



Symantec AntiVirus™ Enterprise Edition

Comprehensive virus protection for every network tier in a single, easy-to-deploy solution

Enterprise-wide virus protection is a core business requirement due to the increasing frequency of rapidly spreading, destructive viruses. Many organizations try to protect against viruses by installing numerous security products, but this approach is costly and difficult to manage.

Symantec AntiVirus™ Enterprise Edition provides virus protection, content filtering, and spam prevention for the groupware server and gateway, and virus protection, firewall, and intrusion detection technologies for the desktop in a single, easy-to-deploy solution. This comprehensive solution eliminates the complexity and cost of a multi-vendor security solution.

> At the email (SMTP) gateway

Symantec Mail Security™ for SMTP provides high-performance, integrated mail protection against virus threats, spam, and other unwanted content at the earliest point of network entry, the Internet email (SMTP) gateway.

- STOPS SPAM through highly integrated, multi-layered antispam techniques such as antispam heuristics, sender blacklists, whitelists, custom filtering rules, as well as support for multiple real-time blacklist services. These layers maximize spam detection while minimizing false positives.
- ZERO-HOUR RESPONSE TO EMERGING THREATS via attachment and subject line blocking enhances protection.
- CUSTOM DISCLAIMER SUPPORT provides the ability to insert custom text – such as legal disclaimer – into outbound messages.
- AUTO-LEARNED WHITELIST automatically captures known and trusted mail domains, simplifying the task of generating a comprehensive whitelist.

> At the Web (HTTP) gateway

Symantec™ Web Security protects HTTP/FTP traffic with scalable, high-performance, one-time scanning using URL content filtering and leading antivirus technologies.

- PREVENTS VIRUSES AND UNWANTED CONTENT from entering the network by integrating list-based and heuristic-based scanning for both Web filtering and virus protection.
- SIMPLIFIES ADMINISTRATION AND ENHANCES SCALABILITY through centralized multi-server policy management capabilities.

> For groupware servers

Symantec Mail Security™ for Microsoft Exchange combines spam prevention, content filtering, and award-winning antivirus technologies to provide an integrated mail security solution for Microsoft Exchange 2000 and 2003 servers.

- OPTIMIZED FOR EXCHANGE 2003 including support for the new Virus Scan API 2.5 and the new Spam Confidence Layer (SCL) method of handling spam messages.
- INTEGRATED HEURISTIC ANTISPAM ENGINE analyzes messages, determines the likelihood that a message is spam, and assigns a Spam Confidence Level (SCL).

KEY POINTS

- > Virus protection, content filtering, and spam prevention for the groupware server and gateway, and virus protection, firewall, and intrusion detection technologies for the desktop
- > **NEW!** Multi-layered spam prevention includes a heuristics antispam engine, blacklists, custom filtering rules, and advanced whitelisting to maximize detection and minimize false positives
- > **NEW!** Auto-learned whitelist automatically captures known and trusted mail domains to generate a comprehensive, effective whitelist
- > **NEW!** Mass-Mailer Cleanup automatically eliminates entire messages infected with mass-mailer worms—not just attachments
- > **NEW!** Custom Disclaimer allows administrators to insert custom text into outbound messages
- > **NEW!** Custom message body filtering rules provide greater flexibility for detecting spam and enforcing email usage policies
- > **NEW!** Expanded threat management detects unwanted applications such as spyware and adware, and identifies the source of blended threat attacks that spread via open file shares
- > **NEW!** Enhanced email protection prevents client systems from spreading worms via email, and also scans Internet email attachments delivered through POP3 mail clients
- > **NEW!** Enhanced remote user protection and management ensures systems are in full compliance with corporate antivirus policy prior to accessing corporate network resources

- SENDER AND RECIPIENT WHITELISTS support for both Exchange 2000 and 2003 allows trusted senders and specified recipient messages to bypass the RBL check and heuristics antispam engine, helping to minimize false positives.
- NEW SPAM STATISTICS provide an overview of trends and effectiveness of spam prevention.

Symantec Mail Security™ for Domino™ is an integrated security solution that stops malicious code, spam, and other unwanted email content from entering Domino databases.

- INTEGRATED HEURISTIC ANTISPAM ENGINE analyzes messages, determines the likelihood that a message is spam, and assigns a spam score and spam tag.
- MASS-MAILER CLEANUP automatically eliminates entire messages infected with mass-mailer worms—not just attachments.
- SUPPORT for Domino 6.5 Server and Client.
- DOMAIN WHITELIST support allows trusted sender email to bypass the heuristic antispam engine and minimize false positive detection.
- COMPREHENSIVE GROUPWARE PROTECTION enables administrators to update without stopping scan services or incurring server downtime.

> **For workstations and network servers**

Symantec AntiVirus™ Corporate Edition provides scalable, cross-platform virus protection for workstations and network servers to ensure enterprise-wide system uptime and user productivity.

- EXPANDED THREAT MANAGEMENT detects unwanted applications such as spyware and adware, and identifies the source of blended threat attacks that spread via open file shares.
- ENHANCED EMAIL PROTECTION prevents client systems from spreading worms via email, and also scans Internet email body text and attachments delivered through POP3 mail clients.
- ENHANCED REMOTE USER PROTECTION AND MANAGEMENT ensures systems are in full compliance with corporate policy prior to accessing corporate network resources .
- STORE AND FORWARD EVENT DATA Enables the client to store event data if it cannot connect to the management server. Event data is held until communication with the parent server is established, ensuring it is always available for alerting, logging, and reporting*.

* Available at additional cost.

> **Centralized management for workstations and network servers**

Symantec AntiVirus Enterprise Edition simplifies administration of workstation and network server protection.

- **CENTRALIZED MANAGEMENT** through the scalable Symantec System Center™ central management console enables IT managers to deploy and update antivirus solutions and definitions and create, enforce, and update policies to ensure network servers and workstations are properly configured across multiple platforms.
- **CENTRALIZED NETWORK AUDITING** identifies which nodes are unprotected and vulnerable to virus attack, as well as those protected by Symantec AntiVirus, McAfee® VirusScan,™ Trend Micro™ Office Scan,™ Computer Associates,™ or other third-party antivirus products.

> **Automatic virus protection cycle**

Symantec AntiVirus Enterprise Edition offers a range of technologies that enhance the solution's automatic response capabilities:

- **INCORPORATION OF LEADING TECHNOLOGIES** The Digital Immune System™ automates the submission of potential virus threats and automatically delivers cures to the problem machine or the entire enterprise. The backend infrastructure consists of hardware resources, architectural design, and the latest scanning engines and Web crawlers. NAVEX™ modular scan engine technology updates virus definitions and scan engines without having to redeploy the software or restart services. LiveUpdate™ technology provides automatic, scheduled delivery of virus definitions to ensure up-to-date protection. Bloodhound™ heuristic detection technology identifies new viruses by detecting virus-like behavior. Bloodhound can detect up to 90 percent of new macro viruses and up to 80 percent of new and unknown executable file viruses, including malicious mobile code.
- **SUSPICIOUS FILE SUBMISSION** Internet-based technologies—along with back-end Closed Loop Automation—allow administrators to submit suspicious files directly and automatically to Symantec via the Internet using HTTPS, without IT intervention. Virus cures can be tested first or automatically deployed to the infected endpoint or the entire enterprise.
- **CENTRAL QUARANTINE** allows administrators to redirect all irreparable, virus-infected files to a safe area on a centralized server for further inspection. This feature strips sensitive, proprietary data from macro virus-infected files, removes the viruses from the main computing environment, and prevents them from spreading throughout the organization

> **Backed by Symantec Security Response**

To provide up-to-the-minute, around-the-clock protection, Symantec AntiVirus Enterprise Edition is backed by Symantec Security Response. At Symantec Security Response, the industry's largest team of experts works to identify and neutralize viruses before they can enter the network and spread across the enterprise. Symantec Security Response provides swift, global response to virus outbreaks and proactive research on future threats.

For more information about Symantec AntiVirus Enterprise Edition, visit

visit <http://enterprisesecurity.symantec.com>

VIRUS PROTECTION, ANTISPAM, AND CONTENT FILTERING ARE KEY COMPONENTS OF SYMANTEC ENTERPRISE SECURITY. SYMANTEC ENTERPRISE SECURITY COMBINES WORLD-CLASS TECHNOLOGIES, COMPREHENSIVE SERVICES, AND GLOBAL EMERGENCY RESPONSE TEAMS TO HELP BUSINESSES RUN SECURELY AND WITH CONFIDENCE.

SYSTEM REQUIREMENTS

SYMANTEC ANTIVIRUS™ ENTERPRISE EDITION 9.0

SYMANTEC ANTIVIRUS™ CORPORATE EDITION 9.0

SYMANTEC ANTIVIRUS FOR 32-BIT WINDOWS CLIENTS

- Windows XP Professional/2000 Professional/Server/Advanced Server/Server 2003 Web/Standard/Enterprise/Datacenter Edition/NT 4.0 Workstation/Server/Terminal Server Edition SP6a
- 32 MB RAM
- 55 MB available disk space
- Microsoft Internet Explorer v4.01 or later

SYMANTEC ANTIVIRUS FOR 64-BIT WINDOWS CLIENTS

- Windows XP 64-Bit Edition Version 2003/Server 2003 Enterprise/Datacenter 64-Bit Editions
- Intel® Itanium 2 processor
- 64 MB RAM
- 70 MB available disk space

SYMANTEC ANTIVIRUS MANAGEMENT SERVER – 32-BIT WINDOWS

- Windows 98/98 SE/Me Windows XP Professional/2000 Professional/Server/Advanced Server/Server 2003 Web/Standard/Enterprise/Datacenter Edition/NT 4.0 Workstation/Server/Terminal/Terminal Server Edition SP6a
- 111 MB disk space
- 15 MB disk space for AMS2 server files (If you choose to install AMS2 Server)
- 64 MB RAM
- Microsoft Internet Explorer v4.01 or later

Notes: Symantec AntiVirus Corporate Edition does not support the scanning of Macintosh volumes on Windows servers for Macintosh viruses.

SYMANTEC ANTIVIRUS MANAGEMENT SERVER - NETWORK

- NetWare 5.1 SP3 or higher, 6.0 SP1 or higher
- 116 MB available disk space
- 20 MB disk space for AMS2 server files (If you choose to install AMS2 Server)
- 15 MB RAM (above standard NetWare RAM requirements) for Symantec AntiVirus NLMs

SYMANTEC SYSTEM CENTER

- Windows NT 4.0 Workstation and Server with Service Pack 6a; Windows 2000 Professional, Server, Advanced Server; Windows XP Professional; Windows Server 2003 Web, Standard, Enterprise, and Datacenter Editions.
- Microsoft Internet Explorer v5.5 SP2
- Microsoft Management Console version 1.2. If MMC is not already installed, you will need 3 MB free disk space (10 MB during installation)
- 36 MB disk space
- 32 MB RAM

SYMANTEC SYSTEM CENTER SNAP-INS

Alert Management System Console

- 24 MB available disk space in addition to the Symantec System Center requirements

Symantec AntiVirus Snap-In

- 6 MB available disk space in addition to the Symantec System Center requirements

Symantec Client Firewall Snap-In

- 1 MB available disk space in addition to the Symantec System Center requirements

AV Server Rollout Tool

- 130 MB available disk space in addition to the Symantec System Center requirements

NT Client Install Tool

- 2 MB available disk space in addition to the Symantec System Center requirements

QUARANTINE CONSOLE

- Windows NT 4.0 Workstation and Server with SP6a; Windows 2000 Professional, Server, Advanced Server; Windows XP Professional.
- Microsoft Internet Explorer v5.5 SP2 or later
- Microsoft Management Console version 1.2. If MMC is not already installed, you will need 3 MB free disk space (10 MB during installation)
- 35 MB available disk space
- 32 MB RAM

QUARANTINE SERVER

- Windows NT 4.0 Workstation and Server with SP6a; Windows 2000 Professional, Server, Advanced Server; Windows XP Professional; Windows Server 2003 Web, Standard, Enterprise, and Datacenter Editions.
- Microsoft Internet Explorer v5.5 SP2 or later
- 40 MB available disk space
- Minimum swap file size of 250 MB
- 500 MB to 4 GB disk space recommended for quarantined items
- 64 MB RAM

Note: If you are running Windows ME or Windows XP, system disk space usage will be increased if you have the System Restore functionality enabled. Please consult your Microsoft Operating System documentation on how System Restore works.

SYMANTEC MAIL SECURITY 4.5 FOR MICROSOFT EXCHANGE

SERVER SYSTEM REQUIREMENTS

- Intel Server class 32-bit processor
- Windows 2000 or 2003 Server/Advanced Server/Datacenter with SP3 and SP4
- Microsoft Exchange 2000/2003 with SP3 or later
- 512 MB RAM
- 190 MB available disk space to install (260 MB for remote installation)
- Microsoft Internet Explorer v6.0

MULTI-SERVER CONSOLE REQUIREMENTS

- Intel Server class 32-bit processor
- Windows 2000 (SP4), Windows XP, Windows Server 2003
- 140 MB available disk space for Mail Security Console installation
- Microsoft Management Console v1.2
- Microsoft Internet Explorer v6.0

CONSOLE

- Windows 2000 Professional with SP3 and SP4 or Windows XP
- Microsoft Internet Explorer v5.01 or later
- 61 MB available disk space to install

SYMANTEC MAIL SECURITY 4.0 FOR DOMINO

LOTUS DOMINO SERVER

- Lotus Domino Server versions: 6.5, 6.0.3, 6.0.2 CF2, 6.0.2 CF1, 5.0.11, 5.0.12, and 5.0.13
- Running the following operating systems:
 - Windows 2000 Server/Advanced Server SP4;
 - Windows Server 2003/Enterprise Edition (6.0.3 and 6.5 only based on IBM support of Windows 2003)

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.

LOTUS NOTES CLIENT

- Lotus Notes versions: 6.5, 6.0.3, 6.0.2 CF2, 6.0.2 CF1, 5.0.11, 5.0.12, and 5.0.13
- 128 MB RAM minimum (256 MB RAM or more recommended)
- 300 MB available disk space

SYMANTEC MAIL SECURITY FOR SMTP 4.0

SOLARIS™

- SPARC-based server
- Solaris 8 or 9
- 256 MB RAM minimum (512 MB or more recommended for optimal performance)
- 50 MB to install
- 500 MB minimum after install for mail processing
- Microsoft Internet Explorer v6.0 or later –OR– Netscape Navigator v7.02

WINDOWS™ 2000 SERVER

- Intel® Pentium® III or IV or compatible
- Windows 2000 Server/2003 Server with SP4
- 256 MB RAM minimum
- 50 MB to install
- 500 MB minimum after install for mail processing
- Microsoft Internet Explorer v6.0 or later –OR– Netscape Navigator v7.02

SYMANTEC WEB SECURITY 3.0

SYMANTEC WEB SECURITY FOR WINDOWS NT™

- Intel Pentium II or compatible processor, or better
- Microsoft Windows NT Server 4 with SP6a
- At least 256 MB RAM
- At least 500 MB available disk space for program files, online documentation, configuration files, etc.
- Minimum 400 MB - 1 GB additional disk space required (1 GB or more preferred)
- Internet access, World Wide Web browser
- Correctly configured DNS server which contains both A and PTR records

SYMANTEC WEB SECURITY FOR WINDOWS 2000

- Intel Pentium II or compatible processor, or better
- Microsoft Windows 2000 Server with SP2
- At least 256 MB RAM
- At least 500 MB available disk space for program files, online documentation, configuration files, etc.
- Minimum 400 MB - 1 GB additional disk space required (1 GB or more preferred)
- Internet access, World Wide Web browser
- Correctly configured DNS server which contains both A and PTR records (SWS functions on Windows 2000 Server with the same level of compatibility as Windows NT Server 4.0. However, it does not adhere to Windows 2000 Server Logo Requirements.)

SYMANTEC WEB SECURITY FOR SOLARIS™

- Sun SPARC based system
- Solaris 7 and 8 operating system
- At least 256 MB RAM
- At least 500 MB available disk space for program files, online documentation, configuration files, etc.
- Minimum 400 MB - 1 GB additional disk space required (1 GB or more preferred)
- Internet access, World Wide Web browser
- Correctly configured DNS server which contains both A and PTR records

BROWSER REQUIREMENTS

- Any CERN HTTP Proxy protocol compliant browser, such as:
 - Microsoft Internet Explorer v5.0 or later - OR - Netscape Navigator v4.7 or later

WORLD HEADQUARTERS

**20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408 517 8000
800 721 3934**

www.symantec.com

**For Product Information
In the U.S., call toll-free
800 745 6054**

**Symantec has worldwide
operations in 38 countries.
For specific country
offices and contact numbers
please visit our Web site.**