# 10 Ways to Keep Students Safer with End-to-End Security

From end-user devices, to the underlying network, to the students, teachers, and staff themselves, Cisco Meraki is helping schools remain safe and secure at several touch points. By integrating endpoint security, network security, and physical security, Meraki enables schools to create a safe campus environment that empowers students to focus on learning, teachers to focus on teaching, and IT to focus on proactive projects.

## BLOCK HARMFUL CONTENT

Students require freedom to research topics for their next paper, study for an upcoming test, and complete homework assignments, without worry of encountering harmful or distracting content. Be in control of the content your students can access by blocking P2P traffic and file sharing, adult content, social media sites, and other undesirable content across 70+ categories, while allowing access to Safesearch, Youtube for Schools, and other whitelisted sites and education applications. Regardless of if students are on student-owned or school-owned devices, control the content they have access to while on campus and at home.

## ENABLE STUDENT SAFETY

Keeping students safe and secure on campus is a top priority. With smarter security cameras, easily see who is entering the campus, when students are wandering the halls during class time, and where students and staff congregate outside of school hours. Quickly find important security incidents when they occur and track patterns in behavior for improved security measures. Give access to the principal, CIO, teachers, or even law enforcement to view individual, or a grouping, of cameras for increased visibility and response times.

## STOP MALICIOUS FILES AND VIRUSES

Many security incidents occur when loading a risky website, opening an unknown email attachment, or clicking on an unsecure link - severely compromising sensitive student and school data. Stop malicious threats and files before they enter the network by preventing them from being downloaded, protect devices from phishing attacks, and analyze files retrospectively to spot malicious behaviors and flag for future attacks.

## ENSURE STUDENT PRIVACY

As the amount of online assignments, faculty curriculum, and student research continues to grow, the amount of student data generated is never ending. To protect this valuable data, set up the first line of defense by restricting who can access certain parts of your network with group or user-based policies. With features like intrusion detection and prevention and anti-virus/ anti-phishing scanning, breathe easy knowing the network is secure, inside and out.

## SECURE END USER DEVICES

As 1:1 and BYOD programs continue to grow, along with the overwhelming amount of distracting and unsafe content, securing endpoint devices has become increasingly important. Prevent students from accessing blacklisted or unsecure sites on both school and student-owned devices with group policies and advanced malware protection. Easily see the devices that join the network with visibility into client behavior, enabling the shut down of rogue devices as needed. By protecting all of the devices that students and teachers use every day, the network can remain secure from endpoint security vulnerabilities.

## MITIGATE RISKS OR INCIDENTS

Security cameras are one method to help mitigate risks or incidents on campus. With complete and high-quality video coverage, students are less likely to engage in theft, violence, cheating, and vandalism. If an incident does occur, security teams can quickly identify the who, what, and when of the situation with motion search capabilities and give access to administrators or law enforcement to view live or past footage as needed. This not only improves response times and holds individuals accountable, it enables security and IT teams to easily assist in and alleviate high-stress situations.

## FIND LOST OR STOLEN DEVICES

With each student having an average of 3 to 5 devices at any given time, keeping track of these devices can be a headache. By using real-time location data from GPS, Wi-Fi, or IP address, finding lost devices is a cinch. Plus, with geofencing capabilities, receive an alert when a school-owned device leaves a designated area, and apply or remove settings as needed. If a device is stolen, use advanced search capabilities on security cameras, to identify the culprit. And, if a device can't be retrieved, easily remote wipe its content for added security.

## PROTECT AGAINST CYBER ATTACKS

Schools and colleges big and small are regular targets for cyber criminals. These attackers can not only gain access to private student data, but can damage or destroy a whole computer system or network, putting the entire school district or college's network at risk. By blocking suspicious IP addresses, shutting down rogue APs and SSIDs, classifying attack profiles, and providing easily-digestible security reports to see where attackers are coming from, IT can keep networks secure and protected against these attackers.

## PATCH FIRMWARE VULNERABILITIES

Cyber attacks unfortunately happen frequently, and each time it is a reminder of the importance of keeping computer systems and complex networks patched. With a cloud-managed solution, firmware updates guard against the latest security threats, while intrusion prevention updates daily to protect against new vulnerabilities. Plus, these updates are all done automatically, no need to manually download or patch an IPS or worry about a misconfiguration.

## LOCATE TRESPASSERS

As hundreds, thousands, or tens of thousands of students walk the campus everyday, picking out those who shouldn't be there can be a challenging task. With built-in person detection technology, see how many people enter a frame at a given time, allowing you to easily spot patterns and anomalies. Receive notifications when someone enters a frame during a designated time and quickly find suspicious activity with motion search capabilities.

With the perfect blend of endpoint, network, and physical security, Meraki provides the safest environment for schools, colleges, and the surrounding community. The full stack of Meraki solutions, including endpoint management, security appliances, access points, and security cameras, all work together seamlessly to provide a secure offering for schools. Meraki keeps devices protected, data encrypted, and students safe, while enabling IT to spend more time on proactive security projects, and less time managing and troubleshooting security solutions.

Learn more in this on-demand webinar: **meraki.com/videos/k12-end-to-end-security**