

Symantec™ Multi-tier Protection

Trusted protection from malware and email-borne threats for multiplatform environments

Overview

Symantec™ Multi-tier Protection safeguards enterprise assets and lowers risk by providing unmatched protection against threats for laptops, desktops, mobile devices, mail servers, and SMTP gateways. It includes Symantec™ Endpoint Protection, Symantec™ Mail Security, and Symantec Brightmail™ products to provide multi-layered protection stopping spam, viruses, and data loss while reducing security risks.

Endpoint protection

Symantec Endpoint Protection delivers more than world-class, industry-leading antivirus and antispyware signature-based protection. It also provides advanced threat prevention that protect 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 all the capabilities 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 Multi-tier Protection also includes the Symantec AntiVirus™ for Linux®, Symantec AntiVirus™ for Macintosh® solutions, and Symantec Mobile AntiVirus for Windows® Mobile.

Groupware protection

Symantec Mail Security for Microsoft® Exchange and Symantec Mail Security for Domino® provide highly effective email protection against viruses and threats while enforcing company security policies on Exchange and Domino servers. Symantec Premium AntiSpam™, based on the Symantec Brightmail antispam technology, offers 97% antispam effectiveness and less than one in a million false positive rate¹. Its multi-layered spam prevention leverages multiple filtering technologies, including spam signatures, heuristics, reputation filters, language identification, and proprietary methods. It integrates seamlessly with Symantec Mail Security products to provide best-in-class antispam protection.

Gateway protection

The Symantec Brightmail™ Gateway delivers effective and accurate antispam and antivirus protection for both inbound and outbound email and instant messaging (IM). Advanced content filtering and structured data protection support helps organizations control sensitive data, reduce the risks associated with data loss, and meet regulatory compliance and corporate governance demands. Brightmail Gateway is simple to administer and catches more than 97% of spam with less than one in a million false positives¹. Continuous automatic updates, global and self-learning local IP reputation analysis, and comprehensive reporting ensure that Brightmail Gateway effectively and transparently responds to new spam threats to minimize network downtime and preserve employee productivity.

¹ Symantec Mail Security earned InfoWorld's "Technology of the Year" for Best Mail Security, InfoWorld—Jan 07, 2008, http://www.infoworld.com/slideshow/2008/01/149-2008_technology-5.html

Data Sheet: Endpoint Security

Symantec™ Multi-tier Protection

Symantec also offers a range of consulting, technical education, and support services to guide you through the migration, deployment, and management of Symantec Multi-tier Protection and help you realize the full value of your investment. Essential Support Services provide confidence that your critical assets are protected around the clock. For organizations that want to outsource security monitoring and management, Symantec also offers Managed Security Services to deliver real-time security protection.

Note: The Symantec Brightmail Gateway offers either a physical or a virtual appliance form factor with the same features and functionalities. The Symantec Multi-tier Protection bundle includes licensing for the virtual appliance and software subscription for the physical appliance. The appliance hardware is sold separately.

Key benefits

Secure

Industry-best threat landscape intelligence—Symantec protection mechanisms utilize the industry-leading Symantec™ 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.

Multilayered defense—The integrated Symantec Endpoint Protection solution for Microsoft® Windows operating systems, Symantec AntiVirus for Linux and Macintosh, and the award-winning Symantec Brightmail Gateway, Symantec Premium AntiSpam, Symantec Mail Security for Microsoft Exchange, and Symantec Mail Security for Domino solutions are included. This combination provides heightened protection against the evolving threat landscape for multiplatform networks, and it protects against email-borne virus threats and security risks in a turnkey package with guaranteed interoperability.

Comprehensive protection

Symantec Multi-tier Protection integrates best-of-breed technologies to stop security threats—even 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, bots, and rootkits.

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

Simple

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 Brightmail Gateway also provides powerful on-demand reporting, unified administrative controls, and flexible work flow that simplify ongoing management and drive down administrative costs.

Seamless

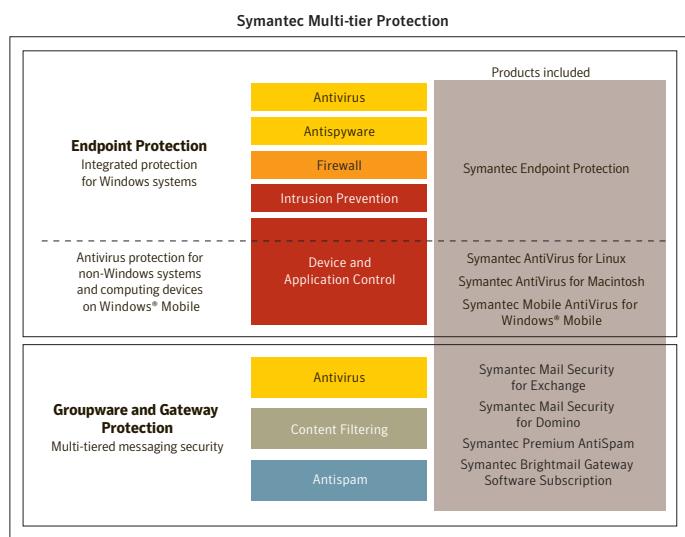
Optimized performance—Never sacrifice system performance for protection. Symantec Endpoint Protection provides fast boot time and application load time, enabling comprehensive protection with optimal performance.

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.

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 are easier.

Data Sheet: Endpoint Security

Symantec™ Multi-tier Protection



Key features

More than antivirus

Antivirus and antispyware—Symantec Endpoint Protection 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—Protecting 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—The Symantec Endpoint Protection portion of Symantec Multi-tier Protection provides antivirus, antispyware, desktop firewall, IPS, device and application control, and network access control (with the purchase of a Symantec Network Access

Control license) on a single agent—all managed by a single management console.

Symantec AntiVirus for Linux and Macintosh, and

Symantec Mobile AntiVirus for Windows Mobile—

Symantec AntiVirus for Macintosh and Symantec AntiVirus for Linux remove viruses from email attachments, Internet downloads, and other sources to safeguard the enterprise network. Symantec Mobile AntiVirus for Windows Mobile enables secure mobile computing by providing comprehensive virus protection against malicious threats that target Windows Mobile operating systems.

Antispam and messaging security protection

The Symantec Brightmail-based antispam technology delivers greater than 97 percent effectiveness and a false positive rate of less than one in a million, making it one of the industry's most accurate solutions.

- Scans inbound and outbound email and IM traffic for compliance with regulatory and governance requirements
- Provides incident management and reporting capabilities that enable organizations to implement policies and analyze and manage violations
- Delivers automatic spam signature updates every 7 minutes to help ensure effective, real-time protection against new threats
- Offers unparalleled protection, as evidenced by the industry's only record of 39 consecutive VB100 awards since 1999
- Provides real-time analytics and reporting, gaining visibility into email and IM usage and growth patterns

Data Sheet: Endpoint Security

Symantec™ Multi-tier Protection

Symantec Endpoint Protection product family

	Symantec Endpoint Protection	Symantec Multi-tier Protection	Symantec Multi-tier Protection
	Small Business Edition		
Antivirus	X	X	X
Antispyware	X	X	X
Firewall	X	X	X
Device and application control	X	X	X
Intrusion prevention	X	X	X
Symantec™ Mail Security for Microsoft Exchange		X	X
Symantec™ Mail Security for Domino			X
Premium AntiSpam (for Groupware)		X*	X*
Brightmail Gateway software subscription			X*
Symantec Mobile AntiVirus for Windows Mobile			X*
SAV for Linux	X	X	X
SAV for Mac		X*	X

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

* New additions.

Note:

- If a customer does not want to use SEP when they purchase a bundle, they may install SAV. They just need to go directly to Customer Care.
- In the new bundle, SEP version is SEP 11.0.2 (MR3).
- Brightmail Gateway included in the bundle can be used as a virtual appliance. VMware is not included in the bundle.

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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 <i>Symantec Endpoint Protection Manager 11.x communication troubleshooting</i> on the Symantec Support Web Site.	The following operating systems are supported: <ul style="list-style-type: none"> • 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

Data Sheet: Endpoint Security

Symantec™ Multi-tier Protection

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

Component	32-bit	64-bit
Display	Super VGA (1,024x768) or higher-resolution video adapter and monitor	Super VGA (1,024x768) or higher-resolution video adapter and monitor
Database	<p>The Symantec Endpoint Protection Manager includes an embedded database. You may also choose to use one of the following versions of Microsoft SQL Server:</p> <ul style="list-style-type: none"> Microsoft SQL Server 2000 with Service Pack 3 or later Microsoft SQL Server 2005 <p>Note: Microsoft SQL Server is optional.</p>	<p>The Symantec Endpoint Protection Manager includes an embedded database. You may also choose to use one of the following versions of Microsoft SQL Server:</p> <ul style="list-style-type: none"> Microsoft SQL Server 2000 with Service Pack 3 or later Microsoft SQL Server 2005 <p>Note: Microsoft SQL Server is optional.</p>
Other requirements	<p>The following other requirements must be met:</p> <ul style="list-style-type: none"> Internet Information Services server 5.0 or later with World Wide Web services enabled Internet Explorer 6.0 or later Static IP address (recommended) 	<p>The following other requirements must be met:</p> <ul style="list-style-type: none"> 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 (continued)

Component	32-bit	64-bit
Operating system	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> Windows® 2000 Server/Advanced Server/Datacenter Server with Service Pack 3 or later Windows XP Professional with Service Pack 1 or later <p>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 <i>Symantec Endpoint Protection Manager 11.x communication troubleshooting</i> on the Symantec Support Web Site.</p> <ul style="list-style-type: none"> Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Web Edition/Small Business Server 	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> 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 <p>Note: If you use Microsoft Clustering services for the SEPM server, you must install the SEPM server on the local volume.</p>
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	<p>The following other requirements must be met:</p> <ul style="list-style-type: none"> Internet Information Services server 5.0 or later with World Wide Web services enabled Internet Explorer 6.0 or later Static IP address (recommended) 	<p>The following other requirements must be met:</p> <ul style="list-style-type: none"> 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	<p>1 GHz on x64 only with the following processors:</p> <ul style="list-style-type: none"> Intel Xeon with Intel EM64T support Intel Pentium IV with EM64T support AMD 64-bit Opteron™ AMD 64-bit Athlon™ <p>Note: Itanium is not supported.</p>

Data Sheet: Endpoint Security

Symantec™ Multi-tier Protection

Symantec Endpoint Protection Console

Component	32-bit	64-bit
Processor	1 GHz Intel Pentium III	<p>1 GHz on x64 only with the following processors:</p> <ul style="list-style-type: none"> • Intel Xeon with Intel EM64T support • Intel Pentium IV with EM64T support • AMD 64-bit Opteron™ • AMD 64-bit Athlon™ <p>Note: Itanium is not supported.</p>
Operating system	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> • 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 <p>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 <i>Symantec Endpoint Protection Manager 11.x communication troubleshooting</i> on the Symantec Support Web Site.</p> <ul style="list-style-type: none"> • Windows Server 2003 Standard Edition/ Enterprise Edition/ Datacenter Edition/ Web Edition/ Small Business Server • Windows Vista® (x86) 	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> • 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) <p>Note: The Symantec Network Access Control installation CD contains a 64-bit application.</p> <p>Note: If you use Microsoft Clustering services for the SEPM server you must install the SEPM server on the local volume.</p>
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	<p>The following other requirements must be met:</p> <ul style="list-style-type: none"> • Internet Explorer 6.0 or later • Java™ Runtime Environment 5.0, update 13 or above recommended 	<p>The following other requirements must be met:</p> <ul style="list-style-type: none"> • 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	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> • 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

Data Sheet: Endpoint Security

Symantec™ Multi-tier Protection

Quarantine Console (continued)

Component	32-bit	64-bit
Other requirements	<p>The following other requirements must be met:</p> <ul style="list-style-type: none"> • Internet Explorer 5.5 Service Pack 2 or later • Microsoft Management Console version 1.2 or later <p>If MMC is not already installed, you need 3 MB free disk space (10 MB during installation).</p>	Not tested

Symantec Endpoint Protection

Component	32-bit	64-bit
Processor	400 MHz Intel Pentium III (1 GHz for Windows Vista)	<p>1 GHz on x64 only with the following processors:</p> <ul style="list-style-type: none"> • Intel Xeon with Intel EM64T support • Intel Pentium IV with EM64T support • AMD 64-bit Opteron™ • AMD 64-bit Athlon™ <p>Note: Itanium is not supported.</p>
Operating system	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> • 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 • Windows Vista (x86) Home Basic Edition/Home Premium Edition/Business Edition/Enterprise Edition/Ultimate Edition 	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> • 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 <p>Note: If you are using Microsoft Clustering Services, you must install the client on the local volume.</p>
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

Central Quarantine Server

Component	32-bit	64-bit
Processor	600 MHz Intel Pentium III	Not tested
Operating system	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> • 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
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	<p>The following other requirements must be met:</p> <ul style="list-style-type: none"> • Internet Explorer 5.5 Service Pack 2 or later 	Not tested

Data Sheet: Endpoint Security

Symantec™ Multi-tier Protection

Symantec Endpoint Protection (continued)

Component	32-bit	64-bit
Other requirements	Internet Explorer 6.0 or later Terminal Server clients connecting to a computer with antivirus protection have the following additional requirements: <ul style="list-style-type: none">• 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

Symantec AntiVirus for Macintosh 10.2 Administration Server

Operating system requirements:

- Mac OS X Server 10.4.11–10.5.x

Hardware requirements:

- Xserve G5, Xserve, Power Mac G5, Power Mac G4, Macintosh Server G4, Power Macintosh G3 (Blue & White), Macintosh Server G3 (Blue & White), iMac, eMac, or Mac mini computer
- 256 MB of RAM; at least 512 MB of RAM for high-demand servers running multiple services
- Built-in FireWire
- 4 GB of available disk space

Other software requirements:

- As an included add-on component, the Symantec Administration Console requires that Macintosh clients with Symantec AntiVirus 10.2 for Macintosh run under Mac OS 10.4.11–10.5.x.

Note: Mac OS X Server 10.4.11–10.5.x is required. Mac OS X Server 10.4 and 10.5 software includes Apache and MySQL.

Symantec AntiVirus for Macintosh 10.2 Administration Console

Supported Administration Console browsers:

- Mac OS X + Safari 1.2.x, Firefox 2
- Mac OS X + Safari 1.2.x, Firefox 2 Windows XP Pro + Internet Explorer 6 SP2, Firefox 2
- Red Hat Linux + Netscape 7

Symantec AntiVirus for Macintosh Client 10.2

Operating system requirements:

- Macintosh OS X version 10.4.11–10.5.x

Hardware requirements:

- G3 processor or higher (G4 800 MHz or better if running Mac OS X 10.4.11 or Mac OS X 10.5.x)
- 192 MB of RAM
- 40 MB of available hard disk space for installation
- Internet connection required for LiveUpdate

Symantec Mail Security for Microsoft Exchange

Operating system requirements:

- Microsoft Windows® 2000 Server/Advanced Server/Data Center (SP4)
- Microsoft Windows Server 2003 Standard/Enterprise/ Data Center (SP1)
- Microsoft Windows Server 2003 x64 or Windows Server 2003 R2 x64, Standard or Enterprise Edition
- Microsoft Windows Server 2008 x64 Standard or Enterprise Edition

Data Sheet: Endpoint Security

Symantec™ Multi-tier Protection

Minimum system requirements:

For Microsoft Windows Server 2003 x64 or 2008 x64

Standard or Enterprise Edition:

- Intel® Server-class 32-bit processor
- 1 GB of RAM

For Exchange Server 2007:

- x64 architecture-based computer with Intel processor that supports Intel Extended Memory 64 Technology (Intel EM64T), or AMD processor that supports the AMD64 platform
- 2 GB of RAM minimum

For all versions of Exchange:

- 325 MB available disk space for Symantec Mail Security for Microsoft Exchange
- .NET Framework version 2.0
- Microsoft Data Access Components (MDAC) 2.8 or higher
- Microsoft DirectX® 9.0

Console-only installation requirements:

Operating system

- Windows 2000 (SP4)
- Windows 2003 (SP1)
- Windows XP (SP1)

Minimum system requirements:

- 512 MB of RAM
- 250 MB available disk space
- .NET Framework version 2.0
- Microsoft DirectX 9.0

Symantec Mail Security for Domino

System requirements:

- Lotus Domino® server version 6.5.x or 7.x
- Microsoft Windows 2000 Server, Windows 2000 Advanced Server, Windows Server 2003, or Windows Server 2003 Enterprise Edition
- Lotus Notes® client
 - Lotus Notes version 6.5.x or 7.x
 - 128 MB RAM minimum (256 MB or more recommended)
 - 300 MB available disk space

Note: Domino server should be sized based on Domino system requirements. System requirements should take into account additional needs such as file system antivirus protection, backup operations, and other business-critical applications unique to the environment.

Symantec Gateway Protection

Supported Internet browsers:

- Microsoft Internet Explorer® 6.0, 7.0
- Firefox 2.0

Supported virtualization platforms:

- VMware Server 1.0.4
- VMware ESX Server 3.0.2

Note: VMware is not included in the bundle.

Data Sheet: Endpoint Security

Symantec™ Multi-tier Protection

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.



Copyright © 2008 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, Symantec AntiVirus, and Premium AntiSpam are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Domino, Lotus, and Lotus Notes are trademarks of International Business Machines Corporation in the United States, other countries, or both. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Novell is a registered trademark of Novell, Inc. in the United States and other countries. Microsoft, Active Directory, Windows, Windows Server, and Windows Vista are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. Printed in the U.S.A.

10/08 12836805-3