

# McAfee Endpoint Protection Suite

Secure Windows PCs against real-time malware and unauthorized devices

Traditional desktops and fixed systems within your LAN probably have layers of gateway or network security to protect them. Yet they still need essential security to block advanced malware, control data loss and compliance risks caused by removable media, and provide safe access to critical email and web applications. The McAfee® Endpoint Protection Suite integrates these core functions into a single, manageable environment ideal for safeguarding traditional desktops and other systems that have limited exposure to Internet threats.

## Key Points

- Essential protection that consolidates endpoint and data security
- Reduces the time and effort spent deploying and managing security
- One-stop-shopping for the right protections for traditional and fixed desktops



Best Anti-Malware Solution and  
Best Enterprise Security Solution

What do call centers, engineering design studios, and doctors' offices have in common? Their users rely on tower-based PCs and traditional desktop systems that never leave the office. Since these systems don't visit wireless hot spots, help kids browse the Internet at night, or get left at airports, they have a lower risk of being hacked, picking up malicious downloads, or being stolen while carrying sensitive data

However, corporate users rely heavily on web-enabled applications and email, so even these fixed machines require sophisticated protection against the targeted, real-time malware these applications convey. Your email server should have an extra dose of anti-malware, backed up by malware protection on each endpoint itself.

In addition, most modern PCs have multiple USB ports and DVD drives. In the case of call centers, engineering design studios, and doctors' offices, an unhappy worker might take home customer databases, engineering designs and other intellectual property, or patient records and financial data. Device controls can help you restrict use of removable media and portable storage to avoid these data losses.

The McAfee Endpoint Protection Suite seamlessly integrates proven security to help you manage all of these risks, delivering both operational efficiencies and cost savings with the convenience of a single solution.

## 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 is 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 are exposed.

McAfee Global Threat Intelligence file reputation closes this gap, providing real-time, always-on protection based on the multi-vector threat insight gathered by McAfee Labs™. It quarantines or blocks viruses, Trojans, worms, adware, spyware, and other potentially unwanted programs that steal confidential data and sabotage user productivity.

## 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 protects your email server to prevent malware from reaching user inboxes.

## Comprehensive device control

We make it possible to prevent critical data from leaving your company through removable media, such as USB drives, iPods, Bluetooth devices, recordable CDs, and DVDs. Tools help you monitor and control data transfers from all desktops, even if a device is physically disconnected from the corporate network.

**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 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**

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

**Proactive web security**

Many web threats are silent and invisible to web surfers. Help ensure compliance and reduce risk from web surfing by warning users about malicious websites before they visit. You can also authorize and block website access based on users and groups, controlling user access to sensitive or inappropriate sites, such as gaming or adult content.

**Management that lowers operational costs**

All of the capabilities of the McAfee Endpoint Protection Suite are managed by McAfee ePolicy Orchestrator® (ePO™) software, a centralized platform that manages security, enforces protection, and lowers the cost of security operations. Web-based for easy access, it provides intelligent security for quick and effective decisions and greater control.

McAfee ePO can reduce the cost of managing IT security and compliance by more than 60 percent (source: MSI International survey of 488 medium-sized and large enterprises).

This open management framework takes advantage of a single agent and single console design. Compared to old-style point solutions, our streamlined approach dramatically simplifies installation and maintenance of defenses and their associated rules and policies. It eliminates the system impact of multiple agents and the decision inefficiencies of multiple consoles. When policies need to be revised, updates happen quickly, accurately, and consistently.

You can 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.

**Learn More**

For more information, visit [www.mcafee.com/endpoint](http://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
Desktop firewall	Ensures that network-based attacks are prevented and only legitimate network traffic is allowed
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
Email server security	Protects your email server and intercepts malware before it reaches the user inbox
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 and block website access

