Technical Brief

How McAfee Endpoint Security Intelligently Collaborates to Protect and Perform

McAfee® Endpoint Security provides customers with a collaborative framework that enables endpoint defenses to be adaptive and intelligent, leveraging observations from multiple sources to detect and inform each other in real time and halt emerging forms of attacks. In this paper, we look at how this integrated approach boosts performance, productivity, and speeds detection and containment of threats.

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 was built with an integrated framework that allows individual McAfee defenses to work together while also helping to deliver an integrated security system that enables the exchange of actionable information between products more efficiently than individually deployed and managed solutions.

One inherent advantage of this structure is each of the integrated components (Firewall, Threat Prevention, Web Control, and Adaptive Threat Protection) can adapt using updated information that can automate workflows to stop future attacks. Modules can work off each other, interacting in real time, and can learn from each other as they analyze and act on new potential malware and advanced threats.

Security That Doesn't Operate in Silos

The McAfee Endpoint Security 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.

intel Security

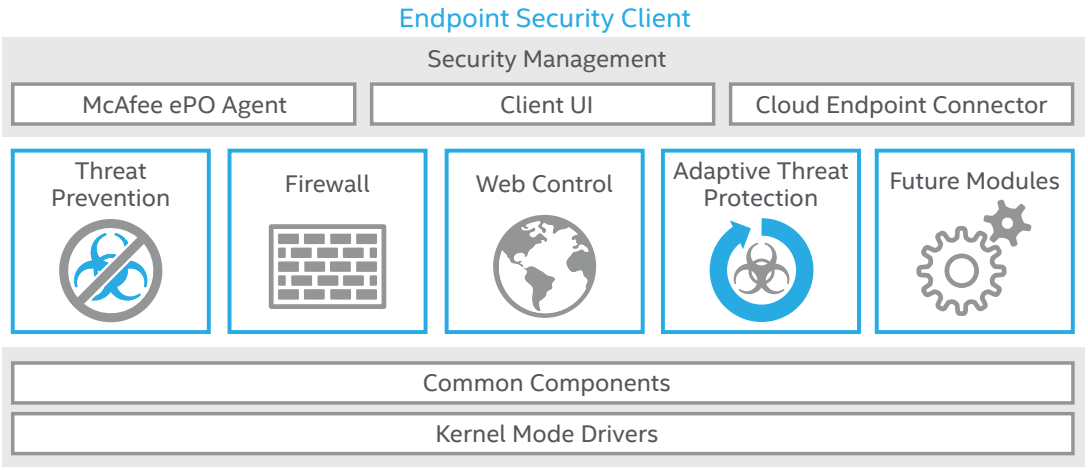

Figure 1. The McAfee Endpoint Security client architecture unites multiple modules, enabling them to communicate and work together to deliver stronger protection.

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, 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 Work?

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

Use Case

Download of a malicious file from the web

A file hash is McAfee Web Control to McAfee Threat Prevention, triggering an ODS.

Malicious file are detected and blocked before they have full access to the system.

Forensics data is captured (source URL, file hash, and other information).

Event data is shared with other modules and McAfee ePO software and is visible in client user interface.

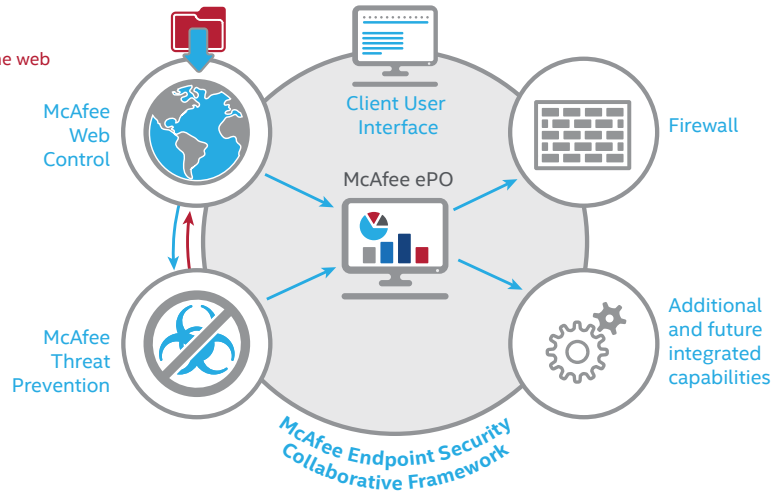

Figure 2. How McAfee Endpoint Security handles malicious file downloads from the internet.

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 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.

How DAC Works
Using McAfee Endpoint Security Threat Intelligence

Figure 3. McAfee Endpoint Security and Dynamic Application Containment.

A good example of the available defenses that integrate with McAfee Endpoint Security is Dynamic Application Containment (DAC).[1] DAC protects by containing unknown applications and preventing them from performing malicious behavior. The unknown application is able to run, but will be limited as to what actions can be performed.

DAC provides an extra layer of security, by reducing the ability of greyware to make unexpected changes on the system and is lightweight minimizing impact to your endpoints. DAC can look at what an application is trying to do without endangering the endpoint. It will restrict and secure 'patient zero' at the first sign of suspicious activity. It also provides greater flexibility to Security Administrators when dealing with applications with unknown reputations

As shown in the above example, DAC also allows other defenses to perform further analysis of the unknown file, such as detonation within a sandbox (McAfee Advanced Threat Defense) or post-execution process tracing (McAfee Active Response). This allows for greater visibility into the behaviors of the applications that are running within the environment and the ability to identify indicators of compromise (IoCs).

Zero-day malware often hides by obfuscation, which means that it uses methods to mask and avoid detection. To combat threats like these, McAfee Endpoint Security can call upon Real Protect,[2] a machine learning technology. Real Protect compares in detail, many attributes, and uses a math-based machine learning model to compare known-malware elements and unmask the attack. Real Protect can also go beyond static analysis by performing dynamic behavior analysis to detect malware that attempts to hide in the file system, but performs malicious actions as a process. Analysis happens on the endpoint and compares in the cloud what it sees with a wealth of threat behaviors to reach a conclusion. If convicted as malicious, Real Protect will then take action to remediate the threat, learning from the behaviors it has witnessed.

Management That Doesn't Sacrifice Flexibility or Simplicity

Complexity is the enemy of productivity. This philosophy inspired the McAfee Endpoint Security 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 was designed for use with touch screens, such as Windows tablets for even greater ease of use.

McAfee Endpoint Security 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 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.

Manage on Your Terms

McAfee Endpoint Security keeps management simple and flexible.

- **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.
- **Cross-platform support:** Protection for desktops and servers across Windows, Macs, and Linux. Windows and Mac systems can be managed with common policies with the data gathered by endpoints of either operating system sharing insights with McAfee ePO software.

Performance That Understands Time Is Money

Protection and simplicity aren't worth much without performance. That's why McAfee Endpoint Security 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 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 provides several performance improvements compared to legacy McAfee products. Initial on-demand scans are 48% faster, Idle CPU use is 18% faster, file copy is 32% faster, and endpoints shut down faster with McAfee Endpoint Security. Adaptive scanning boosts performance and productivity by avoiding scans on known, trusted processes while prioritizing those that appear suspicious.
- **Zero-impact user scans:** McAfee Endpoint Security 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.

Intelligent, Effective Protection Starts Here

McAfee Endpoint Security 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, 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 at **www.mcafee.com/nextgenendpoint**.

Learn more about McAfee Endpoint Threat Protection at **www.mcafee.com/ETP** and McAfee Complete Endpoint Threat Protection at **www.mcafee.com/CETP**.

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

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