

What's the #1 sign
of trust on the web?



COMPUTERWORLD

[Home](#) [News](#) [Topics](#) [Departments](#) [Services](#) [Subscriptions](#) [Events](#)

You may retrieve this story by entering QuickLink# 24846

[Return to story](#)

Start-up takes a bite out of denial-of-service attacks

By [LINDA ROSENCRANCE](#)
NOV 19, 2001

Like many health care companies, Hamilton Scientific Ltd. relies on the Internet access for front- and back-office operations, but the Roseland, N.J.-based firm can't afford any errors when patients' health and privacy are on the line.

The NetDetector, a security appliance from Monmouth Junction, N.J.-based Niksun Inc., helps Hamilton Scientific keep medical records private by monitoring the network for suspicious activity, identifying attacks and recording activity for later forensic analysis.

The physician-owned developer of medical Internet applications runs a virtual medical record and patient database that physicians, hospitals, payers, practicing specialists and pharmacies can access over the Internet.

"The whole idea is if you live in New York, and you travel to Texas and get in an accident, you want the hospital to be able to access your records as if you had been living there all your life," says Michael Nusbaum, chief operating officer at Hamilton Scientific. "Niksun helps us secure our data so health care organizations can get records electronically."

"Security is a priority for us. We have our own security in place, but we wanted another layer in case people get through our security so we could see what was going on and monitor it," Nusbaum says. "At the time we chose Niksun, it was the first company to have what we were looking for."

Internet security cameras

Niksun CEO Parag Pruthi says his firm's security appliances, NetDetector and NetVCR, allow companies to know exactly what is happening on their networks at all times and to take any necessary action if an attack occurs. The products

continually monitor networks, alert managers to possible attacks and provide specific information on how to set filters to block attacks.

NetDetector functions as a surveillance camera for the network that sits outside the firewall, intrusion detection system or customer servers and records all Internet Protocol activity. Organizations can use the data it gathers to analyze network events and network intrusions.

NetDetector time-stamps recorded data, analyzes sessions, detects unusual activities, sets alarms for real-time alerts and gathers forensic evidence for post-event analysis and legal prosecution.

NetDetector doesn't stop attacks; it provides the information required for the security administrator to define the appropriate access control list (ACL) on the router or firewall to block the attack.

"Since NetDetector is capturing all the traffic, it can help the security administrator determine which traffic he is being flooded with," says Juan Pablo Pereira, product manager for NetDetector at Niksun. "In addition, the administrator can manually test certain filters or ACLs on the recorded traffic to see how the proposed filter will affect the network -- what traffic will get blocked and what traffic will get through."

Pruthi claims NetDetector's recording capabilities are so complete that it can recreate the activity of a system intruder, keystroke by keystroke -- even if all logs are deleted.

"The NetDetector makes the unknown known," Pruthi says.

Pruthi likens Net Detector to a surveillance camera in a convenience store that helps store managers know who's been inside and what that person is doing.

"We built a surveillance system in the network to aid in the investigation of network events and intrusions and help companies recover rapidly from security breaches," he says. "'As a result [of the terrorist attacks] of Sept. 11, it is critical to secure government and enterprise networks around the world."

NetVCR sits on WAN or LAN links and identifies network-performance problems to aid in enforcement of service-level agreements and quality of service agreements and to ensure that IP traffic for enterprise customers, carriers and service provider networks runs smoothly.

Chris Christiansen, an analyst at IDC in Framingham, Mass., says the real benefit of Niksun's products is that they give enterprises the ability to not only look at real-time data, but also to go back in time, take a historical snapshot of the data and then overlay it onto the real-time data to detect any anomalies.

"Niksun's products are all about keeping track of the traffic that is occurring on the network," says Peter Lindstrom, an analyst at Hurwitz Group Inc. in Framingham. "The two products record all traffic, replay it and present it in trends and graphs so [enterprises] know what's going on in the network."

Pereira says Niksun is currently working on developing stronger centralized management features, including configuration, alerting and reporting, which are required for large-scale deployment.

Niksun Inc.

1100 Cornwall Road
Monmouth Junction, N.J. 08852
(732) 821-5000

Niche: Niksun's network activity monitoring and archiving software can filter out denial-of-service attacks and provide forensics evidence for tracing and prosecuting the source of an attack.

Company officers:

- Parag Pruthi, CEO and president
- Mahendra Pratap, vice president of solutions engineering
- Eric S. Tollar, vice president of engineering
- Jayne Fitzgerald, vice president of business development and operations

Milestones:

- June 1997: Company founded
- May 2000: NetVCR and NetDetector launched
- October 2001: NetDetector 1.2 released

Burn money: \$30 million in second-round funding from The Hillman Co., Redwood Venture Partners LLC, ABN Amro Private Equity, Satwik Venture Capital Partners and Beachhead Capital

Products/pricing: NetDetector costs \$15,000 to \$70,000; NetVCR costs \$15,000 to \$70,000. Associated consulting services typically range from \$100,000 to \$1 million per project.

Customers: Hamilton Scientific Ltd., Galileo International Inc., Pennsylvania Power & Light Inc. and others

Red flags for IT:

- Technology and scalability aren't yet proven in large-scale implementations.
- NetDetector can detect, trace and alert IT managers to attacks, but it can't prevent them.

The Buzz: State of the Market

A Different Focus

Unlike traditional intrusion-detection systems, products like those of Niksun Inc. focus on identifying denial-of-service attacks and provide the information needed to quickly filter out the source of the attack.

As the number of illegal access attempts continues to climb, the market for such products is growing rapidly. Framingham, Mass.-based IDC predicts that revenues in the worldwide intrusion-detection and vulnerability assessment market will exceed \$1 billion by the end of 2003. According to IDC, organizations are purchasing intrusion-detection and vulnerability assessment products to increase control over and awareness of their networks.

Monmouth Junction, N.J.-based Niksun faces several competitors in this emerging market, and most are small vendors or start-ups.

Niksun's appliances can identify denial-of-service traffic, but it doesn't actively block it without intervention -- a capability that at least one other vendor offers. However, Niksun does offer extensive activity archiving for forensic analysis and prosecution. "I don't believe the other companies have that [forensics] capability," says Peter Lindstrom, an analyst at Hurwitz Group Inc. in Framingham.

All of these vendors offer products aimed at helping companies detect, trace and react to network denial-of-service attacks by placing sensors outside the corporate firewall, as well as at Internet service provider locations. Niksun's direct competition includes:

[Mazu Networks Inc.](#)

Cambridge, Mass.

Start-up Mazu claims that its TrafficMaster Inspector and Enforcer can detect denial-of-service attacks and automatically block them. The product identifies an attack, then filters out the hostile traffic to eliminate it, says Mazu.

[Arbor Networks Inc.](#)

Waltham, Mass.

Arbor says its Peakflow DoS software monitors traffic to detect and trace denial-of-service attacks and recommends filter settings to block them.

[Asta Networks Inc.](#)

Seattle

Asta's Vantage System uses an array of sensor devices outside the firewall to optimize network traffic flow and filter out denial-of-service attack traffic.

Source: Computerworld

Sponsored Links

Sun and Oracle -- FREE Database Cluster Solutions iSeminar

Sys Admins - Upgrade Your Site to 128 bit SSL Encryption

Avaya's ECLIPS Portfolio Standards-based IP Telephony Solutions

[About Us](#) [Contacts](#) [Editorial Calendar](#) [Help Desk](#) [Advertise](#) [Privacy Policy](#)



Copyright © 2002 Computerworld Inc. All rights reserved. Reproduction in whole or in part in any form or medium without express [written permission](#) of Computerworld Inc. is prohibited. Computerworld and Computerworld.com and the respective logos are trademarks of International Data Group Inc.