EXECUTIVE OVERVIEW

SECURING K-12 LEARNING IN A MOBILE WORLD

What to embrace and what to avoid

Unlike enterprises, school districts must contend with providing access for students, buying cycles that lead to separate domains and multivendor equipment, and inconsistent policy management and enforcement.

Faced with 1:1 initiatives and Common Core standards, school districts need to address the basics. One of the first steps involves creating a mobility rollout plan that covers authentication, differentiated access and visibility.

TACKLING AUTHENTICATION HURDLES

Mobility initiatives often lack an identity store for K-8 grades. Students do not have assigned logins and passwords due to trust or a lack of resources. Maintaining an Active Directory for 20,000 kids can be a big challenge and some youngsters are unable to remember or safeguard passwords.

Having students connect to a guest network using pre-shared keys can fast-track a project but this approach doesn't offer adequate security to ensure that only the right people can connect to the school network.

An Active Directory (AD) is often used in the higher grades, but many K-8 schools are looking to cloud solutions or something simple. Also, many schools from K-12 lack a policy enforcement solution that can differentiate access for students, teachers, staff and administration.

Best practices should include:

- The ability to use student IDs that are tied to an application suite or an internal database that can ease the management of an Active Directory
- Device certificates which can eliminate passwords and enable single sign-on access.
- Per-session authentication and visibility for each connection.

The new policy solution should also provide the ability to join multiple domains. This allows for convenient, centralized management in cases where each school has its own domain name and identity store.

MANAGING THE MULTIVENDOR ENVIRONMENT

The use of multivendor wireless and wired infrastructure due to schools purchasing in different buying cycles is no longer an issue when deploying a policy and access enforcement solution.

Districts can now deploy a single appliance that supports consistent security rules, regardless of vendor. Policies are consistent over Wi-Fi, wired and VPN for any defined role.

The rollout of mobile devices can also be a challenge. Most district IT organizations have no way to onboard and configure multiple types of devices. Nonetheless, workflows that enable self-configuration or large-scale configuration are now a requirement.

Schools need to look for the following:

- Wizard-based configuration options – one method that can include certificates and automated distribution.
- Workflows that can easily integrate with mobile device management (MDM) solutions to control the use of devices on and off campus
- The ability to easily start over every year or semester as devices are reassigned to new students.

The combination of policy management and EMM/MDM make it easier to track location and app usage of IT-issued and BYO devices as well as determine whether they're connected via Wi-Fi, wired and VPNs. MDM without policy management does not address many issues.

MIGRATING FROM LEGACY AAA

While useful in the age of modems and IT-issued desktop computers, old AAA solutions were not designed for mobile computing. With students and staff connecting at school and at home, IT must embrace a policy management platform that uses contextual data for enforcement.

Protecting users and resources now requires authentication, authorization and trust. A device without a profile and EMM/MDM agent should be remediated before getting network access. Lost or stolen devices must be quickly blacklisted so they can't connect.

Additionally, access to specific network information must be controlled and enforced based the individual user's unique role – student, teacher, staff, administration or even guest. It's the best way to protect data as well as users.

Best practices include implementing the following services:

- A role-based policy management platform that includes enterprise-class AAA services and flexible policy enforcement capabilities.
- Built-in device profiling services that store device-specific data and attributes so they can be used as part of a policy.
- Full visibility and compliance reporting.

THE END RESULT

Based on customer interaction, mobility is now a requirement across school districts of every size. The goal is to deploy a solution that quickly addresses user and security requirements, while ensuring privacy.

Your best bet is to start with an integrated solution that automates security and related workflows while at the same time meets district requirements, mitigates risks and can be deployed in phases.