



Symantec Brightmail AntiSpam™ 6.0 Evaluation Guide

INSIDE

- › Executive summary
- › What's new?
- › Evaluating email security solutions
- › Running a live evaluation
- › Feature checklist
- › Conclusion

Table of Contents

| | |
|--|----|
| Executive summary | 1 |
| What's new? | 1 |
| Brightmail Control Center | 1 |
| Centralized administration | 2 |
| Group policies | 2 |
| Improved reporting | 2 |
| Improved filtering technologies | 2 |
| Integrated Brightmail Reputation Service | 2 |
| Improved quarantine management | 2 |
| End-user enhancements | 2 |
| Evaluating email security solutions | 3 |
| Building your evaluation criteria | 3 |
| Sample score card | 5 |
| Running a live evaluation | 8 |
| Live evaluation types | 8 |
| Your definition of spam | 8 |
| Best practices | 9 |
| Evaluation checklist | 10 |
| Feature checklist | 11 |
| Antispam engine | 11 |
| Antivirus | 12 |
| Content filtering | 12 |
| End-user features | 13 |
| Mail management | 13 |
| System management | 15 |
| MTA integration | 15 |
| Conclusion | 16 |

> Executive summary

Today, more than 300 million email users are protected by Symantec's antispam and email security technologies. Over 2,500 businesses, governments, and organizations worldwide have embraced Symantec Brightmail AntiSpam for its:

- Continuing effectiveness in stopping spam despite the constantly evolving tactics of spammers
- Filtering accuracy—ensuring that legitimate mail is not misclassified as spam
- Simple, hands-off administration

Symantec Brightmail AntiSpam 6.0 is the next step forward in the evolution of Symantec's comprehensive threat protection. This evaluation guide provides an in-depth look at important improvements and new features contained in Symantec Brightmail AntiSpam 6.0. The evaluation methodology guidance presented here will help system administrators and other reviewers properly evaluate the functionality and capabilities of Symantec Brightmail AntiSpam 6.0. It also contains relevant information for people who are using previous releases of Brightmail AntiSpam.

This guide is divided into four main sections:

- **What's new.** A quick summary of the new features and enhancements for this version.
- **Building evaluation criteria.** Resources and guidelines to help you evaluate antispam solutions.
- **Running a line evaluation.** Best practices on deploying Symantec Brightmail AntiSpam in your environment.
- **Feature checklist.** A walk-through of Symantec Brightmail AntiSpam 6.0.

With Symantec Brightmail AntiSpam 6.0, Symantec had several key goals. First was the continuing desire to extend overall spam-fighting effectiveness. As the most visible result of an antispam solution, the catch-rate affects stakeholders from the data centers to the executive suites. By tracking spam trends, researchers at Symantec uncovered new approaches to catching spam, leveraging proprietary technologies as well as the data culled from its vast spam-analysis infrastructure. In folding these new techniques into its arsenal, Symantec has, as always, ensured that the technology does not come at the expense of trapping legitimate mail.

Another important goal was to deliver more administrator control. Many administrators told us that they wanted to combine Symantec's set-it-and-forget-it model with optional tools to provide more visibility and control into their spam problems. We've responded with powerful management enhancements such as an intuitive administrator interface, a new group policy framework, and consolidated reporting and logging, among others.

> What's new?

While continuing to deliver on the best email antispam filtering accuracy (99.9999%)¹ and effectiveness rates (95%)² on the market, Symantec Brightmail AntiSpam 6.0 offers new features designed to thwart the latest spamming techniques. This section summarizes the major additions of this release.

Brightmail Control Center

The Brightmail Control Center (Control Center) is a Web-based cross-platform configuration and administration center built in Java™. Each customer installation has one Control Center, which also houses the Web-based Quarantine and supporting software. You can configure and monitor all of your Scanner components (which perform all message filtering) from the Control Center. The Control Center replaces the configuration file, the Configurator, and the administration console used in previous releases.

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

² "eWeek," 2003

Centralized administration

You can now configure and manage multiple Scanners from one Control Center. Previously, the server that was filtering email needed to be configured individually.

Group policies

You can now specify an unlimited number of user groups, identified by email addresses or domain names, 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.

Improved reporting

For added convenience and clarity, preset reports are now separated into two groups: antispam reports and antivirus reports. You can choose from a selection of reports; each report can be customized to include specific date ranges, time period groupings, and various delivery and output options. For some reports, you can filter based on specific recipients and senders of interest.

Improved filtering technologies

Numerous improvements have been made to the Symantec Brightmail AntiSpam filtering technologies, including enhanced effectiveness for URL filters and heuristic filters; filtering on mailto: links in messages; improved filtering on MIME headers; and the next generation of attachment signatures, which target comparisons to specific message components with precision.

Integrated Brightmail Reputation Service

The Brightmail Reputation Service provides comprehensive email source analysis and reputation filtering. Leveraging extensive research on email traffic, the service increases filtering effectiveness by determining the reputation of originating IP addresses, as a source of spam or of legitimate email. The Brightmail Reputation Service is automatically integrated and filters messages using the same automated delivery model as the other filters used in Symantec Brightmail AntiSpam.

Improved quarantine management

Quarantine is now managed via the Control Center. Quarantine can be deployed for end-user access or administrator-only access.

You can manage the size of the Quarantine by deleting messages based on the number of days in the Quarantine, the total size of the Quarantine database, or each user's storage usage. The Quarantine digest now supports View and Release links, enabling users to review or recover an individual message without logging in.

End-user enhancements

Using the Brightmail Plug-In for Outlook, end users can now define the languages in which they want to receive messages. This feature, which leverages product's ability to identify the language of a message in one of 11 different languages, rids the inbox of spam written in different languages.

> Evaluating email security solutions

This section includes a series of guidelines to help you evaluate your needs and requirements in an antispam solution. It contains the following topics:

- **Building your evaluation criteria.** A summary of the key criteria to look for when evaluating competing solutions and vendors.
- **Sample scorecard.** A convenient worksheet that you can use to summarize the results of your evaluation. The decision factors provided are weighted so that the results can be tailored to your specific needs.

Building your evaluation criteria

As you evaluate different solutions, keep these two primary decision factors in mind:

- **Overall results of live evaluation.** This includes the overall filtering performance and accuracy metrics, including the spam catch rate and false positive occurrences, if any. It also includes the amount of time spent administering the solution. The live evaluation results will be the best guide to how the software will perform on a day-to-day basis, and should be the most important factor in your final evaluation decision.
- **Features included with the solution.** A competitive antispam solution needs to have a solid set of technology, administration, and management features. The rest of this section highlights some key quality and product feature areas on which to focus when reviewing your requirements and evaluation criteria. For a summary of the features included in Symantec Brightmail AntiSpam 6.0, see the Feature Checklist.

ACCURACY

Accuracy is the largest differentiator between antispam products. Accuracy refers to the false positive rate, or the percentage of legitimate email messages that are incorrectly identified as spam. At the core, an antispam solution should do no harm. Incorrectly filtering small amounts of legitimate mail creates the same productivity loss as spam. Users are forced to find their email in ever-growing quarantines, and IT is forced to handle end-user complaints. For a company receiving 100,000 messages a day, even a 1% false positive rate results in 1,000 messages mistakenly sidelined every day. Once an antispam solution starts misidentifying legitimate and important business communication, it becomes more trouble than it's worth.

Look for solutions that:

- Produce low or no false positives
- Have a track record, through product reviews or customer validation, of having extremely low or negligible false positive rates
- Employ a balanced mix of technologies to guard against overaggressive filtering
- Have safeguards for preventing, detecting, and resolving suspected false positives
- Provide quarantine options to let users ensure that legitimate messages are not lost

EFFECTIVENESS

After accuracy, effectiveness is the bottom-line criteria by which to judge an antispam solution. Effectiveness refers to the percentage of spam caught by an antispam solution. It is obviously very easy to be 100% effective—simply block all mail, both spam and non-spam. It is much harder to be both effective and accurate. Many solutions are overly aggressive and don't have substantial safeguards against false positives. Such solutions force you to make the hard trade-off between accuracy and effectiveness. Effectiveness and accuracy must be examined in tandem.

Look for solutions that:

- **Have consistently high effectiveness.** Spam-catching rates above 95% are considered best-of-breed.
- **Keep up-to-date.** Timely and automatic updating of filters is essential if you want to keep pace with changing spam attacks.
- **Leverage research on spam trends and traffic.** The only way to keep up with spammers is to monitor their changing techniques and attacks in real time and adjust defenses as appropriate. Consider the vendor's research facilities, the visibility into global spam traffic, the expertise of the antispam detection staff, and service levels of coverage.

ADMINISTRATION OVERHEAD

One of the objectives of using an antispam solution is to restore employee productivity. Solutions that require significant amounts of administration or put the burden on your end users to develop and train antispam filters defeat that main objective. Some solutions require weeks or months of administrative attention and filter training before they are effective. An ideal solution will not require any maintenance or tuning of antispam filters. That said, not all enterprises or organizations are alike. An antispam solution needs to be feature-rich and customizable to give administrators control and visibility into their organizations' spam problems. For example, administrators should be able to choose how to handle filtered messages, quarantine messages, generate useful reports, and other tasks.

Look for solutions that:

- **Are immediately effective out of the box.** Filter tuning should never be required, and updates should occur without bringing down the server or leaving it unprotected.
- **Provide the right level of management features.** Key management and administration features include robust reporting, centralized graphical administration, automated filter updates, and methods for creating policies for different users.
- **Integrate with standard mail transfer agents (MTAs) and mail servers.** Solutions that rely on custom or proprietary MTAs give rise to scalability and failover concerns. The best solutions work across multiple industry-standard mail servers—such as Exchange and Sendmail—and do not disrupt current systems or require new product training.

ANTISPAM TECHNOLOGY

Focus on vendors that employ a breadth of detection techniques. Strong antispam vendors offer an array of techniques, ranging from heuristics to signatures to reputation-based filtering. Because spam attacks are complex, a multilayered approach or a combined approach is necessary.

OTHER FILTERING TECHNOLOGIES

Email is frequently the vehicle for other problems in addition to traditional spam. This includes threats such as viruses and spamming worms. It can also include non-system-level threats, such as unwanted attachments (e.g., MP3s and others). Antivirus protection and content-filtering tools add an important layer of protection to basic antispam solutions. The ideal solution should also have a method of setting up lists of trusted senders who can bypass spam filtering. Similarly, administrators should be able to specify a list of denied senders, from whom messages can be treated as appropriate.

Look for solutions that provide:

- Real-time, automatically updated antivirus protection
- Flexible content filtering tools to block inbound messages with specified attachment types, embedded content in the body and headers, sizes, and other criteria
- Organizational allow and deny lists

MAIL MANAGEMENT

Look for solutions that provide:

- A group policy framework so that different groups of users can have mail handled in different ways
- A selection of spam quarantine options
- Definable administration roles and privileges

SYSTEM MANAGEMENT

Look for solutions that provide:

- Auto-updates of antispam filters.
- Consolidated and easy-to-manage logging and monitoring capabilities.
- Performance and scalability—the antispam solution should never be the bottleneck for your mail infrastructure. It should be easy and cost-effective to add additional servers for failover or future growth.
- Integration with industry-standard mail servers.

USER PREFERENCES

Look for solutions that provide tools for users to set up personal allow/block lists and other inbox personalization tools.

COMPANY STRENGTH AND MARKET ACCEPTANCE

Fighting spam is an ongoing commitment. The antispam vendor should have solid financials, a demonstrated track record, and a large customer base. Look at factors such as the length of time in the business, key strategic technology partners, and reviews by independent third parties and analysts. You need to ensure that the product you choose will be around for the long term.

Sample score card

Just as every mail network and company is unique, every antispam product has different strengths and weaknesses. This section contains a handy scorecard that you can use when evaluating antispam solutions.

STEP 1: WEIGH DECISION FACTORS

To get the most out of your evaluation, you should have an idea of which factors are most important and relevant based on your needs and environment. The following chart shows recommended weights that you should give to different evaluation factors when determining which product is the best. These weights have been compiled based on the types of questions Symantec sees regularly in antispam RFPs and other requirements documents. While you may choose to modify the weighting breakdown in the features depending on your needs, we strongly recommend that you not change the weighting of the first three factors. When completing your evaluation scorecard, you will rate each factor on a scale of 1 to 10. These ratings will then be multiplied by the percentage weighting, and added up to give an overall product score. Any score above 9 is considered competitive.

| Decision Factor | Recommended Weight | Your Weight (if different) |
|---|--------------------|----------------------------|
| Live Test Results | | |
| Effectiveness How well does the solution catch spam? Competitive solutions don't miss more than 5% of incoming spam. | 15% | <input type="text"/> % |
| Accuracy (false positives) Does the solution misidentify legitimate mail as spam? There should be zero tolerance in this category. Penalize a solution heavily for false positives. | 15% | <input type="text"/> % |
| Time spent administering How much time does it take to install and administer the solution? Track time spent on tasks such as keeping filters up-to-date, dealing with false positives, and dealing with missed spam. | 15% | <input type="text"/> % |
| Features | | |
| Antispam technology What is the breadth and scope of the vendor's antispam technology? How innovative has it been in dealing with challenges from spammers? | 10% | <input type="text"/> % |
| Antivirus technology Does the solution offer automatically updated and integrated virus protection? | 5% | <input type="text"/> % |
| Content filtering Does the solution offer an array of tools to filter based on content and source so that you can enforce corporate mail policies? | 5% | <input type="text"/> % |
| Mail management Does the solution offer a flexible and powerful way to manage filtered mail? Look for features such as group policies and reporting. | 5% | <input type="text"/> % |
| System management How is administration made easier over the long term? Is the solution scalable and easily integrated in common mail environments? | 5% | <input type="text"/> % |
| User preferences | 5% | <input type="text"/> % |
| Others | | |
| Reviews and analyst reports What types of product reviews and analyst coverage has this solution received? | 10% | <input type="text"/> % |
| Company strength How long has the company been in business? How focused is it in the email security market? Does it have a solid financial background? | 10% | <input type="text"/> % |
| | 100% | 100% |

STEP 2: COMPLETE EVALUATION SCORECARD

In the scorecard below, assign a 1 to 10 score for each decision factor for each antispam solution you evaluate. To obtain the final score, multiply each individual score by the weight given that category, and then add up all those resulting numbers. If necessary, you can transfer any changed weightings based on your choices in the previous section.

As shown in the provided evaluation grid, features are critical, but they are secondary to the chief goal of simply stopping spam and preserving legitimate mail. As such, the results of the live test are weighted higher than the features.

| | | Symantec | | Vendor 2 | |
|----------------------------------|-------------|----------------------------------|---------------------------------|--------------|---------------------------------|
| Solution | | Symantec Brightmail AntiSpam 6.0 | | | |
| | Weight | Score (1-10) | Weighted Score (score * weight) | Score (1-10) | Weighted Score (score * weight) |
| Decision Factor | | | | | |
| Live Test Results | | | | | |
| Effectiveness (spam caught) | 15% | | | | |
| Accuracy (false positives) | 15% | | | | |
| Time spent administering | 15% | | | | |
| Features and Capabilities | | | | | |
| Antispam technology | 10% | | | | |
| Antivirus technology | 5% | | | | |
| Content filtering | 5% | | | | |
| Mail management | 5% | | | | |
| System management | 5% | | | | |
| User preferences | 5% | | | | |
| Others | | | | | |
| Reviews and analyst reports | 10% | | | | |
| Company strength | 10% | | | | |
| Totals | 100% | Score _____ | Weighted Score _____ | Score _____ | Weighted Score _____ |

> Running a live evaluation

The live evaluation is the most important part of the evaluation process. To maximize your results, you should:

- Decide up-front how extensive your evaluation needs to be
- Agree on a definition of spam
- Understand the best practices to help you produce the most meaningful results
- Go through a final evaluation checklist

Live evaluation types

Regardless of the evaluation type you choose, you need to ensure that your evaluation mimics real end-user experience, tests in an environment that is fair, and produces statistically significant results. This section provides some guidance to help you ensure that your evaluation is as accurate and useful as possible.

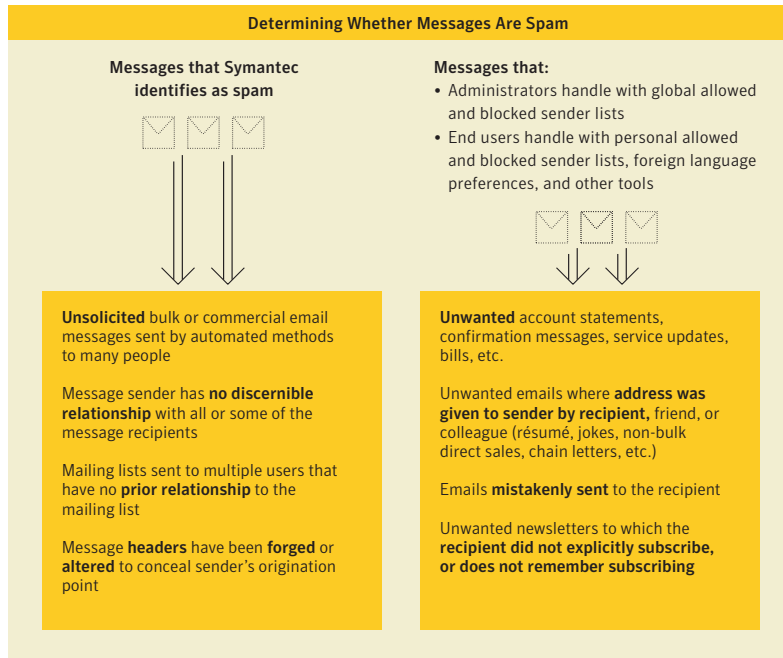
There are two basic approaches you can take when evaluating antispam solutions. Product reviewers who wish to get a quick sense of the effectiveness of an antispam solution can take a small and rigorous approach, where the performance and filtering statistics are scrupulously monitored for a short period of time. Enterprises and other organizations should take a more holistic approach, letting the solution operate over time in the production environment and tracking user feedback and administration overhead.

| Evaluation Type | Suitable for | Helpful Hints |
|-----------------|--|---|
| Small | Product reviewers | <ul style="list-style-type: none"> • Test for a minimum of 2–4 days • Use a sample size of at least 3,000 messages • Test during the same days of the week if evaluating multiple solutions • Use a minimum of two mailboxes • Examine individual mailboxes for false positives and spam-filtering effectiveness |
| Large | Mail administrators and other evaluators | <ul style="list-style-type: none"> • Test for 2–4 weeks • Use a sample size of at least 50,000 messages • Involve the whole company or as many diverse users as possible • Configure filtering software to tag the subject line for spam messages • Instruct employees to report false positives |

Your definition of spam

To properly monitor and evaluate a solution's effectiveness and accuracy, it is imperative that you clearly delineate between spam and non-spam. To set expectations, you should clearly communicate this definition to all testers.

Symantec uses the guidelines outlined in the following figure to distinguish spam from legitimate email communication. For other unwanted email that is more personal or organization-specific, Symantec offers other tools.



Best practices

The following best practices are guidelines to help you ensure that your evaluation gives you the necessary data for you to make an informed decision about an antispam product. They will also help minimize frustration as you roll out the filtering product.

PREPARE YOUR USERS

You will get the best results if your evaluation involves a diverse set of end users. The ideal situation is to test using all the employees. If you are choosing an evaluation that involves end users, inform them of their critical role in the evaluation. They will need to take a few minutes each day to review their inbox and report misidentified messages. You should provide easy-to-follow instructions so that the users know how to report misidentified messages and relay feedback to the evaluation administrators.

TEST SOLUTIONS USING LIVE INCOMING MAIL

You should always test with your company's live email. Determining how responsive vendors are to current spam attacks is crucial. Testing using old collected spam will produce inaccurate and irrelevant results. Symantec Brightmail AntiSpam is a real-time solution with filters that are maintained to detect current spam attacks. To optimize performance, filters are removed once attacks have subsided. There are many mail flow configuration options you can choose from:

- **Place the solution in your production mail environment and process mail inline.** This scenario gives you the most accurate idea of how an antispam solution will work in your environment. For smaller organizations for which all users are participating in the evaluation, this is the best option. By filtering mail inline, you minimize the overhead of checking multiple accounts. If only a subset of the company is participating in the test, you can set up policies so that only those specific users will have their mail filtered.

- **Relay mail to testers from your production environment to a test evaluation system.** If you do not want to place the antispam solution directly into production, you can place it on a separate test system. Incoming mail can be relayed to this machine, where spam filtering will be performed. The test system can then relay to the message store for retrieval by the users participating in the evaluation.
- **Run an administrator-only evaluation.** In this scenario, you fork off a copy of all incoming mail and send it to a test system that is configured with the antispam product. As the evaluation administrator, you will log into the quarantine and keep track of filtering performance.

DO NOT FORWARD SPAM TO BE TESTED

Forwarding messages alters the format of emails. For example, the From header is changed. Similarly, many email clients alter the body of the message when an email is forwarded. Some of the Symantec Brightmail AntiSpam rule technologies are designed to analyze message headers as they are received directly from spammers. To promote accuracy, neither the Symantec Brightmail AntiSpam header nor body-based filters are designed to work on messages altered in this way.

Evaluation checklist

| |
|---|
| Prepare your environment |
| <ul style="list-style-type: none"> • Browse the <i>Symantec Brightmail AntiSpam Deployment Guide</i>, included in the downloaded software distribution or on your CD. • Confirm that you meet the minimum system and mail flow requirements. |
| Ensure that Symantec filters can reach your environment |
| <ul style="list-style-type: none"> • HTTPS communication with the BLOC™ (Symantec Brightmail Logistics and Operations Center) is necessary for registration, downloading updated filters, and transmitting statistics. • If you plan to deploy Symantec Brightmail AntiSpam from behind a corporate firewall, ensure that outbound connections to TCP port 443 are allowed. |
| Install Symantec Brightmail AntiSpam |
| <ul style="list-style-type: none"> • Follow the instructions in the <i>Symantec Brightmail AntiSpam Installation Guide</i>. • Become familiar with the Control Center administrator interface. |

> Feature checklist

Antispam engine

| Feature | Description |
|--|---|
| Open Proxy List | Constantly updated list of open proxy servers, which are frequent conduits for spam. |
| Suspect IP List | Constantly updated list of IP addresses from which virtually all of the outgoing email is spam. |
| Safe IP List | Constantly updated list of IP addresses from which virtually no outgoing email is spam. |
| URL filters | Identifies and filters a spammer's intended URL, which is often disguised and leads to spam Web pages. |
| Heuristics | Proactive filtering technology that evaluates the content of incoming messages based on telltale characteristics of spam and legitimate mail. Includes language-agnostic and language-aware heuristics. |
| BrightSig2™ | Signature technology that eliminates randomization and HTML-based filter evasion techniques. |
| Attachment signatures | Targets a specific MIME attachment, for example, a pornographic image used in a specific spam attack. |
| Header filters | Tight, targeted, regular expression-based filters based on real-time attacks or derived based on commonalities or trends present in spam messages. |
| Body hash | First-generation signature technology. |
| 10-minute updates | Filters automatically downloaded from Symantec to customer sites via secure HTTPS every 5–10 minutes. No need for server restart or administrator intervention. |
| Language identification | Language of the messages can be identified as belonging to one of 11 languages. Software can then run only the filters that apply to the message's language. Users can adjust language preferences to deny or allow email based on language identification by Symantec. |
| Language-specific heuristics | Specially tuned heuristics based on one of 11 languages target non-English spam. Supported languages include Chinese, Dutch, English, French, German, Italian, Japanese, Korean, Portuguese, Russian, Spanish. |
| Language expertise | Technicians deployed across the global analyze spam and create targeted filters in over 15 languages. |
| 24-hour-a-day false positive resolution | All possible false positives are analyzed and corrected by Symantec technicians. |
| Global operations centers | Globally distributed spam analysis and operations centers in the United States, Ireland, Australia, and Taiwan. Provide 24x7 monitoring of spam attacks and filter performance at customer sites. |
| Spam detection network | Includes the largest honeypot network (over 2 million decoy email addresses and domains). Also includes submissions and statistics from over 300 million email inboxes. |
| Missed spam submission | End users can use their email clients (such as Microsoft® Outlook® or Domino™) or use a Web-based interface to submit missed spam to Symantec. If warranted, Symantec will adjust filters. |
| False positive submissions | Using convenient submission tools, Symantec's user community—300 million strong—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. |

Antivirus

| Feature | Description |
|--|--|
| Automatic updates | Antivirus signatures and definitions created by Symantec and updated at customer sites as soon as they are available. |
| Choice of actions | Set policies to handle messages with viruses: 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 | Adjustable heuristics for more or less aggressive identification of viruses. |
| Adjustable scanning thresholds | Specify maximum size and scanning depth levels to reduce exposure to zip bombs that tax processing. |
| Choice of rule sets | Pick the type of antivirus signatures. |

Content filtering

| Feature | Description |
|--------------------------------------|---|
| Custom Filters Editor | Use a graphical interface to enforce company policies by creating global, server-level filters. Quickly activate and deactivate individual filters, display their activation status, and organize the order in which rules are run. |
| Multiple criteria | You can write complex rules using multiple combinations of 16 different message parameters, scanning based on content, headers, MIME types, and a host of other criteria. |
| Unlimited conditions | There is no limit to the number of conditions you create in your content filter. |
| Allow/deny lists | Set up organization-wide lists of blocked and allowed senders (also known as blacklists and whitelists). Email from trusted senders is always delivered, and email-blocked senders can be handled as you choose. |
| Flexible sender specification | Specify allowed and blocked senders by: <ul style="list-style-type: none"> • Email address/sender name • Domain name • IP address • DNS block or allow lists |
| Third-party lists | Configure lookups to third-party lists of allowed or blocked services to which you subscribe. |
| Multiple actions | For messages matching content filters, you can choose to delete, forward on to an email address, modify the messages, or perform other actions. |
| Text file import | Import manually coded filters written in the Sieve language. Also import lists of allowed and blocked senders. |

End-user features

| Feature | Description |
|-----------------------------|---|
| Blocked senders list | Using their email client, users can specify addresses that will always be blocked. The entries are in addition to organization-wide block lists defined by administrators. |
| Allowed senders list | Users can designate senders who are allowed to bypass antispam filtering. Includes convenient auto-population of trusted senders from the Microsoft Outlook address book. |
| Allowed recipients | Users can designate recipient aliases to accommodate mailings that use a general email address. |
| Allowed 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. Submissions can be made using email clients such as Outlook or Domino, or by using a Web-based interface. |

Mail management

| Feature | Description |
|---|---|
| Group policies | Create groups of users based on email addresses or domain names (wildcards permitted). Each defined group can have unique email-filtering actions, based on seven different categories of email. Also supports importing of group members from a text file. |
| Multiple actions for filtered mail | For spam, suspected spam, allow/block, and content filters: <ul style="list-style-type: none"> • Deliver the message normally • Delete the message • Deliver the message to the recipient's spam folder • Save the message to disk • Forward the message • Quarantine the message • Modify the message Also, specific actions for worms and unscannable content. |
| Multiple actions for filtered mail for viruses | <ul style="list-style-type: none"> • Clean messages of viruses and deliver each cleaned message normally, with a notification to the recipient • Discard the message • Deliver the message normally |
| Adjustable spam threshold | 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 | Messages classified as one of the following: <ul style="list-style-type: none"> • Spam • Suspected spam (matching the adjustable Spam Scoring range you specify) • Email from blocked senders • Emails infected with viruses • Mass-mailing worms • Unscannable emails (could not be scanned due to size restrictions or other variables) • Custom-filtered emails (matching content filters you create) |
| Submissions | Users can submit missed spam or false positives to Symantec for analysis. |
| Quarantine for Exchange | <ul style="list-style-type: none"> • Automatically sorts spam into each recipient's spam folder in Microsoft Outlook • Lets users submit misidentified messages to Symantec • Includes configurable spam retention period • Supports Microsoft Exchange 2003 Spam Confidence Layer (SCL) method of categorizing and foldering spam messages after filtering |
| Quarantine for Domino | <ul style="list-style-type: none"> • Automatically sorts spam into each recipient's spam folder in Domino • Lets users submit misidentified messages to Symantec • Includes configurable spam retention period |
| Administrator Web-based Quarantine | Administrators can log in and review spam messages that the Symantec software has quarantined for all users in their organization. Administrators can access Quarantine and configure settings from the Control Center. |

Mail management (cont.)

| Feature | Description |
|---|--|
| End-user Web-based Quarantine | Users on your network can log in to their personal quarantine at any time and view their quarantined messages. |
| Security | Support for SSL (Secure Sockets Layer) encryption in Control Center to protect passwords and content. Administrators can choose the connection level to use during the installation process (SSL or no-SSL option). |
| Email notification | Quarantine can send a periodic email summary to users, listing the newly quarantined spam messages, and including links for users to immediately release messages to their inbox or to log in to their personal quarantines. |
| One-click release of quarantined messages | Recipients of spam quarantine digest can click links to immediately release or view caught spam messages—without having to log in. |
| Alias expansion | Quarantine automatically resolves all aliases and delivers messages to the appropriate quarantine account for the underlying email address. |
| Misidentified message submission | Messages identified by administrators and users as missed spam or false positives are automatically sent to Symantec for analysis. |
| Administrator notification for submissions | Administrators can receive a copy of all misidentified messages sent by users to Symantec. |
| Spam expunging and size thresholds | Configurable retention period for spam messages. Also included are thresholds to control the quarantine database size and the messages number limit on a global and per-user basis. |
| Flexible LDAP support | Quarantine can access LDAP directories such as: <ul style="list-style-type: none"> • Microsoft Active Directory® (Exchange 2000 and Exchange 2003) • Exchange 5.5 • Sun™ ONE Directory Server Also included are fully configurable LDAP query settings and attributes to match your LDAP schema. |
| Quarantine message search | Users and administrators can search messages in Quarantine using multiple criteria, including To Headers, From Headers, message body, Subject Headers, Message ID Headers, and time range. |
| Customizable notification template | Customizable delivery frequency, message content, content type (HTML, text, or both). Also specify whether digest includes embedded view message and release message links to enable users to access messages without logging in. Choose whether to deliver digest to distribution lists. |
| Consolidated reporting | View consolidated filtering performance statistics for all Brightmail Scanners. |
| Multiple preset reports | A total of 19 different reports are available. Choose from the following reports, each available for antispam and antivirus: <ul style="list-style-type: none"> • Mail Summary (covers both spam and virus filtering) • Spam Detection • Spam Top Sender Domains • Spam Top Senders • Specific Senders • Top Sender HELO Domains • Top Sender IP Connections • Top Recipients Domains • Top Recipients • Specific Recipients |
| Report export | Export report data for use in any reporting or spreadsheet software for further analysis. |
| Report scheduling | Schedule reports for generation and email delivery. |

System management

| Feature | Description |
|---|---|
| Web-based administration center | Provides summary dashboard of filtering performance, centralized administration of all Symantec software, and remote administration using a Web browser from anywhere on the Internet. |
| Installation and update process | Installations, upgrades, and updates with graphical wizards. |
| Automated filter downloads and statistics transfer | Secure HTTPS polling from customer sites initiates download of updated filters. The same process transmits statistics from customer sites to the BLOC, allowing the BLOC to gauge the performance and effectiveness of deployed filters. Spam filtering is never stopped during the update process |
| Assignable administrator privileges | Create additional administrator accounts, granting each administrator the desired level of management privileges for different components of Symantec Brightmail AntiSpam. You can assign any or all of the following management roles: <ul style="list-style-type: none"> • Manage Quarantine • Manage status and logs • Manage reports • Manage group policies 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. |
| Automated email alerts | Alerts are sent to administrators or other parties when the following conditions arise: <ul style="list-style-type: none"> • 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 |
| Consolidated logs | Logging levels can be set on a 5-point sliding scale, and the settings can apply to individual filtering computers or to all. You 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. |
| Consolidated status view | View the following from one central location: <ul style="list-style-type: none"> • Quarantine information (if you are using the Web-based Quarantine) • The configured Brightmail Scanners in your network, along with any associated components • The basic status (running or not) of the Scanners and components |

MTA integration

| Feature | Description |
|-------------------------------------|---|
| Exchange integration | With this integration, Symantec Brightmail AntiSpam filters messages as they reach your Microsoft Exchange Server 2003 or Microsoft Exchange 2000 Server. Installing Symantec Brightmail AntiSpam directly on the Exchange server is a common deployment for enterprises and is designed to support from hundreds of users to hundreds of thousands of users. |
| IIS SMTP Service integration | The filtering software integrates tightly with the IIS SMTP Service for Windows®. Symantec Brightmail AntiSpam can support any MTA (including Exchange 5.5 and Lotus Notes®) provided it is receiving mail and working in a relay situation with the IIS SMTP Service. |
| Sendmail integration | Symantec Brightmail AntiSpam also integrates directly with Sendmail 8.12.1x or later or Sendmail Switch 3.1. Integrated through Sendmail's Militer interface, this version is designed for customers in Solaris™ and Linux environments. |
| MTA SDK | Also provided is a comprehensive Software Development Kit (SDK) that gives customers the tools to incorporate Symantec's message-filtering functions into other MTAs and mail servers. |

> 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.

Given the number of competing vendors and solutions, selecting the right antispam product can be daunting. This guide presented some best practices to help decision-makers properly evaluate and compare antispam solutions. The evaluation process should begin with a clear understanding of the criteria on which a solution should be judged. Accuracy, effectiveness, and low administration are by far the most important decision factors. These factors should be closely tracked in the live evaluation—where the antispam solution works in the production environment. Evaluators should also take a hard look at the available features. Which features are crucial given an organization's needs? Which are simply nice to have?

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 enable 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>.

SYMANTEC IS THE GLOBAL LEADER IN INFORMATION SECURITY, PROVIDING A BROAD RANGE OF SOFTWARE, APPLIANCES, AND SERVICES DESIGNED TO HELP INDIVIDUALS, SMALL AND MID-SIZED BUSINESSES, AND LARGE ENTERPRISES SECURE AND MANAGE THEIR IT INFRASTRUCTURE. SYMANTEC'S NORTON BRAND OF PRODUCTS IS THE WORLDWIDE LEADER IN CONSUMER SECURITY AND PROBLEM-SOLVING SOLUTIONS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS OPERATIONS IN MORE THAN 35 COUNTRIES. MORE INFORMATION IS AVAILABLE AT WWW.SYMANTEC.COM.

WORLD HEADQUARTERS

**20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408 517 8000
800 721 3934**

www.symantec.com

**For Product Information
in the U.S., call toll-free
800 745 6054**

**Symantec has worldwide
operations in 35 countries.
For specific country
offices and contact numbers
please visit our Web site.**