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:

- **Rollback remediation:** Automatically reverses changes made by malware and returns systems to a healthy state.
- **On-demand scanning:** More control over on- demand scanning (ODS) using Command Line Scanner and a new CPU limiting capability.
- **Story Graph:** Visualizes threat event details in an easy-to-read format.
- **Edge Browser support:** All web control functionality available in the Microsoft Edge browser.
- **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.

Connect With Us

- **Integration with MVISION EDR:** McAfee Endpoint Security works with our Endpoint Detection and Response (EDR) tool by surfacing details about threats and threat events for incident responders.
- **Migration assistant:** A tool for existing customers to make migration easy. Performs automatic tasks and moves your existing policies into McAfee Endpoint Security.

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 IPS 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: How does rollback remediation work?

A: When malware attempts to compromise and endpoint, malicious actions like calling on **executables that grant system access or filenames** are altered to deliver a payload. With McAfee Endpoint Security rollback remediation enabled, a system snapshot is established and changes that are made are recorded. When McAfee Endpoint Security detects threats, rollback remediation will automatically reverse the system changes made and return a system to its previously healthy state. This keeps the user and system productive while also saving a support call and a potential lengthy remediation period if a system re-image would have been required.

Q: What is the Story Graph?

A: The Story Graph is a data visualization tool introduced with McAfee Endpoint Security version 10.7 that can be viewed with the management console Threat Event area. It is designed to present threat events in an at-a-glance format with a tree of events to allow administrators to easily see the

lifecycle, connected actions, and severity of a threat. Using the Story Graph, event and process details can be examined more rapidly and speed the time for an administrator to understand how a threat arrived and make policy changes to prevent future threats faster.

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.

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 10.7 will meet their needs. Version 10.7 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.

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 migrate to McAfee Endpoint Security?

A: The Endpoint Upgrade Assistant (EUA) is the recommended path for migrating to McAfee Endpoint Security. It is a McAfee ePO software **package specifically designed to remove VirusScan** Enterprise and legacy products from managed endpoints. The EUA will download the McAfee® Agent and McAfee Endpoint Security from your McAfee ePO server and then automatically perform an upgrade and install McAfee Endpoint Security. Your local VirusScan Enterprise and McAfee Host IPS product policies will also be migrated to McAfee Endpoint Security.

Alternatively, you can choose to perform your migration manually. In a 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 for customers needing help with deployments, 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, in our expert center, and in our upgrade deployment guide.

6220 America Center Drive
San Jose, CA 95002 888.847 8766
www.mcafee.com