

## Juniper Networks Solution Portfolio for Healthcare

Networking and Security Best Practices Help Healthcare  
Providers Improve Quality of Care and Lower Overall Costs



## Healthcare Solution Overview

---

Healthcare providers continually strive to deliver the highest quality care, make that care easily accessible, and deliver services at the lowest reasonable cost. To accomplish these goals, innovative healthcare organizations are increasingly leveraging their IT investments. There are several IT initiatives within the healthcare sector that Juniper actively supports. For those who deploy them, these initiatives are considered best practices to ensure the quality, safety and authorized availability of vital healthcare information and services. These initiatives include:

1. Security for Wireless LAN (WLAN) Deployments
2. Physician and Patient Portal Access
3. Healthcare Data Center Consolidation
4. Firewall Security Upgrades
5. Intrusion Detection and Prevention (IDP) Deployments
6. Network-based User Authentication
7. Resilient Network Routing
8. Electronic Medical Record (EMR) and Patient Health Information (PHI) Access Control

## Challenges

For healthcare providers, the challenge to provide easily accessible, highest quality care is sometimes at odds with the challenges of containing the cost of care and maintaining the confidentiality of patient health information. For healthcare IT organizations, the challenge is to improve the quality of patient care through the use of innovative technologies, to enable reductions in patient care costs, and to provide security for PHI, limiting access to authorized users only. In short, the quality of patient care is often at odds with the cost of patient care, and authorized access to PHI is often at odds with the obligation to restrict access to only those who are authorized to have such access.

## Trends

The growing trend among savvy healthcare IT executives is to leverage IT to create a business advantage by improving the quality of healthcare while reducing the cost of such care. In addition, the network that provides granular access control and heightened network security can ensure that proper access is granted to those with authorized access to PHI, while those without authorization are denied access. This serves to protect the healthcare facility from Health Insurance Portability and Accountability Act (HIPAA) non-compliance and to improve the audit process for HIPAA with granular audit reporting capabilities. Furthermore, IT is effectively leveraged to enhance the quality of patient care, improving the marketability of the healthcare provider while lowering total operating cost to also improve margins for the organization.

# Juniper Networks Solution Portfolio for Healthcare

## Security for Wireless LAN (WLAN) Deployments

Hospitals and clinics frequently deploy wireless LANs to lower cost and improve operational efficiencies. Expensive equipment in short supply may be connected to the wireless network via locators to track that equipment as it is moved from location to location within the facility. Additionally, healthcare providers will often use electronic tablets to transmit healthcare information and to record distributed doses of pharmaceuticals. This information can be immediately transmitted over the WLAN from the patient's bedside to the nursing station, allowing the nursing staff to spend more of their time with patients providing high quality care with greater efficiency.

Many healthcare providers are turning to Juniper's Odyssey Access Client (OAC) for 802.1X access control as they secure their WLAN environment, 802.1X is the IEEE standard for port-based network access control. This solution provides device access to a wireless LAN port and prevents access to the wireless LAN port if authentication fails. A benefit within the 802.1X standard is that the user/device is authenticated before an IP address is provided, which adds to the robustness of security in this network port access solution.

Juniper's OAC also allows healthcare organizations to consolidate 802.1X clients into a single client across several devices and throughout the facility. This saves staff training time with one common 802.1X client to learn, and it lowers ongoing support costs with one client to manage and support across the organization. In addition to providing robust port access control for wireless LANs, OAC is an excellent solution for controlling port access on wired LANs throughout the facility as well. OAC offers a robust extensible framework (EAP) to exchange network security credentials and integrates well with Juniper's Steel-Belted Radius® (SBR) to provide powerful authentication and data privacy capabilities. OAC supports Microsoft windows operating environments as well as MAC OS and the xSec protocol for Windows Mobile/CE.

The combination of robust port access security with ease of use and lower support costs makes OAC an ideal solution for healthcare providers, as they strive to realize improved security with lower than traditional cost throughout their facilities.

### **Physician and Patient Portal Access**

Physician, patient and additional partner portals are easy to create, deploy and support with Juniper's Secure Access platform. Enhanced security is provided through access controls based on the user and device accessing the network. HIPAA requirements can be enforced with specific access rights to patient health information. Furthermore, a cache cleaner ensures that confidential information is not left on remote devices being used to access the network. Physicians may be granted access to confidential medical records while patients are granted access to a portal for scheduling appointments or electronically requesting information that would otherwise be requested over the telephone or in writing.

The physician and patient portal improves authorized access granular control, serves to automate various requests for information and enhances network security. The added security for remote access combined with the ability to consolidate remote access to a single solution serves to enhance user satisfaction, provider access to critical information, and lower total cost for healthcare providers.

### **Healthcare Data Center Consolidation**

Data center consolidation projects serve to lower cost and provide better oversight and security for confidential information. Both of these benefits can be achieved by reducing multiple data centers to as few as two to provide disaster recovery through physical separation of stored information. However, when data centers are consolidated from a large number down to a much smaller number, several IT issues must be considered. Typically, bandwidth access may need to be increased at the fewer number of data centers. And with more users accessing a smaller number of servers over a greater distance, applications may run noticeably slower. Additionally, with a greater amount of confidential information stored in fewer locations, security needs and concerns increase at the consolidated data center locations.

Juniper's leading solution to enable data center consolidation is the DX platform. As with other industries, many of the applications within healthcare are migrating to Web-based applications hosted from consolidated data centers. The DX platform specifically addresses the need to accelerate Web-based traffic while providing additional Server Load Balancer (SLB) and SSL off-load benefits. SSL off-load greatly reduces the need for additional costly data center servers while supporting an increasing user base. To provide best-in-class security and availability to data centers, the DX platform is frequently deployed with Juniper's firewalls, intrusion detection and prevention system (IDP) and high-performance routers.

### **Firewall Security Upgrades**

Modern firewalls are migrating to include Unified Threat Management (UTM) capabilities. These capabilities include antivirus, anti-SPAM, URL filtering, and intrusion detection and prevention (IDP). By consolidating UTM within the firewall, healthcare IT staff can reduce the cost of deploying and maintaining a layered security architecture. In addition, this consolidation can serve to consolidate purchasing, support and maintenance contracts for IT security solutions, adding to the savings in terms of administration and contract processing costs.

Although there are many benefits in consolidating threat management capabilities into a single platform, the obvious concern is that the IT staff may be forced to compromise on the quality of the solution in any one area (for example, sub-optimal throughput performance within the firewall hardware to support a high quality and properly integrated IDP implementation). Juniper firewalls have been designed for full utilization of the integrated UTM capabilities without a significant degradation in performance. Additionally, Juniper has integrated best-in-class third-party solutions for UTM, so that healthcare IT staff is not forced to sacrifice between performance and antivirus, anti-SPAM or other UTM capabilities.

## **Intrusion Detection and Prevention (IDP) Deployments**

As data networking threats have migrated to the application layer, IDP is an increasingly essential layered security solution for the well protected organization. Juniper's IDP provides the most comprehensive intrusion detection and prevention solution with eight different methods of detection. These methods include both signature-based detection and protocol anomaly detection. Given this comprehensive set of detection methods, Juniper's IDP can detect intrusions for which signatures have not yet been written.

Given the importance of security to confidential patient health information and the fact that increasingly security risks are emerging from within the organization as opposed to outside of the organization, IDP is a business necessity for today's healthcare provider, as it can be used very effectively to detect and prevent suspicious behavior by authorized users of the network. This solution is also an ideal and effective addition to ensure HIPAA compliance, as any solid compliance process must include effective auditing and reporting. IDP provides granular visibility and an audit trail to ensure and improve upon HIPAA compliance and is typically a fundamental element of the network security audit process for HIPAA.

## **Network-based User Authentication**

Juniper's Steel-Belted Radius (SBR) is the industry-leading and de facto standard for RADIUS to provide Authentication, Authorization and Accounting (AAA) services. RADIUS is an essential building block of any robust network access control solution. Additionally for healthcare, should a network security breach occur, the accounting capabilities enabled by Juniper SBR can help to identify the source of the security breach. Where a large number of users have access to the network such as within healthcare provider environments, Juniper's SBR enhances fundamental and necessary network security.

## **Resilient Network Routing**

The benefits of resiliency in network routing are difficult at best to measure in terms of probability and cost of network outages. However, as it is increasingly important for the network to be up and providing access to routine business applications and critical patient information at all times, the cost of network outages is becoming just too costly to risk. Routing infrastructure is vulnerable to attack and can be overwhelmed at times, bringing networks to their "knees." Juniper's routing platforms with JUNOS are fundamentally designed to withstand such attacks and enable network administrators to address these attacks in real time. This being said, the most frequent reason for a network outage is a mis-configuration caused by human error. Here as well, JUNOS is enhanced with commit commands and configuration role-back capabilities to greatly reduce the potential for human error and to quickly recover from such errors should they occur. The fundamental design in terms of hardware, software and design methodology allows Juniper to bring to market routing platforms and new software releases that are robust and statistically have a lower probability of failure.

## **Electronic Medical Record (EMR) and Private Health Information (PHI) Access Control**

Network access control (NAC) is an emerging IT solution category and an ideal solution for providing network access control for EMR and PHI. Juniper's solution for network access control is the Unified Access Control (UAC) architecture. UAC with the Infranet Controller provides coordinated network access and dynamic policy to firewalls acting as Infranet Enforcers on the network. UAC can grant policy-based access to EMRs and PHI on a per-user or per-device basis. Should security parameters change on the device accessing the network, UAC can dynamically address these changes and enforce the appropriate policy. By architecturally integrating RADIUS and 802.1X solutions (as discussed above), Juniper provides a comprehensive and robust access control solution, one that is scalable and can be cost-effectively deployed in the most sensitive areas such as a data center or across an entire healthcare organization.

CORPORATE HEADQUARTERS  
AND SALES HEADQUARTERS  
FOR NORTH AND SOUTH AMERICA

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)

EAST COAST OFFICE

Juniper Networks, Inc.  
10 Technology Park Drive  
Westford, MA 01886-3146 USA  
Phone: 978.589.5800  
Fax: 978.589.0800

ASIA PACIFIC REGIONAL  
SALES HEADQUARTERS

Juniper Networks (Hong Kong) Ltd.  
Suite 2507-11, 25/F  
ICBC Tower  
Citibank Plaza, 3 Garden Road  
Central, Hong Kong  
Phone: 852.2332.3636  
Fax: 852.2574.7803

EUROPE, MIDDLE EAST, AFRICA  
REGIONAL SALES HEADQUARTERS

Juniper Networks (UK) Limited  
Building 1  
Aviator Park  
Station Road  
Addlestone  
Surrey, KT15 2PG, U.K.  
Phone: 44.(0).1372.385500  
Fax: 44.(0).1372.385501

Copyright 2007 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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.

## Solution Planning, Implementation, and Deployment

Juniper has its own professional services organization as well as several partners within healthcare to assist healthcare providers architect and deploy these or other best practice solutions. As these solutions often have a significant level of integration with the existing healthcare providers IT infrastructure and systems unique to the industry, specialized experience is often necessary and greatly valued. Juniper's market leading solutions and experience in providing these and other solutions for healthcare providers, combined with the expertise of our partners who specialize in providing solutions across the healthcare industry, set Juniper apart from others in the industry.

## Summary—Helping Healthcare Enjoy the Benefits of Networking Best Practices

Juniper makes available many network safety and performance enhancing solutions to address specific healthcare industry related needs. These solutions or components of a larger solution serve to help healthcare providers improve the quality of care while lowering overall costs. Through the solutions discussed here and other related solutions, greater accessibility of healthcare enabling information is made accessible to care providers and patients without sacrificing network performance or the security of private health information as it is subjected to potential attacks. Through the thoughtful use of IT innovation, today's healthcare providers have the opportunity to enhance the quality and accessibility of the care they provide their patients with cost-effective solutions that increase staff efficiency and keep sensitive information secure.

## 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).



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