

**NIKSUN**

# NetDetectorLive™ Cybersecurity

## Cyber Forensics



Detect and deter cyber security attacks and discover yet unknown methods of breach



Protect confidential data from information leaks, theft, unauthorized access, insider threats and abuse



Check for compliance and adherence to acceptable use policies and regulatory compliance



Lawful intercept for CALEA; reproduce non-tampered network events as evidence to facilitate audits, investigations, etc.



Clear understanding of the when, what, what else, how of non-compliant network events

### Challenge

Cyber threats are one of the leading concerns for governments across the world in their homeland security initiatives. Many have recognized the need to reduce the vulnerabilities in national critical cyber infrastructure as one of their top security concerns. Various cybersecurity measures have been adopted in the past, but quite a number of these past initiatives have failed to yield successful results. It is now clear that cybersecurity risks cannot be avoided and that tools and solutions (along with processes and personnel) are needed to manage and contain the risks that exist perpetually.

Cybersecurity risks are constantly changing and newer techniques are being exploited by cyber terrorists and criminals faster than detection and avoidance techniques can be developed. Law enforcement agencies are finding themselves severely handicapped in tracking and tracing the activities of those hiding behind a web of computers and internet nodes. As such, governments and large organizations are highly concerned about the possibility of large-scale disruption that may be unleashed by rogue nations or terrorist organizations bent on creating havoc and chaos.

### Solution

NIKSUN's NetDetectorLive provides real-time surveillance over IP networks and has the capability to monitor all of the data flowing across the network. NetDetectorLive also does content inspection to provide visibility and control over how vulnerabilities are being exploited or how sensitive/confidential information is being breached. Besides content inspection, NetDetectorLive creates metadata on all content for easy search and inspection minutes to years after an event. This rich metadata allows for each search and reconstruction of events and contents triggering the events. This metadata along with content categorization allows for accurate and simplified analysis into the complete activity of criminal or subversive organizations.

### How it Works

NetDetectorLive constantly records and matches the content of all or a user defined filtered subset (i.e. adhering to a policy for surveillance) of applications communicating on the network. NetDetectorLive metadata is then warehoused in the NIKSUN Knowledge Warehouse (NKW). Each user can be provided appropriate access controls for accessing specific pieces of information. These users can easily search the NKW or apply a search to actual raw packet data that is warehoused for deep forensic analysis. The search tool is similar to web based search tools such as Google hence it does not require any special training.

In addition, users may define content and transaction inspection categories in NetDetectorLive such that if specific events match the category definition, they are then tagged and warehoused. This categorization allows for not only easy search by specific categories such as "worms", "back doors", "policy violations", "data leaks", "pornography" etc. but also for real-time alerting when events match specific categories.

The real-time event generation capability of NetDetectorLive can be useful for time-sensitive surveillance and monitoring operations such as cybersecurity emergency response teams. On detection of a violation, NetDetectorLive generates immediate alarms that identify anomalous events. The linking of the event to the sessions down to packet level information enables rapid forensic investigations.

NetDetectorLive provides a clear path to understand the reason behind a security/policy breach and provides complete information for intelligence. In addition NetDetectorLive provides the context within which it occurred. NetDetectorLive's reconstruction capability allows it to analyze how, why and with what intent it occurred. Because all network activity including packets, sessions and applications are searchable, time-stamped and stored in the NKW, it becomes very easy to identify information such as: which user(s) were involved, what information was moved, whether it left the network, to whom it was sent and whether the event was malicious or not.

## Features & Benefits

### Information Protection

Governments would like to protect critical information from getting into the hands of anyone who is not authorized to have that information. NIKSUN NetDetectorLive defends against leaks for sensitive content and confidential information to criminals, spies or other external sources via internet services such as web, email, ftp, telnet or chat etc. NetDetectorLive categorizes sessions based on content and matches against rule sets to provide proactive alerts on information leakage. Because new methods of leaking information are always being discovered, NetDetectorLive also keeps records of all content (per the policy of the organization) which can be searched in case any breach is discovered.

### Protection of Critical Infrastructure

One of the primary goals of government agencies and large organizations is to block intrusions and stop the hijacking of computers used for breaching and attacking national infrastructure, weapons systems and their operations. In addition, the goal of this activity is to identify and bring to justice those responsible. If hackers were to get a hold of such control systems, they can wreak havoc with national electrical grids, power (or energy) generation systems, remote weapons systems, financial systems, transportation systems, dams and bridges, treasury, remote environment sensing and alerting systems, etc. Having the ability to increase knowledge of the tactics and methods of attack being tried by terrorists before they are able to succeed has proven to be extremely valuable. NIKSUN NetDetectorLive's Violation Event Viewer provides easy access to the breach alerts and their corresponding data. In addition, the NetDetectorLive's Google like search feature and reconstruction capability provides an easy and fast way to sift through large amount of data quickly and efficiently to spot malicious activity.

### Application Reconstruction

Besides searching network application content for sensitive information, on the occurrence of an anomalous incident a user has the option to reconstruct the application session within which the anomaly transpired. NetDetectorLive can regenerate exact web, chat, email, FTP and other TCP/IP sessions, within the policy of local environments. When the consequence of an incident is likely to be deliberated within a court of law, or before an authoritative body (for example: a human resources audit), the information within the NIKSUN Network Knowledge Warehouse can be presented not only as metadata but also as an exact replication of the incident itself. Incompliant email, chat, web and other TCP/IP sessions can be reconstructed exactly as they occurred, allowing security administrators to see precisely what the violator had on their screens, as proof of a policy violation. NetDetectorLive's ability to record incidents and present them as irrefutable evidence of the truth has proved to be of great value to customers, providing a basis for lawful action, non-repudiation and protecting the image of businesses in the face of society.

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 converged 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© 2010 NIKSUN. All rights reserved. NK-DS-NDL10.1