Healthcare Provider Improves Data Security with Access Control

Sentara Healthcare relies on Cisco ISE for identity and access policy strategy

EXECUTIVE SUMMARY

- Healthcare: 2345 beds in 10 acute care hospitals, six outpatient facilities, seven nursing centers, three assisted living complexes, plus eight advanced imaging centers
- Headquartered in Norfolk, VA
- 35,000 endpoints; 3680 provider medical staff and three medical groups with 618 providers

CHALLENGE

- Segregate clinical data from consumer data, and clinical or medical devices from patient care systems, thereby protecting patient privacy

SOLUTION

- Best-in-class secure access solution for innovative healthcare organization
- Tight integration between Cisco SNSBU, Cisco Services, and a Cisco Certified Partner

RESULTS

- Narrowly defined access controls by device, system, user, access method, posture, and timeframe for patient data protection and network security
- HIPAA-compliant

Challenge

Sentara Healthcare, based in Norfolk, VA, is a healthcare industry leader and a technology innovator that continually looks at ways to improve patient care and streamline operations. Sentara's portfolio of care includes 2345 beds in 10 acute care hospitals, six outpatient facilities, seven nursing centers, three assisted living complexes, plus eight advanced imaging centers. More than 600 physicians are affiliated with Sentara, which offers an array of services, including health coverage plans, home health and hospice services, and rehabilitation/physical therapy services. Sentara is recognized for its advances in heart and kidney care, stroke care, and infection prevention.

Initially, Sentara's IT team looked to strengthen its security posture by segmenting and segregating clinical data from consumer data, and clinical or medical devices from patient care systems. After a review of best options with a Cisco team, including a Cisco Certified Partner, Sentara selected the Cisco® Identity Services Engine (ISE). As Sentara also planned to bring its new Virginia Beach, Va.-based Princess Anne Hospital online, the organization's leadership decided to further enhance its patient care services through quicker access to data, while maintaining Health Insurance Portability and Accountability Act (HIPAA)-compliant security designed to safeguard against unauthorized access to electronic protected health information (ePHI).

Given the trend toward lower-cost computing, data center virtualization, and consumerization of endpoints, Sentara decided to utilize thin client systems wherever patient services were delivered. This choice allowed ubiquitous but secure access to patient records and simpler charting for clinicians. Sentara also opted to utilize IP telephony for a richer set of communication services and a more flexible approach to telephony operations to streamline staff mobility between facilities. Recognizing that the types of devices accessing the network would constantly evolve, the IT team was determined to help ensure that it could securely differentiate services for both Sentara-managed endpoints and non-Sentara endpoints.

Key to the success of the project was the ability to offer access services, providing open ports in facilities where individuals could plug in. Segmenting clinical devices from patient care systems also was critical to address HIPAA patient security requirements.

Solution

In late 2010, Sentara then sought a solution that could meet identity and access policy needs with the ultimate safeguards in place. After researching different market options, Sentara learned that Cisco was working on a next-generation policy platform, the Cisco Identity Services Engine (ISE), a core component of the Cisco SecureX framework, a new context-aware security architecture to meet the needs of the new borderless enterprise. After learning about ISE's comprehensive services for endpoint access, robust architecture, and flexible deployment model, Sentara became an early adopter prior to the product's general availability.

Working with the Cisco Secure Network Services Business Unit (SNSBU), which is responsible for ISE, Cisco Services and a Cisco Certified Partner, Sentara set up a proof-of-concept to run through various use cases. Among those areas that were leveraged by Sentara were endpoint profiling, along with appropriate and dynamic access controls for its HP thin clients, IP phones, printers, medical devices, building systems, and security devices. Clinical devices in the mix included the electronic medical records (EMR) system, registration, radiology, and Picture Archiving and Communication System (PACS) imaging system.

> "Cisco ISE met our use cases with flying colors. Given our commitment to increase the level of care we provide through innovative uses of technology, we are excited to be working with Cisco as we extend the Princess Anne care model to other Sentara Healthcare facilities."
> **— Chad Spiers, Director, Voice and Data Infrastructure Services, Sentara Healthcare**

For direct patient care, Sentara needed to address the network access needs of hundreds of device types, including a GE Clinical electrocardiogram (EKG) machine, linear accelerator, Philips computed tomography (CT)-scan machine, Alaris infusion pumps, glucometers, and even temperature-monitoring probes for refrigerators.

The company was also interested in 802.1X access for Sentara-owned computing platforms, as well as a browser-based access control solution tied to its Active Directory infrastructure as a backup mechanism to help ensure Sentara-authorized users always have some degree of access. As an extra measure of security, the extended Sentara team looked to include port-level controls to prevent unauthorized access. Most importantly, the solution needed to provide high availability services to support a 24-hour hospital, as well as the entire health system.

PRODUCT LIST

TrustSec
- Cisco BioMed Network Admission Control (NAC) with Cisco Identity Services Engine (ISE)

Routing and Switching
- Cisco WS-C3750X-48P Access Switches

Security
- Cisco ASA Firewall

Wireless
- Cisco 3500 CleanAir

Management
- HP OpenView

Cisco Security Planning, Design and Implementation Services

The initial pilot was focused on patient rooms at Princess Anne Hospital. With system profiling under way at the hospital, the goal is to implement more fully Cisco ISE into additional locations, including corporate and medical offices, as well as its hospitals.

Results

According to Chad Spiers, director, Voice and Data Infrastructure Services, Sentara, "Cisco ISE met our high water mark for use cases with flying colors. We also are interested in seeing how Cisco evolves device profile feed services, given its longstanding relationship with leading healthcare device manufacturers such as

Philips, and GE."

"Given our commitment to increase the level of care we provide through innovative uses of technology, we are excited to be working with Cisco as we extend the Princess Anne care model to other Sentara Healthcare facilities," he adds.

Spiers points out that many of the devices used at Sentara are FDA regulated or vendor controlled, and although most are Windows based, some devices cannot be fixed by simple patching. The Cisco intelligent profiling provisioning capability has provided the Sentara team with assurance in securing their network. The team also is able to provide access to various constituents in a "time share" format, enabling entry during certain days and times of day to Sentara physicians vs. non-Sentara providers. The ability to provide specific access control policies by device, network pathway, and user is an important advantage for Sentara, says Spiers.

With the use of the Netflow collector, the Sentara team can also better analyze traffic to create the optimum security posture.

Spiers adds that the tight integration between the Cisco SNSBU and Cisco Services teams, along with a Cisco Certified Partner, was a positive experience for his Sentara team. The three groups worked alongside the Sentara team, with Cisco Services onsite through the proof-of-concept phase. The Cisco team met with Sentara to understand the organization's needs before providing specific guidelines and a workable architecture that would allow room for growth, including the addition of the Guest and Profiler components.

"Sentara is following the model from our latest Cisco BioMed NAC 2.0 solution, which is based on Cisco's Identity Services Engine," says Curt Mah, Cisco healthcare solution architect. "By extending access based on contextual identity information, healthcare providers can ensure that the correct access policy is applied dynamically to the correct device. This improves operational efficiency and better serves patients."

For More Information

To learn more about Cisco Identity Services Engine, visit http://www.cisco.com/en/US/products/ps11640/index.html.

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 C36-697117-00 02/12