3 Ways to Increase Network Security for Hybrid Education

A recent Center for Digital Education survey of more than 125 K-12 decision-makers found 81 percent of schools will continue offering some version of online hybrid courses in the future. But making the transition to a hybrid learning environment requires new considerations, especially when it comes to managing and securing the network.

"The current situation is a testament as to why it's valuable to go with a network solution that is simple and completely cloud-managed," says Charles Hiestand, network and systems administrator for Reading School District in Pennsylvania.

He notes that the district's cloud-managed network solution largely automates its own upkeep and many security measures, which is critical now that both staff and student devices are being used outside the district's firewall.

This issue brief discusses the essential security capabilities a cloud-managed network solution can provide so schools and districts can be confident they are securely supporting hybrid learning.

WIRELESS SECURITY

A cloud-managed network provides greater visibility and control through a centralized dashboard, which is essential for hybrid learning environments where devices are accessing the school network outside the firewall. In addition, it makes it easier and faster to classify and prioritize applications and create per-application rules to control bandwidth and block inappropriate applications, enhancing the security of a wireless network.

"Our cloud-managed network solution has proven it can simplify things," says Hiestand. "We're able to manage the whole stack of networking across 25 school sites with a team of two. Even firmware upgrades are just a couple of clicks and you can update 2,000 devices at once."

Hiestand also notes that having a simple and flexible cloud-managed network can make it easier to deploy wireless access in new locations, such as outdoors, to help increase internet access for students who may not have it at home.

"Early on when we were fully remote and we weren't sure what the best approach to internet connectivity was, having our cloud-managed network allowed us to very quickly deploy outdoor Wi-Fi to 10 locations."

ENDPOINT SECURITY

In addition to the wireless network, schools also have a responsibility to secure school-issued devices, including laptops, tablets, Chromebooks and more. Michael Singer, a product marketer in switching, wireless and endpoint security at Cisco Meraki, noticed this has led to schools looking for a better solution than they currently have in place.

"A lot of schools are leaning toward implementing security solutions like endpoint management. Before, it was 'nice to have,' but now there's a big push for it because they know they need things to work so they can support hybrid learning environments," says Singer.

He points out that using an endpoint security solution is the best way to securely manage devices because it gives schools the ability to configure and control the devices they own. For example, schools can configure devices so they are only used for school-intended apps, such as a portal to do homework. Schools can also automatically configure devices so multiple devices can be set up at once, a significant time savings for IT. Finally, an endpoint security solution gives IT the ability to automatically push updates, ensuring devices always have the latest firmware.

> **"One of the big challenges we've seen, especially in K-12, is that there are often only one or two IT folks to help implement tech. So, in a school that doesn't have many resources it can be quite overwhelming and confusing to go shopping around for network solutions, especially if you don't know what you need or what you want to prioritize."**
>
> Michael Singer, *Product Marketer in Switching, Wireless and Endpoint Security, Cisco Meraki*

FIREWALL SECURITY

A K-12 Cybersecurity Cost Report by the Consortium for School Networking (CoSN) shows almost all school districts are using some sort of firewall to protect the network.[1] Yet, only a small minority (3%) are using any kind of cloud application firewall security despite the fact that the majority use cloud applications as their data hubs.

What's more, a school district's firewall becomes significantly less effective once the student leaves the school's network. This is particularly true if students are using personal devices to access resources on cloud apps.

To ensure firewalls are robust enough to support hybrid learning, schools should look for a next-generation firewall that provides cloud application firewall security. In addition, having a firewall that provides CIPA-compliant content filtering and search protections, malware/anti-phishing scanning and automated intrusion prevention software that updates daily to protect against the latest threats will increase network security and better protect students from exposure to inappropriate content.

SECURITY SOLUTION CONSIDERATIONS

There are a lot of network security solutions on the market that can provide security in the key areas discussed, but this can sometimes lead to overwhelm.

"One of the big challenges we've seen, especially in K-12, is that there are often only one or two IT folks to help implement tech," says Singer. "So, in a school that doesn't have many resources it can be quite overwhelming and confusing to go shopping around for network solutions, especially if you don't know what you need or what you want to prioritize."

Following are two important considerations to help make this process easier:

Single system vs. multiple solutions. Many security solutions only focus on one aspect, such as wireless networking or firewalls. To simplify your IT environment, look for a security solution that allows you to manage your wireless network, endpoints and firewalls from a single system. This will make it easier to manage and provide greater visibility to help spot security vulnerabilities.

"A big benefit for us is our solution is truly a single pane of glass. Every product exists within the same universal interface; we only had to learn it once," says Hiestand.

Using a cloud-based solution that can be remotely managed through a dashboard also makes troubleshooting the entire network faster and more cost effective than having to go on site.

Simplicity. Look for a solution that is simple and quick to deploy and doesn't require a lot of custom configuration. This allows schools to focus valuable IT resources on other priorities and means less dependency on district IT staff.

For Hiestand, these requirements — a single system and simplicity — have been critical to managing his district's network with minimal IT manpower. He also notes that having a cloud-managed network solution has simplified just about every aspect of managing the network.

"Even complex network tasks like core routing and VPN configuration can be really simple," he says.

GREATER SECURITY FOR SUSTAINABLE EDUCATION

Securing your network is not a nice to have — it's an essential part of supporting hybrid learning. A cloud-based network solution, with the right security capabilities, can cover your wireless network and endpoints, and offer firewall protection. This will make your network more secure on and off campus and ensure the education environment is sustainable under any circumstance.

This piece was developed and written by the Center for Digital Education Content Studio, with information and input from Cisco Meraki.

[1] "K-12 Cybersecurity Report," COSN, Fall 2019.

PRODUCED BY: CENTER FOR DIGITAL EDUCATION

The Center for Digital Education is a national research and advisory institute specializing in K-12 and higher education technology trends, policy and funding. The Center provides education and industry leaders with decision support and actionable insight to help effectively incorporate new technologies in the 21st century. **www.centerdigitaled.com**

FOR: CISCO Meraki

Cisco Meraki offers education institutions the power, flexibility, and control they need to keep students and staff connected and secure. The intuitive, cloud-based Meraki dashboard includes features such as advanced network analytics, programmability with APIs, and robust threat prevention, enabling IT teams to save time, reduce operating costs, and enhance student experiences. Learn more at: **meraki.cisco.com/industries/primary-education**