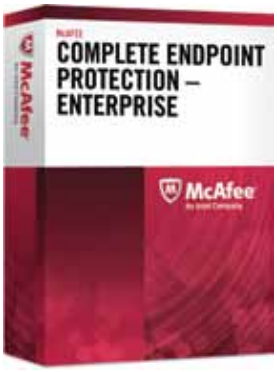
McAfee
An Intel Company

McAfee Complete Endpoint Protection—Enterprise

Strong, fast, scalable defense for every device, every threat



The McAfee® Complete Endpoint Protection—Enterprise suite extends the industry's highest scoring threat protection to all of your devices, safeguarding systems and data with dynamic application control, behavioral zero-day intrusion prevention, instant risk assessment, hardware-enhanced security to defend against rootkits, and integrated global threat intelligence. Unprecedented real-time visibility into security and risk and centralized management empower your IT security team to keep employees productive and endpoints secure.

Key Advantages

- Deploy fast, top-rated hardware-enhanced protection to protect against today's stealthy, zero-day, and advanced persistent threats (APTs).
- Choose dynamic application control to reduce the application attack surface without labor- and time-intensive whitelist management.
- Use the McAfee ePO platform for unified management across all protection methods across all your endpoints: PCs, Macs, Linux systems, virtual machines, servers, smartphones, and tablets.
- View security health and act in real time to remediate vulnerabilities and stop threats in their tracks.
- Direct security efforts where they are needed most based on risk, relevance, and countermeasures in place.

Built for strength, speed, and simplicity, McAfee Complete Endpoint Protection—Enterprise suite makes it easy to get security right, from turnkey installation to rapid response. One unified solution covers all the devices in your enterprise—PCs, Macs, Linux systems, virtual machines, smartphones, tablets, and servers. It reduces management complexity and cuts costs, while protecting endpoints ruthlessly against rootkits, mobile malware, targeted web and email attacks, and persistent threats. You achieve a level of powerful, efficient protection and management that's just not possible with individual point products.

Complete Simplicity

Installation is simple—in as few as four clicks and 20 minutes, your security is ready to go. Unified, real-time management with McAfee® ePolicy Orchestrator® (McAfee ePO™) software streamlines your policy management workflow across all of your devices and provides a single pane of glass for visibility. The suite integrates instant access to critical security data and proven responses within the natural workflow, so administrators can respond as much as 10 to 1,000 times faster.

With dynamic application control, trusted updaters and users can install new software if they follow authorized processes, eliminating the frustrations and delays of manual whitelisting. And we include tools that help you easily manage risk and prioritize protection for your most important assets, based on which emerging threats are affecting which assets and whether you have proper mitigations in place.

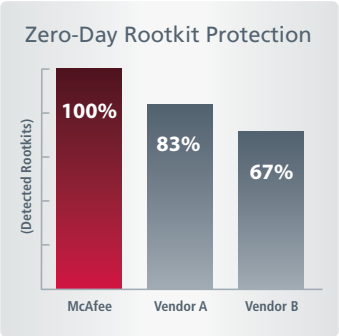
Complete Protection

When it comes to threat protection, you can't do any better than McAfee Complete Endpoint Protection—Enterprise. Only McAfee takes protection into the hardware and throughout the application layer to ensure the best results.

In a recent NSS Labs test, McAfee achieved the highest possible score in defending against exploit and evasion attacks. In a study by West Coast Labs, McAfee scored 100% in malware protection with the combination of McAfee Application Control, McAfee VirusScan® Enterprise, and McAfee Host Intrusion Prevention. Dynamic whitelisting through application control protects users from harmful applications and code originating from zero-day threats or advanced persistent threats (APTs).

Included in the suite and available only from McAfee is hardware-enhanced protection beyond the operating system through McAfee Deep Defender. It earned a perfect score in a recent comparative review by AV-TEST on protection against stealthy attacks like rootkits.

Beyond signatures and beyond the operating system, behavior and reputation systems integrate with cloud-based McAfee Global Threat Intelligence™ to protect against cyberthreats across all vectors—file, web, message, and network. Only McAfee connects endpoint and network security to block and tackle malware everywhere in your network. We see more, know more, and protect our customers better.



Source: AV-TEST report, *Proactive Rootkit Protection Comparison Test.*

Complete Performance

Through focused scans and focused actions, McAfee Complete Endpoint Protection—Enterprise suite provides you with trust-based security that supports business rather than slowing it down. Superior performance across all platforms comes from advanced smart scanning and memory management techniques that optimize CPU and memory usage. Customers using application control experience ultra-low CPU and memory usage, while avoiding excessive scans and .DAT update cycles.

Protect Endpoints Against All Phases of Malicious Attack

Let's take a look at how modern threats operate and how McAfee Complete Endpoint Protection—Enterprise and McAfee Global Threat Intelligence defend you against them at every stage of attack.

McAfee Leads the Industry in Threat Protection

- In a recent NSS Labs *Corporate AV/EPP Comparative Analysis, Exploit Evasion Defenses,* McAfee achieved the highest possible score in protection against exploit and evasion attacks.
- McAfee core endpoint anti-malware products (McAfee VirusScan Enterprise, McAfee Host Intrusion Prevention and McAfee SiteAdvisor® Enterprise) achieved the highest block rate and an overall score of 97 percent for all threats blocked in the exploit protection test analyzed in the NSS Labs *Corporate AV/EPP Comparative Analysis, Exploit Protection Defenses* report.
- In a comparative review by AV-TEST, McAfee Deep Defender scored 100% in proactive protection against zero-day rootkit and kernel stealth attacks.
- A recent West Coast Labs study showed that McAfee Application Control, McAfee Host Intrusion Prevention, and McAfee VirusScan Enterprise provided 100% malware protection against 7,300 malware samples by allowing only authorized software to run on COE and fixed-function computers.

Four Phases of an Attack

McAfee researchers have studied the vast majority of attacks and have categorized them into four distinct phases, plus a pre-attack phase. Here is how some of the key security technologies in McAfee Complete Endpoint Protection—Enterprise suite block these attacks in your environment. The sooner attacks are stopped, the lower your costs and risk of data loss.

Phases of an Attack	How McAfee Complete Endpoint Protection—Enterprise Defends You
Pre-Attack Phase: Attacker attempts to find a vulnerable system.	• Instant visibility into the security health of your endpoints allows you to reduce the attack surface easily and efficiently. • You can prioritize risk based on real-time threat updates, threat relevance, and countermeasures in place.
Phase 1: Contact is made with a system, usually through a malicious website that hosts and downloads malware. Other access points are removable media, unsolicited messages, and network access through misconfigured or unsecured wireless networks.	• Safe surf and search and web content filtering reduce the chance of exposure to or drive-by downloads of malware. • Device control blocks use of unapproved storage media that may be infected with malware. • Network connection reputation shuts down botnets, denial-of-service attacks, and malicious traffic. • Mobile anti-malware prevents compromise of smartphones and tablets.
Phase 2: Code runs on target machine to exploit vulnerabilities in common, legitimate applications or in the operating system itself. If the malware can subvert the protections in existing software, it can write its code to disk.	• Below-the-operating-system detection enhanced by hardware blocks kernel and boot-level rootkits. • Host intrusion prevention blocks exploits and shields unpatched vulnerabilities. • Dynamic application control allows installation of only known good files or applications based on dynamic whitelisting. • On-access scanning monitors memory and network traffic. • Secure container for mobile email protects enterprise data on devices.
Phase 3: Malicious code is hidden on the system and made to persist, so that it can survive reboot and stay hidden from security measures and from the user.	• Traditional antivirus and anti-malware. • Hardware-enhanced security protects against rootkits and other stealthy attacks. • Host intrusion prevention protects during startup and off the network.
Phase 4: Attack executes its instructions to support its malicious activity—from stealing identities and intellectual property theft to bank fraud.	• Whitelisting prevents malicious software from tampering with known good application files and prevents execution of bad code. • Host-based firewalls prevent connections to known malicious bot networks and limit the loss of sensitive data.

McAfee Complete Endpoint Protection—Enterprise suite provides:

Feature	Why You Need It
Integrated, unified management	Efficiently manage policies for, maintain, and report on all your security and compliance tools from a single, centralized web-based console.
Real-time questions and actions	Instantly see and take immediate action to adjust the security state and health of McAfee products on endpoints.
Hardware-enhanced security	Stop the most sophisticated rootkits and stealthy attacks with protection below the operating system.
Device control	Prevent loss of sensitive data by restricting use of removable media.
Dynamic application whitelisting	Prevent unwanted applications and malware from installing and executing with minimal impact on system performance, users, or administrators.
Host IPS and desktop firewall	Guard against unknown, zero-day threats and new vulnerabilities, and reduce patch urgency.
Advanced anti-malware	Use behavioral anti-malware to block viruses, Trojans, worms, adware, spyware, and other potentially unwanted programs that steal confidential data and sabotage user productivity.
Antispam	Eliminate spam, which can lead unsuspecting users to sites that distribute malware and phish for personal and financial data.
Safe surf and search	Ensure compliance and reduce risk from web surfing by warning users about malicious websites before they visit. Allow administrators to authorize or block website access.
Mobile device management	Simplify provisioning and deprovisioning of mobile devices and transparently secure them, the corporate data they use, and the IT networks they access.
Host web filtering	Control users, whether they are web surfing on or off the corporate network, through content filtering and enforcement of website access by user and groups.
Email server security	Protect your email server and intercept malware before it reaches the user inbox.
Instant risk assessment and prioritization	Pinpoint which critical assets are vulnerable to which threats. Get instant, actionable data correlation on emerging threats to quickly identify whether the proper protection is in place. Reduce unnecessary time spent patching and diagnosing issues.
Multi-platform protection	Protect the full range of endpoints required by mobile and knowledge workers, including Macs, Linux, Microsoft Windows, virtual machines, mobile devices, and servers.
Global threat intelligence	Defend against new and emerging threats and remediate swiftly with real-time threat intelligence gathered by millions of sensors worldwide across file, web, network, and email vectors.

Security Connected from McAfee

The McAfee Complete Endpoint Protection—Enterprise suite helps you optimize your security and risk posture as you reduce costs and increase agility. Through the Security Connected framework from McAfee, it streamlines and automates protection and incident management processes to reduce security overhead. With real-time security management across network, endpoint, content, and data protection as well as global threat intelligence, McAfee helps you identify, prioritize, and resolve risks to your business. For more information, visit: www.mcafee.com/complete-endpoint-enterprise.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

60214ds_complete-protection-ent_0513_fnl_ASD