Social networks, cloud applications, blogs, wikis, RSS feeds, and content-sharing sites have become essential business tools for enterprise users, and IT organizations are struggling to make them safely accessible from inside and outside the corporate environment. A cornerstone of this effort is the secure web gateway, a traffic inspection solution that scans inbound and outbound web traffic to find and block hidden threats.

Unfortunately, cybercriminals are working just as hard to exploit the growing volume of enterprise web traffic, and their attacks are ever more stealthy, intelligent, targeted, and costly. Inevitably, an increasing number are slipping past conventional gateway defenses.

**The Sandbox and the Security Sand Trap**

In response, some organizations are adding dynamic analysis to their gateway security in the form of out-of-band sandbox appliances. The sandbox runs suspect executables in a secure virtual environment (with a combination of operating system, browser, and applications) and monitors runtime behavior to detect malicious intent. However, this apparent gain in detection accuracy is often 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 gateway and then begin the task of finding and fixing the endpoints that were compromised during this time. Other limitations of existing sandbox solutions include:

- A costly requirement for one dedicated sandbox appliance for each perimeter security sensor (web gateway, email gateway, firewall, and IPS).
- A single, generic virtual execution environment that may overlook attacks designed for a different host environment.
- A reliance on dynamic analysis alone that renders the sandbox vulnerable to intelligent malware that can detect virtual environments and delay revealing behaviors.

**Key Advantages**

- Finds, freezes, and fixes advanced malware and stealthy attacks hidden in web content.
- Adds true static code analysis and target-specific sandboxing to web security with no increase in gateway workloads.
- Plug-and-play threat blocking with no delay for human intervention.
- A single, centralized sandbox service that can simultaneously support other network security systems.
- Matches each virtual execution environment to the destination host system.
- Reports are automatically integrated into McAfee® Web Gateway workflows.
A Security Connected Web Gateway and Sandbox Solution

McAfee, part of Intel Security, offers a solution to all these challenges: a tightly integrated combination of McAfee Web Gateway, the number-one rated, anti-malware solution for web threats, with McAfee Advanced Threat Defense, the industry’s most powerful and complete advanced threat detection appliance. The web gateway 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 an 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 Orchestration® (McAfee ePO™) software 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**: Tightly integrated McAfee security products instantly stop infiltration attempts and isolate infected endpoints.
- **Fix**: Scan across the environment for newly discovered infiltrations and initiate the endpoint remediation process.

Figure 1. Centralize deployment of advanced network defenses with the Security Connected approach.

Because this solution follows the Security Connected approach to enterprise security integration, it delivers 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 Web Gateway with no delay caused by human intervention.
- **A centralized sandbox service**: McAfee Advanced Threat Defense can simultaneously support other network security systems, including email gateways, firewalls, and intrusion prevention systems. This reduces costs, simplifies security architecture, and shortens the response time from new attack detection to network-wide blocking.
- **A hyper-efficient inspection process**: Web gateway appliances perform initial filtering and malware analysis, and route only the content that cannot be passed or convicted by gateway analytics to the sandbox.
Solution Brief

- **Targeted sandboxing:** McAfee Advanced Threat Defense matches each virtual execution environment to the destination host system. This improves detection accuracy and reduces both analysis time and the number of false positives.

- **Report and workflow integration:** Reports generated by McAfee Advanced Threat Defense are automatically integrated into McAfee Web Gateway workflows, providing users with feedback and scanning results.

**McAfee Web Gateway**

McAfee Web Gateway is the industry-leading anti-malware solution that provides an organization's main line of defense against evolving web-borne threats. It allows an organization to provide flexible, policy-based user access to web applications and resources while greatly reducing the risk to internal systems and information.

McAfee Web Gateway is a proxy platform that first enforces internal access policy on all user-initiated web requests and then applies a series of local and global inspection techniques to determine the nature and intent of all web traffic content in real time. Detection analytics include signature-based antivirus and a combination of reputation (file and source), categorization, and geo-location intelligence provided by McAfee Global Threat Intelligence (McAfee GTI). Finally, McAfee Web Gateway applies a patent-pending proactive approach to zero-day malware detection that combines emulation and heuristics to predict the behavior and understand the intent of a file or executable. Even SSL-encrypted content is decoded and inspected for concealed attacks. The result is an extremely high catch rate and immediate, preemptive blocking that stops attacks dead at the gateway. Independent testing has verified that McAfee Web Gateway identifies and blocks between 95% and 99% of zero-day malware.

McAfee Web Gateway also secures outbound traffic by scanning user-generated content across all key web protocols (HTTP, HTTPS, and FTP) to prevent the loss of confidential information by either innocent user error or covert action by a bot-infested host. Integrated support for data loss prevention (DLP) policies blocks regulated or sensitive data from exfiltration, while built-in file encryption protects information uploaded to external file sharing and collaboration sites, such as Box, Dropbox, and others.

The most powerful feature of McAfee Web Gateway is the integration that gives it access to the insights and capabilities of other McAfee security solutions. Of particular importance to this solution are seamless integrations with the following:

- McAfee Global Threat Intelligence, which collects, analyzes and distributes URL reputation and other data from more than 100 million endpoints in 120 countries around the world, providing up-to-the-minute data on malware-infected sites.

- McAfee Advanced Threat Defense, 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:

- 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.

- Dynamic sandbox analysis that executes the file code in a virtual run-time environment and observes the resulting behavior. Unique among existing sandbox solutions, McAfee Advanced Threat Defense configures virtual run-time environments to match the target host based on queries to McAfee ePO software. It can store and use custom gold images and supports a wide range of virtual machine types. 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. Delivery delays for content under analysis are configurable, giving the security team control of the latency imposed and risk assumed.

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 network security sensors.

An Efficient Closed-Loop Solution for Advanced Threat Prevention

The combination of McAfee Web Gateway and McAfee Advanced Threat Defense provides exceptionally efficient protection against web-borne advanced malware. This automated, closed-loop solution finds sophisticated attacks, freezes them in their tracks, and fixes affected host systems without the need for manual intervention by overworked IT personnel.

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