JUNOS PULSE MOBILE SECURITY SUITE

Product Description

Juniper Networks® Junos® Pulse Mobile Security Suite provides a comprehensive solution that includes mobile device security, mobile device management (MDM), mobile data security, and mobile application management (MAM) and content control. It is a key component of the Juniper Networks Junos Pulse solution which securely connects, protects, and manages both personal and corporate-issued mobile devices, in enterprise and service provider networks. As part of Juniper’s Simply Connected portfolio, the Junos Pulse Mobile Security Suite can also be deployed with Juniper’s market-leading SSL VPN platform to deliver a broad mobile security and secure BYOD solution; or Junos Pulse Mobile Security Suite may be used as a standalone service for mobile device, app and data security and management. The Junos Pulse client app can be downloaded to or preloaded onto an end user’s smartphone or tablet, as a simple, interactive user interface to the Junos Pulse Mobile Security Suite, which is managed from the cloud as a Software as a Service (SaaS) hosted offering from Juniper Networks or one of our managed service partners.

Features of the Junos Pulse Mobile Security Suite include:

• On-device antimalware/antivirus (Anti-malware)
• Loss and theft protection (Anti-theft/loss)
• Mobile device management (MDM)
• Mobile application management and content control
• Integration with Juniper SSL VPN and UAC solutions
• Service provider-ready SaaS architecture

As mobile threats are rapidly increasing in number and sophistication, and hackers continue to be financially motivated to steal data, identities, and to intercept corporate communications, the time is now to protect mobile devices, and the sensitive data and critical applications on them. The Junos Pulse Mobile Security Suite provides protection against viruses and malware, loss and theft, as well as other emerging threats for Apple iOS, Google Android, Research In Motion’s BlackBerry, Microsoft Windows Mobile, and Nokia Symbian-based mobile devices.

On-device malware protection updates automatically to defend your mobile device, OS, apps and data in real time against malicious software that may be downloaded from various app stores, or through files sent via Multimedia Messaging Service (MMS).
Short Message Service (SMS), Bluetooth, e-mail, Near Field Communications (NFC) and other means. Device loss and theft protection ensures that your sensitive data remains secure should your mobile device be lost or stolen. Control and monitoring capabilities ensure that appropriate device usage can be monitored and maintained at all times. And, mobile device management (MDM) ensures that any device accessing your network, cloud, resources and data meets a standard of security-focused requirements, as determined by your organization.

Defend Your Mobile Life with Junos Pulse Mobile Security Suite.

Architecture and Key Components
Junos Pulse Mobile Security Suite provides one of the industry’s most comprehensive mobile security solutions, offering a wide range of security and management functionality across a broad set of devices and mobile operating platforms. For example, Figure 1 depicts the Pulse Mobile Security Suite on a Google Android device. When a user acquires a new device, they simply visit the appropriate app store for their mobile platform to download the Junos Pulse app which includes the ability to provision and manage the Junos Pulse Mobile Security Suite. The Junos Pulse app is free to download, and all licensing for Junos Pulse Mobile Security Suite is managed from the Saas-based service management console.

The Junos Pulse Mobile Security Suite delivers a comprehensive array of mobile device security and management capabilities, including the following features.

Mobile Device Management (MDM)
Junos Pulse Mobile Security Suite
MDM Capabilities for Apple iOS
Junos Pulse Mobile Security Suite delivers MDM capabilities for Apple iOS devices such as the Apple iPhone and iPad. By supporting MDM capabilities on Apple iOS, Junos Pulse Mobile Security Suite is easing the workload of overburdened IT teams when it comes to the consumerization of IT, as well as their ability to effectively and efficiently address “Bring Your Own Device” (BYOD). By empowering IT teams to remotely manage mobile device features, apps, and security policies on a user’s Apple mobile device, Junos Pulse Mobile Security Suite provides enterprises and service providers with needed security and management for personal mobile devices, apps and data.

The following are the MDM features of the Junos Pulse Mobile Security Suite for Apple iOS devices, including the Apple iPhone and iPad:

Comprehensive Apple iOS device configuration, including:
- Accounts, including defining VPN, Wi-Fi, and Microsoft Exchange accounts
- Policies and policy enforcement, such as defining and enforcing device passcode strength, expiry, maximum passcode age, number of passcode attempts before initiating remote device wipe, control on-device encryption, and application restrictions such as disallowing use of a mobile device’s camera, screen capture capabilities, access to and the use of specific disallowed or offending applications, browser access, application store access and the like on a user’s personal or corporate-issued iOS device when used within the enterprise, or when accessing the corporate network or cloud and its resources
- Restrict the use of Siri and other iOS convenience features
- Limit diagnostic data sent to Apple
- Allow users to move messages from a Microsoft Exchange ActiveSync account, or enable users to send outgoing mail for specific ActiveSync accounts only from the iOS mail App
- Enable access to iCloud Services, and configure and enable Backup, Document Sync and Photo Stream capabilities in iCloud
- Provisioning of certificates through Simple Certificate Enrollment Protocol (SCEP) configurations
- Restrict user acceptance of untrusted Transport Layer Security (TLS) certificates

Inventorying of Apple iOS devices, for which the following attributes may be collected:
- Device information such as phone number, Unique Device Identifier (UDID), device name, model name, Apple iOS version and build number, device serial number, International Mobile Equipment Identity (IMEI), device ID, mobile equipment identifier (MEID), integrated circuit card ID (ICCID), and more
- Compliance information such as installed profiles, certificates, the presence or absence of a passcode, etc.
- Enrollment of users and devices
- Asset management of Apple iOS devices via polling and gathering data from devices, including an inventory of apps loaded on a device
Feature restrictions for the camera, which blocks access to the
• downloaded on-device camera apps 7
the default camera app included in Android to block even
camera API in Google Android, going deeper than simply blocking
existing password before a new passcode is required 4, auto-lock,
maximum number of failed attempts before device wipe and more
• Enforce on-device encryption for data-at-rest in internal storage 4
• Feature restrictions for the camera, which blocks access to the
camera API in Google Android, going deeper than simply blocking
the default camera app included in Android to block even
downloaded on-device camera apps 3
• Inventorying of Android devices, for which the following attributes
may be collected:
• Device information such as Android OS version and build
number, device model, device ID, phone number, International
Mobile Equipment Identity (IMEI), mobile equipment identifier
(MEID), integrated circuit card ID (ICCID), and more

Enhanced provisioning for:
• Remote configuration of VPN settings, such as adding, modifying,
or removing an accept point configuration for Android devices
from the Junos Pulse Mobile Security Gateway, and allowing the
built-in VPN client in the Junos Pulse mobile app to be configured,
with continued support of VPN Proxy, and additional support for
VPN On-Demand 8.
• Remote configuration of Wi-Fi settings, such as adding,
modifying, or removing an access point configuration on Android
devices from the Junos Pulse Mobile Security Gateway, with the
ability to preconfigure Android devices for access to protected
wireless networks using a variety of authentication protocols,
including Extensible Authentication Protocol–Protected
Extensible Authentication Protocol (EAP-PEAP) and Extensible
Authentication Protocol–Tunneled TLS (EAP-TTLS). Android Wi-
Fi provisioning can also control changing of the active service set
definition (SSID), making use cases such as the provisioning of
captive portals by wireless LAN (WLAN) devices more intuitive.
• The Pulse Mobile Security Suite also enables certain, specific
Android devices to automatically remove any disallowed,
offensive, or dangerous applications, including detected malware,
from a user’s mobile device, without user interaction, approvals,
or notification, to enforce encryption for data-at-rest stored on
the device’s SD card, and to disable Bluetooth and Wi-Fi on an
Android device 3.
• Microsoft Exchange ActiveSync (EAS) profiles contain
configuration data to allow for the synchronization of e-mail,
contacts, calendar, tasks, and notes from a messaging server to
a mobile device. Junos Pulse Mobile Security Suite also enables
administrators to remotely configure Microsoft EAS account
information such as adding, modifying, or removing an EAS profile
from the Junos Pulse Mobile Security Gateway for select, specific
Android devices 3.

Junos Pulse Mobile Security Suite also supports Google Cloud
Messaging (GCM). GCM is a framework from Google which allows
application servers to send lightweight messages to Android
applications. GCM is available for all devices running Pulse Mobile
Security Suite supported Android versions 4; the devices must
also have Google Play installed to be eligible. GCM enhances the
command delivery mechanism in Junos Pulse Mobile Security
Suite. Junos Pulse Mobile Security Suite will continue to ensure
that messages are delivered to user mobile devices by first
attempting delivery with GCM, and should that fail, SMS will
be used as a secondary delivery method. The message delivery
status is displayed in the Pulse Mobile Security Gateway, allowing
administrators to easily determine which devices have not yet
responded to sent commands.

Junos Pulse Mobile Security Suite MDM Capabilities for Google Android
Junos Pulse Mobile Security Suite also delivers vital, security-
focused device management capabilities for Google Android
to help secure and manage Android devices, apps and data by
enforcing device password policies and on-device encryption.

Junos Pulse Mobile Security Suite secure device management for
Android offers:
• Passcode policies and enforcement, requiring the use and setting
of passcodes, requiring alphanumeric passcodes 3, minimum
passcode length 4, minimum number of non-alphanumeric
characters 3, password history 4, number of previous passcodes
that cannot be reused 3, maximum passcode age 4, age of the
existing password before a new passcode is required 4, auto-lock,
maximum number of failed attempts before device wipe and more
• Enforce on-device encryption for data-at-rest in internal storage 4
• Feature restrictions for the camera, which blocks access to the
camera API in Google Android, going deeper than simply blocking
the default camera app included in Android to block even
downloaded on-device camera apps 3
• Inventorying of Android devices, for which the following attributes
may be collected:
• Device information such as Android OS version and build
number, device model, device ID, phone number, International
Mobile Equipment Identity (IMEI), mobile equipment identifier
(MEID), integrated circuit card ID (ICCID), and more
Rooted and Jailbroken Device Detection

In order to successfully secure Google Android and Apple iOS mobile devices, and to determine if the mobile devices should be allowed access to a secure network or cloud, SMBs, enterprises, and service providers need to know whether user devices have been compromised. That determination also must include whether the Android device has been “rooted” or the iOS device has been “jailbroken”.

Jailbroken iOS devices and rooted Android devices can lead to many security issues. For instance, jailbroken iOS or rooted Android devices can not only download apps from “official” app stores such as Google Play or the Apple App Store, but they can also “sideload” apps from unofficial channels and app stores, and other methods, which can leave devices – not to mention the critical apps and sensitive data on them – open to infection and exploit. Also, jailbroken and rooted devices may leave access to protected features and file system areas open to malware, such as virulent spyware. Jailbroken or rooted mobile devices represent new risk points for SMBs, enterprises and service providers with respect to securing their network, as well as ensuring secure mobile device access to their network, cloud, and sensitive resources.

Junos Pulse Mobile Security Suite can detect when a rooted Android device or jailbroken iOS device attempts network or cloud access. Junos Pulse Mobile Security Suite utilizes the existing Junos Pulse client app support for determining rooted and jailbroken mobile devices as its foundation, and integrates granular reporting features. An indicator in the Pulse Mobile Security Gateway will show administrators which mobile devices have been rooted or jailbroken. Users will also be served a notice in real-time indicating that their mobile device has been rooted or jailbroken. Finally, a dedicated report may also be run from the Pulse Mobile Security Gateway showing all rooted or jailbroken mobile devices.

Proactive Malware Protection

Viruses and malware cause unwanted billing, damage to or theft of valuable user and corporate data, and can render mobile devices unusable. The Junos Pulse Mobile Security Suite protects mobile devices against viruses, spyware, trojans and other malware delivered via e-mail, SMS, MMS, direct download, NFC, Bluetooth, or infrared transmission. It also scans downloaded apps for embedded viruses and malware. This is a unique, on-device solution, delivering around the clock, location independent, connected and unconnected protection for mobile devices, mobile operating systems, apps and data built from the ground up for today’s mobile devices. It takes into account the specific needs of mobile devices, such as limited device memory, CPU utilization, and has been optimized to address limited battery capabilities, minimizing device and network performance impact. Figures 2 and 3 illustrate how the antivirus/antimalware module of the Junos Pulse Mobile Security Suite looks on a Google Android device.

The Pulse Mobile Security Suite employs on-access scanning to monitor the integrity of files every time they are accessed. It will protect your Android, BlackBerry, Windows Mobile, and Symbian-based smartphone or tablet from malware by automatically detecting malicious code infections as they attempt to infect the mobile operating system. Junos Pulse Mobile Security Suite also addresses recursive archive scanning on Android devices, supporting .zip, .gzip, and .cab archives, with support for more extensions and file types being added. Archives up to 16 MB in size—which can be increased, depending on your mobile device— are scanned without being unpacked to local storage, decreasing the potential threat of device infection. The antimalware function also scans secure digital (SD) cards upon insertion, in addition to scanning all data going to and coming from your device to ensure that it is free from infection.

Also, a periodic full scan of a mobile device can drain the device’s battery, and can also drain CPU capacity. Junos Pulse Mobile Security Suite enables a periodic full antivirus scan of a mobile device only when the device is plugged into a power source, such as an A/C adapter or USB port. Once the user connects their mobile device to a power source, the full antivirus scan of their mobile device will commence. A configurable pop-up message can be displayed to the user letting them know that the charging of their device may take longer than usual since a full antivirus scan of their device has been initiated. If a full antivirus scan of a mobile device is overdue – as determined by the time period set by the SMB, enterprise or service provider – and the device is not connected to a power source, the user will receive an on-device notification indicating that a full device scan is needed, and the “Scan” button will turn amber with a warning message. Should the user cancel a full device antivirus scan, that cycle will be skipped and a new pop-up message will be shown to the user, stating that the scan will start in the next cycle.

Key anti-malware capabilities of the Junos Pulse Mobile Security Suite include:

- Protection against current and emerging mobile threats via automatic virus definition updates from the Juniper Networks Mobile Threat Center (MTC)
- Real-time monitoring and scanning of any file received via SMS, MMS, Bluetooth, Wi-Fi, infrared, NFC or desktop sync
- Real-time monitoring and scanning of any downloaded app
- Delivers 24/7/365, on- or off-premise, connected or unconnected mobile device, OS, app and data protection
- Scans archives, including .zip, .gzip and .cab archives without being unpacked to local storage
- Scans internal memory, memory card, and/or full device on demand
- Full device antivirus scan while charging
- Subscription-based licensing entitles users to automatic updates, with seamless transfer to new devices
also have the option to remotely lock a device, remotely set off an alarm on a lost or stolen device, or wipe data from a remote device to ensure that personal and business data cannot be accessed or exploited if a mobile device falls into the wrong hands. Certain data stored on the device can be remotely backed up and easily imported onto a new device—even if the new device has a different mobile OS. With these capabilities, you can minimize the risk of loss or exploitation of sensitive corporate data when employees lose their mobile devices, or if they are stolen.

Also, for certain Google Android versions and specific devices, Junos Pulse Mobile Security Suite can disable the USB port on a mobile device to ensure that the device cannot be connected to and accessed from a computer.

Key loss and theft protection capabilities in the Junos Pulse Mobile Security Suite include:

- Remote GPS tracking in case of loss or theft
- Remote device lock to make sure stored data and saved passwords are not accessible
- Remote data wipe to ensure personal or business data (contacts and calendar) no longer exist on the device
- SIM change notification and proactive security measures
- Remote backup of personal or business PIM data (contacts and calendar)
- Disable the device USB port when locked

Advanced Protection for Lost and Stolen Devices (Anti-Theft)

The loss and theft protection capabilities of the Junos Pulse Mobile Security Suite enable an enterprise or SMB IT administrator, or a service provider to quickly and easily pinpoint the exact location of a lost or stolen mobile device and have that location displayed in an online map. Users and administrators also have the option to remotely lock a device, remotely set off an alarm on a lost or stolen device, or wipe data from a remote device to ensure that personal and business data cannot be accessed or exploited if a mobile device falls into the wrong hands. Certain data stored on the device can be remotely backed up and easily imported onto a new device—even if the new device has a different mobile OS. With these capabilities, you can minimize the risk of loss or exploitation of sensitive corporate data when employees lose their mobile devices, or if they are stolen.

Also, for certain Google Android versions and specific devices, Junos Pulse Mobile Security Suite can disable the USB port on a mobile device to ensure that the device cannot be connected to and accessed from a computer.

Key loss and theft protection capabilities in the Junos Pulse Mobile Security Suite include:

- Remote GPS tracking in case of loss or theft
- Remote device lock to make sure stored data and saved passwords are not accessible
- Remote data wipe to ensure personal or business data (contacts and calendar) no longer exist on the device
- SIM change notification and proactive security measures
- Remote backup of personal or business PIM data (contacts and calendar)
- Disable the device USB port when locked

Mobile Application Management and Content Control

Mobile application management and content control features of the Junos Pulse Mobile Security Suite allow administrators to define strict application policies, and content monitoring and control settings. This includes restricting the types of applications installed on mobile devices, as well as controlling and monitoring data such as SMS and MMS that resides on devices. The following actions can be taken by administrators to bolster their application management and content control policies on smartphones, tablets, and other mobile devices:

- View applications installed on mobile devices
- Define a blacklist of applications that should not be allowed on mobile devices
- Monitor SMS, MMS, or e-mail message content
- Monitor phone call log and contacts
- View photos stored on the device

These features enable enterprises to control the types of applications deployed on their employees’ mobile devices, regardless of whether it is a personal or corporate-issued device. For service providers, these features enable parental control services, whereby parents can control the use of their child’s mobile device. The Pulse Mobile Security Suite enables a parent to monitor a child’s device and mobile activities via a web-based user self-service provisioning portal. With this easy-to-use and access interface, parents can view a list of all applications currently installed on their child’s mobile device, monitor the mobile device, and even track the location of their child’s device via GPS.
Simple, Flexible On-Demand Deployment

The Junos Pulse app for mobile platforms enables simple, scalable, and flexible feature deployment for the Junos Pulse Mobile Security Suite, including the following:

- Over-the-air (OTA) license enablement and registration
- Automatic boot upon device restart
- Intuitive, interactive user-friendly interface
- Full logging capability with ability to e-mail logs for troubleshooting

Junos Pulse Mobile Security Suite provides localization for all text inputs and display fields in the Junos Pulse client as well as for the Junos Pulse Mobile Security Suite and the Junos Pulse Mobile Security Gateway, supporting the following languages:

- Chinese (Simplified and Traditional)
- English
- French
- German
- Italian
- Japanese
- Korean
- Spanish

### Table 1: Junos Pulse Mobile Security Suite Features Supported by Mobile OS

<table>
<thead>
<tr>
<th>Junos Pulse Mobile Security Suite Feature</th>
<th>Apple iOS 4.X, 5.X, and 6.0</th>
<th>Google Android 2.3.X, 3.0 (Honeycomb), 4.0 (Ice Cream Sandwich), and 4.1 (Jelly Bean)</th>
<th>Windows Mobile 6.0, 6.1, and 6.5</th>
<th>Nokia Symbian 5th Edition, and Symbian ^3</th>
<th>Blackberry 5.0, 6.0, and 7.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus/Antimalware</td>
<td>*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mobile Device Management (MDM)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>Available only for certain Android versions and/or on specific Android-based mobile devices**</td>
<td>✓</td>
</tr>
<tr>
<td>Device Encryption Controls</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enhanced Device Passcode Requirements</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchange ActiveSync Provisioning</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Usage Restrictions</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN Provisioning</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wi-Fi Provisioning</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Based Client User Interface</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prohibited Applications</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCEP Service Support</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable Voice</td>
<td>*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Alarm/Scream</td>
<td>*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>GPS Locate and Track</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lock/Unlock Device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Wipe Device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lock/Wipe on SIM Change</td>
<td>*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Monitor and Control</td>
<td>*</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Application Inventory</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Removal</td>
<td>*</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Log</td>
<td>*</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Images Log</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MMS Messages Log</td>
<td>*</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 1: Junos Pulse Mobile Security Suite Features Supported by Mobile OS (continued)

<table>
<thead>
<tr>
<th>Junos Pulse Mobile Security Suite Feature</th>
<th>Apple iOS 4.X, 5.X, and 6.0</th>
<th>Google Android 2.3.X, 3.0 (Honeycomb), 4.0 (Ice Cream Sandwich), and 4.1 (Jelly Bean)</th>
<th>Windows Mobile 6.0, 6.1, and 6.5</th>
<th>Nokia Symbian 5th Edition, and Symbian *3</th>
<th>Blackberry 5.0, 6.0, and 7.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS Messages Log</td>
<td>*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Voice/Call Log</td>
<td>*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Automatic Registration</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Self-Service Web Portal</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Backup and Restore Contacts/Calendar</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Anti-spam</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Endpoint Firewall</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Bundles (Service providers only)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*The features of the Junos Pulse Mobile Security Suite are dependent on the roots and hooks made available within the supported mobile operating systems for Juniper to use to adapt features and functions. As mobile OS developers and device manufacturers open access to more roots and hooks for developers, the list of features within the Junos Pulse Mobile Security Suite is likely to expand in future versions.

**Please refer to the Junos Pulse supported platforms document for further details about supported Android devices.

Fast, Convenient Software as a Service (SaaS) Deployment

The Junos Pulse Mobile Security Suite is a Software as a Service (SaaS) hosted solution, allowing for quick, simple deployment by SMBs, enterprises, government agencies, and service providers. The Junos Pulse Mobile Security Gateway is the easy-to-use, cloud-based console for managing and controlling all of the Junos Pulse Mobile Security Suite features and functionality for supported mobile devices.

IT administrators can manage mobile device security and management policies by logging into the web-based Junos Pulse Mobile Security Gateway console using any SSL-enabled Web browser. The management console is hosted in a Juniper Networks or service partner’s secure data center, and is available to IT administrators anytime, from anywhere they are able to access an Internet connection and access the Web.

Key benefits of the SaaS solution include:

- Manage all Junos Pulse Mobile Security Suite features across the entire breadth of an organization’s mobile device deployment
- Quickly deploy and secure personal and business mobile devices, expediting risk mitigation
- Decrease overall security—and specifically, mobile security—costs
- Scale quickly to protect new mobile devices and users, and monitor and manage security coverage simply and quickly
- Add or leverage new mobile security features and capabilities as soon as they are released by Juniper Networks

Key capabilities of the Junos Pulse Mobile Security Gateway include:

- Web-based access and control of all mobile device security and management policies
- Detailed security reports on infections, updates, firewall rules, and the latest threats
- For service providers, the ability to create specific bundles of Pulse Mobile Security Suite features for business and consumer subscribers, with up-sell capabilities and feature availability for specific Pulse Mobile Security Suite features

Junos Pulse Mobile Security Suite and Juniper SSL VPN Gateways and Appliances

Endpoint device integrity and host checking are key features of the Junos Pulse Secure Access Service, which runs on Juniper Networks MAG Series Junos Pulse Gateways, as well as on Juniper Networks SA Series SSL VPN Virtual Appliances. Combining Junos Pulse Mobile Security Suite with Juniper’s award-winning SSL VPN ensures that SMBs, enterprises, government agencies and service providers are able to connect, protect and manage personal and corporate issued mobile devices, and effectively address BYOD.

Juniper’s Host Checker verifies that a mobile endpoint device meets corporate security policy requirements before granting the device mobile or remote access to a network or cloud, and its resources. Several enhancements have been made to Host Checker to address mobile device policy compliance. When Juniper’s SSL VPN solutions are deployed, Junos Pulse deploys Host Checker, which assesses Apple iOS and Google Android mobile devices for policy compliance, including:

- **Version Restrictions**: A policy can be configured which limits network or cloud access to only iOS and Android mobile devices running specific mobile OS versions.
- **Jailbroken or Rooted Device Detection**: A policy may be designed to prevent network or cloud access from jailbroken iOS devices or rooted Android devices, since jailbroken iOS devices and rooted Android devices are more prone to threats and malware exploits than non-jailbroken or non-rooted devices.
- **Enforcement of Junos Pulse Mobile Security Suite**: A policy may be configured which enforces that the Junos Pulse Mobile Security Suite be enabled on iOS or Android mobile devices prior to their being granted network or cloud access, ensuring that the mobile device is effectively clean of and protected against potential malware and exploits, and enabling greater control of security for mobile devices that are granted access to a network or cloud.
Also, full Layer 3 SSL VPN mobile, remote network and resource access is available on Apple iOS devices, as well as devices running Google Android 4.0 (Ice Cream Sandwich), Android 4.1 (Jelly Bean), and also select Android-based devices from various mobile device manufacturers through Junos Pulse interfacing with Junos Pulse Secure Access Service running on MAG Series gateways or as a virtual appliance.

Many customers, including service providers, large enterprises, and government agencies, also require IPv6 support for major mobile platforms. Apple iOS mobile devices connecting from an IPv6 network are able to connect to the IPv6 interface of the MAG Series gateways running Junos Pulse Secure Access Service, or the SA Series SSL VPN Virtual Appliances. Juniper’s SSL VPN gateways/appliances allow simultaneous connections from IPv4 and IPv6 IOS endpoints.


Features and Benefits

Junos Pulse Mobile Security Suite offers broad mobile operating system platform coverage with a comprehensive range of security applications, including antivirus/antimalware, anti-theft, identity protection, mobile device management, mobile application management, content control, antispam, endpoint firewall, and parental controls. Below are some of the significant features and benefits of the Pulse Mobile Security Suite.

Table 2: Features and Benefits

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
<th>Table 2: Features and Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanning of files received over all network connections</td>
<td>Protects mobile devices from potential malware that can infiltrate from multiple sources, including via SMS, MMS, Bluetooth, Wi-Fi, 2.5G, 3G, 4G, infrared, NFC or desktop sync.</td>
<td></td>
</tr>
<tr>
<td>Loss/theft protection</td>
<td>Mitigates the risk of losing corporate and personal data on a lost or stolen smartphone or tablet by remotely locating, tracking, setting off an alarm, locking or wiping the device contents, and turning off the USB port for specific Android devices.</td>
<td></td>
</tr>
<tr>
<td>Mobile device management (MDM) capabilities</td>
<td>• For Apple iOS devices, the ability to define and control mobile device configurations, including accounts, policies and policy enforcement, application restrictions, certificates provisioning, querying and collecting mobile device and compliance information, asset and application management, controlling on-device encryption, GPS location data, to enable access to iCloud Services and configure and enable Backup, Document Sync and Photo Stream capabilities in iCloud, and device management configuration options such as remote lock and wipe, clearing passcodes, and configuring and provisioning profiles, enabling enterprises and service providers to control the manner in which Apple iPhones and iPads access and use their network and its resources, restrict the use of Siri and other iOS convenience features, limit diagnostic data sent to Apple, and restrict user acceptance of untrusted TLS certificates.&lt;br&gt;• For Google Android devices, the ability to define and enforce comprehensive passcode policies, configure device management options such as remote lock and wipe, ensure data stored on-device and data at-rest is safe and encrypted, remote configuration of VPN and Wi-Fi settings, feature restrictions for camera, gather specific device data and inventory Android devices.&lt;br&gt;• For certain, specific Google Android-based devices, the ability with proper permissions and access rights to automatically remove any disallowed, offensive, or dangerous applications, including detected malware, from a user’s device without user interaction, disable Bluetooth and Wi-Fi, remotely configure Microsoft EAS account information, and ensure data stored on the SD card—in addition to data stored on the device—is encrypted, to further protect the enterprise and service provider network from threat and misuse.</td>
<td></td>
</tr>
<tr>
<td>Google Cloud Messaging (GCM)</td>
<td>Google Cloud Messaging (GCM) is a framework from Google which is available for all mobile devices running supported Android versions and that have Google Play installed, allowing application servers to send lightweight messages to Android applications, enhancing the command delivery mechanism.</td>
<td></td>
</tr>
<tr>
<td>Support for Apple’s iPhone Configuration Utility (IPCU)</td>
<td>Leverages Apple IPCU allowing administrators to export configuration profiles for Apple mobile devices, which may support new Apple iOS mobile device management (MDM) features as soon as Apple has released them, saving time and effort.</td>
<td></td>
</tr>
<tr>
<td>Inbound and outbound traffic monitoring</td>
<td>Protects mobile devices from accessing harmful or questionable content and prevents malicious content from being transferred to the device.</td>
<td></td>
</tr>
<tr>
<td>Remote backup/restore</td>
<td>Allows remote backups of personal and business data, and easily imports data into a new mobile device, if needed.</td>
<td></td>
</tr>
<tr>
<td>Mobile device monitoring and control</td>
<td>If desired, can enable service providers to protect subscribers’ children’s smartphones from exploit, and SMBs and enterprises from IP theft, corporate espionage, and device misuse by allowing a view into all messages (SMS, MMS, and e-mail content) sent and received, providing call logs of all voice conversations conducted on the mobile device, and enabling the viewing of all photos stored on the mobile device.</td>
<td></td>
</tr>
</tbody>
</table>
Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit www.juniper.net/us/en/products-services.

Ordering Information

Each SKU includes the following:

- License to deploy Junos Pulse Mobile Security Suite on as many devices as indicated in the SKU
- Subscription license for the duration indicated in the SKU
- Service and support for the duration indicated in the SKU
- Junos Pulse Mobile Security Gateway as a Hosted (SaaS) deployment

<table>
<thead>
<tr>
<th>Model Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESS-MSS-xU-#YR</td>
<td>Mobile Security Suite (MSS)</td>
</tr>
<tr>
<td># = Number of years subscription (1, 2, or 3 years)</td>
<td></td>
</tr>
<tr>
<td>x = Number of users (50, 100, 250, 500, 1,000, 2,000, 2,500, 5,000, 7,500, 10,000, 15,000, 20,000, 25,000)</td>
<td></td>
</tr>
</tbody>
</table>

1 The Junos Pulse for Windows Mobile client may be downloaded from www.juniper.net/support/products/pulse/mobile/3.0/#sw.
2 Apple iOS 5.0.
3 Android 2.2 or greater.
4 Android 3.0 or greater.
7 Supported on mobile devices running Google Android 4.0 or later; also compatible with Samsung MDM API 2.0 or later.
8 Android devices running Android 4.0 and higher; or Samsung devices running Android 2.3.3 or higher. For a complete list of supported devices, please refer to the Supported Platforms document at: www.juniper.net/techpubs/en_US/junos-pulse-mobile4.1/information-products/pathway-pages/junos-pulse-mobile/index41.html.

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.