XenTegra | cisco Partner

Case Study: How a Major New York Children's Hospital Turned a Rogue Laptop Scare into Zero Trust Reality

At a Glance

Organization: Major New York Children's Hospital (Anonymous)

Industry: Healthcare / Operational Technology (OT)

Environment: Hybrid Cisco network with Cisco Identity Services Engine (ISE), Cisco Secure Connect, and thousands of clinical IoT devices.

The Engagement: A high-impact security remediation project focused on Cisco Identity Services Engine (ISE), Cisco Secure Connect, and wireless policy enforcement.

The Challenge

The hospital had strong security tools in place, but a startling incident revealed they weren't working as intended. A hospital administrator, seeking a better connection for their personal laptop, plugged into a patient room wall jack and immediately gained full administrative access to the entire network.

The root cause was not a failure of hardware, but of process. Years of staff turnover and band-aid fixes had created a silent accumulation of misconfigurations known as "Technical Knowledge Debt."

> ***The number one enemy of networks for the most part is not black hat hackers...it is actually your own network and technical knowledge debt. That technological debt adds up until it bites you.***
>
> — LeeAnn Larson,
> Security Solutions Architect at XenTegra

The Solution

The hospital needed more than a report; they needed a fix. XenTegra was engaged to perform a surgical, month-long remediation of the identity environment.

Using a proven engineering framework, XenTegra:

- Identified the specific gaps in port-level security.
- Consulted subject matter experts to ensure patient care would not be disrupted.
- Resolved the drift between Cisco ISE policies and on-premise enforcement.
- Validated the security posture by physically attempting to break it.

Outcomes

The engagement transformed the hospital's network from a liability into a fortress of Zero Trust.

- **Absolute Rogue Blocking**: Unauthorized devices can no longer connect to the network. Attempts to plug in unmanaged devices are now instantly identified and blocked.
- **Modernized Posture**: The hospital is now operating with "up-to-date bleeding-edge industry best practices," ensuring their security evolves as fast as the threats do.
- **Verified Security**: The client has moved from assuming they are secure to knowing they are secure through physical validation and ongoing pen-testing services provided by XenTegra.

The Full Story: From Rogue Laptop to Systemic Risk

When a hospital administrator plugged a personal laptop into a patient room jack, they unexpectedly gained full administrative access, bypassing all identity checks.

This wasn't a hardware failure, but a symptom of "Technical Knowledge Debt." XenTegra found that years of turnover and band-aid fixes had left the environment riddled with silent risks:

- **Legacy SSIDs** for medical devices were broadcasting in the clear.
- **Pre-shared keys** had not been updated in years.
- **"Ghost" Users** lingered in Active Directory long after departure.

While the hospital had a Zero Trust roadmap on paper, configuration drift was actively eroding security in practice.

XenTegra's 5-Step Remediation Process

The XenTegra team utilized their proven engineering framework: Identify, Research, Discover, Resolve, and Validate, to turn a chaotic vulnerability into a structured Zero Trust environment.

1. **Identify: Defining the Behavior**
   The team analyzed the discrepancy between expected and actual network behavior, pinpointing a critical failure in identity enforcement that allowed dormant ports to bypass security controls.
2. **Research: Consulting the Experts**
   To protect patient care operations, engineers reviewed historical configurations and consulted external experts to validate the remediation strategy before touching a single setting.
3. **Discover: Data Gathering**
   XenTegra conducted a holistic audit of every switch and access point, uncovering critical gaps like unmanaged legacy SSIDs and significant policy drift across the hybrid environment.
4. **Resolve: 42 Hours of Policy-by-Policy Tuning**
   In a 42-hour surgical engagement, the team executed a policy-by-policy overhaul of Cisco ISE to update credentials, remove ghost users, and enforce strict Zero Trust alignment.
5. **Validate: Physical Rogue Testing**
   Moving beyond dashboard verification, the client physically tested ports and Wi-Fi across the facility, confirming that unauthorized rogue devices were now instantly blocked.

Why This Story Matters for Healthcare IT Leaders

For overloaded IT and security teams, this story is familiar: tools are in place and projects are completed, but over time, staff turnover and unplanned growth create identity risks that are hard to see until something goes wrong. XenTegra approaches these environments with a critical understanding: Healthcare is Operational Technology (OT). "Nobody treats healthcare like it's operational technology," notes Larson. "Hospitals have smart beds...they are just as hackable as a little programmable logic controller in a factory."

Because smart beds, IV pumps, and imaging systems all ride the backbone, technical debt is not just an IT problem, it is a patient safety risk. A failure in identity enforcement puts these clinical devices at risk of lateral movement attacks. XenTegra specializes in uncovering and resolving this hidden risk, ensuring that Cisco ISE, Secure Connect, and clinical networks work together without fail.

Next Step: Uncover Your Hidden Risks

Visit **xentegra.com/core-networking-assessment/** to turn Zero Trust into operational reality.

Don't wait for an accident to expose your vulnerabilities. Schedule a complimentary Secure Networking Assessment from XenTegra to:

- Identify hidden configuration drift and technical debt.
- Validate Cisco ISE and Secure Connect policy enforcement across wired, wireless, and medical devices.
- Get practical remediation plans that prioritize patient care.