm supporting placement in network and cyber security.
Leathwaite – Global search firm Leathwaite is focused on executive positions within the financial services industry.
Ken Leiner Associates – Ken Leiner Associates is a search firm focused on VP, operations, marketing, and engineering positions.
Lenzner Group – Lenzner Group is an executive search group focused on security, risk management, and cyber intelligence.
LJ Kushner and Associates – LJ Kushner and Associates is an executive search firm focused on information security.
Manta Security Management Recruiters – Florida-based recruiting firm Manta Security focuses on security management.
McIntyre Associates – Boutique search firm McIntyre Associates focuses on cyber security positions.
Momentum Security Recruitment – Momentum specializes in recruiting across the UK, Europe, Middle East, and Africa.
Nclav – Nclav is a platform from Jonathan Martinez for connecting hiring companies with security practitioners.
Nicholson Search – Nicholson Search focuses on business intelligence, CRM, IT management, and cloud computing positions.
121 Silicon Valley – 121 Silicon Valley provides executive search and recruiting services for software companies.
Pinnacle Placements – San Francisco firm Pinnacle Placements addresses security industry recruiting and search opportunities.
Potomac Recruiting – Potomac Recruiting serves consulting, IT services, healthcare, and government sectors around the world.
Reflik – Reflik is a social recruiting platform for obtaining referrals of top talent in various industries.
Romack – Romack provides a range of professional staffing services in various areas of technology.
Russell Reynolds – Russell Reynolds specializes in senior executive and board-level opportunities around the world.
Sabat Group – New Jersey-based recruiting firm Sabat Group focuses on placing information security professionals.
Secure Recruiting International – Tampa-based Secure Recruiting has focused on cyber security industry recruiting since 1997.
SecurityHeadhunter – Florida search firm SecurityHeadhunter focuses on information security recruitment.
SecurityRecruiter –SecurityRecruiter provides recruiting, education, and career coaching for information security professionals.
Secur1ty – Secur1ty provides a social platform for connecting customers with security experts on demand.
Silverbull – Connecticut-based Silverbull specializes in cyber security, IT, and related technology search and recruiting.
Software Placement Group – Software Placement Group provides recruiting services focused on software and sales positions.
Spencer Stuart – Spencer Stuart has emphasis on placing senior executive and board-level positions.
SRP Careers – SRP Careers is a Phoenix-based agency with a range of focus including technology jobs.
SSR Personnel – SSR Personnel focuses mostly on fire, safety, and physical security positions globally.
Stanley Reid & Company – Stanley Reid & Company focuses on technical recruiting for cyber and computer network operations.
Syndicus – Syndicus places IT staffing and consulting service positions including emphasis in health and life sciences.
Templar Shield –Cyber security consulting and staffing firm Templar Shield offers professional recruitment services.
Tiro Security – Tiro Security is a cyber security consulting firm with staffing and executive search services.
Top Dog Recruiting – Top Dog provides mid and senior level recruiting services in IT, engineering, healthcare, and IT security.
Toptal – Toptal is a unique service that provides means for companies to hire expert free-lancers in various technology areas.

Tri-Secure – Tri-Secure offers cyber security, telecom, and data center recruitment services in London.
Via Resource – Via Resource offers search and recruitment services focusing on information security and risk management.
ZRG Partners, LLC – ZRG Partners offers cyber security recruiting and related support services.

Control 48: Security R&D

Security Research and Development (R&D) involves the forward-looking investigation and corresponding results that stem from pure and applied research in cyber security algorithms, technology, and architecture. Precious few enterprise security teams have the capacity to sponsor internal security R&D, and if so, then it is more than likely being done by a Fortune 50 company – and with only a couple of exceptions, is not likely to be much good. That said, companies of all sizes and shapes can learn to *consume* security R&D, and by this, we mean more than just detailed information on the latest malware being reported on CNN. Instead, we mean absorbing useful results being reported by computer scientists specializing in this area. Cyber security R&D prior to the mid-1990's was a vibrant component of the community (go back and look at the conference proceeding agendas from the time), but seemed to become depressed with the invention of the web during that era, and its attendant business opportunities. Since then, security R&D has been mostly focused on developing deeper understanding of malware, and creating more lethal means for offensive attack. While academics at universities and government-funded research centers do their best today to make important research contributions, the reality is that cyber security R&D is largely irrelevant to the enterprise level, and absolutely nothing from the research community has been helpful in stopping the worldwide jailbreak of malware exploits, data loss, and availability attacks. If you ask the typical CISO, for example, what sort of research they read and follow, you'll hear that they scan Brian Krebs' website – or something like that. Recently, however, the embryonic beginnings of some excellent security R&D are finally starting to result in creative new approaches such as deep learning and artificial intelligence-based solutions. Vendors have been the first to jump on these bandwagons, but CISO teams are advise to learn to read and understand this research, if only to become better buyers of the attendant technology products. The bottom line is that without vibrant cyber security R&D funded at all levels of industry, academia, and government, the premise that an enterprise can stop nation-state attackers is fatally flawed. The offense continues to innovate at a rapid pace, so the defense must do so as well. The view here is that R&D results will be as important to enterprise cyber defense in the coming decade as new tools, techniques, and processes. We in the defensive community must simply up our game and become smarter.

General Outlook

The general outlook for security R&D solutions involves transition from practical, business-oriented results in the late 90's such as signatures of attack to more holistic, threat-oriented R&D solutions addressing foundational issues. This R&D transition is also beginning to move from pure offense to a broader perspective on both offense and defense – and this means more than just academic research in cryptography. First generation security R&D from 1998 to 2007 involved mostly offensive R&D including signatures. Some businesses began to fund R&D,

but only the largest. Focus on science and theory dried up almost completely during this era amidst the dot-com gold rush. Second generation security R&D from 2007 to 2016 involved the early beginnings of some defensive R&D focused on threats, and academics discovered that cyber security would help them get grants and gain tenure – which resulted in some uneven contributions. A slight return to scientific and theoretical results occurred during this era, often from government organizations. Third generation security R&D from 2016 to 2025 should expect to see dramatically improved results that are applicable to the enterprise from many different sources in academia and government. Enterprise teams will continue to mostly consume R&D, rather than fund it. The best enterprise teams with the highest success rates in stopping advanced attacks will attribute part of their excellent results to a steady ingest of great security R&D ideas, techniques, and results.

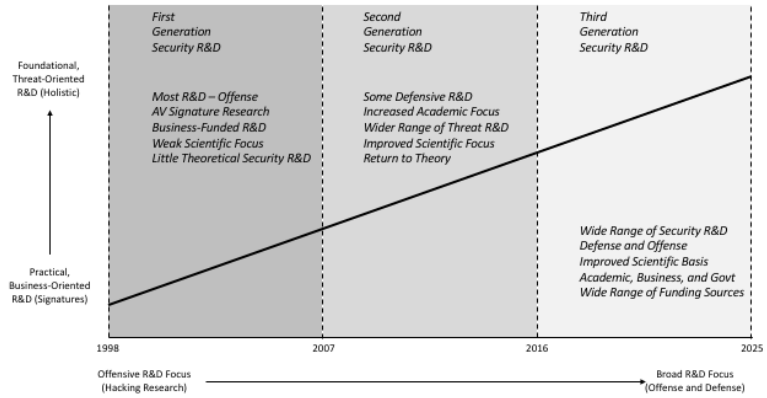

Figure 48. 2018 Security R&D Outlook

The TAG Cyber degree of confidence in this predictive outlook is moderate, since almost no CISO teams consider security R&D to be part of their program today. Instead, they invite vendors to come into their conference rooms to tout their latest machine learning advance. This is not an ingest of R&D by enterprise, and the fact that it remains the only lifeline to the research community today introduces risk to the outlook prediction in this area. Perhaps as more students graduate from academic cyber security programs with degrees and certificates, the habit of reading and using security R&D will increase.

Advice for Enterprise Security Teams

Get your team together today and discuss this issue. To be a proper cyber defender, you will need to be consistently knowledgeable of the best available research results in cyber. Start a weekly lunch and learn, for example, with your team, where each week, someone reports on a paper they have read. Select materials from the best researchers at great institutions such as universities, federally funded research institutes, and even large companies. Be careful to not confuse vendor marketing with research results. Some of the larger vendors do offer some useful tutorials, but these are more than likely designed to lead the horse to water (so to speak). Of all the security controls in the TAG Cyber Security Annual, this might be the most difficult to consistently support, simply because so many CISOs and their team members did not

come from the research community. But this is no excuse: You must start today to consume a regular diet of security R&D and you will see how powerful this can be in designing the best protection of your assets.

Advice for Security Technology Vendors

Vendors have already figured out that security R&D is an important differentiator in their product marketing. The problem is that most of this R&D has been focused on malware and threat identification. Security "research" is usually connected to finding reported vulnerabilities or stolen credit cards on the dark web, and this is not what is meant here by R&D. The recent introduction of machine learning, deep learning, and artificial intelligence research is a better example of the sort of thing the best vendors in the coming decade will be doing. Here's an idea: Why not get out there today and start sponsoring booths at IEEE, ACM, and similarly research-oriented conferences. The papers are ten times better than the big mammoth conferences (which have become terrible, by the way), and the people you will meet will be interesting, capable, and potential buyers of your solution. As a bonus, the booth fees are lower.

List of Support Vendors

Adventium Labs – Adventium solves hard problems in cyber security research and development (R&D) with emphasis on automated reasoning.

Applied Physics Laboratory (APL) – Part of Johns Hopkins, APL includes an R&D program focused on various aspects of cyber security, mostly for defense purposes.

AT&T – AT&T maintains a group of security researchers focused on innovation and forward looking solutions for mobility and virtualization security.

BlueRISC – BlueRISC provides hardware-assisted endpoint security for anti-tamper and cyber protection.

Brookings Institute – Brookings is a think tank in Washington that offers forward-looking views on cyber security and related issues.

CSIS – CSIS is a DC-based organization that includes many major retired and former officials from government and industry with a unique insight into future trends in cyber security.

ERNW – ERNW is an independent IT security services and consultation company specializing in knowledge transfer.

Galois – As part of its computer science and mathematics services, Galois provides R&D in several areas of computer security.

Google – Google includes a cyber security research team focused on innovation in various aspects of security and privacy.

HPE Security Research – HPE operates a major corporate cyber security research group with a long-standing tradition in supporting R&D objectives.

IBM – The Watson Research group at IBM continues to provide excellent R&D output in so many different areas including cyber security research and development.

IOActive – IOActive provides a range of security hardware and software assessments and research services.

Kyrus – Kyrus focuses on security research, reverse engineering, computer forensics, and secure software development.

Lincoln Laboratory – Lincoln Laboratory is a Federally funded research institute connected with MIT.

Maryland Cybersecurity Center – Connected to the University of Maryland, the Maryland Cybersecurity Center supports research, education, and outreach.

McAfee – The McAfee team continues to provide advanced research in malware techniques and structures.

Microsoft Research – Microsoft continues to maintain one of the leading corporate-funded research teams.

MITRE – MITRE is a US Federally-funded organization focused on a variety of research and development solutions including cyber security.

Naval Research Laboratory – NRL is one of the original research laboratories in cyber security with capability in formal methods.

NSS Labs – NSS Labs provides expert cyber security research and analysis services for enterprise customers, with emphasis on practical, hands-on experience and test with security products.

NYU Tandon Engineering – Several research activities are supported at NYU led by Nasir Memon.

Oxford University – Oxford provides cyber security and privacy research with focus on formal methods.

RAND Corporation – RAND conducts research in cyber space and cyber security with emphasis on government-related issues.

Reservoir Labs – Reservoir Labs provides a range of scientific and technical research in areas such as network technology and security.

Sandia National Laboratories – Sandia is a Federally funded national laboratory includes cyber security program.
SecDev Group – SecDev Group is a cyber research think tank that provides open intelligence to improve awareness in cyber security and related areas.
Securosis – Securosis is an independent security research and advisory firm offering insights into Web 2.0, APT protection, and security investment.
SRI International – SRI is a non-profit research institute that has pioneered many areas of cyber security including intrusion detection.
Symantec – As part of its endpoint solutions, Symantec provides advanced research in malware techniques and structures.
Syndis – Syndis is a security think tank in Iceland offering a range of services including penetration testing.
TechGuard – TechGuard provides a range of cyber security and information assurance solutions for commercial and government customers including security R&D.
Tel Aviv University – Tel Aviv University supports cyber security research and sponsors Cyber Week each year.
University College London – University College London includes an information security research group focused on cryptography, anonymity, authentication, and other areas.
US Army Research Laboratory – The US Army's research lab includes programs in cyber security research and information assurance.
Wapack Labs – Wapack Labs provides cyber threat analysis, security research, and intelligence services.

Control 49: Security Training and Awareness

Security training and awareness programs involve the education, teaching, and messaging required to improve the cyber skills of security experts, IT professionals, senior executives, and everyday support staff. As you would expect, this wide range of training targets begs a commensurate wide range of education approaches. Cyber security experts, for example, require specialized focus in aspects of their discipline such as firewall administration, vulnerability management, and compliance automation. IT professionals, in contrast, need more basic introductions to cyber security, but in ways that do not insult their technical backgrounds and knowledge. Senior executives might be the most difficult for security training and awareness programs because they tend to be entrenched in world views based on experience that might be at odds with cyber security concepts. For example, senior executives demand attribution and motivation explanations after an attack, only to be annoyed when they are taught that these are not easily obtained – or frankly even relevant to protection initiatives. Day-to-day support staff are usually subjected to awareness programs designed to reduce the likelihood that they will do something incredibly stupid from a security perspective. Such programs traditionally have been terrible, with long boring emails, poorly produced videos, and trite brochures that would insult the intelligence of even the most ardent Luddite. The trend in security training and awareness is positive, however, with organizations now realizing that learning programs are intended to inspire, motivate, and drive people to action. Accordingly, better use of professionally developed content, improved integration with social networks, and more appropriate messaging are all attributes of modern enterprise security training and awareness programs. This trend will continue, and in fact, accelerate, especially for day-to-day support staff awareness. Expect video to be the primary delivery mechanism, which surprisingly makes YouTube (of all things) a vital component of the typical enterprise cyber security infrastructure.

General Outlook

The general outlook for security training and awareness involves transition from general education to more domain-specific training, especially for experts. The transition also involves shift from conventional (translation: boring) InfoSec sessions for staff to much-improved experiences using social, video, and viral means for delivery. First generation security training and awareness programs from 1998 to 2007 involved uneven quality, lack of much creativity, and mostly ineffective programs leading to poor results. Second generation security training and awareness programs from 2007 to 2016 introduced early video use with improved quality, more creativity, and on-line learning. The results remained largely ineffective, as evidenced by the jailbreak of incidents, break-ins, and data loss experienced by business and government during this period. Third generation security training and awareness programs from 2016 to 2025 should expect to see highly professional programs of high quality with emphasis on video and social networks. More domain-specific options will be available for experts in areas such as ICS, IoT, mobile, virtualization, and cloud. On-line options will improve as well, with massive open on-line courses (MOOC) being offered on world-class platforms at low cost.

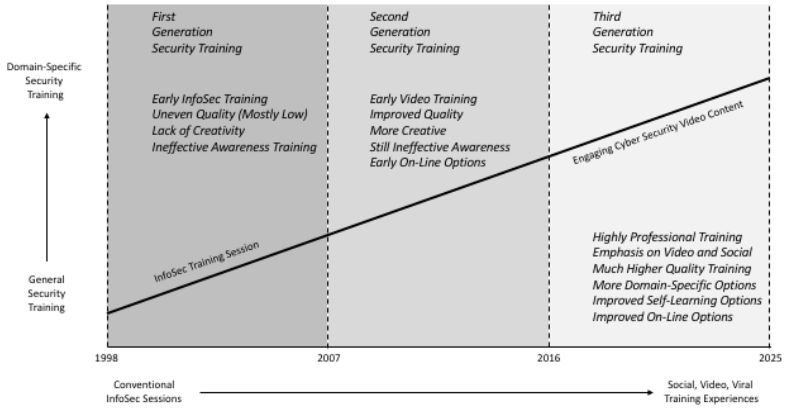

Figure 49. 2018 Security Training and Awareness Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since the trends have already begun to shift to much higher quality training and awareness programs. MOOC offerings from the more popular on-line learning platform companies are now excellent, often provided by some of the greatest universities in the world.

Advice for Enterprise Security Teams

Rethink your training and awareness program if you are still sending bad security warning emails with the title: “Attention: All Staff.” This is not the way to inspire your staff toward improved security decision-making. Look for vendors who can provide you world-class training content videos, often on a subscription basis. Also, recognize that training experts and making staff aware are two separate activities that should be managed and budgeted separately. Too many companies forget that experts require continued training, especially in a field as dynamic and changing as cyber security.

Advice for Security Technology Vendors

If you provide security awareness and training course, then you don't need to hear it here that you are busy. The good news is that will continue so long as you focus on inspiring and engaging your learners. Do not rest on old, traditional training methods: Be creative. If you provide training such as Phish testing, or other active means for teaching staff to make better security decisions, then you are also busy. But you must also recognize the need to continually improve your means for delivering learning messages. Just because you sold ten Phish tests last year doesn't mean that CISOs will come to the view that they can get hacked just as easily with you as without. If you train experts, then make sure you offer lots of domain-specific options. This has not been an issue for the companies offering learning events and mini-conferences. These are excellent resources for experts. One last point is that if you run conferences, then please try to improve the content. Security conferences are devolving into social events with vacuous information from speakers and panels.

List of Support Vendors
Above Security – Above Security includes training as part of a large portfolio of managed and consulting services.
Accumuli – Training is included as part of larger set of service offerings from Accumuli, which is part of the NCC Group.
Advent IM – Advent IM provides knowledge-based consulting and training services for enterprise customers in the UK.
AppSec Labs – AppSec Labs provides application security services including design, analysis, training, and assurance.
Aspect Security – Aspect Security includes training as part of its application security service suite.
Ataata – The security training start-up offers originally-produced video content to improve cyber awareness in the enterprise.
Attack Research – Attack Research provides a range of security consulting, assessment, and training services.
BHC Laboratory – BHC Laboratory provides independent security consultation and advice for business customers.
Billington Cyber Security – Tom Billington provides world-class cyber security seminars oncyber policy and technology.
BitSec – BitSec Global Forensics offers consulting and training to government and law enforcement.
Bitshield Security – Bitshield security provides IT security consulting and professional training for customers in the Philippines.
BugSec – BugSec offers a range of information security services and products for enterprise customers.
CIS – The Center for Internet Security (CIS) includes a range of training and awareness resources in support of the CIS Controls.
CompliancePoint – CompliancePoint provides a range of compliance assessments, consulting, and managed IT.
CyberCrocodile – CyberCrocodile offers information technology education specializing in information security.
Cyber Diligence – Cyber Diligence is a forensics firm that provides a range of computer crime and investigative training.
Cyber Gym – Cyber Gym offers real-world cyber defense-training arena for critical infrastructure organizations in Israel.
Denim Group – Denim Group provides secure software, including app development, assessment, training, and consulting.
Fortalice – Fortalice provides security consultation and training services for business and government.
Fox IT – Fox-IT combines human intelligence with technology to provide security solutions and training for customers.
Global Learning Systems – Global Learning Systems is a Maryland-based company offering security awareness training.
The GRC Group – The GRC Group provides GRC training, certification, and resources for enterprise professionals.
GRC 20/20 Research – GRC 20/20 Research provides research, workshops, and consulting support in GRC for enterprise.
Grid32 Security – Grid32 provides a range of security services including penetration testing and vulnerability assessment.
HackLabs – HackLabs provides a range of security consulting and training services including penetration testing.
H-Bar Cyber Solutions – H-Bar Cyber Solutions provides a rage of security consulting, compliance, and security training services.
IANS – IANS offers seminars with expert coordinators focused on a variety of practical cyber security topics.
Infinigate – Infinigate is a UK-based value added reseller that includes security training and consulting services.
InfoSec Institute – Information security training from InfoSec Institute includes hands-on and boot camp offerings.
InfoSec Skills – InfoSec Skills offers training courses in the UK and Australia to support professional cyber careers.
InfoSecure – Part of BeOne Development Group, InfoSecure provides awareness and security training.
Internetwork Defense – Internetwork Defense is a small training consultancy offering CISSP training boot camps.
Interskill – Interskill provides mainframe training with catalog of IBM mainframe and security courses.
IT Security Experts – IT Security Experts is a UK-based group offering security consulting and training.
justASC – justASC is a UK-based information security consulting company that includes training and awareness.
Kindus Security – Kindus Security is a UK security consulting company with on-line security training.
Learning Tree – Learning Tree offers a range of networking, data, application, business and cyber security training.
Lunarline – Lunarline offers a range of cyber security products and services including training.
MAD Security – VAR security solutions and consulting firm MAD Security offers range of security training options.
Maven Security – Maven Security provides security consulting and training including Web and network security assessments.

MediaPro – Pacific Northwest firm MediaPro provides a range of awareness, security, and privacy training.
Metacompliance – Metacompliance provides GRC, compliance, and security awareness for customers in the UK.
Meta Intelligence – Meta Intelligence provides intelligence services, risk management, security training, and pen testing.
MIS Institute – MIS Institute offers courses in internal audit, IT audit, and information security.
Navixia – Swiss information security consulting firm Navixia offers a range of security awareness training.
Offensive Security – Offensive Security provides information security training, certifications, and services.
Optiv – Value added reseller Optiv offers information security solutions and training services as part of its solution set.
PA Consulting Group – PA Consulting Group is a large consultancy that offers information security training for customers.
Palo Alto Networks – PAN offers security training services including a Certified Professional Services Provider (CPSP) program.
Parameter Security – Parameter Security operates a Hacker University training program.
Pentester Academy – Pentester Academy offers technical courses in Javascript, Forensics, Shellcoding, and penetration testing.
Phish Labs – Phish Labs provides security and training services focused on detecting and preventing phishing-related threats.
PhishMe – Phishme provides a service for using simulated phishing scenarios to train employees about the threat.
Phoenix TS – Phoenix TS provides vendor certifications, learning resources, and instructor-led course in IT, cloud, and security.
RavenEye – RavenEye provides security consulting including ethical hacking, PCI DSS QSA services, and penetration testing.
Red Tiger Security – Red Tiger Security is a SCADA consulting services firm offering courses in securing ICS/SCADA systems.
RedVector – RedVector provides online education and training for various industries including some cyber security offerings.
Root9b – root9b provides advanced cyber security training and consulting along with regulatory risk mitigation services.
Safelight – Part of Security Innovation since 2014, Safelight offers a range of security training options.
SANS – SANS offers a full curriculum of cyber security courses, education, and training from expert instructors.
SCADAhacker – SCADAhacker offers expert training services and resources for securing ICS/SCADA systems.
Secure Ninja – Secure Ninja offers a specialized range of cyber security training and IT security services.
The Security Awareness Company – Winn Schwartau offers information security training and resources.
Security Awareness, Inc. – Security Awareness Inc. offers security awareness for government and commercial customers.
Security Innovation – Security Innovation offers software security services and application security training.
Security Mentor – Security Mentor is a California-based training and security awareness services firm.
SecurityOrb – SecurityOrb is an information security and privacy Website with training and awareness resources
Security University – Security University specializes in CISSP, CompTIA, and Q/ISP security training.
See Security – Israel-based See Security is an information security and cyber warfare college offering advanced training.
Skillbridge Security – Skillbridge Security provides a range of cyber security training services including tailored courses.
Symantec – Now part of Symantec, The Hacker Academy provides modules and instructor-led sessions in information security.
Symosis – Symosis provides assessments, gap analysis, security training and due diligence.
Syntrio – Syntrio is a compliance and training organization that includes cyber security training courses.
TAG Cyber – TAG Cyber offers various on-site and virtual cyber security training offerings.
TeachPrivacy – TeachPrivacy offers a range of privacy and information security training including HIPAA.
Trail of Bits – Trail of Bits provides expert cyber security research and training services for customers.
Varutra – Varutra is a security consulting firm located in India that offers information security training.
VigiTrust – VigiTrust provides security training, compliance readiness, GRC, and related security professional services.
Visible Statement – Visible Statement provides 24/7 information security awareness solutions in multiple languages.
Wombat – Wombat offers interactive security training and phish simulation services. Wombat acquired ThreatSIM in 2015.

Control 50: Security Value Added Reseller (VAR) Solutions

Security value added reseller (VAR) solutions involve the bundled collections of product resale, expert consulting, system integration, purchasing support, management advice, and other tailored professional services offered to ease the enterprise task of selecting and buying cyber security products and services from vendors. Early VAR solutions were designed to do the paperwork involved in buying from many different hardware and software solutions from security vendors (and other types of vendors as well). Over time, the security VAR developed into a one-stop shop for organizations who preferred to outsource much of the purchasing, contracting, and other administrative tasks when putting together a security architecture. The good news for security VARs is that this further evolved into a trusted advisory role, one that supported as intimate a business relationship as one might find in a long-time consultant. The

bad news, however, is that with the clear shift from lengthy deployment cycles for hardware products to immediate point-and-click provisioning of software appliances, the role of the security VAR will certainly shift. Whether this shift is good or bad for the value-added security industry remains to be seen, but clearly the available business opportunities will change. The most aggressive security VARs will adjust and expand their consulting offers, and some will emphasize some aspect of their service that is less easy to virtualize, such as a local geographic knowledge in a remote region.

General Outlook

The general outlook for security value added reseller (VAR) solutions involves transition from hardware product sales and support to architectural strategy and planning support. This transition also involves shift from administration of product resale to solutions consulting via trusted partnerships. First generation security VAR solutions from 1998 to 2007 involved one-stop purchasing support for mostly hardware deals with heavy transaction orientation. Many VARs included in their value proposition the ability to sell into a local region based on cultural knowledge or language abilities. Second generation security VAR solutions from 2007 to 2016 involved an increase in solution offerings, still mainly transaction oriented, but with early focus on building lasting partnerships through guidance and consultation. Third generation security VAR solutions from 2016 to 2025 should expect a massive shift to self-provisioned virtual appliances, which will force VARs to serve in a more consultative role. The good news is that business for security VARs in the coming years will shift from transactional to strategic.

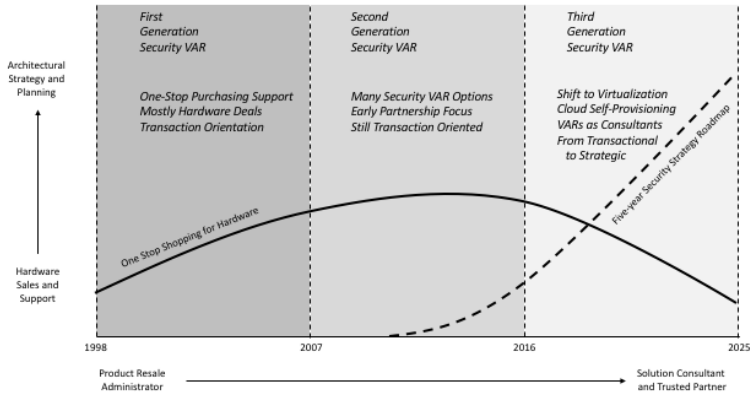

Figure 50. 2018 Security Value Added Reseller Outlook

The TAG Cyber degree of confidence in this predictive outlook is high, since the ability to provision via point-and-click portal interfaces has already begun to change the way CISO teams purchase products. SDN infrastructure from IPS teams will also include this ability to self-provision applications into service-chained run-time objects – which will only contribute further to the evolution of the security VAR role in business.

Advice for Enterprise Security Teams

The advice here is to spend some time this year with any security VAR solution providers you deal with today, and ask for a description of their roadmap for dealing with the shift to self-provisioned software. If they tell you that it will be business-as-usual in the coming years for value-added security, then you have the wrong partner. If you have a trusted partnership with an existing security VAR, then take advantage of this by investing in the relationship. Help them become a valued consultant to your business, offering guidance as you navigate the complexity of multiple vendor offerings across cloud, mobile, virtual, and related emerging technologies.

Advice for Security Technology Vendors

Security VARs must immediately take advantage of their relationships to develop deeper, more strategic partnerships as trusted consultants. Even security VARs located in a remote region, where their services include local, cultural and language support, must be mindful that point-and-click interfaces know no geographic boundaries. The vast number of value-added resellers will collapse and consolidate in the coming years, and the one who will survive are those who decide to adapt and evolve immediately, not waiting for those lucrative hardware resale deals to diminish. This is the year to act.

List of Support Vendors

ABR-PROM – ABR-PROM has been providing solutions such as SecPoint to customers in Poland since 2000.
AccessIT – AccessIT provides IT security and infrastructure solutions through VAR partnerships with major technology providers.
Accunet – Accunet provides storage, data center, security, network, and virtualization solutions since 1997.
Aggeios – Aggeios is a value added reseller of managed IT services, information security, and data center located in Kuwait City.
TenFour – Previously Alliant, the solution provider offers utility IT services, security, unified communications, and more.
Alpine Cyber Solutions – Alpine focuses on value added security solutions for customers in the Baltimore-Philadelphia market.
Alvea Services – ALVEA Services provides managed IT security and business continuity solutions through channel partners.
Alus Outsourcing – Alus Outsourcing provides information security and related services to customers in Brazil.
Aman Information Security – Aman Information Security is a Qatari-owned consulting and VAR security solution firm.
ARAMA TECH – ARAMA TECH offers VAR security solutions including GRC in the Netherlands and Denmark.
Arcon – Arcon is a managed security services provider serving enterprise customers in Latin America.
Asgent – Asgent provides network security and value added reseller solutions for SMB, primarily in Japan.
Assuria – Assuria provides security solutions, security software, and managed SIEM.
AVP Sistemas – AVP Systems is a VAR solution provider located in Ecuador and serving Latin America.
Axxum Technologies – Axxum offers value added services in cyber security and information assurance.
Baicom Networks – Baicom Networks is a Latin American value added security solution provider in Argentina.
Bridgeway Security Solutions – Bridgeway is a consultative reseller offering support and guidance for businesses in the UK.
Br-secure – Brazilian value added security solution provider Br-secure offers a range of technology partners.
Carahsoft – IT solutions provider Carahsoft focuses on trusted government offerings including cyber security.
Cirosec – Cirosec is a German information security consulting firm with value added solutions through partners.
Colvista – Colvista is a Latin American IT provider in Bogota offering consulting and integration services.
Comda – Comda is an integrator of security solutions in Israel with focus on biometrics, access control, and digital signing.
Conquest Security – Conquest provides security services and solutions in conjunction with a set of security technology partners.
CriticalStart – CriticalStart is a security consulting firm located in Texas area with penetration testing, risk, and VAR solutions.
CyberDefenses – CyberDefenses provides a range of security professional services for business and government customers.
CyberHound – CyberHound provides security solutions including NGFA and secure Web gateway via technology partnerships.
Denver Cyber Security – Denver Cyber Security provides IT security services via partnerships with Solutionary and Wombat.
DigitalScepter – Services firm DigitalScepter offers a range of value added reseller security solutions.
Digivera – Digivera provides information security, managed services, and technology consulting services.
Dimension Data – NTT parent owned IT services firm Dimension Data offers VAR security solutions.
E-Data Teknoloji – Value added reseller security solution provider E-Data Teknoloji is located in Turkey.
eMazzanti Technologies – eMazzanti provides IT technology consulting for business including various IT security services.
Empowered Networks – Canadian firm Empowered Networks offers technology services and solutions including security.
Enterprise Technology Partners – Enterprise Technology includes information assurance and VAR offerings.
eSecurityToGo – eSecurityToGo provides value added security and networking solutions including IT security consultation.

E-SPIN – Part of a group of companies in Malaysia, Hong Kong, and China, E-SPIN offers VAR services.
ETEK – Bogota-based value added reseller ETEK offers a range of cyber security and related services.
Fortress – Singapore-based value added reseller Fortress provides IT security with an office in Malaysia.
GigaNetworks – Florida-based firm GigaNetworks offers network security solutions including VAR services.
GuidePoint Security – GuidePoint Security provides information security solutions using a range of technology partners.
HardSecure – HardSecure provides values added resale (VAR) security solutions including consulting.
Infinigate – Infinigate is a VAR in the UK offering security services from companies such as Corero, Dell, and Trustwave.
Infogressive – Lincoln, Nebraska firm Infogressive offers cyber security VAR services and training.
InfoGuard – InfoGuard provides ICT security products, professional services, and managed security for business customers.
InfoLock – infoLock provides information security consulting, integration, and value added resale (VAR) services.
Intellect Security – Intellect Security provides value added data security and encryption solutions.
Intrinium – Cloud and managed IT consulting firm Intrinium offers a range of VAR solutions including security.
IPS – IPS is a small Canadian value added reseller (VAR) of cyber security products and services for business.
iSecure – Woman-owned IT security provider located in Rochester and offering VAR security solutions.
ISnSC – ISnSC is a Middle Eastern penetration testing and IT security solutions vendor with VAR capabilities.
Italtel – Italian telecommunications and IT solutions firm Italtel offers a range of managed and VAR services including security.
ITC Secure Networking – ITC Secure Networking is a UK-based integrator including services from the company's SOC.
IT2Trust – IT2Trust is a Scandinavian value added distributor of IT and network security solutions.
Lumenate – Lumenate provides a range of value added solutions including security and compliance through partners.
MAD Security – MAD Security provides VAR solutions, in addition to a range of security training services.
MindPoint Security – MindPoint Group provides a range of managed, compliance, and cloud security services.
Mission Critical Systems – Mission Critical Systems is an IT security reseller in the Southeast United States and Caribbean.
MSPStream – Managed IT services and solutions provider MSPStream offers a range of cyber security solutions.
M.TECH – M.TECH is a regional IT security VAR focused on security solutions offered through security technology partners.
Namtek – Namtek is a New Hampshire-based security controls and services provider with VAR capabilities.
NCC Group – Accumuli Security, part of NCC Group, provides value added security professional, managed, and training services.
Netpolean Solutions – Netpolean is a security solutions value added reseller (VAR) focused on the Southeast Asia region.
Network Security Group – Network Security Group provides security solutions through security technology partnerships.
Nexum – Nexum is a security solutions provider working with technology partners supported from Nexum SOC centers.
NH&A – NH&A provides security solutions for enterprise customer through partnerships with security technology providers.
Norseman Defense Technologies – Norseman is a small VAR provider serving Federal Government customers in the DC area.
Nuspire – Nuspire provides a range of managed security and network solutions through a variety of technology partners.
OneSecure – OneSecure Technology provides enterprise security solutions including email, network, data, and Web security.
Optiv – Optiv is a VAR cyber security solutions provider built from the recent merger of Fishnet Security and Accuvant.
Performanta – Performanta provides a range of security VAR, technical, and consulting services to business customers.
ProactiveRisk – ProactiveRisk is a New Jersey-based VAR with security, software, and supply chain focus.
Proficio – Proficio is a VAR solutions provider emphasizing managed security services including SOC and SIEM.
Referentia – Referentia is a VAR solutions provider located in Honolulu that includes cyber security offering.
ReliaQuest – ReliaQuest is a security consulting firm located in Florida that includes VAR security solutions.
RRC – Ukrainian VAR solutions provider RRC includes a range of resale offerings for data security.
SaaS Security – VAR security solutions provider SaaS Security in Norway supports technology partners including Proofpoint.
Secure Commerce Systems – Secure Commerce Systems is a VAR solutions provider in Texas that offers security products.
SecureNation – VAR security solutions provider SecureNation is located in Baton Rouge, Louisiana.
Securicon – Information security consulting firm Securicon is located in Northern Virginia offering VAR security solutions.
Security in Motion – Security in Motion provides IT security solutions including security technology products.
Seguridad IT – Seguridad IT is a VAR security solutions provider in Spain with extensive Cisco product offerings.
Sengex – Sengex provides a range of security solutions for mobile and data protection through partner integration.
Sharper Technology – Sharper Technology is a veteran owned IT infrastructure and data security VAR solutions provider.
Simet Teknoloji – Simet is a Turkey-based VAR solutions provider focused on computer and network security.
SNB Group – SNB Group is a VAR solutions provider in the Middle East focused on data storage, security, and IT.
Starlink – Starlink is a security advisory and value added solutions provider located in the Middle East.
STEBRI – STEBRI is an IT Solutions provider located in Slovenia with a range of cyber security offerings.
Supya Security – Supya Security is a Turkish VAR solutions provider that includes resale offerings for data security.
Syntegrity – Syntegrity provides security products and services including support for identity and access management.
Techlab – TechLab provides managed and value added data security products and services including mobile device security.
Templewood Homeland Security Solutions – Templewood offers cyber security solutions through partnerships.
Torus Technologies – Torus Technologies provides VAR security solutions along with a range of security consulting offerings.
Towerwall – Towerwall is a security consulting and VAR security solutions provider located in Massachusetts.

2B Secure – 2B Secure is a security consulting firm that provides value added reseller solutions in information security.
2Keys – Canadian firm 2Keys provides design, integration, and operating security solutions with VAR capability.
VILSOL – Managed security services and VAR solutions provider VILSOL offers next-generation firewalls in Latin America.
Westcon – Westcon Group is a VAR and distributor of network, unified communications, data center, and security solutions.
Wontok – Wontok provides value added services and endpoint security solutions
X-mart Solutions – X-mart Solutions is a VAR solution provider located in Sao Paulo, Brazil serving Latin America.