



Symantec AntiVirus™ for Microsoft® Internet Security and Acceleration (ISA) Server

Enhanced virus protection for Web and SMTP traffic

INSIDE

- > The need for virus protection at the network perimeter
- > Deployment and implementation
- > Symantec virus protection capabilities

Contents

- Executive summary 3
- The need for virus protection at the network perimeter 3
 - Blended threats 3
 - Microsoft® Internet Security and Acceleration (ISA) Server 4
- Deployment and implementation 4
 - Web and email filters 5
 - Array support 5
 - High-performance scanning 5
 - Automatic load balancing 5
 - Symantec virus protection capabilities 6
 - Bloodhound™ 6
 - LiveUpdate™ 6
 - NAVEX™ 6
- Product configurations 7
 - Virus and malicious code blocking 7
 - Configuring antivirus settings through the ISA Management console 7
 - What happens when a file is scanned 8
 - Mail policy options 8
 - Configuring ISA Server SMTP and Web filters 9
 - Configuring the HTTP redirector filter 10
- Understanding alerting and logging 10
 - Alerting 10
 - Activating SNMP and SMTP alerting 10
 - Customizing alert messages 11
 - Logging 11
- Summary 12

> **Executive summary**

With the rising number of Microsoft® Internet Security and Acceleration (ISA) Server users leveraging the Internet throughout the collaborative workcycle increasing daily, organizations are now finding it necessary not only to address the need for expanded network access and defend against the ever-increasing sophistication of network attacks, but to also realize just how complex the process of securing distributed information assets can be as well.

While email-based attacks remain the leading source of infections, the Web itself is also an entry point for malicious content, and the scope of network security is now expanding to address this threat. In addition to addressing potential threats from email (SMTP), enterprises are also deploying defenses for Web (HTTP/FTP) traffic, especially when faced with rapidly evolving *blended threats*—that is, advanced attacks that employ multiple methods to propagate, as well as to discover and exploit network vulnerabilities. Today's blended threats are penetrating the corporate network simply by infecting trusted Web pages visited by unsuspecting Web surfers. In addition, the growing use of Web-based email extends the boundaries of the corporate network. These factors make virus protection for HTTP traffic crucial to an organization's overall network security posture.

> **The need for virus protection at the network perimeter**

Traditionally, IT personnel have focused on centralized security at the datacenter-level only. However, due to the “openness” of today's corporate networks and the fact that business-critical information is more readily available at every level of these networks, this focus has changed. Simply choosing appropriate protection for each network level is no longer enough to ensure the security and productivity of these corporate environments. Now the prevalence of *blended threats* in the picture has made it even more critical for IT departments to focus on the ever-expanding definition of the network perimeter and the security requirements that go along with it.

BLENDING THREATS

Firewalls control the traffic entering and leaving a corporate network, thereby providing a first line of defense against external attacks. However, advancements in the complexities of intrusions and threats no longer allow a firewall alone to provide an adequate level of protection. In fact, blended threats are now known to enter a network through the standard ports in use on a perimeter firewall. Blended threats combine the characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread attacks. By utilizing these multiple methods and techniques, blended threats are able to spread rapidly and cause widespread damage. And because blended threats attack through multiple network protocols in addition to the SMTP gateway, prevention now requires the implementation of security measures at both the SMTP and HTTP gateways.

MICROSOFT® INTERNET SECURITY AND ACCELERATION (ISA) SERVER

Symantec AntiVirus™ software is one of the fastest, most effective virus protection solutions available for detecting and preventing malicious virus attacks that leverages the ISA Management console to handle configurations. Symantec AntiVirus™ for ISA Server uses award-winning technologies that are optimized for speed to protect organizations from virus threats with minimal impact on the existing network infrastructure. The solution not only protects the corporate network against blended threats by blocking their entry through Web and email gateways, but scans the traffic served through the ISA Server to stop them before they enter the network, for enhanced virus protection throughout the corporate environment.

The reliable virus scanning and repair functions of Symantec AntiVirus for ISA Server are easily managed through the ISA Management console. At the same time, advanced features enable administrators to configure automatic and immediate updates of virus definitions, block email-borne viruses before a cure is available, and filter email messages that consume excess bandwidth. By leveraging this solution, ISA Server customers are assured of continued productivity while protecting valuable information assets.

> **Deployment and implementation**

Several options are available for deployment, however, Symantec AntiVirus for ISA Server Web and email filters must first be installed on each computer that is running ISA Server. If the implementation uses an array of computers running ISA Server, the Web and email filters need to be installed on each computer in the array. Symantec AntiVirus Scan Engine, the component that provides the virus scan and repair services for Symantec AntiVirus for ISA Server, should be installed before the Symantec AntiVirus for ISA Server Web and email filters so that the connection to the scan engine can be verified.

Symantec AntiVirus for ISA Server can be installed on the same computer as ISA Server (that is, an “on-box” configuration) or on a different computer on the network (an “off-box” configuration.) When Symantec AntiVirus and ISA Server are in an off-box configuration, files are passed to the antivirus scanning engine by way of a socket over the network. ISA Server users provide an appropriate IP address and port number for the scan engine so the filters can contact it.

Designed to protect the traffic passing through the ISA Server, Symantec AntiVirus for ISA Server only scans files from client applications that are configured to pass files to the virus scan engine. Because both ISA Server and Symantec AntiVirus for ISA Server handle potentially infected files, they are vulnerable without real-time virus protection of the operating system. To protect the host computers, a file server antivirus solution should be installed.

WEB AND EMAIL FILTERS

Symantec AntiVirus for ISA Server Web and email filters enable each ISA Server to communicate with Symantec AntiVirus for ISA Server so that files can be submitted for scanning. The email and Web filters must be installed on each server running ISA Server software. The Symantec AntiVirus for ISA Server email filter provides scanning for email traffic, while the Web filter provides HTTP and FTP over HTTP traffic scanning. Both filters redirect files through Symantec AntiVirus for ISA Server for virus scanning and repair services before forwarding them to their intended destinations.

The Symantec AntiVirus for ISA Server email filter is written as an application filter extension to ISA Server and is used when running ISA Server in firewall or integrated mode. Incoming and outgoing SMTP traffic is redirected by transparent proxy for virus scanning by the SMTP filter before it is forwarded to its destination.

This filter is written using the Internet Server Application Programming Interface (ISAPI). The Web filter can be used when running ISA Server in cache, integrated, or firewall mode. To ensure flexibility, administrators can install both the SMTP filter and the Web filter or customize the installation by installing only one filter.

ARRAY SUPPORT

Symantec AntiVirus for ISA Server supports configurations in which a single antivirus scan engine handles the scan and repair services for a single ISA Server, as well as arrays in which single or multiple scan engines handle scan and repair services for several ISA Servers.

HIGH-PERFORMANCE SCANNING

Symantec AntiVirus for ISA Server has a very small overhead impact to Web traffic and can scan hundreds of thousands of email messages during a normal work day. This high-performance scanning operation makes the protection of traffic transparent to users even under heavy volumes.

AUTOMATIC LOAD BALANCING

Symantec AntiVirus for ISA Server allows administrators to configure SMTP and Web filters independently in order to allocate scan engine resources to meet the specific needs of the organization. It also allows separate scan engine specifications for servicing Web or SMTP traffic or the ability to use multiple scan engines to provide scanning for both filters. When multiple Symantec AntiVirus for ISA Server products are in place and registered, load distribution across all registered implementations are handled automatically.

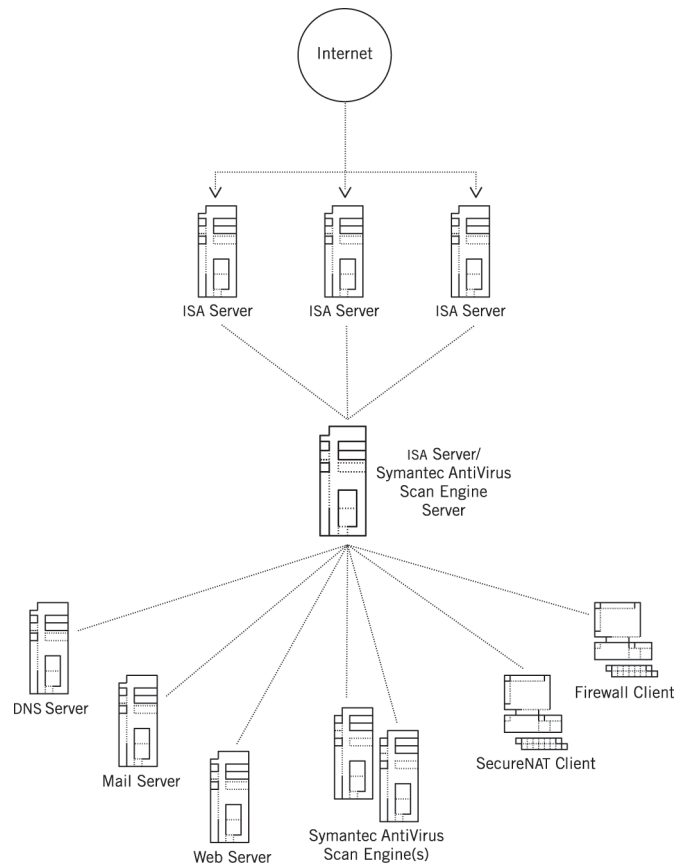


Figure 1. ISA Server array configuration with Symantec AntiVirus Scan Engine(s) component installed on network and on ISA Server.

SYMANTEC VIRUS PROTECTION CAPABILITIES

Symantec AntiVirus for ISA Server leverages all three of the antivirus engine technologies available in the award-winning line of Symantec virus protection products. Every one of these key technologies is capable of detecting viruses, worms, and Trojan horses not only in each of the major file types, but in the various compressed file formats (such as ZIP, LZH, ARJ, and tar) as well.

Bloodhound

Bloodhound™ is Symantec's revolutionary heuristic technology which analyzes programs, identifies unknown malicious code, and enables the user to repair an infected file immediately. Due to the way in which Bloodhound actually monitors macro virus behavior, it can detect and repair infections before new virus strains can proliferate or further mutate. Bloodhound technology has been shown to protect against more than 90% of new macro viruses and more than 80% of new file viruses. This antivirus engine technology is the only product on the market today that provides real-time protection against new macro viruses.

LiveUpdate

Symantec AntiVirus for ISA Server uses LiveUpdate™ to receive the latest virus definitions from Symantec™ Security Response automatically or manually without interrupting to virus scanning on the Windows 2000 Server, Sun® Solaris®, and Red Hat® Linux® platforms.

NAVEX

Another Symantec exclusive modular engine technology, NAVEX™ allows Symantec Security Response to provide the most advanced up-to-date antivirus solutions to customers across all platforms without interruption to virus scanning or requiring restart of the server. NAVEX technology delivers instant protection by separating the scanning application from the extensible scan engine, which can be improved upon and/or updated independently and is distributed as part of the standard Symantec virus definitions via LiveUpdate. LiveUpdate provides compact, easy-to-install updates without the need to redeploy the application.

> Product configurations

Symantec AntiVirus™ for ISA Server provides administrators with a range of configuration options to stop email- and Web-borne viruses from infiltrating the corporate network.

VIRUS AND MALICIOUS CODE BLOCKING

Symantec AntiVirus for ISA Server utilizes Symantec virus protection technologies to detect known and unknown viruses and other malicious code at the email and Web gateways. Administrators are able to configure the product to scan a myriad of file types, including the default file types included in the administrative interface. It can also exclude specific file types, such as GIF files, which are not capable of transmitting viruses.

If and when a virus is detected, the following options are available:

- REPAIR – The virus is repaired and the message is delivered
- DELETE – The infected file is deleted and the message is delivered
- LOG ONLY – Incident of virus is logged and the message (along with the infected file) is delivered

CONFIGURING ANTIVIRUS SETTINGS THROUGH THE ISA MANAGEMENT CONSOLE

One of the benefits of Symantec AntiVirus for ISA Server is most virus protection configuration options for the Web and email filters can be done through the ISA Management console.

When configuring virus protection for Symantec AntiVirus for ISA Server, administrators need to address the following:

- ATTEMPTING TO REPAIR INFECTED FILES – Scanning files to indicate whether they are clean or infected, then choosing whether to attempt to repair or delete any infected files that are found
- SELECTION OF THE TYPES OF FILES OR ATTACHMENTS TO BE SCANNED – Preserve bandwidth and improve performance by scanning only those file types that are capable of transmitting viruses, limiting them by extension and MIME type, or scanning all file types for maximum security
- BLOCKING ACCESS TO INFECTED FILES – Denying access to irreparably infected files
- ALERTING USERS THAT A VIRUS WAS FOUND – Adding text to the body of infected email messages to warn the message sender and recipient of the infection

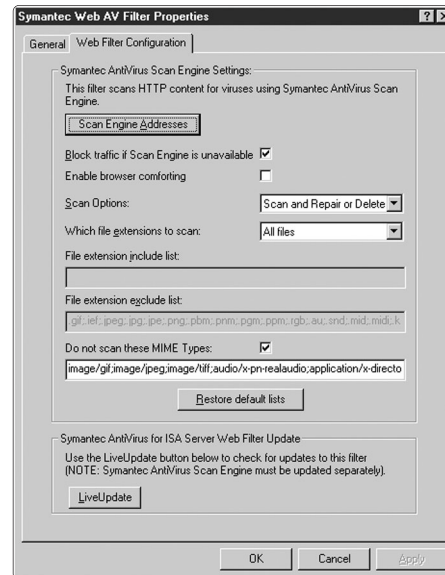


Figure 3. Symantec AntiVirus for ISA Server Web filter configuration.

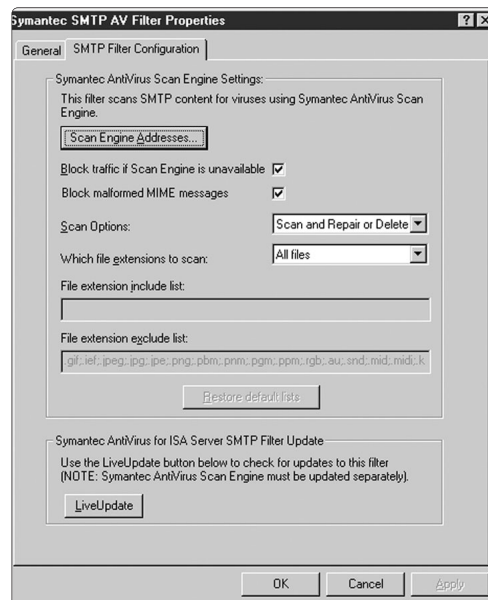
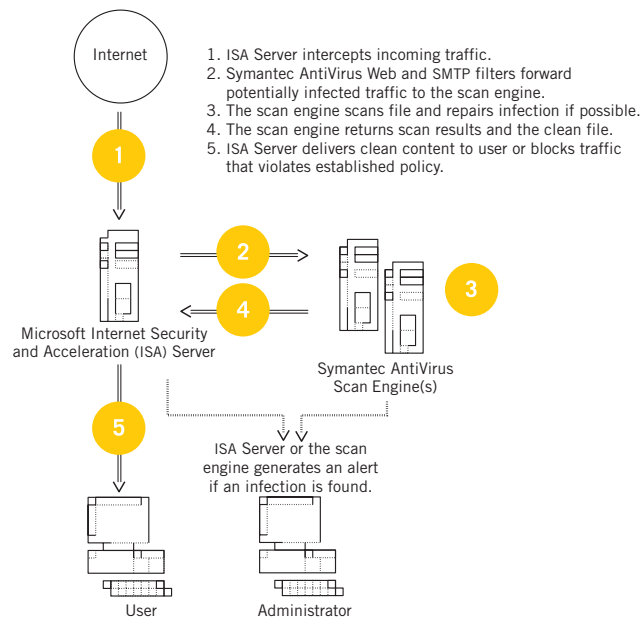


Figure 4. Symantec AntiVirus for ISA Server email filter configuration.

WHAT HAPPENS WHEN A FILE IS SCANNED

Once Symantec AntiVirus for ISA Server and the Symantec AntiVirus for ISA Server Web and email filters are installed and properly configured, the specified files are passed to the scan engine for analysis. If a virus is detected, the scan engine performs one or more of the following actions, depending on the configuration options selected:

- RECORDS A LOG ENTRY TO INDICATE THAT AN INFECTION WAS FOUND – Administrators are able to activate additional logging and alerting options in Symantec AntiVirus to supplement the logging and alerting through ISA Server and the Application Event Log
- ATTEMPTS TO REPAIR THE INFECTED FILE – The scan engine will repair an infected file, if possible, and will pass a clean file back to the system running ISA Server
- DELETION OF IRREPARABLE FILES – In the event that a file cannot be repaired, Symantec AntiVirus for ISA Server can be configured to delete the file



When the Symantec AntiVirus™ Scan Engine component is configured to delete irreparable SMTP files, infected attachments may be deleted from email messages. When infected Web traffic is detected, access to the file is denied. For both SMTP and Web traffic, irreparable files are deleted from the container or archive file in which they are embedded, and the remaining clean contents are forwarded to the intended destination. If the Symantec AntiVirus Scan Engine component does not find a virus, it indicates that the file is clean so that the file can be processed appropriately.

MAIL POLICY OPTIONS

Administrators have the ability to use mail policy settings to impose general restrictions on email, protecting the network even further. For example, once the characteristics of a new virus are understood during a virus outbreak, this information can be used to block the infected attachment or email.

Administrators are also able to configure the mail policy to block messages that otherwise would overload the mail server. Several configuration options are available, including message-blocking by:

- SPECIFIC FILE EXTENSION – Blocking messages that contain executable files
- SUBJECT LINE – Blocking messages that contain specified words or phrases
- TOTAL MESSAGE OR ATTACHMENT FILE SIZE – Blocking messages by imposing limits on the total size of a message or attachment

When configuring policy options, administrators can avoid overlapping or conflicting policies if they use the policy options on either the scan engine component or the ISA Server, but not both. This is important if the Symantec AntiVirus™ for ISA Server is providing scanning services for other client applications on the network in addition to ISA Server.

CONFIGURING ISA SERVER WEB AND EMAIL FILTERS

Symantec AntiVirus for ISA Server provides virus scanning for email and Web traffic through the use of independent filters. For flexibility, the email (SMTP) filter properties allow administrators to specify how virus scanning is implemented for the email filter. To change the email filter properties, administrators access the Symantec AntiVirus for ISA Server email filter configuration.

In order for virus scanning to occur for Web traffic, administrators need to enable the Symantec AntiVirus for ISA Server Web filter and ensure that the HTTP redirector filter is configured appropriately. Web filter properties enable administrators to specify how to implement virus scanning for the Web filter. To change the Web filter properties, administrators access the Symantec AntiVirus for ISA Server Web filter configuration.

Administrators are able to perform the following functions when configuring the email or Web filter:

- Specify an IP address and port number for each Symantec AntiVirus Scan Engine component that will provide scanning services for the filter
- Test the connection to the Symantec AntiVirus Scan Engine component that will provide scanning services for the filter
- Block email (SMTP) or Web traffic if the scan engine is unavailable
- Set the email or Web filter scan policies
- Specify which file types to scan
- Block malformed MIME messages (email filter only)
- Enable browser comforting (Web filter only)
- Prevent specific MIME types from being scanned (Web filter only)

CONFIGURING THE HTTP REDIRECTOR FILTER

When utilizing the Symantec AntiVirus™ for ISA Server Web filter, administrators need to configure the HTTP redirector filter and may do so through the ISA Management console. The redirector filter allows HTTP requests to be redirected through the local Web proxy for filtering by the Web filter.

Administrators perform the following steps to configure the HTTP redirector filter:

1. In the left pane of the ISA Management console, expand the *Extensions* tab and select *Application Filters*
2. In the right pane, right-click *HTTP redirector filter* and select *Properties*
3. Under the General tab in the Symantec AntiVirus for ISA Server Web Filter Properties dialog box check *Enable this filter*, then click *OK*
4. Under the Options tab, click *Redirect to local Web Proxy service*, then click *OK*

> Understanding alerting and logging

Because the Symantec AntiVirus for ISA Server Web and email filters and the Symantec AntiVirus Scan Engine are separate components that can be installed on different computers, separate logging and alerting features are available in each component.

Alerting for the Symantec AntiVirus for ISA Server filters is handled through the ISA Server alerting subsystem, and events are logged to the Application Event Log. The Symantec AntiVirus Scan Engine component also includes comprehensive logging and SMTP and Simple Network Management Protocol (SNMP) alerting capabilities, including startup, shutdown, virus definition updates, infections found, and so on. Administrators can activate SNMP and SMTP alerting individually by providing the necessary information for the delivery of the alerts and the specific events on which to generate alerts.

When configuring logging and alerting on the Symantec AntiVirus Scan Engine component, administrators should consider the logging and alerting features that are available directly through the Symantec AntiVirus for ISA Server filter, particularly if the Symantec AntiVirus Scan Engine component runs on the same computer as the ISA Server.

ALERTING

During installation of the Symantec AntiVirus for ISA Server Web and email filters, administrators can choose to set up default alerts. If default alerts are not established, alerts for selected events are configured automatically in the ISA Server alerting subsystem. If the default alerts are not set at installation, the standard ISA Management tools are used to establish the desired alerts.

Activating SNMP and SMTP alerting

To activate SNMP alerting, the administrator provides the SNMP community string and the IP address for a primary SNMP console that will receive the alerts. A second SNMP console can also be identified. Alerts are sent to both the primary and secondary SNMP consoles in all cases.

To activate SMTP alerting, the administrator identifies a primary SMTP server for forwarding alert messages and specifies the email addresses of the recipients and the local domain for the Symantec AntiVirus for ISA Server. The administrator can also identify a second SMTP server.

Customizing alert messages

Symantec AntiVirus™ for ISA Server alert messages can be customized by editing the message string file. The message string numbers in the file identify the usage for the message string and are labeled as follows:

- 1000 SERIES Message strings that are numbered in this manner are used to build the SNMP and SMTP alerts and standard log entries. Log entries and SMTP and SNMP alerts can be generated for many activities, including startup, shutdown, virus definition updates, and infections found.
- 2000 SERIES These message strings are used to update email messages when an infected attachment is discovered and subsequently repaired or deleted (if it cannot be repaired). This type of alert message notifies the recipient if a scanned email message that one or more attachments contained in the message were infected. Variables can be used to customize these alert messages.
- 4000 SERIES Message strings numbered in this manner are used to build log entries. In most cases, administrators will not need to edit alert strings, but alert messages for the Symantec AntiVirus Scan Engine can be customized if necessary.

LOGGING

Log entries generally contain more detailed information about an event than the alert for the same event. For example, the alert text for a violation indicates only that a violation has been detected but does not specify the type of violation. The log entry for the event contains more detailed information, such as whether the breach was a virus, container, or mail policy violation.

Symantec AntiVirus for ISA Server automatically logs selected events to the Application Event Log on the computer on which ISA Server is running. The 4000 series of message strings are used to build log entries and are customizable if necessary. Additional logging options are also available through Symantec AntiVirus for ISA Server. To appropriately configure the scan engine logging, administrators should consider the unique event-logging needs of the particular site.

If default alerts are established at installation, event logging is configured automatically. Symantec AntiVirus for ISA Server events are not logged to the Application Event Log if default alerts are not set up at installation. However, administrators can manually configure event logging after initial configuration.

> **Summary**

Viruses can spread easily in today's hyper-connected Internet environment, posing serious threats to business operations and financial investments. Implementing virus protection at the email and Web gateway is a critical step in protecting the corporate network against these viruses and other related threats. ISA Server software aggregates all HTTP, FTP, and SMTP traffic and serves as a logical point for implementing security measures.

The features offered by Symantec AntiVirus™ for ISA Server provide reliable virus scan and repair services that are easily managed through the ISA Management console and optimized for high performance. It also provides comprehensive protection against email-borne viruses, worms, and malicious Web content. Symantec AntiVirus for ISA Server is backed by Symantec Security Response, the world's leading Internet security research and response organization.

SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOFTWARE AND APPLIANCE SOLUTIONS TO INDIVIDUALS, ENTERPRISES AND SERVICE PROVIDERS. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY ASSESSMENT, INTRUSION PREVENTION, INTERNET CONTENT AND EMAIL FILTERING, AND REMOTE MANAGEMENT TECHNOLOGIES AND SECURITY SERVICES TO ENTERPRISES AND SERVICE PROVIDERS AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS IS A LEADER IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM



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.