

White Paper



The drivers for web security in the cloud

...not least of which are the higher levels of protection afforded

The economics of using software delivered as a service, especially those provided in the cloud, makes this delivery option a compelling choice for many organisations

Fran Howarth

This document is sponsored by



Executive summary

The internet has become a key business tool for organisations in all types of industry and its importance continues to grow as an ever wider range of devices, such as smartphones, allow immediate, always-on connectivity. Its importance is not lost on hackers, who are looking to attack networks via the web as many see this as the greatest opportunity for their exploits to be successful. Their chances of success only increase with growing demand for interactivity of services and more collaboration, leading to ever more sensitive information flowing around communications networks.

Organisations are under pressure to guard against these threats, but at the same time are being forced to keep a tight control on costs—the new mantra for doing business in today's economic environment. This is leading to growing interest in new delivery models where access to applications and services is provided on a pay-as-you-use basis. This provides organisations using such services with not only the benefits of lower upfront investments in terms of software licences, the hardware needed to run the tools and the lowered cost of implementing the system, but also offers them enhanced protection capabilities against web-borne threats, as protection is applied directly where the threats are—in the cloud—so that attacks can be stopped before they even reach the organisation's network.

This paper is the second in a series of four papers that examine the realities of web threats and looks at the promise that cloud-based solutions bring for organisations in terms of providing a higher level of protection against the increasingly complex and sophisticated threats being seen today. The previous paper explored the nature of threats and future papers in the series will look at what components are vital for achieving a good level of protection and the benefits that are available from using protection services based in the cloud. As malware threats continue to rise, this series of papers is intended to be read by organisations in any industry that are trying to stem the tide of increasingly malicious web-borne threats.

Fast facts

- New technology delivery models speed time to implementation by lowering setup times and associated administrative burdens. This means that such services can even benefit consumers in an ad hoc manner, such as providing temporary protection for contractors using network services or for allowing users who are temporarily unable to reach office premises to keep productive by providing them with secure access to the information resources that they need to do their jobs.
- A cloud-computing model allows organisations to reduce their capital expenditures on software and hardware, replacing those costs with more predictable monthly subscription payments that can be scaled up or down as needed according to the number of users needing access.
- By using a service based in the cloud, where the threats are coming from, and using a service provider with guarantees over the level of service, organisations will be able to benefit from a better level of protection than if they were running the service in-house themselves.

The bottom line

The pressure to keep networks secure and boost levels of data security are key drivers for all organisations, especially as regulatory pressures continue to grow, demanding that security is applied holistically throughout an organisation. Given the growth in attacks being seen over the web that aim to steal sensitive data from networks, organisations should look to bolster their capabilities to defend against web threats, since this has become the prime vector of attack for hackers. No organisation can afford to rest on its laurels, but should instead take a close look at the options available and, in particular, at services based in the cloud.

Collaboration and interactivity on the rise

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.

Organisations looking for lower cost technology delivery models

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.

The rise of cloud computing

“Cloud computing is 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.”

Source: NIST

What organisations require is access to enterprise-class security applications and services without the upfront costs. The use of software as a service 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 that 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 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.

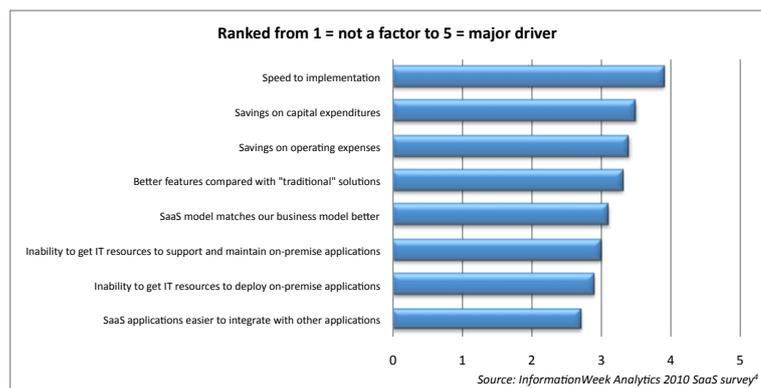


Figure 1: Major drivers for deploying SaaS applications

Why web security should be consumed in the cloud

Among the many technologies and services that are rife for consumption in the cloud are web security controls. Rather than having to license software for every device under protection and to update that software as new countermeasures are developed for each new threat, it makes a great deal of sense to move the protection closer to where the threats are emanating from—the cloud. Not only does this fulfil the key requirements of organisations today in terms of speed to implementation through lowered set-up costs, and the ability to save on capital expenditures and operating costs, but it also means that a better level of protection can be supplied. This is because updates for new threats seen can be pushed automatically to all end users as updates to the application so that users do not need to manually perform updates themselves. All users will also benefit from the “wisdom of the crowd” as, when a new threat is seen targeting one customer, a countermeasure can be developed that can then be supplied to all customers so that everyone has the latest, most-up-to-date protection available.

Summary

The economics of using software delivered as a service, especially those provided in the cloud, makes this delivery option a compelling choice for many organisations. Cloud-based services are becoming increasingly important for a wide range of services, from the management of customer relationships to outsourced management of infrastructure operations. Web security, in particular, is well suited to this delivery model owing to ease of set up, lowered costs of using the service and the access to higher levels of threat protection that it enables.

Reference

1 <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

This document is copyright © 2010 Bloor Research. No part of this publication may be reproduced by any method whatsoever without the prior consent of Bloor Research.

Due to the nature of this material, numerous hardware and software products have been mentioned by name. In the majority, if not all, of the cases, these product names are claimed as trademarks by the companies that manufacture the products. It is not Bloor Research's intent to claim these names or trademarks as our own. Likewise, company logos, graphics or screen shots have been reproduced with the consent of the owner and are subject to that owner's copyright.

Whilst every care has been taken in the preparation of this document to ensure that the information is correct, the publishers cannot accept responsibility for any errors or omissions.



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