Case Study

Broward College

Highlights

Objective

Broward College needed a secure, efficient and flexible way to manage the personal and college-owned devices connecting to its network, spanning four campuses and seven satellite locations.

Solution

After looking at several solutions, Broward College selected ForeScout CounterACT for its extensive functionality and deployment ease that did not require agents. CounterACT provides real-time network visibility, flexible controls, BYOD policy enforcement and support for compliance.

Results

- Increased visibility and control of personal and college-owned devices brought in by students and staff
- Time-saving endpoint security policy configuration and enforcement without disrupting the end-user experience
- Seamless integration with existing network and security infrastructure to preempt issues and improve threat detection and response
- Support for compliance with PCI, FERPA, HIPAA mandates and copyright laws

"With CounterACT, the reduction of risk is invaluable. We went from very little visibility to complete visibility and control."

Matt Santill
Chief Information Security Officer (CISO
Broward College

ForeScout

ForeScout CounterACT Increases Visibility, Control and Compliance at Broward College

BROWARD COLLEGE℠

Customer Overview

Broward College is one of the largest colleges in the U.S. with more than 68,000 students. Between its four large campuses and seven satellite locations in South Florida, the school supports a broad array of devices simultaneously connected to its core network at any given time.

Broward's IT team designed their IT and security strategy to align with the college's goals. In higher education, the students and faculty are the customers. Therefore, the most important mutual objective was to invest in technologies that create an environment for student success, including the ability for its faculty, staff and students to use any device to facilitate learning. In order to advance their bring your own device (BYOD) strategy, the IT team had the responsibility to ensure that their information assets would remain adequately protected, that their network could minimize threats and that operation availability would remain strong.

The first step in achieving the college's main goal was to gain visibility into all of the devices connecting on the network. Determining whether connecting devices were college-owned or personally-owned, or potentially rogue or unmanaged, was also a top priority. The team wanted to ensure they had network controls in place based on the type of user, the type of connected device and the secure configuration of that device. The team was also looking to use automation to reduce staff hours spent on more mundane tasks, such as adding devices like printers to their VLANs and effort spent remediating security issues.

"We didn't just want to scan or run reports to see what types of devices were connected; that is too passive and reactionary," said Matt Santill, chief information security officer (CISO) at Broward. "We wanted complete visibility and immediate control to block or warn users as we saw compliance violations."

Broward reviewed several network access control (NAC) products including Aruba ClearPass, Enterasys and ForeScout CounterACT™. The Broward teams initially considered Enterasys because they use the vendor for their wired network and contemplated going with Aruba, which they use for wireless.

However, both solutions lacked several essential functions. For example, Enterasys used agents, which would require too much manual effort from the IT team. Plus, it only looked at managed devices connecting to the network and lacked many inspection and post-admission capabilities. Aruba did not offer enough support for the school's wired network without a significant investment and also lacked many features such as endpoint discovery and classification. Both approaches had limited third-party integration.

Why ForeScout?

After an extensive review process, Broward ultimately selected ForeScout CounterACT for several key reasons, led by CounterACT not requiring agents. They saw that CounterACT's ability to deliver full network visibility into the devices on the network, as well as extensible policy enforcement capabilities added great value beyond the competition. Finally, the ForeScout ControlFabric™ technology would allow them to integrate with other security solutions already deployed, allowing them to further leverage the investment in CounterACT.

"CounterACT gave us complete visibility and control without having to implement 802.1X," said Santill. "We could immediately see the device type, the connected user, opened ports, running processes, vulnerabilities and security issues on every device on the network. This was real-time visibility without having to run an independent scan or report. We not only had significantly more visibility, but we could take faster, more informed action."

How ForeScout Helped

Broward College initially deployed CounterACT in December 2013. They started with two CounterACT CT-10000s and an Enterprise Manager, which have delivered the following benefits.

Real-time Visibility

CounterACT gives the IT team visibility into the devices connecting to Broward's network and allows them to immediately spot trends and details they otherwise would have missed.

For example, before installing CounterACT, they did not realize how many devices were actually connecting and were floored by the actual numbers. CounterACT identifies how many people are logged in using a single individual's user account across the entire network from which the IT team can identify suspicious behavior. In one instance, Santill noted that he saw some user accounts logged in from more than 20 separate machines, thereby alerting IT and triggering them to assess if those users were handing out their login credentials or if someone was actually gaining unauthorized access.

"With CounterACT, the reduction of risk and added time-saving is invaluable. We went from very little visibility to complete visibility and control," said Santill.

Full Network Control

Using ForeScout, Broward can isolate devices using CounterACT's virtual firewall technology. They can block off infected or compromised email inboxes, mainly on student devices, while still allowing the end user to surf the Internet or do their work. They have successfully been able to block a variety of viruses and mail bots without interfering with the learning environment. This protects other student and faculty machines on the network from infection, giving Broward full control of their network environment.

"Before CounterACT, we had no way to take action without doing so directly from the firewall," said Santill. "Now, with ForeScout, we have it set up so that it talks to all of our switches, as well as the wireless controller. So if we see some type of network violation or spam originating from a computer, we can block the port that computer is on."

Policy Configuration & Enforcement

Broward was able to easily create custom policies to meet the needs of different IT and information security departments within the school. The staff was able to quickly modify built-in templates, test policies and adjust controls according to each department's requisites.

BYOD

In the past, Broward had an Acceptable Use Policy (AUP) but could not effectively enforce controls. With CounterACT, Broward is able to provide students and faculty with a solid BYOD experience that automatically limits network resource access for personal devices that don't adhere to the college's security policies and notifies users to promote acceptable behavior.

Automation

With ForeScout, Broward has been able to automate processes in its network security routine that they were previously forced to perform manually. For example, the IT team was able to save a great deal of time automating VLAN assignments for different device types and users.

Security Software Integration

The college benefits from ForeScout's ControlFabric technology, which allows CounterACT to exchange information with other security solutions and enable these solutions to invoke CounterACT network enforcement and endpoint remediation capabilities. Currently, Broward integrates its ForeScout solution with its QRadar SIEM system, allowing the IT and information security teams to see real-time device and user information sent by ForeScout.

"We can take action on any suspicious behavior we're seeing from CounterACT itself or in our SIEM using CounterACT to do network isolation or simply sending message pop-ups," said Santill. "We do that on a regular basis, especially for inappropriate content and other types of policy violations by sending those users a notification on their desktop saying they're breaking college policy."

Privacy and Regulatory Compliance

Not only does CounterACT assist Broward in enforcing its own policies, it also allows the school to comply with a variety of privacy regulations such as Payment Card Industry (PCI), Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPAA).

To improve compliance with all of these regulations, Broward uses CounterACT to create an inventory list of machines that access sensitive data on a regular basis. Using this list, they are able to separate individuals that access this data into specific groups inside the management console. This allows them to more easily keep an eye on users and systems and to identify those violating security policies.

Copyright Law Compliance

Broward is also required to comply with the Digital Rights Millennium Copyright Act. CounterACT helps the college to comply with this mandate by notifying the IT and information security teams when a user is committing copyright infringement or running peer-to-peer software on their machines. It also allows IT to take action on that software.

Broward either remotely terminates the program so non-compliant users cannot access it anymore or sends a message to the individual, letting the user know that they have violated a network policy.

"We feel that CounterACT is one of the best security tools currently on the market," said Santill. "It not only provides immediate operational value, but the visibility allows us to plan strategically for the future."

> *"We feel that CounterACT is one of the best security tools currently on the market. It allows us to plan strategically for the future."*
>
> **Matt Santill,**
> **Chief Information Security Officer (CISO),**
> **Broward College**

Take the ForeScout Challenge

Let us know which ForeScout solution is right for you, and we'll arrange a free on-site evaluation.

About ForeScout

ForeScout delivers pervasive network security by allowing organizations to continuously monitor and mitigate security exposures and cyberattacks. The company's CounterACT platform dynamically identifies and assesses network users, endpoints and applications to provide comprehensive visibility, intelligence and policy-based mitigation of security issues. ForeScout's open ControlFabric technology allows a broad range of IT security products and management systems to share information and automate remediation actions. Because ForeScout's solutions are easy to deploy, unobtrusive, flexible and scalable, they have been chosen by more than 1,500 enterprises and government agencies in 54 countries. Headquartered in Campbell, California, ForeScout offers its solutions through its network of authorized partners worldwide.
Learn more at www.forescout.com.

ForeScout

ForeScout Technologies, Inc.
900 E. Hamilton Ave.,
Suite 300
Campbell, CA 95008
U.S.A.

Contact Us
T 1-866-377-8771 (US)
T 1-408-213-3191 (Intl.)
F 1-408-371-2284 (Intl.)
www.forescout.com