Case Study

State Garden

ForeScout CounterACT® Provides State Garden with Visibility and Policy-Based Control of Devices

INDUSTRY

Manufacturing

ENVIRONMENT

667 endpoints ranging from traditional desktop PCs and laptops to networked production-line machines spanning adjacent buildings

CHALLENGE

- Maximize efficiency of limited IT security resources and personnel
- Protect company assets from unauthorized or non-compliant devices connecting to the network
- Automate endpoint compliance and remediation
- Orchestrate multisystem security

SOLUTION

- ForeScout CounterACT appliance
- ForeScout Extended Module for Rapid7 Nexpose

RESULTS

- Gained seamless transition from evaluation to deployment upon purchase
- Received outstanding visibility of traditional and manufacturing (IoT) devices
- Automated endpoint discovery, classification and remediation
- Achieved flexible policy management and enforcement
- Orchestrated Vulnerability Assessment/CounterACT integration via ForeScout Extended Module for Rapid7 Nexpose
- Quickly built custom integrations

Overview

State Garden has been bringing the freshest, highest-quality produce to food markets for over 75 years. From humble beginnings in Boston's North End in 1938, the Company has grown to be a top producer of both conventional and organic tender leaf greens, spinach, chopped kale, cooking greens and celery hearts in the Northeast. Like any modern company with production lines, State Garden faces cybersecurity challenges, in that nearly every system and machine in their facility is technology-driven and networked.

Business Challenge

The production floor at State Garden is highly mechanized. Optical sorters, produce shakers, custom-built scales and other production-line machines are all networked via wired or wireless connections. According to the Company's Director of Information Technology Billy Lewis, "machine manufacturers understand the need for device security, as there are no longer air gaps in production networks. In a perfect world, every networked device should undergo vulnerability assessment testing and be monitored. However, in today's world, these IoT devices must be secured."

State Garden has a relatively manageable environment—at least from the standpoint of endpoints. At last count there were 677 devices on the network—desktops, laptops, mobile devices, wireless routers, printers, fax machines and previously mentioned production equipment. All of the Company's buildings are connected via fiber and there is only one entry point into the network from outside, which minimizes complexity. However, as in any modern organization, everything that is connected to the network is at risk.

Why ForeScout?

An unusual set of circumstances led State Garden to deploy ForeScout CounterACT®. The process began when Lewis was tracing wires through ceilings to determine which switch port some devices were using. He mentioned the problem to a friend who happens to be a ForeScout customer. His friend told him that CounterACT could identify the port effortlessly—in moments.

Lewis installed the CounterACT demo. "The interface made perfect sense in about three seconds," he said. "We installed it, got it up and running and I knew instantly that CounterACT was going to do a lot more than figure out what network jack went where or what devices were plugged in to what network port."

From there, Lewis tested out the policy engine, got pricing on the CounterACT appliance, and pulled the trigger. "Our evaluation set us up for a 100-percent seamless install of CounterACT," Lewis said. "It was pretty funny," he added, "because all we had to do was back up the demo configuration, restore it and reboot the appliance!"

> **Our evaluation set us up for a 100-percent seamless install of CounterACT. All we had to do was back up the demo configuration, restore it and reboot the appliance!"**
>
> **— Billy Lewis, State Garden Director of IT**

Business Impact

Although State Garden is a major supplier of salad greens in the Northeast, Billy Lewis and one administrator manage the entire IT environment, including security. CounterACT is a large part of the reason why two people are able to cover so much ground. As Lewis says, "CounterACT is like having a whole IT security department. One little box in a server rack is like a full IT staff working 24 hours a day, seven days a week, 365 days a year, no matter what."

More specifically, CounterACT does the following for State Garden:

Visibility

Agentless visibility lets CounterACT see managed, unmanaged and IoT devices the instant they connect to State Garden's network. That includes desktops, laptops, tablets, smartphones, sensors, network infrastructure, peripherals, production-line equipment and rogue devices. Wired or wireless, corporate-issued or personally owned—State Garden IT can see them.

IT Director Lewis commented that they can classify just about anything on the fly. "We identify what's out there, get visibility into what kind of device it is and then take action based on that information," he said. "If it's a new device, we take certain actions based on policies. If it's an existing device, we don't have to worry because the actions have already been taken by CounterACT."

Guest Access

CounterACT lets customers automate visitor, contractor and partner enrollment while enforcing policy compliance. For State Garden, Lewis set up a policy that sends unknown devices to a guest Virtual Local Area Network (VLAN) segment instantly. State Garden IT is then notified via email and text that there is a new device on the network. IT can then tell the user to accept the terms and conditions of the State Garden network, after which the dissolvable CounterACT agent automatically installs on their system and does a non-intrusive scan to ensure that the appropriate antivirus is installed. "It helps a lot because we can go back to the person and say, 'Just an FYI, your antivirus isn't running or isn't up to date,' or 'Did you know that you're missing a whole bunch of patches?'" Lewis said.

Endpoint Compliance

Unlike systems that simply forward alerts and send IT staff scrambling, CounterACT assigns devices to the appropriate access control list or VLAN segment based on policies. This allows customers to limit access to necessary resources within a restricted VLAN, safely quarantine devices for remediation or further analysis or terminate access at the switch. At State Garden, all unknown devices accessing the network are sent to a restricted VLAN where they are scanned for vulnerabilities. Non-compliant devices don't go any further.

Endpoint Remediation

CounterACT proactively identifies unsecured endpoints on the network and can automatically remedy the problem based on policies. However, State Garden does both automated and manual device remediation. "We use CounterACT for people on laptops that are coming and going from the network because they may not be here at two o'clock in the afternoon when the automatic updates are pushed out," Lewis said. "If a system connects and it's missing updates, CounterACT will actually tell the system to go ahead and pull the updates without waiting until two o'clock."

> **CounterACT is like having a whole IT security department. One little box in a server rack is like a full IT staff working 24 hours a day, seven days a week, 365 days a year, no matter what."**
>
> **— Billy Lewis, State Garden Director of IT**

Application Blocking

State Garden doesn't have much of a need for application blocking because the Company uses relatively few applications, and it's a rare event when something unauthorized comes across the wire. However, they do keep tabs on cloud storage and use CounterACT to restrict access to Dropbox. "If CounterACT observes that there's a Dropbox client on an unauthorized system, it stops it from being run," noted Lewis.

Vulnerability Assessment

State Garden faced a common challenge of scanning mobile devices that come and go from the network. As a result, users often missed the regularly scheduled vulnerability assessment (VA) scans. The ForeScout Extended Module for Rapid7 Nexpose® resolves this issue. CounterACT automatically detects when a new device enters the network and informs Nexpose. If the device has missed a scan, Nexpose performs one. "If a Rapid7 Nexpose scan comes back on a device and it has multiple vulnerabilities, CounterACT can automate remediation," Lewis said. "But if for some reason something fails in the process, like a Windows® update stops running, we can put the device on a different VLAN and take manual action. It gives us a wonderful array of choices in how we handle the device going forward."

State Garden's Billy Lewis puts it best:

> "We integrate CounterACT with other products, whether it's via ForeScout Extended Modules or custom integrations that we are building ourselves. CounterACT is kind of like a Rosetta Stone in that it can function as a translator to pass information back and forth. It takes the guesswork out of everything because it's speaking a common language for all these different devices, endpoints and software packages, and it gives me the information I need in just the way I asked for it."

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