The healthcare industry is going through a transformational period. Mobility, bring your own device (BYOD), and the explosion of medical-specific devices and applications are driving the way patient data and clinical systems are accessed, transmitted, and delivered. Electronic Medical Records (EMRs) and Electronic Health Records (EHRs) are further driving the volume of data as patient files, x-rays, lab results, and other sensitive medical records are transmitted across the network. Today, nearly one-third of healthcare providers use mobile devices to access EMRs or EHRs. Driving this demand are sophisticated and robust applications. The digitalizing of sensitive patient data is well underway, and this is making new care models possible—as collaboration, telemedicine, and electronic health initiatives transform healthcare delivery and outcomes.

According to a recent study, healthcare practitioners are relying more and more on mobile devices, as four out of five physicians say that they rely on their smartphones and tablets to access, retrieve, and submit sensitive patient medical data with over 80 percent of doctors using mobile apps every day. Further, more than 25,000 mobile healthcare (mHealth) applications are in use today, with millions of downloads collectively. The healthcare industry is faced with a new reality—healthcare applications are impacting mobility, professional applications for caregivers are driving BYOD, and hospital authorized applications are enabling access to clinical services.

### The Challenge

Clinician mobility presents difficult provisioning, management, and security issues for corporate policy and information security officers, leaving IT leaders with several key challenges. These include enabling mobility across a wide variety of devices, enabling physicians and other healthcare practitioners to securely access and send sensitive patient data whether they are on premise or at a nearby public café, and deploying and enforcing corporate and regulatory policies uniformly across the main hospital, data center, and remote healthcare facilities.

The BYOD phenomenon is driving mobility across the healthcare industry as doctors roam within a facility, campus, or between facilities, as well as collaborate with other healthcare practitioners around the world. Furthermore, digitizing patient data allows simple accessibility and use, but with that comes patient privacy and security concerns coupled with government regulatory and compliance issues.

To effectively enforce security and access policies, reliably protect sensitive patient data and healthcare applications from unauthorized users, loss, or theft, and enable caregivers to utilize personal mobile devices, healthcare organizations require a reliable and resilient security solution. The ideal solution must ensure that only authorized users are able to access the network, that strict policy controls are enforced from any location and from any device, and that there are preventive measures in place to ward off an attack. The solution must also give IT control over lost, stolen, or infected devices.

Today’s IT leaders are faced with several key challenges on the path to securing mobility for caregivers, the ability to safely connect to various ecosystems, to foster evolving new care models, and to robustly safeguard patient data:
• **Broad coverage**: Resilient security from the device, network, and application to the data center and the cloud.

• **Deployment flexibility**: Enforce policies consistently across all devices attached to the network, wipe data and access rights from lost and stolen devices remotely, enable security and access from a single client, and reduce IT overhead by better managing complexity.

• **BYOD strategy**: Whether it is a physician, caregiver, consultant, administrative staff member, or guest, healthcare organizations need to create identity-aware, consistent yet differentiated policies for user access and authentication, as well as simplifying authentication for all users and devices via a single sign-on (SSO) and well-defined, user-based, access parameters.

• **Regulatory and compliance**: Healthcare organizations are faced with greater responsibility and risk than ever, as Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH), and Payment Card Industry Data Security Standard (PCI DSS) regulatory requirements outline and enforce regulations to protect patients and their sensitive medical and financial data, and drive the mandatory need for healthcare providers to deploy auditable policies and reporting.

The Juniper Networks Secure Clinical Mobility Solution

Juniper Networks’ Secure Clinical Mobility Solution provides the healthcare industry with a sophisticated portfolio of mobile security technologies that uniquely address the challenges of mobility and BYOD, providing healthcare professionals with secure access to patient medical information in order to make informed decisions and improve patient outcomes. Juniper Networks’ Secure Clinical Mobility Solution delivers a cohesive portfolio of technologies that gives hospital clinicians and independent caregivers secure access to patient data as needed—anywhere, anytime, and from any device.

The Secure Clinical Mobility Solution is device-agnostic. It establishes security at the user profile level, allowing users to access the healthcare network or cloud using a SSO safely through any device from any location. This solution gives healthcare providers the ability to control network access regardless of the device being used. Healthcare IT departments are now able to control which applications users access, and who can access the network remotely—all from a single pane of glass. By offering consistent, identity-based security policies for each user, healthcare IT departments can empower users to use their device of choice. Access and security policies are uniformly enforced regardless of the device type, so that lost or stolen smartphones and tablets can be locked or have their data deleted remotely.

Secure Clinical Mobility Solution enables exceptional patient outcomes by:

• Allowing physicians to have access to critical patient data at the point of care
• Aiding patient care collaboration by enabling remote clinicians to securely access patient data from any device and from any location
• Securely enabling the use of smartphones and tablets from any location as a primary medical device

![Secure Clinical Mobility Network](image)

**Usage Scenario:**
- Caregivers need anytime/anywhere access to data
- IT needs to safeguard patient data
- CISO must have BYOD strategy

**Solution Benefits:**
- Access critical patient data at point of care
- Access to critical information enables better care decisions
- Secure access to network, applications and data anytime, anywhere
- Enable BYOD culture

Figure 1: Driving secure mobility across healthcare

Products: SRX Series, Junos Pulse, UAC, STRM Series
With Juniper’s Secure Clinical Mobility Solution, hospitals, healthcare systems, clinics, and other healthcare providers are able to:

- Control the network connection and the device
- Allow users to self-provision
- Enforce uniform authentication, access, and security policies and protocols, on premises and off
- Improve the delivery of patient care by enabling disperse care provisioning to any device

**Solution Components**

Juniper’s Secure Clinical Mobility Solution consists of the following technologies.

**Junos Pulse and Junos Pulse Mobile Security Suite**

Juniper Networks® Junos® Pulse enables fast, simple, and secure network, application, and data access for mobile and non mobile devices. As the multiservice, multi-device interface for Juniper’s industry-leading SSL VPN, mobile device security and management, network access control (NAC), application acceleration, and connection management offerings, Junos Pulse is the only client healthcare providers need to ensure security for their caregivers, patients, and user devices.

Junos Pulse and the Junos Pulse Mobile Security Suite work together to simply connect, protect, and manage a clinician’s mobile experience. Pulse and the Mobile Security Suite connect caregivers and their devices to healthcare networks, clouds, applications, and data through secure, mobile remote access. This solution protects mobile users, their personal or corporate-issued devices and apps from malware and loss or theft, and it centrally manages mobile devices to dynamically control apps.

Pulse Mobile Security Suite enables caregivers to use the mobile device of their choice, regardless of whether it is a personal or corporate-issued device, and it empowers IT to quickly and easily provision, secure, and manage those devices. Junos Pulse provides integrated and secure network, application, and data connectivity anytime, anywhere for a simplified end user experience. Mobile Security Suite also enables healthcare IT to consistently enforce endpoint security, differentiated, role-, and identity-aware access, and it minimizes risk of loss of sensitive corporate and patient data from compromised, lost, or stolen mobile devices.

Junos Pulse and Junos Pulse Mobile Security Suite enable clinicians and physicians to:

- **Connect securely**—Enables anytime, anywhere secure mobile, remote, and local access for all major smartphones, tablets, and laptops
- **Protect constantly**—Protects personal or corporate-issued smartphones and tablets, as well as the sensitive data on them, from malware, loss, theft, and other threats
- **Manage comprehensively**—Maintains control over mobile devices, ensuring that users, devices, and apps meet corporate security strictures and regulatory compliance requirements
- **Secure BYOD**—Ensures that all personal and corporate mobile devices accessing the network and its critical resources and data are protected and configured appropriately

**SRX Series Services Gateways**

Juniper Networks SRX Series Services Gateways are high-performance security, routing, and network solutions ideal for the healthcare industry. The SRX Series packs high port density, advanced security, and flexible connectivity into a single, easily managed platform that supports fast, secure, and highly available hospital data centers and outpatient clinics. Branch SRX Series gateways deliver secure and manageable networks for thousands of sites. A wide variety of product options efficiently support a range of performance, functionality, security, and budget requirements—connecting and protecting from a handful to thousands of caregivers.

The consolidation of routing, WAN connectivity, switching, and Unified Threat Management (UTM) simplifies deployment and administration, while delivering fast and consistent service quality regardless of clinician location. UTM services include best-in-class antivirus, antispy, URL filtering, firewall/VPN, and AppSecure application-level security that enable the branch SRX Series gateways as full featured solutions. The routing services of the SRX Series gateways include IPv4 and IPv6 unicast and multicast, extensive Network Address Translation (NAT), quality of service (QoS), performance and service-level agreement (SLA) monitoring, and flow management features.

**Juniper Networks SSL VPN and Unified Access Control**

Juniper delivers comprehensive, seamless, secure network and application access control to networks, clouds, applications, and data based on identity, location, device, and security posture.

- Juniper’s SSL VPN—deployed via the Junos Pulse Secure Access Service or Juniper Networks SA Series SSL VPN Virtual Appliances—delivers secure, role-based mobile and remote access to networks, clouds, applications, and data regardless of device used. By using the ubiquitous Secure Sockets Layer (SSL) protocol (the security protocol found in all standard Web browsers), both Pulse Secure Access Service and SA Series Virtual Appliances will eliminate the need for cumbersome, pre-installed client software, internal server changes, and costly maintenance and desktop support. Secure Access Service or SA Series Virtual Appliances also automatically check the security posture of user devices attempting network connection to ensure that they meet the appropriate access and security policies set by healthcare compliance requirements (such as HIPAA). And, if a device is found to be noncompliant, its access can be denied until it complies with security policies.

Both Secure Access Service and SA Series Virtual Appliances work across device types; it doesn’t matter if the user’s device is a desktop, laptop, smartphone, tablet, or other device. Pulse Secure Access Service or SA Series Virtual Appliances ensure secure, remote access to healthcare networks, clouds, applications, and sensitive patient data from any device.

But, secure mobile and remote access, while vitally important, is only one form of access control.

- Juniper Networks Unified Access Control—deployed via the Junos Pulse Access Control Service—combines the best of LAN and cloud-based access control with security technologies, while enabling enterprises to leverage their existing, heterogeneous network investments. For healthcare organizations, this means standards-based, cost-effective, reliable protection for all
confidential data on their LAN or private cloud, regardless of user device, role, or location. UAC is a flexible, scalable solution that simplifies the deployment and management of network and application access control, resulting in quicker, cost-effective HIPAA compliance and better overall network security.

Pulse Access Control Service and UAC leverage the same security posture checks for devices as Pulse Secure Access Service or the SA Series Virtual Appliances, ensuring LAN access from devices that meet the healthcare organization’s and compliance regulator’s requirements. Access Control Service and UAC also address the common problem of how to provide and provision appropriate local network, application, and data access for contractors and temporary guests with an easy-to-use Web interface designed for use by nontechnical staff. Enterprise guest users may be granted role-based, customizable, time-based access privileges on the network for the duration of their stay or deployment.

Comprehensive, seamless, secure healthcare network, application, and data access control is provided when both Juniper’s SSL VPN and UAC are deployed together. Using an industry-standard protocol (the Trusted Network Connect’s IF-MAP), user session data is shared between Pulse Secure Access Service (or SA Series Virtual Appliances), and Pulse Access Control Service (or UAC). This provides healthcare caregivers and other users—whether remote or local—with seamless, secure access via a single login to corporate resources protected by access control policies shared by Juniper’s SSL VPN and UAC solutions, simplifying the end user experience, as well as the deployment of access and security policies for healthcare IT staff.

UAC and Secure Access Service (SSL VPN) use a single enabling user interface and gateway—Junos Pulse and Juniper Networks MAG Series Junos Pulse Gateways, enabling healthcare organizations to deploy a single client for all devices (mobile and non mobile) as well as a single gateway. This solution provides differentiated, secure mobile, remote, and LAN-based access control to the network, cloud, applications, and data that is identity-, location- and device-aware with consistent, centrally managed authentication, access, and security policies.

Juniper Networks MAG Series Junos Pulse Gateways

MAG Series Junos Pulse Gateways enable secure mobile, remote, and LAN access with consistent policy control. MAG Series gateways are purpose-built appliances or modular chassis that work with Junos Pulse—the only multiservice, multi-device enabling security, access, and application client healthcare organizations will ever need.

Interfacing with service modules running Pulse Secure Access Service, the MAG Series delivers Juniper’s market-leading SSL VPN—Pulse Access Control Service—to provide Juniper’s renowned UAC network, application, and data access control—Junos Pulse Application Acceleration Service. The MAG Series gateways can deliver secure mobile and remote access to deployments as small as 100 concurrent users up to as many as 40,000 concurrent SSL VPN users; or for 200 concurrent guest users up to 60,000 concurrent UAC/NAC users. Also, MAG Series gateways can deliver application acceleration to as few as 25 concurrent Windows device users up to 4,000 concurrent Windows device users.

![Secure Clinical Mobility Solution](image)

**Figure 2:** Secure Clinical Mobility Solution—delivering reliable and resilient security across the device, network, cloud, application, and data center.
The MAG Series Junos Pulse Gateways, in conjunction with the Junos Pulse client, can lower OpEx and CapEx costs dramatically for healthcare organizations. This is because they reduce the number of management and software installation updates required on corporate-issued and personal mobile (and non-mobile) devices used by employees, as well as decreasing the number of appliances to deploy and maintain on the network.

**STRM Series Security Threat Response Managers**

Juniper Networks STRM Series Security Threat Response Managers can take data from virtually any network and security appliance to provide an “aerial” view of the network that administrators need to be proactive. Network-wide monitoring, correlation from multiple feeds, and reporting from a single STRM Series console means that all device logs are correlated and consolidated to enable identification, mitigation, and reporting of complex and blended attacks. Not only does the STRM Series allow IT administrators to be proactive, it also eases compliance reporting by including over 500 predefined and easy to customize reports. Like the other products in Juniper’s solution, the STRM Series can be scaled as you grow. All supported devices and reports are included, so there are no management cost surprises and unanticipated complexity challenges as your network is required to support new demands and devices.

**Summary—Delivering Secure and Reliable, Security for Clinician Mobility**

Juniper’s Secure Clinical Mobility Solution delivers pervasive, resilient, reliable, and comprehensive security for the healthcare industry. As mobility and BYOD continues to impact healthcare, the ability to predictably and uniformly deploy security protocols across the healthcare environment is critical. Juniper Networks Secure Clinical Mobility Solution provides a cohesive portfolio of seamless, interacting, and integrated technologies that allow hospital clinicians and independent caregivers quick and secure access to patient data anywhere, anytime, and from any device with a minimum of user interaction. Hospitals are able to centrally manage, customize, and enforce consistent yet differentiated identity-, location-, and device-aware security and access control policies. Physicians and other caregivers can then securely access critical patient information—many times closer to the patient—enabling them to make faster, better, more informed patient care decisions.

**Next Steps**

For more information about Juniper Network’s solutions for healthcare, please contact your Juniper Networks sales representative or visit [www.juniper.net/solutions](http://www.juniper.net/solutions).

**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](http://www.juniper.net).

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