

# White Paper



## When the cloud improves security

...move protection to where the threats are

Through combined, integrated web and email protection, organisations will be in a better position to protect personal and sensitive corporate information from online and internal threats

[Fran Howarth](#)

## Executive summary

---

Malware threats are on the rise and the attacks are growing in sophistication and complexity. Individuals and specific organisations are increasingly being targeted, using exploits that rely on more than one attack vector, often combining a phishing email with web-borne malware. Many attacks today play to human nature, using social engineering techniques to trick users into giving away information or downloading content riddled with a malicious payload.

This paper discusses how security threats are emerging and the importance of combining protection against email and web-borne attacks since today's threats increasingly use a combination of the two vectors. This makes them harder to detect and mitigate, leaving organisations that are relying on traditional security protections exposed. Since fighting malware infections is not a core competency of most organisations, especially small and medium ones, the answer for many will be to subscribe to the services of an expert services provider with its own array of resources based in the cloud.

### Fast facts

- The majority of organisations have deployed protection for their email communications, but many of these are based on outdated technology that is not up to the job of protecting against the complex threats seen today.
- Malware delivered over the web is an even more serious problem, but not enough organisations are taking the threats seriously.
- New technologies on the market are available to mitigate those threats, combining protection for email communications and web-based applications and content.
- New technology delivery mechanisms offered as a service take much of the pain out of the fight to keep threats at bay and are suited for even the smallest of organisations.

### The bottom line

With attacks increasingly targeted at specific individuals or organisations, even the smallest organisation cannot afford to be complacent. However, many lack the resources to adequately protect themselves. The answer is to outsource email and web protection to a service provider with data centres based in the cloud—taking protection to where the threats are coming from to prevent bad traffic from ever reaching the organisation and helping to ensure that sensitive data cannot inadvertently be leaked.

## Today's threat landscape

---

Having been on the wane in recent years, malware attacks are on the rise again. Malware is a term that refers to malicious software that is designed to cause damage to computer networks. The term covers a variety of programs including viruses, worms, Trojans, spyware, adware, crimeware and root kits. According to the Computer Security Institute, which conducts an annual survey of computer crime and security, malware infections had been falling as a percentage of overall security threats seen by respondents since 2005. In 2008, 50% of respondents reported that they were the victim of a malware attack, but in 2009 this had risen to 64.3%, making malware infections the most prevalent form of attack.

According to one estimate, there was as much malware produced in 2007 as in the previous 20 years put together. By another estimate, there were 73 million malware variants in 2009, with 2,465 new websites hosting malware being seen daily. In 2009, the spam rate globally was 87.7%, translating to 107 billion messages per day, and the virus rate worldwide was one in 286.4 emails.

Not only is the problem of malware increasing, the attacks are becoming increasingly targeted with the aim of gaining access to sensitive data produced and stored by both individuals and companies. This is because hackers have realised the value of such information, which can be used to commit crimes such as identity theft and fraud. Any organisation or individual that possesses sensitive and valuable data can be an attractive target for such criminals, who are increasingly organising themselves into criminal networks.

Particular threats that are on the rise are those affecting websites. According to the Anti-Phishing Working Group, 95% of attacks rely on HTML as a delivery mechanism and the number of phishing attacks is growing at 28% per month. During the second half of 2009, the growing popularity of social networking services such as Twitter and their increased use in spam emails led to an upsurge in the use of shortened URLs, which spam filters find harder to detect than traditional URLs. Other social exploits seen to be increasing include those related to world events, such as the global credit crisis, and news events.

For example, the death of Michael Jackson in June 2009 was a world event that caused a huge upsurge in traffic over the internet of

anything from 11% to 20% higher than normal, causing many popular websites to collapse under the strain. His death also caught the attention of hackers, who cashed in on interest in Jackson's untimely death by distributing malware such as Trojans that look to capture banking details via malicious hyperlinks in websites pertaining to carry news of the event and through spam emails.

Social networking sites in particular are proving to be an increasingly popular target for hackers, phishers and spammers looking to distribute malware. Such sites are popular targets since they encourage self-published content and promote profile customisation to users. This leads many to publish large swathes of personal information on these sites, such as home address, phone number and social preferences. In some cases, users log into such sites using their corporate email address, or give details about their employer online. There have even been cases in the news involving companies such as Virgin Atlantic, retail store Argos and directory enquiries service 118 118, where employees have placed derogatory information about the companies or their customers on social networking site Facebook, which could do much to damage the reputations of the firms involved and lose them business.

Attacks against social networking sites, including Wikipedia, MySpace and YouTube, have been seen recently using blended methods that combine the use of phishing emails with web-based malware in an attempt to trick users into clicking on a link that plants a worm on their computer. Another exploit uses popup adverts that urge a user to click on a link that installs a Trojan on their computer.

### Blended and targeted attacks on the rise

Where there has been a decrease seen in malware recently is in the mass distribution of malware through email communications. Not only have many organisations and individuals put in place technology to filter emails for malware, users have become more savvy about the threat that emails pose. As users have become more wary of security exploits launched en masse, attackers have responded with more targeted exploits against specific individuals or organisations, often using information gleaned about those targeted to try to trick users into thinking that the communication is genuine.

## Today's threat landscape

---

As attacks that purely rely on email as the vector of attack are proving less successful, attackers are turning to blended mechanisms to try to make their exploits more successful, using a combination of email and web-based exploits. For example, a phishing email may be sent to a user containing a link that takes them to a certain website where a malicious payload is delivered to the user. In this scenario, the email itself is the threat, but it is the website that does the damage. Conversely, a user could click on content such as a video that is tainted with malware, download it and send to a contact via email. In this case, the email is the secondary transport mechanism for the web-based threat.

An example of the way that threats are evolving is the attack against Google and some 20 other organisations in China in early 2010, which is the most sophisticated attack seen to date against commercial enterprises. The attackers made use of up to a dozen pieces of malware delivered as obfuscated software via SSL connections to deflect internal firewalls and intrusion scanning devices in order to allow the malware to burrow deep into Google's internal network. The attack started with a spear phishing email—a highly targeted phishing exploit aimed at specific end users at the organisations selected—which contained malicious attachments with payloads aimed at stealing confidential information from the network, including source code. The attacks used different, custom-developed malware payloads to deliver highly targeted attacks, increasing the likelihood that the attack would be successful.

## Traditional protective technologies less than effective

Malware has long been recognised as a problem by organisations and individuals alike, leading to use of technologies to try to protect users from infection. The Computer Security Institute found in its 2009 computer crime and security survey that 99.1% of respondents were using anti-virus software, 97.9% had deployed firewalls and 89.9% were using anti-spyware software. However, just 60.4% of respondents were using web or URL filtering technologies to protect themselves against malware picked up on websites.

### Traditional email security products fail against new threats

However, while many of the products, such as anti-virus, in use in organisations today provide protection against existing, known threats, they do little to protect against the new types of threat being seen, which are growing in complexity and sophistication. Malware writers are increasingly writing multiple variants of a single exploit to increase the chances that the exploit will be successful. Traditional anti-malware technologies deploy signatures to identify malware, but this method relies on the use of a sample of malware that has already been released to create those signatures. Anti-malware technologies relying on signatures also need frequent updates so that users have the latest signatures available, which can be a management headache and which can lead to security issues if those upgrades are not done on a timely basis.

Criminals looking to hack into networks have much to gain financially from their exploits, making hacking increasingly profitable. With ample resources at their disposal, hackers are now testing their exploits against anti-malware technologies available on the market or will purchase anti-malware appliances to test malware variants in a lab before targeting the market. As well as this, they are increasingly writing polymorphic and other types of viruses, which encrypt parts of themselves or modify themselves on the fly to get around signatures.

To try to improve detection capabilities, anti-malware technologies have come onto the market that employ heuristic analysis to

identify new malware or variants of a known piece of malware. Technology that uses heuristics looks for known sources, text phrases or content patterns that are known to be associated with emails or websites containing viruses. However, heuristics are known to flag a number of false positives and therefore must be thoroughly tested by the technology vendor offering the technology.

### Organisations not doing enough to protect against web-based threats

In terms of web-based threats, many organisations are leaving protection against malware threats to chance. As the survey referenced above from the Computer Security Institute shows, just 60.4% of respondents are deploying web or URL filtering technologies. However, the same survey shows that malware infections are the most prevalent type of threat facing organisations today—and becoming more so—and the majority of those threats are web-based.

Web security tools help protect organisations against crimeware and malware entering their organisation, and against confidential data leaking out of their networks. Yet, modern internet tools are making websites even more of a security risk owing to the high level of interactivity that Web 2.0 and social networking applications enable. It is estimated that 80% of internet users accessed social networking sites in 2009 and criminals tend to target places where people congregate.

The issues of Web 2.0 applications and social networking sites are not just a problem because of the programming tools and techniques used to create them, which tend to expose more of the business logic such as access controls to users, and therefore to hackers as well, but also because traditional security mechanisms struggle in tracking such sites. Traditional web filtering technologies rely on databases of URLs and honeypots for tracking and classifying websites, but such tools have problems keeping up with the dynamically changing content of Web 2.0 applications and social networking sites, making them less than effective.

## Traditional protective technologies less than effective

---

### Mobile technologies opening up the perimeters

One other factor hindering organisations in their efforts to protect themselves against today's malware threats is the increased mobility being seen in the workplace. The International Telecommunications Union estimated that there were 4.6 billion mobile phone subscriptions worldwide at the end of 2009. Increasingly used as a business tool, today's generation of mobile phones are known as smartphones and offer capabilities similar to those of a computer, able to store large amounts of information. It is difficult to extend traditional security software installed on in-house servers to mobile workers without requiring them to have VPN technology installed on each device to be protected in order to create a secure communications tunnel to the organisation's network. This situation leads to more expense and administrative headaches—especially given the importance of mobile connectivity. As yet, attacks targeting mobile devices have only been seen at relatively low levels, but hackers are increasingly turning their attention to mobile devices as more individuals use them to read emails and surf the internet.

## Moving protection to the cloud

The vast majority of organisations have put some form of technology solution in place for protecting themselves against email threats but, as the data above from the Computer Security Institute demonstrates, less attention is paid to web security. However, the web is now the prime vector of attack for hackers, albeit often combined with email communications. Organisations are also making greater use of web-based applications that provide a richer experience and more functionality. For example, many organisations now blog, contribute to wikis and make use of social networking sites.

Owing to the limitations of traditional protective technologies, against email threats in particular, many organisations are looking to upgrade their existing investments. Virtually every organisation has some form of protection in place for emails, but many of the products used are not effective against the latest threats. There is also growing interest in web security products owing to the increased publicity that these threats are getting. In particular, negative coverage of exploits against social networking sites including Facebook, YouTube and MySpace are helping to drive awareness of the security issues involved in use of the web.

As discussed earlier, the problems involved in traditional email and web security products include the frequent updates that are required to guard users against known threats, with the software installed on each device to be protected needing to be updated on a regular basis. For web security products, URL filtering and website reputation tools need to be updated regularly as well, which can be a huge administrative task for an organisation managing the products itself. Plus, whilst many early products do a good job at catching older, known threats, many lack the speed and agility to identify threats associated with the dynamic online content associated with social networking sites and other Web 2.0 applications.

As traditional mechanisms for guarding against malware exploits struggle to keep up with the new challenges being seen, new types of delivery mechanisms for security services are increasing in popularity. These include the use of software delivered as a service via subscriptions as opposed to purchasing licences to use the software and install it on devices needing protection. Such services have grown in scope over the past decade, when the first of such services centred on customer relationship management and sales force automation

applications. Today, the range of services offered has expanded considerably and now includes access to security technologies.

The use of software provided as a service from a provider with data centres based in the cloud makes a lot of sense for some security services such as web and email security since the protection is moved to where the threats are coming from—primarily the internet and associated applications. The use of such services provides users with lots of benefits and has few drawbacks. By outsourcing such services to a third party, the service provider aids organisations by ensuring that bad traffic is prevented from ever reaching the network in the first place, as well as preventing data from being inadvertently leaked out of the organisation. The outbound controls that are offered perform at least the basic functions of data loss prevention tools, providing organisations with a better ability to improve their data security posture.

To use the service, users just need to connect via an internet browser to receive the benefits of protection against threats emanating from the cloud. This makes the use of such a service useful for mobile workers not physically present in an office, since they can access the service directly without having to set up a VPN connection to reach the resources that they wish to access. With mobile technologies growing in importance, it is essential that mobile workers are not left out in the cold.

Providers offering such services generally maintain threat centres staffed by researchers who analyse the latest threats being seen worldwide over the internet and develop countermeasures to guard against those threats affecting their customers. Because all of their customers connect to the service in a similar fashion, updates developed as a result of a threat seen to one customer can then be automatically sent out to all customers, providing them with the benefits of the wisdom of the crowd.

### New technologies provide protection against the latest threats

Most such services are able to respond not just to known threats, but can also provide protection against new threats as they deploy new identification techniques using heuristics and other behavioural mechanisms to gauge if a new file exhibits the characteristics associated with malware. If each organisation were

## Moving protection to the cloud

---

to attempt to use such tools for an in-house software deployment, the administrative burden would be huge, especially in terms of ensuring that all devices are up to date regarding the latest security threats. Thus, any organisation looking to provide such services to its users by itself is facing a game of catch up, with limited resources constantly trying to stay ahead of the latest threats. By outsourcing these functions to a third party, the problem is put in someone else's hands.

A cloud-based service provider that is constantly researching the latest threats and applying countermeasures at the point where the threat comes from is in the position to prevent threats from entering the organisation in the first place, rather than internal resources spending their time putting out fires. This means that protection can be provided faster and, through use of advanced techniques, can actually provide a better level of protection than software deployed within the organisation with all the associated administrative headaches.

A further benefit is that the service is delivered by those who are experts in the field, backed up by guaranteed service levels governing such things as availability of the service and business continuity services should one data centre fail or become overloaded.

Industry analysts Gartner predicted in July 2008 that cloud-based malware and spam detection in email and instant messaging will grow from 20% of the market for total messaging security revenue in 2008 to 60% over the next five years, and that email security services in the cloud will jump from 20% of the total email security market in 2008 to reach 70% by 2013. This compares to growth for the overall security-as-a-service market, which it estimates will see compound annual growth rates of 30% from 2007 to 2012.

However, the web security market is less mature. Gartner estimates that just 1% of the secure web gateway market was based in the cloud in 2008, but that this will rise to 25% by 2011. IDC concurs, stating that the SaaS sector of the web security market will see growth exceeding that of software and appliances to reach US \$513 million by 2013, translating to a compound annual growth rate of 46.5% from 2008 to 2013.

## What the ideal cloud-based service should offer

With today's threats looking to combine different vectors of attack in an attempt to make the exploit more successful than merely sending out malware as a mass email communication, hoping that users will be hoodwinked into downloading the malware, organisations should look for a service from a technology vendor that specialises in both email and web security. It is no longer sufficient to have protection for one or the other in isolation.

Through combined, integrated web and email protection, organisations will be in a better position to protect personal and sensitive corporate information from online and internal threats. To do this, they must be able to inspect everything that goes in to or out of the organisation via electronic communications channels to block malicious code, prevent loss of information, and enforce security and acceptable internet use policies.

Some of the essential elements that any such service should offer include the following:

- Anti-malware, anti-spyware and virus protection: the cloud-based service should scan all inbound and outbound traffic for malware, using a variety of techniques, including heuristic filters to protect against new, previously unseen, threats. The combination of email and web security capabilities is vital for protecting against blended threats combining email and web attacks.
- Content filtering: the service should provide content filtering for both email communications and for threats emanating from the internet. For emails, it should filter all inbound and outbound communications, including as many different attachments as possible, using a wide variety of software applications. For more granular levels of control, filters

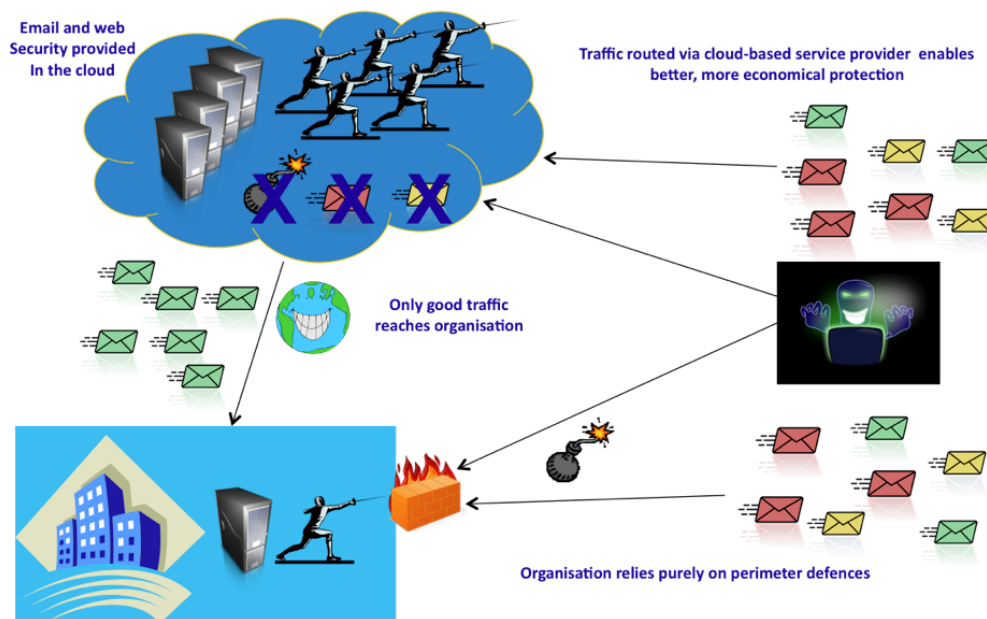


Figure 1: How a cloud-based email and web security service works

## What the ideal cloud-based service should offer

---

can be set differently for different classes or groups of users according to need. The service should also filter content for spam, which is estimated to account for nearly 90% of all emails. For web content, it should offer advanced filters for URL and web content scanning, and should be able to block websites in categories deemed unacceptable to the business, such as gambling or pornography. Any site containing malware should be automatically blocked by the service and some services will guide users as to which websites are allowed, have been blocked or that potentially contain malware, allowing them to make more informed decisions. The service should also offer real-time heuristics for detecting new phishing sites as they are set up.

- Threat research centres: to ensure that the protection offered by a cloud-based service is up to date, the technology vendor should provide more advanced protection than merely reacting to threats as they are seen. Rather, its researchers should also proactively look for new threats, using automated web crawlers that actively search for websites infected with malware, and should ensure that all information is placed in its threat database so that users are protected from those sites. To do this, the vendor must have substantial computing resources, based in the cloud where the threats are coming from.
- Policy management: any web and email security service should enable organisations to easily manage and enforce the policies that guide their business. These include acceptable internet use policies, which guide the behaviour expected of users and which can include time quotas, such as time periods when use of social networking sites is allowed or overall limits on the time that can be spent surfing the internet. It should also be able to enforce policies related to encryption of emails to prevent sensitive information from leaking out of the organisation and should provide support for email archiving policies for preventing data loss and achieving regulatory compliance.
- Logging and reporting capabilities: any service chosen should log all activity put through the service, including every email sent or received and every website visited, with the data compiled into reports that can be provided via a web-based management portal. To be useful for management purposes, these should show activity broken down by account, group or role in the organisation and should monitor how the internet and email communications are being used.
- Service level agreement: when any business processes are outsourced to a third party, it is essential that the terms and conditions are clearly laid out in a service level agreement, including penalties that will be applied should service levels fail to be achieved. Guarantees should include the level of uptime to be provided and 100% detection rates for all known malware for an email and web security service, and sometimes for unknown malware also. The security controls put in place by the service provider should also be detailed, including background checks and certifications required for staff and the service provided, such as SAS 70 standards, and granular access controls to prevent data access by those not authorised to do so. Other things to be included are guarantees that policy changes will be made within a specified time period, and global load balancing capabilities across multiple, geographically dispersed data centres for business continuity purposes.
- Coverage for mobile workers: for today's business environment, the ability to extend protection to mobile workers is a must so that protection is guaranteed against malware and web threats for workers using mobile devices when working remotely. To do this, the service should provide a direct interface for mobile devices so that remote workers do not need to establish a VPN connection to access the service via the corporate network.
- Rapid deployment and scalability: a key factor in any cloud-based service is that it should be easy to get started with and use since no hardware or software needs to be deployed for users to access the service. Rather, users should just be able to sign up to the service via a web-based interface to gain immediate access. It is also important that the service is highly scalable as email volumes continue to grow and for adding new users to the service when required.

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

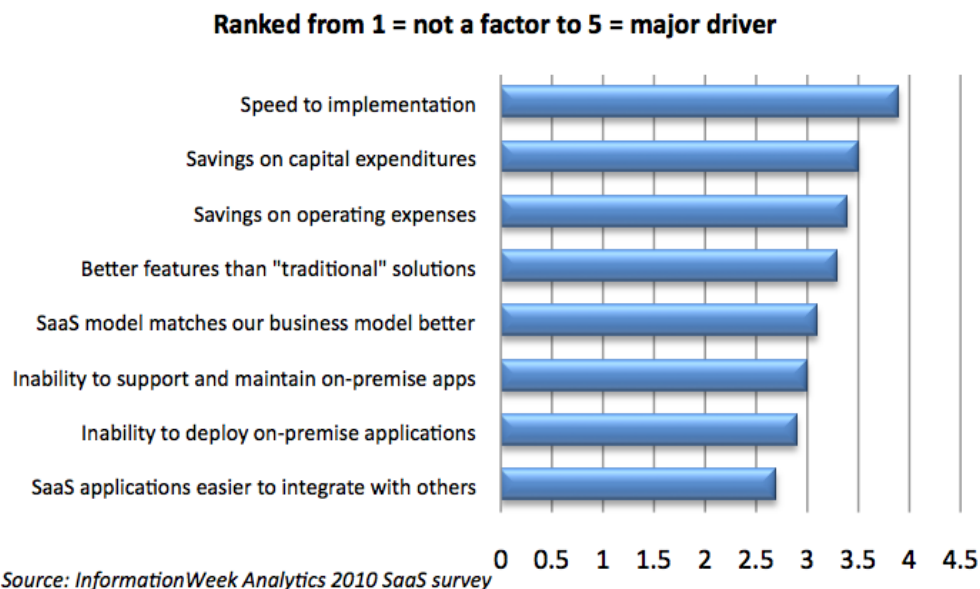


Figure 2: Reasons for choosing a cloud-based service

As Figure 2 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.

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

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

---

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 threats posed by email have long been known, but malware infecting web-based applications and content is actually a greater threat. With nearly two-thirds of organisations reporting that malware is the greatest threat that they face, often using a blended mechanism of email and malicious payloads delivered over the internet, organisations of all sizes should look for technology that can counter such threats simultaneously. It is no longer sufficient to have protection for one or the other in isolation.

Through combined, integrated web and email protection, organisations will be in a better position to protect personal and sensitive corporate information from online and internal threats. To do this, they must be able to inspect everything that goes into or out of the organisation via electronic communications channels to block malicious code, prevent loss of information, and enforce security and acceptable internet use policies.

For many organisations looking to protect their networks and users from harm, cost and complexity and lack of skilled resources are considered to be barriers, but this does not need to be the case. Email and web security services based in the cloud provide high levels of protection at a price affordable to even the smallest organisation.

### Further Information

Further information about this subject is available from  
<http://www.BloorResearch.com/update/2032>

## 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](http://www.BloorResearch.com)  
email: [info@BloorResearch.com](mailto:info@BloorResearch.com)