

# McAfee Endpoint Security

## Frequently Asked Questions

### Overview

McAfee® Endpoint Security is our integrated, centrally managed endpoint protection platform. It replaces legacy technologies like McAfee VirusScan® Enterprise with a single agent for multiple technologies, including our most advanced defenses like machine learning-based analysis and behavioral monitoring.

#### Q: What is it?

**A:** McAfee Endpoint Security is our modern, integrated endpoint security platform. It replaces several legacy McAfee products that were deployed as point products (VirusScan Enterprise, McAfee SiteAdvisor®, McAfee Host Intrusion Prevention [McAfee Host IPS], and others) with a single-agent architecture and integrated advanced defenses like machine learning analysis, containment, and endpoint detection and response (EDR).

#### Q: What are some of the new technologies in McAfee Endpoint Security?

**A:** Our latest release offers:

- **Machine learning:** Pre-execution and post-execution analysis detects zero-day threats by what they look like and how they behave

- **Application containment:** Contains malicious applications and processes on endpoints even when they are offline.
- **Behavior monitoring:** Records process-level behavior while analyzing for attack techniques and procedures (TTPs). Alerts are prioritized with attack “playback” of events.
- **EDR:** Integrated, easy-to-use incident hunting and response.
- **Migration assistant:** A tool for existing customers to make migration easy. Performs automatic tasks and moves your existing policies into McAfee Endpoint Security.

Connect With Us



## CUSTOMER FAQ

**Q: How is it different from VirusScan Enterprise?**

**A:** McAfee Endpoint Security outperforms VirusScan Enterprise, giving you a 25% higher protection rate. It also simplifies your environment by providing a single agent to deploy and manage in your environment. The number of policies you'll manage are also reduced, saving you time while simplifying workflows. Customers have saved as much as 40 hours per week by moving to McAfee Endpoint Security.

**Q: What capabilities of McAfee Endpoint Security replace VirusScan Enterprise, SiteAdvisor, and McAfee Host IPS?**

**A: Threat Prevention:** Includes several new, advanced malware scanning features to defend against emerging and targeted attacks. It is a replacement for VirusScan Enterprise. However, unlike VirusScan Enterprise, it includes exploit prevention capabilities similar to those found in McAfee Host Intrusion Prevent to mitigate a broader set of endpoint threats, such as fileless attacks, ransomware, and zero-day attacks.

**Web Security:** Prevents users from browsing to malicious or unauthorized websites and serves as a replacement for SiteAdvisor Enterprise.

**Firewall:** Stops malicious inbound and outbound network traffic and replaces the host intrusion prevention firewall feature of McAfee Host IPS.

**Q: What does Application Containment do?**

**A:** It protects endpoints from encounters with zero-day threats that were not otherwise prevented or detected. By monitoring the behavior of applications and stopping any malicious action during run-time, damage is avoided. It is lightweight and doesn't require a cloud connection, so users are protected, whether they are on or off the network.

**Q: How does the McAfee machine learning capability work?**

**A:** We use machine learning behavior classification to detect zero-day threats in near real time. Threats are analyzed through comparison with and analysis of established malware attributes. Analysis is further expanded through behavioral and memory analysis techniques. Executables are unpacked to detect sophisticated threats with obfuscated code variants that can generally remain undetected by static detection methods alone.

**Q: Do the machine learning or Application Containment technologies require an internet connection?**

**A:** Because McAfee Global Threat Intelligence is leveraged to get the latest information on threat behaviors and the 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.

## CUSTOMER FAQ

**Q: How long does it take to migrate from VirusScan Enterprise?**

**A:** Customers have been able to migrate as many as 14,000 endpoints within a week by just spending a few hours a day on migration. Migration time will vary, depending on the total number of endpoints and on your environment. If you have up-to-date versions of the McAfee agent, McAfee® ePolicy Orchestrator® (McAfee ePO™) software, and VirusScan Enterprise, you're ready to migrate immediately. If out-of-date versions are in use, updates may be required first. We also have migration software tools, best practice guides, training, and professional services available to help guide and simplify migrations as well.

**Q: You refer to McAfee Endpoint Security as a platform—what does that mean?**

**A:** Unlike legacy McAfee technologies, which were managed and deployed as point products, McAfee Endpoint Security unites its capabilities on a common architecture that uses a single agent. This provides higher performance and better protection in addition to allowing components to work together for stronger threat analysis and insights. Because an integrated approach is used, McAfee Endpoint Security provides a platform to add integrated defenses now and in the future instead of introducing more point products and management consoles.

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

**A:** Yes, customers that use McAfee Host IPS currently with McAfee content or those that 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 McAfee Host IPS functionality customers require, including:

- Custom access protection rules (file/registry/process), including user-based inclusions/exclusions
- Exploit prevention with enhanced exclusions, as well as support for general privilege escalation protection (GPE)
- Data execution protection (DEP)
- Supervisor mode execution protection (SMEP)

Customers will be able to operate McAfee Endpoint Security and McAfee Host IPS on the same machine, as co-existence is supported.

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

**A:** Yes, both Mac OS and Linux are supported. Also, both Microsoft Windows and Macintosh systems can be managed by the same policy configurations in McAfee ePO software and cross-OS Threat Prevention extensions exist to simplify management.

## CUSTOMER FAQ

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

**A:** Current McAfee Endpoint Suites customers are entitled to McAfee Endpoint Security at no additional cost. However, some features may require an additional purchase, depending on your current entitlement. Contact your sales representative or partner for more information and for help determining what best fits the requirements of your environment.

**Q: How do we move our existing policies to McAfee Endpoint Security?**

**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 McAfee 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 into McAfee ePO software, and McAfee Endpoint Security will be available within Software Manager. You can also use your grant number to download the software package and install it via McAfee ePO software.

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

**A:** Additional materials can be found on [this page](#) and in our [expert center](#).



2821 Mission College Blvd.  
Santa Clara, CA 95054  
888.847 8766  
[www.mcafee.com](http://www.mcafee.com)

McAfee and the McAfee logo, VirusScan, SiteAdvisor, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2018 McAfee, LLC. 3774\_0218  
FEBRUARY 2018