



ForeScout's Network Access Control Makes the Grade at Marquette University

“CounterACT keeps the network safe and people appreciate that we're keeping it clean and fully functional for them.”

Michael Wiedower
Security Analyst
Systems & Messaging
Marquette University

Marquette University, located in Milwaukee, Wis., is a Catholic, Jesuit university with approximately 11,500 undergraduate and graduate students from every state and 80 countries. U.S. News & World Report ranks Marquette 82nd among the nation's top 100 universities in the 2008 edition of America's Best Colleges, while BusinessWeek ranks the university's College of Business Administration among the top 50 undergraduate business schools in the nation.

With 3,500 resident hall endpoints and 4,000 wireless faculty and student users, the university's IT department was faced with a daunting task—to monitor faculty and students' personal computers and laptops and ensure no infected devices could enter the network to cause disruptions or outages or contaminate other resources.

“Essentially, we had to come up with a way to detect and monitor 8,000 devices using the network,” said Michael Wiedower, security analyst - systems & messaging, Marquette University. “We initially attacked the problem by spending over \$5,000 a year to create and distribute CD-ROMs that included security upgrades and patches to every student and staff member. But the infections continued because, as soon as patches from one CD were installed, more new ones were needed, ones that weren't on the CD.”

Marquette University began looking at Network Access Control (NAC) solutions, including those from Cisco and ForeScout Technologies. Wiedower's team placed priority on solution flexibility, including the ability to work without a client installed on each endpoint, as well as the ability to tailor policy enforcement. Marquette University looked carefully at each solution and selected ForeScout's CounterACT.

Why ForeScout?

“Most of our users come onto the network as guests (machines that are not owned by the university) and therefore we're not able to demand client installs,” said Wiedower. “It is therefore impossible to reach every guest; it also comes down to end-user privacy. We simply needed to ensure that only uninfected devices use the network, and that's what CounterACT helped us accomplish.”

Marquette's network is able to distinguish faculty from students, which allows the security team to enforce a CounterACT security policy directed to student machines. For students – also recognized as “guests” by the network – CounterACT simply monitors devices and, once an infection is detected, the browser session is hijacked to inform the user that he or she must remediate the device in order to comply with security policies and access the network.

Once an infection is detected, CounterACT instantly deploys a virtual firewall around the infected device, allowing the user access only to remediation resources and isolating the infected device from the rest of the network. The student or guest is then directed to self-remediation options (such as a site for downloading anti-virus updates or Microsoft security patches) or given the option of bringing the device to a campus IT center where it can be brought into compliance by the helpdesk staff.

“The bottom line is that only when the device is infection-free can it can rejoin the network,” said Wiedower. “CounterACT ensures that end-users with infected devices have no choice but to comply.”

How ForeScout Helped

- » Virus and worm outbreaks are caught and contained immediately. If a student tries to gain network access with an infected device, CounterACT blocks it entirely. CounterACT then guides the user to where he or she can fix the problem and bring the device into compliance in order to regain access the network.
- » Device interrogation is seamless. Users remain productive while their device is being monitored for presence of self-propagating malware or worms.
- » NAC policy enforcement is deployed without use of a client or agent installed on the end-user device, keeping the network safe while avoiding academic freedom and students' privacy rights issues.

The ForeScout Difference

With ForeScout's CounterACT, Marquette not only saves thousands on CD-ROM creation and distribution, but the solution also ensures devices remain compliant with security policies all the time. “The CD system, while it worked for a time, was antiquated and overwhelming in terms of the work required, and by the time CDs were distributed, new updates would become available, causing the need for another run,” said Wiedower. “CounterACT eliminates those costs and headaches. With CounterACT, if a user's device is acting badly, we will catch them and stop them. False positives are also extremely low with CounterACT. We are now looking into options of what more we can do with NAC, such as offering deeper level interrogation for guests upon their request.”