

# Roaming Workers

The Weakest Link in Corporate Web Security

---

*A ScanSafe White Paper April 2008*

TABLE OF CONTENTS

	PAGE
TABLE OF CONTENTS	2
1.0 INTRODUCTION	3
2.0 THE MOBILE CHALLENGE	3
3.0 THE IMPLICATIONS OF UNRESTRICTED WEB ACCESS	4
4.0 THE WEAKEST LINK	5
5.0 THE CONVENTIONAL APPROACH	5
6.0 FINGERS CROSSED	6
7.0 SAAS WEB SECURITY FOR ROAMING WORKERS	6
8.0 DRAWBACKS OF SAAS WEB SECURITY FOR ROAMING WORKERS	7
9.0 SCANSAFE ANYWHERE <sup>+</sup>	8
10.0 SUMMARY AND CONCLUSION	9
11.0 ABOUT SCANSAFE	9

## 1.0 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 roaming and remote workforce. It will be seen that there are many potential areas of legal and operational risk which the application of conventional solutions has failed to address. These solutions will be examined. The paper concludes that the SaaS Web Security model has unique features which make it the most secure and cost effective way of delivering productive access to the Internet for remote and roaming workers.

**“How do you improve the Web security of remote workers without wasting precious IT resource and budget?”**

## 2.0 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 do not fill you with confidence then you are not alone. 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<sup>1</sup>, 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 brought into sharp focus.

**“By the end of 2011, IDC expects nearly seventy five percent of the US workforce to be mobile”**

---

<sup>1</sup> IDC Worldwide Mobile Worker 2007-2011 Forecast and Analysis

### 3.0 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 organisations understand that the legal implications of unfiltered Web use could be grave.

The entertainment industry serves as an excellent example of why this is the case. This industry has, over the last few years, taken an increasing aggressive approach to copyright infringement. Notwithstanding popular belief to the contrary, downloading MP3's or films via P2P file-sharing will usually constitute copyright infringement, even if the download is for private use only.

Copyright owners initially concentrated on detecting and suing individual infringers. The International Federation of the Phonographic Industry ('IFPI') has sued over 6,000 individual file sharers in the UK, Austria, Denmark, Germany and Italy for copyright infringement. However, the IFPI has more recently started to take action against organizations rather than individuals, for example by writing to every university in Britain to point out the legal implications of unlicensed Internet copying (i.e. injunctions, damages, costs and possible criminal sanctions). In the United States, the Recording Industry and Association of America ('RIAA') sued an Arizona company because its employees were using the company's resources to distribute copyrighted music. The claim was reportedly settled for \$1 million.

The legal risks are only part of the picture. The impact of unrestricted Web access on compliance with government or industry regulations relating to effective systems and processes for data control could also be severe. Many employees are blissfully unaware, when they are updating their Facebook profile or searching for dancing cats on YouTube, 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 exploits of browser vulnerabilities are increasing and these exploits happen in ever decreasing periods of time. 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 competitive advantage. The brand and credibility of an organization could be seriously compromised. There is some evidence that cyber criminals are now specifically targeting laptop users, encouraged to do so by the finding that corporate laptops hold on average \$525,000 worth of sensitive data.<sup>2</sup>

The problems above are compounded when a compromised laptop is then plugged by its unwitting owner back into the corporate network. Any malware can now spread through the network with ease. This can cause serious productivity losses for both workers unable to access key business applications and the IT team that have to clean up the network – no easy task.

**“Downloading MP3's or films via P2P file-sharing will usually constitute copyright infringement, even if the download is for private use only. “**

---

<sup>2</sup> iBahn, October 2007

## 4.0 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 roaming workers 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 a roaming workers laptop use within the last twelve months.<sup>3</sup> Why?

The fact that roaming workers 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.<sup>4</sup> 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. However, perhaps the most alarming finding of this particular study was the fact that illegal file sharing Websites are requested 8.5 times more often than they would be by the same user whilst in the office. This is not just a drain on productivity. It places a significant strain on network resource and the wider implications should worry any CIO.

**“Sixty five percent of respondents to a survey 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 a roaming worker than they are when that worker is in the office”**

## 5.0 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 could 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. 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. If a server rather than a dedicated gateway appliance is used as a

**“The annual costs of owning and managing software applications can be up to four times the cost of the initial purchase”**

<sup>3</sup> ScanSafe Roaming Security Survey January 2008

<sup>4</sup> ScanSafe Analysis April 2008

platform for content filtering and/or malware detection, the organization faces the challenge of keeping the operating system patched and up to date as well as the security products themselves. Often, the responsibility rests with the end user in terms of 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 are likely, one way or another, to find their way onto the corporate WAN. In summary, this approach still exposes the enterprise to breaches of security and productivity losses, with the attendant legal and operational implications.

### 6.0 FINGERS CROSSED

**“The fingers crossed approach is fraught with risk “**

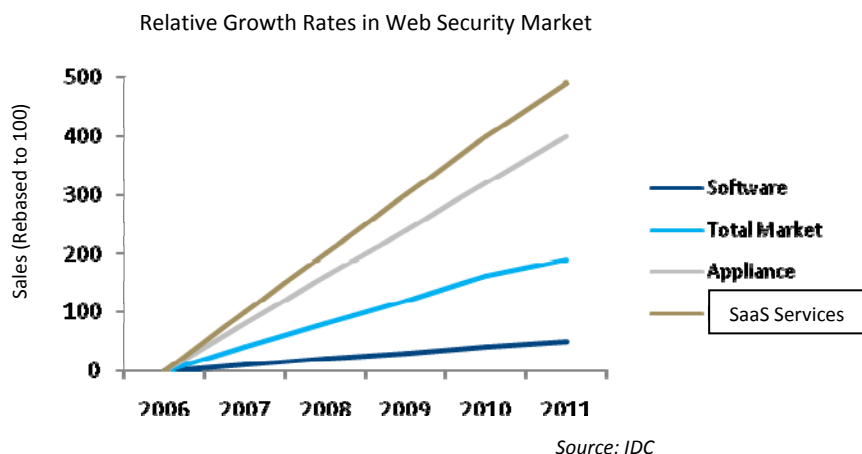
Unfortunately, the only alternative to the scenario set out above and one that is frequently lived out in response to requests from irate users is to create exceptions and allow remote users to alter their proxy settings and access the Web freely, with no content filtering being applied. This throws 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.

### 7.0 SaaS WEB SECURITY FOR ROAMING WORKERS

**“SaaS Web Security allows an enterprise to work smart”**

So, how do you improve the Web security of remote workers without wasting precious IT resource and budget?

The answer may lie in the adoption of Software-as-a-Service (‘SaaS’) Web Security. 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, training, security updates etc. are assumed by the Web SaaS Security vendor in exchange for a recurring, usually annual subscription fee.



The adoption of SaaS Web Security for roaming workers brings many benefits. Web requests generated by remote users are filtered in the Internet ‘cloud’ and malware removed before serving clean traffic back to the user. Corporate AUP can be applied to 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 and the fact that the VPN is removed as the single point of failure 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 resource can concentrate on strategic activities and actually contribute to their organizations bottom line rather than spending large amounts of their time solving problems generated by several products which together only deliver a partial solution. Service Level Agreements are standard and SaaS Web Security for roaming workers is infinitely scalable. As the remote workforce increases the enterprise can capacity plan and budget with confidence.

## 8.0 DRAWBACKS OF SAAS WEB SECURITY FOR ROAMING WORKERS

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 remote users is the perceived loss of operational control, in particular policy granularity and reporting. There are also concerns around the storage of sensitive and business critical data. 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 fairly easy to counter. Provided you choose the right SaaS Web Security provider, confidential data is at least as safe as it would be in the hands of the owners – if not considerably safer. Reporting data is automatically and continuously aggregated across internal corporate users and roaming 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 mobile workers is managed via Web based portals, allowing application of corporate AUP’s to any user anywhere in the

**“SaaS Web Security for the remote workforce typically leads to a 30-40% reduction in costs from the first year when compared to the equivalent product based solution. “**

world, from anywhere in the world. It is, arguably, a good deal more flexible and granular than conventional models of Web security.

The issue of cost is more complicated. Software and hardware costs are fairly straightforward but the manpower resource associated with them is often underestimated or omitted altogether when undertaking a Total Cost of Ownership ('TCO') analysis. 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 remote workforce typically leads to a 30-40% reduction in costs from the first year when compared to the equivalent product based solution.

### 9.0 SCANSAFE ANYWHERE<sup>+</sup>

**“The Anywhere<sup>+</sup> service is supremely easy to manage”**

The global leader in SaaS Web Security is ScanSafe, and their Anywhere<sup>+</sup> service is the world's first SaaS Web Security for the mobile workforce. The Anywhere<sup>+</sup> service extends ScanSafe's award-winning Web malware scanning and Web filtering services to an organisations roaming and remote employees.

The service is implemented via a simple configuration change which routes an organization's Internet traffic through the ScanSafe global datacenters which are located throughout Europe, the U.S. and Asia. Web traffic is scanned in real time, allowing AUP enforcement and blocking Web malware and other inappropriate content such as phishing attempts before they reach the user and your network. Anywhere<sup>+</sup> 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 which makes business critical data a good deal more secure. This ameliorates compliance with data control regulations as does the excellent reporting functionality. The client-side of the service is also password protected to prevent unauthorized tampering by end users.

The Anywhere<sup>+</sup> service is supremely easy to manage. Policy changes can be implemented immediately because there is no need to wait for client software to try to update itself on its own schedule. Policy changes are active within seconds, globally.

## 10.0 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 the AUP of an organization being breached by remote and roaming workers are severe – doing nothing is not be 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 remote workers
- Implementation of SaaS Web Security is the most cost effective way to secure the Internet for roaming workers for the vast majority of organizations

**“SaaS Web Security is the most cost effective way of delivering the highest level of Web security and the best user experience for remote workers”**

## 11.0 ABOUT SCANSAFE

ScanSafe is the largest global provider of Web Security-as-a-Service, ensuring a safe and productive Internet environment for businesses. ScanSafe solutions keep viruses and spyware off corporate networks and allow businesses to control and secure the use of the Web and instant messaging. As a SaaS solution, ScanSafe’s services require no hardware, upfront capital costs or maintenance and provide unparalleled real-time threat protection. Powered by its proactive, multilayered Outbreak Intelligence™ threat detection technology, ScanSafe scans more than 20 billion Web requests and blocks 200 million threats each month for customers in over 80 countries.

With offices in London and San Francisco, California, ScanSafe is privately owned and financed by Benchmark Capital and Scale Venture Partners. The company received the CNET UK Business and Technology award for Security Product of the Year 2008, a 2007 CODiE award for Best Software as a Service Solution, the 2008 and 2007 SC Magazine Europe Award for Best Content Security Solution and was named one of Red Herring’s Top 100 Technology companies. For more information, visit [www.scansafe.com](http://www.scansafe.com).

## ROAMING WORKERS – THE WEAKEST LINK IN CORPORATE WEB SECURITY

### Contact ScanSafe

ScanSafe US  
185 Berry Street  
San Francisco, CA 94107

T: 415 692 2000  
F: 415 536 5949  
E: [info@scansafe.com](mailto:info@scansafe.com)

### ScanSafe EMEA

The Connection, 198 High Holborn  
London WC1V 7BD

T: 020 7959 0630  
F: 020 7959 0631  
E: [info@scansafe.com](mailto:info@scansafe.com)

### About ScanSafe

Founded in 1999, ScanSafe is the leading global provider of Web Security-as-a-Service, ensuring a safe and productive Internet environment for businesses. As a SaaS solution, ScanSafe's services require no hardware, upfront capital costs or maintenance and provide unparalleled real-time threat protection. Powered by its proactive, multilayered Outbreak Intelligence™ threat detection technology, ScanSafe scans more than 20 billion Web requests and blocks 200 million threats each month for customers in over 80 countries.

For more information visit [www.scansafe.com](http://www.scansafe.com)