

# University of Rochester Medical Center

University of Rochester Medical Center Expands Oversight and Control Over Personally-owned and Medical Devices with Forescout

## SAVINGS

to IT resources were greater through continuous monitoring

## 15,000

unknown devices discovered

## EASY

classification, grouping and monitoring of medical devices



### Industry

Healthcare

### Environment

15,000 employees: includes nonemployee doctors, researchers and other care giver personnel regularly connecting to the URMC network

### Challenge

- Increased demand for BYOD amongst the Center's doctors, researchers and other personnel
- Need for operational oversight of network endpoints, including medical devices and live saving systems
- Ability to support HIPAA and HITECH compliance

## Overview

University of Rochester Medical Center (URMC) is one of the nation's top academic medical centers and the hub of the University's patient care, health research, teaching and community outreach missions. The Center has three hospitals and supports research and medical schools separate from the University – bringing the grand total of employees to approximately 15,000.

With the BYOD trend in full force among employee and non-employee doctors, researchers and other care giver personnel, a growing number of personally-owned devices, many of which are unsecured and unauthorized, were regularly connecting to the URMC network. This made it necessary for the Center's IT team to have insight and control over all of the endpoints attempting to connect or on the medical center network. However, due to the time-critical and life-saving nature of the healthcare industry, a secure network with no disruption to users and service is also essential, as taking a device offline (especially an unidentified one) in a hospital setting can potentially put a life at risk, adding a unique level of complexity to securing the network. As such, technical controls must be granular and flexible.

## Business Challenge

"The healthcare sector is now facing pressure to implement an effective BYOD strategy," said Michael Pinch, chief information security officer for URMC. "Since this has brought 15,000 or more additional devices onto our network, we really needed to take the next step to enhance our network security and to gain a complete inventory of the devices connected to our network to allow for the fingerprinting of these unique endpoints."

In addition to the user devices accessing the network, many of the Center's endpoints are also medical devices and equipment such as heart monitors and

## Security Solution

- Forescout platform

## Use Cases

- Device visibility
- Network access control
- Incident response
- Device compliance

## Results

- Comprehensive monitoring and control over network connections and usage of devices ranging from smartphones and tablets to heart monitors, medical kiosks and ultra sound machines
- An unobtrusive inspection and granular, policy-based enforcement of all devices requesting access to, or currently accessing network resources
- Greater IT resource savings through continuous monitoring, intelligence and informed response

ultra sound machines. The FDA regulates these medical devices and prohibits modifying and installing software on these systems – including agent technology.

Another major government regulation, HIPAA, specifies requirements for securing patient health information (PHI), is also an urgent driver for URM to deploy an effective network access security solution into its environment. In addition, because visiting and community doctors also handle patients' sensitive medical information, there is yet another layer of complexity in implementing a secure BYOD solution, as these visiting employees often use their own devices to access patient data.

To address the myriad challenges, URM sought to implement an agentless network security solution that would assess the status and security posture of any connecting user, device, system and application before gaining access to their network – without disrupting medical staff and researchers while expanding safeguards to protect network availability and sensitive patient data. In turn, the medical center would strengthen its HIPAA compliance efforts.

## Why Forescout?

After having the opportunity to review solutions from Bradford, Cisco and Forescout, URM's IT and networking teams, asset management department, and risk and compliance teams mutually decided to adopt the Forescout platform to gain visibility and control over the Center's rapidly evolving network.

"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," said Pinch. "Forescout's flexible policy engine also played a big role in the selection as they allow us to group devices, enforce policies and remediate devices quickly and easily."

URM uses the Forescout platform virtual firewall technology for network enforcement, which allows the IT team to logically create segregated networks of users based on who they are, or their device characteristics – dynamically and without impacting network switch settings. In addition, the team utilizes the Forescout platform to identify medical devices and place them in an isolated group, allowing the URM UT team to quickly discover suspicious behavior and rectify situations, while ensuring that all critical medical equipment remains operational.

"When we notice on the network that a device is misbehaving, rather than blocking it, which might be the default path taken for an end-user device, we can treat it separately and automatically create a high priority ticket to have someone go out and examine the device," explained Pinch. Pinch's team also leverages Forescout's orchestration capabilities architecture to enable interoperability with URM's network and security infrastructure. This bi-directional integration allows the Forescout platform and systems to share intelligence and better respond to exposures. URM employs Microsoft System Center Configuration Manager (SCCM) for patching, updates, and deploying encryption and antivirus to over 19,000 machines residing on their network.

---

“The Forescout platform’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, Chief  
Information Security Officer,  
University of Rochester Medical  
Center

---

## Business Impact

For years, URMC had full-time interns whose sole focus was to fix broken antivirus and SCCM clients. Using Forescout’s integration with MS-SCCM and Sophos, the Forescout platform can dynamically find systems that are vulnerable or not adhering to policy. Furthermore, the Forescout platform can remediate the endpoint issue without the need to dispatch human resources to address the problem. This also serves to validate compliance with HIPAA and by ensuring full disk encryption services, enables URMC to apply data breach safe harbor defenses.

To date, URMC has discovered numerous use cases for the Forescout platform, but Pinch is particularly looking forward to integrating the Forescout platform with Bromium.

URMC’s ability to detect and isolate threats using the Forescout platform, will be significantly strengthened by a Bromium integration, and will help protect sensitive patient data information, and fortify HIPAA compliance and anti-virus solutions.

## Looking Forward

“What I’m most excited about is an integration with Bromium, a product for sandboxing zero-day attacks and APTs,” said Pinch. “While we could put the Bromium client on every computer, we are instead going to put it on our users that are most often compromised. From here, we can use Forescout to get the intel on every identified piece of malware found by Bromium, and Forescout can then check every other machine on the network for the same running processes, allowing us to gain exponential benefits from our other toolsets.”

URMC is also exploring ways to further leverage its the Forescout platform investment to expand its BYOD and other security policies, with the ultimate goal of automating more tasks to preempt threats, fix problems and respond to issues.



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

Learn more at [Forescout.com](https://www.forescout.com)

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at [www.forescout.com/company/legal/intellectual-property-patents-trademarks](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 05\_20