Technical Brief

How McAfee Endpoint Security Intelligently Collaborates to Protect and Perform

McAfee® Endpoint Security 10 provides customers with an intelligent, collaborative framework, enabling endpoint defenses to communicate, share intelligence, and take action against advanced threats. This framework allows these defenses to perform together in real time. The increased performance and management functionality improvements McAfee Endpoint Security 10 Security provides simplify ease of use for administrators and keep users productive.

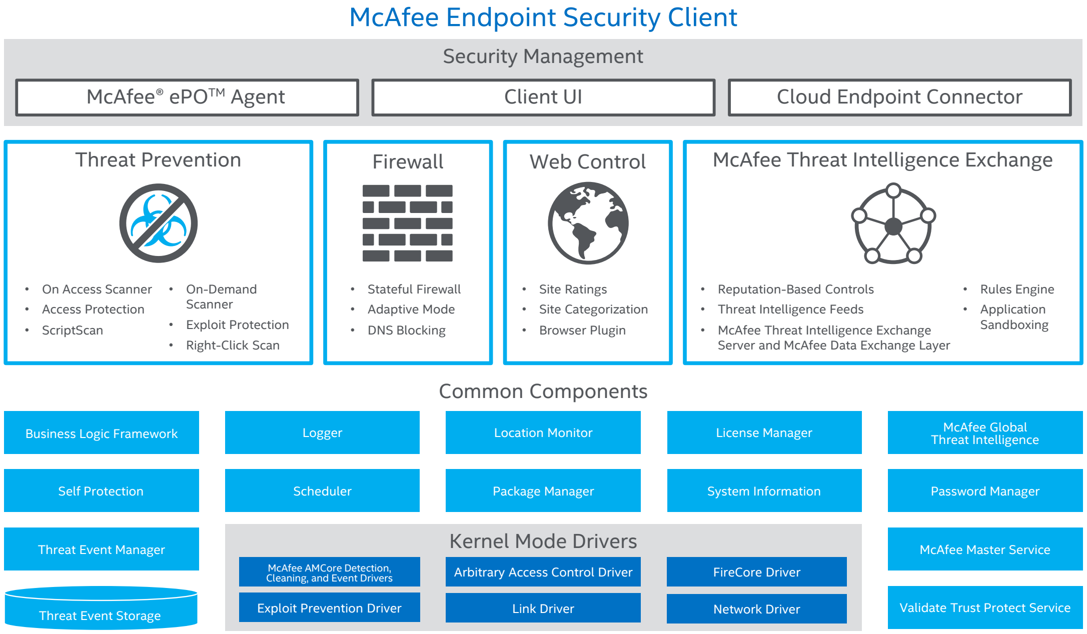
Stronger Protection that Works Together

Products that operate in silos not only make administrators less productive, they don't allow the insights gained from one solution to inform and strengthen others. This is one reason why McAfee Endpoint Security 10 was built with an integrated framework that allows individual Intel Security defenses to work together while also helping to deliver an integrated security system that enables the exchange of actionable information between products with better performance.

One inherent advantage of this structure is the ability to deliver Firewall, Threat Prevention, and Web Control modules more quickly, speeding the time to protection by eliminating the need to recreate common services. Modules can work off each other, enabling the modules, interacting in real time, and learning from each other as they analyze and act on new potential malware and advanced threats.

Revamped to Reduce Redundancy

The McAfee Endpoint Security 10 client creates a common service layer—the McAfee Endpoint Security Platform. Common services such as logging, installation, data updating, and self-protection reside on a single layer.



McAfee Endpoint Security Client

Security Management

McAfee® ePO™ Agent | Client UI | Cloud Endpoint Connector

Threat Prevention
- On Access Scanner
- Access Protection
- ScriptScan
- On-Demand Scanner
- Exploit Protection
- Right-Click Scan

Firewall
- Stateful Firewall
- Adaptive Mode
- DNS Blocking

Web Control
- Site Ratings
- Site Categorization
- Browser Plugin

McAfee Threat Intelligence Exchange
- Reputation-Based Controls
- Threat Intelligence Feeds
- McAfee Threat Intelligence Exchange Server and McAfee Data Exchange Layer
- Rules Engine
- Application Sandboxing

Common Components

Business Logic Framework | Logger | Location Monitor | License Manager | McAfee Global Threat Intelligence

Self Protection | Scheduler | Package Manager | System Information | Password Manager

Threat Event Manager | McAfee Master Service

Threat Event Storage | Validate Trust Protect Service

Kernel Mode Drivers

McAfee AMCore Detection, Cleaning, and Event Drivers | Arbitrary Access Control Driver | FireCore Driver

Exploit Prevention Driver | Link Driver | Network Driver

Figure 1. The McAfee Endpoint Security 10 client architecture unites multiple modules, enabling them to communicate and work together to deliver stronger protection.

For an example of how the client works, let's say one of your end users downloads a malicious file from the web. In McAfee Endpoint Security 10, the Web Control module sends a file hash of the file that is being downloaded to the Threat Prevention module. The Threat Prevention module then triggers an immediate on-demand scan of the file. Using McAfee Global Threat Intelligence (McAfee GTI)—which correlates real-world data and the latest threat information to notice anomalous behavior and predict and protect across McAfee security products—you can configure sensitivity in McAfee® ePolicy Orchestrator® (McAfee ePO) software for these types of scenarios. Then, based on the results of the scan, the necessary actions will be taken.

How Does McAfee Endpoint Security 10 Work?

Here's what happens when a user downloads a malicious file from the web.

1. A file hash is sent from Web Control to Threat Prevention, triggering an on-demand scan (ODS).
2. Malicious files are detected and blocked before they have full access to the system.
3. Forensics data is captured (source URL, file hash).
4. Event data is shared with other modules and McAfee ePO software and is visible in the client user interface.

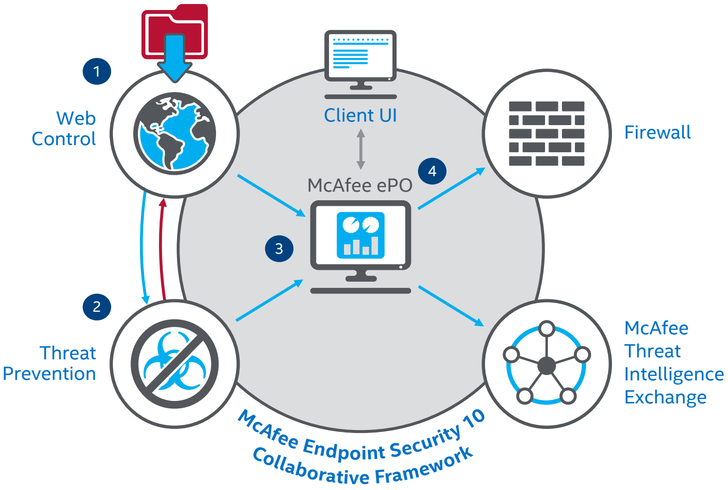

1
Web Control
Client UI
McAfee ePO
4
Firewall
3
2
Threat Prevention
McAfee Threat Intelligence Exchange
McAfee Endpoint Security 10 Collaborative Framework

Figure 2. How McAfee Endpoint Security 10 handles malicious file downloads from the Internet.

This provides significant advantages, as the file is scanned at a point of entry with a higher McAfee GTI sensitivity level since it is coming from the web—before it has full access to the system. This also allows the product to capture better forensics data (such as source URL, attack vector, and file hash) if detection occurs, which is logged locally in user-understandable language and sent to McAfee ePO software. This event data helps administrators better understand where they are exposed and rapidly take action. In short, McAfee Endpoint Security 10 provides faster scanning, more actionable information, and better performance.

Customers that leverage the available McAfee Threat Intelligence Exchange are able to gain even stronger insights into threat events. McAfee Threat Intelligence Exchange does this by combining integrated intelligence from multiple sources with contextual data from the encounter to enable better decision-making to handle never-before-seen and potentially malicious files. McAfee Threat Intelligence Exchange also combines imported threat information from McAfee Global Threat Intelligence, third parties, and Structured Threat Information eXpression (STIX) files with locally collected intelligence from your security solutions to share advanced threat insights across your entire network in real time.

Working in conjunction with these modules is another key innovation: the McAfee Anti-Malware Core (McAfee AMCore) engine. This next generation anti-malware framework is built on five pillars:

- **Intelligent trust:** Scans run much faster by whitelisting all files previously scanned and deemed safe, requiring only a limited set of untrusted files' events to be scanned. For instance, if a Microsoft installer is trusted, all files dropped by that installer are trusted. However, if an installer has not yet been scanned or is suspicious, a full set of its events is scanned.
- **Context and reputation aware:** McAfee AMCore quickly detects known threats by utilizing cloud lookups for known blacklisted and whitelisted files, while using traditional generics and heuristics to classify each.
- **Adaptive behavioral scanning:** Malware families follow certain behavioral patterns. The McAfee AMCore engine introduces events data locally, feeding that data to the backend. If any file or process is acting maliciously, McAfee AMCore increases the event and collects more data. If the file or process is deemed malicious, McAfee AMCore takes action.
- **Built-in false mitigation:** When relying on behavioral patterns, false detections can occur. McAfee AMCore helps prevent false positives by performing local checks for files signed against a list of trusted publishers, and McAfee GTI reputation checks against file hashes.
- **Performance and future expansion:** McAfee AMCore is extensible, enabling Intel Security to deploy future scanners and content without requiring point product binary updates. This also means a reduction in .DAT size (approximately 55%) and significantly faster .DAT updates.

Management That Doesn't Sacrifice Flexibility or Simplicity

Complexity is the enemy of productivity. This philosophy inspired the McAfee Endpoint Security 10 client to be highly intuitive. If a user wants to run a scan or if a help desk wants to retrieve logs, the client is easy to navigate. The user interface keeps things simple, as well, by providing meaningful information in understandable language with information on overall status, event management, received updates, and scans in progress. To accommodate an increasingly mobile workforce, McAfee Endpoint Security 10 was designed for use with touch screens, such as Windows tablets for even greater ease of use.

McAfee Endpoint Security 10 architecture also offers greater management flexibility. Administrators still have the option to pick and choose the protection modules they want for their endpoints based on their system type and environment. Making module choices can be done at any time—during installation or once deployed. For example, an administrator who hasn't decided whether or not to use the Firewall module can simply install it and disable it. If they decide to use the Firewall module in the future, they can easily enable it through the McAfee ePO platform. An administrator who knows they will never use the Firewall module can simply choose not to install it on the endpoints during the installation process. Threat Prevention and Web Control modules will continue to function, and there will be no references to the Firewall module in the client UI.

Raising the simplicity bar even further, McAfee Endpoint Security 10 leverages the integrated endpoint-assisted security installation (EASI) installer to offer an accelerated and simplified deployment process. The administrator experience has been optimized for downloading, installing McAfee ePO software, configuring policies, and deploying endpoint products. The new client installer decreases install time to approximately 90 minutes for McAfee ePO. The modular plug-and-play protection client allows products to be added with ease. Administrators can save time and stress with a one-click installation experience.

Performance That Understands Time is Money

Protection and simplicity aren't worth much without performance. That's why McAfee Endpoint Security 10 was designed to help ensure reliable performance so everyone can get to work.

- **Functionality de-duplication:** The integrated common service layer in McAfee Endpoint Security 10 eliminates redundancies caused by multiple point product installations on a single machine. Now there is only one firewall, one self-protection, one access protection, and one buffer overflow protection. Functionality de-duplication also helps to reduce confusion over what to install. The Memory Protection capability combines memory protection from McAfee VirusScan® Enterprise, McAfee Host Intrusion Prevention System, and McAfee Application Control in the client. This means that you will always receive maximum memory protection as part of the client even if you only use the Threat Prevention module.
- **Faster performance and lower system impact:** McAfee Endpoint Security 10 provides faster performance on full and quick system scans; the booting system; suspend, hibernate, and resume; and network operations (UNC File Copy).
- **Improved protection effectiveness:** McAfee Endpoint Security 10 enhances the protection that works well today with additional scanners provided by our McAfee AMCore integration. In a third-party test, the key areas of usability, performance, and protection were analyzed. McAfee Endpoint Security 10 scored a total of 17.5 out of a possible 18, with marked improvements over previous Intel Security products demonstrated in the performance and protection test results.
- **Zero-impact user scans:** McAfee Endpoint Security 10 allows administrators to configure on-demand scans in "scan on idle" mode. When this is enabled, on-demand scans will only run when the system is idle. User systems are idle during certain time periods, such as when users take lunch or coffee breaks. The new feature takes advantage of this idle time to perform scans. When the user is active, the scan pauses automatically. Even if a user reboots, the scan will not terminate; rather, it will simply stay paused until idle. With this advancement, users may never notice scans again.

Manage on Your Terms

McAfee Endpoint Security 10 provides a single pane of glass to manage all of your endpoints.

- **McAfee ePO On-Premises (5.1 and higher)**: It's easy to deploy one product that includes all of the recommended baseline protection technologies.
- **Unmanaged/standalone**: Those who don't use an Intel Security management system will find it easy to install the new endpoint security client using the integrated installer. This can also be used for deploying the product using third-party deployment tools.

Intelligent, Effective Protection Starts Here

McAfee Endpoint Security 10 offers a holistic approach to security for businesses. You'll no longer need multiple vendors or point products to protect your systems. Instead, you'll be able to replace, reduce, and simplify your environment with intelligent endpoint protection, actionable threat forensics, strong protection performance, and a collaborative protection framework built with today and tomorrow in mind. As an IT professional, you can rest assured, knowing your focus won't be on cumbersome deployments, time-consuming day-to-day management, or complex interfaces. With McAfee Endpoint Security 10, securing endpoints takes minutes, you get management that you can take with you, and you gain more time to focus on keeping your IT focus strategic.

Learn more about McAfee Endpoint Security 10 at **www.mcafee.com/nextgenendpoint**.

Learn more about McAfee Complete Endpoint Protection at **www.mcafee.com/endpoint**.

Download the free trial at **http://www.mcafee.com/us/downloads/endpoint-protection/endpoint-suite-evaluation-center.aspx**.

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