# Symantec™ Protection Suite Enterprise Edition

Trusted protection for endpoints and messaging environments

Overview

Symantec Protection Suite Enterprise Edition creates a protected endpoint and messaging environment that is secure against today's complex malware, data loss and spam threats, and is quickly recoverable in the event of failure. Reduce the cost of securing your environment and more effectively manage the inherent risks of today's IT infrastructures with Symantec's proven endpoint security, messaging security and system recovery technologies.

Symantec Protection Suite Enterprise Edition is an unparalleled combination of award-winning technologies from the world leader in security and data protection that enables you to completely protect, easily manage and automatically control the assets most crucial to your business.
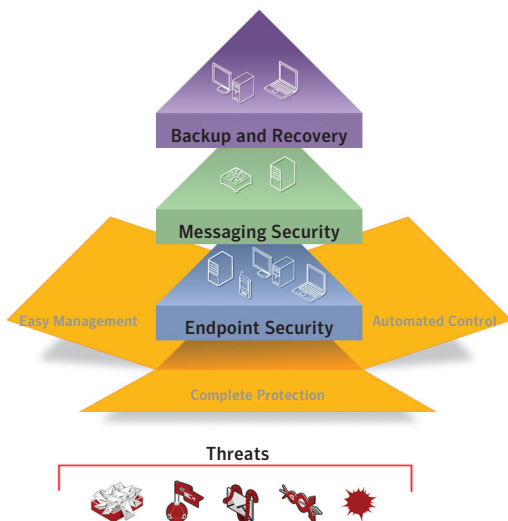
Endpoint Security

More than antivirus

Symantec Protection Suite delivers more than world-class, industry-leading antivirus and antispyware signature-based protection. It provides advanced threat prevention that protects your endpoints - laptops, desktops, servers and mobile devices - from targeted attacks and attacks not seen before. It includes turnkey, proactive technologies that automatically analyse application behaviours and network communications to detect and block suspicious activities, as well as administrative control features that allow organisations to deny specific device and application activities deemed as high risk. In addition, the new suite features built-in software-based network access control to ensure endpoints remain in compliance with IT policy regardless of where or how they connect to the network. This multi-layered approach significantly lowers risks, giving confidence that business assets are protected. Protection Suite's endpoint security includes all these capabilities now, with the ability to enable individual components as needed.

Messaging Security

Antispam and messaging security protection

Symantec Protection Suite provides effective and accurate antispam and antivirus protection for both inbound and outbound email and instant messaging (IM). Protection Suite's messaging security components can be deployed both at the messaging server level on Microsoft® Exchange and Lotus Domino® and at the gateway level with physical or virtual appliance-

Confidence in a connected world.

✱symantec™

based security. Advanced content filtering and data loss prevention help organisations control sensitive data, reduce the risks associated with data loss, and meet regulatory compliance and corporate governance demands. Protection Suite's messaging security is simple to administer and catches more than 97% of spam with less than one in a million false positives. Continuous automatic updates, global and self-learning local IP reputation analysis, and comprehensive reporting ensure that the Protection Suite effectively and transparently responds to new spam threats to minimise network downtime and preserve employee productivity.

Backup and Recovery
Full system and data recovery

Symantec Protection Suite further extends system protection to include disk-based system recovery for Microsoft® Windows based desktops and laptops which enables businesses to recover from system loss or disasters in minutes, not hours or days — even to dissimilar hardware platforms, to virtual environments or in remote, unattended locations.

Key Benefits
Protect Completely
Multi-layer protection from endpoint to gateway

Deploy proven technologies—Protect with confidence with the market-leading endpoint security, messaging security, data loss prevention and system recovery vendor.

Protect against more threats—Secure your environment against data loss, malware and spam by accurately identifying and addressing risks consistently across different platforms.

Protect end-to-end—Protect endpoints, messaging servers and gateways proactively with more than traditional antivirus and antispyware.

Safeguard intellectual property—Secure sensitive data and valuable confidential information at the gateway with advanced content filtering and data loss prevention.

Rely on trusted research—Protect proactively with real-time security intelligence that provides early threat warnings and protection from newly evolved threats.

Rapidly recover with ease—Recover individual files and folders in seconds or complete Windows systems in minutes reliably and with confidence, even to dissimilar hardware or virtual environments.

Manage Easily
Unified management and administration

Simplify implementation & operations—Quickly deploy with minimal disruption to your environment through easy management and optimised utilisation of system resources

Manage with ease—Streamlined management with optimised workflows for critical security tasks, freeing administrators and end-users from unproductive tasks

Confidence in a connected world.

✦symantec™

Flexible and scalable configuration—Meet IT policy requirements with granular control over policies and features which are easily configurable and selectively deployable

Eliminate environment complexity—Deploy integrated essential endpoint and messaging security technologies as unified solutions with coordinated management

Streamline processes—Eliminate additional steps and costs with one decision, one purchase and one vendor for complete protection

Reduce operational costs—Reduce the time, cost and expertise needed to manage multiple technologies

Control Automatically
Automatic backup & recovery, monitoring, updating and enforcement

Ensure compliance—Achieve, prove and enforce adherence to IT policy and regulatory objectives with ease

Regulate sensitive information—Identify and control the flow of sensitive information via email and IM, as well as to and from endpoints

Effortlessly update—Adapt to risks faster and take action within minutes with the Symantec Global Intelligence Network, one of the largest security research networks in the world

Gain increased visibility into your environment—Provide increased insight into actions, events and status from endpoints and messaging infrastructure with insightful reporting

Minimise downtime—Get your business systems back up and running quickly by restoring from both event–driven and scheduled recovery points

Key Features

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

Single agent and single management console—Antivirus, antispyware, desktop firewall, intrusion prevention, device and application control, and network access control are all in a single agent — managed by a single management console.

Antivirus for Linux, Mac, and Windows Mobile—Remove viruses from email attachments, Internet downloads, and other sources to safeguard the enterprise network. Enables secure mobile computing by providing comprehensive virus protection against malicious threats that target Windows Mobile operating systems.

Confidence in a connected world.

symantec™

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.[1]

- Scans inbound and outbound email for compliance with regulatory and governance requirements

- Provides incident management and reporting capabilities that enable organisations to implement policies and analyse and manage violations

- Continuously delivers automatic spam signature updates and reputation scoring to help ensure effective, real-time protection against new threats

- Offers unparalleled protection, as evidenced by the industry's only record of over 40 consecutive VB100 awards since 1999

- Provides real-time analytics and reporting, gaining insight into email and IM use and growth patterns

System recovery—Enables rapid, reliable recovery of computer data and systems.

- Create while-you-work backups of the entire system, without disrupting user productivity

- Home page view immediately identifies the backup status of computer systems

- Run backups automatically when the Symantec ThreatCon level reaches or exceeds the level you specify

1. Symantec Brightmail Gateway 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

Confidence in a connected world.   symantec™

How to choose the right Endpoint Security product

Protection technology	10–99 seats		100+ seats	
	Symantec Endpoint Protection Small Business Edition	Symantec Protection Suite Small Business Edition	Symantec Endpoint Protection	Symantec Protection Suite Enterprise Edition
Endpoint security				
Antivirus/Antispyware	•	•	•	•
Desktop firewall	•	•	•	•
Intrusion prevention	•	•	•	•
Generic Exploit Blocking	•	•	•	•
Device and application control			•	•
Antivirus for Macintosh®		•		•
Antivirus for Linux®			•	•
Antivirus for Windows® Mobile				•
Network access control self-enforcement				•
Messaging security				
Antivirus/Antispam/Antiphishing		•		•
Reputation-based spam filtering				•
Content filtering/Compliance		•		•
Data loss prevention				•
Microsoft® Exchange		•		•
Gateway software subscription & Lotus Domino®				•
Backup and recovery				
Backup live desktops and laptops		•		•
Restore to any hardware		•		•
Threat-driven backups		•		•

Note: Symantec Protection Suite Enterprise Edition Messaging Security features available for Exchange, Domino, Gateway and Instant Messaging, while Symantec Protection Suite Small Business Edition Messaging Security is only available on Exchange.

Confidence in a connected world.

symantec™

Minimum System Requirements

Hardware / Software	Operating Systems / Browsers	Memory (min)	Hard Disk (min)
Endpoint Protection Client Workstations and Servers			
Processor: Intel® Pentium® or compatible, 32-bit and 64-bit Note: No Itanium® support	Windows® 32-bit and 64-bit: - 2000 Professional, Server, Advanced Server, Data Centre Server, Small Business Server (Service Pack 3 or later) - XP Home Ed., Professional Ed., Tablet PC Ed., Embedded Ed., Media Centre Ed. (Service Pack 1 or later) - Server 2003 Standard Ed., Enterprise Ed., Data Centre Ed., Web Ed., Small Business Server, Computer Cluster Server, Storage Server - Vistas® Home Basic, Home Premium, Business, Enterprise, Ultimate - Server 2008 Standard Ed., Enterprise Ed., Data Centre Ed., Web Ed. - Small Business Server Standard Ed., Premium Ed. Linux® 32-bit and 64-bit: - Red Hat® Enterprise Linux 3.x, 4.x, 5.x - SUSE Linux Enterprise (server/desktop) 9.x, 10.x - Novell® Open Enterprise Server (OES/OES2) - VMware ESX 2.5, 3.x - Ubuntu 7.x, 3.x - Debian 4.x	256 MB RAM	600 MB
Endpoint Protection Management Server			
Processor: Intel Pentium or compatible, 32-bit and 64-bit Note: No Itanium support	Windows 32-bit and 64-bit - 2000 Server, Advanced Server, Data Centre Server, Small Business Server (Service Pack 3 or later) - XP Professional Ed. (Service Pack 1 or later) - Server 2003 Standard Ed., Enterprise Ed., Data Centre Ed., Web Ed., Small Business Server, Computer Cluster Server, Storage Server - Server 2008 Standard Ed., Enterprise Ed., Data Centre Ed., Web Ed. - Small Business Server Standard Ed., Premium Ed. - Essential Business Server Standard Ed., Premium Ed.	1 GB	2 GB
Endpoint Protection Management Console			
Processor: Intel Pentium or compatible, 32-bit and 64-bit Note: No Itanium support	Windows 32-bit and 64-bit: - 2000 Professional, Server, Advanced Server, Data Centre Server, Small Business Server (Service Pack 3 or later) - XP Professional Ed. (Service Pack 1 or later) - Server 2003 Standard Ed., Enterprise Ed., Data Centre Ed., Web Ed., Small Business Server, Computer Cluster Server, Storage Server - Vista Home Basic, Home Premium, Business, Enterprise, Ultimate - Server 2008 Standard Ed., Enterprise Ed., Data Centre Ed., Web Ed. - Small Business Server Standard Ed., Premium Ed. - Essential Business Server Standard Ed., Premium Ed.	512 MB	15 MB
Endpoint Protection Database			
	Embedded database provided. Also supports: - Microsoft SQL Server 2000 (Service Pack 3 or later) - Microsoft SQL Server 2005		4 GB
AntiVirus for Linux Client			
(not managed by Endpoint Protection Manager)	Linux 32-bit and 64-bit: - Red Hat® Enterprise Linux 3.x, 4.x, 5.x - SUSE Linux Enterprise (server/desktop) 9.x, 10.x - Novell® Open Enterprise Server (OES/OES2) Linux 32-bit only: - VMware ESX 2.5, 3.x		
AntiVirus for Macintosh Administration Server			
- Xserve G5, Xserve, Power Mac G5, Power Mac G4, Macintosh Server G4, Power Macintosh G3 (Blue & White), Macintosh Server G3 (Blue & White), iMac, eMac, Mac mini computer - Built-in FireWire	Mac OS X Server 10.4.11-10.5.x Note: Mac OS X Server 10.4 and 10.5 includes Apache and MySQL	256 MB RAM 512 MB RAM for high-demand servers running multiple services	4 GB

Confidence in a connected world.

symantec™

Hardware / Software	Operating Systems / Browsers	Memory (min)	Hard Disk (min)
AntiVirus for Macintosh Administration Console			
	- Mac OS X + Safari 1.2x, Firefox 2 - Windows XP Pro + Internet Explorer 6SP2 - Red Hat Linux + Netscape 7		
AntiVirus for Macintosh Client			
- G4 800 MHz	Mac OS X 10.4.11-10.5.x	192 MB RAM	40 MB
Mobile AntiVirus for Windows Mobile			
	Mobile Device: - Microsoft Windows Mobile 6 Standard, Professional - Microsoft Windows Mobile 5.0 SmartPhone and Pocket PC Administration Tools: - Microsoft Windows 2000, XP, and 2003 Server		2.5 MB
Mail Security for Exchange			
Processor: - Intel server-class 32-bit (for Server2003 x64 or Server 2008 x64) - Intel 64-bit that supports Extended Memory 64 Technology or AMD 64-bit {for Exchange Server 2007) Software Components: - NET Framework v.2 - Microsoft Data Access Components (MDAC) 2.8 or higher - Microsoft DirectX® 9.0	Microsoft Windows: - 2000 Server, Advanced Server, Data Centre (Service Pack 4 or higher) - Server 2003 Standard Ed., Enterprise Ed., Data Centre Ed. (Service Pack 1 or higher) - Server 2003 x64 or R2 x64 Standard Ed., Enterprise Ed. - Server 2008 x64 Standard Ed., Enterprise Ed. - Small Business Server Standard Ed., Premium Ed. Console-only installation: Windows 2000 (Service Pack 4 or higher), Windows 2003 (Service Pack 1 or higher), Windows XP (Service Pack 1 or higher)	- 512 MB RAM - 1 GB RAM for Windows Server 2003 x64 or Windows Server 2008 x64 - 2 GB RAM for Exchange Server 2007	325 MB
Mail Security for Domino			
	Microsoft Windows: - 2000 Server, Advanced Server - Server 2003 Standard Ed., Enterprise Ed. Lotus: - Domino® server 6.5.x, 7.x - Notes® client 6.5.x, 7.x	128 MB RAM (256 MB RAM recommended)	300 MB
Brightmail Gateway			
Physical Appliances: - Brightmail 8300 Series - Mail Security 8300 Series - Mail Security 8200 Series Virtual Appliances: - 2 CPUs min, 4 CPUs recommended	Administrator Console: Microsoft Internet Explorer 6.0, 7.0 Firefox 2.0 Virtual Appliances: VMware ESX and ESXi 3.x	Virtual Appliances: 2 GB (4 GB recommended)	Virtual Appliances: 30 GB min
Backup Exec System Recovery Desktop edition			
Processor: - 233 MHz or greater, as required by the operating system Software Components: .Net Framework v.2	Windows(R) 32-bit or 64-bit operating systems: - Windows Vista(R) Ultimate, Business, Enterprise - Windows XP Media Centre Ed., Professional Ed., Home Ed. (SP2 or later) Virtual platforms (for converted recovery points): - VMware ESX Server 2.0, 3.0 and 3.5 - VMware Server 1.0 - VMware GSX Server 3.x (replaced by VMware Server) - VMware Workstation 4, 5, and 6 - Microsoft Hyper-V - Microsoft Virtual Server 2005 R2 and later - Citrix XenServer 4.x	- Agent:512 MB - User interface and Recovery Point Browser: 512 MB - Recovery Disk: 512 MB minimum (dedicated), /68 MB min if multilingual version - LightsOut Restore feature: 1 GB	250-390 MB Additional: Sufficient hard disk space on a local hard disk or network server for storing recovery points

Confidence in a connected world.

symantec™

Services

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

Visit our website
http://enterprise.symantec.com

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 website.

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

Symantec Dublin
Ballycoolin Business Park
Blanchardstown
Dublin 15
Ireland
Phone: +353 1 803 5400
Fax: +353 1 820 4055

Confidence in a connected world.