WHITE PAPER: WEB SECURITY

Choosing a Solution for Web-Filtering:

Software, Appliance, or Cloud Service?

Symantec.cloud

White Paper: Web Security

Choosing a Solution for Web-Filtering:

Software, Appliance, or Cloud Service?

Contents

Executive Summary

There are three types of web security solutions: software-based, appliance-based and cloud-based services. Each of these categories – and each individual offering within them – needs to be evaluated against the following key buying criteria:

- Accuracy of threat protection
- Ease of installation and use
- Total cost of ownership (TCO)

Software and appliance-based solutions have significant weaknesses which undermine their suitability as a cost-effective option for business. For instance, TCO is significantly higher than initial purchase price and installation/maintenance will require substantial, ongoing commitment of in-house resources. Cloud services, on the other hand, offer valuable benefits: lower TCO, minimal commitment of in-house resources, and constant, uninterrupted protection against inappropriate web use and the increasing threat posed by web-born viruses and spyware.

Symantec.cloud is a global leader in cloud web security services. Providing a solution that is simple to install and use, Symantec.cloud offers outstanding performance in enabling businesses to set up and enforce acceptable usage policies that are flexible, fit-for-purpose and accommodate evolving needs and priorities. In parallel, its proprietary technology, Skeptic, equips Symantec.cloud to achieve unrivalled Internet-level detection and blocking of web-born malware and converged threats. Calculated on a per-user, per-month basis, these capabilities are delivered at highly competitive cost. The result is a service that doesn't just help businesses maximize productivity, profitability and protection against legal risks arising from web usage – it also means the web's many business-building benefits can be harnessed effectively and comprehensively.

The Rising Tide of Web Threats

It's indisputable. In the course of a few short years, the World Wide Web has demonstrated its ability to add real value to the operations of all kinds of organizations. It's become a key communications tool allowing commercial transactions to take place quickly and effectively, regardless of barriers imposed by time and distance. It's secured a vital niche as a medium that businesses can exploit to promote themselves, their products and their values. It's also established itself as an indispensable source of information and intelligence which can inform and improve business decision-making.

Yet like any other communication medium, the web brings risks as well as benefits. Every bit as serious as email-born threats, these risks have the potential to deliver damaging – and in some cases crippling – blows to organizations that don't have adequate protection in place.

Web threats can be divided into two broad categories: inappropriate web use and web-born malware:

Inappropriate web use:

Arguably, this is the number one web-related issue facing businesses today. Efficiency, productivity, bandwidth and corporate reputation can all take a big hit if employees squander office hours on inappropriate surfing activities.

Unfortunately, the web now offers more potential distractions than ever before. The key examples which eat up valuable in-house resources include chat rooms, iPlayer and other streaming media, online games and file downloads.

Statistically speaking, visits to adult and illegal websites are less common. Nevertheless they expose businesses to severe legal risks, e.g. from failure to protect staff from indecent images, cyber bullying and sexual harassment. As well as prosecution, fines and other penalties, the results can include loss of client trust and unwelcome media coverage.

A complicating factor, however, is the need for businesses to strike the right balance in their approach to web usage. The key is to ensure that your organization as a whole and your individual employees are properly protected, but also that motivation, creativity and wider business benefits aren't compromised by over-draconian restrictions. Social networking websites, for instance, can play a valuable role in fostering important professional relationships and the recruitment of high-caliber staff.

Web-born malware:

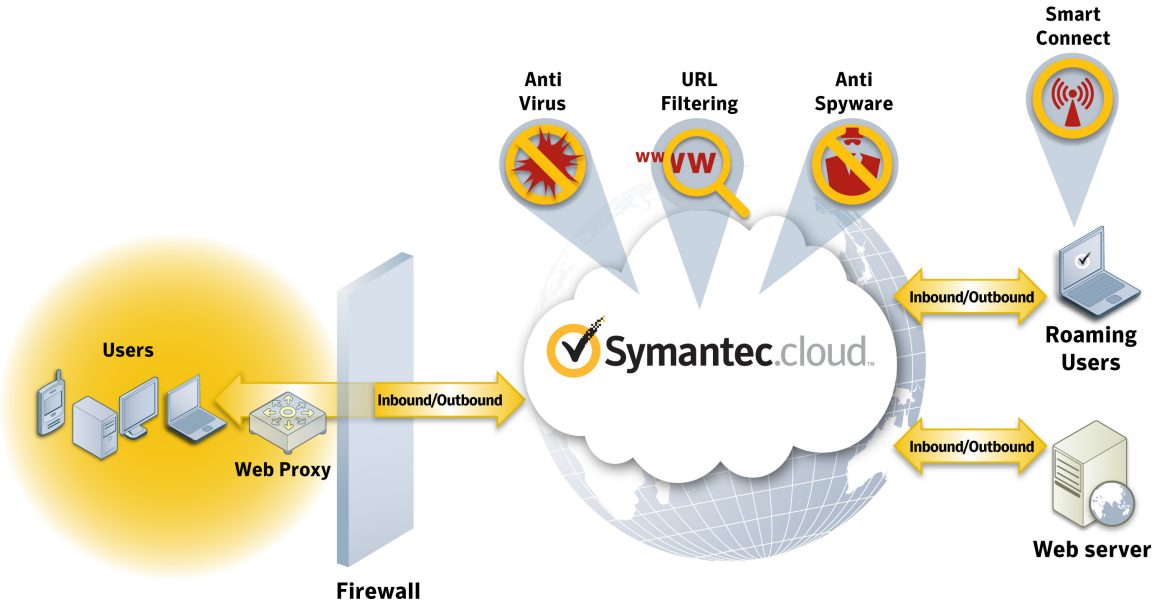
Increasingly, websites are becoming the preferred delivery mechanism for damaging malware such as viruses, as well as spyware and adware. In some cases, simply visiting an infected website will be enough to download unwanted programs onto a computer. Even if such programs are discovered before they bring your network down or surreptitiously leak sensitive financial or client data to a criminal third party, cleaning and rebuilding a polluted machine will have unwelcome resource implications. Blocking access to malicious websites and infected downloads is therefore absolutely vital to safeguarding your organization's productivity.

The need to counter web-born malware has become all the more urgent in the face of a developing and significant trend on the messaging and web security landscape. Increasingly, the "bad guys" are mixing and merging their attacks across vectors. A classic example of such "converged threats" is the use of spam emails to advertise – and carry links to – websites polluted with aggressive viruses or spyware. The uncomfortable truth is that the web is now firmly locked into the armory of tools and techniques which the increasingly professional, sophisticated criminal gangs behind most cybercrime now routinely deploy.

In the face of this alarming and continually evolving threat landscape, what should businesses do? An increasing number of vendors are responding to the rising tide of web-based threats by promoting web security solutions alongside their better established email security offerings. But how can you determine which products or services are the most efficient, easy to use and cost-effective? Outlining the key issues to consider when evaluating the options, this guide aims to help you reach the right decision for your business.

Web Security Options: In Brief

Web security solutions fall into three basic categories: software-based solutions, appliance based solutions and cloud services (sometimes also known as hosted services or SaaS – "software as a service"):



- *Software-based solutions* require on-site installation of licensed web security software between the customer's web browsers and their network boundary.
- *Appliance-based solutions* are also installed on the customer's premises. But unlike software solutions, this involves setting up hardware in the form of additional hardware between web browser and network boundary.
- *Cloud services*, by contrast, don't usually involve installing hardware or software on the customer's premises. Instead, the customer's web traffic is routed through – and processed by – the service vendor's infrastructure, consisting of data centers sited at major Internet hubs. The cloud service model normally involves the customer paying a regular subscription fee in return for a web monitoring and control service and/or protection from web-born malware.

Software-Based Solutions

Compared with email security, web security represents a relatively new market. Many businesses are not yet aware of the severity of the web threat and so are yet to make the decision to invest in a protection solution. With regard to those businesses that have already made such a decision, authoritative data is still lacking on the options they are choosing.

But it seems likely that a majority are committing themselves to software-based solutions, mirroring their email security purchasing decisions. In 2007, software-based email security solutions generated an estimated $1348 million globally, more than appliance-based solutions and cloud services combined.[1]

Symantec.cloud believes this picture will change significantly. Essentially, this is due to the drawbacks associated with software-based solutions. These relate directly to the drain on in-house resources that such solutions customarily involve and also to in-built characteristics that inhibit continuous, reliable protection:

- Although the initial price of a software-based solution may seem attractive, TCO can be substantially higher. This is because investment in additional hardware and/or software will almost certainly be essential, and it will

1-"Worldwide Messaging Security 2007-2011 Forecast and 2006 Vendor Shares", IDC 2007.

be necessary to devote sufficient in-house resources to managing and administering the solution. In addition, a software solution will typically have to be replaced within 3-5 years, generating a further commitment to hardware and software renewal.

- It is essential that a software-based solution and the system it serves have the capacity to keep pace with (i) increases in overall levels of web traffic and (ii) demand "spikes" where the number of webpage requests far exceeds the average figure. Under-capacity can lead to web access being compromised, damaging business continuity and customer relations. Eliminating worries about capacity will inevitably have financial implications.
- Setting up fit-for-purpose acceptable usage policies and enforcing them accurately using a software-based solution can be extremely resource-hungry. For instance, there can be a substantial support training requirement which, in many cases, will have to be met by in-house IT staff, deflecting them from other business critical activities. Installing software patches will also involve sidetracking IT staff from important tasks.To maintain effective protection against web-born malware, software-based solutions must continually be updated with the latest signatures. Failure to do so can open a window of vulnerability which malware may exploit mercilessly, with devastating consequences for your business.
- Even where businesses have large IT departments and extensive IT skills, ensuring that in-house web security know-how keeps fully up-to-speed with an ever-changing threat landscape is at best difficult and, at worst, impractical. This, however, is a prerequisite to ensuring that a software-based solution can provide the watertight protection businesses need.

In summary, software-based web security solutions require substantial investment and continual reinvestment, in terms of both in-house staff time and capital/maintenance costs.

Appliance-Based Solutions

Similarly, web security solutions that involve on-site installation of hardware appliances have a number of drawbacks:

- As with software-based solutions, the headline price of a web security appliance may seem tempting, but the TCO will be much less attractive. Above all, extensive input from in-house IT staff will be needed to adjust appliance settings, install patches when issued and respond to requests for technical support from end-users. It will also be vital to maintain accurate projections of changing capacity needs and ensure these are catered for in a timely and efficient way.
- Installing, deploying and testing appliances can take several days. Further, fine-tuning settings to make sure local factors and conditions are properly accommodated can also be quite time consuming. Inevitably, web availability will be restricted and perhaps even curtailed completely during the installation and set-up process.
- Relying on in-house appliances raises critical questions regarding management and capacity. Above all, as web traffic expands, more appliances will have to be installed and maintained – all of which will impact web availability, IT budgets, network storage and corporate bandwidth. Failure to cater to increased demand could result in degradation of performance and in extreme cases interruption of service and severance of web contact.

- Should an appliance go offline (e.g. due to a power or system failure), web access will be interrupted and business could be lost. As insurance against this, organizations often invest in additional "redundant" appliances. But these require further financial outlay, use valuable bandwidth, soak up storage capacity and need further administration.
- Relying on web security appliances will involve a heavy burden in terms of the time taken to frame and implement the right acceptable use policy for your organization.
- Eliminating windows of vulnerability that web born malware can exploit will be paramount.This will necessitate a high state of vigilance and a sophisticated understanding of malware threats among in-house IT staff. Supplementing internal expertise with external consultancy may prove unavoidable – a practice also characteristic of organizations that invest in software-based solutions.
- Because of the legal dimension associated with web usage, those responsible for managing and administering your appliances will need to maintain an excellent awareness of relevant legislative and regulatory frameworks. The penalties for noncompliance can be extremely severe. This applies to software-based solutions too. Overall, appliance-based web security solutions tend to be high outlay and high maintenance, and involve an open-ended commitment in terms of budgets and in-house staff resources.

Overall, appliance-based web security solutions tend to be high outlay and high maintenance, and involve an open-ended commitment in terms of budgets and in-house staff resources.

Cloud Services

In the field of email threat protection, cloud services are gaining an increasing market share. Generally speaking, vendors of such services have earned a reputation for upstream innovation which translates directly into rapid deployment of leading edge protection capabilities on their clients' behalf. The functionality, flexibility and ease of customization they offer are also playing a key role in their rising popularity.

This growing preference for cloud services is now becoming evident in web security too. The main benefits that cloud services generally aim to provide include:

- Predictable TCO, delivering significant savings compared to software and appliance-based solutions. This is because (i) cloud service providers can achieve substantial economies of scale and (ii) there should be no "hidden extras". Because a cloud service uses the vendor's infrastructure, away from subscribers' networks, the need to install, maintain and keep reinvesting in on-site software and hardware is basically eliminated. Valuable corporate bandwidth is also preserved.
- Ease and speed of set-up, with minimal disruption to web access, maximizing business continuity and employee productivity.

- Complete scalability and failover protection. Temporary and long-term increases in demand for web access can be seamlessly accommodated. Subscribers should also be immune from the effects of server crashes and planned or unplanned power outages.
- Incorporation of policy engines for development and automatic, accurate enforcement of acceptable use policies. An important spin-off from this benefit is the minimal amount of training required, removing a major burden on in-house IT staff.
- Non-stop, constantly updated protection from web-born malware. Cloud service providers employ technicians and engineers who work day-in, day-out to understand and neutralize web security threats. To replicate this level of specialist expertise within an average IT department is simply not feasible.
- Releasing in-house IT resources from the relentless, and often impossible, task of monitoring/controlling web usage and providing effective protection against increasingly virulent web-born malware and converged threats.

The following table summarizes the principal performance factors of software-based solutions, appliance-based solutions and cloud services:

The Symantec.cloud Approach

Cloud web security services offer businesses important advantages. But how are prospective subscribers to differentiate between the increasing number of vendors coming to market with such services?

Symantec MessageLabs Web Security.cloud solution provides capabilities in:

- Monitoring employees' web browsing behavior, which includes highlighting bandwidth used and the potential need to put web usage controls in place.
- Control of websites that can be visited and files that can be downloaded from them.
- Interception of viruses, spyware and adware.

Other vendors offer services which ostensibly perform the same tasks. However, Symantec.cloud outperforms its competitors in three critical areas:

1. Accurate protection:

Harnessing the world's most advanced and stable network, consisting of 15 data centers spanning five continents, Symantec.cloud delivers industry-leading zero hour Internet-level protection against web-born threats. Underpinning this capability is the use of multiple signature-based anti-malware scanners and Symantec.cloud's unique, proprietary threat detection technology, Skeptic.

For almost a decade now, Skeptic has led the way in predictive threat detection. As it relentlessly scans for malware, it constantly adds to its enormous reservoir of knowledge, updating itself to deal with every new threat that appears on the landscape – however novel or sophisticated that threat may be. The other scanners used by Symantec.cloud are all best-of-breed commercial offerings that stop known malware threats and so act as a perfect complement to Skeptic.

Delivering such comprehensive threat protection has become all the more essential with the increasing trend towards threat convergence (see page 5). Moreover, Symantec.cloud is the only vendor to retain its email, web and Instant Messaging (IM) security services in-house. This means that when a threat is detected in one vector, the solution can be applied across other vectors with the greatest possible speed and efficiency. Because Symantec.cloud's email, web and IM services form part of a single system and are not devolved to partner organizations, they can be managed as an integrated whole.

2. Ease of installation and use:

Simplicity of set-up, configuration, use and administration are all hallmarks of MessageLabs Web Security service, which function with equal effectiveness regardless of a customer's web browser configuration. 24/7/365 client support is included in the subscription fee.

The services also offer unrivalled flexibility. Thanks to the policy engine incorporated, they can be customized to meet the precise and changing priorities of any business, wherever in the world they are located. This is absolutely essential in today's business environment where every organization needs to devise an acceptable web usage policy that matches their exact requirements and circumstances as closely as possible.

As well as allowing you to govern web access at group or even individual user level, MessageLabs Web Security service enables you to set time based rules, e.g. to permit web surfing during lunch hours – an approach that can benefit staff motivation. Similarly, the service is designed to accommodate the increasingly blurred lines between employees' home and work lives and private and professional identities. In many ways, the web has played a key role in blurring these lines

and creating challenges and opportunities as a result. The industry-leading flexibility inherent in Symantec.cloud's intuitive policy-building engine therefore delivers vital benefits.

Administration of the service is undertaken from a user-friendly, web-based portal. This generates a whole range of management information, configuration tools, service statistics and reports in real-time. So you remain fully informed about the service's performance and about patterns of web usage for individual employees, groups of employees and the organization as a whole. Furthermore, the client doesn't need to be involved in service updates and upgrades, which are undertaken automatically by Symantec.cloud.

Added to this, close study of customer feedback and exactly what this feedback signifies helps Symantec.cloud continually refine and improve its services. Vendors with smaller client rosters inevitably receive less feedback on which to base service improvements – yet another competitive edge for Symantec.cloud.

3. Total cost of ownership:

As noted earlier, cloud services can offer businesses a lower TCO than software and appliance-based solutions. The "hidden extras" associated with the latter two options can be substantial and may include: investment in additional hardware or software, installation of increased storage capacity, bringing more bandwidth online to cope with demand, and making considerable in-house IT support available to provide a training and troubleshooting resource. But the TCO of a cloud service should stay stable and predictable – a massive benefit when it comes to budgeting and ensuring expenditure forecasts are as accurate as possible.

So how does the cost of MessageLabs Web Security service compare with other cloud web security services? Calculating on a per-user, per-month basis – the most accurate framework for estimating actual costs – Symantec.cloud is extremely competitive with the less effective, less comprehensive, less user friendly, less flexible solutions provided by other vendors.

The Best Option for Business

As this guide explains, MessageLabs Web Security service are specifically designed to help businesses take control of the many potential threats that can arise from web usage on a daily basis. This, in turn, equips businesses to protect their productivity and valuable in-house resources.

Crucially, Symantec.cloud offers benchmark protection not just compared with software and appliance based solutions but also with the growing number of rival cloud web security services now available. Quite simply, Symantec.cloud helps ensure that, for your business, the web remains a business-boosting asset – and doesn't become a destructive, risk-laden liability.

For more information or for a free trial of MessageLabs Web Security service please visit www.MessageLabs.com or call **(866) 460-0000**

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

About Symantec.cloud

Symantec.cloud uses the power of cloud computing to secure and manage information stored on endpoints and delivered via email, Web, and instant messaging. Building on the foundation of MessageLabs market leading software-as-a-service (SaaS) offerings and proven Symantec technologies, Symantec.cloud provides essential protection while virtually eliminating the need to manage hardware and software on site.

More than ten million end users at more than 31,000 organizations ranging from small businesses to the Fortune 500 use Symantec.cloud to secure and manage information stored on endpoints and delivered via email, Web, and instant messaging.

Symantec.cloud helps IT executives to protect information more completely, manage technology more effectively, and rapidly respond to the needs of their business.

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

Symantec.cloud North America
512 7th Ave.
6th Floor
New York, NY 10018 USA
1 (646) 519 8100
1 (866) 460 0000
www.MessageLabs.com

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

1/2011 21169190