SECURING THE HEALTHCARE ECOSYSTEM

Delivering Healthcare Applications Securely Anytime, Anywhere Through the Junos Pulse Mobile Security Suite

Challenge
Mobility is a top priority for many healthcare providers. Yet securing health information remains a top concern for healthcare institutions and patients alike.

Solution
Juniper Networks Junos Pulse Mobile Security Suite is a comprehensive solution that gives mobile device users in healthcare provider environments secure access to healthcare information and applications, protecting devices and the healthcare provider’s network from threats.

Benefits
• Mitigates the risk to sensitive healthcare data from compromised, lost, or stolen mobile devices
• Provides real-time protection from mobile viruses and malware
• Monitors inbound and outbound traffic, scanning files over all network connections
• Enables healthcare providers to remotely locate, lock, wipe, back up, and restore devices

Mobility forges a clear path to putting the most up-to-date information at clinicians’ fingertips, which ultimately saves time, reduces error, and improves the quality of care. Clinicians can use smartphones and tablets to access patients’ electronic health records, check lab results, view patient scans, and double-check medical references—whenever they need to and wherever they are. Whether for telemedicine, remote diagnostics, or even billing and administration, mobility is bringing new efficiencies to all facets of the healthcare delivery process.

Patients can use mobile applications to make appointments, view their own health records, get test results, and communicate with their physicians and other caregivers. Chronically ill patients can be monitored at home more easily, ensuring higher compliance with medications. With more and more consumers and healthcare professionals using smartphones, tablets, and other mobile devices, these trends will likely grow at an ever-increasing rate.

A significant concern for individuals and healthcare providers alike is the security related to these highly sensitive communications and transactions. Patients expect that their personal health information will be kept confidential, even when mobile—and that expectation is backed by federal law. Yet the integrity of healthcare transactions is only as secure as the integrity of the mobile device on which the interaction is conducted, and the environment within which the interaction occurs.

The Challenge
As people wholeheartedly embrace a mobile lifestyle, they are looking for the convenience of mobility in all aspects of their daily routines. For people accustomed to mobile banking and online shopping, accessing healthcare information through their mobile phones is an easy next step. The ability to make medical appointments, access test results, renew prescriptions, and view physician instructions from smartphones, tablets, and other mobile devices is a major convenience. Similarly, physicians and other caregivers can provide a higher quality of care with greater efficiency by accessing patients’ medical records, medical applications, and databases via tablets and smartphones.

But the security related to these highly sensitive communications and transactions is a significant concern for consumers and healthcare providers alike. Providers are under the strict provisions of the Health Insurance Portability and Accountability Act (HIPAA), which provides federal protections for personal health information. In addition, many providers must comply with the Payment Card Industry Data Security Standard (PCI DSS) requirements, which prescribe security measures to protect credit and debit card transactions.

However, any healthcare interaction or communication is only as secure as the mobile device and the situation from which the transaction is performed. Healthcare providers that overlook mobile security leave themselves exposed to financial and legal liability, as well as damage to their brand and diminished patient trust.
Healthcare providers may provide mobile security by authenticating users using Secure Socket Layer (SSL) technology to protect communications, and by providing antiphishing measures to verify the identity of the healthcare website. But these steps fail to address critical device and environmental security vulnerabilities. Security threats not presently addressed by existing mobile security include:

- Spyware capable of obtaining sensitive user authentication information
- Exposure or theft of personal information or records due to loss or theft of the mobile device
- Susceptibility to network-based attacks due to a lack of device firewall
- The use of unauthorized devices
- The use of unauthorized healthcare applications
- SSL “man-in-the-middle” attacks capable of intercepting user authentication credentials

**The Juniper Networks Junos Pulse Mobile Security Suite Solution**

The single best way to address today’s mobile security issues is for healthcare providers to offer Juniper Networks® Junos® Pulse Mobile Security Suite to their mobile device users. Junos Pulse Mobile Security Suite is a comprehensive solution that includes mobile device security, mobile device management (MDM), and control. Pulse Mobile Security Suite can be deployed with the market-leading Juniper Networks SA Series SSL VPN Appliances or MAG Series Junos Pulse Gateways, or it can be used as a standalone solution. Mobile Security Suite includes a client component, Juniper Networks Junos Pulse, and the Junos Pulse Mobile Security Gateway, which is available as a software-as-a-service (SaaS)-hosted offering from Juniper. At the end user device, all functionality converges on the Junos Pulse client, which serves as the user interface for Juniper’s SSL VPN products and additional Junos Pulse services such as the Mobile Security Suite, including:

- Antivirus
- Antispam
- Personal firewall
- Loss/theft protection (anti-theft)
- Backup and restore
- Application monitoring and control
- Mobile device management (MDM)

The Mobile Security Suite is a comprehensive security and device management solution spanning a broad range of mobile platforms. It protects mobile devices against viruses, spyware, trojans, worms, device theft, loss, and other threats that might befall them. It enables healthcare providers to provide users of smartphones, tablets, and other mobile devices with secure remote access to their healthcare information. Users can conduct transactions while mobile, with Mobile Security Suite protecting the user’s mobile device and the healthcare provider’s network from a wide range of threats.

The Junos Pulse Mobile Security Suite supports most major mobile operating system platforms. It provides protection from viruses and malware, from physical compromise, as well as other threats for Apple iOS, Google Android, Research In Motion’s BlackBerry, Microsoft Windows Mobile, and Nokia Symbian-based mobile devices. The Mobile Security Suite is a unique solution that takes into account specific challenges presented by smartphones and mobile devices, such as limited device memory and limited battery capabilities. It also will not negatively impact device or network performance.

When a mobile user opens a mobile healthcare application that includes Junos Pulse Mobile Security Suite, the client analyzes the security posture of the wireless environment from which that user’s device is broadcasting. If a “man-in-the-middle” attack scenario is not detected, the user will be allowed to submit credentials for authentication to the mobile healthcare application. The Mobile Security Suite analyzes the user’s mobile device, communicating the device’s security posture and unique device identity to authenticate both the user and device. This communication also ensures that the device is registered and permitted to be used for mobile healthcare. In this way, the Pulse Mobile Security Suite offers multifactor authentication of the user and device for the mobile healthcare transaction.

Juniper Networks Unified Access Control delivers granular, identity-based network and application access control on the LAN. When UAC or another access control solution is deployed with Mobile Security Suite, it will receive the state of the device’s security posture. It will also determine if the user’s device meets a minimum baseline of security requirements for network and application access as determined by the healthcare provider. Using existing Lightweight Directory Access Protocol (LDAP) capabilities, user and device authentication credentials are passed to the existing mobile healthcare authentication infrastructure. Based upon configured policies, authorizations, and user and device authentication, access to the mobile healthcare application may be permitted, limited, or blocked.

**Features and Benefits**

Junos Pulse Mobile Security Suite offers the broadest platform coverage with the most comprehensive range of security applications in the industry, including antivirus, antispam, endpoint firewall parental controls, anti-theft, identity protection, and MDM. Below are some of the significant features and benefits of the Mobile Security Suite.
**Junos Pulse Mobile Security Gateway**

The Junos Pulse Mobile Security Gateway is an easy to use console for managing and controlling all of the features and functionality of the Mobile Security Suite. The Mobile Security Gateway is available as an SaaS-hosted option for easy deployment without the need for an onsite server, wireless setup, or maintenance.

The hosted SaaS deployment of the Mobile Security Gateway enables a web-based console using any SSL-enabled Web browser from which administrators can create and manage the mobile security and remote management policies of the Mobile Security Suite. The management console in the SaaS deployment is hosted by Juniper Networks in our secure data center, with protected access enabled so that administrators for healthcare providers can manage policies at any time, from virtually any location.

**Solution Components**

The Mobile Security Suite is comprised of the Junos Pulse Mobile Security Gateway management console and the Juniper Networks Junos Pulse mobile client. These components are required to deploy security on mobile devices.

**Junos Pulse**

Junos Pulse clients are available for download by users or healthcare providers in the following app stores of each mobile platform:

- Junos Pulse for iOS: Apple App Store
- Junos Pulse for Google: Android Market
- Junos Pulse for Nokia Symbian*: The Nokia Store
- Junos Pulse for BlackBerry: BlackBerry App World
- Junos Pulse for Windows mobile client can be downloaded from www.juniper.net/support/products/pulse/mobile/#sw.

**Summary—Secure Clinical Mobility with the Junos Pulse Mobile Security Suite**

With the explosion of smartphones, tablets, and intelligent mobile devices, and the ever increasing use of these devices to access healthcare information and applications, the potential for threats to sensitive patient information and corporate financial data is real and emergent. The ability to ensure secure access to personal health information and financial data, and to enable protected transactions while assuring the healthcare provider’s network and application security, should be a paramount concern and effort for healthcare organizations today.

Junos Pulse and the Pulse Mobile Security Suite deliver the secure, assured mobile healthcare application services that today’s consumers and caregivers require. These solutions secure mobile devices from viruses and malware, regardless of mobile operating platform, while mitigating sensitive data loss or theft and exploitation when a mobile device is lost or stolen. Simultaneously, Junos Pulse and the Mobile Security Suite provide healthcare organizations with the assurance that a compromised user device or unauthenticated user cannot hack or breach their network, healthcare and administrative applications, delivering an unprecedented level of mobile security and peace of mind.
Next Steps
For more information on Juniper Networks Junos Pulse and Junos Pulse Mobile Security Suite, please refer to the Juniper Networks website at www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse/, and please contact your authorized Juniper Networks representative.

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.