Take Action Now

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

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 Medical Device Security, part of the Forescout Continuum Platform, can deliver zero-touch threat prevention through an easy-to-deploy, integrated solution that provides unmatched visibility and protection for medical and IoT devices, as well as IT 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 device visibility.

Features and Benefits

Intelligent auto-classification

Zero-trust policies can only be enforced when grounded in complete device context, and gathering this context manually is nearly impossible. Based on our deep packet inspection and AI engine, 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

Clinical asset risk assessment

An essential element of zero trust is to understand the security posture and risk profile of all connected devices. Our device-centric risk management (DCRM) approach provides ongoing risk assessment of healthcare medical device assets including vulnerability and compliance profiles. The solution then offers a prioritized list of asset groups and recommended actions to remediate or mitigate the risks associated with these assets on three distinct protection layers: on-device, on-network, on-perimeter.

The classified asset profiles are then pushed to the Forescout Device Cloud to enrich the data repository of real-time asset profiles that iincludes IT, IoT, OT and IoMT. We provide a unified enterprise-wide device visibility view along with a centralized policy engine that continuously assesses all connected devices for policy compliance and automates policy enforcement through heterogeneous enforcement points such as network infrastructure, next-gen firewalls, and endpoint management and security tools.

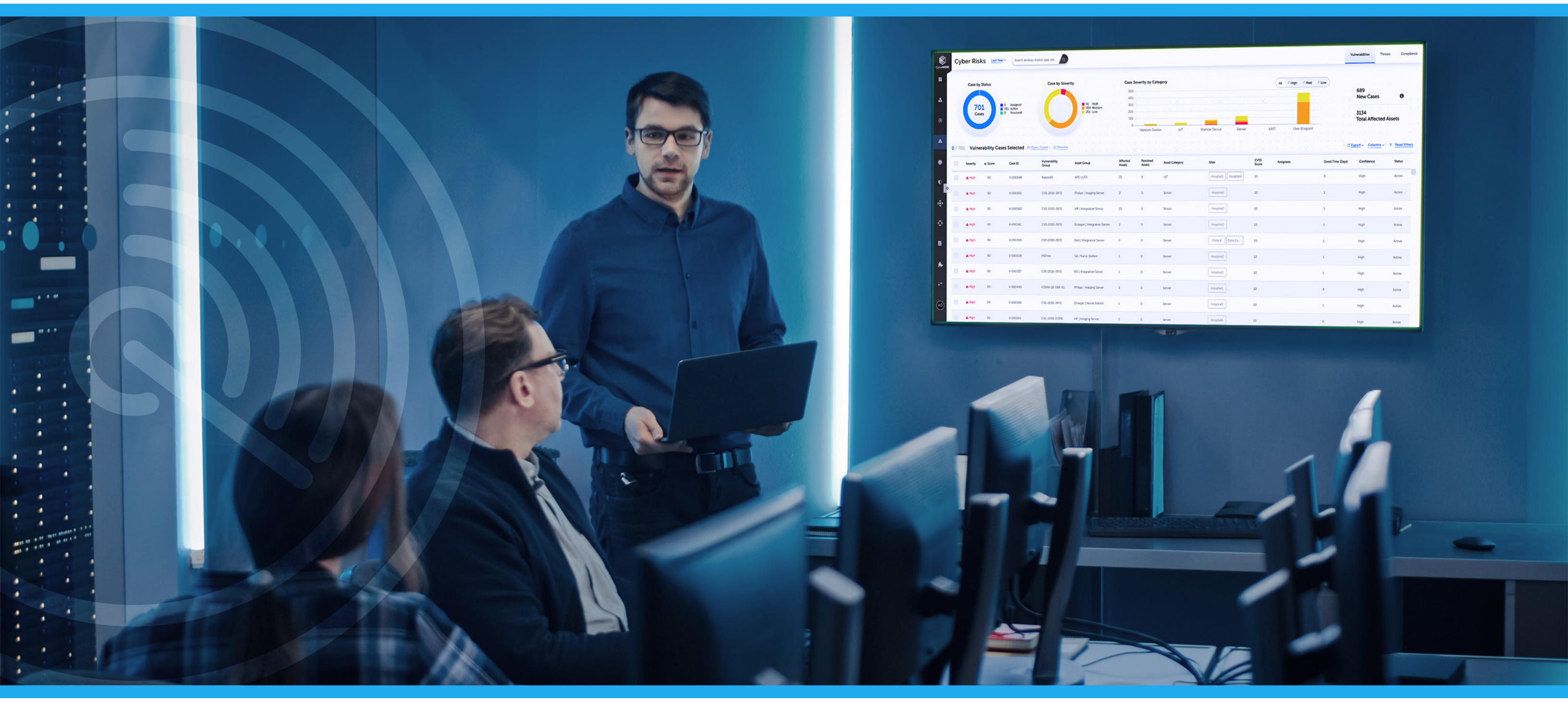
Automated network segmentation

Forescout Medical Device Security facilitates the design and implementation of zero trust policies, enabling you to automatically classify and group clinical assets into meaningful groups based on their workloads. From there, simply define the group-based segmentation policies that reflect only required communications among groups or least trust access relationships.

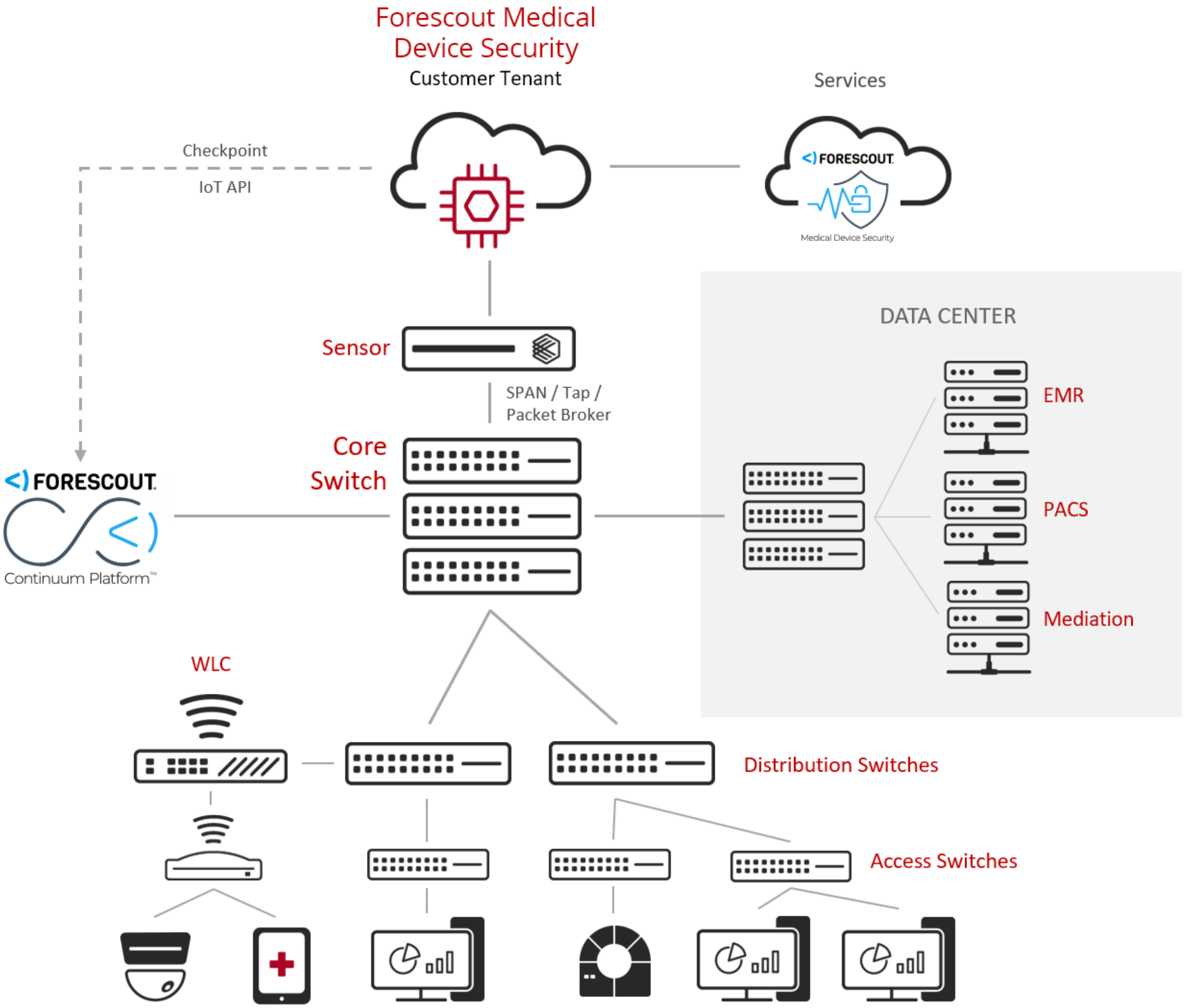
We also automatically generate proactive security policies based on granular medical device insight and send those policies to the Forescout Continuum Platform to deploy and enforce. This streamlines an otherwise resource-intensive process, dramatically reduces the potential attack surface and protects critical processes from being disrupted.

Incident response

Forescout continuously monitors medical devices’ behavior patterns looking for signs of compromise or significant deviations from baseline. Once an attack is detected, you can automate a response using our capabilities to quarantine the compromised device — containing and ultimately expunging the threat while limiting its impact.



Architecture



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