Healthcare Provider Builds Secure Network from the Ground Up

Brooks Rehabilitation used Cisco solutions to build a new high-performance, highly secure network foundation.

EXECUTIVE SUMMARY

BROOKS REHABILITATION

- Healthcare
- Headquartered in Jacksonville, Florida
- Approximately 1300 employees

CHALLENGE

- Build high-performance and secure healthcare network
- Protect private patient information
- Streamline labor-intensive security audits

SOLUTION

- Implement new routing, switching, security and wireless solutions to create a Cisco Medical-Grade Network

RESULTS

- Improved protection of clinical applications and patient information
- Increased visibility into and control over network
- Improved operational efficiency and productivity

Challenge

Brooks Rehabilitation is a major provider of inpatient and outpatient rehabilitation services, serving thousands of patients throughout Florida and Georgia. The organization encompasses a state-of-the-art, 143-bed acute physical rehabilitation hospital, a research center, and 25 satellite outpatient clinics. Providing secure, high performance network services for such a large, widespread organization can be challenging enough on its own. Imagine building a new network from scratch while supporting two other disparate networks. That was the task before the Information Technology department at Brooks Rehabilitation.

Previously, Brooks Rehabilitation had two separate networks. One network was managed by Brooks, and the other network shared services with another medical facility, Memorial Hospital. Memorial's IT department managed some of the network needs for the Brooks organization. In 2006, however, Brooks Rehabilitation decided to migrate all services from both networks to one unified network that was flexible enough to handle both current and future needs of the organization. That meant building a new network, virtually from the ground up while supporting daily business needs on the existing systems.

> "We have all of these solutions providing multiple layers of defense, and they are all linked together. We can maintain a clear picture of the overall health and security of our network and be able to know with confidence what is happening at all times. We didn't have that kind of visibility in the past."
> **—Michael Helinsky, Director of Information Technology Operations, Brooks Rehabilitation**

"In effect, we were starting up a multi-million dollar a year company from scratch while keeping the existing business running," says Mike Helinsky, Director of Information Technology Operations at Brooks Rehabilitation. "It was a huge team effort to pull the whole thing together."

The task presented a unique opportunity to create a brand new, state-of-the-art network infrastructure for the health system. The new network had to meet rigorous demands for security and manageability, while providing information at the point of care. Brooks Rehabilitation facilities use a variety of technologies: an electronic medical record, wireless devices to access information at the point of care, guest wireless access in the inpatient hospital, as well as the typical communications and financial applications on which any large organization relies. The organization needed a solid infrastructure foundation that could deliver outstanding performance for a variety of applications and that could protect private health information (PHI) in a multitude of environments.

Brooks Rehabilitation also had to help ensure that the network met rigorous Health Insurance Portability and Accountability Act (HIPAA) security compliance requirements. It had to support an efficient security logging and reporting process to streamline compliance with security audits. Helinsky was also looking for a comprehensive solution that would allow his staff to maintain visibility into the security state of the entire environment at all times. These were previously time-consuming, labor-intensive projects.

"We wanted to build our network with technologies that have been tested, tried, and validated in demanding healthcare environments," says Helinsky. "It had to be easy to support, highly secure, and cost-effective."

Solution

Brooks Rehabilitation was already using Cisco® platforms at its remote outpatient clinics, and the IT staff had previously used Cisco network solutions at the primary hospital in conjunction with the Memorial Hospital network. Based on the staff's experience working with Cisco, as well as an extensive review of the technology options, the organization chose Cisco to support the entire network overhaul.

"When I think about Cisco, the two words that immediately come to mind are reputation and scalability," says Helinsky. "Cisco is the industry standard, and I have had very good experiences working with them."

Building the Hospital Network

To serve as the backbone for Brooks Rehabilitation Hospital and the larger health system network, the organization deployed redundant Cisco Catalyst® 6500 Series switches with Firewall Services Modules and Intrusion Detection System Modules. The security services modules provide robust perimeter protection and advanced intrusion prevention system (IPS) intelligence to identify and block malicious threats. Since these capabilities are integrated into the fabric of the network itself, they provide pervasive protection.

To provide an additional layer of defense, Brooks Rehabilitation will be implementing Cisco Network Admission Control (NAC). The solution authenticates every user and device attempting to gain access to the wired network, providing critical protection in a busy hospital environment. The Medical-Grade Network with the layered security approach helps ensure proper access to data, without impeding clinical workflows. Cisco NAC also provides confirmation of endpoint security posture resulting in a reduced possibility for malware outbreaks, thereby saving the company time, money, and potential bad publicity from an outage due to these types of events.

To monitor security information throughout the wired and wireless environment, Brooks Rehabilitation uses the Cisco Security Monitoring, Analysis, & Response System (MARS). The solution provides Brooks IT employees with the network insight that they need to identify, correlate, and rapidly respond to any security threats, and serves as a central clearinghouse for security logging and reporting.

Brooks Rehabilitation also uses Cisco IronPort email and Web security to lock down the organization's email traffic and provide state-of-the-art defenses against constantly changing Internet threats. The Cisco IronPort S650 web security appliance closely inspects web and application traffic to guard against spyware and other threats from malicious web sites. The Cisco IronPort C150 email security appliance blocks spam and helps ensure that PHI cannot leave the health system via email.

Securing Information at the Point of Care

Brooks Rehabilitation uses more than 100 Cisco Aironet® 1200 Series wireless access points deployed throughout the hospital and satellite clinics to bring information and services to the point of care. The organization uses Cisco 4400 Series Wireless LAN Controllers and the Cisco Wireless Control System to manage and protect all wireless services.

These solutions optimize wireless application performance, encrypt confidential communications, and guard against threats such as rogue access points. They also feed security event information directly to the Cisco Security MARS, where Brooks engineers can view them as part of the overall security state of the entire organization.

Managing the Environment

To configure and manage the hundreds of devices across the Brooks Rehabilitation network, Helinsky's team uses CiscoWorks LAN Management Solution (LMS) and Cisco Security Manager (CSM). CiscoWorks LMS simplifies network configuration, administration, monitoring, and troubleshooting to help IT engineers work more efficiently and rapidly identify and resolve any issues. CSM simplifies the task of managing security across the large, dispersed environment by allowing Helinsky's team to configure all security devices and policies across the network from a single, centralized interface.

Results

Brooks Rehabilitation completed the bulk of the network overhaul in early 2008, and the organization continues to bring new network and security services online. Already though, Helinsky believes that the health system is more secure than ever before.

"The interoperability of all of our security solutions is a major benefit," he says. "We have all of these solutions providing multiple layers of defense, and they are all linked together. We can maintain a clear picture of the overall health and security of our network and be able to know with confidence what is happening at all times. We didn't have that kind of visibility in the past."

The Cisco network defenses are also allowing Brooks to take full advantage of state-of-the-art wired and wireless healthcare applications. For example, therapists can make notes, check patient histories, and update medical records using laptops and handheld devices at the point of care, providing more effective care without worrying about compromising confidential patient information.

As the nerve center of the new network environment, the Cisco Security MARS provides unprecedented visibility into and control over the Brooks Rehabilitation network. Those capabilities boost the efficiency of IT employees and provide substantial savings for the organization.

"The Cisco Security MARS shows us all of the security events happening on the network at a glance, and eliminates the need for my staff to look in 10 different places to find out what is going on," says Helinsky. "Without Cisco Security MARS, I would need to dedicate at least one staff member to focus solely on network security and log monitoring, and staff that role 24 hours a day."

PRODUCT LIST

Routing and Switching

- Cisco Catalyst 6500 Series Switch
- Cisco Catalyst 3500 Series POE Switch

Security and VPN

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco Catalyst 6500 Series Firewall Services Module
- Cisco Catalyst 6500 Series Intrusion Detection System Services Module (IDSM-2)
- Cisco Network Admission Control (NAC)
- Cisco Security Monitoring, Analysis, & Response System (CS-MARS)
- Cisco Security Manager (CSM)
- IronPort S650 Web Security Appliance
- IronPort C150 Email Security Appliance

Wireless

- Cisco Aironet 1200 Series Access Points
- Cisco 4400 Series Wireless LAN Controller
- Cisco Wireless Control System

Management

- CiscoWorks LAN Management Solution (LMS)

The Cisco Security MARS solution has also simplified Brooks Rehabilitation's annual security auditing process. "The Cisco Security MARS lets us take a historical view of our network and generate detailed reports covering everything from the previous audit to the present," says Helinsky. "To provide that information in the past required a lot of time and a major manual effort."

Ultimately, Helinsky believes that Brooks Rehabilitation's Cisco network foundation will allow the organization to deliver outstanding care across the entire health system, in a secure, scalable environment that clinicians and patients can trust.

Next Steps

In the coming months, Helinsky plans to expand the use of the Cisco IPS and Cisco Security MARS solutions to automate the Brooks Rehabilitation network's response to many security issues, allowing the network to dynamically shut down ports and intervene in security events. Helinsky also plans to extend Cisco NAC to the wireless environment and will implement an advanced Cisco Unified Communications solution, including IP-based voice services, unified messaging, web conferencing, and a Cisco IP contact center.

For More Information

To find out more about the Cisco solutions for healthcare organizations, 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.**

Printed in USA

C36-485738-01 03/09