Off-Network Workers – The Weakest Link to Corporate Web Security

Google

"By the end of 2011, IDC expects nearly seventy five percent of the US workforce to be mobile."

"A consultant for a Big 5 audit firms was discovered playing poker during the day while connected to the client's network."

Introduction

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

"How do you improve the web security of remote workers without wasting precious IT resource and budget?"

This paper considers the type and severity of risk to the enterprise posed by use of the internet by its off-network (roaming) and remote workforce. It will be seen that there are many potential areas of brand, operational and security risk which the application of conventional solutions has failed to address. These solutions will be examined. The paper concludes that web security delivered via the Software as a Service (SaaS) model has unique features which make it the most secure and cost effective way of delivering productive access to the internet for remote and off-network users.

The Mobile Challenge

Have you ever used an open, unsecured wireless connection because you desperately needed to access a particular email? How many calls does your support desk receive from staff complaining that web access from their laptop is slow because they are being forced through the corporate internet gateway? Do your mobile workers ever switch off or disable security features because they think they're slowing them down? Are your mobile workers working at all or just aimlessly web surfing and chatting to friends? If the answers to these questions aren't overwhelmingly positive then you are in a majority. Organizations of all sizes are still wrestling with the challenge of applying their web security policy outside of the corporate network and the challenge is only going to grow.

By the end of 2011, IDC expects nearly seventy five percent of the US workforce to be mobile, with Europe not far behind[1], and there is no doubt that the current generation of workers are demanding and receiving more flexibility in their working arrangements. The proliferation of public Wi-Fi hotspots as well as high speed internet access in the home allows employees to work almost anywhere. This increased flexibility can work for employers as well – office space requirements are reduced, business response time increased and staff retention improved. This fundamental shift in the way that people work has created a number of challenges, and, in particular, the difficulty of securing a highly elastic network perimeter has been bought into sharp focus.

The Implications of Unrestricted Web Access

The vast majority of organizations have been convinced of the requirement to enforce an Acceptable Usage Policy ('AUP') for internet use within their corporate network. These organizations understand that the brand and operational implications of unfiltered web usage could be grave.

Recently, a junior consultant for one of the Big 5 audit firms, billing out at over $3000 per day, was discovered by the client playing on-line poker while connected

[1] IDC Worldwide Mobile Worker 2007-2011 Forecast and Analysis

"Sixty five percent of respondents to a survery reported instances of employees deliberately circumventing security features on their laptop."

"Illegal file sharing sites are requested seven and a half times more often by an off-network user than they are when that worker is in the office."

to the client's network. The Senior Audit Partner for the audit firm had to personally apologize to the client CEO for his employee's bad behavior. In addition, the audit firm's CISO had to fly to the client's site and personally assure the client CISO that such behavior would not happen again.

In another case, a regional property management company had so many people streaming internet radio and reruns of popular TV shows over their network that the payroll system crashed – on pay day.

The operational and brand risks are only part of the picture: network security can also be significantly compromised. Many employees are blissfully unaware, when they are updating their social networking profile or searching for dancing cats on video sharing sites, that it is precisely these sites on which malware is most likely to be lurking. The inherent insecurities in Web 2.0 applications have been extensively documented. Incidences of browser vulnerability exploits are increasing and these exploits happen with ever-increasing frequency. Other types of malware can be used to steal confidential data which could breach customer confidentiality and numerous regulations, as well as incur the organization a serious financial penalty and public relations nightmare. There is some evidence that cyber criminals are now specifically targeting laptop users, encouraged to do so by the finding that corporate laptops hold an average $525,000 worth of sensitive data.[2]

The problems above are compounded when a compromised laptop is then unwittingly reconnected by its owner to the corporate network. Any malware can now spread through the network with ease. This can cause serious operational and productivity losses for workers unable to access key business applications as well as the IT team that have to clean up the network.

The Weakest Link

With so much at stake, enforcement of an AUP is a must have. However, as soon as a user leaves the corporate head office, this enforcement becomes no less important, but considerably more challenging. The majority of organizations consider off-network users to be the weakest link in their corporate web security strategy. Ninety percent of respondents to a recent survey stated that they had concerns on the issue and sixty five percent reported instances of employees deliberately circumventing security features on their laptop. Forty percent reported that they had been exposed to a security threat as a direct consequence of an off-network user's laptop getting compromised within the last twelve months.[3] Why?

The fact that off-network users are significantly more likely to access inappropriate material when on the road than they would be in the office isn't terribly difficult to believe. However, a recent study has helped to illustrate just how much user behavior is likely to change when they are out and about.[4] In particular, pornographic material is requested two and half times more often, lingerie, swimwear and nudity sites three times more often and blogs around one and a half times more often. Investment websites are requested twice as often as are ones categorized as humorous. However, perhaps the most alarming finding of this particular study was the fact that illegal file sharing websites are requested seven and a half times more often than they would be by the same user while in the office. This is not just a drain on productivity. It places a significant strain on network resources and the wider legal implications should worry any CIO.

[2] iBahn, October 2007
[3] ScanSafe Roaming Security Survey January 2008
[4] ScanSafe Analysis April 2008

"The annual costs of owning and managing software applications can be up to four times the cost of the initial purchase."

"The fingers crossed approach is fraught with risk."

The Conventional Approach

The traditional methods that organizations have employed to try and mitigate the risks created by a roaming work force have created problems of their own. The conventional approach is to use end-point solutions to create an IPSEC or SSL VPN to ensure a secure connection to the corporate network and couple it with a desktop anti-virus solution to secure the host. This method allows an organization to enforce their web usage policy by subjecting any web requests to content filtering. This often turns out to be considered unsatisfactory both in terms of security and cost. Backhauling traffic via a VPN can create severe network bandwidth congestion and can significantly impact user experience which is, understandably, never popular.

This method also does nothing to resolve the challenges of managing multiple products. These challenges are both financial and operational in nature. According to Gartner, the annual costs of owning and managing software applications can be up to four times the cost of the initial purchase.[5] Consequently, a significant chunk of IT budget can be used in the maintenance of this software infrastructure. One of the biggest ongoing challenges for IT Managers is keeping this infrastructure up to date, like keeping the operating system and the security products themselves patched and up to date. For desktop protection, oftentimes the end user is responsible for accepting malware updates. This is far from ideal. If a request to download an update happens to fall in the middle of an important task it is likely that the user will simply hit the "restart later" button. This leaves the laptop open to attack by zero hour threats which will then find their way onto the corporate WAN. This approach still exposes the enterprise to breaches of security and productivity losses, with the attendant legal and operational implications.

Fingers Crossed

Unfortunately, the only alternative to the scenario set out above and one that is frequently lived out in response to requests from irate users, is to create exceptions and allow remote users to alter their proxy settings and access the web freely, with no content filtering being applied. This throws the door wide open to inappropriate content, zero hour threats and general productivity issues. It also makes illegal file transfers a good deal easier. This "fingers crossed" approach is fraught with risk but it is the situation in which thousands of IT administrators find themselves every day.

Web Security "in the Cloud" for Off-Network Users

So, how do you improve the web security of off-network users without wasting precious IT resource and budget?

The answer lies in the adoption of web security "in the cloud", also known as Software as a Service (SaaS). SaaS applications are based on a recurring subscription fee and the cost is directly aligned to the number of users. No hardware is required and the SaaS application can be run over an existing internet access infrastructure. All of the usual cost associated with maintaining web security software, such content filters, along with the infrastructure on which it resides, as well as training, security updates, etc. are assumed by the web security SaaS vendor in exchange for a recurring, annual subscription fee.

[5] Software-as-a-Service: A Comprehensive Look at the Total Cost of Ownership of Software Applications, S.I.I.A. September 2006

"SaaS web security allows an enterprise to work smart."

"SaaS web security for the roaming workforce typically leads to a 30-40% reduction in costs from the first year when compared to the equivalent product based solution."

The adoption of SaaS web security for off-network users brings many benefits. Web requests generated by users are filtered in the internet 'cloud' and malware removed before serving clean traffic back to the user. Corporate AUP are enforced for all users regardless of location and management is also simplified because no endpoint updating is required. The experience of the remote worker is also improved because there is no longer any need to backhaul traffic via a VPN. The VPN can be reserved for access to corporate applications and is removed as the single point of failure and latency for internet access. Also, all web traffic flowing to the datacenters is SSL-encrypted leading to improved security over the very public internet.

These benefits allow an enterprise to "work smart" by focusing their energies on activities core to their business. Precious IT resources can concentrate on strategic activities and actually contribute to their organization's bottom line rather than spending large amounts of their time solving problems generated by partial solutions. Service Level Agreements are standard and SaaS web security for off-network users is infinitely scaleable. As the remote workforce increases, the enterprise can do capacity planning and budgeting with confidence.

Drawbacks of SaaS Web Security for Off-Network Users

Given the long list of benefits associated with SaaS web security as a way of securing the virtual network boundary, you'd be forgiven for wondering why every organization on the planet isn't signing up. One objection to SaaS web security adoption for off-network users is the perceived loss of operational control, in particular policy granularity and reporting. Other objections to this approach arise due to the difference in SaaS from the traditional software pricing model and the perceived greater cost over a multi year period.

The perception of reduced operational control is understandable since there are no moving parts within your organization to touch or manage. However, provided you choose the right SaaS web security provider, you will have better scalability, reliability, security and instantaneous enforcement than you will with an on-premise solution. You get more control of your reporting data as well. Reporting data is automatically and continuously aggregated across internal corporate users and off-network users so summary and detailed information on specific user web activity is easy to generate and schedule for future reference.

When it comes to policy setting and reporting, SaaS web security for off-network users is managed via web-based portals, enforcing corporate AUP's for any user anywhere in the world, from anywhere in the world. Policy updates take just a few seconds to become active and does not rely upon the remote client having to download URL and policy database updates. SaaS web security is more flexible and granular than conventional models of web security.

The issue of cost is more complicated. In a typical Total Cost of Ownership ('TCO') analysis, software and hardware costs are easily calculated but the manpower resource associated with them is often underestimated or omitted altogether. However, when this manpower resource is correctly quantified, the SaaS web security route usually becomes the most cost effective option – particularly if an organization has multiple internet gateways. In the vast majority of cases the adoption of SaaS web security for the roaming workforce typically leads to a 30-40% reduction in costs from the first year, when compared to the equivalent product-based solution.

"The Off-Network Protection service is supremely easy to manage."

"SaaS web security is the most cost effective way of delivering the highest level of web security and the best user experience for off-network users."

LEARN MORE

For information about Google Web Security for Enterprise and Off-Network Protection, visit www.google.com/a/help/intl/en/security/web.html

Google Web Security Off-Network Protection

Google Off-Network Protection service extends Google Web Security for Enterprise web malware scanning and web filtering services to an organization's off-network and remote employees.

The service is implemented via a simple configuration change which routes an organization's internet traffic through global datacenters. web malware is blocked and AUP's are enforced in real time. Web malware and other inappropriate content, such as phishing attempts, are blocked before they reach the user and your network. Off-Network Protection allows seamless roaming between different network interfaces, including wired, wireless and 3G. Furthermore, log information is securely in the hands of the administrator, not on a file on a laptop, making business critical data a good deal more secure. This ameliorates compliance with data control regulations, as does the extensive reporting functionality. The client-side of the service is also password protected to prevent unauthorized tampering by end users.

The Off-Network Protection service is supremely easy to manage. Policy changes are active within seconds, globally. There is no need to wait for client software to try to update itself on its own schedule.

Summary and Conclusion

The conclusions reached by this paper are as follows:

- The proportion of the global workforce becoming mobile has, and will continue to increase
- Increased mobility can bring significant business benefits to the enterprise but makes web security even more challenging
- The implications of an organization's AUP being breached by off-network users are severe – doing nothing is not an option
- Conventional methods of mitigating the web security risks posed by a roaming workforce are only partially effective and are expensive and time consuming to implement and manage
- SaaS web security delivers the highest level of web security and the best user experience for off-network users
- Implementation of SaaS web security is the most cost effective way to secure the internet for off-network users for the vast majority of organizations

Google™