

ADAPTIVE SECURITY FOR THE HEALTH/PHARMA VERTICAL

Intelligent Security Solutions That Work Together to Reduce Risk

Challenge

Healthcare and pharmaceutical companies face significant security issues. Today facilities are operating out of multiple locations, a variety of users approach the network with different devices, and access highly confidential data and life critical online applications.

The risk of a breach and the cost of non-compliance all require healthcare and pharmaceutical facilities to take a renewed look on how to reduce risk.

Solution

Juniper security solutions for healthcare reduces risk by leveraging the power of device collaboration. The solution improves on the ability to detect, mitigate and report on stealthy and sophisticated attacks while also delivering proactive compliance.

Benefits

Healthcare organizations and pharmaceutical companies can realize:

- Consistent and uncomplicated security across the distributed healthcare environment
- Compliance for multiple audiences
- Supports life critical applications
- Safety net for devices that cannot be patched or updated
- Security + performance without tradeoff
- Supports a multi-vendor approach
- Unparalleled capex & opex savings

Healthcare and pharmaceutical organizations are more sophisticated than ever before; but with that sophistication, they also face new challenges. On one hand, these organizations face some of the same challenges as many enterprises. Organizations are becoming more distributed—with remote clinical offices, trial sites, rehab facilities, outsourcing, and off-site workers. Each office and individual requires unique yet seamless access to applications and resources via a plethora of different, often unsupported devices. Network performance and uptime are critical, and security is a must. IT staff is stretched to the limits, and may not even be on site at remote clinics.

There are however, challenges that are unique to a healthcare environment. Electronic charting (EMR), patient telemetry, labs and requisitions, that have traditionally been transported manually now travel electronically—placing much more stress on the network; stress that the network was never designed to handle. Secondary, to maintain compliance across the distributed deployment is also a hard and fast requirement which the network and its deployed technologies were never designed to support. The possibility of a data breach or compliance failure is multiplied with every location which is opened, application which goes online, user and endpoint device that is granted network access. And as healthcare becomes increasingly distributed and more reliant on the network, risk will continue to increase significantly if we continue to manage the network as we always have.

More locations and more users with more devices accessing new services all add to security and compliance risks inherent in healthcare, nevertheless the basis of these threats is the underlying network itself. With more organizations requiring WiFi for RFID, patient tracking and telemetry the network is only becoming more complex, with more vectors for security and compliance risk. Many healthcare and pharmaceutical organizations are made up of businesses that have merged or technology may have been deployed as a “quick fix”. The result is a patchwork of disparate networks and applications never meant to work together. Needless complexity and infrastructure sprawl was introduced in the network and the result is unacceptable security and compliance risk. End users are incredibly diverse, and can include caregivers, transcriptionists, billing/insurance workers, students, guests, and patients themselves. IT managers may have to learn many different management systems just to push a single policy across the network, and getting overall visibility of events on the network as a whole is virtually impossible. Data gathering across the organization to demonstrate compliance is time consuming at best. By the time a breach or questionable traffic has been detected it is often too late to do anything about it, sometimes with devastating results.

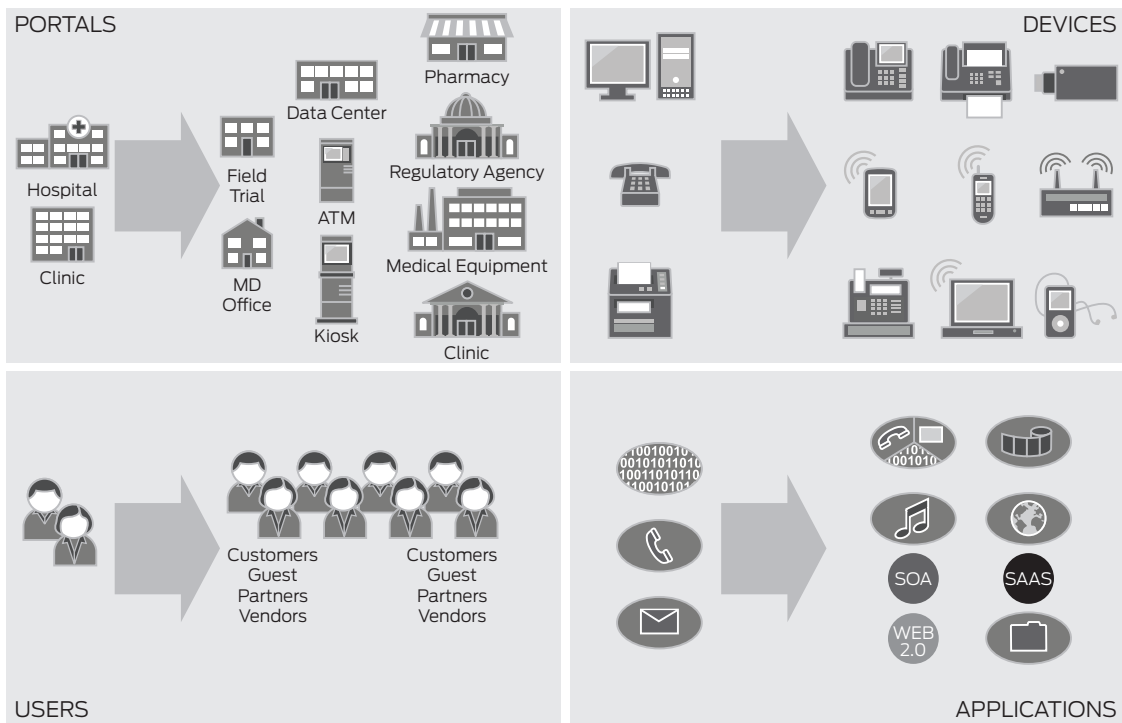


Figure 1: Supporting more applications, more devices, and more locations for more users and diverse audiences

All of these factors combine to create an environment that is ripe for exploitation, security breaches, or non-compliance with industry and government regulations. Juniper Networks® can help, with security solutions for healthcare that work better because they work together. Juniper Networks solutions deliver a consistent and comprehensive approach to security while providing you with the freedom to deploy best-in-class elements that are right for every user and location in your organization. Juniper products can be added incrementally which eliminates forklift upgrades. With Juniper, you move from reactive to proactive, by deploying the right security which will protect your environment both today and tomorrow while allowing you to focus on delivering world class care without risk.

The Challenge

Healthcare organizations and pharmaceutical companies face unique security and compliance challenges. Hospital systems, remote drug trial locations, and clinics have highly distributed topologies with a complex patchwork of different network elements. Bridging and securing these different networks—each of which could have its own IP addressing scheme, applications, authentication mechanisms, and connectivity structure to provide a consistent user experience—has been virtually impossible. Each location typically has its own security infrastructure as well, resulting in organizational silos made up of point products not designed to communicate with each other, let alone the rest of the network. The heterogeneous audience—including caregivers, pharmacies, third-party billing agencies, and patients—requires access to the network and applications to do their jobs or in the case of patients, to access services. Many users require network

access with their third-party and unmanaged devices. In other cases, devices such as MRIs, CAT scans, and other medical devices connect to the network and cannot be taken offline to be upgraded. Adding patches can actually invalidate the manufacturer's warranty. This results in unpredictable service, inconsistent security and unacceptable risk.

And, these stresses are only going to grow. Diagnostics and other hospital operations that have traditionally been physical and transported manually are now digital and communicated electronically, placing greater burden on the network and security infrastructure. Healthcare applications, from digital radiography and MRIs to medication dispensing and nuclear medicine are incredibly bandwidth intensive, straining network resources to the limit and increasing latency levels. These specialized applications must also share bandwidth with activities already running on the network, such as billing and logistics, as well as guest services—which can often be a revenue producer for these organizations. RFID tags, now commonly worn by caregivers as well as found on medical devices and other equipment, add to network traffic and complexity. Because RFID tags can be required for grant, stimulus, and compliance purposes, their use is slated to become more broadly adopted. While going digital poses problems in healthcare/pharmaceutical networks, its benefits have secured this technology a strong foothold in these industries. In fact, one of the stimuli included in the American Recovery and Reinvestment Act of 2009 is the HITECH Act, a \$19 billion Electronic Health Records (EHR) funding provision that adds both enticements and regulatory control. While this portion of the act is built around EHR, it is likely to affect other networked areas, including:

- RFID
- Guest Networking
- Barcode Medication Administration (BMCA)
- Patient Telemetry and Bedside Monitoring

All of these network demands take place on a backdrop of requirements designed to maintain the security and privacy of PHI and other confidential information, now mandated by local, state, and federal regulations. The networks of many healthcare organizations, however, are often not designed to protect against or prevent data breaches—particularly with so many groups interacting with each component of PHI, insurance, and payment details. The opportunities for a data breach grow every time a record is accessed, with repercussions that directly affect a healthcare organization’s business. According to Ponemon Institute, while the average customer “turnover” or “churn” due to a data breach was generally 3.6 percent, in healthcare it was much higher at 6.5 percent. And the cost of a healthcare breach, at \$282 per record, was more than twice that of the average retail breach at only \$131 per record¹. Medical ID theft has outstripped credit card theft as a money-making opportunity. While credit cards with CVV fetch \$10 to \$20, health records now fetch \$50 to \$60 each. Interestingly, while HIPAA laws do protect against divulging patient records, they do not protect against the sharing of information for billing purposes. Compliance with the Payment Card Industry Data Security Standard (PCI DSS) has often been overlooked by healthcare organizations, many of whom regularly accept credit cards as payment. According to SC Magazine, the fines levied by Visa alone can be up to \$500,000 per incident.

The Juniper Networks Healthcare/Pharmaceutical Security Solutions

Juniper Networks offers healthcare organizations and pharmaceutical companies the industry’s only adaptive, security, access, and acceleration solutions that leverage a dynamic, cooperative product portfolio. These solutions provide both protection and performance enhancements, combined with network-wide visibility and control across the distributed footprint of the healthcare organization or pharmaceutical company. The result is a suite of products designed to increase security and application delivery while reducing the TCO associated with accelerating service and application delivery throughout the healthcare organization.

Each Juniper security product is best in class in its own right. But because they are from Juniper, these products offer something that other products don’t—a solution made up of elements that work together to provide value beyond the sum of its parts. This solution empowers the network itself to change based on parameters you set, as variables within the user environment, application type, and threat landscape change. All policy creation and solution configurations are managed through a single platform, Juniper Networks Network and Security Manager (NSM). With NSM, you can easily push a policy across your entire

network with only a single provisioning solution to learn. This significantly decreases operating costs, and enables faster policy/configuration changes, as it reduces the opportunities for human error. Juniper Networks Series Security Threat Response Manager (STRM) provides a single portal on security and network activities by showing you what’s going on throughout your network in real time. The STRM Series can take data from all of your network and security devices, regardless of vendor, to provide an “aerial” view of your network. The STRM Series also comes prepackaged with over 2,000 different reports, greatly simplifying the generation of network security, trending, and compliance reports that you need. Juniper’s solutions for healthcare enable you to get out of the reactive cycle of chasing threats that have already happened or scrambling to compile the information you need to meet a compliance audit, and allows you to be proactive. With Juniper, your network does the work for you.

Juniper Networks solutions for healthcare can be deployed incrementally, because each piece adds more value to the whole regardless of the order in which components are implemented. Because Juniper builds its products to open industry standards, devices interoperate with each other as well as with standards-based products from other vendors, including most major healthcare applications. This provides you greater choice and flexibility than proprietary solutions designed to lock you in to a specific vendor. Juniper solutions provide you with the identity-aware, product-specific security and application acceleration—as well as the network-wide visibility, mitigation, control, and reporting that you need to adapt and protect your network and organization against constantly evolving threats.

Key characteristics of these solutions include:

- A highly integrated and collaborative security solution that proactively identifies, mitigates, and reports on security and compliance threats.
- Application acceleration functions that ensures the secure delivery of life-critical health services.
- Comprehensive and consistent solutions approach across all locations.
- Optimum application performance and layered security without trade-offs.
- A full spectrum of identity and application-aware services.
- Granular, policy-based network and application access control, regardless of the user’s location.
- Centralized visibility and control reduces management complexity, false positive alarms, and overall costs.
- Automatic remediation and user self-remediation options for noncompliant devices significantly increase user productivity as well as overall network security.
- Automation of mundane threat mitigation and reporting activities that frees up IT staff.

¹ Network World—Data-breach costs rising, study finds—2/2/2009

Features and Benefits

Juniper Networks solutions enable healthcare organizations and pharmaceutical companies to realize a host of benefits, including the following.

Scalability, Consistency, and Performance Without Sacrificing Security

Juniper Networks products feature a consistent platform and OS, regardless of the deployment size. Juniper Networks security for healthcare solutions can all be managed by NSM, so there is only one management platform to learn and one console from which to push policy. This flattens out the learning curve associated with platform deployment, as well as ensuring consistency and reduces human errors. A single management solution such as NSM lightens the day-to-day load on your IT staff and frees them up to enhance your network, instead of spending all their energy just keeping it running.

All Juniper products are designed to scale via right-sized form factors or modular devices to which you can easily add capabilities as needed. And Juniper also delivers performance with innovative features like the dynamic delivery of its application acceleration client, which can speed remote application access by up to 10X. Remote users can get access to Web-based applications they need while significantly reducing the performance hit that comes from running an application across the WAN. Juniper gets your users more productive, faster—wherever they are.

Response to Network Threats in Real Time—Auditing and Documentation All the Time

Because Juniper Networks products are designed to work together, you can configure the network to dynamically respond to threats in real time, as well as to document events across your entire deployment. You can configure security devices to react to threats, data leakage, or unusual traffic early in an event cycle so you can stop an attack before it starts—instead of trying to pick up the pieces afterward. It's also easy to use and deploy automatic or user self-remediation, which lowers the burden on your IT helpdesk staff

by letting the solution help users automatically, or by letting users help themselves. Users are back online and at work fast and user satisfaction goes up while IT staff productivity is raised as well.

Juniper's cooperative security products also free IT staff from the time-consuming, error-prone process of manually correlating logs and compiling data, dramatically simplifying day-to-day management. You'll have a bird's-eye view of what's happening on your network, giving you the power to stop attacks before they can start, and making it easy to handle forensics should they be required. And Juniper also eases compliance records and auditing by compiling all the information that you need automatically via thousands of easily customized pre-formatted reports. Not only does this save time, but it enables you to simplify meeting requirements associated with stimulus grants.

Granular User-Identity/Role-Based Access for All Users and All Devices

Healthcare organizations and pharmaceutical companies must provide access to applications, resources, to a wide variety of different users—from caregivers and specialists to business-oriented users like transcriptionists, insurance professionals to patients who may be using pay-to-play services such as internet, VOIP and movies. It is critical that authorized users gain access only the information that they need. Juniper Networks makes it easy, with access products that provide granular access rights based on user identity. Access can be consistently restricted to only the applications, data, or portions of data the users need to do their jobs, whether they are coming into the network remotely or from the LAN. The solutions can also monitor applications running on the network. For example, if a user attempts to access instant messaging, peer-to-peer, or other bandwidth-intensive or potentially dangerous applications that are in violation of the hospital's policy, the network can be configured to alert IT or even suspend the user's network and application access until the user closes the violating application. This automatically prevents application misuse and can limit potential threats launched by users already on your network.

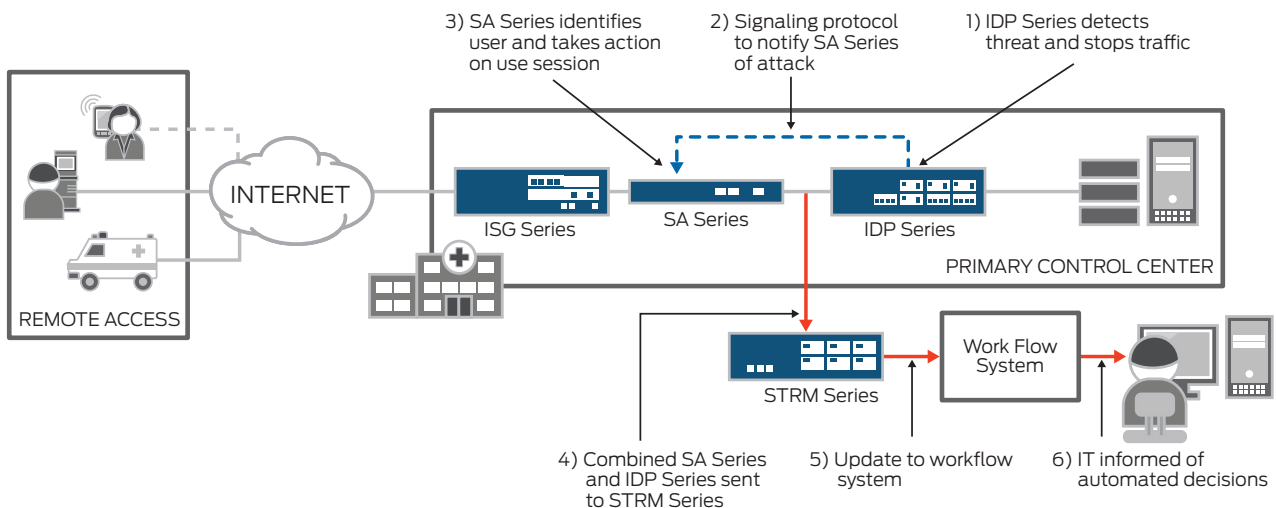


Figure 2: Security use case of Juniper's collaborative security for healthcare

Juniper also eases the process to deploy portals or extranets, enabling clinicians, guests, or patients themselves to get access to applications or resources that they need. Juniper’s security and access products work with whatever combination of authentication and authorization infrastructure you use, from simple passwords to dual-factor schemes that allow access to portions of PHI. Because it is difficult to ensure the security posture of a managed device, let alone an unmanaged device, Juniper’s access products also feature dynamically provisioned anti-spyware and anti-malware functionality.

Raise Performance and Security—Lower TCO

Juniper Networks solutions for healthcare reduce your TCO while they deliver flexibility and performance, whether you implement them incrementally or all at once. Juniper’s security products

feature a streamlined set of operating and management systems flattening the learning curve associated with new platform deployments. Because Juniper Networks products are standards-based, they will fit in seamlessly with your existing networking and security equipment. This means that you can focus your investments on the areas most important to you—no forklift upgrades required.

Solution Components

Juniper Networks is a leader in network security, with innovative products recognized as best in their respective categories by press and analysts around the world. Juniper’s solutions of security, access, and acceleration products that may be deployed across an entire network include the following:

| FEATURE | DESCRIPTION |
|--|--|
| A complete family of firewall/VPN solutions | <ul style="list-style-type: none"> • This suite of firewalls and integrated security products is tailored for specific uses, including Juniper Networks ISG Series Integrated Services Gateways and Juniper Networks SSG Series Secure Services Gateways. • A tightly integrated set of unified threat management (UTM) capabilities protects against malware, worms, viruses, trojans, denial of service (DoS), and blended attacks |
| SRX Series Services Gateways | <ul style="list-style-type: none"> • These gateways provide firewall, IDP, VPN, and other network and security services. They are based on Juniper’s revolutionary Dynamic Services Architecture—a stable, scalable platform designed to allow you to build the network you need today, with all of the headroom you could want for tomorrow. • SRX Series Services Gateways are available in a variety of form factors, enabling you to buy what you need for each location. |
| WXC Series Application Acceleration Platforms | <ul style="list-style-type: none"> • The WXC Series client significantly accelerates applications, ensuring an unparalleled user experience. • When combined with user credentials, the WXC Series can ensure personalized delivery options while maintaining the highest level of security regardless of location. |
| IDP Series Intrusion Detection and Prevention Appliances | <ul style="list-style-type: none"> • High-performance devices have up to 30 Gbps throughput. • These are available as standalone devices or integrated functionality in select firewalls, including the ISG Series and SRX Series platforms. |
| End-to-end access control solutions | <ul style="list-style-type: none"> • Market-leading Juniper Networks SA Series SSL VPN Appliances deliver secure, granular remote access control at the group or individual level. • Juniper Networks Unified Access Control delivers granular, dynamic LAN-based network and application access control based on user identity, device security state, and location information, leveraging your existing network infrastructure—from user authentication to access points and switches, to Juniper firewalls and IDP Series appliances—through an open, standards-based architecture. • UAC and SA Series share user session data, enabling users’ access via a single login to networked resources protected by uniform access control policies—delivering “follow-me” policies with a consistent user access experience whether users are connecting to the network locally or accessing it remotely. |
| Network and Security Manager | <ul style="list-style-type: none"> • This enables centralized provisioning of Juniper Networks routing, switching, and security products. |
| STRM Series Security Threat Response Manager | <ul style="list-style-type: none"> • A single console is provided for log, compliance and reporting, event correlation across diverse data sources, application-level monitoring, and network-based anomaly detection for Juniper and other network and security vendors. |

Summary: Intelligent Security and Performance for Healthcare and Pharmaceutical Organizations

Juniper Networks solutions offer healthcare organizations and pharmaceutical companies robust and highly cooperative, network-wide solutions consisting of tightly integrated network security, access, and acceleration products. These solutions deliver industry-leading, identity-aware network security, access, and acceleration that are dynamic and optimized for healthcare—as well as the consistent, network-wide visibility and control essential to meet strict compliance guidelines and protect your organization from today's sophisticated, highly volatile threats. Juniper Networks solutions help you achieve a sustainable competitive advantage that you can implement over time, realizing the benefits of superior products that work better, because they work together.

Next Steps

For more information on Juniper Networks, please visit www.juniper.net/adapt or contact your Juniper Networks representative. If you are interested in learning about financing offerings, please ask about Juniper Financing Advantage, provided by IBM Global Financing. Juniper offers comprehensive funding options at very competitive rates.

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.

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

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

Copyright 2010 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.