SOLUTION BRIEF

Fortinet Cynerio Healthcare IoT Solutions

Real-time and Automated Cybersecurity for Healthcare IT Networks

Cynerio's Healthcare IoT Security combined with the Fortinet Security Fabric ensures safe and expedited cybersecurity for clinical environments.

Joint Solution Components

- Fortinet Security Fabric, FortiGate, FortiNAC, FortiSIEM, FortiSwitch
- Cynerio Healthcare IoT Security Platform

Joint Solution Benefits

- Real-time discovery and visibility into every connected healthcare IoT device pushes the information into the FortiGate Device Inventory
- Medically contextualized device behavior and network topology profiling
- Frictionless deployment and agentless, network-based monitoring
- Multisite deployment and FortiGate integration support
- Real-time alerts sent to the right team members at the right time

Executive Summary

The Cynerio–Fortinet integrations provide healthcare IT security teams with comprehensive insights into risks contextualized according to criticality and care delivery. The frictionless integration delivers enhanced, real-time risk mitigation plans configured according to the NIST Zero-Trust framework to ensure clinical network security, medical service continuity, patient safety, and data confidentiality.

The Rise of Healthcare IoT and the Growing Threatscape

The growing footprint of healthcare Internet-of-Things (IoT) devices is transforming the healthcare industry by accelerating medical procedures and giving patients more control over their medical data and treatment. While increased connectivity affords patients and medical professionals convenience and more accessibility to care, these advancements are widening the attack surface and opening the door for bad actors to exploit healthcare organizations.

Healthcare providers are a particularly attractive target for attackers because of the sensitive patient information they hold (ePHI, Social Security numbers, credit cards, etc.), and because their IT systems are critical to patient care, they create opportunities for extortion. Incidents of MEDJACK (hijacks of medical devices), ransomware, and denial- of-service (DoS) attacks are increasing astronomically. These attacks can disrupt device functionality, deny access to patient records, and slow down hospital networks, which can result in significant fiscal and reputational damage to the hospital, and even patient deaths.

The inherent vulnerabilities of healthcare IoT devices (enterprise IoT, operational technology [OT] systems, and Internet of Medical Things [IoMT]) combined with weak security have made healthcare the easiest, most advantageous and lucrative of targets for threat actors.

- 300% rise in cyberattacks on healthcare since January 2020
- 90% of all healthcare organizations have reported a breach
- 40% of assets run an unsupported operating system (OS)
- 65% of hospitals have low confidence in asset visibility

Healthcare IoT Security's Prime Obstacle

Healthcare IoT devices require regular communications with internal and external endpoints to function optimally and maintain normal clinical operations. For example, medical devices routinely connect to external vendors for software updates and other maintenance procedures, without which their functionality would suffer. Many medical devices also connect to workstations and other devices on the internal network to function properly (e.g., MRI machines and DICOM viewers).

Herein lies the challenge: Every connection adds to a healthcare organization's attack surface and must not be permitted to go unchecked despite many necessary north-south and east-west communications. Traditional IT security tools lack the healthcare insights required to recognize medical and other healthcare IoT devices and their unique behaviors as standard. Implementing security policies blind to clinical context risks device slowdown or shutdown, disrupting medical services and jeopardizing patients.

The Power of Integration

How the Cynerio–Fortinet Integration Works (Joint Solution Description)

1. Using Cynerio's asset discovery, FortiGate Device Inventory provides a single-pane- of-glass view of a hospital's IT network with clinically contextualized inventory and classification for all connected assets, including enterprise IoT, OT systems, and medical devices. Security administrators can implement policies on IoT devices in the same fashion they implement policies for IT devices.
2. Cynerio's asset profiling and operational insights determine devices' uses and roles within clinical workflows, along with which communications with external endpoints are standard versus anomalous and/or suspicious.
3. Cynerio's clinical-impact risk scoring assesses the risk level of every asset on an individual and organizational basis by factoring in hospital-specific workflows, network topography, the asset's clinical criticality, and impact on patient outcomes.
4. Virtual segmentation automatically defines policies and allows them to be tested and edited before they're enforced through the Fortinet Security Fabric. This way, healthcare IT teams can be confident threats are stopped in their tracks and that critical communications and medical services continue uninterrupted.
5. Once verified, the Fortinet Security Fabric enables automatic policy enforcement, macro and microsegmentation, and threat response through the FortiGate next-generation firewall (NGFW), switches, and FortiNAC, facilitating packet filtering, intrusion detection, and malware detection.

Joint Solution Components (contd.)

- Cynerio's Virtual Segmentation capability automatically defines policy that can be edited and tested for violations before being enforced by FortiGate or FortiNAC
- Cynerio automatically updates policies and policy addresses as they're enforced by switches (e.g., FortiSwitches) and firewalls
- Safe risk mitigation with segmentation policies infused with clinical context
- High-performance FortiSwitches and FortiGate firewalls enforce policies and prevent intrusions and unauthorized device-to-device communications
- Firewall affords granular control and visibility of users and devices for thousands of discrete applications
- Third-party and vendor access management in concert with FortiGate

Use Cases

Zero-Trust Segmentation of Critical Clinical Devices

Cynerio understands which devices are most at risk on healthcare IT networks (e.g., IV pumps) and which ones need to be protected using segmentation. Cynerio then maps out expected communications behaviors and automatically creates remediation policies based on the NIST Zero-Trust security framework. Policies can be tested virtually to gain confidence that they will not interrupt clinical services and workflows before being pushed to the Fortinet Security Fabric and enforced by the firewall, switch, or network access control (NAC), ensuring attack surface reduction and robust security.

Vendor Access Management

A third-party vendor has access to the hospital's network and is attempting to access it. Cynerio identifies the source as a medical device vendor, locates every device on the network to which the vendor is authorized to connect, and compiles a list of services (patching, OS updates, etc.) the vendor is authorized to conduct on approved devices. Cynerio pushes all of this information into the Fortinet Security Fabric and the FortiGate NGFW allows it to conduct routine maintenance, implement patches, and ensure optimal device functionality while blocking all other unauthorized communications.

Misconfigured Devices

Cynerio identifies devices on the hospital's network that allow access to public communications (e.g., web browsing, Windows updates, etc.) and unauthorized device-to-device connections (access for device maintenance). Cynerio continuously monitors communications, sends real-time alerts on anomalous activity, and suggests policies to limit these communications, enabling hospitals to enforce them through the Fortinet Security Fabric.

Joint Solution Components

Cynerio

Cynerio configures policies infused with clinical security intelligence that can be seamlessly pushed into Fortinet Fabric-Ready Firewall (NGFW), FortiSwitches, and FortiNAC. Using Cynerio's Virtual Segmentation capability, teams can test policies for violations and edit them as needed before enforcing them on the live network. Once policies have been approved, Cynerio syncs with the Fortinet Security Fabric to enforce the policies through FortiGate and FortiNAC and extend them over hospitals' multisite IT networks.

Cynerio is an artificial intelligence (AI)-powered, full-suite healthcare IoT platform that takes a risk-based approach to cybersecurity and asset management to help hospitals achieve security fast. It adapts to rapidly evolving threats, technological advancements, and healthcare industry standards. Empowering hospitals with foresight and a toolbox of easily deployable, scalable, and adaptable IT security solutions tailored to healthcare, Cynerio gives hospitals the ability to act fast, ensure compliance, and maintain robust security posture.

Fortinet

FortiNAC

FortiNAC is the Fortinet network access control (NAC) solution that enhances the Security Fabric with control, and automated response for everything that connects to the network. FortiNAC provides protection against IoT threats, extends control to third-party devices, and orchestrates automatic responses to a wide range of networking events. Cynerio's software acquires immense downstream IoT device data that when combined with FortiNAC can be leveraged to act appropriately to anomalous activity with great surgical precision. Execution of policies occurs at the lowest layers of the infrastructure, allowing microsegmentation to occur with the least amount of disruption and maximum isolation.

FortiGate

FortiGate NGFWs utilize purpose-built security processors and threat-intelligence security services from FortiGuard Labs to deliver top-rated protection, as well as high-performance inspection of clear-texted and encrypted traffic. FortiGate NGFWs reduce cost and complexity by providing full visibility into applications, users, and networks. The benefit of FortiGate working in concert with FortiNAC provides higher layer awareness, so policy intelligence can be applied in a way that is most effective.

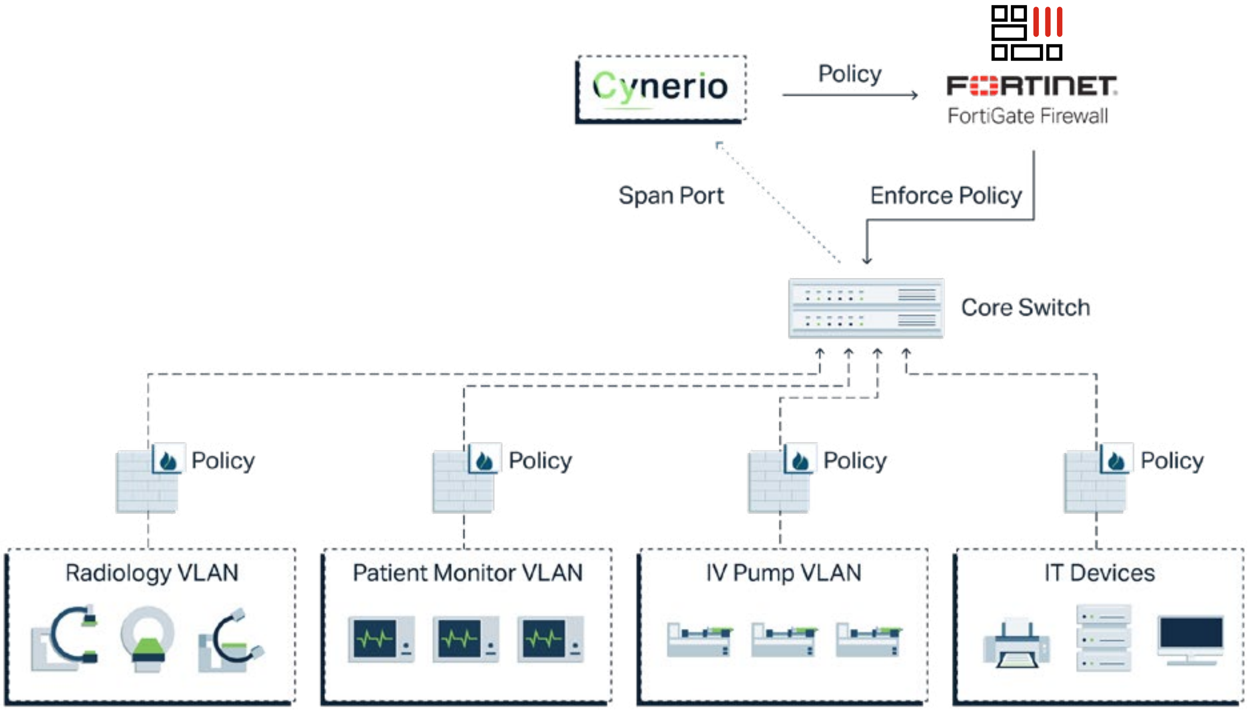

Figure 1: Fortinet FortiGate architecture diagram.

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 put your focus on what matters most: your patients. For more information, visit us at www.cynerio.com.

September 20, 2021 1:41 PM

Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 3:sb-fortinet-and-cynerio-healthcare-iot-solutions_092021:sb-fortinet-and-cynerio-healthcare-iot-solutions_092021

792694-A-0-EN