Case Study

For This Leading North American Energy Company, Network Security Wouldn't Be Complete Without Device Visibility, Classification and Control

INDUSTRY

Energy

ENVIRONMENT

20,000+ endpoints, including UNIX and Windows workstations, PCs, tablets, smartphones, and IoT devices. Approximately 3,500 employees are distributed across 25+ sites in North America.

SECURITY SOLUTION

- ForeScout CounterACT®
- CounterACT Enterprise Manager

RESULTS

- Gained real-time visibility and policy-based control of devices connecting to the network
- Automated discovery, identification and classification of endpoints, including IoT devices
- Reduced network planning and deployment in field locations by several weeks
- Obtained automated asset inventory and reporting for patch management and overall device management
- Detected 400 vulnerable hosts and addressed WannaCry attack vulnerabilities within 48 hours

Overview

As a major producer of natural gas, oil and natural gas liquids, this company employs more than 3,500 people throughout its extensive operations in North America. The company's network environment is also extensive, comprising a corporate network infrastructure as well as many subnets at widely dispersed offices and field sites. More than 20,000 endpoints, including IoT devices, access the network daily.

Wherever its engineers and technologists are on the North American continent, they require secure networks and workstations that can safely transmit and collect pressure measurements and flow data from field offices, oil wells and compressor stations. It's the kind of information that's needed for conducting business, but also for production accounting and regulatory reporting. As you might expect, in the energy sector, network and data security can mean the difference between an uneventful day on the job and a major crisis.

For endpoint visibility, classification and access control, as well as network segmentation and other use cases, the company relies on the ForeScout platform.

Business Challenge

> *"With ForeScout, we're able to extend our network into an untrusted space and still get a trusted solution."* — Manager of IT, North American Energy Company

This leading energy producer is always going into unchartered territory in search of new opportunities to expand production. Often this entails arriving at a remote site and setting up infrastructure from scratch in isolated locations with unique challenges and a relatively unfamiliar cast of characters—vendors, partners and visitors. Regardless of the difficulties, the network has to go up quickly and remain secure.

The company's manager of IT puts it this way:

> "Let's say I have our corporate network out here and Joe Construction Company wants to stand up a network. We don't want those two networks to exist in the same space. We need a tool to make sure the construction company is not plugging into our network. ForeScout is an excellent solution from that perspective. It's how we cordon off things."

Other security challenges that must be continually addressed include:

- Maintaining a strong security posture without impeding energy discovery and production
- Adding IoT and other types of new devices to networks without adding vulnerabilities
- Ensuring managed devices meet baseline network access requirements
- Maintaining accurate asset inventories for patching and reporting purposes

> **We spent weeks trying to come up with the technical architecture that would give our users secure access to the corporate network without comingling with the vendor's network. ForeScout resolved all of this without adding complex design or costly capital gear. Within a week, it was deployed and off we went."**
>
> **— Manager of IT, North American Energy Company**

- Sustaining the transmission, collection, integrity and confidentiality of production data
- Keeping rogue activity and unknown devices off the corporate network
- Securely accommodating bring your own device (BYOD) and guest endpoints
- Getting as much value as possible from existing network and security tool investments

Why ForeScout?

This leading North American energy producer was an early ForeScout platform adopter. Really early. In fact, the ForeScout platform has been a mainstay of cybersecurity for them since 2007. "At that time," says the company's IT Manager, "we were starting to branch out from firewalls and content filters to expand our view into the corporate network. We looked at a couple of big-name competitors, but their approach kept changing from switched fabric to a more centralized approach, and then back again. I can't speak to how ForeScout landed on our doorstep, but it was the most capable solution, for sure."

The company ran the ForeScout platform in real-time-monitoring mode for a number of years, mostly identifying devices on the corporate network and diverting them onto the guest network if they weren't corporate-owned or were non-compliant with baseline configuration policies. However, over the years, IT has taken advantage of more and more ForeScout capabilities and greatly expanded its use cases.

Business Impact

The ForeScout platform's straightforward, reliable agentless visibility and access control have been critically important in terms of security and productivity. The company has obtained significant value other ways as well.

Managing Assets and Keeping Endpoints Compliant and Secure

The company's IT staff members often pull reports from ForeScout to establish everything from the number of specific models of PCs and workstations in the environment at any given time to which versions of software exist on each managed endpoint. In the absence of a configuration management database, such information is essential for understanding the current state of the company's installed user base. Reports on software configurations especially came in handy in May 2017 when the WannaCry ransomware attack was infecting more than 300,000 computers in organizations all over the world. (See "Making Sure WannaCry Was Somebody Else's Problem" below.)

Eliminating Rogue Devices and Unauthorized Traffic

In addition to using the ForeScout platform for hardware and software classification and reporting, the company has created custom policies to identify and control potentially harmful connected devices and applications. Examples of these devices and applications include USB devices, TeamViewer software, and unauthorized switch ports that have hubs attached to them. Of special concern are dual-homed endpoints that can be plugged into the corporate network and push data onto the Internet without going through the company's firewalls or any other form of inspection. If those endpoints, other unauthorized devices or applications are detected, they are kicked off the corporate network and onto the guest network where they can't do any harm.

> **Within 48 hours we were locked up against WannaCry entirely. ForeScout gave us a level set as to where we stood. It's one of our key sources of truth."**
>
> **— Manager of IT, North American Energy Company**

Accelerating Time to Productivity with Secure Network Segmentation

The company recently began a project to construct two large plants in a remote location. Company employees were working side by side with employees of a third-party vendor while plans were being developed. The vendor provides services to many companies, so the energy company wanted to enforce separation between the vendor's employees and its own employees on the network. The company's manager of IT shares the details:

> "We spent weeks trying to come up with the technical architecture that would give our users secure access to the corporate network without comingling with the vendor's network. ForeScout resolved all of this without adding complex design or costly capital gear. Within a week, it was deployed and off we went."

Detection, Identification and Classification of IoT Devices

Scattered among the 20,000+ devices on the company's network at any given time are IoT devices of all kinds, including VoIP phones and smart printers as well as LCD displays in the lobbies of the company's major offices. The ForeScout platform detects them. It also detects and tracks security cameras at headquarters and field sites.

"We aren't currently doing anything fancy here—just trying to ensure that the cameras stay on the network so that they can report back to our central DVR and our security staff can monitor them," says the IT manager. "To make sure the cameras stay on the corporate network and don't get kicked onto the guest network, we have customized the ForeScout policy to key in on a combination of open ports and NIC vendor identification as well as banner information and a whitelist based on MAC addresses."

The company's IT group has plans to implement smart TVs and smart video-conferencing systems. However, because these types of systems enable Internet-based streaming, conference calling and screen-sharing, they are susceptible to hacking—not something to take lightly when dealing with C-level offices and conference rooms.

"As we think about buying smart TVs for our boardroom and corporate offices, with ForeScout, we don't have to be as concerned about staying on top of what everybody is doing every day," notes the IT manager. "ForeScout manages all that unexpected stuff for us. It's low overhead on our part and the business keeps functioning."

All of that "unexpected stuff" is detected, identified and classified thanks to the ForeScout platform's advanced classification engine, which provides an extremely granular view of what's on the network.

Automating Tasks Through Integration

Because ForeScout has multiple technology partnerships with leading network infrastructure and security tool vendors, the energy company can automate information sharing and orchestration of policy-based actions between leading network, security, mobility and IT management products and the ForeScout platform. Perhaps most important, it can accelerate system-wide threat response while reducing the risk and costs associated with manual analysis and correlation. The energy company's ultimate plan is to use ForeScout's integration capabilities to orchestrate and automate unification of the company's myriad security technologies.

For instance, IT is taking advantage of ForeScout-ArcSight technology integration to enhance its SIEM with improved real-time endpoint data visibility. ForeScout-ArcSight integration eliminates visibility gaps resulting from the periodic nature of the SIEM's log entries. The ForeScout platform closes the gaps by continuously discovering network endpoints in real time and feeding that data into the SIEM, thus providing a significant increase in situational awareness and proactive risk reduction. In the near future, the company also plans to use the ForeScout Extended Module for ArcSight to automate remediation of endpoints that fall out of compliance due to outdated operating systems and applications, as well as to take policy-based mitigation actions to contain and respond to threats.

Making Sure WannaCry Was Somebody Else's Problem

The WannaCry attack in May 2017 targeted Windows-based computers by encrypting data and demanding ransom payments. Organizations that were hit hard were ones that failed to install patches that Microsoft had issued two months prior to the worldwide attack. WannaCry had no effect on this energy company because it has an efficient, standardized process in place that ensures patches are deployed promptly. However, like any global cyberattack, the ransomware event did get IT staff's attention.

"When WannaCry hit in the news, the question became, How patched are we?" says the company's IT manager. "Our vulnerability-management tool is server-based, and there's some question as to how accurate our endpoint patch management tool is, so we looked at what ForeScout could do. It quickly identified where the gaps were—we discovered we had 400 vulnerable hosts, including a subset that had been patched but not yet rebooted—and then generated reports so we could parse out tasks to our desktop folks. Within 48 hours we were locked up against WannaCry entirely. ForeScout gave us a level set as to where we stood. It's one of our key sources of truth."

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