

Symantec Brightmail Operations

Email borne threats continue to increase in volume and complexity, and today's threats are more dangerous and potent than ever before. These threats pose a tremendous risk to individuals and organizations, damaging IT assets, threatening intellectual property, and adversely affecting employee productivity. Symantec, the industry leader in security solutions, offers a range of products that protect organizations from threats such as spam, viruses, phishing attacks, and other types of malware. With advanced capabilities in gathering intelligence on threats, an extensive collection of people and processes dedicated to fighting malware, and sophisticated technologies built into a range of award-winning products, Symantec is the preferred partner to organizations across all industries to help protect valuable information and ensure systems are available.

Intelligence Gathering

Symantec leverages multiple sources to gather intelligence and data on spam, viruses and other types of malware. This data is analyzed and leveraged by Symantec's portfolio of solutions to help customers protect their organizations from threats to their messaging systems, IT infrastructure, and valuable data.

Symantec Global Intelligence Network

At the core of Symantec's backend technologies is the Symantec Global Intelligence Network, which encompasses some of the most extensive sources of Internet threat data in the world to offer comprehensive and up-to-date protection against the latest threats. Elements of the Global Intelligence Network include:

- Monitored security devices in more than 70 countries, allowing Symantec to understand key threats that are impacting corporate networks. These devices log more than 2 billion events daily
- 40,000 registered sensors in more than 200 countries which determine if new threats are localized, global, or targeted against a specific industry
- More than 120 million virus submission systems provide the insight to determine if these are new threats, variants of existing threats, or renewed activity from existing threats. These generate more than 200,000 code samples daily – which are analyzed by Symantec analysts

In addition, the Global Intelligence Network includes a number of additional sensors tracking data specific to:

- Vulnerabilities: Symantec maintains one of the world's most comprehensive vulnerability databases
- Symantec Honeynet: A virtual network of unprotected systems designed to attract malicious activity
- Symantec Probe Network: more than two and a half million decoy email accounts focused on collecting fraud, phishing and spam samples

Probe Network

The Symantec Probe Network is a patented system of more than 2.5 million decoy email accounts focused on collecting fraud, phishing, and spam samples. The Probe Network has a global presence, including targeted deployments for foreign language content, and can gauge global spam and phishing activity. This network gathers more than 30 million probe messages per day. On a broader scale, Symantec also collects anonymous customer statistics on billions of email messages daily. . Symantec protects over 800 million mailboxes against spam and virus threats. Customers can submit messages to Symantec, which automatically conducts an assessment on these messages to determine if they are legitimate. If a message is deemed illegitimate, automatic rules and filters are created, which are in turn pushed out to customer sites to protect them against such attacks.

Report Generation and Portals

Symantec makes it simple for customers to access to Symantec's backend data through report generation and web portals. Symantec publishes a yearly report, the Symantec Internet Security Threat Report, that provides a detailed update of worldwide Internet threat activity and includes:

- Yearly Report:

The Symantec Internet Security Threat Report, provides a detailed update of worldwide Internet threat activity and includes analysis of network-based attacks, reviews of known vulnerabilities, highlights of malicious code, and an assessment of trends in phishing and spam activity.

The latest Internet Security Threat Report can be found at www.symantec.com/threatreport.

- Monthly Report

The State of Spam report goes into detail on current spam and malware trends. The report is available at www.symantec.com/spam.

- Daily Portal

Brightmail IQ Services provides real-time access to the latest spam trends and IP reputation. Reporting live data directly from Symantec's extensive collection of global data, this portal is the latest offering in Symantec's portfolio of back-end access tools.

Security Operations

Symantec leverages automated systems and various tools to gather intelligence globally, in addition to a skilled team of people behind this vast network, which plays a key role in processing and analyzing the data generated by the Global Intelligence Network. This highly skilled group of people and these automated processes and tools generate frequent updates to email security and virus defenses at customer sites. Symantec products at customer sites then process data based on these updated filters, reputation information and virus definitions.

Security Response

Symantec's Security Response team has been combating threats for over 15 years and consists of more than 200 security specialists working around the clock, 365 days a year. Security research centers around the world provide unparalleled analysis of and protection from malware, security risks, and vulnerabilities

In addition to the more than 200 Security Response specialists, Symantec has a global team of intrusion experts, security engineers, virus hunters, threat analysts, and technical support professionals who provide fast and accurate analysis of security data - 24 x 7 - to help customers guard against complex Internet threats and other security risks.

Anti Spam Technology Group

Anti Spam researchers and software developers are tightly integrated with operations teams. The result is fast and efficient feedback loops where new threats drive immediate response as well as ongoing Research and Development. The Anti Spam Technology group is responsible for bringing new technologies to bear to combat latest threats.

Technology

Antispam and Antivirus

The Brightmail Antispam™ engine has been fighting spam for more than 10 years. Unlike many other competitors, Symantec's Brightmail engine employs a toolkit of many different antispam technologies generated over several years. These technologies can be categorized at a high level into two buckets – reputation-based and content-based approaches. Reputation looks at the threat sending history and potential of a particular IP address, while content filters look at the actual email content to determine if a message is spam. This toolkit approach allows Symantec to quickly and automatically generate the majority of rules and heuristics that offer the best balance between effectiveness, accuracy, and performance. Additionally, due to the breadth of technology available, Symantec has the ability to catch newest threats associated with the leading edge of spam. Automatic rule generation is enhanced by a team of analysts that review and optimize defenses against the most complex threats.

The Symantec AntiVirus™ engine similarly uses a breadth of technologies. In particular, the antivirus engine combines both traditional signatures and definitions, generated by the in-field submissions, with advanced heuristics and day zero technology for identifying never before seen threats. The combination of reactive and proactive technologies has allowed Symantec to record more than 40 consecutive VB100 scores, a designation made by the independent Virus Bulletin test center for catching all “in-the-wild” viruses during a test cycle, an unbroken track record since November 1999. Symantec leads the market in antivirus performance and identification.

Content Filtering and Data Loss Prevention

Symantec Brightmail technologies include an advanced content filtering engine and compliance workflow to ensure that corporate and regulatory policies can be effectively implemented over email. The innovative filtering engine includes the ability to do traditional control filtering, using regular expressions, keywords, dictionaries, and attachments lists, combined with advanced technologies such as true filetyping of attachments and structured data matching from Symantec Data Loss Prevention. Compliance workflow includes the ability to create complex conditions including Boolean logic, multiple verdicts per message, and flexible actions such as archiving or enforcing TLS encryption.

Bringing it All Together

The combination of Symantec's intelligence gathering, security operations and technology, creates a formidable defense for organizations against today's threats and complex malware. Protecting valuable data and assets is more important than ever, and ensuring up-time and employee productivity is key to an organization's economic and competitive success. Symantec allows organizations to focus on selling their products to their customers knowing that their information is protected and safe.

Visit our website

<http://enterprise.symantec.com>

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com