

WHITE PAPER

A Definitive Guide to The IPS Technology Landscape

Essential Solution to Selection Criteria



Executive Summary

Intrusion prevention systems (IPS) lie at the heart of security for corporate data centers and other security-conscious locations. But different IPS devices work better for some companies than for others. Selecting the right IPS solution for a specific facility requires careful consideration of various issues, from scalability and performance to the incorporation of threat intelligence, to the ability to protect data and applications in both public and private clouds. Following is a guide to the key factors that a director of security should consider in selecting an IPS solution.

IPS In Flux

IPS technology inspects the contents of packets passing through the network, much like carry-on baggage is scanned as part of airport security. For large corporate campuses and data centers, and for businesses with acute security needs, IPS functionality plays a crucial role in the corporate security infrastructure. But selecting an IPS solution is challenging. The market for IPS is in turmoil right now, and navigating the turbulence is a key challenge for directors of security whose organization needs the deep inspection IPS offers.

Companies can implement IPS either through standalone IPS devices or through next-generation firewalls (NGFWs) that include IPS functions. Standalone devices tend to provide more robust inspection capabilities and performance. Using NGFW-integrated IPS, on the other hand, streamlines administrative tasks and may reduce costs. The amount of savings depends on how many other NGFW features are enabled in the same device and the throughput the company requires. In general, performance and security needs will dictate the appropriate IPS form factor.

The markets for both standalone and NGFW-integrated IPS are changing rapidly. In the past few years, some vendors have expanded their presence in the space, while others have sold off or discontinued their IPS technologies. IBM announced in 2017 the end of sales (EOS) for its Network Security (XGS) product line.¹ Cisco, likewise, discontinued the Cisco IPS that it previously sold alongside ASA firewalls; McAfee announced EOS for its M-series and I-series devices;^{2,3} and Trend Micro is ending its S-series and NX platforms.⁴

Even among vendors who remain committed to the market, IPS technology is changing so rapidly that periodic hardware upgrades are practically required. Directors of security in companies that need IPS capabilities should evaluate their options regularly. In this evolving market, they have their work cut out for them.

Characteristics of Successful IPS

The first place to look when evaluating prospective IPS devices is their basic feature set. Signature matching is fundamental to every IPS, so directors of security need to understand the signature-matching engine within each of their IPS options.

The most basic form of signature is string matching, where a signature simply looks for an exact match of known bad payloads. This kind of approach requires larger sets of signatures, as vendors must create a new signature not only for each new threat but also for each variation of that threat. These signatures will match only one payload.

Don't be tempted by vendors with the largest set of signatures, because that could indicate that they heavily rely on string matching, which requires a much larger signature set than those needed by other approaches. Due diligence should reveal the size of the signature set and give some indication to how sophisticated or efficient the vendor is when it comes to signatures. For some less-sophisticated IPS solutions, protection ends at the signature engine.



Markets for both standalone and NGFW integrated IPS are changing rapidly. Some vendors are expanding their presence in the space, while others are selling off or discontinuing their IPS technologies.



Finding IPS solutions that deliver more string matching and sophisticated signature sets to block known vulnerabilities is crucial.

Companies that need more effective IPS inspection, however, should consider vendors that can do more than string matching. Sophisticated signature sets include lists of known vulnerabilities, making one signature capable of blocking many different variants of an attack targeting that same vulnerability. This approach to signatures is more efficient than string matching and results in a smaller number of total signatures. Examining the IPS signature count and cross-referencing that with detection rates of reputable third-party benchmarks (e.g., NSS Labs) should identify these vendors as scoring well and having lower signature counts. Vendors with too few signatures, but low detection rates, are simply not doing the research necessary to protect companies, while vendors with too many signatures are not efficient in their designs, probably relying on old technology.

Sophisticated IPS devices also supplement their block decisions with contextual information, such as user behaviors and heuristics, detection of network and application protocol anomalies, and other variations from historical norms. These features augment intrusion detection and prevention system capabilities, reducing the number of alerts and false positives.

These IPS capabilities are the table stakes. Among the IPS solutions that are effective in these areas, the director of security should then select those that meet the following requirements:

1. Scalability and Performance

Performance is a key factor driving many companies to select standalone IPS rather than functionality integrated into an NGFW. The additional load on a firewall appliance that must now inspect packets and payloads for IPS will slow down network traffic. Signature matching alone can reduce some NGFWs' speed by as much as 30%.

IPS needs to scale for increasing growth in traffic volumes, both inside the data center and on the network perimeter. There are a couple of ways IPS vendors can build scalability into their devices. One is by incorporating a security processing unit.

The CPU-based architecture of traditional security devices can become a bottleneck for a firewall or an IPS. A single high-end processor may struggle to keep up with the network demands for high bandwidth along with the security demands for deep inspection. Security decision-makers should carefully consider an architecture that separates network processing from security processing so resources can be applied efficiently as needed and one process is not held hostage by the other, reducing throughput for both processes.

The ability to inspect encrypted traffic is crucial for any IPS. However, it can be extremely processor-intensive, and many vendors struggle to do this at speed. As a result, overall throughput is dramatically reduced, or worse, the IPS simply passes the encrypted traffic without inspecting it. Offloading this task from the primary processor to a specialized content processor overcomes this challenge. Although adding a content processor to an IPS does not increase the device's overall throughput, it reduces performance degradation that can result from activating certain security capabilities, such as decryption.

2. Advanced Threat Prevention Capabilities That Leverage Threat Intelligence

Advanced threat prevention (ATP) is designed to ferret out malware and ransomware that specifically target a network's security gaps. It's a critical functionality in the ongoing "arms race" between security professionals and cyber criminals. Over the course of just three months in 2017, FortiGuard Labs reported on 14,904 new pieces of malware—an average of 160 per day.⁵

That's why directors of security should expect prospective IPS solutions to include ATP within their devices. They should also expect those ATP capabilities to integrate with a threat intelligence service. Some IPS providers have their own threat intelligence capabilities, which supplement the native functionality of the devices with ongoing updates about zero-day and other emerging threats. The tight integration achieved by a vendor's own threat intelligence often equates to faster response times through this automation.



Signature matching alone can reduce some NGFWs' speed



IPS vendors must incorporate high-quality threat intelligence and demonstrate a long-term commitment to threat research.

Either way, a director of security evaluating IPS solutions should make sure that the shortlisted IPS solutions incorporate high-quality threat intelligence, and that the IPS vendors have demonstrated a commitment to threat research. The size and consistency of a vendor's threat research budget is a clearer indicator of commitment than a mere verbal claim.

3. Removing Walls Between NOCs and SOCs

Traditionally, a company's security operations center (SOC) functions separately from the network operations center (NOC). They have different staff and different management processes. But such siloed operations will almost certainly lead to duplication of effort, perhaps even to staff working at cross-purposes.

Worse, barriers between the NOC and SOC may undermine a company's overall security posture. The NOC contains a great deal of information about the corporate network, including where a specific application is running and whether security patches are up to date. When an attack surfaces, the NOC can answer questions about which endpoints are vulnerable and how alarmed the security team should be. This information can be vital to mounting a fast and effective response to any type of attack.

The NOC lacks the information needed to identify and root out those attacks. The SOC stores detailed data about emerging threats, which will help the organization identify prospective attacks before they can affect corporate systems. But a SOC, without the knowledge base of the NOC, does not have the network insights for staff to effectively judge the organization's vulnerability and respond.

A recent survey found that among companies that have a SOC, 22% didn't have a NOC, 12% reported that their NOC and SOC teams have very little direct communication, and 21% said their NOC and SOC teams work together only in an emergency.⁶

The most effective security posture integrates data from corporate NOCs and SOCs. A company shopping for IPS capabilities should look for solutions that break down the NOC and SOC silos by combining information about security threats with data on network vulnerabilities.

4. Integration Into a Comprehensive Security Ecosystem

Traditionally, a company's security operations center (SOC) functions separately from the network operations center (NOC). They have different staff and different management processes. But such siloed operations will almost certainly lead to duplication of effort, perhaps even to staff working at cross-purposes.

Another reason for tightly integrating corporate security solutions is to optimize efficiency and minimize costs. Running siloed systems often means staff must perform the same tasks in different ways within different systems. At the same time, the tasks take longer to complete, as moving from one solution's interface to another's will require them to shift gears. Certainly, getting new staff up to speed takes longer in a siloed scenario, and the company might even need to retain a larger security team to staff all the different systems.

In contrast, tightly integrated solutions that offer similar interfaces and workflows enable staff who use one system to easily take on management of another. To optimize both efficiency and effectiveness of their company's security processes, directors of security should look for IPS solutions that integrate with the company's other security products to provide tightknit functionality and transparent visibility.



NOC and SOC integration remains a challenge, with 12% of organizations reporting that their NOC and SOC teams have very little direct communication and 21% indicating that they only work together in the event of an emergency.



Integration of IPS into a broader security fabric architecture is critical if an organization wants to improve their chances of thwarting zero-day attacks and other advanced threats.

5. Incorporating The Clouds

A final area of consideration is the ability to protect applications and data in the cloud. Almost every company runs some form of cloud-based application, and most run quite a few. Fortinet has found that the typical company uses 62 different applications in the cloud.⁷ Another recent survey found that 85% of organizations with more than 1,000 employees are using more than one cloud—multiple public clouds, multiple private clouds, or a hybrid environment that includes both.⁸

It thus goes to reason that an IPS solution should not only protect on-premises software and data but also be capable of functioning in both public and private clouds. As part of the due diligence process, the director of security should evaluate where the company's data and applications reside, and the ability of prospective IPS solutions to protect them, regardless of location.



Cloud adoption is exploding, with 85% of organizations with over 1,000 employees reporting the use of more than one cloud solution.

Making The Decision

Despite the urgency to minimize risk, especially considering the volatile IPS market, directors of security should not compromise on due diligence in selecting an IPS system. They must ensure their prospective IPS solutions will scale to accommodate both current throughput and projected future growth. They must evaluate whether those systems will integrate efficiently into their current security ecosystem, or will create (or perpetuate) the problem of information silos. And, as with every security solution selection process, they must consider price and performance issues. A tall order, perhaps. But with the increasing vendor commitment to next-generation IPS, diligent buyers can now be confident they will find a solution that meets their needs.

¹ [“Software withdrawal and support discontinuance: IBM QRadar Network and IBM Security Network Appliance selected programs,”](#) IBM United States, August 15, 2017.

² [“End of Sale and End of Life for McAfee Network Security M-Series Sensor Appliances,”](#) McAfee, modified April 7, 2017..

³ [“Current Network Security Platform software version information,”](#) McAfee, modified May 8, 2018.

⁴ [“TippingPoint End of Life \(EOL\) dates,”](#) Trend Micro, July 14, 2017.

⁵ [“Fortinet Threat Landscape Report Q3 2017,”](#) Fortinet, November 28, 2017.

⁶ Nelson Hernandez, [“NOC/SOC Integration: Opportunities for Increased Efficiency in Incident Response within Cyber-Security,”](#) SANS Institute InfoSec Reading Room, January 26, 2018.

⁷ [“Fortinet Threat Landscape Report Q3 2017,”](#) accessed April 6, 2018.

⁸ [“RightScale 2017 State of the Cloud Report,”](#) accessed April 6, 2018.



www.fortinet.com