Case Study

Queens College

ForeScout CounterACT® Provides Queens College with improved Network Visibility, Asset Intelligence and Complaince

INDUSTRY

Education

ENVIRONMENT

5,000 in faculty and staff, with a student population of nearly 20,000

CHALLENGE

- Ensure visibility and management of corporate assets as well as the connecting personal and corporate devices being used by faculty and students

SOLUTION

- CounterACT's effectiveness in corporate asset management
- Continuous monitoring and mitigation of threats and security exposures

RESULTS

- Increased network visibility
- Improved asset management
- Flexible policy management and enforcement
- Improved network uptime
- Help desk savings through adoption of automated processes

Overview

Queens College is a senior college of the City University of New York, the third largest university system in the U.S. in terms of enrollment. With a faculty and staff of 5,000 and student population of nearly 20,000, the school was inundated with not only a large number of college-owned devices but the powerful surge of the bring your own device (BYOD) trend in recent years as well.

Business Challenge

The College's IT and asset management teams desired a solution that would not only let them better manage and organize corporate assets, but also monitor its network with more complete visibility and control. Before searching for a network access control (NAC) solution, the school had virtually no way to appropriately estimate the number of devices, including desktops and laptops, that were connecting to its networks. Being able to identify and classify these endpoints was an essential component while looking to improve the school's network security. In addition, the school had to securely manage users and mobile devices connecting to their computing resources.

Another issue that prompted Queens College's IT team to search for a NAC platform was the outbreak of more sophisticated threats, including zero-day attacks. Prior to deploying CounterACT®, it was not uncommon for hundreds of computers on the network to be regularly infected and spreading malware to other machines. Malware and other threats even consumed enough bandwidth to take the college network services offline.

IT was forced to conduct manual investigations, even going through firewall logs to identify infected devices and, one by one, to disable their network ports. At that time, the user and help desk didn't know why their network ports went down, requiring more resources to determine the source and scope of problems which could take weeks to resolve.

Why ForeScout?

Queens College initially turned to ForeScout CounterACT to help protect them against the onslaught of advanced threats and propagating worms, which in the past would have infected hundreds of computers, literally bringing the network to a crawl.

"Once we had CounterACT in place, the first time a new worm broke out, we had only three computers that became infected. They were immediately isolated and the infection was contained," said the school's Director of Network Services and Internet Security Officer Morris Altman.

"Additionally, those three users were automatically notified about the problem, and instructed to call our help desk so we could fix it. Instead of weeks, the problem was solved in less than a day and had minimal impact on our students, faculty and staff," Altman added.

> **With FireEye and ForeScout, we know the details, security posture and activity of all devices on our network, and we can automatically isolate violations, malware and affected systems before anything gets out of hand."**
>
> **— Morris Altman, Director of Network Services and Internet Security, Queens College**

The ForeScout Difference

Key differentiators that contribute to Queens College's overall success:

- Gained network visibility and asset intelligence to support BYOD
- Network control, policy enforcement and compliance
- Automation of help desk alerts and time savings

After such a positive experience with the initial implementation, the networking team expanded its use of ForeScout CounterACT to enhance visibility and control over who and what types of devices are connecting to its networks. More recently, the college integrated CounterACT with FireEye to identify and quarantine advanced persistent threats (APTs).

Business Impact

As conscientious professionals, Queens College's IT and networking teams have maintained its CounterACT appliance, modules and integrations as updates have been released. The school is currently using CounterACT Enterprise Manager, which centralized the administration of four CounterACT 4000s. These have provided the following benefits:

Real-Time Visibility

CounterACT gives Queens College's IT and networking teams comprehensive, real-time visibility into connecting wired and wireless devices. The networking team is able to see what version of software and operating systems users are running on their endpoints, which tells them how many devices are on the network, the type of devices, and if they have vulnerabilities, such as out-of-date software.

"Until we had CounterACT, we really didn't have an idea of how many devices were on our networks," said Altman. "We discover all sorts of things, and it's a learning experience. We now know that we have about 6,000 wireless and 5,000 wired endpoints at any given time. This helps when deploying policies, for instance. You monitor, learn and then make educated decisions."

This detailed insight into network devices allows Queens College to understand the diversity of devices and prioritize the devices or operating systems they support when new applications are released. For example, if only 10 users have Windows phones and thousands have Android and iPhone devices, the priority shifts.

Asset Intelligence and BYOD

The visibility also offers insight for enterprise asset management. For example, Altman works closely with the asset management team lead to remediate missing patches or broken security agents. Because ForeScout CounterACT does not require agents and offers granular, role- and device-based policies, the approach facilitates personal device use with rich network and wireless guest management and monitoring that does not impact user experience.

Network Control, Policy Enforcement and Compliance

Queens College is also using CounterACT to block unauthorized and noncompliant users. Like all colleges and universities, the school must comply with regulations such as the Digital Rights Millennium Copyright Act. The ForeScout solution assists IT in enforcing take-down notices for music and movies with copyright violations that are downloaded from peer-to-peer software.

"We were using a device called a package shaver to help control copyright issues for a long time, and when it stopped working, I looked at CounterACT and was able to rewrite a policy to detect when this was going on," said Altman. "We then started blocking people from the network

and were able to notify them of their violation, therefore improving our compliance with the regulation."

The College also blocks unauthorized applications from running on the network, and CounterACT allows the IT teams to notify students and faculty when their machines are lacking up-to-date software, including common applications that often become infected such as Adobe Flash Player, Adobe Reader and Java. This also supports the Family Educational Rights and Privacy Act (FERPA) by keeping all endpoints up-to-date, which allows the school to reduce the risk of information disclosure.

Automation and Time Savings

Queens College is using CounterACT to automate help desk alerts. Prior to CounterACT, individuals with infected machines would have to call the help desk on their own. Now, with ForeScout, the help desk knows of the issue, often before the user notices, and calls them first to resolve the issue quickly and conveniently. "Automation makes it possible for us to survive," stated Altman.

Strong Interoperability

Queens College has been able to integrate CounterACT to its existing wired, wireless and security infrastructure leveraging ForeScout ControlFabric® technology. The College combined CounterACT with FireEye to address APTs. While FireEye does have the ability to block outbound malware communications when installed inline, Queens elected not to deploy that functionality due to worries about bandwidth and availability. Instead, when FireEye spots an infected computer, it sends a message to CounterACT with the IP address, the severity level and the infection name, whereby a ForeScout policy is invoked to quarantine the system.

Improved Network Uptime

With CounterACT, Queens College is currently seeing improved network uptime. Prior to deploying the ForeScout appliance in the early 2000s, the school would have security incident-related network outages as least two or three times per year.

"Now with CounterACT, we haven't had outages anymore. We're up nearly 100 percent of the time," said Altman.

Use Cases for All IT Departments

CounterACT benefits span across the entire IT team at Queens College. Asset management uses it for visibility into the network while the endpoint team monitors device posture, the help desk examines what's going on with devices when issues are reported, and the network and security teams constantly monitor for risks and exposures. Students and staff can even use CounterACT desktop support for personal patches.

Quality Technical and Customer Support

Since Queens College's procurement of ForeScout CounterACT, they have received exemplary customer service and support. Altman noted that ForeScout immediately takes action when problems arise and regularly checks in to make sure CounterACT is running well.

"As a matter of fact, ForeScout is one of the best companies I know for listening to customers," said Altman. "We're consistently having people checking in with us, seeing how things are going, helping and making suggestions. It's great. From the sales team to the engineers and support staff, they're all dedicated, they all care, and they all seem to love the company and our success. That means a lot."

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

Version 2_17