Data Sheet

McAfee®

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. Get the McAfee® Endpoint Protection—Advanced suite and rest peacefully. With integrated, proactive security to combat sophisticated malware and zero-day threats, this suite protects endpoints when they leave your network and helps protect your network when they return. Its integrated intrusion prevention secures Windows endpoints—including the ones that stay in the office—from advanced persistent threats. Centralized policy-based management, access control, and auditing keep all of your endpoint assets safe and compliant.

Key Points

- Guard endpoints 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 a single agent

In late 2008, laptops outsold traditional fixed and tower PCs for the first time, and the notebook era began.

—*IDC: Notebooks Finally Outsell Desktops in U.S.;* http://www.pcmag.com/article2/0,2817,2333549,00.asp

SC MAGAZINE
AWARDS
2010
WINNER
Honored in the U.S.

Best Anti-Malware Solution and
Best Enterprise Security Solution

Only behavioral and system-level defenses can protect endpoints against the most insidious malware, designed to avoid signature-based detection and work before patches are released. 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 WiFi network, anyone might listen and pick up more than the news.

Simply being out of the office can cause PCs to miss patches and other updates, becoming extra vulnerable to zero-day threats. 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.

The 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.

Always on, real-time malware protection

With the unprecedented growth of advanced persistent threats, enterprises cannot depend on solutions that use only signature analysis for endpoint protection. There's a gap of 24 to 72 hours from the time a threat is identified to the moment its signature is applied to endpoints. In the meantime, your data and systems lie exposed. The built-in McAfee Global Threat Intelligence file reputation service closes the gap, providing real-time, always-on protection based on insight gathered by McAfee Labs™.

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 anti-virus on your email server prevents malware from reaching user inboxes.

Zero-day and vulnerability shielding

Say goodbye to emergency patching. Host intrusion prevention patrols your endpoints against malware, blocks malicious code from hijacking an application, and provides 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.

McAfee sets the industry standard

- Recognized for four straight years by Gartner as a leader in Endpoint Security and Mobile Data Protection
- First to manage broad range of security products including endpoint, network, data, web, and email security with one console
- First to deliver single agent and single console for endpoint security
- First product to have unified management platform for endpoint security and compliance management
- First product to manage both McAfee and third-party security products
- First to combine policy auditing and policy enforcement in a single engine
- First to combine endpoint security and data protection in one truly integrated suite

Supported Operating Platforms

Workstations (Note: 64-bit operating system support is available for some technologies)

- Windows 7 or Embedded
- Windows Vista
- Windows XP Home, Professional, Embedded (WEPOS), Tablet PC
- Windows 2000 Professional with Service Pack 2 (SP2) or higher

Servers (Note: 64-bit operating system support is available for some technologies)

- Windows 2008 Server, Hyper-V, Core, Datacenter, Storage Server, Cluster Server, Small Business Server
- Windows 2003 Server, Storage Server, Cluster Server, Datacenter, Small Business Server
- Windows 2000 Server, Advanced Server, Small Business Server

Email server requirements

- Microsoft Exchange 2003 SP1; 2007 (64-bit); 2010 (v7.0.2)
- Microsoft Exchange 2000 SMB, 2003 Server, or Advanced Server
- Lotus Domino 6.0.3-6.0.5; 7.0; 8.0 (32-bit); 8.5 (32-bit)

Stateful desktop firewall

You can control desktop applications that can access the network to stop network-borne attacks and down-time. Deploy and manage firewall policies based on location to deliver complete protection and compliance with regulatory rules.

Flexible network access control

When travelers return to the enterprise network, you can ensure they don't bring back any hitch-hikers. Network access control limits access to the corporate network to the compliant systems you permit. Regardless of how endpoints connect to the network, network access control discovers and evaluates endpoint compliance status, enforces the appropriate network access policies, and provides automated remediation of any issues.

Efficient policy auditing and compliance

Agent-based policy auditing scans your endpoints and documents 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, 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.

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 control—both authorize and block—website access, protecting users and ensuring their policy compliance whenever and wherever they are web surfing.

Management that lowers operational costs

For efficiency and comprehensive visibility across your security and compliance status, McAfee ePolicy Orchestrator® (ePO™) software provides a single, centralized, platform that manages security, enforces protection, and lowers the cost of security operations. Web-based for easy access anywhere, it provides intelligent security for quick and effective decisions and greater control.

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 ePolicy Orchestrator simplifies security management.

Learn More

For more information, visit www.mcafee.com/endpoint, or call us at 888.847.8766, 24 hours a day, seven days a week.

Feature	Why You Need It
Single integrated management	McAfee ePolicy Orchestrator (ePO) provides instant visibility into security status and events and direct access to management for unified control of all your security and compliance tools
Device control	Lets you monitor and restrict data copied to removable storage devices and media to keep it from leaving company control
Host IPS and desktop firewall	Provides zero-day protection against new vulnerabilities, which reduces the urgency to patch existing systems, and controls desktop applications that can access the network to stop network-borne attacks and related downtime
Anti-malware	Blocks viruses, Trojans, worms, adware, spyware, and other potentially unwanted programs that steal confidential data and sabotage user productivity
Anti-spam	Helps eliminate spam, which can lead unsuspecting users to sites that distribute malware and phish for personal and financial data
Safe surf and search	Helps ensure compliance and reduce risk from web surfing by warning users about malicious websites before they visit and letting administrators authorize or block website access
Host web filtering	Controls 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	Protects your email server and intercepts malware before it reaches the user inbox
Network access control	Limits malware infections by preventing noncompliant systems from accessing the network
Policy auditing	Provides tightly integrated compliance reporting for HIPAA, PCI, and more

McAfee®

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