Extending the reach of healthcare organizations with secure networking

Improve productivity in healthcare organizations by enhancing network security.

Abstract

As the healthcare industry addresses the stress and pressures being placed on it by an aging population, a shortage in healthcare professionals, demands for quality of service, and new government regulations - the industry is looking for ways to do more with less.

The key to success is secure technology: not just deploying it, but embracing it. Connecting the healthcare community simplifies communications, coordinates efforts, reduces paperwork and puts the information in the hands of caregivers and staff. This , subsequently increases productivity, reduces costs and improves the process of care.

A secure network mitigates the risks of intrusion, infection and attacks. Providing secure remote access, inspection of the all information being transported, global management and business continuity, maximizes the benefits of connecting the healthcare community and improves their service to the community.

The case for connectivity

There is not a more dynamic sector than healthcare as an intersection of societal and business trends. The demand for healthcare services is increasing due to a growing and aging population. This, in turn, is increasing the demand for professional care providers, facilities and related business services.

At the same time, the healthcare sector is under relentless operational pressure. There is a shortage of qualified and skilled personnel. According to projections from the U.S. Bureau of Labor Statistics, more than one million new and replacement nurses will be needed by 2012. A study by University of Chicago found that schools are not training enough geriatric medicine professionals to keep up with the growth in the elderly population, which is estimated to be 20 percent of the total population by the year 2030.

Governmental changes at both executive and legislative levels may result in new laws that impact Medicare and other healthcare funding, putting a greater emphasis on cost-cutting and productivity across all economic sectors. The underlying cost structure is distorted by regulation and geography. And the conventional market forces that drive other industries do not translate.

Advances in technology are also driving increased connectivity in healthcare organizations, with once emerging trends like broadband Internet, wireless access, device mobility, voice/video over IP (VoIP) convergence, and cloud-based Web software-as-a-service (SaaS) becoming mainstream and ubiquitous among physicians, clinicians, administrators, researchers, suppliers and even patients.

The single greatest factor in facilitating this increased need for connectivity in the healthcare community is the adoption of secure networking technology.

Making the connection

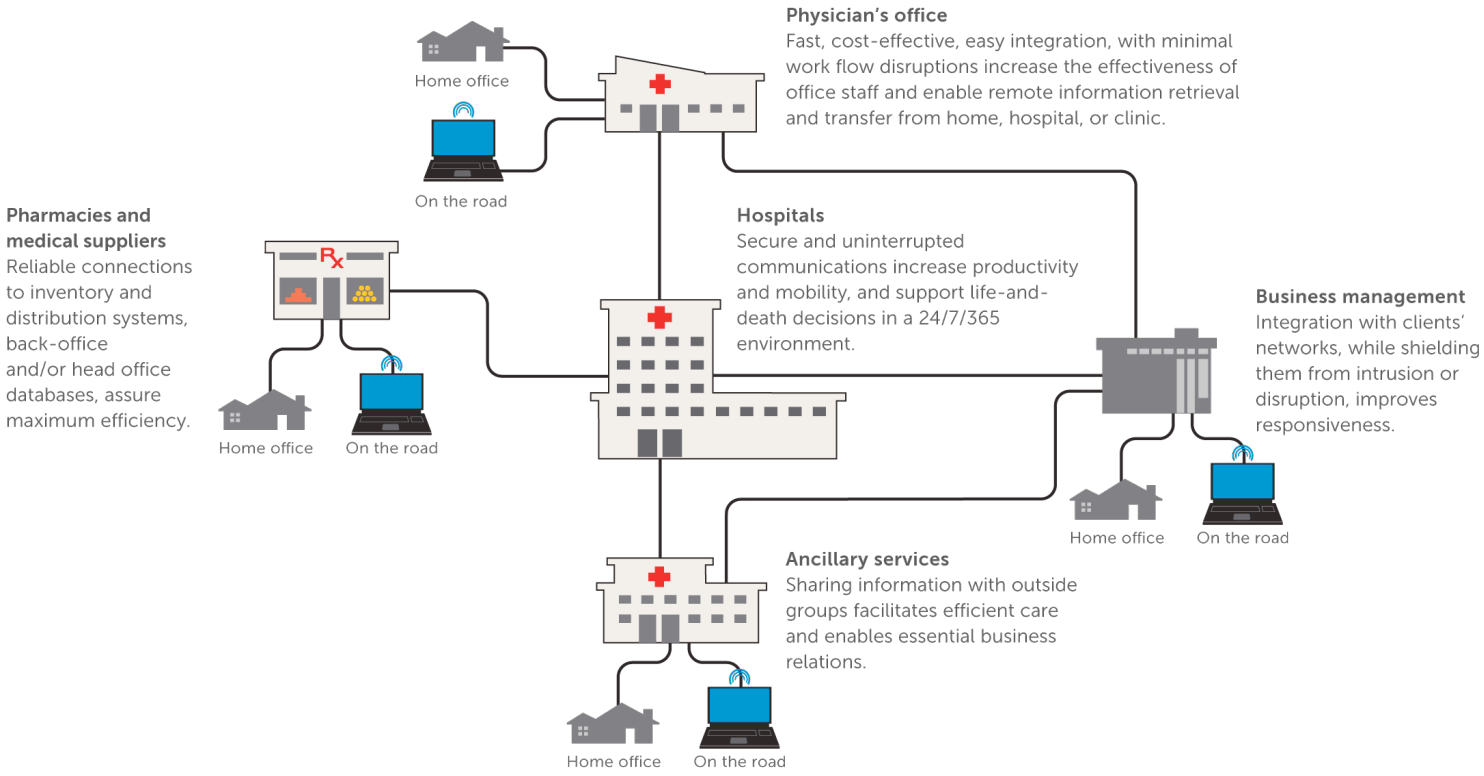
Using secure networking technology, it is now possible for a rural physician to have radiological analysis performed by a premier urban clinic's radiologist from his or her home, consult with a nationally recognized specialist, transfer all the patient's records to the nearest major hospital with the push of a button, while the financial side of all these transactions is handled by a claims processing center in India. Each of these steps is focused on healthcare's central mission: providing responsive, quality care. Just as important, the mission can be achieved with greater efficiency at a lower cost by securely leveraging the Internet.

Traditionally, healthcare providers have been hesitant to rely on the Internet as a secure information artery. While other sectors of business and the economy are using the Internet to address operating costs, personnel scheduling and even service quality issues, many healthcare organizations still have not embraced the interconnected operational communities that improve communications, productivity and reduce costs. But by addressing network security, the way is cleared for addressing other operating issues in a healthcare organization.

Each segment of the healthcare community enjoys its own benefits from secure connectivity and access to the other constituencies. But each link is critical and must be secured against delay, disruption and data loss or corruption. While security used to be seen as an

extra layer of technology, it is now an integral consideration for even the most basic functioning of an extended network that can include the broader distributed operations of the healthcare community including hospitals, doctors' offices, ancillary services, pharmacies, medical suppliers, and business services (see Figure 1, below),

Figure 1. Extended healthcare information network



Healthcare organizations continually look to technology solutions to increase mobility and enhance productivity. Their primary objective: bring information to staff when and where they need it. Whether in front of patients or in the back office, secure access to the right information is crucial to getting the job done. Popular tools include Internet and wireless-enabled Physician Order Entry systems, remote patient-administration applications, browser-based workflow automation applications, wireless handheld devices, and self-service patient portals. By aiding information flow, these solutions improve patient care, worker productivity, employee satisfaction and ultimately increase profitability.

Securing the connection

Networking used to mean bundles of wires strung throughout a building. Today's healthcare network environments may include endpoint computing devices that are fixed-site or mobile, wired or wireless, personally-owned or IT-managed. Network administrators need a flexible solution to address the myriad of security concerns associated with a dynamic and changing network environment.

Digital platforms broadly describe any healthcare information system—whether it's transmitting written or spoken records, x-ray or sonogram images, or other therapy-related data. Many of these systems run on open operating systems like Microsoft® Windows, putting them at risk from fast spreading worms and viruses. In every case, these systems are linked via a network that can be impacted by seemingly unrelated security issues. An e-mail-borne virus outbreak can slow overall network performance and even infect or destroy data living on your network. Without inspecting and monitoring the data that flows across the entire network, it opens the organization up to attacks that can devastate a business.

Wireless networking creates an unprecedented opportunity for healthcare organizations to make information available whenever—and wherever—healthcare professionals need it. However, if a wireless network is not properly secured, it's vulnerable to hackers. In order to take advantage of the mobility and productivity benefits of wireless—and to protect confidential information and uptime—a security-based approach to wireless is essential.

VPNs (virtual private networks)—a secure, dynamic connection between offices using the Internet—offer all the convenience and ubiquity of the Internet, with the privacy of a dedicated network. Healthcare enterprises securely connect their distributed organizations including major facilities, small offices, and home-based offices in a safe, cost-effective manner—no matter where people or facilities are located. However, VPN connections open new pathways for cyber threats. Without the proper security solutions on both ends of the connection to contain these threats, viruses and other attacks can run rampant.

With a proven security-based mobility and productivity solution in place, healthcare organizations empower their staff with the right information at the right time — whether in the office, in the halls, at a home office or on the road.

Dell™ SonicWALL™ offers healthcare organizations a range of easy, robust, and scalable healthcare solutions that deliver superior price-to-performance.

HIPAA compliance & reporting

Dell SonicWALL solutions apply 3DES and AES encryption to extend beyond HIPAA requirements. Dell SonicWALL solutions map to every requirement of HIPAA, including specifications for access controls, audit controls, integrity, authentication, and transmission security. Dell SonicWALL management and reporting solutions provide flexible, powerful and intuitive tools to correlate data from up to thousands of distributed Dell SonicWALL devices from a centrally-managed console.

Wireless solutions

Dell SonicWALL Secure Wireless solutions scale to virtually any network deployment, whether to connect patient data entry tablets, inventory scanners, guest WiFi hotspots or physician PDAs. Secure Wireless is a total security solution that integrates universal 802.11n/b/g and 3G wireless with an enterprise-class firewall/VPN gateway.

Network protection

Dell SonicWALL Network Security Appliance (NSA) solutions are engineered to reduce risk, cost and complexity by integrating automated dynamic security capabilities, high-speed Reassembly-free Deep Packet Inspection™ (RFDPI) and robust security services.

Secure remote access

Dell SonicWALL Secure Remote Access (SRA) solutions offers healthcare organizations and field clinics uninterrupted network access during natural disasters, fires, power outages or other disruptions. Dell SonicWALL SSL VPNs provide secure remote access portals to mission-critical resources from home offices, labs, field clinics, partner sites or virtually any other endpoint.

Email security

Dell SonicWALL Email Security (SES) delivers a powerful framework for driving HIPAA compliance initiatives by intelligently identifying e-mails and attachments that violate compliance policies, providing e-mail monitoring, archiving and reporting and applying multiple policy-based enforcement actions.

Backup and recovery

Dell SonicWALL Continuous Data Protection (CDP) offers end-to-end disk-based backup and flexible disaster recovery options. Low-touch CDP

transparently and automatically protects data and applications, while enabling self-directed restoration of files.

Benefits of secure connectivity

Enhanced patient care

A network secured by Dell SonicWALL is much less susceptible to downtime or bottlenecks, so all aspects of patient care can proceed at the fastest rate possible. Providing patients with greater access enables them to take a more active role in managing their care. Patients can log on and check their test results, schedule appointments, reorder prescriptions, communicate with their physicians and more. Physicians have decision-support tools at their fingertips, helping them to make the best diagnosis and check prescription doses immediately. They can even securely connect to pharmacies to place the prescription order directly. When the patient arrives at the pharmacy, the prescription is ready and waiting for them.

Increased productivity

Dell SonicWALL blocks malware attacks that can bring down critical systems and applications. Dell SonicWALL can eliminate junk mail and phishing attacks from inboxes, allowing staff to collaborate productively over e-mail. With Dell SonicWALL technology, specialists can securely share diagnostic analyses with hospitals, clinics or caregivers anywhere in the world in real time, speeding implantation of best treatment, and eliminating unnecessary travel expenses. Continual data backup can enable recovery of critical information at its most current state to recover from disasters or other operational disruptions.

Accelerated revenue streams

With Dell SonicWALL protection, insurance claims can be securely submitted online. Codes are automatically attached to procedures to ensure that the submission is accurate. Supporting documents can be securely sent as well. Eliminating errors and incorrect codes means being reimbursed on the first submission and eliminate as much as 30 days or more from the payment cycle.

Streamlined regulatory compliance

Ensuring the security of patient and financial information is one of the key pressures facing healthcare organizations today. With all the confusion and hype around HIPAA (Health Insurance Portability and Accountability Act), many healthcare organizations simply don't know what they need to do. The good news: by implementing a complete Dell SonicWALL security solution, you can transcend the technical requirements of HIPAA and set the foundation for realizing real business benefits.

Lower operating costs

Making staff more productive by eliminating or automating as many administrative tasks as possible is the key to more cost-effective resource utilization. Connecting systems, partners, pharmacies and ancillary sites in the healthcare community over a secure network helps achieve that goal. Providing staff with secure remote access from home and on the road allows them to stay on top of their workload when they're out of the office.

Greater staff retention

Dell SonicWALL adds flexibility back to the lives of physicians and healthcare staff, giving them the ability to leave the office in time to catch a child's ball game or just eat dinner with the family. They no longer need to be tied to their desks to get their paperwork done. They can securely access the files and resources they need from home at any hour of the day. Support functions like transcription can also be conducted by home-based personnel living wherever they choose, opening up the pool of resources available to healthcare professionals.

Summary

It is widely recognized that information is critical to the treatment of any patient. Giving caregivers access to that information anytime from anywhere can yield important productivity gains. But users need to be sure that the information will be accurate, timely and confidential. Dell SonicWALL provides comprehensive solutions to meet all these needs and securely extend the reach of the healthcare community.