One of Nation's Most "Unwired" Campuses Blocks Malware for Wireless Users

Trinity University uses Cisco Network Admission Control to deny network access to devices with malware and viruses.

EXECUTIVE SUMMARY

Trinity University

- Education
- San Antonio, Texas, United States

CHALLENGE

- Reduce malware and virus infections
- Enforce security policies for wireless users
- Strengthen security without impeding academic freedom

SOLUTION

- Deployed Cisco Network Admission Control (NAC) to identify and remediate machines with malware and vulnerabilities before they are admitted to the network

RESULTS

- Reduced malware infections
- Eliminated malware-related network performance issues
- Improved stability and reliability of computing environment

Challenge

Trinity University is one of the top private undergraduate institutions in the United States, ranking first among western U.S. universities by U.S. News & World Report for 15 consecutive years. Founded in 1869, the university today offers 37 majors on its 117-acre campus in San Antonio, Texas.

As with any large computing environment, protecting users and the Trinity University network from viruses and malware is a constant challenge. Unlike a private enterprise, however, the university's IT staff must try to secure an environment in which thousands of new users appear each year, bring their own laptops from home, and require unfettered access to the Internet.

"We have 2000 students arriving each year with their own personal computers, and we don't have a lot of control over them," says Douglas Cooper, systems administrator for Trinity University. "That opens us up to a variety of risks, including viruses, malware, spyware, and student machines being compromised."

As a result, university IT staff historically spent significant time and resources dealing with those issues.

"We were constantly running around cleaning machines and trying to isolate infected computers," recalls Cooper. "We could spend more than eight hours a week dealing with malware. It was slowing down the network significantly, which had a major effect on students and faculty."

To address the problem, the university deployed a NAC solution in 2005 aimed at helping ensure that all users complied with security policies, such as having up-to-date antivirus and operating system software. But the system was not a complete solution. First, there was no way to configure it to separate internal users, such as students and staff, from guest users. This was a big problem, especially during the summer, when the university hosted conferences with thousands of attendees. Providing Internet access meant exposing the university network to these users. The solution was also extremely inflexible.

"We had no internal control over the software, so if we wanted to create custom checks for specific policies, we had to ask the vendor to add that, and wait for them to provide it," says Cooper. "If we needed to make an urgent change, there was no way to do it."

The biggest problem with the previous NAC system, however, was that it did not support the wireless environment. Trinity was named one of the 10 "most unwired college campuses" in the United States by Intel Corp and supports as many as 900 wireless users at a time, with the figure growing each year. The lack of admission control for wireless users was a major hole in the university's network defenses.

"The wireless network is a shared resource for everyone on campus, and supports a broad range of applications," says Alfredo Zapata III, chief information technology officer, Trinity University. "It supports our voice over IP system, building controls, and door access systems. It is critical for us to maintain the stability of that network."

> "With all of the voice services, building systems, and other applications we now support on the network, it is critical that it remains stable, and Cisco NAC is a key component in making that happen. Today, our users don't even think about those kinds of disruptions, and that means we're doing our job."
>
> **—Alfredo Zapata III, Chief Information Technology Officer, Trinity University**

Solution

Trinity University needed a more flexible, comprehensive NAC solution. Since deploying the previous NAC system, the institution had become an end-to-end Cisco® environment, relying on Cisco for its wired, wireless, and security infrastructure. When the time came to consider a new NAC implementation, Cisco was a natural choice.

"Cisco NAC gave us a broad range of administrative tools that we did not have in the past," says Zapata. "There weren't any other products that could provide the user management and administrative flexibility of the Cisco solution. In addition, being basically an end-to-end Cisco environment, the ability to integrate NAC easily and maintain it as part of a single network and security solution was a big plus."

"We really liked the rules capabilities and the ability to set up different kinds of access for different users," adds Cooper. "The ability to classify users, log management, and integrate fully with our Windows environment was very nice."

Trinity University deployed Cisco NAC throughout its entire wireless environment, as well as for wired users in the institution's 15 dormitories. The solution is now being extended through the rest of the wired environment, including all academic and administrative facilities. Users download a software client onto their machines, which integrates with the university's user authentication system to check for security compliance as part of a single sign-on process. If users have not updated their antivirus software or patched their operating systems, for example, they are required to remediate those issues before they are granted access to the network. As a result, users with infected machines or known vulnerabilities now fix those problems before even entering the university network.

Cisco NAC gives Trinity University the flexibility to make changes to the security checks the system performs, and provides much more flexibility in managing users.

"We have created different roles for students, faculty, remote users, guest users, and other types of users," says Cooper. "Depending on the type of user, we perform a number of health checks on their system and software before admitting them to the network."

In addition to managing users, university IT staff also use Cisco NAC to help control the use of special devices on campus, such as gaming consoles.

"Before, we had to handle management of all of those devices manually," says Cooper. "The administrative overhead, especially at the beginning of the year when students first arrive on campus, was quite significant. Now, we are able to identify an Xbox or PlayStation that is connecting to the Internet, and pre-populate policies and roles for those devices automatically."

"We have also had situations where students built mini-servers in their dormitories, and tried to offer services from them, which we don't allow," says Zapata. "Cisco NAC helps us immediately identify that kind of activity and control it."

The Cisco NAC solution integrates with other Cisco security solutions in the Trinity University environment to create a comprehensive network defense system. Protecting the network edge, for example, is the Cisco Catalyst® 6500 Series Firewall Services Module, which embeds advanced firewall protection within the core network switch. To guard against malware and other Internet attacks, the university uses Cisco intrusion prevention system (IPS) solutions. And, to support secure remote access and virtual private network (VPN) connections, Trinity University uses the Cisco ASA 5500 Series Adaptive Security Appliance. Integrating all of these solutions into a single network defense command center is the Cisco Security Monitoring, Analysis, & Response System (MARS). With the combination of Cisco NAC, firewall, IPS, and security monitoring solutions, the Trinity University IT team can rapidly identify and respond to threats anywhere in the environment.

Results

Trinity University has now used Cisco NAC for nearly two years, and the results have been profound. Students can work and communicate on the network with confidence, knowing that the environment is protected, without intrusive restrictions on their ability to use the Internet. The network is no longer plagued by performance issues caused by malware infections. And, IT staff can focus on maintaining and enhancing the university's technology environment, instead of dealing with malware infections.

"From an administrative standpoint, we've seen dramatic improvement," says Cooper. "We still see the occasional infected machine, but with Cisco NAC in place, we spend far less time dealing with those types of issues."

"Cisco NAC is now protecting us from a variety of malicious activities, and keeping our core network safe from viruses and malware," says Zapata. "The ability to protect our wireless users is also a huge improvement, since we now have many users using wireless connectivity almost exclusively. We know that wireless users, along with all of the wired users in our dormitories, have up-to-date software, are running the proper antivirus, and are safe."

With Cisco NAC, Trinity University is able to maintain multiple levels of access for faculty and students, guests and internal users, wired or wireless connectivity, and to extend NAC protection across all of those scenarios. As a result, there is no longer any circumstance in which guest Internet users at conferences have access to the university network.

Having the ability to make changes to security policies and update the NAC software in house has also been a major improvement. That capability alone allows the Trinity University IT team to respond much more quickly to changing threats and head off many problems before they can affect the network and its users.

"We have the flexibility now to customize registry and health checks, and protect our environment in ways that we couldn't before," says Cooper. "When we transitioned from one antivirus product to another, for example, it was easy to incorporate those changes into the NAC software without inconveniencing our users."

Ultimately, Cisco NAC lets the IT team provide what students and faculty need most: a stable, reliable network infrastructure.

"Before we had Cisco NAC, we frequently had performance issues in the network because of malware that wasn't caught quickly enough," says Zapata. "With all of the voice services, building systems, and other applications we now support on the network, it is critical that it remains stable, and Cisco NAC is a key component in making that happen. Today, our users don't even think about those kinds of disruptions, and that means we're doing our job."

PRODUCT LIST

Routing and Switching

- Cisco Catalyst® 6500 Series Switch

Security and VPN

- Cisco NAC
- Cisco IPS 4200 Series Sensor
- Cisco Security Monitoring, Analysis, & Response System (MARS)
- Cisco Catalyst 6500 Series Firewall Services Module (FWSM)
- Cisco ASA 5500 Series Security Appliance

For More Information

To find out more about Cisco NAC, visit http://www.cisco.com/go/nac

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C36-554429-00 08/09