

Symantec™ Mail Security for SMTP 5.0

Integrated antivirus, content filtering and antispam for any messaging environment

Availability	2
What is Symantec™ Mail Security for SMTP 5.0?	2
How is Symantec™ Premium AntiSpam Related?	2
Value Statements	3
Target Market.....	7
Key Points.....	8
What's New?.....	9
Continuing Features & Benefits.....	12
System Requirements.....	19
Licensing, Support and Maintenance.....	20

Control Information

Date First Issued	January 6, 2006
Date Last Revised	July 28, 2006
Audience	Symantec global sales
Distribution Control	Limited initially to Symantec employees. After legal review, channel partner and customer versions will be available.
Author	Allison Fung, Sales Tools and Enablement



Availability

Following are the first customer ship dates in each region (subject to change without notice). Consult your regional marketing manager for launch dates and activities.

Region	Language	First Customer Ship
North America	English	May 24, 2006
LAM	International English	May 24, 2006
EMEA	International English	June 15, 2006
	French (end user portion)	
APAC	International English	June 14, 2006
Japan	International English	June 12, 2006
	Japanese (end user portion)	

What is Symantec™ Mail Security for SMTP 5.0?

Symantec™ Mail Security for SMTP 5.0 is a comprehensive and flexible email security software solution that stops inbound and outbound email-borne threats from impacting the organization, damaging productivity, and compromising security.

Symantec Mail Security for SMTP 5.0 features best-of-breed Symantec Brightmail AntiSpam and Symantec™ AntiVirus technologies to protect against email-borne threats such as viruses, spam, phishing, directory harvest attacks, compliance violations, and other unwanted content at the earliest point of network entry, the Internet email (SMTP) gateway. From a single Web-based console, administrators can easily apply varying policies for different users or groups, gain insight into trends and attack statistics, track messages that have traversed the system, and customize and monitor all aspects of an organization's email security.

As a major part of the Enterprise Messaging Management (formerly Email Security & Availability) solution, Symantec Mail Security for SMTP 5.0 is one of three strategic deployment options for messaging gateway security. Along with appliances and our hosted solution, Symantec Mail Security for SMTP 5.0 offers the customer the most flexibility in deployment of any messaging security vendor.

How is Symantec™ Premium AntiSpam Related?

Symantec™ Premium AntiSpam refers to the subscription-based antispam protection based on the Brightmail AntiSpam engine. This level of protection is distinguished from the "basic" antispam capability available in Symantec Mail Security for SMTP 4.x, which is less effective on today's spam attacks.

When customers purchase a Symantec Premium AntiSpam subscription, they receive ongoing antispam filter updates, the best combination of effectiveness (spam catch rate) and accuracy (false positive rate) available in the marketplace today, and a low cost of administration.



Value Statements

Functional IT

Functional IT Needs	Reduce spam volume	Keep email secure	Simplify deployment and management	Meet regulatory and corporate compliance objectives
Value Proposition Symantec Mail Security for SMTP 5.0 protects email at the SMTP gateway through best-of-breed of antispam, antivirus, and content filtering technologies.				
How We Deliver	Most accurate, industry-leading antispam and response	Industry-leading antivirus and response	Flexible, easy deployment and management	Content filtering technologies
Key Messages	<ul style="list-style-type: none"> Highest spam accuracy of 99.9999% (less than 1 false positive in every million messages) 97.96% effectiveness Integrated, award-winning Symantec Brightmail AntiSpam technology Increase end-user productivity and trust through more effective spam prevention Lower total cost of ownership due to proven accuracy and effectiveness 	<ul style="list-style-type: none"> Integrated, award-winning Symantec Antivirus technology New Day Zero virus prevention stops early-stage viruses Minimize network disruptions caused from virus outbreaks Ensure protection from email-borne viruses delivered via spam and from known or emerging threats Timely and accurate security updates from worldwide support and security research organization Eliminate spyware With integrated 	<ul style="list-style-type: none"> Automatic and accurate spam and virus updates delivered every 5-10 minutes enable timely protection with zero administration Leverages existing customer infrastructure Level of control is your choice; rely on default settings built upon common email policies, or customize to meet your needs Gain insight into filtering performance with powerful monitoring tools Quickly track status of individual messages 	<ul style="list-style-type: none"> Helps organizations comply with corporate and regulatory requirements Protects confidential information Enables IT managers to categorize and control messages flowing through the mail system Enables IT managers to create content filtering policies based on user groups



		LiveUpdate™ functionality, virus definitions can be deployed across the enterprise without stopping scan services or incurring server downtime		
--	--	---	--	--



<p>Proof Points</p>	<ul style="list-style-type: none"> • Industry-leading Brightmail AntiSpam technologies • Review of submitted false positives by email security experts at Symantec Security Response • High spam detection rate combined with an industry-leading accuracy rate against false positives ensures the flow of legitimate mail • Non-English language spam detection • Global, real-time antispam content from Symantec Security Response • Broadest array of technologies including URL technology, optimized heuristics, Signature technology, Reputation filters, and more • Automatic spam and virus updates every 5-10 minutes ensure the most effective, real-time protection • Antifraud defense includes Sender ID, URL fraud filters, and Sender policy framework 	<ul style="list-style-type: none"> • Award-winning AV leveraging information gathered from Deepsight sensors around the globe • Most consistently certified virus protection in the industry • More definition updates generated (than competitors) 	<ul style="list-style-type: none"> • Centralized Control Center makes it easy to monitor, configure, and customize multiple scanners on a network • Granular policy control for users and groups • Multiple actions or combinations of actions to customize email filtering • Over 50 ready-to-use report formats; reports can be generated in real time, or scheduled and exported 	<ul style="list-style-type: none"> • Flexible actions for policy violations including notification, quarantine, etc. • Inbound and outbound group policies dynamically populated from existing directory services • Customized reports show compliance trends and violations • Keyword scanning in attachments • Keyword scanning within zips and containers • Keyword frequency • True file typing • Content compliance enforces email content policies based on keyword dictionaries, attachment types, and custom filters
----------------------------	---	--	---	--



Partners

Channel needs	Grow consistent, profitable business	Increase customer satisfaction	Create service opportunities	Manage costs
Value Proposition	Symantec Mail Security for SMTP 5.0 enables partners to deliver on customer demands and grow revenue with the only email gateway security product that integrates Brightmail AntiSpam with Symantec AntiVirus for secure mid-market email infrastructures.			
How We Deliver	Subscription-based licensing	Proven, trusted technologies	Value-added services	Ease of support
Key Messages	<ul style="list-style-type: none"> • Volume opportunity • Recurring revenue-stream through renewal-based subscription service • High margin revenue for very little additional work. • Upsell opportunities for existing Symantec customers • Cross sell opportunities for other SMS gateway and groupware products 	<ul style="list-style-type: none"> • Best-of-breed technologies ensure customer confidence • Increase the effectiveness of spam prevention and protection • Reduce the business impact of false positives • Minimize risk of downtime from virus outbreaks 	<ul style="list-style-type: none"> • Provide your customers with deployment and installation services including scalability and high availability configurations for complex environments • Offer integration services including integration with directory services • Customize group and mail policies as part of an overall compliance solution 	<ul style="list-style-type: none"> • Close sales easier with Symantec and Brightmail brand recognition • Minimize routine service calls for ongoing product maintenance • Reduce support costs by leveraging Symantec's global support organization for first-line customer support
Proof Points	<ul style="list-style-type: none"> • Annual subscription renewal required for continued updates and patches. • Subscription-renewal reports/rates • Premium AntiSpam and AntiVirus subscriptions • Incremental revenue 	<ul style="list-style-type: none"> • Proven industry-leading false positive accuracy • 97.96% antispam effectiveness rate • Automatic antispam content delivered globally from Symantec Security 	<ul style="list-style-type: none"> • Symantec education services • Extensive group policy support • Integration with directory services • Full text scanning of email and enclosures based on configurable 	<ul style="list-style-type: none"> • Automatic rules updates frees IT administrators from having to tune filters • Minimal tuning required for product to function • Highest antispam accuracy of 99.9999%



	<p>opportunities on expanding platform</p> <ul style="list-style-type: none"> New mail security technologies to address emerging threats 	<p>Response</p> <ul style="list-style-type: none"> Automatic AntiVirus content delivered globally from Symantec Security Response Centers Centralized aggregated reporting 	keyword lists	<p>(less than 1 false positive in every million messages)</p> <ul style="list-style-type: none"> 97.69% antispam effectiveness
--	---	--	---------------	---

Target Market

Primary – Large Enterprise (5000+)

Vendor Criteria	<p>Incident response (reliability)</p> <p>Multi-layered spam prevention (blacklists, whitelists, heuristics, etc.)</p> <p>Post-sales service and support (also local support)</p> <p>Manufacturer's products already installed</p> <p>Vendor credibility (financial stability)</p>
Product Criteria	<p>"Best of Breed" (quality) point solution</p> <p>Performance and scalability</p> <p>Reliability (proven technology)</p> <p>Third-party certifications</p> <p>Ease of manageability</p>
Decision Maker	<p>Senior AV administrators</p> <p>Senior IT managers/directors</p> <p>Senior security administrators</p>
Approvers	<p>Chief Technology/Security/Information Officers</p>
Key Verticals	<ul style="list-style-type: none"> Financial Services State and local government agencies Pharmaceutical Legal firms Healthcare Medical High-tech Manufacturing Academic institutions



Secondary – Enterprise (501-5000)

Vendor Criteria	<p>Incident response (reliability)</p> <p>Multi-layered spam prevention (blacklists, whitelists, heuristics, etc.)</p> <p>Post-sales service and support (also local support)</p> <p>Manufacturer’s products already installed</p> <p>Vendor credibility (financial stability)</p>
Product Criteria	<p>“Best of Suite” (overall value covering all tiers)</p> <p>Performance and scalability</p> <p>Reliability (proven technology)</p> <p>Third-party certifications</p> <p>Management ease</p>
Initiators	<p>IT (security) managers</p> <p>CXO (of a “security incident” has occurred)</p>
Users	<p>Anti-virus administrators</p>
Influencers	<p>CXOs</p> <p>Directors of Technology</p> <p>Security/Network/System Administrators</p>
Key Verticals	<ul style="list-style-type: none"> • Financial Services • State and local government agencies • Pharmaceutical • Legal firms • Healthcare • Medical • High-tech • Manufacturing • Academic institutions

Key Points

Symantec Mail Security for SMTP 5.0 includes comprehensive virus protection for the Internet email gateway and integrates multiple filtering and blocking technologies to reduce spam and eliminate undesirable email content. Symantec Mail Security for SMTP 5.0 allows you to:

- Simplify and strengthen your gateway software solution from the leader in email security.
- Expand your content filtering and compliance capabilities.
- Augment your administrative capabilities.
- Increase your overall threat protection.

What's New?

Feature	Description	Benefits
Comprehensive Email Threat Protection	<p>New!</p> <ul style="list-style-type: none"> Day Zero virus prevention sends messages with suspicious attachments to the new suspect virus quarantine Spyware/adware dispositions triggers for messages containing spyware or adware threats <p>Improved</p> <ul style="list-style-type: none"> Email Firewall to reduce impact of directory harvest, spam, and virus attacks Antiphishing defenses with Sender Policy Framework (SPF) and Sender ID standards. Antispam powered by the Brightmail engine and the Sender Reputation Service Virus scanning powered by the NAVEX engine 	<ul style="list-style-type: none"> Reduces spam volume Minimizes infection, cost of clean-up, and downtime due to malicious code. Improves security and efficiency of messaging infrastructure Increases user productivity Mitigates emerging threats such as phishing, spyware, directory harvest attacks, and other unwanted content
Inbound and Outbound Content Control	<p>New!</p> <ul style="list-style-type: none"> True File type recognition automatically recognizes file types without relying on filename extensions or MIME type Scan inside attachments for keywords and regular expressions. Extract content from nearly 300 word processing, spreadsheet and presentation file formats. Keyword frequency controls for more accurate filtering <p>Improved</p> <ul style="list-style-type: none"> Keyword dictionaries that ship pre-populated with offensive words and phrases Content Filter Editor creates global, server-level filters to enforce company policies. There is no limit to the number of conditions administrators can create in the content filter. Attachment stripping removes large or prohibited attachments as per organization policies Annotations/disclaimers automatically append or prepend text (such as confidentiality disclaimers or marketing tag lines) to messages Custom notifications generated on the fly in response to content violations Interoperability with archiving tools 	<ul style="list-style-type: none"> Helps organizations comply with legal, regulatory, and corporate compliance objectives Protects proprietary or confidential information Helps ensure a hospitable work place environment
Flexible Mail Management	<p>Improved</p> <ul style="list-style-type: none"> Separate inbound and outbound policies for different groups and users Dynamic group population and alias 	<ul style="list-style-type: none"> Meets unique email requirements of end users and groups in the organization



Feature	Description	Benefits
	<p>expansion leveraging existing LDAP directories</p> <ul style="list-style-type: none"> • Extensive and combinable actions (delete, quarantine, archive, reroute, and more) • End-user management of personal allow and block lists and language selections via the Web 	<ul style="list-style-type: none"> • Eliminates need to enter, manage, and maintain user and group information in multiple systems • Reduces administration by empowering users to manage their own email preferences over the Web
<p>Reporting and Message Tracking</p>	<p>New!</p> <ul style="list-style-type: none"> • Graphical message tracking provides comprehensive information on any message processed by the system. Search by arrival/departure time, subject, from/to, verdict, action, final delivery status, and more <p>Improved</p> <ul style="list-style-type: none"> • Consolidated logging and reporting over all deployed mail scanners • Over 50 graphical reports that can be generated ad hoc or on a scheduled basis. Reports can be exported for offline analysis and emailed to specific individuals 	<ul style="list-style-type: none"> • Gives greater control, and visibility into how system is performing • Demonstrates product ROI • Identifies crucial trends such as the top recipients of spam or viruses or the top compliance policies that were triggered. • Increases administrator productivity by reducing time required for administrators to resolve user questions and help desk calls regarding "lost" messages • Aids troubleshooting when tracking problems in the mail infrastructure
<p>Easy, Powerful, and Secure Administration</p>	<p>Improved</p> <ul style="list-style-type: none"> • Centralized, Web-based administration that controls all aspects of spam, virus, and content filtering across all servers with one interface • Antivirus management with LiveUpdate gives added control over the timing and type of definition updates • Automated antispam filter updates every 10 minutes from Symantec Security Response • Multiple administrator roles with view only or modify access to different portions of the management interface • Web-based spam Quarantine deployed in an admin-only mode or for all users • Embedded MTA with support for per-domain routing, address rewriting, TLS support for secure email 	<ul style="list-style-type: none"> • Reduces administration complexity and intervention • Decreases IT admin time managing email security • Allows administrators to offload tasks and management • Decreases possible downtime and increases comfort since administrators can deploy definitions on their own schedule



Feature	Description	Benefits
	<ul style="list-style-type: none">• IP access control to limit which hosts and networks can access the Control Center• Remote syslog support• System alerts emailed to specific individuals when operating conditions warrant• Full Internationalization• French and Japanese localization for end users	

Continuing Features & Benefits

Feature	Description	Benefits
Comprehensive Spam Prevention	<p>Directory Harvest Attack (DHA) Prevention detects directory harvest attacks before they have a chance to impact the mail server. In DHA attacks, malicious senders generate email addresses using common surnames and proceed to bombard the mail server. By tracking the bounced messages, spammers can obtain a list of valid email address within an organization.</p> <p>Spam Attack Prevention detects possible spam attacks by examining the frequency and quality of the messages received from incoming IP addresses.</p> <p>Administrator-defined Blocked Senders recognizes blocked senders (identified by IP address) for the organization. The senders can be identified at the DNS or local level.</p> <p>Reject Messages</p> <ul style="list-style-type: none"> Allows the MTA (Mail Transfer Agent) to reject the message based on the quality or behavior of the sender. This is helpful in response to messages sent from senders who are disseminating spam or otherwise using abusive tactics. Sends a delivery failure notification, along with customizable text by the administrator. Failure notifications are valuable if the sender is unknowingly (via a compromised machine) sending spam or other unacceptable content. <p>Integrated Sender Reputation Service Data leverages the reach and visibility of Symantec's Probe Network along with sender data culled from filtering statistics. Based on objective analysis of sending patterns at the network level, the Sender Reputation Service can identify abusive senders and prevent them from connecting to the server.</p> <p>Third-party Lists lets administrators configure lookups to third-party lists of allowed or blocked sender services to which the administrator subscribes.</p>	<ul style="list-style-type: none"> Reduces future spam attacks Detects and stops directory attacks and other attempts to harvest email addresses Stops spam attacks that consume resources and threaten business continuity Lets administrator decide how email from blocked senders will be handled Improves processing by allowing the MTA to reject messages Allows scanners to automatically block or allow SMTP connections based on sender profile and reputation data from the Sender Reputation Service Gives administrators configuration control to third-party sender lists
Industry-leading Brightmail AntiSpam Protection	<p>Safe IP List provides a constantly updated list of IP addresses from which virtually no outgoing email is spam. Symantec manages the IP address list.</p>	<ul style="list-style-type: none"> Helps limit false positives



Feature	Description	Benefits
	<p>Language Features</p> <ul style="list-style-type: none"> • Language Identification—Identifies the text of the message as belonging to one of 11 languages. Symantec Mail Security can then run only the filters that apply to the message's language. Lets both administrators and end users adjust language preferences to deny or allow email based on language identification by Symantec. • Language-specific Heuristics—Provides specially tuned heuristics for 11 different languages. Supported languages include: <ul style="list-style-type: none"> - Chinese - Dutch - English - French - German - Italian - Japanese - Korean - Portuguese - Russian - Spanish • Language Expertise—Technicians deployed across the globe analyze spam and create targeted filters in over 15 languages. <p>Filtering Technologies and Signatures</p> <ul style="list-style-type: none"> • Updated URL Filters—Identifies and filters a spammer's intended URL, which is often disguised and leads to spam Web pages. This URL technology was invented by Brightmail, and is now in its fourth generation. • BrightSig2 Filters—Includes signature technology that eliminates randomization and HTML-based filter evasion techniques. • Header Filters—Uses tight, targeted, regular expression-based filters based on real-time attacks or derived based on commonalities or trends present in spam messages. • Body Hash Filters—Includes first-generation signature technology. • Attachment Signatures—Targets a specific MIME attachment, for example, a ZIP file that contains a virus. <p>Filter Updates and False Positive Resolution</p> <ul style="list-style-type: none"> • 10-Minute Updates—Automatically downloads filters from Symantec to customer sites via secure HTTPS every 5–10 minutes. No need for server 	<ul style="list-style-type: none"> • Enables the engine to run only the filters that apply to the message's language, resulting in better performance • Enables users to define the languages in which they want to receive messages • Provides faster and more accurate detection and response times for network protection <ul style="list-style-type: none"> • Uses over 20 different filtering technologies that together maximize spam detection (95% effectiveness) and minimize false positives (less than 1 false positive in one million messages)¹ • Identifies and filters mail that enters the gateway accurately and effectively <ul style="list-style-type: none"> • Offers fast and convenient filter updates • Provides fast false positives response

¹ Yankee Group 2004



Feature	Description	Benefits
	<p>restart or administrator intervention.</p> <ul style="list-style-type: none"> • 24-Hour per Day False Positive Resolution—Provides quick false positive resolution. False positives are analyzed and corrected by Symantec technicians within 24-hours. <p>Global Operations Centers and Largest Honeypot Network</p> <ul style="list-style-type: none"> • Global Operations Centers—Symantec has globally distributed spam analysis and operations centers in the United States, Ireland, Australia, and Taiwan. They provide 24x7 monitoring of spam attacks and filtering performance at customer sites. • Spam Detection Network—Includes the largest honeypot network (over 2 million decoy email addresses and domains). Contains submissions and statistics from over 300 million email inboxes. <p>Spam Submission</p> <ul style="list-style-type: none"> • Missed Spam Submission—Users can submit missed spam to Symantec via email. If warranted, Symantec will adjust filters. • False Positive Submissions—Use convenient submission tools, Symantec’s user community—300 million—can quickly inform Symantec as soon as possible in the event of a misidentified message. • Submission Responses—Based on the submissions, Symantec will adjust filters if warranted to improve filtering quality. 	<ul style="list-style-type: none"> • Consists of several centers working cooperatively on three continents, comprising a round-the-clock protection network that spans the globe • Makes it easy for users to send missed spam and false positive spam to Symantec
<p>Award-winning Virus Protection</p>	<p>Advanced, Automated Antivirus Technologies</p> <p>Scans and detects viruses by integrating Symantec’s award-winning antivirus technology. Antivirus protection includes automatic virus definition updates, flexible policies to handle messages with viruses, and specific defenses against mass-mailing worms and the associated spawned emails. Antivirus protection also includes:</p> <ul style="list-style-type: none"> • Rapid, Reliable Scanning and Repair—Provides rapid and reliable virus protection by scanning all incoming and outgoing Internet email (SMTP) traffic via a multi-threaded scanning system to reduce network impact. Also repairs viruses within email attachments, including popular compressed file formats, such as: <ul style="list-style-type: none"> - Zip® - MIME/UU - LHA/LZH - TAR 	<ul style="list-style-type: none"> • Provides up-to-date virus protection • Proactively protects users’ system from virus infections • Provides fast response for new threats • Eases the management burden of manually initiating the update process during outbreak situations • Enables administrators to respond to threats quicker and more proactively



Feature	Description	Benefits
	<ul style="list-style-type: none"> - GZIP - ARJ - CAB - LZEXE <ul style="list-style-type: none"> • Content Blocking—Enables administrators to: <ul style="list-style-type: none"> - Block email messages based on subject line, attachment name, and maximum message size - Prevent external sites from bouncing or relaying messages through your customers' mail servers - Detect non-standard MIME messages that contain malicious content - Use any and multiple DNSBL-based blacklist services to stop spam based on source - Customize domain/address block lists to prevent delivery of email messages from specific senders or domains • Up-to-date Protection with LiveUpdate™ <ul style="list-style-type: none"> - Enables administrators to download virus definition updates from Symantec™ Security Response via the Internet during installation and to schedule future, automatic updates to run as often as the organization's security policy requires* - Provides digitally signed and verified virus definition updates to ensure that they have not been altered <p>*A current subscription is required in order to receive antivirus updates and support from Symantec Security Response. One year of Gold Maintenance is bundled with Symantec Mail Security for SMTP 5.0.</p> <ul style="list-style-type: none"> • Action Choices—Lets administrators set policies to handle messages with viruses (i.e., clean and deliver the message, deliver the message normally, or delete the message). • Mass-mailing Worm Auto-deletion—Automatically removes not only the mass-mailing worm but also the associated spawned emails, which can number in the hundreds and serve no valuable purpose. • Variable Scanning Levels—Includes adjustable heuristics for more or less aggressive identification of viruses. 	
<p>Convenient Email Content Control</p>	<p>Content Compliance helps administrators control sensitive email content and enforce content rules to conform to Information Technology (IT), Human Resources (HR), and other regulatory policies.</p> <ul style="list-style-type: none"> • Dictionary Filters enable administrators to define or import a pre-defined dictionary of prohibited words or phrases. This feature assists with HR and regulatory compliance-related issues. 	<ul style="list-style-type: none"> • Makes it easy for organizations to control sensitive email content and enforce content rules to conform to IT, HR, or other regulatory requirements • Provides a



Feature	Description	Benefits
	<ul style="list-style-type: none"> • Content Filter Editor allows administrators to create custom filters using a graphical interface. These global, server-level filters can be used to enforce company policies. Administrators can quickly activate and deactivate individual filters, display their activation status, and organize the order in which rules are run. • Annotations allow administrators to automatically add text to mail, such as a legal disclaimer or commercial information. • Archive automatically sends a copy of a filtered message for a specified category (for example, spam) to a specific administrative account. This allows administrators to review the nature of messages targeting the organization. • Attachment Blocking enables administrators to scan for attachments with specific size or content attributes. Administrators can create filters to block attachments based on file size, true file type, file name, MIME type, or file extension. 	<ul style="list-style-type: none"> • convenient graphical editor
<p>Powerful System Management</p>	<p>Gives administrators control and visibility into their organizations' email security issues via:</p> <ul style="list-style-type: none"> • Web-based Administration lets administrators use a Web browser to view a real-time dashboard of consolidated filtering performance. • Global Management allows administrators to configure, manage, and monitor all scanners, from a central location using a Web browser. • Automated Filter Downloads and Statistics Transfer provides secure HTTPS polling from customer sites that initiates download of updated filters. The same process transmits statistics from customer sites to Symantec, allowing Symantec to gauge the performance and effectiveness of deployed filters. The process requires no administrator intervention and filtering is never stopped during the update process. • Multiple Administrator Accounts let organizations define multiple administrators and assign each specific privileges, allowing them to divide up administrative tasks. 	<ul style="list-style-type: none"> • Reduces administration burden and provides flexibility to meet the organizations' unique needs
<p>Flexible Mail Policies and Administration</p>	<p>Includes the following flexible email management features, designed to support different levels of administrator involvement.</p> <ul style="list-style-type: none"> • Group Policies—Lets administrators specify user groups, identified by email addresses, domain names, or LDAP groups and customize mail filtering for each group. For example, an organization might choose to quarantine spam and suspected spam for review by the legal department but delete spam for the human resources department. • LDAP Synchronization—Allows Symantec Mail 	<ul style="list-style-type: none"> • Lets administrators manage mail security in a way that makes sense for their organizations



Feature	Description	Benefits
	<p>Security for SMTP 5.0 perform one-way LDAP synchronization from existing directory stores, eliminating the need for dual entry of user information. The supported source directories include Windows 2000 Active Directory, Windows 2003 Active Directory, iPlanet/Sun Messaging Server 5.1, Lotus Domino, and Microsoft Exchange 5.5.</p> <ul style="list-style-type: none">• Flexible Actions—Administrators can assign a variety of actions to policies, based on the message verdict.• Adjustable Spam Threshold—Allows configurable definition of suspected spam for more aggressive filtering. Use policies to set up a unique action for messages identified as suspected spam.• Multiple Filtering Categories—Lets messages be classified as one of the following:<ul style="list-style-type: none">- Spam- Suspected spam (matching the adjustable spam scoring range specified)- Email from blocked senders- Emails infected with viruses- Mass-mailing worms- Unscannable emails (could not be scanned due to size restrictions or other variables)- Spyware/Adware- Encrypted- Suspect Virus- Custom-filtered emails (matching content filters created by administrator)• Administrator Web-based Quarantine—Allows administrators to log in and review spam messages that Symantec Mail Security for SMTP 5.0 has quarantined for all users in their organization. Administrators can access quarantine database and configure settings from the Control Center.• User Quarantine Digest—Sends a periodic email summary to users, listing the newly quarantined spam messages. Includes links for users to immediately release messages to their inbox or log in to their personal quarantines.• Alias Expansion—Allows quarantine to automatically resolve all aliases and delivers messages to the appropriate quarantine account for the underlying email address.• Misidentified Message Submission—Automatically sends messages identified by administrator and users as false positives to Symantec for analysis.• Administrator Notification for Submissions—Allows administrators to receive a copy of all	



Feature	Description	Benefits
	<p>misidentified messages sent by users to Symantec.</p> <ul style="list-style-type: none">• Spam Expunging and Size Thresholds—Provides configurable retention period for spam messages. Includes thresholds to control the quarantine database size and the messages number limit on a global and per-user basis.• Quarantine Message Search—Lets users and administrators search messages in quarantine using multiple criteria	
Customizable User Tools	<p>Lets users log into a special section of the Control Center and select appropriate settings. The customizable user features include:</p> <ul style="list-style-type: none">• Allowed/Blocked Senders List—Using either the end user web interface or a plug in for Microsoft Outlook for Notes, users can specify addresses that will always be allowed or blocked. The entries are in addition to organization-wide allowed/blocked lists defined by administrators.• Allowed/Blocked Languages—Users can either specify languages in which they want to receive email or in which they don't want to receive email. Users can choose from 11 supported languages.• Submissions—Users can submit missed spam or false positives to Symantec for analysis.• End User Quarantine—Using an Internet browser, users can log into their personal quarantine at any time and view their quarantined messages.	<ul style="list-style-type: none">• Empowers a user to manage and customize their filtering

System Requirements

Solaris®

Computer	UltraSPARC server
Operating system	Solaris 9 or 10
Memory	1G RAM (2G or more recommended)
Available disk space	512 MB disk space minimum (2 GB or more recommended)

Windows® 2000/2003 Server

Computer	Intel® Pentium® 4 processor or compatible
Operating system	Microsoft® Windows 2000 Server (SP4), Windows Server™ 2003 (SP1), Windows Server™ 2003 Japanese (SP1)
Memory	1G RAM (2G or more recommended)
Available disk space	512 MB disk space minimum (2 GB or more recommended)

Linux Server

Computer	Intel® Pentium® 4 processor or compatible
Operating system	RedHat ES /AS 3.0 (Update 5)
Memory	1G RAM (2G or more recommended)
Available disk space	512 MB disk space minimum (2 GB or more recommended)

LDAP Synchronization

Microsoft Active Directory 2000 and 2003
Sun™ ONE Directory Server
Microsoft® Exchange 5.5
Lotus Domino® 6.5

Spam Folder Agent

Lotus Domino 6.5
Microsoft® Exchange 2000 and 2003

Web Browser

Microsoft® Internet Explorer 6.0

Firefox® 1.5

Licensing, Support and Maintenance

An overview of how this product is licensed, plus available Support and Maintenance can be found in the [Licensing/Support/Entitlement QuickStart](#) for Symantec Mail Security for SMTP 5.0, now available on SCORE.

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec, the Symantec logo, Symantec AntiVirus, Symantec AntiVirus Enterprise Edition, Symantec Brightmail AntiSpam, Symantec Mail Security, Symantec Security Response and LiveUpdate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners.