INDUSTRY SPEAKS

Technology Foundations of Student Success

The vast, rich web of integrated technologies required to meet students' — and all users' — expectations continues to grow. Complex integration and management are the order of the day as cloud, AI, and data-rich capabilities advance, commanding not only greater speeds and power from the network but rapid agility, dynamic scale, and growth.

There's never been a more critical time to focus on higher education's core constituents, given the current environment that institutions now find themselves in: waging multi-front battles against persistent enrollment declines and the challenges of pandemic recovery. New learning modalities and alternative credentials place additional pressure on institutions to improve the student experience. As colleges and universities invest in technology to meet expectations for seamless access to resources and personalized, anytime-anywhere support, they must also lay the foundation for innovation moving forward.

PRESENTED BY: CAMPUS TECHNOLOGY

SPONSORED BY: LUMEN®

The ability to meet, maintain, or even exceed user expectations rests squarely on a core set of five critical technology areas that include: network infrastructure, unified communications and collaboration, cybersecurity and Secure Access Service Edge, IoT and connected campus technologies, and managed services.

Three experts from Lumen recently sat down with *Campus Technology* Editor-in-Chief Rhea Kelly to discuss how institutions of every shape and size can meet such multi-faceted challenges. New approaches to network architecture, cloud-based solutions, and managed services may ensure consistent support and improved security posture even as recruiting and retaining IT resources present additional roadblocks to digital transformation.

Network Infrastructure: The Backbone of It All

What are students' and all constituents' expectations? First and foremost, users expect anytime, anywhere access to the campus network and data, whether working from home or performing on-site research in Alaska. They want access to real-time data and analytics that provide insight into student performance, notifications and alerts regarding physical security events, or the status of a student's load of laundry. Administrators expect IT and IS teams to enable such services despite shrinking budgets, even as security risks grow with every new device or platform students and faculty expect to use to advance in-classroom and remote learning.

What are students' and all constituents' expectations? First and foremost, users expect anytime, anywhere access to the campus network and data, whether working from home or performing on-site research.

"The 2023 incoming freshman class will consist of students whose high school experience was defined by the pandemic and learning remotely," said Scott Pohlman, director of business development for higher education at Lumen. "This class will show up with a different view of what the student experience should look like. They'll still want to have traditional learning opportunities, in class and around other people, but they'll also want the ability to have a remote experience, if they want to take a class from the library, and so on. Delivering a high-

quality learning experience, regardless of location, is crucial. It's really content anytime, anywhere."

Colleges and universities need a strong but flexible wide area network (WAN) that can easily scale to support such access as well as future growth. Software-defined WAN (SD-WAN) virtualizes network architecture, allowing for centralized control and dynamic routing as capacity needs change.

As more services, applications, and infrastructure shift from on-premises to the cloud, costs also rise, and institutions must balance their use of public cloud services with their own private infrastructure. Effective monitoring of cloud usage requires robust infrastructure on campus and the ability to connect with different cloud providers whenever necessary; delivering results while saving on the bottom line.

Where should institutions start when planning and addressing areas of the network infrastructure to replace or upgrade first? "As you look at your VPN, is it time to move to a next-gen firewall that can bring in things like AI? An SD-WAN not just across your campus, but across your system throughout the state? It's difficult to think of a campus as a discrete thing anymore. In most community college systems, there are locations in geographic outposts in a more rural part of the state and the server is in a closet with a mop and maybe a basketball, and there are people whose jobs are everything. There's three to five people who are security, IT, and operations," said Matt Kenslea, director of business development for higher education at Lumen. "How does that institution afford something? The system makes an investment that

As more services, applications, and infrastructure shift from on-premises to the cloud, costs also rise, and institutions must balance their use of public cloud services with their own private infrastructure.

brings the smaller campuses into the fold, lets them take advantage of a technology or services that they wouldn't be able to fund on their own, but as part of the system they can participate."

Cybersecurity and SASE: Everything, Everywhere Is an Edge

The concept of **secure access service edge (SASE)** offers a means for higher education to achieve zero trust access to remote or hybrid learning

What Is Zero Trust?

The National Institute of Standards and Technology defines the zero trust security model as "a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The zero trust security model eliminates implicit trust in any one element, component, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses."

Source: NIST Computer Security Resource Center

and working environments, which can now be delivered while meeting real-time context and security compliance. These converged network and security-as-a-service capabilities allow institutions to mitigate the outsize security risks inherent to open access networking and collaboration, traditionally a part of research and instruction in higher education.

"The university was built to be an open system," Kenslea said. "It's one of the most porous environments, and you're talking about data that's a target for nation-state actors. There's enormous value in the campus systems and environments. Attracting and maintaining the staff to manage these technologies is a huge challenge."

Generally, there are three primary options for SASE adoption today, **according to Gartner**: a single-vendor offering, explicit pairing of two vendors (one for network, one for security), and managed SASE. Gartner reports that demand for single-vendor SASE tends to come from smaller enterprises that don't have strongly siloed network and security teams and don't require best-of-breed across all capabilities, and from architecture teams in large global multinational enterprises.

"Access servers have been virtualized and put into public cloud platforms, or public and private clouds, and SASE is the leading edge of that front," Pohlman said.

The SASE framework can be deployed gradually — typically alongside opportunities to update or refresh existing infrastructure — and consists of:

- **SD-WAN**, Software-Defined Wide Area Network.
- **NGFW**, Next Generation Firewall expanding on capabilities of traditional firewalls to increase their ability to identify and block potential threats.
- **SWG** or Secure Web Gateway to protect users and institutions from inappropriate or hazardous content, enforce policies, and prevent unauthorized data transfer or theft.
- **CASB**, Cloud Access Security Broker to protect the increasing number of cloud or SaaS application used by most colleges and universities today.
- **ZTNA**, Zero Trust Network Access, an integrated framework providing for Least Privilege access to specific resources as opposed to admission to the entire environment provided by traditional VPNs.

"There are providers that build SASE devices, but, as time goes on, all of those vendors are going to become software companies," Pohlman predicted. "Even the router companies are going to become software companies, so you're going to have a high-performance box either on your campus or at a provider edge. You can download virtual machines to run your security, to do a lot of different things. It's going to make

SASE, by the numbers

BY 2025:

80%

of enterprises will plan or approve a strategic plan to unify web, cloud services, and private application access using a SASE/SSE architecture.

↑ UP FROM 20% IN 2021

65%

will have consolidated individual SASE components into one or two explicitly partnered SASE vendors.

↑ UP FROM 15% IN 2021

50%

of new SD-WAN purchases will be part of a single-vendor SASE offering.

↑ UP FROM 10% IN 2022

Source: Gartner

prices come down, but it also provides a lot of flexibility because you don't have an embedded device. If you need to make a change, and it's running on a virtual machine, you can make that change very quickly. It makes the marketplace evolve much quicker. One of the hallmarks of a SASE framework is that it's centrally managed. If you don't have technical resources or staff out at the edge school, it's often managed by a service provider, which takes a lot of that administrative burden and risk off of those campuses."

Keeping the Campus Connected

A large part of ensuring a satisfactory student experience rests not just in enabling anytime, anywhere learning, but in access to data and monitoring, sensors, and smart devices that alert and track everything from student progress to laundry cycle status.

"It's not just the students, because it's also the faculty, the visitors, the alumni. It's everyone who's touching the campus. Creating that connected campus, when you think about everything that can be monitored, helps the administration, the staff, the faculty make better decisions," said Lumen's Michelle Watson, senior director of SLED — national technology strategy and business development. "The number of devices that are connected to the internet and all of the valuable data created; monitoring attendance, security operations, physical security, classroom use, you name it."

From a physical security standpoint, campuses increasingly rely on IoT technologies to control door locks and link security systems, alarms, and video cameras. Some systems can help users identify the safest walking route to and from class or campus buildings. Alerts can be sent to campus police if users don't reach their destination by a certain time. Sensors can track traffic patterns and pedestrian crossings to determine if any logistical or safety changes need to be made.

"A smart campus is more than a collection of applications, platforms, or infrastructures leveraged in a siloed manner around campuses," **according to Deloitte**. "It uses next-generation technologies like artificial intelligence, machine learning, blockchain, facial recognition, smart sensors, and beacons — technologies strategically placed to trigger communications, take attendance automatically, derive venue analytics, automate processes, monitor and initiate workflows, and offer many more innovative practices that digital natives are accustomed to."

Essential, Equitable Connections

The Infrastructure Investment and Jobs Act signed into law in 2021, provides $65 billion in funding for broadband expansion and access.

The act established the Broadband Equity, Access, and Development Program, administered by National Telecommunications and

Elements of the Smart Campus

Smart student
Digital student

Smart classroom and lab
Next-gen classroom and labs

Smart teaching and research
Instructions and research

Smart housing and dining
Logistics and services provisioning

Smart mobility
Campus mobility and safety

Smart events
Event logistics and services

Smart stadiums
Fan experience and operations

Smart student administration
Student administration

Smart operations
Campus and building operations

Information Administration, to provide $42.5 billion in matching grants to states. Of particular interest to higher education is the act's $1 billion for the **Middle Mile Broadband Infrastructure Grant Program**, administered by the NTIA, and earmarked for building, improving, and acquiring broadband and fiber infrastructure that connects to the internet backbone, with priority given to unserved and underserved areas — often the same areas where rural community college systems and land grant institutions operate.

"This is really talking about those last-mile connections and connecting them to the services they're trying to get to," said Pohlman. "It's very expensive and difficult to build into rural areas, where you might have to spend $200,000 to connect 10 users. Just like rural electrification 100 years ago, you need a federal presence to do that. We're starting down that path but there's a lot more to be done."

Areas that have less than 25 Mbps download speeds and 3 Mbps upload speeds are considered "unserved," while areas with 100 Mbps download speeds and 25 Mbps upload are considered "underserved." States are eligible for grants administered by Middle Mile Broadband offices within each state.

"What really would be helpful is for the higher education community to reach out and make contacts with these broadband offices, engage them and help them understand how that money could be spent," noted Pohlman. "They need help, and I've seen that particularly in the regional networks."

Areas that have less than 25 Mbps download speeds and 3 Mbps upload speeds are considered "unserved," while areas with 100 Mbps download speeds and 25 Mbps upload are considered "underserved."

MORENet in Missouri, for example, "is really engaged with the state of Missouri's broadband office, so I encourage everyone to figure out where your broadband office is in your state and reach out and offer your help, let them know what your issues are," Pohlman said.

"It's leveraging the higher ed voice to create that partnership with communities, create those synergies and provide that forecast, so to speak, on where we can get the most value," added Watson.

Unified Communications and Collaboration: Delivering the New Normal

"In the old days, UC was really just about video and speaking over the webcast," Pohlman said. "Today a lot of these applications have an open API, and companies that specialize in education have built ease of use for the video and voice into the API, while wrapping around more advanced student engagement services. They're trying to maximize engagement through interactive whiteboards, polling features, and incorporate multimedia tools. All of that is really geared toward more classroom management."

HyFlex — or "hybrid" and "flexible" — environments offer new unified communications and collaboration (UCC) capabilities that break down barriers to asynchronous or digital learning and virtual/augmented instruction. Some education-specific platforms incorporate AI capabilities to create thumbnail galleries that help instructors better identify and engage with students, for example.

"The key attribute is flexibility, and being able to meet user communities where they are," Pohlman said. "You're going to see the scope and scale of what these UCC platforms can do expand exponentially."

Similarly, it's important that departments, colleges, or satellite campuses within larger university systems work together from similar sets of data. When those units don't share information or data, there is no way to understand how the system engages constituents in an optimal way, or a way that makes sense for the users. Shared data sets put the focus on the most important piece of the institutional mission: the student experience.

Managed Services: Keeping It All Flowing Smoothly

On the operations side, incorporating managed services can level the playing field for institutions looking to stay competitive, exceed user expectations, and provide access to the latest technologies. As smaller institutions try to compete with larger R1 research campuses or the private sector, retaining knowledgeable and experienced IT staff becomes more difficult, not to mention affording the tools and resources required to keep it going. Allowing vendors to manage operations for cloud-based services and connectivity becomes a smart means to achieving the benefits of next-gen infrastructure without having to worry about who will manage it all. Managed services enable new and emerging technologies to be provisioned rapidly and expertly supported, ensuring a more frictionless student experience and improving institutions' ability to attract and retain students and faculty.

"When you take a look at how managed services can solve problems and provide solutions from a staffing and technology perspective, I just view it as critical component in the space," Watson said.

Learn More

Lumen's enterprise platform combines networking, edge, cloud, collaboration, and security to power amazing experiences for higher education. Find out how to build a strong technology foundation for your campus at **lumen.com/highered**.