Cynerio

Healthcare IoT Cybersecurity Platform
Secure. Faster.

Attack Detection and Response (ADR) for Healthcare IoT

Solution Overview

Threat actors targeting hospitals are increasingly using connected medical devices and other IoT infrastructure as their way in. With ransomware and breaches on the rise, healthcare providers need to take a more aggressive stance against the attackers targeting them, and the Cynerio IoT Attack Detection and Response for Healthcare module provides the tools to keep patients and the devices connected to them safe from harm from day one. Cynerio's ADR for Healthcare IoT empowers hospitals to immediately identify attacks and quarantine connected devices exhibiting malicious or suspicious activity. Cynerio IoT forensic data then allows for thorough remediation and rapid recovery measures to be carried out when the device is not in use.

Benefits

- ✅ First-of-its-kind solution empowers hospitals to discover, contain and mitigate threats on IoT, OT and IoMT devices

- ✅ Prevent ransomware and other attacks so they don't affect patient health or care

- ✅ Security tailor-made to defend the medical device ecosystem without disrupting healthcare workflows

- ✅ Stop attacks on day one of implementation – no need to wait for inventory or segmentation processes to finish to receive protection

- ✅ Cut through the noise - high-fidelity attack alerts based on deep healthcare IoT expertise

- ✅ Bring live IoT attack intelligence into the visibility of your SIEM and other IT security tools

- ✅ Safely prolong the lifecycles of otherwise unprotectable medical devices

- ✅ Easily extend IT security to IoT with automation, out-of-the-box rules and hands-on help

How Cynerio ADR for Healthcare IoT Works

1 Get alerts about live attacks on medical and other IoT devices

2 Immediately contain and quarantine attacks without disrupting device functionality or patient care

3 Conduct forensic analysis and investigate incidents and understand the scope of attacks

4 Effectively respond to attacks by integrating Cynerio IoT attack visibility with IT security enforcement

5 Compile detailed attack reporting and carry out proactive risk reduction to prevent future attacks

Cynerio ADR for Healthcare IoT Features

IoT Attack Alerts

Get immediate notification of malicious device activity without false positives. Cynerio alerts hospitals to suspicious behavioral anomalies, complemented by attack detection data from other Cynerio deployments, machine learning, and dozens of vulnerability and threat intelligence feeds collected from global sources.

IoT Attack Containment and Quarantine

Any attack observed on a device protected by Cynerio can be immediately isolated in a medically safe manner that enables hospitals to cut off the device's online connections and further remediate the incident later without impacting service availability or patient care.

Cynerio ADR for Healthcare IoT Features

## IoT Attack Forensics for Investigation

Collect detailed forensics on all IoT devices along with the connections between them and investigate device metadata through deep packet inspections. This forensic data can then be ingested by your Security Incident and Event Management (SIEM) platform to enrich attack investigations being carried out across IT infrastructure.

IoT Attack Response

Turn Cynerio into the "brains" of your IoT security and send its data about device risks and attacks to your IT security solutions for enforcement and "muscle." Micro-segmentation, new firewall rules and other remediation measures limit attacker reconnaissance, lateral movement, and ransomware shutdowns, with live agents available to help with the most complex attacks if needed.

IoT Post-Attack Recovery and Reporting
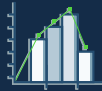
The Cynerio portal is no black box; it shows everything the solution is doing to mitigate live attacks, including detailed reporting on potential PHI exfiltration, how risk exposure is decreasing over time, and step-by-step instructions broken down by affected device and attack type to ensure full remediation and recovery going forward.

Complement with Proactive Risk Reduction

Once you have found and addressed the live threats on connected devices with ADR for Healthcare IoT, give your hospital a more preemptive IoT threat posture in the future. Cynerio's rapid risk reduction finds and remediates the most critical healthcare IoT risks within 30 days so they can't be exploited by attackers as threats evolve.

About Cynerio

Cynerio is the one-stop-shop Healthcare IoT security platform. With solutions that cater to healthcare's every IoT need – from Enterprise IoT to OT and IoMT – we promote cross-organizational alignment and provide hospitals the control, foresight, and adaptability they require to stay cyber-secure in a constantly evolving threatscape. We empower healthcare organizations to stay compliant and proactively manage every connection on their own terms with real-time IoT attack detection & response and rapid risk reduction tools, so that they can focus on a hospital's top priority: delivering quality patient care. For more information visit www.cynerio.com, or follow Cynerio on Facebook, Twitter, and Linkedin.

Forrester
Wave Leader
2020

Gartner
Cool Vendor
2020