



Symantec™ Client Security

Integrated antivirus, firewall, and intrusion detection for remote users and networked clients

> The need for integrated client security

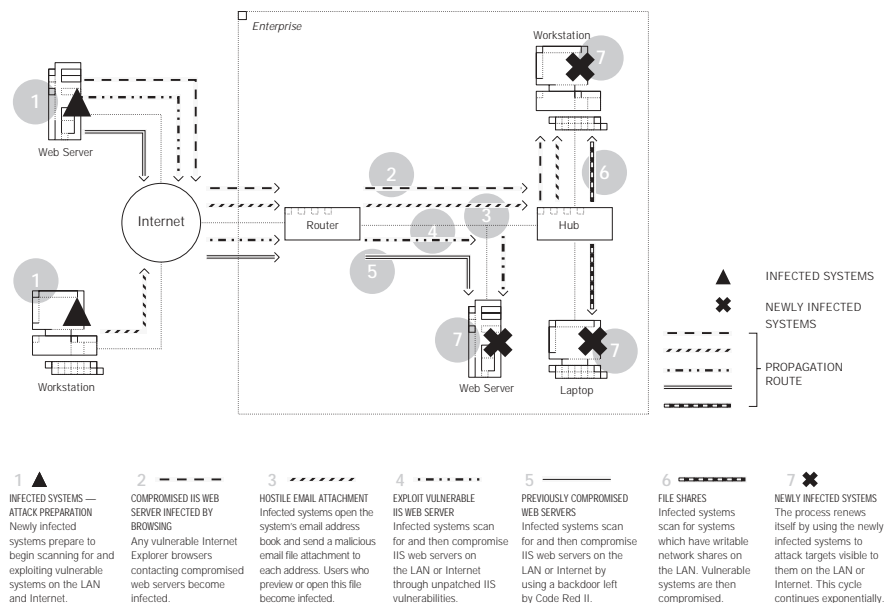
Today's open business environment involves providing easy access to the corporate network for a variety of constituents, including contractors, partners, and customers. As more and more people traditionally considered "outsiders" are granted legitimate network access, a perimeter firewall does not provide an adequate level of protection against intrusions and threats. In addition, blended threats (such as Nimda, CodeRed, and Slammer) infiltrate networks by exploiting the vulnerabilities of isolated security products. Blended threats are also known to enter a network via the standard ports in use on a perimeter firewall. Thus, even with a perimeter firewall in place, organizations are not safe from these attacks.

A client firewall provides an additional layer of security for the applications and data that reside on clients which travel outside the perimeter firewall and connect to the network, as well as desktop clients residing inside the security perimeter. Integrating this client firewall with antivirus protection and intrusion detection, in turn, enables organizations to proactively protect against complex blended threats.

To eliminate security gaps for remote users and networked clients, Symantec has integrated client firewall and intrusion detection with its antivirus technology and made them interoperable as part of Symantec Client Security. This integration, plus the ability to interact, enables these security technologies to efficiently protect against a variety of threats.

KEY POINTS

- > Provides enhanced protection for remote users and networked clients against blended threats through integrated management and response
- > Ensures security policy enforcement by integrating and centralizing installation, deployment, management, and updating
- > Optimizes resources, helping to reduce the administrative and support costs of laptop and desktop client protection
- > Integrated client firewall technology provides a dedicated layer of protection to ensure the security of confidential information stored on remote and networked clients
- > Conserves network bandwidth by rapidly updating clients with antivirus definitions, firewall rules, and intrusion detection signatures
- > **New!** Maximizes uptime and productivity by enabling administrators to proactively secure unprotected nodes before an event can occur
- > Maximizes deployment flexibility by providing the ability to pre-configure antivirus, firewall, and intrusion detection installation packages
- > **New!** Extensive platform support for workstations and servers, including Windows® Server 2003 and Netware® Secure Console
- > **New!** Supports 64-bit Intel® Itanium™ 2 hardware
- > Backed by Symantec™ Security Response, the world's leading Internet security research and support organization



Multiple methods of propagation are one of the characteristics of a blended threat. Each numbered pathway in this diagram represents a different way in which Nimda spreads. Standalone firewalls or virus protection on the client do not provide adequate protection against these complex Internet threats.

Symantec Client Security protects laptops outside the firewall from being used by hackers to gain unauthorized enterprise network access during an ISP connection. The integrated security also provides better protection against blended threats for desktop clients residing inside the firewall perimeter.

Symantec Client Security is the only single-vendor solution that integrates a comprehensive range of technologies for increased protection at the client tier. Multiple integrated technologies from a single vendor make it possible to coordinate management and response, resulting in increased protection and lower administrative and support costs, reducing total cost of ownership.

> **Comprehensive protection**

Symantec Client Security combines integrated protection, proven technologies, and a range of security features to protect remote users and networked clients against attacks, ease interoperability issues, and provide administrator peace-of-mind:

- **CLIENT SECURITY POLICY ENFORCEMENT** Symantec Client Security offers client security policy enforcement through the integration of multiple technologies. The client firewall technology and the real-time antivirus scanning technology will scan all traffic that travels in or out of remote user machines and networked clients. The firewall will determine the threat level of outgoing files based on the firewall rules. At that point the client firewall calls the antivirus technology to scan the outgoing file for viruses—even if the real-time protection has been disabled. If a virus is found, the firewall technology automatically increases security measures and blocks that file from exiting the remote or networked client.

Through integration of client firewall and intrusion detection technologies, scanning and comparing all incoming and outgoing traffic with known sets of signatures enables an offending IP address to be blocked if an intrusion attempt is detected.

- **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. In conjunction with a backend infrastructure consisting of hardware resources, architectural design, and the latest scanning engines and Web crawlers, the Digital Immune System ensures the highest levels of service availability.
- **INTEGRATED CLIENT FIREWALL TECHNOLOGY** Symantec's client firewall is an integral part of the Symantec Client Security solution. Client firewalls serve as a dedicated layer of protection at the client tier and control specific application access to the network, thereby ensuring the security of a company's information assets stored on remote user machines or networked clients.

> Integrated security management

Integrated security management via Symantec's proven infrastructure, Symantec™ System Center, offers a comprehensive view of antivirus, firewall, and intrusion detection functions. This enables advanced yet simplified security management of complex threats across all clients, including remote users, in an enterprise network. Administrator resources are optimized in this approach, since installation, reporting, and updates can be handled from one console. Management capabilities include:

- **INTEGRATED MANAGEMENT** Using Symantec System Center, administrators can configure, install, manage, and update client antivirus, firewall, and intrusion detection functions from one management console. Administrators can also configure, implement, and enforce corporate network policies from the console.
- **LOGICAL GROUP MANAGEMENT** Create and manage logical groupings of clients and servers within server groups. This feature is especially useful for organizations that need to handle similar functional entities in the same way, reducing the infrastructure cost of managing the solution.
- **EASE OF INSTALLATION** Symantec Packager™ technology provides the ability to pre-configure antivirus, firewall, and intrusion detection component installation packages, to maximize deployment flexibility and minimize deployment costs. Three pre-configured deployment options are available: fully-managed, lightly-managed, and thin-client.
- **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.

> 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, an integrated response capability enables enterprises to respond faster to security breaches and virus outbreaks, improving the overall security posture of the network.

This integrated updating and response is accomplished through Symantec™ Security Response, the world's leading Internet security research and support organization. Using Symantec's award-winning LiveUpdate™ technology, Symantec Client Security delivers virus definitions, firewall rules, and intrusion signatures via a single response mechanism. Symantec tests and verifies its update content across the integrated technologies prior to distribution.

INTEGRATED SECURITY 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.

FOR MORE INFORMATION VISIT [HTTP://ENTERPRISESECURITY.SYMANTEC.COM](http://enterprisesecurity.symantec.com)

SYSTEM REQUIREMENTS

SYMANTEC CLIENT SECURITY 1.1

SYMANTEC CLIENT SECURITY FOR 32-BIT WINDOWS CLIENTS

- Windows 98/98 SE/ME; Windows NT 4.0 Workstation with SP6a; Windows 2000 Professional; Windows XP Home/Professional
- 64 MB of RAM minimum
- 115 MB disk space
- Internet Explorer 5 or later
- Intel Pentium processor at 150 MHz (Pentium II or higher recommended)

SYMANTEC CLIENT SECURITY-ANTIVIRUS ONLY FOR 32-BIT WINDOWS CLIENTS

- Windows 98/98 SE/ME; Windows NT 4.0 Workstation/Server/Terminal Server with SP6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Home/Professional; Windows Server 2003 Web/ Standard/ Enterprise/Datacenter
- 32 MB RAM minimum
- 46 MB disk space
- Intel Pentium processor (Pentium II or higher recommended)

SYMANTEC CLIENT SECURITY-ANTIVIRUS ONLY FOR 64-BIT WINDOWS CLIENTS

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

SYMANTEC CLIENT SECURITY-FIREWALL/INTRUSION DETECTION ONLY FOR 32-BIT WINDOWS CLIENTS

- Windows 98/98 SE/ME; Windows NT 4.0 Workstation with SP6a; Windows 2000 Professional; Windows XP Home/Professional
- 64 MB of RAM minimum
- 70 MB disk space
- Internet Explorer 5 or later
- Intel Pentium processor at 150 MHz (Pentium II or higher recommended)

NOTE: Symantec firewall product versions other than Symantec Client Firewall version 5.0, Symantec Desktop Firewall version 2.01, Norton Personal Firewall version 2.5, and Norton Personal Firewall version 2002 must be uninstalled manually. There is currently no support for 64-bit operating systems.

SYMANTEC CLIENT SECURITY MANAGEMENT SERVER FOR 32-BIT WINDOWS

- Windows NT 4.0 Workstation/Server/Terminal Server with SP6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Professional; Windows Server 2003 Web/Standard/Enterprise/Datacenter
- 32 MB RAM (64 MB or higher recommended)
- 111 MB disk space (65 MB disk space for Symantec AntiVirus Corporate Edition server files and 46 MB disk space for the client disk image)
- Intel Pentium processor (Pentium II or higher recommended)
- Optional installation of AMS2 Server requires 15 MB disk space

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

SYMANTEC CLIENT SECURITY MANAGEMENT SERVER FOR NETWORK

- 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 client disk image)

- Intel Pentium processor (Pentium II or higher recommended)
- Optional installation of AMS2 Server requires 20 MB disk space

SYMANTEC SYSTEM CENTER

- Windows NT 4.0 Workstation/Server with SP6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Professional
- 10 MB disk space
- 64 MB RAM
- Internet Explorer 5.5 with SP2
- Intel Pentium processor (Pentium II or higher recommended)
- Microsoft Management Console version 1.2

NOTE: If MMC is not already installed, 3 MB free disk space is required (10 MB during installation) The following are additional requirements when using Symantec System Center Snap-ins

Alert Management System Console

- 10 MB disk space
- Symantec AntiVirus Snap-in
 - 5 MB disk space
- Symantec Client Firewall Snap-in
 - 1 MB disk space
- AntiVirus Server Rollout Tool
 - 130 MB disk space
- NT Client Install Tool
 - 2 MB disk space

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/Server with SP6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Professional
- 64 MB RAM
- 35 MB disk space
- Internet Explorer 5.5 with SP2
- Intel Pentium processor (Pentium II or higher recommended)

- Microsoft Management Console version 1.2

NOTE: If MMC is not already installed, 3 MB free disk space is required (10 MB during installation)

QUARANTINE SERVER

- Windows NT 4.0 Workstation/Server with SP6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Professional; Windows 2003 Web/Standard/Enterprise, Datacenter
- 128 MB RAM
- 40 MB disk space
- Internet Explorer 5.5 SP2
- Intel Pentium processor (Pentium II or higher recommended)
- 500 MB to 4 GB disk space recommended for quarantined items
- Minimum swap file size of 250 MB

SYMANTEC CLIENT FIREWALL ADMINISTRATOR

- Windows NT 4.0 Workstation/Server with SP6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Professional
- Internet Explorer 5.5 SP2
- 130 MB disk space (115 MB for JRE 1.4 install)
- Java Runtime Environment 1.4.0 (installed with the Symantec Client Firewall Administrator)

NOTE: If you are running Windows ME or 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.

LEGACY SUPPORT VIA NORTON ANTIVIRUS CORPORATE EDITION 7.6

NORTON ANTIVIRUS CORPORATE EDITION 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 FOR NETWORK 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 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.