Cisco Increases Patient Data Security for Healthcare Provider

Cisco engineers help Sentara deploy new Identity Services Engine to enforce security policies for patient records.

EXECUTIVE SUMMARY
SENTARA • Healthcare • Norfolk, Virginia, USA • 30,000 employees, 2,345 beds
CHALLENGE • Safeguard confidential patient data • Authenticate and authorize all legitimate devices and users for network access • Assign appropriate security policies for patient data and clinical devices
SOLUTION • Cisco Professional Services • Cisco Identity Services Engine
RESULTS • Smooth implementation of hospital-wide security policies • Compliance with security mandates • Knowledge transfer to in-house staff

Challenge

Since its founding in 1888, Sentara Healthcare has flourished using the latest technologies and practices to deliver outstanding medical services. Today, Sentara operates over 100 facilities, including 10 hospitals, and is a leader in heart, kidney, and stroke care. **Modern Healthcare Magazine** cites Sentara as the nation's most integrated healthcare system; it is the only provider in the top 10 for all 14 years of the magazine's survey.

Sentara relies on networked technologies to bolster its ability to provide excellent patient care, and found that it could reduce costs by replacing bulky computer pushcarts that caregivers move to and from patient rooms with mobile, thin-client medical devices. Staff could then move freely between patient rooms and use these compact devices from the patients' rooms.

This solution, however, required a new security strategy. Sentara had to identify and authenticate users and devices to help ensure only authorized staff access hospital networks. It also had to segment critical patient care devices such as infusion pumps and CT systems from clinical devices like its electronic medical records system, PACS imaging system, and financial solutions. Because FDA mandates require that only manufacturers modify medical device software for upgrades or develop security patches, Sentara had to prevent any inadvertent or unauthorized changes that could disrupt system functionality and/or affect the integrity of patient-related information.

"To meet our stringent security needs, Sentara needs to dynamically lock down every network port, so our staff, and only our staff, can move about our facilities and use medical systems," says Chad Spiers, director, Voice and Data Infrastructure Services, Sentara. "We can't let just anyone plug their own device into a port and access highly-confidential patient records. We must identify every device and assign it an appropriate level of security based on its functionality."

Solution

Sentara, along with Savant, a long-time strategic partner, initially considered the Cisco Network Admission Control (NAC) solution, which enforces security compliance on networks. However, they learned that Cisco offered a new-generation identity and access control policy platform to replace NAC - the Cisco Identity Services Engine (ISE). A Cisco engineer spent a week with the Sentara/Savant team, explaining how ISE enforces compliance and boosts security by deploying policies across networks. “For a new product, ISE is very mature,” says Spiers. “We gained confidence when Cisco offered its Professional Services to ensure a smooth implementation.”

Cisco Professional Services carefully outlined Sentara’s security requirements and supported Sentara/Savant engineers as they rigorously tested ISE at Sentara’s Norfolk data center for nearly four months. Satisfied that ISE would meet its needs, Sentara decided to launch the solution at its newly constructed 160-bed Princess Anne Hospital in Virginia Beach, Virginia. Cisco Professional Services validated relevant configurations and performed a code risk analysis and a readiness assessment to make sure that the hospital’s network was ready for a production deployment. The Sentara/Savant IT team next installed an ISE appliance at the hospital, and the platform went live with the rest of the network at the hospital’s opening in August, 2011.

> “Cisco Professional Services was invaluable. They…ensured we had everything we needed for testing and production.”
> **— Bill Fosket, network engineer, Savant**

“Cisco Professional Services was invaluable,” says Bill Fosket, network engineer, Savant. “They reduced our learning time and ensured we had everything we needed for testing and production.”

Results

With the help of Cisco Professional Services, Sentara deployed ISE to dynamically implement security policies, starting with patients’ rooms throughout the hospital, so only physicians and other authorized users have ubiquitous, 24-hour access to network resources. Using ISE, the hospital also permits patients and guests to access the Internet and allows vendors to access patient care devices, helping ensure medical services are always delivered without interruption.

“Testing resolved any issues, and ISE has proved rock solid, especially for a new product,” says Spiers. “Cisco gave us control over whom and what enters our network, enabling us to meet our security and compliance needs. ISE will offer excellent visibility into our wired and wireless networks, so we always know the status of every user, device, and port.”

> “We know we can count on Cisco Professional Services as we deploy new networked technologies to deliver superior healthcare.”
> **— Chad Spiers, Director, Voice and Data Infrastructure Services, Sentara**

Today, Sentara is deploying ISE at its hospitals, clinics, and physician offices to gain robust, policy-driven network security across its infrastructure, and the solution will scale to meet Sentara’s expected growth. Additionally, throughout the project, Cisco Professional Services educated and prepared Sentara’s IT staff, so that, in Fosket’s words, “everyone now has a strong understanding of how ISE works.” As a result, Sentara’s IT staff will likely install ISE and deploy policies at its other sites, avoiding the costs of outside providers.

"As more and more medical devices become IP enabled and Sentara increasingly relies on network connectivity, Cisco's expertise and solutions give us an infrastructure that is safe, secure, and always under our control," concludes Spiers. "We know we can count on Cisco Professional Services as we deploy new networked technologies to deliver superior healthcare."

For More Information

To find out more about the Cisco Security Professional Services, go to: http://www.cisco.com/go/securityconsulting.

To learn more about Cisco Identity Services Engine, visit http://www.cisco.com/go/ise.

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 C36-697119-00 01/12