EMPOWERING MOBILE PRODUCTIVITY

Deploy and Provision Granular Role- and Device-Based Access, Security, and Management Policies for Mobile Devices

Challenge

Enterprise users today are mobile and demand simple, secure connectivity to be effective for their employers. They want access to networked or cloud-based applications 24/7/365 from anywhere in the world via smartphones, tablets, or similar mobile devices, and from Wi-Fi or 3G/4G-enabled laptops.

Solution

The Pulse solution provides fast, easy, secure access from smartphones, tablets, laptop PCs, and similar mobile devices to enterprise networks and the cloud, enabling users to access corporate networked and cloud-based applications, enterprise and personal e-mail, or the Web.

Benefits

- Broad support for mobile operating systems, devices and access methods
- Most secure and scalable solution for mobile device connectivity and access
- Standards-based and simple to use
- Single, consistent set of access control policies for remote and mobile access

Today's workers are mobile. They need to be connected to their corporate network or cloud-based applications around the clock and around the world—anytime, anywhere. Lack of fast network, cloud, and application connectivity and access impacts productivity, which impacts revenues and profits. Secure connectivity and access is as vital a requirement as pervasiveness and speed.

In order to be productive, today's mobile users demand fast, secure corporate network and cloud access from anywhere in the world at any time of day or night, and their number is rising astronomically. Rising just as quickly are the numbers and varieties of devices with which mobile users attempt network and cloud access. As more and more mobile users with diverse devices require network access, and as more organizations embrace the use of personal mobile devices and "Bring Your Own Device" (BYOD) initiatives, mobile device and network security can be compromised, and the number of issues and problems spawned can swell. The success of today's enterprises and service providers is predicated on their ability to enable authenticated, authorized mobile users with controlled but secure, fast, and seamless access to all necessary network resources—from any mobile device, anywhere, at any time, to effectively maximize security and productivity.

The Challenge

Enabling basic connectivity across mobile platforms such as Apple iPhones, Google Android devices, smartphones, tablets and similar mobile devices, as well as 3G- and 4G-enabled laptops, can be a daunting challenge. From corporate-issued laptops with 3G and 4G capabilities to Wi-Fi enabled mobile devices, to business or personal smartphones, fast, secure, authenticated, and authorized access to corporate resources is a necessity for today's global, mobile workforce. Mobile workers also do not want the burden of dealing with different agents, clients, or applications to access their network and its resources; they just want easy access from anywhere and any device to the data they need, and they want it now.

Enterprises and service providers alike are challenged to seamlessly enable secure network connectivity and access for users from any device, anywhere, at any time, while simultaneously limiting connectivity and access only to authorized users and to certain necessary resources. At the same time, the number, sophistication, and cost of breaches and network threats pose a continuing challenge. Breaches and threats continue to grow exponentially, forcing enterprises and service providers to ensure that mobile users and their devices are authorized and secure before they are allowed network or application connectivity.

The proliferation of mobile device usage is driven in many instances by employees and users seeking (or now being instructed) to use their own personal mobile devices, including smartphones, tablets, and personal or business provided laptops, to access corporate data.

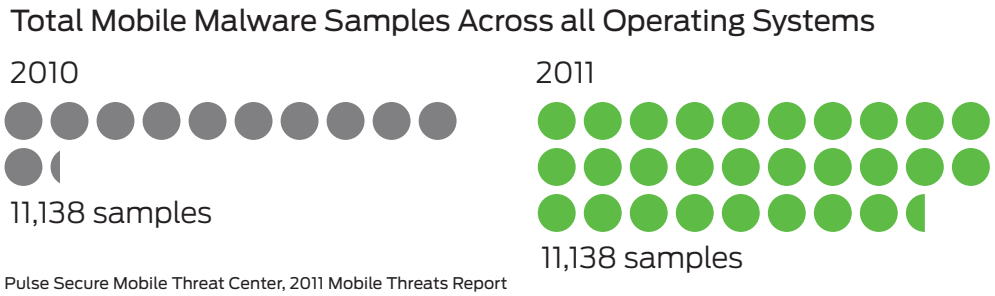

Figure 1: Total Malware Samples Across all Operating Systems

However, this practice can raise a number of issues. Mobile devices represent a new platform that enterprises need to secure, since they are now used as often as desktops and laptops for corporate access.

- Many companies do not employ multifactor authentication or at least are unable to implement multiple authentication methods for their mobile users, even when using company-issued devices, not to mention personal mobile devices.
- Inconsistent security policies between local and mobile or remote access can wreak havoc and create opportunities for breaches and hacks. Security policies should be consistent and uniform across an enterprise, regardless of access means, to avoid this problem.
- Attaining uniform security policies becomes more complex when a personal mobile device is used to access the corporate network or cloud and data. How can an enterprise or service provider maintain a uniform level of security across enterprise-issued mobile devices and personal mobile devices when they are used to access networked or cloud-based corporate data and applications?

Pulse and Mobile Device Solution

Pulse enables mobile devices, smartphones, Wi-Fi enabled devices, and 3G- and 4G-enabled laptops to securely access corporate data and applications.

Some enterprises limit network and application access for mobile users and their devices. Although these enterprises may allow employees to use personal or enterprise-issued mobile devices for calls, they might limit the user's mobile e-mail access, for example. Some enterprises also do not allow employees access to enterprise applications and data from their personal mobile devices. These business practices are mainly driven by the security concerns of the enterprise or of service providers providing enterprises with their managed services. However, Pulse Secure can neutralize these concerns.

Pulse increases enterprise productivity by enabling employees to be much more productive from their mobile devices than they have ever been before. This is accomplished using Pulse Secure MAG Series Gateways running Connect Secure, which enable secure remote access for employees and teleworkers using laptops and desktops remotely, as well as mobile users and their devices. Pulse supports a broad variety of mobile access methods in conjunction with the MAG Series gateways, including secure web-based access, ActiveSync for secure access to Microsoft Exchange servers, application tunneling, or full Layer 3 VPN access.

Pulse, in conjunction with the MAG Series gateways and Pulse Connect Secure, enables service providers and enterprises to deploy granular role- and device-based security policies for the provisioning of mobile device access, regardless if the device is a personal mobile device or enterprise issued. Pulse enables service providers and enterprises to leverage the same access and security policies and role-based information they have already developed and used for network and application access by non-mobile devices. This greatly simplifies the enterprise user's mobile access experience as well as the provisioning of security and access policies for mobile devices, saving deployment costs and administrator time.

Pulse enables service providers and mobile operators to consider new levels of service offerings that may be substantial drivers of profitability and differentiation, increasing their mobile device sales, average revenue per user (ARPU), and retention rates. Mobile device usage has enabled carriers to better utilize network bandwidth and increase ARPU. However, as more personal mobile devices are being used to access corporate networks and data, service providers are looking to increase ARPU by enabling new mobile applications that also increase customer retention. Pulse addresses this need, helping service providers secure network- and cloud-based application access, as well as deliver mobile device security and management for their enterprise customers while increasing smartphone sales, per-unit revenues, retention rates, and customer satisfaction.

Features and Benefits

Broadest Support for Mobile Devices and Access Methods

Pulse enables enterprises, managed service providers, and mobile access providers to offer anytime, anywhere access to enterprise applications and data using virtually any web-enabled device. These include smartphones, tablets, and Wi-Fi enabled devices, as well as 3G- and 4G-enabled laptops running a broad range of computer and mobile operating systems, including Apple Mac OS and iOS, Google Android, Microsoft Windows and Windows Mobile, Nokia Symbian, Linux, and others.

Pulse Secure supports a broad variety of mobile access methods, working in conjunction with the MAG Series gateways and Pulse Connect Secure:

- Pulse supports web-based access which delivers strong authentication—including multifactor authentication—regardless of mobile platform or OS.
- Supports ActiveSync, allowing mobile users access to e-mail and calendaring functions.
- Pulse supports application tunneling, which enables application access with granular policies supported in Microsoft Windows Phone, iOS and some Android versions.
- Pulse supports Layer 3 VPN access enabling full network and application access for Apple iOS devices such as the Apple iPhone and iPad, and select Google Android devices.

Standards-Based and Simple to Use

Pulse leverages the open, industry standards of the Trusted Network Connect (TNC), among others, to enable easier integration. For laptop users, Pulse offers "plug-and-play" connectivity via secure web-based access. All mobile users need is Pulse and a mobile Internet connection and, with proper credentials and authorizations, they can access the enterprise network or the cloud for their applications and networked data.

Most Scalable and Secure Solution for Enterprise Mobile Device Connectivity

Pulse leverages the capabilities of Pulse Secure's market-leading SSL VPN gateways to offer the most scalable mobile remote access service on the market with the lowest operating costs. Pulse also includes endpoint security checks for laptop PCs to ensure that only healthy laptops are granted access to the enterprise network. Noncompliant mobile devices may also be automatically remediated.

Unique Custom User Experience

MAG Series Pulse Gateways with Pulse Connect Secure provide a lucrative managed services opportunity for service providers. Either through a single, physical gateway, or through Pulse's virtual SSL VPN in a service provider's data center, each enterprise customer can enjoy a distinctive, custom, remote access user experience.

Consistent Policies for Mobile and Remote Access Control

Pulse enables enterprises and service providers to create and enforce consistent remote access and mobile access policies across their networks, saving time and cost while ensuring that granular access policies are enforced uniformly, regardless of the access device and method.

Solution Components

Pulse includes a software client for mobile devices (smartphones, tablets, laptop PCs, and similar mobile devices), which interfaces with Pulse Secure MAG Series Pulse Gateways running the Pulse Connect Secure. The gateways communicate with the Pulse client to enable secure connectivity and access to the corporate network or cloud. This provides strong protection for enterprise data communicating between the mobile device and the corporate network, and the implementation and enforcement of uniform security policies for all enterprise users—mobile or otherwise—regardless of the user's mobile access method or device used.

Pulse consists of the same components, whether it is used with Wi-Fi enabled devices or on laptops with 3G/4G cards. The combined Pulse solution thus enables remote access and enterprise LAN access control on Microsoft Windows-based laptops; remote access and network access control (NAC) for Apple Mac OS or Linux-based laptops; and secure, mobile remote access—which also supports LAN-based NAC on the network—for mobile operating platforms and devices. The easy-to-use, intuitive Pulse user interface allows Wi-Fi and 3G/4G-enabled laptops running Windows, Mac OS, or Linux to access networked and cloud-based applications and data from anywhere, anytime with its "location aware" capabilities. These capabilities allow a user—without any intervention—to automatically connect to and access authorized corporate applications and data, based on location.

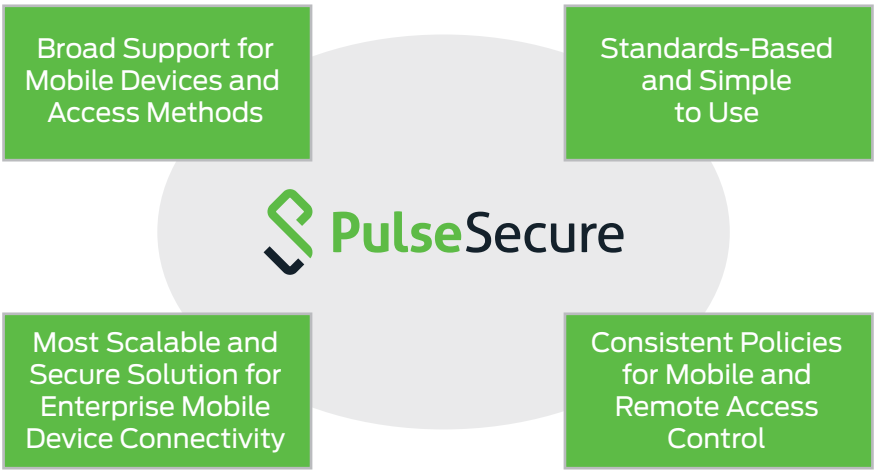

Figure 2: Pulse Secure: Features and Benefits

Summary—Pulse Empowers Secure Mobile Productivity

Secure, remote mobile access: Pulse increases mobile users' productivity through anytime, anywhere secure network or cloud-based application and data access. It protects networks, applications, and data from any mobile device that does not adhere to proper access and security policies. And, it regulates and restricts mobile user access to only those resources for which the user has appropriate credentials and authorization to view and access.

Broad cross-platform access: Pulse enables simplified smartphone, tablet, and similar mobile device deployment. Pulse supports the broadest range of mobile operating systems and devices. At the same time, Pulse saves costs as compared with other secure connectivity and access solutions or mobile security and device management solutions, and it provides revenue generating opportunities for service providers.

Simple and consistent: Pulse is easily deployed and provides simple mobile device connectivity, security, and management options. Pulse also enables enterprises and service providers to create and enforce consistent mobile and remote access policies. Pulse has been developed and delivered by Pulse Secure, a proven market leader and one of the few, if not the only vendor able to converge and address enterprise and service provider mobile remote access, security, and management needs today, as well as into the future as their needs evolve.

Next Steps

For more information on Pulse Secure, please refer to the Pulse Secure website at **www.pulsesecure.net** and contact your Pulse Secure representative.

About Pulse Secure, LLC

Pulse Secure, LLC is a leading provider of access and mobile security solutions to both enterprises and service providers. Enterprises from every vertical and of all sizes utilize the company's Pulse virtual private network (VPN), network access control and mobile security products to enable end user mobility securely and seamlessly in their organizations. Pulse Secure's mission is to enable open, integrated enterprise system solutions that empower business productivity through seamless mobility.

Corporate and Sales Headquarters

Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
www.pulsesecure.net

SB001 Aug 2014