

Why to Subscribe to Symantec Premium AntiSpam

Symantec Premium AntiSpam™ add-on subscription service, powered by Brightmail technology and response, provides best-of-breed spam prevention for Symantec Mail Security™ and Symantec AntiVirus™ Enterprise Edition customers. It delivers the best combination of effectiveness and accuracy in the market today, without requiring manual rule creation or administrative overhead. The solution leverages over 20 filtering technologies, and offers a spam detection rate of 95% and the highest accuracy rate against false positives (99.9999%)*. Symantec Premium AntiSpam (SPA) is an integrated service for Symantec Mail Security customers. It does not require a separate server and can be activated by simply purchasing a subscription and entering a license key – no additional installation is required.

The primary difference between the existing spam tools in Symantec Mail Security (SMS) and the new Symantec Premium AntiSpam subscription is that SPA is a service offering, providing market-leading technologies and ongoing updates to catch the latest spam and stay ahead of spammer innovation.

Symantec Mail Security includes basic spam prevention tools – including real-time blacklisting, content filtering rules and heuristic spam analysis of messages – which require manual rule creation in order to achieve optimal detection rates. Used alone, these tools provide a lower spam detection rate and significantly higher false positive rate when compared to the Symantec Premium AntiSpam service. However, when SPA is activated in SMS, all tools

(except the AntiSpam Heuristics Engine), will still be available for rule creation, if desired.

Free administrators, reduce overhead, eliminate user complaints

Mail administrator(s) spend hours creating and tuning rules, to keep up with spam techniques as they continue to evolve. In addition, administrators must monitor their spam prevention solution to prevent false positives. This is not an efficient way to handle spam as it is prone to error and requires constant hands-on attention of the administrator – diverting their focus from other key IT projects.

Symantec Premium AntiSpam protects you from the most recent spamming techniques and automatically stops spam from reaching your users. The administrator does not need to define the content filtering rules since they are automatically set – eliminating an error-prone, inefficient process. Symantec Premium AntiSpam's false positive rate is only 1 in 1 million** – almost completely eliminating the misdetection of legitimate mail as spam. Users no longer complain that their legitimate business emails are not arriving and administrators do not need to spend hours searching through the quarantine to look for false positive messages.

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

** The Yankee Group



Automated, multi-layered spam detection

Symantec Premium AntiSpam automatically evaluates each message against multiple spam detection layers that are updated every 5-10 minutes. Each message passes through the different layers and is then scored and classified as spam, potential spam or a legitimate message (see Figure 1). Administrators pre-set how to handle spam based on this score. Legitimate messages are delivered to the recipients, and spam and potential spam can be rejected, quarantined, modified or sent to an alternative recipient.

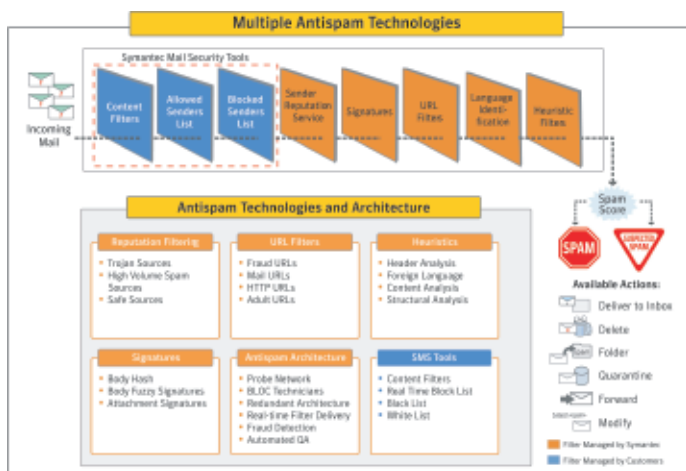


Figure 1. Layers of detection

Multi-layered spam detection is the best approach to accurately identify spam rather than relying on the score of a single filter. Symantec Premium AntiSpam adds the following layers to the existing tools found in Symantec Mail Security:

Symantec Reputation Service

The Symantec Reputation Service evaluates messages against three lists:

- The Open Proxy List - a dynamic database containing IP addresses of identity-masking relays, including proxy servers with open or insecure ports.
- The Safe List - a list of IP addresses from which virtually no outgoing email is spam.
- The Suspect List - a list of IP addresses from which virtually all of the outgoing email is spam.

Signature Filters

When messages flow into Symantec's Brightmail Logistics and Operations Centers (BLOC), they are characterized using proprietary algorithms into a unique signature, which is added to the database of known spam. Using this signature, seemingly random messages that originated from a single attack are grouped into signature files. By distilling a complex and evolving attack to its DNA, more spam can be deflected with a single filter. Signature Filters include BrightSig2 Filters, Body Hash Filters and Attachment Filters.

URL Filtering

Spam containing a URL call-to-action is increasingly pervasive because spammers want to direct readers to a specific Web site for contact information or purchasing instructions. URL Filters catch messages based on specific URLs found in spam. Although these URLs do not change frequently, spammers attempt to obfuscate and disguise them. As a result, these URLs appear to be unique across similar spam messages.

Header Filters

Header Filters are regular expression-based filters that are applied to the header lines of a message. Header Filters can be used to compare email messages to spam messages seen

by BLOC, and to exploit commonalities or trends present in spam messages.

Heuristics Engine

Heuristic filters target new spam attacks by evaluating messages against characteristics of spam and characteristics of legitimate mail. Unlike other products, the heuristic engine does not require manual updates as the engine is frequently retrained and updated by Symantec.

Fighting spam around the clock

Symantec Premium AntiSpam is backed by the same BLOC infrastructure used in our Symantec Brightmail AntiSpam product. This includes the Probe Network, which consists of over 300 million email users and over 2 million decoy mailboxes used to monitor spam and detect and respond to new spamming techniques. The Probe Network generates signature files, trains the heuristic engine, updates URL filtering lists and keeps the Symantec Reputation Service lists up-to-date. Immediate response to new spamming threats is important to your business and only Symantec sends you automatic updates every 5-10 minutes based on the latest information gathered by the Probe Network.

Stop spam in any language

Non-English spam is becoming more and more of a problem for national and international organizations. Symantec has worked with numerous global customers to build its 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.

Symantec Premium AntiSpam examines the contents of a message to determine its language. Once the language of the message is identified, Symantec 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. Symantec Premium AntiSpam includes a series of new heuristics that target specific languages other than English.

In addition, the Outlook plug-in – available with Symantec Premium AntiSpam – allows users to choose which languages they want to receive mail in. All other languages are then rejected as spam.

Conclusion

Spam is constantly evolving and manual processes alone are not enough to ensure accurate detection and prevention. A service-based solution provides hands-free response, better accuracy and fewer false positives. It also frees IT resources for more strategic tasks.

Symantec provides antispam capabilities to 9 out of the top 12 ISPs. The unique Probe Network ensures that Symantec can quickly respond to new trends and techniques and our ability to deliver updates frequently ensures fast response and accurate detection.

Adding a Symantec Premium AntiSpam subscription to an existing Symantec Mail Security installation allows

Overview: Why to Subscribe to Symantec Premium AntiSpam

customers to take advantage of Brightmail technology and response within an application they are already familiar with. No additional installation or hardware is required – simply install a license key to the Symantec Mail Security product to activate Symantec Premium Antispam.

Symantec Mail Security customers should evaluate Symantec Premium AntiSpam, powered by Brightmail technology and response, in their organization to see the impact of this industry leading service that offers a spam detection rate of 95% and the highest accuracy rate against false positives (99.9999%)*.

More information

Visit our Web site

<http://enterprisesecurity.symantec.com>

To speak with a Product Specialist in the US

Call toll-free 800 745 6054

To speak with a Product Specialist outside the US

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

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

Symantec World Headquarters

20330 Stevens Creek Blvd.

Cupertino, CA 95014 USA

408 517 8000

800 721 3934

www.symantec.com

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



Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Other brands and products are trademarks of their respective holder/s. Copyright © 2004 Symantec Corporation. All rights reserved. Printed in the U.S.A. All product information is subject to change without notice.

12/04 10351118