UNC Pembroke Increases Efficiency in its SOC

How a fast-growing university protects its students and staff with an integrated platform approach

UNC Pembroke's mission to change lives

UNC Pembroke is located in Pembroke, North Carolina, and it is one of 17 campuses in the University of North Carolina System. The 281-acre UNC Pembroke campus consists of more than 49 buildings, and also offers online and distance education. Established in 1887 as a Native American college before joining the UNC school system in the 1970s, the university enrolls nearly 7,700 students and has a faculty of 300 and an overall campus staff of more than 550. UNC Pembroke's mission is to change lives through education by providing its diverse student base the learning opportunities to succeed. The university also supports the community through sponsorships of programs such as Girls Who Code and the Wounded Warrior Project.

As a diverse institution with students, faculty, staff, and visitors from all over the world, the university is a prime target for cybersecurity attacks. The types of data that need to be protected include not only Personally Identifiable Information (PII), but also Payment Card Industry (PCI) data through the campus retail and dining establishments, Protected Health Information (PHI) due to the health clinics' HIPAA compliance, and intellectual property from faculty and student research.

"If any of that sensitive data were to be exposed, there would be huge consequences for the university," says Chief Information Security Officer Don Bryant. "If we were to get shut down with ransomware or have a data exposure, it would take a toll on the university, not only financially, but also our reputation."

Executive summary

Customer name
The University of North Carolina at Pembroke (UNC Pembroke)

Industry
Higher education

Location
Pembroke, North Carolina

Number of students and staff
7,700 students, 298 faculty, 550+ staff

Challenge

- Wide attack surface due to faculty, student, visitor, mobile, and Internet of Things (IoT) devices on the network
- Variety of data to protect, such as Personally Identifiable Information (PII), Payment Card Industry (PCI) data, Protected Health Information (PHI), research, and intellectual property
- Lack of visibility of potential threats across the network

Solution

- Security Enterprise Agreement
  - Cisco® Threat Response
  - Cisco Next-Generation Firewall
  - Cisco Umbrella® (secure Internet gateway)
  - Cisco Stealthwatch® (network traffic analysis)
  - Cisco Advanced Malware Protection (AMP) for Endpoints
  - Cisco Cloud Email Security
  - Cisco Cloudlock (API-based Software as a Service [SaaS] access)
  - Duo (multifactor authentication)
  - Cisco Email Security
  - Cisco Threat Grid

Results

- 60–70% reduction in help desk calls due to malicious files or compromised accounts
- Two-thirds decrease in the number of phishing emails and compromised accounts
- An integrated security platform approach providing unified visibility, streamlined workflows, and improved efficiency

"Having all of Cisco's tools so well integrated really gives us defense-in-depth and layered protection."

Don Bryant
CISO, The University of North Carolina at Pembroke

In search of better visibility for faster threat defense

Goals:

- Gain better visibility across the network
- Automate and integrate security solutions
- Ultimately: build a campus culture of security

When Bryant became UNC Pembroke's Chief Information Security Officer (CISO) a few years ago, he took on the challenge of building out the nascent cybersecurity program for a fast-growing educational institution. As an example of the rapid growth, the number of devices connected to the school network grew from 44,000 to over 60,000 in just this past year.

Bryant, previously with U.S. Special Operations Command in nearby Fort Bragg, had participated in UNC Pembroke's Wounded Warrior Fellowship Program and then accepted the CISO position upon retiring from the U.S. Army. He is also the chair of the IT Security Council for the entire UNC school system.

When he first joined UNC Pembroke, the university had a basic security setup with firewalls and antivirus on the endpoints. Needless to say, Bryant and his small team had some work to do.

"It's a real security challenge working with professors and students who come from all over the world. They've got all these BYOD [Bring Your Own Device] and IoT devices that can be infected," Bryant says.

Due to the growing threat landscape that resulted in a plethora of threat data coming in through multiple security tools, it was imperative for Bryant and his lean team to understand what might be traversing through the university network. They needed to:

- Gain unified visibility, from one central location, into threats hitting the network
- Focus their time and efforts on the high-priority threats that could severely impact the organization
- Simplify security through the integration of their solutions

"As a small security team, we really needed to get to automation and integration quickly," Bryant says.

Choosing the right partner in Cisco Security

Bryant evaluated several options, but Cisco Security had the most diverse portfolio and the broadest, most integrated platform. This platform connects the integrated portfolio and third-party products for a simpler, more consistent experience that unifies visibility, enables automation, and strengthens the security posture.

With Cisco's Security Enterprise Agreement, Bryant has what he calls "an all-you-can-eat security buffet." His team rolled out Cisco Firepower® Intrusion Detection System/Intrusion Prevention System (IDS/IPS), Stealthwatch, AMP for Endpoints, AMP for Networks, and Umbrella, among others. The backbone of this comprehensive platform is Cisco Talos, one of the world's largest threat intelligence organizations.

This platform gave Bryant broad visibility into threats on his network, and next he needed to prioritize which threats to focus on. Bryant implemented Cisco Threat Response, which integrates and aggregates threat data from Cisco and third-party security tools to simplify and accelerate threat investigations and remediation. Threat Response is included at no additional cost with most Cisco Security licenses.

With Threat Response, Bryant has the visibility in a single console to respond, mitigate, and remediate quickly, while also being able to easily pivot to the other security tools—such as Umbrella or Firepower—when needed.

"Being able to have a single pane of glass so we can see where things are traversing and what devices are infected by severity allows us to prioritize our threats and get to the most important ones first. That just frees up a lot of our time to focus on the high-severity threats," he says.

Bryant also notes that the integration of all the solutions was seamless.

"Cisco Threat Response worked right out of the gate, really plug-and-play. It didn't require a bunch of APIs or scripting," he says.

For Bryant, taking a holistic approach with Cisco's security platform means comprehensive protection for students, staff, and visitors of UNC Pembroke. He credits the support of Cisco's account team and NWN implementation team with helping get it all up and running quickly, as well as the Cisco engineering team for ongoing updates.

"I really have a lot of trust and faith in the tools and our partnership," Bryant says. "It's really paid big dividends for us."

Changing the security culture

Implementing Cisco Security has enabled UNC Pembroke to change the security culture, says Kindra Locklear, IT project portfolio manager. Where previously security issues were considered an IT concern, now the business units are proactive rather than reactive.

"Security is now part of our everyday processes that we have on campus," she says.

Further enhancing the culture of security, UNC Pembroke also participates in the Cisco Cyber Defense Clinic, which educates and engages students, interns, and staff through hands-on interaction with cybersecurity technologies.

As for Bryant and his team, Cisco Security has made their Security Operations Center (SOC) more efficient.

"Having a more holistic security platform has really helped us make more progress toward our end goal in a short amount of time," he says.

Results included:

- Instant visibility with Threat Response, and defense-in-depth with layered protection
- More efficient breach defense and faster investigations and incident response
- A decrease in the number of compromised email accounts, from an average of 10–15 per day down to fewer than five
- A 60–70% reduction in calls to the help desk due to malicious files, phishing emails, or compromised accounts

"Since implementing all of our Cisco security tools, up until now, we haven't had any serious incidents or compromises," Bryant says. "We feel very well protected."

For more information

For more information on Cisco Threat Response, visit www.cisco.com/go/threatresponse.

Security built for the future

The security approach UNC Pembroke adopted with Cisco's help positions the university for better protecting its future. Bryant says he feels confident that threats will be remediated quickly and that the students and staff are protected from threats.

One of the factors contributing to that confidence is the ongoing relationship with Cisco and the support the university receives from the Cisco Security team.

"It's more than just a vendor relationship—it is a true partnership," Locklear says. "Cisco is seen as our bridge to making hope possible for our campus. They're breaking down barriers for us."

C36-743465-00 02/20