

University Virtually Eliminates Infections from Internal Users

Virginia Commonwealth University used Cisco security solutions to extend intelligent, centralized security capabilities.

EXECUTIVE SUMMARY
<p>VIRGINIA COMMONWEALTH UNIVERSITY</p> <ul style="list-style-type: none"> • Industry: Higher Education • Location: Richmond, Virginia, United States • Number of Users: 42,000
<p>BUSINESS CHALLENGE</p> <ul style="list-style-type: none"> • Balance need for academic openness with need to protect information and assets • Reduce attacks, infections, and malicious code • Improve efficiency of IT security personnel
<p>NETWORK SOLUTION</p> <ul style="list-style-type: none"> • Deployed Cisco security solutions that require all network endpoints to comply with university security policies, and allow staff to rapidly identify and respond to threats
<p>BUSINESS RESULTS</p> <ul style="list-style-type: none"> • Huge drop in infections on the network • Dramatic reduction in time and resources required to respond to security issues • Improved auditing and reporting capabilities streamline regulatory compliance

Business Challenge

Securing a network for any large organization is fraught with challenges. In a university environment, however, where the need for security must be balanced with the need for academic freedom, those challenges can be even more complex.

“Our security environment is very dynamic,” says Mark Willis, chief information officer for Virginia Commonwealth University (VCU), a Richmond, Virginia-based university with 32,000 students and 10,000 faculty and staff. “At a regulatory level, we have increasing requirements to secure our networks and data. That is almost an anathema to an academic environment which, by its nature, needs to be very open. We struggle to balance these needs and protect our assets from security risks.”

Compounding this challenge, the VCU network itself is far-flung and complex. The university stretches across two campuses, encompassing more than 140 buildings, 1800 network switches, more than 500 servers, and more than 42,000 users. Portions of the network also connect with a large regional medical campus, meaning that many network segments must comply with strict data security regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and industry requirements such as protection of copyrighted materials. In addition, several areas of the university deal with credit card transactions and must meet Payment Card Industry (PCI) requirements. Although the university had long employed strong perimeter security, mitigating the risk from internal threats was a constant challenge.

“Since the Cisco NAC solution has been in place, we have seen an approximately 90 percent drop in infections on the student resident network.”
 —Jesse Crim, Information Security Analyst, Virginia Commonwealth University

“You can secure a network from the outside with firewalls, but it is very difficult to secure it against someone bringing in a laptop and compromising it from within,” says Robert Neale, director of

computing and communications for VCU. “To truly protect our users, we need to know what devices are being connected to the network, that those devices have the latest security patches, and that they are not engaging in malicious activity.”

The problem was most acute in the university’s residence halls, where a constantly shifting population of students brought laptops, gaming systems, and other devices into the environment, many of which were infected.

“The university’s administrative network was constantly being attacked by the student network because of the massive amount of infections,” says Jesse Crim, information security analyst for VCU. “One infected PC would infect an entire floor within minutes. It had become a major issue, and required a lot of time from our IT staff to constantly go out and clean computers.”

In addition, VCU security personnel also struggled to control illegal file-sharing on campus. Each time the university received notification of illegal activity, technicians had to be dispatched to physically track down and shut off switch ports.

Network Solution

Given the scope of the challenges that VCU faced, the university needed more than just a better firewall or antivirus system. It needed an overarching, comprehensive new approach to security that could provide much more visibility into and control over the network. After considering several options, VCU’s IT leaders chose to revamp the security infrastructure with Cisco® security solutions. The university already used Cisco routers and switches, and VCU leaders believed that using Cisco security solutions would allow them to manage the entire environment as a single system.

“Most of the vendors we looked at specialized in just one or two areas,” says Crim. “We wanted a solution that could encompass everything from our routers and switches to network access control to network monitoring, and extend across our entire environment. Cisco had the solutions to bring everything together.”

VCU deployed a variety of Cisco security solutions, including the Cisco Network Admission Control (NAC) Appliance, Cisco firewall and VPN appliances, Cisco Intrusion Prevention System (IPS) solutions, and the Cisco Monitoring, Analysis and Response System (MARS) to serve as the security nerve center for the entire infrastructure. Together, these solutions create the foundation for a Self-Defending Network—a network that can dynamically identify and respond to threats in real time, and continually adapt to a changing environment.

Controlling Network Access

One of the key components of VCU’s revamped security is the Cisco NAC Appliance, which enforces security compliance on all endpoints connecting to the network and helps ensure that they comply with institutional security policies. VCU deployed the NAC solution inline, allowing it to not only alert the security team when an endpoint is noncompliant (for example, if a laptop has out-of-date antivirus or operating system [OS] software) but to actually block that machine from connecting until the issue is resolved.

“Other vendors offer NAC solutions, but the difference with Cisco is the level of integration we could achieve with our other security components,” says Neale. “We know that our NAC solution will communicate with the Cisco Security MARS solution. We know it will work with the switches and security appliances we have. And, we know that we have a partner in Cisco that will stand behind

the solution and continually improve it.”

With Cisco NAC Appliance, VCU is also able to track user and device access histories. The data helps VCU to identify copyright violators and resolve the Recording Industry Association of America (RIAA) reports.

Protecting Against Malicious Threats

To protect critical university assets from infection from machines in residence halls, PC labs, and other public networks, VCU uses the advanced virtual LAN (VLAN) and firewall capabilities of Cisco Catalyst® 6500 Series switches with Cisco Firewall Services Modules. By implementing VLANs at the switch port level, VCU can apply different sets of security policies to different segments of the network, depending on the security profile and requirements of each segment’s users.

To further protect university servers containing sensitive information, VCU uses Cisco IPS 4200 Series Sensors. The sophisticated IPS solutions accurately identify, classify, and stop malicious activity, including worms, directed attacks, reconnaissance, and application abuse.

“We chose the Cisco IPS solution for its rich feature set, its ability to prevent unwanted traffic, and its integration with the rest of the Cisco security solutions,” says Crim. “By deploying the IPS sensors inline, we have much more insight into the types of attacks we’re facing and the ability to block any traffic that is excessive or abusive.”

Versatile Remote Connectivity

VCU uses Cisco ASA 5500 Series Adaptive Security Appliances to handle advanced firewalling and VPN functions. The Cisco ASA appliances can manage thousands of simultaneous remote connections and support both traditional IP Security (IPSec) and Web-based Secure Sockets Layer (SSL) VPN connectivity.

“VCU has a large, heterogeneous network consisting of Mac, Linux, and Windows users, and we wanted a VPN solution that could serve all of them,” says Neale. “The SSL VPN capabilities provide a universal VPN deployment model. We can use it for wireless connectivity, remote access, and even between subnets in our network to protect sensitive information. With the ability to integrate the VPN solution with NAC, we can create policies specifically for remote or wireless users, provide better networking support, and more quickly react to security incidents.”

Monitoring the Environment

To tie all of these security solutions together and correlate security information across the environment, VCU deployed Cisco Security MARS. Cisco Security MARS aggregates and synthesizes the massive amounts of security data typically generated in a large academic network, and uses sophisticated event correlation and validation intelligence to help the security team appropriately identify and respond to threats. The solution provides intuitive topology maps to track attacks in real time, integrates with the Cisco switches and IPS sensors to block attacks in progress, and provides comprehensive reporting to help VCU more easily comply with state and federal regulatory requirements.

“We needed a solution that would integrate our NAC system with the rest of our security services,” says Neale. “With Cisco Security MARS, we can look at suspicious activity across our entire network, correlate that with information coming in from the NAC appliances and other sources, and identify anything that might indicate a problem.”

Business Results

Today, the VCU network is much safer for all users, and the university's assets and information are better protected than ever before. The Cisco NAC solution in particular has provided the VCU security team with unprecedented control over network endpoints. The solution helps ensure that all machines attempting to access the network comply with university security policies, and blocks those that do not until they update antivirus or OS software, or take other remediation steps. The result has been a dramatic improvement in the overall security of the VCU environment. "Since the Cisco NAC solution has been in place, we have seen an approximately 90 percent drop in infections on the network," says Crim.

"The number of complaints we receive about security violations in the residence halls has dropped dramatically, and today there are virtually no attacks originating there," adds Neale. "As a result, we are providing the students with much better service. With no malicious traffic on the network, student Internet and network access is faster, and even their PCs are running better."

Working in concert with Cisco Security MARS and the Cisco routers and switches, the Cisco NAC solution associates every endpoint on the network with a specific user ID and IP address. This allows security staff to troubleshoot security issues much more quickly and to continually track individual machines, even if an attacker attempts to move from one segment of the network to another. These capabilities not only improve the security of the environment, they boost the operational efficiency of the security team.

"In the past, if we found an abnormality or an instance of illegal file-sharing, we had to investigate by tracking the IP address to a specific router and switch, and then physically going to that location to unplug that machine," says Willis. "That required an enormous amount of time and resources. With the Cisco security solutions, we can quickly identify a problem machine and remove it from the network remotely. That recovered staff time has more than paid for the solution already."

The ability to view and manage the entire environment as a single system also makes it easier for the IT security team to comply with security regulations and audits. "Cisco Security MARS allows us to correlate security data from the NAC appliance, the IPS sensors, and all of our network routers and switches across the environment to generate reports," says Crim.

Ultimately, the Cisco NAC and other security solutions have provided VCU with greater visibility into the university network than ever before, and more powerful tools to protect users and information. "Today, we have a global view of the network," says Crim. "Our security is centralized, integrated, and universal. That's what Cisco brings to the table."

Next Steps

In the coming months, VCU IT leaders plan to integrate the networks serving the medical schools and the regional medical center into the main university network. The executive team believes that the robust security capabilities now in place will allow them to meet even the most stringent healthcare security and regulatory requirements.

VCU is also considering deploying Cisco Security Agent on all university servers. The intelligent, host-based intrusion prevention solution will monitor all servers for malicious operating system activity and block both known and previously unknown "day zero" threats. VCU is also currently piloting the Cisco Security Manager, a security information tool that will centralize syslog and netflow data from across environment, and further enhance the university's management, monitoring, and reporting capabilities.

For More Information

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

PRODUCT LIST

Security and VPN

- Cisco NAC Appliances
- Cisco IPS 4200 Series Sensors
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Catalyst 6500 Series Switches with Firewall Services Modules
- Cisco Security MARS



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.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)