IDS PERSPECTIVES

Software or Purpose-Built Hardware?

IN THIS ISSUE

Q&As with IDS Experts:
Andrew Berkuta, HomeBanc
Richard Stiennon, Gartner
Mike Hommer, Miercom

Issue One, Volume 1

Sponsored by:

IntruVert NETWORKS

Intrusion Prevention Through Innovation™

IDS PERSPECTIVES

An analyst, user and product testing expert expound on the differences between IDS software and purpose-built hardware appliances.

ANALYST VIEW

Richard Stiennon, research director, network security, Gartner, Inc.

What trends are driving the intrusion detection system (IDS) market?

The overriding trend is the difficulty of using an IDS and its lack of a positive impact on the overall security of an organization. No matter how much intrusion detection you do, you're not even a little bit more secure at the end of the day. It's your response procedure that has an impact on security, and most organizations aren't prepared for the types of teams it takes to respond effectively to attacks.

Will intrusion prevention adoption be affected by this trend?

The idea evolves naturally after you've gotten involved in IDS. The question is, why am I alerting on an attack? Specifically, known buffer overflow attacks, directory traversal attempts, various unicode messages that come through that a server is not going to respond to—why am I letting those through to my server? My server has no defense mechanism. Here I've just recognized that there's an attack passing through me, why did I let it through? The obvious solution is to block those attacks that you've identified as malicious.

> *"The appliance form factor has more attractions—it's plug and play."* — **Richard Stiennon**

Do you think these intrusion prevention products can do a credible job at that?

Yes, reports from the field are that they're doing it. It's not a matter of blocking everything that your normal IDS alerts on. That's a scary thought. But it's easy to block everything that's outside of the protocol standards. If you just enforce the IETF RFCs for the various protocols, you can block a lot of the attacks that are targeted at your servers.

Do you think appliance-based IDS solutions will grow faster than software-based products?

They are definitely growing faster. The appliance form factor has more attractions—it's plug and play, and you don't have the issue of having to install software, update it on a regular basis, patch it and all the rest. Vendors can also build in features such as hardware acceleration modules and network processors that allow an appliance to operate at a higher throughput. Appliances can have a [Secure Sockets Layer] chip to decrypt SSL sessions, so you can look into those, too.

Is there a business reason for selecting an appliance- vs. a software-based solution?

Yes. Generally, most of the businesses I talk to are attempting to reduce the number of NT, Solaris and other servers they have to support. To manage them properly, those servers have to go through a continual patch process. Appliances generally stand outside that procedure because they are usually stripped down versions of OSs that have been hardened. And if there's an update or a patch to either the security application or the OS, it comes on a single CD or it's downloaded or available for incorporation in flash memory, so the support process is combined, and that makes it a lot easier.

USER VIEW

Andrew J. Berkuta, manager of network and physical security, HomeBanc Mortgage Corp., Atlanta

Why were you looking for an IDS solution?

One of the things that we consistently look at and evaluate is how can we best ensure the integrity of our network to our customers and our associates, to demonstrate that we have a process for providing the best solution that's available inside our network.

We already have firewalls, VPNs and certain other things in place, so we were looking for best-of-breed solutions for intrusion detection, purely IDS boxes, that we could compare apples-to-apples in a bake-off.

It doesn't do you any good to have a very powerful security system if you can't understand it. So ease of use was also very big on my list, and that includes ease of use in disseminating information and in configuration.

How did you compare hardware-based IDS appliances to IDS software?

We took the top five products in the market and compared them side by side. A hacker doesn't care if your IDS is hardware or software; he just wants to know if he can get around it. So we had them sitting right next to each other on the same port. In each case, we wanted to make sure they had a full feature set in terms of detection capability and that they could provide forensics traces, with summary reports that can be presented to an executive. So there had to be breadth of reporting available.

We also wanted to find out if the

> *“Hardware-based systems usually have better performance ‘out of the box’ and scale rather effectively.”*— **Mike Hommer**

appliance solution had gigabit options. For our scope, we limited it to 100M bps Ethernet only. Some appliances or solutions said they could handle gigabit, but when you get into it, you run into limitations. In the case of IntruVert, for the bake-off, we originally got the I-4000 model, which is primarily gigabit. But it would not have been fair to have the I-4000 go up against some of these boxes, where the limitation was 600M bps of aggregate Ethernet capacity. So we used the IntruShield I-2600 instead, to make it a fairer fight.

Why did you ultimately choose IntruVert’s IntruShield?

Looking at the different solutions, it was evident to us which vendor had stopped and evaluated the deficiencies in the market and how to address these issues. With other products, for every network segment, or every other segment, you better put a sensor in there. IntruVert went the extra few yards and offered virtual intrusion detection, which enables you to monitor subnets. When you do the numbers, in terms of how many segments you’re trying to monitor and how many conventional sensors you’d have to buy, even with the discounts other vendors were offering, IntruVert could either meet them or beat them in terms of ROI.

> *“IntruShield has the smallest install and learning curve I’ve ever experienced.”*
>
> —**Andrew Berkuta**

Another differentiator was the process by which IntruShield learns your network, so it provides fewer false positives and more information that’s relevant to you. After two days in learning mode, we were getting relevant events, whereas the others took anywhere from 15 to more than 20 days to provide us with information that was relevant—and we were still getting false positives. That learning mode is important because the network is a living, breathing thing and if there’s a delta between when you change something and when the IDS starts providing valid information, you may be vulnerable. IntruShield has the smallest install and learning curve I’ve ever experienced.

So there’s less to tweak, it’s easy to use, we can manage it ourselves, it has the in-line mode built-in and the information you get from it with the Alert Viewer is in layman’s terms.

TEST LAB VIEW

Mike Hommer, manager of consulting services and private testing, Miercom

How do you approach testing a technology like network IDS?

To properly determine how an IDS system will fare, the traffic must be as authentic as possible to force the system to decode real traffic and not throw false positives because the payload information is filler. This means constructing a test bed that—through scripting and specialized test equipment—is generating authentic Layer 7 transactions comprised of typical network traffic (HTTP, FTP, SMTP, DNS, NNTP, POP3, etc.) at high speeds (up to one gigabit or more).

From a hands-on perspective, what are the implications for hardware- vs. software-based network IDS solutions?

Optimal software-based system performance requires a powerful server. What’s more, scaling requires ever-larger servers or several distributed sensors in order to monitor a single high-bandwidth link. Hardware-based systems usually have better performance “out of the box” and scale rather effectively. While the price of a hardware-based system is usually higher than software-only products, the price of the server required for the software product must be considered when constructing a business case.

In 2002, you conducted an extensive review of IDS solutions. What did you learn about the leading approaches when it comes to accuracy, speed and ease of management?

The hardware-based systems were better able to handle the challenge of gigabit speeds. Additionally, the top systems had excellent management applications that did not overwhelm the user with excessive alarms and provided ways to give high-level system visibility while still capturing enough information to drill down into detail.

If you were advising a large organization purchasing an IDS, what would you tell them are the most important elements to consider when evaluating competitive solutions?

Performance under heavy traffic loads and performance under heavy attack volumes. High traffic loads will determine which systems can keep pace with your current and future network traffic volumes. High volumes of attacks will determine which systems have a management and database architected to handle high volumes of malicious traffic.

Thinking about an Intrusion Detection System?

WE ARE SO CONFIDENT YOU'LL PICK INTRUVERT, WE'LL PICK YOU UP TO PROVE IT.

Now, will you be **checking** any **bags**?

A no-risk offer

We are so confident you'll pick IntruVert that we'll fly you out to San Francisco, pick you up at the airport and whisk you off to our Silicon Valley headquarters to see the new IntruShield IDS in action.*

(Of course, if travel to San Francisco is not convenient for you, we will be happy to come to you instead.)

Why pick IntruVert?

Because IntruVert is the first vendor to integrate signature, anomaly and Denial of Service (DoS) detection methods in a single purpose-built appliance designed to protect you from known, unknown & DoS attacks.

You get the industry's best attack detection with low false positives. The flexibility to prevent attacks in real-time. And a powerful, easy-to-use Web-based Manager application. All with the industry's lowest total cost of ownership.

Don't take our word for it!

We aren't the only ones impressed with IntruShield. Third-party labs consistently judge IntruShield the best in independent tests.

IntruShield secured the top spot in a series of tests conducted by The NSS Group, Network World, Miercom Labs and Neohapsis Labs, beating ISS, Cisco, Symantec, Intrusion, Enterasys, and Snort.**

We promise you will be impressed. Call us at 1-877-IDS-1001 or visit www.intruvert.com/flyout.*

Award-Winning
Next-Generation Network IDS

NetworkWorld BLUE RIBBON

NSS approved

BEST STARTUP
BEST OF INTEROP
NETWORLD+INTEROP
CMP Network Computing INFORMATIONWEEK EETIMES

Independently tested NETWORKS AS ADVERTISED™ MIER COMM. INC.

OSEC
osec.neohapsis.com

Check Point OPSEC CERTIFIED

IntruVert
NETWORKS

Intrusion Prevention Through Innovation™

*IntruVert offer is open to qualifying company IT professionals located within the U.S. (excluding Alaska & Hawaii) considering purchase of an Intrusion Detection System. Promotion ends April 28, 2003 or until IntruVert has issued all airline tickets to qualifying applicants. For application and full details of offer conditions and restrictions, visit intruvert.com/flyout ** More details at intruvert.com/awards.