McAfee Complete Endpoint Protection— Business

Intelligent, connected defenses with easy, centralized management

Key Advantages

- Get top-rated, comprehensive layered protection with intelligent, collaborative endpoint defenses, intrusion prevention and firewall for desktops and laptops, device control, encryption, and more.

- Pre-execution containment isolates ransomware and advanced threats before they infect the system. Combined with machine-learning, behavior classification helps discover zero-day malware and improve detection.

- Unify management across all your endpoints: PCs, Macs, and Linux systems.

- Get actionable threat forensics in understandable language to better understand and rapidly take action against advanced threats.

- Secure confidential data on all devices, removable media, and cloud storage while you share files securely.

Defend your endpoint devices with McAfee® Complete Endpoint Protection— Business, an affordable, all-in-one solution that uses collaborative threat and global threat intelligence to defend against advanced threats, encryption to protect your data, and dynamic application containment and machine learning for desktops and laptops to halt zero-day exploits. Phishing and multistage attacks are also blocked thanks to its email, web, and collaborative endpoint defenses. Lastly, centralized, web-based management eases the day-to-day burden on your IT staff and empowers them to act fast when threats strike.

McAfee Complete Endpoint Protection— Business helps growing organizations get security right, from turnkey installation to rapid response. With one unified solution, you cover PCs, Macs, Linux systems, and more. Reduce complexity, cut costs, and protect against rootkits, targeted web and email attacks, and persistent threats. You get powerful, efficient protection and straightforward management that's available only from McAfee, the market leader in endpoint security.

Advanced Threat Protection

One infected system can bring your business down, and antivirus alone just isn't strong enough for today's sophisticated threats. When it comes to threat protection, you can't do any better than McAfee Complete Endpoint Protection—Business. Our collaborative endpoint framework lets defenses work together to analyze, take action against emerging threats and share forensic data in real time.

Intel Security protects, detects, and corrects malware faster with multiple layers of protection, including intelligent defenses that collaborate against advanced threats, dynamic application containment, and machine learning for desktops and laptops, device control, encryption, and more.

Intel Security provides multiple layers of protection. With advanced encryption, you can automatically secure confidential information and prevent unauthorized access on PCs, Macs, laptops, virtual machines, removable media, and cloud storage such as Box, DropBox, Google Drive, and Microsoft OneDrive. Safeguard your vital assets without hindering system performance—and easily manage and enforce policies from the McAfee® ePolicy Orchestrator® (McAfee ePO™) centralized, web-based management platform.

See more, know more, and defend your organization better with cloud-based McAfee Global Threat Intelligence, which gives you the

full spectrum of new and emerging threats in real time across all vectors—file, web, message, and network. With more than 100 million global threat sensors in over 120 countries, more than 45 billion queries per day, more than 1.5 million files, and 1 million URLs analyzed per day, we offer the market's strongest global threat intelligence.

Easy Deployment, Centralized Management

You may not have security experts in every office—that's why we keep it simple. Your security is installed and ready to go in as few as four clicks. Management is easy with McAfee ePO software—a single pane of glass where you can view security and manage policies for all devices.

Strong and Effective Performance

Our extensible endpoint framework can help you see and remove redundancies to improve your IT operational efficiency. Scanning is optimized for performance, as well with idle-time scanning and self-learning, adaptive scanning that is based on the behavior of files and processes to ensure performance is ready and available when more aggressive scanning power is required.

Intel Security: An Industry Leader

- Leader Forrester Wave™: Endpoint Security Suites, Q4 2016.[1]
- McAfee Endpoint Security is recommended by NSS Labs.[2]

McAfee Complete Endpoint Protection—Business Highlights

Anti-Malware (PCs, Macs, Linux, virtual machines)

McAfee Endpoint Security

Communicates with multiple endpoint defense technologies in real time to analyze and collaborate against new and advanced threats, blocking and quickly halting them before they impact your systems or users.

Dynamic Application Containment

Safely examines behaviors and contains threats like greyware, ransomware, patient-zero threats, and more with no cloud connection required.

Real Protect

- Detects and stops advanced and zero-day threats with real-time behavioral analysis and machine learning that combines pre-execution feature extraction and post-execution behavioral and memory analysis to convict threats.
- Protects against sandbox-aware malware by allowing it to execute the "bad" behaviors, analyze it real-time, and then automatically have Dynamic Application Containment suppress malicious actions before the malware can infect a system.

Application Control

Prevents unwanted applications and malware from installing and executing with minimal impact on system performance, users, and administrators.

Intrusion Prevention and Firewall for Desktops

- Guard against unknown, zero-day threats and new vulnerabilities.
- Reduce patch urgency.

Global Threat Intelligence

- Defend against new and emerging threats across all vectors with real-time intelligence gathered by millions of sensors worldwide.
- Create customized controls to prevent exploits, attacks on memory, and threats that attempt to run with higher privileges.

Web and Messaging Security

McAfee Web Control with URL Filtering and Safe Search

- Warn users about malicious websites before they visit to reduce risk and stay compliant.
- Enforces web browsing policies by authorizing or blocking website access.

Email Anti-Malware and Antispam

- Protect email server and intercept malware before it reaches user inboxes.
- Detect, clean, and block malware from Microsoft Exchange and Lotus Domino servers with McAfee Security for Email Servers.

Data Protection

Device Control

Prevent loss of sensitive data by restricting use of removable media.

Full Disk, File, Folder, Removable Media, and Cloud Storage Encryption

Secure confidential data across PCs, Macs, laptops, network servers, removable media, and cloud storage services.

Management

McAfee ePO Software

- Manage policies, compliance, and reporting from a single, centralized console.
- Simplify management in mixed OS environments using cross-platform policies

Take Control Over the Complete Threat Lifecycle

McAfee Complete Endpoint Protection—Business helps you stay secure and nimble. It provides a collaborative security framework to reduce the complexity of endpoint security environments, better performance to protect you and your users' productivity, and visibility into advanced threats to speed detection and remediation responses. Global, cloud-based threat intelligence helps ensure that new and advanced threats will be met with fast, effective responses and actionable forensics for administrators. Lastly, centralized web-based management that allows other third-party and Intel® Security products to be integrated with a single console provides relief for IT teams who are burdened with multiple solutions to more easily view, respond to, and manage the threat defense lifecycle. For more information, visit: **https://www.mcafee.com/us/products/ complete-endpoint-protection-business.aspx**.

How Our Advanced Threat Defenses Work

Technology	What it does	How it performs
McAfee Endpoint Security 10	Enables communication between multiple threat defenses for detection of seemingly disconnected events as related and part of a targeted attack.	• Threat defenses talk to, learn from, and inform one another of emerging threats. • Adaptive and intelligent scanning leverages observations from multiple sources to detect and inform each other in real time of emerging forms of attacks. • Defenses are informed by localized and global threat intelligence. • Automatic actions are taken against suspicious applications and processes and quickly escalate while informing other defenses and the global community.
McAfee Threat Intelligence Exchange*	Offers expanded threat intelligence from global data sources and third parties, while sourcing local threat intelligence from real-time and historical events.	• Security components gain additional insights into threats targeting organizations in the global network discovered through endpoints, gateways, and other security components. • Threat details collected from malware encounters propagate through the McAfee Data Exchange Layer in milliseconds, reaching all endpoints and giving them the information to proactively immunize against threats. • Enables customization of threat intelligence, such as lists of publisher certificates, file hashes, and risk tolerance decisions based on organizational preferences.
McAfee Active Response*	Expands incident response capabilities with detailed live, interactive, and ongoing investigation insights and analysis	• Automatically captures and monitors context and system state changes that may be an indicator of attack (IoA), as well as attack components lying dormant, and sends intelligence to analytics, operations, and forensic teams. • Allows adjustments to changes in attack methodologies, automatic data collection, alerts, and responses to objects of interest, and offers custom workflows. • Continuous, persistent collectors trigger on detection of attack events, alerting administrators and systems to attack activities.
McAfee Application Control	Blocks unauthorized executables on corporate desktops and fixed function devices.	• Uses a trust model and innovative security features to thwart advanced persistent threats—without requiring signature updates or labor-intensive list management. • Integrates with McAfee Global Threat Intelligence so that users can consistently enable the "known good" applications and code, and block "known bad" and "unknown bad." • When deployed with McAfee Threat Intelligence Exchange, enhances whitelisting with localized threat intelligence to combat unknown and targeted malware instantly. McAfee Threat Intelligence Exchange coordinates with McAfee Advanced Threat Defense to dynamically analyze the behavior of unknown applications in a sandbox and automatically immunizes all endpoints from newly detected malware.

* McAfee Threat Intelligence Exchange, McAfee Active Response, and McAfee Advanced Threat Defense are optional capabilities sold separately for McAfee Complete Endpoint Protection customers.