



Secure Access Service Edge's Flexible, Scalable Security Protects Higher Education's Highly Distributed World

The SASE framework offers simpler solutions for increasingly complex network and data security requirements.

IN HIGHER EDUCATION'S HIGH-BANDWIDTH, super-connected, and widely distributed world, the network is where the user is — every user is an edge. How can institutions ensure broad network protection and data security in this new world? Institutions increasingly turn to the secure access service edge (SASE) framework, which offers not only a more scalable approach to protection but also more efficient network and security management.

"Conversations are very active in higher ed right now around SASE," said Matt Kenslea, Senior Account Director for Education at Lumen. "We believe the value is there, and we believe people are going to start evaluating it and putting it into place."

SASE converges networking and security into cloud-native architecture that shifts the security focus from traffic-flow-centric to identity-

centric, **according to Versa Networks**. “SASE encompasses a package of technologies that embeds security into the global fabric of the network, so it is always available no matter where the user is, where the application or resource being accessed is, or what combination of transport technologies connects the user and the resource,” according to the company.

“In higher education, where the perimeter is so amorphous, this kind of solution really lends itself to protecting that,” Kenslea said. “The users represent the risk. By pushing this out to the edge (to the user), you dramatically increase your security, your ability to update it, and more effectively manage network traffic.”

Absolutely Zero Trust

“In the old days, you connected to a VPN. Users had free reign and could run around the network and access whatever they could get to. But that’s also the way attackers operate,” Kenslea said, citing the massive Solar Winds hack that attacked several components of U.S. government-operated infrastructure and perpetrated a series of data breaches in 2020.

“Those attackers were in the network for over a year before they hit. In a least-privileged, zero-trust world, they wouldn’t have been able to stay. They would have had to reauthenticate, and that’s part of the zero-trust architecture in the SASE framework,” Kenslea said.

Opportunities Abound

“In many cases, institutions may already have a piece or two of the SASE framework’s core components implemented. They bought a new firewall, or they have the secure web gateway. We’ve heard others suggest that the SD-WAN

What is SASE?

SASE unites network, security, and management into a flexible architecture that delivers key technologies for the distributed enterprise.

Essential SASE components include:



Software Defined Wide Area Network (SDWAN), using the ease of implementation and management provided by software to replace legacy technologies and hardware.



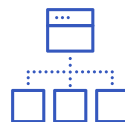
Next Generation Firewall (NGFW), expanding on capabilities of traditional firewalls to increase their ability to identify and block potential threats.



Secure Web Gateway (SWG), to protect users and institutions from inappropriate or hazardous content, enforce policies, and prevent unauthorized data transfer or theft.



Cloud Access Security Broker (CASB), to protect the increasing number of cloud or Software as a Service (SaaS) applications used by colleges and universities today.



Zero Trust Network Architecture (ZTNA), an integrated framework providing for Least Privilege access to specific resources as opposed to admission to the entire environment provided by traditional VPNs.

These are implemented using a cloud-centric architecture, ideally with a single vendor, which not only helps keep costs down, but also improves the overall security posture.

should come first because that's the core and that gets you across. But there are lots of roads to Rome," Kenslea said. "You just need a plan, as with anything else."

Smaller colleges within a larger university umbrella also present opportunities to evaluate the SASE concept on a smaller scale, perform any necessary tests, and learn valuable lessons before scaling out the framework to the entire university.

"One of the main benefits is the ease of deployment and then, once it's implemented, the ease of updating and expansion. If you add another user, you don't have to add more servers. You don't have to download VPN software. No one needs to physically go anywhere. The utility is real."

In the case of research institutions looking to comply more readily or rapidly with federal grant funding requirements or specific security frameworks such as NIST 300, the framework also offers more efficient and flexible ways to set policies through its software-based, hardware-neutral architecture.

"Many SASE projects are driven by the objective to simplify policy management and enforcement and improve the organization's security posture," a recent **report from Gartner** stated. "Because SASE offerings target both network and network security capabilities, the recommended approach is to form a joint team across networking and security to develop a strategic roadmap for adoption."

Users' Expectations Demand SASE's Efficiency

Higher education constituents — students, staff, faculty, researchers, research partners, parents, and anyone else who touches an institution's network — already expect anytime, anywhere

access to data and connectivity to perform their roles, whether they're on campus or halfway around the globe. Given the ever-growing levels of service, and the rapidly exploding volume of data supporting research, teaching, and learning, many institutions may soon discover they have no choice but to start down the path of implementing a SASE framework concept.

80%

of enterprises will adopt a strategy to unify web, cloud services, and private application access using a SASE/SSE architecture by 2025, up from 20% in 2021.*

1/3

of new SASE deployments will be based on a single-vendor SASE offering, up from 10% in 2022.*

"For all of those challenged IT and support staff, this really makes their lives easier," Kenslea said. "Now, you can set policy and controls that — boom — go across the entire environment. There's a lot of value there."

Beyond saving time on configurations, value is realized through fewer hardware upgrades and less maintenance, eliminating expenses for unused network capacity, and reductions to square footage in the data center's footprint.

"The data center is not necessarily the end-all, be-all," Kenslea said. "The network is where the user is, and that's true everywhere."

Colleges and universities can simplify network access, security, and management with SASE solutions on the Lumen Platform. Take this five-question quiz to see which services and levels of support are the right fit for your environment.