Cynerio

MarinHealth Stops IoT Device Malware in Its Tracks and Inspires a New Cynerio Product

MarinHealth

Case Study

Cynerio

marinhealth℠

Location: Greenbrae, California, USA
Founded: 1952 as Marin General Hospital
Bed Count: 327
Notable: The only full-service, acute care hospital in a county of 250,000+

We knew that in order to secure the devices, we needed to segment the network. And to effectively segment the network, we had to be able to see what was happening."
- Scott Christensen, Security and Systems Engineer, MarinHealth Medical Center

The Challenge

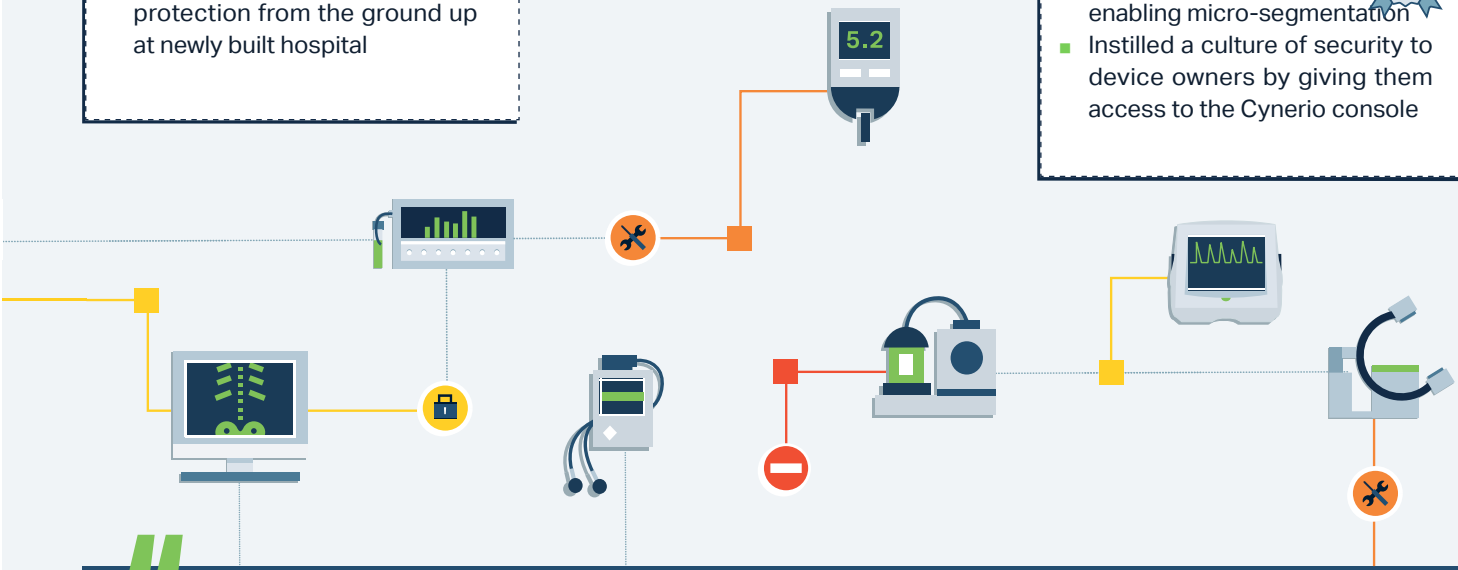
- Achieve visibility into biomedical and other IoMT device activity
- Respond to incidents quickly to contain their impact
- Proactively build security protection from the ground up at newly built hospital

The Cynerio Solution

- Attack Detection & Response (ADR)
- Rapid Risk Reduction (RRR)

Business Impact

- Responded rapidly to 3 malware attacks to date, preventing infection spread from initial device
- Achieved full visibility into all medical IoT devices enabling micro-segmentation
- Instilled a culture of security to device owners by giving them access to the Cynerio console



The value add for Cynerio is that we could look at the traffic at the packet level and see what the devices were talking to and where."
Nader Zamanzadeh, Senior Network Engineer, MarinHealth Medical Center

About Marin Health

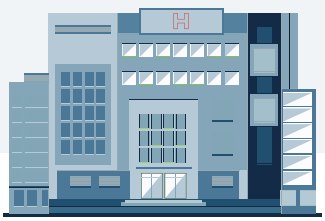
Marin County lies at the north end of the Golden Gate Bridge in California. Known for its magnificent scenery and upscale waterfront towns, it has maintained a feel that is very distinct from San Francisco while making a vibrant contribution to the Bay Area economy. For 70 years, locals have depended on MarinHealth Medical Center, the only full-service, acute care hospital in the county. In 2020, the institution opened a state-of-the-art, seismically resilient replacement hospital building known as Oak Pavilion.

Constructing an entirely new hospital facility gave the network and security team a rare opportunity— building a network from scratch. They were determined to design it with a proactive eye toward security. "We saw it as an opportunity to gain better visibility into the network," recalls Scott Christensen, security and systems engineer for MarinHealth. "There were gaps in what we could see in terms of network traffic, and the biggest was with our biomedical devices."

As with all hospitals, MarinHealth has thousands of medical Internet-of-Things (IoT) devices connected to the network, including a staggering number of distinct device types. Many of them are extremely expensive, and hospitals tend to keep them for many years.

As a result, many medical IoT devices run on legacy operating systems and have longstanding software vulnerabilities that are difficult or impossible to patch. For example, recent research by

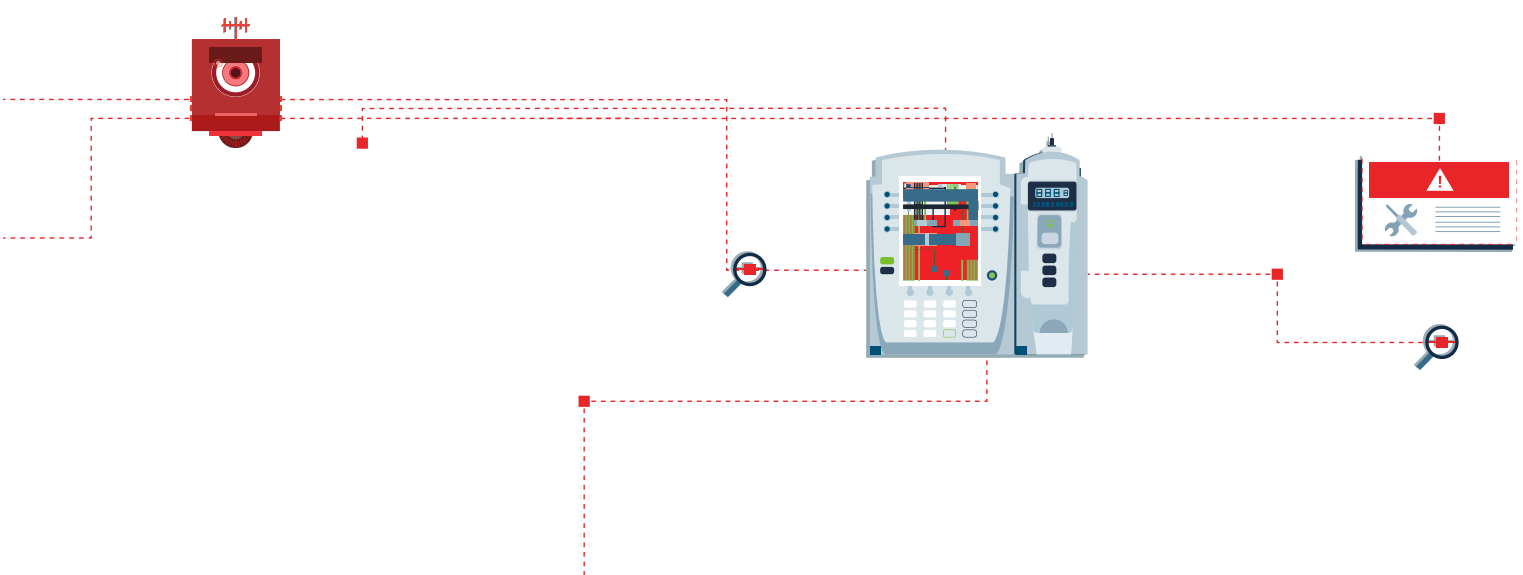
Cynerio found that 73% of all IV pumps—the most ubiquitous medical device at any hospital—have a vulnerability that would jeopardize patient safety, data confidentiality, or service availability if exploited.



Promoting Device Visibility

While they were still in their old facility, MarinHealth deployed Cynerio healthcare IoT risk reduction technology to help the team better understand how their biomedical devices interacted with the network. "We realized that we had basically zero visibility into these devices," Christensen relates. "We knew that in order to secure the devices, we needed to segment the network. And to effectively segment the network, we had to be able to see what was happening."

The Cynerio Customer Success team assisted with the proof of concept (POC) and the initial deployment. "They were very supportive in our efforts," Christensen says. "We had some financial constraints and did not know what scale we could bring to the deployment at the beginning. We also have a very small network and security team—two network engineers and me. The Customer Success team stayed with us and helped us onboard the product. And things blossomed from there."

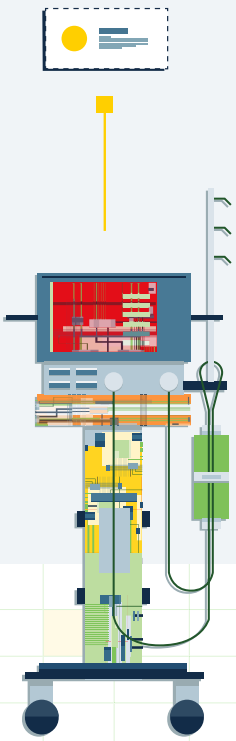


Managing a Malware Event

Not long after Cynerio was fully onboarded, a security incident occurred that wound up being pivotal for both MarinHealth and Cynerio. Looking at the Cynerio console, Christensen saw malicious activity coming from a specific biomedical device running on a legacy operating system. At about the same time, he received an alert about the attack from the Cynerio Customer Success team.

Christensen was able to confirm the command-and-control event using logs from the organization's Cisco Umbrella web filtering solution. "Umbrella was able to tell us that a single IP address was exhibiting anomalous behavior," he describes.

"But with Cynerio, we were able to see which device was potentially infected, and all network activity coming in and out of that device."



Using intelligence from the Cynerio Live research team, the Customer Success team worked with MarinHealth to remediate the malware.

Christensen reached out to the department that owned the system and learned that it was attached to a costly medical device that could not be replaced or removed from the network without negatively impacting patient care. The device's manufacturer was aware of the vulnerability but was unable to issue a patch due to limitations in the legacy operating system. "It turned out that the malware was very old, and was possibly a remnant of a cyber attack we suffered nearly a decade ago," he explains.

Scaling the IoT Security Strategy

Dealing with this event was eye-opening for the MarinHealth team. "We understood that we needed more than just visibility to protect our medical IoT devices," Christensen remembers. "We also needed to use that information to build a micro-segmentation infrastructure." Specifically, the team needed to create an access control list (ACL) for each device so the devices are shielded from everyone not authorized to access them. They began to work with Cynerio to achieve this goal.

The result was that Cynerio quickly became a bigger part of the network planning for the new hospital, which by then was under construction. "We had to add many existing and new medical and biomedical devices to the new network," explains Nader Zamanzadeh, senior network engineer at MarinHealth. "We designed the network for segmentation and realigned them into IP subnets so we could control our ACLs.

"The value add for Cynerio is that we could look at the traffic at the packet level and see what the devices were talking to and where," Zamanzadeh continues. "Without Cynerio, it would have been difficult to tell what the traffic is.

Cynerio is not just looking at the system log; it is sitting on the network looking at the real traffic in real time. Plus, Cynerio's knowledge base on what devices should be doing and how they should be communicating helps us to detect behavior that is out of the ordinary."

Healthcare IoT Attack Detection and Response

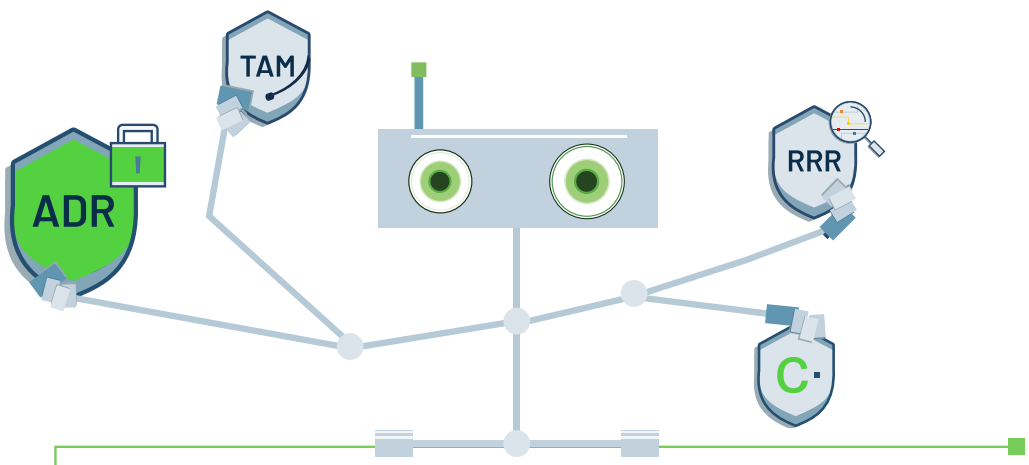
Developing a New Product

The Cynerio team also gained significant insight from the malware event at MarinHealth. "We recognized that this was a very standard attack—something that happens in hospitals on a regular basis," recalls Daniel Brodie, CTO and co-founder of Cynerio.

"We realized that we needed to help our customers more by helping them with threat detection in a way that would address the noise that comes from so many alerts coming from multiple security solutions."

Cynerio worked closely with MarinHealth to develop a new product offering to address these challenges, called Attack Detection and Response (ADR). The hospital participated in many cycles of beta testing and was a charter customer when the product became generally available in early 2022.

ADR is a first-of-its-kind solution that empowers hospitals to discover, contain, and mitigate threats on IoT, operational technology (OT), and Internet-of-Medical Things (IoMT) devices. Its features include alerts about IoT attacks like the one experienced at MarinHealth, containment and quarantine of affected devices in a medically safe manner, post-attack recovery and reporting, and forensics for post-attack investigations.



The Cynerio portal is really designed for system ownership and self-management. So we are encouraging device owners to use the portal themselves and educate themselves on the security risks of their devices."

– Scott Christensen, Security and Systems Engineer, MarinHealth Medical Center

Stopping More Attacks

Since the initial attack at the old facility, two similar incidents have occurred at MarinHealth's new hospital. These cases involved workstations rather than medical devices and the malware was newer. Christensen was able to confirm the malware with MarinHealth's Carbon Black endpoint detection and response (EDR) solution, which reported endpoint activity with some inbound and outbound connections. Since these devices were not providing patient care, he was able to simply remove them from the network.

"We saw that even with standard endpoints, Cynerio was a complement to our EDR system," Christensen contends. "Carbon Black reported the activity, but with Cynerio we could see the malicious signatures."

Looking to the Future

With ADR fully deployed, the MarinHealth team is finalizing the network and security strategy for the new facility. They plan to complete ACLs for all remaining medical IoT devices, sharpen their incident response processes, and put more emphasis on examining forensics after each attack to understand how it occurred—and how a similar event can be prevented in the future.

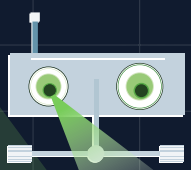
The team also is working to cultivate more of a culture of medical IoT device security across the organization. "The Cynerio portal is really designed for system ownership and self-management," Christensen explains. "So we are encouraging device owners to use the portal themselves and educate themselves on the security risks of their devices."

About Cynerio

Cynerio is the one-stop-shop Healthcare IoT security platform. With solutions that cater to healthcare's every IT need—from Enterprise IoT to OT and IoMT—we promote cross-organizational alignment and give hospitals the control, foresight, and adaptability they require to stay cyber-secure in a constantly evolving threatscape. We give you the power to stay compliant and proactively manage every connection on your own terms with powerful asset management, threat detection, and mitigation tools so you can focus on healthcare's top priority: delivering quality patient care.

Using Cynerio to bring visibility for their IoT devices, and working with them to develop new technology to improve detection and response, has been a win-win for MarinHealth.

"Our partnership with Cynerio has been instrumental in securing our medical devices," Christensen concludes. "This will improve both patient safety and the quality of patient care."



Thank You!

Cynerio

www.cynerio.com