White Paper

The benefits of basing email and web security in the cloud

...including cost, speed, agility and better protection

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

... the outsourcing of email and web security defences to a cloud-based service provider is one area where there are many benefits and few drawbacks

Fran Howarth

Executive summary

Organisations face a range of security threats, many of which focus on their main channels of communication—email and the internet. They must protect themselves against these threats, but every single euro in their budget needs to be justified and all spending is under scrutiny. However, those threats are becoming increasingly sophisticated and complex and must be taken seriously, but many security controls being used are not up to the job since they are only designed to counter threats that are already known about. Because of this, organisations should take a look at newer controls, now available, that can proactively protect them against the threats that they face.

One viable option that is suited to organisations of any size is to subscribe to email and web security services based in the cloud, using the latest behavioural detection techniques backed up by global threat intelligence services. Such services are quick and easy to set up and ongoing management tasks are handled by the service provider. The costs of such services can also be lower than technology implemented in-house since there is no requirement for upfront investments in software licences and the hardware to house them.

This paper is the third in a series of three that discusses cloud-based email and web security services and describes the benefits that use of such services can bring to organisations. The first two papers describe today's threat landscape and outline what organisations should look for when evaluating a service provider.

Fast facts

- Cloud-based services can be accessed almost immediately, taking away the time spent implementing the technologies in-house.
- By using cloud-based services, no upfront costs are incurred in the purchase of software licences and the hardware to house them.
- The global threat intelligence services provided by cloud-based web and email security vendors use the latest behavioural-based technologies and scanners to constantly look for new threats, write countermeasures for them and send out updates to all customers automatically, meaning that protection is superior to traditional technologies.
- Better protection against today's complex, blended threats is also provided by combining email and web security in one streamlined service.
- The use of cloud-based services provides an easier way of enforcing security policies.

The bottom line

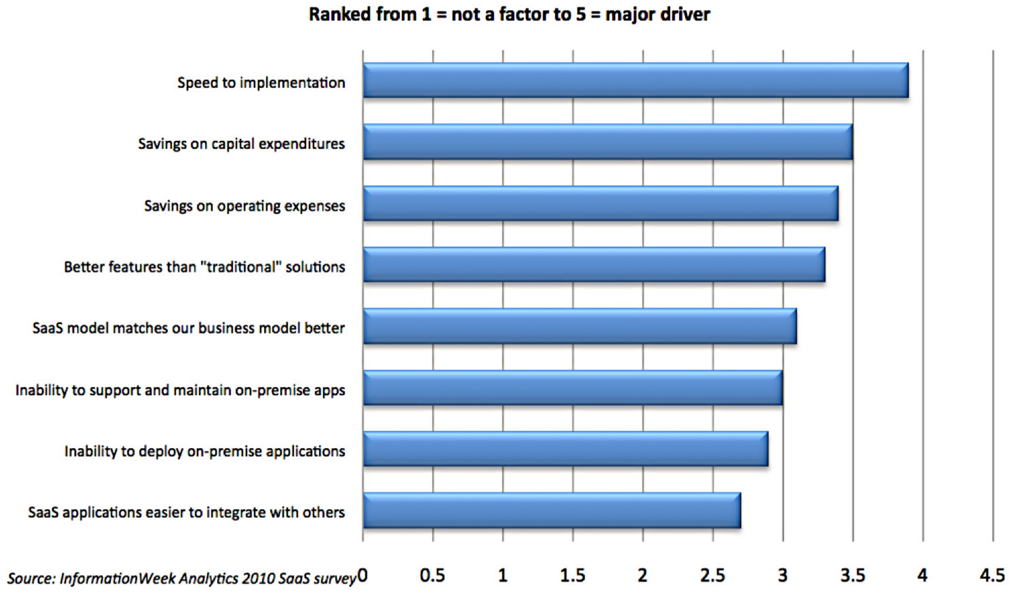
The outsourcing of none-core competencies to a service provider is a common strategy for organisations and makes a lot of sense for services such as email and web security. Today's threat landscape is complex and no organisation is immune from security threats, no matter their size. The low upfront investment and the high level of protection that such services provide are key benefits of subscribing to such services rather than having to deploy the technology themselves, with all the associated costs and administrative headaches that are associated with in-house deployments. They are also suited to any organisation, regardless of size, providing even the smallest company with the same level of protection that their larger counterparts can afford.

The benefits of using a cloud-based service for email and web security

As the figure below shows, speed to implementation and reduced cost are the primary drivers for organisations looking to subscribe to cloud-based services rather than run their own deployments in house. Organisations of all sizes are under cost pressures, made worse by the recent economic slowdown, and will see the benefit from the reduction in capital expenditures that use of such services allows. This is because the hardware to run the service is provided by the cloud-based provider, requiring that no investments in IT infrastructure components are required, and the software licences are provided on a subscription basis, generally paid for on a monthly basis, rather than needing to purchase the licences upfront. This means that the service is provided as a predictable monthly operating cost. Plus, the costs of administering and managing a web and email security deployment in-house are reduced, whilst at the same time ensuring that all users have the latest up-to-date protections through upgrades to the software.

Because of the low upfront costs required to make use of this service and because the service is handled by a service provider, smaller organisations will benefit from using protection in the cloud. Whereas the investment required in installing technology in-house and managing the implementation can be fairly expensive, making this option most suited to larger companies with the budgets required and access to the relevant expertise to run the service themselves, the low costs of a subscription-based service make it ideal for organisations of any size, even the very smallest. Especially important are threats that are being increasingly targeted at specific individuals or organisations, and small companies are just as much at risk as their larger counterparts. The prime benefit of using such a service for smaller organisations is that their lack of budget or in-house expertise need no longer be a disadvantage.

Because the service provider handles the entire service on behalf of an organisation, users will also benefit from being able to get up and running fast, rather than having to spend time deploying and testing the technology themselves. Users can be signed up to the service via a secure browser interface and extra users can be added as required owing to the flexibility of a subscription-based service.



Source: InformationWeek Analytics 2010 SaaS survey

Figure 1: Reasons for choosing a cloud-based service

The benefits of using a cloud-based service for email and web security

Although the relatively low cost and high speed of implementation of cloud-based services are compelling benefits for the use of such services, another key reason for using such services is that the level of protection provided can be better than that offered through an in-house implementation. Threats seen today are becoming increasingly complex and sophisticated, often using email communications and websites in combination to increase their chances of success. Such threats are becoming too complicated for organisations to resolve on their own, and especially small and medium organisations with limited resources and other priorities than upgrading software regularly.

Hackers are also increasingly testing their exploits against anti-malware protections and are writing more variants of each exploit to try to defeat traditional, signature-based mechanisms and static filters. A cloud-based service provider that is constantly looking for new threats and writing protections against them using newer behavioural-based techniques and through proactively crawling the internet for malware, can provide a better level of protection by defeating the threats at the point from where they are emanating. New protections can then be simultaneously pushed out to all users of the service, with no action required on the part of users to perform upgrades themselves.

Better protection will also be seen from use of a service that provides both email and web security capabilities in an integrated fashion so that protection can be applied to both email and web-based threats, which is important in dealing with the blended attacks that combine both vectors that are increasingly becoming prevalent.

One final benefit seen from use of such a service for email and web security is that it can help to shield users from social engineering attacks that are becoming a common part of the threat landscape. Educating users is of much value, making them aware of the risks and how to avoid them, such as not giving away too much personal information that can be used against them or clicking on links that could lead to them being infected with malware. However, no user can be vigilant all the time and it is all too easy to make mistakes. Acceptable use policies are essential, but they need to be enforced by the technology that is being used. A policy is a bit like a speed limit—everyone knows that speed limits exist on roads for our own safety, but without speed cameras and police to enforce the limit, many people would believe there were no sanctions and would drive at the speed they wished. In the same way, an acceptable use policy is only useful when it can be enforced.

Summary

The benefits of outsourcing none core competencies to a service provider are many; this is a common strategy followed by many organisations for a wide variety of needs. Given the complex, highly targeted nature of today's security threats, the outsourcing of email and web security defences to a cloud-based service provider is one area where there are many benefits and few drawbacks. With lower upfront costs than implementing technology in-house and with the service administered by experts, organisations of any size from any industry will benefit from ensuring that their communication channels are secured without the expense and administrative headache of managing the controls themselves, freeing themselves up to get on with the tasks of running the business.

Further Information

Further information about this subject is available from
http://www.BloorResearch.com/update/2045

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

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