



NetDetectorLive™

Cyber security, data leakage prevention, and real-time surveillance

Features & Benefits

- » *Real-time inbound and outbound application monitoring with granular application content search*
- » *Real-time alerts of different IOCs, regulatory and internal company policy violations*
- » *Reconstruct application sessions and policy violations for audits and evidence*
- » *Integrated Signature & Anomaly based detection*
- » *Capture and store all communication sessions to search current and historic user activity*
- » *Real-time metadata generation for Layers 2-7 Metadata (IP, TCP, UDP, HTTP, DNS, Email, FTP, Chat, IRC, SSH, RADIUS, QUIC, etc.)*
- » *Role-based access control*
- » *Plug-and-play device with web-based intuitive user interface*



Challenge

Targeted cyber attacks across global networks have increased in impact as well as frequency. Web-based cyber threats, distributed denial-of-service (DDoS) attacks, incidents due to malicious code, and information loss due to malicious insiders, are having huge financial consequences on organizations. The loss associated with an attack is directly proportional to the time taken to resolve it. This puts organizations under pressure to quickly and accurately pinpoint the cause of a security breach.

Cyber security analysts need advanced network forensic solutions that can rapidly search through terabytes of data to provide them with the comprehensive visibility to detect, investigate and resolve attacks and breaches.

Solution

NIKSUN NetDetectorLive is a network forensics appliance that is uniquely capable of super fast forensics search, session reconstruction, and real-time detection of security violations.

Based on NIKSUN's next-generation technology, NetDetectorLive monitors all data flowing across the IP network and uses deep packet inspection techniques to accurately recognize, classify and analyze all applications, sessions and content traversing the network. Metadata is created in real-time on all content including email, IM, FTP, HTTP, and DNS. This metadata is made immediately available for fast search and investigation. Metadata can be stored in the NIKSUN Network Knowledge Warehouse (NKW) - a data repository - for long periods of time. NetDetectorLive searches through terabytes of data to return results in a fraction of the time that other retrospective forensic analysis tools take, rendering it indispensable for rapid forensic investigation and risk mitigation. NetDetectorLive alerts on suspicious traffic based on metadata content, for immediate notifications on policy violations, data exfiltration, malware, indicators of compromise (IOCs) and cyber attacks.

Rule-based Content Alerts

NetDetectorLive is pre-packaged with an extensive set of robust, content-based rules that are designed to detect and alert on a wide array of potential policy violations or activities that could be precursors to a violation. Similar sets of rules are grouped into logical categories. For example, rules that define user activity on hacker research, steganography or the download of password cracking software are logically categorized as "Insider Threats." Awareness of such suspicious activity within the network can help organizations take adequate measures to prevent the occurrence of a data breach.

More importantly, users have the flexibility to define and categorize their own rules. Rules can be defined on keywords, file names, file types, or specific field values for email and chat applications. Exact content matching can be done on files and URLs. Sensitive documents and files can be uploaded to NetDetectorLive so that precise content matching of network flows can be done against these uploaded documents, and additionally, against files to detect leakage of classified information and other instances of non-compliance. For instance, it is possible to upload a list of files that includes confidential.doc, proprietary.pdf, etc. and, if one of these documents appears as an attachment to an email, an alert is raised.

Event Analysis

On the detection of a violation, NetDetectorLive immediately generates an event. Events are tied to actual sessions and users can seamlessly pivot into multiple analysis paths to examine related sessions, applications or even the packets associated with these events. This provides a clear path to understand the reason behind a security or policy breach. All information associated with an event, including the users involved, information exfiltrated, whether it left the network, or whether the event was malicious or not, is available providing the complete, undeniable context of what happened.

Package Offerings

To better meet any organization’s needs, NetDetectorLive is offered in two product forms: NetDetectorLive Standard and NetDetectorLive Advanced. Compared to NetDetectorLive Standard, NetDetectorLive Advanced offers additional functionalities, such as keyword search, content-based alerts, and more (as seen in the table below):

Feature	NetDetectorLive Standard	NetDetectorLive Advanced
Dynamic Application recognition	●	●
Real-time metadata generation for Layers 2-7 Metadata (IP, TCP, UDP, HTTP, DNS, Email, FTP, Chat, IRC, SSH, RADIUS, QUIC, etc.)	●	●
ASCII and HEX view of Application Sessions	●	●
Integrated Signature and Anomaly based detection	●	●
TLS Compliance	●	●
Reconstruction of files, web pages, and other content for immediate retrieval		●
Raw string/keyword search on content (e.g., search for a word in a web page)		●
Real-time content-based alerts (Data Leakage Detection, etc.)		●

Technical Information

- » *Network Interfaces Supported (Full-duplex, Half-duplex) - 1GigE (copper/fiber), 10GigE (fiber) or 20/40/60/80/100GigE (fiber)*
- » *Protocols Supported - TCP, UDP, SCTP, IPv4, IPv6, fragmented IP, IEEE 802.3 (Ethernet), Ethernet MPLS, VLAN (ISL, IEEE 802.1q and stacked 802.1q), DNS, ICMP, HTTP, HTTPS, SSL/TLS, SMB, MSSQL, Oracle QinQ, Multicast, ISO8583, FIX, GTP, SIP, CDMA2000, RADIUS, Diameter, FTP, Email, Chat, SSH and many more.*
- » *Applications Reconstructed - Several hundred, including voice, video, web, FTP file transfers, chats, email, images, NetBIOS, peer-to-peer, IRC, DNS, wireless (LTE, CDMA2000, IMS), and desktop applications (Microsoft, Adobe, etc.).*
- » *Form Factors - A variety of 1U, 2U and 4U+ form factors are available. Internal storage scales to tens of terabytes. Unlimited external storage options are available.*
- » *Integration - Authentication - TACACS+, RADIUS, LDAP, Active Directory, and CAC. All NIKSUN products integrate with NIKSUN NetOmni™ Full Suite for enterprise-wide data aggregation, reporting, and visualization.*

Interested in learning more?

For more information, please visit us online at niksun.com.



457 North Harrison St. • Princeton • NJ 08540 • USA
 t: +1.609.936.9999 • toll free: +1.888.504.3336
 f: +1.609.419.4260
 info@niksun.com • www.niksun.com

NIKSUN, NIKSUN Logo, and other NIKSUN marks are either registered trademarks or trademarks of NIKSUN, Inc. in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners. For more information, including a complete list of NIKSUN marks, visit NIKSUN’s website at www.niksun.com. Copyright© 2020 NIKSUN, Inc. All rights reserved. NK-DS-NetDL-0520-1.0