NIKSUN

Virtual NetDetector™

Comprehensive and Actionable Solution for Securing Virtual Networks

Features & Benefits

» *Eliminates network blind spots with proactive monitoring of traffic within a virtual server*

» *Lossless full packet capture (FPC): known for not dropping packets; chosen by the U.S. Government Department of Defense (DoD) for FPC up to and exceeding 100 Gbps system throughput*

» *Awarded Common Criteria Certification by the National Information Assurance Partnership (NIAP) which is operated by the National Security Agency*

» *Real-time alerts of different IOCs, regulatory and internal company policy violations*

» *Rich Executive Dashboards and comprehensive reports for automated and optimized workflows*

» *Forensics: Advanced analytics for granular forensic analysis, including Application Reconstruction and artifact extraction*

» *Threat Intelligence: Ability to ingest NIKSUN out of the box and third party threat feeds*

» *Integrated Signature & Anomaly based detection with retrospective analysis*

» *Application Recognition: Classify and analyze many applications based on content*

» *Intuitive and powerful UI: "google- like" interface for actionable intelligence; Ingest, correlate and search a wide variety of data for Indicators of Compromise*

» *Plug-and-play device with web-based intuitive user interface and role-based access control (RBAC)*

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 NetDetector is a full-featured appliance for network security monitoring built on NIKSUN's award-winning NikOS architecture. It is the only security monitoring appliance that integrates signature-based IDS functionality with statistical anomaly detection, analytics and deep forensics with full-application reconstruction and packet level decodes. Recognized as the industry's best security monitoring and forensics appliance to safeguard against increasingly sophisticated cyber attacks.

Users are informed of security breaches and attacks as they occur and can automatically initiate interdiction actions to prevent the 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.
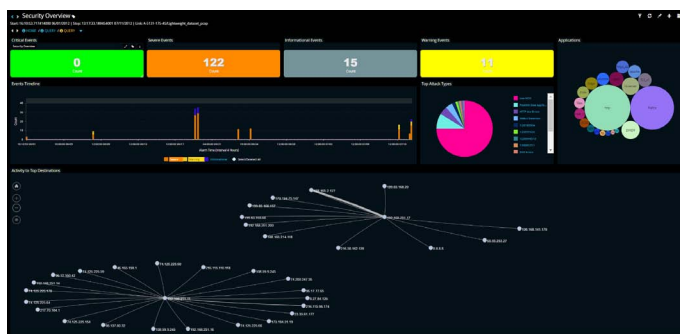
Security Overview

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. Virual 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.

Dynamic Application Recognition and Plug-ins

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 all rogue applications and malware.

Integrated Anomaly and Signature-based IDS

NIKSUN NikOS Everest Virtual NetDetector offers an integrated anomaly and signature-based IDS solution for fast and accurate detection of intrusions and zero-day attacks. 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.

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. Full reconstruction of DNS protocol exchanges comes standard with the Virtual NetDetector. This enables users to quickly and easily detect interactions with blacklisted DNS servers, which is often a precursor to sophisticated cyber attacks. It also provides faster tracing of occurrences of DNS spoofing or DNS Denial of Service attacks.
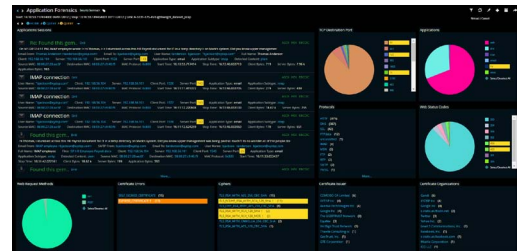
Application Forensics

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