Cyber Security Solution for Healthcare IoT

Secure Any Connected Device to Ensure Patient Safety and Ongoing Healthcare Services

MAIN BENEFITS:

Instantly secure all your existing IoT devices and safely implement new ones.

Cut down security man hours with auto-detection and remediation of threats.

Keep critical medical processes undisrupted with adaptive policies and no need to patch devices.

MAIN CAPABILITIES:

Risk Analysis: expose all your IoT related risks.

Auto-segmentation: minimize your risk exposure with auto-generated policies.

Threat Prevention: Blocks known and Zero-day attacks.

TAILORED FOR DIFFERENT IOT ENVIRONMENTS IN HOSPITALS:

Smart Building

Camera

Thermostat

Elevators

Smart Office

Printer

Light Bulb

TV

Medical Devices

Clinical Refrigerator

Patient Bed

PACS server

Infusion Pump

MRI

Connected Devices: Hospitals' Biggest Security Gap

While connecting Internet-of-Things (IoT) devices to the clinical network delivers clear benefits for hospitals and clinics, it also exposes them to new cyber-threats. From infusion pumps, patient monitors, and MRI machines to clinical refrigerators and even wheelchairs, IoT devices are inherently vulnerable and easy to hack. Many of these devices run on unpatched software, are misconfigured, or use unsecured communication protocols. Furthermore, hospitals own extensive and diverse device inventories of multiple vendors, models, and functionalities, with many shadow un-managed devices (connected to the network without anyone's knowledge).

And while healthcare IoT environments have become increasingly complex, IT security solutions have remained far behind, with limited visibility and control over IoT devices and their associated risks. This security gap increases the risk of a successful cyber-attack where critical devices can be shut down, damaged, manipulated, or used to infect other systems on the network. Mainly to steal patient data (PHI), or to launch ransomware attacks. It is time to take action and keep every device secure.

Check Point Cyber Security Solution for Healthcare IoT

Check Point offers the industry's most comprehensive cyber-security solution for healthcare IoT, keeping any connected device on the clinical network protected. That includes medical devices, smart office, and smart Building devices.

With clinical domain expertise, the solution prevents IoT related attacks and continually minimizes IoT attack surfaces. All in a way that is easily scalable and non-disruptive to critical medical processes.

Main solution capabilities:

- IoT Risk Analysis: Expose All your IoT Related Risks.
- Auto-Segmentation: Minimize your Risk Exposure with Auto-generated IoT Policies.
- Threat Prevention – Block Known and Unknown IoT Related Attacks.

Solution components:

CHECK POINT SECURITY MANAGEMENT

CHECK POINT SECURITY GATEWAYS

IoT DISCOVERY ENGINE
TECHNOLOGY PARTNERS:
CYBER MDX
MEDIGATE
ARMIS
ordr
Cynerio

IoT NANO AGENT

How It Works

1. IoT Risk Analysis: Expose All your IoT Related Risks

The solution continually performs a comprehensive risk analysis of your entire IoT environment to expose all the risks associated with your devices at any given moment. From a single console, you can view all your connected devices classified based on their risk level, and even drill down for a risk analysis per device.

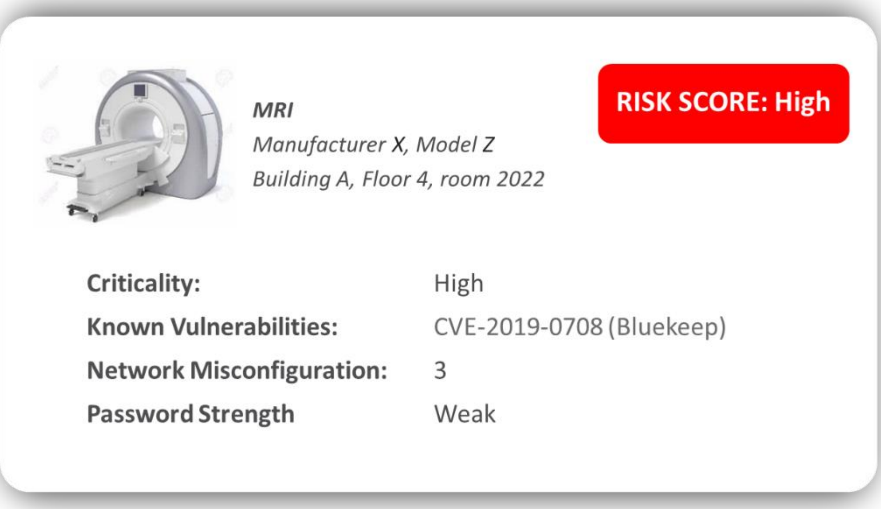
IoT Risk Analysis is based on three sources:

a. **IoT Discovery-** by integrating with third-party IoT discovery platforms, the solution auto-identifies all your devices, tags them based on their attributes (e.g., device type, manufacturer, model, firmware version, and MAC address), and analyzes their behavior in real-time to detect anomalies. Powered by the industry's largest ecosystem of IoT discovery, it is capable of identifying hundreds of thousands of IoT device profiles across different IoT environments, including medical devices, clinical IoT, smart office, and smart building.

b. **Firmware Risk Assessment**- exposing inherent security flaws associated with the firmware of every connected device (and also with embedded third-party components) including:

- Weak credentials: easily brute-forced, publicly available, or unchangeable credentials.
- Known vulnerabilities: list of all CVEs classified based on their severity and attack vector (Network/physical attack).
- Suspicious listed domains
- Hardcoded security flaws, such as operating system misconfiguration.

c. **IoT-specific Threat Intelligence –** the solution identifies IoT threat trends and malicious patterns via Check Point's *ThreatCloud*, which aggregates threat indicators (IoCs) from over 100 Million gateways, endpoints, and IoT devices worldwide.



MRI
Manufacturer X, Model Z
Building A, Floor 4, room 2022

RISK SCORE: High

Criticality:	High
Known Vulnerabilities:	CVE-2019-0708 (Bluekeep)
Network Misconfiguration:	3
Password Strength	Weak

Figure 1: Drill down for a risk analysis per device

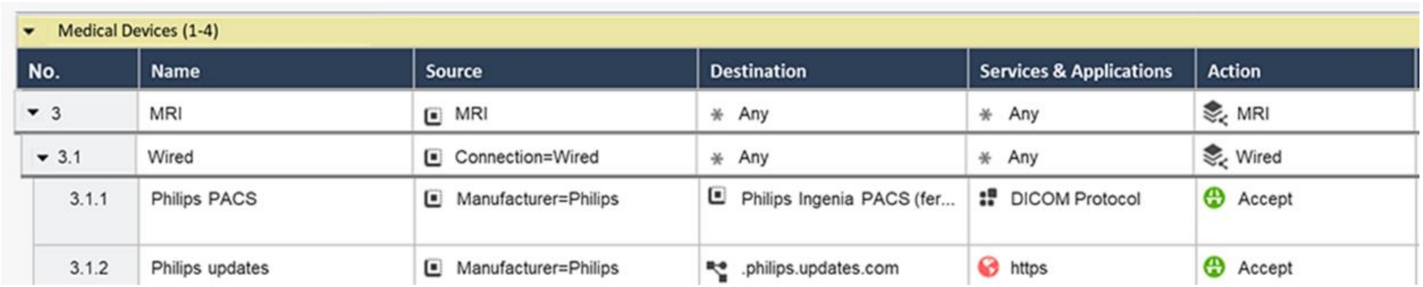
2. Auto-Segmentation: Minimize your Risk Exposure with Auto-generated IoT Policies.

Based on the IoT risk analysis, the solution automatically generates and enforces a policy for every device in your environment. This automated process saves you months of manual policy configurations and ensures your IoT devices are secure from the first moment they connect to your network.

These auto-generated policies instantly minimize your IoT attack surfaces by creating network segmentation, one that allows only authorized access to (and from) your IoT devices and ensures devices use only communication protocols they were designed to use.

Example policy use cases:

- Prevent medical imaging devices from communicating with nurse workstations.
- Allow ultrasound machines to communicate with PACS servers using the DICOM protocol only.
- Prevent high-risk devices (e.g., MRI, CT) from communicating using unsecured protocols (e.g., HTTP).



Medical Devices (1-4)

No.	Name	Source	Destination	Services & Applications	Action
3	MRI	MRI	Any	Any	MRI
3.1	Wired	Connection=Wired	Any	Any	Wired
3.1.1	Philips PACS	Manufacturer=Philips	Philips Ingenia PACS (fer...	DICOM Protocol	Accept
3.1.2	Philips updates	Manufacturer=Philips	.philips.updates.com	https	Accept

Figure 2: Auto-generated Policy Example for MRI machine

In the policy example in Figure 3, rule 3 defines an access policy for the MRI machines.

- Rule 3.1.1 allows Philips MRI machines, with a wired connection, to communicate with the Philips dedicated PACS server, via DICOM protocol only.
- Rule 3.1.2 allows them to also communicate with the specific manufacturer domain (philips.updates.com) using only HTTPS protocol.

3. Threat Prevention – Block Known and Unknown IoT Related Attacks

Based on the IoT risk analysis, the solution automatically activates security protections against known and Zero-day IoT related attacks, both for network-based and device-level attacks.

a. **On-Device Runtime Protection**: monitors the behavior of the device at run-time and blocks known and unknown device-level attacks before the device is compromised. Examples of attacks are shell injection, memory corruption, and control flow hijacking.

b. **Protect unpatched devices from known exploits:** automatically activates security protections against known CVEs through virtual patching, by installing the appropriate IPS signatures on the gateways (over 300 available signatures for IoT related threats). That allows effective protection against unpatched devices or devices running on legacy operating systems and software; without disrupting critical processes and business operations.

Summary

While Healthcare IoT devices are extremely vulnerable and easy to hack, they are also poorly, or not at all, protected. Check Point enables you to reduce exposure to the IoT cyber-risk and proactively mitigate IoT related threats and vulnerabilities, without disrupting critical medical processes.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com