FORESCOUT

> 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**

Deploying the ForeScout Platform in Healthcare

A 10-Step Guide

As anyone responsible for security in a healthcare organization knows, healthcare networks are prime targets. Health insurance credentials, protected health information and other confidential files simply contain too much valuable information for greedy, conscience-free cybercriminals to pass up. As of June 30, 2016, 1,573 breaches affecting 159,002,174 patients were reported to HHS.[1]

Clearly, better, **smarter** network security solutions must be put in place.

ForeScout protects the networks of healthcare organizations by enabling IT professionals to see and control devices connected to the network—even unmanaged, agentless devices such as fetal monitors, infusion pumps and those of which the organization has no previous knowledge. These visibility and control capabilities enable healthcare organizations to keep rogue devices and others that do not meet internal security standards off the network—thus preventing cybercriminals from seeding malware into private network environments and altering or stealing data or holding your organization for ransom. In addition, ForeScout can orchestrate information sharing among the security tools commonly in use in healthcare organizations, and can help demonstrate compliance with federal and state regulations while providing authorized user populations and new devices—including medical devices—with secure network access in a cost-effective, efficient manner.

While general enough to be of use to anyone rolling out a key network security solution of any kind, this document provides guidance on how best to deploy the ForeScout platform within your healthcare organization. With the right amount of IT planning and project oversight, your ForeScout implementation can progress quickly and with minimal disruption. And, once in place, this versatile platform can improve the security posture of your organization, help address compliance issues and optimize IT resources.

The 10-Step Process

1 Assign a project owner; identify success criteria

To ensure the success of any IT project, assigning a project owner is recommended. This person is often the individual who approved purchase of the solution and is responsible for reporting on the status of the deployment to senior management. The project owner is instrumental in addressing internal roadblocks that may arise during the deployment process. He or she is also in charge of establishing and documenting high-level criteria for success concerning each phase of the implementation. This is essential in order for progress to be measured and reported effectively. Initial purchase requirements can be used as the basis for establishing these criteria.

2 Create a cross-functional deployment team

Unless properly implemented, a system-wide security tool deployment has the potential to impact employees in every department of the organization as well as consultants, contractors, partners and others. The cross-functional deployment team works with the project owner to objectively evaluate which groups should be involved in the implementation before, during and after deployment. The team should comprise key individuals from each department with the initial goal to become familiar with the security solution and its capabilities, identify use cases and examine potential impact on operations and processes. At a minimum, IT departments (operations, network, security, endpoint and help desk) and various business units should be represented.

3 Identify and prioritize use cases

The cross-functional deployment team should create specific use cases that span topics such as device requirements, security configuration requirements, compliance requirements, how to manage contractor devices, how to register and segregate guests, how to manage corporate-provisioned and personal mobile devices, etc. Use cases should be ranked and categorized according to organizational needs and acceptable risk levels. This will help prioritize the ForeScout platform deployment and policy considerations, as well as enforcement and remediation requirements.

4 Agree upon key security issues to be addressed by ForeScout

Key security issues can include:

- Guest management
- Wireless and/or remote access
- Mobile security
- Connected medical device management (Internet of Things endpoints)
- ePHI protection
- BYOD management
- Asset inventory
- Internal security policy compliance
- External regulatory (HIPAA, HITECH, etc.) compliance
- Automation with existing security tools to leverage investments already made*

These items may have been identified during the preliminary evaluation, and should be formally documented now that use cases have been identified and prioritized. Some items may be addressed in the initial product rollout while others can be phased in later, but all should be captured in the deployment plan. It is at this stage that detailed success criteria should be agreed upon and documented for later use in measuring ROI.

5 Formulate policies to address use cases and security concerns

Review how security issues are currently addressed (or not), and develop policies for moving forward. For example, if there is currently no antivirus policy, the team should create one with consideration of the following:

- What endpoint antivirus product is required and how current must signature files be?
- How will non-compliant endpoints be handled?
- Should incidents be logged and an internal department notified?

Another example would be defining secure VLAN segments for medical devices, vendor-owned systems and other operational systems, and controlling appropriate access to these areas. During this stage of implementation, internal deployment obstacles such as inadequate policies or processes, lack of cooperation between departments, organizational issues and any additional network equipment requirements are identified. The project owner can help to address or remove these roadblocks.

6 Determine deployment timeline and milestones

Create a ForeScout platform roll-out plan and timeline. Include planning, installation and activation phases by location, segment or business unit and allow time to assess the success of the rollout before moving on to the next location. ForeScout platform operating procedures and responsible parties should also be established during this stage. To avoid impact on user experience, identify exceptions and security gaps, initially deploying the product in audit-only mode with enforcement and remediation actions disabled. Be sure to outline the criteria for enforcement and remediation, and have agreement from all departments on the deployment team before proceeding.

7 Inform IT staff and end users about network access control policies

The use of additional technical controls to discover and classify endpoints, identify security posture violations and enforce policies makes it imperative that departments are notified of new or modified policies or operational changes. It's advisable to communicate with HR and legal departments to relay acceptable use policies that ForeScout CounterACT®, a core component of the ForeScout platform, can enforce. Educating IT departments about ForeScout's capabilities may also help to expand its use and value. For example, help desk staff may consider using CounterACT to facilitate incident response when resolving IP, MAC and endpoint location investigations.

8 Audit the internal network, assess compliance and expand enforcement

ForeScout CounterACT provides real-time security posture assessment of endpoints. This audit data presents the deployment team with a detailed view of the steps needed to achieve agreed-upon compliance levels. Initially deploying the ForeScout platform in See mode only provides both a test run to see how incidents will be handled and an opportunity to further prepare users for process changes of which they need to be aware. Once endpoint exceptions are identified and an acceptable level of compliance is reached, more advanced enforcement and automated remediation options can be initiated to maintain and further improve endpoint compliance. An enforcement schedule should be included in the deployment timeline.

9 Refine policies, procedures and operations

CounterACT offers powerful features to identify devices—managed and unmanaged, wired and wireless, PC and mobile—attempting to access network resources. Once the platform has been deployed and fully activated, organizations often identify policies and procedures that need to be added or modified, including infrastructure integration, upgrading, exceptions, remediation and reporting. These can be documented, reviewed, phased-in and refined regularly, depending on the maturity of the implementation.

10 Monitor and report on deployment results

The ForeScout platform deployment team should meet regularly to assess the success of the deployment and evaluate how security concerns and compliance requirements are being addressed. By reviewing the success criteria, performance metrics can be easily shared and new policies, exceptions and initiatives can be discussed and agreed upon.

[1]Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

* ForeScout Extended Modules are an integral part of the ForeScout Platform. They enable integration of CounterACT with a wide range of security tools in multiple categories, including Advanced Threat Detection (ATD), Enterprise Mobility Management (EMM), Vulnerability Assessment (VA), and Security Information & Event Management (SIEM) and Endpoint Protection Platform (EPP). In addition, the Open Integration Module (OIM) enables technology partners, systems integrators, and customers to integrate security and management systems with CounterACT. For details, visit http://www.forescout.com/products/extended-modules.

Maximize the Impact of Your ForeScout Implementation

ForeScout certified consultants are cybersecurity experts who can help you quickly **See** managed, unmanaged and Internet of Things endpoints on your network, **Control** them and **Orchestrate** information sharing and process automation among your existing security tools.

Additional Resources

ForeScout Healthcare Solution Brief
Boost healthcare security, privacy and compliance
https://www.forescout.com/company/resources/healthcare-solution-brief/

ForeScout Internet of Things Solution Brief
See and control IoT devices that are invisible to traditional security products
https://www.forescout.com/company/resources/internet-things-solution-brief/

ForeScout Ransomware Solution Brief
Using visibility, control and multivendor orchestration to reduce your attack surface and unify response
https://www.forescout.com/company/resources/ransomware-solution-brief/

University of Rochester Medical Center Case Study
Medical center expands oversight and control over personally owned and medical devices with CounterACT
https://www.forescout.com/company/resources/university-of-rochester-medical-center-case-study/

Northern Health and Social Care Trust Case Study
Healthcare organization gains real-time network visibility and control of endpoints, including embedded systems and medical devices
https://www.forescout.com/company/resources/northern-health-and-social-care-case-study/

SANS: Healthcare Provider Breaches and Risk Management Road Maps
SANS survey reveals security practices in healthcare in light of record breaches
http://www.forescout.com/security-risk-healthcare-organizations-today-sans-report/

Acronym Glossary

BYOD (Bring Your Own Device)
ePHI (electronic Protected Health Information)
HIPAA (Health Insurance Portability and Accountability Act)
HITECH (Health Information Technology for Economic and Clinical Health Act)
IoT (Internet of Things)
IP (Internet Protocol)
MAC (Media Access Control)
ROI (Return on Investment)

About ForeScout

At ForeScout Technologies, we are transforming security by offering the unique ability to see devices the instant they connect to your network, control them and orchestrate information sharing and operation among disparate security tools. Unlike traditional security solutions, ForeScout products achieve this without requiring software agents or previous device knowledge. Our solutions integrate and unify system-wide security management, helping you overcome security silos, automate workflows and gain significant cost savings. Learn more at www.ForeScout.com.

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