Filling the Medical Device Security Gap

Reducing the risk of cyberattacks with a zero-trust architecture

Dayton Children's is a US$600 million pediatric integrated delivery network with an acute care teaching hospital, two primary campuses, and another 20 ambulatory care sites.

Dayton Children's believes that cybersecurity is a key part of its commitment to the relentless pursuit of children's health. That's why it is committed to a zero-trust architecture.

Significant organizational growth in the last 10 years came with a proliferation of connected devices, especially Internet of Things (IoT) devices, Internet of Medical Things (IoMT) devices, and increased Bring Your Own Device (BYOD) adoption. There are approximately 25,000 devices on the hospital's network. These include not only smart TVs and security cameras, but also critical medical devices like X-ray machines, MRI machines, and robots that aid in neurosurgery.

While connected medical devices are key to the patient care journey, more connections mean greater risk. Medical and IoT devices are some of the lowest hanging fruit for malicious actors due to legacy operating systems associated with FDA certified devices—some of which cannot support modern endpoint protection software. Providing superior medical care requires solving for patient safety, and that includes controlling access to those devices on the network. With patient information and medical and IoT devices working in tandem to provide better care for sick children, the impact of an attack on medical devices could cost lives.

Like many health systems, Dayton Children's has limited money, time, and people to devote to cybersecurity. But it realized it could gradually implement a zero-trust architecture to improve patient care while reducing organizational risk at relatively low cost.

Zero-trust architecture helps secure the entire network

Zero trust is an approach to cybersecurity that validates every stage of a digital interaction based on the principle of "never trust, always verify." Whether it's an intravenous pump or a camera, Dayton Children's Chief Information Security Officer Nicholas Schopperth's goal is to limit that device's network access to specific IP addresses.

By moving to a zero-trust architecture, Dayton Children's could segment its devices and only allow them to connect to specific virtual LANs—limiting access between devices as well as limiting device access to the network. If a malicious actor was to gain access to a vulnerable device, that device could not be used to connect to other devices on the network.

Schopperth's team deployed Cisco Secure Network Analytics for faster, simpler, cloud-based network monitoring, and Cisco Umbrella to extend the hospital's security footprint for remote devices. From there, it needed help

Specialists in exceptional care and unwavering compassion, Dayton Children's is a teaching hospital that provides primary and specialty healthcare services for infants, children, and teens.

Industry:	Healthcare
Location:	Dayton, Ohio
Size:	4000 employees
Website:	childrensdayton.org

> *We have a variety of Cisco products, and what I love is that they're designed to work with each other in a way that you can correlate if something is going on. The further left on the attack chain that we can go, the better we are.*

Nicholas Schopperth
Chief Information Security Officer
at Dayton Children's Hospital

classifying devices, managing IoT/IoMT flows and deciphering communication patterns to identify any anomalies. For this, it turned to Cisco partner Ordr, which had impressed Dayton Children's with its efforts in building an API for integration with the hospital's IT service management platform. "Cisco Identity Services Engine (ISE) and Ordr have helped identify device types and put them into their own segmented VLANs," said Schopperth.

Having identified granular device context, baselined "normal" device communications flows, and performed behavioral analytics of devices and users with Ordr Connected Device Security, the cybersecurity team generated policies and access controls that could be automated and enforced using Cisco ISE on Cisco wireless controllers and firewalls. The added benefit of using Cisco solutions for all endpoints and the Cisco compatible Ordr Connected Device Security solution is that communication is more reliable and secure across the entire environment.

Security, easily managed, at reduced cost

Dayton Children's network is no longer flat, so if a device somehow becomes compromised, the damage can't spread to other devices, sites, or systems. By having the ability to stop a cyber intrusion in its tracks, Dayton Children's can help ensure patient care is minimally impacted.

Dayton Children's saw the benefits of its new architecture when a partner organization experienced a ransomware attack. As the ransomware began scanning Dayton Children's network through a shared connection, the hospital's newly implemented Cisco alert systems sounded an alarm. In just five minutes after receiving the alert, Dayton Children's cybersecurity engineers used Ordr device context to drop its connection with the partner. In another five minutes, five MRI machines that had been scanned by automating Ordr policies on Cisco infrastructure were automatically quarantined. The security team then began the process of reimaging those devices to get them back on the network and serving patients safely. Notably, every device that had Cisco Secure Endpoint installed was untouched.

Dayton Children's has significantly reduced its exposure to attacks. Without this technology, quarantining these devices would have taken much more time. And with each passing minute, more machines could have been infected and care could have been impacted.

The hospital's cybersecurity team finds the zero-trust architecture not only effective, but easier to manage. It reduces the number of solutions and limits network exposure by using an end-to-end Cisco architecture and Ordr's device security solution, and the reduced administrative overhead promotes innovation and growth in other areas.

"We have a variety of Cisco products, and what I love is that they're designed to work with each other in a way that you can correlate if something is going on," remarks Schopperth. Having Cisco SecureX as a single pane of glass to consolidate monitoring and find the source of any breach faster also makes Dayton Children's more proactive and less reactive. Schopperth continues, "The further left on the attack chain that we can go, the better we are,"

Dayton Children's strives to provide the best possible care, and that requires diligent work behind the scenes. The patients and families who walk through the hospital's doors might not know about Dayton Children's cybersecurity practices, but the safety of their children's care relies on them.

Challenges

- A proliferation of Internet of Things (IoT) and Internet of Medical Things (IoMT) devices in need of a modern cybersecurity posture
- Securing 25,000 new devices connecting to the network, including critical medical devices
- Limited financial and personnel resources for a complete cybersecurity overhaul

Solutions

- Cisco Umbrella
- Cisco Secure Network Analytics
- Cisco Identity Services Engine (ISE)
- Cisco SecureX
- Cisco Secure Firewall
- Cisco Secure Client (formerly AnyConnect)
- Cisco Secure Endpoint
- Ordr Connected Device Security

Results

- A network less vulnerable to cyberattacks and security threats
- Enhanced patient safety and protection for the privacy of children's personal data
- Reduced software management and administrative overhead
- Fast, easy expansion to new sites as needed
- A secure, zero-trust architecture