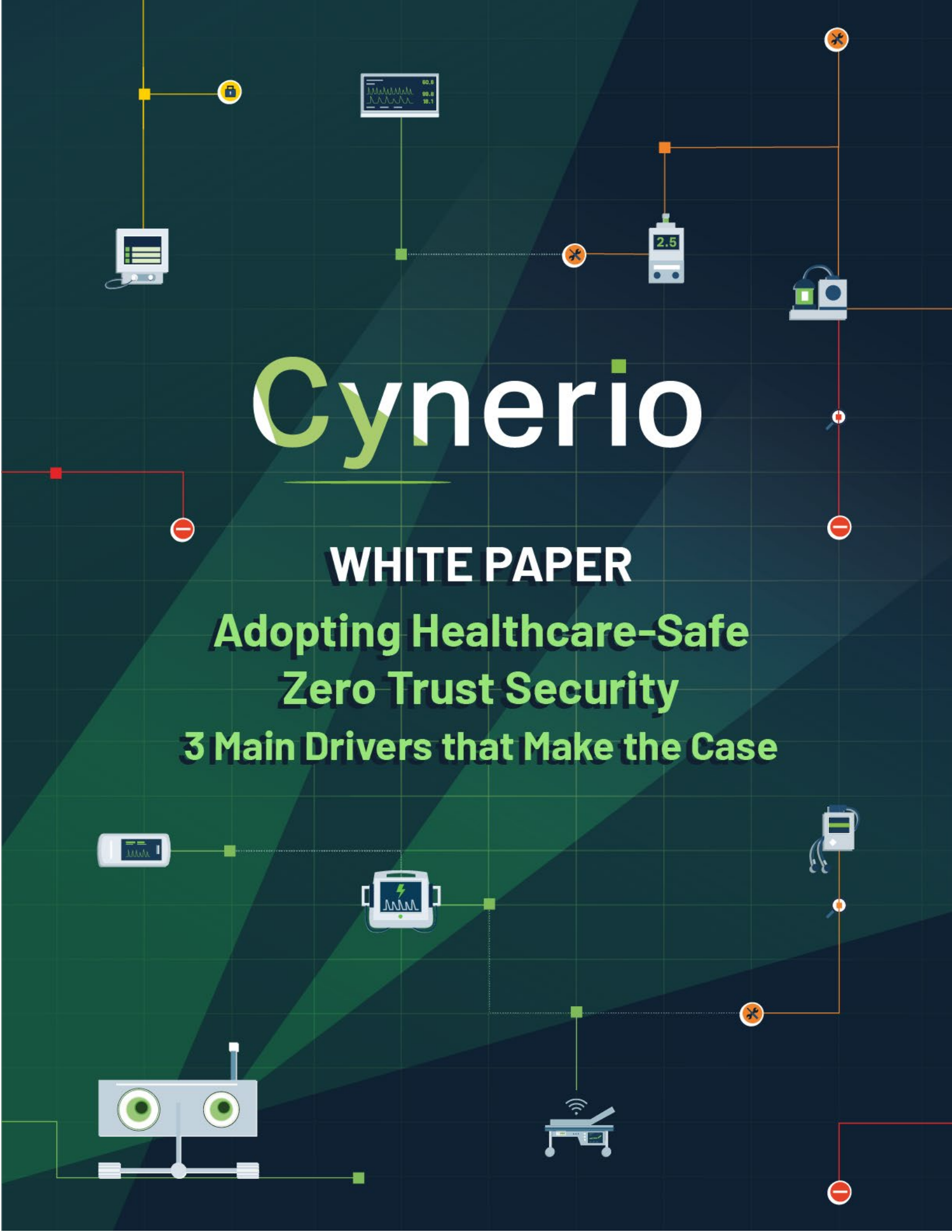

Cynerio
WHITE PAPER
Adopting Healthcare-Safe
Zero Trust Security
3 Main Drivers that Make the Case

Cynerio

Adopting Zero Trust Security for Healthcare: 3 Main Drivers that Make the Case

Zero Trust is a comprehensive security model that is gaining momentum in the enterprise, with 72% of organizations across every sector planning to implement it by 2021. The Zero Trust approach does away with the traditional security perimeter, assuming that every user or device on the network could potentially be malicious.

In a healthcare environment, the Zero Trust approach is possibly the only way to eradicate three imminent and growing threats: ransomware, outdated vendor firmware (such as the Ripple20 and Urgent11 vulnerabilities), and unsecured services such as Telnet or HTTP ports with no authentication.

However, there are significant challenges healthcare organizations face when trying to implement Zero Trust. In this white paper, we'll lay out these challenges, and suggest a path towards implementation of Zero Trust in the healthcare industry.

Cynerio

Table of Contents

Cynerio

Chapter 1: What Is Zero Trust?

Before we dive into the unique challenges of healthcare organizations and connected medical and IoT devices, we'll provide a general overview of the Zero Trust model, a paradigm that is rapidly gaining momentum in security organizations.

What Is a Zero Trust Architecture?

In the past, organizations were focused on building a security perimeter and making sure attackers cannot penetrate it. Zero Trust is a new architecture that assumes no security perimeter. All events and connections on the network are considered unreliable and malicious, meaning that even inside the old perimeter, every component must be secured.

Zero Trust is a new security architecture that assumes no security perimeter

The Zero Trust architecture was introduced to address new threats and security vulnerabilities created by cloud systems, containers and other ephemeral, short-lived computing systems, Internet of Things (IoT) devices, the growing sophistication of social engineering attacks, and the increasing prevalence of insider threats.

The NIST 2020 Zero Trust Report defines Zero Trust as a cybersecurity paradigm that treats all entities as potential threats, and shifts from perimeter-based defenses based on static networks, to dynamic defenses. According to NIST, Zero Trust security views every entity as a possible threat:

- **Users**—employees, contractors or guests to the organization could be malicious
- **Assets**—equipment and systems are assumed to be compromised
- **Resources**—confidential data such as personally identifiable information (PHI) are assumed to be accessible by bad actors

The goal of a Zero Trust architecture is to keep networks protected even when faced with increasingly complex threats and complex, shifting boundaries. In order to achieve this, users, devices, and applications receive the least privileges they need to function. This means:

- Any access between two components in the network is authenticated
- Even after authentication, an entity should not have more privileges than it actually needs
- Even authenticated, authorized entities might be controlled by bad actors, as in the case of compromised accounts

Achieving these principles, even in ordinary networks, is complex and requires a paradigm shift in security best practices, security tooling, and IT architecture.

Cynerio

6 Principles of Zero Trust Networks

The recent NIST report defines six principles that should guide the structure of networks, to make them true **Zero Trust networks**. These principles apply broadly, not only to the on-premises corporate network, but also to network infrastructure outside the organization, for example, the public cloud or public Wi-Fi networks used by employees on the go.

1. No Security Perimeter	All assets on the network should act as if an attacker has penetrated the network. All communication in the network must be secure, including authentication and encryption of every connection.
2. Non-Enterprise-Owned Devices	Devices on the network may not be owned by the organization, and may need access to resources inside the network to perform their function. These can include bring your own device (BYOD) personal devices, devices operated by external contractors, etc.
3. No Resource Is Trusted	Every asset being accessed by an entity should undergo a security evaluation using a policy enforcement point (PEP)—a policy engine that checks whether the entity is authorized to access it. Credentials alone should not be enough to access any resource on the network. The policy engine should evaluate requests based on the type of device requesting access (enterprise or non-enterprise), and other security criteria.
4. Non-Enterprise Resources	Resources on the network may not be owned by the enterprise, and nevertheless need to be protected— for example, cloud services. These resources may need access to their local network, which is not operated by the enterprise.
5. Local Networks Are Not Trusted	The basic assumption is that for a remote resource using their local network, the local network is hostile. Traffic may be monitored and modified by attackers. All communications should require confidentiality, integrity verification, and authentication.
6. Consistent Policy Across Enterprise and Non-Enterprise Infrastructure	Whether an asset or workflow "lives" in the enterprise-operated network or outside it, the same security policies should be applied. The architecture should also support devices that move from enterprise networks to non-enterprise networks, or between on-premise and public cloud environments.

Adoption of Zero Trust

Zero Trust is gaining momentum as a mainstream model for security management. According to the Cybersecurity Insiders 2020 Zero Trust Adoption Report, 72% of organizations are planning to implement Zero Trust by 2021, 19% have started implementing Zero Trust, and another 15% have a working Zero Trust strategy.

72% of organizations are planning to implement Zero Trust by 2021

The primary security measures being considered by organizations as part of a Zero Trust implementation (taken from the 2019 report):

- Multi-factor authentication (68%)
- Detection of anomalous behavior (61%)
- Securing access from BYOD devices (57%)

Another indicator of rapid growth of the field is the new Forrester Wave Zero Trust eXtended Ecosystem Platform report released in September 2020.

Now that we have clarified the significance and basic principles of Zero Trust, let's review the application of Zero Trust in healthcare environments.

Cynerio

Chapter 2: Three Drivers for Adopting Zero Trust

There are many reasons to implement Zero Trust architecture in healthcare organizations. However, in this white paper we'll focus on three severe threats, which affect almost every healthcare organization, and which only Zero Trust strategies can truly mitigate.

Cynerio research based on data from hundreds of healthcare security projects indicates these are the three most severe threats affecting healthcare organizations today.

1. **Ransomware**—widely prevalent in connected healthcare environments due to outdated and unpatched operating systems in myriad devices
2. **Outdated Firmware**—many devices run embedded operating systems which are even less frequently updated than consumer OSs, and their vulnerabilities are not well known
3. **Unmanaged Services**—devices commonly ship with open communications protocols, like Telnet, FTP or HTTP, which are not authenticated and contain vulnerabilities

Driver #1: Ransomware

Healthcare organizations are extremely vulnerable to ransomware attacks because:

- They operate thousands of vulnerable devices, including connected medical equipment, which can serve as a bridgehead for an attack
- Employee awareness is low, infection typically occurs via phishing emails
- Ransomware spreads fast from vulnerable devices to other parts of the network, compromising medical devices and blocking access to patient data

Windows Is the Central Vulnerability

According to a Forescout report, which reviewed 75 healthcare organizations with 1.5 million connected healthcare devices:

- 59% of connected medical devices were running Windows operating systems.
- Of those, 71% were running versions that expired in 2020, including Windows 7, Windows 2008, and Windows Mobile.

Microsoft retired its Windows Embedded Standard 7 operating system on Tuesday, October 13, 2020. All systems running it no longer receive support or security updates.

59% of connected medical devices run Windows—of these, 71% run expired versions that no longer receive security updates

Windows Embedded Standard 7 is used in many critical medical devices, from vendors like Philips, GE, Becton Dickson, Siemens, Hologic, Carestream, Ortho Clinical Diagnostics, and bioMerieux.

The worst part is that many of these devices cannot be patched or upgraded for risk of disrupting critical patient care.

Healthcare Ransomware Attacks On the Rise

According to a recent report from Check Point, there was a 50% rise in ransomware attacks in Q3 of 2020. Healthcare is currently the most targeted industry for ransomware. The threat rose sharply throughout 2020, with an increase of 71% in October, the month Windows stopped support and security updates for Windows Embedded Standard 7.

Ransomware attacks increased by 71% in October 2020—the month support ended for Windows Embedded Standard 7

Here are a few alarming examples of ransomware threats that compromised healthcare organizations in 2020:

- **United Health Services (UHS)**—a ransomware attack hit 400 UHS hospitals and clinics across the US for three weeks.
- **Dusseldorf University Hospital**—a ransomware attack shut down services and caused the death of a patient.
- **France University Hospital Center**—an attack shut down all 6,000 PCs in the hospital and forced a return to pen and paper.
- **University of Vermont Health Network**—an attack caused a system-wide network outage, with no electronic communications. The ransomware disrupted cancer treatments, and caused inaccessibility to electronic medical records (EMR) for a month. 300 staff members were given leaves of absence, and 129 left the organization.
- **CISA/FBI warning**—in October, the US Cybersecurity and Infrastructure Security Agency (CISA), the FBI, and the Department of Health and Human Services (HHS) issued a warning against ransomware attacks on US hospitals.

A Real-Life Attack Example: Ryuk

Infamous for	Entry Points	Lateral Spread	What's Affected
• UHS attack • Dusseldorf University Hospital attack	• Phishing emails • EternalBlue • TrickBot, Emotet	• Can infect and encrypt an entire network within **5 hours**	• VoIP phones • Radiology devices • Lab systems • EKGs

Ryuk was the ransomware behind the 2020 attacks on United Health Services (UHS) and Dusseldorf University Hospital.

It operates as follows:

1. **Entry points**—Ryuk typically penetrates networks via phishing emails with a malicious link, malicious websites distributing bots (TrickBot, Emotet), or the EternalBlue vulnerability (SMB port 445 on old Windows machines).
2. **Deployment**—usually happens weeks after the first bot is installed on a device in the network.
3. **Automated scanning**—the Ryuk bot collects data identifying vulnerable points on the network into which Ryuk can be successfully deployed (Windows domain controllers).
4. **Manual hacking activity**—once Ryuk is inside, attackers initiate manual activities like network reconnaissance and lateral movement to gain access to and compromise domain controllers.
5. **Encryption**—once in control of domain controllers, Ryuk begins encrypting data.

Cynerio found that nearly 15% of all Healthcare IoT devices across its deployments contain the EternalBlue and other TCP/IP stack vulnerabilities are completely unpatched and unmanaged.

Why Zero Trust Is the Solution

Healthcare organizations cannot tolerate ransomware and cannot use reactive measures—detection and response—to mitigate the threat. This is because:

- **Ransomware infections move rapidly**—they spread laterally from device to device across flat networks. For example, Ryuk can spread and infect an entire corporate network in as few as 5 hours.
- **Medical devices are critical to patient care**—once ransomware enters the network, it can leverage connected medical and IoT devices to spread, due to their vulnerable operating

systems. If these devices are infected, patient records can be compromised and medical treatment disrupted, posing a direct risk to patient safety.

Only a Zero Trust architecture can ensure:

- **Limited lateral movement**—the primary risk of ransomware is its ability to spread laterally and infect the entire network. With Zero Trust security, unauthorized connections between devices are blocked, limiting the ability of ransomware to spread.
- **Attacks cannot cause harm**—when vulnerable devices are isolated from other parts of the network, the organization can be confident that ransomware won't cause a complete shutdown.

Driver #2: Outdated Vendor Firmware

In the previous section we discussed the dangers of connected medical and IoT devices based on outdated PC operating systems. Next, we'll discuss another category of devices: those based on proprietary, embedded operating systems. In many respects, these represent an even bigger threat.

Why is vendor firmware so vulnerable?

- **Software code** was not written with security in mind and typically has not undergone security review
- **Authentication** is weak or nonexistent, and in many cases credentials are hardcoded
- **Data transfer** is often based on proprietary communications protocols, which are non-secured, unencrypted, and difficult to monitor
- **Firmware updates** are rarely, if at all, issued by vendors
- **Sparse security research** means that vulnerabilities are not well understood, and take much longer to be discovered than in consumer operating systems

Real-Life Vulnerability Examples: Ripple20 and URGENT/11

Let's review two families of vulnerabilities recently discovered by researchers, which affected millions of connected healthcare IoT devices worldwide.

Cynerio research discovered that roughly **96%** of infusion pumps in healthcare facilities across its deployments were affected by URGENT/11 or Ripple20 TCP/IP stack vulnerabilities.

Ripple20

Ripple20 is a series of 19 critical vulnerabilities, with 4 more recently discovered, in the Treck TCP/IP stack, a software library built into many medical and IoT devices and embedded in third-party components of operating systems. In many devices, Treck is a low-level component and administrators may not be aware it is used on the device.

63% of infusion pumps, including the commonly used Baxter Sigma model, are vulnerable to Ripple20.

Vulnerability details
Flaws discovered in the Treck stack enable remote code execution, allowing attackers to compromise targeted medical and IoT devices. Ripple20 vulnerabilities are embedded in Treck's TCP/IP Internet protocol suite library, which is built into the source code of a wide variety of medical and nonmedical devices.

Severity and consequences
Ripple20 vulnerabilities can lead to:

- Exposure and theft of protected health information (PHI)
- Denial of Service (DoS) attacks and shutdown of clinical networks
- Tampering with device functionality to interfere with medical treatment

Devices affected in clinical environments
Ripple20 is especially concerning because it affects critical care equipment, which means that attackers can physically harm patients, for example by administering excessive dosages of medication. Ripple20 vulnerabilities affect devices including:

- Baxter, Sigma series and B. Braun infusion pumps
- CareStream Radiology devices
- Schneider APC/UPS devices
- Digi capsule connectivity engines
- HP and Ricoh printers

Urgent/11

In October 2019, the US Food and Drug Administration (FDA) officially warned device manufacturers and hospitals about the URGENT/11 family of vulnerabilities.

Vulnerability details
URGENT/11 vulnerabilities were found in IPnet, a network communications component that is no longer supported by its original developer, yet is incorporated into software applications, equipment, and systems used by a variety of healthcare IoT and industrial devices.

Severity and consequences
A system affected by URGENT/11 can allow attackers to:

- Take remote control of medical and other IoT devices, disrupting clinical workflow
- Change the functionality of a medical device

- Cause logical flaws that can interrupt normal functionality
- Use a device to perform denial of service (DoS) attacks
- Exfiltrate sensitive data from the device or connected systems

Embedded operating systems affected
A series of operating systems, used by medical and IoT devices, are affected by URGENT/11. However, not all versions of these operating systems include the vulnerable IPnet component.

- Wind River VxWorks
- ENEA Operating System Embedded (OSE)
- Green Hills INTEGRITY
- Microsoft ThreadX
- ITRON
- IP Infusion ZebOS

Types of devices affected in healthcare environments
URGENT/11 was discovered in equipment by manufacturers including GE Healthcare, Philips, Schneider Electric, and Siemens, in the following device categories:

- Patient monitors
- MRI machines
- Firewalls
- VoIP phones
- Printers

Nearly 33% of infusion pumps across Cynerio's deployments, including the prominent Alaris model, are vulnerable to URGENT/11.

Real-Life Vulnerability Example: DNSpooq

Access Points with DNSpooq

Access points like Cisco, Aruba, Netgear, Comcast, and GE are non-medical IoT devices that play a significant role in healthcare network infrastructure. Many of these access points are affected by a group of vulnerabilities dubbed DNSpooq. These vulnerabilities were discovered in dnsmasq, an open-source DNS caching software built into firmwares found across many IoT and network infrastructure devices.

Vulnerability details
These vulnerabilities can enable cache poisoning and buffer overflows, resulting in:

- Unauthorized access to the clinical network

- Data exfiltration (compromised ePHI)
- Denial of service (compromised clinical workflows and operational continuity)

Severity and consequences
Cynerio research discovered that nearly 15% of all access points in healthcare facilities across its deployments are impacted by this vulnerability.

Every wireless and mission-critical medical and IoT device that connects with an affected access point is at risk, including:

- Infusion pumps
- Patient monitors
- Glucometers
- Radiology devices

Why Zero Trust Is the Solution

As evidenced by the Ripple20 and URGENT/11 vulnerabilities, firmware is often outdated, unpatchable, and unsecure.

Successful exploitation of vulnerabilities enables attackers to embed malware on devices, while IT and security teams have limited ability to detect and eradicate the infection. Devices often do not support antivirus or other security controls, and cannot be scanned with traditional security scanners.

IV pumps are an example of a highly vulnerable category of devices, which are also critical to patient care. An average hospital can have hundreds of pumps connected to the network. There may be no update for the vulnerabilities affecting the pumps, and even if there is, it can be challenging to deploy it to hundreds of devices manually, without interrupting patient care.

Only a Zero Trust architecture can ensure that:

- **Malware cannot communicate with command and control (C2)**, preventing remote control of devices
- **Infections cannot spread** to other parts of the network
- **Attackers cannot perform denial of service (DoS)** using vulnerable devices
- **Attackers cannot exfiltrate data** from vulnerable devices using malware

Driver #3: Unmanaged Services

Many connected medical and IoT devices come with communications services that are enabled by default, and pose a significant threat to healthcare organizations. These include:

- Telnet or SSH terminal access

- Open HTTP ports
- FTP server enabling remote upload and download of files
- VNC server enabling remote control

What are the security concerns with these open services?

- Some protocols, such as Telnet, are not authenticated
- Protocols that do have authentication may be configured with default or hardcoded passwords, which are the same for a large number of devices
- Devices may have old versions of the service (for example, an old version of FTP), which has vulnerabilities, and cannot be updated

In many cases, the healthcare organization is not aware that these services exist on the devices, and so are not aware of the risk.

With thousands of devices in an average hospital, it is infeasible for IT and security teams to manually test every device to discover open services. Traditional network scanning tools often cannot recognize these devices as medical devices. In some cases, scanning can interrupt their clinical operation.

Real-Life Vulnerability Examples: Basic HTTP Authentication and Vulnerable Services in Radiology Ecosystems

Basic HTTP Authentication

Many non-medical IoT devices are critical to the operational continuity of healthcare ecosystems. These devices are commonly managed over HTTP with basic authentication and default passwords.

Vulnerability details
Two examples of critical non-medical IoT devices are IP cameras and attendance clocks. They are both commonly managed over HTTP with basic authentication, which risks exposing credentials over plaintext.

Cynerio found that over 58% of attendance clocks across its deployments were being managed with basic HTTP authentication and default passwords, or with the same password shared across multiple clocks.

Similarly, over 25% of IP cameras in one hospital system were being managed with basic HTTP authentication, with credentials shared between all cameras.

Severity and consequences
Basic HTTP authentication and shared credentials can:

- Provide threat actors with easy access to live video streams of hospital activity
- Jeopardize the safety of the hospital
- Compromise patient privacy
- Expose PHI in the form of photo and video images

Vulnerable Services in Radiology Ecosystems

Radiology ecosystems are particularly susceptible to vulnerable services. Cynerio research found that more than 50% of servers in radiology ecosystems run a vulnerable service, e.g. HTTP, FTP, or SSH.

Vulnerability details
Radiology servers run old systems like OpenSSH_4.3 and OpenSSH_4.2, which was released in 2006. Each of these servers stores significant amounts of personal patient data.

Cynerio research discovered that 50% of PACS and RIS servers are impacted by vulnerable services, along with 2 in 3 VNA servers. 25% of mammography machines were found to run an outdated IIS or OpenSSH service, with many running OpenSSH_6.0, which was released almost ten years ago.

15% of MRI machines were found to be vulnerable to OpenSSH services, including the 15-year-old OpenSSH_4.2 service.

Severity and consequences
Vulnerable HTTP, FTP, SSH services and others can potentially:
- Expose large quantities of ePHI to unauthorized users and threat actors
- Impact the operational and business continuity of affected radiology departments

Real-Life Vulnerability Examples: Default Passwords and Telnet

Unsafe Protocols and External Vendor Connections
Many radiology devices use default passwords or weak credentials and are managed using Telnet and other unsafe management protocols like REXEC. Cynerio has found that more than 40% of CT machines across its deployments are managed unsafely by technicians, potentially exposing credentials and classified patient data in cleartext.

Unsafe protocols like these place healthcare facilities at risk of disruptive supply chain attacks (e.g. SolarWinds), especially since they are commonly used by vendors to connect to devices from external locations. Cynerio found that around 25% of CT machines are managed by vendors in this way.

We'll go into detail on two vulnerabilities affecting a large percentage of medical and IoT devices in healthcare environments—default passwords and the Telnet protocol.

Default Passwords

Many medical and IoT devices use generic protocols like FTP and HTTP with default passwords which cannot be changed, or are left unchanged by device operators. These communications protocols are required for necessary device maintenance, such as updates and patches. Hospital IT teams are often unaware when vendors communicate with devices to conduct maintenance.

Default passwords are often hardcoded. But even if they can be updated by hospital IT and biomed personnel, they often remain unchanged due to concerns over affecting the warranty and interoperability of essential medical devices.

Vulnerability details
Medical and IoT devices with default passwords are an inherent risk to clinical networks. Default passwords provide open access to the device that can:

- Allow unauthorized parties to gain control over device functionality, posing a risk to patients
- Grant unauthorized access to sensitive data stored on the device (e.g. ePHI)
- Lead to the theft and corruption of data
- Cause unscheduled device downtime, placing patients at risk
- Make medical devices susceptible to automated "drive-by" attacks, not specifically targeted at medical devices
- Serve as an entry point into the wider clinical network

Severity and consequences
Default passwords affect devices that are mission-critical in clinical environments and have a significant impact on patient care, including:

- Hemodialysis devices
- CT scanners
- Fluoroscopy and MRI machines

If an attacker uses a default password to compromise even one of these devices, they can compromise the entire clinical workflow. To place this in perspective, Cynerio found that one-third of CT machines across its deployments use default passwords providing backdoors into clinical networks.

Cynerio found ⅓ of CT machines across its deployments use default passwords providing backdoors into clinical networks

Telnet

The Telnet protocol is commonly found on radiology devices and embedded devices, including blood coagulation checkers. It was originally intended for remote configuration and remote support.

Vulnerability details
Most implementations of the Telnet protocol are not authenticated. Attackers can identify the presence of the service by scanning a hospital network, and effortlessly gain access to the device.

In many cases, the service uses a default password. Even if the password is changed, it is commonly transferred over cleartext, allowing attackers to eavesdrop on communications and steal it.

Severity and consequences
Via the Telnet protocol, attackers can:

- Gain access to sensitive information
- Disrupt care or completely shut down the device
- Gain complete control over the device

Why Zero Trust Is the Solution

Many medical devices require remote communications services for routine maintenance and function. These services enable connections locally, through the cloud, or via third-party vendors. Unmanaged services pose an inherent risk to clinical networks.

A Zero Trust architecture will typically "blacklist" these insecure protocols and allow them only for essential communications like maintenance and software updates. If necessary, it will allow the use of these protocols only in the relevant clinical context, and when communicating with known and trusted entities. This can dramatically reduce the risk associated with these protocols.

Only a Zero Trust architecture can ensure that:

- **Every connection is authorized**, verified, and authenticated
- **Communications are controlled on a case-by-case basis**—a service or connection is only allowed if it is needed for device functionality, is scheduled, and behaves according to specified parameters

Cynerio

Chapter 3: Why Is Zero Trust Difficult to Achieve in Healthcare IoT?

As we showed in the previous chapter, there are severe threats facing connected devices, and Zero Trust is possibly the only practical measure that can mitigate these threats.

However, there are several unique challenges that prevent healthcare organizations from applying Zero Trust strategies.

1. Poor Visibility

Healthcare facilities have thousands of medical and IoT devices that are invisible to the network, and may be unknown to IT and security teams. Many devices do not support connectivity over standard network protocols, making it difficult to discover them using traditional methods. At the same time, they may be open to the Internet and represent an attractive target for attackers.

Why it impacts Zero Trust:

- If you don't know about a device, or cannot manage it, you also cannot apply Zero Trust policies to it.
- Implementing a security strategy for healthcare devices requires mapping and profiling Healthcare IoT assets. Due to the large number of devices and the lack of an automated way to identify and query them, this can take months or even years.

2. Proprietary Protocols and Lack of Authentication

Healthcare IoT devices often run obsolete protocols that may be unauthenticated, unencrypted, and lack basic access controls. Examples of commonly used protocols are HL7, DICOM, POCT1-A, ASTM, VOXP, BACnet, Modbus, LonWorks, MQTT, PJL, and MNET.

Why it impacts Zero Trust:

- Standard IT security tools don't recognize proprietary healthcare protocols and cannot inspect communications.
- Standard Zero Trust tools will typically flag communications over proprietary protocols as anomalous and set policies to block them, but in a healthcare environment, this can disrupt clinical workflow and endanger patients.
- Even if these protocols have authentication capabilities, they are not integrated with the hospital's identification and access management (IAM) infrastructure, making it difficult to enforce policies. In some cases, changing credentials may invalidate warranties on these devices.

3. Devices Are Insecure by Default

Many Healthcare IoT devices have inherent vulnerabilities, such as open services with minimal authentication used for remote support, management, and monitoring. For example, radiology devices commonly arrive with open Telnet or RDP services.

Why it impacts Zero Trust:

- Zero Trust requires blocking open, unauthenticated communications
- However, these services are built into devices by default, and cannot function without them

4. External Connections to Vendors and Cloud Services

Many devices must connect to cloud services or third-party vendors to function properly. For example, vendors typically connect to devices remotely to perform maintenance or updates.

Why it impacts Zero Trust:

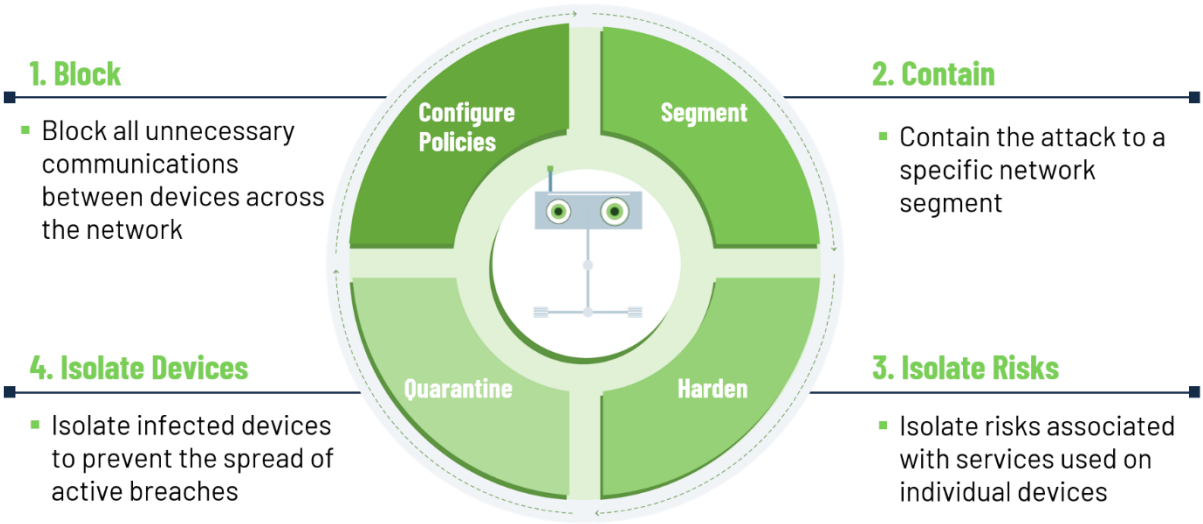
- Zero Trust requires blocking Internet access on critical devices
- However, when devices require cloud services or external vendor connections to function, it is impossible to shut off public Internet access
- VPN connections are not a solution because healthcare organizations have no control over the security of the vendors devices communicate with

Chapter 4: Zero Trust Security Measures for Healthcare IoT

Achieving Zero Trust in healthcare organizations is a huge challenge. Here are several ways you can take your organization one step further to a protected, Zero Trust environment.

Cynerio's Zero Trust implementation model consists of four stages:

1. Configuring policies to block unnecessary communications with Healthcare IoT devices
2. Segmenting the network to contain attackers to a specific segment
3. Hardening services running on connected medical and IoT devices to reduce their security impact
4. Quarantining infected devices to prevent a breach from spreading



1. Defining Policies

The first step to Zero Trust implementation is understanding which communications are absolutely necessary to maintain clinical workflows and medical device functionality, and which are not.

Map out your organization's devices and identify the following for each category of devices:

- What other devices does this category of devices communicate with?
- Does it need to communicate over the Internet? Is Internet communication isolated in a VPN tunnel?
- Does it need to communicate with the device vendor?
- Does it currently have access to other devices, networks, or the Internet, which is not required for normal operations?
- Is its network communication isolated in a VLAN?
- What types of communications protocols does it use?
- Does the device need to send or receive Protected Health Information (PHI) as part of its normal operations?

This information can be the basis for defining security policies in subsequent stages.

2. Network Segmentation

Because connected Healthcare IoT devices have numerous security vulnerabilities, a highly effective strategy is to isolate them from other parts of the network, to limit the attack surface.

Segmenting Healthcare IoT devices involves:

- Ensuring connected medical devices can only communicate with devices or systems that are part of their clinical process

- Blocking external communications, unless needed to communicate with the device vendor or another known entity

When defining segmentation policies, cooperate closely with clinical engineering/Healthcare Technology Management (HTM) teams to ensure segmentation does not interrupt clinical data flows, which can disrupt patient care.

3. Service Hardening

Evaluate connected medical and IoT devices and do as much as you can to:

- Apply the latest security patches
- Perform software upgrades
- Require authentication on all communication channels
- Close unused ports
- Limit unnecessary device functions

However, many of these connected devices do not support basic security activities like patching, and may be hardcoded with default, unsecure settings. In this case:

- Focus on devices that pose the highest risk, in terms of security vulnerabilities, their criticality to patient care and/or the sensitive data they hold
- Prioritize security patches or configuration changes that address the most severe known vulnerabilities

4. Detecting and Quarantining Infected Devices

When a connected medical device becomes infected with malware or is breached by an attacker, you cannot simply disconnect it from the network or shut it down. Many devices are used for timely, critical patient care.

Therefore, the recommended approach is:

1. Establish monitoring and incident response procedures to identify breaches and infections in real time
2. Keep devices functional at all times
3. Leverage network segmentation to isolate a device and prevent attackers from communicating with other parts of the network
4. Wait for planned device downtime, and use this opportunity to patch or clean the device to eradicate the threat

By following this process, you can protect Healthcare IoT devices and the surrounding network against threats without disrupting clinical operations or causing damage to critical medical equipment.

Cynerio: Visibility, Assessment and Protection for Healthcare IoT

Healthcare is Cynerio's only business and our mission is simple: protect healthcare's weakest link to ensure patient safety, data confidentiality, and service availability. Our full-suite Healthcare IoT cybersecurity platform automates end-to-end, continuous asset discovery for every connected medical, IoT device, and OT system in the clinical ecosystem. We view cybersecurity as a standard part of patient care and cover every threat vector with proactive and preemptive attack prevention tools, automated risk reduction, threat mitigation, and step-by-step remediation programs built on the NIST Zero Trust framework to get healthcare facilities secure fast.

For more information, visit the company's website at www.cynerio.com.

Cynerio

Healthcare IoT Cybersecurity

Secure. Faster.

www.cynerio.com