UBM

InformationWeek
Tech Digest
JANUARY 2014



Intrusion-Prevention Systems

# The IPS Makeover

Next-gen intrusion-prevention systems have fuller visibility into applications and data. But do newer firewalls make IPS redundant?

Powered by SECURITY dark READING

# The IPS Makeover

## Next-gen intrusion-prevention systems have fuller visibility into applications and data. But do newer firewalls make IPS redundant?

**By John Sawyer**

**More organizations are** deploying next-generation firewalls that include advanced application inspection and content awareness features, including many of the same features they have been they have been getting from old-school intrusion-prevention systems. That overlap has IT security leaders wondering: Do we still need a traditional, single-task IPS?

IPS vendors are rapidly adding new capabilities to make systems more functional and effective, hoping to resuscitate a category that has long been a staple of the IT security arsenal.

The data suggests that the IPS still has relevance, but its hold is fragile. In the 2013 InformationWeek Strategic Security Survey, only 43% of respondents considered IPS to be "highly effective" at securing their organizations. That response rate is down 3 points from the year before. The firewall fared better: 62% rated their firewalls as highly effective in 2013, though that was down from 66% in 2012. While the two systems stop different types of attacks, it's clear that IT groups view the firewall as more efficient than the IPS.

To frame the future relevance of IPS, we need to step back and look at how the first-generation IPS historically has been deployed. The IPS was almost exclusively part of the enterprise's perimeter protection strategy. It was placed in-line just behind the firewall, where it could recognize malicious attacks and block them. Because most blocking was based on known attack signatures, the IPS has been very good at reducing the noise of attackers' automated scans, which helps security teams focus on identifying successful and potentially more advanced attacks. Unfortunately, as attackers have pursued more targeted attacks on users and client-side applications, traditional IPS technology has had trouble keeping up, because most IPS products don't inspect the full application stack.

This is where next-generation firewalls step in, adding the ability to

inspect and block traffic at the application level. The next-generation firewall, or NGFW, has helped enterprises consolidate security features into a single piece of hardware — but some experts argue that this approach may put too many eggs in one basket.

NGFW products today are a Frankenstein's monster of sorts, tacking features taken from other security tools onto the firewall's conventional packet-filtering role. New add-ons include reputation-based IP and URL blocking, a feature that traditionally is found in Internet security gateways, as well as malware sandboxing features.

But the shining star of the NGFW is its application and content awareness capabilities, which allow the firewall to perform deep packet inspection and identify application-specific traffic and file content. Doing so gives IT security teams granular control of specific applications, since they don't need to restrict traffic solely by IP address and port. They can base NGFW policies on an application such as Skype, BitTorrent, or voice over IP.

Unlike traditional firewalls, the next-generation firewall also can handle the standard blocking capabilities that have been the IPS' s bailiwick. Network engineers can now use one device in-line to monitor and block traffic instead of two. IPS vendors, in response, are seeking ways to reengineer and add new capabilities to their products to keep them competitive.

**Inspection, Detection, Prevention**

Vendors such as Sourcefire, Hewlett-Packard, and IBM are pushing "next-generation IPS" products that go beyond signature-based blocking. According to a Gartner report, "Defining Next-Generation Network Intrusion Prevention," a next-generation IPS has a minimum of five specific features:

1. Standard first-generation IPS capabilities, which means the ability to recognize signatures and block known vulnerabilities and threats at wire speeds. This is just the starting point.

2. Application awareness and full-stack visibility, meaning the ability to identify applications and enforce policies at the application layer and not just by ports and protocols.

3. Context awareness, meaning the abil-

ity to use multiple data sources to make informed decisions on whether to block certain traffic. These sources can include vulnerability management data, reputation feeds, and user identities.

4. Content awareness, which is the ability to analyze and understand files such as executables, PDFs, and Office documents and make decisions on whether to block or allow them in near real time.

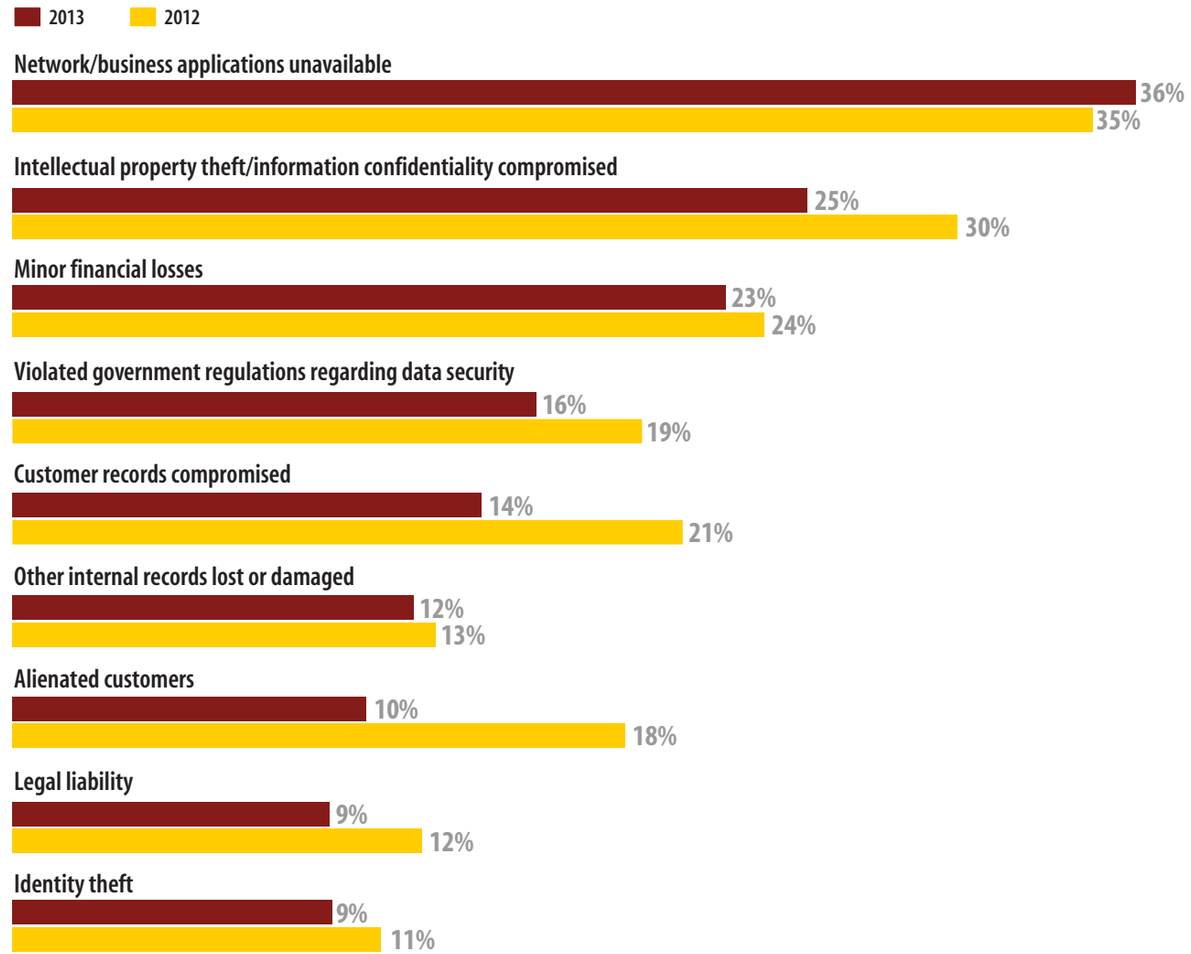
5. An agile engine that provides the ability to integrate and add new features and information sources as technology and threats evolve.

With the arrival of next-generation IPS technology, the standalone IPS appliance will likely become a thing of the past. As next-generation IPS takes on additional data sources, the platform on which it runs must evolve to handle different inputs from systems across an enterprise network. Companies can deploy multiple monitoring and prevention appliances at various choke points in the network to give both visibility and blocking capabilities.

Data from those choke points then goes into a central IPS console that is part of a larger monitoring system. Depending on the vendor, that larger monitoring and manage-

## Attack Fallout

What were the effects of attacks your organization has experienced?




Data: InformationWeek Strategic Security Survey of 217 business technology and security professionals at organizations with 100 or more employees in March 2013 and 183 in March 2012 experiencing a security breach within the past year

ment piece could be part of the IPS platform itself, or it may be integrated within the vendor's security information and event monitoring product; many SIEM and IPS vendors have merged over the last five years.

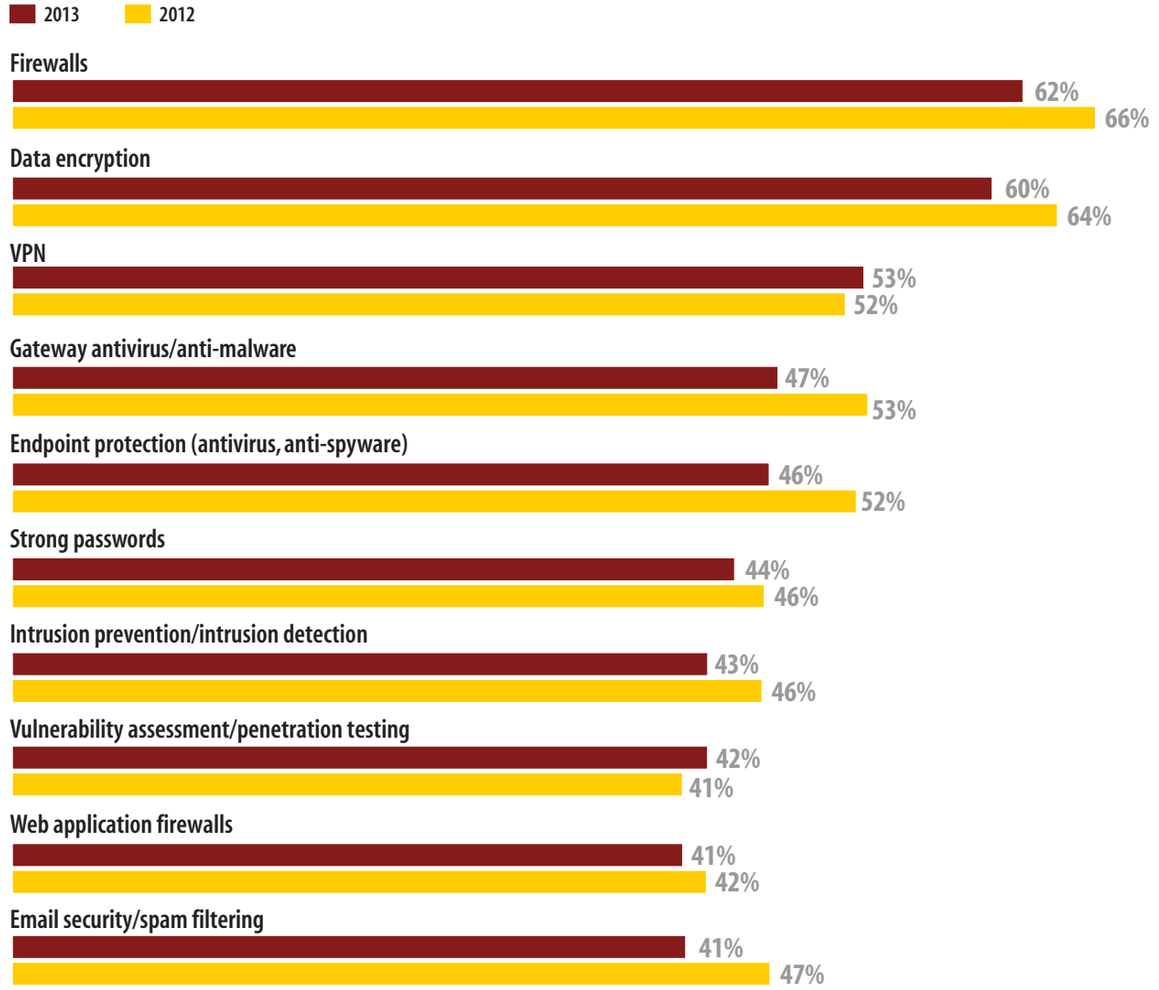
**Lessons From Network Security Monitoring**

The IPS evolution has some parallels with what we've seen in network security monitoring, or NSM, which more security analysts and security operations center teams are using. NSM involves collecting and analyzing warnings in order to respond to intrusions. NSM gives security operations center teams the network visibility they need to deal with a range of sophisticated threats. While NSM doesn't prevent the attacks, the monitoring of many information sources helps detect intrusions early so they can be handled quickly and effectively.

Taking a lesson from NSM's playbook, the next-generation IPS will collect information from servers, desktops, and network devices — potentially anything that produces a log — to make more informed decisions on whether to block network activity. The more data that's input into the system, the more data that's available to analyze and correlate, reducing the chance for false posi-

## Most Effective Security Practices

Which of these security technologies or practices are very effective in protecting your organization from internal or external security threats?




Data: InformationWeek Strategic Security Survey of business technology and security professionals at organizations with 100 or more employees in March 2013 and March 2012 using each security technology or practice (varies)

tives. Ultimately, the goal is not only to prevent attacks, but to detect successful attacks quicker to prevent catastrophic damage.

**Who Goes There?**

Of the five minimum characteristics of next-generation IPS, context awareness is of particular interest to the many enterprises that have undergone "deperimeterization" over the last several years. Context awareness allows companies to treat network traffic differently based on its source. Web traffic coming from a guest wireless network is treated with more restrictions than traffic coming from the marketing department. The latest Apache web server exploit may generate a different priority of alert than an attack being launched against a Microsoft IIS web server.

Traditional IPS products don't provide this sort of contextual decision-making. If traffic matched the signature, it was blocked. Some IPS products could define rules that change the blocking behavior based on where the traffic came from or was going to, but these were statically defined and not dynamic enough to follow users moving across the network.

Context awareness changes the way an IPS treats traffic based on various inputs into the system. Companies can integrate their user- and group-based traffic controls with Microsoft Active Directory, letting them set rules based on the user's identity. Similarly, a next-gen IPS can use vulnerability management data and configuration management databases to provide context on whether a specific exploit will be successful against the intended target.

In a sense, the next-generation IPS is becoming a sort of hybrid system made up of first-generation IPS technology, newer next-generation firewall systems, and SIEM products. It can block based on known attacks and provide some of the same deep content visibility as the NGFW, but it also offers the context awareness and insight that comes from SIEM. Of course, it's still an open question whether this new generation of IPS systems will be as popular as the old generation.

**Choosing A Next-Generation IPS**

While naysayers question the relevance of IPS technology, next-generation offerings do provide an interesting set of features. One major difference is that next-generation IPS is no longer a single, standalone appliance. The options include multiple "sensor" appliances that companies can deploy at the Internet gateway and at different choke points within the network.

The next-generation IPS can use many sources of information, which affects the size of the appliance needed to cover an entire enterprise network. Some of the collection and analysis work may be off-loaded to a separate SIEM; in other cases, the IPS product itself may perform that analysis. Depending on the level of SIEM integration, one system may collect data from all of the sensors, or several systems may receive logs from throughout the network and then correlate the data. Your choice of vendor and product line will dictate much of this design.

**In a sense, the next-generation IPS is becoming a hybrid system made up of first-generation IPS technology, newer firewall systems, and SIEM products.**

When choosing the right next-generation IPS, you'll need to evaluate the vulnerability management systems your company already has in place and whether those systems can integrate with an IPS. The more information

the IPS has about the network it's protecting, the better decisions it can make when blocking and alerting on attacks.

In addition to working with vulnerability management systems, some IPS products include passive vulnerability detection to supplement active scanning systems. The passive component runs directly on the sensors and reports back to the central management console. The vulnerability data is then used to provide context to attacks, helping analysts determine an attack's potential success based on whether it targeted a vulnerable system.

The heavy use of virtualization in the enterprise is also pushing some vendors to provide a "virtual IPS" that integrates with the underlying hypervisor and virtual switches in the enterprise. A virtual IPS provides security teams with the ability to inspect traffic that they might not have been able to see with nonvirtual IPS. Companies should evaluate virtual IPS options based on whether they're compatible with the virtual environments they already use.

Last, but certainly not least, reporting is important. Many first-generation IPS products had horrible reporting capabilities, and most companies simply fed the alerts into their SIEM or centralized logging systems for analysis and alerting. This is why so many IPS and SIEM vendors and products have merged in recent years. Test the reporting of any next-generation IPS product, and be sure it will integrate well with any SIEM systems you might use in the future.

*John Sawyer is a senior security analyst with InGuardians. Write to us at editors@darkreading.com.*