Virtual NetDetectorLive™

Virtual Solution for Cyber Security, Data Leakage Prevention, and Real-time Surveillance

DATASHEET

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 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*
- *Long-term storage of metadata in the NIKSUN Knowledge Warehouse (NKW)*

Challenge

The benefits associated with virtualization have led to the proliferation of virtual networks and the explosion of cloud computing. Both public and private clouds that share infrastructure present new security problems, which have complicated the deployment of otherwise appealing new technologies. Total visibility into the virtual network infrastructure and cloud environments, in terms of proactive monitoring and security of virtualized network functions, is just as critical as insight into the physical network. Cyber security problems are just as real but more difficult to diagnose.

Targeted cyber attacks across global networks have increased in impact as well as frequency. Web-based cyber attacks, distributed denial-of-service (DDoS) attacks, attacks 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

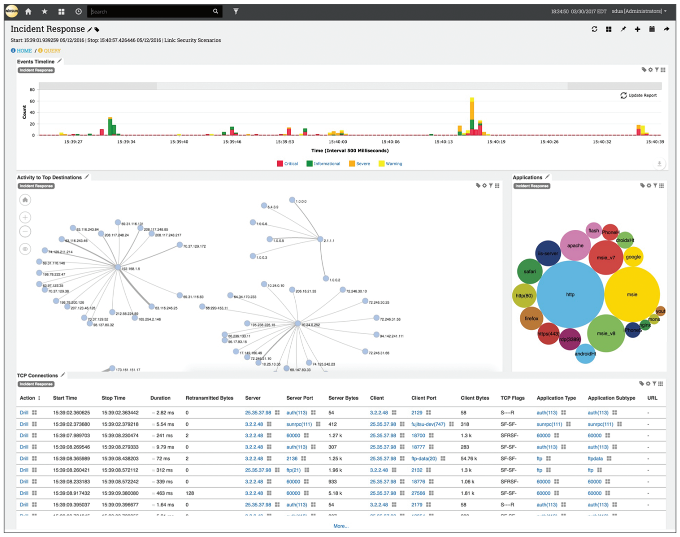
NIKSUN's Virtual NetDetectorLive is a real-time data capture and analysis solution that fits right into your virtual environment. It is equipped with the same uniquely powerful, award-winning NIKSUN technology that is available in NIKSUN's flagship NetDetectorLive appliance. It is uniquely capable of super fast forensics search, session reconstruction, and real-time detection of data leakage and security violations, bringing today's most advanced network forensic tools into virtual and cloud environments.

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. This metadata is made immediately available for fast search and investigation. 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. It alerts on suspicious traffic based on metadata content, for immediate notifications on policy violations, data exfiltration, malware and cyber attacks.

Combine Visibility Into Both Physical and Virtual Network

NIKSUN's Virtual NetDetectorLive is a real-time data capture and analysis solution that fits right into your virtual environment. It is equipped with the same uniquely powerful, award-winning NIKSUN technology that is available in NIKSUN's flagship NetDetectorLive appliance. It is uniquely capable of super fast forensics search, session reconstruction, and real-time detection of data leakage and security violations, bringing today's most advanced network forensic tools into virtual and cloud environments.

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. This metadata is made immediately available for fast search and investigation. 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. It alerts on suspicious traffic based on metadata content, for immediate notifications on policy violations, data exfiltration, malware and cyber attacks.



Incident Response

Start: 15:39:01.939259 05/12/2016 | Stop: 15:40:57.426446 05/12/2016 | Link: Security Scenarios

Action	Start Time	Stop Time	Duration	Retransmitted Bytes	Server	Server Port	Server Bytes	Client	Client Port	Client Bytes	TCP Flags	Application Type	Application Subtype	URL
Drill	15:39:02.360625	15:39:02.363442	≈ 2.82 ms	0	25.35.37.98	auth(113)	54	3.2.2.48	2129	58	S----R	auth(113)	auth(113)	-
Drill	15:39:02.373680	15:39:02.379218	≈ 5.54 ms	0	3.2.2.48	sunrpc(111)	412	25.35.37.98	fujitsu-dev(747)	318	SF-SF-	sunrpc(111)	sunrpc(111)	-
Drill	15:39:07.989703	15:39:08.230474	≈ 241 ms	2	3.2.2.48	60000	1.27 k	25.35.37.98	18700	1.3 k	SFRSF-	60000	60000	-
Drill	15:39:08.269546	15:39:08.279333	≈ 9.79 ms	0	3.2.2.48	auth(113)	307	25.35.37.98	18777	283	SF-SF-	auth(113)	auth(113)	-
Drill	15:39:08.365989	15:39:08.438203	≈ 72 ms	2	3.2.2.48	2136	1.25 k	25.35.37.98	ftp-data(20)	54.76 k	SF-SF-	ftp	ftpdata	-
Drill	15:39:08.260421	15:39:08.572112	≈ 312 ms	0	25.35.37.98	ftp(21)	1.96 k	3.2.2.48	2132	1.3 k	SF-SF-	ftp	ftp	-
Drill	15:39:08.233183	15:39:08.572242	≈ 339 ms	0	3.2.2.48	60000	933	25.35.37.98	18776	1.06 k	SFRSF-	60000	60000	-
Drill	15:39:08.917432	15:39:09.380080	≈ 463 ms	128	3.2.2.48	60000	5.18 k	25.35.37.98	27566	1.81 k	SF-SF-	60000	60000	-
Drill	15:39:09.395037	15:39:09.396677	≈ 1.64 ms	0	25.35.37.98	auth(113)	54	3.2.2.48	2179	58	S----R	auth(113)	auth(113)	-

Security Overview Report

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 and the download of steganography or 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 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. Precise, real-time content matching can be done on files and URLs to detect leakage of classified information and other instances of non-compliance.

Incident Response / Application Forensics

Virtual NetDetectorLive 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. Additionally, 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.

Technical Information

Models: Virtual NetDetectorLive

Database Size: 4 TB / 8 TB

Network Interface: 1 Gbps / 10 Gbps

Scalability: Unlimited instances for continuous growth and scalability

Virtual/Cloud Support and Management: OpenStack [Kilo, Liberty, Mitaka, Newton, Ocata]; KVM; VMWare ESX/ESXi [4.x, 5.x, 6.x]; AWS; XEN; Hyper-V; Oracle VM

Applications Reconstructed: Several hundred, including voice, video, web, FTP file transfers, chats, email, images, NetBIOS, IRC, DNS, wireless (LTE, CDMA2000, IMS), and desktop applications (Microsoft, Adobe, etc.).

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

NIKSUN®

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

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.