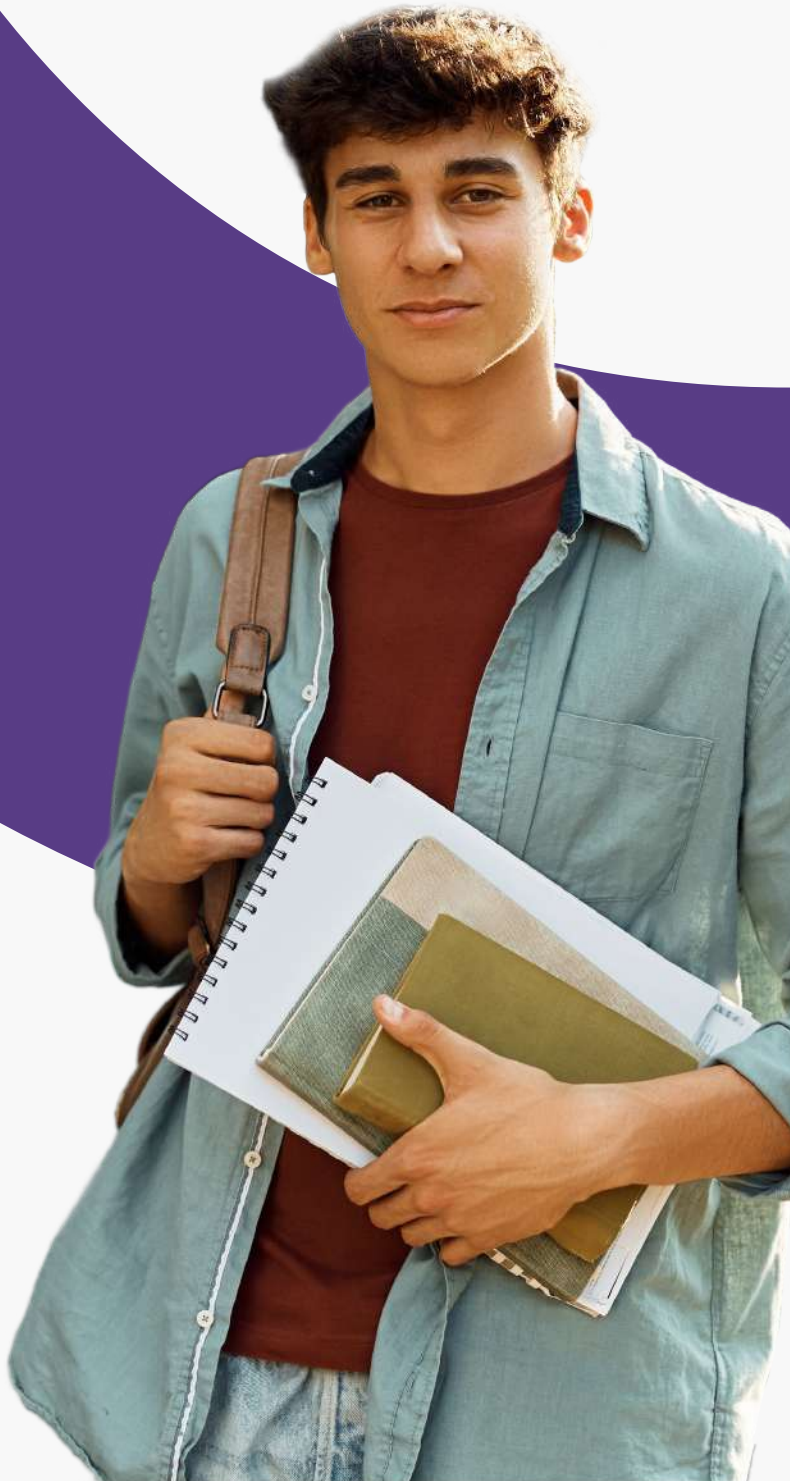
acre Security



WHITEPAPER

# The 2026 Education Security Landscape: Integrating Cyber, Physical, and Human Defense

# Table of Contents

# Introduction

## The New School Security Reality 2026

School security in 2026 stands at a critical inflection point. Cyberattacks are shutting down classrooms for weeks. Current AI surveillance tools promise safety but deliver controversy. And even the most tragic events often come down to the simplest failures — a door that wouldn't lock, a system that didn't talk to another.

Despite spending billions on security, schools still face the same core problem: fragmentation. Each tool solves one issue, but none of them speak the same language. When physical, digital, and human systems remain disconnected, schools are left with blind spots that attackers — digital or physical — exploit.

The result? A paradox of progress. We've never had more technology in schools — yet our students have never been more digitally connected—and more reliant on systems that must work together.

Acre Security believes the solution starts with one unifying idea: Security starts with the door — and the identity behind it.

By connecting physical and digital access, from doors and visitor management systems to identity credentials and AI-driven alerts, schools can finally move from reacting to threats to preventing them. It's a shift from "keep bad out" to "let the right people in".

Because the future of school safety isn't about more technology. It's about the right layers, working together — seamlessly, intelligently, and humanely.

- Schools under pressure (digitally): **82% of K-12s reported cyber incidents in the last 18 months**; lost days and six-figure daily costs turn IT failures into campus safety issues.
- **Security starts at the door: 97% restrict entry; 93% use cameras**—yet gaps persist when identity and doors aren't linked.
- **AI is assistive, not magic**: Districts are spending big, but without verified identity + access data, AI creates noise and risk.
- **Identity is the new perimeter**: Unifying physical access with digital credentials closes the front-door and back-door.
- Integrate before you innovate: **Connect doors, identity, cameras, and HR to automate onboarding/offboarding and emergency actions**.
- Measure what matters: Uptime, false-positive reduction, time-to-lockdown, and maintenance SLAs beat gadget counts.
- Acre's edge: Proven uptime, millions of transactions/day, identity-first architecture, and automation that reduces manual load.

**82%**
of K-12s reported cyber incidents in the last 18 months.

Security starts at the door:
**97%**
restrict entry;
**93%**
use cameras

**AI**
is assistive, not magic.

Chapter 1:

# The Digital Deluge – Cyberattacks and Their Physical Consequences

In the last 18 months, U.S. schools have faced an unprecedented wave of cyber incidents. According to the Center for Internet Security, 82% of K–12 institutions reported at least one cyberattack between July 2023 and December 2024 — totaling nearly 9,300 confirmed incidents across roughly 5,000 districts. These weren't minor disruptions: ransomware, data breaches, phishing campaigns, and denial-of-service attacks all contributed to halting learning across the country.

The U.S. Government Accountability Office found that school cyberattacks lead to an average of 12.6 lost school days per incident — up from just 8.7 in 2021 — and can cost districts more than $500,000 per day in recovery, remediation, and downtime. Recovery can take two to nine months, leaving not just IT systems but entire communities scrambling to resume normal operations.

**The Hidden Truth: Under-reporting**

Despite the concerning figures, the true scale of attacks on schools may be far higher. Many districts quietly pay ransoms or delay disclosure to avoid reputational damage, insurance complications, or compliance penalties.

A joint investigation by Wired and The 74 found that over 300 school cyberattacks in the U.S. went unpublicized or were revealed only months later, often handled behind the scenes by lawyers, insurers, and breach-coaches operating under attorney-client privilege. The report suggests that the 9,300 confirmed incidents may represent only the visible portion of a much larger crisis.

Beyond academics, these attacks cripple essential services — transportation, cafeteria systems, payroll, and emergency communication channels — creating cascading effects that stretch far beyond the network. Education has now overtaken healthcare and government as the top-targeted sector for ransomware in the U.S.

A 2023 survey by Sophos found that 80% of K-12 organizations and 79% of higher-education institutions reported ransomware attacks in the past year. Industry commentary now points to education as one of the most-targeted sectors for ransomware, often surpassing sectors like government and healthcare. Meanwhile, cyber-insurance providers are tightening terms for school districts, demanding stronger controls — from multi-factor authentication to regular audits — as premiums climb and underwriting becomes more rigorous.

CASE STUDY:

### PowerSchool Breach (2024)

In late 2024, hackers infiltrated PowerSchool, a leading student-information system serving more than 60 million students globally. The attackers stole contact information, birthdates, medical alerts, and Social Security numbers, and later demanded ransom payments to prevent data leaks. Multiple districts reported follow-up extortion attempts, where criminals emailed schools directly, threatening to publish student records if they refused to pay.

This breach highlighted the growing supply-chain risk in education: one vendor compromise can expose thousands of schools simultaneously — turning a digital vulnerability into a nationwide challenge.

**When Digital Threats Become Physical Risks**

The boundary between cyber and physical security has blurred. In early 2026, a Google Classroom phishing campaign demonstrated how online threats can translate into real-world danger. Attackers impersonated teachers inside the platform, sending malicious links to students. Those links harvested login credentials, unlocking class schedules, personal details, and in some cases, GPS-enabled device data.

This pattern is increasingly common. A single compromised account can disable surveillance cameras, open electronic locks, or trigger a cascade of false alerts. As schools digitize more infrastructure — from doors to bus routes — every endpoint becomes a potential entry point.

**A Fragmented Frontline**

Yet despite the clear escalation, most schools still manage security through disconnected systems: one vendor for cybersecurity, another for physical access, a third for visitor management. That fragmentation

"Phishing isn't just about stealing passwords anymore — it's a blueprint for real-world targeting"

"A predator posing as a teacher can use those same tactics to pinpoint a child's location or infiltrate a school's access system. AI-powered security can create a digital perimeter — one that alerts administrators before a digital threat becomes a physical danger."

**Jeff Groom**
Director of AI Engineering at Acre Security

leaves gaps that attackers exploit — whether it's a weak password or a propped-open door.

Acre Security's work with education clients shows that integrated access control can close those gaps. When physical door systems, identity databases, and cloud monitoring platforms communicate, schools gain early-warning intelligence — like detecting an unfamiliar login pattern moments before a physical breach attempt.

Acre in practice. With 99.9% uptime under our SaaS terms, Acre processes millions of secure transactions daily across education clients—surfacing patterns others miss (credential sharing, anomalous after-hours access, repeated failed badge attempts). These signals drive early warnings instead of forensic excuses.

Why it matters to people. When ransomware hits, it's not just servers—lunch payments stall, special-ed services pause, buses lose tracking, learning stops. Integrating doors, identity, and cloud monitoring helps districts prevent digital incidents from becoming campus incidents.

"Every threat leaves a signal,"

"The challenge isn't the lack of data — it's the lack of connection."

**Jeff Groom**
Director of AI Engineering at Acre Security

Chapter 2:

# Back to Basics: School Security Starts with the Door

When discussions around school safety turn to ransomware, AI, or data leaks, it's easy to forget the most effective barrier against danger is still the one that can be locked.

According to the U.S. Department of Education's Indicators of School Crime and Safety 2023 report, 97% of public schools restrict access to their buildings during class hours, and nearly all require visitor sign-ins and ID badges. Ninety-three percent use security cameras for real-time monitoring — up from just 61% in 2010. These numbers show how far schools have come in securing their perimeters, but they also reveal a critical imbalance: adoption has outpaced integration.

Acre Security's perspective: "The door is still where every safety strategy begins. When doors, credentials, and alerts connect through a single identity framework, schools can move from manual reaction to automated prevention."

**The Weak Link in a Strong Chain**

Even with billions invested in safety infrastructure, breakdowns often occur at the most basic level. The 2022 Uvalde school tragedy — where an unlocked door allowed an attacker to enter — remains a sobering reminder that major incidents often begin with basic mechanical failures.

Meanwhile, an investigation by The Wall Street Journal found that U.S. schools have spent over $100 million on so-called "bulletproof" window films — products marketed to stop gunfire but which manufacturers confirm cannot repel bullets. In practice, these films may delay entry by a few seconds — critical time — but they are no substitute for reliable doors, locks, and integrated alert systems.

**Acre Insight: "The most advanced technology won't matter if the fundamentals fail. A door that's monitored, automated, and identity-linked outperforms any temporary or single-layer solutions."**

### Why the Door Still Matters

The most effective school security strategies don't rely on any single layer — they build from the door outward. A locked, monitored entry point, supported by verified identity and automated alerts, forms the foundation for everything else.

**97%** of schools already control door access.

**93%** use cameras for verification and response.

But only a small fraction link these systems with digital identity platforms such as Entra ID or HR databases — meaning a former employee's credential could still unlock a classroom.

Acre's cloud platform addresses this gap. Its integration with Microsoft Entra ID allows schools to automate onboarding and off-boarding — eliminating manual credential management and reducing errors that compromise security. These automated workflows also enhance data integrity, ensuring access rights always match current roles.

"When your doors talk to your data," says an Acre Security engineer, "you gain a sixth sense for risk. It's not about closing schools off — it's about ensuring the right people are always let in."

### Measured Performance and Reliability

While school budgets are tightening, reliability remains non-negotiable. Acre's cloud access platform maintains a 99.9% uptime guarantee under its SaaS terms — a critical benchmark for schools that depend on 24/7 access visibility.

Customer satisfaction reflects that dependability: Acre's education clients rate its service at 4.74 out of 5 on post-resolution feedback, indicating both the strength of its technology and the responsiveness of its support teams.

**From Hardware to Harmony**

This isn't a call for more gadgets — it's a call for cohesion. Acre's connected-access architecture enables schools to:

- Link doors, cameras, and visitor systems through one cloud-based identity backbone.
- Automate emergency responses — instant lockdowns, real-time alerts to first responders, and immediate credential revocation.
- Predict maintenance issues before they cause downtime, improving operational resilience.

By treating every door as both a physical and digital sensor, schools can unify their first line of defense. In a world where a cyberattack can open a real door, that unity isn't just smart — it's essential.

School security starts with the door. Nearly every school locks and screens visitors—yet incidents expose the same basic failures: a door that doesn't latch, a credential that wasn't revoked, a gate propped open.

Close the loop with automation:

- Health checks flag doors held/forced open and issue real-time alerts (email/text).
- Maintenance integration creates auto work orders and verifies repair.
- Identity sync with HR/Entra ID auto-revokes access on role changes.

**The outcome:** fewer blind spots, faster fixes, and less manual chasing.

The next evolution isn't about more technology — it's about smarter intelligence. The following chapter explores how AI, when grounded in physical reality, can strengthen human judgment rather than replace it.

Chapter 3:

# The AI Gold Rush — Promise, Progress, and Proof

AI has become education's latest frontier. From predictive analytics to AI-driven cameras, districts are racing to implement smart technologies that promise safer, faster responses to threats. But amid the excitement, one truth remains: AI is only as effective as the systems it's built upon.

"Current AI surveillance tools promise greater safety but continue to spark debate"

"Without reliable data from physical systems—doors, access logs, identity credentials—AI is guessing. You can't automate trust."

**Jeff Groom**
Director of AI Engineering at Acre Security

### Current AI Tools, Real-World Results

Since 2018, at least 65 U.S. school districts have bought or tested AI gun-detection systems, spending more than $45 million on deployments across 30-plus states. These tools, which use machine-learning to identify weapons from camera feeds, illustrate the speed of adoption—and the uneven results.

In one case, a knife passed undetected through an AI scanner at a New York high school, leading the district to remove the system entirely. The lesson: without reliable data from doors, credentials, and verified identity systems, "intelligent" sensors can misfire.

### Accuracy, Equity and Backlash

Facial-recognition systems highlight the same pattern. Independent testing by the U.S. National Institute of Standards and Technology (NIST) found false-positive rates that were 10× to 100× higher for certain demographic groups in many commercial algorithms.

Following these findings, New York State banned K-12 facial recognition in 2023, citing persistent bias and privacy concerns.

These controversies underscore a growing consensus: AI can help detect anomalies, but unchecked surveillance introduces ethical and operational risk—especially in schools.

### From Reaction to Prediction

The real opportunity for AI lies not in surveillance, but in orchestration—using data from existing physical and digital systems to predict and prevent incidents before they occur.

- A badge scanned after hours.
- A door held open too long.
- A pattern of failed logins at a lab entrance.

Individually, these are routine events; combined, they form a threat signature. Acre Security is developing an AI layer that correlates physical-access and identity data to generate actionable, privacy-safe insights—enhancing human oversight rather than replacing it.


### The Data Dilemma

Every new layer of AI security generates new data — from biometric scans and behavioral logs to door events and real-time location trails. These datasets hold immense operational value but also create a larger attack surface.

A 2024 analysis by Comparitech found that U.S. schools and colleges have experienced over 3,700 data breaches since 2005, exposing more than 37 million records. Nearly 1,000 of those breaches occurred in 2023 alone — a record year for education-sector data compromise.

Globally, education accounted for 17% of all confirmed data breaches and 14% of confirmed data disclosures, according to the Verizon Data Breach Investigations Report (DBIR) 2024, underscoring just how vulnerable the sector has become.

"Every AI feature brings promise and pressure," says an Acre Security advisor. "The same data that powers safety can, if mishandled, create new risks for the very people it's meant to protect."

As schools collect more personal data in the name of safety, they also assume greater liability. The next phase of AI in education must focus not just on innovation, but on data governance, identity hygiene, and ethical design — the foundations of true digital trust.

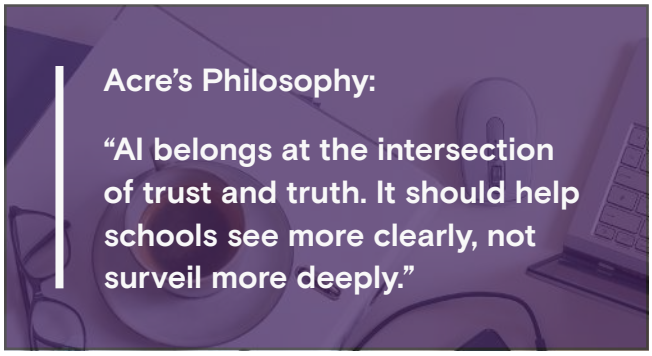
### Integrating AI with Physical Foundations

Acre Security's advantage lies in its starting point: verified identity and access. Its cloud platform already unifies doors, credentials, and building telemetry, allowing AI to operate on clean, contextualized data rather than fragmented signals.

This approach enables:

- Anomaly detection — flagging unusual access patterns before they escalate.
- Policy automation — adjusting permissions dynamically based on role, risk level, or behavior.
- Predictive maintenance — identifying failing locks or sensors before they disrupt operations.

When AI is trained on data derived from physical verification — rather than unverified digital inputs — it moves from speculation to signal. That's the key to building systems that anticipate threats rather than react to them.




**Quiet Confidence in an Overheated Market**

The global market for AI in education is forecast to reach $2.5 billion by 2027. Yet many vendors continue to chase the latest algorithmic trend rather than addressing the fundamentals — integration, privacy, and identity.

Acre's approach remains deliberately restrained. It favors clarity over hype, ensuring that each new capability is tested against a single standard: does it make schools measurably safer?

"AI isn't about more alerts — it's about better awareness"

"Schools need visibility they can trust, not complexity they can't control."

**Jeff Groom**
Director of AI Engineering at Acre Security

What wins in 2026: AI that correlates verified door/identity events (after-hours badge + held-open door + failed logins) to raise actionable, low-noise alerts. That's assistive intelligence—not ambient surveillance.

The next chapter explores data sharing and transparency — how schools can collaborate with insurers, technology partners, and law enforcement while maintaining public trust and safeguarding student privacy.

When tech overpromises:

A district that spent $4M on AI scanning later removed it after a weapon slipped through. The takeaway: evaluate outcomes, not demonstrations. Pair AI with controlled entry + identity or you're automating false confidence.

Chapter 4:

# Data Sharing and Transparency — The Connected Ecosystem

In modern schools, security doesn't end at locked doors or threat detection—it extends into the flow of data between systems, vendors, insurers, and agencies. But while information sharing can enable faster response and smarter prevention, it also raises important considerations around privacy, compliance, and trust.

### Sharing Isn't Simple

Federal law like the Family Educational Rights and Privacy Act (FERPA) restricts how schools share student education records and mandates that third-party ed-tech vendors meet strict criteria when handling that data.

For example, schools transmitting student records to cloud vendors must ensure the vendor acts as a "school official," retains access controls, and uses data only for educational purposes. Despite this, many districts lack clarity. A report by Public Interest Privacy highlights that the "school official exception" was broadened in 2008 to allow data sharing with vendors under unclear terms—creating risk of misuse and eroding community trust.

### A Growing Risk: Vendor Ecosystems & Data Access

As schools rely on 100+ ed-tech and security vendors, the question isn't just "who holds the data" but "who controls the flow." The National Student Data Privacy Association (NSDPA) points out that many schools still manage vendor access with spreadsheets, lacking real contract tracking, breach notification protocols or standardized audits.

Where vendors share building access, identity systems and data analytics, schools must ensure agreements cover: data ownership, security requirements, and deletion policies upon contract termination.

### Insurance, Compliance & Incident Transparency

Cyber-insurance providers increasingly require schools to demonstrate transparency, documented vendor controls, and timely incident reporting. The UK-based insurer Zurich Insurance Group notes that multi-academy trusts must now show evidence of audits and vendor due-diligence to qualify for tailored cyber cover.

In the U.S., while statute differs state-to-state, schools are seeing increased pressure from both insurers and regulators to publish breach-response plans, vendor oversight frameworks and data-sharing logs—all part of the "new normal" of school safety governance.

### Balancing Transparency & Trust

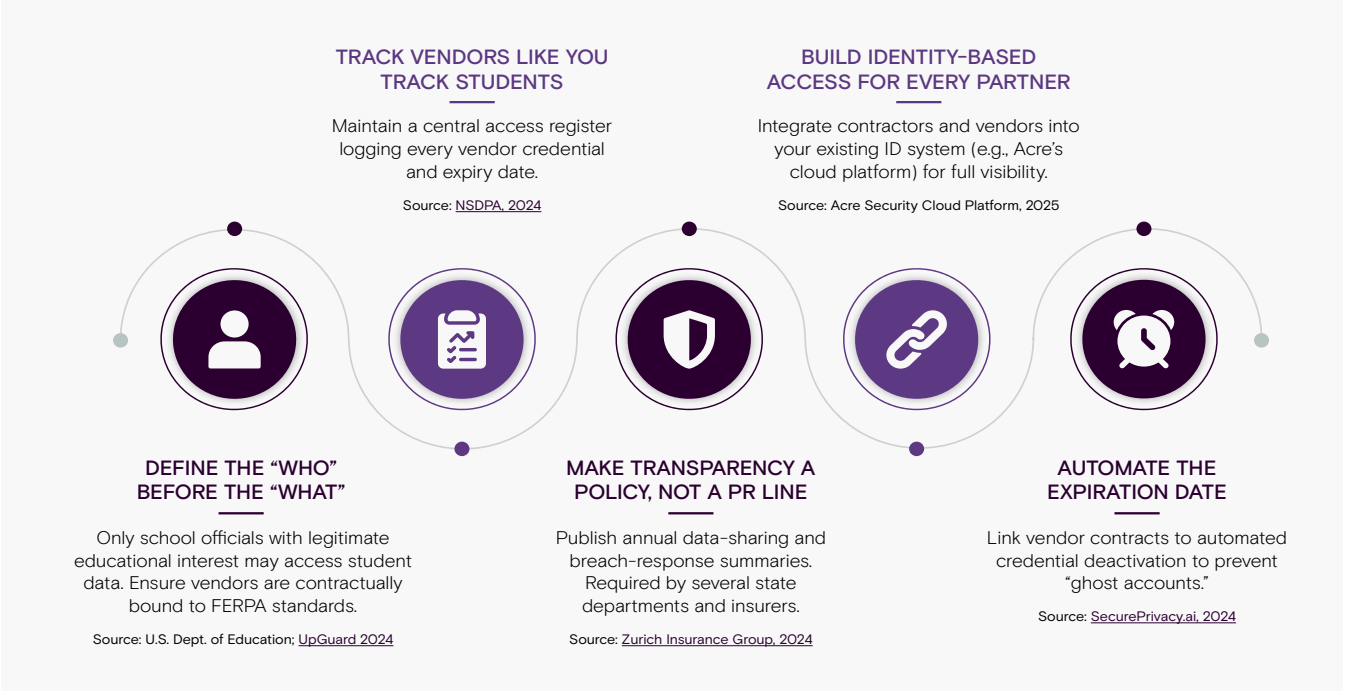
Parents, students and communities expect schools to keep them safe and respect privacy. That means data-sharing policies must be open, understandable and defensible. The U.S. Department of Education's website for ed-tech vendors emphasizes that every contract must clearly define how student data will be used and who has access.

When breaches happen—or when vendors misuse data—the reputational fallout is real. Schools aren't just repairing networks, they're repairing trust.

### Acre's Role: Bridging Access, Identity & Governance

Acre Security connects the dots by providing a unified access and identity backbone that schools can link to vendor systems, audit logs and response workflows.

- When a vendor contract is signed, the school can attach the vendor's credentials in the same identity directory used for staff and students—ensuring every badge, login or API call traces back to a verified identity.
- When an incident triggers, system logs show which credential was used, what system was accessed, and which door was opened—enabling rapid, transparent response.
- With policy-driven automation, schools can disable "vendor" profiles the moment contracts expire or privileges change, reducing the risk of ghost access points.




The takeaway is consistent across research and policy: controlling the data chain strengthens the entire security chain.

In the final chapter, we'll tie all these threads together—showing how schools can adopt a layered approach to security, centered on identity, that protects both safety and privacy in 2026 and beyond.

Chapter 5:

# Building the Future of School Security — Identity as the New Perimeter

### From Chaos to Clarity

The education sector sits at the intersection of two converging challenges: relentless cyberattacks and reactive, fragmented security investments. Over the past 18 months, 82% of K-12 schools reported at least one cyber incident, according to the Center for Internet Security. Districts have poured millions into new safety technologies—AI cameras, ransomware defense, even "bulletproof" window films—yet the results remain uneven.

The challenge isn't a lack of innovation; it's a lack of integration. Schools continue to treat cybersecurity, physical access, and vendor oversight as separate domains when in reality, they're parts of the same system.

"Identity is the new perimeter"

"The only way to secure a borderless network is to know exactly who is on the inside."

**Jeff Groom**
Director of AI Engineering at Acre Security

### The Identity-First Model

Across industries, the security paradigm is shifting from "keep the bad out" to "let the right people in." According to ISACA's Identity as the New Security Perimeter (2023), modern protection depends less on firewalls and more on verifying who is requesting access, from where, and why.

For education, this model translates directly into safer campuses. A unified identity system connects physical access (doors, cameras, visitor logs) with digital authentication (accounts, cloud apps, HR databases). When a student badge, staff login, and contractor credential share one framework, anomalies become visible before they turn into incidents.

Microsoft's Education division describes this transition as "real-time risk assessment—safeguarding against compromised identities and unauthorized attacks".

### Why Identity Matters More than Ever

Schools are dynamic ecosystems—students transfer, staff rotate, vendors come and go. Each change adds risk if identity access isn't updated.

Without a unified system:

- Departed staff may retain active credentials.
- Vendors may keep expired API keys.
- Students may reuse unsecured devices.

Acre's integrations with Microsoft Entra ID and identity-governance frameworks automate these transitions—provisioning and de-provisioning access in real-time. Microsoft calls this "a simple, secure, and efficient technology environment that maximizes learning while protecting schools".

### From Compliance to Confidence

Identity-based access doesn't just enhance safety—it simplifies compliance. FERPA, COPPA, and state-level privacy acts all revolve around who can see what data and when. By embedding these permissions directly into the identity layer, schools can satisfy audits automatically.

According to ISACA and other industry research, organizations with strong identity-governance frameworks report significantly lower risk of insider incidents and faster response times. For districts under scrutiny from parents, insurers, and regulators, that transparency builds trust where fear once lived.

"In education, identity isn't just a credential—it's the connective tissue of security"

"It unites the physical and the digital, the human and the automated."

**Jeff Groom**
Director of AI Engineering at Acre Security

### The Road Ahead

The next frontier isn't about adding more sensors or AI—it's about connecting what schools already have.

Acre Security's roadmap focuses on three commitments:

1. Integration before innovation — ensuring every tool adds measurable value to the existing infrastructure.
2. Transparency as a standard — making data access and usage auditable by default.
3. AI that augments human judgment — turning identity data into insight, not surveillance.

How to measure success:

| | | |
|---|---|---|
| 01 |  | Time-to-lockdown during drills/ incidents (target: ↓ by 40–60%). |
| 02 |  | False-positive rate on alerts (target: ↓ materially quarter-on-quarter). |
| 03 |  | Mean time to repair for door faults (target: auto-created work orders; ↓ to <24h). |
| 04 |  | De-provision lag after HR change (target: 0 mins; fully automated). |
| 05 |  | Uptime of access platform (target: ≥99.9%). |

These convert strategy into board-level outcomes.

In this model, safety becomes systemic. Schools evolve from reactive targets to resilient ecosystems—where access, identity, and accountability are inseparable.

"Effective school security isn't about more technology—it's about connected trust.

"Acre Security helps schools build that trust—one identity, one door, one data point at a time."

# Appendix


01 82% of K-12 schools recently experienced a cyber incident | K-12 Dive
https://www.k12dive.com/news/k-12-schools-experienced-cyber-incident-cis/741915/

02 Ransomware attacks in education jump 23% year over year | K-12 Dive
https://www.k12dive.com/news/ransomware-attacks-education-jump-23-percent-h1-2025/753483/

03 US school districts facing extortion attempt after hack, software provider says | Reuters
https://www.reuters.com/world/us/us-school-districts-facing-extortion-attempt-after-hack-software-provider-says-2025-05-07/

04 Does Facial Recognition Belong in Schools? It Depends Who You Ask | EdSurge News
https://www.edsurge.com/news/2024-12-05-does-facial-recognition-belong-in-schools-it-depends-who-you-ask

05 Will Facial Recognition Technology Make Schools Safer? - Timothy Dimoff
https://timothydimoff.com/2024/09/10/facial-recognition-technology-make-schools-safer/

06 DIGITAL SURVEILLANCE: “WILD WEST” - CAUTION URGED ON FACIAL RECOGNITION ROLLOUT IN US SCHOOLS - Sight Magazine
https://sightmagazine.com.au/features/digital-surveillance-wild-west-caution-urged-on-facial-recognition-rollout-in-us-schools/

07 FEATURE-Can tech protect US schools from mass shootings? | Reuters
https://www.reuters.com/article/business/media-telecom/feature-can-tech-protect-us-schools-from-mass-shootings-idUSL8N3789I5/

08 Records show repeated issues with Robb Elementary doors before massacre, CNN reports
https://www.ksat.com/news/local/2025/09/05/records-show-repeated-issues-with-robb-elementary-doors-before-massacre-cnn-reports/

09 States Emphasize School Violence Prevention, Not Just Security
https://www.edweek.org/leadership/states-emphasize-school-violence-prevention-not-just-security/2025/02

acre Security

## Let’s Build Safer Schools - Together.

Talk to our team here.

Press inquiries? Reach us at press@acresecurity.com