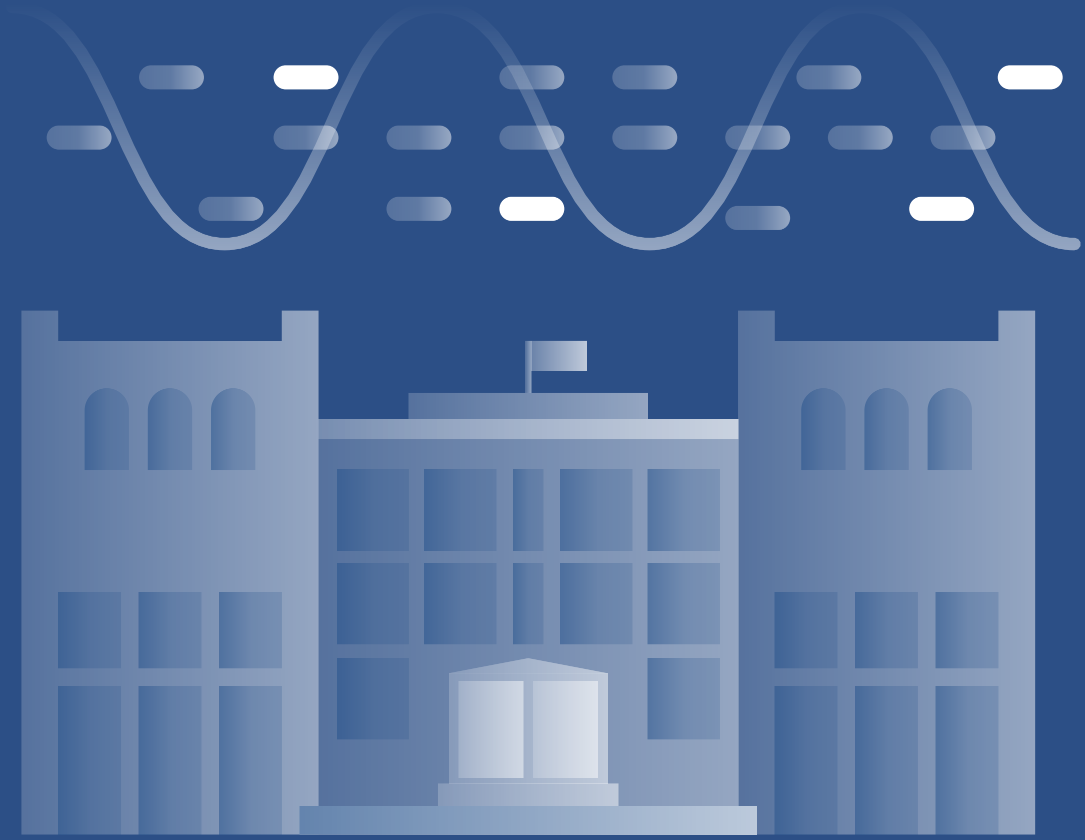
cloudcover®



Shifting From Reactive CyberSecurity to Proactive CyberSafety in Schools

How one large public school district created an efficient way to detect, analyze, and respond to network security threats with CloudCover's CyberSafety CC/B1 Platform™

Virtual learning, lack of funding contributing to staggering increase in cyberattacks in schools and districts

Cyberattacks are one of the most serious threats schools and universities face. Not only do they disrupt education and school operations, but they also affect data privacy in their ability to expose the personal information of students, parents, and staff. And they're on the rise. 2020 was a record-breaking year for publicly disclosed cybersecurity incidents in K-12 public schools, with 408 data breaches directly linked to identity theft and credit card fraud. This is an 18% increase from the same type of incidents disclosed in 2019 and averages out to more than two cyberattacks per school day (Levin, 2021).

In the world of cyberattacks, schools — public and private — are easy targets. Schools generally don't have the funds for a well-outfitted cybersecurity program and — like many industries — don't have the means to hire an IT professional specifically dedicated to these efforts. Often, the person leading these measures at a school is also the same one who's managing all aspects of a school's technology program. This confluence of factors means it's not possible to effectively manage the cybersecurity of a school's network and data security and develop ongoing training for the rest of the district.

When there isn't a proactive cybersecurity plan, it can lead to breakdowns in responsible use of technology for both staff and students. If a school community's data is left unsecured, it can lead to FERPA (Family Educational Rights and Privacy Acts) violations. Schools and districts might limit access to and use of cloud-based software — software that makes it easy for teachers and staff to store and share their students' personally identifiable information — as they may not feel comfortable with the risk. Weak firewalls, unsecured users and unmonitored networks are additional consequences.

The lack of cybersecurity also has more far-reaching, external risk. If a breach were to happen that affected a school's or district's data privacy, there might be school closures, lawsuits, and millions of dollars in recovery costs — this in a sector with already tight budgets.

The challenge

Metropolitan school district concerned with data and network security breaches

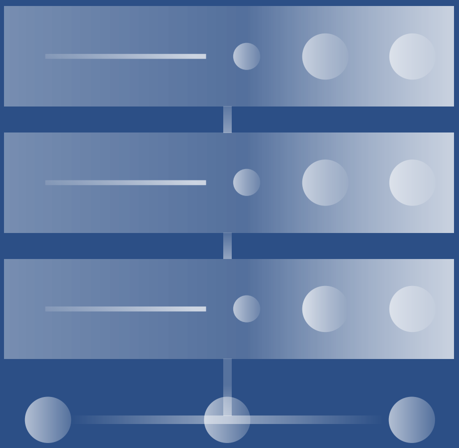
Out of the many potential cyberthreats, there are a few that schools and districts especially need to be cautious of:

- **Data breaches:** Student records and school documents transmitted from a secure to insecure environment and used by hackers
- **Denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks:** School servers being deliberately overloaded with requests, causing a website or system to be shut down and unable to access
- **Phishing:** School employees — or students — being sent emails falsely claiming to be legitimate organizations to procure sensitive information such as passwords, credit card numbers, bank account numbers, and other personally identifiable information
- **Malware:** Students or school staff downloading a piece of malware disguised as legitimate software through peer-to-peer file sharing, email attachments, or links

These threats were all a concern for one of our partners, a large public school system located in a sizeable metropolitan suburb. The district had 9,000 students spread across 13 districts and was responsible for the network security of over 4,000 Windows and Mac computers.

The school system's administration network had an array of problems:

- Network connections would be lost whenever the network crashed
- The existing spam filter did not meet compliance requirements, nor did it have adequate service or support from the manufacturer
- The IP video security system the district installed to monitor and protect the students wasn't secure, opening them up to additional risks



From a test to a solution

Implementing CloudCover's CyberSafety CC/B1 Platform™

In talking to the school district, the situation felt precarious. There was a sense that even if they bought an entirely new — and most likely expensive — data security solution, they believed they could only mitigate the hacking. And, because their various vendors couldn't address some of the concerns they had about their disparate systems and data, it felt like they could never completely protect themselves. They wanted to stop thinking about their cybersecurity efforts as a potential reactive scramble and get to a place of proactive, anticipatory preparedness.

The CC/B1 Platform was an ideal match for the district's goals. The AI-driven security orchestration, automation, and response (SOAR) platform can:

- Predict, anticipate, and block threats by applying multi-layer security algorithms at top speeds
- Collect threat-related data from all corners of a network and streamline them to create a clear, easily seen picture of an organization's data landscape
- Act as a "risk-aware engine" that proactively inserts security code, alerting the district's technology of an attempted breach of data privacy, and stop it within microseconds and with 99.9999999% accuracy

The district's IT staff decided to install CC/B1 for a complimentary 60-day trial to identify existing vulnerabilities, and chose a configuration that includes filtering, intrusion protection, and anti-spam. The network security-agnostic nature of the CC/B1 meant it would function seamlessly with the district's existing cybersecurity stack, enhancing the investments that were already in place.

The results

Immediate, accurate cybersecurity protection in microseconds

The district saw results from the very beginning of the trial. One of the members of the IT team remarked, "Nothing else we looked at even came close to the effectiveness, flexibility, and the price of CC/B1. The decision to purchase was a logical one." After the trial, the platform was rolled out further to protect instant messaging, peer-to-peer, and IP video for multiple locations and access points throughout the district, as well as all network routers and switches.

21,977
viruses stopped

252,181
spam emails identified

384,169
attacks blocked

99.96%
effectiveness of district email's platform

Behind these numbers lies a more impactful outcome — peace of mind for the district's IT staff. After hearing plenty of claims and promises from cybersecurity companies without the results to match, they found a solution that helps them sleep at night — knowing their cybersecurity solution is doing its job.

Mitigate cyberattacks at your school or district by taking a look at CloudCover's CyberSafety CC/B1 Platform — check it out for yourself or contact us directly to learn more.

References
Levin, Douglas A. (2021). "The State of K-12 Cybersecurity: 2020 Year in Review."
EdTech Strategies/K-12 Cybersecurity Resource Center and the K12 Security Information Exchange.
https://k12cybersecure.com/year-in-review/

Readiness and Emergency Management for Schools (REMS). "K-12 Cybersecurity 2020 Review."
https://rems.ed.gov/docs/Cybersecurity_K-12_Fact Sheet_508C.PDF