University Improves Network Security and IT Efficiency

John Carroll University uses Cisco security solutions to reduce information security risks on campus.

EXECUTIVE SUMMARY

John Carroll University

- Higher Education
- Cleveland, Ohio, United States
- 4000 users

CHALLENGE

- Balance need for academic openness with need to protect information and assets
- Reduce virus and worm outbreaks
- Improve efficiency of IT security personnel

SOLUTION

- Deployed Cisco security solutions to help ensure that all PCs connecting to the network comply with university security policies and cannot propagate viruses or worms.

RESULTS

- Eliminates virus and worm outbreaks on campus
- Prevents extremely costly manual efforts to remediate infected PCs
- Improves the manageability of the network and the efficiency of the IT staff

Challenge

John Carroll University, located in University Heights, Ohio, is a Jesuit Catholic university that inspires individuals to excel in learning, leadership, and service in the region and the world. The university has 3000 undergraduates and nearly 700 graduate students. *U.S. News & World Report's* 2009 college guide ranks John Carroll among the top 10 universities in the Midwest that grant master's degrees. Originally founded as St. Ignatius College in 1886, the University was renamed in 1923 to honor America's first Catholic bishop, John Carroll of Maryland. John Carroll is one of 28 Jesuit colleges and universities located in the United States.

The university is committed to providing a state-of-the-art learning environment for students, providing classrooms with a broad range of network-enabled multimedia technologies and a wireless network that blankets the campus. With ubiquitous technology, however, come significant information security risks.

"As a university, we have to support academic freedom, so we can't really lock down the staff or student PCs," says LaMarr Parker, associate director of network systems, John Carroll University. "Our challenge is to be open and flexible, yet as secure as possible."

The biggest challenge was securing the residence halls. The campus has 1000 resident rooms with at least two Ethernet ports each. This means there is the potential for more than 2000 foreign PCs inside the university network, none of which can be centrally controlled. Despite the best efforts of the John Carroll IT team, the situation often meant serious virus and worm outbreaks, some of which were extremely disruptive.

"Several years ago, we had a major virus outbreak that brought our internal network to its knees," says Parker. "We had to literally cut off all of the subnets the students were using just to restore connectivity to the Internet and campus resources. We had about 500 infected PCs on the network."

The attack crippled the day-to-day network operations of the university and prevented many students from going online for weeks. But the biggest problem was the operational effort required to clean all the infected PCs.

"We had to physically go to each room and check every PC, at that time, about 1200," says Parker. "We're a small university, and we have an IT department of maybe 30 people. We had the programmers out, the executive director out, work-study students out. We had every resource that the IT department could muster working 24 hours a day, trying to get the student PCs patched so they wouldn't bring down our network. It was devastating. It was six weeks before we felt as though our heads were above water."

The university had purchased a site license for an antivirus solution and the rights to provide every student on campus with antivirus software. But how could the university help ensure that students installed the software and kept it up to date? And how could they compel students to always patch and update their operating systems (OSs)?

Solution

After exploring the options, John Carroll University leaders found the ideal solution: Cisco® Network Admission Control (NAC). Cisco NAC examines every device attempting to log onto the campus network to verify that it complies with campus security policies, in particular, that it has up-to-date OS and antivirus software. For devices that don't, the Cisco NAC system provides access to all of the steps needed to bring the device up to date, and helps ensure that those steps are taken before granting access.

Unlike some "in-band" NAC solutions that require a separate appliance for all entry points into the network, the Cisco NAC solution works directly with the Cisco routers and switches deployed on campus, allowing a single Cisco NAC appliance to enforce policy compliance for all users and devices across the entire environment.

In addition to Cisco NAC, John Carroll University also uses Cisco firewall technology to protect the campus network from external threats. The university had previously used standalone firewall appliances, but when the campus switching infrastructure was upgraded, IT leaders chose to deploy a Cisco Catalyst® 6500 switch with integrated Cisco Firewall Services Module (FWSM) in the core network. The solution provides robust perimeter defense delivering 5 Gbps of throughput and supporting up to 100,000 connections per second and 1 million concurrent connections.

"The ability to implement firewall services that are integrated with our core network switch was a real benefit to us," says Parker. "The firewall module uses the backplane of the switch very effectively and gives us faster throughput. Having everything centralized in one device also helps us with control and management."

In addition to the FWSM, John Carroll University also deployed the Cisco Catalyst 6500 core switch with integrated Wireless Services Module (WiSM) to provide the security and management nerve center for the campuswide wireless network, and the Network Analysis Module (NAM) to provide enhanced network monitoring and visibility. John Carroll University also uses a Cisco VPN solution to provide secure remote connectivity, allowing off-site users to access the internal network just as securely as if they were on campus.

The partnership with Cisco for all aspects of the university's IT needs—security, wireless, routing and switching—is no accident. Over the years, the university's leaders have developed a great deal of confidence in Cisco solutions, and in the support and commitment, they receive from Cisco.

"The level of support that we receive from Cisco is crucial to our ability to support this campus," says Parker. "If we have an equipment malfunction, I can have a response within four hours. With other solutions, particularly with our previous firewall solution, there was no such thing as a four-hour response. If our firewall were to go down on a Saturday, we could be down until Tuesday. That would be completely unacceptable."

> "Our residence hall network has had zero virus or worm attacks since we deployed the Cisco NAC solution. Honestly, I don't know how we would survive without it."
>
> **— LaMarr Parker, Associate Director of Network Systems at John Carroll University**

Results

Cisco NAC has made a significant difference for John Carroll University, providing real and lasting benefits to students, staff, and the IT organization. While the open nature of the environment means that PCs still arrive on campus with viruses and worms, the attacks are not able to propagate across the network and affect the rest of the university.

“Our network has not been brought down once due to virus or worm infections, and our residence hall network has had zero virus or worm outbreaks since we deployed the Cisco NAC solution” says Parker. “Honestly, I don’t know how we would survive without it.”

Today, Cisco NAC inspects all PCs attempting to log onto the university network and dynamically recognizes whether OS and antivirus software is up to date, even if the students are using their own third-party software. The solution also recognizes other PC-based security services, such as integrated firewalls, and inspects those services as well. When a student PC needs a patch or update, the problem is remedied immediately, before the noncompliant PC can affect the rest of the environment.

The integrated firewall services provided by the Cisco Catalyst 6500 switch also make the campus safer, while reducing the administrative burden on IT staff and lowering utility costs.

“Being able to integrate so many security features, as well as wireless and management features into our core network switch has made management a lot easier,” says Parker. “We can closely monitor the network, recognize if there is a problem, and react before anything goes down. Our power consumption is also reduced now that we can support multiple services with a single switch, instead of having separate devices.”

The fact that John Carroll University now uses Cisco solutions for its entire wired, wireless, and security infrastructure has also paid dividends.

“All of the Cisco devices can continuously communicate with each other and function as a single system,” says Parker. “The ability to manage the entire environment remotely also makes a big difference. With the infrastructure we have in place now, we can troubleshoot any device from a single, centralized location.”

Ultimately, these security and management capabilities allow John Carroll University to provide a safer, more productive campus environment for students and staff. And, they help ensure that the university can allow students to take advantage of all that technology has to offer the academic experience, without sacrificing stability or security.

PRODUCT LIST

Routing and Switching

- Cisco Catalyst 6513 Switch with Sup720
- Cisco Catalyst 6513 Series Switch with FWSM, WiSM, and NAM

Security and VPN

- Cisco NAC
- Cisco FWSM for Cisco Catalyst 6500 Series Switch

Wireless

- Cisco Aironet® 1131 & 1242 Wireless Access Points
- Cisco WiSM for Cisco Catalyst 6500 Series Switch

Network Management

- Cisco NAM for Cisco Catalyst 6500 Series Switch

For More Information

To find out more about Cisco NAC and other Cisco security solutions, visit: http://www.cisco.com/go/security.

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

C36-548907-00 06/09