

# EMPOWERING MOBILE PRODUCTIVITY

## Deploy and Provision Granular Role- and Device-Based Security Policies for Smart Phone and Mobile Device Access to Enterprise Applications and Data

### Challenge

Users today are mobile and demand simple, secure connectivity to networked or cloud-based applications 24/7/365 from anywhere in the world via smart phones, other mobile devices, or Wi-Fi or third- or fourth-generation (3G/4G)-enabled laptops, so that they can be effective and productive for their employers.

### Solution

Junos Pulse for mobile devices and smart phones provides fast, easy, secure access to enterprise networks and the cloud, enabling users access to corporate networked and cloud-based applications, enterprise and personal email, or the Web.

### Benefits

- Broad support for mobile operating systems and devices
- Most secure and scalable solution for mobile device connectivity and access
- Standards-based and simple
- Broad support for access methods to different types of corporate applications
- 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 will impact productivity, which impacts revenues and profits. Secure connectivity and access is as vital a requirement as pervasiveness and speed.

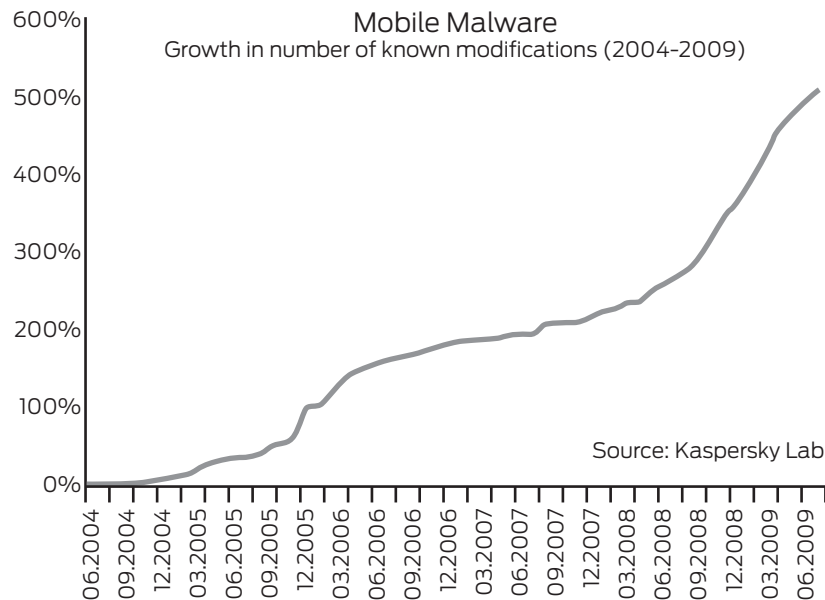
And, the legions of mobile users who, in order to be productive demand fast, secure corporate network access and access to the cloud from anywhere in the world at any time of day or night, is rising astronomically. Rising just as quickly are the numbers and varieties of devices with which mobile users attempt network and cloud access. As more and more mobile users with diverse devices require network access, 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 controlled but fast and seamless access to all necessary applications—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, Microsoft Windows Mobile devices, smart phones, and other 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 and personal smart phones, fast, secure, authenticated, and authorized access to corporate resources is a necessity for today's global and mobile workforce. Mobile workers also do not want the burden of dealing with different agents, clients, or applications; they just want easy access to the data they need, and they want it now.

Enterprises and service providers alike are challenged to seamlessly enable network connectivity for users on any device, from anywhere at any time, while simultaneously limiting connectivity and access to only authorized users and to only 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 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 to use their own personal mobile devices, including smart phones and personal or business provided laptops, to access corporate data.



However, this practice potentially raises a number of issues. Mobile devices represent a new genre of 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?

### Juniper Networks® Junos Pulse and Mobile Devices

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

Many 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 also might limit the user's mobile email access, for example. Some enterprises also do not allow employees access to enterprise applications and data from their personal mobile handsets. These business practices are mainly driven by the security concerns of the enterprise or of service providers providing their managed services. However, the Junos Pulse for mobile devices solution can neutralize these concerns.

Junos Pulse increases enterprise productivity by making enterprise employees that much more productive with their mobile handsets than they have ever been before. This is accomplished using Juniper Networks SA Series SSL VPN Appliances, the same appliance that enables secure remote access for employees and teleworkers using laptops and desktops remotely as well as mobile users and their devices. Junos Pulse supports a broad variety of mobile access methods in conjunction with the SA Series SSL VPN Appliances, including secure web-based access; ActiveSync, providing secure access to Microsoft Exchange servers; application tunneling; or full Layer 3 VPN access.

Junos Pulse enables service providers and enterprises to deploy granular role and device-based security policies for the provisioning of mobile handset access, whether the device is a personal 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, simplifying 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.

For service providers and mobile operators, Junos Pulse enables them to consider new levels of service offerings that may be substantial drivers of profitability and differentiation, increasing their mobile handset 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. These applications include mobile payment and remittance, mobile corporate email and IM, field and sales force automation, customer relationship management (CRM), intranet access and browsing, and even mobile video conferencing and

presentations. Junos Pulse addresses these needs, helping service providers secure network and cloud-based application access for their enterprise customers, while increasing smart phone sales, per unit revenues, retention rates, and customer satisfaction.

## Features and Benefits

Junos Pulse for mobile devices delivers:

- **Broadest support for mobile devices and access methods**

Junos 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 smart phones, Wi-Fi enabled devices, as well as 3G- and 4G-enabled laptops running a broad cross section of computer and mobile operating systems, including Microsoft Windows and Windows Mobile, Apple Mac OS, Linux, Symbian OS, and others.

Junos Pulse supports a broad variety of mobile access methods, working in conjunction with the SA Series SSL VPN Appliance. Pulse supports web-based access which delivers strong authentication – including multi-factor authentication – regardless of mobile platform or OS. It also supports ActiveSync, allowing mobile users access to email and calendaring functions. Pulse also supports application tunneling which enables application access with granular policies supported in Microsoft Windows Mobile. Pulse supports Layer 3 virtual private network access enabling full network and application access with Nokia Symbian devices.

- **Standards-based and Simple**

Junos Pulse for mobile devices is a standards-based mobile device access solution, leveraging the open, industry standards of the Trusted Network Connect (TNC), among others, to enable easier integration. Pulse offers “plug-and-play” connectivity via secure Web-based access. All mobile users need is a Web browser 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**

Junos Pulse for mobile devices leverages the capabilities of the market-leading SA Series SSL VPN Appliances, which offer the most scalable remote access service on the market – supporting up to 30,000 concurrent user sessions – with the lowest operating costs. Junos Pulse also includes endpoint security checks to ensure that only healthy mobile devices are granted access to the enterprise network. Noncompliant mobile devices may also be automatically remediated.

- **Unique, custom user experience**

SA Series appliances, on which Pulse for mobile devices is based, provide a lucrative managed services opportunity for service providers. With a single SA Series appliance placed in the service provider’s data center and the remote access capabilities hosted by the service provider, full virtualization enables each enterprise customer to enjoy a distinctive, custom remote access user experience.

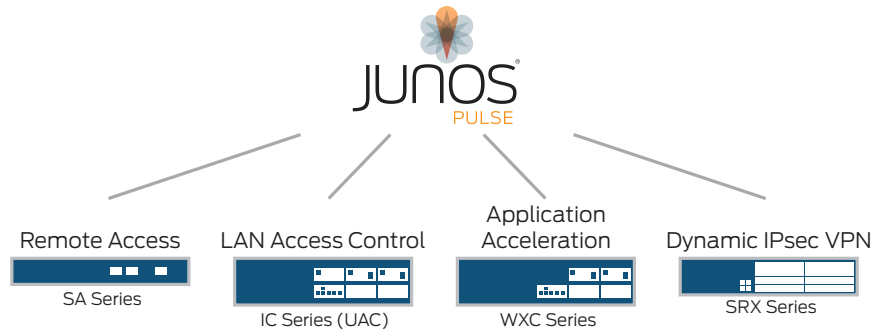
- **Consistent policies for mobile and remote access control**

By leveraging the SA Series SSL VPN Appliance, Junos Pulse enables enterprises and service providers to create and enforce consistent remote access and mobile access policies, saving time and cost while ensuring granular access policies are enforced uniformly regardless of the access device and method.

## Solution Components

Junos Pulse for mobile devices is comprised of a software client for various mobile handsets, which interfaces with Juniper Networks SA Series SSL VPN Appliances. The SA Series appliance communicates with mobile device software clients and enables secure connectivity and communication with the corporate network or cloud. This provides strong protection for enterprise data and uniform security policies for all enterprise users – mobile or otherwise – regardless of the user’s mobile access method or the device used.

Junos Pulse consists of the same components, whether it is used with Wi-Fi enabled devices or on laptops with 3G/4G cards. However, when used with Wi-Fi and 3G- and 4G-enabled laptops, Junos Pulse can also deliver built-in WAN acceleration capabilities for Microsoft Windows operating systems. This is available when the SA Series appliance is deployed with a Juniper Networks WXC Series Application Acceleration Platform. The SA Series appliance dynamically provisions the Junos Pulse client, Juniper’s integrated, multiservice network client that enables remote access, enterprise LAN access control, and WAN acceleration. The easy-to-use, simple, intuitive user interface of Pulse allows Wi-Fi- and 3G-/4G-enabled devices to access networked and cloud-based applications and data from anywhere, anytime with its “location aware” capabilities. Junos Pulse’s “location aware” capabilities allow a user—without any intervention—to automatically connect and to access authorized corporate applications and data, based on their location.



## Summary—Junos Pulse Enables Secure Mobile Productivity

- Secure mobile access:** Junos Pulse, when used with mobile devices 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 smart phone and other mobile device deployment. Pulse supports the broadest range of mobile operating systems and devices. At the same time, Pulse for mobile devices, Wi-Fi and 3G/4G saves costs as compared with other mobility solutions and provides revenue generating opportunities for service providers.
- Simple and consistent:** Junos Pulse is easily deployed and provides simple mobile connectivity options. Pulse also enables enterprises and service providers to create and enforce consistent remote access and mobile access policies. Junos Pulse has been developed and delivered by Juniper Networks, a proven market leader and one of the few, if not the only vendor able to converge and address enterprise and service provider remote access needs today, as well as into the future as needs evolve.

## Next Steps

For more information on Juniper Networks Junos Pulse for mobile devices, please refer to the Juniper Networks web site, at [www.juniper.net/us/en/products-services/software/software-platforms/junos-platform/junos-pulse/](http://www.juniper.net/us/en/products-services/software/software-platforms/junos-platform/junos-pulse/); and please contact your Juniper Networks representative.

## About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at [www.juniper.net](http://www.juniper.net).

### Corporate and Sales Headquarters

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
Phone: 888.JUNIPER (888.586.4737)  
or 408.745.2000  
Fax: 408.745.2100  
[www.juniper.net](http://www.juniper.net)

### APAC Headquarters

Juniper Networks (Hong Kong)  
26/F, Cityplaza One  
1111 King's Road  
Taikoo Shing, Hong Kong  
Phone: 852.2332.3636  
Fax: 852.2574.7803

### EMEA Headquarters

Juniper Networks Ireland  
Airside Business Park  
Swords, County Dublin, Ireland  
Phone: 35.31.8903.600  
EMEA Sales: 00800.4586.4737  
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.