AT-A-GLANCE

Protecting Student Data: More Than Mobile Security

HIGHLIGHTS

- An end-to-end secure environment to protect student data
- Encryption with automation of policy enforcement reduces the risk of error and management burden
- Immediate, secure, onboarding of devices such as Chromebooks to support instant school-wide access

Simple-to-Manage, Pervasive Network Security as a Standard

As efforts focus on making networks and information more accessible and available, concerns grow about the risk to private student data. It is a concern shared by everyone involved in providing education, and recognition is growing that mobile security is only one aspect to securing student data. Just over half of teachers cite "student privacy concerns" as an issue when using wireless internet access in class[1], while 64 percent of IT leaders say this issue is "more important" than it was just 12 months ago[2].

For administrative purposes, and to ensure schools play their required role in the oversight of student welfare, student data must be regularly updated, collated, stored and on occasion, reported on. At the same time more personalized learning approaches are enabled by technology in classrooms. The promise of personalized learning could significantly improve student outcomes, but also relies on access to Student Information Systems (SIS) where sensitive data lives.

With more access being provided to "guest" users and student's own (often unsecure) devices, paired with an increase in the use of wireless access points and range of platforms and Web portals hosted offsite, an accessible education must not lead to a breach in private information. Student data must therefore be completely secure both where it is held and stored, and while it is in transit over wireless networks on campus or wired networks between school, district, or cloud hosting provider locations.

State-level legislators are already moving to increase the level of protection and restrictions already set out in the Family Educational Rights and Privacy Act and Children's Online Privacy Protection Act. In fact, in 2016 there was draft federal legislation that called for schools to face financial penalties for any breach of security resulting in student data being compromised. Yet security must not compromise connectivity, access to instructional tools, or resource availability.

[1-2] Consortium for School Networking, *K-12 IT Leadership Survey Report - 2016*.

Securing Student Data with the Brocade Ruckus Edge Networking Product Family

As systems and user devices change, new access points are added, and more student data is transferred between sites, platforms and portals, the risk of student data being compromised grows. A holistic security strategy is critical to address all possible entry points and ensure both wired and wireless networks are protecting the data they carry.

In the wired LAN environment, Brocade® ICX® switches support true end-to-end IP security (IPsec) and Media Access Control Security (MACsec) encryption, while extending site-to-site IPsec VPN out to deliver encryption from the wiring closet. The switches also support remote access encryption using SSL. Brocade MLXe routers for data center connectivity and traffic aggregation, and Brocade vRouter technology, provide complete data security across the WAN, cloud environments, and between data centers. Students can securely access, download and view class and educational materials remotely, as can other users such as parents and caregivers, teaching staff, and those who may want access to OER materials.

With wired connections secured, attention must also be turned to securing data carried by the wireless infrastructure. Encryption of the data in transit is one element, which the Ruckus ZoneFlex™ access point helps address with MACsec link layer encryption to protect Wi-Fi communication between devices. For additional security across mid-sized campus areas the Ruckus ZoneDirector™ controller offers Dynamic Pre-Shared Keys (PSK) to eliminate the requirement to configure and update individual PC client devices with unique encryption keys. And dynamic VLAN assignment seamlessly extends existing security policies to the WLAN.

However, a more significant issue is ensuring only certain devices and users can receive and access potentially sensitive information and the network itself in the first place. This means managing hundreds or even thousands of potentially non-compliant, Wi-Fi-enabled user devices, requiring almost immediate recognition and access approval or denial, presenting a massive logistical challenge to K-12 IT teams. Ruckus Cloudpath™ software provides automated, self-service onboarding to provide fast connectivity for students and teaching staff using their own devices and guests on-campus, while improving security by also automating the enforcement of the appropriate access policies for each user and device.

The Cloudpath Enrollment System (ES) is a security and policy management platform which hides the complexity of certificate-based security underneath an intuitive workflow-based administrative console. By avoiding passwords, Cloudpath eliminates the management burden and security risks presented by PSK and captive portal logins by automating access controls, use policies, authentication, and network privileges. This ensures that both users and their devices can only access sensitive data, such as student data, if they meet stringent security requirements—regardless of how many concurrent connections are being requested. Encrypted wireless can be provided without the need for a support ticket, and users, devices and policies for all wireless connections are tracked in real time to identify and address issues as they occur.

Cloudpath ES enables content filtering to function as intended on encrypted traffic. Cloudpath is a certificate authority and enforces web proxy on the device to send all traffic to the content filtering appliance and enforces the use of the client certificate for encryption.

Cloudpath ES also supports automated provision of TPM-stored security certificates for certificate-based Wi-Fi access and web authentication. An added bonus for K-12 IT administrators is the Google Admin Console Cloudpath extension available for scalable onboarding of Chromebook devices.

Cloudpath software can uniquely enable content filtering to function as intended on encrypted traffic. As remote access and use of digital platforms drives greater reliance on cloud platforms and cross-campus Wi-Fi, embedding security into the network from the start ensures K-12 IT owners can focus on enabling the transition to digital learning, rather than trying to manually address the security of the systems currently in place.

LEARN MORE

- *Ruckus Cloudpath ES*
- *Dublin Unified School District*
- *Webinar: "Secure Device Onboarding for School Networks"*

Protecting Student Privacy: More Than Mobile Security

While mobile security is a vital component in protecting student data, the increasing adoption of Wi-Fi means it is no longer enough. By building on the security and encryption embedded in a Ruckus network, solutions that automate onboarding and policy enforcement help ensure that student data in transit is secure and that networks are open only to those who should have access.

These solutions are already enabling K-12 institutions, school districts and IT suppliers across the world to protect student data and support improved student outcomes.

To join them, visit https://www.ruckuswireless.com/solutions/primary-education.

To learn more: Read our white paper: *Future Ready Networks for Education Technology*.

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

Ruckus Wireless Office
Sunnyvale, CA USA
T: +1-650-265-4200
ruckuswireless.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

BROCADE | Ruckus™