

# RWJBarnabas HEALTH

“The Forescout platform allows us to quickly discover and classify devices and infrastructure on heterogeneous networks as hospitals and clinics join RWJBarnabas Health.”

– Hussein Syed, Chief Information Security Officer

## Environment

12 hospitals, 250 clinics and outpatient surgery centers and thousands of doctors’ offices comprising 75,000 devices connected to the network environment

## Industry

Healthcare

## Why They Chose Forescout

- 20+ active and passive techniques provide full device visibility with confidence
- Agentless posture assessment of Windows, macOS, Linux and IoT devices
- Implement network segmentation to reduce risk from attacks like Mirai
- Heterogeneity: Automate network controls in any existing multivendor network
- One platform for visibility and control across mixed M&A environments



## 100% Identified

of IoT communications



## 1-2 Keystrokes

versus hours to hunt devices



## 83% Reduced Time

to remediate devices

## Business Challenge

With RWJBarnabas Health being a healthcare system, administrators must deal with issues that many of their counterparts in other industries never have to face. Those issues include: adding new types of medical devices to networks without adding vulnerabilities, maintaining a strong security posture without impeding medical care, continually expanding safe network access to clinicians, labs, insurers, research organizations and contractors, as well as new hospitals, clinics and doctors’ offices as they join the system through new contracts or M&A, and staying compliant with strict regulations (HIPAA, HITECH).

## Positive Business Outcomes With Forescout

For RWJBarnabas Health, visibility was key. IT security teams had to know what was on their networks, in addition to preventing rogue devices from logging on and spreading malware or stealing data. They also needed to identify and classify endpoints to assess for compliance and place them on the appropriate network segments. And that’s where the Forescout platform proved especially useful.

- 60% increase in visibility in unmanaged assets such as medical devices, printers, cameras and other IoT devices
- Visualization of all traffic communication paths on the network
- Reduced attack surface from medical devices with EOL OS by implementing network segmentation
- Agentlessly assess compliance upon network connection and limit noncompliance devices to restricted VLAN until remediation
- Quick visibility and control of devices in mixed M&A environments due to multivendor support, including the ability to quickly find assets in seconds following mergers



Download full  
case study to  
learn more

Contact Forescout today to help your  
organization achieve amazing results.

references@forescout.com