Virtual NetDetectorLive™

Virtual Solution for Cyber security, data leakage prevention, and real-time surveillance

Features & Benefits

- *Eliminates network blind spots with proactive monitoring of traffic within a virtual server*
- *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, etc.)*
- *Plug-and-play device with web-based intuitive user interface and role-based access control*

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 Virtual 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, Virtual 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. Virtual 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. Virtual 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.

Combine Visibility Into Both Physical and Virtual Network

Appliances can be deployed across multiple virtual servers and within a private or public cloud for complete monitoring across your virtual infrastructure, providing a total view of the virtual world, including both north-south and east-west traffic. Traffic from deployed appliances can also be pulled into NIKSUN NetOmni to present a unified view across the virtual, LAN, WAN and MAN environments.

Virtual NetDetectorLive™ monitors virtual network traffic for user-defined

and threshold-based behaviors, while packets are analyzed and compared to preset signatures. Incident alerts are linked to all packet information corresponding to an event occurrence. These alarms are available for further forensic investigation through an easy-to-use GUI that enables you to navigate anywhere with a single click.

Rule-based Content Alerts

Virtual 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.

Users also have the flexibility to categorize and define their own rules based on keywords, file names, file types, or specific field values for different applications. Exact content matching can be done on files and URLs. Sensitive documents and files can be uploaded to Virtual 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.

Package Offerings

To better meet any organization's needs, Virtual NetDetectorLive is offered in the following product forms:

Feature	Virtual NetDetectorLive Standard	Virtual 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 & 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.)		●
Real-time content-based alerts (Data Leakage Detection, etc.)		●

Technical Information

- *Database Size: 4TB / 8TB*
- *Network Interfaces Supported* - 1 Gbps / 10 Gbps
- *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.).*
- *Virtual/Cloud Support and Management - OpenStack [Kilo, Liberty, Mitaka, Newton, Ocata, Train]; KVM; VMWare ESX/ESXi [5.x, 6.x]; AWS; XEN; Hyper-V; Oracle VM*
- *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