



Symantec AntiVirus™ Corporate Edition

Comprehensive virus protection for workstations and network servers enterprise-wide

Enterprise-wide virus protection is now a core business requirement due to the increasing frequency of rapidly spreading, destructive viruses. However, virus protection at the firewall and email gateway alone does not provide sufficient protection. Comprehensive virus protection at the workstation and network server tiers is needed to ensure enterprise-wide system uptime and user productivity.

> Comprehensive, award-winning virus protection

Symantec AntiVirus™ Corporate Edition provides scalable, cross-platform virus protection for workstations and network servers throughout the enterprise. It also provides additional protection for storage environments that reside outside the workstation and network server tiers. Award-winning Symantec antivirus technologies are employed to detect and protect against viruses, worms, and Trojan horses in all major file types, including mobile code and compressed file formats. The solution provides advanced scanning and repair services that place minimal resource demands on the existing network infrastructure. A reduced virus definition file size and multi-threaded server rollout speed update distribution, and growing traffic volumes are easily accommodated with automatic load balancing across multiple servers, to ensure highly scalable virus protection.

> Centralized policy management

Centralized management capabilities allow IT administrators to manage individual users and functional groups of users and create, deploy, and lock down policies and settings to keep systems up-to-date and properly configured at all times. All workstation and network server settings can be locked down so users cannot change them, or administrators can configure and monitor workstations and network servers via the management console. If a virus is detected, a repair is automatically launched and an alert is broadcast to the IT administrator via the Symantec System Center console. The central management console is capable of managing hundreds of thousands of nodes.

> New features provide enhanced protection and flexibility

A network audit feature enables administrators to identify which nodes are protected by Symantec AntiVirus or Computer Associates, McAfee®, Panda, Sophos, or Trend Micro antivirus products. The network audit feature also identifies unprotected nodes that are vulnerable to virus attack. This allows administrators to proactively secure nodes before an event can occur, ensuring system uptime and user productivity.

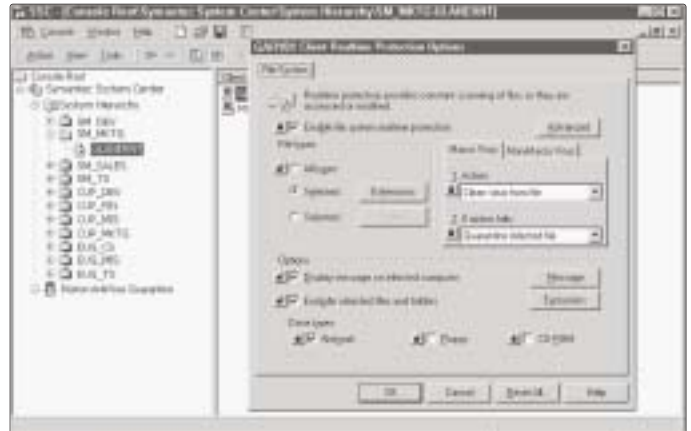
In addition, Symantec AntiVirus Corporate Edition is compatible with Windows® Server 2003, Netware® Secure Console, and 64-bit Intel® Itanium™ 2 hardware, enabling uninterrupted protection as businesses migrate to the latest technology.

KEY POINTS

- > **NEW!** Centralized network auditing capabilities help identify unprotected nodes, as well as those protected by Symantec AntiVirus™ Corporate Edition and select third-party antivirus products
- > **NEW!** Extensive platform support, now including Windows® Server 2003 and Netware® Secure Console
- > **NEW!** Supports 64-bit Intel® Itanium™ 2 hardware
- > Provides advanced, enterprise-wide virus protection and monitoring from a single management console
- > Enables enforceable antivirus policy management across multiple platforms
- > Ensures system uptime and user productivity by enabling administrators to proactively secure unprotected nodes before an event can occur
- > Assures rapid deployment and automatic virus protection through a reduced virus definition file size and multi-threaded server rollout
- > Eases administration by offering logical group management for workstations and servers
- > Enables up-to-the-minute protection for mobile workstations via “roaming” virus definition update capability
- > Backed by Symantec™ Security Response, the world’s leading Internet security research and support organization

> Easy installation and deployment

The Symantec System Center™ management console enables the centralized deployment of virus definitions and product updates to multi-platform workstations and network servers, reducing the cost of deploying updates across the enterprise. And, Symantec Packager™ technology enables administrators to create a deployment package that defines which components to install on each system. Centralized distribution reduces deployment headaches, such as “sneaker nets”, failed jobs, and bad installations. It also simplifies enterprise planning and the creation of server hierarchies and groups. The installation process intelligently anticipates problems that may be encountered, greatly reducing the likelihood of failed installations that could lead to network problems.



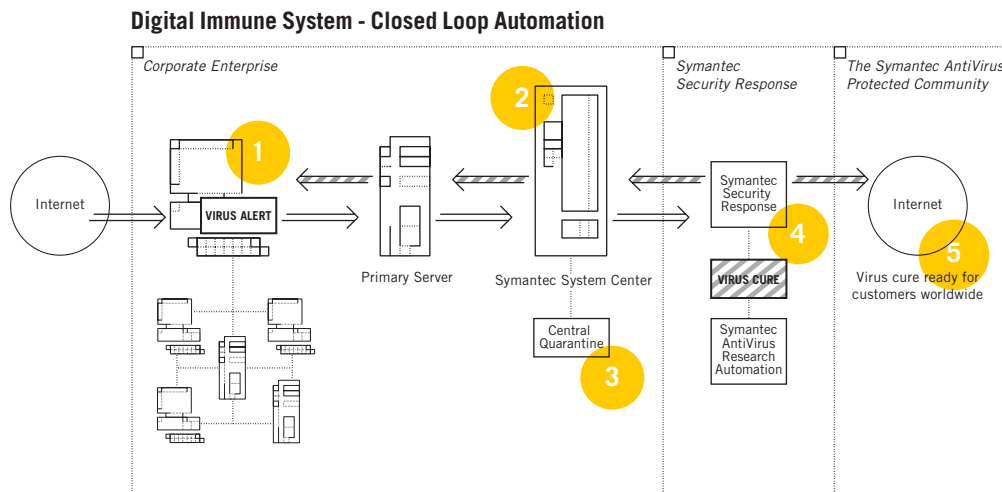
The Symantec System Center provides automatic node discovery, installation, real-time configuration and lock down, on-demand management tasks, event logging, alerting, and automated responses from a central console.

> Automatic virus protection

The Digital Immune System automates the submission of potential threats and automatically delivers cures to the problem machine or the entire enterprise. In conjunction with a sophisticated, back-end infrastructure consisting of hardware resources, architectural design, and the latest scanning engines and Web crawlers, the Digital Immune System ensures high levels of service availability. Combined with around-the-clock vigilance from Symantec Security Response—the world’s largest antivirus research and response organization—Symantec AntiVirus Corporate Edition greatly reduces the turnaround time on new virus submissions and cures. The following technologies enhance the solution’s automatic response capabilities:

- NAVEX™ modular scan engine technology updates virus definitions and scan engines without the added requirement of redeploying the software and rebooting the system, ensuring maximum up-time and lowering total cost of ownership.
- LIVEUPDATE™ technology provides automatic, scheduled delivery of virus definitions to ensure up-to-date protection.
- BLOODHOUND™ heuristic detection technology identifies unknown 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.
- Internet-based technologies along with back-end Closed Loop Automation allow administrators to easily submit suspicious files directly and automatically to Symantec via the Internet using HTTPS—without IT intervention. The cure can be tested first or automatically deployed to the infected endpoint or the entire enterprise. Closed Loop Automation significantly cuts response time for fast-moving threats, helping to reduce the likelihood of network downtime during attacks.
- 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.

- Utilizing breakthrough automated macro virus analysis and repair technology, Symantec AntiVirus Research Automation (SARA) analyzes samples submitted to Symantec Security Response and emails a virus definition to cure the new virus.
- Virus Definition Transport Method (VDTM) allows administrators to simply push new virus definitions to managed network servers and workstations. Incremental virus definitions further accelerate the update process.



Within the Corporate Enterprise

1 DETECTION AND QUARANTINE - 2:00 am
 Symantec AntiVirus heuristic Bloodhound technology detects suspicious virus activity.
 The suspect files are safely quarantined on the workstation and a copy is sent to the Central Quarantine Server via the Symantec System Center console.
 - 2:05 am

2 VIRUS SUBMISSION - 2:10 am
 The quarantined file is ready for submission. IT administrators have the option of stripping content before automatically submitting the infected file to Symantec via the Internet (HTTPS).

REAL-TIME SUBMISSION TRACKING

3 Utilizing the Central Quarantine Console the administrator can track the status of the submission in real-time.

Symantec Security Response

4 VIRUS CURE AND DEPLOYMENT - 3:00 am
 The virus is analyzed by SARA and a remedy is created and tested. The new virus definition is automatically and securely delivered back to the customer's Central Quarantine Server via the Internet (HTTPS).
 - 3:10 am

The IT administrator can test the new remedy first or deploy it directly to the infected system(s) or the entire enterprise.
 - 3:15 am
5 The virus cure is now available, via Symantec Security Response to all Symantec AntiVirus customers worldwide.
 - 3:20 am

For more information about Symantec AntiVirus Corporate Edition, visit <http://www.enterprisesecurity.symantec.com>

VIRUS PROTECTION IS A KEY COMPONENT 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™ CORPORATE EDITION 8.1

Microsoft's recommended system requirements for memory and processor are implied.

SYMANTEC ANTIVIRUS FOR 32-BIT WINDOWS CLIENTS:

- Windows 98, Windows 98 SE, Windows -ME; Windows NT 4.0 Workstation, Server, and Terminal Server Edition with Service Pack 6a; Windows 2000 Professional, Server, Advanced Server; Windows XP Home, Professional; Windows Server 2003 Web, Standard, Enterprise, and Datacenter Editions.
- 46 MB disk space

SYMANTEC ANTIVIRUS FOR 64-BIT WINDOWS CLIENTS:

- Windows XP 64-bit Edition Version 2003; Windows Server 2003 Enterprise and Datacenter 64-Bit Editions
- 80 MB disk space
- Intel Itanium 2 processor

SYMANTEC ANTIVIRUS MANAGEMENT SERVER FOR 32-BIT WINDOWS

- Windows NT 4.0 Workstation, Server, and Terminal Server Edition with Service Pack 6a; Windows 2000 Professional, Server, Advanced Server; Windows XP Professional; Windows Server 2003 Web, Standard, Enterprise, and Datacenter Editions
- 111 MB disk space (65 MB disk space for Symantec AntiVirus Corporate Edition server files and 46 MB disk space for the Symantec AntiVirus Corporate Edition client disk image)
- 15 MB disk space for AMS2 server files (if you choose to install AMS2 Server)

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

SYMANTEC ANTIVIRUS MANAGEMENT SERVER - NETWARE:

- NetWare 5.x, 6 SP1
- 15 MB RAM (above standard NetWare RAM requirements) for Symantec AntiVirus NLMs
- 116 MB disk space (70 MB disk space for Symantec AntiVirus Corporate Edition server files and 46 MB disk space for the Symantec AntiVirus Corporate Edition client disk image)
- 20 MB disk space for AMS2 server files (If you choose to install AMS2 Server)

SYMANTEC SYSTEM CENTER:

- Windows NT 4.0 Workstation and Server with Service Pack 6a; Windows 2000 Professional, Server, Advanced Server; Windows XP Professional
- Microsoft Internet Explorer 5.5 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)
- 10 MB disk space

SYMANTEC SYSTEM CENTER SNAP-INS:

Alert Management System Console

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

Symantec AntiVirus Snap-in

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

AV Server Rollout Tool

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

NT Client Install Tool

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

SYMANTEC PACKAGER

Symantec Packager runs only on Windows NT-based operating systems and requires the following system requirements:

- Supported operating systems:
 - Windows NT Workstation 4.0/Server 4.0 with Service Pack 6a
 - Windows 2000 Professional/Server with Service Pack 2
 - Windows XP Professional
- Microsoft Internet Explorer 5.5 or later
- Windows Installer 2.0
- If Windows Installer 2.0 is not present, Symantec Packager installs it during installation
- Pentium II 300 processor (or faster)
- 64 MB RAM (128 MB recommended)
- 60 MB disk space
- CD-ROM or DVD-ROM drive

SYMANTEC PACKAGER INSTALLATION PACKAGES

Although Symantec Packager runs only on Windows NT-based operating systems, packages that you create using Symantec Packager can be installed on the following operating systems:

- Windows NT 4.0 with Service Pack 6a
- Windows 98
- Windows Millennium Edition (ME)
- Windows 2000
- Windows XP Home Edition/Professional Edition

QUARANTINE CONSOLE

- Windows NT 4.0 Workstation and Server with Service Pack 6a; Windows 2000 Professional, Server, Advanced Server; Windows XP Professional
- Microsoft Internet Explorer 5.5 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)
- 35 MB disk space

QUARANTINE SERVER

- 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 5.5 SP2
- 40 MB disk space
- 250 MB minimum swap file size
- 500 MB to 4 GB disk space recommended for quarantined items

NORTON ANTIVIRUS CORPORATE EDITION 7.6 FOR WINDOWS 95 CLIENT:

- Windows 95
- 32 MB RAM minimum
- Intel 486 processor (Pentium or faster recommended)
- 43 MB disk space (80 MB during installation)
- WINSOCK 2.0 or later

NORTON ANTIVIRUS CORPORATE EDITION 7.6 FOR NETWARE SERVERS:

- NetWare 4.11 with Support Pack 9; NetWare 4.2 with Support Pack 9; NetWare 5.x with or without Support Pack 2
- 3 MB RAM (above standard NetWare requirements) for Norton AntiVirus NLMs
- Required with NetWare 4.1x: LIBUPF (located in Support Pack 7 or later)
- 70 MB disk space for Norton AntiVirus server files and 46 MB free disk space for the Norton AntiVirus client disk image
- 10 MB disk space for AMS2 files (20 MB during installation)

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408.517.8000
800.721.3934

For Product Information
In the U.S., call toll-free
800.745.6054.

www.symantec.com

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