Build a Secure and Connected Future for Students

How unified cybersecurity and networking pave the way for education's tech future

Technology Creates Both Challenges and Opportunities in Education

Education is evolving to teach the skills required to thrive in today's world. Technology is a crucial part of the learning environment today but it's becoming more and more complex. Applications are distributed in the cloud, data center, and as a service. Students are connecting to the campus internet with more devices than ever—from a simple laptop to smartphones, tablets, and multimedia entertainment consoles—increasing the threat via a variety of internet connections. We can clearly see new challenges emerge, such as networks that can't keep up with demand, an increased risk of data loss and disruption from cyberattacks, and the lack of necessary cybersecurity skills, resources, and funding. In addition, many schools are trying to close the digital divide for students both on and off campus.

For educational institutions that lack modern infrastructure and IT resources, embracing new technology is daunting. However, the right solutions can speed transformation. In this eBook, we'll examine trends driving tech adoption in education, unique challenges faced by IT teams, and how the convergence of cybersecurity and networking can protect data and advance digital learning. Through a series of use cases, you can explore multiple ways to enhance education for both K-12 and higher education.

Initiatives Driving Technology Adoption

As schools work to offer greater support and personalization for students, they must also adopt new technologies to reach today's digital-native students. The following initiatives provide better student experiences but also increase IT complexity.

Flexible learning modes

Nearly all K-12 schools in the U.S. are back to full-time, in-person instruction for the 2023-2024 school year, although 16% offer remote learning as an option.[1] While younger students are primarily back in the classroom, higher education is a different story. Ninety percent of two-year institutions and 78% of four-year institutions plan to add more online courses to attract enrollment.[2] These digital courses are in high demand, with online or hybrid class registrations for fall of 2022 reaching capacity ahead of in-person courses.[3]

Increasing digital access

For younger students, school districts are helping provide digital access. Fifty-six percent of public K-12 schools provide internet services for their students outside of school (such as at libraries or in other public spaces), while 45% provide internet access to students' homes. In addition to connectivity, 94% of schools provide devices like tablets or laptops, and 87% provide technical support for students.[4] This effort helps close the digital divide for students but also places burdens on schools and school districts to provide both technology and support.

Emerging classroom technology

Whether provided by schools or brought by students, the number of devices in the classroom is increasing, and there's more to come. New technologies like augmented reality, virtual reality, and artificial intelligence will soon become more common in education. These technologies need high-speed connectivity, will place greater demand on campus networks, will introduce additional cyber risk with the increase in the digital attack surface, and additional security vulnerabilities caused by BYOD.

Safer campuses

With news stories of on-campus violence affecting students of all ages, safety is top of mind for many, even impacting the choice of college for over one-third of female students.[5] The Clery Act requires colleges and universities to report campus crime data, but incident reporting is largely a manual process that requires going through a member of security staff. More schools are investing in technology to help improve safety, from security cameras to mobile app-based access control systems to enter classrooms and dormitories.

[1] "School Pulse Panel: Learning Mode," Institute of Education Sciences, October 2022.

[2] "Higher Ed Pulse Check: Cost, Value and Enrollment Concerns on Today's Campuses," Bay View Analytics and Cengage, September 2022.

[3] Debbie Truong, "Overwhelming Demand for Online Classes Reshapes Higher Ed," Governing, October 2022.

[4] "School Pulse Panel: Technology," Institute of Education Sciences, October 2022.

[5] Melissa Ezarik, "Students Mostly Feel Safe on College Campuses, but Not Equally So," Inside Higher Ed, June 2022.

Top Challenges for School IT Teams

IT teams in education face a number of difficulties that make security and compliance particularly challenging. These include:

Rising cyberattacks

Schools and their data are common targets for cyberattacks, with a reported 1,065 cyberattacks per week targeting educational institutions in 2021, a 75% increase over 2020.[1] Cyberattacks in schools are expensive, causing losses of up to $1M per attack.[2]

Ransomware is a particular concern for the education sector, according to an advisory issued by the Cybersecurity and Infrastructure Security Agency (CISA).[3] In 2022, there were 89 ransomware attacks that impacted over 2,000 schools.[4] Perhaps the most notable ransomware attack on public education was against the Los Angeles Unified School District, the second-largest public school district in the U.S. When the LAUSD refused to pay the ransom, attackers leaked 500GB of stolen data on the dark web.[5] In higher education, a ransomware attack that disrupted admissions, combined with pandemic-related challenges, forced Lincoln College in Illinois to close after 157 years in operation.[6]

Resource constraints

Many schools aren't equipped to deal with increasingly sophisticated cyberattacks. The Nationwide Cybersecurity Review found K-12 schools averaged a cyber maturity score of 3.55 out of 7 (a satisfactory score is 5/7), and while that score has improved over time, it lags behind other sectors. Lack of funding was the top concern cited by schools, as only 8% or less of IT budgets are allocated for cybersecurity. Other concerns included lack of strategy and cybersecurity personnel.[7]

Compliance requirements

Personally identifiable data collected by schools about their students and faculty is subject to data privacy regulations. The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student records, and the Children's Online Privacy Protection Act (COPPA) governs the collection, use, and disclosure of personal information of children under 13. The Children's Internet Protection Act (CIPA) requires that schools monitor online activities and block inappropriate content for students under 18. In addition to federal regulations, new state privacy laws have gone into effect in 2023 that require institutions to adapt their policies. Schools must demonstrate compliance with these regulations, which can be a manual and time-consuming process.

1. Shaun McAlmont, "3 big reasons that it's time for higher education to crack down on cybersecurity," University Business, September 2022.
2. "As Cyberattacks Increase on K-12 Schools, Here Is What's Being Done," Government Accountability Office, December 2022.
3. "Alert AA22-249A: #StopRansomware: Vice Society," Cybersecurity and Infrastructure Security Agency, September 2022.
4. "The State of Ransomware in the US: Report and Statistics 2022," Emsisoft Malware Lab, January 2023.
5. Carly Page, "Hackers leak 500GB trove of data stolen during LAUSD ransomware attack," TechCrunch, October, 2022.
6. Bill Chappell, "Lincoln College closes after 157 years, blaming COVID-19 and cyberattack disruptions," NPR, May 2022.
7. "K-12 Report: A Cybersecurity Assessment of the 2021-2022 School Year," Center for Internet Security and Multi-State Information Sharing & Analysis Center, November 2022.

Combine Performance and Security to Maximize Digital Learning

To overcome technology challenges and be better equipped for digital learning in the classroom and online, educational institutions need fast and secure connectivity and reliable digital infrastructure. Whether you choose to adopt technologies such as SD-WAN or 5G, connections must support growing traffic demands, be easy to manage, and be affordable so all students can participate equally.

Schools also need robust security solutions to stand up to sophisticated attacks. Yet these solutions must also work with limited IT budgets and personnel. Experienced Managed Security Service Providers (MSSP) can help identify, implement, and manage the right mix of security products, services, and solutions to effectively defend against ransomware and other attacks.

See how the convergence of cybersecurity and networking solutions can help your institution expand digital learning options and provide a safer environment for students, faculty and education institutions.
The following four use cases demonstrate possible applications.

Connect the Decentralized Campus

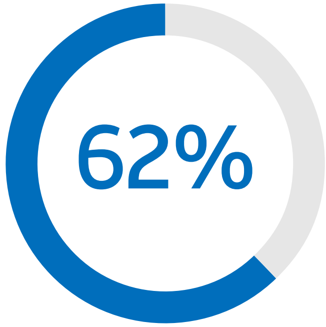
Defend Against Ransomware

Comply with Data Protection and Privacy Regulations

Build a Smarter and Safer Campus

Use Case: **Connect the Decentralized Campus**

As institutions of higher education embrace technology to enable learning and collaboration, they accelerate their adoption of cloud services and support for mobile applications. They are also deploying a wide range of Internet-of-Things (IoT) devices as part of smart campus initiatives. With the influx of these new technologies, however, come increased risks to network security and to the intellectual property and personal data connected to it.



of students want better on-campus Wi-Fi[1]

AT&T SASE Branch with Fortinet offers a better alternative for secure, high-speed networking for school campuses. It can be deployed more quickly and at lower costs than traditional networks, has built-in security features, and can reliably connect multiple locations, whether they're schools within the same district or university branches. Using SD-WAN to allow traffic to travel between campus locations via the public internet or a virtual network eliminates or reduces the need for MPLS.

AT&T SASE Branch with Fortinet combines networking and security to optimize performance and prevent malicious traffic. Reducing complexity through consolidation will accelerate outcomes. By focusing on consolidating vendors and point products—across both security and networking, establishments can consistently apply threat intelligence and security services across the digital attack surface.

Benefits:

- High-performance networking across locations
- Fewer learning disruptions
- Reduced risk of a cyberattack or outage

[1] "Students' Perspective on Technology on Campus," Inside Higher Ed and College Pulse, November 2022.

Use Case: **Defend Against Ransomware**

A ransomware attack can lock access to systems, disrupting administration and classes. If it results in a data breach, private data can end up on the dark web, as in the LAUSD breach. As many schools lack funding and personnel for cybersecurity, they can struggle to respond quickly to an attack.

Siloed security tools can also contribute to the challenge. They require greater time for management and manual correlation of data to detect issues. Consolidating security with a single platform offers shared intelligence and insights in addition to easier management.

For an effective defense against ransomware, AT&T provides secure connectivity to deliver better experience for students and faculty as well as flexible managed services backed by Fortinet's industry-leading security platform.

For institutions that lack the skilled cybersecurity staff to defend against ransomware, a managed service can provide protection backed by security experts 24/7/365. With the right defenses in place, you can vastly reduce the chance of a data breach or downtime.

Benefits:

- Lower risk of a costly breach
- Faster response to multiple types of threats
- Complete, around-the-clock coverage

Use Case: **Comply with Data Protection and Privacy Regulations**

Educational institutions are subject to a growing number of regulations designed to protect data privacy and prevent students from accessing inappropriate content. Personal devices are also brought to school by students that may be used to access unauthorized content or distracting applications like social media on the school's Wi-Fi network. Consistent, targeted security policies are needed to ensure data is protected and access is limited without impeding educational use of the internet. However, network policies are often fragmented, making them difficult to manage.

In addition, compliance with these laws isn't enough—schools must also prove they are compliant, and reporting processes are often manual and time consuming.

Robust web filtering, network segmentation, and unified policy management can reduce the challenges of complying with regulations. Filters prevent access to inappropriate content and can block undesirable applications from working on students' personal devices while on school Wi-Fi. Segmentation gives precedence to higher-priority network traffic and increases security, such as by putting unmanaged personal devices on a different segment than managed educational devices.

Single pane of glass management ensures consistent policies across the entire network, which may encompass multiple schools, and a solution with built-in reporting tools makes demonstrating compliance easier with automation.

Benefits:

- Data protection and content filtering that meets or exceeds regulations
- Fewer distractions from student devices
- Faster and easier compliance reporting

Use Case: **Build a Smarter and Safer Campus**

Internet of Things (IoT) and operational technology (OT) devices can modernize systems throughout the campus. They can be used to improve energy efficiency by shutting off lights and HVAC systems in unused spaces, in classrooms for smart whiteboards and attendance tracking, and around campus to improve physical security with mobile-based access to classrooms and dorms and smart surveillance. The challenge with IoT and OT is that they expand an already diverse and complex attack surface. For many institutions, their current security can't scale to handle the massive growth in endpoints that IoT and OT would bring.

However, a managed solution designed to connect and secure IoT and OT could help your institution take a big technological leap forward. Look for a solution that can:

- Simplify physical security management by integrating voice, video, and surveillance systems with cybersecurity architecture for comprehensive campus security
- Connect, verify, and monitor all devices connected to the network to prevent access by malicious or compromised devices
- Detect threats based on real-time information and threat intelligence
- Integrate security across multi-cloud and edge deployments

With improved integration and automated threat detection, security can scale to accommodate the increased demand IoT and OT bring. In turn, schools can begin to implement new technologies to improve efficiency, safety, and sustainability.

Benefits:

- Detect physical security or infrastructure issues faster
- Harden the IoT and OT attack surface to reduce risk
- Support new educational technologies securely

Convergence of Cybersecurity and Networking from AT&T Business Powered by Fortinet

AT&T Business, backed by Fortinet provides secure connectivity that allows educational institutions to deliver better experiences for students and faculty. Power secure digital learning with flexible managed services backed by an industry-leading security platform for reliable and safe communication and modern digital infrastructure.

AT&T Business is a leading managed SD-WAN provider with a wide breadth of network integration solutions. Fortinet brings a broad portfolio of security and networking products in a unified platform with single pane of glass management to simplify operations. AT&T's managed services backed by Fortinet technology provide high-performance networking and security at scale to maximize digital learning and ensure the physical and digital safety of networks and students.

business.att.com • fortinet.com