Symantec AntiVirus™ Gateway Solution

Comprehensive virus protection, spam prevention, and content filtering for Web and email traffic at the Internet gateway

The most common transmission routes for viruses and worms are through email and Web traffic. In addition, the growing volume of unsolicited email (spam) and inappropriate Web surfing poses risks to corporate security, liability, and employee productivity. Effective security at every network tier—especially virus protection at the Internet gateway—is essential in today’s Internet-enabled network environments.

Symantec AntiVirus Gateway Solution provides multi-layered protection against viruses, spam, and unwanted email and Web content at the Internet gateway. This bundled solution includes Symantec Mail Security™ for SMTP (for Internet email traffic) and Symantec™ Web Security (for HTTP/FTP traffic) to protect the network against complex Internet threats.

New features in this release

The latest version of Symantec AntiVirus Gateway Solution includes the following enhancements:

- **ENHANCED ANTISPAM HEURISTICS** improves processing and analysis of email traffic to detect and tag spam messages with the latest spam definitions.
- **AUTO-GENERATED WHITELIST** prevents false positives by automating the collection of known and trusted email domains to build a comprehensive whitelist and avoid unnecessary scanning of legitimate email traffic.
- **ENHANCED WHITELIST SUPPORT** provides greater flexibility for whitelist entries that now include an email address, as well as support for wildcarding domains.
- **FLEXIBLE SCORE-BASED SPAM HANDLING** offers flexible policy settings for dealing with messages based on spam score assigned by the heuristic antispam engine.
- **CUSTOM SPAM FILTERING RULES** allows administrators to create their own spam filtering rules based on message body content. This complements custom rules based on spam headers such as sender blocking and subject line blocking.
- **MASS MAILER CLEANUP OPTION** deletes messages generated by mass mailer worms.
- **CUSTOM DISCLAIMER OPTION** allows custom text (such as legal disclaimers) to be added to outbound email messages.
- **CUSTOM MESSAGE BODY FILTERING RULES** create message body filtering rules to enforce email usage policy.

Key Points

- Combines two industry-leading Symantec solutions for comprehensive, multi-layered protection against viruses, spam, and unwanted email and Web content at the Internet gateway
- **NEW!** Auto-learned whitelist automatically captures known and trusted mail domains to generate a comprehensive, effective whitelist and reduce false positives
- **NEW!** Enhanced antispam heuristics engine for greater effectiveness
- **NEW!** Flexible, customizable filtering rules scan message body text for keywords and phrases, eliminating spam and other undesirable content
- **NEW!** Mass Mailer Cleanup automatically eliminates entire messages infected with mass mailer worms—not just attachments
- **NEW!** Additional spam tagging and handling options offer greater flexibility
- Secure remote management, advanced outbreak alerting, and concise reporting to view key performance and scanning metrics and overall system status
- Enables transparent virus definition and scan engine updates without restarting services or reinstalling software
- Scheduled delivery of antivirus, heuristic antispam, and URL filter list updates for up-to-date protection
- Backed by Symantec™ Security Response, the world’s leading Internet security research and support organization
Symantec ANTIVIRUS GATEWAY SOLUTION

Comprehensive, high-performance virus protection

Symantec AntiVirus Gateway Solution provides scalable and reliable virus scanning for the email and Web gateway to enhance security without sacrificing performance.

- MINIMAL RESOURCE DEMANDS Advanced scanning and repair services are optimized for speed to minimize latency of email and Web traffic.
- COMPREHENSIVE PROTECTION Award-winning Symantec antivirus technologies detect and protect against viruses, worms, and Trojan horses in all major file types, including mobile code and compressed file formats.

Viruses transmitted via Web and email traffic are notoriously fast-spreading, so a fast, proactive cure is required.

- HOUR-ZERO PROTECTION Blocking file types can stop outbreaks at the network perimeter.
- MASS MAILER CLEANUP Detection of mass mailer worms enables administrators to eliminate the entire message, not just the attachment, to free mail server resources.

Symantec AntiVirus Gateway Solution combines signature and heuristics-based detection technologies leveraging the following Symantec technologies to help prevent viruses from entering the network:

- LIVEUPDATE™ Automatic scheduled delivery of virus definitions ensures up-to-date protection.
- BLOODHOUND™ Heuristic detection technology that can detect up to 80 percent of new and unknown executable file viruses, including malicious mobile code.
- NAVEX™ Modular scan engine technology that updates virus definitions and scan engines without the added requirement of restarting or reinstalling software. This ensures maximum up-time and helps lower the total cost of ownership.

Multi-layered spam prevention

Spam poses a significant threat to enterprise email resources by consuming valuable bandwidth and email storage space, negatively impacting end-user productivity, and potentially exposing the organization to legal liability. To combat this increasingly sophisticated threat, organizations need a solution that provides multiple antispam techniques and layers of protection.

Symantec Mail Security for SMTP—the email scanning component of the Symantec AntiVirus Gateway Solution—controls spam by combining various detection and false positive prevention layers, including antispam heuristics, support for multiple real-time blacklist services, sender blacklists, filtering rules to detect spam, and enhanced whitelisting. These layers work together to maximize detection and minimize false positives.
Symantec ANTIVIRUS GATEWAY SOLUTION

- **SPAM DETECTION**
  - CUSTOM BLACKLIST
  - ENHANCED HEURISTIC ANTI-SPAM ENGINE
  - LIVEUPDATE SUPPORT FOR SPAM DEFINITIONS
  - FLEXIBLE AND MULTIPLE REAL-TIME BLACKLIST SUPPORT
  - SUBJECT LINE RULES
  - MESSAGE BODY SPAM RULES

- **FALSE POSITIVE PREVENTION**
  - ENHANCED CUSTOM WHITELIST
  - AUTO-GENERATED WHITELIST

- **SPAM HANDLING**
  - CUSTOM SUBJECT LINE TAG
  - X-BULK HEADER TAG
  - FLEXIBLE SCORE-BASED SPAM HANDLING

- **Real-time Web filtering**

  Symantec AntiVirus Gateway Solution provides scalable and reliable virus scanning for the email and Web gateway to enhance security without sacrificing performance.

  - **COMPREHENSIVE CONTENT FILTERING** Symantec’s patented, multi-lingual Dynamic Document Review™ (DDR) technology works in conjunction with Symantec’s massive categorized URL database to provide comprehensive Web content filtering. DDR exceeds simple keyword searches to analyze context-sensitive word relationships, and works in real time to determine whether or not to block inappropriate Web content, even if that content is not yet categorized in an existing filtering list. DDR effectively detects and blocks new or newly accessible sites, formerly accepted sites whose content has changed, and once blocked sites with new domain names.

  - **SIMPLIFIES ADMINISTRATION** For simple, enterprise-wide installation, configuration, and management, Symantec Web Security provides an intuitive HTML-based Web interface and secure SSL support for external directories (including LDAP, Active Directory, and Windows NT users/groups).

  - **SUPPORTS BROWSING PROFILES** Administrators are able to create, schedule, and enforce customized browsing profiles according to organizational policies using 30 pre-defined categories—such as sex, gambling, and intolerance—on a system-wide, per-user, per-computer, or per-group basis.

  - **CENTRALIZED POLICY-BASED MANAGEMENT** To further streamline administration, centralized multi-server policy management leverages LDAP and Active Directory, allowing administrators to automatically modify scanning and filtering policies for every Symantec Web Security server within their network, from any server that is connected to the network. Any changes made to the virus scanning or Web content filtering settings on any Symantec Web Security server are automatically propagated to all other Symantec Web Security servers in the network.
Backed by Symantec™ Security Response

For even more security intelligence and timely, around-the-clock protection, Symantec AntiVirus Gateway Solution is supported by Symantec Security Response, the world’s leading Internet security research and support organization. Symantec Security Response provides swift, global responses to security events and proactive research on future threats.

For more information about Symantec AntiVirus Gateway Solution, visit http://enterprisesecurity.symantec.com

VIRUS PROTECTION, ANTIISPAM, 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 GATEWAY SOLUTION 4.0

All applications within the Symantec AntiVirus Gateway Solution bundle require one of the following Web browsers:
- Microsoft Internet Explorer 6.0 or later
  - OR - Netscape Navigator 7.02

SYMANTEC WEB SECURITY 3.0

WINDOWS NT/2000/2003
- Intel Pentium III or compatible processor, or better
- Microsoft Windows NT Server 4 with SP6a or Windows 2000 Server with SP2 or Windows Server 2003
- 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 functions on Windows 2000 Server and Windows Server 2003 with the same level of compatibility as Windows NT Server 4.0. However, it does not adhere to Windows 2000/2003 Server Logo Requirements).

SOLARIS
- Sun SPARC-based system
- Solaris 7 or 8
- 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 CERTN HTTP Proxy protocol compliant browser, such as
- Microsoft Internet Explorer v5.0 or later
  - OR - Netscape Navigator v4.7 or later

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 6.0 or later
  - OR - Netscape Navigator v7.02

WINDOWS 2000 SERVER
- Intel Pentium III or IV or compatible
- Windows 2000 Server with SP4
- 256 MB RAM minimum
- 50 MB to install
- 500 MB minimum after install for mail processing
- Microsoft Internet Explorer 6.0 or later
  - OR - Netscape Navigator 6.0 or later
  - OR - Netscape Navigator 7.02