AGILEBLUE

The AI-Native SecOps Platform

EDUCATION

CYBER THREAT BRIEF

Safeguarding Schools and Universities from Today's Advanced Threats

2026

TABLE OF CONTENTS

Education is a Top Cyberattack Target	02-04
AI Is Amplifying Present-Day Cyber Risks	05
The Ransomware Threat	06-07
Vulnerability Exploits	08-10
Software Supply Chains Risks	11
Why Educational Institutions Need AI-Driven SecOps	12
Why AI-Native? Checklist: What to Look for in an AI-Native SecOps Platform	13
Conclusion	14
References	15

Education Is a Top Cyberattack Target

Less than a month into a new school year, the administrators of a rural Texas school district serving more than 4,000 students discovered they'd been locked out of their buildings and facilities by a ransomware attack. The attack took down several of the district's core operational systems, including phones, air conditioning, thermostats, security cameras, and electronic building access controls.[1] Cafeteria staff couldn't prepare meals for the students, who receive free breakfast and lunch because of high poverty rates in the surrounding communities.[2] Parents, many working hourly jobs, had to scramble to find childcare when classes were canceled. By the time IT teams were able to restore systems, an entire week's learning had been disrupted.

This incident represents a well-documented pattern that has played out across schools and universities in the U.S. over the past few years. Attackers know that educational institutions have high-value data and very little tolerance for operational disruption. They also know that many have slender cybersecurity budgets, making the risk of detection low while the potential payoff for a successful attack is high. The Cybersecurity and Infrastructure Security Agency (CISA) has described K-12 schools as "target rich, cyber poor," because they hold large amounts of sensitive data but often lack the resources to protect it.[3] Threat research shows education to be the most-often-targeted vertical in cyberattacks, a position it has held for three years straight.[4]

Ransomware remains the dominant threat in education, with 65% of schools having experienced at least one ransomware attack over the past year.[5] Flat networks are common in educational institutions, which often lack internal network segmentation expertise and have little tolerance for the operational disruption that re-architecting networks can cause. But without robust, policy-based segmentation, attackers can move laterally after gaining an initial foothold in the environment, leaving high-value systems—such as school information systems (SIS), learning management systems (LMS), and financial and HR apps—vulnerable. In these environments, the compromise of a single endpoint allows attackers to push ransomware to file servers, domain controllers, and core administrative systems across an entire campus.

Target Rich, Cyber Poor

- CISA

Identity remains the top attack vector across industries,[6] and identity ecosystems in education tend to be complex, increasing security risk if robust controls and monitoring are not in place. Many educational institutions integrate legacy apps with modern cloud infrastructures, so syncing Active Directory (AD) with a cloud identity service like Entra ID is common. Multi-vendor technology environments (e.g., Microsoft, Apple, and Google) are also common, leaving IT and security teams with multiple overlapping control planes and complicating policy enforcement, log correlation, and real-time investigation. The fact that many third parties (such as contractors, substitute teachers, and volunteers) require access only adds to the challenge, as do overlapping roles (student workers, for instance).

In the education sector today, cybersecurity stakeholders confront something akin to the perfect storm. They need to act at speed, but manual triage workflows often leave threats unreviewed for days. Overnight volume spikes create alert backlogs that teams struggle to clear, while log retention time limits mean investigations need to be finished quickly. But all too often, investigations stall, held back by alert volume, noise, and manual workflows.

This threat brief will highlight current and emerging cyber threats targeting the education sector. It aims to translate security intelligence into actionable insights that help leaders set priorities and build security operations (SecOps) program roadmaps for the year ahead, explaining why AI-native solutions are needed to counter today's complex, AI-driven threats.

AI Is Amplifying Present-Day Cyber Risks

Widespread AI adoption hasn't fundamentally changed the nature of cyberattacks. But it has made it faster and easier to launch them, especially at scale.

AI-powered threat actors are tireless, enabling multi-factor authentication (MFA) fatigue attacks to continue for weeks on end. AI can enumerate SIS/LMS API endpoints in seconds, or leverage automation to find vulnerabilities in student portals or legacy web apps.

Deepfake voice clones are now so authentic-sounding that they can trick biometric authentication systems,[7] let alone harried helpdesk workers tasked with resetting passwords.

AI's capabilities are multiplying the pressure on SecOps teams to contain threats, conduct investigations, and initiate response actions faster than ever before.

The **Ransomware** Threat

Schools and universities have long been among ransomware operators' preferred targets. It's well known that they hold large volumes of personally identifiable information (PII), student health records, financial data, and in the case of research universities, invaluable intellectual property.

When security teams have limited visibility across networks, bad actors can establish persistent access long enough to distribute malware widely, often completing lateral movement before a full investigation can even begin.

Unmanaged devices (including student-owned devices) allow threat actors to gain a foothold inside the environment without detection, while unsegmented networks permit lateral movement. Because districts face massive public scrutiny if schools are forced to close due to IT system outages, prolonged disruption increases pressure to pay ransoms. Across all sectors experiencing ransomware attacks, education had the second-highest propensity-to-pay in 2024.[8]

Typical ransomware attack sequence:

01

Lateral Movement:

Attackers quickly compromise Active Directory to gain additional end-user and administrator credentials, then quietly move across servers, cloud databases, and other data repositories. Ransomware operators often look for backups and snapshots to thwart recovery efforts.

02

Exfiltration:

The attackers exfiltrate sensitive data to a remote location, enabling them to threaten victims with its disclosure even if recovery is successful.

03

Encryption:

Threat actors leverage domain controllers or IT management tools to distribute the ransomware payload across the environment, encrypting data and taking down critical systems as they go.

Ransomware: Real-World Impact

Threat researchers have documented 180 ransomware incidents between Q1 and Q3 of 2025, though only 63 of these have thus far been confirmed by the victims. The average ransom demanded was $444,400, with threat actor groups Interlock, Fog, Qilin, SafePay, and Medusa claiming credit for the largest number of attacks.[9]

Among these, an attack on the Cherokee County School District in March 2025 was the largest in scale, with more than 46,000 people impacted. The district's systems were offline for over a week, and social security numbers, passport numbers, financial information, and personal health information (PHI) were included in the 624 GB of data allegedly stolen—an impact consistent with delayed detection and response.[10] Interlock claimed responsibility for the breach. Interlock has launched at least eight successful ransomware attacks on school districts this year, typically using sophisticated social engineering tactics that involve tricking end users into downloading a malicious payload onto their devices. [11]

Districts with legacy (or no) email filtering in place are susceptible to these attacks, while those that don't enforce conditional access policies are vulnerable to session hijacking. Insufficient segmentation between systems containing student information and those with employee, financial, and administrative information also enables this type of attack to succeed.

Vulnerability Exploits

Security teams in K-12 and higher education are tasked with protecting sprawling attack surfaces, a challenge that's been amplified with widespread shadow AI and unmanaged application use. Teachers often download unauthorized AI tools, creating risk, and there's limited oversight of this behavior in most schools. Faculty-created websites may have exposed directories or weaknesses in authentication systems. Many are abandoned at the semester's end, leaving them unmaintained and, eventually, running past-end-of-life software.

The larger the attack surface, the more difficult it is to find and fix software flaws. Many educational institutions operate a mixture of legacy on-premises systems and newer cloud solutions, making visibility difficult. Administrators tend to resist the downtime that patching requires, especially when it has to be balanced with teaching schedules and limited maintenance windows. Threat researchers have observed that 35% of successful ransomware attacks involve the exploitation of known software vulnerabilities, making this one of the top causes of data breaches in education.[12]

Vulnerability Exploits: Real-World Impact

The Oracle E-Business Suite (EBS) is widely used for back-office management, finances, and procurement in higher ed. Over the course of 2025, a zero-day vulnerability into the platform opened a back door into the Ivy League, with Harvard, Dartmouth, and the University of Pennsylvania all disclosing breaches of their EBS systems. The University of Phoenix was also impacted, and the Cl0p extortion group has claimed responsibility for the attacks, publishing what it claims is confidential data from the schools on its leak site. [13]

Universities often rely on aging enterprise resource planning (ERP) systems but lack the resources to maintain them. EBS, in particular, leaves a blind spot for security operations teams, since logs are not normalized and signals are difficult to correlate with activity taking place elsewhere in the environment. The result is that highly privileged EBS accounts become high-value targets.

Exploiting an Unpatched Vulnerability

Initial Access:

Hackers gain access to a self-checkout kiosk in a school library, targeting a known but unpatched software vulnerability.

Establishing Persistence:

The attackers install a lightweight backdoor onto the kiosk, adding a script to the startup task queue to ensure it will be launched whenever the machine reboots.

While conducting reconnaissance, the attackers discover that the kiosk is on the same weakly-segmented LAN as faculty workstations, making lateral movement possible once keylogging software harvests credentials.

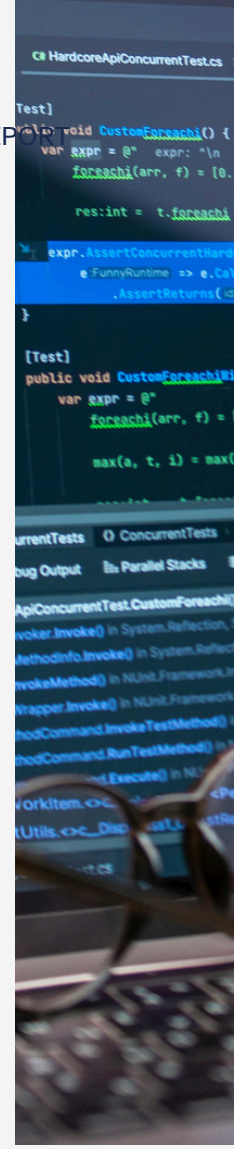
Escalation:

Once they've gained access to the faculty workstation, the attackers re-use cached tokens to reach an application server hosting SIS software.

Exfiltration:

The threat actors exfiltrate files containing sensitive information as well as student social security numbers.

Software Supply Chains Risks



Organizations across industries are vulnerable to software supply chain risks, and educational institutions are certainly no exception. Because large numbers of schools and universities depend heavily on a small set of shared EdTech vendors, it's not unusual for a single upstream compromise to cascade across thousands of educational institutions. It's challenging for educational institutions to assess the strength of a vendor's security controls, especially in a sector where SaaS businesses often grow faster than their security programs. SecOps teams rarely have visibility into or control over third-party apps. Many schools also overlook the risks inherent in student-facing systems (such as homework portals, cafeteria card systems, and transit apps), even though they're integrated with core organizational applications.

Real-World Impact

The PowerSchool data breach, which took place in December 2024, perfectly exemplifies the downstream cascade of consequences from a breach. PowerSchool's SaaS platform is used by more than 18,000 school districts to support over 60 million students around the world. Attackers breached a central PowerSchool database containing a wealth of student and staff data. PowerSchool reportedly paid the attackers $2.85 million bitcoin to have them delete the stolen data. Despite this, the threat actors have continued to send extortion emails including samples of the stolen data to schools since the incident. Investigations have shown that the initial attack vector was credential compromise, and that the attackers then leveraged a legitimate IT maintenance tool to conceal their activities within the network. [14]

Why Educational Institutions Need AI-Driven SecOps

The incidents described above are diverse, yet they represent only a small fraction of the threats that security teams in K-12 and higher education have to confront on a daily basis. What links them together is that these attacks all succeeded because of coverage and visibility gaps that allowed threat actors to achieve their objectives before defenders could respond.

Lean education sector SecOps teams must harness AI's power as a force multiplier if they are to successfully block ransomware before it can spread or detect threats before valuable data can be exfiltrated. AI can do what human security analysts can't do fast enough or at scale—reconcile access logs across Google Workspace and Azure AD, correlate SIS login anomalies with activities taking place on endpoints, and surface actionable signals before damage is done. This means that AI can level up small teams so that they can handle the scale, speed, and complexity of today's threat landscape.

Key Capabilities that Improve Outcomes

Speed and accuracy make it possible for an AI-native security operations center (SOC) platform to respond at machine speed. Automated threat triage cuts through the noise, automatically handling 90% of Level 1 and 2 alerts, so that lean teams can focus on what matters. Context-aware detections can flag what's truly suspicious in an individual environment, even if that environment incorporates legacy systems, devices that provide only limited telemetry (like student Chromebooks), or multiple unmonitored applications.

When AI is trained on real-world threat data that's specific to the education sector, **false positives and alert fatigue are minimized.** Using live incident data and analyst input in feedback loops enables the platform to adapt as the threat landscape evolves, so that it becomes smarter every day. This way, detections will be tailored to the specific ways in which attackers are exploiting flat networks to move laterally, for example, or deleting logs to conceal evidence of their presence.

Seamless integrations are key for ensuring that the organization will continue to get value from its existing security stack. Without data silos, it's possible to attain full visibility—even across complex hybrid environments that include a mix of EdTech SaaS apps, legacy systems, and student-owned devices. This translates into unified protection.

A **holistic platform approach** improves performance consistency while reducing maintenance overhead and costs. If the AI SOC platform includes modules that replace multiple point solutions, it will eliminate data silos, improve response accuracy, and make tuning and maintenance easier. Such holistic visibility can help security teams fill in the gaps when telemetry is sparse.

Why AI-Native?

AI-native means that AI capabilities aren't just plugged into the platform (that is, calling a third-party LLM tool like ChatGPT), but instead the entire platform was built around AI from the ground up. A purpose-built AI engine performs detection, prioritization, and investigation, and can recommend or initiate response actions. This means that there are no external API calls, which translates into low latency. Low latency is especially important for rapid response across networks where bandwidth is limited or variable. AI-driven detection and prioritization can separate true signals from noise, even in complex hybrid environments.

Checklist: What to Look for in an AI-Native SecOps Platform

- ☑ Ensure that the platform can ingest logs from Google Workspace, Azure AD, SIS and LMS solutions, and legacy apps and servers with no normalization delays
- ☑ Make sure that the solution can seamlessly correlate signals across these diverse systems to rapidly identify compromised accounts, lateral movement, or abnormal data access
- ☑ Look for a system that supports rapid containment even in bandwidth-constrained environments
- ☑ Verify that response logic is deterministic and explainable, so that the technology can be used in highly-regulated environments subject to legal privacy protections
- ☑ Require capabilities like AI-driven investigation, case summarization, and response playbook initiation that can accelerate containment to keep ransomware from spreading
- ☑ Look for a vendor who can help you fill in coverage gaps, especially on holidays, nights, and weekends—when many ransomware attacks are launched

Conclusion

In the coming months and years, attackers will further advance their adoption of AI, increasing the speed and autonomy with which they operate. Not only will phishing emails become hyper-personalized, but social engineering will turn into a continuous automated operation, with self-modifying lures that adapt in real time, based on what's successful. AI agents will conduct reconnaissance, string together exploits, move laterally, and exfiltrate data without human input, outpacing security teams that rely on manual investigations and after-the-fact response. Bots will be able to enumerate flat networks, hunt for exposed vulnerabilities, and auto-test stolen credentials against EdTech apps at scale. The end result is that persistent access will become even easier for bad actors to obtain, and the time window that defenders have to respond—before harm is done—will shrink.

To get ahead of tomorrow's threats, security operations teams need an autonomous, AI-driven, all-in-one platform backed by around-the-clock expert human support. This will enable continuous monitoring of the complex distributed IT ecosystems that learners rely on. An AI-native SecOps platform delivers the response speed, visibility, and investigative depth that schools and universities require to keep pace with increasingly automated threats.

AI-Native Protection. Human Support. Real Peace of Mind.

AgileBlue combines 24/7 AI-powered threat protection with a dedicated SOC team and proactive support that never goes dark.

It's why 96% of our clients stay with us—because we don't just detect threats, we act on them.

CONTACT US

WATCH A CLIENT TESTIMONIAL

References

[1] The Record, "Uvalde school district says ransomware attack forcing closure until Thursday," September 2025.

[2] Uvalde Hesperian, "Community Advocate Organizes Feeding for Uvalde School Kids," September 2025.

[3] CISA, Cybersecurity Best Practices: Cybersecurity for K-12 Education.

[4] Check Point Research, "Cyber Attacks Surge Against Education Sector Ahead of Back-to-School Season," August 2025.

[5] Sophos, The State of Ransomware in Education 2025.

[6] Microsoft, Microsoft Digital Defense Report 2025.

[7] University of Waterloo, Waterloo News: How secure are voice authentication systems, really?, June 2023.

[8] Sophos, The State of Ransomware in Education 2025.

[9] Comparitech, "Education Ransomware Roundup: Q1-Q3 stats on attacks, ransoms, and data breaches," October 2025.

[10] Comparitech, "South Carolina school district notifies 46,000 of data breach involving SSNs, financial info, and health data," September 2025.

[11] CISA, Cybersecurity Advisory, #StopRansomware: Interlock, July 2025.

[12] Sophos, The State of Ransomware in Education 2025.

[13] The Record, "University of Phoenix says 'numerous individuals' impacted by Oracle EBS breach," December 2025.

[14] TechTarget, "PowerSchool data breach: Explaining how it happened," May 2025.