McAfee Gateway Anti-Malware

Security. Connected Intelligence. Performance.

McAfee® Gateway Anti-Malware is a multiplatform threat protection component incorporated into McAfee web gateway products, including McAfee® Web Gateway and McAfee® Web SaaS, McAfee® Advanced Threat Defense, McAfee® Network Security Platform, and is available to McAfee® Security Innovation Alliance Partners via a software development kit (SDK). The engine—designed for deployment at the network perimeter or in the cloud—detects and blocks a broad range of malware threats—everything from viruses and worms to adware, spyware, ransomware, and exploits.

While antivirus products running on desktop computers can use on-access scanning and real-time behavior analysis to effectively detect threats, McAfee Gateway Anti-Malware inspects mobile code in a safe simulation environment, applying patented threat classification technologies to predict potential run-time behavior—before emerging malware threats, zero-day threats, or targeted attacks can enter the network.

The Technologies Powering McAfee Gateway Anti-Malware

McAfee Gateway Anti-Malware uses data mining to collect behavioral, geometric, and semantic characteristics. Once this information has been gathered, unattended machine learning trains the next classifier models for run-time interpretation. Here is how it works:

- McAfee Gateway Anti-Malware disassembles and emulates active content: Windows executables, JavaScript, Visual Basic Script, Java, Flash, PDF, and Microsoft Office documents. Emulation of JavaScript also acknowledges browser specifics, such as the differences between Microsoft Internet Explorer versus Firefox.
- McAfee Gateway Anti-Malware can predict the potential run-time behavior and analyzes geometric and semantic file characteristics.

Connect With Us

- It compares traits against machine-learning trained intelligence to assess overall threat likelihood.
- It reports suspicious files as down-selection for optional malware handling sandboxes or for reporting (SIEM).
- McAfee Gateway Anti-Malware provides 24/7/365 re-training of intelligence based on the latest McAfee worldwide threat knowledgebase.

McAfee Threat Intelligence Exchange and Security Information and Event Management (SIEM) Contribution

McAfee Gateway Anti-Malware computes malware probability scores for suspicious objects and content. This can be used to contribute more local intelligence to threat correlation on McAfee Threat Intelligence Exchange via DXL, which both are available as integration options in McAfee products or for third-party partners through the McAfee Security Innovation Alliance.

In addition, it can enrich the data feeds sent to a SIEM by adding a risk value to the data stream that is sent into a SIEM.

Windows Emulation Technology

In collaboration with Intel Engineering, McAfee Gateway Anti-Malware supports enhanced emulation technology designed to improve detection accuracy and efficiency, adding support for SSE3+, AVX, 64-bit, and more. This enables safe simulation on a CPU level and detection of behaviors at the lowest level possible and at the same time ensure high levels of accuracy when posing as a virtual CPU.

Key Features

- Designed for the network perimeter and cloud with real-time analysis at the gateway
- Allows data to be scanned in transit prior to it being embedded into backend systems, such as SharePoint or file sharing platforms
- Increased protection compared to traditional pattern-based antivirus
- Responds to and fulfills the zero-day protection requirement
- McAfee Security Innovation Alliance partners can build security into an application framework or the ecosystem by leveraging McAfee Gateway Anti-Malware software development kit (SDK)

System Requirements

Supported Platforms:

- Intel or AMD with 64-bit and SSE 4.2 or higher
- McAfee Linux OS, 64-bit or a Linux distribution compatible with CentOS 6 or higher

System Requirements:

- Memory: Minimum 1 GB of memory for GAM processes
- Disk: Minimum 1 GB of free hard disk space for McAfee Gateway Anti-Malware updates
- McAfee Gateway Anti-Malware product ID (SDK)
- McAfee® Global Threat Intelligence (McAfee GTI) serial number (SDK)
- Antivirus product ID (SDK)
- Access to McAfee GTI cloud (This is to determine file and web reputation, which is critical to McAfee Gateway Anti-Malware in order to establish context that allows more accurate file classification.)

Key Benefits

- Optimized for the network
- Applies unique patented emulation and threat classification capabilities.
- Focuses on web objects, such as HTML, JavaScript, Flash, Java, PDF, Microsoft Office documents (and Windows executables) that are in motion
- OEM McAfee Gateway Anti-Malware SDK available to cloud application providers, Infrastructure-as-a-Service (IaaS) providers, and gateway vendors.

Conclusion

Organizations and users can do more over the web today than ever before. Today's web offers a dynamic, real-time user experience. However, the web has also become a more dangerous place, with increasingly sophisticated attacks released every day.

Award-winning McAfee Gateway Anti-Malware provides one of the strongest protection available against web-delivered threats. It empowers organizations with secured internet access, while reducing risk through an advanced security approach that combines powerful, local intent analysis with cloud-based protection powered by McAfee® Labs.

Learn More

Find out **https://www.mcafee.com/enterprise/en-us/products/web-gateway.html**.

McAfee™
Together is power.

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