Solution Brief

Advanced Threat Defense Analysis for Web Gateway

Stop stealthy malware at the network edge.

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, attacks slip past conventional gateway defenses.

A Tightly Integrated Web Gateway and Sandbox Solution

McAfee offers a solution: a tightly integrated combination of McAfee® Web Protection (on-premises McAfee Web Gateway and Web Gateway Cloud Service) with McAfee advanced threat analysis solutions (on-premises McAfee Advanced Threat Defense and McAfee Cloud Threat Detection). Flexible deployment options for both McAfee Web Gateway and advanced threat analysis solutions—physical, virtual, and cloud—support every network.

McAfee 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 analysis solutions enhance detection with advanced malware inspection techniques, including in-depth static code analysis and machine learning to improve sandboxing capabilities and broaden detection of highly camouflaged, evasive threats.

Tight integration reduces time from encounter to containment and protection from advanced threats, enables efficient alert management, and maintains throughput and policy enforcement. McAfee advanced analysis solutions combined with the in-line scanning capabilities of the Gateway Anti-Malware Engine in McAfee Web Gateway provide the strongest protection solution available for Internet-delivered threats.

For a complete end-to-end solution, add McAfee Endpoint Protection, McAfee Threat Intelligence Exchange and McAfee Active Response to optimize security operations response and efficiency with visibility and action, such as issuing new configurations, implementing new policies, removing files, and deploying software updates that can proactively mitigate risk.

Key Advantages

- After McAfee Web Gateway analysis, files that remain suspicious are automatically sent to McAfee Advanced Threat Defense for maximum detection capabilities.
- In-depth static code analysis is added to web security with no increase in gateway workloads.
- Plug-and-play threat blocking acts immediate, without delay for human intervention.
- A single, centralized sandbox service can simultaneously support other network or endpoint security systems.
- Prevent patient zero by withholding files from users during analysis.
- Analysis results are automatically integrated into McAfee Web Gateway workflows.
- Flexible deployment options support every network—physical, virtual, and cloud.

intel Security

Tight integration of this end-to-end solution delivers operational and defensive advantages that are unique in the industry, including:

- **Plug-and-play threat blocking:** Attacks discovered by McAfee advanced analysis solutions 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 from intrusion prevention systems to endpoint. This reduces costs, simplifies security architecture, and shortens the response time from new attack detection to network-wide blocking.
- **A hyper-efficient inspection process:** McAfee 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.
- **Report and workflow integration:** Analysis results generated by McAfee advanced analysis solutions are automatically integrated into McAfee Web Gateway workflows, providing users with feedback and scanning results.
- **Web-only deployments**
  - **Single console management with McAfee ePO™ Cloud:** The McAfee cloud-based management platform, offers a single pane of glass for both the web gateway and advanced analysis.
  - **Off-network protection:** Included in the McAfee Endpoint Protection 10.5 bundle, off-network endpoint traffic is easily routed to the cloud for McAfee Web Gateway protection and policy enforcement, along with advanced analysis.
  - **Avoid backhauling traffic:** Reduce network costs by taking all public internet traffic directly to the cloud for policy enforcement and analysis, rather than backhauling to a central location.

McAfee Web Gateway

McAfee Web Gateway 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 patented proactive approach to zero-day malware prevention that uses machine learning intelligence and emulation to predict the behavior of files and active web content (HTML, JavaScript). 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 by covert action via a bot-infected host. Integrated support for data loss prevention (DLP) policies blocks regulated or sensitive data from exfiltration, while application controls enable risk-mitigation for cloud 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, enhances McAfee Web Gateway protection.
- McAfee Threat Intelligence Exchange enables security solutions to share intelligence to improve protection and reduce incident response times. With threat intelligence from McAfee Web Protection, endpoints are protected as soon as a new zero-day threat is discovered. Contextual information for incident response such as source/destination IP, file hashes, and URLs is shared with your security information and event management (SIEM) solution. McAfee Web Protection also improves its own protection capabilities with information from other sources through McAfee Threat Intelligence Exchange.
- McAfee Endpoint Security can easily and intelligently route traffic to a McAfee Web Gateway appliance while on network and cloud-based McAfee Web Gateway when off-network for policy enforcement and analysis.
- McAfee Advanced Threat Defense, the advanced malware detection component of this solution, automatically receives files that remain suspicious after analysis by the Gateway Anti-Malware Engine, providing maximum threat detection capabilities.

The Sandbox: McAfee Advanced Threat Analysis Solutions

Advanced threat detection solutions from McAfee identify sophisticated malware and convert threat information into action and protection. These solutions optimize existing security investments by enhancing detection with advanced malware inspection techniques, including in-depth static code analysis and machine learning to improve sandboxing capabilities and broaden detection of highly camouflaged, evasive threats.

Tight integration between our advanced threat detection solutions and other McAfee products lowers costs and reduces the time between detection and correction, converting malware identifications into protection to thwart similar attacks. Flexible deployment options support every network—physical, virtual, and cloud.

McAfee Advanced Threat Defense
Detect sophisticated malware and automate protection and investigation workflows to correct and recover post attack. McAfee Advanced Threat Defense provides in-depth static code analysis that enhances behavioral malware analysis and sandboxing capabilities to detect hidden, evasive threats. This unparalleled analysis generates both summary reports to help you understand the scope of an attack and prioritize actions and highly detailed reports with analyst-grade data on malware.

McAfee Cloud Threat Detection
This convenient cloud service plugs into existing your McAfee solutions to identify advanced malware and automate protection. With the efficiencies of a cloud-based solution, you can easily take advantage of significant compute horsepower to operate an array of the latest analysis techniques to enhance detection and optimize existing security investments.

An Efficient Closed-Loop Solution for Advanced Threat Prevention

The combination of McAfee Web Gateway and McAfee advanced threat analysis solutions 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**.

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