

# McAfee Endpoint Protection—Advanced Suite

## Protection against zero-day attacks and help with regulatory compliance

A mobile workforce plus increased regulation could equal a security nightmare. With integrated, proactive security to combat sophisticated malware and zero-day threats, McAfee® Endpoint Protection—Advanced Suite, part of the McAfee product offering, protects endpoints when they leave your network and helps protect your network when they return. Its integrated intrusion prevention secures desktops and laptops from advanced threats. Centralized policy-based management, multiplatform support, and auditing keep all of your endpoint assets safe and compliant.

The increasing sophistication of attackers is challenging security practitioners to have the visibility and tools they need to detect and defend against advanced threats. Although every endpoint is at risk from the subtle technologies criminals use today, portable systems face extra threats. Laptops venture to hotels, coffee shops, and home offices without traditional protective layers, such as web and email gateways, network firewalls, and network intrusion prevention systems. On a Wi-Fi network, anyone might listen and pick up more than the news.

PCs can miss patches and other updates, becoming even more vulnerable to zero-day threats by simply being disconnected from the corporate network. And those patches and other updates are increasingly required for regulatory compliance. Beyond more stringent industry

regulations, your governance controls may expect you to manage distribution of sensitive data as well as appropriate web use—on-site or on the road.

McAfee® Endpoint Protection—Advanced Suite puts you in charge with broad protections, compliance controls, and unified management. Whether you want to keep viruses, hackers, spammers, data thieves, or auditors at bay, this seamless solution has the perfect combination of capabilities and cost savings.

### Intelligent, Collaborative Defenses

Organizations need a strategy for threat protection, detection, and correction, as well as a security framework that empowers security components to collaborate against targeted attacks for rapid detection and action. That's why McAfee Endpoint Security 10 (included with the suite), communicates with multiple

### Key Advantages

---

- Guard Microsoft Windows, Mac, and Linux devices against system, data, email, and web threats, and the risk of noncompliance.
- Consolidate endpoint and data security efforts with an integrated solution from one vendor—securing stronger protection at a lower cost.
- Enable increased protection immediately, with the simplicity and efficiency of centralized management and an extensible endpoint security framework.

## DATA SHEET

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. Its framework helps remove duplicate technologies and connect other McAfee solutions to enable simpler management and stronger defenses. Additionally, McAfee Global Threat Intelligence (McAfee GTI) provides insights from the largest volume of observations and analysis available in the market.

### Advanced Email Virus and Spam Protection

Our solution scans your inbound and outbound emails to intercept spam, inappropriate content, and harmful viruses. We can quarantine suspicious emails to prevent evolving email threats from affecting your network and users. And, a layer of antivirus on your email server prevents malware from reaching user inboxes.

### Zero-Day and Vulnerability Shielding

Say goodbye to emergency patching. Exploit and intrusion prevention technologies patrol your desktops and laptops against malware, block malicious code from hijacking an application and trying to run with higher privileges, and provide automatically updated signatures that shield laptops and desktops from attack. It's safe to implement and test patches on your schedule. Combined with our patented behavioral protection, which prevents buffer overflow attacks, you get the most advanced system vulnerability coverage on the market.

### Integrated Firewall

Bar unsolicited inbound traffic and control outbound traffic with our integrated firewall, which uses McAfee GTI to protect desktops and laptops from botnets, distributed denial-of-service (DDoS) attacks, advanced persistent threats, and risky web connections. Systems are also protected by allowing only outbound traffic during startup until the complete firewall policy has been enforced.

### Efficient Policy Auditing and Compliance

Agent-based policy auditing scans your endpoints and documents to ensure that all policies are up to date. Organizations can measure compliance to best practice policies—ISO 27001 and CoBIT—as well as to key industry regulations.

### Comprehensive Device Control

Prevent critical data from leaving your company through USB drives, Apple iPods, Bluetooth devices, recordable CDs, and DVDs. Tools help you monitor and control data transfers from all desktops and laptops—regardless of where users and confidential data go, even when users are not connected to the corporate network.

### Why Choose McAfee?

---

- We offer a true centralized experience for administrators.
- Our integrated endpoint and security frameworks help you remove redundancies, connect other solutions, and provide an extensible architecture to build on.
- McAfee Global Threat Intelligence offers the strongest volume of threat intelligence on the market. We see and protect more than anyone else.

## DATA SHEET

### Proactive Web Security

Help ensure compliance and reduce risk from web surfing by warning users about malicious websites before they visit. Host-based web filtering ensures that you can authorize and block website access, protecting users and ensuring their policy compliance whenever and wherever they are web surfing. Lastly, private URLs can also be blocked, and the latest versions of multiple web browsers are supported.

### Management that Lowers Operational Costs

For efficiency and comprehensive visibility across your security and compliance status, McAfee® ePolicy Orchestrator® (McAfee ePO™) software provides a single, centralized, platform that manages security, enforces protection, and lowers the cost of security operations.

Correlate threats, attacks, and events from endpoint, network, and data security, as well as compliance audits, to improve the relevance and efficiency of security efforts and compliance reports. No other vendor can claim a single integrated management platform across all these security domains. McAfee ePO software simplifies security management.

### Deploy Quickly and Easily

Enable increased protection without delay. The EASI installer gets your strong protection running in as few as four clicks. Integration with McAfee ePO software lets you deploy and manage security using a single environment.

### Migration Made Easy

Environments with current versions of McAfee ePO software, McAfee VirusScan® Enterprise, and the McAfee agent can leverage our automatic migration tool to migrate your existing policies to McAfee Endpoint Security 10 in about 20 minutes or less.

## DATA SHEET

Feature	Why You Need It
<b>Single integrated management</b>	Instant visibility into security status and events and direct access to management for unified control of all your security and compliance tool with McAfee ePO software
<b>Multiplatform</b>	Protects the full range of endpoints required by mobile and knowledge workers, including Mac, Linux, and Microsoft Windows
<b>Device control</b>	Lets you monitor and restrict data copied to removable storage devices and media to keep it from leaving company control
<b>Intrusion prevention system (IPS) and integrated firewall for desktops and laptops</b>	Provides zero-day protection against new vulnerabilities, which reduces the urgency to patch, and controls desktop applications that can access the network to stop network-borne attacks
<b>Anti-malware</b>	Blocks viruses, Trojans, worms, adware, spyware, and other potentially unwanted programs that steal confidential data and sabotage user productivity
<b>Anti-spam</b>	Helps eliminate spam, which can lead unsuspecting users to sites that distribute malware and phish
<b>Web control with URL filtering and safe search</b>	Helps ensure compliance, warns users before they visit malicious websites, and protects them whether they are on or off the corporate network
<b>Email server security</b>	Protects your email server and intercepts malware before it reaches the user inbox
<b>Policy auditing</b>	Provides tightly integrated compliance reporting for HIPAA, PCI, and more

## Learn More

For more information, visit [www.mcafee.com/endpoint](http://www.mcafee.com/endpoint), or call us at 1 888 847 8766, 24 hours a day, seven days a week.

\* The migration time is dependent on your existing policies and environment.



2821 Mission College Boulevard  
Santa Clara, CA 95054  
888 847 8766  
[www.mcafee.com](http://www.mcafee.com)

McAfee and the McAfee logo, ePolicy Orchestrator, McAfee ePO, and VirusScan are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC.  
417\_0816  
AUGUST 2016