SOLUTION BRIEF

CyberMDX | We protect the things that protect human lives.™

Enrich Policy with IoT and Medical Device Security

By integrating CyberMDX's and Check Point's IoT security solutions, HDOs can manage their devices in one place — from visibility to classification & policy enforcement. Together, it's an umbrella solution that can monitor and protect the entire clinical network.

Check Point
SOFTWARE TECHNOLOGIES LTD

Solution

CyberMDX delivers its granular IoT and medical device security visibility into functional attack prevention by integrating with Check Point NGFW to enforce smart generated security policies.

CyberMDX uses Device-Centric Risk Management (DCRM) to provide on-going risk assessment of all healthcare assets including vulnerability and compliance profiles. The solution then offers a prioritized list of asset groups and recommended actions to remediate or mitigate the risks associated with these assets on three distinct protection layers: on-device, on-network, on-perimeter.

The classified assets are then pushed to the Check Point NGFW platform, tagging the devices using its IoT API. In addition, tagging mechanisms are further leveraged in order to create recommended policy for a set of similar devices.

This highly structured classification methodology and deep understanding of clinical IT environments coupled with Check Point NGFW's enforcement, streamlines the production and implementation of security policies. Without that, a great deal of manual labor would be required.

Use Cases

Enrich Check Point with CyberMDX Classification

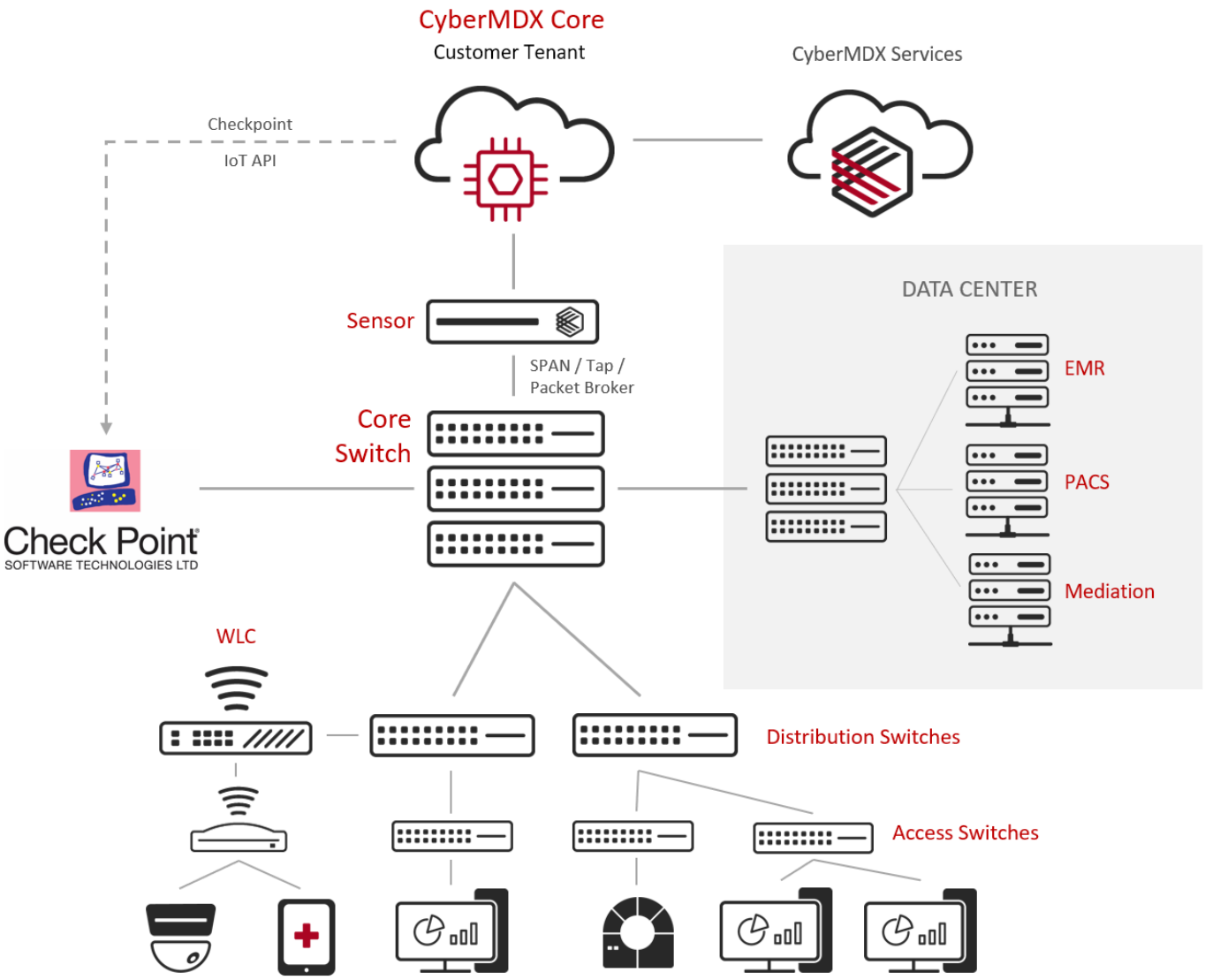
- Tag devices with DCRM classification data and risk-level to enable Checkpoint NGFW to use tags for apply tailored / specific access rules. The enriching data includes identification of medical devices, device type, device model, firmware, location, and more.
- CyberMDX dynamically registers IPs in Checkpoint – keeping the firewall aware of the precise identity of a device behind an internal IP address.

A Joint Solution for Policy and IoT Security

Combines the CyberMDX visibility and detection capabilities with Check Point's Security Gateway to provide healthcare organizations with a comprehensive defense equipped with layers of protection.

Key Features

- Identifies and classifies clinical assets, including medical devices and IoMT
- Auto tags devices with classification data and risk score levels
- Provides policy planning to generate context-aware policies for the entire clinical network
- Continuously detects and mitigates device vulnerabilities through IPS/IDS virtual patching



This diagram illustrates how this integration works in a two layer network architecture and a stand-alone NGFW

Enhance Check Point NGFW with CyberMDX Classification Policies

- Push recommended policies to Checkpoint FW to restrict network access between assets.
- Using Check Point IoT Security Manager, and CyberMDX's DCRM, you can configure context-aware security policies derived by the specific attributes of your medical and IoMT devices to create the following segmentation use cases:
  - Protocol restriction (e.g., Infusion Pump can talk to the PAC server only using DICOM protocol)

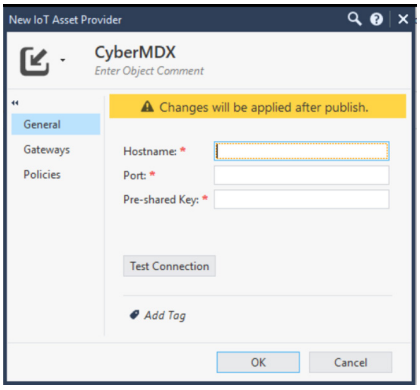
- Out-of-manufacturer-scope restriction (e.g., Philips MRI machines can communicate with a specific Internet domain for SW update)
- Risk score restrictions (e.g., deny access from MRI machines to Internet domains)

- The policies are enforced by perimeter or internal segmentation firewalls in an on-going, automated and scalable way.

Virtual Patching of Medical Devices and IoMT

- Continuously detect vulnerabilities relevant to medical and IoMT devices, and mitigate them through virtual patching of the Check Point NGFW with the appropriate IDS/IPS signatures. That enables you to protect devices running on legacy or unpatchable systems and software.

The diagrams illustrates how CyberMDX enriches the data and streamlines the security policies inside Check Point's firewall



Medical Devices (1-4)

No.	Name	Source	Destination	Services & Applications	Action	Track	Install On
1	Patient Monitoring	Philips IntelliBridge EC10 P...	Philips InteliVue MX450 P...	Any	Accept	Log	Policy Targets
2	High Risk	Risk=HIGH	Any	Any	High Risk	NA	Policy Targets
2.1	Wireless	Connection=Wireless	External Zone	Any	Drop	Log	Policy Targets
3	MRI	MRI	Any	Any	MRI	NA	Policy Targets
3.1	Wired	Connection=Wired	Any	Any	Wired	NA	Policy Targets
3.1.1	Philips PACS	Manufacturer=Philips	Philips Ingenia PACS (fer...	DICOM Protocol	Accept	Log, Accounting	Policy Targets
3.1.2	Philips updates	Manufacturer=Philips	.philips.updates.com	https	Accept	Log	Policy Targets
4	E.C.G.	ECG	Any	Any	E.C.G.	NA	Policy Targets
4.1	E.C.G. PACS	Manufacturer=Belkin Inter...	Belkin International Inc. I...	DICOM Protocol	Accept	Log, Accounting	Policy Targets

About CyberMDX

CyberMDX is an IoT security leader dedicated to protecting the quality care of health delivery worldwide. CyberMDX provides cloud-based cyber security solutions that support the advancement of The Internet of Medical Things. The CyberMDX solution identifies endpoints and assesses vulnerabilities to detect, respond to, and prevent cyber incidents. Deployed worldwide, CyberMDX is designed to integrate with our customers' existing environments through its scalable, easy-to-deploy and agentless solution.

CyberMDX

Contact us today for more information:
cybermdx.com • info@cybermdx.com