



Symantec™ Mail Security
for SMTP 5.0
Evaluation Guide

Symantec™ Mail Security for SMTP 5.0

Contents

| | |
|------------------------------------------------|-----------|
| Introduction | 2 |
| Building your evaluation criteria | 3 |
| What to look for | 3 |
| Decision factor analysis | 4 |
| Evaluation scorecard | 5 |
| Running a live evaluation | 7 |
| Live evaluation types | 7 |
| Your definition of spam | 8 |
| Best practices | 8 |
| Conclusion | 11 |

Introduction

Email has quickly grown in sophistication over the last decade and is now considered to be mission-critical for conducting business. By extension, email has become indispensable as a repository of information and as a legal record. Paralleling this growth in importance are increasing threats to email security, with the predominant threats to the email infrastructure being spam and viruses. Increased costs and compliance pressures are additional challenges that IT departments have to contend with. As a result, organizations with substandard email security protection face numerous consequences, including:

- Lost user productivity due to spam or system downtime
- Security incidents, such as propagation of malicious code and denial of service
- Leakage of sensitive information
- Exposure to regulatory penalties

Today, over 75,000 businesses, governments, and organizations worldwide rely on Symantec for protection of their email gateways. For organizations looking for best-of-breed antispam, antivirus, and content filtering protection in a software-based deployment option, Symantec has traditionally offered two products: Symantec Mail Security for SMTP and Symantec Brightmail AntiSpam. Symantec Mail Security for SMTP 5.0 is a powerful new upgrade to Symantec's software-based email security product line. It features the following high-level enhancements:

- **Consolidates the best features from existing gateway solutions.** To make the selection of software-based email security protection easier, Symantec Mail Security for SMTP 5.0 merges the existing Symantec Mail Security for SMTP 4.x and Symantec Brightmail AntiSpam 6.0 product lines. It also incorporates virtually all the features from the award-winning Symantec Mail Security 8200 Series appliances.
- **Delivers next generation threat prevention.** Day-Zero virus protection, a key new feature in Symantec Mail Security for SMTP 5.0, acts proactively against new virus outbreaks by identifying suspicious virus attachments and removing them from the email stream until new definitions are deployed. Day-Zero detection capabilities, as well as a new set of related policies, deliver crucial protection during the period between the initial discovery of a virus and deployment of official antivirus definitions. Symantec Mail Security for SMTP 5.0 also features the Email Firewall, designed to thwart directory harvest attacks and stop threats at the IP connection level.

- **Improves content filtering and compliance tools.** With enhancements such as true file typing, regular expression and keyword scanning in attachments and containers, and other additions, Symantec Mail Security for SMTP 5.0 makes it easier for administrators to enforce corporate acceptable use policies, as well as conform to legal and regulatory requirements.
- **Expands visibility and administrator control.** Symantec Mail Security for SMTP 5.0 leverages the intuitive administrator Control Center interface which centralizes management of critical tasks such as policy creation, reporting, and monitoring. Symantec Mail Security for SMTP 5.0 also features an advanced message tracking tool, which makes it easy to track the path of any email message that has been processed by the system.

Building your evaluation criteria

Just as every email network and company is unique, every email security product has different strengths and weaknesses. This section summarizes the key decision factors that you should consider when selecting a product. It also includes a handy scorecard that you can use when evaluating email security solutions.

What to look for

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

- **Overall results of live evaluation.** This includes the overall filtering performance of the solution. Among the “bottom line” issues you should track are how accurately the solution blocks spam, how reliably it eliminates viruses in mail attachments, how well it enforces content compliance policies, and how it protects the gateway against attacks and unwanted mail volume. It also includes the amount of time spent administering the solution. The live evaluation results will be the best guide to how your solution 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 email security solution needs to have a solid set of technology, administration, and management features. For a detailed summary of the product features available in Symantec’s latest email security solution, see the Symantec Mail Security for SMTP 5.0 Feature Summary at <http://www.symantec.com/smssmtp>

Table 1., Decision factors for selecting an email security solution, provides a breakdown of the essential evaluation criteria to consider with evaluating vendors and solutions.

Table 1. Decision selecting an email security solution

| Decision factor | Why it's important | Look for solutions that: |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Antispam accuracy (minimal false positives) | An antispam solution should do no harm. Incorrectly filtering small amounts of legitimate mail creates the same productivity loss as spam. | <ul style="list-style-type: none"> • Apply multiple detection techniques • Have consistent effectiveness rates of 95% or higher • Produce low or no false positives (99.9999% is best of breed) |
| Antispam effectiveness (catches the most spam) | Effectiveness is a bottom-line criteria by which to judge antispam capabilities. | <ul style="list-style-type: none"> • Keep up-to-date with automatic filter updates • Leverage research on spam trends and traffic |
| Virus protection | Email is frequently the vehicle for other security threats in addition to traditional spam. This includes threats such as viruses, malicious code, and spamming worms. | <ul style="list-style-type: none"> • Leverage technology from a leading vendor with a proven track record • Defend against early stage, "Day Zero" viruses for which a traditional antivirus signature do not yet exist • Offer fine-grained control over antivirus definition deployment • Provide protection during updates. Many solutions leave the gateway unprotected during virus definition and scanning engine updates • Use heuristic detection technology to identify new viruses by detecting virus-like behavior |
| Content compliance | Regulations and internal policies are driving the need to detect and block privacy violations, offensive and inappropriate content, intellectual property theft, compliance issues, and other dangers in employee email. | <ul style="list-style-type: none"> • Can locate important keywords and patterns within messages, documents and other attachments, as well as within ZIP files • Can flag or prevent confidential or potentially offensive material from flowing through your mail system • Can add custom disclaimers to inbound or outbound email • Can automatically remove unwanted attachments from email |
| Connection management | Solutions need to stop directory harvest attacks, spam attacks, and other high volume threats that impact the resources and capacity of your email infrastructure. SMTP connection management features provide a first level of boundary control. | <ul style="list-style-type: none"> • Reject connections based solely on the IP address of the sender • Automatically detect and mitigate directory harvest attacks, as well as potential spam and virus attacks based on the behavior and reputation of the sender • Works with common sender authentication standards such as Sender Policy Framework (SPF) and Sender ID • Ensure that trusted senders can bypass spam filtering |
| Deployment and system administration | Solutions that are time consuming to deploy or require significant amounts of administration defeat the main objective: to conserve email infrastructure costs and restore employee productivity. | <ul style="list-style-type: none"> • Deploy easily with no disruption to existing systems • Provide immediate protection "out of the box" • Require virtually no ongoing administration • Provide centralized administration and monitoring • Can generate and schedule a variety of reports |
| Mail management | Not all enterprises or organizations are alike. Email security solutions should be customizable enough to let administrators create policies and actions for different groups. | <ul style="list-style-type: none"> • Provide granular control over mail handling • Support easy ways to set up different filtering for different groups, such as integration with existing LDAP directories. • Offer a Web-based quarantine |

Decision factor analysis

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 in **Figure 2** presents one view of the decision factors and recommended weights that you should give when determining which product is the best. These weights have been compiled based on the types of questions Symantec sees regularly in requests for proposals 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) |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------------|
| Threat Protection | | |
| Antispam Effectiveness How well does the solution catch spam? Best of breed solutions don't miss more than 5% of incoming spam. | 15% | <input type="text"/> % |
| Antispam 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"/> % |
| Antivirus protection Does the vendor control the antivirus technology and research? Does the solution provide protection against Day Zero virus outbreak? | 10% | <input type="text"/> % |
| Other Threats Does the solution address content compliance, spoofing, volume management, directory harvest attacks, etc.? | 15% | <input type="text"/> % |
| Management | | |
| Mail Management Does the solution support mail policies, email quarantines, user preferences, etc.? | 5% | <input type="text"/> % |
| System management Does the solution support centralized administration and monitoring? Look for features such as comprehensive reporting and event-based alerting. | 5% | <input type="text"/> % |
| Ongoing Administration How is administration made easier over the long term? Is the solution scalable and easily integrated in common mail environments? | 5% | <input type="text"/> % |
| Other | | |
| 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% |

Figure 2: Decision factor worksheet

Evaluation scorecard

Use the Evaluation scorecard in **Figure 3** to assign a 1 to 10 score for each decision factor for the email security you evaluate. To obtain the final score, multiply each individual score by the weight given that category, and then add up all resulting numbers. If necessary, you can transfer any changed weightings based on your choices in the previous section.

| Solution | | Symantec | | Vendor 2 | |
|----------------------------------|--------|-------------------------------------|---------------------------------|--------------|---------------------------------|
| | | Symantec Mail Security for SMTP 5.0 | | | |
| | Weight | Score (1-10) | Weighted Score (score * weight) | Score (1-10) | Weighted Score (score * weight) |
| Decision Factor | | | | | |
| Live Evaluation Results | | | | | |
| Effectiveness (Spam caught) | 15% | | | | |
| Accuracy (false positives) | 15% | | | | |
| Time spent administering | 15% | | | | |
| Features and Capabilities | | | | | |
| Antispam technology | 10% | | | | |
| Antivirus technology | 5% | | | | |
| Content compliance | 5% | | | | |
| Mail Policies | 5% | | | | |
| System management | 5% | | | | |
| User preferences | 5% | | | | |
| Other | | | | | |
| Reviews and analyst reports | 10% | | | | |
| Company strength | 10% | | | | |
| Totals | 100% | Score ____ | Weighted Score ____ | Score ____ | Weighted Score ____ |

Figure 3: Evaluation scorecard

As shown in the provided evaluation grid, features are critical, but they are secondary to the primary goal of securing email. As such, the results of the live test are given greater weight than the features.

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.

Email security evaluation types in **Figure 4** presents two basic approaches you can take when evaluating email security solutions. Product reviewers who wish to get a quick sense of the effectiveness of an email security solution can take a limited 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 |

Figure 4: Email security evaluation types

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. **Figure 5** presents some guidelines that Symantec uses to distinguish spam from legitimate email communication. For other unwanted email that is more personal or organization-specific, Symantec offers other methods, such as content filtering tools.

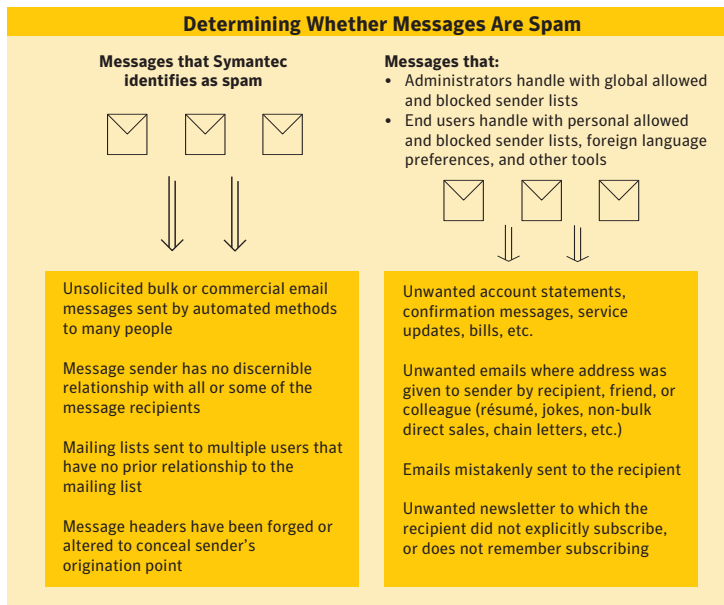


Figure 5: Suggestions for defining spam

Best practices

The following best practices are guidelines to help you ensure that your Symantec Mail Security for SMTP 5.0 evaluation gives you the necessary data for you to make an informed decision about an email security product. They will also help minimize complications as you roll out the email security solution.

Prepare for your deployment

The best way to test Symantec Mail Security for SMTP 5.0 is to place it inline in front of your existing mail server that handles Internet mail. For some organizations, this is the gateway MTA. The solution should be placed in production, at the perimeter or edge of your mail flow. Deploying at the perimeter enables access to all the advanced connection management features of Symantec Mail Security for SMTP 5.0. If it is placed behind devices that alter the incoming IP address or perform NAT modifications, certain connection management capabilities will be unavailable.

Also, you need to ensure that Symantec filters can reach your environment. HTTPS communication with the Symantec Security Reponse Email Security Unit is necessary for registration, downloading updated filters, and transmitting statistics. If you plan to deploy the Symantec Mail Security for SMTP 5.0 servers from behind a corporate firewall, ensure that outbound connections on TCP port 443 are allowed.

You should also gather the IP addresses of applicable servers that will communicate with Symantec Mail Security for SMTP 5.0. This would include the mailbox server, such as Exchange or Domino. In addition, if you will use the LDAP integration feature to create group policies and perform alias expansion, you should identify the LDAP servers that you will access.

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 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 inboxes 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 for SMTP 5.0 is a real-time solution with filters that are maintained to detect current spam, virus, and other attacks. To optimize performance, filters are removed once attacks have subsided.

There are many mail flow configuration options you can choose from. These options enable you to:

- **Place the solution in your production mail environment and process mail inline.** This scenario gives you the most accurate idea of how an email security solution will work in your environment. For organizations in 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 email security solution directly into production, you can place it in a separate test area. Incoming mail can be relayed to this appliance, 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 Symantec Mail Security for SMTP 5.0. 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 antispam filtering technologies are designed to analyze message headers as they are received directly from spammers. To promote accuracy, neither the header nor body-based filters are designed to work on messages altered in this way.

Conclusion

Given the number of competing vendors and solutions, selecting the right email security product can be daunting. This guide presented some best practices to help decision-makers properly evaluate and compare 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 solution works in the production environment. Evaluators should also take a hard look at the available features. Which features are crucial given your organization's needs? Which are simply nice to have?

For more detailed procedures and configuration guidance, see the Symantec Mail Security for SMTP 5.0 product documentation, which is located on the product page (<http://www.symantec.com/smssmtp>).

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 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. Copyright © 2006 Symantec Corporation. All rights reserved.
05/06 10612659