WHITE PAPER:
EMAIL SECURITY

Choosing a Cost-Effective Email Solution

Who should read this paper

Symantec.cloud

WHITE PAPER: EMAIL SECURITY

Choosing a Cost-Effective Email Solution

Contents

Symantec.cloud

Introduction

Managing a portfolio of IT projects is one of the most complex, costly and resource intensive activities that organizations face. In today's sluggish economy, many companies are facing IT budget cuts, which means it's essential to make every IT dollar stretch further.

With a limited budget come limited resources to effectively manage operational performance objectives. Past investments in hardware and software are costly to scale to meet shifting business needs. Hardware and software solutions may require expensive upgrades and maintenance to support new demands and to combat risks arising from new sources and emerging technologies. Additionally, some of these approaches may not conform to the ever changing business governance standards or compliance requirements.

To keep up with the competition, to meet growing needs, and to protect critical data, an organization must make investments in new systems, but must do so within the constraints of shrinking IT budgets and fewer resources.

Reduced IT Spending

Gartner's CIO survey in mid 2009 indicated that 2009 budgets for IT were expected to drop 4.7% below 2008 levels on average.[1] Gartner also indicated CIO and IT executive's budgets would not see any increase in 2010 or 2011. As budgets tighten, it becomes more difficult to keep up with new threats to email security.

Email is arguably the prime communication channel for business, so keeping email secure and functioning has assumed the highest priority. Every day, organizations face potential communications, operations, and intellectual-property disruption from spam and other email borne threats.

Spam now accounts for over 85% of an organization's total email volume on average.

The sophistication of email threats has evolved, going beyond just virus and spam. Virus, spam, and spyware writers are now taking advantage of each other's methods. As a result, different types of attacks have started to merge and pose severe threats to your organization, leading to a significant increase in email-related costs.

Techniques such as image spam use up considerable processing and storage, while spam is also being used to disseminate fraudulent content and steal personal information.

Sophisticated Attacks

Threats to email security have evolved into sophisticated domestic and foreign attacks designed to capture financial, personal, or strategic business information. Threats now come in the form of deliberately malicious acts and exploitive opportunities for hackers and cyber criminals. The impact is serious, and the landscape of victims is getting broader every day. It's evident that no organization can afford to have its network unprotected.

In fact, about one of every 1.12 email messages is spam; about one in every 284 messages contains a virus or Trojan threat; and one in five employees will handle some form of harmful Web content.[2]

Spam now accounts for over 85% of an organization's total email volume on average.[3] More disturbing is the fact that a growing percentage of that spam contains links to malicious websites that host malware. Following this same trend, malware is reaching out to malicious sites to execute additional malware or transmit stolen data. Such attacks fall into the vendor category of "web threats," a category that has grown more than 1,500% over the past two years.

1-McGee, Ken. "Predicts 2010: CIOs and IT Executives Brace for a Tough Year, Even as Economic Indicators Improve," Gartner, Research ID# G00173506, 12/15/2009.
2-MessageLabs Intelligence: 2010 Annual Report
3-Ibid

The magnitude of Web threats and their consequences would make the prospect of protecting, managing, and securing business networks and information a challenge for any organization, but especially one with a restricted budget and limited resources.

One way to sustain and enhance security while optimizing budget monies is to find solutions that are cost-effective and optimize your existing investments in technology, people, and processes.

Appliances

A network appliance is a physical device designed to stand in front of a company's mail server and reject unwanted traffic before it reaches servers or desktops.

Appliances used for Web security, policy control, and to prevent data leakage are intended to validate website certificates to avoid phishing scams or similar security issues, to protect confidential and proprietary information, and to monitor and control sensitive data.

The number of antivirus and antispam appliances has mushroomed lately, with solutions to handle mail servers of all sizes. All are based on industry-standard server hardware, typically running a security-hardened Unix/Linux Operating Systems to provide the platform for mail screening software.

Administration of an appliance can be a time-consuming chore. Management is done via a browser with tools to monitor activity and manage the antivirus and antispam rules, custom black and white lists, and other filtering options. Blocked or quarantined messages can also be examined via the GUI, and some products allow end users to do this themselves.

Comprehensive solutions for defending email systems are often embodied as standalone hardware appliances. But for companies grappling with limited IT staff, any extra box means extra headaches. For them, outsourcing email security to one of the growing number of service providers is a quick, no-fuss way of protecting internal email systems.

– Tech & Trends Magazine

The practicality of appliances is unpredictable because of the patch management, updates, user licenses, and bandwidth usage. There are hidden expenses that come with owning appliances that prevent these devices from being cost-effective.

Patch management is the process of using a strategy to determine which patches should be applied to which systems at a specified time. This process involves determining system vulnerabilities, establishing a baseline of acceptable risk, and then installing the patches. This approach is difficult because an application is part of a larger, more complex system in which changes to one component can dramatically alter the functionality of the whole system.

An antispam appliance is not in itself adequate to protect against internal virus infections. Viruses can enter a LAN via a roaming USB drive, a laptop brought in from the outside, and many other ways. This means that network and perimeter security may be susceptible to increased risks if organizations solely rely on appliance based security solutions.

Depending upon the appliance, implementing and configuring an appliance could require just a few mouse-clicks or a long, complex, costly implementation process of trial and error to get the product working according to a company's specifications.

Desktop AntiVirus Technology

Desktop antivirus solutions are designed to be installed on PCs and laptops to provide protection against viruses. Some industry analysts are proclaiming that this traditional, desktop method used to detect and eradicate viruses, Trojans, spyware, and other malicious code is outmoded.

The main reason is that traditional solutions can't keep up with the flood of virus variants manufactured by a criminal underworld that is beating antivirus vendors at their own game.

In 2010, Symantec.cloud identified and blocked over 339,600 different malware strains in emails, representing over a hundredfold increase compared with 2009.[4]

In the two decades since the first viruses appeared, most antivirus vendors continue to push the same traditional technology. Feature sets have been added and functionality improved, but the products haven't evolved as rapidly as the capabilities of viruses, worms, and botnets.

Products in this category are usually targeted at retail consumers. The reason is that professional IT departments have better things to do than go to every PC and install, configure, lock down, manage, upgrade, tune, train, and fix desktop email security products.

"It's the beginning of the end for antivirus software. The approach antivirus software vendors take is completely wrong. The criminals who are working to release viruses against computer users are testing against antivirus software. They know what works and how to create variants."

– Robin Bloor, partner at consulting firm Hurwitz & Associates

In its test of ten leading desktop antivirus products that focused on effectiveness against attack mechanisms designed to fool or disable antivirus protection, Information Security magazine found that "many antivirus products are surprisingly easy to defeat; they can't detect malware using alternative attack vectors; and they're difficult to manage."

Desktop email security is unattractive to businesses because it's expensive to administer. The labor costs involved with these products usually far exceeds the benefits provided. Even worse, by blocking spam and viruses at the desktop, a company allows unwanted and malicious traffic to travel through its mail server, exposing the server at significant risk.

Cloud Email Security Service

While a host of network appliances and software solutions may claim to effectively address email security issues, they can't offer the same level of expertise, ease of use, convenience, and cost control that an outsourced cloud based service provides.

With a cloud based service, a company can quickly and easily implement and deploy protection at a predictable cost while taking away some of the appliances or in addition to them, which can help an IT group stay within its budget.

By leveraging a cloud security services provider, IT managers can maximize internal resources by focusing on strategically important network enhancements that can help grow business and increase productivity instead of focusing on ongoing operations. Cloud security services from service providers can scale from simple equipment monitoring to comprehensive security management and remote site support with dedicated resources, providing IT organizations with tremendous flexibility and control while minimizing security risks and reducing total cost of ownership.

4-MessageLabs Intelligence: 2010 Annual Security Report

Beyond the advantages of improved resource optimization, businesses can realize cost savings by eliminating the capital expense of acquiring appliances or software licenses, and the implementation, lifecycle management and maintenance costs associated with hardware and software products. Cloud services offer a predictable cost and scalability to help businesses address security needs without extensive resources or investments.

Businesses are turning to service providers for cloud security services to:

- Improve their security posture by identifying security threats and vulnerabilities and recommending responses
- Enhance reliability 24 hours a day, 365 days a year
- Focus IT resources on supporting in-house applications and networks
- Protect IT investments and systems
- Conduct business on the Internet securely
- Reduce total cost of ownership
- Deploy services faster
- Reduce the need to hire specialized IT resources

The Symantec.cloud Difference

The Symantec Email Security.cloud solution represents a significant step forward in the ongoing battle against unwanted email. Symantec.cloud continues to invest in and deploy innovative techniques that free your organization from the time-wasting, network-burdening, efficiency-eroding effects of dealing with unsolicited email, from both known and unknown sources.

In particular, as part of our industry-leading Skeptic™ Technology, Symantec.cloud has increased the identification and rejection of known unwanted email through the deployment of Traffic Management and Connection Management capabilities. Traffic Management slows down spam at the TCP/IP layer, while Connection Management uses heuristics to block unsolicited email at the connection layer and prevents attacks at the user management layer.

Skeptic™ predictive technology learns from each message it sees, evolving and updating in real time to actively protect against the latest spam techniques while providing near-perfect accuracy to virtually eliminate false positives.

Symantec.cloud clients have a range of completely customizable handling options at their disposal for messages identified as spam at the various layers of the service. Intuitive administrator and end-user spam quarantine tools provide for a flexible and productive antispam experience.

"A main advantage of a hosted solution is that the volume of mail coming to your internal network is greatly diminished—by 80 percent to 90 percent in most cases. Also, because the 'bad' e-mail is never received at your location, you need not worry about archiving it, which might be an issue if you're doing the filtering in-house."

– Logan Harbaugh, InfoWorld

Symantec.cloud scans well over 6 billion emails per day, and the intelligence gathered from this unique window on the world's email traffic provides clients with unrivalled protection from emerging threats.

To Learn More

For more information about Email Security.cloud, contact us at **+65 6333 6366** or visit us at www.symanteccloud.com.sg

More Information

AMERICAS

UNITED STATES
512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Toll-free +1 866 460 0000

CANADA
170 University Avenue
Toronto, ON M5H 3B3
Canada
Toll-free :1 866 460 0000

EUROPE

HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
Tel +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone 0800 917 7733

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Tel +44 (0) 203 009 6500
Fax +44 (0) 203 009 6552
Support +44 (0) 1452 627 766

NETHERLANDS
WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801

BELGIUM/LUXEMBOURG
Symantec Belgium
Astrid Business Center
Is. Meyskensstraat 224
1780 Wemmel,
Belgium
Tel: +32 2 531 11 40
Fax: +32 531 11 41

DACH
Humboldtstrasse 6
Gewerbegebiet Dornach
85609 Aschheim
Deutschland
Tel +49 (0) 89 94320 120
Support :+44 (0)870 850 3014

NORDICS
St. Kongensgade 128
1264 Copenhagen K
Danmark
Tel +45 33 32 37 18
Fax +45 33 32 37 06
Support +44 (0)870 850 3014

ASIA PACIFIC

HONG KONG
Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: + 852 6902 1130

AUSTRALIA
Level 13
207 Kent Street,
Sydney NSW 2000
Main: +61 2 8220 7000
Fax: +61 2 8220 7075
Support: 1 800 088 099

SINGAPORE
6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: 800 120 4415

JAPAN
Akasaka Intercity
1-11-44 Akasaka
Minato-ku, Tokyo 107-0052
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: + 852 6902 1130

Symantec.cloud

About Symantec.cloud

Symantec.cloud, a division of Symantec Corporation, offers customers the ability to work more productively in a connected world. More than 31,000 organizations ranging from small businesses to the Fortune 500 across 100 countries use Symantec.cloud to administer, monitor and protect their information resources more effectively. Organizations can choose from 14 pre-integrated applications to help secure and manage their business even as new technologies and devices are introduced and traditional boundaries of the workplace disappear. Services are delivered on a highly scalable, reliable and energy-efficient global infrastructure built on fourteen data centres around the globe.

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

Symantec.cloud Singapore
6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: 800 120 4415
www.symanteccloud.com.sg

Symantec helps organizations secure and manage their information-driven world with **managed services**, **exchange spam filter**, **managed security services**, and **email antivirus**.

7/2011 21169189

Symantec.cloud