MAKING THE GRADE

End-to-End Security in Education

cisco Meraki

Table of contents

INTRODUCTION

Learning environments go digital

Whether they are completing a math test online, giving a science presentation, or virtually attending a field trip, students of all ages are always connected. And while they are preoccupied with completing online school assignments and streaming educational videos, IT teams at primary, secondary, and higher education institutions are hard at work designing and maintaining networks that make this all possible.

As educational institutions start to integrate digital technology into many aspects of learning, network demands exponentially increase. Students are bringing more devices to school and using them to write essays, prepare presentations, conduct research, and take tests, and they expect reliable Internet access to do so. Smart boards, online lectures, real-time productivity applications, video platforms, 1:1 device programs, smart speakers — all of these technologies have enabled instructors to personalize lessons, standardize test taking, and increase collaboration between students.

To support these initiatives, IT teams are deploying and managing more sophisticated wired and wireless networks, without an increase in budget or resources. As more technology is introduced into schools, so are more security risks and vulnerabilities. It's no longer just about keeping the network secure, which is challenging enough on its own, but it's also becoming a requirement to protect end user devices and help ensure the physical safety of students and staff.

End-to-end security practices are imperative for schools and universities, especially those implementing digital learning environments. Deploying the right solutions to keep networks, endpoints, and physical environments protected and secure is paramount to creating safer primary and higher education institutions.

CHAPTER 1

An ever-growing list of security threats

While migrating from traditional to digital learning environments can improve student outcomes, it also opens the door to several security vulnerabilities. From unsecure IoT devices to network vulnerabilities to the physical safety of students and faculty, security threats impact schools around the world.

Many institutions are slowly transitioning away from storing report cards, financial data, and student records in a sea of file cabinets. Today, more systems, courses, and data are being stored online, in the cloud, or on-premises to enable better record keeping and easier access to information. But with student records containing sensitive information, such as birth dates, health data, and information about student behavior and performance, this data migration opens schools up to increased security threats. Cybercriminals are increasingly targeting educational institutions to sell proprietary research to third parties, hold data for ransom, or steal people's identities. Recently,

school districts in the United States[1] and New Zealand[2] had to shut down their systems due to ransomware attacks, while the University of California, Berkeley experienced a data breach that exposed financial data for 80,000 people.[3]

Many security risks are unwittingly introduced by students and faculty connecting their own devices, like smart speakers and gaming consoles, to the network. EdTech noted that IoT devices are frequently brought to campus without any consultation from IT staff:

> **IoT is also arriving on campus in the same way most new technologies arrive: with students and faculty who connect personal consumer devices to the network without consulting anyone. A walk through any residence hall or faculty office suite quickly shows that IoT is everywhere.[4]**

Especially when these devices aren't patched against the latest security vulnerabilities, rogue actors can use the devices as a gateway to infiltrate the network. For example, in 2017, Verizon reported that a university's entire network crashed because 5,000 systems and IoT devices were making requests to the university's DNS servers every 15 minutes in a distributed denial of service (DDoS) attack.[5]

Exacerbating these security threats is the fact that cybercriminals know that school networks can be easy targets. Many school districts and college campuses have outdated networking equipment, since budgets to procure new wireless access points (APs), switches, and security appliances can be limited. Plus, with small, time-strapped IT teams, finding the opportunity to replace outdated networks can be challenging. Even with new networking

---

1 https://www.miamiherald.com/latest-news/article218289740
2 https://www.newshub.co.nz/home/new-zealand/2018/08/taranaki-high-school-shuts-down-computer-system-after-hack
3 https://www.csmonitor.com/USA/Education/2016/0229/UC-Berkeley-breach-Universities-increasingly-targeted-in-cyberattacks
4 https://edtechmagazine.com/higher/article/2017/04/keep-your-campus-both-smart-and-secure-iot-expands
5 http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-sneak-peek_xg_en.pdf

infrastructure, keeping firmware up-to-date is a constant challenge since many systems require manual configuration changes, and therefore are difficult to manage and update en masse. These factors can put many schools at higher risk of a cybersecurity breach.

Surprisingly, one of the most common causes of security incidents is human error. Faculty and students can fall prey to phishing scams sent through email or messaging services and unknowingly hand over sensitive credentials or accidentally download malware. These emails are sometimes disguised as coming from academic leaders requesting students' private financial data for student aid purposes or other school-related activities. According to Federal Student Aid, an office of the US Department of Education, institutions that utilize a SSO (single sign-on) system, but that don't have multi-factor authentication, are most vulnerable to these types of attacks.[6]

In addition, it is no longer just the network that IT teams need to focus on when it comes to securing campuses. Due to advancements in technology, it is becoming the responsibility of the IT team to also manage and maintain systems to mitigate physical threats. While the safety of students and staff is a top priority, deploying and maintaining solutions that empower IT and security teams to partner and provide increased security can be a challenge. A single university might have dorms, cafeterias, libraries, athletic facilities, quads, lecture halls, and more, with parents, visiting students, and guests walking around campus at all hours. All this variability makes it difficult to predict physical security incidents and mitigate them. In addition, as physical threats and natural disasters continue to prevail in schools, having the right technology in place may help leadership respond, act, and prevent future events.

While the thought of conquering all of these security challenges at the same time can seem daunting, there are three areas IT teams can focus on when creating safer learning environments. By evaluating strategies and solutions that address security at the endpoint, network, and physical layers, IT teams and school leaders can create places where students can focus on learning and instructors can focus on teaching.

---

6 https://ifap.ed.gov/eannouncements/083118ActivePhishingCampaignTargetStudentEmailAccount.html

CHAPTER 2

Securing the endpoint: From school- to student-owned devices

When working to address security concerns, an important starting point is with school, student, and staff devices. With the growing number of computers, tablets, and IoT devices brought into classrooms, libraries, labs, and residence halls, it's increasingly important to make sure these devices can access the network safely and have the latest security updates. As more primary school districts institute BYOD or 1:1 device programs, and each college student brings an average of seven devices[7] to campus, the number of devices that IT departments need to monitor is increasing at an unprecedented rate.

To keep school-owned devices secure, an endpoint management solution can help in a variety of ways. By managing all devices through one system, IT administrators can deploy security patches to hundreds or thousands of

7 https://edtechmagazine.com/higher/article/2015/08/report-how-millennials-use-mobile-devices-college

devices in minutes, ensuring school-controlled devices are always up-to-date. This can help, for instance, in keeping tablets that are used to process payments protected against the latest security threats. Most criminal activity starts with the endpoint and many breaches today exploit already known threats or vulnerabilities where a patch exists.[8]

With over 270 schools and 200,000 students and staff, a large Canadian school district needed a way to manage and secure 26,000 iPads and 900 phones. By centrally managing all of their devices using a cloud-based solution, they were able to keep their devices up-to-date and secured with the latest security patches.[9]

Endpoint management solutions can also be used to track lost devices, or remotely wipe stolen devices, to make sure sensitive school information does not fall into the wrong hands. With a system that offers geofencing, IT teams can set boundaries for where specific devices should be contained, and have an alert go off if the device leaves that designated area. Wayne Highlands School District in rural Pennsylvania uses endpoint management to control and keep track of the schools' iPads.[10] Scott Miller, the Director of Technology, explained, "I took an iPad home to see if the geofencing worked — within minutes I had a text message and email alert saying that the iPad had left its territory. I can check a GPS map to see exactly where an iPad is; a student left an iPad on a bus and we were all watching it go up the highway."

With over 270 schools and 200,000 students and staff, a large Canadian school district needed a way to manage and secure 26,000 iPads and 900 phones.

To further protect students using devices in schools, IT teams can implement firewall policies and content filtering measures to block inappropriate and potentially dangerous material and prevent access to blacklisted sites. Students commonly use peer-to-peer file sharing applications and online

8 https://www.bankinfosecurity.com/blogs/do-you-have-dark-endpoint-problem-p-2576
9 https://meraki.cisco.com/customers/k-12-education/large-canadian-public-school-district
10 https://meraki.cisco.com/customers/k-12-education/wayne-highlands-school-district

gaming sites, which can play host to illegal content and malware that can put students' devices, and the entire network, at risk. Applying these security measures to endpoints can also help guard against the threat posed by phishing scams; before someone tries to click a link, the device recognizes the contents as malicious, the link is blocked, and the individual receives an alert.

Another way IT teams can contain potential threats from infiltrating the campus network is by creating separate networks: one for trusted, school-owned devices and another for BYOD devices. Since the IoT devices students bring to school aren't guaranteed to be patched against the latest security vulnerabilities, segregating school-owned from student-owned devices can keep the internal network secure. Plus, with increased visibility into what's on the network, IT teams can quickly identify rogue endpoints and shut them down or lock them as needed. In addition, IoT endpoints and other connected devices should be evaluated for up-to-date security measures. For example, many schools still use outdated security camera equipment, which can serve as an entry point for network attacks.[11]

By keeping endpoints updated and secure, creating segmented networks for BYOD, and blocking harmful content, education leaders can ensure a first line of defense against common security threats.

11 https://cosn.org/sites/default/files/Top%205%20Cybersecurity%20Threats.pdf

CHAPTER 3

Securing the network: From the closet to the classroom

Schools large and small are regular targets for cybercriminals. These attackers can not only gain access to private student data, but also damage or destroy a whole computer system or network, putting the entire school district or university at risk. Therefore, while protecting against edge security threats is crucial, security challenges such as malware, ransomware, and rogue devices are best addressed at the network level.

IT teams can mitigate network threats by creating group or user policies based on different criteria, such as user role or academic department. Students visiting the research lab might be assigned one policy, while teaching assistants and professors who work in the lab full-time might have another policy. This sets a list of rules and restrictions that devices must adhere to depending on their client or device type, SSID, or VLAN. Based on which group policies are applied, IT staff can set Layer 3 firewall rules, Layer 7 firewall rules, content filtering, traffic shaping rules, and more, so that the right people have access to the right permissions and information on the network.

At the Community College of Denver, the IT team created several isolated, protected networks for their HVAC system, gas line monitoring systems, and credit card machines to prevent hackers from accessing the devices.[12]

With new malware threats introduced daily, there are several precautions IT teams can take to protect against cyberattacks. Next-generation firewalls use features like intrusion detection and prevention services (IDS/IPS) to proactively identify malicious traffic and block it before it can enter the network. Even if a student or staff member accidentally downloads a file that doesn't trigger an initial malware alert, advanced malware protection will continue to watch and analyze files to spot malicious behaviors retrospectively, based on similar behavior detection.

Every time a cyberattack occurs, IT administrators are reminded of the importance of keeping networks patched against vulnerabilities. Having to manually update network infrastructure on-site and patch IPS individually is a huge drain on IT teams' time and can potentially result in misconfiguration errors. With a cloud-managed solution, firmware updates can be pushed out automatically to guard against the latest security threats, while intrusion prevention updates happen daily to protect against new vulnerabilities. This ensures networks are patched faster with less risk of a security breach. With their original system, Patrick Brown, CIO, and Marc Benner, Assistant CIO at Illinois College, used to manually update their network firmware, which would take over a week to execute. With their improved cloud-managed solution, they can easily schedule a firmware update to happen all in one night, ensuring the entire network is protected at once.[13]

Another way for attackers to gain access to personal student and financial data is through AP and SSID spoofs. Anyone who purchases an access point and copies the name of the main campus SSID might trick students into accessing a fake network. In university residence halls particularly, a common concern for IT staff is the number of students who plug their own routers into the wired infrastructure and expose the LAN. Advanced network security

12 https://meraki.cisco.com/customers/higher-education/community-college-of-denver
13 https://meraki.cisco.com/customers/higher-education/illinois-college

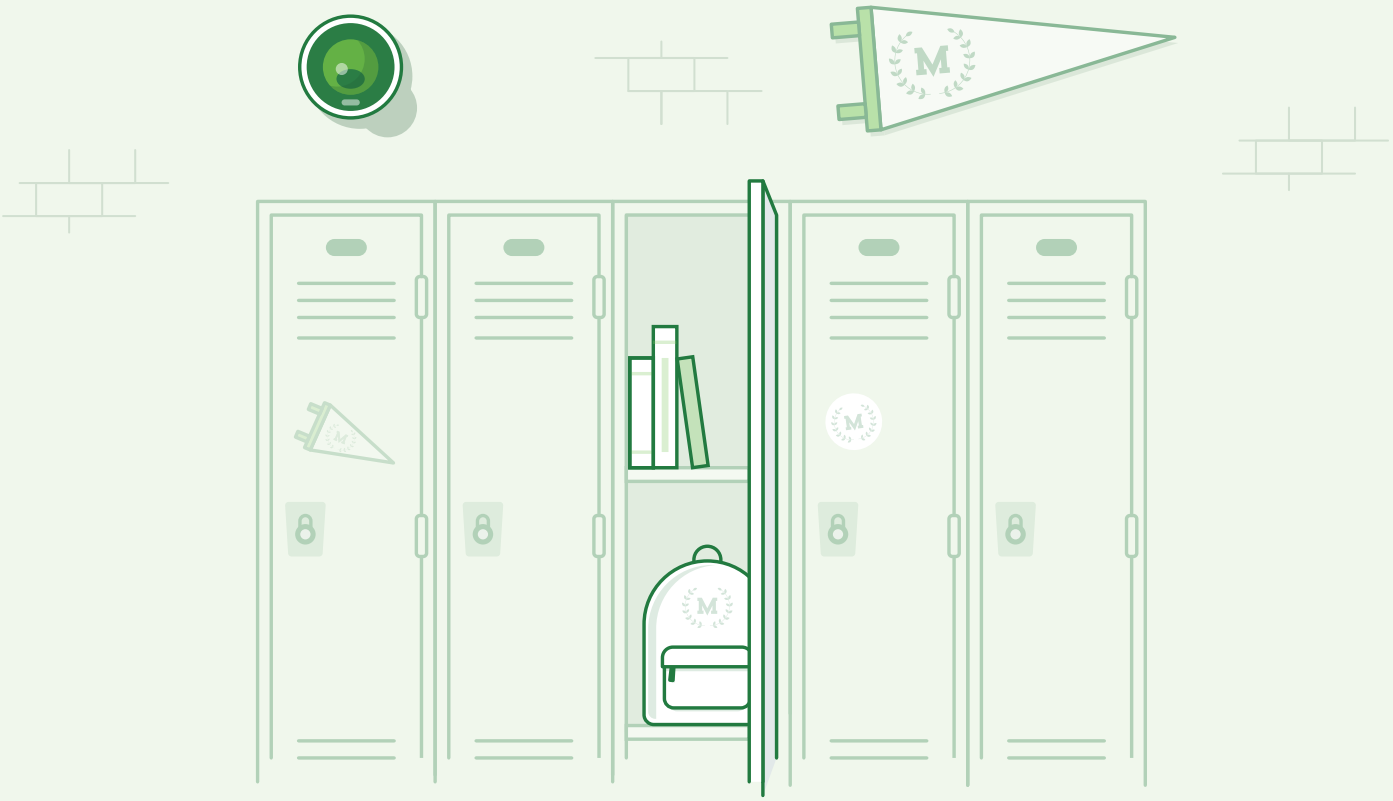
technologies included on some APs can automatically detect and shut down rogue devices, SSIDs, and packet floods using a dedicated scanning radio.

No matter how many security measures IT teams implement, it's also important to consider the response time if a network incident were to ever occur. Many outdated network systems don't provide adequate visibility into what's happening on the network, so incidents occur without IT's knowledge. Having complete visibility can make the difference between a quickly resolved situation and potentially massive damage. Modern networking equipment can provide IT teams with easily digestible security reports on a regular basis, so IT teams can see where attacks are coming from, which clients are impacted, and how best to mitigate the situation, without needing to wade through complex logs. Those responsible for IT can also set up automatic email notifications to alert them when there is a problem, so they can quickly neutralize a threat when it occurs.

While having the necessary network security measures in place is crucial, ensuring that students and staff know how to recognize security threats and respond is just as important. One way to do this is through trainings, where students learn how to set up secure passwords, recognize phishing scams, and deter from clicking on suspicious links. Some IT departments also send fake phishing attempts to students to test their understanding, and remind the ones who click about email best practices.[14]

Having complete visibility can make the difference between a quickly resolved situation and potentially massive damage.

14 http://www.govtech.com/education/papers/Protecting-Students-and-Their-Data-108087.html



CHAPTER 4

Securing the school: From the hallways to the sports fields

The increase in digital technology not only changes learning spaces, but also has a large impact on school safety. As more technically demanding physical security solutions are introduced, IT teams are more frequently becoming responsible for deploying and managing these systems, either independent of or in partnership with school or campus security teams. This is especially true when these new security solutions, including badge access control, visitor management systems, mass notification systems, and security cameras, are being built to connect with the main school network.

Although several measures exist today to protect students and staff, one crucial piece of technology that recently got an upgrade is security cameras. Technological advances in this space are revolutionizing the way education leaders think about video surveillance. With smarter security cameras, IT teams gain access to several benefits and features that help keep students and faculty safer, including faster deployments, increased scalability, quicker response times, and advanced analytics.

By using motion search capabilities, users can quickly identify the who, what, and where of any situation, enabling security and IT teams to easily assist in and alleviate high-stress situations and quickly resolve conflicts.

As campuses grow and buildings are built or renovated, using a security camera system that is flexible and scalable is key to continuous coverage across institutions. Traditional analog or IP security camera systems are generally challenging to install because they must connect to a server that is stored on-premises. Plus, with multiple cameras hooked up to one network video recorder (NVR) or digital video recorder (DVR), when one camera fails, it can bring the entire camera system down, without IT's knowledge. Whether areas on campus are unprotected due to challenging installations or security camera outages, this lack of coverage can be detrimental to school safety. Instead, by implementing a camera system that stores video footage on the camera, schools can deploy cameras much more quickly, and ensure they are capturing key scenes. At Ashland University, a security incident occurred in the dormitories and the school was unable to identify the culprit with its analog-based security system. The IT and security teams knew they needed to quickly upgrade their security solution, so they deployed a solution with the video stored on the camera and managed through the cloud. This allowed them to quickly scale and deploy over 150 indoor and outdoor cameras across the campus in just a few months.

Being able to identify incidents as they happen, or quickly review footage to find specific events, should not be a challenging task. Yet, this is a large pain point for education institutions, who either suffer from poor video quality, manually having to review video footage, or having to be on site running specialized software. After deploying cloud-managed security cameras, Ashland University used the cameras' time and motion search features to identify in minutes the student who vandalized a dorm building, instead of spending hours scrubbing through footage. Security staff can monitor video from anywhere, ensuring students consistently feel protected. By using motion search capabilities, users can quickly identify the who, what, and where of any situation, enabling security and IT teams to easily assist in and alleviate high-stress situations and quickly resolve conflicts.

However, IT teams can't be responsible for the safety of students and staff alone. It is even more powerful if they can gain the help of on-site security teams and local law enforcement to assist when needed. By giving principals/

presidents, CIOs, and law enforcement access to directly view live and recorded camera footage, they can respond to situations much more quickly. But this goes beyond giving access to security cameras—educational institutions should partner with the community to set up automated security notification systems and develop security response plans in case of an incident.

As students walk their schools everyday, finding valuable ways to use and analyze camera footage can be a daunting task. But with the same processors that power smartphones integrated into new camera technology, there are unique ways to use advanced analytics to help keep students safer. Using person detection technology, IT and security teams can view how many people enter a frame at a given time, allowing them to easily spot patterns and anomalies in traffic and behaviors. For example, IT can see who is entering the campus, when students are wandering the halls during class time, and where students are congregating outside of school hours, and make adjustments accordingly. When someone enters a specific frame during a designated time, IT teams can schedule email alerts and respond accordingly.

If there is a fire in a school building, security cameras can notify response teams of what rooms have not been cleared of people yet so they know where to focus their efforts.

In addition to these powerful capabilities come unique integrations and customizations to build fully-fledged security solutions. By connecting mass notification systems, badging applications, emergency alert programs, lights, and other devices with security camera analytics, schools can enhance alerts and responses, automating processes that used to be impossible to complete. For instance, if there is a fire in a school building, security cameras can notify response teams of what rooms have not been cleared of people yet so they know where to focus their efforts. If a student is walking back to their car alone at night, for example, the security camera can trigger the parking lot lights to come on for increased security.

The Reading School District IT team in southeastern Pennsylvania understands the pain of traditional camera solutions, especially with the

responsibility to protect 18,000 students across 25 locations. The district previously relied on security cameras with footage stored on NVRs. “Spinning disks like to die all the time, and typically when that one hard drive would die it would take the whole unit down. We’d lose about 20 cameras, and that just wasn’t appropriate,” said CR Hiestand, the district’s Network and Systems Administrator. After deploying cloud-managed security cameras, the district’s IT can focus on using the analytical capabilities of the cameras, including motion search and people detection, to help protect students and staff.[15]

In order to keep students safer while at school, it’s necessary that school leaders deploy modern technology to keep campus communities secure. IT teams who invest in the right physical security solutions can focus less on maintaining and troubleshooting technology and more on minimizing incidents on campus.

15 https://www.youtube.com/watch?v=dLH1mgdNd-E

CONCLUSION

Keep students safer with end-to-end security

Digital technologies are changing education at an extremely rapid pace. Just a couple of decades ago, computers in the classroom were a novelty; now, schools routinely deploy devices like iPads and Chromebooks to every student in 1:1 programs. Network security once consisted almost entirely of blocking access to inappropriate sites;[16] now, it's vital to protect vast amounts of digitally stored student data using advanced firewalls. Schools used to rely on paper logs to sign guests in and out of a building or campus; now, many digitally log guests and automatically provision access badges that determine where guests can go.

IT teams are quickly recognizing that technology not only has an immense impact on student outcomes, but also can dramatically alter the security landscape. In many ways, the security threats that schools face are advancing

16 https://searchnetworking.techtarget.com/feature/How-the-basics-of-network-security-have-evolved

at a greater pace than the monetary and human resources schools have at their disposal. That's why it's important for schools and universities to deploy technologies that are intuitive to manage and can scale effectively to protect against the latest security threats.

With the perfect blend of endpoint, network, and physical security, Cisco Meraki helps enable a safer environment for schools, universities, and the surrounding community. Meraki end-to-end security solutions, including access points, endpoint management, security appliances, and security cameras, all work together seamlessly to provide a secure offering for schools. With Meraki, IT teams can detect and block a wide range of threats, such as rogue devices, malware, phishing scams, and viruses, all while reducing operational costs, simplifying multi-site deployments, and using bandwidth more efficiently to ensure optimal performance without sacrificing security or data privacy. Meraki MV security cameras help IT teams ensure physical safety across campus with cameras that are simple to deploy and manage and provide robust analytics to better prevent, respond, and deter incidents in schools.

All Meraki products are managed entirely through an intuitive, web-based dashboard and are updated automatically through the cloud, enabling a new level of scalability and control as the security landscape evolves.

To learn more about how Meraki offers primary and higher education institutions the power, flexibility, and control they need to keep learning environments safe, visit meraki.com/videos/k12-end-to-end-security.

LEARN MORE ABOUT MERAKI FOR EDUCATION

meraki.com/videos/k12-end-to-end-security

cisco Meraki