SOLUTION BRIEF

Content Threat Removal for Web Gateways

Web browsing with total peace of mind

Content Threat Removal for Web Gateways integrates with McAfee® Web Gateway to ensure that users can access, download, and upload documents and images over the web and social media, secure in the knowledge that they are 100% threat-free.

Content Threat Removal destroys known, zero-day threats, and even completely undetectable exploits concealed in content, without the need to detect the threat or isolate users from the business content they need to do their jobs.

McAfee Compatible Solution

- Deep Secure Content Threat Removal for Web Gateways
- McAfee Web Gateway 7.6.2 and above
- Gives users a totally safe browsing environment, free from the worry of malware-infected documents and content
- Works with existing McAfee Web Gateway solution, dropping seamlessly into the boundary of your cyberdefense
- Delivers a low-risk, low-cost route to total protection from content-borne threats

McAfee COMPATIBLE

DEEP SECURE

Connect With Us

The Business Problem

Organizations depend on the web to share information, inform key business processes, and conduct transactions. But existing detection-based perimeter web defenses are failing to cope with the onslaught of known, unknown, and zero-day threats concealed in business documents and images. Unchecked, this attack vector is a potentially existential threat, leaving the organization with a significant and unquantifiable business risk.

Content Threat Removal for Web Gateways is the only way to defeat not just known but also zero-day and unknown threats in content as it crosses the web boundary because it doesn't rely on detection or sandbox detonation. Instead, it uses a unique process of information extraction and transformation to ensure total protection.

McAfee and Deep Secure Joint Solution

Integrating with McAfee Web Gateway, Deep Secure's Content Threat Removal Platform offers complete threat removal from business documents and image formats without the need to detect the threat or isolate the user.

Content Threat Removal works by extracting business information from content received via the web gateway. The data carrying the information is then discarded, and new safe business information is created from scratch for onward delivery.

The solution also provides the world's first defense against attacks, command and control channels, and the covert exfiltration of sensitive information concealed in images using steganography.

A completely undetectable attack vector, the joint solution is able to totally nullify the threat posed by steganography because, far from trying to detect threats in images, it automatically destroys them as a part of the threat removal process, leaving the user with pixel-perfect, threat-free content.

The security team is satisfied because alerts into their security operations center are reduced and content is safe to consume by the business without impacting the user experience. Every document and image, message and web page, is fully usable and revisable. Content Threat Removal gives users real content—threat-free—not just simplistic facsimiles.

Benefits of integration with McAfee Web Gateway:

- Defeats unknown and undetectable content threats, such as poly-formatted files
- Defeats evasion techniques like steganography
- Maintains the user experience without isolating them from their content
- Leverages existing web gateway investments
- Works alongside with or as a replacement for multiple antivirus scanners and sandboxing

Challenges

- The free flow of business information is the lifeblood of any organization.
- Criminals use regular business content (documents and images) to commit ever more sophisticated cybercrimes.
- 20% of new exploits in content are undetectable until it is too late.

McAfee Solution

- McAfee Web Gateway 7.6.2 and above
- Deep Secure Content Threat Removal for Web Gateways

Results

- Removes document or image-borne threats in web content as it crosses the network boundary
- Destroys the threat posed by image steganography
- Nullifies the threat of malware infiltration in content
- Nullifies the threat of covert data exfiltration.
- Forces attackers out into the open by destroying command-and-control channels
- Zero impact on SOC alerts
- Works with existing web gateway investment

Solution Reference Architecture

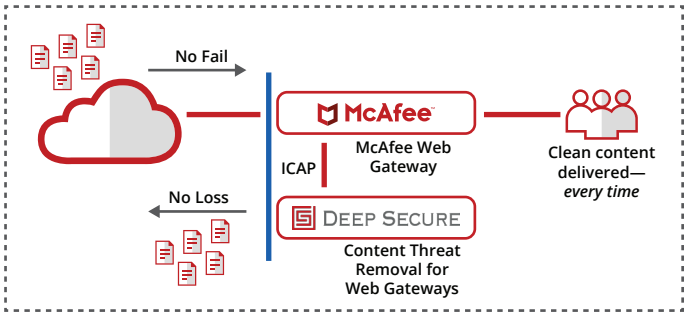

Figure 1. Content Threat for Web Gateways integrates with McAfee Web Gateway using ICAP.

About Deep Secure

In 2016, Deep Secure made a game-changing breakthrough pioneering a disruptive technology that delivers Content Threat Removal (CTR), simultaneously defeating known, zero-day, and even undetectable content threats.

About McAfee Web Protection

McAfee Web Protection uses secure gateway technology to protect every device, user, and location from sophisticated threats. McAfee Web Protection is a unified solution combining on-premises McAfee Web Gateway and cloud-delivered McAfee Web Gateway Cloud Service. When deployed together, both on-premises and cloud solutions can be managed with a single console and with a single shared policy that is applied to devices wherever they travel.

Learn More

For more information, contact your McAfee representative or channel partner, or visit **www.mcafee.com**.

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com