Data Sheet: Endpoint Security

Symantec™ Protection Suite Enterprise Edition

Trusted protection for endpoint, messaging, and Web environments

Overview

Symantec™ Protection Suite Enterprise Edition creates a protected endpoint, messaging, and Web 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 using Symantec™ Protection Center, a single sign-on Web console, and more effectively manage the inherent risks of today's IT infrastructures with proven Symantec endpoint security, messaging security, and system recovery technologies. 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.

SYMANTEC™ PROTECTION SUITE ENTERPRISE EDITION
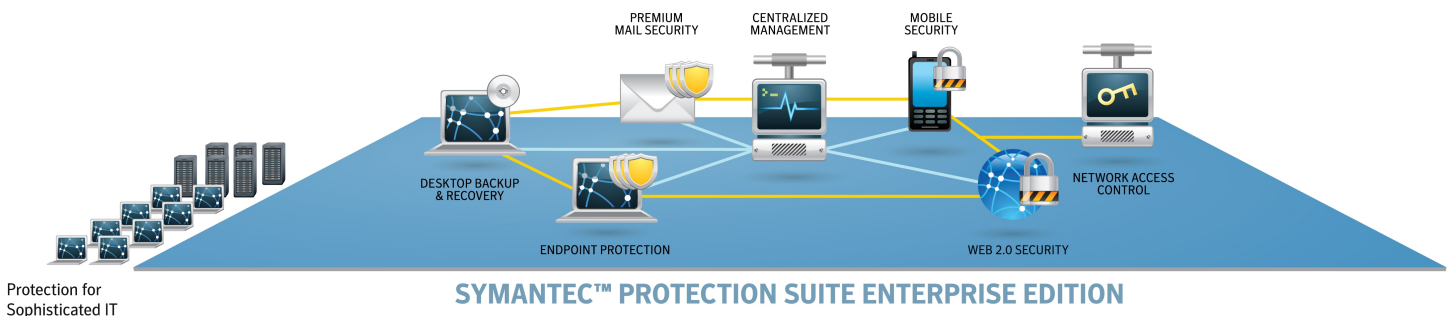
Endpoint security

More than antivirus

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 analyze application behaviors and network communications to detect and block suspicious activities, including administrative control features that allow organizations 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 multilayered approach significantly lowers risk, providing confidence that business assets are protected. The endpoint security of Protection Suite Enterprise Edition includes these capabilities now, with the ability to enable individual components as needed.

Messaging and Web security

Antispam, messaging, and Web security protection

Protection Suite delivers inbound and outbound messaging security, with effective and accurate real-time antispam and antivirus protection, advanced content filtering, data loss prevention, and email encryption. The Protection Suite 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-based security. Advanced content filtering and data loss prevention help organizations control sensitive data, reduce the risks associated with data loss, and meet regulatory compliance and corporate

Confidence in a connected world.   symantec.

governance demands. The Protection Suite messaging security is simple to administer and the messaging security solutions within the suite have been benchmarked at catching more than 99% of spam with very few false positives[1] . Real-time 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. This minimizes network downtime and preserves employee productivity.

Protection Suite Enterprise Edition also offers unpararelled Web security to fend off today's complex Web-borne malware threats. Organizations can safely use the Web to conduct business, communicate with partners and customers by deploying Symantec™ Web Gateway. Web Gateway gives organizations the ability to detect infected endpoints, monitor inbound and outbound Web traffic for threats, and safely use today's Web 2.0 applications.

Backup and recovery

Full system and data recovery

Protection Suite extends its 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. It centrally manages backup and recovery tasks for multiple desktops and laptops across the entire organization.

Key benefits

Protect completely

Multi-layer protection from endpoint to gateway

- **Deploy proven technologies.** Protect with confidence with the market-leading endpoint security, messaging and Web security, data loss prevention, and system recovery vendor.
- **Protect against more threats.** Secure your environment against data loss, malware, spam, botnets, and other Web 2.0 threats by accurately identifying and addressing risks consistently across different platforms.
- **Protect end-to-end.** Protect at the endpoint, messaging server, and Web and messaging 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—now including support for Windows 7.

[1.] VBSpam (VirusBulletin-Fighting malware and spam), March 2010 - http://www.virusbtn.com/vbspam/index, author: Martijn Grooten

Confidence in a connected world.   symantec.

Manage easily

Unified management and administration

- **Reduce operational overhead and manage with ease.** Efficiently manage your environment with Symantec Protection Center, a single sign-on Web console that provides administrators full access to configuration management, report generation, and dashboard views of multiple Symantec protection technologies.
- **Simplify implementation & operations.** Quickly deploy with minimal disruption to your environment through easy management and optimized utilization of system resources.
- **Boost productivity.** Streamlined management with optimized workflows for critical security tasks, freeing administrators and end-users from unproductive tasks.
- **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.
- **Centrally manage backup.** Manage physical to virtual conversions, off-site copy capabilities and backup destination monitoring from a central location.
- **Easily replace existing software.** Remove existing solutions install new clients and report on them.

Control Automatically

Automatic backup and 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 on to and off of 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 visibility into actions, events, and status from endpoints and messaging infrastructure with insightful reporting.
- **Minimize 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.

Confidence in a connected world.   ✚ symantec™

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.

Antispam and messaging security protection. Symantec Brightmail™ has been benchmarked at catching more than 99% of spam with very few false positives[2] .

- Scans inbound and outbound email for compliance with regulatory and governance requirements
- Provides incident management and reporting capabilities that enable organizations to implement policies and analyze and manage violations
- Continuously delivers real-time 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
- Allows customers to encrypt sensitive outbound email without managing any additional infrastructure.
- Supports virtualized Exchange environment

Web security. Protect against Web 2.0 threats, including spyware, botnets, viruses, other types of malware, and provides control for Web and application use.

- Fast protection at the Web gateway across multiple protocols for inbound and outbound Web traffic
- Protects against malware threats on all Web 2.0 file transfer channels
- Inspects, detects, and blocks active and dormant botnets

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
- Centrally manage backup and recovery tasks for multiple desktops and laptops across the entire organization

[2.] VBSpam (VirusBulletin-Fighting malware and spam), March 2010 - http://www.virusbtn.com/vbspam/index, author: Martijn Grooten

Confidence in a connected world.

symantec™

Which Symantec™ Protection Suite is right for me?				
Protection technology	**Symantec Protection Suite Enterprise Edition**	**Symantec Protection Suite Enterprise Edition for Endpoints**	**Symantec Protection Suite Enterprise Edition for Gateway**	**Symantec Protection Suite Enterprise Edition for Servers**
Endpoint security				
Antivirus/Antispyware	•	•		•
Endpoint firewall	•	•		•
Intrusion detection/prevention	•	•		•
Device & application control	•	•		•
Protection for Macintosh®	•	•		•
Protection for Linux®	•	•		•
Protection for Windows® Mobile	•	•		
Protection for AIX, HP-UX, Solaris, VM				•
Network access control self-enforcement	•	•		
Network access control for Gateway and Guest			•	
Data loss prevention		•		
File access control and audit				•
Messaging and Web security				
Antivirus/Antispam/Antiphishing	•		•	
Reputation-based spam filtering	•		•	
Content filtering/Compliance	•		•	
Data loss prevention	•		•	
Microsoft® Exchange	•		•	
Lotus Domino®	•		•	
Messaging Gateway software subscription	•		•	
Web Gateway software subscription	•		•	
Backup and recovery				
Backup live desktops and laptops	•			
Restore to any hardware	•			
Server backup and disaster recovery				
Threat driven backups	•			
Central management console				
Single sign-on management and reporting access	•	•	•	•
Endpoint management				
IT process automation		•	•	•
Hardware and software inventory		•		
OS and application patch management		•		

Confidence in a connected world.

symantec™

Minimum System Requirements

Hardware/Software	Operating Systems/Browsers
Symantec™ Endpoint Protection/Network Access Control	
Windows Agent* (includes network access control)	Microsoft® Windows® XP Professional, Windows Server® 2003, Windows Vista™, Windows 7, Windows Server 2008, Windows 2000 Server (32–bit)
Mac Agent	Mac OS X 10.4–10.5x (PPC) Mac OS X 10.4–10.6 (Intel®)
Endpoint Protection Manager	Windows 2000 Server (32–bit), Windows XP Professional, Windows Server 2003, Windows Server 2008, Windows Business Server 2008 Microsoft Internet Information Services (Web server) Microsoft® SQL Server™ 2000 SP3 or SQL Server 2005 (optional) Note: No Itanium® hardware support
Symantec™ AntiVirus for Linux	
Client for Workstations and Servers (not managed by Endpoint Protection Manager)	Red Hat® Enterprise Linux, SUSE® Linux Enterprise (server/desktop), Novell® Open Enterprise Server (OES/OES2), VMware® ESX, Ubuntu®, Debian®, Fedora®
Symantec™ Mobile Antivirus for Windows® Mobile	
Mobile Device Agent	Microsoft Windows Mobile 6 and 6.1 Standard, Professional Microsoft Windows Mobile 5.0 SmartPhone and Pocket PC
Administration Tools	Microsoft Windows 2000 Server, XP Professional, and 2003 Server
Symantec™ Mail Security for Exchange	
Exchange platform: – Microsoft Exchange Server 2003 – Microsoft Exchange Server 2007 – Microsoft Exchange Server 2010 Hardware virtualization: – VMware ESXi 3.5/4.0; vSphere 4.0 – Microsoft Hyper-V Server 2008 – Windows Server 2008 with Hyper-V technology	Microsoft Windows: – Server 2008 R2/SP2; Standard/Enterprise (64-bit only) – Server 2003 R2/SP2; Standard/Enterprise (32-bit or 64-bit) Management console: – Windows 7/Vista/XP – Windows Server 2008 R2/SP2; Standard/Enterprise (64-bit only) – Windows Server 2003 R2/SP2; Standard/Enterprise (32-bit or 64-bit)
Symantec™ Mail Security for Domino®	
	Microsoft Windows (32-bit or 64-bit): – Windows Server 2003/2008 IBM Lotus®: – Domino Server 7.x, 8.0.x, or 8.5.1 (32-bit or 64-bit) – Notes® Client 7.x or later
Symantec Brightmail™ Gateway	
Physical appliances: – Brightmail 8300 Series – Mail Security 8300 Series	Administrator console: Microsoft Internet Explorer 6.0, 7.0, 8.0 Firefox 2.0, 3.0 Virtual appliances: VMware ESX 3.5 (rev 4 or later) VMware vSphere 4.0 VMware ESXi 3.5 (rev 3 or later), ESXi 4.0
Symantec™ Web Gateway	
Physical appliances: – Web Gateway 8400 Series	Administrator console: Microsoft Internet Explorer 6.0, 7.0 Firefox 3.0
Symantec Backup Exec™ System Recovery Desktop Edition	
Processor: – 233 MHz or greater, as required by the operating system	Windows®: – Windows 7 Ultimate, Enterprise, Professional – Windows Vista Ultimate, Business, Enterprise – Windows XP Media Center Ed., Professional Ed., Home Ed. (SP2 or later)

* Operating system support is for 32-bit and 64-bit unless stated otherwise

Confidence in a connected world. symantec™

Services

Symantec offers a range of consulting, technical education, and support services to guide organizations through the migration, deployment, and management of Symantec Protection Suite and help realize the full value of your investment. Essential Support Services provide confidence that 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.

More information

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 consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec helps organizations secure and manage their information-driven world with **high availability**, and **disaster recovery** solutions.   20024156-5 05/10

Confidence in a connected world.   symantec™