Customer FAQ

McAfee Endpoint Security

Frequently Asked Questions

Overview

You're facing new challenges in light of the increase of advanced malware. Limited integration between threat detection, network, and endpoint technologies lengthens your response time and complicates remediation. In addition, it's often difficult to translate malware information into action and remediation. To help arm you with the defenses and tools today's advanced threats require, our endpoint protection defenses are built upon an integrated security framework: McAfee® Endpoint Security.

Below are a few frequently asked questions (FAQs):

Q: **What is it?**

A: McAfee Endpoint Security is our collaborative protection for McAfee Endpoint Protection Suite customers. It provides a framework that allows multiple endpoint defense technologies to communicate in real time to analyze and collaborate against new and advanced threats.

Q: **What is new in McAfee Endpoint Security version 10.5?**

A: McAfee Endpoint Security provides a collaborative security framework that reduces the complexity of endpoint security environments, delivers better performance that protects productivity, and offers visibility into advanced threats that speeds detection and remediation responses. Its extensible architecture provides a framework for IT teams who are burdened with multiple solutions to more easily view, respond to, and manage the threat defense lifecycle.

Our 10.5 release introduces several new technologies and improvements:

- **Real Protect.**[1] Applies state-of-the-art machine learning techniques to identify malicious code based on both what it looks like and what it might do (pre-execution analysis) and what it does (dynamic behavioral analysis)—all without signatures.
- **Dynamic Application Containment.**[2] This release includes the ability to contain a single instance of a process.
- **McAfee Client Proxy integration**. McAfee Endpoint Security is now ready for Multi-Layered Web Gateway Security which provides pervasive protection wherever a user travels, eliminating the gap of off-network protection by connecting endpoints to the Web Gateway cloud service.

- **Migration Assistant**. The automatic migration capability now includes McAfee ePolicy Orchestrator® (McAfee ePO™) system tree groups and McAfee VirusScan® Enterprise policies for workstations and servers. The assistant will also now generate equivalent McAfee Endpoint Security Web Control multi-slotted policies during migration.
- **Firewall Module**. HTTPS suffix now available for domain reachability location criteria.
- **Threat Prevention Module**. On-Demand Scans now include a registry scanning option. Administrators can create custom services Access Protection rules and Access Protection rules now include Windows Services. Custom Application Exploit Prevention is available along with McAfee-supplied intrusion prevention system (IPS) signatures. Lastly, Windows Application protection has been added to Exploit Prevention rules.

Q: **What are the key areas of improvement?**

A: McAfee Endpoint Security version 10.5 continues the positive improvements that we've already witnessed in prior releases:

- Zero-impact user scans only run when the device is idle and resumes after shutdown or restart.
- Our framework allows us to deploy future scanners and content without requiring point product binary updates.
- Idle CPU use is 18% faster than McAfee VirusScan Enterprise.
- Boot time is 18% faster than McAfee legacy endpoint security.
- CPU utilization is 89% better than McAfee legacy endpoint security.
- First-time scans for McAfee Endpoint Security 10.1 run more than 30% faster over our legacy endpoint security solutions.

Version 10.2 Improvements:

- Initial on-demand scans are 48% faster over McAfee VirusScan Enterprise.
- Applications launch 57% faster compared to McAfee Endpoint Security 10.1.
- Endpoints shut down 27% faster than McAfee Endpoint Security 10.1.
- File copy with McAfee Endpoint Security 10.2 is 32% faster than deployments of McAfee VirusScan Enterprise/McAfee Host Intrusion Prevention for Server/McAfee SiteAdvisor® Enterprise.

Version 10.5 Improvements over McAfee legacy endpoint security:

- The user interface launches 34% faster.
- Web browsing is 17% faster.
- Reduced impact to endpoint performance.
- File Copy is performed 17% faster.
- Installation of applications occurs 38% faster.
- System boot times are 12% faster.

Q: **What is included with McAfee Endpoint Security?**

A: There are three core modules:

- **Threat Prevention Module.** Includes several new advanced malware scanning features to defend against emerging and targeted attacks. It is a replacement for McAfee VirusScan Enterprise, however unlike VirusScan Enterprise, it includes exploit prevention capabilities similar to those found in Host Intrusion Prevention.
- **Web Security Module.** Prevents users from browsing to malicious or unauthorized websites and serves as a replacement for McAfee SiteAdvisor Enterprise.
- **Firewall Module.** Stops malicious inbound and outbound network traffic and replaces the Host Intrusion Prevention System Firewall feature of Host IPS.

The **Adaptive Threat Protection module** is a new module which is available as part of the Complete Endpoint Threat Protection suite (formerly Complete Endpoint Protection—Enterprise). This module houses Dynamic Application Containment (DAC) and Real Protect technologies. Both DAC and Real Protect integrate with the McAfee Endpoint Security framework. Customers interested in obtaining DAC and Real Protect should contact a sales representative or their partner for information on how they can migrate from their current suites to obtain these capabilities.

Q: **What is Dynamic Application Containment (DAC)?**

A: DAC is a capability that traces and contains threats like greyware and secures 'patient-zero.' It is lightweight and doesn't require a cloud connection so users are protected no matter their location. DAC detects and contains greyware immediately to stop 'infection' before it begins for endpoints both on and off the network. It is available as part of the McAfee Complete Endpoint Threat Protection suite.

Q: **What is Real Protect?**

A: Real Protect uses machine-learning behavior classification to detect zero-day threats in near real time enabling actionable threat intelligence. It stops known threats by comparison and analysis of established malware attributes, then combats and convicts the unknown using behavioral and memory analysis. It unpacks executables to detect sophisticated threats with obfuscated code variants, undetected by static detection methods.

Q: **Do either Real Protect or DAC require an internet connection?**

A: Dynamic Application Containment works with or without a connection while Real Protect requires a connection. However, because Real Protect and DAC leverage McAfee Global Threat Intelligence to get the latest information on threat behaviors and the Real Protect cloud aids in the decision process when determining the intent of behaviors, an internet connection is recommended to help avoid any false positive convictions and to combat the newest emerging threats as they appear in real time globally.

Q: **How does the web gateway cloud service work with McAfee Endpoint Security?**

A: Integration of McAfee Client Proxy into McAfee Endpoint Security enables the endpoint the ability to redirect HTTP and HTTPS traffic transparently to McAfee Web Gateway or McAfee Web SaaS cloud. The re-directed traffic can be scanned for malware, reputation and category-based filtering along with SSL decryption—all managed by McAfee ePO or cloud ePO software for an integrated user experience. Customers using McAfee Client Proxy with McAfee Endpoint Security will see a dramatic reduction in infected endpoints, pervasive protection wherever their users travel, and elimination of the gap caused by off-network protection.

Q: **What are the advantages of the common architecture in the McAfee Endpoint Security platform?**

A: Along with higher performance and better protection, the common architecture allows the modules to work together to provide improved security. For example, when a file gets downloaded, the Web Control module sends a file hash to the Threat Prevention module. The Threat Prevention module triggers an immediate on-demand scan on the file. You can also configure McAfee Global Threat Intelligence sensitivity in McAfee ePO software for these types of scenarios. Based on the results of the scan, the product will take the necessary action.

Q: **Does McAfee Endpoint Security offer full Host Intrusion Prevention for Server functionality?**

A: Customers that use Host Intrusion Prevention for Server currently with McAfee content or who manage signatures provided through McAfee updates will find that McAfee Endpoint Security version 10.5 will meet their needs. Version 10.5 offers most of the Host Intrusion Prevention for Server functionality customers require including the following:

1. Custom Access Protection Rules (File/Registry/Process), including user-based inclusions/exclusions.
2. Exploit Prevention now has enhanced exclusions as well as support for General Privilege Escalation Protection.
3. Data Execution Protection.
4. Supervisor Mode Execution Protection.

Customers will be able to operate McAfee Endpoint Security and Host Intrusion Prevention for Server on the same machine as there is co-existence of both. It is also worth noting that there are advanced features of the Threat Prevention module (Generic Buffer Overflow Protection, Data Execution Prevention, and advanced Access Protection rules) that provide protection against advanced targeted attacks. Lastly, the Threat Intelligence Exchange module can also be added to the McAfee Endpoint Security platform providing further advanced threat protection capabilities.

Q: **Are Macintosh and Linux systems supported?**

A: Yes, McAfee Endpoint Security supports both Mac OS and Linux. Also, both Windows and Macintosh systems can now be managed by the same policy configurations in McAfee ePO software and Cross-OS Threat Prevention Extensions exist to simplify management. Administrators no longer need to manage Threat Prevention policies for the Macintosh platform separately.

Q: **Is there an additional charge or cost?**

A: Current Endpoint Suites customers are entitled to McAfee Endpoint Security at no additional cost. The Adaptive Threat Protection module is available only to Complete Endpoint Threat Protection (formerly CEE suite) customers. Customers may purchase or migrate to the Complete Endpoint Threat Protection suite using cross-grade paths or at the time of renewal. Two additional add-on packages are also available for purchase—McAfee Endpoint Threat Defense and McAfee Endpoint Threat Defense and Response which offer these technologies along with others like McAfee Active Response. Contact your sales representative or partner for more information and for help determining what best fits the requirements of your environment.

Q: What is available to aid in migrating our existing policies?

A: We have created a Migration Assistant tool that will aid you in migrating data to the McAfee Endpoint Security platform.

There are two approaches that can be taken:

- **Automatic Migration**. Customers can create new policies and client tasks automatically, based on current product settings, and assign them to groups and managed systems based on current assignments.
- **Manual Migration**. Customers select the settings to migrate and, optionally, edit them. Manual migration does not retain assignments.

Help is also available from the Intel Security Professional Services team including upgrade assessment, design, pilot planning, and optimization.

Q: How do we get access to McAfee Endpoint Security?

A: You simply log in to McAfee ePO software, and it will be available within Software Manager. You can also get access by using your grant number to download the software package in order to install it via McAfee ePO software.

Q: Where can I go to learn more about McAfee Endpoint Security?

A: Additional materials can be found on the McAfee Endpoint Security landing page and within online help.

[1] The solution includes hosted data centers located in the United States used to check file reputations and store data relevant to suspicious file detection. Although not required, Dynamic Application Containment will perform optimally with a cloud connection. Full Dynamic Application Containment and Real Protect product capabilities require cloud access, active support and are subject to Cloud Service Terms and Conditions.

[2] Ibid.

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

1873_1016
OCTOBER 2016