Case Study

FORESCOUT

HAWORTH®

Haworth

Global Manufacturer Secures IT and OT Network, Achieves Dramatic ROI With Forescout

INDUSTRY

Manufacturing

ENVIRONMENT

12,000 wired and wireless devices across 20 production facilites and 55 sales offices worldwide; 6,200 employees.

CHALLENGE

- Lack of visibility into all devices on network, including IoT and OT devices
- Insufficient visibility into security hygiene of newly acquired companies
- Necessity of continual uptime in OT environment
- Small security team with limited time and resources

SOLUTION

- Forescout platform
- Forescout Enterprise Manager
- Forescout Extended Module for Palo Alto Networks Next-Generation Firewall

USE CASES

- Device visibility
- Device compliance
- Network access control
- Network segmentation
- Incident response

Overview

With a focus on innovation and productivity, Haworth Inc. designs and manufactures adaptable workspaces, including raised floors, movable walls, systems furniture, seating and Workware™ wired and wireless technology devices for real-time collaboration. The Holland, Michigan-based company employs 6,200 people worldwide in 20 production facilites and 55 sales offices. With the recent acquisition of several lifestyle design companies, Haworth needed network access control (NAC) that would permit only authorized devices that meet corporate security standards to access its corporate network.

To meet the company's NAC needs as well as fill other security gaps, such as rogue device detection and containment, Haworth implemented the Forescout platform. With its granular visibility and control, the Forescout solution dramatically improved the security posture of both IT and production environments. Furthermore, integrating it with the company's firewalls allowed automation of security tasks, freeing up Haworth's information security team tremendously. The Forescout platform also proved its worth beyond the security realm and is used by other operational areas, including network management.

Business Challenge

"For these use cases and others, we needed not only greater visibility and control, but also the ability to classify devices, segment networks by device and look for indicators of compromise—all in real-time."

— Joseph Cardamone, Senior Information Security Analyst and North America Privacy Officer, Haworth

Senior Information Security Analyst and North America Privacy Officer Joe Cardamone leads information security strategy at Haworth. As part of a three-person information security team, Cardamone and his colleagues strive to protect both corporate and production environments throughout Haworth's global enterprise. The company's recent acquisition of many autonomously run companies exacerbated the challenge.

Devices owned by its new affiliates weren't the only assets for which the team needed greater visibility and control. For instance, they needed a better, faster way to locate high-risk IoT devices and prevent them from receiving or transmitting any unauthorized communications. They also needed to easily identify and secure its proprietary Workware digital collaboration devices, which constantly move between locations and whose software and hardware are frequently updated.

RESULTS

- Rapid time to value: 97 percent of endpoints discovered and categorized out of the box within first seven hours
- Real-time visibility into all devices the instant they connect to the network
- Easier protection of OT and continually moving devices thanks to dynamic network segmentation
- Network access control for newly acquired companies connecting to the corporate network
- Savings of 20 hours per week by automating security tasks
- Additional time savings from automating manual processes to find and isolate high-risk devices
- Ability to maximize efficiency of three-person IT security team
- Granular visibility that aids security, IT groups and the network team
- Discovery of 60 percent more devices than expected

Why Forescout?

An Easy-to-Deploy, Easy-to-Use "Information Powerhouse"

Cardamone and his team conducted proof of concepts for the Forescout platform and a solution from a vendor that already had a significant presence in the company and the initial backing of Haworth's network team. Forescout emerged as the clear winner.

"The Forescout platform is an information powerhouse that, unlike our alternative, is quick to deploy and very easy to use," states Cardamone. "From a single pane of glass, I can see across our entire environment with highly granular detail and manage protection with a right click on my mouse. The GUI is very intuitive and the information so clear that even new team members and other departments outside security—including the network team—can use it and benefit from it."

Business Impact

Rapid Deployment and Time to Value Out of the Box

Deployment of the Forescout platform took less than a day. "We started implementation at lunchtime and when I fired up my computer that evening, 97 percent of our environment had already been discovered and classified," he recalls. "Within seven hours we had detailed visibility of our global environment. That's impressive."

Value of Comprehensive, Granular Visibility Demonstrated from the Beginning

The accurate visibility provided by the Forescout platform proved its worth immediately upon implementation. "We thought we had around 7,500 devices on our networks but the Forescout platform discovered more than 12,000 IP addresses," notes Cardamone. "We also discovered security gaps we didn't know about, such as a dozen wireless access points installed in our showrooms. The newfound visibility allowed us to block those devices as well as contact the local administrators to remediate them."

"But that's just the tip of the iceberg," continues Cardamone. "The amount of information we get back from the Forescout platform is incredible. While many other tools discover the IP addresses of endpoints, it is by far the best solution I have ever used to properly find, identify and control systems. It has been beyond valuable to us."

"Often we can automate action against an endpoint, but when manual intervention is needed, a simple right click is all it takes," continues Cardamone. "I can also enable Level 1 or 2 staff to take Level 3 actions in a crisis without giving access to privileged functions. The Forescout platform has powerful capabilities right out of the box but is also very customizable. The sky's the limit on what we can do with it."

Visibility into Device Hygiene of Acquired Companies

The Forescout platform provided visibility into the acquired companies and the device hygiene level at each. "If their devices haven't been patched in a long time, we know it, and can take action" says Cardamone. "The Forescout platform also checks the patching and antivirus status and operating system of any affiliate device that attempts to connect to the corporate network and blocks those that don't meet our criteria."

> The amount of information we get back from the Forescout platform is incredible. While many other tools will find the IP address of endpoints, it is by far the best tool I have ever used to properly find, identify and control systems. It has been beyond valuable to us."
>
> **— Joseph Cardamone, Sr. Information Security Analyst and NA Privacy Officer, Haworth**

Simpler but More Customizable Network Segmentation

Using the Forescout Extended Module for Palo Alto Networks® Next-Generation Firewall, Cardamone quickly integrated the Forescout platform with the company's firewalls to enable on-the-fly network segmentation based on accurate, real-time, contextual information provided by the Forescout solution. "With the Forescout-Palo Alto Networks integration, we are no longer limited to segmentation by basic identifiers such as IP or VLAN," explains Cardamone. "We have a lot more options than we would have with only 802.1X because we can base the segmentation on a much deeper, richer endpoint profile."

For instance, in Haworth's manufacturing environment, Cardamone uses the Forescout platform to identify and classify all high-risk IoT devices—primarily those devices that are no longer supported by the manufacturer, such as Windows® XP or Windows 2000 operating systems. Dynamic network segmentation then automatically blocks these devices from receiving or transmitting any information except under very specific authorized circumstances.

Huge, Quantifiable Time Savings from Integration and Automation

In addition, the Forescout-Palo Alto Networks integration enabled Haworth to automate cumbersome, manual processes. Take Haworth's Workware technology devices, for example. Present in Haworth headquarters and showrooms around the globe and run on production VLANs, these devices used to be assigned a static IP address that was then allowed to talk to the guest network through the firewall. With 130 of these devices in headquarters alone, constant updates and changes to hardware and software, and physical moves that changed IP addresses, a manual process simply could not keep pace to provide adequate network access control.

Today, however, the Forescout platform finds them, classifies them and places them in a dynamic access group linked to a firewall policy that allows IP addresses in that group to talk to the guest network on needed ports and applications. "So, whether the device is moved to China or Germany, Forescout finds it and the firewall knows what to do," says Cardamone. "What was once an ongoing, almost impossible manual task is now completely automated."

"If we add up all the time we have saved in our various use cases since installing the Forescout platform and integrating it with our firewall, I estimate savings of about 20 hours each week, or half of a full-time employee," says Cardamone. "Our small security staff can do more to secure our environment but with less work."

Benefits of Forescout Visibility Extend Beyond Security

Haworth operations staff also benefits from the Forescout platform. Technology support technicians use it to physically locate devices. Software management uses it to check for noncompliant applications. Even the network team uses it weekly to find information on ports and switches. And new uses are always in the pipeline. For instance, Forescout will play a critical role when the company transitions to a BYOD policy in the future.

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