

Cybersecurity in schools

Key strategies an IT admin must adopt



With schools transitioning to online learning, it is now more crucial than ever to beef up cybersecurity defenses to combat new and emerging threats.

The six key strategies outlined below can help IT admins prepare for online learning.

01 Protect endpoints

Schools should adopt **proactive strategies** to protect learning devices. They should be equipped with appropriate **restrictions and security configurations**.

In addition, IT should have tools to,

- Enable **firewall and antivirus** on devices.
- Push **Wi-Fi and VPN** configurations to secure online connectivity.
- Enforce **software and OS updates** to patch out vulnerabilities.



02 Enforce data security

Schools must address issues including **protection of personal data** from cyberattacks, **access to data without consent**, **data loss**, and more.

IT administrators must,

- Perform **audits** to **discover and classify** data.
- **Encrypt sensitive data** on apps and devices.
- Enforce **strong passwords** to safeguard data.
- Enforce **containerization** policies to separate personal data from learning data.



03 Manage access controls

Schools must adopt strategies to maintain a database of **identities** and manage their **access privileges** to sensitive data.

Secondly, IT administrators must,

- Enforce **Multi-Factor-authentication (MFA)** to securely verify a student/teacher's identity.
- Adopt **Single-Sign-On (SSO)** technology to help streamline authentication and ensure that minimal time is wasted to authenticate.



04 Secure apps & resources

Adopting a **centralized app repository** equips IT with **complete control** over the **apps and resources** installed on learning devices.

IT administrators should,

- Manage **app permissions and configurations**.
- Deploy **customized app stores** with school-approved apps for students to download.
- Enforce **app blacklists / whitelists** to block students from installing unproductive apps.



Apple School Manager

For schools that have adopted Apple devices into their learning strategies, employing Apple School Manager to strengthen management processes is a no-brainer. (It's free, so duh!)

However, to unleash its true potential, you must pair it with a Unified Endpoint Management (UEM) solution.

Integrating UEM with Apple School Manager (ASM) enables IT to quickly equip students with learning devices via Automated Device Enrollment, easily assign apps and resources to teachers and students via Apple's Apps & Books program, and more.

05 Enforce kiosk lockdown

A kiosk software is designed to lock student devices into a **kiosk mode** and block all the other device functionalities. IT administrators can,

- Lock down student device to the appropriate exam **apps or websites**, and block students from exiting them or accessing any other unrelated apps.
- Set up **locational barriers (geofences)** and lock down student devices that wander outside school zones.



06 Enable remote access

Remote access collectively refers to all the **realtime device monitoring and troubleshooting** activities performed on learning devices.

With remote access features, IT admins can,

- Periodically receive important information on **device performance** and perform **corrective actions**.
- Analyze the system, find and **resolve issues** critical to the device functioning, and reduce unexpected **device downtime**.



Summary

With a suite of functionalities including zero-touch deployment, endpoint security, app and resource management, identity & access management, remote monitoring & troubleshooting, auditing & reporting, and more, Hexnode UEM equips IT teams with all the tools they require to ensure effective cybersecurity in schools.