MEDIGATE FORTINET

INTEGRATION

Protecting Medical and IoT Devices in Clinical Networks

Cybersecurity for healthcare organizations with IoT & IoMT

The exploding number of medical and IoT devices within clinical networks has created an urgency for healthcare delivery organizations to ensure they have visibility into every device connecting and effective measures in place to keep operations and patient care safe from the potential risks they pose. The HIPAA Journal reported that 82% of healthcare organizations experienced a cyberattack on their IoT devices in a 12 month span – the attacks threatened to steal patient data, compromise end user safety, and put intellectual property and the hospital's reputation at risk.

To protect their information and resources, healthcare organizations need to accurately identify and then effectively mitigate the threats from all these IoT and IoMT devices. However, medical devices are not like general IoT devices. They tend to be more fragile, use different protocols, and can even be connected to patients, which means general discovery and mitigation tactics may be ineffective or too disruptive. It takes deep clinical expertise to be able to identify these different devices and understand the role they play in clinical workflows and patient care to establish safe, secure access policies and remediation actions.

Medigate has become a Fortinet Fabric-Ready Partner via the Fortinet Open Fabric Ecosystem Partner Program. As a result, Medigate has leveraged Fortinet's open API's to apply deep integrations into several Fortinet solutions thus becoming an integral part of the Fortinet Security Fabric. Medigate and Fortinet's resulting partnership brings together the clinical and cybersecurity expertise healthcare delivery organizations require to effectively understand, manage and prevent security risks and events that IoT and IoMT introduce to their network. With Medigate and Fortinet, hospitals have the visibility and insights they need to accurately inventory all assets, assess risks, and automate the enforcement of security policies that keep patient data and clinical networks safe.

The Medigate – Fortinet Solution

The Medigate Device Security and Asset Management Platform integrates with Fortinet's next generation firewall, FortiGate, and Fortinet's network access control solution, FortiNAC, to provide hospitals the deep clinical expertise needed to accurately identify and analyze all connected IoT and IoMT devices in their network. This information helps streamline the ongoing management and maintenance of medical devices and automate the enforcement of dynamic access and micro-segmentation policies that keep the network safe.

The solution also maps all internal and external communications of connected devices to proactively detect suspicious activity that deviates from expected clinical workflows and intended manufacturer behaviors. Once threats are detected, access restrictions can be triggered and enforced by FortiGate and FortiNAC to contain the attack and mitigate the risk to the hospital's network to strengthen their overall security posture.

How it Works

The Medigate Platform continuously monitors the network, using deep packet inspection (DPI) to provide a real-time inventory of all the medical and IoT devices connecting and alerting on risky or anomalous activity. Medigate feeds this information, via Fortinet's Fabric-Ready APIs to FortiNAC and transfers IP-based tags to FortiGate, which matches the IP of a device with a tag based on its type, vendor and model. This enables the automated creation and precise enforcement of clinically-driven NAC and firewall policies to prevent risky communications and attack propagation.

Key Capabilities of the Solution

Visibility and Insights

- After collecting network traffic, the Medigate Platform discovers and fingerprints all connected medical and IoT devices using deep packet inspection (DPI) techniques.
- Through integations with other IT management systems and feeds from external sources, Medigate also identifies device locations and available patches and updates.

- Medigate feeds the detailed medical and IoT device information, which includes manufacturer, make, model, OS, software versions, embedded software, etc., to FortiNAC and FortiGate to ensure they have complete and accurate inventories and device profiles.

- Medigate also assesses the risks of each device, based on medical standards and clinical procedures.

Detection and Prevention

- The Medigate Platform analyzes network traffic to monitor device behaviors, examining network and device protocols and drawing on a clinical understanding of a device's expected behavior.

- The Medigate Platform identifies anomalous behaviors and alerts administrators with precise incident information.

- Administrators can take immediate action against suspicious devices through a variety of FortiGate and FortiNAC mechanisms, such as quarantining the device, restricting Internet access, or placing the device in a separate VLAN, to mitigate risks.

Clinical Policy Enforcement

- FortiGate and FortiNAC use Medigate's device and threat data to streamline firewall rules and access policy creation and enforcement.

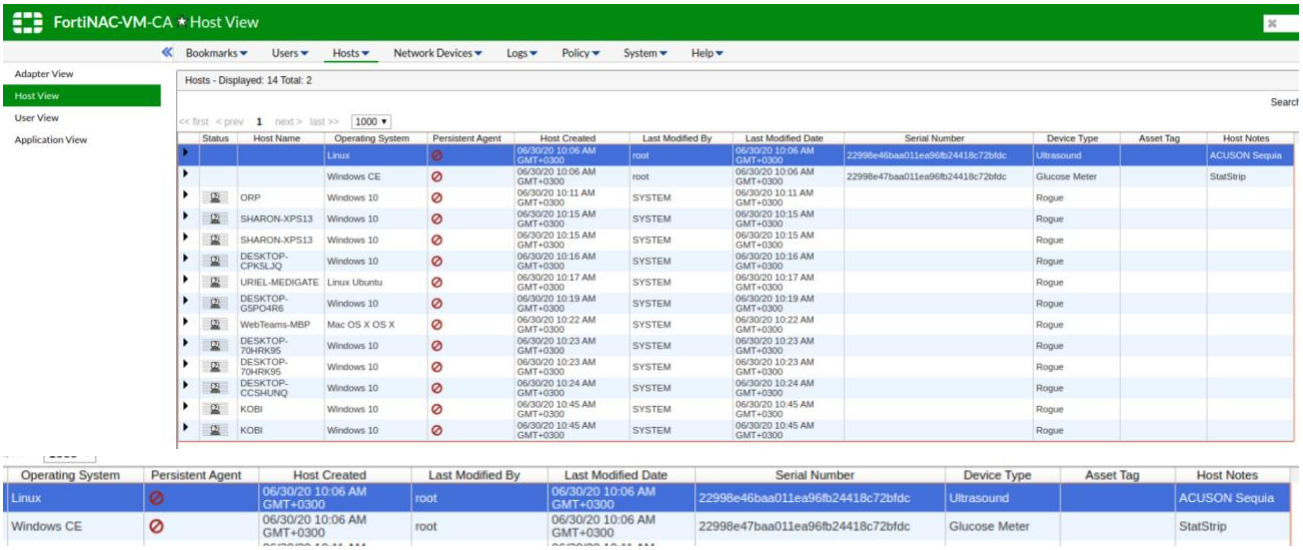
- The Medigate Platform can provide recommendations for clinically-vetted policies, based on the role and behavior of the different devices on the network. It can also recommend specific device and network segmenation policies that group devices by types and functionality to ensure patient care remains uninterrupted and safe.

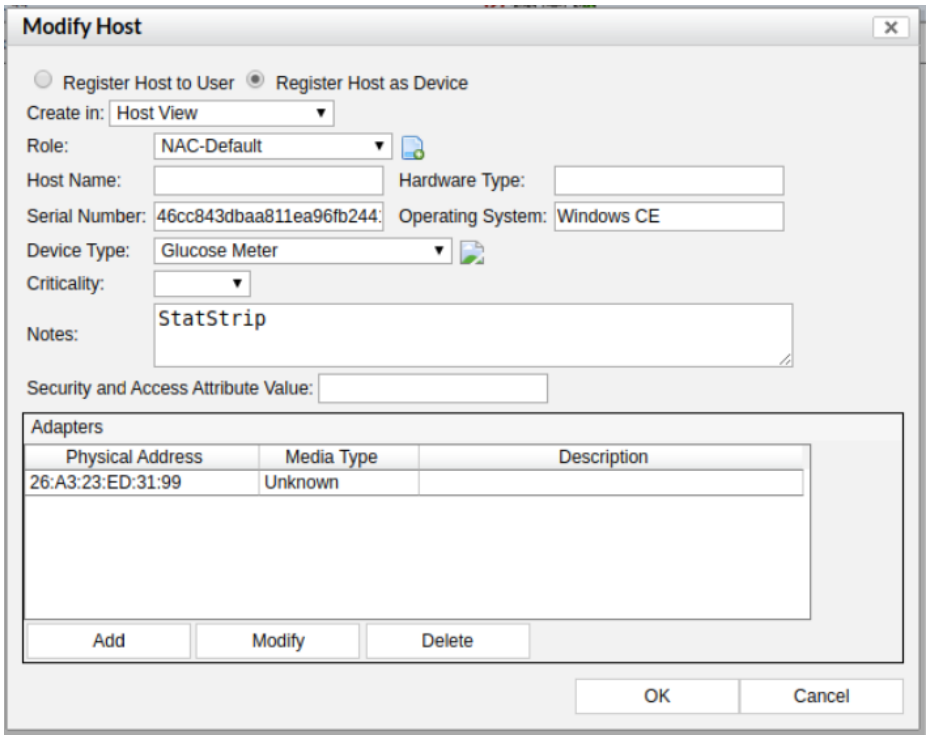
- FortiGate can dynamically create and enforce firewall policies, not just by IPs, but also network zones, tag-to-tag traffic, ports and protocols, that block malicious communications in real time, without affecting the operation of the medical device under attack, to establish a zero trust security stance.

- FortiNAC can establish micro-segmentation and access policies in real-time to contain attacks and ensure only appropriate access to resources.

Clinical Policy Enforcement via FortiGate and FortiNAC

1. The Medigate Platform fingerprints medical IoT devices and creates a detailed profile for each, which is fed into FortiGate and FortiNAC:





2. FortiNAC leverages the attributes populated by Medigate to adjust authorization policies and ensure safe network access.

3. FortiGate attaches devices to relevant device groups leveraging the custom tags. Those groups are used to enforce firewall policies on the network.

Redefining Clinical Network Security

Medigate and Fortinet apply healthcare expertise and an understanding of clinical networks – including manufacturer operating systems (OSes), proprietary protocols, clinical workflows, and expected device functionality – to the creation and enforcement of effective network access and firewall policies. Together, hospitals have what they need to accurately identify devices, pinpoint and assess risks, and enforce security policies and establish clincially-vetted segmentation that will keep their data and operations secure.