Advanced Threat Defense for Next-Generation Firewalls

Block zero-day threats and advanced malware with greater efficiency.

The emergence of next-generation firewall products offers IT organizations the closest thing yet to a one-stop solution for network security. By combining traditional perimeter defense functions (packet inspection, network address translation, and VPN support) with application control, intrusion prevention systems (IPS), and other features, the new firewalls deliver a mix of extended security features, a compact footprint, and ease of management.

The one thing most next-generation firewalls cannot do alone is find and stop advanced malware—the stealthy, evasive, often tightly targeted attacks that are slipping through perimeter defenses in increasing number. Although only a small fraction of the overall threat volume, these sophisticated attacks are disproportionately dangerous and the cost to enterprises when they strike could be high.

Sandboxing the Firewall

In response, some organizations are adding dynamic analysis to their next-generation firewalls, typically in the form of out-of-band sandbox appliances. The sandbox runs suspect executables in a secure virtual environment and monitors runtime behavior to detect malicious intent. Often, though, this improvement in detection accuracy is quickly lost due to poor integration and architectural inefficiency.

For instance, most third-party sandbox products can only support a single firewall instance, meaning that one or more appliances must be deployed and maintained at each location. This greatly increases both capital and operating costs. Other limitations of existing sandbox solutions include:

- No automated attack response. The sandbox can only notify a human security analyst when a new attack is detected. The analyst must manually create new firewall blocking rules, then find and fix the endpoints compromised while the sandbox analysis runs its course.
- A reliance on a generic virtual execution environment that may overlook target-specific attack behaviors
- A reliance on dynamic analysis only, rendering the sandbox vulnerable to various strategies for detecting secure environments and delaying execution of revealing behaviors.

Key Advantages

- Combines the industry’s most powerful anti-evasion capabilities with advanced malware detection to automatically find and freeze stealthy attacks hidden in network traffic.
- Adds true static code analysis and target-specific sandboxing to network security with no increase in firewall workloads.
- Plug-and-play threat blocking with no delay for human intervention.
- Supports multiple remote firewall instances with a central sandbox solution.
Superior Protection Against Zero-Day Attacks and Advanced Malware

Our solution to these challenges is a tightly integrated combination of McAfee Next Generation Firewall, an extraordinarily flexible and configurable high-performance firewall, with McAfee Advanced Threat Defense, the industry’s most powerful and complete advanced threat detection appliance. McAfee Next Generation Firewall provides in-band traffic inspection and threat blocking through a set of 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. Working together, these two products discover and block new, unknown, and stealthy advanced threats. In addition, McAfee Advanced Threat Defense offloads compute-intensive inspection of suspect files, allowing McAfee Next Generation Firewall to apply deep packet inspection to high volumes of traffic without impacting network performance.

Intelligence-Aware Security

The Security Connected threat ecosystem enables rapid sharing of extensive real-time threat information, empowering organizations to fight cybercrime with the latest global and local threat knowledge. Security Connected enables McAfee Next Generation Firewall to leverage threat information from a wide variety of sources, including McAfee Advanced Threat Defense, third-party feeds, and other McAfee security solutions such as:

- **ePolicy Orchestrator® (McAfee ePO™) (endpoint security):** Allows McAfee Next Generation Firewall to obtain contextual information from end users and their host systems, providing valuable insight into endpoint security postures. This information can also be used to simplify workflows when troubleshooting or investigating threats or problems.

- **McAfee Enterprise Security Manager (SIEM):** Ensures continuous monitoring and alerting of compliance status, providing real-time situational awareness while improving security posture and reducing event response times.

- **McAfee Global Threat Information:** Provides McAfee Next Generation Firewall with superior reputation intelligence to protect against globally active advanced threats and malware.

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. McAfee Advanced Threat Defense and McAfee Next Generation Firewall collaborate to defeat sophisticated, targeted attacks. Integration with additional McAfee solutions help to provide a complete, end-to-end solution.
Find: Innovative analytical technologies work together to quickly and accurately detect sophisticated threats across multiple protocols.

Freeze: Tightly integrated McAfee security products instantly stop infiltration attempts and contain infected endpoints.

Fix: Scope newly discovered infiltrations across the environment and initiate the endpoint remediation process.

Because the McAfee Advanced Threat Defense solution for McAfee Next Generation Firewall follows the Security Connected approach to enterprise security integration, it delivers operational and defensive advantages that are unique in the industry, including:

- **Evade and detect**: Combines the industry’s most powerful anti-evasion capabilities with advanced malware detection to automatically find and freeze stealthy attacks hidden in network traffic.

- **Centralized advanced malware protection**: One centrally located McAfee Advanced Threat Defense appliance—or a cluster—can remotely support multiple instances of McAfee Next Generation Firewall, as well as network IPS, web gateways, and email gateways.

- **Plug-and-play threat blocking**: Attacks discovered by McAfee Advanced Threat Defense are automatically blocked by all instances of McAfee Next Generation Firewall with no delay for human intervention.

- **Analysis and sandboxing**: Adds in-depth static code analysis and target-specific sandboxing to network security with no increase in firewall loads.

**McAfee Next Generation Firewall**

McAfee Next Generation Firewall protects enterprise networks with high-performance intelligence-aware security supported by real-time updates from the Security Connected ecosystem. This enables us to deliver the industry’s best defense against advanced evasions, along with complete next-generation firewall protections when and where you need them.

McAfee Next Generation Firewall starts with a solid foundation of protections, including granular application control, intrusion prevention system (IPS), built-in virtual private network (VPN) and deep packet inspection—all in an efficient, extensible, and highly scalable unified design. Then we add powerful anti-evasion technologies that decode and normalize network traffic—before inspection and across all protocol layers—in order to expose and block the most advanced attack methods. See the McAfee Next Generation Firewall data sheet for additional information.

**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 and efficient assessment delivers detection accuracy and reliability with 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 uses a comprehensive knowledgebase created and maintained by McAfee Labs, which currently includes more than 200 million signatures.

- Reputation-based detection uses the McAfee Global Threat Intelligence network to detect newly emerging threats.

- Real-time static analysis and emulation quickly finds malware and zero-day threats not identified with signature-based techniques or reputation.
Solution Brief

- Full static code analysis reverse engineers file code to assess all attributes and instruction sets and fully analyzes 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.

- Dynamic sandbox analysis executes the file code in a virtual run-time environment and observes the resulting behavior. Unique among sandbox solutions, McAfee Advanced Threat Defense configures virtual runtime 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. And since many advanced attacks are designed to evade sandbox detection, McAfee Advanced Threat Defense includes innovative techniques to ensure code execution during dynamic analysis.

These techniques work together in coordination to efficiently identify many types of known and unknown malware. The combination of full static and dynamic analysis reveals the obfuscated and advanced malware not positively identified by analysis engines that are more lightweight.

McAfee Advanced Threat Defense appliances are easily configured to apply only those analyses that have not been performed on upstream IPS, next-generation firewall, email gateway, or web gateway sensors, eliminating the performance penalties of redundant inspections. They scale to throughput capabilities of up to 250,000 objects per day, allowing one advanced malware system to support multiple firewalls.

An Efficient Closed-Loop Solution for Advanced Threat Prevention
The combination of McAfee Next Generation Firewall and McAfee Advanced Threat Defense provides exceptionally efficient network edge security and extraordinarily effective advanced malware detection and response. This automated, closed-loop solution finds sophisticated attacks and freezes them in their tracks, without the need for manual intervention by overworked network operators or security analysts.

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