You Can Do It Too: Reduce the Risk of Cyberattacks with a Zero Trust Architecture

by Christopher Kuhl
Chief Information Security Officer and Chief Technology Officer
at Dayton Children's Hospital

There are three tenets in information security: confidentiality, integrity, and availability. We must keep our data secure and protected from unauthorized access; the data we work with must be accurate and complete; and our services must be available to those who need them. There is a fourth tenet for those of us in healthcare: patient safety.

That doesn't resonate with some organizations whose leaders don't acknowledge cybersecurity's role in supporting the patient. But those organizations who do see the connection are increasingly interested in a zero trust architecture, which helps improve patient safety while reducing organizational risk.

Zero Trust is an approach to cybersecurity that validates every stage of a digital interaction—users, applications, and infrastructure—from the principle of "never trust, always verify." The expansion of remote work, migration to the cloud, and increased adoption of Bring Your Own Devices (BYODs) demand a new security approach. Organizations can no longer assume that everything on their network is to be trusted. Instead, we have to move to more granular security controls to limit the lateral movement of malicious actors.

Organizations can no longer assume that everything on their network is to be trusted. Instead, they have to move to more granular security controls to limit the lateral movement of malicious actors.

This all sounds lofty and ambitious, but if there's one thing I want you to know, it's that deploying this strategy isn't as hard as you might think. When I talk to CISOs at other organizations, their most common excuses for not moving toward Zero Trust include not having enough money, time, or people for implementation. We're all resource-strapped, it's true. But if you bought technology in the past five years that can integrate with other technology and run access lists, it will support Zero Trust.

Implementing Zero Trust isn't this massive undertaking you have to do all at once. It's possible to work piece by piece, even with limited financial and human resources. It's all about where your priorities lie and the risks you want to mitigate. When you have the right partners, it's pretty straightforward. I know because my small team at Dayton Children's Hospital (DCH) built a Zero Trust Architecture from the ground up.

Zero Trust Is a Must in a Hospital Environment

DCH is a pediatric acute care children's teaching hospital located in Dayton, Ohio. Ranked by U.S. News and World Report as one of the best children's hospitals in orthopedic and pulmonary specialties, DCH boasts some of the best physicians in the country and focuses on the relentless pursuit of children's health. Since the 1960s, the hospital has grown to two primary campuses and around 20 remote sites.

As the hospital's physical footprint has expanded, we have also seen a proliferation of connected devices, especially with the growth of IoT and IoMT devices. Today, we have approximately 25,000 devices on our networks. These devices include everything from smart TVs and security cameras to X-ray and MRI machines to robots that aid our neurosurgeons.

I started at the hospital in September 2018 as CISO, working with the CIO to build a security program from scratch. When the existing CTO decided to pursue other opportunities in March 2020, I assumed the additional responsibilities of the CTO role. I worked hard to integrate both the cyber and operational aspects of IT, improving security and pushing the boundaries of the DCH's existing technology limits. I'd say we jumped 20-25 years in technology in one year alone.

I had learned about Zero Trust while at a previous organization, and I knew this was where I wanted to take DCH. The proliferation of IoT and IoMT devices introduces risk, and I recognized the benefit of Zero Trust in reducing that complexity. I told the hospital this was a must from the start, and leadership agreed.

We spent the first year performing a gap analysis of our technology. Simultaneously, I went on a 'PR tour' of sorts, educating people on the necessity of Zero Trust. I spoke to IT and organizational leadership, but I also went to the physicians and nurses on the clinical side. Nobody had heard of Zero Trust, so it took several conversations to explain the benefits from a risk management perspective and tie those benefits to improvements for teams on the ground. Once I got that support, we haven't looked back.

A Stronger Security Posture with Cisco and Ordr

I had been drinking the Cisco Kool-Aid my entire career, so I was familiar and comfortable with Cisco's security solutions. I had experience utilizing Cisco solutions to implement Zero Trust at a previous organization, so it was a "rinse and repeat" situation at DCH. After our initial gap analysis, we deployed Cisco Secure Network Analytics (formerly Stealthwatch) for faster, simpler, cloud-based network monitoring and Cisco Umbrella to extend our security footprint for remote devices. From there, we needed something to help us manage IoT/IoMT flows and decipher communication patterns.

When it came time to look at solutions for building out IoT/IoMT policies and profiles, we talked to three vendors. One tried to strong-arm us into a contract, while another never returned my calls. Then I remembered a proof of concept (PoC) the network team had completed during my early days at DCH. I was impressed, so we returned to take another look at the company, now called Ordr. I was further impressed by their sales approach. They were confident enough that their product would sell itself, so there was no need for pushy sales tactics. The Ordr team even went the extra mile and agreed to build an API for the integration we needed for our ITSM platform—all before we signed an agreement with them. We knew we were entering a valuable partnership.

We now leverage Ordr to help us identify typical communication flows and behavioral analytics of devices as well as users. Our next step was to generate policies and access controls, some of which are automated using Ordr technology and enforced on Cisco switches, wireless controllers, and firewalls. In addition to adopting Umbrella and Secure Network Analytics, we decided to leverage Cisco solutions for all our firewalls and antivirus on all our endpoints, including servers and workstations. The Ordr integrations with our Cisco solutions are seamless. The benefit of using Cisco and Cisco-integrated solutions such as those from Ordr is that they communicate with each other, rendering our entire environment more secure.

Keeping Medical and IoT Devices Out of Reach for Malicious Actors

A Zero Trust framework is essential in the context of medical devices. These devices have to go through strict FDA inspections and certifications in the name of patient safety—as they should—but that notion of patient safety does not include cybersecurity. Manufacturers of medical devices like your insulin pump or MRI machine are not required to consider how cybersecurity might directly impact patient care. Ultimately, the responsibility falls to the hospitals and other organizations that buy these devices to ensure patients are appropriately cared for and safe. Medical and IoT devices are some of the lowest hanging fruit, and malicious actors capitalize on that security gap. Providing the best medical care requires solving for patient safety, and that includes controlling access to these devices on the network.

Providing the best medical care requires solving for patient safety, and that includes controlling access to these devices on the network.

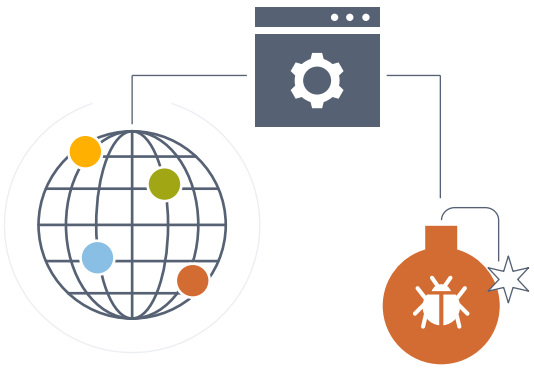
Many hospital networks were stood up decades ago, and they haven't changed much since, but the network at DCH is no longer flat. That means it's no longer possible for someone to log into a workstation or hack into a security camera and see the entire network. And if that security camera or workstation is compromised with ransomware, it can't spread to new devices, sites, or systems because we don't allow it. Using Cisco and Ordr technology, we have significantly decreased incident response time while increasing response capabilities.

We saw our new architecture in action when one of our partner organizations experienced a ransomware attack. We received alerts when the ransomware began scanning our devices via a shared connection that we use to exchange patient information. We asked our partner if they were performing vulnerability scans, and when they answered in the negative, we dropped the connection—just five minutes after we initially received alerts. Within another five minutes, we had automatically quarantined five devices. Within twenty-four hours, four of those five devices were reimaged and back on the network, ready to once again serve patients safely. (The delay with the fifth device was due to the manufacturer.)

Without Cisco technology, Ordr, and a Zero Trust framework, that incident would have gone very differently for DCH. We wouldn't have quarantined anything in 10 minutes; we would have been lucky to get notifications that quickly, and the ransomware could have spread to more devices much faster. Instead, we swiftly identified the problem, notified the partner of the attack, and acted to restore the integrity of our devices.

Pay for the Solution—Not the Cost of a Cyberattack

IT teams should reconsider the argument about the cost of a Zero Trust architecture. It's easier to manage than the alternative, and we reduced our number of solutions by using Cisco from end to end. DCH has significantly reduced the risk of cyberattacks and limited our network exposure while reducing our software



With a Zero Trust architecture, organizations can reduce the risk of cyberattacks and limit network exposure while reducing their software footprint and administrative overhead.

It's also easier to spin up new sites as needed. At the beginning of the pandemic, DCH's leadership team asked IT to spin up four new testing sites on existing parking lots across the region—within one month. Under previous circumstances, that task would have been overwhelming. But with Zero Trust, we could break it down into smaller segments and build them out from there. It's much easier to create a network with 20 pieces of equipment than to integrate those 20 devices into a much more extensive network. Now that we have a blueprint, we can make these business transformations faster while also being more secure. Sure, we get bragging rights for being one of the first hospitals to make this Zero Trust journey, but more importantly, our patients and their data are safer.

Hospital boards face tough decisions, and it's not always easy to choose the right path forward, especially when it comes to technology. But for IT professionals, the answer is staring us in the face. We can spend X hours this year and a considerable amount of money to advance an organization toward a Zero Trust framework that reduces the risk of cyberattacks and improves the core mission of putting patients first. Or we can leave the network and security controls the same as they've always been and pay millions of dollars (according to our cyber insurance organization) each time there's a total security breach.

I've shown you what you can achieve if you take the first steps on your Zero Trust journey. The real question is: What happens if you don't?

About Ordr

Ordr makes it easy to secure every connected device, from traditional IT devices to newer and more vulnerable IoT, IoMT, and OT. Ordr Systems Control Engine uses deep packet inspection and advanced machine learning to discover every device, profile its risk and behavior, map all communications and protect it with automated policies. Organizations worldwide trust Ordr to provide real-time asset inventory, address risk and compliance and accelerate IT initiatives. Ordr is backed by top investors including Battery Ventures, Wing Venture Capital, Ten Eleven Ventures, Northgate Capital, Kaiser Permanente Ventures, and Unusual Ventures.

For more information, visit www.ordr.net and follow Ordr on Twitter and LinkedIn.