Case Study

FORESCOUT

City of Guelph

City of Guelph Fortifies PCI Compliance & Mobile Security with the Forescout platform

SAVED
a tremendous amount of weekly administrative effort

100%
visibility to IP-devices conntected

TIME
saved with automated audit and compliance reporting

CITY OF Guelph
Making a Difference

Industry
State and local government

Environment
2,000 employees spanning 35 sites

Challenge
- Protect sensitive personal information, enable personal mobile device use, and increase visibility into all of the devices attached to the network

Security Solution
- Forescout platform

Overview

The City of Guelph in Ontario, Canada, is a vibrant community of more than 130,000 people that is ranked among the top ten places to live in Canada. The City has about 2,000 employees spanning 35 sites.

Business Challenge

The City's IT team sees network security as an ever-changing landscape, and recently launched a multi-faceted initiative to enhance compliance effectiveness and reporting efficiency, personal mobile device access and overall visibility into the network and attached devices.

The City accepts credit and debit cards for payment, and as part of its on-going PCI-DSS compliance needed to more efficiently generate required detailed reports on network devices, antivirus and patch status. Another goal was to enable employees to use personal mobile devices and further automate access policies for contractors and guests, while at the same time controlling their access and isolating them from the corporate network. Finally, the team wanted to increase visibility into all of the devices attached to the network and examine their security profile in detail against established policies.

Why Forescout?

In the first step, a cross-organizational team with both IT and business unit members extensively evaluated and benchmarked the top device visibility and access control candidates in detail. Next, they brought in additional expertise from security integrator Conexsys to expedite further assessment and implementation.

Use Cases

- Device visibility
- Asset management
- Device compliance
- Network access control
- Network segmentation

Results

- Allowed visibility to all devices connected to the network
- Enabled secure network access using personal mobile devices
- Simplified guest networking

They selected the Forescout platform due to its ease of use and deployment, integrated functionality and built-in templates. Other key considerations were its flexible implementation and policy enforcement.

"According to Shibu Pillai, the City's Network Security Specialist, "we get real-time visibility and can drill down to a specific endpoint and see the entire status of the device, even the Windows update status. Not only do we know everything that's connected, we can properly classify each device and put them on different network segements based on their profile."

"With limited resources we wanted to ensure a timely implementation of our network security solution. Conexsys proved to be a competent IT solution provider and really enabled us to progress rapidly against our agenda with assured results," continued Pillai.

In the first step, a cross-organizational team extensively evaluated and benchmarked the top NAC candidates in detail. Next, they brought in additional expertise from security integrator Conexsys to expedite further assessment and implementation. Other key considerations were its flexible implementation and policy enforcement.

Business Impact

Compliance Reporting

Pillai also appreciates the the way the platform has automated compliance reporting. "In the past we had to run internal assessments to create reports required for PCI-DSS compliance. With Forescout, one interface will deliver us the status of all Windows updates/patches and our antivirus, which saves us a significant amount of time doing audit and compliance reporting."

> "The Forescout platform greatly augments the measures taken by our organization to safeguard our IT infrastructure with regards to automated endpoint compliance and mobile security."
>
> — Shibu Pillai, Network Security Specialist, City of Guelph

Personal Mobile Device Access

"Our Human Resources Department is very pleased with what we've done for our employees with guest networking. The City is now encouraging staff to bring in their personal devices and use them at leisure times in the courtyard or the employee lunchroom. This is a big benefit for our employees because they can sit in one of our lounges or on our patio on their breaks and access the Internet as a guest, without compromising our security at all," recalled Pillai.

Guest Networking

"Prior to implementing this solution, the network access for guests such as contractors was a manual process and not foolproof. It did not guarantee that the devices were safe and after use we had to remember to disable the port. Guests that were unaware of our network access policy would try to connect and then realize IT needed to intervene. This caused delays and put the IT staff in a reactive mode, as meetings and presentations could not proceed without network connectivity. Now when a device is connected, it is automatically checked and connected to the appropriate network without IT intervention. Being able to do this through a single interface saves us a tremendous amount of administrative effort every week."

"Now when a device is connected, it is automatically checked and connected to the appropriate network without IT intervention. Being able to do this through a single interface saves us a tremendous amount of administrative effort every week."

— Shibu Pillai, Network Security Specialist, City of Guelph

FORESCOUT

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