NetDetector Wards Off Network Attacks

By Frank J. Ohlhorst, CRN

May. 21, 2004 4:04 PM EST

With security threats becoming more severe and harder to counter, enterprises are increasingly turning to advanced forensic devices to help fight off attacks and preserve evidence if a security breach occurs. Solution providers selling devices and services to meet security and forensic requirements have hundreds, if not thousands, of solutions from which to choose. Identifying the best solution is further complicated by multiple vendor options and the speed with which threats change.

The Niksun NetDetector, an appliance-based intrusion-detection system, combines packet-capture techniques with advanced reporting capabilities to protect enterprise networks. NetDetector runs on a solid FreeBSD platform, an open-source Unix alternative and leverages the abilities of the open-source intrusion-detection system SNORT to gather and analyze every packet transmitted over a network. The appliance can be configured with multiple NICs to monitor multiple servers or network segments. One of the unique features of NetDetector is the ability to treat each segment as a separate network, which makes investigations and intrusion detection easier. On the hardware side, Niksun provides a multiprocessor 2U rack-mounted unit with at least 2 Gbytes of RAM and as much as 1.46 Tbytes of storage.

NetDetector's browser-based console is simple to use and intuitive to learn, yet it provides an incredible amount of information. Administrators have the ability to track all packets, re-assemble packets and view complete sessions. These capabilities are enhanced by the unit's reporting abilities. What's more, NetDetector accomplishes these tasks in realtime, so an administrator can be alerted of an intrusion as it occurs, monitor the activity and then decide what course of action to take. The ability to reassemble network traffic extends to the file level, allowing administrators to examine file attachments, e-mails, instant-messaging sessions and almost any network activity.

Reconstructing traffic is simplified by the console, which offers a tabbed interface for viewing the most common activities, including Web-page reconstruction, e-mails, FTP, chat sessions and so on. Administrators can delve even deeper to monitor the activity of individuals to track what users did and when.

Other critical investigative information such as IP addresses, MAC addresses, and packet traces are readily available using the same in-depth investigative approach. The unit's canned reports offer excellent detail, allowing administrators to readily create paper archives of activities. All of the unit's reporting supports filtering, which allows administrators to focus on particular activities, users or addresses.

NetDetector costs between $6,995 and $125,000.

Niksun requires solution providers to pass certification training to sell its product. Once certified, partners can receive on-site technical and sales training, sales and technical resources, joint sales efforts, joint advertising and co-op trade show opportunities and access to a dedicated partner Web site with technical support and other materials.

Niksun declined to disclose average solution provider margins, which vary based on revenue.

CHANNEL PROGRAM SNAPSHOTS

> Niksun NetDetector

COMPANY: Niksun
Monmouth Junction, N.J.
(732) 821-5000
www.niksun.com
DISTRIBUTORS: Direct from vendor
TECH RATING: ★★★★★
CHANNEL RATING: ★★★★

CRN TEST CENTER recommended

Note: Vendors can earn up to five stars for technical merit and five for their channel program. If the average of these two scores is four stars or greater, the product earns CRN Test Center Recommended status.

RELATED: VIDEOS | SLIDE SHOWS | CHANNELCASTS | COMMENTS

SHARE: Digg Del.icio.us Facebook LinkedIn Twitter
Email this article | Print article | Reprints | More Security |

Login To Add Your Comments

RECENT ARTICLES

Security Goes Platinum: 25 Scenes From RSA Conference 2011
RSA Conference 2011 had a little bit of everything. While it's impossible to see and do it all, here are 25 scenes from the nation's largest information security conference.

25 More Head-Turning Security Products To See At RSA Conference 2011
Security vendors rolled out their latest and greatest offerings at RSA Conference 2011. Here are 25 that caught our attention on the show floor.

RSA At The Movies: Security Pros Rate Realism Of Hollywood Cybercrime
From The Net to Live Free Or Die Hard, a crew of security professionals at RSA Conference 2011 examined several films to see if these Hollywood cybercrimes could really happen.

More Slide Shows

RELATED VIDEOS

12_08_10_ve_panel_security_opportunities_2011_kelley_final-inxpo_ve

Security Challenges In Healthcare IT

SonicWall's Network Security Appliance 2400

Security As A Cornerstone

How Stuxnet Changes The Game In Security

RELATED ARTICLES

- Gen. Alexander At RSA: Cyber Security A 'Team Sport'
- RSA: Google Exec Says 'A-Team' Required To Fight Security Threats
- Vidyo Ups Channel Ante With Cloud-Based Video Routing
- Five Companies That Came To Win This Week

CHANNELCASTS

- Fighting SMB Cyber Crime: The Next Channel Opportunity
- What Name Do You Give Your Security? (And How to Sell It, No Matter What)
- Communication Tools Attack: The Channel Guide to Securing Customer Networks and More
- Web Application Threats: Real Costs, Real Prevention Strategies for the Channel and Their Customers