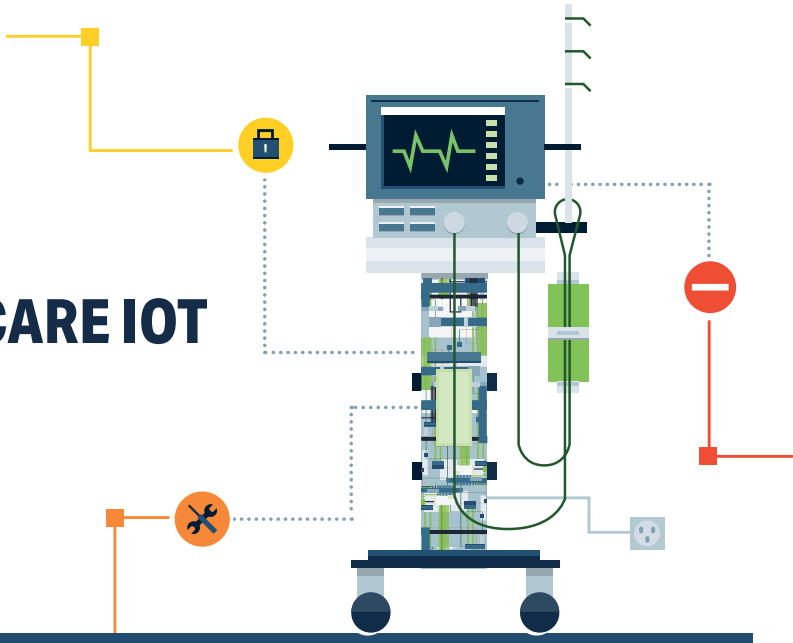
Cynerio

ENABLING NORTH-SOUTH SEGMENTATION IN HEALTHCARE IOT

Securing Clinical Ecosystems from External Cyber Threats



Objective

Secure connected medical devices on the clinical network from external threats.

Client: US Hospital

The Problem

Connecting to external networks is integral to the standard operation of many healthcare IoT devices. However, every external connection increases clinical networks' exposure to threats.

Cynerio Solution

Construct a perimeter firewall policy informed by passive data inspection and MDS² forms.

The Expanding Healthcare IoT and the Accelerating Severity of Cyber Attacks

89% of healthcare organizations suffered data breaches in the last two years. Connected medical devices are often developed without cybersecurity in mind and Healthcare Delivery Organizations (HDOs) lack adequate cybersecurity protocols and firewall strategy. Inefficient network security, device vulnerabilities, and lack of awareness among clinical staff about safe cybersecurity practices increase the attack surface. The larger the attack surface, the easier it is for threats from the Internet to compromise the clinical ecosystem.

The Challenge

The primary goal of HDO IT security teams is to minimize and control medical devices' connections to external networks without interrupting service. **Firewalls lack understanding of medical device communication profiles, inventory and usage, and device criticality to hospital workflow and care delivery. This makes it difficult to create a segmentation policy that does not disrupt services.**

The Cynerio Solution

Cynerio delivers robust north-south segmentation policies constructed with a deep understanding of medical device impact, and of standard and anomalous connections to external networks. Devices' behavior profiles are determined according to Cynerio Live research, machine learning, and MDS² forms to define external connections as:

- Required: Connections must be limited
- Anomalous: Connections must be blocked
- Needed only in specific circumstances at scheduled times (e.g. OS updates, patches, vendor services): Connections must be monitored and limited

Result

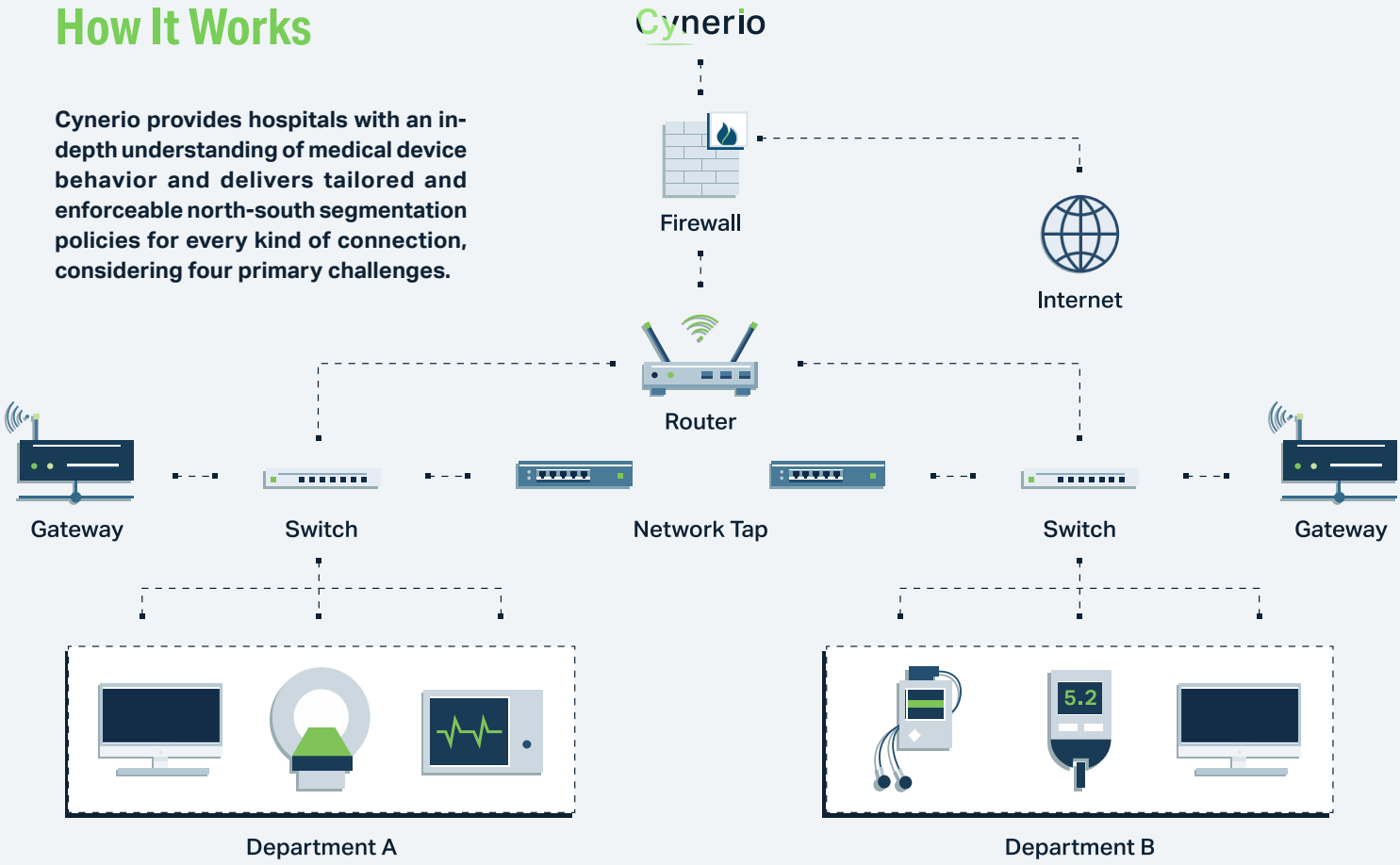
An enforceable north-south segmentation policy.

Cynerio's north-south segmentation policy is pushed to firewalls and enforced to:

- Immediately block traffic
- Restrict traffic to specific IP addresses over particular ports and protocols at specified times
- Constantly monitor device traffic for anomalous communications

How It Works

Cynerio provides hospitals with an in-depth understanding of medical device behavior and delivers tailored and enforceable north-south segmentation policies for every kind of connection, considering four primary challenges.



Challenge	Solution	Result
CHALLENGE 1: Misuse Misuse of a healthcare IoT device occurs when either an app or a person uses it to connect to unauthorized external networks. ■ It is common for medical devices to include pre-installed apps that consistently run in the background and may connect to external networks—unknown to IT security teams ■ Clinical staff and medical professionals may be unaware of safe security practices and connect to external networks to browse the Web or install apps that may connect to external networks	Block all connections and communication with external networks.	**The firewall will immediately block traffic to and from the device from external networks.**
CHALLENGE 2: Misconfiguration Most devices connect to IT services like OS, software, and endpoint protection updates over the network.	Identify misconfigured devices and how to configure them correctly. Cynerio also monitors communications and devises policy to block and limit misconfigured connections.	**The firewall will monitor communications and restrict traffic.**

Challenge	Solution	Result
CHALLENGE 3: Vendor Access Medical devices often require vendor access to receive support services, OS updates and patches, and to send data logs. Although communication with vendors should optimally be conducted over a VPN, VPN connections must still be controlled and monitored considering there is no guarantee as to the security of the vendor's network.	Monitor and limit access to vendors, depending on necessity as outlined by MDS² forms and Cynerio Live research on real-time network behavior.	**The firewall will block traffic to endpoints other than specified vendors and constantly monitor for anomalous communications.**
CHALLENGE 4: Required External Connection Some medical devices require a continuous external connection for standard operation.	Monitor and limit external connections to ensure communication is only with authorized endpoints.	**The firewall will constantly monitor device communications and limit connections to predefined authorized endpoints.**

Example of Specific Security Policies Set by Cynerio and Enforced by Firewalls

North-South Segmentation Rules for a CT Scanner

Source Type	Source IP	Direction	IP	IP Owner	Protocol	Port	Profile
CT	10.1.10.25	Outbound	13.107.4.50	Microsoft	HTTP	80	Windows Update
		Outbound	13.58.126.78	McAfee	HTTPS	443	Endpoint Protection
		Outbound	8.8.8.8	Google	DNS	53	IT
		Inbound	192.68.49.129	Philips	Telnet	23	Vendor Access

Cynerio

About Cynerio

Cynerio is the world's premier medical-first cybersecurity IoT 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.