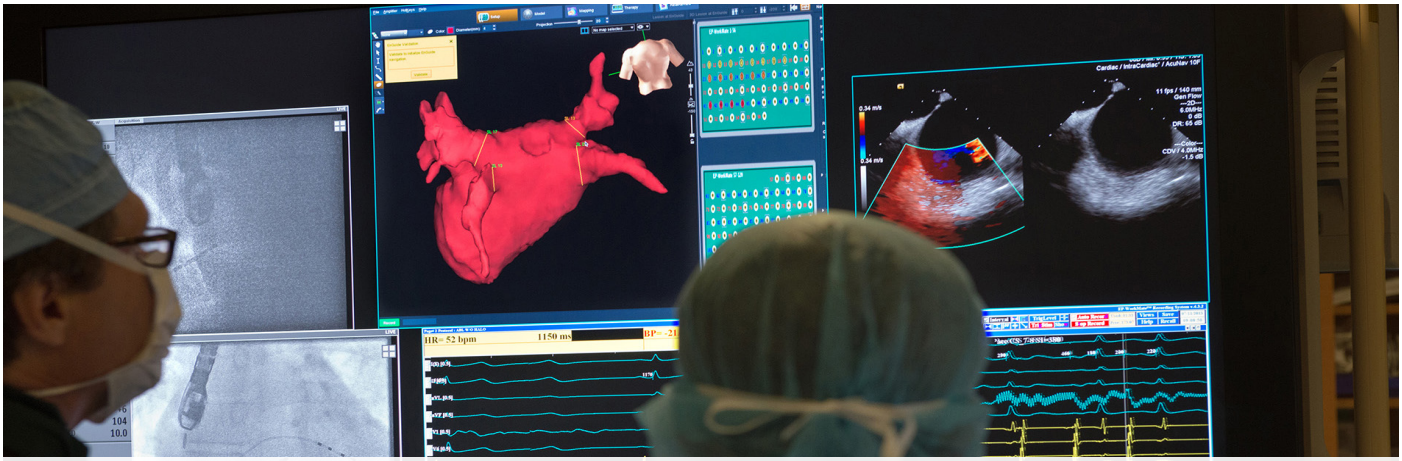

Protecting Digital Healthcare against Emerging Cyber Threats

Sentara Healthcare

Size: Nearly 28,000 team members

Industry: Healthcare

Location: Virginia and North Carolina, United States

Solutions

- Assure reliable healthcare services with Cisco Digital Network Architecture
- Enforce policies consistently across the network with Cisco TrustSec software-defined segmentation
- Control network access rights with Cisco Identity Services Engine
- Gain visibility and conduct real-time analysis of network traffic with Cisco Stealthwatch

Results

- Greater levels of protection for patients and healthcare workers
- Less chance of malware contagion between clinical systems and applications
- Faster threat response and remediation capabilities
- More time for IT to spend innovating and combating new risks

Hopes and Expectations

In this age of digitization, hopes and expectations for healthcare have never been greater. Not only to develop advanced clinical treatments, but also to deliver better patient experiences and outcomes.

For Sentara Healthcare that means doing more with less and providing a highly secure, digital care environment. With 300-plus care sites, including 12 busy hospitals, this is a constantly moving target.

"Connecting medical devices over the network, such as infusion pumps and patient monitoring systems, brings great advantages," says Director of Information Security, Chad Spiers. "But, by its very nature, it also widens the threat surface area and introduces new back door vulnerabilities."

As doctors and nurses increasingly transition away from illegible hand-written notes to using mobile medical devices, pressure grows on IT teams to make sure the right people have the right network access—and they are prioritized over guests and visitors.

Holistic Digital Strategy

Sentara's response was a far-reaching digital strategy. It's founded on Cisco routers, switches, and wireless access points, forming a Digital Network Architecture (DNA) infrastructure that allows hospital campuses and remote sites to collaborate safely and act as a single entity.

"Our Cisco network ensures we always have seamless wired and wireless communications between nurses, pharmacists, and other medical experts—with everyone connected to the correct patient data," says Spiers.

Staying Ahead of the Innovation Curve

Building on this solid foundation, Sentara took advantage of Cisco ONE™ Software for ongoing upgrades and instant access to the latest DNA security solutions. This allows the IT team to innovate and execute quickly, while reducing total cost of ownership by using portable licenses across multiple devices.

Cisco DNA security solutions are helping Sentara to:

Accelerate digital healthcare, safely and securely

Protect vital clinical systems and applications

Deliver better patient experiences and outcomes

"With Cisco ONE Software, we're no longer tied to managing individual appliances; it's now security with automated simplicity," says Spiers.

Rapid, Intelligent Threat Protection

To mitigate the risk of security breaches, the IT team used to spend time and expense continually compiling access lists, changing IP addresses and firewall rules, purchasing new hardware, and building virtual private networks (VPNs). "Network segmentation could take several months," says Spiers. "Now, with Cisco TrustSec and Stealthwatch threat response speed is almost immediate."

Introducing TrustSec and Stealthwatch has also greatly improved visibility into east-west cross-network traffic flows. With real-time analysis and alerts the IT team can see what is happening on the network and quickly spot suspicious traffic behavior, such as worm-like activity, or a hacker attempting to illuminate and map network resources. Should this situation arise risky traffic is immediately dropped and endpoints are isolated for further investigation.

Controlling Network Connections, Endpoints, and Access Rights

To embed security across the hospital campus, Sentara also decided to simplify access control. The Cisco Identity Services Engine (ISE) checks to make sure users and their devices are safe to connect to wired, wireless, and remote connections.

"With Cisco ISE we can see everything hitting our network–who, what, when, where, how, and why," says Spiers. "This adds context to ensure the right people are accessing the right information."

From one single console the IT team easily orchestrates network access–for guests, patients, administrators, and medical staff across the multiple campuses. Clinicians have special rights for data and services, compared to patients and visitors who can browse the Internet and stay in touch with friends and family. Similarly, Cisco ISE policy enforcement can be used to prevent medical teams from attaching to guest wireless networks that bypass security controls.

In addition, Sentara is able to segment and control access to critical-care devices, points-of-sale, building control systems, and other high risk endpoints, along with high value data such as protected health information and payment card details. If required the IT team can provide out of band Internet-only access with different levels of quality of service to patients, guests, and contractors, using the same Wi-Fi network deployed for medical equipment and staff.

Other benefits include quick, automated asset profiling and posture assessment to automatically patch or update Sentara devices when they connect or reconnect to the network. IT management is further improved through the ability to move assets quickly and easily between sites to respond to demand peaks, without the need to modify firewalls.

Risk has been reduced in other areas too. "With Cisco DNA security, it's simpler and less time consuming to satisfy Health Insurance Portability and Accountability, Payment Card Industry Data Security Standard, and other compliance requirements," says Dan Bowden, Sentara Vice President and Chief Information Security Officer.

"Our Cisco network ensures we always have seamless wired and wireless communications between nurses, pharmacists, and other medical experts—with everyone connected to the correct patient data."

Chad Spiers
Director of Information Security
Sentara Healthcare

Using the Network as a Sensor and an Enforcer

Sentara went a step further. The integration of Cisco ISE and Stealthwatch helped turn its network into a security sensor and enforcer. This approach has provided much deeper insight into traffic flows between virtual machines and applications.

As well as adding context to ensure the right people are accessing the right information, Stealthwatch helps uncover attacks that attempt to move laterally across the network, like the recent WannaCry ransomware worm. "Stealthwatch lights up our network traffic flows and flags, or automatically blocks suspicious activity. This gives us near real-time automated defenses against some forms of attack," adds Bowden.

Lowering the overall attack surface in this way prevents the movement of threats across the network, and minimizes the time taken to isolate them. Moreover, it safeguards critical machines running on the network, which left unsecured could result in major patient safety concerns.

Complete Invisibility is the Measure of Success

Unlike before, the IT team can apply security policies on the spot to things like patient databases, scanning applications, and drug management tools. These policies protect the network across wired and wireless devices.

The investment in Cisco DNA security solutions paid back in other ways as well. Sentara completed a full network refresh—securing 140 physical locations and 45,000 endpoints in just 14 months. That result would have been out of reach with the old approach.

As the threat landscape changes at breakneck speed, Spiers acknowledges that 100 percent risk mitigation is an unattainable goal: "It's more about doing the right things, at the right time, and adopting a tightly integrated security strategy," he says. "Get that right and you greatly reduce the chances of a full outbreak."

Increasing automation, through its Cisco network and complementary security suite, has helped simplify compliance and lower the risk of human errors. In addition, the IT team has much-needed headroom to focus on future improvements and keep on top of threat intelligence and emerging risks.

In many ways the biggest measure of success has been the impact at the frontline. "The IT security upgrades have remained completely invisible to our patients, doctors, and medical teams," concludes Spiers. "That's exactly how it should be."

For More Information

To learn more about the Cisco solutions featured in this case study, visit

www.cisco.com/go/customerstories

www.cisco.com/go/dnastories

www.cisco/go/security

www.cisco.com/go/dna.

Products and Services

Security

- Cisco TrustSec
- Cisco Identity Services Engine
- Cisco Stealthwatch
- **Routing and Switching**
- Cisco Catalyst 3650 and 3850 Series Switches

Licensing

- Cisco ONE Software

Wireless

- Cisco Aironet 2700 and 3700 Series Access Points

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.**