Medical Device Security

Access unmatched coverage for your hospital – IT, OT, IoT and IoMT – with a single cybersecurity platform

FORESCOUT

Our solution delivers unparalleled insight and control for your entire healthcare delivery organization's network without disrupting critical business processes.

Quickly pinpoint, prioritize and proactively mitigate risks across your clinical and enterprise-wide network.

Key Features

- Our ability to cover IT, OT, IoT and IoMT ensures superior visibility and cybersecurity for health-care delivery organization networks
- Comprehensive device and network insight through a single integrated point of view
- Automatic device classification and risk score levels
- Dynamic context-aware network access and segmentation controls that increase efficiency while reducing human errors

Solution Overview

With so many connected devices and diverse motives driving bad actors, hospitals have become a cyber battleground. Medical devices introduce a wide range of operating systems and communication protocols and cannot tolerate endpoint agents. Therefore, traditional cybersecurity solutions cannot adequately protect these critical systems.

Forescout's unique approach to medical device security delivers unparalleled insights and control for the entire network without disrupting critical business processes or impacting patient care. The Forescout® Platform is an easy-to-deploy, integrated solution that provides unmatched visibility and protection for IT, medical and IoT devices, ensuring operational continuity along with patient and data safety.

Our solution provides agentless security that continuously identifies and assesses enterprise-wide devices as they connect to a hospital's network. In addition, it enriches medical device profiles and automates policy-driven network access control, segmentation and threat response based on real-time rich, contextual asset intelligence.

Features and Benefits

Intelligent auto-classification

The Forescout Platform combines diverse discovery techniques with cloud-powered intelligence for every medical device connected to your clinical network. This high-fidelity auto-classification of all medical devices includes granular analysis of function, configuration and unique IoMT factors such as FDA class and MSD2 information. Based on our patented deep packet inspection and selective active queries, we can automatically identify and classify all medical assets in a clinical network to provide an accurate, live inventory. This high granularity accounting includes the device's type, vendor, model, software version and hardware IDs (MAC, SN).

Now hospitals can eliminate blind spots and minimize operational risk across the organization by having in-depth visibility into:

- Laptops, tablets, smartphones, BYOD/guest systems and work-from-home devices
- IoT and IT devices across campus, data center, cloud, branch, remote site and edge networks
- Medical devices connected to clinical networks, including infusion pumps, patient monitors, imaging systems and more

Medical asset risk assessment

To safeguard the clinical network, you must first understand the attack surface, then quantify the exposure, vulnerabilities and configuration issues that could pose a risk to patient care and business operations or become the entry point for a cyber breach.

An essential element to success is to have a clear and concise understanding of the configuration requirements, FDA class, criticality and recall status for every medical device. Correlating vulnerability data with the CISA Known Exploited Vulnerabilities catalog and EPSS scoring further enhances the accuracy of an asset's risk score.

Three steps to achieving an accurate assessment of risk:

- Understand configuration requirements by classification and correlate vulnerability exploitability and likelihood through exposed ports
- Determine device criticality by function to provide additional context such as FDA class and recall status
- Track the configuration and behavior changes of each asset to detect anomalies that may increase the risk of compromise, such as internet exposure

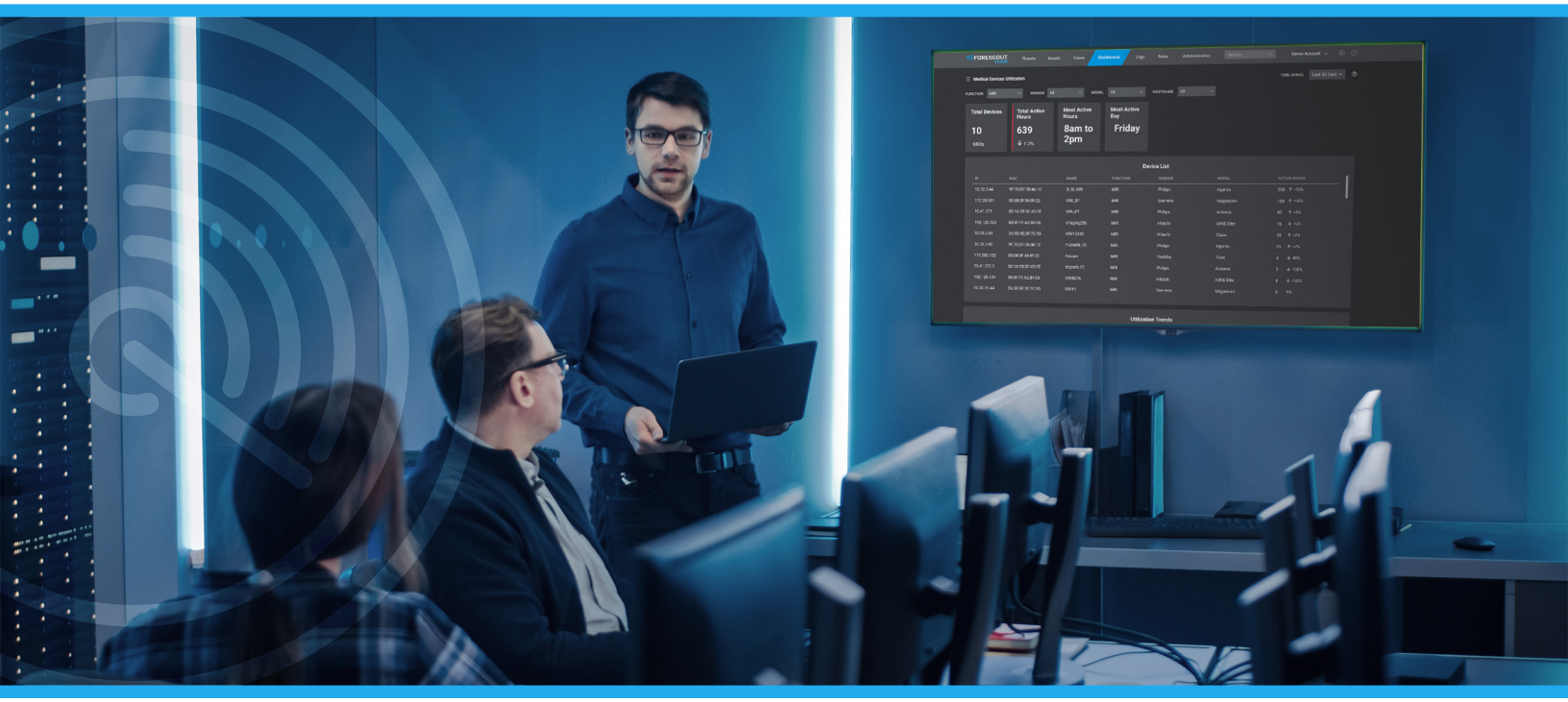
Automated remediation workflows

The Forescout Platform also facilitates security event response by implementing automated workflows to initiate and coordinate policy-based remediation and mitigation actions based on prioritized risk factors, which not only streamlines incident response but also contributes to improved mean time to resolution (MTTR). By responding quickly to real threats using existing security tools, organizations can effectively reduce alert fatigue, allowing security teams to focus on important tasks instead of being overwhelmed by irrelevant alerts. Forescout supports the design and implementation of zero trust policies, enabling you to automatically classify and categorize clinical assets into meaningful groups based on their workloads. Then simply define group-based segmentation or access policies that reflect only the required communication between groups or the least trusted access relationships. We also automatically generate proactive security policies based on granular medical device insight and send these policies to the Forescout platform for deployment and enforcement. This streamlines an otherwise resource-intensive process, drastically reducing the potential attack surface and protecting critical processes from disruption.

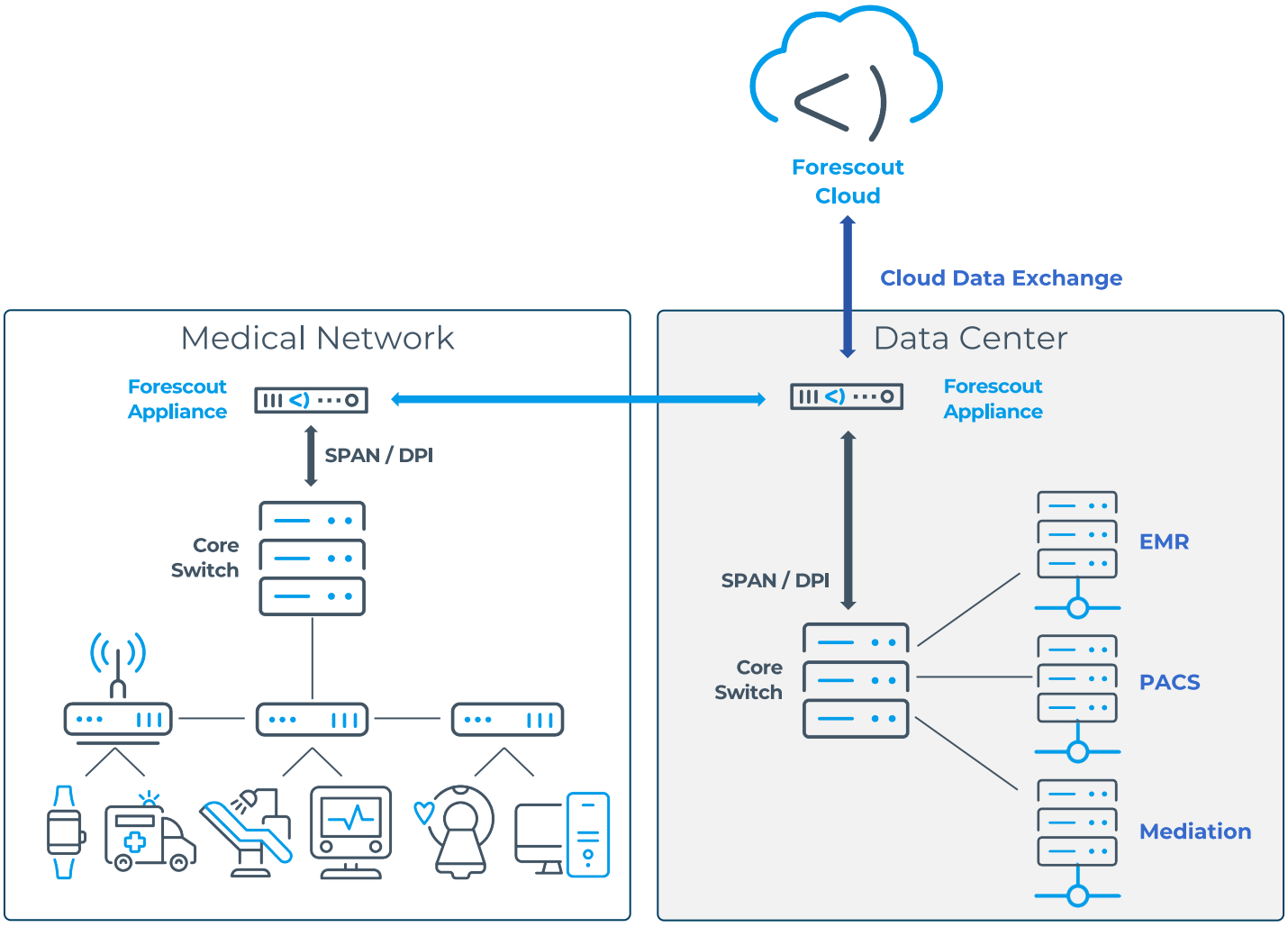
Increased Operational Efficiency

Security teams can reduce operational overhead for asset management by leveraging both real-time and persistent rich, contextual device data to accelerate incident investigation and root cause analysis. Proactively identifying high-risk assets and exposure gaps enables analysts to formulate and then automate remediation processes.

Combining medical device-specific alert data and clinical network logs also aids incident investigation, while eliminating alert noise due to nuisance alerts and false positives enables better detection and faster response to true threats.



Forescout Medical Device Security Architecture



Empower your healthcare organization with unparalleled cybersecurity resilience

Leverage Forescout's innovative solutions to ensure the protection of your medical devices and IoMT landscape. Don't wait for threats to emerge—proactively secure your network, protect patient data, and maintain operational continuity. Contact Forescout today to learn more about our security platform and take the first step towards a safer healthcare environment.

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com