The CyberMDX - Check Point Solution

CyberMDX delivers its granular Internet of Medical Things visibility into functional attack prevention by integrating with Check Point IoT Security Solution to enforce smart generated security policies.

All hospital assets are auto-identified and classified by CyberMDX’s AI engine. The classified assets are then pushed to the Check Point IoT Security 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.

The recommended policies are based on CyberMDX’s Smart-Isolation planning tool which creates context-aware network access policies, tailored to the specific clinical network, and enforced using Check Point’s firewalls. CyberMDX also maintains Check Point concurrence with asset IP addresses (even when those addresses are dynamic).

This highly structured classification methodology, coupled with CyberMDX’s deep understanding of clinical IT environments and Check Point IoT Security Solution’s enforcement, streamlines the production and implementation of finely tuned and robust security policies that would otherwise only be possible with a great deal of manual labor..

The diagram below illustrates how this integration works in a two layer network architecture and a stand-alone NGFW.
Enrich Check Point with CyberMDX Classification

- Tag devices with MDefend classification data and risk-level to enable Checkpoint IoT Security to use tags for apply tailored / specific access rules. The enriching data includes identification of medical devices, device type, device make and more.

- MDefend dynamically registers IPs in Checkpoint – keeping the firewall aware of the precise identity of a device behind an internal IP address.

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 MDefend’s Smart-Isolation policies, 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 – For example: CT scanner can talk to the PAC server only using DICOM protocol.
  - Out-of-manufacturer-scope restriction - For example: Phillips MRI machines can communicate with a specific Internet domain for SW update.
  - Risk score restrictions – For example: Deny access from a highly vulnerable MRI to Internet domains.

- The policies are enforced by perimeter and/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.

Diagrams illustrate how CyberMDX enriches the data and streamlines the security policies inside Check Point’s firewall.

IoT Security Management Console