NIKSUN, the leader in real-time deep forensic analysis, has integrated its NetDetector Alpine, NetDetectorLive, and NetOmni 4.3.1 security products with McAfee® Network Security Platform 7.5. NIKSUN's NetDetector/NetDetectorLive expands security monitoring by combining signature-based intrusion detection system (IDS) functionality with statistical anomaly detection, analytics, and deep forensics with web reconstruction and packet-level decodes. Now you can leverage the industry's best security monitoring and forensics appliance to safeguard against increasingly sophisticated cyberattacks.

Business Problem

Today's enterprise networks are under constant threat. Recent news stories detail how attackers compromise internal systems, exploiting vulnerabilities inherent in both software and hardware and inflicting both financial and reputational damage on a multinational scale. Having an infrastructure that supports a wide variety of tools that are too narrowly focused introduces vast inefficiencies to detection and alerting when threats are present. Knowing that an attack is underway is just the first step. Learning about the nature of the threat and how it evolves is at the heart of preventing future threats. Enter McAfee and NIKSUN.

NIKSUN Solution Overview

NIKSUN's enterprise solution, NetOmni, and flagship appliances NetDetector/NetDetectorLive capture, timestamp, and index all data traversing your IP infrastructure into a statistical, full-packet warehouse. When a security event occurs, you can directly trigger a rich retrospective time-lapse view of the attack across your infrastructure. McAfee has partnered with NIKSUN to offer mutual customers unprecedented forensics. Leveraging the integration with NIKSUN, you can lock on to an event of interest and directly query all data flows from the last few minutes, hours, or days—all with nanosecond precision. The comprehensive data-mining capability provided by the NIKSUN Knowledge Warehouse (NKW) enables quick identification, isolation, and retrieval of pertinent information for analysis. There is no need to manually parse through streams of traffic data to find relevant information. Instead, the NIKSUN NetDetector allows you to directly access corresponding statistical and full-packet data for convenient forensic analysis and minimal mean time to resolution. NIKSUN's powerful data-mining, replay, reconstruction, and forensics capabilities enable rapid determination of the root cause of your security incidents, eliminating guesswork.

Based on NIKSUN's next-generation Alpine technology, NetDetector and NetDetectorLive monitor all data flowing across the IP infrastructure at true 100 Gbps speeds and use deep packet inspection to accurately recognize, classify, and analyze all applications, sessions, and content traversing your infrastructure. Metadata is created in real time on all content, including email, instant messaging (IM), FTP, and HTTP and is made immediately available for fast search and investigation. Offering petabytes of data storage, NetDetector is indispensable for rapid forensic investigation and risk mitigation. Its application reconstruction capability allows users to exact web, chat, email, FTP, and other TCP/IP sessions, with content to be regenerated, allowing security administrators to see when and how a breach occurred.
**Joint Solution**

McAfee Network Threat Behavior Analysis, an integrated component of McAfee Network Security Platform, provides real-time visibility and threat protection of the network infrastructure. Integration of NIKSUN NetDetector, NetDetectorLive, or NetOmni with McAfee Threat Behavior Analysis shows how quickly you can move from receiving alerts on suspicious behavior to full comprehensive views of attack vectors. Leveraging NetDetector’s packet bounce diagram, you can view the path the attack took through your network. You will discover exactly what data was compromised and how with NIKSUN’s Dynamic Application Recognition (DAR) mechanism and plug-in framework for network traffic recognition and processing. The DAR mechanism uniquely recognizes applications using signatures based on the payload, as well as header information, giving you the ability to identify all rogue applications. Application and session reconstruction features provide the deepest and fastest forensics with hundreds of types of metadata, including DNS (answer, data types, query, resolver, and response codes), secure sockets layer (SSL) certificates (Certificate Issuing Authority, SSL cypher, certificate error), and other third-party data. This enables you to quickly and easily detect interactions with black-listed DNS servers, which are often precursors to sophisticated cyberattacks. It also provides faster tracing of occurrences of DNS spoofing or DNS denial-of-service attacks (DoS).

**Key Benefits**

- With the point-click-analyze capability, you can quickly launch NIKSUN analytics straight from the McAfee Threat Behavior Analysis screen.
- User-controllable parameters for flexible access to real-time from full-packet storage for root cause identification and retrospective analysis.
- Search by attack time, SRC, or DEST IP address, port, and application protocol.

**About NIKSUN**

NIKSUN is the recognized worldwide leader in making the unknown known. The company develops a highly scalable array of real-time and forensics-based cybersecurity and performance management solutions for large enterprises, government and 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 Middle East and Asia-Pacific. For more information, please visit [www.niksun.com](http://www.niksun.com).
About McAfee Network Security Platform

McAfee Network Security Platform is a uniquely intelligent security solution that discovers and blocks sophisticated threats in the network. Using advanced threat detection techniques, it moves beyond mere pattern matching to defend against stealthy attacks with extreme accuracy, while its next-generation hardware platform scales to speeds of more than 80 Gbps to meet the needs of demanding networks.

McAfee Network Threat Behavior Analysis seamlessly integrates with the McAfee Network Security Platform intrusion prevention system for a comprehensive and robust security infrastructure. McAfee Network Threat Behavior Analysis collects and analyzes traffic from the entire network—host and applications—to detect worms, botnets, zero-day threats, spam, and reconnaissance attacks. It reports any unusual behavior to help you maintain a comprehensive and efficient network security infrastructure. It comes fully equipped with quad-core processors, a RAID array, distinct flow capacity, gigabit Ethernet connectivity, and offline storage area network connectivity.