

Operations

Butler Group Subscription Services

Security and Policy Management

TECHNOLOGY AUDIT

Symantec

Symantec Mail Security 8000 Family Appliances

Abstract *Symantec Mail Security 8000 Family of Appliances provide a range of protection from e-mail threats including anti-spam, anti-virus, and content control. Many e-mail users have to spend increasing amounts of time dealing with spam, which organisations have to install additional mail servers and other infrastructure to handle. A strength of the Symantec approach, are the integrated solutions that have been developed to address the problem of spam, which include anti-spam and anti-virus filters, and traffic shaping technology, operating at the TCP level, and implemented at the organisation's boundary and mail gateways. The SMS 8240 is an entry-level device, which is best suited to organisations with up to 1,000 users, while the SMS 8260 has been designed to cater for organisations with more than 1,000 users. Because it deals with TCP Traffic Shaping the 8160 has been designed for organisations and ISPs with very high mail streams and generally more than 2,000 users. In Butler Group's opinion, Symantec offers a range of mail security products that will satisfy the requirements of most organisations.*

KEY FINDINGS

- | | |
|--|--|
| ✓ An integrated approach to anti-spam. | ✓ Uses traffic shaping before spam hits the network. |
| ✓ Basic policy management included. | ✓ Uses honey pots to gather information about spam. |
| ✓ BLOC correlates information about spam for Reputation Lists. | ✓ The 8000 Family of Appliances are designed for distributed environments. |

Key: ✓ Product Strength ✗ Product Weakness ⓘ Point of Information

LOOK AHEAD

Symantec does not release details of specific functionality updates for its product-range, but there is a plan to release a new version of the software towards the beginning of the second half of 2005, with the next version of the hardware coming around the end of 2005.

► FUNCTIONALITY

Spam has become a real issue for virtually all organisations that utilise e-mail, creating a wide range of problems. Some of the most commonly claimed issues are the time that end-users spend on a daily basis dealing with spam, the general increase in e-mail traffic caused by spam, the additional storage space, back-up, and other infrastructure resources required for the spam, and the increased difficulty in searching an e-mail system which is full of spam. A less known, but potentially more damaging issue, is that of end-users' computers being high-jacked by spammers to distribute spam e-mails, which could potentially result in the company being held responsible for distributing unsolicited e-mails.

Many organisations are implementing anti-spam filters, but the skill of the perpetrators in amending their spam e-mails to fool the filters into letting their e-mails through can render these ineffective. This means that an administrator has to continuously update the rules for the filters that block spam, which becomes an onerous and time-consuming task.

In eliminating spam many filters issue a high number of false positives – genuine e-mails that are unnecessarily blocked. One way of addressing this problem is by quarantining all blocked e-mails, but this then requires someone to check these e-mails to identify the false positives – another time-consuming exercise.

Butler Group believes that the only way to successfully address the spam issue is to implement a number of measures to block unsolicited e-mails, and Symantec is one vendor that offers a range of anti-spam and anti-virus solutions.

Product Analysis

Symantec provides e-mail protection in the areas of e-mail firewall, anti-spam filtering, anti-virus scanning, content compliance, and message integrity. The company has extended its model from selling software solutions only. It also now sells appliances on top of which sit software, which is provided on a subscription basis.

Symantec Mail Security 8160 shapes traffic at the TCP protocol level by slowing down or throttling the spammers' connection to the extent that the spam messages back up on the spammers' servers. This can be used in conjunction with Symantec Mail Security 8200 Series appliances, which are anti-spam gateway solutions that provide an easily deployed and managed multi-layered approach to combat spam. These use Symantec Brightmail AntiSpam technology. This ability to provide a complete anti-spam solution is one of the strengths of the Symantec approach.

One of the tricks of the spammers is to highjack innocent users' machines, which are used temporarily as hosts to push out spam. Because the sophistication of anti-spam software is continuously improving, it is possible to identify the source of spam relatively quickly. Therefore highjacked machines are generally only used to distribute a limited number of e-mails, before the spammer moves onto another innocent users' machine. Symantec has reacted to this pattern by providing the ability to throttle traffic from a suspect address for a defined amount of time, for example, for 30 or 60 minutes. This means that genuine e-mail from the sender will not be blocked permanently, which it would be if it was blacklisted.

There will also be instances when the filters are unable to determine, with a high level of confidence, whether a series of e-mails from a single source are spam or not from the content alone. There may be a large number of e-mails going to a single domain with a high incidence of misspelled names.

One of the tricks of a spammer is to carry out Directory Harvest Attacks, a method where spammers target a domain with multiple combinations of forenames and surnames. In most cases when a mail system receives an incorrectly addressed e-mail, it will reply to the sender that no such recipient exists. By comparing the original list of sent e-mails and the returned responses, the spammer can then create a list of valid e-mail addresses that can be sold to other spammers.

However, a legitimate e-mail sender can make mistakes in addressing e-mails to multiple recipients. Therefore, in cases where there are some misspelled names, a preferable option is to slow down or throttle the traffic for a period of time, and to continue to analyse the traffic for anomalies. If there are only a few incorrectly spelt addresses in the batch, then the chances are that it is not spam, and the rest of the batch can be released after the defined time period expires.

Symantec's anti-spam products are policy-driven, and the Symantec Brightmail Logitics and Operations Centers (BLOC) administrators develop the rules to trap spam. End-users can create their own whitelists as well as blocked lists of e-mail addresses that they wish to receive e-mails from. There are a number of actions that can be initiated when suspected spam is received. It can immediately be archived, an alert may be sent to an administrator, or it may be quarantined. Users may use a Web-based interface to view their own quarantined e-mails, in order to decide whether they wish to receive them.

Although Symantec does not provide policy management to the extent of a dedicated policy management solution, it does include the ability to prevent certain e-mails from being sent based on rules that are defined. It can also be used to remove attachments from e-mails, or annotate e-mails, for example, by adding a disclaimer to outbound e-mails, based on the identity of the sender.

Product Operation

The 8200 series has been designed to operate in distributed environments where there are multiple mail servers at different locations. Central administration is provided via a Control Center, which pushes out and applies updated configuration settings, software updates, and LDAP directory changes to scanners, which are deployed in front of each mail server. Pulled back and consolidated from each scanner are: logs, statistics for reporting, and mail queue information. Extensive reports are provided, for example, the top addresses receiving e-mail, the top addresses sending e-mail, the top sources of e-mail, or e-mails with attachments over a certain size.

There are a number of ways in which Symantec identifies spam. The SMS 8160 provides Traffic Shaping at the TCP level, on the network boundary. It provides the ability to throttle back the receipt of e-mails from spam addresses, which results in spam being backed up on the spammers' sites. Another action that can be taken is to permanently throttle the traffic from a particular address for a defined period of time, for example 30 minutes or one hour, which should provide enough time for a spammer to move to another address to send e-mail from. This allows for a zero false-positive solution.

This is preferable to utilising a blacklist, as most spammers now use this highjacking method to distribute spam. There would therefore be little point in permanently blocking e-mail from each of these addresses. Symantec believes that incoming e-mail traffic is reduced up to 50% by using the SMS 8160. The major benefit, in Butler Group's opinion, is that this occurs before the spam impacts on the network, and this has the greatest effect on larger enterprises and Internet Service Providers (ISPs) who have the greatest volumes of e-mails.

It is our view that this should not be the only level of protection taken by an organisation. Symantec provides an integrated approach to e-mail security. As part of its anti-spam solutions, it deploys a number of methods to collect information about spammers. It has more than two million honey pots, or spam traps, which are e-mail addresses that do not have a legitimate user assigned to them, and therefore would not normally receive any e-mail.

These addresses are distributed widely over the Web. Any mail received by these addresses is unsolicited, and they receive tens of millions of spam messages each day. All of the information from these messages is sent to the BLOC, where it is analysed. Despite the increasingly sophisticated tricks of the spammers to hide the origin of their e-mails, such as disguising the fact that they are bulk mailings by making each message unique, it is possible to trace messages back to individual spammers. Using this information, Symantec produces spam filters, which are updated every ten minutes to reflect the changes in the behaviour of spammers.

Symantec also provides the Symantec Reputation Services, which examine the mail of all of the mailboxes that are being protected by Symantec, which the company estimates at approximately 300 million, or about 25% of the total e-mail boxes on the Internet. Approximately 120 billion e-mails are scanned every month and this information is used by the Symantec Reputation Services. Every time an e-mail is received by a protected e-mail address, it goes through the filtering process where it receives a spam rating from 0 to 100%, with 0 providing a 100% confidence rating that the e-mail is legitimate, and 100 providing a 100% certainty that the mail is spam.

E-mails are sent back to the BLOC for analysis and correlation, where the originating IP address and the spam score for the sender are examined. From the information gained, organisations are able to set thresholds below which they can be confident that e-mails are legitimate, and above which e-mails are spam. Between these two thresholds they can then monitor mail more closely. Symantec claims that at least 95% of spam can be captured, and that the system has 99.9999% accuracy with less than one in a million legitimate e-mails incorrectly classified as spam. From all of the information received and analysed by the BLOC, the Symantec Reputation Lists are produced, which are updated and distributed every hour.

Symantec claims that customers generally start by quarantining e-mails deemed to be spam, but because of the accuracy of the system many end up deleting these e-mails as soon as they are detected.

The SMS 8200 employs some of the above techniques to provide organisations with a high level of protection. It provides threat protection by utilising the Symantec Reputation Lists, and helps to prevent directory harvest attacks through firewall protection. It also provides anti-spam filtering through Brightmail AntiSpam technology, and anti-virus protection with Symantec AntiVirus technology.

Product Emphasis

Many organisations have no idea how to deal with the problem of spam, particularly if they have to retain e-mails for compliance purposes. Some choose to process and retain spam alongside their legitimate e-mails to prove to a regulator that they are routinely retaining all e-mails. However, this approach requires additional resources to process this high volume of e-mails. A better approach in our opinion, is to reduce the volume of spam before it reaches the organisation's mail servers, which can be achieved using the traffic shaping technology of the 8160. For organisations for which the 8160 cannot be justified, there are still a number of options available that virtually eliminate spam using Symantec's filtering techniques. The accuracy of the technology, affords organisations a level of confidence that if they choose to retain spam for compliance purposes, they can afford to give it a short retention period, and be sure that they are only deleting spam and not content that needs to be retained.

► DEPLOYMENT

The Symantec appliances are simple to install, and a task that an organisation would normally undertake itself. For the 8200, implementation involves putting the appliance into a rack, plugging it in, and configuring it, which can take as little as 15 minutes. An implementation of the 8160 may require advice from a Symantec Sales Engineer, particularly if it is a large deployment, to ensure that the product is configured correctly.

The implementation is an area where partners of Symantec can add value. Although in small and medium sized companies deployment may be a simple process, in complex environments that process many thousands or millions of e-mails per day, there will be a large amount of configuration. An implementation takes on average around half a day for the appliance and software, but very large implementations may take longer.

Symantec has a comprehensive training scheme for partners, which includes classroom and Web-based training, which lead to certification. Partners generally train customers, typically during the implementation.

The appliances can be implemented in a modular fashion in that they may be deployed at multiple gateways, with new gateways added as the organisation grows. All of the appliances are managed from a single central console, regardless of where they are deployed. Customers are also able to choose the software coverage they require for the subscription model from anti-spam, antivirus, or a combination of both. Management of the appliances is minimal, with the major overhead being the analysis of the report that can be generated.

Technical support is provided through Symantec's Tech Support. Gold support incorporates office hours support, which includes next day repair for the appliance, and is included in the price of the product. Platinum support includes full 24x7 support and same day on-site repair of the appliance.

It is a self-contained appliance, which does not require any special hardware. It runs on general-purpose hardware with hardened Linux operating systems along with a hardened Message Transfer Agent, and is not dependent on any third-party products.

Upgrade paths are available for customers of Symantec Brightmail AntiSpam software. The customer simply purchases the appliance and then changes its subscription model to the one appropriate for the appliance.

Licensing is based on purchasing the appliance required, which can be the 8160, 8240, or the 8260. All of these are delivered with a three-year warranty. There are a number of subscription options. Traffic Shaping is the only option with the 8100 Series. The 8200 Series have the option of anti-spam and anti-virus software, or a combination of both.

► PRODUCT STRATEGY

The target market for the appliances is horizontal rather than vertical, as spam affects every organisation that uses e-mail. In terms of company size the SMS 8240, as an entry-level device is targeted at organisations with up to 1,000 users. The SMS 8260 has been designed to cater for organisations with more than 1,000 users. Because it deals with TCP Traffic Shaping, as its major defence against spam, the 8160 has been designed for organisations with very high mail streams, which is typically organisations with more than 2,000 users, and it is also suited to ISPs.

Return On Investment (ROI) is always difficult to calculate for a security product, where the benefits are difficult to assess. However, with an anti-spam solution Butler Group believes that it is easy to calculate the potential return.

It is a relatively simple task for organisations to calculate the total size of their mail flow, including the percentage of spam, and the size of attachments. Once they know the percentage of spam e-mails they are receiving it is relatively easy to calculate how many gateways they require to handle the spam, the number of mail servers and archiving servers, the load on the internal network infrastructure, the number of staff required to administer the mail infrastructure, and most important for managers how much time users are wasting each day dealing with spam. Using this information it is a simple task to calculate the savings, in terms of the reduced resources required, based on the elimination of spam.

Symantec sees its major market opportunity deriving from the growth of spam, which is currently running at around 60% in Europe, and between 80% and 90% in the US. The company expects to see the European figure match that of the US in the near future. Butler Group believes that another opportunity derives from compliance, and a need for organisations to better manage their e-mails and bring the spam issue under control to reduce the size of their archives and improve the discovery and retrieval process.

Symantec's route to market is through the channel. Although it does have a direct sales force, all sales are directed to and fulfilled by the channel. Symantec has many partners ranging from large System Integrators (SIs), to smaller partners.

The major technology partner is Dell, with whom Symantec has a Original Equipment Manufacturer (OEM) deal for the supply of the appliances.

Symantec competes with other anti-spam and anti-virus software vendors, as well as companies that provide these types of protection as a service.

Licensing is different to most solutions. Customers buy the appliance, and the software is offered on a subscription basis, for one, two, or three years, with gold support and next business day on-site repair included in the price. Full 24x7 support and same business day on-site repair is additional and has to be selected at the time of purchase.

Because of the nature of its product, Symantec has a number of different release strategies. The spam filters are updated every ten minutes. The Symantec Reputation Service is updated every hour. The anti-virus software is updated every time a new virus is detected, which can range from several times a day to every few days. Enhancements to the product are planned for about every six months, which is approximately mid-way between major releases. Finally, major releases are planned for once a year, and these incorporate extensive functionality updates.

► COMPANY PROFILE

Symantec was founded in 1982, and is headquartered in Cupertino, California, USA. Employing over 5,000 staff across 36 countries, the company has offices across North America, South America, Europe, and Asia-Pacific, including: Argentina, Australia, Brazil, Canada, China, France, Germany, India, Italy, Japan, Russia, South Africa, Spain, UAE, and the UK.

Symantec is a publicly listed company (NASDAQ = SYMC), and has a corporate mission statement to become the trusted security partner for individuals and enterprises around the world. Currently Symantec provides comprehensive Internet security products, solutions, and services for more than 125 million users worldwide. These range from the largest corporate enterprises, service providers, government agencies, and higher education institutions, to small businesses users and individuals.

Reported revenues for the last three fiscal years are as follows:

March Year End	2004 (US\$ millions)	2003 (US\$ millions)	2002 (US\$ millions)
Revenues	1,870	1,407	1,071

► SUMMARY

The security market place is consolidating, which has left a small number of vendors that offer comprehensive solutions, of which e-mail management is an important element. These companies face stiff competition from vendors who offer e-mail security services, including anti-spam and anti-virus. However, Butler Group believes that there will always be a high proportion of organisations that either for compliance purposes or out of preference prefer to take care of e-mail security themselves. Symantec has developed a number of solutions that handle all aspects of e-mail security, which will suit the requirements of most organisations that process large volumes of e-mail and for whom spam has become an issue, which is impacting on the company.

► CONTACT DETAILS

Symantec Corporation
 World Headquarters
 20330 Stevens Creek Blvd.
 Cupertino
 CA 95014
 USA
 Tel: +1 (408) 517 8000

www.symantec.com

Symantec United Kingdom Ltd.
 Hines Meadow
 St. Cloud Way
 Maidenhead, Berkshire
 SL6 8XB
 UK
 Tel: +44 (0)1628 592222
 Fax: +44 (0)1628 592393

www.symantec.co.uk

Important Notice:

This report contains data and information up-to-date and correct to the best of our knowledge at the time of preparation. The data and information comes from a variety of sources outside our direct control, therefore Butler Direct Limited cannot give any guarantees relating to the content of this report. Ultimate responsibility for all interpretations of, and use of, data, information and commentary in this report remains with you. Butler Direct Limited will not be liable for any interpretations or decisions made by you.

About Butler Group:

Butler Group is the premier European provider of Information Technology research, analysis, and advice. Founded in 1990 by Martin Butler, the Company is respected throughout the business world for the impartiality and incisiveness of its research and opinion. Butler Group provides a comprehensive portfolio of Research, Events, and Subscription Services, catering for the specialised needs of all levels of executive, from IT professionals to senior managers and board directors.

For more information on Butler Group's
Subscription Services, contact:

Europa House, 184 Ferensway, Hull, East Yorkshire, HU1 3UT, UK
Tel: +44 (0)1482 586149 Fax: +44 (0)1482 323577 www.butlergroup.com