SOLUTION BRIEF

Fortinet and CyberMDX Healthcare Security Solution

Comprehensive Visibility and Threat Prevention for Medical Devices and IoMT

Executive Summary

Fortinet and CyberMDX ensure healthcare delivery organizations have complete visibility of all Internet-of-Things (IoT) and medical devices on their network to keep patients safe and maintain critical and essential operations without disruption. Integration with FortiNAC and FortiGate delivers granular insight through a single integrated point of view.

Challenge

Healthcare providers are experiencing increased growth in IoT and unmanaged devices. With this massive adoption in digitization, the attack surface is significantly increasing, creating greater cyber threat exposure. Healthcare organizations are especially vulnerable, given their data is the most sought-after target by bad actors. Additionally, cybersecurity expertise is becoming more scarce, necessitating tools that deliver maximum visibility, simplicity, and automation. Below are four of the most common instances why healthcare organizations are seeking these powerful tools so their cyber practitioners can deliver greater value to the business.

- Lack of device visibility, classification, and policy enforcement into connected devices, both managed and unmanaged
- Vulnerable medical and Internet-of-Medical-Things (IoMT) devices: Many of these devices are exposed to persistent cyber risk as they run unpatched software, are misconfigured, and lack adequate security controls to meaningfully compensate for those shortcomings
- Increasing number of unmanaged connected assets (the endpoint is not a member of Active Directory nor running a management agent)
- Microsegmentation: While microsegmentation is highly effective and resilient from a security perspective, it is quite problematic from an implementation and execution perspective. To properly employ microsegmentation, one needs to identify and classify all the devices connecting to the network, as well as understanding their operational context and IT semantics.

Joint Solution

CyberMDX delivers its granular IoMT visibility into functional attack prevention by integrating with Fortinet FortiGate and FortiNAC to enforce smart generated security policies.

All hospital assets are auto identified and classified by CyberMDX's artificial intelligence (AI) engine. The classified assets are then pushed to the Fortinet FortiGate platform, tagging the devices using Fortinet native application programming interfaces (APIs). In addition, tagging mechanisms are further leveraged in order to create recommended policy for a set of similar devices.

Joint Solution Components

- CyberMDX Healthcare Security Solution
- Fortinet FortiManager, FortiGate, FortiNAC

Joint Solution Benefits

- Auto-identify and classify clinical assets, including medical devices and IoMT
- Auto-tag devices inside FortiNAC with CyberMDX's high-granular classification and risk level
- Use the tags to create and enforce context-aware policies for the entire clinical network, to secure the clinical assets while reducing their attack surface
- Enhance segmentation and microsegmentation processes via automated planning, based on CyberMDX's generated device classifications and context-aware monitoring—saving labor and resources while reducing human errors
- Streamline incident response via FortiNAC's quarantine capability
- Incident response: Once signs of compromise or significant deviations from baseline, you can streamline a response using FortiNAC capabilities to initiate quarantine procedures (assignment to an isolated VLAN)—containing the threat while limiting its impact

FORTINET FABRIC-READY

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 FortiNAC and/or FortiGate. CyberMDX also maintains 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 Fortinet 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.

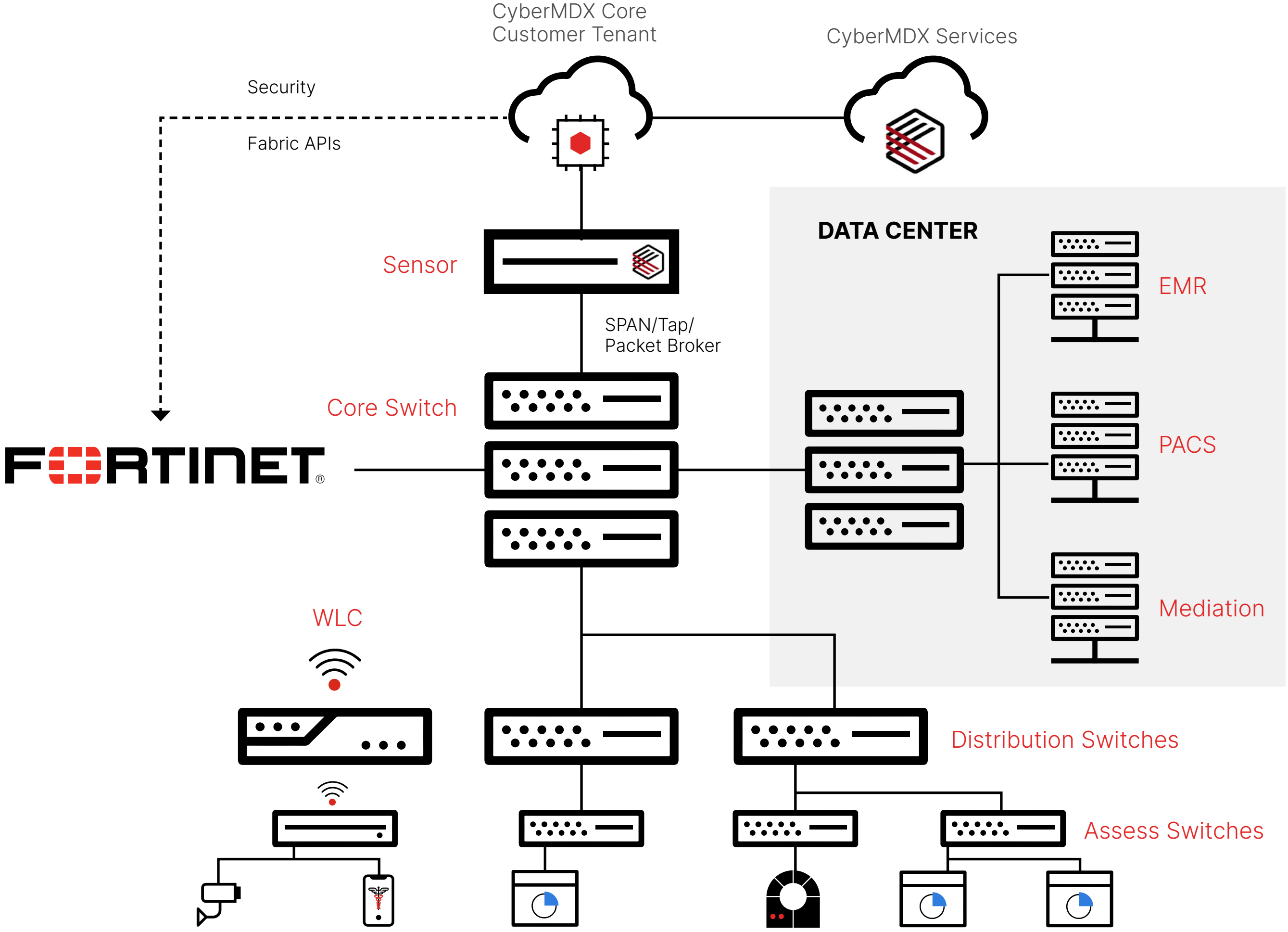
Joint Solution Components

Based on its deep packet inspection and AI engine, the CyberMDX Healthcare Security Solution automatically identifies and classifies all medical devices and assets in a clinical network to form an accurate live inventory. This high-granularity accounting includes the device's type, vendor, model, versions, and hardware IDs (MAC, SN) and clinical network context. On top of this asset mapping, a per-device risk analysis is carried out based on known vulnerabilities, detected threats, original research, and deviations observed from baseline performance measures.

Together, this itemized inventory and individualized risk assessment provide comprehensive visibility into devices and their cybersecurity posture. This data can be pushed to security policy enforcers, boosting their classification functionality and providing them with finely tuned and context-aware policies.

Joint Solution Integration

The Fortinet Security Fabric, including FortiManager, FortiGate, and FortiNac, integration with CyberMDX Healthcare Security Solution allows to leverage the CyberMDX deep classification and risk posture together with Fortinet enforcement capability to one tailored holistic solution that allows the ability to protect the organization assets without any effect on the functionality of the assets and organization.



Joint Use Cases

Use case #1: Clinical Network Hygiene—FortiNAC With CyberMDX

Tag devices within FortiNAC with CyberMDX classification data and risk level to streamline network hygiene. The enriching data includes identification of medical devices, device type, device make and more. This data is used by FortiNAC to apply virtual local-area network (VLAN) assignment policies and downloadable access control lists with the help of CyberMDX's planning tool, to achieve a complete microsegmentation of the clinical network.

Use case #2: Attack Prevention via Network Traffic Restriction—FortiGate With CyberMDX

Tag devices within FortiGate with CyberMDX classification data and risk level and automatically create address groups of similar devices. These address groups can be used within FortiGate to create firewall policies, based on CyberMDX's planning. These context-aware policies, when enforced, block unwanted or malicious communications, hence reducing the attack surface.

About CyberMDX

CyberMDX is an IoT security leader dedicated to protecting the quality care of health delivery worldwide. The CyberMDX Healthcare Security Suite portfolio identifies, categorizes, and protects connected medical devices—ensuring resiliency as well as patient safety and data privacy. With CyberMDX's continuous endpoint discovery & mapping, comprehensive risk assessment, AI-powered containment & response, and operational analytics, risks are surgically mitigated, and assets optimized.

October 19, 2021 1:48 AM
1316101-A-0-EN