

Software-as-a-Service Web Security – Why Switch?

A ScanSafe White Paper May 2008

TABLE OF CONTENTS

	PAGE
TABLE OF CONTENTS	2
1.0 INTRODUCTION	3
2.0 THE DEFINITION & DELIVERY OF SAAS WEB SECURITY	3
3.0 WEB THREATS – THE NEXT GENERATION	3
4.0 THE PROFILARATION OF SECURITY PRODUCTS	4
5.0 THE ESCALATING COST OF THE WEB SECURITY INFRASTRUCTURE	5
6.0 MANAGED SERVICE PROVIDERS	6
7.0 SAAS WEB SECURITY	6
8.0 EXTERNAL DRIVERS OF SAAS WEB SECURITY	7
9.0 BARRIERS TO THE ADOPTION OF SAAS WEB SECURITY	7
10.0 THE EVOLUTION OF SAAS WEB SECURITY	8
11.0 SUMMARY AND CONCLUSION	9
12.0 ABOUT SCANSAFE	10

1.0 INTRODUCTION

This is one of a series of white papers setting out considerations for organizations in relation to corporate use of the Internet, and concerns itself with answering the following question:

“What advantages does Software-as-a-Service (SaaS) Web Security have over traditional methods of Web Security delivery?”

This paper will define SaaS Web Security and the way that these services are delivered and also assess the current Internet threat landscape. It is necessary to cover these areas in order to understand why the typical Web security infrastructure has grown so much in recent years and why the case for a switch to SaaS Web Security has therefore become increasingly compelling.

In addition to exploring the internal reasons that organizations are turning to SaaS Web Security, this paper will also discuss how factors external to individual organizations are driving the take-up. The common barriers to the adoption of SaaS will be covered along with a discussion on how these barriers are becoming less and less significant.

The paper concludes that the SaaS Web Security model has unique features which make it the most cost-effective way of delivering secure and productive access to the Internet.

“What advantages does Software-as-a-Service (SaaS) Web Security have over traditional methods of Web Security delivery?”

2.0 THE DEFINITION & DELIVERY OF SaaS WEB SECURITY

SaaS Web Security is the provision of multi-tenant, purpose-built Web security over the Internet. The SaaS Web Security vendor provides a redundant, scaled, distributed architecture and customers do not pay for the software itself but rather for using it, with access to the application being via a Web browser. Typically, no hardware is required and SaaS Web Security can be run over the existing Internet access infrastructure.

SaaS applications are based on a recurring subscription fee and the cost is directly aligned to the number of users. All of the usual costs associated with maintaining Web security software such as content filters, along with the infrastructure on which it resides, training, security updates etc. are assumed by the SaaS Web Security vendor in exchange for the recurring service fee.

“No hardware is required and SaaS Web Security can be run over the existing Internet access infrastructure.”

3.0 WEB THREATS – THE NEXT GENERATION

In order to understand how the traditional means of delivering Web security have become difficult to manage, it is necessary to discuss the dynamic nature of the target. The Web has gradually become the primary attack vector used by malware authors to distribute malicious code. More worryingly, this code now frequently appears on perfectly legitimate sites. Browser vulnerabilities continue to be exploited in ever-decreasing time windows and Trojans, keystroke loggers, root kits and other Web malware have become major security issues.

In addition to these threats, a new challenge has emerged. The Internet is no longer a static one-way delivery device, but rather a fully collaborative environment that allows Website owners and visitors to interact in real time. The contributions of website visitors can now define and manipulate the website experience, both for themselves and other users. Third party content providers can also influence this experience through targeted advertising, newsfeeds, and other dynamic contributions. This multi-way flow of information is accomplished through Web 2.0

“It is now easier than it has ever been for cyber criminals to inject malware into unsuspecting sites.”

technologies, a collection of scripting languages and applications that have fundamentally changed the nature of the Internet from a one-to-many delivery device to a many-to-many global communication experience. Web 2.0 has generally been viewed as a positive development by CIOs with organizations harnessing wiki, blogs, Rich Site Summary (‘RSS’) feeds, podcasts, content tagging and social networking tools.

However, the symbiotic ideal of Web 2.0 has been tarnished by the harnessing of these applications for less wholesome purposes. It is now easier than it has ever been for cyber criminals to inject malware into unsuspecting sites. Malware is being inserted onto Web pages via insecure advertising servers, compromised hosting networks, straightforward user-contributed content, and even through third party widgets, commonly found on many trusted and popular sites.

4.0 THE PROFILARATION OF SECURITY PRODUCTS

The magnitude of threats arising from the Web has ensured that simply relying on the good character and common sense of employees ceased to be an option some time ago. As the Internet has grown and evolved, so has the market for protection from its less savoury aspects. The majority of organizations have had a gateway-based product in the form of URL filtering software in place for some time.

URL filtering software is sometimes deployed on a standard specification Microsoft Windows server situated within the corporate network perimeter. This means that organizations face the challenge of keeping Windows licensed, patched and up-to-date as well as the filters themselves. Issues are often also caused by an exponentially growing rule base as different rules are enforced for different groups of users. Also, in order to realise the full reporting functionality of traditional Web filtering software, separate databases often have to be installed. This inevitably means the purchase of more hardware, another Windows licence and database licences such as Microsoft SQL Server. These databases are not easy to administer and maintain, and along with the maintenance of the URL filters and platform servers themselves, consume a significant proportion of IT budget and manpower.

“One of the shortcomings of gateway Web security appliances concern their malware blocking capability.”

Consequently, many organizations have moved to specific gateway appliances rather than Windows servers. These appliances have pre-hardened Linux based operating systems, and because they are designed to do nothing but act as a gateway to the Internet they are fast and relatively effective. Deploying URL filtering software on a gateway appliance is often considered the “best-of-breed” way of responding to the Web security challenge because management capability is improved and performance enhanced. However, the approach is not a panacea for all Web security ills.

It should be borne in mind that the vendors of URL filtering solutions initially positioned themselves as Web productivity solutions. This partly explains why one of the shortcomings of gateway Web security appliances concern their malware blocking capability. A straightforward gateway appliance being used as a platform for URL filtering software cannot protect an organization from malware when deployed on its own, no matter how extensive the URL database it references. This is because malware is almost as likely to reside on a perfectly legitimate site as a more obviously unseemly one. Please see the paper “The Failure of Web

Filtering” for a more thorough analysis of why URL filtering alone cannot provide an adequate degree of protection in the current Web threat environment.

A separate appliance to block malware usually has to be deployed if an organization is to be protected from these threats at the gateway level, increasing capital expenditure and ongoing support costs.

Because of the incomplete level of protection that can be implemented at the Internet gateway, increasing reliance has been placed on client based tools to block malware as second layer of defense. These tools provide useful capabilities and can be effective at preventing many Web threats. These tools can be acquired relatively inexpensively and are often provided as part of desktop protection suites that include anti-virus, anti-spam and a personal firewall.

However, client-based tools are most often signature based and therefore leave organizations vulnerable in the “zero hour”. Desktop agents add to the support burden, particularly when it comes to pushing out updates and dealing with any implications that update may have on other applications that the user needs to access. Often, the responsibility rests with the end users in terms of accepting malware updates which is a far from ideal situation. Client-based tools should therefore be considered a “last line of defence” only and certainly not a stand-alone solution.

“Client-based tools are most often signature based and therefore leave organizations vulnerable in the “zero hour”.”

5.0 THE ESCALATING COST OF THE WEB SECURITY INFRASTRUCTURE

As the number of products required to keep up with the evolving threat landscape has grown, so has the difficulty in managing and maintaining this infrastructure. Many organizations significantly underestimate the management overhead of Web security solutions. According to Gartner, the annual costs of owning and managing software applications can be up to four times the cost of the initial purchase.

The cost to an organization of owning and managing the disparate components of a Web security solution are, at best, unpredictable. Unplanned downtime can blow a considerable hole in a fixed IT budget. Appliances can fail for a number any number of reasons, as can the software deployed upon them. If an organization wishes to avoid downtime then it needs to avoid turning the Web gateway into a single point of failure and thus consider a High Availability (‘HA’) infrastructure. This would mean the deployment of at least two appliances. This seriously escalates the initial capital expenditure required and also the manpower required for the initial deployment and ongoing maintenance.

Organizations also need to consider whether the skill sets required for deployment, documentation and maintenance of this solution already reside within the organization. If they do not, then multiple days of expensive consultancy both initially and in the future will be necessary to make the deployment a success.

Further consideration is required if an organization is geographically diverse and has more than one Internet gateway. If appliances are required at multiple Internet gateways the initial expenditure and ongoing management overhead increases still further

On-premise Web security solutions also possess finite scalability. As organizations grow, the Web gateway can start to become a bottleneck. Appliances have very limited upgrade potential in the event of a significant number of new employees being added to an organization. They have zero downgrade potential in the event of the opposite scenario. This lack of agility can lead to

“The cost to an organization of owning and managing the disparate components of a Web security solution are, at best, unpredictable.”

SOFTWARE-AS-A-SERVICE WEB SECURITY – WHY SWITCH?

“forklift” upgrades being required well ahead of the intended lifespan of the solution being realised.

Furthermore, given the pace of change in Internet use and threats in the last eighteen months, the longevity of premise-based solutions should be carefully considered. Web content has become considerably richer in a very short time frame, and concurrency levels within organizations have increased significantly. An industry-leading Web security gateway product might speed up Web access and be efficient at blocking threats at the time of its deployment but could easily be outmoded within a relatively short time frame – certainly well in advance of the intended depreciation schedule.

6.0 MANAGED SERVICE PROVIDERS

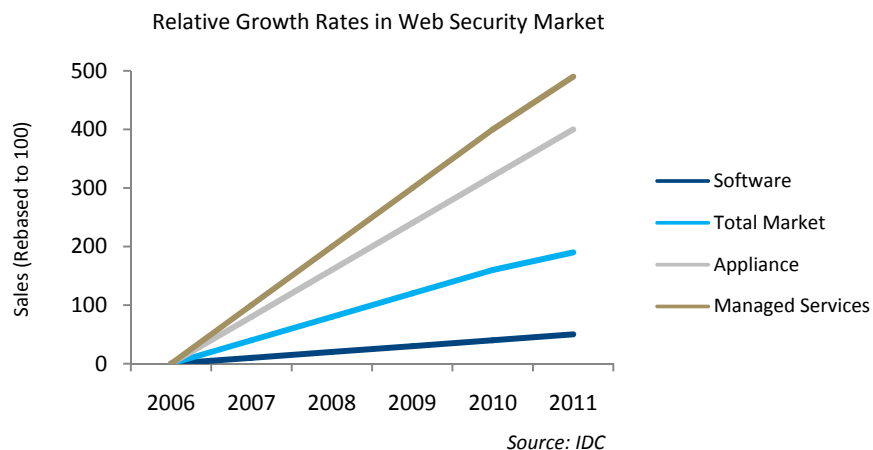
The use of a Managed Service Provider (‘MSP’) is sometimes considered the middle ground between in-house ownership and management of Web security and complete SaaS adoption. The definition between a Managed Service and SaaS can become blurred. However, the distinction is clear.

MSP’s are traditional single-tenant applications hosted by a third party. The servers and/or appliances simply reside in a secure datacenter and an HTML front end allows access to the application. The third parties hosting these applications most often possess no specific expertise in hosted Web security which can have severe implications for the customers. Performance can be poor and the management overhead is reduced only marginally if at all.

7.0 SaaS WEB SECURITY

“The adoption of SaaS Web Security allows IT resource to *innovate* rather than *maintain*.”

Given the serious shortcomings of premise-based Web security solutions it is easy to understand why organizations of all sizes are turning to SaaS Web Security to secure their Internet access, without incurring disproportionate capital expenditure or management overhead. IDC predict that the Web security hosted services market will grow in excess of 36% year on year until 2011. This compares with just 9.1% growth for Web security software. Gartner have predicted that the SaaS market will account for 25% of new business software revenues by 2011.



The SaaS model of Web security delivery brings many benefits. Web requests are filtered in the Internet ‘cloud’ and malware is removed before serving clean traffic back to the user. Corporate Acceptable Use Policy (‘AUP’) can be applied to all users regardless of location and management is simplified because no end-point updating is required. These benefits allow the enterprise to “work smart” by focusing their energies on activities core to their business. Precious IT resource is freed from spending large amounts of their time solving problems generated by the integration and management of several products. Service Level Agreements concerning uptime, latency, false positives and negatives are standard and SaaS Web Security is fully scalable. The enterprise can plan capacity and budget with confidence. In summary, the adoption of SaaS Web Security allows IT resource to *innovate* rather than *maintain*.

8.0 EXTERNAL DRIVERS OF SaaS WEB SECURITY

There are a number of external factors that are driving the adoption of SaaS Web Security. It is arguable that SaaS has come of age. Nick Carr is the former executive editor of the *Harvard Business Review* and continues to write and speak on technology, business and culture. Carr argues in his most recent publication, “*The Big Switch: Rewiring the World, from Edison to Google*” that most IT is a needless hassle and should be as easy to obtain as electricity and as reliable as a utility such as water. This message seems to be resonating with decision-makers as never before.

At the time of writing, escalating energy costs, faltering financial institutions and the subsequent receding of consumer and executive confidence have led the majority of organizations to expect a tough couple of years ahead. Consequently, capital investment may be scaled back to mitigate exposure to an uncertain market place. The ability to utilize applications such as Web security on a pay-as-you-go basis will be a perfect strategy for businesses seeking greater flexibility and control over costs.

There has also been a fundamental shift in the way that people work, with the current generation of workers being granted more flexibility than ever before in their working arrangements. The proliferation of public Wi-Fi hotspots and high speed Internet access in the home allows employees to work almost anywhere. Traditional, on-premise Web security solutions sitting behind a corporate firewall can’t effectively apply AUP and block malware without seriously impacting the Internet experience of remote workers. SaaS Web Security is perfectly suited to securing this highly elastic network perimeter.

“The ability to utilize applications such as Web security on a pay-as-you-go basis will be a perfect strategy for businesses seeking greater flexibility and control over costs.”

9.0 BARRIERS TO THE ADOPTION OF SaaS WEB SECURITY

Given the long list of benefits associated with SaaS Web Security as a way of securing the virtual network boundary, one might be forgiven for wondering why many organizations have not, as yet, climbed aboard the bandwagon. Some of these objections are rooted in distrust of SaaS as a concept, and some relate specifically to SaaS Web Security.

“In the vast majority of cases the adoption of SaaS Web Security typically leads to a 30-40% reduction in costs.”

IT departments have traditionally been somewhat hostile to the concept of SaaS as a whole due to the perception that jobs within IT and SaaS were mutually exclusive. However, a growing proportion of IT professionals have come to view SaaS as a way to overcome cumbersome application and technology deployments such as those for Web security, and the responsibility for maintaining that infrastructure. Their time has been freed up to undertake the strategic tasks that bring them greater fulfillment and their employer more profit.

Another considerable barrier to the wider adoption of SaaS has been the role of the traditional Value Added Reseller (‘VAR’). VARs have been concerned that the rise of SaaS will eliminate the need for their consultancy services and eat into their product revenue. However, more forward thinking VARs are listening to their customers and discovering that there are still consulting and customization opportunities in the SaaS market. Consequently, VARs are now providing SaaS vendors with access to their sales and marketing functions on an unprecedented scale.

Perhaps the largest barrier to wider SaaS adoption has been its perceived greater cost in comparison to the traditional software pricing model. The issue of cost can be complicated. Software and hardware costs are easy to quantify but the manpower resource associated with them is often underestimated or omitted altogether when undertaking a Total Cost of Ownership (‘TCO’) analysis. However, when this manpower resource is correctly quantified the SaaS Web Security route usually becomes the most cost-effective option – particularly if an organization has multiple Internet gateways. In the vast majority of cases the adoption of SaaS Web Security typically leads to a 30-40% reduction in costs over the first year when compared to the equivalent product-based solution.

“Real-time scanning should be considered a “must have” component of any Web security solution.”

10.0 THE EVOLUTION OF SaaS WEB SECURITY

SaaS Web Security has evolved dramatically over the last two years. It was occasionally perceived as being less feature rich than premise-based solutions. This is, and always was, a myth. By their very definition SaaS Web Security vendors have greater visibility of Web traffic than premise-based solutions and can aggregate this real-time data across their customer base. They update their services in real-time and, crucially, with no intervention from the customer. The zero hour threat is not an empty concept. Data aggregated across 2007 shows that in excess of 20% of malware blocks were not signature detected, defining them as zero hour threats.¹ This means that a signature-based anti-virus engine would not have blocked them.

“This means that even with a best-of-breed Web filter in place the information being used to determine whether a site represents a risk is likely to be at least a number of hours old.”

Real-time scanning should be considered a “must have” component of any Web security solution. Many URL filtering vendors claim that the size of their databases and frequency of updates amount to real-time scanning. These claims do not withstand scrutiny. In a recent advertisement, a leading URL filtering vendor claimed it crawled 40 million websites an hour. This sounds like an impressive number until you consider that the April 2008 Netcraft Survey put the total number of URL’s in existence at approximately 165 million. This means that even with a best-of-breed Web filter in place the information being used to determine whether a site represents a risk is likely to be at least a number of hours old. Using URL filtering to defend yourself against malware is like

¹ ScanSafe Global Threat Report 2008

reading yesterday's newspaper to find the current price of your favorite stock. Organizations should consider whether this constitutes an acceptable level of security in such a dynamic threat landscape.

Reporting is another area where SaaS Web Security has overtaken the more traditional methods of delivery. Reporting data for SaaS Web Security is automatically and continuously aggregated across internal corporate users and roaming users, so summary and detailed information on specific user Web activity is easy to generate and schedule for future reference. When it comes to policy setting and reporting, SaaS Web Security is managed via Web-based portals, allowing application of corporate AUPs to any user anywhere in the world, from anywhere in the world. It is, arguably, a good deal more flexible and granular than conventional models of Web security delivery.

Despite the evolution of SaaS Web Security, IT departments can still show resistance to what they perceive as the "outsourcing of security". There are understandable concerns around the storage of sensitive and business critical data and the resiliency of such services. It is worth stating that the vendors of SaaS Web Security are scrutinized far more deeply than the vendors of traditional Web security solutions because of the nature of the service they provide. The infrastructure of a Web SaaS security provider has to be regularly and thoroughly audited, and these vendors must demonstrate how they adhere to laws and regulations concerning the protection and management of customer data. Provided you choose the right SaaS Web Security provider, confidential data is at least as safe as it would be in the hands of the owners – if not considerably safer. Comprehensive Service Level Agreements on availability and quality of service should be standard. No such agreements exist for Web security solutions owned and managed by the customer.

"Confidential data is at least as safe as it would be in the hands of the owners – if not considerably safer."

11.0 SUMMARY AND CONCLUSION

The conclusions reached by this paper are as follows:

- SaaS Web Security is the provision of multi-tenant, purpose-built Web security over the Internet
- Organizations have typically implemented multiple layers of Web security encompassing the Internet gateway and end-point machines but this has become less effective, increasingly expensive and difficult to manage
- Factors such as the desire to exercise greater flexibility and control over costs plus the increasing elasticity of the network perimeter have led more organizations to consider SaaS Web Security
- SaaS Web Security is the most cost-effective way of delivering real-time scanning of all customer Web traffic
- SaaS Web Security can deliver a level of policy granularity and reporting functionality that is equal to or greater than that made available by premise-based solutions
- SaaS Web Security is audited regularly and SLAs on availability and quality of service are standard, in contrast to premise-based solutions
- Barriers to the adoption of SaaS Web Security such as perceived higher cost are breaking down

"SaaS is becoming the norm."

SOFTWARE-AS-A-SERVICE WEB SECURITY – WHY SWITCH?

- The SaaS Web Security model has unique features which make it the most cost effective way of delivering secure and productive access to the Internet

It has become evident that SaaS has moved from a way of delivering selected, vertical applications to becoming the “best practice” method of delivery. In summary, SaaS is becoming the norm.

“A hundred years ago, companies stopped generating their own power with steam engines and dynamos and plugged into the newly built electric grid. The cheap power pumped out by electric utilities didn’t just change how businesses operate. It set off a chain reaction of economic and social transformations that brought the modern world into existence. Today, a similar revolution is under way. Hooked up to the Internet’s global computing grid, massive information-processing plants have begun pumping data and software code into our homes and businesses. This time, it’s computing that’s turning into a utility.”²

12.0 ABOUT SCANSAFE

ScanSafe is the largest global provider of Web Security-as-a-Service, ensuring a safe and productive Internet environment for businesses. ScanSafe solutions keep viruses and spyware off corporate networks and allow businesses to control and secure the use of the Web and instant messaging. As a SaaS solution, ScanSafe’s services require no hardware, upfront capital costs or maintenance and provide unparalleled real-time threat protection. Powered by its proactive, multilayered Outbreak Intelligence™ threat detection technology, ScanSafe scans more than 20 billion Web requests and blocks 200 million threats each month for customers in over 80 countries.

With offices in London and San Francisco, California, ScanSafe is privately owned and financed by Benchmark Capital and Scale Venture Partners. The company received the CNET UK Business and Technology award for Security Product of the Year 2008, a 2007 CODiE award for Best Software as a Service Solution, the 2008 and 2007 SC Magazine Europe Award for Best Content Security Solution and was named one of Red Herring’s Top 100 Technology companies. For more information, visit www.scansafe.com.

² The Big Switch: Rewiring the World, from Edison to Google – Nick Carr

[Contact ScanSafe](#) [About ScanSafe](#)

ScanSafe US
185 Berry Street
San Francisco, CA 94107

T: 415 692 2000
F: 415 536 5949
E: info@scansafe.com

ScanSafe EMEA

The Connection, 198 High Holborn
London WC1V 7BD

T: 020 7959 0630
F: 020 7959 0631
E: info@scansafe.com

Founded in 1999, ScanSafe is the leading global provider of Web Security-as-a-Service, ensuring a safe and productive Internet environment for businesses. As a SaaS solution, ScanSafe's services require no hardware, upfront capital costs or maintenance and provide unparalleled real-time threat protection. Powered by its proactive, multilayered Outbreak Intelligence™ threat detection technology, ScanSafe scans more than 20 billion Web requests and blocks 200 million threats each month for customers in over 80 countries.

For more information visit www.scansafe.com