








NetDetector®

Comprehensive & Actionable Solution for Securing Networks

 <p>Protect intellectual property from information leaks and theft</p>	 <p>Clear understanding of the how, what, when and what else of security events</p>	 <p>Maintain governance over business assets and procedures</p>	 <p>Complete protection against hacks, DoS attacks, breaches and malicious vulnerability exploits</p>	 <p>Assess risk as per actual network history spanning months with NetDetector's unlimited storage option</p>
---	---	---	--	---

Features & Benefits

- Capture intrusions the first time, as they occur
- Integrated anomaly and signature IDS
- Drill-down to packet-level information for granular forensic analysis
- Replace manual investigation processes with proactive discovery, classification and analysis of diverse applications and protocols
- Option to reconstruct application sessions and security breaches for forensic analysis and evidence
- Traffic capture and multi-time-scale analysis on a variety of interfaces such as Ethernet (10/100/1000/10000 Mbps), ATM (OC3/OC12), POS (OC3/OC12/OC48), etc.
- Ad-hoc and scheduled reporting on multiple time scales (sub-milliseconds to months)
- Support for lawful intercept and CALEA
- Plug & Play device with intuitive web-based interface & Role Based Access Control

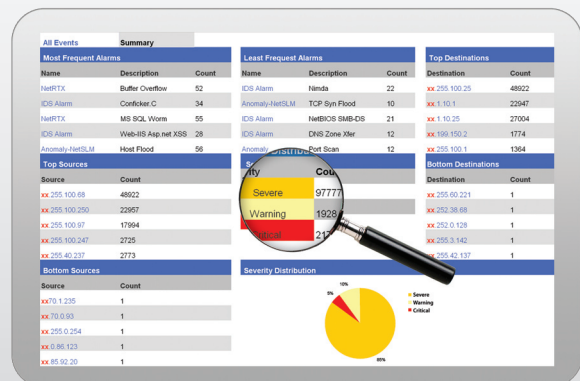
Network security today is a delicate balance between technology, best practices and an ongoing understanding of who is accessing data and what they are doing with it. With security threats becoming more damaging and difficult to foresee, forestall and recover from, it is essential to maintain continuous visibility into enterprise networks and use advanced forensic analysis intelligence to fight off attacks, perpetuate sensory recognition and memory of network incidents for high levels of network insight and evidence of malicious events.

Proactive Network Surveillance Solution

NIKSUN's NetDetector is an appliance-based network security solution that integrates several critical security functions into a single architecture. It is, all at once, a traffic capturing, forensic analysis and security reporting device that continuously surveys the network in real-time and at line speeds to gather and analyze every packet on the network. Users are informed of security breaches, intrusions, anomalies, data leaks and attacks *as they occur*. More than just a simple IDS, NetDetector is an analyzer that never forgets. It quickly answers critical questions such as *how a breach occurred, what are the consequences of a hack, precisely what was compromised, who was affected, why it occurred and how corrective measures may be initiated*.

Anomaly & Intrusion Detection

NetDetector integrates both anomaly and intrusion detection into one platform to safeguard the network with fewer false positives. Besides standard signature based intrusion detection, NetDetector also monitors the network for user-defined and threshold-based anomalies. Providing high customization options and integration with a variety of SIEM applications, NetDetector can be configured to any environment for a full suite of complementary detection methods.



NetDetector Event Viewer Summary of Alarms

Continuous Traffic Capture & Inbound/Outbound Forensic Analysis

All network applications, services and underlying infrastructure are constantly under surveillance over the link that the NIKSUN appliance is tapped into. It is possible to monitor multiple servers and network segments via a single appliance. All inbound and outbound packets are captured, time-stamped and indexed using NIKSUN's patented technology into the NIKSUN Network Knowledge Warehouse. Packets are simultaneously analyzed and compared to preset signature and anomaly definitions; as soon as an anomaly in network traffic is detected an alert is immediately sent out to the user. Incident alerts are directly linked to all packet information corresponding to the event; administrators only have to click a mouse to initiate the investigation process and determine root-cause. With NetDetector and its embedded NIKSUN Network Knowledge Warehouse, it is extremely simple to precisely determine the extent of a security breach, the information or systems compromised, files transmitted and applications affected.

TCP Sessions & Application Reconstruction

With its indexed database, NetDetector equips users with the unique capability to trace and reconstruct attacks exactly as they were executed- keystroke by keystroke, packet by packet- and determine the exact origin, path of progression and time of the attack along with insight into the vulnerabilities exploited. Reconstruction is highly useful for audits or to produce evidence of breaches in a court of law. It also supports lawful intercept and CALEA.

Participants	Instant Messaging
dtmqxx20	Yo, I got 50
y2k67xx6	I can give you 1 for it
dtmqxx20	Ok. check paypal
y2k67xx6	Got it. 5455-0987-xx90-8557
dtmqxx20	What is the expiration day?
y2k67xx6	It is 08/09
dtmqxx20	I need the 4 digit codes as well
y2k67xx6	7447
dtmqxx20	How many days
y2k67xx6	I won't use for more than 2 days

NetDetector Application Reconstruction

Other Integrated Capabilities

NetDetector facilitates highly customizable on-demand and scheduled reporting in multiple time frames- from sub-milliseconds to months. Forensic reports can be exported to a variety of preferred formats and documented for reference, evidence and analysis. An integrated web-based console makes the entire process of security investigation very intuitive, significantly reducing training and human resource costs. Optional pre-configured NetXperts scripts facilitate automated analysis. Scripts can also be assigned to initiate response-actions to standard events. Integration with third party SEIM solutions allows cooperation and consistency within enterprise-wide operations and procedures.

Technical Information

Network Interfaces supported (Full Duplex, Half Duplex): 10GigE, 10/100/1000 Mbps (copper/fiber), T1/E1, V.35, X.21, T3/E3, HSSI, OC3, OC12, OC48

Protocols Supported: TCP/IP, UDP/IP, IPv6, IPv4, Ethernet MPLS, Frame Relay, PPP, Bay PPP, CISCO HDLC, PoS (OC3/OC12/OC48), ATM (OC3/OC12), MLPP, WCP, STAC, VLAN (ISL & IEEE 802.1q), IEEE 802.3 (Ethernet), IP fragments

Form Factors: A variety of 1U and 2U form factors are available for data centers, core networks, central offices and remote branch applications. Internal storage scales to several terabytes. Unlimited external storage option available.

Integration: TACACS+, RADIUS, LDAP, Active Directory and various network performance and security tools (SEIM, NMS)



100 Nassau Park Blvd
Princeton
NJ 08540
t: +1.609.936.9999
toll free: +1.888.504.3336
f: +1.609.419.4260
info@niksun.com
www.niksun.com



About NIKSUN: NIKSUN is the premier provider of patented multi-timescale network and security monitoring and real-time analysis solutions that identify, alert, analyze and report on incidents that impact performance, security, compliance applications and services. NIKSUN's NetOmni Suite is the only technology available today that offers large organizations the ability to consolidate views into globally distributed high-speed covered networks according to user responsibilities. NIKSUN empowers organizations to make fast, accurate decisions that assure network performance, security and compliance goals are met and data integrity is protected.

NIKSUN, the NIKSUN logo, NetDetector, NetVCR, NetVoice are either registered trademarks or trademarks of NIKSUN, Inc. in the United States and/or other countries. Other product & company names mentioned herein may be trademarks of their respective owners. NIKSUN, Inc. shall not be liable for damages of any kind for use of this information, which is subject to change without notice and may include typographical errors, inconsistencies, omissions, mistakes, etc. Copyright© 2009 NIKSUN, Inc. All rights reserved. NK-DS-ND09.05