TXOne Networks

2022 /Q4

OT Zero Trust

Boosts Healthcare Cybersecurity

txOne networks

TXOne Networks

OT Zero Trust

Boosts Healthcare Cybersecurity

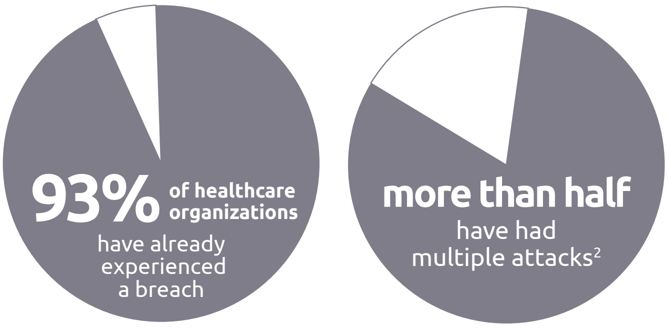
txOne networks

OT Zero Trust
Boosts Healthcare Cybersecurity

Table of Contents

Introduction

In Germany, a woman died enroute to an out-of-town emergency room. She was redirected to this more distant location because her local hospital was shut down as they grappled with a ransomware attack.[1] Hospitals have become lucrative targets for cybercriminals. They know that we depend on healthcare systems and medical devices to be available and functioning properly when we are ill or hurt. Hospitals may have up to 15-20 networked devices per hospital bed, and there can be more that 85,000 non-IT medical devices in one hospital. Each of these connected devices provide hackers with a chance to launch a ransomware attack and demand a payment that is, all told, cheaper than hiring cyber specialists and easier to recover from than prolonged downtime and bad publicity. 93% of healthcare organizations have already experienced a breach and more than half have had multiple attacks.[2] Many have paid the price.



The IT side had lock-ups that affected operations, leading to a poor patient outcome. From a cybersecurity perspective, this is a common challenge in critical infrastructure OT work environments – wildly differing but life-critical industries such as energy, pharmaceuticals, and water and wastewater treatment all must be secured so that a bad actor cannot use them to cause a catastrophic disaster. The modern hospital requires cybersecurity solutions that can handle these issues without creating challenges that could lead to poor patient outcomes. Life-critical services everywhere in the world have to budget for IT, financial systems, and billing – including cybersecurity – all while maintaining the organization's critical focus on supporting specialists along with the equipment they use to facilitate good outcomes.

[1] *"The untold story of a cyberattack, a hospital and a dying woman." Wired. (2020) https://www.wired.co.uk/article/ransomware-hospital-death-germany (Accessed June 25, 2022).*

[2] *"Largest Healthcare Data Breaches Reported in February 2022 Confirms Need for Network Security Based on Zero Trust Microsegmentation." GlobeNewswire. (March 2022) (Accessed June 19, 2022).*

OT Zero Trust in the Cloud or On-Prem

About half of the United States' healthcare institutions have moved to cloud-based systems. The other half prefer to keep systems confined to the physical premises, citing concerns about HIPAA privacy breaches if patient data resides in the Cloud while also stating that their legacy infrastructure is not ready for retirement.[3]

Medical devices communicating with Cloud systems and those located on premises both need extra OT zero trust protection. First, OT should be separated from IT systems by an OT firewall designed specifically to protect operations. The most effective OT firewalls use adaptive trust lists to keep track of what's going on and only allow trustworthy messages to flow to critical systems. OT firewalls coupled with IPSes can only do this if they understand the special protocols in healthcare systems. Medical devices are often highly specialized and costly. They need robust endpoint cyber hygiene that stops known attacks, guards against zero-day hacks, and avoids future assaults. Remember, only security appliances smart enough to understand OT protocols can perform the deep threat analysis needed to make sure medical devices are trustworthy.

Tech Trends for Healthcare

According to Forbes,[4] medical imaging devices used by radiologists, cardiologists, and pathologists to diagnose a wide variety of conditions are one of the fastest growing areas for improving healthcare. AI is being used to decipher X-rays, CAT scans, and MRIs so doctors can quickly identify diseases like cancer and treat them more effectively. Predictive analytics are being incorporated into clinical pathways for data-driven care decisions. Telehealth proved to be a good way for physicians to remotely care for patients during the Covid pandemic. It will continue to evolve and become increasingly embedded in MyChart and other online portals for viewing lab results and emailing doctors. Collaborative robots or "cobots" are assisting in brain tumor removal and performing surgeries on other parts of the body.

Da Vinci Robotic Surgery Devices[5]

[3] *Theresa Lanowitz, AT&T Cybersecurity Insights Report: "A Focus on Healthcare." AT&T Business (February 2022) (Accessed June 19, 2022).*

[4] *Navneet Gupta. "Five Healthcare IT Trends To Watchout For In 2022." Forbes (2022) (Accessed June 21, 2022).*

[5] *URL for image: https://www.researchgate.net/figure/Da-Vinci-robotic-systems-have-three-major-components-the-surgeon-console-the-surgical_fig1_281377370*

Threats to Medical Devices

Threat actors know that hospitals and laboratories cannot allow malware to shut down life-saving medical devices or refrigeration units storing vaccines. They see an easy payday by launching ransomware attacks. More sinister hackers are striving to craft attacks that tunnel from IT or hit OT systems directly. They want to take direct control of equipment and hold it hostage with the threat of being able to command medical devices to misbehave should the ransom not be paid.

When you look behind the firewall at high-tech healthcare, the threat landscape is expanding every day. The challenges for medical device manufacturers lie in their need to meet the health and safety needs of patients while maintaining regulatory compliance and increasing profits for shareholders. Adding the complexities of cybersecurity into the mix can seem overwhelming. While manufacturers grapple with developing security patches and obtaining regulatory clearance for upgrades, hospitals and labs must find ways to protect the equipment they are using in the meantime.

The costs are high for purchasing and maintaining medical equipment, such as MRI or CT scanning machines that can find cancerous tumors, and lab equipment such as LC/MS systems that use robotic arms to load syringes with samples in preparation for molecular analysis used to develop new vaccines and conduct DNA research.[6] Sometimes, these machines cannot be connected to the network to download the latest virus signatures and other protections. Other equipment such as anesthesia machines, sterilizers, electrosurgical units, and infusion pumps may be connected to the internet but they might not have been inspected to wipe away supply chain malware. IT anti-malware was never designed to handle the configurations necessary for these specialty machines, and uninspected devices may be deployed with ransomware and inadvertently spread it in stealth mode.

Telemedicine devices need remote connections so that doctors can monitor vital signs from a distance which makes them easy targets for hackers. Many of these critical machines may be running on outdated operating systems that are too old for security patches but are still functioning properly. Even if a hospital had the funds to buy upgraded equipment, it takes on average 3-7 years for manufacturers to develop a new device from conception to installation at a hospital or lab.

[6] *Scientists use liquid chromatography / mass spectrometer systems for studying how quickly drugs leave the body or detecting compounds (such as illegal drugs) from a sample.*

Depending on the class of a device, FDA certification alone can take from a few weeks for 510(k) clearance of Class 1 non-invasive device up to 8 months for Class 3 devices that follow the PMA (premarket approval) pathway.[7]

Building systems used in hospitals and labs are another attack vector that is often overlooked. HVAC[8] systems have vulnerabilities that may impair their ability to purify the air and stop infectious diseases from spreading. In some parts of the world, simply turning off the air conditioning would create a life-threatening emergency, as patients and healthcare professionals might suffer heat strokes. Backup generators also need to be secure to keep the lights on during surgery and to keep life-saving devices working during an unforeseen power outage.

In 2020, Stellar trust lists were recommended to protect medical devices and building systems. Rather than blocklist known malware, Stellar trust lists only allowed trustworthy control commands. Two years later, Stellar trust lists have been tested and proven successful even under increasingly aggressive threats. Stellar provided a good foundation for OT zero trust to advance trust analysis techniques that can protect endpoints, networks, and those highly valued legacy devices and standalone systems.

Now, OT zero trust offers a wider range of protections for medical devices and healthcare building systems. OT firewalls segment networks into critical and non-critical microsegments and keep operations away from IT. If one segment becomes infected, it can be quarantined which will mitigate the damage. Trust lists only allow trustworthy messages and control commands based on the current circumstance. Virtual patches secure devices from zero day attacks and prevent ransomware propagation. OT zero trust was specifically designed to provide granular control over healthcare protocols by supporting 50+ variants of both IT and OT protocols for hospital network access control including HL7, DICOM, and Modbus. Endpoints are locked down using allow lists that immunize them against ransomware. Plug-and-scan USB technology wipes malware from legacy devices and standalone systems. All these security appliances report to the OT defense console, where you can see what's going on at any time on a single monitor.

[7] *"Robert Fenton. How Long Does the FDA Medical Device Approval Process Take?" Qualio. (2021) (Accessed June 20, 2022).*

[8] *HVAC – Heating, Ventilation, and Air Conditioning.*

OT Zero Trust Cyber Inoculations

OT zero trust portable security devices are the solution to many of the challenges that hospitals and labs are facing. Laboratory and hospital equipment tend to be standalone, proprietary systems that are highly specialized and highly regulated and were not connected to the internet until recently. Some of these devices are not capable of network connectivity, but for those that can connect, they may be running on vulnerable operating systems too old to patch.

OT zero trust designed plug-and-inspect security devices specifically for these legacy and air-gapped devices. Simply plug in the device to a USB port and watch it wipe away malware and take an inventory of the computer information and software apps. This inventory is then sent to the OT defense console, where it undergoes further threat analysis to find ways to guard against every CVE or MITRE ATT&CK vector targeting your medical device, even those that have not been developed yet. Machine learning systems are hard at work evaluating data and making informed predictions about where attackers may strike next. Additionally, virtual patches protect against zero day attacks while manufacturers are busy developing upgrades.

By conducting OT zero trust health checks before deploying any device, supply chain malware can be wiped away. Reinforce cyber protections by scheduling routine inspections in between patient visits as needed. Nurses and technicians can also use OT zero trust portable security devices to safely share data among equipment without worrying about infecting them.

Telemedicine

During the pandemic, doctors and nurses began demanding better human safeguards so they could stay healthy while treating patients with highly-communicable diseases. Healthcare organizations looked at better ways to safely extend health services beyond the walls of the clinic. Telehealth or telemedicine emerged as a way for doctors and nurses to use video conferencing along with remote patient monitoring (RPM). RPM relies on cloud technologies and RPM devices to monitor patients at home. This protects healthcare workers while allowing patients to heal in the comfort of their own home, but it unfortunately introduces potential holes in security.

By scanning RPM devices with an OT zero trust portable security inspector before deployment, cybersecurity technicians or management can oversee the device's status on their OT defense console. System inventory from each patient is uploaded and analyzed so that cyber defenses could be customized for their unique, individual circumstances. RMP devices with built-in internet connectivity connect to home routers and begin trust listing immediately. They apply virtual patches to zap zero day threats and stop new threats on the horizon by using machine learning threat intelligence.[9]

[9] *"National Cybersecurity Center of Excellence Security Guidance." NIST. (Accessed June 19, 2022).*

2022 Ransomware Trends

One of the first known ransomware attacks against healthcare was launched as the ultimate insider attack. A biologist distributed 20,000 infected floppy disks in 1989 at a World Health Organization conference. Back then, floppy disks were used to share what we in the modern day would call apps. This ransomware would reboot 90 times before showing a message from PC Cyborg Corporation demanding that $189 be sent to an address in Panama. The biologist was arrested and charged, but later declared mentally unfit to stand trial.

Fast-forward to this century, and ransomware attacks have become far more sophisticated and costly. In 2016, the Hollywood Presbyterian Medical Center paid $17,000 for one such attack. In 2017, WannaCry exploited 200,000 systems across 150 countries including 70,000 British national healthcare systems, and the cost of this attack was estimated at £92 million. In 2019, over one billion medical images were leaked over a three month period.

Attacks spiked during the Covid-19 pandemic. McAfee reported observing 374 covid-themed threats per minute in the first quarter of 2020. In December 2020, the SolarWinds infected dynamic link library burst onto the scene as one of the most diabolical supply chain attacks in history. Since it was disguised as a vendor patch, it quickly and quietly infected 18,000 downstream customers, including healthcare organizations.

In January 2021, a Belgian hospital was hit by a Windows bitlocker encryption attack and an alert was issued warning about Iran-linked BitLocker attacks.[10]

In 2020, the FDA issued a warning about vulnerabilities found in medical equipment used in nursing bays to monitor patients' vital signs, including their temperature, heartbeat, and blood pressure. Bad actors could control these devices remotely and generate false alarms or silence real ones. The medical device manufacturer did not have a security patch ready, so they advised hospitals to separate this equipment from wider hospital networks while they developed an upgrade.[11]

Recently, three disturbing trends have emerged: **RaaS (ransomware as a service), hijacking legitimate tools, and LOTL (living off the land)**.

[10] *"Historical Ransomware Activity Leveraging Legitimate Tools." Ransomware Trends in the HPH Sector (Q1 2022). Department of Health and Human Services Cybersecurity Program. (May 2022).*

[11] *Mariella Moon. "FDA warns hospitals about security flaws in some GE medical equipment." Engadget. (January 2020) (Accessed June 19, 2022).*

RaaS

Ransomware as a Service is making it easier for thieves without technical skills to launch an attack. Initial Access Brokers (IAB) are selling network access so that RaaS groups have more time to focus on developing more sinister attack payloads. IAB and other remote access products are regularly advertised on cyber criminal forums. More than half of forum ads promote general VPN/RDP access to healthcare organizations. The top RaaS groups are LockBit, Conti, SunCrypt, ALPHV/BlackCat, and Hive.

Hijacking Legitimate Tools

To make it easier to operate in stealth mode, bad actors are crafting attacks by taking over legitimate tools such as Windows SafeMode, Microsoft's BitLocker, and FileZilla FTP.[12]

LOTL

Living Off The Land attacks use tools that are readily available in the target environment rather than deploying custom tools and malware. For example, Powershell can execute malicious commands or Task Scheduler can schedule malicious scripts. Strategically placed, legitimate commands can do significant damage by deleting files in an important folder.[9]

Ransomware Lawsuits

Even with all the evidence supporting the need for good cyber hygiene, some healthcare organizations still lag behind. Patients and healthcare insurance organizations are beginning to apply financial pressure.

On top of that, patients are suing over ransomware attacks. According to a study by the U. S. law firm Baker Hostetler, ***out of 58 ransomware lawsuits filed in 2021, healthcare organizations made up 43***.

The U. S. Centers for Medicare and Medicaid have been denying extensions for filing claims because of cyber attacks. They cite that healthcare providers "could have feasibly received information describing how to prevent the occurrence of cyber attack and did not address the risks in a complete and timely fashion." These denials result in a significant loss of revenue for late filing healthcare organizations.[13]

[12] *"CyberArk, Living Off the Land Ransomware Attacks: A Step-By-Step Plan for Playing Defense." Cyberark. (August 2021).*

[13] *Jeff Lagasse, "Patients increasingly suing hospitals over data breaches." (2022) (Accessed June 18, 2022).*

Deploy OT Zero Trust Cyber Defenses

Inspect every device before it is deployed to wipe away supply chain malware and to take a system inventory. Use the OT zero trust portable security device to alleviate the pain point caused by outdated operating systems that cannot be patched. Hospital machines frequently have accessible USB ports. Restrict access to only OT zero trust portable security devices for sharing data.

Segment operations away from IT networks. Most threats continue to come from the enterprise IT network through phishing emails or other hacks. A DMZ (demilitarized zone) with unidirectional OT firewalls guarding operational technology is recommended. MicroSegment sensitive equipment so it can be quarantined, if necessary. Rely on intrusion protection systems that have been designed to analyze OT protocols and machines.

Lock down and continually evaluate the trustworthiness of each control command and network message on a case-by-case basis. Allow only trustworthy control commands to reach equipment.

Reinforce cybersecurity through continuous inspections and monitoring to ensure identification of vulnerabilities. Install virtual patches to stop zero day attacks. Rely on advanced threat intelligence to help predict protections against new attacks.

Regulatory Compliance

OT zero trust supports compliance with FDA, GMP, GLP, and other medical device, hospital, or laboratory regulations in the USA, as well as international regulations. Additionally, medical devices in the USA are categorized as ICS and security advisories released by ICS-CERT apply. OT zero trust complies.

While HIPAA pertains to patient privacy, an assault on medical devices or hospital building systems that results in leaking patient data could cascade into a plethora of regulatory violations. The key to good cyber hygiene is adopting the attitude of expecting the unexpected. You never know what kind of malware hackers are concocting.

While OT zero trust protections are state-of-the-art, researchers are always striving to find new and better ways to protect you. In fact, NIST just published a new best practices guide. OT zero trust cyber defenders are working now to review the *NIST Special Publication 1800-30, Securing Remote Patient Monitoring Ecosystem*.[14] Stay tuned to the TX One Network blog for updates...

Never trust – always verify.

[14] *“National Cybersecurity Center of Excellence Security Guidance.” NIST. https://www.nccoe.nist.gov/healthcare/securing-telehealth-remote-patient-monitoring-ecosystem?msclkid=249ed7a1afa011ec89d2a84405e8b0a194d53de0af9f11ecb5dce3af61132f5a (Accessed June 19, 2022).*

txone.com