

Symantec™ Protection Suite Enterprise Edition for Servers

Complete and high performance protection where you need it

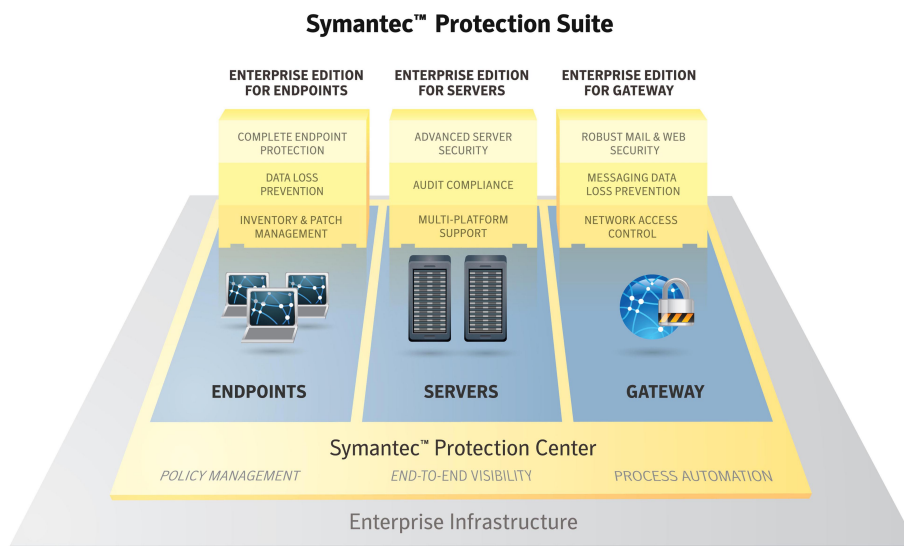
Overview

Symantec™ Protection Suite Enterprise Edition for Servers delivers high-performance protection against physical and virtual server downtime with policy-based prevention, using multiple protection technologies combined in a single cost-effective suite. Leveraging the new Symantec security management solution, Symantec™ Protection Center, the Protection Suite Enterprise Edition for Servers consolidates access to threat, security, and operational dashboards that give decision makers deep visibility across the security infrastructure while delivering real-time and actionable information. Enforce flexible controls against the known and unknown vulnerabilities impacting your critical systems. Leverage behavioral and vulnerability-based detection with advanced antivirus, host-based firewall with application control, intrusion prevention, and device control to protect against zero-day attacks, harden systems, and maintain compliance.

This suite provides a flexible server security solution that controls user and application behaviors, blocks inappropriate network traffic and events, and provides real-time and signature-based approaches to accommodate server workloads based on a variety of server profiles. It controls system behavior by preventing specific actions that an application or user might take and by auditing system processes, files, log data, and critical settings for inappropriate activity. Its centralized management console enables administrators to configure and maintain security policies, manage users and roles, view alerts, and run reports across heterogeneous operating systems.

Protection Suite Enterprise Edition for Servers also provides unique process automation capabilities to track, manage, and control all aspects of a proactive response workflow. Response processes can be automatically executed via email, Web forms, or handheld devices or by setting up a queue of workflow tasks requiring action.

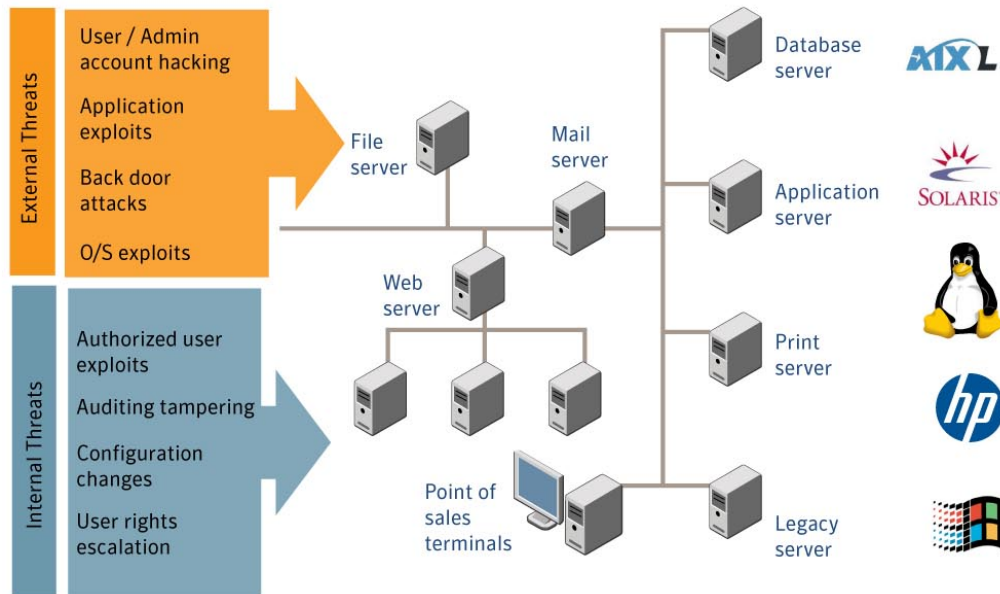
For meeting protection requirements, this solution suite delivers comprehensive audit evidence via consolidated event logs, and advanced log analysis and reporting. Symantec Protection Suite Enterprise Edition for Servers is a comprehensive solution for server security. It is an unparalleled combination of highly effective technologies from the world leader in security and data protection that enables organizations to protect, easily manage, and automatically control the server assets most crucial to their business.



Key benefits

Proactive protection against known and unknown vulnerabilities

- Provides behavioral and vulnerability-based detection with advanced antivirus, host-based firewall with application control, intrusion prevention, and device control
- Protects against misuse by authorized people and programs through system and device controls, which lock down configuration settings and file systems and also prevent installation and execution of unauthorized executables
- Blocks network traffic and prevents unauthorized changes to system resources



Effective granular controls across broad physical and virtual server environments

- Provides broad platform coverage including Windows®, Solaris®, Linux®, AIX®, HP-UX®, and VMware ESX (host and guest); and it includes Virtual Agent for unsupported and less common platforms
- Includes adaptive risk-profile protection to set protection levels based on server types to monitor and enforce performance and risk mitigation requirements
- Prevents installation and operation of unauthorized executables

Policy-based operation for easy deployment and low-cost administration

- Automates policy-based responses to events with multiple actions and countermeasures, including console alerts, email, SNMP trap, disabling the user account, executing a command, or logging the behavior for analysis later
- Expands detection policies via the console, allowing more detection rules to be handled with fewer policies and less-complicated editing
- Enforces flexible policy-based restrictions against known and unknown vulnerabilities even before patches exist or have been deployed

Purpose driven management integration

- Offers a single sign-on and management access to protection components across heterogeneous systems with Symantec Protection Center management console
- Provides a cross-platform server auditing capabilities that help enable compliance reporting with a graphical reporting engine
- Employs unique workflow automation to develop, track, manage, and control all aspects of a proactive security response process

Symantec Protection Suite Enterprise Edition for Servers includes:

Symantec™ Critical System Protection—offers protection for servers against malicious behaviors, blended threats, and known and unknown vulnerabilities by utilizing proactive, behavior-based Host Intrusion Protection through exploit prevention and system controls—along with Host Intrusion Detection based monitoring, notification, and auditing—with advanced event analysis and response capabilities to ensure host integrity and compliance across both physical and virtual server platforms.

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

It also includes: Symantec™ Protection Center which provides single sign-on and purpose-driven management integration across multiple Symantec endpoint, data loss prevention, messaging, and web protection technologies from a single centralized web console.

Symantec™ AntiVirus for Linux®—provides complete virus and spyware protection for Linux servers to enable enterprise-wide system uptime. The solution automatically detects and repairs the effects of viruses and other malicious intrusions to keep systems operational during potential security disruptions.

Symantec™ Workflow—connects people, processes, and information to optimize efficiency, enforce policies, reduce costs, and automate redundant tasks. Accelerate the delivery of IT and business processes without having to know complicated code or adding undue costs. Symantec Workflow helps to ensure nothing slips through the cracks by auditing and enforcing human and automated activities. Give process creation-power to the people who actually define processes, with a visual, self-documenting workflow designer. Provide higher-level process management and oversight while integrating Symantec and other environments to make business process seamless and cost-effective throughout the organization.

Other Symantec Protection Suite enterprise family options:

- **Symantec™ Protection Suite Enterprise Edition for Endpoints**
- **Symantec™ Protection Suite Enterprise Edition for Gateways**

Symantec Protection Suite Enterprise Edition family comparison matrix

How to choose the right security product				
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		•		

Common use cases

Hacker attacks

Outside parties can often attempt to compromise known vulnerabilities or create their own and leverage worms and buffer overflows to penetrate systems and hide malicious activities by changing registry log files. Symantec features that help limit outsider access include blocking inbound worm attacks, detecting buffer overflows, preventing targeted file downloads, and having the ability to mitigate registry file and program changes that are used to hide access attempts. Hacker attempts to infiltrate application or Web servers can be mitigated by preventing inappropriate inbound connections or being able to determine where multiple unsuccessful login attempts have been made, blocking the installation of unapproved executable files, and being able to selectively lock down certain files or directories. Leveraging features such as these can help automate the process of securing against inappropriate access, improve protection against data theft, and reduce the impact that attacks may have had on the performance of your network resources.

Insider abuse

An increasing number of attacks stem back to insider abuse, where deliberate changes in configuration settings provide back-door access. In this case, features that monitor changes made by administrators, prevent unauthorized network communications, can identify user rights changes to systems or even preventing unauthorized installation of applications. This can benefit your organization by reducing the risk of inappropriate access, minimizing the time and effort invested in tracking and researching breach activities and increasing your effectiveness in enforcing the policies you create.

Misconfigured systems

Misconfigured systems, whether intended or not, are often one of the main causes of system breaches. Features that audit for any new applications being introduced on critical systems or monitor key files and configurations for any changes—such as in Active Directory—can help mitigate potential compromises. Vulnerabilities are often exploited to facilitate system changes. Whether vulnerabilities are known or are new and undetermined, real-time policy monitoring combined with exploit-focused signature protection can block attempts to take advantage of those vulnerabilities. These features can minimize application failures due to compromise, reduce risk where patch requirements may not have been met, and eliminate a variety of other undesired configuration related downtime events.

Policy enforcement

Most organizations establish some level of policy for how servers will be protected, based on the type of server (i.e., application vs. database vs. file vs. print, etc.) and the criticality of service they provide. Protection policies covering areas such as USB device access, administrator access, application services, configurations, and file and log changes can be grouped with varying degrees of prevention and detection rules. This allows for more stringent enforcement of policies on more critical systems while providing a more liberal set of policies on less critical systems. Adaptive risk profile protection allows for setting policy-based protection levels based on server types to balance performance with risk-mitigation requirements. This feature provides a flexible server security solution that controls user and application behaviors, blocks inappropriate network traffic and events, and provides real-time and signature-based approaches to accommodate server workloads based on a variety of server profiles.

Data Sheet: Endpoint Security
Symantec™ Protection Suite Enterprise Edition for Servers

System requirements

Hardware/Software	Operating Systems/Browsers	Memory (min)	Hard Disk (min)
Critical System Protection Agent (Windows®)			
x86 32-bit, Intel® EM64T or AMD64 platforms	Microsoft® Windows® 2000 Professional / Server / Advanced Server / Windows XP / Windows Server 2003, 32-bit and 64-bit, including R2 and SP2 versions / Windows Server 2008, 32-bit and 64-bit, including R2 and SP2 versions, Microsoft® Windows® NT Server	256 MB RAM	100 MB
Critical System Protection Agent (Red Hat® Linux®)			
x86 32-bit, Intel EM64T or AMD64, Hagemem (32-bit) platforms	Red Hat Enterprise Linux ES (3.0, 4.0, and 5.0)	256 MB RAM	100 MB
Critical System Protection Agent (SUSE® Linux)			
x86 32-bit, Intel EM64T or AMD64 platforms	SUSE Enterprise Linux® (8, 9, and 10)	256 MB RAM	100 MB
Critical System Protection Agent (Sun™ Solaris™)			
Sun SPARC32/SPARC64; EM64T or AMD64 platform (V10 only)	Sun Solaris (8, 9, and 10) 32-bit and 64-bit	256 MB RAM	100 MB
Critical System Protection Agent (IBM® AIX®)			
PowerPC® platforms	IBM AIX 5L (5.1, 5.2, 5.3, 6.1) 32-bit and 64-bit	256 MB RAM	100 MB
Critical System Protection Agent (VMware)			
x86 32-bit	VMware ESX 3.5 Host	256 MB RAM	100 MB
Critical System Protection Agent (HP-UX®)—IDS only			
PA-RISC or Itanium® 2 platform (IA64)	HP-UX 11.23 and 11.31 (11i v2 and v3) 64-bit	256 MB RAM	100 MB
Critical System Protection Agent (HP-UX®)—IDS only			
PA-RISC platform	HP-UX 11.i (11.11) 64-bit	256 MB RAM	100 MB
Critical System Protection Agent (HP Tru64 UNIX®)—IDS only			
Alpha platform	HP Tru64 UNIX 5.1B-3	256 MB RAM	100 MB
Critical System Protection Management Server			
	Microsoft Windows 2000 Server / Windows Server 2003 / Windows Server 2008, 32-bit and 64-bit, including SP2 and R2	1 GB RAM	1 GB
	SQL Enterprise Server 2005 SP2, SQL Enterprise Server 2005 Express, SQL Enterprise Server 2008, 32-bit and 64-bit		
Critical System Protection Management Console			
	Windows 2000 Server / Windows Server 2003 / Windows XP, 32-bit and 64-bit	256 MB RAM	150 MB
	Java™ client or Web Console (Internet Explorer 8)		
Symantec™ Endpoint Protection Client for Servers (Windows®)			
Processor: Pentium® III 300 MHz (1 GHz for Vista) Note: No Itanium support	Windows XP, Windows Server 2003, Windows Vista®, Windows 7, Windows Server 2008, Windows® 2000 (x86)	256 MB RAM (1 GB recommended) for Windows XP (x86), 1 GB RAM (2–4 GB recommended) for most systems, 4 GB RAM for all editions of Windows Business Server 2008 (x64)	180 MB disk (plus an additional 440 MB during install), 700 MB disk (x64)
Endpoint Protection Manager			
Processor: Intel Pentium or compatible, 32-bit and 64-bit Note: No Itanium support	Windows 2000 (32-bit), Windows XP, 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)	1 GB RAM (2–4 GB recommended)	4 GB disk for the server; plus 4 GB for the database
Symantec AntiVirus™ for Linux® for Servers			
(not managed by Endpoint Protection Manager or Protection Center)	Red Hat® Enterprise Linux, SUSE Linux Enterprise (server/desktop), Novell® Open Enterprise Server (OES/OES2), VMware® ESX, Ubuntu®, Debian®, Fedora®		
Workflow Server			
	Windows Server 2000, 2003, 2008 Windows SQL Server 2000, 2005 Microsoft .NET 3.5		
Symantec Management Platform			
	Version 7.0 or later Internet Explorer 7 SQL Server 2005 Windows 2003 Server		

Data Sheet: Endpoint Security
Symantec™ Protection Suite Enterprise Edition for Servers

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

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Symantec helps organizations secure and manage their information-driven world with security management, endpoint security, messaging security and application security solutions.

21027147 04/10