NetDetector® Alpine

Comprehensive and actionable solution for securing networks

DATASHEET

Features & Benefits

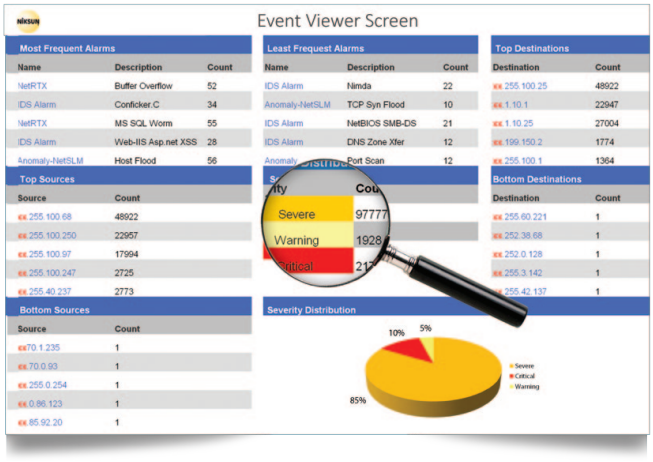
- *Comprehensive big data security intelligence*
- *Ingest, correlate and search a wide variety of data for indicators of compromise*
- *Reconstruct applications and sessions for accurate attribution*
- *Replace manual investigation processes with proactive discovery, classification and analysis of diverse applications of protocols*
- *Integrated anomaly and signature IDS detection*
- *Traffic capture and multi-timescale analysis on a variety of interfaces and over 100Gbps system throughput*
- *Intelligent interception of malicious traffic*
- *Reconstruct applications & TCP sessions for forensic analysis and evidence through context-preserving GUI tabs*
- *Drill-down to packet level information for granular forensic analysis*
- *Ad-hoc and scheduled reporting on multiple timescales*
- *Support for lawful intercept and CALEA*
- *Plug-and-play device with intuitive web-based interface & Role-based Access Control (RBAC)*
- *Seamless integration with NIKSUN NetOmni for network-wide monitoring*

Challenge

The threat of a catastrophic cyber attack is real. Insider threats, zero-day exploits, malware, advanced persistent threats (APTs), and other cyber attacks are now occurring on an unprecedented scale with extraordinary sophistication. Because security threats are becoming more damaging and difficult to foresee, forestall and recover from, it is essential to maintain continuous visibility into networks and use advanced forensic analysis to thwart attacks.

Solution

NIKSUN® NetDetector® is a full-featured appliance for network security monitoring built on NIKSUN's award-winning Alpine 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. It is 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.



Event Viewer Screen

Dynamic Application Recognition and Plug-ins

NetDetector Alpine further improves modularity and scalability by using the new 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

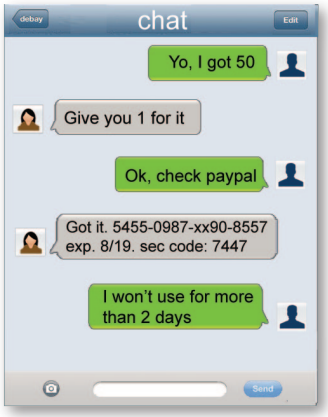
NetDetector Alpine offers an integrated anomaly and signature-based IDS for fast and accurate detection of intrusions and zero-day attacks. The anomaly-based detection utilizes user-defined and threshold-based anomalies. Apart from guarding proactively against new threats, integrated detection capabilities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

Application and Session Reconstruction

The application and session reconstruction feature provides the deepest and fastest forensics with hundreds of types of metadata. A network security analyst keen on quickly parsing through terabytes of data can utilize Quick Mode for fast reconstruction, while Full Mode can be used for in-depth forensics. Full reconstruction of DNS protocol exchanges is available in NetDetector Alpine. 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.

100Gbps Full Packet Capture and Analysis

Recognizing the increasing use of 10Gbps and 40Gbps interfaces in customer networks, NIKSUN has evolved the NetDetector appliance to support these interfaces as well. NIKSUN goes beyond just supporting these high-speed interfaces by providing full packet capture, recording and analysis at system throughputs exceeding 100Gbps.



Chat 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), MPLS, VLAN (ISI, 802.1q and stacked 802.1q), DNS, ISO8583, FIX, GTP, SIP, CDMA 2000, RADIUS, Diameter 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, CDMA 2000, 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-NetD-0215