Case Study

Marquette University Maximizes Security ROI with ForeScout's CounterACT

ForeScout's CounterACT saves thousands in staffing and remediation costs

CounterACT continuously monitors network access and activity on Marquette's hard-wired and wireless network segments. It automatically detects each device that attempts to connect to the network, determines the port to which it is attached, the MAC address of each device, the configuration and respective security posture of the device and the activities being performed by the device post admission. The system applies built-in and customized rules that have been established to enforce access policy, to respond to exceptions and prevent threats.

This type of automatic monitoring of as many as 14,000 devices at once would require the hiring of one or more security employees to set and maintain the controls across a variety of network security devices, as well as monitor the activities of the users. "CounterACT provides a mechanism to identify and monitor every device without having to staff up and offers a host of automated functions to keep our operations secure with little to no IT overhead," Webb says. "We save a lot of time and effort, since we only need to track down host or event exceptions. Automation in CounterACT saves resources because it keeps a history of each client, such as who is connected to where, when and what they are doing. Without CounterACT, gathering this information would involve the use of other tools, other networks and other services, not to mention having a detrimental effect on how fast we would be able to respond," Webb concludes.

The flexibility provided by CounterACT enables Marquette to apply various restrictions to support different policies. "We're an academic environment, so we don't have as much restriction on our students as a corporate network. We don't restrict people from scanning our network, or from poking around. This is a learning environment and we want to encourage our people to use the network. That being said, we keep an eye on endpoint defenses, malicious activity and unwanted behavior. For example, if a user or device goes from exploration to exploitation — that's when CounterACT takes instant remedial action," Webb says.

"To monitor all 14,000 clients connected to our wired and wireless student networks, including all of the respective devices accessing our network, would be a full-time job. CounterACT provides a mechanism to identify and monitor every device without having to staff up and offers a host of automated functions to keep our operations secure with little to no IT overhead."

Justin Webb
Security Analyst,
Marquette University

Unlike some organizations that can either allow full peer-to-peer usage, or restrict it entirely, CounterACT enables Marquette to monitor P2P usage and report on the number of clients using peer-to-peer. "P2P on a wireless and residential network can suck up a lot of bandwidth. We monitor to see how much is being used and use the information provided by CounterACT to maintain network services and to respond to DMCA copyright violations," Webb explains.

Challenge

Detect, monitor and Protect over 14,000 devices accessing the wired and wireless student networks of their campus.

Solution

Marquette determined that ForeScout CounterACT would centralize, and be able to enforce, its access security policies without requiring additional security staff or upgrading the network. CounterACT monitors all network access, offers autonomous operation with little intervention and provides a simple method to mitigate or remediate threats.

Results

» **Complete network visibility**
ForeScout made it easier for Marquette to gain complete visibility and handle threat prevention.

» **Time and cost savings**
The university has saved time and money. They have not had to hire additional security professionals, has had fewer security incidents and hasbeen able to fortify security controls.

» **Automated threat prevention**
CounterACT's built-in policies, policy customization and mitigation options have reduced manual remediation efforts as well as the number of notifications received from outside entities about the network being a threat.

» **Simpleto manage and detailed reporting**

Instead of going to multiplesources, Marquette administrators can pull information from one central place, such as a usage, security or asset configuration reports.

Automated threat prevention is a key feature in CounterACT

CounterACT is capable of monitoring device activity and generating a set of responses. If a device starts acting maliciously, such as propagating a virus, CounterACT can automatically identify the action and respond to eliminate the virus and identify those systems that are infected. In addition, CounterACT can detect when a device that's supposed to be a network printer begins to act as if it is a different type of device. CounterACT detects such unusual activity on a network, and can automatically stop the activity and isolate the offending device.

"At Marquette, the key policies we enforce are auto-remediation and threat prevention," Webb notes. "We have set thresholds that are actively monitored, and when a policy is not adhered to for a certain number of times, they are automatically moved to a segmented VLAN and directed to Marquette's ITS webpage. Here, users can download anti-malware and other software to self-remediate their computer. We also monitor ARP-spoofing on our wired network and other malicious activity. Alerts are generated when certain scanning and particular brute force actions are seen," Webb says.

"CounterACT's built-in policies, policy customization and mitigation options have allowed us to thwart network-based threats on the student network, which has reduced manual remediation efforts as well as the number of notifications we receive from outside entities about our network being a threat to others. This, obviously, means there are less internal threats, as well," Webb continues.

"Security and risk management are only as strong as an organization's ability to understand who is on their network and what their purposes are for being there. At that point, you can define policies — the tough part is determining how you can implement and maintain the security policies. CounterACT enables and automates this process — tracking who does what, when and where becomes much simpler," Webb says. "The ability to readily see all hosts, know their threat levels and whether they are compliant or malicious is invaluable. There has certainly been a cost savings, in that the University has not had to hire additional security professionals, has had fewer security incidents and has been able to fortify security controls."

CounterACT's flexibility enables other uses

CounterACT comes with a library of pre-written policies that can be easily modified to meet a user's specific needs. It also provides the flexibility to create new policies that may extend beyond traditional network access control.

For example, at Marquette, CounterACT has been set to monitor MAC addresses of devices connecting to the student network. When Marquette is notified of a stolen or lost computer, CounterACT is set to add an alert to notify if the 'lost' computer shows up on the student network.

Marquette, like other universities, must comply with the Higher Education Opportunity Act in terms of enforcing copyrights. CounterACT's functionality can assist with the response to copyright violations. "When we receive copyright infringement notifications, we use ForeScout to track the IP address that was used for the violation, and can tell what MAC address registered that IP. Working with other departments, we can then find that computer, whether or not it is still plugged in to the same port," Webb explains.

Simple to manage and exceptional support

Marquette is now using at least 10 CounterACT appliances. With the amount of information being generated by such an active network, you might think that management of all the devices would require multiple managers. It does not.

Management of the entire group of CounterACT devices is performed by a single ForeScout CounterACT Enterprise Manager appliance, which is administered by Webb. Nightly reports are generated, providing an 'overview of just what's going on in the network, handling security issues and only reporting glaring problems.' Webb notes that CounterACT makes it simple to get detailed reports, saving time for his and other departments. "Instead of going to multiple sources, you can pull the information you need from one central place — such as a usage, security or asset configuration report."

Technical support is a factor that is important to any organization. "ForeScout has been nothing but helpful, and has been willing to assist on various types of problems with the utmost patience. We wouldn't have continued to use them, for such a long period of time, if we weren't fully satisfied. Their two-day best practice seminar was useful and packed with practical details," adds Webb.

Webb summarizes the value of CounterACT, from ForeScout, to Marquette University in this way:

"ForeScout's advantage to our organization is that it allows us to focus on more 'pressing' security issues within the institution. ForeScout CounterACT fully integrates within our existing infrastructure to manage the student network security without much administrator intervention. This has actually allowed us to centrally develop and maintain policies and procedures to deal with network threats across network segments. I'm a busy security professional. NAC is important for the security posture of the University. As a crucial defense, it's up there with firewalls, VPNs, IPS and anti-virus. ForeScout just makes it easier for Marquette to gain complete visibility and handle threat prevention. Like other security professionals, I have broad responsibilities and have my hand in a lot of pots. I need to focus on tasks that are of the utmost importance to the University. Without CounterACT, I would have to remediate the various threats on the student network personally — and to have my friend ForeScout do that for me is pretty nifty."