ARMIS®

ARMIS BUYER'S GUIDE

Cyber Resilience in Education

Achieving Cyber Resilience in Education

Multi-faceted environments require assessment, detection, and responses on multiple fronts. New cybersecurity strategies offer new hope for educational environments.

ANTICIPATING OUTCOMES. Identifying and prioritizing threats. Managing response. Those are the hallmarks of cyber resilience, yet achieving that desired state brings its own challenges.

This multi-faceted, holistic protection strategy requires a broad mix of technologies and coordination, from always-on risk assessments and authentication to end-user education and compliance. Colleges and universities and K–12 environments generally approach planning and protection similarly, but some distinctions are important, particularly when it comes to tackling the size or scale of risk exposure or gearing cyber education to younger age groups when building a culture of security.

In both educational settings, universities, and K–12 schools are required to safeguard their critical data, minimize disruptions to learning, ensure secure environments, and maintain reputations and compliance standards. Continuous threat exposure management (CTEM) solutions offer security and IT teams in the education sector an ongoing, comprehensive analysis of their environment. This includes evaluating systems, mitigating risks, and identifying and assessing threats.

This guide highlights the essential tools and preparations that should be a part of any K–20 educational cyber resilience strategy, best practices for implementation and adoption of those strategies, and more.

Cyber resilience boils down to the essentials: Visibility, response, and protection

K–12 and higher education IT and cybersecurity leaders must work with other campus and community leaders to develop a strong cyber resilience strategy to better manage today's persistent, emerging threat landscape.

With remote learning, K–12's cyber exposure is greater than ever before

Truly and deeply understanding the IT assets — and risks they pose — helps teams better prepare for and respond to events, prevent system outages, and preserve tools essential to education's core mission.

K–12 districts require visibility into every device on the network

A CTEM solution can help districts gain accurate, up-to-date information on devices, including their vulnerabilities and security posture, along with reliable data to make more informed decisions on cybersecurity and IT budget allocations.

Higher education must adopt new approaches to cybersecurity to overcome critical skills shortages

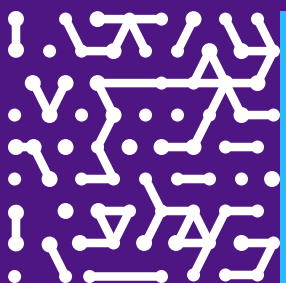
There's help for higher education IT and security teams suffering from a lack of resources and a glut of tools that make choosing the path forward a complex and confusing exercise.

Colleges and universities must manage an explosive growth of connected campus assets

Teams must work to isolate untrusted devices and understand corrupted settings or other vulnerabilities that can expand an institution's attack surface, disrupt connectivity, and open up new risks for data loss.

Asset intelligence holds the key to successful cyber risk management

Comprehensive visibility, automated device classification, risk assessment and prioritization, improved threat detection, and more efficient, streamlined security management all enable K–20 environments' ongoing journey toward cyber resilience.



Five Critical Elements of a Robust Cyber Resilience Strategy

A constantly shifting and complex cyber threat landscape requires new approaches to protection

1. Share responsibilities.
Everyone within the educational IT ecosystem plays a role in ensuring security, including leadership, IT staff, teachers, students, and parents. Create a culture of cybersecurity awareness through training programs and clear communication protocols.

2. Focus on people.
While technology solutions are important in maintaining security, people are always the first line of defense. Training on cyber hygiene practices — the importance of strong passwords, identifying phishing attempts, and reporting suspicious activities — are essential.

3. Take proactive measures.
Rather than wait for an attack to happen, work toward implementing regular assessments of cybersecurity risks, updates to systems and software, and strong access controls to protect sensitive data and comply with data protection standards or requirements.

4. Craft an incident response plan.
Have a clear plan for how to respond to a cyber attack, including steps for containing the damage, recovering data, and communicating with affected parties.

5. Test and update — and repeat.
Cybersecurity threats evolve continuously. Test your environment's defenses regularly and consistently, utilizing a variety of methods: for instance, penetration testing, simulations, and vulnerability assessments. Update any related plans or procedures as needed.

Bottom line

By focusing on a holistic cyber resilience strategy — grounded in the need for true visibility across the entire environment — K–20 institutions of all shapes and sizes will be better prepared to handle cyber threats.

Questions to ask

- What threats do we anticipate?
- What can we afford to lose?
- What is required to maintain compliance?
- How will we recover?
- Where (and how) do we adapt?

Realities of K–12's Cyber Exposure

The many shifts and changes taking place in K–12 environments as a result of greater reliance on new classroom technology tools and online content or instruction do not detract from the segment's core mission of teaching and learning.

ENSURING STUDENT SAFETY, maintaining a lunch program and counseling students are also mission-critical priorities within this setting. New, more targeted risks and malicious threats from ransomware have emerged alongside the many tools that now make up the K–12 environment, such as IoT sensors or other connected components of facilities management, cameras for ensuring physical security, and continued opportunities for untrusted, unconfigured devices to join a K–12 network at any time.

Truly and deeply understanding the IT assets — and risks they pose — helps teams better prepare for, and be able to respond and prioritize events, prevent system outages, and preserve tools essential to the core mission. Schools and districts can face down multiple cyber threats and minimize their threat landscape with help from cyber exposure management platforms, which provide more comprehensive visibility into all connected devices across a school or district network, including traditional computers, laptops, tablets, and IoT devices like security cameras or smart thermostats. Teams can identify and manage vulnerabilities across their entire attack surface, and close gaps before attackers exploit them.

Other key benefits include risk analysis and prioritization, and automated patch management, all of which reduce the workload on busy and distracted K–12 IT teams, as well as ensure faster risk remediation.

Most schools and districts must comply with data privacy regulations in some shape or form, sometimes held to account for multiple layers of compliance. Cyber exposure management solutions track compliance status and identify areas where compliance may be falling off. Offering proactive cyber risk management with early warning detection and a visibly enhanced security posture, these platforms can assist districts in mitigating risks and lowering insurance premiums.

Bottom line

Platforms offer improved threat detection and response by continuously monitoring network activity for suspicious behaviors that might indicate an attack. Such early detection can minimize damage and contain threats. Platforms may provide automated response features that isolate infected devices or otherwise block malicious activity.

Questions to ask

- How do you discover assets that connect to the network?
- Do you have a complete and up-to-date asset inventory across all asset types including managed and unmanaged assets?
- How much manual work is involved?
- Do you trust the data?
- How do you ensure that all your endpoints are properly protected by endpoint security solutions (i.e., they have agents installed and agents are the correct version)?

How One District Gained Visibility Into Every Device On Its Network

In the past it took teams weeks to drill down in switches or firewalls to find vulnerabilities or a compromised device; now it takes a few hours or minutes to pinpoint assets and trigger detection and response

AN ISD NEARLY DOUBLED its student population from 6,700 students to 11,000 in two years, and continues to grow.

The Texas-based IT director soon discovered that some campuses were
more secure than others, and the district lacked a cohesive infrastructure
and consistent approach to security by relying on piecemeal solutions from multiple vendors, which didn't necessarily work together or provide visibility into managed or unmanaged devices on the network, across multiple campuses. As he began work to transform the IT environment, his first step was to understand everything the infrastructure and environment had or did not have. Consultants helped him capture data on the district's security posture with moment-in-time snapshots, but the district's rapid growth meant the information was soon outdated. He turned to a CTEM solution for help. "We are constantly getting the updated data we need," he said.

Bottom line

A CTEM solution helped this district gain comprehensive visibility into devices connecting to the internal network; detailed, accurate, and up-to-date information on devices, including their vulnerabilities and security posture; and reliable data to help the board and superintendent make informed decisions on security budget allocations.

Questions to ask

- Can you contextualize, prioritize, and automate threat responses?
- Do you have total visibility to managed devices and unmanaged BYOD across the entire environment?
- Can you monitor and classify devices in real time for fast, granular reporting?
- Do you need to identify improperly secured and rogue assets faster, and detect and respond to threats faster?
- Do you want to reduce the number of security tools to save time and costs?
- Does your solution Integrate with existing tools for remediation, automation, and orchestration?
- Can you review real-time behavioral analysis to improve the speed and accuracy of incident responses?

New Approaches to Cybersecurity in Higher Education

Emerging technology trends, such as threat intelligence and classroom evolution, will be critical for higher education institutions to deliver on student and staff expectations, operational needs, and university priorities.

CYBER/INFORMATION SECURITY was a priority investment for colleges and universities in 2023, "thanks to ongoing concerns that universities make relatively soft targets for cyber attackers," according to Gartner's Top Strategic Technology Trends in Higher Education report.

"Higher education institutions are viewed as a target-rich environment due to the large amount of sensitive data, intellectual property and personally identifiable information they maintain for students, research and operations. As security threats continue to be pervasive, more institutions are taki ng advantage of threat intelligence (TI) tools and services monitoring network traffic for anomalies and mitigating threats," the report continues.

Indeed, higher education has borne the brunt of cyber attacks since 2020, and has seen ever more — and more severe — attacks since that time. A pervasive lack of resources as well as a glut of tools and solutions make choosing the appropriate mix a complex and confusing exercise. Higher ed "security leaders have an obligation to understand the organization's threat landscape, but remain (overall) immature at quantifying their organizations' cyber-operational risks," Gartner's report continues.

That's even more difficult given higher education's inherent complexities: large networks with varying security and compliance needs; stores of sensitive research data from commercial IP to state secrets; decentralized management models; and an openness of academic mission that may conflict with ensuring that mission can be secured. Threat intelligence and cybersecurity are also critical to meeting student and staff expectations, and other institutional priorities.

Agentless, as-a-service threat intelligence solutions like CTEM provide visibility of all assets, continually verify device behaviors, and provide integrations necessary to contextualize asset threats or automate responses (such as firewall rule changes or micro-segmentation strategies), all with reduced deployment time, improved scalability and potentially lower overhead costs. Simplified management and maintenance allow overworked teams to gain more time back in their day to focus on mission-critical priorities.

Bottom line

CTEMs empower colleges and universities to gain a deeper understanding of their network environment, identify and address vulnerabilities, and ultimately strengthen their overall cybersecurity posture. That comprehensive view allows universities to make betterinformed decisions about resource allocation, prioritize security measures, and proactively mitigate cyber threats.

Questions to ask

- When assessing vulnerabilities, do you have the data you need, such as: What type of asset? Where is it located? How critical is it? Who owns it?
- Would this data help improve your mitigation efforts?
- Do you have a process for prioritizing and remediating vulnerabilities?

How One College Managed the Explosive Growth of Connected Campus Assets

A homegrown tool for managing assets' security posture increasingly alerted the team to false positives.

"**WE DIDN'T REALIZE** that we were running so many different protocols for these peripherals."

A private college operating two campuses in New York manages 150 switches, 300 servers, 2,000 endpoints, and peripheral devices such as printers, scanners, cameras, and projectors. The number of unmanaged devices, used primarily by students and some employees, averaged about 15,000 (five devices per student). Their homegrown tool could not provide a complete picture of what was connected to the network. Upon testing a CTEM, the team identified up to 30,000 devices on its network. Multiple IoT devices had been installed by the maintenance department without notifying IT, and many users were working with outdated operating systems such as Windows 98. Smart TVs used for instructional and entertainment purposes also flooded the network, alongside smart washing machines in the dormitories, not only slowing down network performance but also heightening security risk exposure.

"We didn't realize that we were running so many different protocols for these peripherals —and these could potentially be exploited by malicious actors," the college's assistant IT director said. Using the CTEM, "we set a policy to only allow the TCP/IP communication protocol for these devices. When we eliminated all the other protocols, we had a significant drop in network traffic." The tool also helps teams understand corrupted settings or other vulnerabilities that can disrupt connectivity and lead to DDos, MiTM, or port-spoofing attacks, as well as monitor outgoing communications and isolate untrusted devices to prevent potentially malicious activity from spreading across the network.

Bottom line

Before an agentless solution, the college had little visibility into insider risks and unmanaged IoT devices, as well as difficulty meeting cybersecurity insurance and compliance requirements.

Questions to ask

- Does your team have visibility of all devices — managed, unmanaged, and IoT — across all campus locations?
- Do you have access to actionable information on device security posture and behaviors?
- Do you need to remediate threats faster?
- Can you integrate other tools to automate threat detection and response?
- How difficult is it to adhere to compliance regulations?
- Do you need to improve your institution's security posture to meet cybersecurity insurance eligibility?
- Do you want to reduce burdens on the IT team?

Asset Intelligence Holds the Key to Successful Cyber Risk Management

WITHIN THE EDUCATION ENVIRONMENTS, the Armis Asset Intelligence Engine plays a crucial role in automatically discovering, classifying, and monitoring all connected devices on the network. That translates to several key benefits, including comprehensive visibility, automated device classification, risk assessment/prioritization, better threat detection, and a more streamlined security management operation.

Overall, the Asset Intelligence Engine empowers K–20 institutions to gain a deeper understanding of their network environments, identify and address vulnerabilities, and ultimately strengthen their overall cybersecurity posture. This comprehensive view allows educational leaders to make informed decisions about resource allocation, prioritize security measures, and proactively mitigate cyber threats. Armis, the asset intelligence cybersecurity company, protects the entire attack surface, and manages educational environments' cyber risk exposure in real time.

> **Armis Centrix™, the Armis Cyber Exposure Management & Security Platform, is powered by the Armis AI-driven Asset Intelligence Engine, which sees, protects and manages billions of assets around the world in real time. Armis Centrix™ understands every kind of device. It discovers, monitors, and documents every single asset on the network and provides contextual intelligence about it.**

> **Extensive, multi-faceted intelligence. The Armis Asset Intelligence Engine logs and analyzes billions of assets world-wide in order to identify cyber risk patterns and behaviors. It feeds the Armis Centrix™ platform with unique, actionable cyber intelligence to detect, prioritize and remediate real-time threats across the entire attack surface.**

> **Rapid deployment. A single console provides a complete view and easy management of all assets — with zero configuration.**

Explore what Armis can do to improve higher education and K–12 cybersecurity.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial