Major Medical Institution Safeguards Open Academic Network

Baylor College of Medicine relies on Cisco security solutions to manage access, guard against malware, and improve IT efficiency.

EXECUTIVE SUMMARY

Baylor College of Medicine

- Higher Education/Healthcare
- Houston, TX, United States
- 10,000

CHALLENGE

- Protect against malware in open academic environment
- Reduce manual administration requirements and costs
- Improve efficiency of remote access administration

SOLUTION

- Deployed Cisco network security solutions to protect and control computing environment
- Offered enhanced SSL VPN to mobile users

RESULTS

- Further mitigates risks of major virus and worm outbreaks
- Proactively simplifies complex compliance and change management efforts
- Makes remote access provisioning fast and easy

Challenge

Baylor College of Medicine (BCM) is a premier academic health science center with a diverse mission: to educate the next generation of clinicians, conduct groundbreaking research, and provide the best in patient care. Located within the world-renowned Texas Medical Center campus, the institution collaborates with eight teaching hospitals and has more than US$300 million in research funding.

Supporting this sweeping mission demands a significant technology infrastructure. The College's network connects 43 buildings in and around the Texas Medical Center and approximately 1300 network devices.

"Hundreds of applications rely on Baylor's network," says Jeff Early, director of network services for Baylor College of Medicine. "That includes our primary business applications, clinical systems, academic systems, radiological imaging, and even systems supporting medical devices for patients."

With so much depending on the network, the Baylor College of Medicine IT department must remain constantly vigilant against security threats.

"A network security event is always a concern," says Early. "We especially need to protect patient data, financial data, and password data. Our concerns are not just simply to avoid the potential financial ramifications of a major security incident; we are equally committed to protecting the reputation of the institution."

The key to protecting any network on this scale is securing its endpoints (i.e., customer PCs), which can be a source of malware, especially in an environment where students and guests may use their own personal (non-corporate) laptops.

"Several years ago, the risk of an outbreak affecting multiple systems was greater than today," says Early. "If Baylor experienced such an outbreak, it could disrupt productivity throughout the organization over a period of time."

Guarding against malware, however, is far from straightforward in an academic setting where users demand an open and unfettered computing environment.

"One of the drawbacks of a free and open educational network is that you may see problems only after the fact," says Mike Dunigan, IT security analyst for Baylor. "We had systems in place to block certain types of malware and exploits, but we often had to be reactive rather than preemptive."

The other major responsibility for the IT team is maintaining regulatory compliance. With clinical and financial information constantly traversing the network, the institution has the requirement to enforce compliance standards, particularly with the Health Insurance Portability and Accountability Act (HIPAA). Reviewing audit logs, managing passwords, and verifying computers' antivirus and patch compliance were based on manual processes that required significant time and effort. In addition, the College was seeking to streamline the management of remote access network connections for more than 2000 remote customers each month.

> "Our endpoint protection strategy, including Cisco NAC and several other tools, allows us to tightly control outbreaks. We have not had any major incidents since having these solutions in place. Moreover, the risk of a major incident has been significantly reduced."
>
> —Jeff Early, Director of Network Services, Baylor College of Medicine

Solution

With so many diverse security requirements and areas to protect, Baylor College of Medicine needed a highly versatile, manageable network security defense system. The college turned to Cisco. Baylor has long used an end-to-end Cisco network. Over the past several years, the IT team has employed more and more Cisco technologies for network security, which include solutions for endpoint protection, remote access connectivity, security administration, and more.

Controlling Endpoints

Given the open environment, numerous Internet connections, and frequent guests that characterize the Baylor network, the IT team cannot fully lock down network endpoints. To protect the environment, BCM deployed a multilayered authentication and network admission control (NAC) solution. One key component is Cisco® NAC, which protects several thousand ports and authenticates 6000 users.

"We have a number of controls in place to protect the computing environment against malware and other threats," says Stephen Ford, Baylor College of Medicine's director of IT security and compliance. "Cisco NAC is an important tool within these sets of controls to protect the network and enforce security policy and best practices."

"We use Cisco NAC to secure ports in offices, classrooms, conference rooms, and other open areas," says Stuart Bailey, network engineer. "We can authenticate users and ensure that their antivirus software is up to date. We also assess whether they are current on the latest Windows patches."

Baylor College of Medicine also uses Cisco Security Monitoring, Analysis, & Response System (MARS) to aggregate logs and security event information from devices throughout the computing environment. The solution helps to rapidly and proactively identify and respond to any potential network security event.

"Cisco MARS collects and correlates event and log data from a number of our network and security devices," says Ford. "As a result, team members can now quickly, accurately, and efficiently act on network security events such as virus infections, spam runs, and other network events."

Simplifying Administration

To help the IT team manage diverse administrative and compliance requirements, Baylor College of Medicine uses CiscoWorks Network Compliance Manager (NCM), which streamlines many previously manual tasks. The management tool records configuration and software changes throughout the environment and provides a central interface to track compliance with regulatory and institutional policies.

"We use NCM to track all our device inventories and configurations," says Meena Chockalingam, network architect. "We can perform compliance checks on every device in the network and identify and correct any issues. The tool also allows us to make password changes for all devices from a central interface. These capabilities reduce a huge amount of workload."

"NCM also plays a vital role in administrative audits," says Dunigan. "It gives us a clear record of who had access to which device, any changes they made, and when they made them."

Remote Connectivity

To provide secure VPN connectivity for more than 2000 remote users, Baylor College of Medicine uses the Cisco Adaptive Security Appliance (ASA) 5500 Series. The solution allows the IT department to continue supporting previous-generation IP Security (IPSec) connectivity, while transitioning to Cisco AnyConnect, a Secure Sockets Layer (SSL)-based VPN client. Using the Cisco AnyConnect technology provides a better user experience while reducing IT support costs associated with managing client software.

"When we relied on IPSec, we would have to install a client on every user's machine and manage all of those clients," says Chockalingam. "With Cisco AnyConnect, our users just log in with their web browsers, and the client gets installed and updated automatically."

Results

Today, Baylor College of Medicine is successfully training the clinical leaders of tomorrow and providing students with the open academic environment they need, while protecting sensitive information and assets. The Cisco security solutions have provided the College's IT team with the visibility and control that it needs to support this critical mission.

"Our endpoint protection strategy, including Cisco NAC and several other tools, allows us to tightly control outbreaks," says Early. "We have not had any major incidents since having these solutions in place.

"We've been able to do a very good job keeping unauthorized devices off the network," says Bailey. "We have a level of comfort as an IT department that comes from having a much better idea of what's going on in our environment."

The Cisco network defenses also provide the Baylor IT team with powerful capabilities to rapidly identify and respond to potential problems.

"The Cisco tools give us exceptional visibility into the network," says Jason Glim, manager of Network Services. "We are able to identify events as they occur and respond to them quickly, whether it's a security event, a performance issue, or just network availability. They provide a great deal of value."

The Cisco network administration tools have also made a difference, eliminating much of the time and effort that the team used to devote to manual processes.

"The Cisco Network Compliance Manager is a very powerful, easy-to-understand tool," says Bailey. "It allows anyone on our network team to roll out a password change, for example, without having any scripting background. It makes password change management a breeze."

The Cisco ASA platforms are also helping to improve the team's efficiency, greatly reducing the administrative effort required to support VPN connectivity.

"With the Cisco ASA platform and the AnyConnect client, distributing clients is much easier," says Chockalingam. "We don't have to provide users with a client at all; instead, we just point their browsers to the right location to download it. It's much faster. When we have updates, they are automatically downloaded and pushed to the client, without our team having to redistribute a new package. Our end users don't even realize anything has changed."

Ultimately, Cisco has proven to be an important security partner for Baylor College of Medicine. The institution's leaders plan to continue working with Cisco to address the unique security requirements of this demanding environment.

PRODUCT LIST

Routing and Switching

- Cisco 7600 Series Router
- Cisco 3700 Series Multiservice Access Router
- Cisco Catalyst® 4500 Series Switch
- Cisco Catalyst 6500 Series Switch

Security and VPN

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

Wireless

- Cisco Aironet® Wireless Access Points
- Cisco Wireless LAN Services Module (WLSM) for Cisco Catalyst 6500 Series
- CiscoWorks Wireless LAN Solution Engine (WLSE)

Network Management

- CiscoWorks Network Compliance Manager (NCM)
- CiscoWorks LAN Management Solution (LMS)

"Along with our defense-in-depth approach, Cisco has brought very powerful tools to the table to help us in our security and compliance efforts," says Ford. "Cisco has significant offerings that help us complete our security toolbox, and we plan on expanding those technologies to continue to keep our computing environment safe."

Next Steps

In the coming months, Baylor IT leaders plan to continue expanding the Cisco NAC deployment, including bringing additional buildings online. In addition, the College also plans to increase its use of the Cisco ASA 5500 Series, including deploying a Cisco ASA platform at the institution's disaster recovery facility. In the event of a workforce interruption, such as an epidemic, that prevents users from coming to the campus, the VPN infrastructure will be able to support up to 3000 concurrent VPN customers.

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 C36-580714-00 01/10