Next-Generation Network Security

McAfee and Intel Help Thwart Sophisticated Attacks

BY **TIM KRIDEL**

In enterprise network security, the only constant is change. That may sound cliché, but it's accurate on many different levels. In the 1990s, most attackers were teenagers and college students looking to take down or deface corporate websites. Or they were hackers creating malware to harvest credit card information. Those criminal types are still around—and increasing—while new breeds of attackers are emerging to expand the threats that enterprises, government agencies, and other organizations have to fend off.

"Organized crime has taken on hacking," said Nat Smith, senior product marketing manager at McAfee. "There is evidence that some of the viruses and attacks that have occurred throughout the world have been sponsored by actual countries." The newcomers have different motivations and techniques, which create additional complexity. They're not interested in mischief or creating an alias for themselves. Instead, they're slipping quietly into a network to set up bots that stay under the radar for days, weeks, or months until their mission of destruction is accomplished. This development undermines the effectiveness of traditional strategies such as using a list of signatures to screen traffic for threats.

Ten years ago, all of the bad guys were known, so a signature list was effective. Today, the threats are advanced, persistent, and stealthy: things that can evade detection. Security is not so much about preventing bad guys from putting graffiti on your website, but it's about your data being taken or watched. The new breed of threats are typically highly targeted, such as on a government agency or a specific financial institution. Each attack is customized, which further undermines the effectiveness of signature-centric security. Corporate and nation-state espionage is becoming a major, emerging threat. The days of feeling safe with up-to-date signatures are gone. Security operators need to look beyond that approach.

McAfee isn't alone in warning organizations about the risks of overreliance on signature-centric protection. "The sophistication of attacks increases to a level where traditional signature-only solutions no longer provide adequate protection," Gartner[1] cited in a recent report.

Additionally, the new threats add to the workload for IT staff and other people in the security trenches. In fact, the deluge of alerts and other information from intrusion prevention systems (IPS) makes it increasingly difficult for staff to keep up—and easier for attacks to slip through unnoticed.

All of these emerging challenges add up to the need for next-generation IPS. As Gartner[2] recently described the situation, "Targeted malware can often bypass existing protection technologies, and the resulting data breaches are not detected until a long time has passed and significant data exfiltration has occurred."

BUILDING A NEXT-GENERATION INTRUSION PROTECTION SYSTEM (IPS)

To enable enterprises, governments, and other organizations to counter the new breed of attacks, McAfee and Intel collaborated to produce a next-generation IPS appliance. McAfee Network Security

[1]Verizon 2012 Breach Investigations Report, Gartner 2012
[2]Gartner, December 2012

"The new NS-series hardware is a product of the synergy between Intel and McAfee."

—Nat Smith, senior product marketing manager at McAfee, on the McAfee Network Security Platform NS-series built on the Intel® Xeon® processor E5 family platform

Platform NS-series is built on the Intel® Xeon® processor E5 family platform, which means it has ample compute power to stay ahead of the constant flood of attacks. The appliance uses high bus speeds and solid-state storage to inspect traffic so quickly that the process is unnoticeable to employees and other end users.

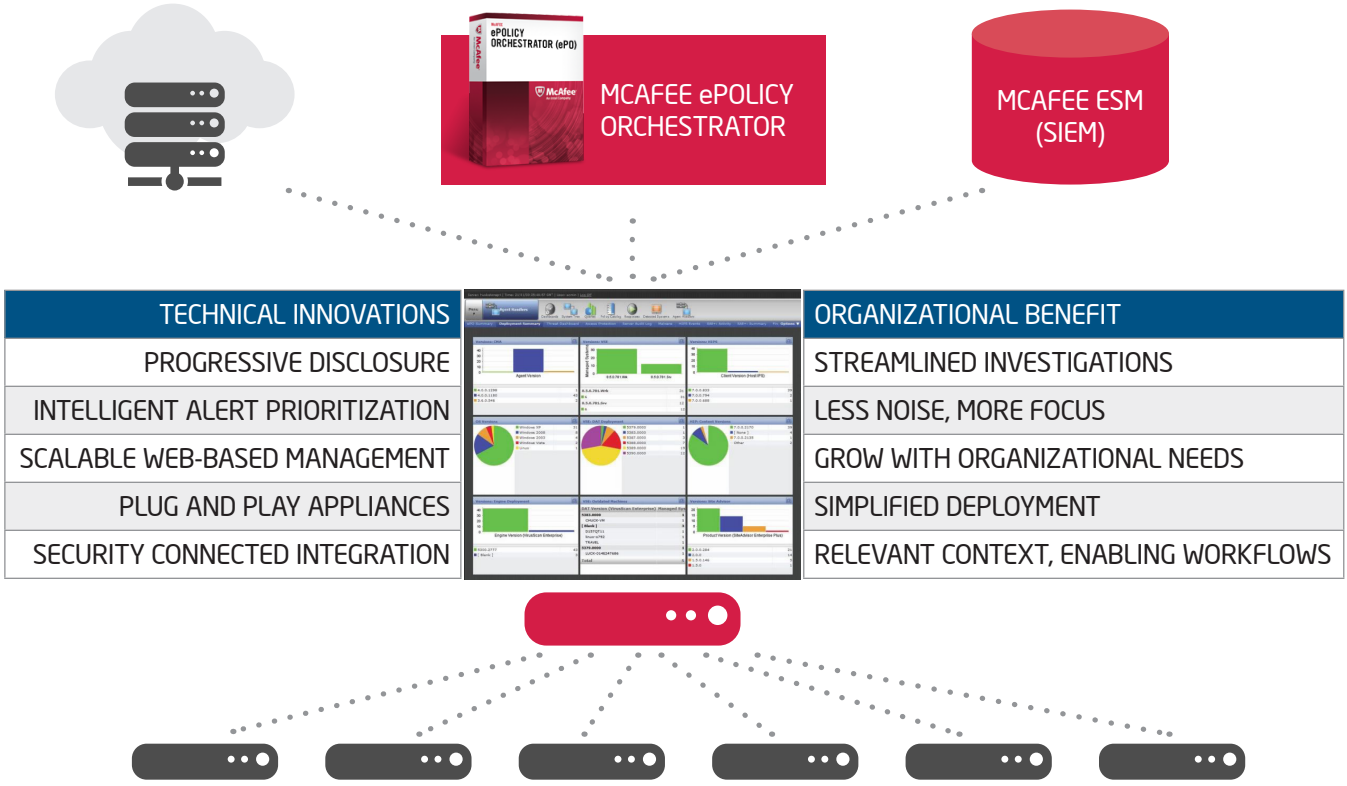
"The new NS-series hardware is a product of the synergy between Intel and McAfee," Smith said. McAfee NS-series is the latest example of how enterprises, government agencies, and other McAfee customers benefit from this working relationship. The Network Security Platform 7.5 release features include:

- **Advanced malware analysis.** Provides real-time emulation and static analysis engines that analyze the executable to extrapolate its behavior, catching stealthy behaviors that may be time-delayed or have different actions depending on the host environment. The Advanced Malware Analysis engine is unique in the IPS space. McAfee Network Security Platform 7.5 also includes an investigation dashboard dedicated entirely to malware.

- **Deep file analysis.** Ferrets out threats, such as JavaScript* buried in PDFs, and uses file-anomaly detection to determine whether the embedded JavaScript, or malformed elements, have malicious intentions. A few other products in the market can check for the existence of JavaScript and block a file if it exists, but the unsophisticated approach blocks both good and bad files because there is no analysis to determine whether the JavaScript is malicious. Shellcode detection and analysis not only detects the presence of malware payload, but can also determine its objectives, providing real-time evaluation of malicious intent.

- **Advanced bot detection.** Automatically seeks out and correlates multiple suspicious alerts that individually are not sufficient to convict malicious behavior, but collectively reliably point to zero-day bots. A specialized command-and-control server reputation service is also used for callback detection. These features directly benefit an organization's bottom line because bots typically are used to facilitate theft and sabotage.

- **Progressive-disclosure interfaces.** This dashboard-style feature (see Figure 1) uses Web 2.0 to make management more efficient and effective. It presents prioritized views of threat information and helps security operators and administrators drill down into details about events such as potential threats, risky hosts, active bots, and advanced malware.



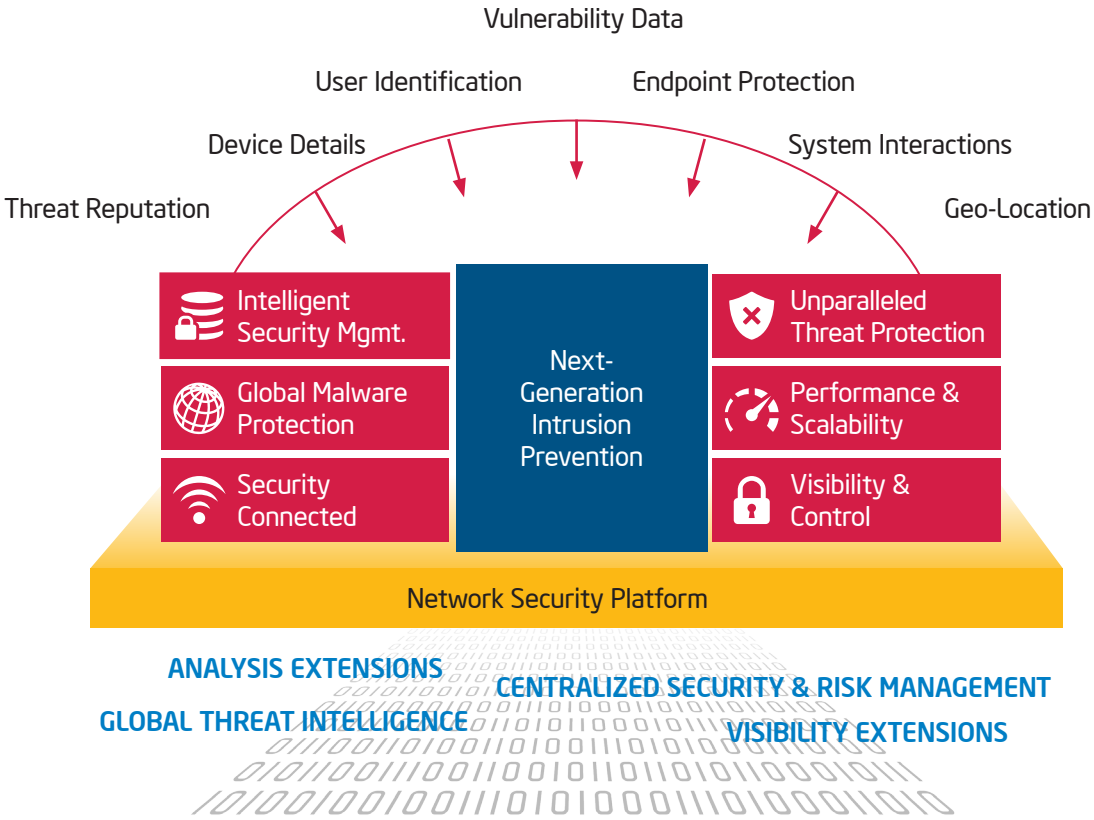
ABOVE *Figure 1: Intelligent security management.*

CONTEXTUAL AWARENESS

In IPS discussions today, "context" and "contextual awareness" are common buzzwords. Both refer to the strategy of maximizing security effectiveness by using external or on-box mechanisms to increase the platform's intelligence. When comparing IPS appliances, it's important to understand the breadth and depth of context a vendor can provide. "McAfee has the industry's richest set of contextual awareness feeds," Smith said. "That gives organizations the ability to dynamically pull in reputation information, network behavior, user information, host configuration, system vulnerabilities, and even dynamically correlate endpoint protection and network protection. The IPS can then use these contextual feeds to affect security decisions."

As the volume and sophistication of threats rise, IPSs typically struggle to keep up. McAfee NS-series takes advantage of Intel® hardware-enhanced security technologies and expertise to maximize performance. For example, McAfee NS-series has 40 gigabits per second (Gbps) of IPS throughput versus the 13 Gbps or less that other IPSs deliver. The NS-9300 will do 40 Gbps with all of the next-generation services enabled. Typically, when vendors benchmark performance, they turn off as many services as possible to give the full processing capabilities to throughput. This is not a real-world test. If those services are turned off to get a higher throughput rating, security is being sacrificed for performance.

Security operators must have ready access to the proper tools and UIs (see Figure 2) in order to effectively manage and act on information. To address this requirement, McAfee Network Security Platform release 7.5 abandons the traditional assumption that one alert



equals one security event. With the need to identify stealthy and zero-day threats based on behavior, tens or even hundreds of alerts are needed to define one security event. Legacy IPS systems built with the assumption that one alert equals one security event are driven by interfaces that list alerts as they come in, one on top of the other, the newest alert going on top.

"Even with the sheer volume of attack alerts, which is accelerating, this model would be overwhelming to most security operators. But when you consider the complication of having to aggregate and correlate related alerts to build the evidence for one stealthy security event, the task becomes all but impossible," said Smith.

McAfee Network Security Platform release 7.5 automatically correlates alerts and highlights the events they indicate. Underlying details such as individual alerts and packet-level forensics are still there when operators need to drill down. This approach maximizes the operators' ability to find and stop attacks.

It also significantly reduces the time and effort needed to do this, meaning security operators are free to focus on other pressing needs, and operational costs go down.

Because networks will remain attractive targets, McAfee Network Security Platform 7.5 ultimately is an investment in both the present and the future. The network is the main point where today's attacks occur, and it's the last place where organizations can afford to cut corners.

ABOVE *Figure 2: Contextual awareness tools.*

GO TO INTEL® SOFTWARE ADRENALINE FOR MORE ARTICLES LIKE THIS ONE. >