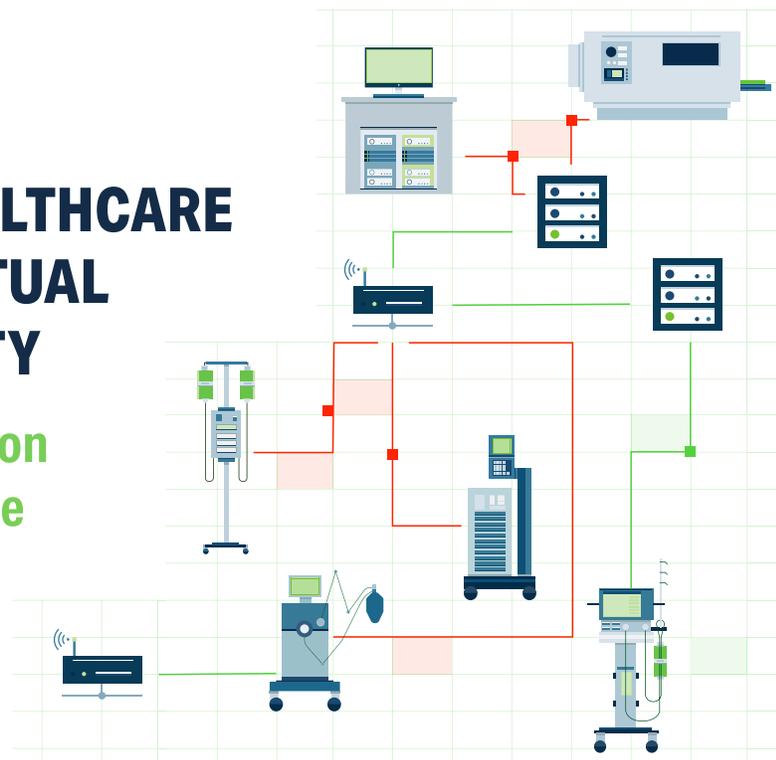




# ENABLING EXPEDITED HEALTHCARE IOT PROJECTS WITH A VIRTUAL SEGMENTATION CAPABILITY

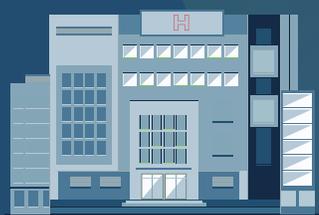
## Enforcing Segmentation Policies on Clinical Networks with Confidence



### Objective

Expedite healthcare IoT security and segmentation projects while providing confidence in continuous medical services.

### Client: US Hospital



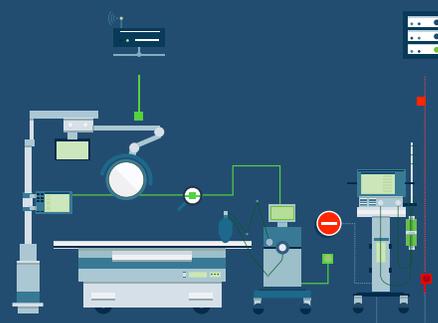
### The Problem

Healthcare IoT devices rely on internal and external connections for standard operations. Enforcing segmentation policies without disrupting critical medical services is difficult and can take over a year. IT teams need dedicated time and tools to be able to:

- Map complex medical device communications
- Analyze communications data and classify as standard/missible or malicious/suspicious
- Continuously monitor dynamic networks and refine policy

### Cynerio Solution

Use the Virtual Segmentation capability to define, test, and monitor segmentation policies for violations before pushing to live clinical network environments.



### Standard IT/IoT Security Solutions Lack Insight and Risk Disrupting Medical Services

Most hospitals struggle to protect their clinical networks and connected medical devices. Standard IT/IoT security solutions lack insight into the unique complexities of medical devices and their required communications. Implementing a solution without taking medical device behaviors

into account risks disrupting medical services and negatively impacting patients. Because of this, confidently implementing a security program is extremely time consuming and often dropped, leaving inherently vulnerable clinical networks exposed to cyber attacks.

## The Challenge



Implementing a segmentation policy that lacks an understanding of clinical contexts could:

- Disrupt medical services and cause harm to patients
- Be too lenient and not follow the best practices of least privilege

These complexities make it difficult for hospitals to create a segmentation policy that can be safely enforced and can delay the execution of security programs for a year or more.

## The Cynerio Solution



Cynerio's **Virtual Segmentation capability** automatically generates robust segmentation policies tailored to a hospital's unique clinical environment. You can **monitor, test for violations, and update** before enforcing them on the live network.

## Result

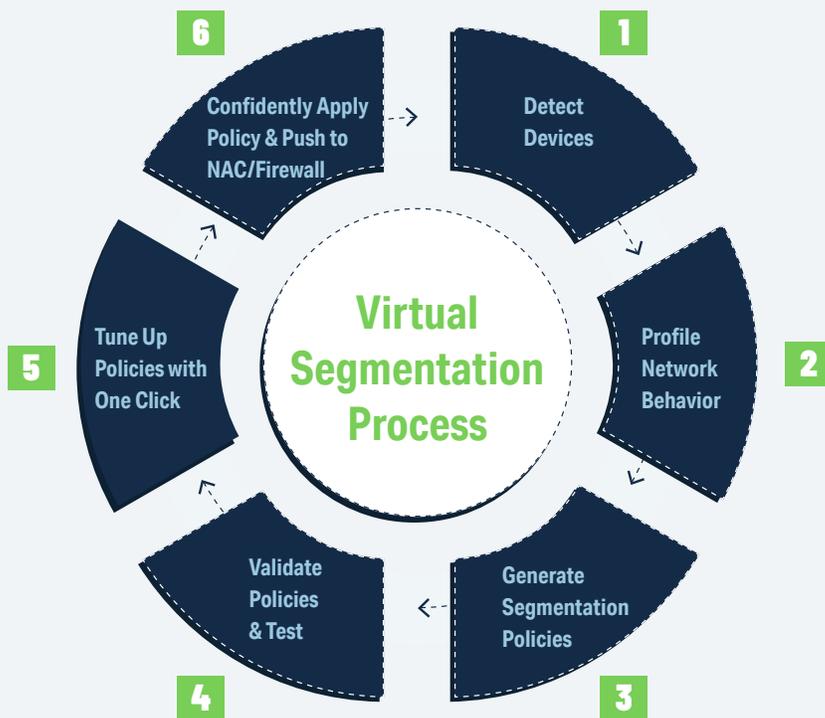


Automatically generate north-south and east-west segmentation policies **prioritized according to device criticality and medical impact**, then **confidently push** them to NAC/firewall.

## Fast & Easy Segmentation

- Customize policies in minutes
- Complete projects in weeks
- Test for safety
- Tune up policies with one click
- Enforce with confidence
- Ensure continuous medical services

## How It Works



# 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.