NetDetectorLive™ Alpine

Cyber forensics

DATASHEET

Features & Benefits

- *Real-time inbound and outbound application monitoring with granular application content search*
- *Extensive set of pre-defined alerts*
- *Real-time alerts of regulatory and internal company policy violations*
- *Reconstruct application sessions and policy violations for audits and evidence*
- *Capture and store all communication sessions to search current and historic user activity*
- *Replace manual investigation processes with proactive discovery, classification and analysis of diverse applications and protocols*
- *Traffic capture and multi-timescale analysis on a variety of interfaces*
- *Role-based access control*
- *Plug-and-play device with web-based user interface*
- *Web-driven intuitive user interface*

Challenge

Targeted cyber attacks across worldwide networks have increased in sophistication as well as frequency over the past few years. Web-based cyber attacks, distributed denial-of-service (DDoS), attacks due to malicious code, and information loss due to malicious insiders, are having a huge financial impact 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 these attacks.

Solution

NIKSUN® NetDetectorLive™ Alpine 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 Alpine technology, it 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 is made immediately available for fast search and investigation. This metadata can even be stored in the NIKSUN Network Knowledge Warehouse (NKW) for long periods of time. NetDetectorLive Alpine searches through terabytes of data to return results in a fraction of the time that retrospective forensic analysis tools take, which makes it indispensable for rapid forensic investigation and risk mitigation. It alerts on suspicious traffic based on metadata content, for immediate notifications on policy violations, data exfiltration, malware and cyber attacks.

Rule-based Content Alerts

NIKSUN's NetDetectorLive Alpine is pre-packaged with an extensive set of robust, pre-defined 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.

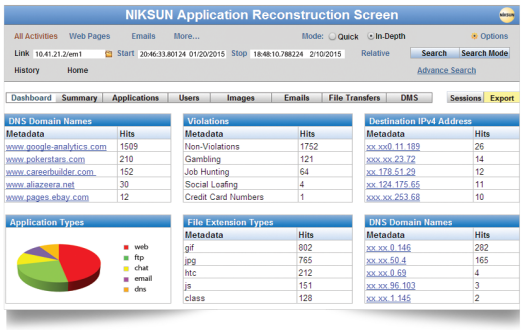
More importantly, users have the flexibility to define and categorize their own rules. Rules can be defined on keywords, file names, file types, or specific field values for email and chat applications. Exact content matching can be done on files and URLs. Sensitive documents and files can be uploaded 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 Alpine immediately generates an event alert. 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.

Application Reconstruction

NetDetectorLive Alpine reconstructs and stores application data in real-time while monitoring network data, making it capable of extremely fast forensics. Users can dive into massive amounts of network traffic to return information of interest in just seconds. Exact web, chat, email, FTP and other TCP/IP sessions are regenerated, allowing security administrators to see *when, what, who* and *how* a breach occurred. Non-compliant sessions can be reconstructed as is and presented as proof of a policy violation. In-depth analysis can be done on information of interest using available retrospective analysis methods.



Application Reconstruction

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, ISO8583, FIX, GTP, SIP, CDMA2000, RADIUS, Diameter and others as well.

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 and Active Directory. 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*.

100 Nassau Park Blvd • 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

About NIKSUN, Inc. NIKSUN is the recognized worldwide leader in making the Unknown Known. The company develops a highly scalable array of real time and forensics-based cyber security and performance management solutions for large enterprises, government & intelligence agencies, service providers and financial services companies. NIKSUN's award winning enterprise solutions deliver unprecedented flexibility and packet capture power. The company's patented real-time analysis and recording technology is the industry's most comprehensive solution for secure and reliable network infrastructure and services. NIKSUN, headquartered in Princeton, New Jersey, has sales offices and distributors throughout the US, Europe, the Mid East and Asia-Pacific. For more information, please visit www.niksun.com.

NK-DS-NetDL-0215