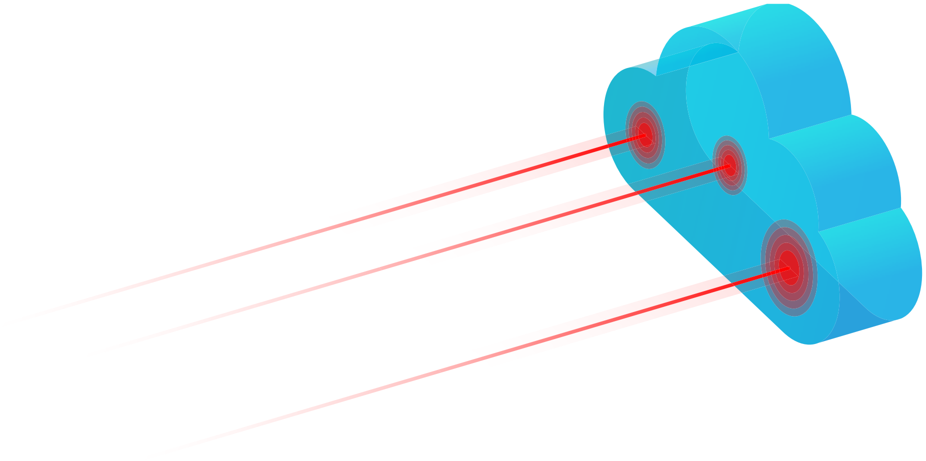
SOPHOS
Security made simple.



Protecting Your Roaming Workforce With Cloud-Based Security

How to use the cloud to secure endpoints beyond your perimeter

By **Tsailing Merrem**, Senior Product Marketing Manager

Remote and roaming workers are constantly checking email, downloading data, and staying productive. Results are their top priority—security is not. IT organizations need to keep up with these high-performers to update their security software and scan their systems for viruses without reducing their productivity.

So how can you empower remote and roaming employees with the tools they need, while still protecting your computing resources and proprietary data—without busting the budget or hiring an army of security specialists? This paper looks at the security challenges posed by employees working beyond the company's secure perimeter, and proposes a transition to a cloud-based security service.

The borderless work environment

Not long ago, securing computing resources was simple and straightforward: build a solid network perimeter with a strong firewall, add host intrusion prevention, and authenticate everyone who enters. Now, companies are reaping the benefits of an increasingly mobile workforce operating outside the network perimeter. According to Forrester Research, these high-risk mobile workers create the most value for your company.[1]

In today's anytime, anywhere, any-device work environment, the new perimeter is the security software on employee laptops. Some of this software is difficult to update while the users are outside the office, requiring VPN connections for access and large update files that can slow down an already spotty connection.

Five security risks of a roaming workforce—and tips to resolve them

Risk 1: Out-of-date software and policy

One common complain among traveling employees is that their security software and policy slips out of date while they work away from the office. When they return, their non-compliant systems are blocked from accessing the network, and all productive activity grinds to a halt while their computers download security updates and apply the latest policy.

The old "layered security" approach that combined network security with local device configuration and security software maintenance simply won't work going forward. Effective protection requires a way to automate security policy configuration, threat updates and enforcement for laptops that spend more time outside of the network than inside—whether they are connected in airports, hotels, coffee shops, remote offices, or employees' homes.

Tip: Choose a cloud-based security subscription service that allows security software and policy updates anywhere without slowing down users.

Risk 2: Personal browsing on company computers

Most employees are well-intentioned and security-conscious, but as the lines between work life and personal life continue to blur, it's understandable that they use work systems for personal tasks. Personal browsing and social media use creates insidious new social engineering opportunities, which cybercriminals are only too happy to exploit.

Facebook, LinkedIn, Twitter and other social networking sites make it easy for employees to

[1] The State Of Workforce Technology Adoption: Global Benchmark, 2012, Forrester Research Inc.

connect with friends, family and peers. Unfortunately, unsuspecting friends and co-workers may click on malicious links they believe to be from trusted acquaintances. Companies with rigid polices banning these sites report only marginal success as many employees either ignore the policies or find ways around them. A more pragmatic solution is to block web threats using an effective web-filtering solution.

Tip: Take advantage of security software web filtering capabilities that block malicious and web-borne threats before they reach the computer.

Risk 3: Exposing sensitive data

Securing proprietary data should be another major priority. Customer lists, account numbers, marketing and business plans, and other sensitive data likely reside on employee notebooks. What happens to that sensitive data if a laptop is lost or stolen? An easy-to-manage encryption solution is a good way to keep data safe for remote and mobile systems.

Tip: To protect data and ensure compliance, be sure that PC security solutions encrypt data on multiple PC and notebook platforms.

Risk 4: Mobile workers in charge of their own security

Making end users responsible for security is like putting the marketing team in charge of building maintenance or the sales organization in charge of accounting. Security is not the average employee's top priority or core competency. Many struggle with technology and most are very unlikely to install, configure, update, and properly use security software. Even if mobile employees could and would perform security tasks, who wants them spending time securing systems rather than doing their jobs?

Tip: Security must be transparent to users without requiring user interaction or expertise.

Risk 5: Unsecure storage devices

USB devices often contain sufficient storage space to easily accommodate massive amounts of data. They are produced for consumer use, lack inherent security, may be difficult to manage, and are easily misplaced. Industries with high compliance requirements such as healthcare, insurance and financial services may restrict the use of such devices. Even if industry standards don't apply, utilization policies and monitoring may be advisable.

Tip: Monitor USB device usage across the business, and deploy a realistic device control policy.

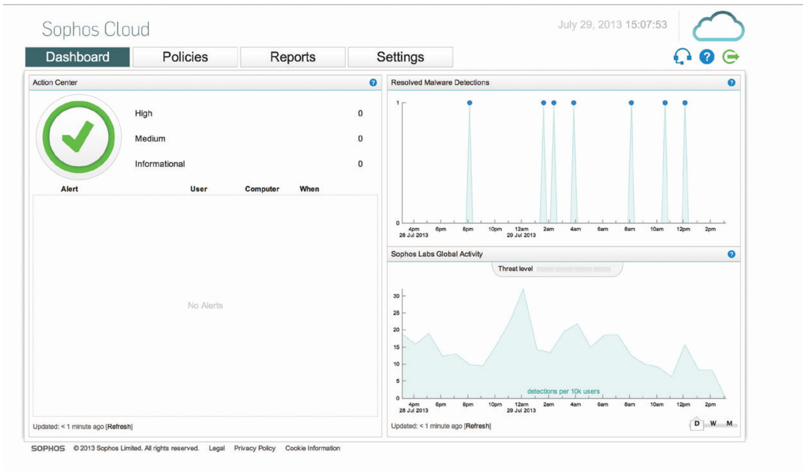
Why the cloud is the perfect fit for today's businesses

Cloud security solutions are transparent for users and simple for administrators. They protect data and endpoints by focusing on individual users, with policies that follow them across systems—wherever they go. With Sophos Cloud, security becomes far easier to use, deploy and manage with one convenient, cloud-based management console that's available from any computer with a browser. Upgrades are automatic, coverage is everywhere, and Sophos Cloud doesn't require complicated server setup or infrastructure maintenance. This simple, pay-as-you-grow, subscription-based service is a cost-effective way to protect your business.

Secure endpoint access everywhere

Most remote and mobile employees already use the cloud. Sophos Cloud helps them use it safely. It delivers comprehensive, cloud-based protection as a service that includes state-of-the-art antivirus protection with advanced malware detection techniques and the latest host intrusion prevention system. This Sophos-hosted service delivers award-winning security and performance that:

- Protects users from infected websites
- Keeps mobile endpoints up to date with Live Protection
- Prevents the use of unwanted removable storage devices such as USB thumb drives, external drives, and more
- Protects Windows-based servers, PCs, notebooks, and Apple desktops and laptops from threats



Sophos Cloud

July 29, 2013 15:07:53

High 0

Medium 0

Informational 0

Alert	User	Computer	When

No Alerts

Updated: < 1 minute ago [Refresh]

Updated: < 1 minute ago [Refresh]

SOPHOS © 2013 Sophos Limited. All rights reserved. Legal Privacy Policy Cookie Information

Figure 1: Sophos Cloud provides reports on all protected devices, computers, and users, viewable by user, by computer, or by device.

Data protection everywhere

Encryption managed by Sophos Cloud provides secure access to confidential data without requiring users to even think about encryption. This cloud-based encryption management solution helps control unwanted removable storage devices like USB sticks, external drives, and more. In addition, it allows users to:

- Effortlessly encrypt data on mobile computers and desktops
- Safely and easily share encrypted files with co-workers and business partners
- Enforce data loss prevention policies across email and mobile endpoints

Protect mobile users without getting in the way

Ask effective managers their secret to success and you'll often get this response: Give employees what they need to be successful without getting in their way. Sophos takes this approach to securing your remote and roaming employees. It's what we call Security Made Simple. Our award-winning products install easily, configure with a few common-sense clicks, and automatically protect you from the latest threats.

Sophos Cloud is designed to be a comprehensive, cloud-based security platform from a company known for making security technologies simple to administer and use. The company's award-winning mobile device management and other services will soon be available via this powerful cloud management console. As modules become available, they can be instantly deployed and efficiently managed for cohesive and integrated security.

Industry experts agree: Sophos offers the best protection

IT analyst firm Gartner Research named Sophos as a leader in three separate Magic Quadrant reports: July 2013 for Unified Threat Management, January 2013 for Endpoint Protection, and September 2012 for Mobile Data Protection. Sophos is the only company to be named a leader in all of these reports.

Sophos scores highest among 20 vendors' antivirus offerings by AV-Comparatives, May 2013

For a complete list of awards and reviews, visit: http://www.sophos.com/en-us/company/press

More than 100 million users in 150 countries rely on Sophos as the best protection against complex threats and data loss. Sophos is committed to providing complete security solutions that are simple to deploy, manage, and use that deliver the industry's lowest total cost of ownership. Sophos offers award winning encryption, endpoint security, web, email, mobile, server and network security backed by SophosLabs—a global network of threat intelligence centers. Read more at www.sophos.com/products.

Sophos Cloud

Get a free trial at sophos.com

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA