



Symantec™ Premium AntiSpam Evaluation Guide

Symantec™ Premium AntiSpam Evaluation Guide

Contents

Executive Summary	2
Evaluating spam solutions	3
Building your evaluation criteria	3
Sample scorecard	6
Running a live evaluation	9
Live evaluation types	9
Your definition of spam	10
Best practices	10
Evaluation checklist	13
Feature overview	13
AntiSpam engine	14
Mail management	15
Conclusion	16

Executive Summary

Today, more than 300 million email users are protected by Symantec's antispam technologies. Over 2,500 businesses, governments, and organizations worldwide have embraced Symantec's solution, powered by Brightmail technology and response, 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

Now existing owners of Symantec Mail Security products may gain the benefits of Brightmail technology and response within the mail security solution they already use and are comfortable with.

Symantec Premium AntiSpam™ – powered by Brightmail technology and response – is an integrated, add-on subscription service for Symantec Mail Security for Exchange, Domino and SMTP. Symantec Premium AntiSpam leverages the industry's best antispam technology, using dynamic, continually updated, multi-layered redundant technologies, that offers a spam detection rate of 95%. It also offers the highest accuracy rate against false positives (99.9999%) ensuring that spam won't reach your users, but legitimate email will.

This evaluation guide provides an in-depth look at Symantec Premium AntiSpam. The evaluation methodology guidance presented here will help system administrators and other reviewers properly evaluate the functionality and capabilities of Symantec Premium AntiSpam.

This guide is divided into – 3 main sections:

- **Building evaluation criteria.** Resources and guidelines to help you evaluate antispam solutions.
- **Running a live evaluation.** Best practices on deploying Symantec Premium AntiSpam in your environment.
- **Feature checklist.** A walk-through of Symantec Premium AntiSpam.

Evaluating spam solutions

This section includes a series of guidelines to help you evaluate your needs and requirements for an antispam solution. It includes 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 scanning and 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 Premium AntiSpam for Symantec Mail Security, see the Feature Checklist in this guide on page 13.

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 legitimate 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. Obviously, this rate is too high. 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 automated filter updates.
- Allow end-user management of quarantined items.

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 multi-layered approach or a combined approach is necessary.

System management

Look for solutions that provide:

- Auto-updates of antispam filters.
- Performance and scalability—the antispam solution should never be the bottleneck for your mail infrastructure.
- Easy and cost-effective means to add additional servers for failover or future growth.

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

In today's mail environment, fighting spam is an ongoing commitment to protect your business and ensure ongoing business communications take place smoothly, safely and interruption free. The mail security 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.

Customers need 24/7 global support and response to meet all types of emergencies. This knowledgeable support should provide a rapid reactive security protection through its incident response program. Proactive security protection should be provided through security updates that can be distributed through automated processes.

Sample scorecard

Every antispam product has different strengths and weaknesses. This section contains a handy scorecard that you can use when evaluating mail security 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 chart on the next page shows recommended weights that you should give to different evaluation factors when determining which product is best. These weights have been compiled based on the types of questions Symantec sees regularly in 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.

Symantec™ Premium AntiSpam Evaluation Guide

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.	20%	<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.	25%	<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"/> %
User preferences	5%	<input type="text"/> %
Mail management	5%	<input type="text"/> %
Others		
Reviews and analyst reports What types of product reviews and analyst coverage has this solution received?	5%	<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?	15%	<input type="text"/> %
	100%	100%

Symantec™ Premium AntiSpam Evaluation Guide

Step 2: Complete evaluation scorecard

In the scorecard below, assign a 1 to 10 score for each decision factor for each mail security 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 viruses and spam and preserving legitimate mail. As such, the results of the live test are weighted higher than the features.

		Symantec		Vendor 2	
Solution		Symantec Mail Security with Symantec Premium AntiSpam			
	Weight	Score (1-10)	Weighted Score (score * weight)	Score (1-10)	Weighted Score (score * weight)
Decision Factor					
Live Test Results					
Effectiveness (spam caught)	20%				
Accuracy (false positives)	25%				
Time spent administering	15%				
Features					
Antispam technology	10%				
User preferences	5%				
Mail management	5%				
Others					
Reviews and analyst reports	5%				
Company strength	15%				
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

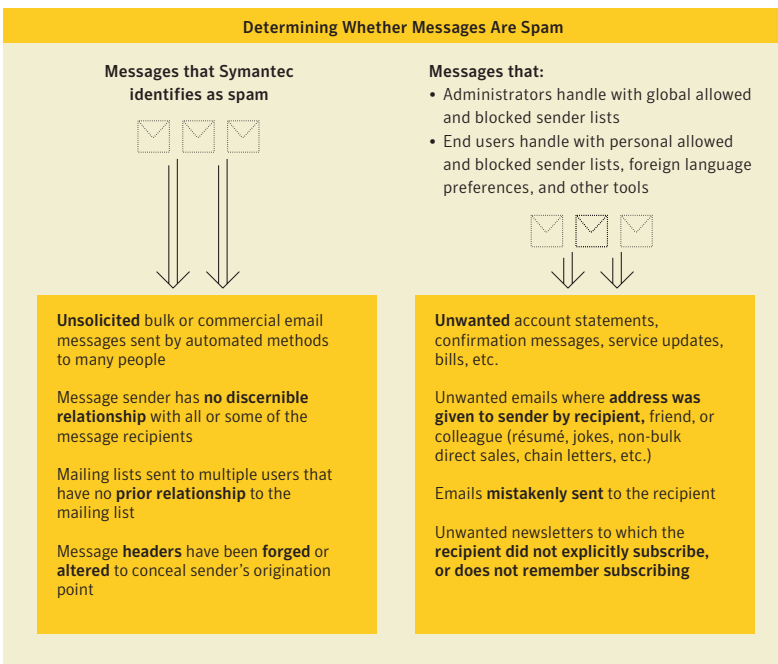
Regardless of the evaluation type you choose, you need to ensure that your evaluation mimics real end-user experience, tests in an environment that is fair, and produces statistically significant results. This section provides some guidance to help you ensure that your evaluation is as accurate and useful 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 Mail Security with Symantec Premium 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 mail security environment. For smaller organizations for which all users are participating in the evaluation, this is the best option. By scanning and 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 and mail security product. As the evaluation administrator, you will log into the quarantine and keep track of spam 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 Premium AntiSpam rule technologies are designed to analyze message headers as they are received directly from spammers. To promote accuracy, neither the Symantec Premium AntiSpam header nor body-based filters are designed to work on messages altered in this way.

Select optimum location for spam prevention

A spam solution can be deployed at the gateway or groupware level. To decide where you want to address spam you should consider several factors including:

- Server load and impact on message throughput
- Ease of administration and deployment
- Hardware and administration costs
- Ability to leverage existing hardware/software investment

In general, spam should be addressed at the first point of entry into a network. The first point of entry may be a gateway or a groupware server depending on the size of the organization and topology of their network.

Generally companies with multiple groupware servers should handle spam on a single gateway server instead of multiple groupware servers as this is more cost effective and easier to administer. Processing spam at the gateway also reduces the burden on the groupware server and allows messages to be rejected prior to entering the mail store. If you currently use Symantec Mail Security for SMTP, you would most likely add the Symantec Premium Antispam service at this tier instead of at the groupware level.

In cases where an organization consists of a single groupware server (no gateway), it may be preferable to simply handle spam at this tier avoiding the inherent administration and hardware expense involved with adding a gateway. This will be preferable if the groupware server can handle the additional processing required for spam detection without significantly impacting message throughput. If the volume of spam starts to impact message throughput, a gateway solution for spam should be considered.

Symantec Premium Antispam can be activated within an existing Symantec Mail Security installation simply by adding a license key (no software install required).

Evaluation checklist

1) Prepare your environment
<ul style="list-style-type: none">• Browse the Symantec Mail Security Administrator's Guide, included in the downloaded software distribution or on your CD.• Confirm that you meet the minimum system and mail flow requirements.
2) 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 Premium AntiSpam from behind a corporate firewall, ensure that outbound connections to TCP port 443 are allowed.
3) Install Symantec Premium AntiSpam
<ul style="list-style-type: none">• Follow the instructions in the Symantec Mail Security and Symantec Premium AntiSpam Installation Guide.• Become familiar with the administrator interface.

Feature overview

Symantec Premium AntiSpam is an add-on subscription service for Symantec Mail Security products (for SMTP, Exchange and Domino). The service is powered by Brightmail technology and response – the spam detection techniques and update service offered through Symantec's Brightmail Logistics and Operations Center (BLOC) provide 95% detection along with 99.9999% accuracy, with little to no administrator intervention.

* Research note by J.P. Gownder of the Yankee Group

The following is an overview of the features that make up Symantec Premium AntiSpam.

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 globe 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.

Mail management

Feature	Description
Multiple actions for filtered mail	For spam, suspected spam: <ul style="list-style-type: none"> • Deliver the message normally • Delete the message • Deliver the message to the recipient's spam folder • Forward the message • Quarantine the message (SMTP only) • Modify the message
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)
Submissions	Users can submit missed spam or false positives to Symantec for analysis.
Quarantine for Microsoft 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
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.
End-user Web-based Quarantine*	Users on your network can log in to their personal quarantine at any time and view their quarantined messages. <i>*(When installed with Symantec Mail Security for SMTP Only)</i>
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. <i>*(When installed with Symantec Mail Security for SMTP Only)</i>
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. <i>*(When installed with Symantec Mail Security for SMTP Only)</i>
Alias expansion*	Quarantine automatically resolves all aliases and delivers messages to the appropriate quarantine account for the underlying email address. <i>*(When installed with Symantec Mail Security for SMTP Only)</i>
Misidentified message submission*	Messages identified by administrators and users as missed spam or false positives are automatically sent to Symantec for analysis. <i>*(When installed with Symantec Mail Security for SMTP Only)</i>
Administrator notification for submissions*	Administrators can receive a copy of all misidentified messages sent by users to Symantec. <i>*(When installed with Symantec Mail Security for SMTP Only)</i>
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. <i>*(When installed with Symantec Mail Security for SMTP Only)</i>
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. <i>*(When installed with Symantec Mail Security for SMTP Only)</i>

Mail management (cont.)

Feature	Description
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. * (When installed with Symantec Mail Security for SMTP Only)
Consolidated spam reporting	View consolidated filtering performance statistics for all spam Scanners.

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 how a solution should be judged. Accuracy, effectiveness, and low administrative overhead 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? Which are simply nice to have?

Symantec's AntiSpam technology provides 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 Premium AntiSpam is best suited for existing customers of Symantec Mail Security products as it can be seamlessly integrated, without further software installation, on the same server as Symantec Mail Security. Symantec Premium AntiSpam leverages the same interface and reporting capabilities as Symantec Mail Security – your administrators are not required to manage an additional separate system.

Symantec Premium AntiSpam provides:

- Multi-layered spam protection. With multiple filtering technologies, it catches more spam while allowing legitimate email to reach end users.
- Flexible spam management.
- 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.

About Symantec

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, California, Symantec has operations in 35 countries. More information is available at www.symantec.com.

Symantec has worldwide operations in 35 countries. For specific country offices and contact numbers please visit our Web site. For product information in the U.S., call toll-free 1 800 745 6054

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
1 408 517 8000
1 800 721 3934
www.symantec.com

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Other brands and products are trademarks of their respective holder/s. Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. NO WARRANTY. The technical information is being delivered to you as-is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice. Copyright © 2004 Symantec Corporation. All rights reserved. Printed in the U.S.A. 12/04 10351119