Distributed Workforce Management in the Cloud:

Spreading IT Security Wherever Employees Roam

Symantec.cloud.

Distributed Workforce Management in the Cloud:

Spreading IT Security Wherever Employees Roam

Contents

Introduction

The ever-increasing availability of faster, wireless network access, wirelessly enabled laptops and other devices, and collaboration tools such as Instant Messaging (IM) are turning the traditional office into an un-tethered workspace that can happen just about anywhere, any time. But all this poses new challenges for IT departments who must monitor and secure the online interactions of these highly distributed and roaming workers.

Remote workers such as teleworkers and employees at remote offices often are "always on," surfing the Net, communicating with colleagues and others, accessing data and applications critical to the business—much of which happens outside of the protections available through the corporate network or VPN. Meanwhile, employees that are highly mobile tend to migrate over numerous network environments and geographic locations, thus increasing opportunities for exposure.

All this makes it more difficult for IT to consistently enforce policies, ensure laptops and other endpoints are protected with the most current security mechanisms and malware protections, and safeguard electronic interactions. To address this complexity, a growing number of companies are opting to call on security experts who can, via hosted or cloud-based solutions, help organizations more efficiently and effectively manage and protect their distributed workforce. The benefits of this approach are numerous: reduced capital investments and operating costs, simplified IT, and the ability to streamline and improve secure information exchange among distributed employees. Cloud-based solutions also can protect much more than just the device by securing and managing the remote workers' movements as they traverse the Internet, access email, send and receive IMs and more.

More Users Are Working Outside of the Traditional Office

It is estimated that the worldwide mobile worker population will have grown from 919.4 million in 2008 (accounting for 29% of the worldwide workforce), to 1.19 billion in 2013, accounting for 34.9% of the workforce.[1] Even among workers who do not consider themselves to be road warriors, market research firm Gartner estimates that today, 45% of workers in the United States are out of the traditional office a minimum of eight hours per week. Adding further proof that the mobility trend is a global phenomenon, analysts at IDC report that the largest number of mobile workers today is found in the Asia-Pacific region. In Western Europe, half of the workforce is considered to be mobile.[2]

Workers today are as likely to do their jobs on their own laptops as they are to labor away on mobile equipment issued by their employers. Regardless of who pays for the equipment, workers at organizations of all sizes are texting, emailing, downloading corporate documents, accessing portals, even surfing the Web to research clients or competitors while on the road, at home, at customer sites, in hotels, on airplanes, or at nearby coffee shops.

The benefits of such an un-tethered workforce are many. Employee productivity ranks high as a desired outcome, allowing workers to do what they have to do from wherever they happen—or need—to be. The evolving distributed workspace means an increasing number of employees have neither a company-provided physical office nor a desk, and their work is increasingly happening 24 hours a day, 7 days a week.[3] Contrary to an assumption that this is turning society into a population of obsessive and stressed out wage-slaves, a growing number of studies suggest that the ability to be

productive nearly everywhere is actually providing more flexibility to address the quality of work and life balance issues. Consider this paradox: a 2009 survey of 100,000 workers conducted by Kelly Services (a workforce service provider) found that 76 percent of respondents feel that the ability to work outside the office, yet remain in constant contact, has been a positive development, even though almost a third are now working longer hours.[4]

Employees today also are leveraging more sophisticated collaboration tools, such as IM, that promise instant communication and knowledge sharing. Collaboration tools, including IM, are vital to ensuring that regular and ongoing communication occurs between employees. While IM has yet to make the inroads that email and telephone have long enjoyed, Forrester Research says the numbers of "instant messaging junkies" are growing among telecommuting information workers, adding that it is time to make this key collaboration tool a corporate priority."[5]

While the flexibility provides undisputed opportunities to enhance productivity, the fact remains that distributed workers do need secure, managed and dependable access to the applications and data necessary to do their jobs, regardless of their location, various workspaces and increased autonomy.

The Challenge for IT Departments

Many experts observe that IT organizations need to plan for increasingly chaotic environments that are no longer in their direct control.[6] IT managers must keep pace with the constant demand for information, make sure that acceptable use and security policies are applied, and determine how to best manage remote systems, users and data/content.

Remote users of electronic communications are susceptible to the same types of information security threats—from malware surreptitiously infecting a computer, to spam email clogging an inbox, or malicious websites unwittingly visited—as users sitting inside an organization's four walls or working within the corporate network.

But it is inherently more difficult to manage and monitor the activity of remote workers, and the devices they use. Typically, remote workers and their laptops are not physically attached to the corporate network, making it more difficult to gain visibility into their systems' status. Remote, more autonomous workers also can make acceptable use policies more difficult to apply and enforce.

Often, organizations don't have the technical expertise or resources to institute and maintain the necessary endpoint protection on the equipment used by remote workers or to regularly and accurately scan devices for active infections. They cannot easily assess the health of these systems and determine whether protection levels are current, nor can they continually secure all of the myriad Internet sites employees visit, the URLs they click on, the emails and IMs they receive and send, or the executable files and other downloads they activate while working outside of the corporate network.

To mitigate risks and ensure remote workers are protected yet able to access the data and resources when and where they need them, IT departments need to:

1. Protect the laptops used by employees to ensure these endpoints are regularly and accurately scanned for active infections, and that they have adequate and up-to-date security levels.

4-Kelly Global Workforce Index, 2009
5-US Telecommuting Forecast, 2009 To 2016, Forrester, March 11, 2009
6-Watchlist: "Continuing Changes in the Nature of Work, 2010-2020" 30 March 2010. G00174602

2. Protect the electronic interactions of the distributed workforce, including email, Web communications and IM, that occur anywhere and at any time.

3. Ensure that company assets are being used properly and that acceptable use policies are being implemented correctly. By blocking inappropriate content, excessive downloads, inappropriate surfing, risky websites, etc., remote workers will be more productive and their devices and interactions will be better protected.

4. Ensure that the interactions of roaming users are secure, regardless of whether they are accessing corporate resources from Wi-Fi hotspots, their homes, or anywhere else.

Cloud-Based Management Ideal for Mobile Workers

The growth of a distributed workforce is driving the need for cloud-based information assurance models that no longer solely depend on implementing internal infrastructure-based security controls. According to Forrester, telecommuting is accelerating the transition to cloud-based computing solutions, which work well for highly distributed organizations. This computing delivery model makes it very easy to deploy messaging security services by simply redirecting email, Web, and IM traffic through the service provider. And, in many cases it facilitates deploying agent-based technologies to remote workers over the Internet rather than via traditional machine-by-machine, on-premise installation techniques. Employees everywhere can access the same cloud service, which is managed and operated centrally.[7]

Cloud solutions can also take the pressure off organizations to maintain large numbers of specialized, in-house staff with skills necessary to manage and secure their distributed workforce. Now these resources can be redeployed to take on other business critical projects. Cloud-based services offer a lower total cost of ownership (TCO) than solutions installed and run in-house, and they can watch for and stop threats before they ever infiltrate a corporate network and wreak havoc.

With cloud-based services for security and management, organizations don't have to restrict how, where and when their employees can take advantage of working remotely. Symantec MessageLabs Web Security.cloud service, for example, provides roaming and remote worker support options to help address these challenges. The service scans all Web content, promoting enhanced accuracy above services that rely solely on URL filtering for threat detection.

Threat intelligence is shared across email, Web and IM for converged threat detection. A roaming agent support option is available that detects a user's geographic location and network changes for optimal service performance. Administrators have at their disposal flexible quota management tools so they can set limits for browse time and bandwidth consumption, and the service features strong URL categorization allowing for more granular policies.

Not all hosted and cloud-based services are alike though. Before adopting this computing model to serve a distributed, mobile workforce, IT departments need to understand and believe in the efficacy of cloud-based services. More importantly, they need to have high expectations of the providers' service level agreements (SLAs), because at the end of the day, the service must be available, accurate and efficient.

7-US Telecommuting Forecast, 2009 To 2016, Forrester, March 11, 2009

Symantec.cloud

Symantec.cloud offers a comprehensive security and management solution for a distributed workforce. The solution is comprised of a variety of components, including Endpoint Protection.cloud, Web Security.cloud, Email Security.cloud and Instant Messaging Security.cloud. Using the power of cloud computing to provide essential protection, Symantec.cloud virtually eliminates the need to manage hardware and software on site. The solution offers one of the most aggressive and comprehensive service level agreements (SLA) in the industry – and Symantec.cloud measures and publishes its SLA results each month.

Symantec.cloud helps IT managers protect the Web, email, and IM interactions of employees that are part of a distributed workforce. It helps organizations consistently develop, apply and enforce acceptable usage policies[8] for all workers, including those working from various locations. Because the service is delivered in the cloud—outside of an organization's network—threats that may exist in email, the Web, and IMs are addressed before they ever enter an organization's network. Management for the distributed workforce is facilitated through the service as well; security and other services can be provisioned and updated to remote, distributed workers over the Internet. All workers can be maintained via a Web-based portal hosted by Symantec.cloud.

In addition, the Web Security.cloud service is optimized to offer protection for workers logging on to WiFi hotspots and restricted access points while maintaining Web filtering policies at all times. And, the Endpoint Protection.cloud service provides an additional layer of security maintaining current protection levels and security policies for workers' laptops—even when they are outside the corporate network.

The Symantec.cloud solutions optimized for a distributed workforce include:

- **Endpoint Protection.cloud**

  The cloud-based solution helps protect an organization's endpoint systems (Windows-based desktops, laptops, and file servers) with advanced technologies for antivirus, antispyware, firewall, and host intrusion prevention, all managed from a single Web-based management console. Security updates are automatic and seamless, so protection of employees' laptops is current whether in the office or on the road.

- **Web Security.cloud**

  This solution blocks Web-borne virus, spyware and phishing threats and controls Web traffic through cloud-based URL filtering. Support for roaming users extends protection and policy enforcement to employees who access the Internet from outside the corporate network.

- **Email Security.cloud**

  The service combines advanced email antivirus, antispam, and content filtering capabilities in an easy-to-manage solution that requires no on-site hardware or software. The email security service supports all mobile devices that send/receive email through corporate exchange servers associated with the service. This means that as long as the end user's email traffic is routed through an associated corporate exchange server, clean email will be delivered to and from the handheld device.

8-Not Just Words: Enforce Your Email and Web Acceptable Usage Policies, MessageLabs, 2008

- **Instant Messaging Security.cloud**

  The service provides security and control for businesses using public IM clients by applying antivirus, URL filtering, content control and logging services to all instant messaging traffic.

Conclusion

Cloud-based services, such as Symantec.cloud's solutions, are particularly appealing for managing an organization's evolving and growing distributed workforce. Organizations do not need to be hindered by their lack of resources to implement and manage these remote workers because Symantec.cloud provides comprehensive, reliable coverage for email, Web and IM but doesn't require expensive on-premise equipment, complex management or extensive expertise.

Using services with automated capabilities to enforce end-user policies can help gain the confidence of customers and business partners. Endpoint Protection.cloud on laptops means regular, accurate scanning of devices for active infections. Regular and real-time monitoring, as well as acceptable usage policies that are more easily applied and enforced, means organizations will be protected from threats lurking in the various Internet sites employees visit, the URLs they click on, the emails and IMs they receive and send, or executables and other downloads they activate while working from remote locations.

More Information

AMERICAS

UNITED STATES
512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Toll-free +1 866 460 0000

CANADA
170 University Avenue
Toronto, ON M5H 3B3
Canada
Toll-free :1 866 460 0000

EUROPE

HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
Tel +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone 0800 917 7733

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Tel +44 (0) 203 009 6500
Fax +44 (0) 203 009 6552
Support +44 (0) 1452 627 766

NETHERLANDS
WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801

BELGIUM/LUXEMBOURG
Symantec Belgium
Astrid Business Center
Is. Meyskensstraat 224
1780 Wemmel,
Belgium
Tel: +32 2 531 11 40
Fax: +32 531 11 41

DACH
Humboldtstrasse 6
Gewerbegebiet Dornach
85609 Aschheim
Deutschland
Tel +49 (0) 89 94320 120
Support :+44 (0)870 850 3014

NORDICS
St. Kongensgade 128
1264 Copenhagen K
Danmark
Tel +45 33 32 37 18
Fax +45 33 32 37 06
Support +44 (0)870 850 3014

ASIA PACIFIC

HONG KONG
Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: + 852 6902 1130

AUSTRALIA
Level 13
207 Kent Street,
Sydney NSW 2000
Main: +61 2 8220 7000
Fax: +61 2 8220 7075
Support: 1 800 088 099

SINGAPORE
6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: 800 120 4415

JAPAN
Akasaka Intercity
1-11-44 Akasaka
Minato-ku, Tokyo 107-0052
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: + 852 6902 1130

About Symantec.cloud

More than 31,000 organizations ranging from small businesses to the Fortune 500 across 100 countries use Symantec.cloud to administer, monitor, and protect their information resources more effectively. Organizations can choose from 14 pre-integrated applications to help secure and manage their business even as new technologies and devices are introduced and traditional boundaries of the workplace disappear. Services are delivered on a highly scalable, reliable and energy-efficient global infrastructure built on fourteen datacenters around the globe. A division within Symantec Corporation, Symantec.cloud offers customers the ability to work more productively in a connected world.

For specific country offices and contact numbers, please visit our website.

Symantec.cloud North America
512 7th Ave.
6th Floor
New York, NY 10018 USA
1 (646) 519 8100
1 (866) 460 0000
www.MessageLabs.com