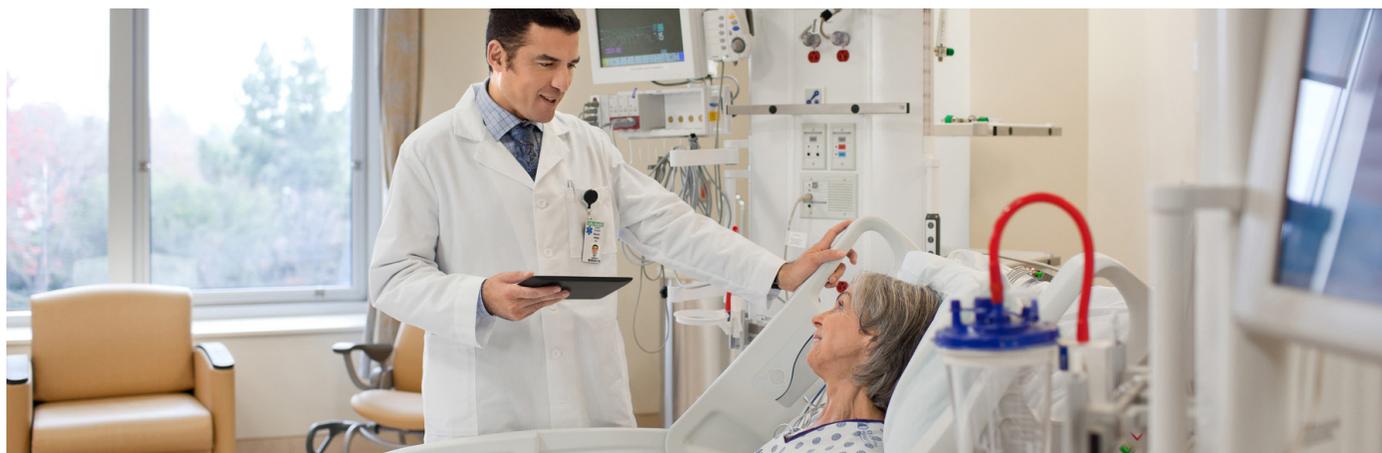# Hospital System Protects Critical Medical Infrastructure

EXECUTIVE SUMMARY

Customer Name: Houston Methodist
Industry: Healthcare
Location: Houston, Texas
Number of Employees: 20,000

Challenge:
- Lacked insight into who and what was connecting to the network
- Unable to effectively monitor and control access to sensitive hospital infrastructure
- Devices not properly configured or secured

Network Solution:
- Cisco® Identity Services Engine (ISE)
  - Secure access
  - Advanced device profiling and discovery
  - Device and user context

Houston Methodist Deploys Cisco Identity Services Engine for Secure Access

Houston Methodist is a nonprofit healthcare organization based in Houston, Texas. It consists of seven hospitals, a research institute, and 20,000 employees, including more than 4,500 physicians. The organization's flagship facility, Houston Methodist Hospital, is consistently ranked among U.S. News & World Report's best hospitals.

Security Challenges

With so many devices connecting to its large, distributed network, Houston Methodist needed a reliable way to keep track of all these assets and grant each one proper, secure access. The security team was responsible for monitoring and protecting a wide variety of devices including PCs; mobile phones and tablets; medical devices such as X-ray, ultrasound, MRI machines, and infusion pumps; and other infrastructure such as facility security cameras. As a healthcare provider, security is paramount to the success of Houston Methodist – with life-saving machines, confidential patient records, intellectual property, and billing systems all under the jurisdiction of the IT team.

Several years ago, the hospital system was challenged by many vendors coming into its facilities and finding ways around security safeguards to connect devices to the network without the proper authorization. Once they were connected, the security team had no way of knowing that the devices were there, who they belonged to, what they were doing, or what type of security they had.

Results:

- Expanded knowledge surrounding network devices and users
- Ability to control which users and machines can obtain network access
- Greater protection for critical, life-saving medical equipment and confidential patient records

"ISE has solved our network access problems. Now, we only allow devices on the network that are supposed to be on there."

Saqib Malik
Network Architect, Houston Methodist

"ISE has helped us correlate a lot of security information from disparate tools, which helps us identify various devices on the network and determine who manages them."

Omar Zaman
Senior Network Engineer,
Houston Methodist

Secure Access with Cisco ISE

After evaluating several products, Houston Methodist chose the Cisco® Identity Services Engine (ISE) to help provide secure access and insight into who and what was connecting to its infrastructure each day. In addition to better controlling access to its network, Cisco ISE also helps Houston Methodist with device discovery and profiling. When the hospital system first started using ISE, they had 2,000 unknown devices on their network – meaning devices that were not properly categorized to fall under a specific security policy. After just a couple of days with ISE, Houston Methodist reduced this number by 85 percent.

According to Houston Methodist's senior network engineer, Omar Zaman, "ISE has brought to the surface problematic machines that needed to be reimaged or rejoined to their respective domain, for example, so that they could get the appropriate security updates."

As a result of this device profiling capability, Houston Methodist was able to fully deploy ISE with almost zero downtime.

"ISE has also solved our network access problems," said Saqib Malik, network architect for Houston Methodist. "Now, we only allow devices on the network that are supposed to be on there. We are able to use the proper authentication and authorization needed to keep our network protected, and can deny access to vendor machines that do not have the appropriate security technologies installed."

"ISE has helped us correlate a lot of security information from disparate tools, which helps us identify various devices on the network, determine who manages them, which switches and ports they are plugged into, and so on," Zaman added. He explained that managing ISE gets easier as time goes on, because the technology begins to recognize specific device types and learns which ones it should and should not allow on the network.

Houston Methodist is currently protecting over 8,500 endpoints with Cisco ISE, and is planning to expand the implementation to cover over 50,000 devices in the near future.

Comprehensive Security

Houston Methodist also chose ISE because it is part of the comprehensive Cisco Security portfolio.

"It will be a lot easier to have ISE working with all the other tools available through Cisco," said Malik. "We can turn to the same vendor to provide support for everything, and we can more smoothly integrate our various security tools."

In addition to ISE, Houston Methodist is currently using Cisco next-generation firewalls and the Cisco Meraki MX60W for security, and looks forward to managing all of these devices through a single pane of glass in the future.

The hospital system is also planning to expand its Cisco Security portfolio with the addition of the Cisco Stealthwatch™ solution and Cisco TrustSec® technology.

"Initially, we were looking at TrustSec technology as a means of separating our credit card processing traffic from the rest of our network for PCI compliance," said Malik. "But, the more we looked at it, we realized that combining Cisco ISE, TrustSec, and Stealthwatch could also greatly expand our network visibility and deliver to us the security-centric network we are looking to achieve. By leveraging our network as a security sensor, we will be able to automate threat detection and quarantining, and dramatically reduce the need for manual threat analysis and mitigation."

The Houston Methodist representatives also noted that the Cisco team has been very helpful and supportive throughout their journey. Zaman said that the team regularly checks in with him and his colleagues to see if they have any issues.

Houston Methodist is now better positioned to protect its critical, life-saving medical equipment, sensitive intellectual property, and confidential patient records.

To find out more about Cisco ISE, go to: http://www.cisco.com/go/ise.