FORESCOUT

Healthcare

Enhance cybersecurity through extended visibility and control for healthcare networks

Today, IT, medical and operational systems of all kinds connect to healthcare networks, and this heightened connectivity increases risk. The Forescout platform can dramatically reduce that risk by providing IT and clinical personnel device visibility of IP-connected devices and the tools to control, automate and orchestrate network security.

Healthcare Cybersecurity Challenges

- Increased number of medical devices on networks, often using outdated operating systems or uncommon firmware
- Many devices are mobile, which are harder to track and secure
- Wide variety of people connecting to and disconnecting from the network: healthcare personnel, office staff, patients, guests, maintenance teams—all requiring different policies
- Teams must help to ensure the integrity and security compliance of a mix of IT, IoT, medical and environmental devices without disrupting operations
- Clinical engineering teams receive mixed priorities about what they can do to their legacy equipment to maintain regulatory compliance without impacting patient care
- Patient data must be protected from loss and cyber incidents to maintain the integrity and confidentiality of electronic protected health information (ePHI)
- Third-party vendors and service providers accessing the healthcare network need oversight to prevent security missteps

> "Forescout showed us things that we didn't know existed—mainly biomedical and environmental devices that were plugged into our network and talking out of the network as well."
>
> **— CISO, major Florida medical center**

The Challenge

Growth of Connected Devices Now Exposes Medical Equipment

Healthcare organizations are facing two major security challenges: They are prime targets for hackers, and their attack surface expands every day as more and more medical devices are connected to networks.

The global IoT healthcare market is expected to grow by 37.6 percent between 2015 and 2020.[1] That's a frightening statistic when you consider that healthcare already ranks number two in breaches.[2]

Clinical devices such as glucometers, electrocardiograms and drug infusion systems are potential targets for hackers despite the efforts of manufacturers to secure their products. Considering the essential role these and other devices play in delivering critical care to patients, extra measures need to be taken to protect them.

Clinical environments use a tremendous variety of connected devices. For example, in any patient care scenario, there is a mix of physical and virtual IT endpoints, including IoT assets that often can't accept agents for technical or regulatory reasons, building automation devices that are overlooked, and clinical devices that have legacy operating systems, or applications that don't meet typical security standards.

The Forescout Platform

The Forescout platform, which now includes SilentDefense™, operates within legacy, new and highly technical network infrastructure without requiring re-engineering of the established network—without disrupting services.

How Forescout Addresses These Challenges

Extended Visibility of Healthcare Devices

The Forescout platform discovers devices upon connection to provide accurate, real-time visibility.

Why Customers Choose Forescout

- **Exceptional, continuous visibility.** See devices that other solutions can't. According to an IDC study, respondents could see 24 percent more devices after deploying the Forescout platform.[3]
- **Non-disruptive discovery and monitoring.** Use passive techniques to discover and monitor assets on sensitive OT networks and critical infrastructure systems.
- **Real-time information.** Gain in-depth situational awareness and control of devices the instant they access your network.
- **Heterogeneous support.** Use common OT interfaces, wired and wireless network infrastructure, operating systems, endpoint software and third-party security solutions, without system upgrades or vendor lock-in.
- **Agentless.** Authenticate, profile and control network access without requiring device agents.
- **Rapid time to value.** Deploy quickly to gain network visibility in hours, accelerating time to value.
- **Compliance.** Automatically identify policy violations, remediate endpoint deficiencies and adhere to compliance mandates.
- **Security orchestration.** Share situational awareness and automate workflows/response actions with leading security and IT management tools.

- Discover IT, IoT and medical devices as they connect to your network without requiring software agents
- Profile and auto-classify devices, users, applications and operating systems without disruption in campus, data center, cloud and clinical environments

Auto-Classify New Devices - The Forescout Device Cloud

The Forescout Device Cloud significantly improves the identification and auto-classification of devices, which is essential for creating effective security policies for network access, device compliance and network segmentation (See Figure 1).

- Forescout research leverages intelligence from over 8 million real-world devices, publishing these new profiles on a frequent basis to help improve classification efficacy and coverage in your environments
- Benefit from crowdsourced device insight from a growing community of over 800 enterprise customers across more than 10 industries

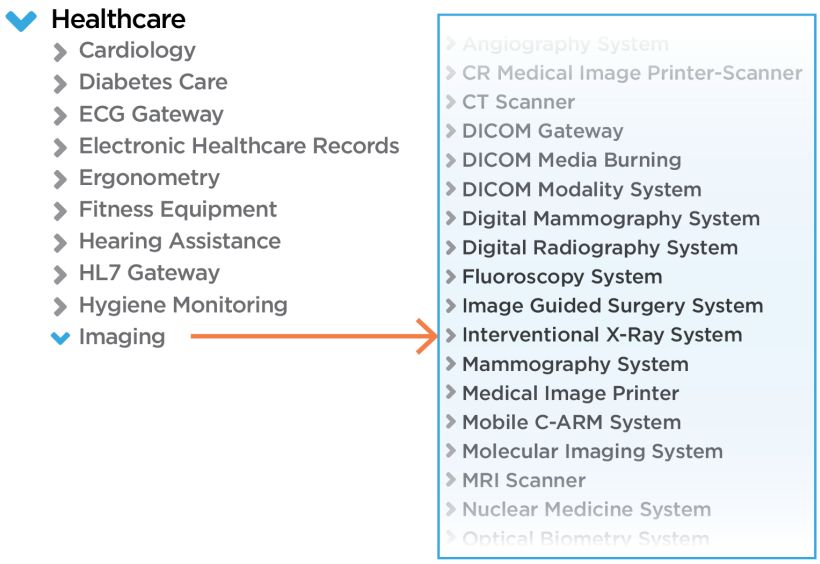


Figure 1: Forescout Device Cloud Classification

Up-To-Date Asset Intelligence and Management

Build an asset inventory of all IP-connected IT, IoT and clinical devices without impacting performance or reliability.

- Gain asset intelligence from IT and clinical devices for richer policies, segmentation and control
- Share contextual data with IT asset management (ITAM) tools or computerized maintenance management systems (CMMS) to build a more accurate asset inventory and maintenance solution

Automated, On-Connect Compliance

Ease compliance with on-connect status and simplify reporting with real-time compliance reports.

- Align with stringent security regulations such as HIPAA and EU NIS
- Increase auditing and compliance team efficiencies by 26 percent on average[3]

Minimizing Risk and Enhancing Throughput: A Network Segmentation Use Case

Forescout lets you dynamically segment specific medical device types using VLAN or ACL assignments.

For example, you can place imaging systems on an imaging VLAN where only authorized users can access them. And, by separating these systems from other traffic, you can maintain the necessary network throughput to transfer large images instead of competing with VoIP phones or large dataset transfers.

Additionally, you can segment video surveillance systems, HVAC systems and other environmental and IoT devices, which can greatly minimize cyber risk exposure in the event that a device is compromised.

By isolating devices by type in various segments, the Forescout platform mitigates further network penetration to business and operational areas that are beyond those segments.

> "Forescout's agentless approach was key, as was its ability to give us full visibility into all devices, including medical devices connected to or attempting to connect to our network."
>
> **— Michael Pinch, CISO, University of Rochester Medical Center**

Continuous Monitoring

Instantly detect issues that go unnoticed by point-in-time vulnerability scanning.

- Assess IT, IoT and clinical devices as well as network functionality for changes in operations, security hygiene and behavior
- Passively illuminate blind spots that periodic scanning tools miss
- Notify IT systems, end users or clinical service desk personnel about security issues

Policy-Based Access Control

Enforce policy-driven network access based on your needs, using factors such as device type, ownership, security hygiene and vulnerabilities.

- Isolate legacy and noncompliant devices on your network, and notify users to remediate or auto-remediate where applicable
- Ease guest or BYOD access. Visitors can receive internet access through a guest VLAN, and lobby kiosks can be placed on secure segments that cannot touch operational healthcare systems or sensitive patient information.

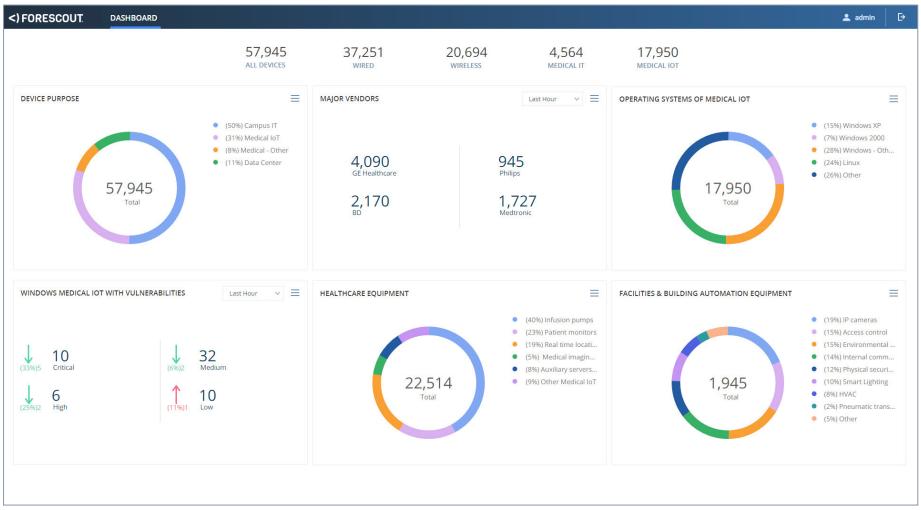
Adaptive Segmentation

Standardize network segmentation policies and management across campus, data center, cloud and critical patient care environments.

- Assign devices into network segmentation zones that contain similar policy and compliance requirements
- Leverage out-of-the-box integrations with next-generation firewalls for device-based policies
- Protect critical assets and minimize potential issues from "east-west" traffic that other security measures might miss

Visualized Device Intelligence

The Forescout platform provides your security operations center (SOC) and incident response teams with a consolidated, up-to-date view of your device landscape along with classification, connection and compliance context.



The Forescout Device Intelligence Dashboard is easily customizable for other IT functions such as risk, compliance and executive reporting.

Forescout + SIEM: An Orchestration Use Case

Forescout works with leading SIEM (security information and event management) tools to detect anomalous behavior and automatically launch policy-based enforcement or remediation actions with Forescout.

For example, if a point-of-care handheld device begins navigating the network and attempts to access an accounting system, automated polices can isolate the system and alert security personnel to the exact location of the device.

Or, if a surveillance camera or barcode scanner in the pharmacy begins broadcasting unusually heavy traffic in the middle of the night, Forescout can isolate the system and inform IT staff.

Orchestrate Information Sharing Among Leading Security Tools

Forescout extends agentless visibility and control capabilities to leading network, security, mobility and IT management products via Forescout Extended Modules.

- Make your existing security investments work better and automate security responses
- Share context and control intelligence among systems to enforce unified network security policy
- Reduce vulnerability windows by automating system-wide threat response
- Provide a higher return on investment from existing security tools and save time due to enhanced workflow automation

Learn more at
www.Forescout.com

FORESCOUT

Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134, USA

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

[1] https://www.psmarketresearch.com/market-analysis/internet-of-things-in-healthcare-market
[2] "*2017 Data Breach Investigations Report*," Verizon
[3] IDC study: https://www.forescout.com/idc-business-value/

© 2019 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners. **Version 01_19**