halcyon

Data Sheet

Ransomware is Targeting K-12 Schools

For superintendents, administrators, CISOs, and IT leaders in education, another day without purpose-built ransomware protection puts your district at risk.

With AI-enhanced tactics, supply chain compromises, and multi-extortion schemes, ransomware operators have not stopped targeting the public education sector.

Why Schools are Being Attacked... and Why now?

K-12 schools accounted for 74% of all education sector ransomware incidents in 2025. Unlike private enterprises, they are often forced to protect students and staff with budgets and tools rarely matching the sophistication of modern threats.

- **Budget Constraints:** Fixed budgets, competing priorities, security often viewed as IT cost rather than a safety investment
- **Open Networks:** BYOD policies, guest access, and academic freedom requirements conflict with security controls
- **Entry Points:** Phishing and social engineering remain the primary threats, with 45% of schools reporting business email compromises.
- **High-Value Data:** Student PII, SSNs, financial aid data, employee records – Case in point: PowerSchool breach exposed 62.4M student records
- **Operational Pressure:** Cannot cancel classes, delay enrollment, or reschedule graduations; attackers exploit fixed timelines

Real Impact: When Schools Get Hit

- **PowerSchool (Dec. 2024–2025):** Credential-based breach compromised personal data of 62M individuals, including custody orders, restraining orders, and student medication records across 18,000+ schools. Despite a $2.85M ransom payment, there was secondary extortion of individual school districts.
- **Cherokee County School District, SC (March 2025):** Interlock ransomware group breached the district's network for two weeks, stealing 624 GB of data including SSNs, health records, and financial information. With 46,119 victims notified, it was the largest confirmed U.S. K-12 breach in 2025.
- **Baltimore City Public Schools (February 2025):** Cloak attack compromised SSNs, passport numbers, absenteeism records, and student maternity status across a district of 75,000+ students, affecting 31,125 people including 1,000+ students and 55% of the district's entire workforce.

2025

251+

Known attacks in 2025
(130 in U.S. alone)

2024 VS 2025

+27%

YoY increase in records breached
(3.1M in 2024 to 3.96M in 2025)

2025

$2.28M

Average recovery for K-12
(highest of any sector)

- **School District Five of Lexington and Richland Counties, SC (June 2025):** Interlock stole 1.3 TB of data including SSNs and financial records, disrupting summer classes, delaying employee paychecks, and locking staff out of accounts.
- **Madison Elementary School District 38, AZ (April 2025):** An Interlock social engineering attack exfiltrated 75 GB of data, including SSNs and financial records, prompting breach notifications to approximately 35,000 people from a single elementary district.

The Good News: Schools Can Fight Back

Immediate Actions:

- MFA everywhere: No exceptions for faculty convenience
- Backup isolation: Air-gapped, tested, recoverable
- Phishing training: Staff and faculty are primary targets to gain entry

Strategic Changes:

- Deploy purpose-built anti-ransomware: EDR isn't enough
- Segment research networks: Isolate high-value data
- Plan for operational continuity: How does a school teach without systems?

Budget Reality:

- Reframe security as safety: Board members understand safety investments
- Calculate true breach cost: Include enrollment impact, reputation damage
- Explore E-Rate and grants: Federal programs can fund security improvements

Halcyon for K-12: Enterprise-Grade Protection Without Enterprise-Scale Hiring

Detect Ransomware That Bypasses EDR

- Halcyon detects and stops, the ransomware groups targeting education orgs, in seconds, not days.

Recovery in Minutes vs Days or Weeks

- Encryption key capture enables rapid recovery vs. weeks of backup restoration, while student learning continues uninterrupted.

Augment Your Limited Staff with No Added Cost

- From alert triage and investigation to threat response and recovery, **Halcyon Ransomware Operations Center (ROC)** does the heavy lifting of ransomware detection for you, at no additional cost.

Learn more at halcyon.ai/industry/education

Request a demo to see it in action: Schedule a demo today.

"Halcyon has given us confidence that we have much greater resilience to any ransomware or exfiltration attacks."

–Jason Miller, Technology Dir., AztecSchools