ForeScout

Healthcare

Increase cybersecurity through visibility and control for today's healthcare networks

Healthcare IT Challenges

- Increased number of managed and unmanaged devices on networks, many of them mobile
- Teams must enable and secure medical devices while ensuring compliance
- Data of patients, providers and the organization must be protected from loss and cyber incidents-especially data that is subject to breach notification rules
- Confusion around what the clinical engineering team can and cannot do to their equipment and services to maintain compliance with regulatory requirements
- Devices must meet baseline requirements to maintain the integrity and confidentiality of electronic protected health information (ePHI) and other data, yet some devices cannot be patched
- Vendor-owned-and-managed systems reside on healthcare networks

If protected health information (PHI) is encrypted by ransomware, it must be reported as a breach.
—U.S. Dept. of Health and Human Services Fact Sheet: Ransomware and HIPAA

Virtually every medical and operational system is connected to today's healthcare networks. Patient data is accessible on mobile devices. Diagnostic systems, electronic medical records and medical devices-from insulin pumps to heart monitors-must be secure and available. ForeScout achieves this by providing secure access to PCs and laptops, smartphones, medical devices and other endpoints while giving IT personnel the tools to control, automate and orchestrate network security.

The Challenge

Healthcare Remains Under Attack While Also Becoming More Connected

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

The global IoT in healthcare market is expected to grow with a CAGR of 37.6% during 2015 – 2020[1]. That's a frightening statistic when you consider that healthcare already ranks number two in breaches.[2]

Cyberattacks on patient data are constantly in the news. According to an Accenture survey[3], 26% of Americans or 1 in 4 have had their patient information stolen. Worse still, unlike credit cards that can be discontinued, protected health information (PHI) lives on. As a result, according to Forrester Research, it sells for 10 times the price of stolen credit card numbers.[4] With security breaches being commonplace, preemptive cybersecurity actions are required for medical devices and devices that access medical data.

IoT devices such as glucometers, electrocardiograms and drug infusion systems are potential targets for hackers and convenient entry points for other systems to access patient data. No matter how much manufacturers have invested in hardening, nearly all IoT-enabled and Internet-connected medical devices are at risk. Considering the critical role these and other devices play in delivering critical care to patients, exploitation or manipulation of medical devices can be a matter of life and death.

How ForeScout Addresses These Challenges:

- Provides visibility into what is on your network-with or without agents
- Discovers and classifies thousands of medical devices, streamlining policy-based monitoring and enforcement of patient care devices
- Enforces policy-driven network access based on device type, ownership, hygiene and vulnerabilities
- Assigns devices into network segmentation zones that contain data with similar policy compliance requirements
- Continuously assesses devices and network behavior for changes in device hygiene and behavior
- Orchestrates information sharing among a variety of security tools, allowing your existing security investments to work better and automate security responses

Key Use Cases

- Network Access Control
- Device Compliance
- Network Segmentation
- Asset Management
- Incident Response

> 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**

Securing Health Industry Networks with ForeScout

A lack of real-time visibility is preventing many healthcare organizations from enforcing cybersecurity policies across the enterprise. Key reasons for this are that unmanaged devices are not equipped with security agents, and that devices come and go from the network as a matter of operations. These conditions are largely undetected by periodic, point-in-time vulnerability scans. Also, providing appropriate levels of access without real-time visibility of devices on the network is problematic because the device type, ownership and hygiene (OS and applications, patches, overall security posture, etc.) are not always known. These gaps in knowledge and security policy enforcement put the entire network in jeopardy.

The ForeScout security platform provides the critical ability to see and monitor wired or wireless devices on the network-everything from conventional computers and smartphones to medical devices, printers and other Internet of Things (IoT) devices. With this information, ForeScout can assign them to the appropriate network segmentation zones that contain data with similar policy compliance requirements. In addition, ForeScout can assign and enforce access policies across the network hierarchy that can be based on device type, hygiene level and ownership.

The ForeScout Security Platform

The ForeScout platform, which comprises ForeScout CounterACT®, ForeScout Extended Modules and the ForeScout Enterprise Manager, operates within legacy, new and highly technical network infrastructure without requiring reengineering of the established network or disrupting services.

ForeScout provides real-time network visibility of managed and unmanaged endpoints as well as devices that are commonly found on healthcare networks, such as laboratory instruments, heart monitors, infusion pumps, X-ray systems and clinicians' handheld devices. ForeScout increases control through security segmentation of the network, and provides policy-based remediation of non-compliant or compromised devices. In addition, it provides extensive interoperability with network infrastructure and enables orchestration and workflow automation among leading security tools to automate and accelerate system-wide response.

Here's how:

See. Without visibility into what is on your network, it's impossible to ensure compliance. ForeScout detects devices the instant they connect to the network without requiring agents. ForeScout's custom policy engine makes it possible to discover networked devices based on known characteristics such as devices, users, applications and operating systems within administrative and medical information systems. ForeScout can automatically identify thousands of medical devices from leading manufacturers (see sample device list in Figure 2) and even monitors vendor-owned medical equipment and other devices, ports and connections that reside on healthcare networks. This saves healthcare IT teams valuable time by providing accurate, real-time inventories of networked medical devices to assist in compliance with FDA and HIPAA requirements. With the ForeScout platform's agentless visibility and classification capabilities, it can assign devices and users to appropriate network segments and prevent unauthorized access to areas of the network where they don't belong.

> ForeScout CounterACT'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**

Control. Once each device on your network is revealed and its purpose is understood, ForeScout lets you choose from a broad range of host and network controls. You can restrict access of non-compliant devices or quarantine a device based upon anomalous behavior and notify its owner of a security concern. Should an employee- or contractor-owned system or mobile device be missing security updates or not have up-to-date antivirus software, the device can be isolated to a secure self-remediation portal and not re-admitted to the network until the user has been informed and taken steps to fix the problem. For corporate-owned devices, ForeScout can automatically perform remediation. It can also enforce guest access agreements and inform staff of equipment-use policies prior to granting access.

In addition, 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 imaging 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 IoT devices, which can greatly minimize 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. Likewise, visitors can be given 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.

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

- 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 help you save time due to enhanced workflow automation

For example, integration between ForeScout and advanced threat detection solutions can automatically isolate an infected system to a secure VLAN or instantly drop the system's port. This can prevent a device from spreading malware or communicating with command and control servers to exfiltrate data or propagate ransomware across the network.

In addition, integration allows security information and event management (SIEM) systems 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, CounterACT can isolate the system and inform IT staff.

1. X-ray device connects to the network.
2. ForeScout discovers the device, determines device type and ownership.
3. ForeScout places X-ray device on the imaging network segment.
4. Third-party SIEM alerts ForeScout of anomalous behavior of mobile device.
5. Based on policy, ForeScout can restrict mobile device network access for further analysis.

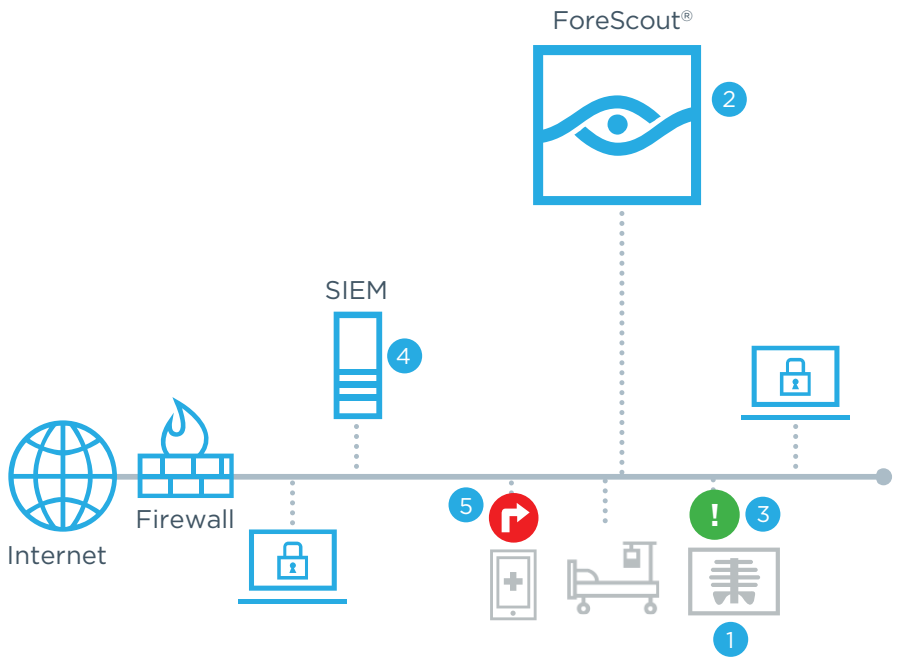

Figure 1: How ForeScout provides visibility and enforces control on healthcare networks.

Discover and classify IoT medical devices

The custom policy engine of ForeScout makes it possible to discover networked devices based on known characteristics. In addition, ForeScout device classification policies can automatically identify thousands of medical devices from leading manufacturers. New device classifications are continually being added, saving healthcare IT teams valuable time by providing accurate, real-time inventories of networked medical devices to assist in compliance with FDA and HIPAA requirements.

In addition to device discovery and classification, ForeScout can detect and block unauthorized USB memory sticks and other peripheral devices. This is an important security consideration given that many medical devices have USB ports for allowing administrators to perform manual firmware updates. The following is a sample list of medical devices that ForeScout can automatically detect and classify.

Electronic Healthcare Records
- CliniComp

Healthcare - General
- 3M
- AAEON-Technology
- Abbott
  - Abbott-Point-of-Care
  - Abbott-Diagnostics
  - Abbott-Optics
- ACIST-Medical-Systems
- Acteon-Group
- Advance-Sterilization-Products
- Advantage-Pharmacy
- Aeroscout
- Alcon-Laboratories
- Alpinion-Medical-Systems
- AmbiCom
- American-Telecare
- Andon-Health
- Applied-Biosystems
- Avizia
- B-Braun-Melsungen
- Bang-Olufsen-Medicom
- Baxter-Healthcare
- Beacon-Medical
- Beckman-Coulter
- Bestcare-Cloucal
- Bio-logic-Systems
- Bio-Rad-Lab
- Biodevices
- bioMerieux-Italia
- Bionet
- BIOPAC-Systems
- Biosoundlab
- Biospace
- Biotronik
- BMT-Medical-Technology
- Boston-Scientific
- C8-MediSensors
- Calypso-Medical
- Camtronics-Medical-Systems
- CardioNet
- Cardiopulmonary-Corp
- CardioTek
- CareCom
- CareFusion
- CarePredict
- Carestream-Health
- CareTech
- CareView-Communications
- Celectronic-eHealth
- Centrak
- CHG-Hospital-Beds
- CirTec-Medical
- CIRTEC-Medical-Systems
- Cerner
- Cogent-Healthcare-Systems
- Colorado-Med-Tech
- Compex
- Compumedics
- Conmed-Linvatec
- Corometrics-Medical-Systems
- Criticare-Systems
- Cutera
- Dainippon-Pharma
- Danaher-Motion-Kollmorgen
- Datex-Ohmeda
- DENTSPLY-Gendex
- Diatek-Patient-Management
- Dictum-Health
- Digiboard
- Dixtal-Biomedica
- Draeger
- Dragerwerk
- Durr-Dental
- Edwards-Lifesciences
- Essilor
- Fisher-Paykel
- Fresenius-Medical-Care
- Fuji
- Fukuda-Denshi
- Gambro-Lundia
- GE-Medical
  - GE-Medical-System
  - GE-Healthcare
- Getinge
- GN-ReSound
- Health-Advice-Monitors
- Health-Hero
- Health-Life
- HealthStream
- HemoCue
- Heraeus-Noblelight
- Hitachi-Aloka-Medical
- Hoana-Medical
- Honeywell
  - Honeywell-HomMed
- HORIBA-Medical
- Hospira
- Huntleigh-Healthcare
- Imatron
- Indiana-Life-Sciences
- InnerSpace
- INSidE-Technology
- Integrated-Medical-Systems
- Intel-GE-Care-Innovations
- Interacoustics
- Invivo
- Ivoclar-Vivadent
- Ivy-Biomedical
- Johnson-Johnson-Medical
- Karl-Storz-Imaging
- KaVo-Dental
- KeyMed
- Kodak-Radiology
- Kollmorgen
  - Kollmorgen-Servotronix
  - Kollmorgen-Corp
- Kontron-Medical
- LABiTec
- Laerdal-Medical
- Leica-Microsystems
- LI-COR-Biosciences
- LifeSync
- LRE-Medical
- Maquet
  - Maquet-GmbH
  - Maquet-Cardiopulmonary
  - Maquet-Critical-Care
  - Maquet-CardioVascular
- Marconi-Medical-Systems
- Masimo
- Medicis
- Medicore
- Medrad
- Medtronic-Diabetes
- Mennen-Medical
- Micropoint-Biotechnologies
- Mindray
- MIR
- MOCACARE
- Moleculars-Corp
- Mortara-Instrument
- NDS-Surgical-Imaging
- Neural-Image
- Nicolet
  - Nicolet-Neuro
  - Nicolet-Instruments
- Nihon-Kohden
- Nipro-Diagnostics
- Nonin-Medical
- Novo-Nordisk
- Olympus
  - Olympus-Soft-Imaging
  - Olympus-Image-Systems
- Omron-Healthcare
- Onyx-Healthcare
- Optimedical-Systems
- ORTHOsoft-Zimmer-CAS
- Ortivus-AB-Medical
- Oticon
- Pacific-Biosciences
- PaloDEx
- Palomar
- Panasonic-Healthcare
- Pharma-Smart
- Philips-Medical
  - Philips-Respironics
  - Philips-CareServant
  - Philips-Healthcare-PCCI
  - Philips-Oral-Healthcare
- Phonak-Communications
- Physio-Control
- Physiometrix
- Planmeca-Oy
- Progeny-Midmark
- Proteus-Digital-Health
- ResMed
- RF-Surgical-System
- Robert-Bosch
- Roche-Diagnostics
- ScottCare
- Secure-Care
- SenTec
- Senticare
- Shenzhen-Lifesense-Medical
- Shimadzu
- SHL-Telemedicine
- Siemens
  - Siemens-Healthcare-Diagnostics
  - Siemens-AG-Healthcare-Sector
- Sigma
- Sirona-Dental-Systems
- Smiths-Medical
- SonoSite
- Spacelabs-Healthcare
- Spectrum-Medical-Limited
- Starkey-Labs
- Stratec-Biomedical
- Stryker
- Tecan-Systems
- Terumo
- Thermo-Fisher-Scientific
- Thoratec
- Tiba-Medical
- Tokyo-Boeki-Medisys
- Toyo-Medic
- tPlus-Medical
- Trendsetter-Medical
- Tunstall-Healthcare
- Varian-Medical-Systems
- Versamed
- Verto-Medical
- VIASYS-Healthcare
- Vigil-Health-Solutions
- Vocera
- Welch-Allyn
- Widex
- Zimmer-Elektromedizin
- ZOLL-Lifecor
- Advanced-Medical-Information
- Applied-Medical-Technologies
- Arkray
- Axis-Shield-PoC
- Becton-Dickinson
- Biotage
- BL-Healthcare
- CardioMEMS
- Care-Everywhere
- Convergent-Bioscience
- Ellex-Medical
- Fluke-Biomedical
- Gem-Med
- Getinge-IT-Solutions
- Getinge-Sterilization
- Haag-Streit
- Heart-Forece-Medical
- Imricor-Medical-Systems
- Innomed-Medical
- Integra-Biosciences
- Integra-LifeSciences
- Intuitive-Surgical
- Jostra
- Leica-Biosystems
- Medav
- MedAvant-Healthcare
- Mediana
- Pointe-Conception-Medical
- Power-Medical-Interventions
- Quantum-Medical-Imaging
- Radiometer-Medical
- Resurgent-Health-Medical
- Soredex
- Sphere-Medical
- St-Jude-Medical
- Valtronic
- VitalCare
- West-Com-Nurse-Call
- Zoe-Medical

Infusion Pumps
- Alaris
  - Alaris-Medical-Systems
- CareFusion-Alaris-Pump

Patient Monitors
- Draeger-Delta
- Draeger-M300
- Philips-Patient-Monitoring

Ultrasound
- Siemens-Acuson-Ultrasound
- Sonosite-MicroMaxx-Ultrasound

X-Ray
- Medison-X-Ray
- Philips-Analytical-X-Ray

Figure 2: The ForeScout platform quickly and accurately discovers and inventories thousands of medical devices, streamlining policy-based monitoring and enforcement of patient care endpoints.

Learn more at
www.ForeScout.com

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] Accenture study: https://newsroom.accenture.com/news/one-in-four-us-consumers-have-had-their-healthcare-data-breached-_accenture-survey-reveals.htm
[4] Forrester, The US Healthcare Security Benchmark 2017 to 2018, Salvatore Schiano and Chris Sherman, January 17, 2018