Case Study

FORESCOUT

Energy Company

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

1 WEEK
to visibility and control

3 TO 4 WEEKS
for networking planning and deployment

48 HOURS
to address WannaCry vulnerabilities

Industry
Energy

Environment
50+ locations across multiple U.S. states. 20,000+ wired and wireless endpoints (including mobile and IoT) in corporate IT network

Challenge

- Provide secure access to corporate networks and separation from vendor networks
- Prevent network access by unauthorized devices
- Maintain strong security posture without hindering energy discovery and production
- Minimize risk of adding IoT and other types of devices

Overview

As a major producer of natural gas, oil and natural gas liquids, this leading American energy 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.

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. The company needs to empower these people to do their job yet keep them from inadvertently or maliciously accessing the corporate network. Regardless of the difficulties, the network must go up quickly and remain secure.

Other security challenges that must be continually addressed include:

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

Security Solution

- Forescout platform
- Forescout eyeExtend for Micro Focus ArcSight ESM

Use Cases

- Device visibility
- Network access control
- Asset management
- Incident response
- Device compliance

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

- 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 cybersecurity mainstay for them since 2007. "At that time, we were starting to branch out from firewalls and content filters to expand our view into the corporate network," recalls the company's IT Manager. "We looked at a couple of big-name competitors, but Forescout was by far the most capable solution."

A proof of concept (POC) on one of the busiest floors at headquarters confirmed that the Forescout platform would meet all the company's visibility and control requirements, and more. After the POC, which helped determine configurations and familiarized staff with the solution, the company's managed service provider implemented the Forescout solution within a week. The company then ran the Forescout platform in real-time-monitoring mode, mostly identifying devices on the corporate network and diverting them onto the guest network if they weren't corporate-owned or did not comply with baseline configuration policies. However, since then, the company's IT staff has taken advantage of more and more Forescout capabilities and greatly expanded its use cases.

Business Impact

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.

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, such as 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 other forms of inspection. If those endpoints or other unauthorized devices or applications are detected, they are kicked off the corporate network and onto the guest network where they can't do harm.

Accelerating Time to Productivity with Secure Network Segmentation

The company recently began a project to construct two large plants in a remote

> "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

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. According to the manager of IT: "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. "To make sure the cameras stay on the corporate 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," explains the IT manager.

> "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."
>
> — Manager of IT, North American Energy Company

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

Automating Tasks Through Integration

The energy company plans to use the Forescout platform'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. 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, the Forescout platform closes the gaps resulting from the periodic nature of the SIEM's log entries. The company also uses Forescout eyeExtend for Micro Focus® ArcSight ESM to automate remediation of endpoints that fall out of compliance due to outdated OSes 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 ransomware attack that wreaked havoc globally had no effect on this energy company because it has an efficient, standardized process in place that ensures patches are deployed promptly. "We still had to ask, 'How patched are we?'" recalls 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 turned to the Forescout platform. It quickly identified where the gaps were—discovering 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 team. Thanks to Forescout, we were locked up up against WannaCry entirely within 48 hours."

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com