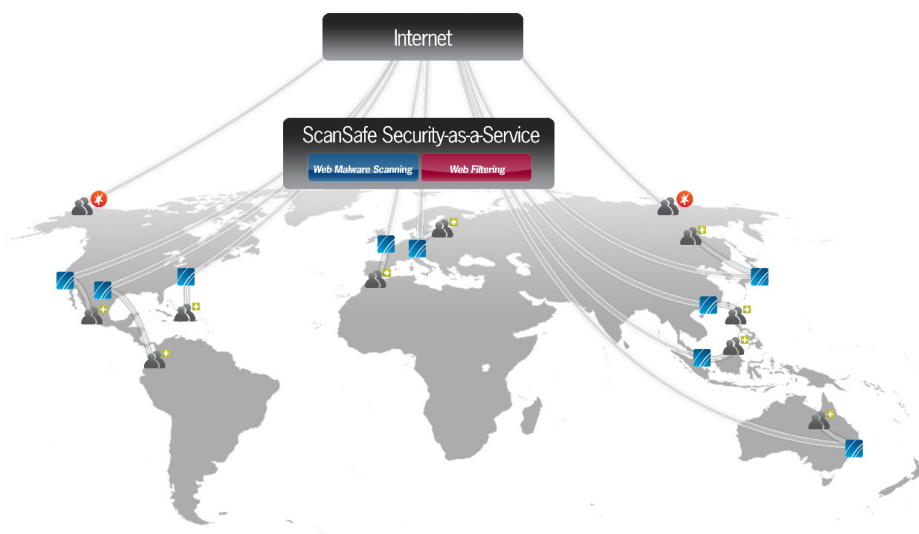


# ScanSafe Anywhere<sup>+</sup>

The number of employees who work outside the traditional office is rapidly increasing and perhaps surprisingly now constitutes the majority of workers for many businesses. A 2008 IDC study on mobile workers estimated that 75 percent of the U.S. workforce will be mobile by the end of 2011<sup>†</sup>. This trend, coupled with the need for 'always-on' connectivity, means that the network boundary is now 'elastic' and the traditional fixed network perimeter is becoming irrelevant.

Roaming employees now connect to the Internet from a variety of locations – from their homes and client offices to airport lounges and hotel hotspots. This increased level of connectivity allows employees to work regardless of location. The clear benefits of employees working outside the office do, however, come with increased risks due to lower levels of security. As a result, cyber criminals are now increasingly using malware to target laptop users in order to gain access to private and confidential information that can be sold, in many cases, for a huge profit. Research shows that laptop computers with business information store an average of \$525,000 worth of sensitive data. This problem is magnified when machines that are infected while remote will then spread that malware throughout the network when the employee returns to the office – drastically increasing the volume of private data that can be stolen.



Traditionally, IT administrators have little or no control over Web content accessed by roaming employees. This situation is not helped by the fact that roaming employees are five times more likely to access inappropriate content on the road than in the office. Even more worrying is that roaming employees only use VPNs 17% of their browsing time. How are they controlled and protected the other 83% of the time?

Legacy solutions to these problems include extending Web security software and appliances out to endpoints through client agents and forcing all Web traffic back through the on-premise solution. This increases cost and management overheads and can require backhauling, which results in latency and increased bandwidth costs.

## Why Anywhere<sup>+</sup>?

- Enable security policy to be enforced enterprise-wide, including remote workers
- Protect resources from undesirable and malicious Web content
- Improve productivity by limiting time spent on recreational surfing
- Centralized reporting for all users regardless of location

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

“Laptop computers with business information store a staggering average of \$525,000 worth of sensitive data that is proving to be a highly attractive lure to Web malware writers.”

<sup>†</sup>Source: IDC, Worldwide mobile worker population, 2007 – 2011 forecast, Doc # 209813, December 2007

## Security Perimeter Anywhere You Want It To Be

Anywhere+ extends the real-time protection and policy enforcement of ScanSafe Web Security to roaming employees. With Anywhere+ it is finally possible to protect roaming employees wherever they are working and however they access the Internet.

Anywhere+ is delivered as a service for complete security, reduced complexity and simplified user management. Anywhere+ removes the performance issues and bandwidth congestion associated with backhauling Web traffic over the corporate VPN, so the security perimeter is now anywhere you want it to be.

## Real-time Malware Scanning and Policy Enforcement

Anywhere+ ensures that roaming and remote employees no longer act as an open bridge into the internal network by stopping all Web threats in the cloud wherever the user is working.

All Web traffic, including SSL encrypted communications flow to the ScanSafe datacenters for real-time scanning to detect inappropriate or malicious content. This is done using encryption, leading to improved security over public networks. With Anywhere+, log information is securely in the hands of IT, not on a file on the local PC. Reporting data is automatically and continuously aggregated across internal corporate users and roaming users. Policy changes can be implemented immediately – no need to wait for client software to try to update itself on its own schedule. Policy changes are active within seconds, globally.

## Prevent Confidential Data Loss

Coupled with granular inbound web policy, Anywhere+ enables an integrated outbound policy to help prevent leaks of confidential or personal data to the Web, which in turn limits the potential exposure to bad press, lawsuits and financial penalties. This policy can be constructed around multiple factors including preconfigured filters for social security numbers etc, file type, file matches, keywords and regular expressions.

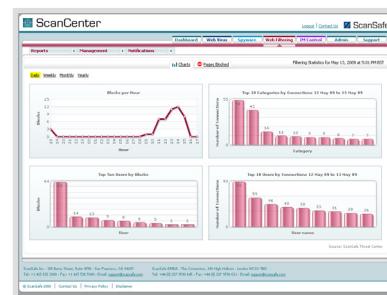
## Transparent Operation and Silent Install

Anywhere+ is deployed through a lightweight driver which forwards Web traffic to the ScanSafe security scanning infrastructure. ScanSafe datacenters are located all over the world from San Francisco to Sydney ensuring that end-users always have optimized performance as well as award-winning security and filtering. Anywhere+ supports a silent installation and is easily deployed using industry standard mechanisms such as GPO or Microsoft SMS.

### About ScanSafe

ScanSafe is the pioneer and largest global provider of SaaS Web Security, ensuring a safe and productive Internet environment for businesses. ScanSafe solutions keep malware off corporate networks and allow businesses to control and secure the use of the Web. As a SaaS solution, ScanSafe eliminates the burden of purchasing and maintaining infrastructure in-house, significantly lowering the total cost of ownership. Powered by its proactive, multilayered Outbreak Intelligence™ threat detection technology, ScanSafe processes billions of Web requests and millions of blocks each month for customers in over 100 countries.

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



Feature	Benefits
Extension of security policy for remote users	Consistent security for all users, regardless of location
Secure traffic without requiring backhaul over VPN	Increase security while eliminating costs and headaches associated with backhauling traffic
Automatically selects optimal data center	Ensure high-performance Web experience
Deployed as a tamper-proof driver	Prevent users circumventing the solution
Centralized, real-time policy control	Control organization as a whole, policy changes enabled in real-time

US: ScanSafe - 185 Berry Street, Suite 4700, San Francisco, CA 94107  
 Tel: +1 415 692 2000 Fax: +1 415 536 5949 Email: [ussales@scansafe.com](mailto:ussales@scansafe.com)

EMEA: ScanSafe - Qube, 90 Whitfield Street, London, W1T 4EZ  
 Tel: +44 (0) 20 7034 9300 Fax: +44 (0) 20 7034 9301 Email: [emeasales@scansafe.com](mailto:emeasales@scansafe.com)

