Solution Brief

Advanced Threat Defense for Network IPS

Broaden protection against stealthy malware.

The network-based intrusion prevention system (IPS) is a mainstay of enterprise security architectures. Deployed in band in conjunction with gateway and host-based security, IPS systems monitor network traffic and endpoint behavior using a range of techniques to detect attacks and trigger defensive responses.

Today, however, an increasing number of unknown, zero-day threats are successfully evading traditional defenses. Stealthy, well-camouflaged, intelligently adaptive, and often carefully targeted, these sophisticated attacks constitute a small but disproportionately dangerous and expensive part of the changing threat landscape.

In response, some organizations are adding dynamic analysis to their IPS infrastructure in the form of out-of-band sandbox appliances. The sandbox launches suspicious executables in a secure virtual environment and monitors runtime behavior to detect malicious intent. Often, though, this apparent gain in detection accuracy is quickly lost to poor integration and manual response processes.

For instance, most third-party sandbox appliances can only alert a human security analyst when a new attack is found. The analyst must manually create new blocking rules for the IPS and firewall and then begin the task of identifying and fixing all the endpoints compromised during the out-of-band sandbox analysis. Other common limitations of existing solutions include:

- A cost-inflating requirement for one sandbox appliance per IPS sensor.
- Reliance on a generic virtual execution environment that may overlook target-specific attack behaviors.
- Reliance on dynamic analysis only, rendering the sandbox vulnerable to various malware strategies for detecting secure environments and delaying execution of revealing behavior.

Key Advantages

- Finds, freezes, and fixes advanced malware and stealthy attacks hidden in network traffic.
- Adds true static code analysis and target-specific sandboxing to network security with no increase in IPS workloads.
- Plug-and-play threat blocking with no delay for human intervention.
- Malware analysis reports automatically integrate into McAfee Network Security Platform workflows.
- Leverage endpoint intelligence and attack context within McAfee Network Security Platform to improve threat detection speed and accuracy.

intel Security

A Security Connected IPS and Sandbox Solution

McAfee, a part of Intel Security, offers a solution to all these challenges: a tightly integrated combination of McAfee Network Security Platform, a high-performance next-generation IPS sensor, with McAfee Advanced Threat Defense, the industry's most powerful and complete advanced malware detection appliance. McAfee Network Security Platform provides in-band traffic inspection and threat blocking through a set of malware detection technologies that are optimized for real-time execution. McAfee Advanced Threat Defense provides a more extensive and resource-intensive set of analyses that include both target-specific sandboxing and true static code analysis. Together, these two devices find and freeze new, unknown, and stealthy advanced threats. For a complete end-to-end solution, add McAfee® ePolicy Orchestrator® (McAfee ePO) software and McAfee Enterprise Security Manager (SIEM) to quickly identify and fix any systems impacted by advanced malware.

- **Find:** Innovative analytical technologies work together to quickly and accurately detect sophisticated threats across multiple protocols.
- **Freeze:** Our tightly integrated security products instantly stop infiltration attempts and contain infected endpoints.
- **Fix:** Our solution automatically scopes a newly discovered infiltration across the environment and initiates the endpoint remediation process.

Security Connected

The Security Connected platform from McAfee, a part of Intel Security, provides a unified framework for hundreds of products, services, and partners to learn from each other, share context-specific data in real time, and act as a team to keep information and networks safe. Any organization can reduce risk and response time and lower overhead and operational staff costs through the platform's innovative concepts, optimized processes, and practical recommendations.

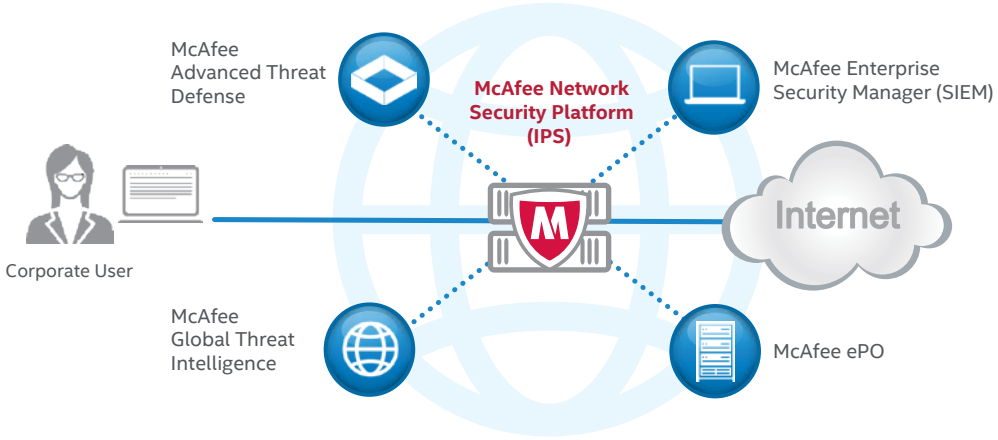

Figure 1. Integration points for finding, freezing, and fixing malware.

Because the McAfee Advanced Threat Defense solution for network IPS follows the Security Connected approach to enterprise security integration, it delivers a range of operational and defensive advantages that are unique in the industry, including:

- **Plug-and-play threat blocking:** Attacks discovered by McAfee Advanced Threat Defense are automatically blocked by McAfee Network Security Platform with no need or delay for human intervention.
- **Report and workflow integration:** Reports generated by McAfee Advanced Threat Defense are automatically integrated into McAfee Network Security Platform workflows, eliminating much back and forth between screens during investigations.
- **Security context visibility:** McAfee Advanced Threat Defense can access and leverage endpoint intelligence and other security context stored on McAfee Network Security Platform to improve threat detection speed and accuracy.

The IPS: McAfee Network Security Platform

McAfee Network Security Platform is a family of IPS appliances that discover and block sophisticated threats in the network, including advanced malware, zero-day threats, denial-of-service attacks, and botnets. Combining an ultra-efficient, single-pass deep inspection architecture with purpose-built, carrier-class hardware, McAfee Network Security Platform delivers line speeds of up to 40 Gbps with a single device and maintains exceptional throughput performance and accuracy regardless of security settings. On-board threat analytics include custom signatures, full protocol analysis, threat reputation, deep file analysis with emulation and JavaScript detection, and threat behavior correlation against application usage based on layer 7 visibility of more than 1,500 applications and protocols.

Perhaps the most powerful feature of McAfee Network Security Platform is its ability to integrate and leverage the insights and capabilities of other McAfee security solutions. Of particular importance to this solution are seamless integrations with:

- McAfee Enterprise Security Manager, a revolutionary security information and event management (SIEM) solution that provides a real-time view of the internal IT environment combined and correlated with global context from the outside world. McAfee Enterprise Security Manager's highly tuned database collects billions of log events and correlates them with other relevant data streams, making multiple years of security event data immediately accessible. It calculates baselines for all incoming data streams to identify anomalies and potential threats before they develop, and simplifies compliance management with hundreds of pre-built dashboards and mandate-specific reports.
- McAfee Advanced Threat Defense is the advanced malware detection component of this solution.

The Sandbox: McAfee Advanced Threat Defense

McAfee Advanced Threat Defense is a multilayered malware detection solution that stacks an extensible series of inspection engines and analytical capabilities in a down-select sequence of increasing computational intensity. This unique approach to complete but efficient assessment delivers a very high level of detection accuracy and reliability with extremely high throughput performance. The on-board analytics applied by McAfee Advanced Threat Defense include:

- Signature-based detection of viruses, worms, spyware, bots, Trojans, buffer overflows, and blended attacks using a comprehensive knowledgebase created and maintained by McAfee Labs, which currently includes nearly 150 million signatures.
- Reputation-based detection using the McAfee Global Threat Intelligence network to detect newly emerging threats.
- Real-time static analysis and emulation to quickly find malware and zero-day threats not identified with signature-based techniques or reputation.
- Full static code analysis that reverse engineers file code to assess all attributes and instruction sets and fully analyze the source code without execution. Comprehensive unpacking capabilities open all types of packed and compressed files to enable complete analysis and malware classification, helping organizations better understand the specific malware they are dealing with and the impact it has on their organization. Full static code analysis provides critical insight into input-dependent behaviors and delayed or hidden execution paths that often do not execute during dynamic analysis and are overlooked by less comprehensive sandbox solutions.

Better Together

- Enhance the value of existing security investments.
- Reduce the need for network re-architecture.
- Broaden and automate protection.
- Minimize remediation and investigation with reliable in-line blocking.
- Streamline work flows through the McAfee Network Security Platform interface.

- Dynamic sandbox analysis that executes the file code in a virtual run-time environment and observes the resulting behavior. Unique among current sandbox solutions, McAfee Advanced Threat Defense configures virtual run-time environments to match the target host based on queries to McAfee ePO software. Analyzing file behavior under the exact conditions of the intended host produces accurate results quickly and efficiently, revealing malicious behaviors that might not be triggered in a generic environment.

These techniques work together in coordination to efficiently identify many types of known and unknown malware. The combination of full static code and dynamic analysis reveals the obfuscated and advanced malware not positively identified through lighter-weight analysis engines.

McAfee Advanced Threat Defense appliances are easily configured to apply only those analyses that have not been performed on upstream IPS sensors, eliminating the performance penalties of redundant inspections. McAfee Advanced Threat Defense appliances scale to throughput capabilities of up to 250,000 objects per day, allowing one advanced malware system to support multiple McAfee Network Security Platform sensors. Along with McAfee Network Security Platform, McAfee Advanced Threat Defense appliances are centrally managed through the web-based interface provided by McAfee Network Security Manager.

An Efficient Closed-Loop Solution for Advanced Threat Prevention

The combination of McAfee Network Security Platform and McAfee Advanced Threat Defense provides exceptionally efficient network IPS protection, along with extraordinarily effective advanced malware detection and response. This is an automated, closed-loop solution that finds sophisticated attacks, freezes them in their tracks, and fixes affected host systems without the need for manual intervention by overworked network operators or security analysts.

For more information on how our solutions can secure your network against stealthy, advanced threats, contact your representative or visit **www.mcafee.com/atd**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com