WHITE PAPER

McAfee
Together is power.

What to Look for in an Intrusion Detection and Preventions System

McAfee Network Security Platform

WHITE PAPER

What to Look for in an Intrusion Detection and Preventions System

McAfee Network Security Platform

Network security is more important than ever. Modern networks are getting faster. They are also increasingly crossing physical boundaries, creating hybrid and cloud environments. Many of these are further complicated by combining multiple cloud service providers, locally hosted virtual environments, and physical infrastructure.

To secure and monitor modern high speed, dynamic, critical networks you need an intrusion detection and prevention system (IDPS) that is able to process and inspect extremely high levels of data flowing through the system. At the same time, your network security solution needs to be flexible enough that it can adapt and grow to match future requirements.

In the "Market Guide for Intrusion Detection and Prevention Systems,"[1] Gartner points out that "IDPS offers the best detection efficacy and performance network security, but firewalls are absorbing IDPS on the perimeter." The guide says that "...stand-alone IDPS enables a number of threat detection workflows. These capabilities are precisely what is needed for organizations that hunt down nascent breaches or are looking for data to justify a decision to block or quarantine or put some other control in place." In its key findings, Gartner says, "Advanced threat intelligence feeds continue to improve IDPS effectiveness by augmenting capabilities, and threat intelligence appliances will not replace them."

Gartner adds that, "Apart from performance, efficacy is usually more important in the data center. Not only do stand-alone IDPS products consistently score at the top of any detection benchmark, but their coverage of server vulnerabilities are also not matched by most firewall products."[2]

Connect With Us

Today's networks are moving towards regularly using 40 Gb and 100 Gb interconnects, and these high-performance networks have become intolerant of any additional sources of latency. As such, an appliance that has been designed to support these high-speed networks without adding any additional latency is crucial. Maintenance windows are short (99.999% uptime equals 5 minutes and 15 seconds annually of downtime), and upgrades, especially where physical appliance replacement is needed, are difficult and complex. Users need IDPS technology that has factored in high availability, as well as fail-open kits, bypass segments, and active-active appliances. In addition, it's important to have a licensing structure that allows for network growth from 10 Gbps to 20 Gbps, 30 Gbps, 40 Gbps, or even 100 Gbps and allows for in-service upgrades to support growth minimizing the need for physical appliance replacement.

When looking to investment protection, your solution's flexibility needs to reflect deployment methods that allow the inspection of traffic without a network redesign or renumber (using Layer 2) inspection technologies. These technologies add negligible latency to network sessions and are customizable to match requirements without dependencies on vendor-created patches or signatures, plus they feature licensing models that meet customer needs for now and future planning.

In its "Market Guide for Intrusion Detection and Prevention Systems"[3] recommendations, Gartner says, "Security and risk management leaders responsible for the security of networks and endpoints should … Implement a stand-alone, next-generation network IDPS as an additional defense layer with best-of-breed detection efficacy."

A well-configured and strategically placed IDPS helps create a robust multilayered defense system within hybrid environments. McAfee® Network Security Platform solutions can detect attacks directed to exploitable vulnerabilities on systems, and it goes a step ahead to reject potentially malicious network packets. It helps mitigate various insider attacks, prevent a stealth attack that moves laterally through the network to increase an attacker's footprint, as well as thwart sophisticated external attacks like denial-of-service (DoS) or distributed denial-of-service (DDoS), thereby helping to close all security gaps and providing comprehensive network security without compromising performance or scalability.

The McAfee IDPS solution provides a single management console, McAfee® Network Security Manager, that can manage, configure, and monitor the deployment of IDPS technology across modern hybrid environments. The hybrid nature of these networks places additional emphasis on the need for segmentation, separating less

> "Security and risk management leaders responsible for the security of networks and endpoints should … Implement a stand-alone, next-generation network IDPS as an additional defense layer with best-of-breed detection efficacy."
>
> —Gartner, Market Guide for Intrusion Detection and Prevention Systems, 1 July 2019, Craig Lawson, John Watts.

secure from more secure environments, or, as Gartner suggests, segregating IT and operational technology (OT),[4] and supporting, for example, NIST 800-153 and DoDI 8523.1.

During 2019, a vast majority of new malware campaigns are expected to use various forms of encryption and obfuscation to conceal the delivery of malware and to conceal ongoing communications, including data exfiltration. A similarly dominant percentage of that enterprise web traffic is expected to be encrypted.[5] SSL decryption of inbound traffic—that is, traffic that originates outside of our immediate network and is targeted to our secure web service—is of particular interest. This channel can be used to mask attacks against your public-facing or intranet websites and can potentially lead to compromise, website defacement, or data loss.

There is a need to counter this attack vector with a comprehensive secure sockets layer (SSL) decryption and inspection technology. McAfee Network Security Platform provides true north-south and east-west traffic scanning and protection with its industry-first inbound SSL inspection technology. McAfee Network Security Platform can support both traditional man-in-the-middle inspection and shared key techniques for inspecting DHCE.[6] McAfee Network Security Platform is also designed with a 100% decryption requirement for outbound traffic while maintaining full inspection capabilities.

The key to discovery of attempted intrusions and taking decisive action against those intrusion is actionable intelligence. With its deep portfolio integrations, McAfee Network Security Platform gives it access to such intelligence. McAfee Network Security Platform integrates with McAfee® Endpoint Security products (a component of HBSS/ESS) to support the concept of network teaches endpoint and endpoint teaches network. Additional vendor-supported integrations include:

- McAfee® Global Threat Intelligence (McAfee GTI)
- McAfee® Web Gateway (secure web gateway)
- McAfee® Advanced Threat Defense (malware sandbox)
- McAfee® Enterprise Security Manager (SIEM)
- McAfee® Threat Intelligence Exchange
- McAfee® Network Threat Behavior Analysis and Endpoint Intelligence Agent (EIA)

These integrations give McAfee Network Security Platform leading threat detection rates (AV-Test, NSS Labs, and others)[7] and an advantage against any intrusion attempt, an advantage provided by the depth of threat intelligence.

Modern threats require advanced detection techniques. McAfee Network Security Platform can intelligently find and protect against known and unknown threats, malware callbacks, DoS, zero-day attacks (threats that use evasion techniques), ransomware, and other advanced threats. McAfee Network Security Platform is a comprehensive malware solution that features inbound and outbound SSL inspection, gateway anti-malware (GAM) engine and zero-day support, heuristic and behavioral analysis, and dynamic analysis (machine learning and malware sandboxing) to stop advanced targeted attacks.

For signatures, McAfee Network Security Platform provides a library of proprietary signatures developed and maintained by McAfee® Labs, as well as customizable signatures. The customization is available in McAfee® UDS (user-developed signatures), as well as industry standard SNORT format. Detection methods provided on the McAfee Network Security Platform include (but are not limited too):

- Signatures (vendor-provided, user-defined and SNORT)
- URL and file reputation (provided by McAfee GTI)
- Embedded PDF emulation
- Gateway anti-malware engine
- Network anomaly detection (threshold-based and self-learned DOS and DDOS protection)

McAfee Network Security Platform is a true advanced threat detection and protection platform capable of supporting modern detection methods, high throughput, low latency, and single-pane-of-glass management. It is integrated solution, sharing threat intelligence from device to cloud.

Learn More

For more information, visit us at **www.mcafee.com/nsp**.

Watch the **McAfee NS9500 video**.

1. Gartner, Market Guide for Intrusion Detection and Prevention Systems, 1 July 2019, Craig Lawson, John Watts.
2. Ibid.
3. Ibid.
4. Ibid.
5. Google Transparency Report—HTTPS encryption on the web
6. High-Performance Inbound SSL Inspection for McAfee Network Security Platform
7. NSS Labs Test Result: McAfee Network Security Platform

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com