Virtual NetDetector™

Comprehensive and Actionable Solution for Securing Virtual Networks

DATASHEET

Features & Benefits

- *Lossless full packet capture (FPC) through 10 Gbps, chosen by the U.S. Department of Defense (DoD)*
- *Eliminates network blind spots with proactive monitoring of traffic within a virtual server*
- *Forensics: Application Reconstruction, metadata analytics, artifact extraction, and Sandbox*
- *Threat Intelligence: Replace manual investigation processes with automated proactive discovery, including support for STIX/TAXII*
- *IDS: Integrated signature detection with retrospective analysis*
- *Anomaly Detection: detect anomalous traffic patterns such as covert channels, port scans, or DDoS attacks*
- *Application Recognition: Classify and analyze many applications based on content*
- *Geo IP analytics and alerting: Upload custom GeoIP mappings*
- *Detailed Analytics and Alerts for DNS and other protocols*
- *Intuitive and powerful UI: "google-like" interface for actionable intelligence*
- *On-demand and scheduled reporting on multiple timescales*
- *Support for lawful intercept*
- *Seamless integration with SIEM for network-wide monitoring and incident response*

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.

Solution

NIKSUN's Virtual NetDetector 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 NetDetector appliance. It offers full packet capture and network security analysis for total visibility, bringing today's most advanced network forensic tools into virtual and cloud environments. NIKSUN is the only security monitoring solution that integrates signature-based IDS functionality with statistical anomaly detection, analytics and deep forensics with full-application reconstruction, and packet level decodes. Users are informed of security breaches and attacks as they occur and can initiate interdiction actions to prevent malicious traffic from entering the network. Users can quickly answer critical questions such as how a breach occurred, what data was exfiltrated, what was compromised, who was affected, and what corrective measures need to be initiated. Data from distributed physical and virtual appliances can be aggregated and viewed on a central NetOmni™ console, not only for an easy-to-access unified view but also for more effective security management.

Dynamic Application Recognition and Plug-ins

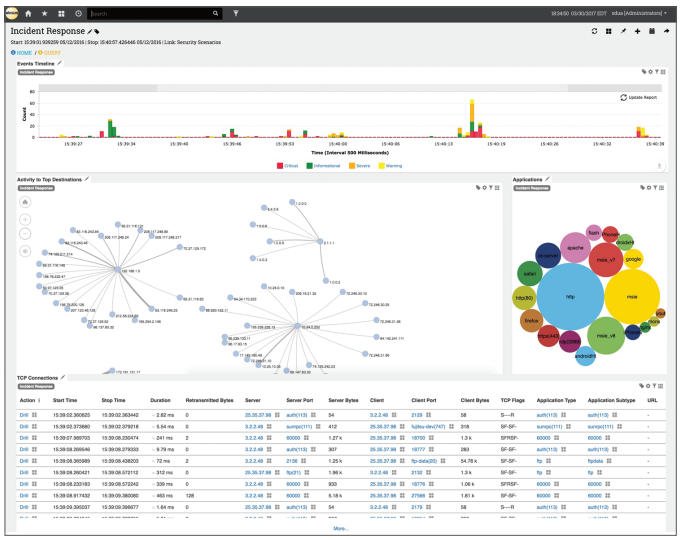
By utilizing the same highly robust NikOS Everest architecture as is available for NIKSUN's flagship appliances, Virtual NetDetector further improves modularity and scalability by using the Dynamic Application Recognition (DAR) mechanism and plug-in framework for network traffic recognition and processing. Port-based or TCP-based classification methods are insufficient to accurately identify the different types of traffic. The DAR recognition mechanism uniquely recognizes applications using signatures based on the payload as well as header information, providing the ability to identify rogue applications and malware.

Integrated Anomaly and Signature-based IDS

Virtual NetDetector offers an integrated anomaly and signature-based IDS solution for fast and accurate detection of intrusions. The anomaly-based detection utilizes user-defined and threshold-based anomalies. Apart from guarding proactively against new threats, integrated detection capabilities can be used retroactively on already captured traffic to identify existing victims of cyber attacks and discover the impact of newly identified zero-day attacks.

Application Forensics and Session Reconstruction

The application and session reconstruction feature provides the deepest forensics with hundreds of types of metadata. A network security analyst keen on quickly parsing through terabytes of data can utilize the new GUI in NikOS Everest for both fast reconstruction and in-depth forensics. Files and potential malware can be extracted from traffic and immediately sent to a Sandbox for inspection and confirmation right in NikOS Everest. Full reconstruction of numerous protocol exchanges comes standard with NIKSUN Virtual NetDetector. This enables users to quickly and easily detect interactions with blacklisted websites, which is often a precursor to sophisticated cyber attacks. It also allows the user to discover non-compliant traffic such as outdated SSL ciphers and engage in root-cause analysis of DDoS attacks.



Security Overview Report

Combine Visibility Into Both Physical/Virtual Networks

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.

Cloud or virtual servers face the same security hazards as physical servers. As traffic between virtual servers or within the cloud is isolated from the physical network, having a holistic detection system residing within those environments is essential to counteract threats. Virtual NetDetector™ 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. The NIKSUN Network Knowledge Warehouse (NKW) stores the indexed packets and provides the necessary data to reconstruct any incident and quickly analyze the traffic within the virtual network.

Technical Information

Models: Virtual NetDetector

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

Supported Protocols: 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, MSSQL, Oracle QinQ, Multicast, ISO8583, FIX, GTP, SIP, CDMA 2000, RADIUS, Diameter and many more

Integration: Authentication - TACACS+, RADIUS, CAC, LDAP and Active Directory. Sandbox, syslog, SNMP v2 & v3, email, bidirectional SIEM. All NIKSUN products integrate with NIKSUN NetOmni™ Full Suite for enterprise-wide 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

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.