

Symantec Brightmail AntiSpam™ 6.0: A Product Overview

INSIDE

- › The growing volume of spam
- › Architecture and deployment
- › Powerful spam and email threat protection
- › Administration made simple
- › Conclusion

Table of Contents

Executive summary	1
What's new in version 6.0	1
The growing volume of spam	2
Architecture and deployment	3
Mail flow summary	3
A closer look: the Scanner and Control Center	4
Spam analysis and filter production (the BLOC)	5
Flexible deployment options	5
Powerful spam and email threat protection	7
Multilayered spam prevention	8
Automatic protection against email fraud and phishing	8
Eliminating viruses and mass-mailing worms	9
Building content filters to enforce company policies	9
Administration made simple	10
Centralized Web-based administration	10
Flexible group policies to handle filtered mail	10
Automated filter delivery and deployment	12
Filtering customization	12
Brightmail Reputation Service	13
Multiple quarantine options	13
System monitoring	15
Empowering users	16
Conclusion	17

> Executive summary

As both the volume and the associated costs of spam continue to grow unabated, organizations are demanding more from antispam vendors. In the past, ad hoc solutions were sufficient—until users found themselves buried under a mountain of unsolicited mail. Organizations are turning to vendors that are intensely committed to the antispam space. For antispam products, the bar has been raised; vendors that simply retrofit antispam protection from existing products, such as content filtering or general-purpose messaging, are missing the mark. Companies want a powerful and aggressive antispam solution, yet they have no tolerance for false positives or extensive end-user administration. Solutions should be easy to deploy and administratively simple, yet adaptable to incorporate countermeasures that fight the ever-changing tactics of today's spammers. They must also be able to dynamically adapt to combat emerging email threats such as phishing and email fraud.

This technology brief includes the following topics:

- **The growing volume of spam.** A look at the drivers and the implications of spam.
- **The Symantec Brightmail AntiSpam architecture.** A high-level view of the architecture and deployment options.
- **Powerful antispam and email threat protection.** An overview of the main features of the Symantec Brightmail AntiSpam software.
- **Administration made simple.** A summary of the powerful administrative tools that allow administrators to centrally manage and monitor email filtering.

Symantec Brightmail AntiSpam software protects over 2,500 of the world's leading enterprises, including Avaya, eBay, Bechtel, Booz Allen Hamilton, Cypress Semiconductor, Deutsche Bank, Lucent Technologies, and Terra Lycos. As the most-deployed commercial antispam solution, Symantec Brightmail AntiSpam now protects more than 300 million mailboxes worldwide, including over 5 million enterprise users. These customers count on Symantec for its expertise in spam filtering, its logical and flexible approach to fighting spam at the customer site, and its ongoing commitment to countering spammers' tactics.

> What's new in version 6.0

Here are some of the features that have been added or enhanced in this version:

- **New Web-based administration center.** The Control Center allows administrators to centrally manage all computers running Symantec Brightmail AntiSpam software from a Web browser. In addition to consolidating configuration, reporting, logging, and other tasks, the Control Center now also houses Quarantine.
- **Group policies to manage filtered mail.** You can now customize mail handling and per-verdict actions for groups of users, identified by email addresses or domain names.
- **Improved filtering technologies.** Among the filtering enhancements are the incorporation of the Brightmail Reputation Service™ for accurate sender-based filtering, added defenses against non-English spam, new attachment signatures to capture images and other embedded content, and updated URL filters.
- **Other enhancements.** This version provides even more preset reports (now separated by spam and virus), new non-English language identification abilities, additional features for the Brightmail Plug-In for Outlook, and much more.

> The growing volume of spam

The growth trend of spam shows no sign of abating. The chief reasons for the growth of spam in the enterprise are:

- **The increasing dependence on email.** As the primary form of business communication, email has become mission-critical in the enterprise. Spammers have a captive audience.
- **The economics of spam.** Processing, bandwidth, email address acquisition, and email software costs continue to fall: spammers need only capture a small response rate to make a profit.
- **The adaptability of spammers.** The attractive economics of the spam business, together with the technical ability and ingenuity of spammers, is a potent combination.

This increase in both the volume and percentage of spam and other email threats not only drains IT resources and business productivity, it also affects how end users view email and antispam filtering. As shown in Figure 1, antispam solutions need to block a correspondingly larger percentage of spam to reduce the actual number of spam email users receive.

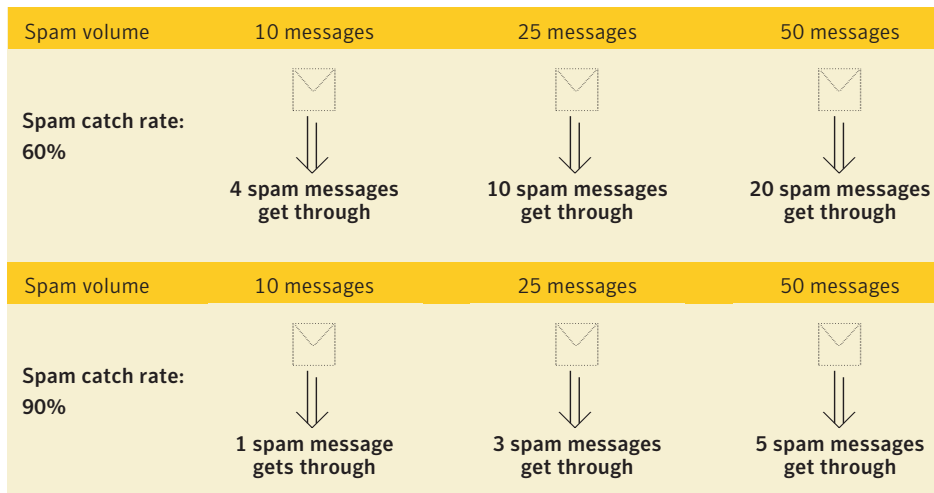


Figure 1. Antispam effectiveness

The best antispam solutions have:

- The highest possible effectiveness rate in order to compensate for the escalating volume of spam
- The lowest possible false positive rate
- Low to zero administration

> Architecture and deployment

The power of Symantec Brightmail AntiSpam begins with its architecture: client/server filtering software backed by Symantec's global email research, threat detection, and filter production operations.

Working in popular enterprise environments and operating systems, including Windows®, Linux, and Solaris™, Symantec Brightmail AntiSpam does not rely on a custom mail transfer agent (MTA). Instead, Symantec Brightmail AntiSpam works across multiple mail servers—such as Exchange and Sendmail—and does not disrupt current systems. Administrators benefit from this architectural decision in many ways:

- **Integration.** The integration of filtering software with existing, well-known messaging systems—in lieu of “reinventing the wheel” with proprietary SMTP services—allows Symantec to focus its best technical resources on optimizing antispam protection. The architecture also produces cost savings in infrastructure and training by using familiar MTAs.
- **Failover.** In addition to failing over to multiple filtering servers—in the unlikely event that the antispam protection momentarily fails—the email server can still deliver mail.
- **Scalability.** Leveraging best-of-breed messaging technologies supports scalability—Symantec Brightmail AntiSpam easily scales to millions of mailboxes. And because Symantec Brightmail AntiSpam is not licensed on a per-server basis, you can add as many servers as needed.

This section takes a closer look at the architecture and deployment possibilities for Symantec Brightmail AntiSpam. It also covers the two unique services managed by Symantec: the Probe Network™ and the BLOC™ (Brightmail Logistics and Operations Center).

Mail flow summary

As mail flows into your mail servers, Symantec Brightmail AntiSpam software running at your site analyzes and filters mail using a variety of techniques, incorporating up-to-the-minute filters from the BLOC.

Along with standard methods such as heuristics and pattern matching, Symantec Brightmail AntiSpam incorporates many proprietary filtering methods, such as advanced signature technologies and reputation-based source filters. Filters are continuously and automatically refreshed by the BLOC to combat the latest spam and other email threats. Administrators can set up centralized policies to perform a variety of actions based on the verdict assigned to each message. For example, administrators can immediately delete spam identified by Symantec Brightmail AntiSpam or choose to route spam to a central Web-based quarantine for a specific set of users.

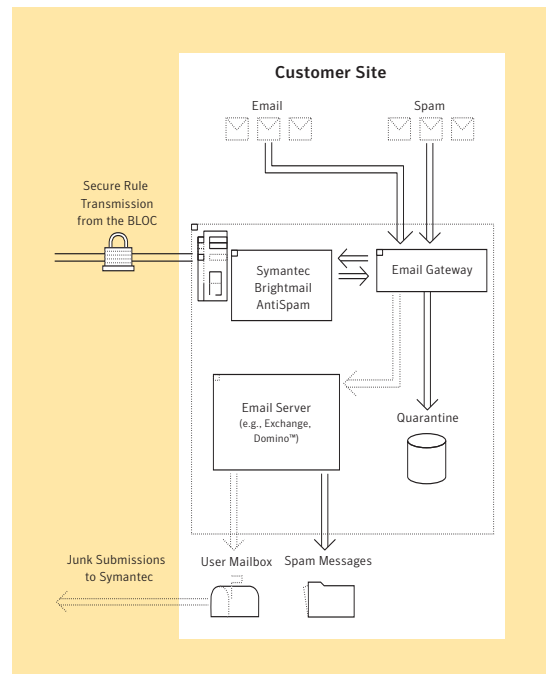


Figure 2. Symantec Brightmail AntiSpam at your site

A closer look: the Scanner and Control Center

Two key software components power Symantec Brightmail AntiSpam:

- **Scanner component.** Performs email filtering. You can have one or many Scanners in your Symantec Brightmail AntiSpam installation.
- **Control Center.** Enables Web-based configuration and administration. With a single Control Center, you centrally configure, monitor, and manage all the Scanners in your network. The Control Center contains Quarantine, an optional storage area for caught spam.

These components can reside on the same computer, or they can be balanced across different machines to meet your mail flow and performance needs.

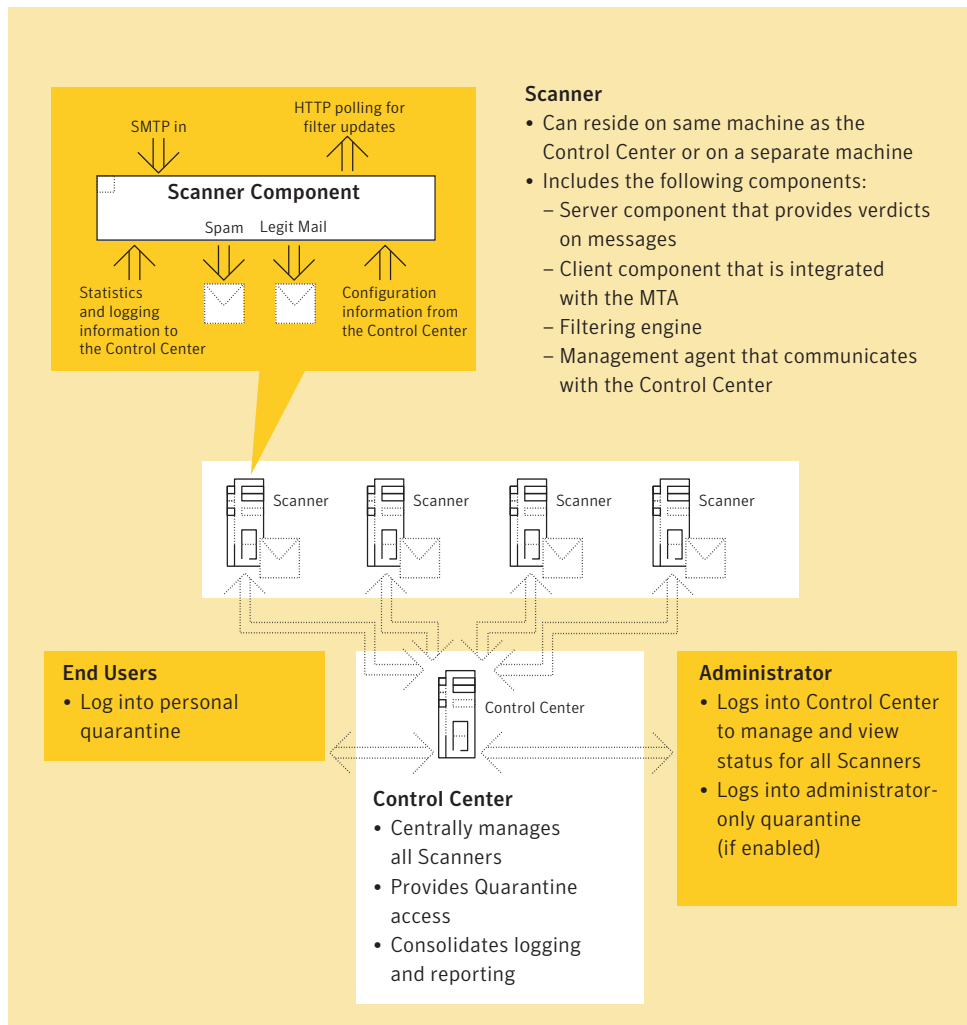


Figure 3. Scanner and Control Center software components

Spam analysis and filter production (the BLOC)

To defend against the constantly changing tactics of spammers, Symantec staffs 24x7 spam-fighting operations centers in North America, Europe, and Asia. Collectively known as the BLOC, these distributed spam-fighting facilities are key components of the Symantec Brightmail AntiSpam architecture.

A prime responsibility of the BLOC is management of the Probe Network, an extensive array of over 2 million decoy email addresses, also known as spamtraps or honeypots. This patented global network of email accounts attracts and collects large quantities of spam—tens of millions of spam messages pass through the Probe Network every day. Symantec uses these decoys to stay current with the very latest spamming tactics.

Messages flow directly from the Probe Network to the BLOC for analysis. Then, sophisticated tools and automated processes go into action, analyzing incoming spam and developing effective countermeasures. The BLOC also develops and tunes other more proactive filters, such as heuristic-based filters. Such filters, which examine characteristics and behaviors that are unique to spam messages, are effective against spam that has not flowed into the Probe Network. Approximately every 10 minutes, antispam filters are pulled down over a secure connection to the Scanners, where the filters are immediately put into action.

The Symantec Brightmail AntiSpam architecture represents a constant feedback loop, starting and ending with your site:

1. The installed Scanner executes filters based on real-time information from the Probe Network and the BLOC.
2. The Scanner constantly reports back to the BLOC regarding the effectiveness of deployed filters. If necessary, adjustments are made in real time to improve effectiveness.
3. Using their email clients, users at your site can choose to easily submit missed spam messages to Symantec, increasing the breadth and reach of the Probe Network with the click of a button.

Some Facts About the BLOC	
• Spam defense coverage:	24x7
• Languages spoken:	12
• Decoy accounts monitored:	Over 2 million
• Decoy (honeypot) spam processed/day:	Tens of millions
• Countries represented by the Probe Network:	Over 20
• Operations center locations:	San Francisco Dublin Sydney Taipei

Flexible deployment options

Symantec Brightmail AntiSpam supports a variety of on-site deployment options, based on your mail infrastructure, total mailboxes, and the available messaging expertise. As shown in Figure 4, Symantec Brightmail AntiSpam is usually set up in the following locations:

- **At the gateway or perimeter.** Symantec Brightmail AntiSpam resides at the outermost gateway layer. This layer contains the gateway MTA, which processes inbound mail and relays it to other relay layers or to the user-facing message store layer.
- **At a post-gateway or internal relay layer.** MTAs at the gateway layer accept mail from the Internet and relay unfiltered mail to the MTA that is integrated with Symantec Brightmail AntiSpam software. The Scanner filters mail from the gateway layer and relays mail to other MTAs downstream.
- **At the native email server.** Symantec Brightmail AntiSpam integrates with the internal mail server, at the last node in any relay chain.

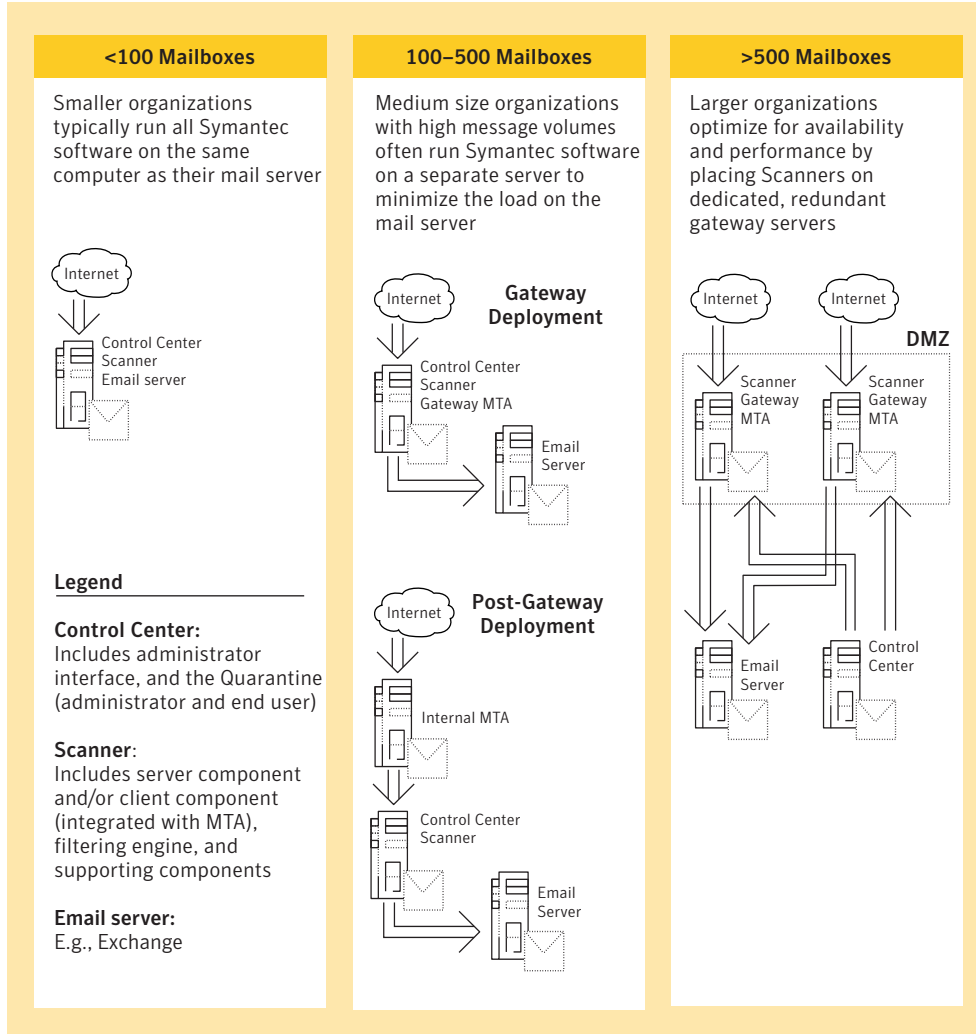


Figure 4. Sample deployment scenarios

Although most customers prefer the control, security, and privacy benefits inherent in deploying Symantec software on-site, the Powered by Symantec program allows you to consider other form factors for Symantec software. Table 1 summarizes the advantages and considerations regarding the available deployment options.

Table 1. Symantec Brightmail AntiSpam deployment options

Deployment	Advantages	Considerations
Gateway	<ul style="list-style-type: none"> • Fights spam at the point of entry. Because spam emanates from the outside world, the gateway is the logical and effective place to deploy the Scanner. • Saves resources. By deploying closer to the gateway, you catch spam before it travels through the internal network and consumes bandwidth and storage. 	<ul style="list-style-type: none"> • Some organizations prefer to have secure gateways with no other services running. In these environments, all other services (including antispam) run behind the first gateway layer. • Some smaller organizations do not have dedicated gateway servers or a gateway layer. Instead, they deploy gateway servers and internal mail servers on the same machine.
Post-gateway relay	<ul style="list-style-type: none"> • Reduced downtime. From an architecture perspective, this method often requires the least amount of downtime. Administrators can build the system, test it, and when it's ready, plug it into production. • Multiple services on one machine. This is an efficient way to deploy Symantec Brightmail AntiSpam in a multilayered scenario on one box. For example, you can easily run antispam, antivirus, and other services on one physical machine. 	<ul style="list-style-type: none"> • Ensure that there are enough available resources on the post-gateway computer if it is running other services (e.g., antivirus, content filtering).
Email server	<ul style="list-style-type: none"> • Integrated solution. This option is ideal for smaller customers that cannot deploy new servers. • Plug-and-play. If you run Microsoft® Exchange as your internal mail server, this option requires no configuration changes to SMTP. 	<ul style="list-style-type: none"> • If you are running multiple mail servers, you will need to install multiple instances of the Scanner.
Hosted Solutions (Powered by Symantec)	Symantec's hosted partners incorporate Symantec Brightmail AntiSpam in their messaging solutions and services for email security and boundary protection. Advantages of hosted management of email include possible cost savings, access to guaranteed service levels, as well as expert help with problematic messaging issues. Outsourcing email can be a good choice for small businesses or other organizations without in-house messaging expertise and resources.	
Appliance Solutions (Powered by Symantec)	Symantec's appliance partners integrate Symantec Brightmail AntiSpam in self-contained gateway hardware products that you install at your site. These appliances are preconfigured with the necessary operating system and application software. An appliance-based solution can save your organization some of the costs associated with server administration, hardware purchases, operating system licensing, and software integration.	

> Powerful spam and email threat protection

Symantec Brightmail AntiSpam provides protection against the following broad categories of email threats:

- **Spam.** Leveraging Symantec's expertise in developing accurate and effective filters, the primary level of antispam protection comes in the form of targeted filters disseminated by the BLOC.
- **Malicious content.** This category includes viruses, mass-mailing worms, and the burgeoning threat of email fraud. Symantec provides specific countermeasures for content of this type.
- **Other categories.** Some sites need to extend filtering to enforce company-specific policies, for example, limiting the attachment sizes for incoming mail. The Custom Filters Editor provides an easy way to create such special-purpose content filters.

Multilayered spam prevention

To keep up with the latest spam attacks, the BLOC employs automated filter creation tools and delivery technologies, delivering updated filters to Scanners approximately every 10 minutes.

As Figure 5 shows, the filters managed by Symantec are only a part of a larger arsenal of filters, including optional filters and lists maintained by administrators and end users. Such an antispam combination is necessary because complex spam attacks require multiple targeted filters and approaches. Different techniques are effective against different types of spam.

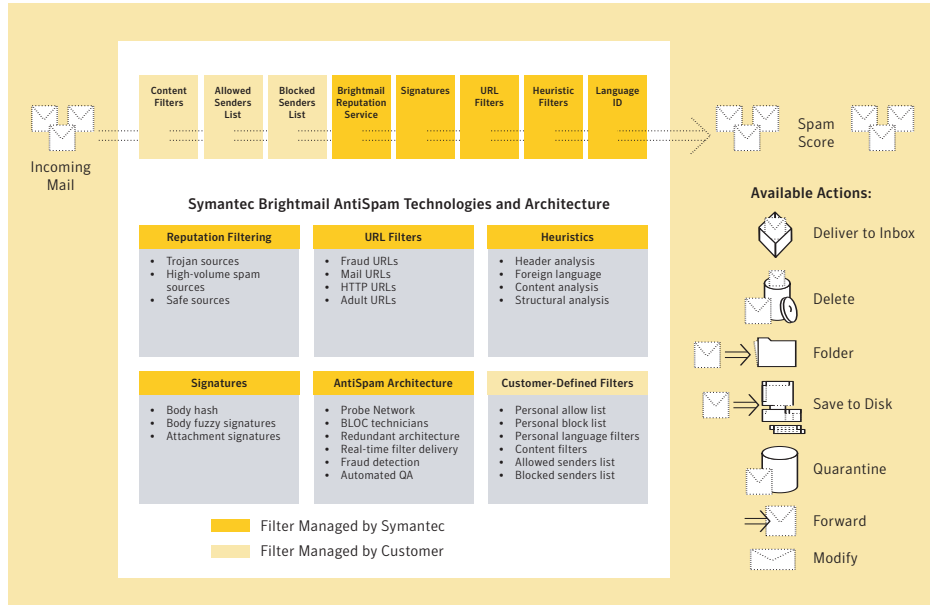


Figure 5. Multiple antispam technologies

Automatic protection against email fraud and phishing

Fraudulent email messages—a dangerous new form of spam attacks—are messages that appear to be sent from a legitimate company’s Web site or domain address, but in fact are not. In reality, spammers are hijacking the company’s brand to attract the attention of customers and potential customers, often to gain personal information (i.e., phishing). Figure 6 shows the number of fraudulent emails filtered by Symantec.

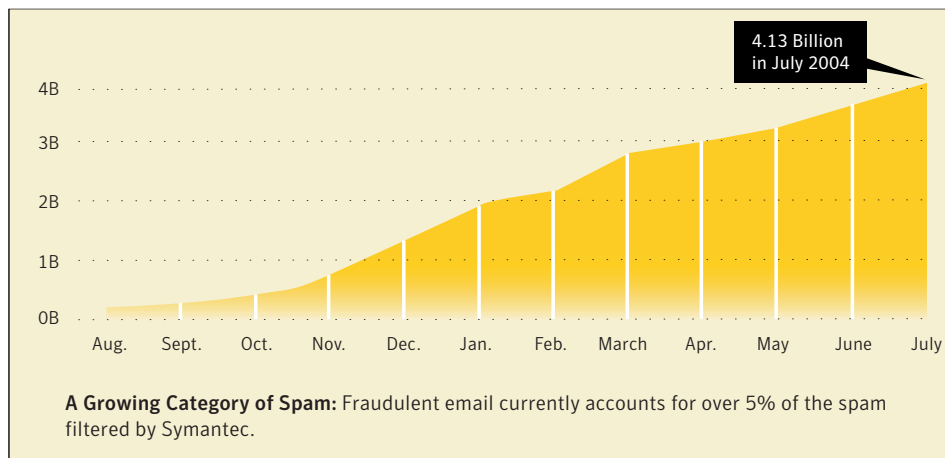


Figure 6. Number of fraudulent emails filtered by Symantec

Because Symantec sees more than 20% of the world’s email traffic and filters over 104 billion email messages every month, it is in a unique position to monitor the Internet for email fraud targeting companies worldwide. Leveraging this detection network, Symantec produces timely antifraud and anti-phishing filters. These filters are automatically incorporated into Symantec Brightmail AntiSpam, ensuring that your end users do not receive these messages.

Eliminating viruses and mass-mailing worms

The Scanners can optionally filter the attachments of incoming email in search of viruses and can clean infected mail. If enabled, antivirus filtering is the first filtering process performed. If no viruses are detected, the message is passed on for spam and other filtering. Upon detection of viruses, the policies you have specified go into effect. For example, the message could be deleted or it could be cleaned and delivered to the recipient’s inbox.

Virus filtering through Symantec Brightmail AntiSpam also provides an important defense against mass-mailing worms, a general class of viruses that use email to propagate. Depending on the payload and the variant, these worms often leave hundreds of spam messages in their wake. The Worm Auto-Delete feature automatically removes not only the worm but also the associated emails. This convenient feature saves users from potentially having to wade through hundreds of inbox messages that, although clean from viruses, serve no valuable purpose.

Table 2. Benefits of deploying antivirus protection

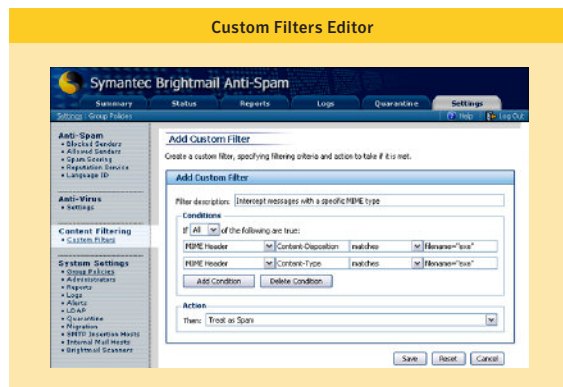
Antivirus Feature	Benefit
Flexible, responsive, and effective antivirus technology	<ul style="list-style-type: none"> Delivers virus definition and engine updates from Symantec as soon as they are available 24x7 monitoring Ensures high level of protection against ever-changing threats
Advanced filtering and analysis	<ul style="list-style-type: none"> Employs heuristics to catch undiscovered viruses Decomposes messages down to multiple levels
Robust and scalable architecture	<ul style="list-style-type: none"> Supports email networks of any size (regional to international) Avoids impeding message traffic by cleaning messages offline Can be placed as a relay in front of your email system
Ease of administration	<ul style="list-style-type: none"> Provides statistics showing the number and percentage of viruses caught

Building content filters to enforce company policies

While most administrators never need to write filters to augment filters created by Symantec, the graphical Custom Filters Editor provides an easy way to create global, server-level filters that:

- Filter email from marketing lists that generate user complaints or use up excessive bandwidth
- Filter out oversized messages
- Block specific types of adult content
- Block chain letters

As with other spam and suspected spam verdicts, administrators can specify how the Scanner treats messages that are filtered by the content filters.



> Administration made simple

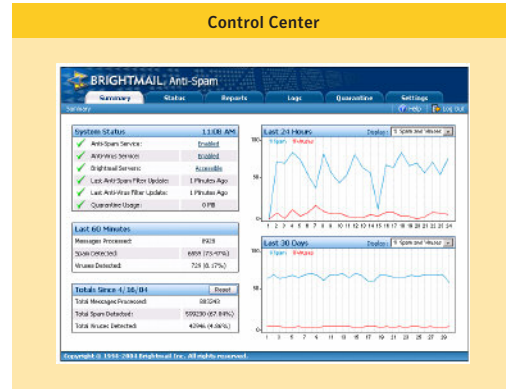
Symantec Brightmail AntiSpam provides the following features that support easy administration:

- Centralized Web-based administration
- Group policies to manage filtered mail
- Automated filter delivery and deployment
- Filtering customization
- Multiple quarantine choices
- System monitoring

Centralized Web-based administration

Symantec Brightmail AntiSpam features the Control Center, a cross-platform, Web-based interface that centralizes all administrative tasks.

The Control Center lets you view information on system status, administer the Quarantine, modify settings for all Scanners and other components, configure event-based alerts, and more—all from one intuitive interface. Other key features are:



- **Consolidated reporting and logging.** To view aggregate reports, filtering summaries, and log information from all your Scanners.
- **Role-based administration.** To balance administration tasks, you can create additional administrator accounts, granting each administrator the desired level of management privileges for different components of Symantec Brightmail AntiSpam. For example, you might want to delegate management of Quarantine to another administrator, who will only be able to view and modify Quarantine settings.

Flexible group policies to handle filtered mail

Symantec Brightmail AntiSpam provides a wide variety of actions for different categories of filtered email. For example, you can delete messages identified as spam by Symantec and quarantine suspected spam. Although you can set identical options for all users, different groups in your organization may have unique filtering needs. Figure 7 demonstrates how group policies let you align specific handling options with arbitrary groups that you define.

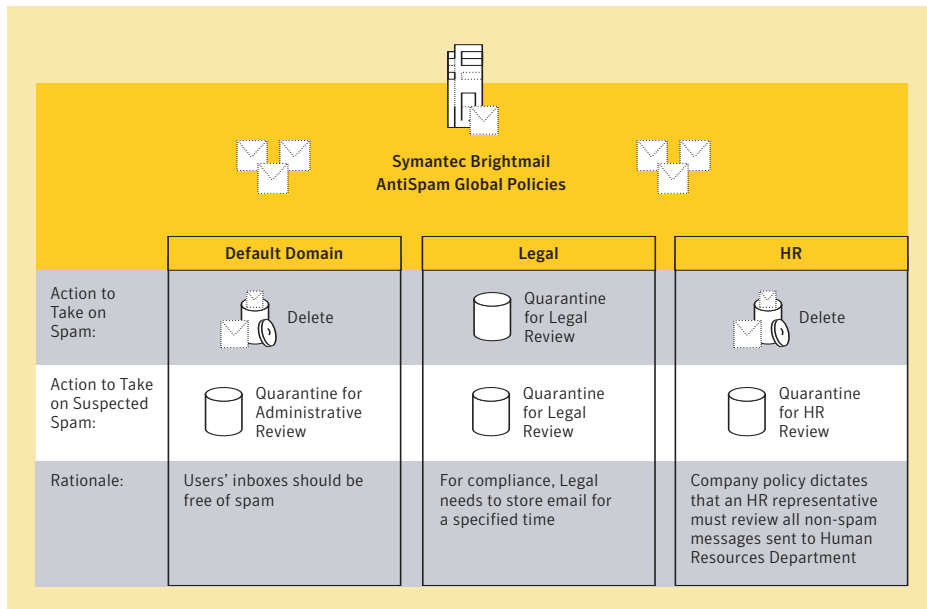


Figure 7. Different filtering policies for different groups

Administrators can specify groups of users based on email addresses or domain names. For each group, administrators can specify email filtering actions for various categories of email (see Table 3).

Table 3. Message categories identified by Symantec Brightmail AntiSpam

Category	Message characteristics
Spam	Identified as spam based on antispam filters designed by Symantec
Suspected spam	Scored in the suspected spam range you configure
Email from blocked senders	Matched against the domain names, IP addresses, or third-party lists queries specified in your Blocked Senders List
Viruses	Virus-infected emails
Mass-mailing worms	Emails that result from mass-mailing worm attacks
Unscannable emails	Could not be scanned due to size restrictions or other variables
Custom-filtered emails	Matched against content filters created by the administrator

Table 4. Actions available for filtered email

Available action	The message is...	Benefits/notes
Clean the message	Cleaned of viruses and delivered to the recipient. Any worms are deleted.	Applies to messages classified as viruses.
Notify recipient of unscannable reason	Cleaned of viruses and delivered to the recipient. Any worms are deleted.	Applies to messages that are large or suspicious enough that filtering is not recommended.
Delete the message	Removed from email stream, discarded. Worms automatically deleted.	No administration or handling is necessary. For spam verdicts, "filtering and dropping" takes advantage of the Symantec Brightmail AntiSpam 99.9999% accuracy rate. ¹
Deliver the message normally	Delivered to recipient's inbox.	Useful for testing purposes. Reports and statistics reflecting spam volume can still be generated.
Deliver to recipient's spam folder	Moves message, using a server-side rule, to a designated folder in the user's Exchange or Domino mailbox.	Relieves end users and administrators of the burden of using email clients to create filters.
Forward	Sends message to a single administrative account for further scrutiny.	Allows administrators to review the nature of spam messages targeting your organization using a familiar email client (e.g., Microsoft Outlook).
Modify the message	Adds a configurable X-header or tags the subject line on a message, for example, X-spam or X-newsletter.	Enables user to create simple client-side filters to handle messages Symantec Brightmail AntiSpam has processed.
Quarantine	The message is sent to the Brightmail Quarantine.	Provides visibility into the spam targeting your organization and assures users that no legitimate mail is lost.
Save to disk	Reroutes message to a specified location on an administrative system.	Enables purging of messages at the discretion of the administrator.

Administrators can easily assign policies for groups that they have defined. Symantec Brightmail AntiSpam supports unlimited numbers of groups of users based on email addresses or domain names (wildcards permitted). Each defined group can have unique email-filtering actions, based on the seven categories of email defined previously. The policies feature also includes support for importing group members from a text file.

¹"Anti-Spam Services for SMBs and Middle-Market End-Users," February 25, 2003
Research Note by J.P. Gownder of the Yankee Group

Automated filter delivery and deployment

Symantec Brightmail AntiSpam provides a secure transmission process, ensuring that Scanners at customer sites always have current antispam filters. Every minute, on-site Scanners initiate a secure HTTPS connection with the BLOC. Using this pull-based connection, filter updates flow from the BLOC to the Scanners. Using a similar mechanism, filtering statistics from customer sites are transmitted to the BLOC, allowing the BLOC to gauge the performance and effectiveness of deployed filters.

This transmission process has many advantages:

- **Easy administration.** Unless they choose to augment antispam filters using the Custom Filters Editor, administrators need never manually write, train, or update existing filters.
- **Up-to-date protection.** The Scanners always have the most current antispam filters, and the BLOC has constant visibility into how effectively those filters are performing.
- **Security and privacy.** Two-way validation guarantees that filters are coming from Symantec and cannot be “spoofed” by any other entity. Also, no confidential customer information is transmitted during the collection of the package of aggregate statistics. The sole piece of customer-specific data sent back to Symantec is the originating IP address for each message. Symantec aggregates these IP addresses to proactively identify open relays and open proxies (relaying through another server allows spammers to anonymously disseminate mail).
- **Availability.** The filtering software is never stopped during the update process. This capability prevents messages from getting through during the update process, which would leave the mail server unprotected. Once the new filtering rules are loaded, Symantec Brightmail AntiSpam immediately switches over to the new filters.

Filtering customization

Armed with a constant flow of updated and targeted filters from Symantec, administrators never need to perform ongoing tuning. For more flexibility and control, the Control Center provides methods to modify and customize standard filtering.

ADJUSTING SPAM SCORING FOR MORE AGGRESSIVE FILTERING

When evaluating messages for spam, Symantec software applies thousands of filters in order to arrive at an overall spam score for each message. To maintain its high accuracy, by default the Scanner sets this threshold value quite high. Some administrators, however, want to tailor the software to reflect the spam tolerance levels of their organization. For example, they may want to be more aggressive in identifying messages that cross a certain threshold. Administrators can specify a range of spam scores that will be considered suspected spam, which is differentiated from legitimate mail and spam.

Among the three mutually exclusive classes of messages, suspected spam refers to a “gray area” of messages that are suspiciously similar to spam, but also share some traits with legitimate messages. After administrators specify a threshold value for their site, the spam score for each message is compared to the threshold value configured for each level. Any messages with scores below the configured suspected spam range will be considered legitimate; any messages above will be considered suspected spam.

The key benefit of adjusting the spam scoring is that, using policies, administrators can specify different actions for suspected spam. For example, for a given group of recipients, administrators can choose to delete spam messages and quarantine suspected spam messages for review. Specifying different actions is a good way to handle the possible false positives that may arise from lowering the spam threshold bar.

TAILORING ACCURACY AND EFFECTIVENESS: ALLOWED AND BLOCKED SENDERS LISTS

In some cases, filtering based on the content of the message isn't needed. For example, administrators might want mail from trusted senders or business contacts to always be delivered, regardless of the spam-like nature of the message. Likewise, messages from senders or IP addresses known to send spam or unwanted mail should be treated as spam. In these and other cases, filtering based on the source or sender of the message is a very effective way to deal with spam and minimize false positives unique to your organization.

Using a simple interface, administrators can customize the filtering provided by Symantec by:

- **Defining an allowed senders list.** Mail coming from an address or connection in an organization's allowed senders list is always treated as legitimate mail. As a result, such mail is delivered immediately to the recipient's inbox, bypassing any other filtering (except antivirus).
- **Defining a blocked senders list.** Administrators can specify how Symantec Brightmail AntiSpam processes mail coming from an address or connection in an organization's blocked senders list. A variety of actions can be performed on such mail, including deletion, forwarding, and others.

Senders can be specified using the following criteria:

- Email addresses and domain names
- Individual IP connections specified by the administrator
- IP connections and network information obtained from third-party lists

Brightmail Reputation Service

Although Symantec Brightmail AntiSpam can query third-party lists of desirable or undesirable domains, IP connections, and networks, the recommended approach is to use the Brightmail Reputation Service.

The Brightmail Reputation Service monitors hundreds of thousands of email sources to determine how much email sent from those addresses is legitimate and how much is spam. This data-driven process provides enough evidence so that mail from a given email source can be blocked, allowed, or treated as suspicious based on the source's reputation value. The service is enabled by default and currently includes the following lists of IP addresses:

- **Open Proxy List.** IP addresses that are open proxies used by spammers.
- **Safe List.** IP addresses from which virtually no outgoing email is spam.
- **Suspect List.** IP addresses from which virtually all of the outgoing email is spam.

The lists are continuously compiled, updated, and incorporated by Scanners in the same manner as other filter updates.

Multiple quarantine options

Symantec Brightmail AntiSpam provides a number of quarantine options for dealing with spam and messages filtered by the Scanner:

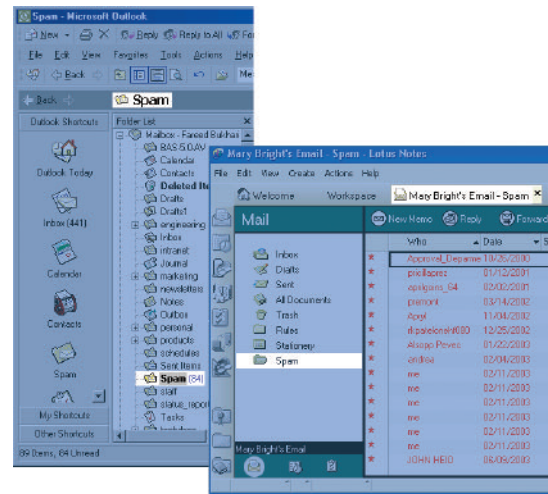
- **Email client-based quarantine.** Software plug-ins and agents work in concert with Microsoft Outlook and Lotus® Domino™ to create user quarantines integrated within the email clients.
- **Web-based quarantine.** The Quarantine component provides both user and administrator quarantines. Users can log in over the Web to review their spam. Administrators can manage Quarantine centrally.

EMAIL CLIENT-BASED QUARANTINES

Using plug-ins available for Microsoft Outlook and Lotus Domino, you can ensure that appropriate messages are automatically directed into each recipient’s spam folder, creating an easy-to-manage quarantine for messages identified as spam. By periodically reviewing their personal quarantines, recipients can verify that no legitimate mail was erroneously sidelined. In the unlikely event of a false positive, recipients can provide feedback that will be examined by the BLOC, enabling incremental improvements to the accuracy of the Symantec filters.

This quarantine feature provides the following benefits:

- No need to install and manage client-side antispam software for each employee
- No need to install separate Scanners onto each email server—only the lightweight agent
- No need for users to write their own client-side filters to folder spam
- No separate login or interface; users can view their quarantine from their mail client



WEB-BASED QUARANTINE

Quarantine is a storage area for messages filtered by Symantec Brightmail AntiSpam. Using a standard Web browser, users can log in and review spam messages that the Symantec software has quarantined for them. Administrators can access Quarantine and configure settings from the Control Center.

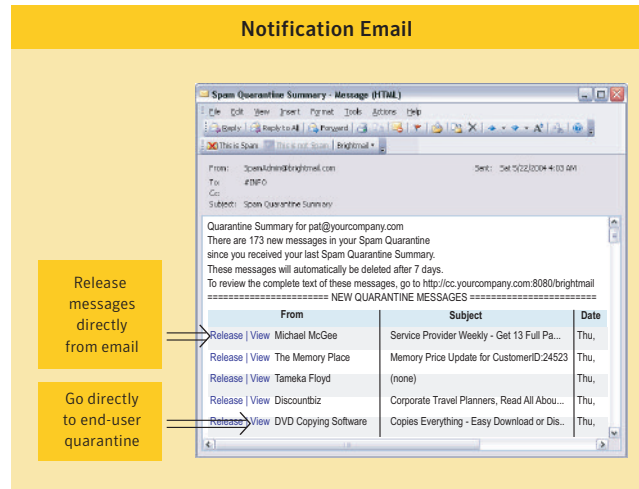
Quarantine is installed on the same computer as the Control Center. Organizations deploying Quarantine enjoy the following benefits:

- **Increased user confidence.** Viewing caught spam in a central quarantine shows your users the success of your filtering measures. Initially, end users prefer to see messages that have been filtered to assure themselves that no legitimate email is lost. As they become familiar with product’s accuracy, users will become confident that legitimate mail is rarely, if ever, quarantined. In the case of a false positive, or if users ever decide to keep a message, they can recover it with a few clicks.



Figure 8. Web-based quarantine

- **Centralized and simple administration.** After initial customization, which includes specifying the retention period for messages and other settings, you don't need to manage Quarantine. In the case of false positives, although you can review false positive submissions, there is no intervention required to get the necessary information to Symantec for incremental filter improvements.
- **Reduced loads on internal mail servers.** Downstream mail delivery, storage, and internal network traffic resources are decreased because quarantined spam is stopped before hitting the mail servers.
- **Automatic notification for users.** Although users can access their personal quarantine at any time, you can configure Quarantine to send an email summary at specific intervals. The summary lists the newly quarantined spam messages and provides links for users to immediately release messages to their inbox or to log in to their personal quarantine and view messages. This notification feature allows users to handle spam quickly and efficiently, rather than dealing with it on a daily or hourly basis.
- **Improved visibility into your spam problem.** Administrators have access to all quarantined messages and false positive submissions. The included search feature lets administrators perform quick queries and further examine the spam that is targeting your organization.



System monitoring

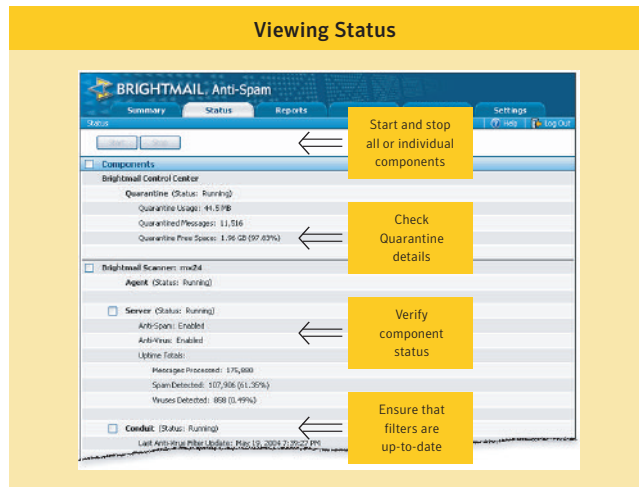
To make system monitoring easier, Symantec Brightmail AntiSpam provides tools to let administrators:

- View status of all Scanners in your network
- Produce detailed reports summarizing spam and virus filtering
- Examine logs
- Set up event-based alerts

VIEWING STATUS

You can easily view detailed status for all your configured Scanners and for Quarantine from one central location on the Control Center. The Status page lists:

- Quarantine information (if applicable)
- The configured Scanners in your network, along with any associated components
- The basic status (running or not) of the configured hosts and components.



DETAILED REPORTS

Symantec Brightmail AntiSpam provides 19 reports summarizing detailed statistics of antispam or antivirus effectiveness at your site. Reporting data provides administrators with key metrics to show the value of Symantec Brightmail AntiSpam as a filtering solution at their site. They can also leverage the collected statistics and spam trend information to help plan for the ongoing storage and resource needs for Symantec Brightmail AntiSpam.

The reports provide the following features:

- **Granular reporting.** Create lists of the most spammed users, most abusive senders, and other reports. Armed with this information, administrators can take proactive measures, such as blocking specific domains and educating employees on how to avoid spam.

- **Consolidated statistics in local time.** Analyze consolidated filtering performance for all Scanners and investigate spam and virus attacks targeting your organization. Regardless of where the Scanners are deployed, reporting data is conveniently presented in the local time zone where the Control Center is located.
- **Export.** Export report data for use in any reporting or spreadsheet software for further analysis.
- **Flexible generation and delivery.** Schedule reports to be emailed at specified intervals.

COMPREHENSIVE LOGS

Each Scanner maintains a database of log information. These logs are all consolidated for viewing within the Control Center. Logging helps diagnose error conditions and keep track of many aspects of the system during its operation.

Logging levels can be set on a five-point sliding scale, and the settings can apply to individual Symantec Brightmail AntiSpam computers or to all. Log filters can also be set at the component level. For example, administrators might choose to log severe errors only for the server component. Administrators can also designate the maximum size and retention period for entries in the log database and save logs to a text file for further review.

PROACTIVE ALERTS

Symantec Brightmail AntiSpam generates alerts when certain operating conditions arise. Symantec Brightmail AntiSpam can automatically send email alerts to administrators or other parties when the following conditions arise:

- A component is not responding or working
- Antispam filters are older than a specified time
- Antivirus filters are older than a specified time
- Quarantine is low on disk space

> Empowering users

Symantec Brightmail AntiSpam enables end users to manage spam on the desktop. User involvement is important to address that final percentage of spam that cannot be addressed adequately on a global basis.

Optional plug-ins and agents, available for popular email clients, empower users to take control of their inboxes.

The Brightmail Plug-In for Outlook is now in its second generation. From a convenient Outlook toolbar, your users can:

- **Create a personal Blocked Senders List.** Users can specify addresses that will always be blocked. While this is unlikely to be effective against professional spammers, who constantly spoof and change their addresses and domains, this approach can be used to block unwanted newsletters or annoying senders. These entries are in addition to those defined by administrators using the Control Center.
- **Create a personal trusted senders list.** Trusted-sender lists let users designate senders who are allowed to bypass antispam filtering. These lists reduce the number of false positives and are a good approach to dealing with legitimate bulk mail or email subscriptions that can look like spam.
- **Specify language preference.** To ward off the growing problem of multilingual spam, users can either specify languages in which they want to receive email or in which they don't want to receive email. All others will be blocked.
- **Automatically import Outlook data.** The plug-in interacts with the Outlook address book and message submissions. The plug-in can automatically compile a list of trusted senders from saved mail and the Outlook contact list.

- **Report false positives and missed spam.** Symantec Brightmail AntiSpam can sometimes miss spam or, in rare instances, produce a false positive. In these circumstances, the plug-in provides a simple way for your users to notify Symantec about the problem—with no administrator action required. Users can immediately submit missed spam or false positives to Symantec for analysis. If appropriate, Symantec will adjust filters to make Symantec Brightmail AntiSpam more effective and accurate.

Symantec also includes a similar mechanism for Lotus Notes® and Domino users. Using a special menu, Domino users can submit misidentified messages to Symantec.

Deployment of the plug-in and other end-user software provides important benefits to the Symantec customer base at large. The distributed submission mechanism greatly increases the reach of the Probe Network, and also gives Symantec continuous visibility into the latest trends and tactics used by spammers. If necessary, Symantec feeds new information from plug-in submissions back into its filter creation, which ultimately increases the antispam protection of all customers.

> Conclusion

Accounting for over half of all Internet mail traffic, the volume of spam continues to grow. Organizations can no longer afford to ignore the flood of spam targeting their servers and employees. The costs in terms of lost IT resources, employee productivity, and legal liability are simply too great. Spam protection is no longer an option—it's a necessity.

Symantec Brightmail AntiSpam, a comprehensive antispam solution that currently protects over 300 million mailboxes, outpaces the competition on many dimensions, including effectiveness, accuracy, and ease of use. Symantec Brightmail AntiSpam provides:

- **Multilayered spam protection.** With over 17 filtering technologies, it catches more spam while allowing legitimate email to reach end users.
- **Flexible spam management and mail policies.** Armed with powerful tools, policies to handle filtered mail, multiple quarantines, and other manageability aids, the administrator can easily customize Symantec Brightmail AntiSpam to meet the unique email requirements of end users and groups in the organization.
- **Powerful administration.** An intuitive Web-based Control Center reduces administrator time and effort required to deploy email policies and oversee the system.
- **Detailed reporting.** Comprehensive reports provide consolidated data on mail flow and filtering activities, giving administrators and managers visibility into how the system is delivering on its business function.
- **Content filtering abilities.** Flexible block/allow lists and a powerful content filtering editor enables administrators to revise or expand the definition of “unwanted” email to match the changing requirements of the organization.
- **Per-user spam control.** Plug-ins and other tools augment popular email clients, enabling end users to take control of their inboxes. For example, users can set up personal allow and block lists, or specify the language in which they want to receive mail.
- **Comprehensive threat protection.** Optional antivirus protection and automatic antifraud filters mitigate the risk of other email threats, including email-borne viruses and phishing.

For more information, visit <http://enterprisesecurity.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 35 countries.
For specific country
offices and contact numbers
please visit our Web site.