Case Study

Hillsborough Community College

Forescout Scores High Marks for Visibility, Policy-Based Control and Third-Party Integration

INDUSTRY

Education

ENVIRONMENT

6,500 college-owned endpoints spread across five campuses with a heavy emphasis on wireless BYOD (another 10,000 simultaneous connections). The environment supports separate domains for employees and students.

CHALLENGE

- Gain visibility into BYOD systems accessing the college network
- Enforce device compliance and security hygiene policies
- Establish multiple authentication domains (students and employees)
- Accelerate response to emerging threats
- Automate endpoint compliance and remediation
- Reduce the need for system reimaging and downtime due to malware

> **We were totally blind as to what systems and devices were live on the network. My first task was to get some sort of visibility so that we could start to classify devices and begin tightening network access controls to secure the college."**
>
> **— Ken Compres, Senior Network Security and Integration Engineer/CSO, Hillsborough Community College**

Overview

Tampa Bay-based Hillsborough Community College (HCC) has grown into one of Florida's largest higher education institutions. Its 2,600 faculty and staff members serve more than 47,000 students annually at five campuses and three academic centers. The ever-increasing digital nature of education coupled with diverse populations of students, professors and support staff posed formidable cybersecurity challenges for HCC information security specialists who sought to offer users secure wired and wireless network access with minimal inconvenience.

Business Challenge

Bring Your Own Device (BYOD) is not just a way of life in college, it's a prerequisite for participating in higher education. The need for secure mobility was painfully obvious to Ken Compres, Hillsborough's senior network security and integration engineer/chief security officer, as he joined the college to bolster its IT security in 2012. Students needed connectivity and wanted to stay mobile, which is understandable given that the college's facilities span 850 acres and more than 64 buildings. At that point, students could go anywhere they wanted on the network and connect with any device. "We were totally blind as to what systems and devices were live on the network. My first task was to get some sort of visibility so that we could start to classify devices and begin tightening network access controls to secure the college," recalled Compres.

Compres and his team began evaluating network access and control solutions, embarking on an ambitious review process that included offerings from the five leading vendors at that time: Forescout Technologies, Cisco®, Blue Coat®, Aruba® and Pulse Secure®. According to Compres, "We had to be thorough. With a network access control solution, you don't want to put something on the network that would hinder the user experience, break peoples' computers or become overly intrusive to users. In addition, you need to fully understand how easily the technologies integrate into your existing environment."

Evaluation units were obtained and set up in a test lab for a side-by-side assessment that began during the summer of 2012 and concluded in January of the following year. Solutions were judged on the following criteria:

1) Agentless deployment capabilities
2) Ability to authenticate users against two separate domains, with and without LDAP*
3) Ease of management, ability to separate user environment
4) Scalability
5) Compatibility with devices and network infrastructure
6) Ability to perform Simple Message Service (SMS) messaging without incurring additional costs

SOLUTION

- Three Forescout CounterACT appliances
- CounterACT Enterprise Manager
- Forescout Extended Module for FireEye NX and EX

RESULTS

- Automated endpoint discovery, classification and remediation
- Orchestrated ATD/CounterACT integration via Extended Module for FireEye
- Accelerated incident response and containment to instantly stop CryptoLocker propagation
- Cut user downtime and IT tech reimaging/system restoration time from 300 hours per month to less than 18 hours
- Reduced data loss
- Minimized impact on users

> **We have a very large 802.1X implementation. Forescout Technical Support worked with us to customize the solution, allowing each CounterACT appliance to support more than 1,000 wireless access points. Forescout Tech Support has been fantastic!"**
>
> **— Ken Compres, Senior Network Security and Integration Engineer/CSO, Hillsborough Community College**

Why Forescout?

After extensive evaluation, the Hillsborough team chose Forescout CounterACT®. Several factors led to their decision. "Agentless visibility offers a huge advantage, and CounterACT was the only one that supported agentless operation," said Compres. "CounterACT, allowed us to gain the necessary insight into the network by integrating with existing technologies and components. In addition, a second finalist began crashing and preventing computers from communicating with anything else, so it was a no-brainer to go with Forescout," added Compres, who also appreciated the fact that CounterACT can send text messages without incurring additional costs of an SMS appliance.

After gaining in-depth visibility insights into who was on the network, the team began to carefully define the appropriate VLAN* segments for various connection scenarios and test rules to enforce policies. The rules would automate policy-based enforcement of student and employee network access based on their access privileges and endpoint compliance status, as well as limit access of agentless IoT devices. The IT team began a phased deployment of CounterACT, placing Forescout's SecureConnector on employee systems and using the dissolvable version of SecureConnector on student systems to allow agentless visibility and control.

Hillsborough's massive mixed environment includes more than 1,000 Aerohive® wireless access points, which initially placed added performance demands on the CounterACT appliances. Forescout Technical Support worked with Compres and his team to customize the solution using an innovative whitelisting technique, allowing each CounterACT appliance to support more than 1,000 wireless access points. This approach proved so successful that it ultimately became a supported 802.1X feature within CounterACT. "Forescout Tech Support has been fantastic! I look forward to collaborating with them on additional projects in the future as new needs arise," stated Compres.

Business Impact

According to Compres, CounterACT's impact on HCC's ROI is anything but academic. "Once we had CounterACT in place, our need to reimage infected computers dropped significantly—from 20 to 25 each month to just 1.5 systems. It takes a support tech five to six hours to reimage the system and restore the user's documents, files and applications. Moreover, the user is unproductive during that time, so you are literally wasting 12 hours per incident 20 to 25 times per month. That's a 240- to 300-hour productivity gain per month."

In addition, CounterACT does the following for Hillsborough Community College:

Agentless Visibility

CounterACT sees desktops, laptops, tablets, smartphones, sensors, network infrastructure, peripherals and wearable devices—without requiring existing management agents. That's a major advantage over Compres' early days at HCC. "Today we know what's on our network—including IoT devices such as printers, VoIP* phones and security cameras. CounterACT classifies the device and slips it onto the appropriate VLAN segment," said Compres.

> **With CounterACT, our need to reimage infected computers dropped from 20 to 25 each month to just 1.5. When you consider staff resources and user downtime, that's a 240- to 300-hour productivity gain each month."**
>
> **— Ken Compres, Senior Network Security and Integration Engineer/CSO, Hillsborough Community College**

Continuous Monitoring

Once users are allowed onto Hillsborough's network, CounterACT continuously monitors their devices. "Security doesn't end with compliance and remediation," insists Compres. "Everything must be monitored. Is a device scanning the network? Is it attempting to do some type of SNMP* trap or scan other devices on the network? We need these insights to not only protect our assets on the network, but the devices and personal data of our users."

Guest Access

CounterACT lets customers automate visitor enrollment while enforcing policy compliance. This is particularly important in college environments where students use multiple device types on any given day that vary wildly in terms of compliance levels.

When a user attempts to log on via one of the college's wireless access points, the access point queries CounterACT for 802.1X authentication. The college also allows guests to authenticate via Facebook, Google or directly through CounterACT, which sends a confirmation email or SMS text to the end user to confirm their identity.

Endpoint Remediation

CounterACT proactively identifies unsecured endpoints on the network and can automatically remedy the problem based on policies. When an unknown student device attempts to connect, CounterACT prompts the user to install the dissolvable version of SecureConnector. Within seconds, the system determines the device's patch level and the antivirus engine it's running, including the version level. "If they are compliant, we allow them to access the network resources. If not, we limit their access to Internet-only," explains Compres. Hillsborough performs automatic remediation of both managed systems and BYOD devices, granting appropriate access to resources upon system compliance.

FireEye Integration

Integration between CounterACT and FireEye® is another example of successful collaboration between Hillsborough and Forescout Technologies. Upon acquiring FireEye NX in 2012 and seeing the access control and management capabilities of CounterACT, Compres began wondering, "How can I leverage this information from FireEye to make CounterACT even smarter and automate threat response and remediation?" The team at Hillsborough began working to integrate the two solutions and eventually shared its use cases and preliminary results with Forescout. After several iterations of development and refinement, Forescout delivered an integration module to Compres for his team to beta test. "We immediately tested it in our environment and it worked great," said Compres. Today, the solution has evolved into the Forescout Extended Module for FireEye NX.

> **We evaluated the five leading access and control solutions. Forescout was the only one that supported agentless operation and provided the flexibility to integrate with other solutions."**
>
> **— Ken Compres, Senior Network Security and Integration Engineer/CSO, Hillsborough Community College**

Shortly thereafter, the value of the integration became readily apparent. Compres explains:

> "One of our systems became infected with CryptoLocker ransomware. As soon as it tried to communicate with the command and control server to begin propagating the ransomware across the network, FireEye saw this and immediately informed CounterACT, which blocked communications by dropping the infected system's port. CounterACT alerted me—it was amazing to watch the scenario unfold. Upon losing their connection, the user tried to connect to four different ports. CounterACT immediately blocked them all. This malware could have encrypted all of our data files accessible to this user—including network shares and documents—across our network. In the end, we had to only reimage one system."

In a more recent example, a Hillsborough user downloaded a malicious payload via email. "It was a zero-day payload that our antivirus software missed. Immediately, we started seeing a higher-than-normal volume of email being sent from that user's mailbox. The integration we have with Forescout and FireEye quickly determined the system was attempting malicious attacks against other network resources and allowed us to stop the system before it caused any damage." And without FireEye integration? As Compres explains, "That same attack hit a neighboring county and brought down a critical departmental email server for two days."

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

*VLAN (Virtual Local Area Network)
VoIP (Voice over Internet Protocol)
SNMP (Simple Network Management Protocol)
LDAP (Lightweight Directory Access Protocol)