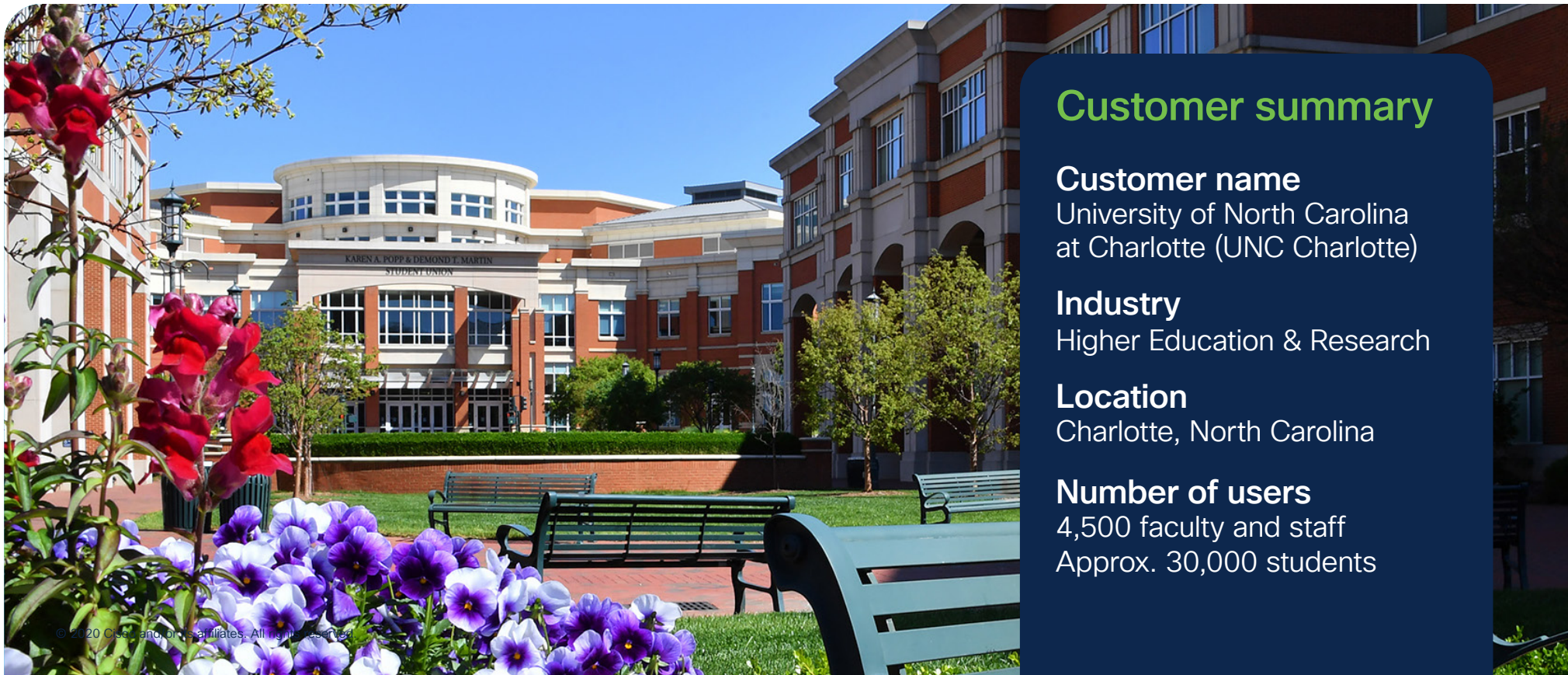
University of North Carolina at Charlotte

Best practices for advancing security maturity in Higher Education

How one university simplified its security experience with a single built-in, cloud-native platform.



Customer summary

Customer name
University of North Carolina at Charlotte (UNC Charlotte)

Industry
Higher Education & Research

Location
Charlotte, North Carolina

Number of users
4,500 faculty and staff
Approx. 30,000 students

The challenges

- Increase security control through greater accountability methods
- Implement seamless and flexible security that was invisible to users
- Strengthen operations and service delivery
- Create a more efficient and agile IT environment

Big campus, big data

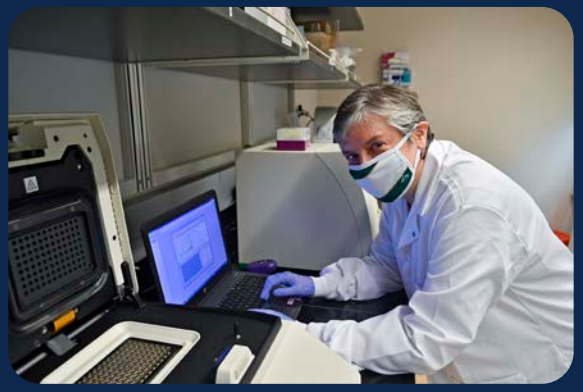
For the University of North Carolina at Charlotte (UNC Charlotte), security is at the forefront of everything they do. As the state's leading urban research university, it is home to a variety of internationally competitive programs that focus on advanced discovery and application. So keeping a large amount of unique data, and access to it, secure is critical to their success

UNC Charlotte serves a large and varied population of users. It's the largest regional urban campus in the state, with 8 colleges, almost 30,000 students, and 4500 faculty and staff. Together they power 236 undergraduate, 140+ graduate, and 24 doctoral programs.

Intelligent security for intelligent users

As Vice Chancellor for OneIT and the CIO at UNC Charlotte, Dr. Mike Carlin helps guide their security strategy. This included the roll-out of a university-wide blended IT model in 2020 that was the outgrowth of a state audit 3 years earlier. The audit had identified various risks within their existing IT model and spurred Dr. Carlin and his team to undertake a deeper assessment of their IT approach.

Their findings guided them to seek increased security control through greater accountability to the CIO. In addition, he was charged by the university's governing body to find a way to implement robust security in a manner that let users continue their daily workflows without interruption or awareness of the processes running behind the scenes. And do so in a seamless and flexible manner.



As their response evolved, Dr. Carlin and his team developed a cloud first initiative and sustainable infrastructure plan for the large campus while also leveraging open source technologies. They were also inspired to seek "intelligent security" built around integrated and automated solutions. With help from Cisco, UNC Charlotte addressed these key challenges, and more.

"Cisco SecureX tools allow us to be proactive rather than reactive. This puts UNC Charlotte ahead of the game, because if you're always reactive you never gain traction."

Dr. Mike Carlin
Vice Chancellor for OneIT / CIO University of North Carolina at Charlotte

Additional security challenges as a larger institution

With nearly 35,000 users accessing their network throughout the day, Dr. Carlin and his team faced several security issues in addition to those raised by the state audit and mandated by university leadership. Institutions of higher education face a constant challenge: manage costs downward where possible and ensure secure access to the network by students, faculty, staff, and visitors regardless of their location or device type.

As a major research university, UNC Charlotte's IT team was mandated with protecting a large amount of raw data, intellectual property and potentially sensitive personal data. Growth in users adds to this stress on a network and its security, and is a constant issue for larger universities. It requires a more strategic understanding of scaling with some level of future-proofing that can handle unexpected growth spurts.

With the unexpected appearance of COVID-19, the need to transition users to remote use introduced the issue of scalability (including speed of and costs associated with licensing and deployment). The pandemic also resulted in some students and staff relying upon shared devices. As a result, malicious threats increased.

The threats that keep UNC Charlotte awake at night

For Jesse Beauman, the Assistant Vice Chancellor for Enterprise Infrastructure at UNC Charlotte, malicious threats are what keeps him up at night. He is responsible for the university's infrastructure including servers, storage, and security. He sees the biggest threats to their campus coming from email attachments and malware, including those unknowingly embedded in online ads and banners.

It's a tried and true approach that has continued to evolve over the years and can enable a single click by the user with the power to upend an entire security system. That's led Mr. Beauman and his team to seek upfront security and any opportunity to educate their users to think first rather than click first on emails links and other potential traps.

The value of a collaborative long-term partner

From growing user numbers and the need to keep research data secure, to meeting mandates and overcoming the unexpected, the UNC Charlotte IT team faced significant challenges. So they turned to their long-time collaborative partner in IT, Cisco, for expert guidance through an honest and open dialogue based on mutual trust.

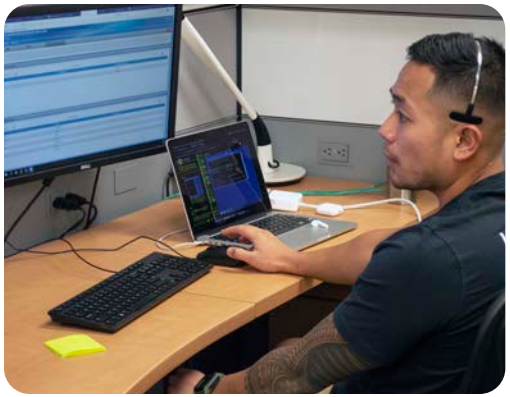
Together, they began to develop a strategy that would increase control of their security protocols while embedding greater accountability. They would also seek to strengthen their operations and service delivery while a creating a more agile and efficient IT environment. Plus, the partnership would develop ways to implement a seamless and flexible threat-centric security model that would provide deeper visibility and protection for the growing number of end-devices connected to their network. But with caveat: it would have to be invisible to users, allowing their workflows to continue uninterrupted.

"The bad guys are now moving at the speed of the machine, so our automation principle is to move at that same speed. Cisco solutions allow us to do so."

Jesse Beauman, M.S.
Assistant Vice Chancellor for Enterprise Infrastructure, UNC Charlotte

The Solution: SecureX

- Secure Network Analytics (learn more)
- Umbrella (learn more)
- Secure Endpoint (learn more)
- Secure Firewall (learn more)
- Secure Workload (learn more)
- Identity Services Engine (learn more)



A unified view for a rapid and targeted response

By collaborating with Cisco, a trusted leader in IT for higher education and research, UNC Charlotte has unified their security solutions into an integrated platform, providing one view into their security environment – across the network, users and endpoints, cloud edge, and applications – and greater efficiency with automated workflows. By deploying Cisco SecureX, UNC Charlotte enabled deeper visibility into their network and all end-devices connected to it, rapidly increasing their incident response from days to just minutes.

SecureX connects your Cisco Secure portfolio and your infrastructure by uniting industry-leading solutions like Secure Network Analytics, Umbrella, Secure Endpoint, Secure Workload, and Secure Firewall into a seamless threat-centric security approach. This enables targeted and highly responsive proactive security for users without interrupting their workflows. SecureX empowers UNC Charlotte's various security solutions to share threat information with each other in real-time, eliminating gaps in threat detection and response times. Plus, it integrates with the university's email system, shielding the largest target for potential breaches.

"It's great to integrate that much information into one location. SecureX really reduced our response time and moved us from a reactive response posture to a proactive security posture."

Jesse Beauman, M.S.
Assistant Vice Chancellor for Enterprise Infrastructure, UNC Charlotte

Cisco SecureX: Protecting UNC Charlotte

A simplified security experience

UNC Charlotte faced numerous security challenges that required a unified and targeted response. One that would simplify their workload while providing deeper visibility, and work with their users' workflows, instead of bogging them down. They turned to Cisco SecureX as the solution:

- Simplicity – Integrate your technology together, Cisco or otherwise, for true turnkey interoperability – not only a connected backend architecture but also a consistent frontend experience.
- Visibility – A customizable dashboard provides one view across your security infrastructure, accelerating time to detect and investigate threats while maintaining contextual awareness.
- Efficiency – Automate your workflows to reduce manual tasks, and accelerate remediation time to lower costs and strengthen security.

Unified for maximum threat protection

With Cisco SecureX, you simplify your security with the broadest, most integrated platform. It's a cloud-native, built-in platform experience that connects our Cisco Secure portfolio and your infrastructure. Plus, it's integrated and open for simplicity, unified in one location for visibility, and maximizes operational efficiency with automated workflows.

Get started at cisco.com/go/securex

The Results

- Simplified control of security solutions by unifying them in one location for visibility
- Seamless and flexible security that protects users behind-the-scenes without interrupting workflows
- Integrated automated security that enhances operations while embedding agility and efficiencies

Unity creates simplicity in security

By simplifying security operations via a single platform, SecureX lets the UNC Charlotte network share information rapidly among various security solutions. It also means UNC Charlotte take a rapid response, stopping threats in their tracks, all in a single console. This happened recently with an attempted attack via the leading entry point for malicious malware at UNC Charlotte: email.

The threat, disguised as an attachment from a trusted source, was clicked. Cisco Secure Endpoint, our endpoint security solution that integrates with SecureX, immediately detected the threat and quarantined it. This prevented the malware from spreading. At the same time, UNC Charlotte's security team received an alert stating the threat had been received on a specific endpoint, as well as where the compromised email had come from. This allowed them to rapidly block that sender on all devices connected to their network.

Through SecureX, the team uploaded the malicious attachment and detonated it in an isolated environment. This let the UNC Charlotte team understand how a successful breach would have unfolded and revealed the malware's command and control destination. Via Cisco Umbrella, they blocked that origination point. SecureX also allowed them to see any machines the malware may have attempted to talk to after detonation and diagnose them as well. Thanks to SecureX, the entire breach defense event took less than ten minutes.

Seamless, flexible, and invisible to users

For Dr. Carlin, protecting UNC Charlotte users' research and private data in a transparent way that doesn't interfere with workflows is a mandate. "We've found a nice mix of things that work," he states. "Seamless . . . invisible to our customers." By implementing SecureX, UNC Charlotte added flexibility for their users to securely access the university's network regardless of device, location, or

1.5 Million Bad emails blocked daily by Cisco Email Security

Malicious URL attempts blocked by Cisco Umbrella each day and increasing **11,000**

1,000 System compromises stopped each day by Cisco Secure Endpoint

use. This is critical to maintain the open community of users found in higher education and hybrid learning environments. SecureX protects UNC Charlotte from the biggest threat to their campus network, malware, by seamlessly leveraging multiple security solutions, including AMP for Endpoints, to constantly scan, detect, and remediate threats. It also leverages Umbrella for DNS filtering to actively protect users against malicious URLs while they're working online. And it's all invisible to UNC Charlotte users.

Integrated and automated security

SecureX empowers UNC Charlotte with an intelligent security that is threat-centric and seamless due to its ability to orchestrate and automate a variety of industry-leading solutions.

As the COVID-19 pandemic unfolded, an increasing number of students, faculty, and staff connected hundreds of laptops and other devices that were new to UNC Charlotte's network. Malicious threats increased. SecureX was easily integrated into their existing infrastructure, quickly becoming a force multiplier thanks to automation that amplified IT staff productivity by a factor of nearly 4 over their usual daily output.

4x Increase in IT staff daily output after Cisco SecureX deployed at UNC Charlotte

Best practices to advance security maturity in higher education

For UNC Charlotte, simplifying their security was a task that began with understanding the true nature of their infrastructure. They realized the need to design for security that flexed with the user while working seamlessly in the background. Design was important and helped drive that success. It also proved that you can have advanced security without spending a fortune.

Be honest: Take a good look at your existing team and infrastructure to assess your true weaknesses. Analyze how your campus and network functions. Automation is great but you'll need to assess staff resources honestly and understand when and where on your campus network the greatest user needs are now and may be in the future . This will enable you to allocate resources accurately upfront, filling the correct gaps with the correct solutions.

Get buy-in: Spend time to educate your chancellor, governing board, and other leadership on what the issues are and how a unified security solution can help. Explain at a high level how the technology works. Make the value of taking action clear and what the risks are if they do nothing.

Pilot first: Prep a small test using the proposed solution. Make sure it is of sufficient size and user mix to provide realistic data. Test various scenarios, including threats, plus experiment with cross-platform integration to detect any issues that may prove roadblocks on larger deployments.

Engage your IT partner: Open a dialogue with a trusted IT partner. Be honest upfront about what you're looking for and what you're not interested in. Seek input on design and how to maximize your existing IT infrastructure to reduce any new costs. Start with your partner account team since they'll have existing familiarity with your situation.

Seek seamless and flexible: An agile security infrastructure can flex with your needs and future security threats. So seek tools that can perform a core function while being highly configurable and integratable. You want capabilities to identify, isolate, and control any threats so look for solutions that seamlessly work together towards that end. Remember that university IT environments and users are a complex mix and one size doesn't fit all, especially for a research campus. So it pays to be open to new ideas and approaches that may seem impossible - and let the "possible" emerge.

Spend wisely: Let's face it - you have a limited budget, the sky is not the limit. So buy only the products and solutions that are going to have concrete value in protecting your campus network and its users. If you're not going to use it to it's full potential or its going to be disruptive to your IT environment, avoid it. Save that money for a solution that might be a bit more costly but will drive solid results.

Next steps

See how universities can optimize facilities, improve outcomes, and provide a safer environment for students and educators.
Visit: Cisco for Higher Education.