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 responsible for both enabling and securing medical devices and 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 patient health information (ePHI) and other data, yet some devices cannot be patched
- Vendor-owned-and-managed systems reside on healthcare networks

If personal 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 Is Under Attack

Healthcare organizations have found themselves at ground zero in the high-stakes cyberattack battlefront. As of June 30, 2016, 1,573 breaches affecting 159,002,174 patients were reported to the U.S. Department of Health and Human Services. Cybercriminals were especially busy in the first half of 2016. Their weapon of choice was (and still is) ransomware, a particularly heinous form of extortion that can shut down hospital operations. According to a U.S. interagency task force, "On average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015)[1].

Here a few healthcare breach examples:

- "Hollywood Presbyterian Medical Center paid the ransom of 40 bitcoins, which is currently worth $16,664, in order to restore its computer system." —NPR, February 2016
- "Methodist Hospital Declares 'Internal State of Emergency' After Ransomware Infection" —KrebsonSecurity, March 2016
- "King's Daughters' Health, based in Madison, Ind., purposefully shut down its computer systems after discovering a user's files were infected with ransomware." —Healthcare IT News, April 2016

Cyberattacks intent on stealing patient data are on the rise as well, which isn't surprising when you consider medical records fetch up to 60 times more money than credit cards on the dark web[2]. It is relatively easy to cancel a credit card, but changing a social security number is another matter entirely. With security breaches becoming commonplace, preemptive cybersecurity actions are required for medical devices and devices that access medical data.

How ForeScout Addresses These Challenges:

- Provides visibility into what is on your network—with or without agents
- Enforces policy-driven network access based on endpoint type, ownership, hygiene and vulnerabilities
- Continuously assesses endpoints 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

> A medical dispensary device was compromised after 20 USB sticks containing malware were scattered around a hospital. Within seven days, the sticks had been plugged into 15 different devices. From there, the researchers were able to bypass the login for the dispenser."
>
> **— Forbes, *"White Hat Hackers Hit 12 American Hospitals to Prove Patient Life 'Extremely Vulnerable,'"* Feb 23, 2016**

Securing Health Industry Networks with ForeScout

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

ForeScout provides administrators with 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. CounterACT can assign endpoints to the appropriate network segmentation access policies across the network hierarchy, from switches to access and distribution layers. These policies can be based on device type, hygiene level and ownership.

The ForeScout Security Platform

The ForeScout security platform, which comprises ForeScout CounterACT®, ForeScout Extended Modules and the ForeScout ControlFabric® Architecture, operates within legacy, new and highly technical network infrastructure without reengineering the established network or disrupting services.

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

Here's how:

See. CounterACT detects devices the instant they connect to the network without requiring agents. It profiles and classifies devices, users, applications and operating systems within administrative and medical information systems. It even identifies, classifies and monitors vendor-owned medical equipment and other devices, ports and connections that reside on healthcare networks.

Without visibility into what is on your network, it's impossible to ensure compliance. Since CounterACT's custom policy engine makes it possible to discover networked devices based on known characteristics, it can automatically identify thousands of medical devices from leading manufacturers (see sample device list below). 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. And, thanks to CounterACT's agentless visibility and classification capabilities, it can assign devices and users to appropriate network security 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, Chief Information Security Officer, University of Rochester Medical Center**

Control. Once each device on your network is revealed and its purpose is understood, CounterACT 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, CounterACT can automatically perform remediation. It can also enforce guest access agreements and inform staff of equipment-use policies prior to granting access.

In addition, CounterACT lets you segment specific medical device types using VLAN or ACL assignments. Imaging systems, for example, can be placed on an imaging VLAN where only authorized users can access them. And, when imaging devices are separated from other traffic, they can maintain the necessary throughput to transfer large images rather than competing with VoIP phones or large dataset transfers. Moreover, a hospital's video surveillance systems, HVAC systems and other IoT devices can be securely segmented, greatly minimizing exposure in the event that a device is compromised by not allowing network penetration 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 CounterACT's agentless visibility and control capabilities to leading network, security, mobility and IT management products via ForeScout Extended Modules.

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

Security information and event management (SIEM) systems can detect anomalous behavior by a device or user and automatically launch policy-based enforcement or remediation actions with CounterACT. 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 text security personnel about the issue, including 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.

This unique ability to orchestrate multivendor security allows you to:

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

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

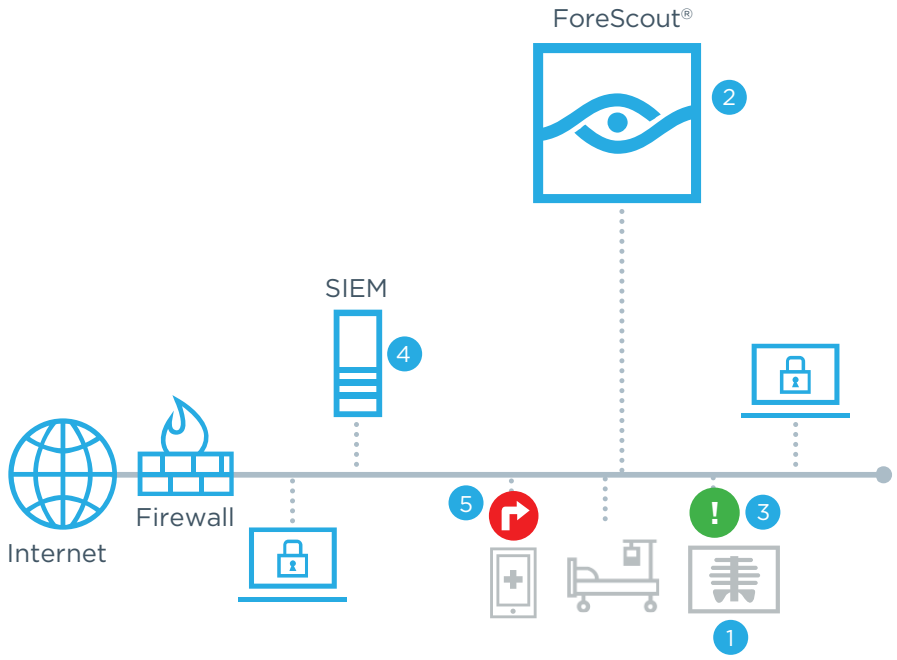

Figure 1: How ForeScout provides visibility and enforces control on healthcare networks.

Discover and classify IoT medical devices

The custom policy engine of CounterACT makes it possible to discover networked devices based on known characteristics. In addition, CounterACT 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, CounterACT can also 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 allowing administrators to perform manual firmware updates. Following is a sample list of medical devices that CounterACT 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: CounterACT 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] United States Government Interagency Guidance Document, *How to Protect Your Networks from Ransomware*, https://www.justice.gov/criminal-ccips/file/872771/download

[2] CNBC http://www.cnbc.com/2016/03/10/dark-web-is-fertile-ground-for-stolen-medical-records.html