White Paper

McAfee
An Intel Company

McAfee Network Security Platform: The Next-Generation Network IPS

Table of Contents

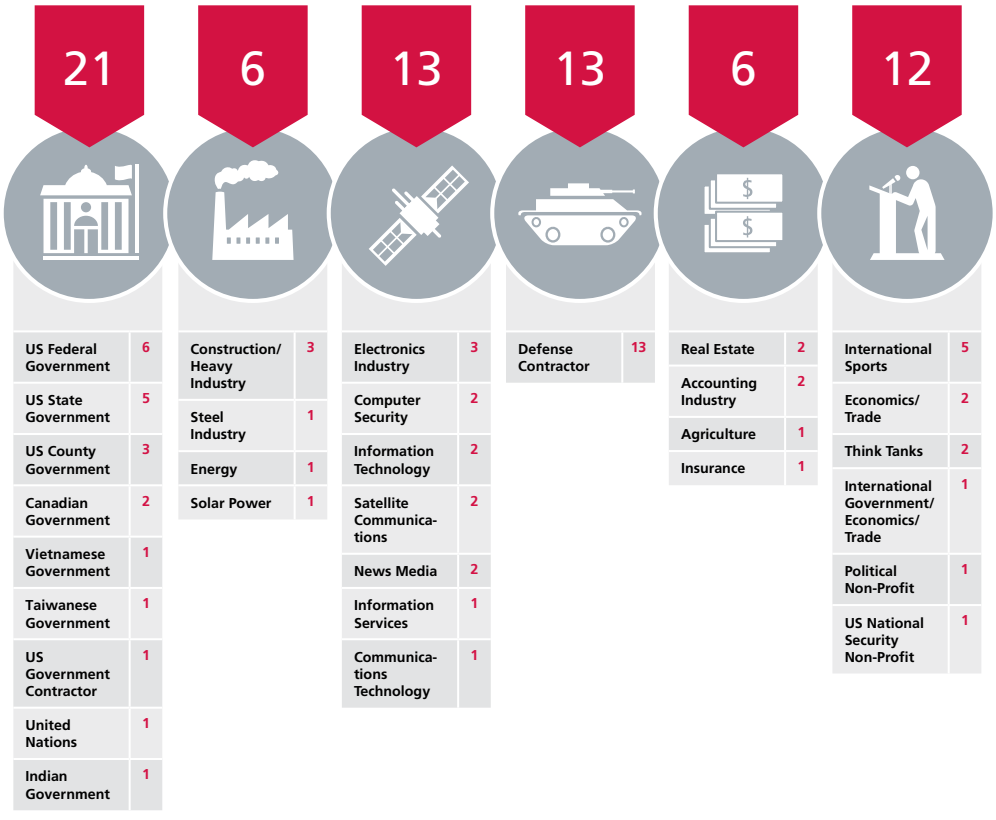
A More Highly Evolved IPS Solution

The evidence is alarming: the intrusion detection and prevention systems that currently protect most enterprise IT environments from malicious penetration, surveillance, and data theft are woefully underprepared for the latest attack methods. A new class of targeted threats has rendered traditional network security models ineffective and has exposed essential enterprise assets—trade secrets, intellectual property, and customer records—to critical levels of operational, financial, and compliance risk. IT organizations that are already overloaded managing complex environments and planned migrations to cloud- and service-based infrastructures must now find and deploy a new generation of security solutions that can achieve higher levels of security efficacy while reducing total cost of ownership.

Targeted threats: the Achilles heel of traditional IPS

Targeted threats are to traditional intrusion detection what stealth aircraft are to radar. They use many traditional attack techniques—phishing, social engineering, embedded malware, and traffic obfuscation—but deploy them in complex orchestrations. By targeting specific vulnerabilities, users, and client systems, they seek to acquire undetected access to key assets. Once inside and disguised as legitimate traffic, they establish long-term residency to siphon off valuable data with impunity.

While recent headlines have focused on the most sensational examples of highly organized and well-funded attacks—Google, Adobe, RSA, Lockheed Martin, SONY, and PBS—thousands of undisclosed attacks have quietly plagued government agencies and corporations large and small worldwide. In fact, new data suggests that targeted attacks are being launched against an ever-widening range of industries and companies. In Operation Shady RAT, for example, data from a single command and control server showed evidence that one attack organization successfully hacked 70 companies across 32 industries.



Source: McAfee Labs™

Figure 1. In Operation Shady RAT, McAfee identified 71 compromised parties, comprising more than 31 unique organization categories.

"Targeted attacks are a much higher risk to the bottom line, and are generally launched by more sophisticated attackers who are motivated to penetrate defenses quietly to get inside and steal information—for as long as possible, because that maximizes their revenue opportunities. These same techniques were later used by politically motivated techniques. Gartner believes that, through year-end 2015, financially motivated attacks will continue to be the source of more than 70 percent of the most damaging cyberthreats."

—Gartner
Strategies for Dealing with Advanced Targeted Threats
August 2011

Stages of a targeted attack

For entry, many targeted threats use spear-phishing techniques. They try to persuade the user to click on seemingly harmless links. For example, attacks seeking access to financial data will often target senior finance officials by sending them a legitimate-looking Microsoft Excel file innocuously named "Recruitment Plan." Initial-stage malware downloads often happen together with the bait file and execute quietly in the background in order to avoid detection by the user.

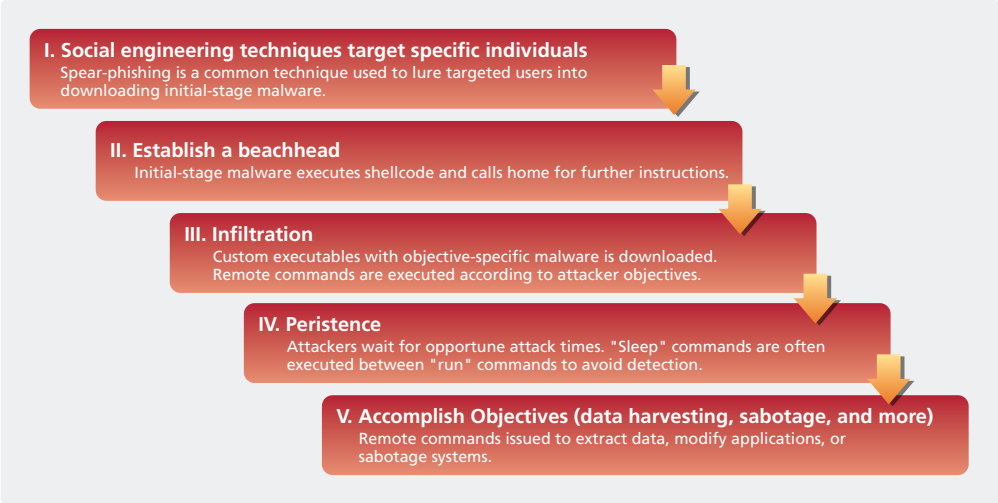


Figure 2. How a targeted attack works.

Becoming a tougher target

To harden network defenses against targeted attacks and respond more effectively to those that initially succeed, organizations need to set several goals for their security controls and management capabilities. These include:

- Establishing a baseline of extremely high-efficacy security to minimize the likelihood of successful attacks through intelligent "next-generation" network security controls
- Quickly detecting successful attacks and assessing their severity to minimize the scope and impact of the event
- Streamlining forensic analysis with integrated workflows to facilitate root cause analysis with minimal time and effort and deploy future protection

Achieving these goals will hinge on the presence of a next-generation IPS solution with specific threat detection and blocking capabilities including the ability to:

- Detect and interrupt targeted threats at key stages of the attack sequence with multitiered defenses
- Detect and block the initial malware download when a privileged user falls for a spear-phishing stratagem
- Detect shell code execution and the attempts of a malicious agent to contact its command and control server
- Detect and block the secondary downloads of objective-specific malware
- Detect and block the reconnaissance and sabotage exploits of successfully implanted agents
- Detect and block improper data extraction and export

Requirements for next-generation network intrusion prevention

Gartner Research recently introduced several new criteria for "next-generation network intrusion prevention" that, if adopted, will help organizations deal with the new threat landscape. The Gartner definition for next-generation network intrusion prevention includes the following:

- *Standard first-generation IPS capabilities to support vulnerability-facing signatures and threat-facing signatures*—An IPS engine that can perform detection and blocking at wire speeds and rapidly develop and deploy signatures, is a primary characteristic. Integration can include features such as providing suggested blocking at the firewall, based on IPS inspection.
- *Application awareness and full-stack visibility to identify applications and enforce network security policy*—This needs to occur at the application layer, independent of the port and protocol, rather than only ports, protocols, and services. Examples include the ability to block families of attacks, based on identifying hostile applications.
- *Context awareness to bring information from sources outside the IPS to make improved blocking decisions or to modify the blocking rule base*—Examples include using directory integration to tie decisions to user identities and using vulnerability, patching state and geolocation information (such as where the source is from or where it should be from) to make more effective blocking decisions. It could also include integrating reputation feeds, such as blacklists and whitelists of addresses.
- *Content awareness of various file types and communications*—It should be able to inspect and classify inbound executables and other similar file types, such as PDF and Microsoft Office files (which have already passed through antivirus screening), as well as outbound communications. In addition, it should make pass, quarantine, or drop decisions in near real time.
- *Agile engine*—It should support upgrade paths for the integration of new information feeds and new techniques to address future threats, including hitless upgrades, global threat intelligence integration, scalable hardware, signature updates, Snort-capable), packet capture, and complementary solutions (Source: Gartner, *Defining Next-Generation Network Intrusion Prevention,* 2011)

While Gartner addresses the minimum requirements for next-generation network IPS, there is also a clear need for network IPS solutions to dramatically reduce the operational overhead that would otherwise accompany investigation and eradication of stealthy, multistage attacks. The human expertise required to fight the new threat exceeds available resources in most organizations. Next-generation network IPS must do more of the heavy lifting, guiding junior analysts to the right insights so they focus on policy and response, not on manual event correlation. Critical management capabilities of next-generation IPS solutions must include:

- Eliminating the need to fine-tune IPS policies to achieve security effectiveness
- Automating otherwise manual event correlation and alerting
- Integrating event inputs for end-to-end attack visibility without multiple tools and views
- Context integration for intuitive, informative views
- Simple, application-centric controls that mirror organizational policy
- Workflows that mirror natural event investigation and resolution

McAfee Network Security Platform: True Next-Generation IPS

First-generation IPS capabilities

Why it's important

While Gartner uses the term "standard" to describe first-generation IPS capabilities, there remains wide disparity among network IPS vendors when it comes to baseline protection against common vulnerabilities and exploits. In 2010 NSS Labs tested all major network IPS vendors across 1,150 exploits targeting the most common operating systems, applications, and infrastructure systems. The results were alarming, with the tested systems blocking, on average, a little more than 60 percent of the sampled attacks. To a large degree, this failing reflects fundamental shortcomings in many existing IPS solutions. A more complete description of first-generation IPS features that are prerequisite for the development of next-generation capabilities includes:

- The ability to conduct multifactor traffic inspection that goes beyond signature- or statistical anomaly-based detection to reliably identify and block new, emergent threats on first exposure
- A highly efficient inspection engine capable of maintaining line rate performance even with aggressive security policies and variable, real-world traffic conditions (small packet sizes, high volumes of HTTP or encrypted traffic) that have been shown to reduce the throughput performance of many in-line systems by as much as 50 percent
- A flexible and extensible platform architecture that allows new detection methodologies to be added and integrated as they evolve
- Comprehensive threat research to characterize new emerging threats with near real-time integration into the inspection engine

How McAfee delivers it

McAfee® Network Security Platform features an ultra-efficient inspection architecture that enables full characterization of attacks based on a comprehensive and extensible range of detection methods. These currently include:

- *Stateful deep packet inspection*—The unique ability of McAfee Network Security Platform to fully inspect and characterize every flow it sees, including fragmentation re-assembly and streaming analysis (that is, identifying required parameters in a sequence of packets), allows it to more accurately identify potential threats. Complete characterization includes identifying the protocol, application, application parameters (for example, "HTTP get" versus "HTTP post"), and application payload (for example, file name, md5 hash, file structure, and embedded payload). This provides the baseline upon which all the following detection mechanisms operate to identify malicious traffic.
- *Signature-based and statistical anomaly detection*—Like all IPS solutions, McAfee Network Security Platform employs both signature-based defenses and statistical anomaly detection, but its unique stateful inspection engine and vulnerability-based signatures (backed by McAfee Labs, the industry's most robust research organization, and complemented by the platform's integrated vulnerability assessment) are uncommonly efficient and effective. In fact, McAfee Network Security Platform achieves industry-leading blocking accuracy with approximately half the number of signatures used by other leading solutions. As a result, it delivers maximum security effectiveness at full line-speed performance with any combination of aggressive security policies and variable traffic conditions.

- *Protocol anomaly detection*—Protocol anomaly detection identifies deviations from normal protocol use based on behavior and state, such as client request state or server send state. This allows the IPS engine to detect emerging threats that evade statistical models and have no traditional signatures. Adept at thwarting packet fragmentation, stream segmentation, and other obfuscation techniques for bypassing perimeter defenses, it also allows McAfee Network Security Platform to spot obfuscation attempts at both the protocol and file levels.
- *Heuristic analysis*—Heuristics provide yet another detection technique for assessing protocol, file, and system behavior, allowing McAfee Network Security Platform to identify intrusion attempts that escape traditional IPS defenses. It's particularly useful for characterizing bot behavior to uncover infected systems, and for identifying SQL injection techniques in server-side attacks.
- *Continuous, real-world threat research*—Research provides each of these detection methodologies their unique ability to support accurate, real-time identification and blocking decisions. With a global research footprint, McAfee Labs gives McAfee Network Security Platform the industry's most comprehensive global threat intelligence. Backed by more than 450 researchers, a portfolio of more than 400 patents, and a network of millions of sensors spanning the Internet, McAfee Labs delivers unparalleled protection against both known and emerging threats via a complete suite of security products.

Application awareness

Why it's important

When it comes to the natural evolution of network IPS, application visibility and control are absolute requirements. IT needs to know what applications are in use on the network, how much bandwidth is being used at different locations and the risks and threats associated with each application. Just as application visibility has been widely adopted in next-generation firewalls, next-generation IPS solutions require the same level of visibility and control.

In part, this is because static ports have become redundant. Most of the applications traditionally supported by stateful firewalls used static port assignments (port 25 for SMTP, port 80 for HTTP), and it was possible to make identification and blocking decisions based largely on port destination. Today, a vast number of applications use HTTP and port 80, and port-based decision-making is no longer a viable security strategy for most organizations.

Indeed, some new applications today don't use static ports at all. Instead, most P2P and IRC applications port hop or assign a port dynamically. Traditional firewall and IPS provide no visibility or control over these applications that are rapidly growing in number.

Only by understanding application usage requirements and intelligently implementing granular controls around approved communications and file transfer mechanisms can organizations mitigate the risk of threats being delivered through port-agile applications.

How McAfee delivers it

McAfee Network Security Platform provides these capabilities and more with layer 7 detection and identification of more than 1,100 applications, including granular visibility into sub-applications, like the growing Zynga portfolio of Facebook games and IRC chat in Yahoo! Mail. For each application, McAfee Network Security Platform provides analytics and graphical reporting for essential metrics, including risk rating, aggregate threats, and bandwidth consumed. Enhanced rule definition simplifies application access control and includes the ability to correlate application activity with network attacks to enable more intelligent response and enforcement decision-making.

Context awareness

Why it's important

In the context of network security, context awareness is the ability to deliver additional, relevant information to the IPS engine to enable more accurate decisions—to allow, alert, or block more quickly, accurately, and securely with fewer false positives.

Without contextual information about potential threats, system vulnerabilities, user behavior, and dozens of other factors, network IPS devices have almost no chance of detecting sophisticated multivector attacks. Many such attacks begin with a perfectly inconspicuous file download from a malicious site—a PDF, bitmap, Microsoft Office document, or Java Archive (JAR). If the IPS system has real-time reputation information about the file, the site's IP address, or its geographical location, the odds of a timely block go up significantly. If the IPS system also has system information such as the nature of the connection, client system vulnerabilities, or normal system behavior patterns, the odds of success rise dramatically.

It is not sufficient that context information simply be made available for administrator reference. It must be fully integrated into the IPS solution to enable automated block decisions wherever possible and highly efficient workflows when manual investigation is unavoidable.

How McAfee delivers it

McAfee Network Security Platform offers a range of contextual feeds which are correlated in real-time to increase security effectiveness and reduce false positives.

- McAfee Global Threat Intelligence™ (McAfee GTI™) feeds are integrated at the sensor and manager level to dynamically increase in-line prevention effectiveness against unknown and emerging threats. McAfee GTI assesses the reputation of network communications based on the reputation of billions of unique IP, file, URL, protocol, and geolocation data from around the globe.

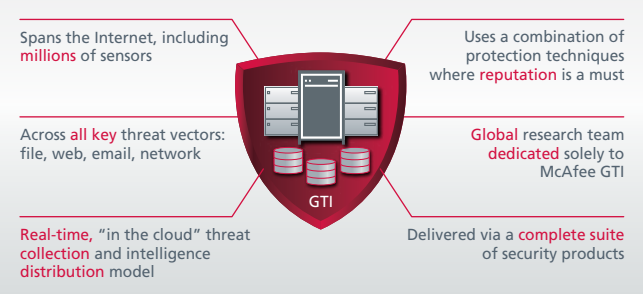


Figure 3. How McAfee GTI works.

- System-level contextual inputs actively shape intrusion prevention effectiveness. McAfee Network Security Platform incorporates user information, host intrusion alerts, system vulnerability information, and host-level risk assessments to recommend security policy improvements and speed incident response.
- Time-based behavioral context provides the ability to correlate activity across various time frames, from seconds to weeks. In contrast to traditional IPS that typically performs point-in-time analysis, McAfee Network Security Platform uses both short-term heuristics and long-term behavior analysis to correlate and identify malicious activity.

Differentiating capabilities include:

» *Activity burst botnet heuristics*—The ability to track potential botnet behavior over time and across multiple systems using dozens of botnet heuristics to identify new and known bots with unmatched levels of confidence

» *Behavior-based threat detection*—Flow-based behavior analysis that incorporates rich layer 7 data allows organizations to establish a baseline of normal system activity and detect infected systems by their anomalous behavior

» *Impact analysis and mapping*—The use of time-charted flow information to assess the scope and impact of an attack by mapping the interactions between infected devices and detecting irregular data flow patterns

Content awareness

Why it's important

More and more, hackers are using targeted client-side attacks to access critical enterprise assets. Next-generation security solutions need the ability to detect malicious content as it crosses network boundaries before it can compromise a host system or open a covert channel to attackers. Visibility into the packet alone isn't sufficient. An IPS solution must be able to reassemble application fragments and chunked traffic, decode and reassemble files, and decompress payloads embedded in files. All content must be identified and inspected as it passes through the network, so that abnormalities can be detected and malicious payloads can be stopped before delivery.

Content awareness capabilities range from standard to advanced:

- Standard content detection includes the ability block known malicious content (packets, files, executables) using signatures
- Proactive content detection uses global reputation information gathered from worldwide sensor nets to identify malicious content entering or leaving the network—in real time, without existing signatures
- Advanced content detection uses packet and stream forensics to detect abnormalities, unknown malware, and shell code

How McAfee delivers it

McAfee uses all three levels of content awareness to identify malicious content. Standard content detection (signature-based) and proactive (reputation-based) detection techniques are cornerstones of McAfee Network Security Platform. The latest release adds advanced content detection through a combination of on-box advanced file inspection and out-of-the-box integration with advanced malware detection, network forensics, and data loss prevention tools. The result is a network security solution that is deeply content aware. With its on-box capabilities, McAfee Network Security Platform can automatically detect anomalies in protocol and files and alert administrators, even with threats it has never seen before. Its detection capabilities include JavaScript hidden in PDF files, Flash in XLS, and executable code in documents.

At an even deeper level, McAfee Network Security Platform can detect concealed malware through the presence of shell code packaged within content, a critical capability for detecting advanced targeted attacks. It can identify JavaScript shell code in HTML or PDF files, for instance. Once the shell code is detected, administrators can extract the payload and write custom signatures to block future attacks and prevent propagation within the network.

Agile engine

Why it's important

Network security is a moving target, affected by the rapid evolution of attack methodologies, networking requirements, and highly dynamic IT environments. Organizations don't have the budget or operational flexibility to rip and replace network security solutions as needs change.

For example, not only must today's network intrusion prevention solutions be able to scale to several times current network capacity without a "rip-and-replace" event, but they must also adapt to the needs of private and public cloud architectures, having the ability to protect floating virtual infrastructure. In addition to adapting to new IT architectures, next-generation network IPS must also be able to consume new, more sophisticated threat inspection and investigation models that are delivered either as new on-box features or deployed seamlessly through completely integrated, pluggable extensions to the core platform, allowing organizations to manage a single solution with completely integrated workflows.

How McAfee delivers it

McAfee Network Security Platform is a purpose-built platform designed with evolving security requirements in mind. Through hitless upgrades, organizations can easily take advantage of McAfee Global Threat Intelligence reputation feeds, heuristic-based botnet detections, layer 7 application awareness, and several other recent innovations. The platform is able to accommodate these upgrades with little to no impact to performance through dedicated and specialized processing resources within the device.

As performance requirements grow, organizations can easily scale performance up to 80 Gbps through a modular inspection architecture that allows organizations to elegantly cluster several McAfee Network Security Platform sensors and manage the stack as a single device. Additionally, platform extensions allow for integration with advanced security tools. It accepts external intelligence feeds and data flows for richer inspection, enables policy-based packet capture and provides flows to externally integrated devices, laying the framework for a range of advanced inspection functions.

Future of Next-Generation IPS

For the most part, traditional intrusion prevention technologies use "detect and protect" methods of attack detection that rely on mostly binary decision logic: "allow if safe" and "block if malicious." All other activity is left to alerts, which become the problem of security analysts to investigate. The goal of next-generation network IPS technologies should be to sufficiently automate analysis and assessment capabilities to both speed and ease the investigation of malicious events.

Take, for example, the detection of a drive-by PDF download that is part of a broader targeted attack. Today's sophisticated network intrusion prevention devices can alert and even block a suspicious event, but what if this event is just part of a broader attack? Full analysis should involve asking and answering several additional questions:

- *Who initiated the download*—what user, what system, with what group affiliations?
- *What led to download event*—web browsing, a phishing email, a USB device attachment?
- *What source data is available*—sender ID, site, IP address, location, reputation?
- *What other events are related to this activity*—command and control, spam, bot activity, file transfers?

Organizations must also be able to assess threat exposure, not just for the system in question, but for the entire network:

- *What is the system-level risk*—the known host vulnerabilities, protection profile, system type, and business data value?
- *What other systems may be affected*—what's known of the activity history, related communications, threat propagation behavior?
- *What data is at risk*—have files been transferred, communications encrypted, user accounts compromised?

McAfee believes the future of next-generation intrusion prevention must address these issues with a level of automation that approaches artificial intelligence. Building on the industry's most advanced network IPS, McAfee is working to deliver a solution that not only includes the intelligence to address advanced threats, but also has the ability to dynamically assess their impacts, recommend protective measures, and automatically deploy appropriate defensive measures in the context of the attack type.

Conclusion

Targeted attacks are taking a steep toll on organizations whose network defenses can't secure systems and data against stealthy, persistent, adaptive and well-camouflaged threats. IPS vendors need to evolve more sophisticated capabilities to detect and block complex threats, and their enterprise customer can't wait for the results.

Fortunately, they don't have to. McAfee Network Security Platform delivers industry-leading security effectiveness, scalable in-line performance, and next-generation IPS controls that take the guesswork out of security management. Now organizations can unify network security across physical and virtual environments, streamline security operations, and protect themselves from emerging malware, zero-day attacks, denial-of-service exploits and advanced targeted attacks.

The next generation of network IPS is ready to deploy today. To find out more, visit www.mcafee.com/networksecurity.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

40603wp_next-gen-ips_0212_fnl_ASD