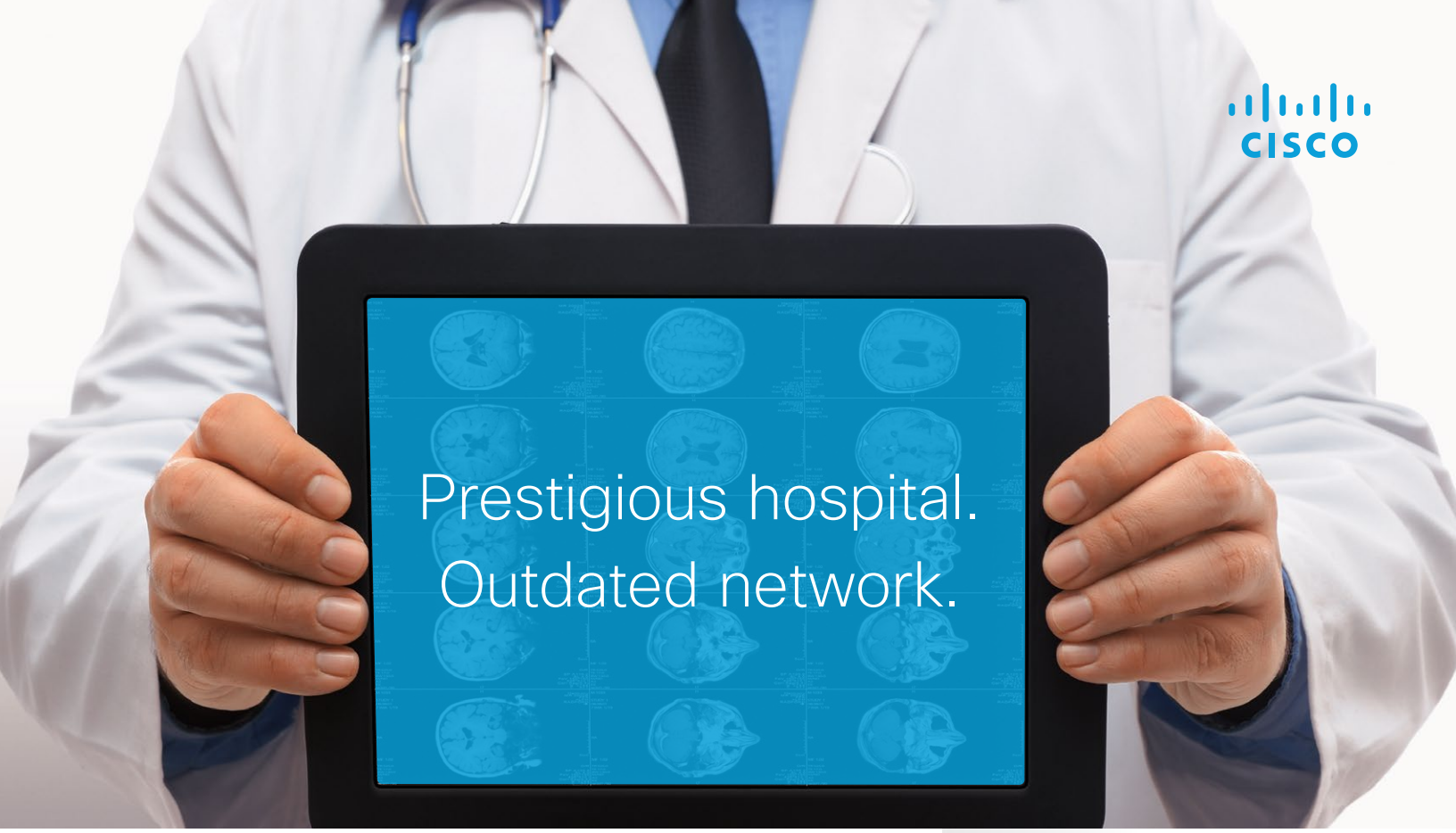


What happens when a cutting-edge medical center suffers from outdated network security?

It's possible to lead the world in an industry—medicine in this case—and to simultaneously lag behind when it comes to network security. One large national hospital system faced serious IT challenges. Network investment had been put off to the point of opening critical security vulnerabilities. A massive attack surface and limited visibility meant a threat could penetrate the network and remain hidden for months. It put critical systems, employees, patients, and the hospital's reputation at risk.

> "We have done ourselves a disservice by letting our network infrastructure degrade to the point where it can no longer support business services."
>
> — Customer statement

CHALLENGE

- Secure 500 sites and thousands of devices.
- Enable network segmentation for HIPAA and PCI compliance.
- Gain visibility and control over threats.

SOLUTION

- Architectural network refresh along with security implementation
- Network as a sensor (NaaS) and network as an enforcer (NaaE)
- Cisco IOS® NetFlow, Cisco® Identity Services Engine (ISE), Cisco StealthWatch®, and Cisco TrustSec® solutions
- Cisco consulting services for guidance at every step

RESULTS

- Prevents lateral spread of advanced threats with network segmentation
- Provides deep visibility for better access, policy, and control
- Delivers improved safety and accessibility of patient information

Problem

Several factors combined over time to put this hospital especially at risk.

A flat network

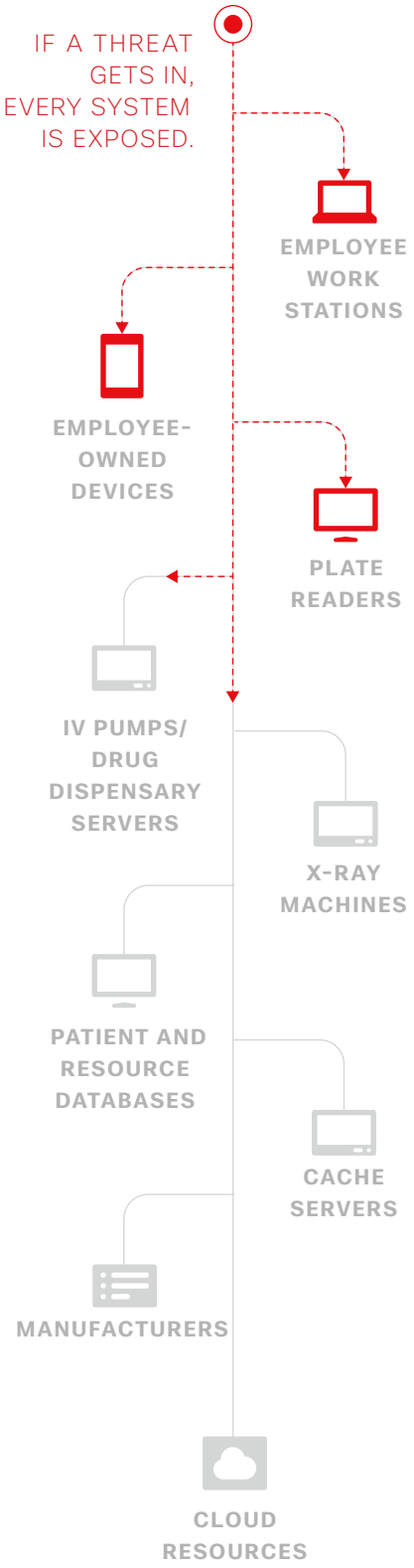
The hospital's aging network infrastructure—including outdated switches—left it open to threats. Most hospital networks have parallel networks that separate clinical systems, research facilities, guest access, and administration. In theory, different networks should never touch each other.

However, this hospital had a flat network without separation or network segmentation. Rather than separating by function, VLANs were assigned by floor. Doctors, staff, students, and medical equipment shared the same network, multiplying the attack surface and exposing the hospital to threats. Gaining visibility into suspicious behaviors on the network was challenging, and ensuring compliance with HIPAA and other regulations was a struggle.

Device overload

The hospital had more than 15,000 nonupgradable endpoints, and many of them were interconnected. Heart machines, lung machines, proton-beam therapy machines, and others were connected to the network and even to the Internet.

The hospital needed to gain control of its flat, exposed environment. Some endpoints were running versions of MS-DOS that had been installed as far back as 1992, leaving the network vulnerable to advanced or sophisticated threats. More than 600 Windows NT4 devices and nearly 7000 Windows XP devices on the hospital's network suffered from end of support, lack of patches, and an inability to run current antivirus software. To make things more difficult, FDA approval required devices to remain as originally shipped from the manufacturers, so a system upgrade could mean noncompliance.



A patchwork of unsuccessful solutions

IT had tried to make things work. They segmented the network using traditional models. They patched and established VLANs. They even tried transparent firewalls to limit user access to appropriate files and resources without much success. Buying new devices would mean spending lots of money without solving the underlying issues. The team faced a harsh reality: They needed more visibility, insight, and control, while meeting compliance guidelines.

> "The client asked, what percentage of the infrastructure could even do policy segmentation today? The answer: less than 10 percent of their current network."
>
> – Cisco consultant

Fixing the problem

Third-party consultants, hospital IT professionals, and hospital executives agreed that something had to be done, and that they should step back and look at security holistically. The right strategic approach was to find a way to understand how the applications, users, and devices were connected and to put network controls in place.

Cisco security consultants led a 2-week workshop with engineers, business analysts, and executives. Concluding that the hospital needed a more advanced network that could support segmentation, the team crafted a high-level network design, an 18-month rollout plan, and a detailed governance model. The most intelligent approach was to use the architecture supporting the network (NetFlow) to link its security and networking together.

The plan was simple:

- Upgrade legacy switches, routers, and wireless technology to incorporate key security solutions including NaaE and NaaS, allowing for visibility, segmentation, and control.
- Engage the Cisco Advanced Services team to ensure a successful implementation within the allocated time.
- Standardize the process for adding new components onto the network.

Solution

Cisco secures the network.

Cisco NaaS turns your network into a threat monitor or sensor. It includes NetFlow technology, which is already embedded into most Cisco IOS networking devices; Cisco StealthWatch solutions; and the Cisco Identity Services Engine (ISE).

- Cisco IOS NetFlow was created by Cisco to provide visibility into the network. NetFlow tracks every network conversation with a record that includes source, destination, timing, and protocol information for deep visibility. It can tell who is talking to whom, with what, from where, and for how long, including how much data was exchanged, storing months of information.
- Cisco StealthWatch adds threat intelligence through analytics to NetFlow data to accelerate response. The Cisco StealthWatch solution can analyze network audit trails, identify anomalous activity, and zero in on the root causes of attacks. With the solution, you can detect network traffic flows and behavior associated with advanced persistent threats (APTs), distributed-denial-of-service (DDoS) attacks, and insider threats.
- Cisco ISE provides contextual data including who, what, where, when, and how users and devices are connected and accessing network resources.

Cisco NaaE enforces security policies. It extends capabilities by activating Cisco TrustSec technology already embedded in Cisco ISE.

- Cisco TrustSec technology works with ISE to contain the scope of an attack. Cisco TrustSec technology uses security group tagging to create virtual network segmentation, and ISE enforces policies across the segments. Segmentation allows for quarantining of threats to limit malicious activity.

> “If there’s a physician in a remote clinic who is accessing a ton of records at 5:30 p.m. after the clinic is closed, this is abnormal.
>
> If I have NetFlow enabled, this will be flagged.”
>
> – Cisco consultant

These solutions not only help the hospital identify threats, but also help it understand legitimate data flows and logical traffic groupings to determine network segmentation.

Cisco TrustSec technology can be integrated easily with newer switches, access points, and firewalls. With Cisco TrustSec solutions, the hospital doesn't need to worry about the IP addresses. It can focus on classification. And the clarity provided by NetFlow allows the team to develop a set of rules that make sense. ISE creates user policies and puts users into groups. Granular business and policy rules allowed the hospital to enforce access, enabling the appropriate communications for the appropriate devices.

It is vital to be able to isolate medical equipment and data from the rest of the network so the hospital can prevent attacks by enforcing segmentation and user access. Now even if attackers get in, their access is limited to one network segment.

Results

Bonus benefit: Outstanding security drives innovation.

- Employee satisfaction
- Productivity
- Quality research
- More meaningful patient experiences

Beyond the immediate security and compliance benefits, the hospital had witnessed a significant unexpected benefit: operational efficiency. They have reduced manual updates, human error, and repetitive tasks, and the network team can now quickly identify application, server, and network performance issues.

The new agile network gives patients and employees what they want most: security, speed, availability, and improved services. It is the foundation for other future technologies. With security covered, the hospital can begin rolling out new applications that connect employees with each other and with patients in innovative ways. New mobility, information-sharing, and collaboration applications have potential to further streamline operations.

To learn more about these Cisco solutions, visit cisco.com/go/networksecurity.

TECHNOLOGY BENEFITS

- Security woven in at every level—switches, routers, and access points
- Upgraded network architecture across the hospital
- Deep and broad visibility into unknown devices and unusual traffic patterns
- Authentication of users and devices
- Enforced policies across wired, wireless, and VPN topologies

BUSINESS BENEFITS

- Keep current with constant waves of new users, devices, and applications.
- Reduce manual updates, human error, and repetitive tasks.
- Easily comply with audits for HIPAA, PCI, and other regulations.
- Reduce downtime costs and liability.
- Ultimately deliver more accurate and reliable patient care.

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**.