Case Study

FORESCOUT

American Energy Company

Leading U.S. Power Producer Trusts Forescout for Comprehensive Visibility of Its Corporate Network and Critical OT Infrastructure

TWO
month roll-out of visibility and control

20%
unknown devices discovered

SHADOW
IT uncovered

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
- Necessity of continual uptime in OT environment
- Legacy equipment and devices that cannot be disrupted in any way
- Myriad state and federal regulations related to cybersecurity
- Lack of visibility into all devices on network, including IoT and OT devices

Overview

One of the largest generators of power in the U.S., this company employs thousands of people across more than 50 locations in multiple states. As a public utility and power provider, the company has critical SCADA infrastructure and manufacturing execution systems (MES) to protect. It is also subject to extensive state and federal regulations which require strict network access control (NAC) and other safeguards.

To provide the comprehensive, real-time visibility needed to address these issues, the company turned to Forescout. Deployed in just over two months, the Forescout platform helped the company meet its NAC compliance requirements as well as filled other security gaps in its corporate IT infrastructure. In addition, the agentless Forescout solution provides visibility using non-disruptive methods in the company's critical operational technology (OT) environments, including manufacturing and control systems in a nuclear power plant.

Business Challenge

"As part of our Zero Trust model, complete visibility is essential, but obtaining it cannot impact operations in any way."
– Director of Security
Operations, IT and Control Systems, American Energy Company

The company must ensure 24x7x365 uptime of its critical power generation facilities and comply with ongoing regulatory requirements and associated internal and external audits. In addition, as a power company, it is already a target for hackers with malicious intent. "To protect against these persistent external threats as well as guard against anything that increases risk exposure, such

Security Solution

- Forescout platform
- Forescout eyeManage
- Forescout eyeExtend for Splunk

Use Cases

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

Results

- Rapid time to deployment and granular visibility in both IT and OT networks
- Real-time visibility into all devices the instant they connect to the network
- Discovered upwards of 20 percent more devices than expected in first OT environment
- Uncovered shadow IT and 14,000 more devices than expected on corporate network
- Automatic alerting as new asset detected or critical asset goes offline
- Passive real-time asset discovery, classification, and alerting in controlled infrastructure
- Easier compliance with regulatory requirements
- Visibility capabilities certified for factory acceptance by major OT vendors

as rogue devices or system vulnerabilities, we knew we needed better device visibility and access control," says the company's Director of Security Operations, IT and Control Systems.

The company also desired greater visibility within its multiple OT environments. "We needed to know if there were any unknown assets or assets that are no longer communicating for some reason," explains the company's director of security operations for IT and control systems. "As part of our Zero Trust model, complete visibility is essential, but obtaining it cannot impact operations in any way."

Why Forescout?

A Simpler Solution: Agentless Visibility Plus Rapid Time to Value

To address the need for NAC, the energy company first considered a product from a vendor that already has a large presence in the company. However, that solution would have required a minimum of 18 months to deploy because of its complexity. Then the Director of Security Operations, IT and Control Systems remembered Forescout. "After revisiting Forescout, we chose it because of its agentless approach—no need for 802.1X or hardware and configuration changes—and ease and speed of deployment."

"The Forescout platform was one of our most successful deployments ever," continues the Director of Security Operations, IT and Control Systems. "Had I known how easy it was to deploy, I would have shipped it directly to all our different locations rather than to one central location. All we had to do was put it on the rack and plug it in. In two months, we had deployed all the hardware and were up and running, collecting data in discovery mode, providing more visibility than we have ever had before."

Non-Disruptive, Continuous Visibility for OT

The company also decided to extend the Forescout platform's capabilities to its critical OT environment. "What distinguishes the Forescout platform is its ability to give us active awareness using passive monitoring techniques that don't risk impacting our operations or systems' capabilities," notes the Director of Security Operations, IT and Control Systems. "That capability allowed us to confidently deploy it aggressively and deeply within our OT environment. We are completely aware of our network security posture at all times."

Business Impact

Unknown Devices Exposed in Corporate and OT Networks

When the Forescout platform went live, the company was surprised by the number of devices it found. "We thought we had 6,000 devices on our corporate network, but Forescout found over 20,000," notes the director of security systems, IT, and control systems. "We hadn't accounted for IoT devices and had many more mobile devices than we realized. We also discovered Shadow IT we didn't know about, such as numerous workstations with server software installed."

> "What distinguishes the Forescout platform is its ability to give us active awareness using passive monitoring techniques that don't risk impacting our operations or systems' capabilities. That capability allowed us to confidently deploy it aggressively and deeply within our OT environment."
>
> — Director of Security Operations, IT and Control Systems, American Energy Company

The Forescout platform also found more devices in the company's first OT environment in which it was installed—20 percent more switches and other network infrastructure devices than expected. "There was nothing alarming in these newly discovered devices, but it was still good to know about them, so we can track them along with all our other network assets," says the Director of Security Operations, IT and Control Systems.

Accurate Awareness of OT Security Posture Without Impacting Operations

The company is rolling out the Forescout platform across its power generation facilities using both active and passive methods to provide comprehensive visibility to each site's OT network. "We use active methods where we can and passive methods where we can't, such as on many of our legacy systems," explains the Director of Security Operations, IT and Control Systems. "Either way the Forescout platform gives us total awareness in real time of all devices on the network, including configuration information and asset classification— all without impacting uptime or quality of operations."

"We are also automatically alerted whenever a device enters or leaves the network," he continues. "We have a high degree of confidence in the quality of information we are receiving. That information gives us a solid foundation upon which to build business services."

Certified by Major OT Vendors Before Using in Critical Power Generation Plants

Before implementing the Forescout platform in one of its industrial OT environments, one of the company's subsidiaries racked a Forescout appliance with all the relevant SCADA and programmable logic controller equipment and sent it to Rockwell, Honeywell, and Siemens to conduct factory acceptance tests. After the tests confirmed that Forescout could provide visibility without hindering equipment performance, the company deployed the Forescout platform across all 38 of its power plants, including Purdue Enterprise Reference Model Level 1, 2, and 3 systems at a nuclear power plant. Using the Forescout Extended Module for Splunk, the company also integrated the Forescout platform with its SIEM to enhance out-of-band data aggregation and reporting.

Faster, Easier Device Hygiene and Compliance

"One of our first use cases was to figure out which machines were running antivirus protection," notes the Director of Security Operations, IT and Control Systems. "What our endpoint protection console told us contradicted what we could see for ourselves. Using the Forescout platform, we could see much faster and more accurately than within the antivirus solution's console whether endpoints had AV protection installed, and, if so, which version. From within the Forescout dashboard, we tagged all devices with antivirus signatures that required updating."

> "The real-time accuracy and completeness of the visibility that Forescout provides is what really impresses us."
>
> — Director of Security Operations, IT and Control Systems, American Energy Company

Now the Forescout platform is used to determine the exact version of antivirus protection and location of machines before new updates are pushed out across the enterprise. "We used to spend a lot of time trying to find a device," the Director of Security Operations, IT and Control Systems adds. "Now we know exactly what switch port it's on, or, if it's wireless, what wireless access point it is registering through, plus who owns it and the device's hygiene status."

If the device in question needs to be blocked from accessing the network, it is simple to do so. Right click, choose a blocking method, and the device is off the network.

Future Use Cases for Forescout Visibility

"The real-time accuracy and completeness of the visibility that Forescout provides is what really impresses us," states the Director of Security Operations, IT and Control Systems. "I no longer have to spend a week onsite collecting data, which will be out of date the minute I leave. Instead I have total visibility across the network at my fingertips."

"The comprehensive, granular visibility that we now have with Forescout can help in so many ways beyond just NAC," adds the Director of Security Operations, IT and Control Systems. "We have only begun to tap the potential of the platform. For instance, in the future we will look at integrating it with our ServiceNow® configuration management database to improve accuracy and efficiency in asset management. We can also use it to extend visibility quickly and easily across new acquisitions."

FORESCOUT®

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com

©2024 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents is available at www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners. 06_01