

JUNOS PULSE: SECURING TODAY'S MOBILE, CONNECTED LIFE

An Integrated Approach to Mobile
Security and Device Management,
and Secure Network Access

Overview

Today, our world is digital, mobile, and converging. In the year 2000, there were 284 million Internet connections. Today, there are over 2 billion. In the year 2000, the number of mobile devices worldwide was around 700 million. Today, it's over 4 billion. We've moved from chat rooms to video conferences, from dial-up connections to broadband wireless connections.

Just think: It took the radio 38 years to reach 50 million listeners. Television reached 50 million viewers in 13 years. The Internet took only four years. The Apple iPod reached 50 million users in just three years. And, it took social networking site Facebook only nine months to reach 50 million users!

In today's mobile and connected culture, there are more users who are doing more things—all while they are mobile. The network, particularly the mobile network, is an integral part of our day-to-day life.

Trends and Challenges

While today's mobile, connected life clearly has its benefits it also has its challenges and pitfalls.

Business and government must support users who are full- or part-time telecommuters, remote workers, or mobile workers across an increasingly global, mobile work environment. Enabling fast, secure network access for these users is vital to productivity. Many of these same users demand that their personal smartphones, tablets, and other personal mobile devices be allowed access to the corporate network. And, now many companies are allowing users' personal mobile devices access to their network, public and private clouds, and resources as part of a Bring Your Own Device (BYOD) push. But, if users are not receiving sanctioned enterprise network access, many are sneaking their personal mobile devices onto the corporate network anyway.

Adding to the problems facing enterprises if they are embracing BYOD and empowering users to access the enterprise network and resources with their personal smartphones and tablets, or if mobile users go rogue and access the enterprise network on their own with their unmanaged, unapproved personal mobile devices is the exploding number, resilience, and virulence of mobile malware threats, security exploits, and attacks. Mobile threats, exploits and attacks are growing at a magnitude even larger and faster than what was previously experienced with desktop and laptop PCs. Combine these factors together, and your IT department is often overwhelmed and overmatched.

And, finally, consumers—you, me, and everyone else who's a part of today's mobile, connected world—use mobile devices for just about everything. Mobile devices span the scope from laptops, to tablet devices and smartphones. Even the smallest form-factor intelligent mobile devices are just little computers in the palms of our hands. As such, we have and will continue to store sensitive, private data and information on these devices, such as bank account information, credit card numbers, social security and other identification numbers, personal photos and text messages, even medical data. This makes smartphones, tablets, and other mobile devices a gold mine for identity thieves and hackers. It also makes mobile devices dangerous if lost. Imagine your vital financial, personal or business data—even pictures of your children—falling into the wrong hands.

Juniper Networks Junos Pulse

Juniper Networks® Junos® Pulse addresses these mobility challenges, delivering connectivity, security and management for mobile devices at scale, allowing enterprises to secure network access and personal or corporate issued mobile devices for employees and other users, and enabling service providers to deliver secure access, mobile security, and device management as managed services for their enterprise and consumer customers.

Junos Pulse delivers secure, mobile remote network access, reinforced by strong mobile security against malware, viruses, loss or theft, and other exploits, and robust mobile device and application management.

Junos Pulse provides enterprises, service providers and users with a complete, end-to-end solution to secure mobility.

Secure Access and Connectivity

Enterprises and service providers alike are challenged to deliver secure, mobile remote network access while limiting resource access based on user authentication, authorization and identity.

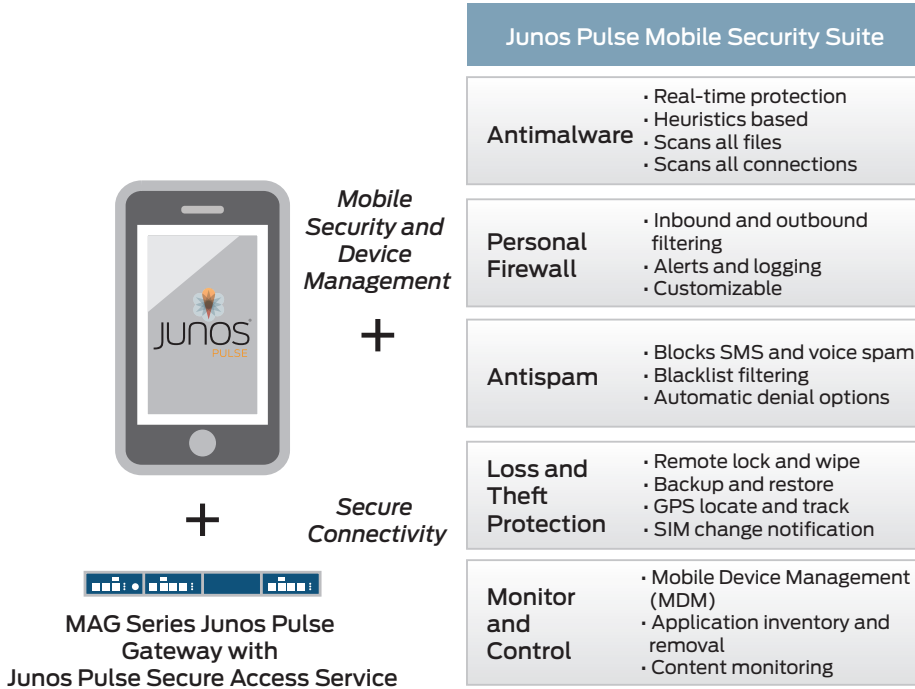
Junos Pulse, through the Junos Pulse Secure Access Service in conjunction with the MAG Series Junos Pulse Gateways or the SA Series SSL VPN Virtual Appliances (or the legacy SA Series SSL VPN Appliances) leverages Juniper's industry-leading SSL VPN technology to deliver simple, secure, authenticated access to corporate networks and resources for mobile users from any supported personal or corporate issued smartphone, tablet, or mobile device. Junos Pulse is a simple, integrated mobile user interface for the Junos Pulse Secure Access Service on the MAG Series gateways or the SA Series virtual appliances, protecting enterprises, their networks and clouds, and their sensitive applications and data by securely enabling granular, role-based mobile remote network and application access over a broad range of mobile operating platforms and mobile devices.

Junos Pulse and the Junos Pulse Secure Access Service on MAG Series gateways or the SA Series virtual appliances (or legacy SA Series appliances) together deliver a broad range of purpose-driven remote network and application access methods, including complete Layer 3 VPN access, secure e-mail and calendaring via secure ActiveSync proxy, as well as browser-based application access. Junos Pulse provides mobile remote users and their transmitted information with unparalleled data in transit security. Junos Pulse enforces a simple, consistent level of authentication and access control to smartphones, tablets, and mobile devices, as well as laptops and remote desktop PCs. Enterprises can grant complete or limited network and cloud access, or deny access based on centrally-defined corporate security and access policies. A host check performed on a user's device—regardless if it's a remote desktop PC, laptop, smartphone or tablet, managed or unmanaged, personal or corporate issued—can determine whether or not the device is compliant with enterprise security and access policies. Endpoint devices running Microsoft Windows, Apple Mac OS and Linux may be checked prior to and during a network access session to verify if the device security posture meets enterprise security and access policies. Device security policies can check for installed and running endpoint security applications, such as antivirus, personal firewall, antimalware, antispam, as well as custom-built device checks for specialized customer requirements. Apple iOS and Google Android mobile devices can be checked prior to and during a network access session to restrict access based on mobile operating system version, whether the device has been jail-broken or rooted, and as to whether or not the Junos Pulse Mobile Security Suite has been installed and is operational on the device. Junos Pulse also supports multifactor authentication, including the use of soft and hard tokens. Junos Pulse provides full Layer 3 VPN access for all Apple iOS devices—including Apple iPhones and iPads, any mobile device that runs Google Android 4.0 (Ice Cream Sandwich), and select Android-based devices from various mobile device manufacturers. Please refer to the Junos Pulse supported platforms document¹ for further details about supported Android devices. Also, in conjunction with the MAG Series gateways and Junos Pulse Secure Access Service or the SA Series virtual appliances (or legacy SA Series appliances), Junos Pulse enables authenticated, authorized users and their compliant mobile and remote devices seamless, transparent single sign-on (SSO) to cloud- and web-based applications, leveraging their authenticated SSL VPN session. And, finally, Junos Pulse provides detailed audit logs, perfect for use in regulatory compliance audits.

¹The Junos Pulse Supported Platforms Guide can be found under "Software Documentation" at www.juniper.net/techpubs/en_US/release-independent/junos-pulse-mobile/.

Comprehensive Mobile Security and Device Management

As users continue to demand mobile remote access to corporate networks and applications from their personal smartphones, tablets, and similar mobile devices, enterprises and service providers—many of whom already deliver managed access services to their SMB and enterprise clients—face a complex security problem: A personal mobile device left unprotected or unchecked can lead to the loss, theft, and compromise of valuable, confidential data—both corporate and personal.



Junos Pulse: Securing Mobility

Junos Pulse and the Junos Pulse Mobile Security Suite deliver a comprehensive mobile security, management, and control solution and protect smartphones, tablets, and other mobile devices from viruses, malware, spam, loss, theft, physical compromise, and other looming threats. Junos Pulse Mobile Security Suite delivers Day Zero malware protection through its powerful, heuristics based antimalware services. It also delivers mobile device configuration and management, and monitoring and control services that are purpose-built to secure and manage mobility. Junos Pulse—via the Junos Pulse Mobile Security Suite—can track and locate a lost or stolen mobile device, back up data from these devices, and wipe and lock the device, all remotely. It can remotely sound an alarm on a mobile device, send an alert when its SIM card has been removed, swapped, or replaced, and continue to track the device even if the SIM card has been removed.

Junos Pulse Mobile Security Suite includes support for mobile device configuration and management capabilities² for Apple iOS, helping enterprises to manage and secure Apple iPhones, iPads and iPod touch devices connecting to their network. On Apple iOS devices, Junos Pulse Mobile Security Suite can enforce and set passcode policies, provision and remove Microsoft Exchange profiles—which also removes corporate-synched e-mail, contacts and calendar events, provision VPN and Wi-Fi settings, perform remote locate and track³ and remote lock and wipe of a lost or stolen mobile device, and inventory and

² Please note: Apple iOS mobile device configuration and management functionality in Junos Pulse Mobile Security Suite is available only to customers who have applied to and are members of the Apple iOS Enterprise Developer Program. For more information on the Apple iOS Enterprise Developer Program please go to <http://developer.apple.com/programs/ios/enterprise/>.

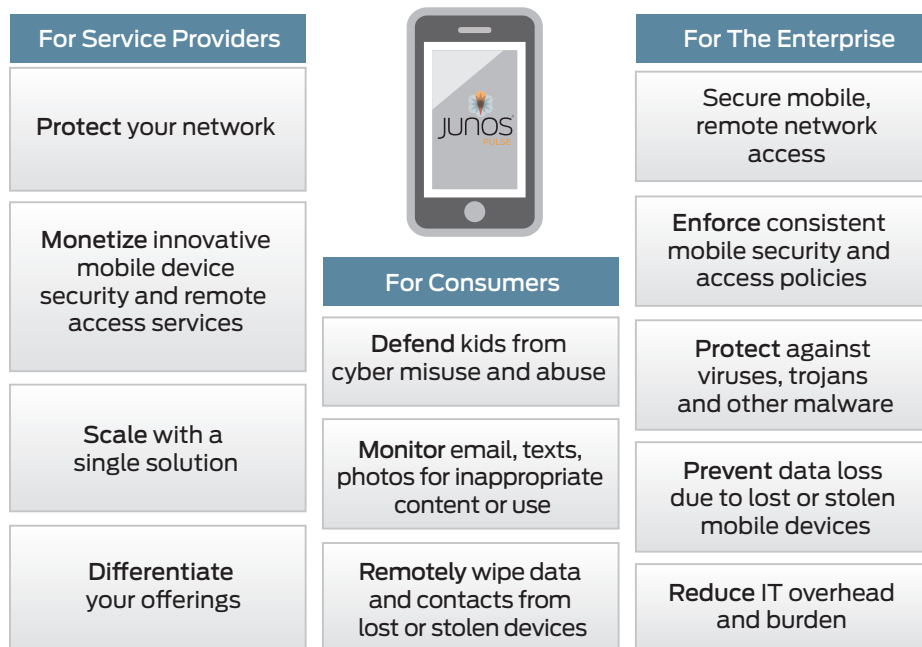
³ Please note: Supports Apple iPhones and 3G- and 4G-enabled Apple iPads only. Apple iPod touch devices and Wi-Fi only Apple iPads do not allow GPS location data to be accessed and collected.

restrict applications. Junos Pulse Mobile Security Suite eases an enterprise's mobile device management (MDM) burden, extends their corporate security policies - even addressing and securing BYOD policies, simplifies and protects the consumerization of IT, and ensures corporate information cannot be exploited on a lost or stolen mobile device.

Junos Pulse Mobile Security Suite also allows apps on certain Google Android devices to be automatically removed from a user's mobile device without user interaction required, with the proper permissions and access rights. The Junos Pulse Mobile Security Suite also allows an administrator to automatically remove malware, if detected on an Android device, once again without user interaction. These capabilities are available for Android-based mobile devices from specific manufacturers. Please refer to the Junos Pulse supported platforms document⁴ for further details about supported Android devices.

As a managed service, the Junos Pulse Mobile Security Suite delivers robust security against malware and viruses, which translates into increased breadth of offerings and revenues for service providers, mobile network operators (MNOs), and managed service providers (MSPs).

Junos Pulse Mobile Security Suite also protects you, your children, and your financial security by securing your smartphones, tablets, or other mobile devices from viruses, malware, and spam, preventing lost or stolen devices from ruining your economic security, alleviating identity theft, and protecting your family—especially your most valuable asset, your children—by securing your child's mobile device from and monitoring it for inappropriate use and contact.



Junos Pulse Delivers Secure Mobility to Mobile Device Users

Junos Pulse Mobile Security Suite is flexible, securing and managing personal mobile devices through a zero touch deployment model. A cloud-based, Software-as-a-Service (SaaS) offering, Junos Pulse Mobile Security Suite speeds and simplifies deployment and user rollout, expedites the mitigation of risk of infection, exploitation or infiltration from insecure or ill-secure mobile devices accessing the corporate network, decreases overall security costs—and specifically, mobile security costs, is highly-scalable, and enables enterprises and service providers to add new mobile security features or to take advantage of new security features and capabilities quickly and remotely. Junos Pulse Mobile Security Suite includes the Juniper Networks Junos Pulse Mobile Security Gateway, a hosted, web-based administrative management console from which Junos Pulse Mobile Security Suite features and services are provisioned, managed, and maintained by enterprises and service providers.

⁴The Junos Pulse Supported Platforms Guide can be found under Software Documentation at www.juniper.net/techpubs/en_US/release-independent/junos-pulse-mobile/.

Junos Pulse, through the Junos Pulse Mobile Security Suite, enables service providers to offer profitable premium, managed services to their enterprise and consumer subscribers, increasing average revenue per user (ARPU), providing competitive differentiation, and raising user satisfaction levels.

Summary—Security for Today’s Mobile, Connected Life

Junos Pulse powerfully yet simply centralizes mobile security, device and configuration management, and access services, delivering secure, mobile remote access, while insuring the integrity and secure use of managed and unmanaged, personal and corporate-issued smartphones, tablets, and mobile devices. Junos Pulse, enabling and integrating Juniper’s SSL VPN offerings - including the MAG Series Junos Pulse Gateways and Junos Pulse Secure Access Service, or SA Series SSL VPN Virtual Appliances (and legacy SA Series appliances) - and Junos Pulse Mobile Security Suite, delivers a robust, secure mobility solution supporting most major mobile devices and operating systems with an unparalleled depth and breadth of mobile access, security, management and control services.

Junos Pulse secures the critical aspects of your mobile, digital life, 24/7—protecting your company, your corporate and personal data, your identity, and your family. It’s secure, fast, simple, and transparent, and it’s always on and always connected—just like you!

Junos Pulse securely connects, protects and manages your mobile, connected life.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at 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

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

Copyright 2012 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.

 Printed on recycled paper