White Paper

Bloor

Why web security is best served in the cloud

Move protection to where the threats are

A White Paper by Bloor Research
Author : Fran Howarth
Publish date : February 2010

... managing web-borne threats is becoming a major headache for today's resource-strapped organisations

Fran Howarth

This document is sponsored by

Executive summary

No business is an island. For every organisation, the ability to communicate effectively with employees, customers and business partners, and to provide its employees with access to information as and when they need it requires that it maintain an online presence and enable its employees to access information on the internet. However, the reality today is that the internet and the web-based applications that run over it are the preferred method of attack for financially motivated hackers. In order to protect themselves from threats emanating online and to aid in ensuring that data security objectives are met, web security technologies are key defences in any organisation's security arsenal.

However, in deploying such technologies, there are choices to be made: should an organisation purchase software licences and hardware to run the system in-house, or should it use the services of a third party provider? Purchasing software licences is the traditional method of accessing software applications, but each extra application that is licensed requires IT resources to set up the system on each device to be protected, and it must manage the processes of keeping the software up to date and properly configured. For many technology implementations, that may be the best choice, but with email, and in particular, the internet, being prime vectors of attack using increasingly complex and sophisticated exploits designed to bypass traditional defences, managing web-borne threats is becoming a major headache for today's resource-strapped organisations.

This paper discusses the new generation of web security offerings provided by service providers in the cloud, where protection is applied at the point where the threats are being seen—that is, directed at web-based applications. In taking the protection nearer to the threats, organisations can benefit from vastly improved internet security as the threats are stopped before they ever reach the network. This paper discusses the reality of web-based threats today, and discusses the drivers for cloud-based computing and the benefits that organisations will see from use of a dedicated service provider for handling functions that are necessary, but that are not a core competence of the organisation. It is intended to be read by executives at companies of all sizes, and especially those at small and medium organisations that have little to gain from running such services themselves.

Fast facts

- Hackers are increasingly financially motivated and the internet is becoming the prime vector of attack, using increasingly sophisticated and complex exploits.
- The need for cost-effective solutions to protect an organisation from harm and to boost its data security efforts is driving take up of web security technologies.
- Owing to the dynamic nature of web-based threats seen today, protection based in the cloud that can stop threats from ever reaching networks providse many advantages over in-house deployments.
- The benefits of using a cloud-based solution include reduced risk of exposure to security exploits, added value through improved data security and regulatory compliance capabilities, and the ability to cut the costs of procuring and managing the technology, which also translates to higher productivity and greater operational efficiencies.

The bottom line

Today we live in an information age, with always-on, instant communications seen as a necessity for doing business. New technologies that have been developed to enable this include the internet and mobile technologies, allowing greater flexibility for workforces in terms of when, how and where they work. These new technologies not only allow easier access to information resources for employees, customers and business partners, but also for hackers as well. Because the threats that hackers pose are growing so rapidly, with malware, in particular, showing growth after years of decline, and with exploits becoming increasingly complex and sophisticated, it is time for organisations to consider their options. Among the most promising developments that they should consider is the option of accessing web security protection from a service provider based in the cloud, where protection can be applied directly at the point where the threats are being targeted—at internet applications. In so doing, organisations can benefit not only from higher levels of protection, but will also see the benefits to the bottom line owing to the lower levels of investment that are required for such services when compared to applications implemented and managed in-house.

The realities of web security today

Moving online is a crucial business initiative for organisations in order to reach more customers in a more profitable manner. However, moving online not only provides greater exposure to customers, but to hackers as well. As a result, security is an increasing concern as criminals know that a successful attack can be profitable for them. In our private and business lives, we need to be constantly on our guard to ensure that we are one step ahead. To carry out their attacks, criminals will often try to infiltrate computer systems using malware, which can be a variety of malicious software programs such as viruses, worms, Trojans or spyware.

In the past, most malware was designed to cause damage such as defacing a website and was aimed at hackers gaining kudos among their peers. As the use of computers and other devices for communicating over public networks such as the internet and via email continues to grow, so too does the amount of valuable information contained in those communications. Personal information is highly prized by criminals as it can be used to steal identities for fraudulent purposes, as is the intellectual property and commercial databases maintained by organisations.

According to an InformationWeek 2009 survey[1] of almost 600 businesses in the US, when respondents were asked what types of security breaches or espionage they were most likely to encounter in 2010, 62% cited worms, 51% viruses and 43% phishing attacks, which are aimed at luring users into giving away information or clicking on webpage links that take them to malicious websites where malware can be automatically downloaded onto their devices. Having been steadily on the decline since 2005, the CSI computer crime and security survey 2009[2] found that malware attacks are on the rise again and were the most prevalent type of attack seen by organisations, cited by 64.3% of respondents, up from 50% in 2008.

Not only are malware attacks increasing, but they are becoming increasingly sophisticated in order to challenge the defences that computer users are putting in place. Of respondents to the InformationWeek survey referenced above, the top reason for increased vulnerability to security threats, cited by 73% of respondents, is the increasing sophistication of threats against their networks. In particular, attackers are looking to use blended or hybrid threats that combine threat vectors such as use of the internet and email to carry out more complex attacks that have more chance of succeeding. It used to be common for attacks to be sent out for propagation to as many machines as possible, often through mass email communication. Today, attacks are more frequently targeted at specific organisations and the number of variants of specific pieces of malware has increased exponentially to try to evade tools used to filter such emails and web pages for malware.

To defend themselves, organisations and consumers alike have looked to deploy anti-malware tools to prevent infections from exploits such as viruses and spyware, and firewalls to cordon off their networks. Organisations are also stepping up their attempts to educate their employees in security awareness and public sector organisations provide information to the general public regarding how to protect themselves with initiatives such as www.getsafeonline.org in the UK. In England, lessons in safe use of the internet will become a compulsory part of the primary school curriculum from 2011 onwards to inculcate awareness of security issues among schoolchildren from a young age.

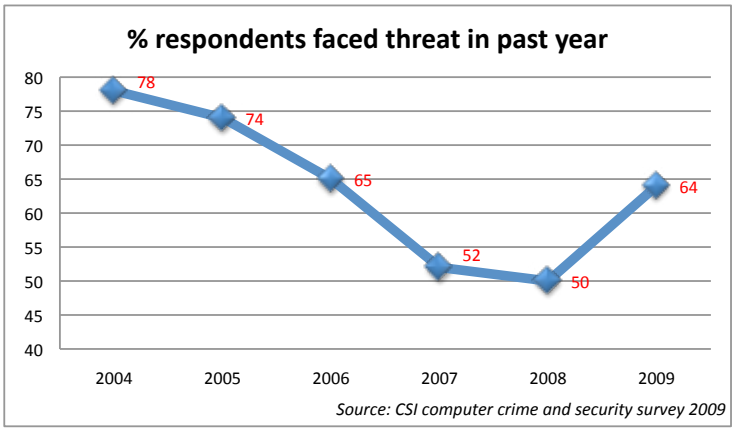

Figure 1: Organisations facing malware attacks by year

The realities of web security today

The web as the preferred vector of attack

As a result of initiatives such as these, users are becoming savvier, having learnt not to click on links in emails or open attachments from unknown senders. This means that hackers must become more inventive. They are increasingly turning their attention to web-based applications, looking to exploit the vulnerabilities that they contain to hack networks or to carry out social engineering attacks against unsuspecting users. According to figures from Webroot, 85% of new malware infections seen today are the result of web-based exploits. International standards group, the Web Application Security Forum, concurs, stating that it has seen a steady growth in web application security problems and that most web applications are vulnerable to attack.

As well as moving online to reach more customers, organisations are increasingly allowing more flexible working practices enabled by mobile technologies connected to the internet. According to iSuppli Corporation[3], which provides research in the electronic value chain, sales of laptop computers exceeded those of desktops for the first time in the third quarter of 2008 and will continue to grow in relative importance. Laptops allow employees to work from wherever they like, whenever they want, by connecting the laptop to the corporate network via the internet. Internet connectivity also means that geographically remote branch offices can take advantage of resources contained on the core corporate network.

Moving protection to the cloud

For some years, tools for defending against hackers have been in the form of software to be installed on each device being protected or appliances deployed on-premise. However, to be effective, such protection needs to be constantly updated. Traditionally, anti-virus tools used signatures that identify known malicious patterns in executable code. When installed as software on each device or provisioned centrally from an appliance, the time taken to discover vulnerabilities, create a signature, and test and deploy patches means that there will always be a gap in security.

Today, such an approach is not considered to be sufficient owing to the wide variety of new malware or versions of existing viruses for which no signatures have yet been written, also known as zero day threats. To get around these problems, vendors have started to offer solutions based on heuristics that look for certain types of behaviour to see if it performs malicious actions. Others are starting to offer whitelisting services, in which software that is known to be benign are routinely allowed to run.

Managing licences for each user that requires the tools and ensuring that all machines have up-to-date protection is an expensive and time-consuming task. Today, threats are moving to the web so it makes sense that the protection is there also. An important new trend being seen in technology delivery is software as a service (SaaS), where organisations can subscribe to a service provided in the cloud, rather than purchasing the hardware and software licences required to run the technology in-house. Such services provide access to the malware defence technologies required, as well as providing policy management and enforcement services for internet use and access control. With SaaS, security is placed in the hands of the service provider. The service provider performs real-time analysis of threats encountered through the sending of a digital hash of any file found to the analysis centres it maintains in the cloud for instantaneous analysis in order to determine if the file is malware. This allows updates to be immediately sent to all users of the service without the requirement for users to perform updates themselves.

The drivers for web security in the cloud

Given the importance of an online presence, organisations of all sizes are under pressure to protect their networks from abuse. They need to ensure that users do not download unauthorised software that could be compromised with malware; to be able to block users from accessing inappropriate or harmful content; and to monitor how network resources are being used. For many, keeping up with the growth and increasing complexity of threats, as more exploits target web-based applications, is an uphill battle.

Organisations are also under increasing pressure to ensure that information does not leak out of their networks inadvertently. Although stolen or lost mobile devices and careless email communications are prime culprits in allowing data to be lost or inappropriately communicated, the growing use of Web 2.0 applications such as blogs, wikis and social networking sites that encourage more interactive communications can lead to personal or sensitive company information being made accessible over the web. The use of such services can also leave users vulnerable to social engineering attacks. For example, many social sites, such as Facebook, encourage users to disclose a great deal of personal information about themselves, which has led to scams such as an imposter using the information gleaned from a personal profile to make unauthorised password changes and the "friends in distress" money-making scam, in which someone hijacks an account and sends messages to the friends of that user, claiming to be in trouble and needing financial help. Social engineering exploits also try to trick users into clicking on links in web pages that contain malware. If the computer is also used for work purposes, that could lead to malware threats being introduced into the organisation.

At the same time as they are under pressure to protect their networks, all organisations are being pushed to find ways to reduce costs in today's challenging economic environment, with upfront capital expenditures particularly under fire. The need to purchase licences for security tools for all users that need them, along with the hardware to manage the tools, is a large upfront item of expenditure for many organisations. Plus, deploying security tools in-house requires that IT resources be dedicated to the task, ensuring that updates are distributed to all, managing security policies and configurations, and putting out fires should users bypass controls or fail to keep their software up to date. This puts enormous pressure on resource-strapped organisations that are trying to do more with fewer resources. In particular, small and medium organisations tend to have just a skeleton IT staff that must manage all IT used in the organisation, not just the security aspects.

This is further complicated by the proliferation of mobile working and by expanding businesses that open up more geographically dispersed offices to service customers around the world. Deploying software and managing updates when a user is working remotely is an even more pressing challenge.

What organisations require is access to enterprise-class security applications and services without the upfront costs. The use of SaaS applications and services provided in the cloud fulfils those needs. Cloud computing is defined by the National Institute of Standards and Technology and the Cloud Security Alliance as a model for enabling network access to a shared pool of configurable computing resources such as networks, servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction. Rather than owning the physical infrastructure, organisations can rent use of the resources they require, paying for just the resources they consume, which is often done on a subscription basis, with usage scaled up or down as required. Thus, costs can be taken out of operating budgets, avoiding upfront capital expenditure on licences and equipment.

Use of services hosted in the cloud is especially important for organisations with large numbers of employees working remotely, whether at home or in branch offices, as they can be sure that each user has the latest protection applied to their devices. The ability to scale up the number of subscriptions to add extra users to a service as required, without the need for an administrator to set up the service for each user centrally, has additional benefits. For example, the Federation of Small Businesses in the UK estimates that three million people in the UK missed work on the first working day of 2010 owing to severe weather conditions, costing businesses some £600 million as workers were not able to securely access corporate

The drivers for web security in the cloud

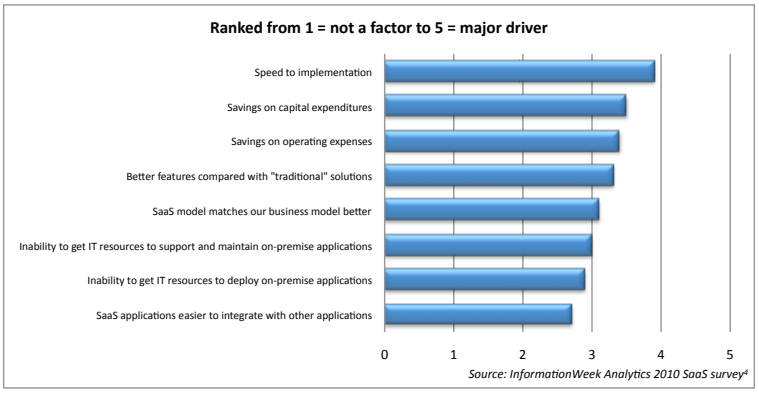

Figure 2: Major drivers for deploying SaaS applications

networks remotely. The UK's Centre for Economics and Business Research estimates that more than 2,000 companies could go bankrupt as a result. Such a situation clearly illustrates the need to provide secure remote access for employees to work from home in order to minimise productivity losses.

What the ideal cloud-based web security service should provide

Taken as a whole, the purpose of implementing web security tools is to be able to protect the organisation from threats, boost data security and regulatory compliance efforts, and to enable the business through improved productivity for all, including mobile workers.

To be effective, a web security service provided in the cloud should provide the means to stop viruses and other malware reaching an organisation, protect against phishing attacks and data loss, and prevent any other web-based threats from reaching the corporate network by filtering out malicious websites. It should be capable of protecting any device from web-based exploits whether the device is within the confines of HQ, or is accessing the network remotely. It must be capable of identifying users and authenticating them against permissions set in corporate directories in order to be able to enforce acceptable internet use policies.

The following services should be provided as part of any web security services package:

- Anti-malware, anti-spyware and phishing controls: for protecting against such threats, organisations should look for tools that provide protection beyond signatures that have been written to protect against known malware. Because malware variants are being released so fast the solution chosen should also offer heuristic filters, which look for patterns commonly associated with malware. This allows for protection against previously unseen variants of malware, or zero day threats, owing to the discovery of certain characteristics that point to the sample being malware. The use of heuristics will also boost the ability of the service to detect phishing attacks by looking for patterns associated with malware, in addition to databases of known compromised sites. Given the increasing prevalence of blended threats using a combination of web and email exploits, organisations should look for a service from a vendor that also offers email security products.

- Web content and URL filtering**:** web content and URL filtering enables organisations to protect themselves against malicious content such as malware or spyware embedded in web pages, or material that an organisation deems inappropriate, such as pornography or advertising. An organisation can set access policies according to role, group or individual in the organisation, and can limit access to specific categories of website to create customised URL lists. However, owing to the dynamic nature of the internet, organisations are advised to look for a service provider that keeps its database of malicious, inappropriate or compromised URL lists up to date with regular scans. In order to see what type of traffic is being filtered, the system should be able to provide reports of which users have requested which resources via a management console for audit purposes and to ensure that controls set are working as intended.

- Acceptable use policies**:** acceptable use policies are used by organisations to define which users can access which resources and the behaviour that is expected of them. This is particularly important given the expansion in the use of Web 2.0 applications such as blogs, wikis and social networking sites. The term Web 2.0 was coined in 2004 and such applications are proving to be popular with individuals looking for greater interactivity with friends and business contacts. At first, organisations looked to block their use within the work environment, but many are now realising that they too can benefit from greater use of Web 2.0 within their business. For example, most hiring managers will check a potential employee's posting on business networking site LinkedIn at the very least before extending an offer and some are proactively using Web 2.0 technologies to reach new customers and find potential employees. For this reason, many organisations are looking to allow their users access to Web 2.0 applications—although many will look to limit their use to a certain time period, such as over lunch, or to specific groups, such as human resources only. Therefore, organisations should look for a service that provides support for the quotas set in acceptable use policies to be enforced by placing limits on time spent online, bandwidth, number of sites accessed, or limiting access to certain applications to particular time periods.

- Ability to scale as required**:** given the increasing mobility of today's workforce, any service chosen should provide access directly via an internet browser, without requiring a user to first connect to the corporate network, which is often done with the aid of virtual private network technology that needs to be installed on each device by IT administrators. The service should also al-

What the ideal cloud-based web security service should provide

low new users to be registered directly via the browser interface through self-service tools so that users can start to use the service quickly when they need it. This will also allow an organisation to scale up usage of the service should a disaster occur or bad weather conditions prevent employees from travelling to work—as was seen in early January in the UK owing to heavy snowfall that made travelling impossible for some. In such a scenario, an organisation should be able to instantly request new users are temporarily added to the service to provide secure web access to prevent security incidents that could affect the performance of the business.

- Vulnerability analysis**:** a security threat increasingly being seen is that vulnerabilities are more often targeting not the actual browser, but the extensions and plug-ins that are made available for the browser. Most users are aware of the need to keep software applications up to date with the latest patches and upgrades, but less attention is generally paid to extensions and plug-ins to browsers, which are growing in popularity, in the main part for the added functionality that they enable for Web 2.0 applications. A useful addition to a web security service is the provision of vulnerability scanning capabilities to look for vulnerabilities in the operating system, applications and browsers on individual devices to report on any vulnerabilities that remain unpatched so that remediation action can be taken.

- Service level agreement**:** when choosing a web security service, an important aspect to consider is the terms and conditions of the service level agreement (SLA) that governs the service contract. This should not only include guarantees for uptime for the service and for 100% detection of all known viruses and spyware, but should also include penalties that will be applied should service levels fail to be achieved. Since the SLA is such a vital agreement governing the service, including the security controls that the provider puts in place, its importance cannot be over-stated. Security provisions that should be considered include background checks and certifications for staff and the service provided, such as SAS 70 standards, and granular access controls to avoid any service representatives being able to access sensitive corporate information.

- Business continuity services**:** in order for the provisions of the SLA to be achieved, organisations should look for a service provider that has multiple geographically dispersed data centres that can guarantee failover and redundancy in the case of one data centre being unavailable. The system should use load balancing techniques to route web traffic to the nearest available data centre so that performance latency is minimised in order to maintain a fast browsing experience, which can be further enhanced through use of download acceleration and high-performance proxies.

The following diagram depicts the main elements that should be provided in a web security services suite:

Figure 3: Elements needed in a typical web security services suite

The benefits of a cloud-based service for web security

When assessing any security technology system, the key questions that organisations ask themselves are: how does it add value, and how does it reduce both risk and costs. When considering web security technologies, this translates to how does it reduce risk by preventing security incidents, add value by improving data security and regulatory compliance capabilities, and cut costs by providing greater operational efficiencies, productivity and business enablement.

Whilst these are questions organisations ask themselves with any deployment, the decision to use cloud-based services adds an extra dimension as the organisation is effectively outsourcing the service to a third-party provider. Whilst this means that costs can be lower than for systems installed on-premise, organisations will need to make efforts to ensure that the service provider has the scale, financial stability and reliable systems in place to ensure the long-term continuity of service required.

Reducing risks through improved threat protection

The risks from interacting via the internet are real and growing in sophistication and complexity. This is leading many organisations to look at beefing up their security tools to guard their users and networks against these threats. Traditionally, this has meant installing tools on user devices and the network, trying to contain the threats from entering the network at a device level. However, this can mean that an organisation must handle licences for each software tool, install agents on user devices, and strive to keep protections up to date and ensure that all devices and applications are patched against the latest security exploits.

Such an approach to web security can be a management headache for IT staff, especially where organisations are under cost pressure and cannot afford to add more IT resources to cope with the strain. Because of this, many have switched from installing software on every device under control and have turned to the use of appliances where multiple security tools are brought together, with centralised management capabilities easing the administrative burden. Although such appliances are usually deployed in pairs, with one server acting as a failover in case of service outage, they can constitute a single point of failure—for example, should a misconfiguration be made that would affect all the users served. It is also hard to scale appliances as new users are added—for example, following a merger of two organisations. One further challenge with in-house software or appliance deployments is that catering to mobile users is a challenge, requiring that each device has virtual private network technology installed to ensure the security of the connection to the network resources.

For many organisations, outsourcing web security to a service provider brings many benefits. By using a service based in the cloud, protection against threats is brought nearer to where those threats are located, making it easier and more effective to protect users against security threats such as malware, as countermeasures for the threat are based in the cloud, meaning that threats can be eliminated even before they reach the network.

Many service providers offering cloud-based web security services maintain research and analysis centres in the cloud staffed by dedicated researchers who analyse the latest threats by scouring the web for malware threats, including variants, and using heuristics to look for patterns that indicate malware previously unseen in order to build new definition sets that can be pushed out to all customers simultaneously to provide updated protection to all, without requiring users to install updates themselves. The researchers will also look at threats facing particular customers, developing protections that are applicable to all other customers as well. In this way, all customers can benefit from the wisdom of the crowd, allowing all customers to be updated with new malware defences simultaneously.

Adding value by improving data security and compliance initiatives

The need to protect sensitive data is one of the most pressing security concerns facing organisations today. Data and information are the lifeblood of organisations, providing them with competitive advantage in the form of intellectual property, which is extremely valuable to competitors. As well as this, organisations of all sizes—not just the largest multinationals—collect large amounts of data regarding their own employees, as well as customers, in order to serve them better. However, that information is valuable to criminals who look to steal such information in order to commit crimes such as identity theft and fraud.

The benefits of a cloud-based service for web security

Protecting that information from loss is more than just a security concern. Although it is far easier to leak information out of an organisation via email, the role of the web in data loss is often overlooked. As blended threats become more common in order to stand more chance of being successful, email threats and web threats are more often being seen in combination. For example, an email may direct a user to a bogus website, where they may be asked to fill in personal information that can be stolen by criminals for financial gain.

To counter such emerging threat vectors, a combination of technologies is required, but, whilst many organisations have in place systems for securing email, the importance of the web as a vector of attack is often overlooked. By adding web security capabilities to protections applied to email, organisations will be able to ensure greater accountability over their important data. For example, web content and URL filtering will enable organisations to ensure that their employees are not visiting compromised sites that could be laced with malware or spyware that aims to steal confidential information, such as looking for passwords or combinations of numbers that can indicate credit cards or bank account numbers.

Through use of a cloud-based web security service, organisations can enforce policies aimed at protecting sensitive data. For example, policies can be set that state that certain users or groups of users may only access particular types of URL, placing websites with content such as pornography or gambling on block lists. To ensure that such policies are enforced, the service will match requests as they are routed through their service in the cloud to check that the request is in adherence with policies that a particular organisation has set.

However, organisations may wish to block or limit access to websites that do not contain malicious or inappropriate content, such as social networking sites that can prove to be a drain on productivity if used excessively. Whilst many organisations today see the value of such sites, as well as other Web 2.0 applications such as wikis and blogs, they may wish to limit use of such sites to a specific time of the day, such as over lunch breaks, or to limit usage to a period of, for example, one hour per day per use to avoid excessive usage. They can also restrict access to such applications to specific roles in the organisation, such as human resources or marketing.

By elevating policy enforcement points to the cloud, all outbound content can be checked before access to a particular website is granted by the service provider, taking the burden away from in-house resources. This is particularly important as a cloud-based provider will have the resources and scale to constantly check URLs and content for malware such as viruses and spyware to ensure that protections are kept up to date. This also has the benefit of freeing up IT resources that would otherwise be spending time policing which sites are safe or appropriate to access to focus on more value-added tasks, such as policy development and procedures for mitigating data risk. This is one area where use of a cloud-based service can add value to an organisation by allowing it to focus on its core needs of developing policies related to data security.

A cloud-service provider can also add value to an organisation by providing it with an easier mechanism for proving that its assets have not been compromised by user activity by providing reports on all access attempts and whether security vulnerabilities had been encountered or data compromised by malware. These reports can add value by allowing an organisation to prove that it has not been compromised by web exploits, and therefore can aid in its regulatory compliance efforts.

One further benefit of use of a cloud-based web security solution is that it is far easier to extend use of the system to mobile or remote users than an in-house system, where users generally have to authenticate themselves via a secure virtual private network technology system. This provides an extra expense and administrative burden for organisations as each device needs to have virtual private network technology installed and managed for updates. Through use of an in-the-cloud service, users can connect seamlessly to the service from wherever they are through use of just a browser, allowing mobile users or those working from remote offices to more easily set up and use the service without requiring virtual private network technology to be installed. This is because the service provider handles all authentication requests, verifying that a user is entitled to access the resources they have requested against permissions set in corporate directories.

The benefits of a cloud-based service for web security

Cutting costs through business enablement

Use of a cloud-based service enables rapid, easier deployment. Because it is easy to set up, users can be rapidly added as required following an expansion such as a merger with another organisation, or should extra users need the service to overcome a particular problem, such as inclement weather or a flu outbreak that prevents employees from getting to work. By being able to add subscribers on the fly, such situations can turn from being a disaster where employees are unable to function, to one where they can be quickly and efficiently added to the service for as long as the disaster continues.

Because access to the technology is provided as a service, the initial costs of set up are reduced. In particular, capital expenditures on hardware to house the applications are no longer required, nor are upfront investments for software licences for each user that needs the services. This is a particular benefit in today's economic climate where budgets are being cut back and capital expenditures, in particular, are under scrutiny. Through use of a cloud-based service, licences are paid on a subscription basis, with organisations needing to only pay for the number of users requiring the service in a particular month—rather in the same way as we just pay for the amount of electricity that we use every month. This means that the costs of the service can be taken out of operating budgets, where most organisations generally have greater flexibility.

Another benefit of using a cloud-based service is that it can provide almost unlimited capacity, with no real restrictions on how many users in the organisation can have access to it. This means that the incremental costs of scaling up the deployment can be reduced. For example, a server installed in-house can handle only a limited number of end users. When that limit is reached, further hardware will need to be purchased for the service to be available to more users. In contrast, service providers maintain massive data centres in the cloud comprising banks of virtualised servers that can easily scale to cater for more users as required.

Organisations using cloud-based services will also benefit from greater productivity for their IT personnel, who can be freed from the tasks of administering and managing the deployment, managing licences, performance and availability, and testing and deploying security patches. They also need to spend less time constantly monitoring the system for audit purposes to ensure that the controls in place are working effectively and that compliance is being achieved with regulations, such as those pertaining to data protection. Rather, such tasks can be offloaded to the service provider with high levels of expertise and with service levels guaranteed in such areas as uptime, security, reporting and audit. By outsourcing such tasks, the organisation is freed to focus on its core competencies—that is, running the business, rather than putting out fires and policing users to ensure that policies are adhered to.

Another area where costs can be reduced is that a cloud-based service can push updates to all users quickly and simultaneously so that all users have the latest, up-to-date protection. When software is deployed in-house, with agents installed on each device, ensuring all users are adequately protected is a time-consuming task that drains productivity. In an in-house deployment, a device that has not been patched in a timely manner is a security risk that can cost the organisation dearly should an incident occur that has to be remediated. Through use of a cloud-based service, with updates quickly and automatically deployed to users, the risk of an incident occurring, and therefore the costs of remediating that incident, is reduced considerably.

> *"Through use of a cloud-based service, with updates quickly and automatically deployed to users, the risk of an incident occurring, and therefore the costs of remediating that incident, is reduced considerably"*

Summary

Faced with the challenges of needing to protect their organisations from the complex and sophisticated threats that are being seen today, the use of web security tools can do much to controls risks emanating from the internet and give organisations peace of mind that their employees and networks are safe. However, the new austerity of today's economy means that all organisations are looking to curb costs and to do more with fewer resources. Where an activity is not core to the organisation, as is the case with preventing malware and other exploits from damaging resources, it makes sense to consider outsourcing capabilities to experts that have the necessary resources and systems in place to provide a secure service at a compelling price.

Cloud computing is the new face of outsourcing and its use can remove many of the burdens of implementing and managing technology applications for cash and resource-strapped organisations, whilst also boosting security capabilities by providing a higher level of security as threats can be countered at their point of impact so that they never reach the organisation's network in the first place. Provided as a dedicated service, organisations will also benefit from the scale of the proposition offered, with resources available to constantly scan the internet for new threats as they appear, developing countermeasures that can then be pushed out automatically to all customers of the service to ensure that protections are up to date, even for new threats previously unseen. The ability to achieve better protection against threats at a lower price tag than for traditional technology deployments should prove to be a draw for all organisations, from the very smallest to the multinational.

References

1 http://www.strategicsecurity.informationweek.com/

2 http://www.gocsi.com/2009survey/

3 http://laptoplogic.com/news/laptop-sales-exceed-desktop-sales-globally--20319

4 http://analytics.informationweek.com/issue/181/informationweek-full-issue-january-18th-2010.html

Further Information

Further information about this subject is available from http://www.BloorResearch.com/update/1081

Bloor Research overview

Bloor Research is one of Europe's leading IT research, analysis and consultancy organisations. We explain how to bring greater Agility to corporate IT systems through the effective governance, management and leverage of Information. We have built a reputation for 'telling the right story' with independent, intelligent, well-articulated communications content and publications on all aspects of the ICT industry. We believe the objective of telling the right story is to:

- Describe the technology in context to its business value and the other systems and processes it interacts with.
- Understand how new and innovative technologies fit in with existing ICT investments.
- Look at the whole market and explain all the solutions available and how they can be more effectively evaluated.
- Filter "noise" and make it easier to find the additional information or news that supports both investment and implementation.
- Ensure all our content is available through the most appropriate channel.

Founded in 1989, we have spent over two decades distributing research and analysis to IT user and vendor organisations throughout the world via online subscriptions, tailored research services, events and consultancy projects. We are committed to turning our knowledge into business value for you.

About the author

Fran Howarth
Senior Analyst - Security

Fran Howarth specialises in the field of security, primarily information security, but with a keen interest in physical security and how the two are converging. Fran's other main areas of interest are new delivery models, such as cloud computing, information governance, web, network and application security, identity and access management, and encryption.

Fran focuses on the business needs for security technologies, looking at the benefits they gain from their use and how organisations can defend themselves against the threats that they face in an ever-changing landscape.

For more than 20 years, Fran has worked in an advisory capacity as an analyst, consultant and writer. She writes regularly for a number of publications, including Silicon, Computer Weekly, Computer Reseller News, IT-Analysis and Computing Magazine. Fran is also a regular contributor to Security Management Practices of the Faulkner Information Services division of InfoToday.

Copyright & disclaimer

2nd Floor,
145–157 St John Street
LONDON,
EC1V 4PY, United Kingdom

Tel: +44 (0)207 043 9750
Fax: +44 (0)207 043 9748
Web: www.BloorResearch.com
email: info@BloorResearch.com