

PRODUCT DATA SHEET

Secure Mobility for ScanSafe

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 2009 IDC study on mobile workers estimated that more than 75 percent of the U.S. workforce will be mobile by the end of 2013[†]. This trend, coupled with the need for 'always-on' connectivity, means that the network is becoming borderless.

Roaming employees now connect to the Internet from a variety of locations – from 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. 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. Legacy solutions are invasive and easily circumvented, requiring users to activate VPN connectivity in order to control the traffic and enable security.



Borderless Control

The real-time protection and policy enforcement of ScanSafe Web Security can easily be extended to roaming employees wherever and however they access the Internet with the Cisco AnyConnect Secure Mobility client. Security and policy are enforced even when mobile devices are accessing the Internet without using VPN.

By allowing mobile users to utilize the local Internet connection while still enforcing security and policy, Secure Mobility for ScanSafe enables the security perimeter to be anywhere you want it to be.

[†] Source: IDC, Worldwide Mobile Worker Population, 2009 – 2013 Forecast, Doc # 221309, December 2009

Why Secure Mobility?

- 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

“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.”

Real-time Malware Scanning and Policy Enforcement

Ensure 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 flows directly to the ScanSafe datacenters for real-time scanning to detect inappropriate or malicious content and all communication between an endpoint and the ScanSafe data center is encrypted to ensure no snooping of data over public networks.

Using the ScanSafe service all reporting and policy controls are centralized, so as well as enforcing policy for roaming users, administrators can also report on their activity in real-time. Any policy changes can be rolled out globally in under one minute, ensuring immediate control over all users including those who are not within the confines of an office.

Prevent Confidential Data Loss

As well as offering granular inbound web policy, ScanSafe Web Security 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. Policy can be constructed around multiple factors including dictionaries, preconfigured IDs and regular expressions.

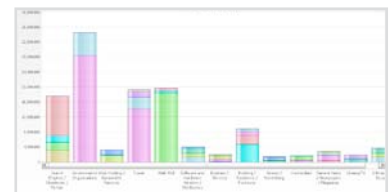
Transparent Operation

With Secure Mobility for ScanSafe web security is always-on ensuring that secure web connectivity is transparent to the end user - all web traffic is automatically forwarded to the ScanSafe data centers. 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.

About ScanSafe

ScanSafe is the pioneer and largest global provider of cloud 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 cloud 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



ScanSafe US - 950 Elm Avenue, San Bruno, CA 94066 Tel: +1 650 989 7100 Fax: +1 650 989 6543 Email: ussales@scansafe.com

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



ScanSafe is now part of Cisco.

