SOLUTION BRIEF

Fortinet and Medigate Protecting Clinical Networks

Dynamic Policy Enforcement That Keeps Medical and IoMT Devices Safe

Executive Summary

Fortinet and Medigate have partnered to give hospitals the visibility they need into all their medical, Internet-of-Medical-Things (IoMT), and Internet-of-Things (IoT) devices and the tools to confidently automate the enforcement of dynamic access and microsegmentation policies to keep their network safe.

Challenge

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.

Joint Solution

Medigate has become a Fortinet Fabric-Ready Partner via the Fortinet Open Fabric Ecosystem Partner Program. As a result, Medigate has leveraged Fortinet open application programming interfaces (APIs) 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 and assess risks, and automate the enforcement of security policies that keep patient data and clinical networks safe.

Solution Components

- Medigate Medical Device and Asset Management Platform
- Fortinet FortiGate Next-Generation Firewall
- FortiNAC

Joint Solution Benefits

- Gain complete visibility into connected medical, IoMT, and IoT devices
- Take immediate action against suspicious devices to mitigate risks
- Dynamically create and enforce policies to block malicious communications in real time and establish a zero-trust stance
- Establish microsegmentation to prevent attack propagation

FORTINET Fabric-Ready

Joint Solution Components

- **Medigate Medical Device and Asset Management Platform**
  Medigate's medical device security and asset management platform combines medical workflow, device identity, and clinical protocol knowledge with the latest cybersecurity threats, to enable hospital networks to operate existing and new medical devices on their network while ensuring patient privacy and safety.
- **Fortinet FortiGate**
  FortiGate next-generation firewalls (NGFWs) utilize purpose-built security processors and threat-intelligence security services from artificial intelligence (AI)-powered FortiGuard Labs to deliver top-rated protection and high-performance inspection of clear-texted and encrypted traffic. NGFWs reduce cost and complexity with full visibility into applications, users, and networks and provide best-of-breed security. Other products that complement FortiGate's security profile include FortiGate Secure Web Gateway and the FortiWeb.
- **Fortinet FortiNAC**
  FortiNAC is the Fortinet network access control (NAC) solution that enhances the Security Fabric. FortiNAC provides protection against IoT threats, extends control to third-party devices, and orchestrates automatic responses to a wide range of networking events.

Joint Solution Integration

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 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.

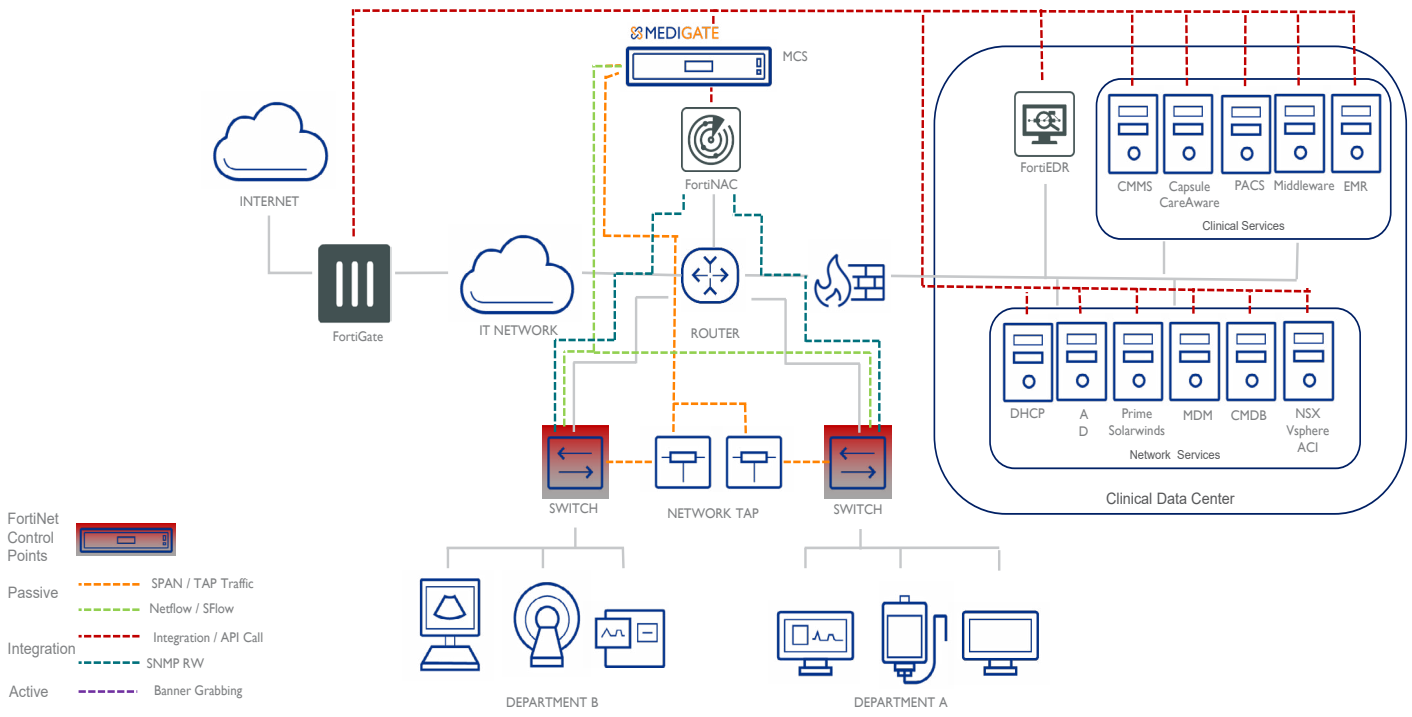

Figure 1: Marketecture: Medigate visibility and Fortinet control.

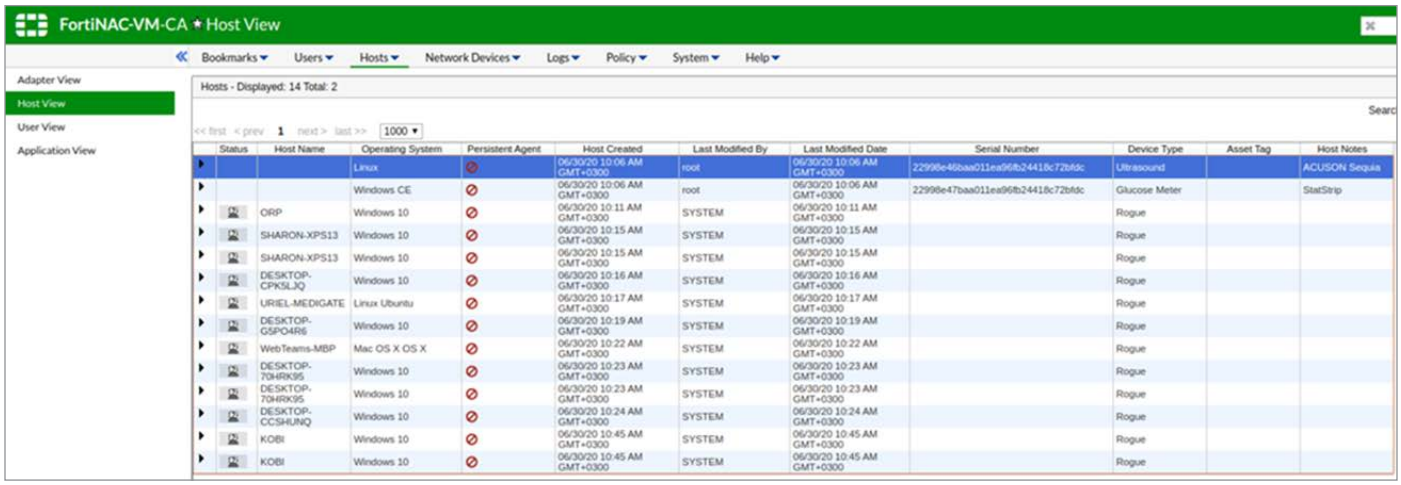

Figure 2: FortiNAC and FortiGate leverage device attributes populated by Medigate to adjust policies to ensure safe network access.

Joint Use Case

Clinical Policy Enforcement

The Medigate platform seamlessly integrates detailed device profiles into FortiGate and FortiNAC to block malicious communications in real time without affecting the operation of the medical device under attack. Organizations have the tools they need to implement microsegmentation best practices and support advanced, zero-trust security policies. Granular policy enforcement through segmentation also allows more efficient virtual local-area network (VLAN) and access control list (ACL) assignment and enables remediation of threats.

About Medigate

Medigate provides the industry's first and leading dedicated medical device security and asset management platform, enabling providers to deliver secure, connected care. Medigate fuses the knowledge and understanding of medical workflows and device identity and protocols with the reality of today's cybersecurity threats. With Medigate, hospital networks can safely operate all medical devices on their network, enabling deployment of existing and new devices to patients while ensuring privacy and safety.

October 3, 2020 5:00 AM

796107-0-0-EN

D:\Fortinet\Solution Brief\Grey Solution Brief\Medigate\sb-fortinet-and-medigate-protecting-clinical-networks-1032020\sb-fortinet-and-medigate-protecting-clinical-networks-1032020