Cynerio

ENABLING MICROSEGMENTATION FOR DEVICES RUNNING AN UNSUPPORTED WINDOWS OS

Securing Clinical Ecosystems Against Unpatchable Connected Devices

Objective

Secure unpatchable medical devices running Windows 7 and other unsupported operating systems.

Client: US Hospital

The Problem

Medical devices with long life cycles outlive the operating systems running on them by years and manufacturers rarely issue device updates. **Insecure and unpatchable devices expose hospitals to cyber risk but cannot be haphazardly disconnected because they are essential to patient care and network infrastructure.**

Cynerio Solution

Deliver an enforceable microsegmentation strategy for all devices running unsupported OS that reduces the attack surface without interrupting service.

Unsupported Windows OS & Increasing Cyber Attacks on Healthcare IoT

The healthcare industry is particularly vulnerable to cyber attack, largely due to the prevalence of at-risk connected medical devices. Many devices are not developed with cybersecurity in mind and even more run outdated and unpatchable operating systems like Windows 7. The more devices there are running unsupported operating systems translates into larger attack surfaces and indefinite exposure to cyber risk.

The Challenge

Devices running unsupported OS, like Windows 7, are more vulnerable to cyber attack but cannot be disconnected from the clinical network without interrupting services. Hospital IT teams must reduce the attack surface by limiting the ability of devices to communicate with external networks and other devices without disrupting operational workflow or obstructing medical care.

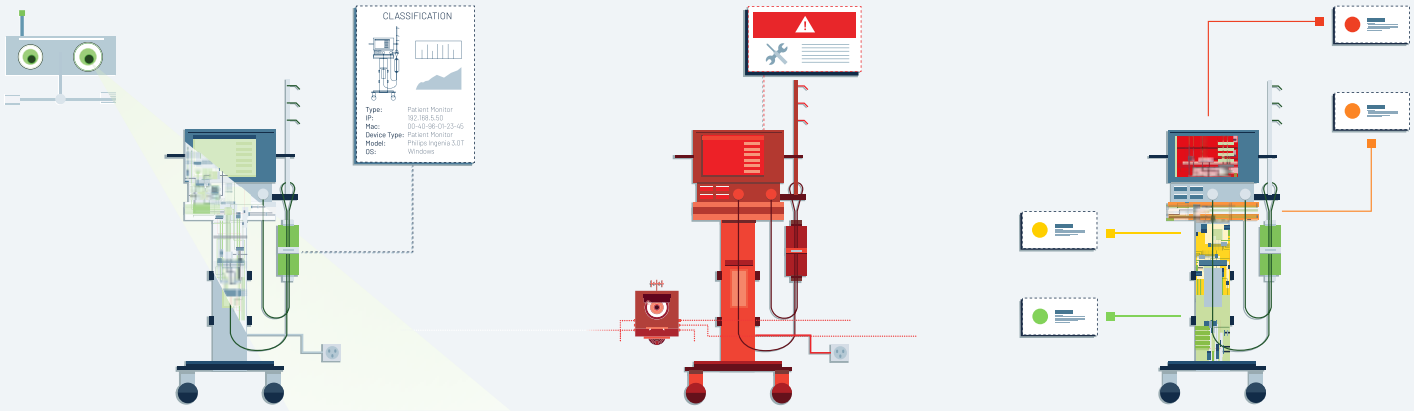
The Cynerio Solution

Cynerio takes a medical-first approach to solving the challenges of healthcare IoT security and prioritizes device risk according to impact on care delivery and hospital-specific workflows. This approach enables IT security teams to build and enforce microsegmentation policy that leverages existing security tools and network infrastructure.

Result

An effective, device-specific microsegmentation policy that limits device connections to trusted entities, minimizing the attack surface and providing tools to respond to suspicious cyber events.

How It Works



Step 1: Identify

Identify devices running Windows 7 and other unsupported OS. Determine the model and vendor, along with the device's purpose and impact on clinical operations..

Step 2: Assess Risk & Prioritize

Conduct an organization-wide risk assessment to determine device impact on clinical workflow. Prioritize devices according to criticality and impact on business/organizational infrastructure.

Step 3: Profile Communications

Gain insight into device communications that considers devices' expected and actual communications within the context of your organization's unique network architecture to easily identify anomalous behavior.

Step 4: Tag Devices in NAC

Tag devices in the NAC to which specific policy will be applied and place the devices in an object group.

Step 5: Devise ACL Policy

Devise microsegmentation policy and verify it according to actual device communications. Flag policies that may impact patient care.

Step 6: Enforce Policy

Segment devices into separate VLANs and push policy to the NAC. Verify that expected communications are unaffected.

Fact Boxes

40%

40% of all connected medical devices in the global clinical ecosystem run a Windows OS.

Nearly 50%

Nearly 50% of medical devices running a Windows OS now run the unsupported Windows 7.

Almost 20%

Almost 20% of all medical devices in the global clinical ecosystem run Windows 7.

Windows 7 EOL

Windows 7 EOL is only the latest in a long list of far more outdated operating systems critical medical devices still run: Windows Server 2008/R2, Windows Vista, Windows XP, Windows 98, Windows 2000.

Example of A Device-Specific Microsegmentation Policy Set by Cynerio

Segmentation for Unsupported CT Scanner Running Windows 7

Source / Destination	Direction	Port	Transport	Protocol	Profile
192.168.0.55	Outbound	4000	TCP	DICOM	Medical
192.168.255.255	Outbound	137	UDP	Netbios	IT
192.120.0.10	Outbound	53	TCP	DNS	IT
192.168.0.54	Outbound	5000	TCP	DICOM	Medical
192.168.0.222	Inbound	23	TCP	TELNET	Management

*A typical **CT Scanner** can far outlive the already unsupported Windows 7 operating system running on it.

Cynerio

About Cynerio

Cynerio is the world's premier medical-first IoT cybersecurity solution. We view cybersecurity as a standard part of patient care and provide healthcare delivery organizations with the insight and tools they need to secure clinical ecosystems and achieve long-term, scalable threat remediation without disrupting operations or the delivery of care.