

## CASE STUDY

---

### **Worldwide Telecommunications Leader: Securing and Managing the Global Networking Infrastructure**

Sponsored by: NIKSUN® Inc.

---

Charles J. Kolodgy  
July 2007

## INTRODUCTION

Drastic expansion in network reach and complexity, coupled with rising traffic volume, means that today's enterprises face a corresponding increase in the depth and breadth of network security threats. Identifying and reducing suspicious traffic, usually the harbinger of malicious intent, in such an evolving environment have become an absolute necessity for corporations, especially large international entities.

Corporations are enhancing their IP traffic by migrating to convergent and integrated IP networks that incorporate multiple applications and services, including multimedia such as voice and video. Many enterprises have not had the time or resources to build the necessary security and control systems for their networks. Issues such as permanent visibility on the network to identify events in real time are neglected. To meet this demand, innovative companies such as NIKSUN® have stepped in to offer enterprises the solutions they require.

NIKSUN®, founded in 1997, is a leading provider of scalable and integrated network security solutions. NIKSUN provides a wide range of offerings for security, forensics, compliance, network-to-application availability, and performance. For this case study, IDC interviewed a leading North American telecommunications vendor (also referred to in this case study as "the company") that has been using NIKSUN solutions since 1999. The interview took place in June 2007 with a senior networking strategist.

---

## Selection Process

In 1999, this global telecommunications company lacked efficient and continuous traffic logging, and it undertook an evaluation process for traffic logging solutions from multiple vendors. Using a set of required capabilities and features, the company conducted a thorough evaluation of competitive offerings, eventually selecting NIKSUN's Real-Time Network Surveillance Solution.

NIKSUN's solution met the network security, protection, and management requirements set forth by the company, surpassing the technology that the company had previously implemented. NIKSUN also provided a very attractive blend of tools. By opting for NIKSUN's technology, the company has its eyes and ears continuously on the network, achieving a holistic view of its global infrastructure.

---

## Implementation

The NIKSUN Real-Time Network Surveillance Solution was implemented in 1999. Today, the company uses 55 appliances or probes to cover its global network from North America to Europe and Asia. The probes are strategically located at the company's perimeter, key access points, key distribution links, and core level.

Implementation was seamless due to the plug-and-play nature of NIKSUN technology. The solution is so user friendly that end-user training was unnecessary. Early detection and isolation of worms, viruses, and other attacks on the network have allowed the company to avoid widespread infection of its machines worldwide. Catastrophic events such as those caused by self-propagating malware like Code Red or Melissa have been avoided, saving the company substantial expenses associated with recloning of infected machines and loss of employee productivity.

---

## Ongoing Operation

The company has deployed two NIKSUN products, NIKSUN NetDetector<sup>®</sup> and NIKSUN NetVCR<sup>®</sup>. Both are designed to provide end users with a holistic view of potential problem areas. This is an approach that allows for enterprise-level rather than local treatment of adverse events and incidents. The teams that use the NIKSUN products are all able to tap and use the same knowledge repository to solve problems, meeting the needs of both the team and the enterprisewide.

☒ **NIKSUN NetDetector:** This full-featured appliance provides network security surveillance, detection, analytics, and forensics. By distributing multiple units throughout the enterprise and centrally managing them along with aggregated reporting and analysis, the system offers unmatched levels of security. NetDetector acts as a security camera and motion detector for the telecommunications company's network. It continuously captures and stores network traffic, locating bits of actionable data from the large volume of raw data on the network. Alerts on specific signatures and traffic patterns are generated. NetDetector's multiple functionalities include:

- ☐ Continuous real-time surveillance
- ☐ Capture and storage of network events
- ☐ Down-to-packet-level drill-down forensic analysis
- ☐ Signature and anomaly detection
- ☐ Advanced on-demand and scheduled reporting
- ☐ Integrated event viewer

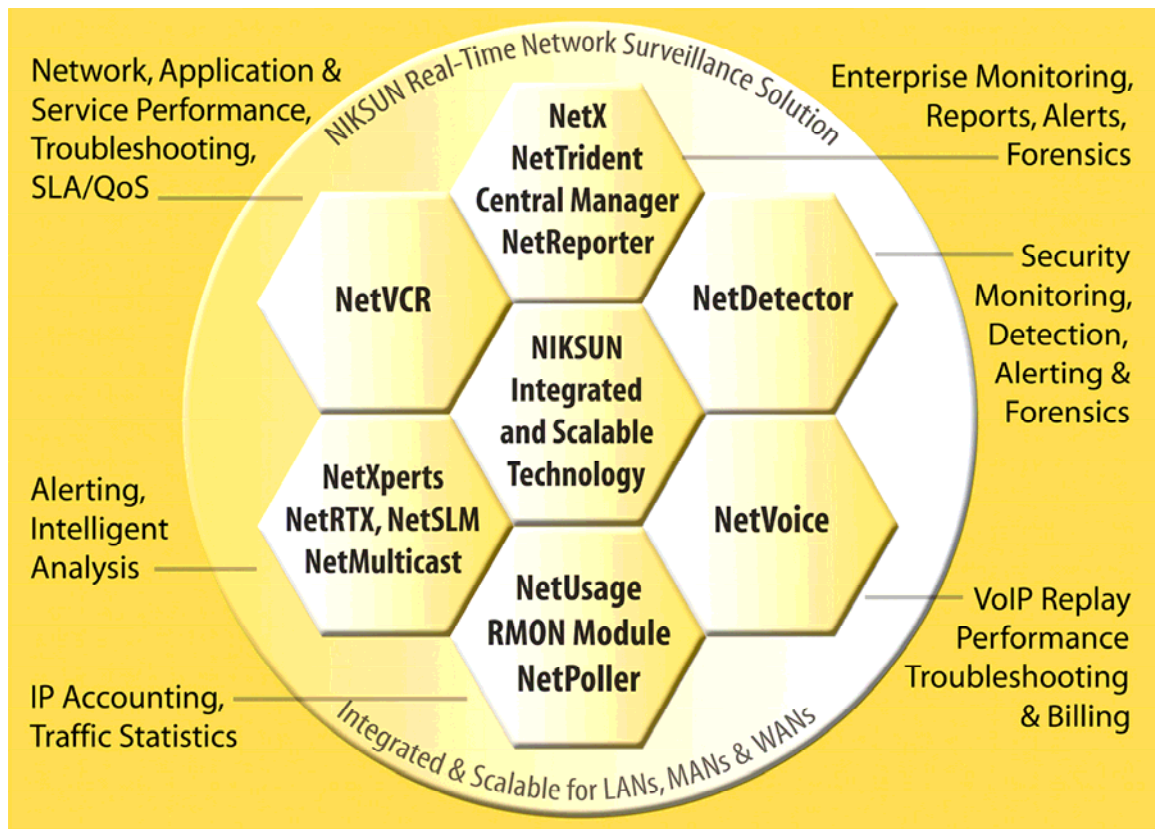
☒ **NIKSUN NetVCR:** This full-function data mining network appliance proactively alerts users to network, service, or application performance issues. It allows for remote troubleshooting through a secure Web connection. Functionalities include:

- ☐ Complete real-time visibility into the network
- ☐ Capture of network events as they occur
- ☐ End-to-end, proactive monitoring and troubleshooting of network and application performance
- ☐ Drill-down forensic analysis
- ☐ Fully integrated performance reports, both scheduled and on demand, on all traffic

Figure 1 shows the products available from NIKSUN. They are part of NIKSUN's Real-Time Network Surveillance Solution.

**FIGURE 1**

NIKSUN Real-Time Network Surveillance Solution



Source: NIKSUN, 2007

## Benefits Achieved

The network strategist IDC interviewed believes that the NIKSUN deployment has provided major benefits for managing its worldwide operations. The company is able to successfully troubleshoot network problems and automatically generate network usage reports. These reports allow the company to rapidly answer critical questions such as: Who is talking to whom on the network? How much traffic is present at a given time? Does bandwidth need to be increased or decreased in specific areas?

In 2005, the company performed a formal business analysis to determine the value derived from the probes after five years of use. By its calculations, each time a computer is infected, it costs the company an average of \$1,200 for recloning (labor, downtime, etc.). With NIKSUN, the company was able to reduce the number of machines needing recloning by 90%.

The cost savings have been substantial. Using very conservative estimates regarding the number of computers infected annually, the company cited savings of \$100,000 to \$150,000 by not having to perform triage on the infected machines. In addition, another \$500,000 to \$750,000 was saved by having the machines up and running, avoiding the loss of productivity. By having information-rich network usage reports that identify applications and services that may have configuration issues, isolate inappropriate use of the network, and determine shrinking and growing segments, a total of \$300,000 was also saved. Engineers take the report information and can make key decisions about links and circuits that need to be augmented or reduced.

Other benefits besides cost avoidance were directly tied to NIKSUN technology:

- Since NIKSUN has Snort, a leading intrusion detection system (IDS), already imbedded, the company can use it as a primary IDS.
- NISKUN appliances or probes, which are distributed throughout the company's global network, are multifunctional and handle multiple applications while only requiring a very small footprint on the network. The result is significant cost savings and simplified network management.
- NIKSUN's ability to detect anomalous traffic in a more heuristic manner allows the telecommunications company to develop replicable methods and approaches to learn about and solve problems occurring daily on its global network.
- Unlike the company's prior solution, NIKSUN required no significant amount of configuration due to its plug-and-play and ease-of-installation aspects. Once the probe is dropped into network traffic, it simply starts to record and analyze.
- NIKSUN provides the ability to manage and monitor any media types.

One of the main benefits of the NIKSUN offering is its modularity, which has allowed the company to handpick only those modules that are applicable to its requirements. The multiuse aspects of the NIKSUN solution were frequently mentioned, such as the ability to perform protocol analysis, IDS, and report generation through a single standalone appliance. An open API was also cited as a major benefit of the NISKUN solution.

The company is contemplating further investment in NIKSUN technology in the near future. It is currently in the process of testing other offerings, including NIKSUN® NetVoice®, a voice over IP (VoIP) network-management and security-monitoring solution, as well as NIKSUN® NetOmni™.

The network strategist interviewed by IDC has high praise for NIKSUN, saying "If I were building a network or if I were managing a network, I would certainly want to have NIKSUN probes in there in key locations. It is a tool that gets used everyday by our engineers, by our security staff, and by network management. So I would be hard pressed to imagine not having one, at least one deployed depending on your network and your situation."

---

## **Challenges**

As a relatively small player in the IT security field, NIKSUN must contend with many of the same challenges faced by emerging companies: gaining recognition and getting on the bid lists of prospects. Another challenge will be for a company of its size to keep up with the dynamics associated with network protocols today and in the future. These challenges are being successfully met by NIKSUN today. With the same due diligence and attention to detail that the company has shown in the past, as evidenced by customer enthusiasm for its products, it should be able to position itself for the future. IDC feels that NIKSUN products and services are well suited for the needs of many enterprises.

---

## **Summary and Recommendations**

NIKSUN offers an array of solutions that are worth an evaluation by organizations facing the challenging need for robust and secure global IP infrastructures and services.

IDC recommends that organizations first come to an understanding of the current and future requirements for their IP infrastructures and services. Building on that understanding and examining the options in the marketplace will require investment. That investment should pay off for many organizations.

---

## **Copyright Notice**

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2007 IDC. Reproduction without written permission is completely forbidden.