



Symantec™ Client Security

Threat protection through integrated antivirus, firewall, and intrusion detection for remote, mobile, and networked client systems

> The need for integrated client security

Mobile and remote users increasingly need access to the enterprise network, requiring organizations to protect critical business assets that reside on networked and remote client systems. Many organizations rely on point products dispersed throughout the enterprise, which provide inadequate protection and are costly to implement and manage. For instance, blended threats (such as Nimda, Code Red, and Blaster) are difficult to prevent because they are designed to elude the security products commonly deployed across the perimeter of today's enterprises. In addition, security administrators are challenged to identify and respond to legitimate threats in real time because these products lack centralized management capabilities.

Symantec Client Security provides integrated antivirus, firewall, and intrusion detection capabilities managed through a central console to proactively protect against today's evolving blended threats.

> Integrated security management

Integrated security management via the Symantec™ System Center offers a comprehensive view of virus protection, firewall, and intrusion detection. Management capabilities include:

- **CENTRALIZED MANAGEMENT FROM A SINGLE CONSOLE:** Using Symantec System Center, administrators can configure, install, manage, and update client virus protection, firewall, and intrusion detection functions—and configure, implement and enforce corporate network policies—from one management console. Administrators can also install Symantec Client Security and easily move clients between management servers from the central management console. Centralized logging and alerting for each of the integrated technologies help transform security data into actionable information.
- **CLIENT SECURITY POLICY CREATION AND DEPLOYMENT:** Merge policy file feature merges firewall rules, helping administrators avoid manual integration or creation of new rules. A policy test button enables client firewall policies to function as created when deployed. Three pre-configured firewall policies are included: standard, remote, and hardened. Administrators can configure and lock down antivirus and client firewall policies to control such activities as when the real-time scanner is turned on; what occurs when a virus, worm, or Trojan is detected; and what end-user interaction with the product is permissible, to name a few.
- **SYMANTEC VPN SENTRY:** Allows the administrator to ensure that mobile and remote systems connecting to corporate resources via VPN and login script are compliant with security policies. Specifically, it checks to ensure that antivirus software is installed and real-time protection is turned on; virus definitions are up-to-date; and the client firewall is installed, enabled, and follows appropriate policy. The administrator can also create policies through the VPN server that allow non-compliant systems to gain access to network resources that help address compliancy issues.

KEY POINTS

- > Protects networked PCs, critical systems, and remote and mobile users from unwanted network intrusions, as well as from viruses, Trojans, and worms
- > **NEW!** Symantec VPN Sentry assures remote and mobile users are in full compliance with corporate policies
- > **NEW!** Location awareness ensures corporate security policy is adhered to, regardless of location
- > **NEW!** Client Profiling minimizes the number of alerts that the end-user sees
- > **NEW!** Threat Tracer identifies the source of blended threat attacks that spread via open file shares such as Nimda
- > **NEW!** Outbound email worm heuristics prevent client systems from spreading worms via email
- > **NEW!** Expanded Threat Detection recognizes unwanted applications such as spyware and adware
- > **NEW!** Internet Email Attachment Scanning of incoming emails delivered through POP3 mail clients such as Microsoft® Outlook®, Eudora®, and Netscape Mail
- > **NEW!** In-Memory Scanning detects threats and terminates suspect processes in memory before they can cause damage

- **LOGICAL GROUP MANAGEMENT:** Administrators can create and manage logical groupings of clients and servers within server groups, or multiple logical groups from a single parent server. This is especially useful for organizations that need to handle similar functional entities (such as departments or business units) in the same way, reducing the infrastructure cost.
- **INSTALLATION AND MIGRATION:** Symantec Client Security now includes a new Microsoft Installer that provides the ability to pre-configure antivirus, firewall, and intrusion detection component installation packages. The installation footprint size has been reduced from 50 megabytes to under 25 megabytes. Three pre-configured deployment options are available: fully-managed, lightly-managed, and thin-client. In addition, a security software uninstaller minimizes the cost of switching from a third-party antivirus product to Symantec Client Security.
- **CENTRALIZED NETWORK AUDITING:** Administrators can identify 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.
- **SCALABLE PROTECTION:** Administrators can manage hundreds of thousands of clients through the Symantec System Center.
- **REDUCED COST OF OWNERSHIP:** By providing improved security administration, including centralized event management and response capabilities, Symantec Client Security eases the administrative burden and helps lower the cost of managing security at the network, mobile, and remote client level.

> **Integrated response**

Symantec Client Security provides a common deployment and updating function for antivirus, firewall, and intrusion detection, helping to reduce the overhead, risk, and management of updates. In addition, integrated response enables enterprises to respond faster to security breaches and virus outbreaks, improving the overall security posture of the network. Virus definitions, firewall rules, and intrusion signatures are tested and verified by Symantec across the integrated technologies prior to distribution via a single response mechanism. The following features help administrators respond rapidly to maximize containment and recovery:

- **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.
- **STORE AND FORWARD ALERTS:** Store and Forward Alerts enable infected mobile user to store event data and forward it to a management server after reconnecting to the corporate network, ensuring that critical event data is always available to help transform security data into actionable information.
- **FAST RESPONSE TO THREATS:** Symantec Client Security allows administrators to force a LiveUpdate session to occur immediately on single or multiple clients, minimizing response time to fast-spreading threats. For even faster, automated response, push technology is incorporated into a management server associated with the Symantec System Center. The management server can be scheduled to automatically retrieve virus content updates from Symantec or from a central LiveUpdate Server. It then pushes these updates to secondary servers that in turn push the updates to client systems.

> **Protection for critical systems, remote and mobile users**

Symantec Client Security provides end-point protection that prevents intrusions from entering the network through inadequately secured remote and mobile users, as well as critical systems. It protects laptops outside the firewall from being used by hackers to gain unauthorized enterprise network access through dial-up, DSL/Cable, and VPN connections. This also provides better protection against blended threats for desktop clients residing inside the firewall perimeter.

- **EXPANDED THREAT DETECTION:** Scans for programs that can compromise the security of the system (e.g., viruses, worms, and Trojans), privacy of client data (e.g., spyware, trackware, and adware), or that can be used with malicious intent (e.g., dialers, joke programs, remote access and hack tools).
- **LOCATION AWARENESS:** Enables the client firewall to adjust policies based on the machine's location, to ensure policy enforcement regardless of where or how the machine is connected to the corporate network or Internet.
- **CLIENT PROFILING:** Minimizes the number of pop-ups that the end-user sees as the firewall application discovers which applications are accessing the Internet or network through the firewall.
- **INTERNET EMAIL ATTACHMENT SCANNING:** Virus scanning of incoming email body text and attachments that are delivered through POP3 mail clients like Microsoft® Outlook®, Microsoft Outlook Express, Eudora® and Netscape Mail provides protection against fast-moving, email-based threats.
- **THREAT TRACER:** Identifies the source of blended threat attacks, such as Code Red and Nimda, that spread via open file shares, which can be used to prevent further attacks of the same type.
- **BEHAVIOR BLOCKING:** New behavior blocking features include outbound email worm heuristics and ad blocking. Outbound email worm heuristics prevent client systems from spreading worms, such as SOBIG.F, via email. Administrators can also set the firewall to block unwanted ad banners, ensuring maximum employee productivity.
- **ENHANCED FIREWALL PROTECTION:** Advanced functionality ensures the security of information assets stored on remote user machines or networked clients. An integrated secure port blocks access to known Trojan ports. The firewall provides a higher level of application security by inspecting both the executed application as well as the application's sub-components (DLLs).
- **INTEGRATED PROTECTION:** The client firewall technology scans all traffic that travels in or out of remote user machines and networked clients, while the real-time antivirus scanning technology scans files that are created, moved, copied, renamed, or executed. The firewall, antivirus, and intrusion detection technologies then intelligently interact to investigate potential threats or to increase security measures and block suspected files from infiltrating the network. When no data is written to disk, on-demand in-memory scanning identifies and removes in-memory threats before they have the chance to propagate or cause damage. The antivirus technology can terminate the suspicious processes and handle the disposition of threat-infected files.

For more information visit: <http://enterprisesecurity.symantec.com>

VIRUS PROTECTION, ANTISPAM, & 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 CLIENT SECURITY 2.0

(SYMANTEC CORPORATE EDITION 9.0/
SYMANTEC CLIENT FIREWALL 7.0
MINIMUM SYSTEM REQUIREMENTS)

MICROSOFT'S RECOMMENDED
SYSTEM REQUIREMENTS FOR
MEMORY AND PROCESSOR ARE IMPLIED.

SYMANTEC CLIENT SECURITY FOR 32-BIT WINDOWS CLIENTS:

- Windows 98, Windows 98 SE, Windows Millennium Edition; Windows 2000 Professional; Windows XP Home, Professional.
- 80 MB of disk space
- 128 MB of RAM
- Internet Explorer 5.01 SP2 or later
- Intel Pentium processor at 150 MHz (Pentium II or higher recommended)

SYMANTEC ANTIVIRUS FOR 32-BIT WINDOWS CLIENTS:

- Windows 98, Windows 98 SE, Windows Millennium Edition; 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.
- 55 MB of disk space
- 32 MB of RAM
- Internet Explorer 4.01 or later
- Intel Pentium processor at 150 MHz (Pentium II or higher recommended)

SYMANTEC ANTIVIRUS FOR 64-BIT WINDOWS CLIENTS:

- Windows XP 64-Bit Edition Version 2003, Windows Server 2003 Enterprise and Datacenter 64-Bit Editions
- 70 MB of disk space
- Intel Itanium 2 processor
- 64 MB of RAM

SYMANTEC CLIENT SECURITY MANAGEMENT SERVER - 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 of disk space (65 MB of disk space for Symantec AntiVirus Corporate Edition server files and 46 MB of disk space for the client disk image)
- Optional installation of AMS2 Server (requires 15 MB of disk space)
- 64 MB of RAM
- Internet Explorer 4.01 or later
- Intel Pentium processor at 150 MHz (Pentium II or higher recommended)

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

SYMANTEC CLIENT SECURITY MANAGEMENT SERVER - NETWARE:

- NetWare 5.1 SP3 or higher, 6.0 SP1 or higher
- 15 MB of RAM (above standard NetWare RAM requirements) for Symantec AntiVirus NLMs
- 116 MB of disk space (70 MB of disk space for Symantec AV Corporate Edition server files and 46 MB of disk space for the Symantec AV Corporate Edition client disk image)
- 15 MB of RAM (above standard NetWare RAM requirements) for Symantec AntiVirus NLMs.
- Intel Pentium processor at 150 MHz (Pentium II or higher recommended)
- Internet Explorer 5.5 with SP2
- Optional installation of AMS2 Server requires 20 MB of disk space

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.
- Internet Explorer 5.5 SP2
- Microsoft Management Console 1.2. If MMC is not already installed, you will need 3 MB of free disk space (10 MB during installation)
- 36 MB of disk space
- 32 MB of RAM
- Intel Pentium processor at 150 MHz (Pentium II or higher recommended)

SYMANTEC SYSTEM CENTER SNAP-INS:

- Alert Management System Console
- 24 MB of disk space in addition to the Symantec System Center requirements
- Symantec AntiVirus Snap-in
- 6 MB of disk space in addition to the Symantec System Center requirements
- Symantec Client Firewall Snap-in
- 1 MB of disk space in addition to the Symantec System Center requirements
- AntiVirus Server Rollout Tool
- 130 MB of disk space in addition to the Symantec System Center requirements
- NT Client Install Tool
- 2 MB of disk space in addition to the Symantec System Center requirements

QUARANTINE CONSOLE:

- Windows NT 4.0 Workstation and Server with Service Pack 6a; Windows 2000 Professional, Server, Advanced Server; Windows XP Professional
- Internet Explorer 5.5 SP2
- Microsoft Management Console 1.2. If MMC is not already installed, you will need 3 MB of free disk space (10 MB during installation)
- 35 MB of disk space
- 32 MB of RAM
- Intel Pentium processor at 150 MHz (Pentium II or higher recommended)

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.
- Internet Explorer 5.5 SP2
- 40 MB of disk space
- Minimum swap file size of 250 MB
- 500 MB to 4 GB of disk space recommended for quarantined items
- 64 MB of RAM
- Intel Pentium processor at 150 MHz (Pentium II or higher recommended)

SYMANTEC CLIENT FIREWALL ADMINISTRATOR

- 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
- 80 MB of disk space
- 64 MB of 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.

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
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.