Data Sheet: Endpoint Security

Symantec™ Endpoint Protection

The next generation of antivirus technology from Symantec

Overview

Advanced threat protection

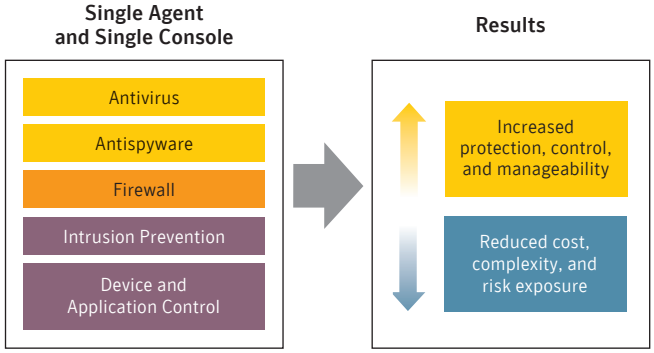
Symantec™ Endpoint Protection combines Symantec AntiVirus™ with advanced threat prevention to deliver an unmatched defense against malware for laptops, desktops, and servers. It provides protection against even the most sophisticated attacks that evade traditional security measures, such as rootkits, zero-day attacks, and mutating spyware.

Symantec Endpoint Protection delivers more than world-class, industry-leading antivirus and antispyware signature-based protection. It also provides advanced threat prevention that protects endpoints from targeted attacks and attacks not seen before. It includes turnkey, proactive technologies that automatically analyze application behaviors and network communications to detect and block suspicious activities, as well as administrative control features that allow you to deny specific device and application activities deemed as high risk for your organization. You can even block specific actions based on the location of the user.

This multilayered approach significantly lowers risks and gives you the confidence that your business assets are protected. It is a comprehensive product that gives you the capabilities you need now, along with the ability to enable the pieces you need, as you need them. Whether the attack is coming from a malicious insider or is externally motivated, endpoints will be protected.

Symantec Endpoint Protection increases protection and helps lower your total cost of ownership by reducing administrative overhead as well as the costs associated with managing multiple endpoint security products. It provides a single agent that is administered by a single management console. This simplifies endpoint security administration and provides operational efficiencies such as single software updates and policy updates, unified and central reporting, and a single licensing and maintenance program.

Symantec Endpoint Protection is easy to implement and deploy. Symantec provides a range of consulting, technical education, and support services that guide organizations through the migration, deployment, and management of the solution and help them realize the full value of their investment. For organizations that want to outsource security monitoring and management, Symantec also offers Managed Security Services to deliver real-time security protection.



A unified approach to endpoint protection

Key benefits

Secure

Comprehensive protection—Symantec Endpoint Protection integrates best-of-breed technologies to stop security threats—even from the most devious new and unknown attackers—before they penetrate the network. It detects and blocks malicious software in real time, including viruses, worms, Trojan horses, spyware, adware, and rootkits.

Proactive protection—TruScan™ Proactive Threat Scan is a unique Symantec technology used to score both good and bad behaviors of unknown applications, enhancing detection and reducing false positives without the need to create rule-based configurations.

Industry-best threat landscape intelligence—Symantec protection mechanisms leverage the industry-leading Global Intelligence Network to deliver an unparalleled view of the entire Internet threat landscape. This intelligence results in actionable protection and peace of mind against evolving attacks.

Simple

Single agent, single console—A full range of security technologies are integrated into a single agent and a centralized management console, with an intuitive user interface and Web-based graphical reporting. You are able to set and enforce security policies across the enterprise to protect your critical assets. Symantec Endpoint Protection simplifies management, reduces system resource usage, and requires no additional agents when adding Symantec Network Access Control support. Symantec Network Access Control features are automatically enabled on the agent and management console with the purchase of a license.

Easy to deploy—Because it requires only a single agent and management console and it operates with an organization's existing security and IT investments, Symantec Endpoint Protection is easy to implement and deploy. For organizations that want to outsource security monitoring and management, Symantec offers Managed Security Services to deliver real-time security protection.

Lower cost of ownership—Symantec Endpoint Protection delivers a lower total cost of ownership by reducing administrative overhead as well as the costs associated with managing multiple endpoint security products. This unified approach to endpoint security simplifies administration and provides operational efficiencies such as single software updates and policy updates, unified and central reporting, and a single licensing and maintenance program.

Seamless

Easy to install, configure, and manage—Symantec Endpoint Protection makes it easy to enable/disable and configure desired technologies to fit into your environment.

Symantec Network Access Control ready—Each endpoint becomes "Symantec Network Access Control ready," eliminating the need to deploy additional network access control endpoint agent software.

Leverages existing security technologies and IT investments—Symantec Endpoint Protection works with other leading antivirus products, firewalls, IPS technologies, and network access control infrastructures. It also works with leading software deployment tools, patch management tools, and security information management tools.

Integration with Altiris endpoint management solutions—Distributing software packages, migrating older Symantec AntiVirus™ or other antivirus deployments, and viewing new agent rollout status and activity is easier.

Key features

More than antivirus

Antivirus and antispyware—Provides unmatched, best-of-breed malware protection, including market-leading antivirus protection, enhanced spyware protection, new rootkit protection, reduced memory footprint, and new dynamic performance adjustments to keep users productive.

Network threat protection—A rules-based firewall engine and Generic Exploit Blocking (GEB) block malware before it can enter a system.

Proactive threat protection—Providing protection against unseen threats (i.e., zero-day threats), it includes TruScan Proactive Threat Scan, which does not rely on a signature.

Single agent and single management console—Antivirus, antispyware, desktop firewall, IPS, device and application control, and network access control (with the purchase of a Symantec Network Access Control license) are provided on a single agent—all managed by a single console.

Symantec Endpoint Protection product family

	Symantec Endpoint Protection	Symantec Endpoint Protection Small Business Edition	Symantec Multi-tier Protection
Antivirus	X	X	X
Antispyware	X	X	X
Desktop firewall	X	X	X
Intrusion prevention	X	X	X
Device and application control	X	X	X
Symantec Mail Security for Microsoft® Exchange		X	X
Symantec Mail Security for Domino®			X
Symantec Mail Security for SMTP			X

Shaded area = Centrally managed by a single agent and single console

Minimum system requirements

Symantec Endpoint Protection Manager, Console, and database

Component	32-bit	64-bit
Processor	1 GHz Intel® Pentium® III	1 GHz on x64 only with the following processors: ▪ Intel Xeon with Intel EM64T support ▪ Intel Pentium IV with EM64T support ▪ AMD 64-bit Opteron™ ▪ AMD 64-bit Athlon™ Note: Itanium is not supported.
Operating system	The following operating systems are supported: ▪ Windows® 2000 Server/ Advanced Server/ Datacenter Server/Small Business Server with Service Pack 3 or later ▪ Windows XP Professional with Service Pack 1 or later **Note:** Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for *Symantec Endpoint Protection Manager 11.x communication troubleshooting* on the Symantec Support Web Site. ▪ Windows Server 2003 Standard Edition/ Enterprise Edition/ Datacenter Edition/ Storage Edition/ Web Edition/ Small Business Server	The following operating systems are supported: ▪ Windows XP Professional x64 Edition with Service Pack 1 or later ▪ Windows Server 2003 Standard x64 Edition/ Enterprise x64 Edition/ Datacenter x64 Edition with Service Pack 1 or later ▪ Windows Compute Cluster Server 2003 ▪ Windows Storage Server 2003 **Note:** If you use Microsoft Clustering services for the Symantec Endpoint Protection Manager server you must install the Symantec Endpoint Protection Manager on the local volume.
Memory	1 GB RAM minimum (2-4 GB recommended)	1 GB RAM minimum (2-4 GB recommended)
Hard disk	4 GB for the server, plus an additional 4 GB for the database	4 GB for the server, plus an additional 4 GB for the database
Display	Super VGA (1,024x768) or higher-resolution video adapter and monitor	Super VGA (1,024x768) or higher-resolution video adapter and monitor

Symantec Endpoint Protection Manager, Console, and database (continued)

Component	32-bit	64-bit
Database	The Symantec Endpoint Protection Manager includes an embedded database. You may also choose to use one of the following versions of Microsoft SQL Server: ▪ Microsoft SQL Server 2000 with Service Pack 3 or later ▪ Microsoft SQL Server 2005 **Note:** Microsoft SQL Server is optional.	The Symantec Endpoint Protection Manager includes an embedded database. You may also choose to use one of the following versions of Microsoft SQL Server: ▪ Microsoft SQL Server 2000 with Service Pack 3 or later ▪ Microsoft SQL Server 2005 **Note:** Microsoft SQL Server is optional.
Other requirements	The following other requirements must be met: ▪ Internet Information Services server 5.0 or later with World Wide Web services enabled ▪ Internet Explorer 6.0 or later ▪ Static IP address (recommended)	The following other requirements must be met: ▪ Internet Information Services server 5.0 or later with World Wide Web services enabled ▪ Internet Explorer 6.0 or later ▪ Static IP address (recommended)

Symantec Endpoint Protection Manager and Console

Component	32-bit	64-bit
Processor	1 GHz Intel Pentium III	1 GHz on x64 only with the following processors: ▪ Intel Xeon with Intel EM64T support ▪ Intel Pentium IV with EM64T support ▪ AMD 64-bit Opteron™ ▪ AMD 64-bit Athlon™ **Note:** Itanium is not supported.

Symantec Endpoint Protection Manager and Console (continued)

Component	32-bit	64-bit
Operating system	The following operating systems are supported: ▪ Windows® 2000 Server/ Advanced Server/ Datacenter Server with Service Pack 3 or later ▪ Windows XP Professional with Service Pack 1 or later **Note:** Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for *Symantec Endpoint Protection Manager 11.x communication troubleshooting* on the Symantec Support Web Site. ▪ Windows Server 2003 Standard Edition/ Enterprise Edition/ Datacenter Edition/ Web Edition/ Small Business Server	The following operating systems are supported: ▪ Windows XP Professional x64 Edition with Service Pack 1 or later ▪ Windows Server 2003 Standard x64 Edition/ Enterprise x64 Edition/ Datacenter x64 Edition with Service Pack 1 or later ▪ Windows Compute Cluster Server 2003 ▪ Windows Storage Server 2003 **Note:** If you use Microsoft Clustering services for the SEPM server you must install the SEPM server on the local volume.
Memory	1 GB RAM minimum (2 GB recommended)	1 GB RAM minimum (2 GB recommended)
Hard disk	2 GB (4 GB recommended)	2 GB (4 GB recommended)
Display	Super VGA (1,024x768) or higher-resolution video adapter and monitor	Super VGA (1,024x768) or higher-resolution video adapter and monitor
Other requirements	The following other requirements must be met: ▪ Internet Information Services server 5.0 or later with World Wide Web services enabled ▪ Internet Explorer 6.0 or later ▪ Static IP address (recommended)	The following other requirements must be met: ▪ Internet Information Services server 5.0 or later with World Wide Web services enabled ▪ Internet Explorer 6.0 or later ▪ Static IP address (recommended)

Symantec Endpoint Protection Console

Component	32-bit	64-bit
Processor	1 GHz Intel Pentium III	1 GHz on x64 only with the following processors: ▪ Intel Xeon with Intel EM64T support ▪ Intel Pentium IV with EM64T support ▪ AMD 64-bit Opteron™ ▪ AMD 64-bit Athlon™ **Note:** Itanium is not supported.
Operating system	The following operating systems are supported: ▪ Windows® 2000 Professional/Server/ Advanced Server/ Datacenter Server/Small Business Server with Service Pack 3 or later ▪ Windows XP Professional with Service Pack 1 or later **Note:** Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for *Symantec Endpoint Protection Manager 11.x communication troubleshooting* on the Symantec Support Web Site. ▪ Windows Server 2003 Standard Edition/Enterprise Edition/ Datacenter Edition/Web Edition/ Small Business Server ▪ Windows Vista® (x86)	The following operating systems are supported: ▪ Windows XP Professional x64 Edition with Service Pack 1 or later ▪ Windows Server 2003 Standard x64 Edition/ Enterprise x64 Edition/ Datacenter x64 Edition with Service Pack 1 or later ▪ Windows Compute Cluster Server 2003 ▪ Windows Storage Server 2003 ▪ Windows Vista (x64) **Note:** The Symantec Network Access Control installation CD contains a 64-bit application. **Note:** If you use Microsoft Clustering services for the SEPM server you must install the SEPM server on the local volume.
Memory	512 MB of RAM (1 GB recommended)	512 MB of RAM (1 GB recommended)
Hard disk	15 MB	15 MB
Display	Super VGA (1,024x768) or higher-resolution video adapter and monitor	Super VGA (1,024x768) or higher-resolution video adapter and monitor

Symantec Endpoint Protection Console (continued)

Component	32-bit	64-bit
Other requirements	The following other requirements must be met: ▪ Internet Explorer 6.0 or later ▪ Java™ Runtime Environment 5.0, update 13 or above recommended	The following other requirements must be met: ▪ Internet Explorer 6.0 or later ▪ Java Runtime Environment 5.0, update 13 or above recommended

Quarantine Console

Component	32-bit	64-bit
Processor	600 MHz Intel Pentium III	Not tested
Operating system	The following operating systems are supported: ▪ Windows® 2000 Professional/Server/ Advanced Server/ Datacenter Server/Small Business Server with Service Pack 3 or later ▪ Windows XP Professional with Service Pack 1 or later ▪ Windows Server 2003 Standard Edition/ Enterprise Edition/ Datacenter Edition/ Web Edition ▪ Windows Vista (x86) Home Basic Edition/ Home Premium Edition/ Business Edition/ Enterprise Edition/ Ultimate Edition ▪ Windows Server 2008 Standard Edition/ Enterprise Edition/ Datacenter Edition/ Web Edition	Not tested
Memory	64 MB of RAM	Not tested
Hard disk	35 MB	Not tested
Display	Super VGA (1,024x768) or higher-resolution video adapter and monitor	Not tested

Quarantine Console (continued)

Component	32-bit	64-bit
Other requirements	The following other requirements must be met: ▪ Internet Explorer 5.5 Service Pack 2 or later ▪ Microsoft Management Console version 1.2 or later If MMC is not already installed, you need 3 MB free disk space (10 MB during installation).	Not tested

Central Quarantine Server

Component	32-bit	64-bit
Processor	600 MHz Intel Pentium III	Not tested
Operating system	The following operating systems are supported: ▪ Windows® 2000 Professional/Server/ Advanced Server/ Datacenter Server/Small Business Server with Service Pack 3 or later ▪ Windows XP Professional with Service Pack 1 or later ▪ Windows Server 2003 Standard Edition/ Enterprise Edition/ Datacenter Edition/ Web Edition ▪ Windows Vista (x86) Home Basic Edition/ Home Premium Edition/ Business Edition/ Enterprise Edition/ Ultimate Edition	Not tested

Central Quarantine Server (continued)

Component	32-bit	64-bit
Memory	128 MB of RAM	Not tested
Hard disk	40 MB, 500 MB to 4 GB recommended for quarantined items, and 250-MB swap file	Not tested
Display	Super VGA (1,024x768) or higher-resolution video adapter and monitor	Not tested
Other requirements	The following other requirements must be met: ▪ Internet Explorer 5.5 Service Pack 2 or later	Not tested

Symantec Endpoint Protection

Component	32-bit	64-bit
Processor	400 MHz Intel Pentium III (1 GHz for Windows Vista)	1 GHz on x64 only with the following processors: ▪ Intel Xeon with Intel EM64T support ▪ Intel Pentium IV with EM64T support ▪ AMD 64-bit Opteron™ ▪ AMD 64-bit Athlon™ **Note:** Itanium is not supported.

Symantec Endpoint Protection (continued)

Component	32-bit	64-bit
Operating system	The following operating systems are supported: ▪ Windows® 2000 Professional/Server/ Advanced Server/ Datacenter Server/Small Business Server with Service Pack 3 or later ▪ Windows XP Home Edition/Professional with Service Pack 1 or later/ Tablet PC Edition/Media Center Edition ▪ Windows Server 2003 Standard Edition/ Enterprise Edition/ Datacenter Edition/ Web Edition/ Small Business Server ▪ Windows Vista (x86) Home Basic Edition/ Home Premium Edition/ Business Edition/ Enterprise Edition/ Ultimate Edition ▪ Windows Server 2008 Standard Edition/ Enterprise Edition/ Datacenter Edition/ Web Edition	The following operating systems are supported: ▪ Windows XP Professional x64 Edition with Service Pack 1 or later ▪ Windows Server 2003 x64 Edition ▪ Windows Compute Cluster Server 2003 ▪ Windows Storage Server 2003 ▪ Windows Vista Home Basic x64 Edition/Home Premium x64 Edition/ Business x64 Edition/ Enterprise x64 Edition/ Ultimate x64 Edition ▪ Windows Server 2008 Standard x64 Edition/ Enterprise x64 Edition/ Datacenter x64 Edition/ Web x64 Edition **Note:** If you are using Microsoft Clustering Services, you must install the client on the local volume.
Memory	256 MB of RAM	256 MB of RAM
Hard disk	600 MB	700 MB
Display	Super VGA (1,024x768) or higher-resolution video adapter and monitor	Super VGA (1,024x768) or higher-resolution video adapter and monitor
Other requirements	Internet Explorer 6.0 or later Terminal Server clients connecting to a computer with antivirus protection have the following additional requirements: ▪ Microsoft Terminal Server RDP (Remote Desktop Protocol) client ▪ Citrix® Metaframe® (ICA) client 1.8 or later if using Citrix Metaframe server on Terminal Server	Internet Explorer 6.0 or later

Symantec AntiVirus for Linux® client

- Linux distribution supported:

Component	32-bit	64-bit
Red Hat® Enterprise Linux 3.x, 4.x, 5.x	X	X
SUSE Linux Enterprise (Server/Desktop) 9.x, 10.x	X	X
Novell® Open Enterprise Server (OES/OES2)	X	X
VMware ESX 2.5.x, 3.x	X	

Not centrally managed by the Symantec Endpoint Protection Manager

Additional administrator tools

Live Update Administrator

- Operating system supported: Microsoft Windows 2000, 2003, and XP
- Processor: Intel® Pentium® 4 1.8 GHz
- Memory: 512 MB of RAM
- Hard disk: 5 GB

More information

Visit our Web site

www.symantec.com/endpoint

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our Web site.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help businesses and consumers manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Confidence in a connected world.