Cybersecurity Solutions for K-12.

Despite a common misconception among schools and school districts that they are not on the radar of threat actors, the reality tells a different story. Schools are, in fact, **highly targeted environments** due to their wealth of data and extensive networks of system users.

A breach or disruption in these environments can have severe consequences, impacting both the safety of students and staff and the continuity of educational services. Despite these risks, many districts are forced to do a lot with a little when it comes to building and maintaining cyber resilience.

For K-12 schools, cyber incidents are so prevalent that, on average, there is more than one incident *per school day.*

Cybersecurity and Infrastructure Security Association (CISA)

81% OF DISTRICTS

81% of districts say their top concern is insufficient funding

$3.8 MILLION

The average cost to remediate a school ransomware attack ballooned to $3.76 million in 2024

491 RANSOMWARE ATTACKS

Between 2018 and July 2024, a total of 491 ransomware attacks impacted educational institutions

123K SCHOOL LUNCHES

K-12 lost 12.6 school days on average in 2023 from ransomware attacks. That downtime calculates to $548,185 per day, or about 123,744 school lunches for one day

Top Cybersecurity Threats in K-12

- Unauthorized Disclosure & Data Breach
- Phishing & Social Engineering
- Ransomware & Malware
- Denial-of-Service Attacks
- Weak Credentials
- Advanced Persistent Threats (APT)

Top Security Concerns by EdTech Leaders

- Insufficient funding
- Escalating threat sophistication
- Absence of documented processes
- Lack of a comprehensive cybersecurity strategy
- Shortage of cybersecurity expertise

How ArmorPoint Helps Secure K-12

Comprehensive solutions like ArmorPoint Managed SOC, that can easily integrate with the tools you're provided are essential to provide a secure environment that protects both student and staff data and ensures educational services continue without interruption.

With ArmorPoint Managed SOC, districts get access to:

24/7 monitoring | Direct access to SOC analysts | Data visibility and control | 365-day data retention | Unlimited data ingest | Integration Marketplace | Response & remediation | Automated alerts

FAQs

→ HOW DOES ARMORPOINT ENHANCE OUR EXISTING SECURITY TOOLS?

While many districts often have access to cybersecurity tools like CrowdStrike, Microsoft Defender, and SentinelOne at low or no cost, these tools alone may not meet the full spectrum of your security needs.

Here's how ArmorPoint enhances your existing tools:

- **Dedicated U.S.-based Support:** True 24x7x365 support to address any security concerns as they come up
- **Advanced Monitoring:** Proactive monitoring of security detections from these tools to catch threats that may be missed
- **Data Centralization:** Integration of various security tools into a single, unified dashboard, providing comprehensive visibility and control over your school's cybersecurity posture

→ WHAT SOLUTIONS DOES ARMORPOINT RECOMMEND FOR SECURING STUDENT CHROMEBOOKS?

Many school districts equip students with Google Chromebooks, which, due to their design as low-resource devices, cannot support traditional security agents.

ArmorPoint recommends network segmentation as a practical solution to protect these devices. By segregating the school network, Chromebooks remain on a separate, secure segment, reducing the risk of threats spreading to more critical network areas.

Choose ArmorPoint for unparalleled cybersecurity support tailored specifically for the unique needs education. Schedule a consultation today to get started.

armorpoint.com sales@armorpoint.com