

Medical Center Boosts Security to Deliver Excellent Care

Blessing Hospital uses security and wireless solutions to protect vital clinical information and deliver exceptional patient care.

EXECUTIVE SUMMARY

Blessing Hospital

- **Industry:** Healthcare
- **Location:** Quincy, Illinois, United States
- **Number of Employees:** 2700

Challenge

- Provide stronger, more reliable protection against malicious code and network attacks
- Extend clinical applications and information to the bedside
- Improve application performance at remote clinic sites

Solution

- Replace previous security technologies with more robust solutions.
- Implement secure, highly reliable wireless infrastructure
- Equip remote sites with platforms offering integrated security, remote connectivity, and application acceleration services

Results

- Improved visibility into security state of the network at all times
- Improved accuracy and efficiency of clinicians at the bedside
- Enhanced application performance in the data center and at remote clinic sites
- Enable company and key executives to maintain and benefit from established working relationship.

Business Challenge

Since 1875, Blessing Hospital has served as the premier regional hospital and trauma center in Western Illinois. Now encompassing a second hospital and several small satellite clinics, Blessing Health System today serves approximately 100,000 patients each year. As the first choice for patients throughout this large, rural region, Blessing Hospital is committed to providing the highest-quality care. An important part of that commitment is helping ensure that vital clinical information systems are protected from downtime and that confidential patient information is secure. To that end, Blessing Hospital always strived to provide strong network security. By 2007, however, the organization was outgrowing its network defenses. Even with security solutions in place, the hospital still occasionally fell prey to back-door malicious code intrusions and network attacks.

“Our previous IPS (intrusion prevention system) solution, an open-source application, was very difficult to manage and not always reliable,” says Kevin Rainey, senior network administrator at

Blessing Hospital. “It was very difficult to get updates, and we had issues with our sensor failing periodically. We would have to monitor every day, and constantly watch the alerts and logs to see if it was functioning correctly.”

Beyond the security issues, the network defenses provided limited logging and reporting capabilities. This made compliance with regulatory standards, such as the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry (PCI) requirements, a significant operational challenge.

“Cisco is the number-one market leader in network and security solutions, and it’s hard to imagine working with anyone else. If there is something we need to do that other vendors can’t support, we know Cisco can do it for us.”

— Kevin Rainey, Senior Network Administrator, Blessing Hospital

“Every month we do a security scorecard, which includes making sure our software is all patched and up to date, and that all security incidents are logged,” says Rainey. “That meant going out and scanning all of our 2000-plus systems, which took a lot of time and resources.”

In addition to these concerns, Blessing Hospital was planning to roll out a new electronic medical record (EMR) application that would allow clinicians to access patient information and clinical tools at the bedside. For the implementation to succeed, the hospital needed a secure, reliable, and manageable wireless network infrastructure.

Blessing Health System was also searching for a way to enhance connectivity with its satellite locations throughout the region. These facilities relied on clinical applications as much as on-site hospital employees did, and accessed patient records and other data services from the Blessing Hospital data center. Supporting these requirements consumed a large amount of Blessing Hospital’s wide-area network (WAN) bandwidth, and application performance at the remote sites was often poor.

Solution

To address all of these issues, Blessing Hospital turned to Cisco. The hospital had long relied on Cisco® routers, switches, and security appliances. Based on the hospital’s experience working with Cisco and its confidence in Cisco technologies, the hospital’s IT leaders entrusted Cisco with the entire network and security overhaul.

“Cisco is the number-one market leader in network and security solutions, and it’s hard to imagine working with anyone else,” says Rainey. “If there is something we need to do that other vendors can’t support, we know Cisco can do it for us. There is also a high level of comfort in knowing that so many consulting companies and integrators in our area have chosen Cisco to be their vendors, and provide expert support for Cisco products.”

Blessing Hospital turned to Burwood Group, a Cisco Gold Partner based in Chicago, to provide expert guidance throughout the implementation. The hospital’s IT group had worked with Burwood in the past and found the technology integrator to be highly competent and professional.

“Burwood Group’s engineers are top notch,” says Rainey. “You ask them a question, and they immediately know the answer. We’ve never worked with a Burwood technician who didn’t intimately understand the architectural and product issues at hand.”

Securing the Network

To replace Blessing Hospital’s older Cisco PIX firewalls and its third-party IPS solution, the hospital deployed Cisco ASA 5500 Series IPS Edition Adaptive Security Appliances with integrated IPS modules. The solutions combine industry-leading Cisco firewall and virtual private network (VPN) technology with adaptive intrusion defenses into a single platform.

“The Cisco PIX solutions did a very good job for us, but the Cisco ASA platforms take it one step further,” says Rainey. “They react to changing network conditions and threats, and they have multiple feature sets built in, which makes administration easier.”

The transition from the Cisco PIX solution to the ASA platforms proved to be a painless, straightforward task.

“We were able to basically copy and paste our configurations from the Cisco PIX firewalls into the ASA platforms,” says Rainey. “The IPS configuration was also very smooth. We ran it in monitoring mode initially, and then fully implemented it inline after a few weeks. We’ve had absolutely no issues with it since.”

Boosting Application Performance at Remote Sites

To enhance connectivity with regional clinics, the organization replaced the firewall and VPN termination equipment at those sites with Cisco 3845 Integrated Services Routers. The solutions provide robust network security with integrated Cisco IOS[®] Software firewall features, as well as secure VPN connectivity with the Blessing Hospital data center. As part of the overhaul, Blessing Hospital redesigned the network topology to take advantage of Cisco IOS Software-based Dynamic Multipoint VPN (DMVPN) capabilities. Instead of requiring every remote clinic to route all traffic through the central data center, clinics can now dynamically build VPN connections and communicate directly with each other over the Internet.

The Cisco remote-site platforms also include Cisco Wide-Area Application Services (WAAS) Software, a powerful application acceleration solution that allows remote clinicians to access vital information and services even over slower Internet connections. Back in the Blessing Hospital data center, the organization also uses the Cisco ACE Application Control Engine Module to provide intelligent load-balancing and content-switching services that boost application performance and help the hospital make the most efficient use of data center resources.

Bringing Information to the Bedside

To support the new EMR application, Blessing Hospital deployed the Cisco Unified Wireless Network. Drawing on industry-leading wireless technologies, the solution provides exceptional reliability and performance, as well as the stringent security that a healthcare environment demands. Using the Cisco Catalyst[®] 6500 Series switch with Wireless Service Module (WiSM), Blessing Hospital network engineers can manage the entire wired and wireless infrastructure as a single system.

Results

Within just a few months of the network overhaul, Blessing Hospital and its satellite clinics were already realizing significant benefits. One of the biggest improvements has been the hospital’s newfound visibility into its security environment, and its improved ability to protect essential clinical systems and patient information.

“The Cisco IPS solutions give us a much more detailed view of our network, from the outside to the inside,” says Aaron Strong, security compliance analyst at Blessing Hospital. “For example, we were able to recognize that one server in our network was getting bombarded with almost 10,000 intrusion attempts every day. Once we realized what was happening, we were able to block the source and knock the attacker out completely. Without the Cisco IPS solution, we never would have had that visibility.”

The Cisco security solutions also provide sophisticated management and reporting features that allow IT staff to operate more efficiently and streamline regulatory compliance reporting.

“The logging we get from the Cisco ASA solutions is tremendous,” says Rainey. “We get automated alerts from the system whenever there is an attack on our network, and we always know when it’s working. It has been extremely reliable.”

Beyond the improved security, the ability to combine multiple functions into a single device provides significant cost and operational benefits to Blessing Hospital.

“It translates to less complicated installations, less maintenance, and less administrative overhead,” says Rainey. “The integrated IPS capabilities in particular have had a major impact. If we had to use an external IPS solution, we would have had to build out our network capacity, at a significant cost. The Cisco ASA solution allows us to avoid that capital expense, as well as the ongoing operational expense of the added rack space, power, and cooling costs that separate appliances would require in our data center.”

Blessing Hospital is also realizing cost and efficiency benefits from the Cisco remote-site solutions and the Cisco IOS Software DMVPN capabilities.

“Using DMVPN is helping us realize significant bandwidth savings,” says Rainey. “With the ability for our clinics to communicate with each other directly, we expect to see a 25 percent drop in traffic traversing our data center.”

The most important benefit that Blessing Health System has realized, however, is the ability to provide an even higher level of care to patients. Thanks to the Cisco remote-site solutions and intelligent application acceleration tools, remote clinicians can now access the vital information and services that they need to care for their patients more reliably than ever before. At the hospital, the Cisco wireless infrastructure and EMR application are also helping to improve the safety and overall quality of care.

“The ability to use wireless computers in patient rooms really benefits our nurses,” says Rainey. “They don’t have to jot down notes or constantly walk back and forth to a central nurse station to access or enter information. They can do everything right at the bedside.”

Ultimately, the versatile Cisco solutions deployed throughout Blessing Health System are helping the organization deliver healthcare more securely and efficiently, and bring all of the benefits of state-of-the-art clinical care to patients across western Illinois.

Next Steps

Blessing Hospital continues to explore a variety of technology innovations to further improve the efficiency, security, and manageability of the clinical network. The organization is currently piloting the Cisco LAN Management Suite (LMS) and Cisco Security Manager (CSM), which will further streamline network administration, policy management, and regulatory compliance for the hospital. Blessing Hospital is also considering deploying the Cisco Security Monitoring, Analysis, and Response System (MARS) to serve as the network monitoring “nerve center” for the entire environment. Finally, the hospital is evaluating Cisco Security Agent, a host-based intrusion detection system that protects PCs and servers against both known and unknown attacks by blocking suspicious operating system behavior.

PRODUCT LIST

Routing and Switching

- Cisco Catalyst 6500 Series Switch
- Cisco Catalyst 3845 Integrated Services Router

Security and VPN

- Cisco ASA 5500 Series IPS Edition
- Cisco IOS Software Firewall

Wireless

- Cisco Aironet 1100 and 1200 Series Access Points
- Cisco Wireless Services Module (WiSM) for Cisco Catalyst 6500 Series Switch
- Cisco Wireless Control System

Data Center

- Cisco ACE Application Control Engine Module for Cisco Catalyst 6500 Series Switch

Application Acceleration

- Cisco Wide-Area Application Services (WAAS) Software

For More Information

To find out more about the Cisco security solutions visit: <http://www.cisco.com/go/security>.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)