Few colleges or universities could have been fully prepared for the speed or scope of the pandemic or the security risks it created in the massive push to remote learning. The challenges inherent in supporting so many off-campus systems, however, present a pivotal opportunity for higher education IT leaders.

The need to institute a more integrated, zero-trust approach to securing near-term and future digital learning initiatives is now more imperative than ever. For most higher education institutions, the network infrastructure that’s fundamental to supporting teachers, researchers, students and administrators still suffers from a lack of total visibility of who, and which devices, are connecting to campus resources.

An estimated 19.7 million students are projected to attend colleges and universities in fall 2020. The ability to verify identity, enable secure access and defend remote users at anytime from anywhere will define how schools come out ahead against cyberthreats.

Fortunately, it’s possible to build an agile security strategy to meet today’s remote learning demands without requiring schools to tear down their existing infrastructure, according to IT security experts.

“It makes sense in this new environment for leaders to accept that there are new and greater risks, and these changes require an integrated security framework,” says Steve Caimi, cyber specialist at Cisco Systems.

Improving return on a multiplicity of tools
One of the biggest security challenges higher education IT leaders need to tackle, he and others say, is the sheer number of solutions that IT departments have accumulated to address various security issues. That’s why a growing number of institutions are turning toward a vendor-ecosystem approach where they can invest in tools that are known to work together.

“When customers invest in cybersecurity, a lot of times they end up buying dozens of different tools from different vendors,” Caimi says. “Not only does it take a lot of time to manage different vendor capabilities, it’s even harder to integrate.

Cisco fully understands those challenges, so we integrated our portfolio through our SecureX platform to make security operations fast and incredibly effective.”

Cisco holds a longstanding leadership position in the cybersecurity community, he says, that’s been enhanced by the company’s acquisitions and partnerships which allows Cisco to stay ahead of cyberthreats.

“What we do is pull together a set of cybersecurity solutions that function as an integrated suite of capabilities. We are simplifying security so that organizations can benefit from things like multifactor authentication and other security capabilities that might have been hard to set up in the past. Now security is simple enough that even small teams in a small school district can set them up,” Caimi says.

For example, Cisco’s acquisition of Duo Security in 2018 amplified Cisco’s leadership in zero-trust security, to offer a more comprehensive access solution across the environment and all applications, explains Jamie Sanbower, principal architect at Cisco Systems, in an interview with EdScoop’s sister publication earlier this year.

But the other benefit of working with Cisco, according to Caimi, is that Cisco’s experts can look holistically across a client’s network to help IT leaders understand where their greatest vulnerabilities are, and how they can replace or augment current tools strategically to get the highest return-on-investment.

The speed and scale of access has changed, Caimi says, and there are different types of security risks that come from distance learning that are launching today en masse.

Working toward a zero-trust security model ultimately helps higher education institutions to unify user and device protections at scale, to more easily verify identity, to enable secure access and to defend remote users.

Today, a number of universities are turning to Cisco’s suite of tools such as Cisco Duo, AnyConnect, Umbrella and AMP for Endpoints to integrate their security strategy and mitigate a number of potential threats.
Account takeovers
The University of Michigan’s Departmental Computing Organization (DCO), for instance, recognized weak passwords as a top risk for the program.

Leaders saw an opportunity to secure user accounts with a dual multifactor authentication tool. In less than two weeks, the department integrated the Cisco Duo tool to protect over 60 UNIX and Windows servers and internal web applications. After the tool was added, no more accounts were compromised, according to Don Winsor, DCO coordinator and adjunct professor.

“Additionally, the university substantially cut down on time to investigate security incidents,” Caimi says. That has translated into a huge benefit to the IT department in terms of people resources that can now focus on more pressing tasks.

Slow incident response time
George Washington University needed a solution that offers a high level of protection for various user bases, with a low level of interaction required to implement the solution, according to Mike Glyer, director of information security services at the university.

They turned to Cisco Umbrella because the cloud-delivered solution combines multiple security functions into one tool — from intelligence on current and emerging threats, visibility across access points and protection against phishing and malware attacks. The tool extends protection to devices, remote users and distributed locations anywhere.

Ransomware and malware threats
Sam Houston State University needed to improve detection capabilities with visibility and control over endpoints wherever users take their devices.

While other tools help prevent threats or verify identity, Cisco’s Advanced Malware Protection (AMP) provides deep insight into endpoint behavior so IT teams can detect, contain and remove advanced malware for any device connecting to the university’s network.

“AMP gives us the visibility and control of our endpoints to provide the IT security needs of the university, without inhibiting academic freedom and research,” says Tim McGuffin, information security officer for the university.

Poor visibility across the network
Remote learning introduces a lot of added concerns for university networks with new and unrestricted devices, as well as SaaS-based and unsanctioned apps, accessing university systems. The lack of full visibility of what’s connecting to their networks, combined with low user awareness of potential threats, exposes institutions to greater risks.

Caimi shared how North Carolina, Chapel Hill addressed those risks by integrating Cisco’s Firepower solution to be able to set up a secure virtual campus within roughly six days.

Using Cisco’s Firepower Management Center increases the effectiveness of Cisco security solutions by providing centralized, integrated and streamlined management. It operates like an administrative nerve center to provide unified management of firewalls, application controls, intrusion prevention, URL filtering and advanced malware protection.

Integrated security in one platform
All of these use cases illustrate that there shouldn’t be a need to rip and replace infrastructure, and schools will end up reducing costs to IT that can be reallocated to other programs.”

SecureX is at the heart of Cisco’s security integration solution, connecting Cisco’s security portfolio with an organization’s infrastructure. The platform ensures that security teams have a unified view of their security tools. It is a cloud-native, built-in platform which requires no API connections or middleware to make security tools work together.

The platform orchestrates the tools automatically so that security teams can spend their time working on strategic problems. With automated workflows, the system can run to discover and remediate problems so teams can reduce threat dwell time.

“We built a platform with the mindset of maximizing the efficiency and effectiveness of security operations teams. Getting started is simple, because it’s a built-in platform experience that integrates all Cisco secure products. All customers need to do is sign-in with secure multifactor authentication and they can see actionable intelligence, investigate threats and respond automatically all in one place,” Caimi says.

Learn more about creating safe learning environments on both physical and virtual campuses.