K12 schools and districts are not immune to cyber threats. Schools collect, generate, process and store a wealth of data that could be valuable to cyber criminals including personally identifiable information on faculty, staff, students and parents, academic records, health and insurance data and financial transactions. And, schools increasingly rely on technology to operate - from adaptive learning platforms to daily operations.

**BROAD ATTACK SURFACE**

School network infrastructures are complex. The network supports many different types of connected IoT devices. Students, teachers, staff and guests connect to the school network with a variety of personal or school-assigned devices. Wi-Fi security cameras are being used to support campus safety initiatives. Building automation and access control offer efficiencies, savings, and, yes vulnerabilities. All of this widens the attack surface and makes a secure network more challenging.

**CLOSING THE GAPS**

Although education institutions are investing in cybersecurity, recent breach statistics suggest there are opportunities for improvement to stay ahead of threats. Let’s investigate how modern security solutions from Aruba can help education institutions better:

- Gain visibility into everything connected to both wired and wireless networks
- Ensure that the appropriate IT access policies are applied to users and devices

**AT A GLANCE**

There have been 533 publicly-disclosed cybersecurity-related incidents involving U.S. public schools since 2016. During 2018, the misuse and abuse of school technology and IT systems resulted in 122 publicly-disclosed K12 cybersecurity incidents. This equates to a rate of about one new publicly-reported incident every three days. Cyber incidents include:

- Phishing attacks resulting in the disclosure of personal data
- Ransomware attacks
- Denial-of-service attacks
- Other cyber incidents resulting in school disruptions and unauthorized disclosures

- The K12 Cybersecurity Resource Center

**SECURE INFRASTRUCTURE**

For over 15 years, Aruba has delivered high performance networks that include many built-in security features.

- The newest Wi-Fi certified protocol WPA3™ was co-authored by Aruba experts and delivers a range of security and ease of use features.
- Secure boot delivers anti-tampering features for access points.
- Military grade encryption and VPN ensure traffic is secure.
- The Aruba Policy Enforcement Firewall (PEF) enables user/application visibility and policy enforcement based upon user, role, application, device and location.

Reference Sources:
The K12 Cybersecurity Resource Center
ACCESS CONTROLS
Security starts with visibility of who and what is connected to your network and what they are doing on the network at all times.

• **Know What is on the Network**
  Today, many IoT devices are built on standard hardware platforms. That can make it extremely difficult to know exactly what is on your network. For example, a security camera and smart thermostat could both be built on the same Linux platform. ClearPass Device Insight uses machine learning to identify devices based on multiple attributes, traffic destination, and communication frequency. Knowing what is on the network is the first step in protecting it.

• **“Zero Trust” Access to the Network**
  Aruba ClearPass NAC (Network Access Control) delivers discovery, profiling, authentication and authorization of users, their devices and IoT devices before letting them on the network or giving them access to IT resources. These pre-admission controls are critical because cybercriminals are adept at quickly advancing and moving laterally within seconds after gaining access to a network.

• **Precise Control of Access to IT Resources and Assets**
  ClearPass provides adaptive, granular policy-based access controls by user, device, role and location, including for applications. These controls ensure that each user, device or IoT only has access to the network and IT resources and assets they are approved for.

• **Intelligent Segmentation**
  Aruba Dynamic Segmentation leverages the Aruba secure infrastructure, PEF and ClearPass to deliver a network edge that securely connects and automatically partitions user and device traffic across wired and wireless networks based upon policies.

NEXT STEPS FOR A HEALTHIER SECURITY POSTURE
With advanced access controls and network security, and interoperability with over 140 multi-vendor network and security solutions, you can rest assured with the visibility and confidence that your security posture is in a much healthier state.

LEARN MORE
• [https://www.arubanetworks.com/solutions/security/](https://www.arubanetworks.com/solutions/security/)