

Symantec Brightmail AntiSpam™ 6.0

What is Symantec Brightmail AntiSpam?	2
Key Points.....	2
What's New	2
Features and Benefits.....	5
Symantec Brightmail AntiSpam vs. Other Symantec Products	9
System Requirements.....	9
30-day Free Trial.....	10
Licensing Symantec Brightmail AntiSpam	11

What is Symantec Brightmail AntiSpam?

Symantec Brightmail AntiSpam™ combines effective spam catching with a high accuracy rate that helps prevent false positives. Deployed at the email gateway, this easy-to-manage solution defends against spam, email fraud, viruses, and other unwanted email. With flexible spam management capabilities and automated filter updates, it meets enterprise security needs without imposing a significant administrative burden.

Symantec Brightmail AntiSpam is sold as a subscription service, and can be deployed at the SMTP gateway for large companies or at the email server level for smaller companies.

Key Points

Symantec Brightmail AntiSpam:

- Catches spam with a 95% effectiveness rate¹;
- Prevents false positives with a 99.9999% accuracy rate²;
- Minimizes the administrative burden with automatic, timely, secure updates every 10 minutes;
- Helps protect 300 million users³
- Filters 15% of worldwide email⁴;
- Filters 100 billion emails/month⁵;
- Protects 9 of the 12 US ISPs⁶.

What's New

Symantec Brightmail AntiSpam 6.0 raises the bar for enterprise antispam software. It includes new features that increase spam-catching effectiveness, additional language identification abilities, two significant new administration capabilities, and per-user non-English language filters. The latest improvements in this release stem from Symantec's leadership in tracking and analyzing spam trends globally.

¹ Source: "eWeek," September 2003

² "Anti-Spam Services for SMBs and Middle-Market End-Users," 25 FEB 2003; Research note by J.P. Gownder of the Yankee Group

³ Brightmail Finance purchase order data

⁴ IDC and Brightmail S-1 statement

⁵ Brightmail BLOC/Business Intelligence (June 2004 data)

⁶ "Top 22 U.S. ISP by Subscribers," Q1 2004



Reputation Filtering

The Brightmail Reputation Service is delivered as multiple lists with each tracking different reputation criteria. The Open Proxy List (OPL), introduced in version 5.5, tracks spam sources that are compromised machines. Symantec Brightmail AntiSpam 6.0 will include two new lists:

- **Suspect List** – A list of IP addresses consisting of email sources producing high levels of spam. Membership on the Suspect List is used as part of the criteria to determine if a message is spam.
- **Safe List** – A list of IP addresses that Symantec data indicate do not send spam. Messages originating from IP addresses on the Safe List will not be scanned for spam. Senders cannot request or pay to be placed on this list.

Advanced Non-English Language Spam Detection

Non-English spam is becoming a larger problem for national and international organizations. Symantec Brightmail AntiSpam 6.0 extends its foreign language antispam technology to include:

- **Language Identification** – Symantec Brightmail Anti-Spam 6.0 examines the contents of a message to determine its language. Symantec Brightmail can also tag the language of the message so that an end user can treat messages in foreign languages as spam.
- **Language-specific Heuristics** – Once the language of the message is identified, Symantec Brightmail will run only the heuristics that apply to that language, significantly improving performance. Heuristics detect spam by looking for characteristics of a message that occur in spam but not in legitimate email. Each characteristic has a number of points associated with it. If the message has over a certain threshold of points it is marked as spam. Version 6.0 includes a series of new heuristics that target specific languages other than English.
- **Global Brightmail Logistics and Operations Centers (BLOC)** – With BLOCs now operational in Dublin, Sydney and Taipei as well as in San Francisco, Symantec has antispam specialists working round the clock in a wide range of languages. Technicians in each BLOC can augment Symantec's automated technologies and monitor effectiveness and accuracy of international spam.
- **Global Probe Network** – Symantec has worked with numerous global customers to build its foreign language Probe Network to over 20 countries, giving Symantec wide visibility into non-English language spam. This enables Symantec to detect and block foreign language spam more effectively. To keep pace with the global spam



threat, Symantec is constantly expanding the reach of the Probe Network by adding global ISPs.

Enhanced Filtering Technologies

- **Enhanced URL Filters** – Since the introduction of URL filters, spammers have attempted to disguise their URLs, making them more difficult to locate in a message. After studying a wide array of spammer techniques, Symantec Brightmail AntiSpam version 6.0's URL filters are now even more effective at extracting purposely hidden URLs and comparing them with Symantec Brightmail AntiSpam's filters.
- **Email Call-to-Action** – An increasing percentage of the call-to-action within a spam message is to ask the user to reply via email to the spam message rather than clicking a link and being taken to a Web URL. Symantec Brightmail AntiSpam 6.0 includes filters for both “mailto” and http URL call-to-actions.
- **Attachment Signatures** – Attachment Signatures, which target specific MIME attachments, are the latest example of Symantec's signature technology. With fuzzy algorithms similar to BrightSig2, Attachment Signatures enable Symantec to create filters based on a particular MIME attachment (for example, a specific pornographic image used in a real-time spam attack) and stop that attachment from reaching customers. Attachment Signatures make it unnecessary to block entire categories of certain attachments.

New Web-based Control Center

Symantec Brightmail AntiSpam 6.0 includes a completely new administration experience that adds new functionality while at the same time making common tasks easier. The Control Center is a cross-platform, web-based interface that provides information on system status, spam quarantine, and server settings. Two of the most important new features are:

- **Global management** – Administrators at large companies typically run multiple filtering servers. With the Control Center, administrators can now make server changes on one management console and the configuration changes will automatically be pushed out to each of the deployed filtering servers. The Control Center also allows administrators to view logs and reports for either individual servers or all servers combined.
- **Role-based security** – Many organizations have a security best practice that states that administrators should have access to only the functions necessary to perform their jobs. Symantec Brightmail AntiSpam 6.0 supports an organization having several different administrators each with different privileges. Some administrators can have access only to the quarantine while others can make server setting changes.

Powerful Group Policies

When an organization deploys an antispam solution, it determines what the policy will be for different types of email. A common policy with Symantec customers is to delete spam and quarantine suspected spam. Symantec Brightmail AntiSpam 6.0 features more powerful policies. Now administrators can create groups composed of domains of users or specific individuals. For example, an organization might want to create a default policy for all users in company and a separate policy for 20 users whose business function requires spam to be treated differently from the default policy. As antispam legislation spreads internationally, national laws dictate new requirements for organizations on how to handle spam. Symantec Brightmail 6.0 allows enterprise email administrators to define antispam rules in accordance with local laws.

End User Non-English Language Spam Filtering

A typical end user may speak two languages, but often receives spam in a variety of languages. Symantec Brightmail AntiSpam 6.0 allows an end user to select the language(s) that he wants treated as spam. The server will identify the language of the message and any message in those languages will be moved directly into the user's spam folder in Microsoft® Outlook®.

Features and Benefits

Multi-layered Spam Protection

Using 17 filtering technologies, Symantec Brightmail AntiSpam catches more spam while allowing legitimate email to reach end users.

- **Spam signatures**, highly accurate filters based on spam messages flowing into the Probe Network, protect against real-time spam attacks while safeguarding against false positives.
- **Heuristic filters** target new spam attacks. Unlike heuristic filtering technologies in other products, Symantec Brightmail AntiSpam administrators need never train filters to maintain effectiveness.
- **Reputation filters** leverage the reach and visibility of the Probe Network to filter messages based on the quality or the reputation of the sender.
- **Language identification** is part of a larger foundation of language-based technologies that allow Symantec Brightmail AntiSpam to stop spam messages that are written in different languages.

Benefits

- Promotes increased end user productivity by reducing time required to review, report, and delete spam.



- Decreases IT administrator time spent on managing the organization's spam problem.

Flexible Spam Management and Mail Policies

Allows the IT administrator to customize policies for handling spam, such as:

- Modify subject line or header to flag email determined as spam, i.e. email containing the phrase "Buy Now";
- Delete;
- Forward to an email address such as spam@symantec.com for review;
- Hold in an Administrator Quarantine (separate holding system) where users can view their spam email;

Per-user Quarantines

- Web-based quarantines provide both administrator and user quarantines.
- Groupware quarantines for Exchange and Domino sort spam into each recipient's spam folder, creating an easy-to-manage quarantine for messages identified as spam.

Customized Mail Policies

- Allow the IT administrator to create groups composed of domains, sub-domains or specific individuals.
- Allow the IT administrator to take different actions (delete, quarantine) for each disposition (spam, suspect spam, etc.) for each group.
- Allow the IT administrator to adjust the spam threshold

Benefit

Enables the IT administrator to meet the unique email requirements of end users and groups in the organization.

Powerful Administration

Provides the IT administrator with the ability to customize, configure, and monitor the system from a single centralized console.

- **Web-based Control Center**
- **Global management of multiple servers** allows the IT administrator to make changes quickly and consistently. The administrator only has to push out policy once for multiple servers.



- **Flexible LDAP integration** allows the IT administrator to connect to different types of LDAP servers and their configurations.
- **Role-based administration** provides flexible enhanced security at the granular level by allowing the IT administrator to assign different permissions. For example, a Help Desk can configure email, but only IT department personnel can start or stop the system. This allows the IT administrator to set what people in the organization can and cannot do.
- **System alerts** free the IT administrator from having to actively monitor systems. Proactive system alerts let the IT administrator know when a component has a problem.

Benefits

- Reduces time and effort to deploy email policies and oversee the system.
- Gives the IT administrator greater control, efficiency, peace of mind, and visibility into how the system is performing.

Reporting

Provides the IT administrator with data on mail flow and filtering activities. For example, reports demonstrating effectiveness show the percentage of all email caught as spam. Reports also show trends such as the percentage of email caught as spam going up or down.

- **Centralized and consolidated reports** and logs organize data from multiple servers.
- **Scheduled reports** automatically email reports at specified intervals.
- **Multiple categories** separate filtering by spam, suspected spam, allow lists, block lists, and others
- **Granular details** let the administrator view reports based on recipient, sender, recipient domain, sender domain, and IP address.

Benefits

- Gives IT administrators and managers visibility into how the system is delivering on its business function.
- Eliminates time spent manually gathering data on system performance.
- Helps organizations determine the effectiveness of their anti-spam investment.



Content Filtering

Allows the IT administrator to quickly write custom filters that flag specific message characteristics such as words, phrases, or attachment types.

- Custom content filters are written by the IT administrator using the Brightmail Control Center (web-based central administration) or the Sieve scripting language to tailor filtering to the needs of the organization
- Customize filtering using:
 - Block Lists – Block by sender, IP address or via DNS-based real-time lists
 - Allow Lists – Allow by sender, IP address or via DNS-based real-time lists (Administrators can create custom lists of allowed senders and blocked senders or can use third party lists. The lists included in the Brightmail Reputation Service are deployed by default.)
- Custom Filters Editor allows the IT administrator to write custom mail filters using any of 16 types of filters including subject or body keywords

Benefit

The definition of “unwanted” email is different for every corporation. Content filtering enables the IT administrator to revise or expand the definition of “unwanted” email to match the changing requirements of the organization.

Per-user Spam Control

Provides plug-ins and tools for popular email clients that give end users customization and configuration features for managing their email. For example, the language preference feature enables users to choose the language(s) in which they wish to receive email.

- **Plug-ins and agents** available for popular email clients provide powerful spam management tools for users such as the “This is Spam” button available in Outlook. A similar function is available for Lotus Notes® users.
- **Personal preference options** allow users to select languages, white lists, and black lists.
- **Allow/block lists** allow end users to create personal lists of blocked senders.
- **Language preference** allows end users to set language filtering preferences.
- **Submissions** forward messages flagged as “This is Spam” to Symantec for review.

Benefit



Enables end users to take control of their inboxes by giving them greater control over their message flow.

Comprehensive Threat Protection

Mitigates risk of multiple email threats.

- Optional antivirus feature scans and cleans messages for viruses and worms.
- Antivirus definitions and engines protect users from email-borne viruses

Benefit

Gives IT administrator and manager peace of mind. Single vendor interface facilitates system management. Procurement from a single vendor simplifies the purchase process.

Symantec Brightmail AntiSpam vs. Other Symantec Products

- Symantec Brightmail AntiSpam is separate from other Symantec products that provide spam protection, such as Symantec Mail Security for SMTP or Symantec AntiSpam for SMTP Gateways. Owning one of these products does *not* entitle a customer to receive a free copy of Symantec Brightmail AntiSpam.. There is no migration plan at this time.
- It delivers combined effectiveness (spam catch rate) and accuracy (false positive rate). It also has powerful administration (strong reporting, customization and management options), but does not require a significant amount of administration time.
- Symantec Brightmail AntiSpam 6.0 is sold on a pure subscription model, i.e., a per-user per-year cost paid upfront, rather than a perpetual license. A user is defined as a distinct email address that will receive spam filtering.
- Symantec Brightmail AntiSpam 6.0 includes optional AntiVirus protection (powered by the Symantec AntiVirus engine), which is also sold on a subscription basis. Note: this feature is not available as a standalone subscription without spam filtering.

System Requirements

Hardware Requirements

Hardware requirements vary depending on the number of email users and the amount of email traffic. The minimum specifications are suggested guidelines. These apply to computers with the following software installed:

- Brightmail Control Center
- Brightmail Scanner



Solaris™

Computer	UltraSparc processor
Operating system	Sun™ Solaris 8 or 9 (Solaris 8 requires Sun patch 112438)
Memory	512 MB RAM minimum
Available disk space	250 MB minimum

Windows®

Computer	Intel® Pentium® 4 or compatible
Operating system	Windows® 2000 Server or Windows Server 2003
Memory	512 MB RAM minimum
Available disk space	250 MB minimum

Linux®

Computer	Intel® Pentium® 4 or compatible
Operating system	Red Hat Linux ES/AS 3.0
Memory	512 MB RAM minimum
Available disk space	250 MB minimum

30-day Free Trial

As part of the sales process, Symantec can encourage prospects to download a 30-day free trial of the software from the Symantec Web site. Upon completing the Web-based form and downloading the software, the customers will receive a license file by email. This license will give the prospects the opportunity to deploy the product and receive updated antispam filters for 30 days. There are number of resources, such as an installation guides and an evaluation guide that will help prospects setup, deploy, and evaluate the solution. After the 30-day period, antispam filter updates will cease, and prospects will need to go to <http://www.symantecstore.com/renew>, or contact their sales representative to purchase the product.



Licensing Symantec Brightmail AntiSpam

Note the following details about the licensing process:

- Per-mailbox per-year subscription model. Customers purchase a subscription based on the number of mailboxes (distinct email accounts) that they want to protect. Unlike traditional Symantec products, it is not sold on a perpetual license model.
- Subscription includes: software, upgrades, 24x7 filter updates (content), and support.
- Subscription length: Customers purchase subscriptions for 1, 2 or 3 year terms, with discounts applied for terms over 1 year. By choosing a 2-year or 3-year subscription, customers can save approximately 13% and 26%, respectively, off the annual price.
- Optional antivirus protection*: Optional antivirus protection is available. Customers who want combined antis spam/antivirus protection must purchase an additional subscription for Symantec AntiVirus™. Antivirus protection is not available as a standalone subscription.

Symantec Brightmail AntiSpam 6.0 uses the Enterprise Licensing System (ELS). To begin operating according to the terms purchased, a new customer will do the following:

1. Receive Serial Number printed on the License Certificate following purchase.
2. Enter Serial Number at <https://licensing.symantec.com>.
3. Receive a ZIP archive file containing license material via email.
4. Extract ZIP to produce the license file (.slf extension).
5. Start the Symantec Brightmail AntiSpam Registration Wizard.
6. Specify the location of the license file (.slf extension).
7. Click Next or Enter to validate the license.

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. , BLOC, Brightmail, Brightmail AntiSpam and Symantec AntiVirus are trademarks of Symantec Corporation. Intel and Pentium are trademarks or registered trademarks of Intel Corporation. Microsoft, Outlook, Windows, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation. Other brands and products are trademarks of their respective holder(s). Copyright © 2004 Symantec Corporation. All rights reserved.