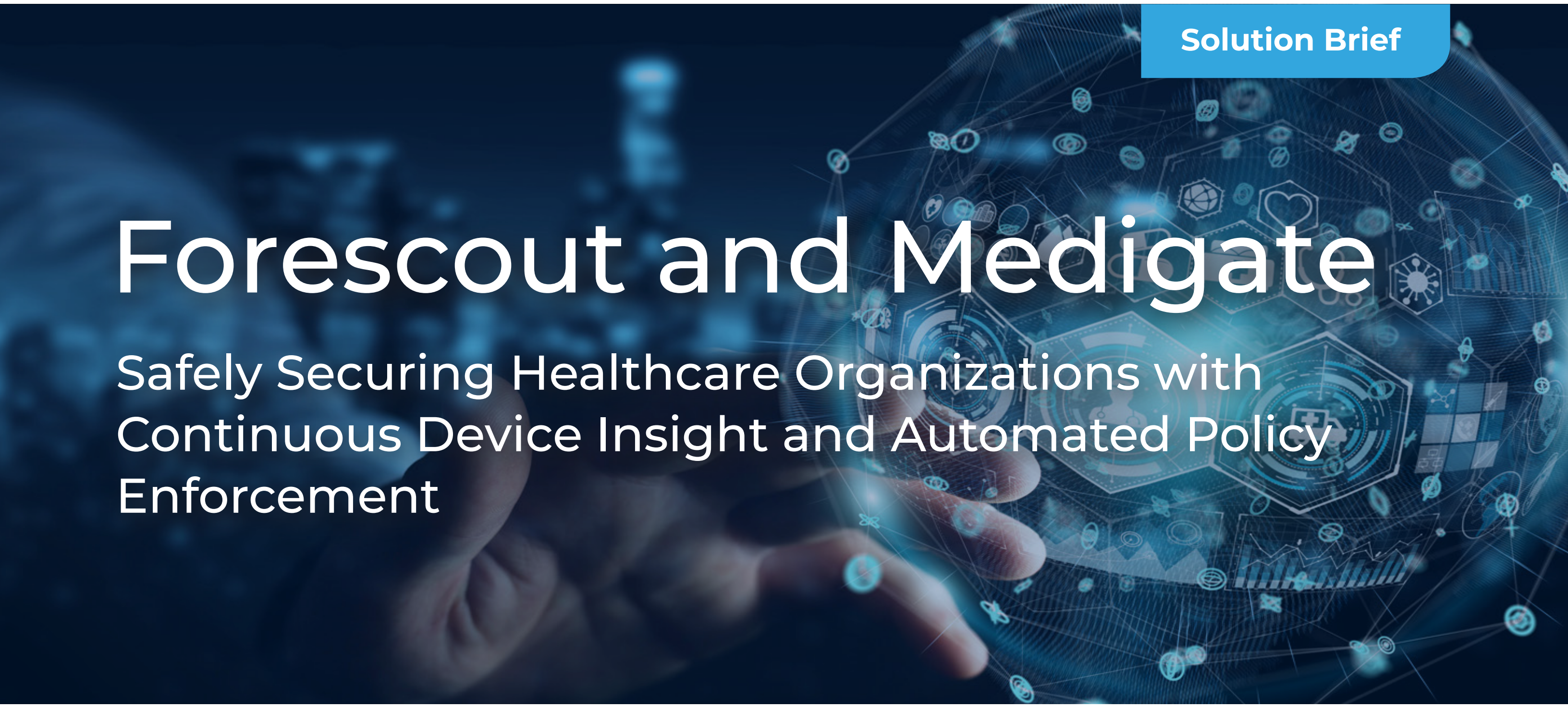


Solution Brief

Forescout and Medigate

Safely Securing Healthcare Organizations with Continuous Device Insight and Automated Policy Enforcement

> “The IoT endpoint market in Healthcare is forecasted to hit .36B units in 2020, a growth of 29% year-over-year.” [1]
>
> — Gartner

The Challenge

Today’s IP-enabled medical devices, better known as the Internet of Medical Things (IoMT) devices, have improved the quality of care offered by health delivery organizations (HDOs). IoMT devices can lower costs, reduce errors and waste and enable better performance and asset tracking. The U.S. Food and Drug Administration (FDA) classifies and regulates medical devices according to their function and risk to patients. Subject to strict FDA requirements, medical device manufacturers spend much of a product’s lifecycle in rigorous testing. However, with time-to-market, cost and other pressures, many medical devices can still enter the market and become placed on clinical networks, putting healthcare organizations as well as patients at risk.

Clinical networks naturally place patient safety as the number-one priority. Disruption of service to key devices such as infusion pumps, implantable pacemakers, pulse generators and automated external defibrillators could result in loss of life. Therefore, organizations are unwilling to take such devices down for long periods of time to patch and update them to the latest firmware or operating system. This can leave them more vulnerable to cyberattacks. Further increasing risk is the fact that clinical networks are now typically connected to corporate IT networks containing commonly vulnerable IoT systems such as security cameras, point-of-sale devices and HVAC/building automation systems, as well as myriad corporate and guest mobile IT endpoints.

Benefits

- Gain passive and in-depth insight into clinical devices
- Reduce IoMT management overhead and compliance costs
- Mitigate risk by continuously enforcing device security and configuration compliance
- Streamline adoption of new IoMT and IoT innovations

Highlights

- Enterprise-scale device lifecycle, performance and security management
- Real-time IoT, IoMT, IT and OT device discovery, classification and assessment
- Rich medical device context, threat and vulnerability management
- Dynamic access control and segmentation enforcement without affecting operations
- Targeted policy enforcement based on rich contextual device profiles
- Automated remediation processes leveraging orchestration with leading security and management vendors

Security, IT and clinical engineering teams alike are challenged with discovering and monitoring a vast array of device types that often speak proprietary protocols. Even when these teams discover previously unknown devices, they are not always able to obtain the depth of details needed for effective management and security. Healthcare organizations must continuously see, assess and collect rich contextual information about devices beyond the basics. This context is crucial in order to implement granular access control, segmentation and other policies to properly protect clinical data and patient care services as well as meet regulatory compliance such as HIPAA and HITRUST.

The Solution

Forescout and Medigate have joined forces to provide a unique solution for healthcare organizations that continuously discovers, assesses and classifies all IoMT, IoT, operational technology (OT) and IT devices, streamlining and simplifying management while also mitigating risk of compromise across heterogeneous device types and network tiers.

Medigate is a leader in providing cybersecurity and clinical asset management for HDOs. Utilizing the industry-leading medical device signature database developed by Medigate Research Labs, the solution fingerprints each device with deep packet inspection (DPI) techniques and collects deep contextual medical device information, enabling dynamic medical device inventory management and facilitating passive and advanced vulnerability detection and prevention capabilities without requiring the use of software agents.

Forescout leads the market in IT, IoT and operational technology (OT) device visibility and control. Forescout provides agentless, continuous and absolute device visibility, paired with data insight and context-aware, policy-driven controls to mitigate and remediate risk in real time.

Together, Forescout and Medigate products protect healthcare organizations and patient digital services with advanced cybersecurity and device management. This is achieved by automatically sharing information for increased device intelligence, proactively detecting and reducing vulnerabilities/threats, granularly enforcing segmentation and network access rules, plus immediately containing medical device threats while facilitating remediation without harming patent safety.

Achieving Healthier Healthcare Operations

The integration between Forescout and Medigate products provides a practical solution that fits seamlessly into existing corporate and clinical networks, while supporting HDO needs for 100-percent uptime, reduced costs and protection of patient data and services. Our joint solution provides:

- Automatic discovery, identification and classification of all connected devices
- Comprehensive, contextually rich device intelligence for enhanced device lifecycle and security management
- Passive monitoring for device performance, vulnerabilities and compliance
- Dynamic segmentation, access control and threat containment for devices across the campus, clinical network, data center and cloud instances at scale
- Streamlined, provable compliance with frameworks like HITRUST and regulations such as HIPAA

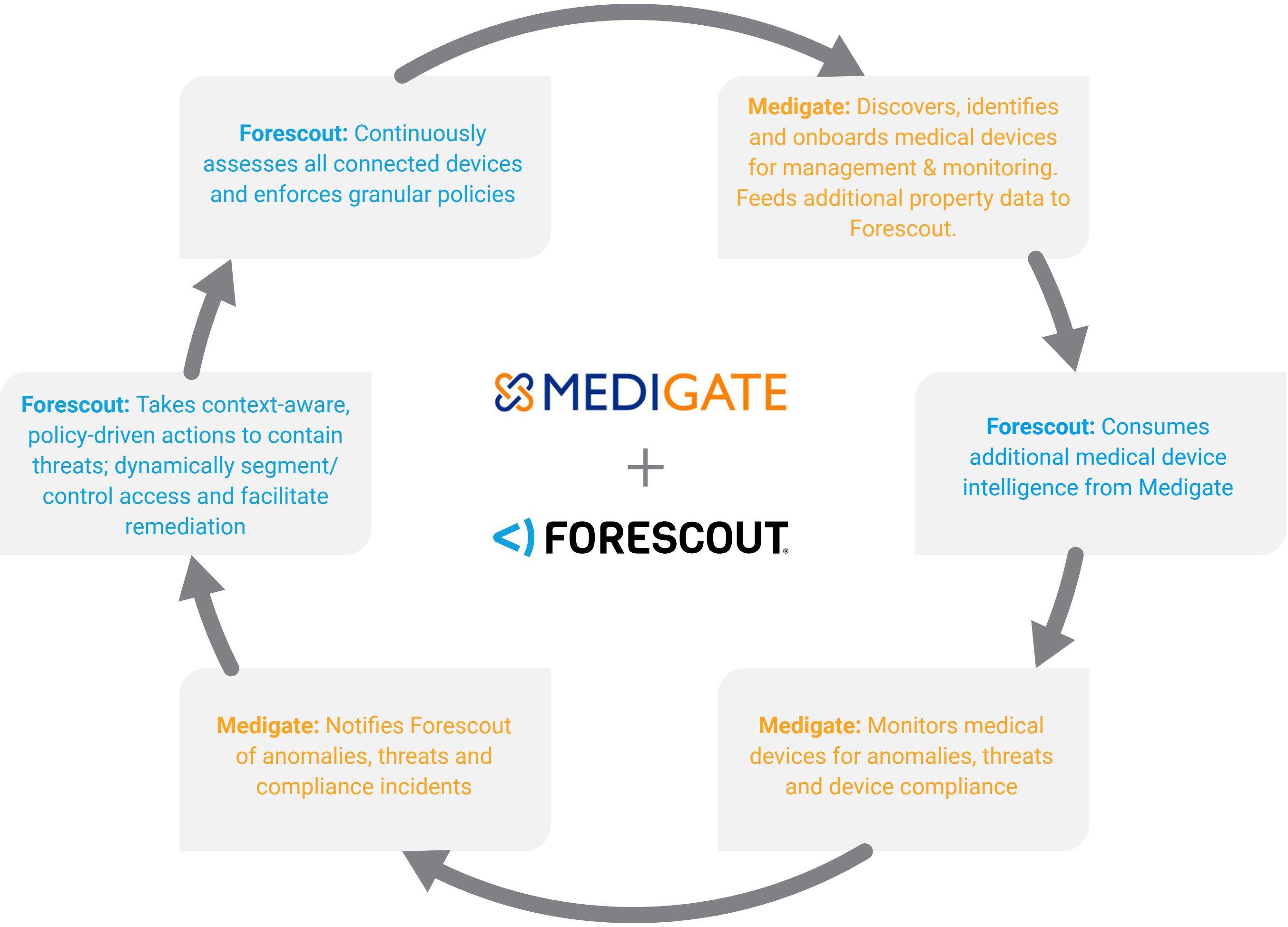
> “Forescout is a force multiplier. The visibility and automation ability that it gives the security department, it’s invaluable.”
>
> – CISO, major Florida medical center

How it Works

HDOs rely on technology principles such as device visibility, network access control and segmentation to be the foundation of network security and device compliance. Medigate’s knowledge of clinical workflows and device functionality, as well as its extensive database of medical device expected behaviors and proprietary protocols, are instrumental for effectively protecting clinical networks and services.

The Forescout platform now integrates with Medigate technologies to apply real-time, deep medical device information to automatically enforce granular access control, segmentation and other compliance policies for clinical networks. The Forescout platform also extends these capabilities across all connected devices in the HDO for a cohesive, centralized device and control platform. Additionally, as the Medigate platform detects medical device vulnerabilities or threats, it notifies the Forescout platform which immediately contains threats and can help facilitate remediation. Once a device is remediated, the Forescout platform allows it back on network per policy.

Both companies’ technologies use passive monitoring and deep packet inspection to collectively provide in-depth and accurate device data. Below are the details on how the integration creates the end-to-end device compliance and network security that is critically important for clinical networks:



Forescout: Continuously assesses all connected devices and enforces granular policies

Medigate: Discovers, identifies and onboards medical devices for management & monitoring. Feeds additional property data to Forescout.

Forescout: Consumes additional medical device intelligence from Medigate

Medigate: Monitors medical devices for anomalies, threats and device compliance

Medigate: Notifies Forescout of anomalies, threats and compliance incidents

Forescout: Takes context-aware, policy-driven actions to contain threats; dynamically segment/ control access and facilitate remediation

MEDIGATE + FORESCOUT

How both platforms work together to reduce cybersecurity risk

Summary

Together, the Forescout and Medigate platforms dramatically improve IoMT, IoT, IT and OT device discovery, classification, monitoring, management and security. The joint solution helps organizations gain rich, contextual insight into their clinical and IT networks, benefit from sophisticated clinical network analysis to detect threats and implement granular policies to automatically enforce network access control, segmentation, device compliance and contain threats.

Automating security and management processes based on rich contextual, real-time device intelligence, reduces operational costs and risk while increasing corporate IT and clinical engineering staff efficiency. Ultimately, corporate and patient data and services are better protected, new healthcare innovations can be fostered and more positive patient outcomes achieved.

FORESCOUT + MEDIGATE

[1] Gartner Press Release on IoT Trends, August 2019: https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io

To learn more, contact Medigate@Forescout.com or visit
Forescout.com and Medigate.io

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591