Advancing K–12 Network Security with Zero Trust

Rising cyberattacks, new federal requirements, and an evolving education landscape have pushed cybersecurity to the forefront for just about every district IT leader. Here's how zero trust can help institutions prepare for current and future threats.

PRESENTED BY: CAMPUS TECHNOLOGY

SPONSORED BY: Charter COMMUNICATIONS | Spectrum ENTERPRISE™

Finding Ways to Solve the Cybersecurity Challenge

Federal agencies lend their support to K–12 schools.

MORE THAN 2.6 MILLION STUDENTS ACROSS the United States were affected by ransomware attacks alone from 2018 to 2021, the U.S. **Government Accountability Office (GAO) reports**. Factoring in other kinds of incidents, the total number of students impacted by cybersecurity breaches during that time is even larger.

As malicious threat actors increase their attacks on K–12 networks, with "potentially catastrophic" effects on educators, students, and their families, U.S. government agencies such as the GAO and the Cybersecurity and Infrastructure Security Agency (CISA) are stepping up to help schools and districts secure their cyber infrastructure.

The assistance comes at the request of Congress, which enacted the K–12 Cybersecurity Act of 2021 to protect K–12 institutions from cyberattacks.

Network security breaches have resulted in lost money and instructional time for schools from coast to coast. K–12 officials who've experienced a cyberattack reported that the loss of learning ranged anywhere from three days to three weeks and the recovery time ranged from two to nine months, the GAO says.

In an October 2022 report, the GAO recommended that the U.S. Department of Education develop metrics for measuring the effectiveness of K–12 cybersecurity products and services, as well as a way to coordinate cybersecurity efforts between schools and various federal agencies.

Recommendations

CISA published **its own report** in January 2023, with cybersecurity recommendations for schools and districts. CISA's suggestions include:

Focus on high-impact strategies first.

Because K–12 school systems often have limited resources, leaders should "leverage security investments to focus on the most impactful steps" initially, CISA says, prioritizing strategies such as deploying multi-factor authentication (MFA), mitigating known exploited vulnerabilities, implementing and testing data backups, creating an incident response plan and launching a comprehensive cybersecurity training program.

Once leaders have taken these steps, they can progress to other measures, such as fully adopting CISA's **Cybersecurity Performance Goals** and building a cybersecurity plan around the National Institute of Standards and Technology (NIST) **Cybersecurity Framework**.

Elevate cybersecurity as a top priority.

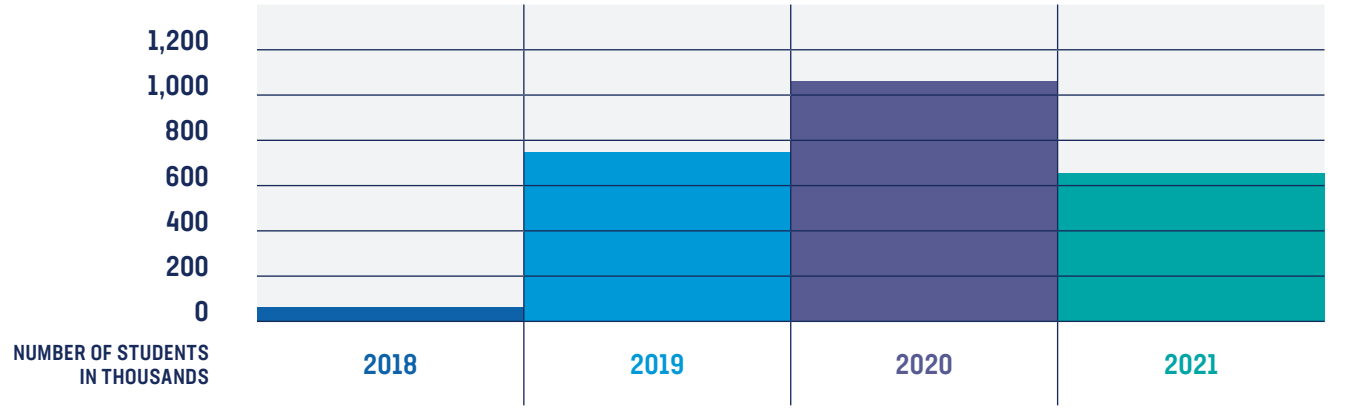
Cybersecurity risk management must become a top priority for the leaders in every K–12 district, CISA says. Leaders must take creative approaches to securing the necessary resources to make this happen.

Superintendents and school boards are critical to these efforts. "Change must come from the top down," the organization notes. "Leaders must establish and reinforce a cybersecure culture. Information technology and cybersecurity personnel cannot bear the burden alone."

Collaborate with other partners.

"No K–12 institution is an island," CISA writes. "Information sharing and collaboration with peers and partners is essential to build awareness and sustain resilience." K–12 districts should participate in information sharing forums such as the **K12 Security Information Exchange** (K12 SIX) and establish relationships with CISA and FBI field personnel, among other entities.

NUMBER OF U.S. STUDENTS AFFECTED BY RANSOMWARE ATTACKS, 2018-21



Source: GAO analysis of Comperitech study on K–12 school ransomware attacks. | GAO-23-105480

Zero Trust: A New K–12 Paradigm

Here's how this approach can protect campus networks.

AS K–12 LEADERS LOOK TO SHIELD THEIR network from attacks, the nature of cybersecurity is changing. With more applications running in the cloud and users accessing resources from any location, school district networks can no longer be protected by establishing strong perimeter defenses. Instead, districts need modern defenses that extend the network edge to each user and application.

An approach that's catching on among all types of organizations is the concept of "zero trust."

Zero Trust Defined

According to the National Institute of Standards and Technology (NIST), zero trust is "an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location."

Zero trust involves a shift in philosophy. In the past, once users have logged onto a school district network and been authenticated, they've generally had wide latitude to explore and access basic resources.

Zero trust eliminates the assumption that anyone on the network can be trusted. In a zero-trust approach, all network users are authenticated,

authorized, and continuously validated before gaining access to data and applications, whether they're located on or off campus.

"Zero trust arose from the recognition that modern IT systems are highly distributed," says Doug Levin, national director for the K12 Security Information Exchange (K12 SIX). The pandemic demonstrated that not every user of a school district's network is going to be on campus, Levin adds.

To implement this approach, school systems need strong identity and access management tools to verify users' credentials. District IT staff must be able to know who's on the network at all times, as well as which applications they're using and how they're connecting. "It's critical for school districts to ensure that users have access to the resources they need, but no more," Levin says.

Zero trust also calls for networks to be finely segmented, with permission to access various resources depending on contextual factors such as the user's role, device, location and the application or data being requested.

Benefits of Adoption

By 2025, 60% of organizations worldwide will embrace zero trust as a starting point for their cybersecurity strategy, **Gartner predicts**. One reason so many organizations are moving in this direction is because it ensures that network users are only accessing the data and resources they're authorized to use.

Not only does zero trust provide enhanced security against both external and internal threats; it also helps institutions respond to attacks faster and more effectively if someone does breach the network.

Under a zero-trust approach, IT staff have full visibility into the devices on their network — and they're constantly tracking these devices. This means IT staff should be able to identify attacks or anomalies nearly instantly as they occur, thus accelerating their response time.

What's more, because networks are highly segmented in a zero-trust approach, attackers are limited in how far they can move through the network laterally if they should gain access, which significantly reduces the surface area of an attack.

Under a zero-trust approach, IT staff have full visibility into the devices on their network — and they're constantly tracking these devices.

By limiting the attack surface and accelerating the response time, zero trust helps school systems minimize the damage caused by a successful cyberattack.

"Many of the ways that school districts find themselves being compromised are addressed in a shift to a zero-trust architecture," Levin says.

A Roadmap for Implementing Zero Trust

Adopting zero trust is a multistep process.

ZERO TRUST IS "NOT LIKE INSTALLING A firewall," says IT consultant Joel Snyder, owner and senior partner at Opus One. "It involves moving from an old security architecture to a new one. That takes time and many steps."

Implementing zero trust is a journey. But the journey isn't necessarily linear.

"It's not so much about moving from point A to point Z," Snyder says. "It's often more cyclical in nature." School districts typically progress toward zero trust in phases. However, "phase two might involve redoing, refining or improving some of the steps from phase one," he explains.

If zero trust is best accomplished in phases, then phase one involves having sound identity and access management (IAM) practices and technologies in place.

"Identity is your base for everything to do with zero trust," Snyder says. "Decisions about when and how to micro-segment your network, that's kind of up to you. But without a good identity and access management system as the foundation, nothing else is going to work."

Moving Toward Maturity

An Executive Order issued by the Biden Administration in 2021 called on federal agencies to develop migration plans for moving toward a zero-trust architecture. To help agencies develop their plans, the Cybersecurity and Infrastructure Security Agency (CISA) created a draft version of a **Zero Trust Maturity Model** that K–12 organizations can follow as well.

CISA's model is built on five distinct cybersecurity pillars: identity, devices, network environment, application workload, and data. For each pillar, the model describes what security might look like across three stages of zero trust maturity: traditional, advanced, and optimal. (For a high-level view of this model across each maturity stage, see the sidebar.)

K–12 leaders must decide for themselves how far (and at what pace) they'd like to travel on the journey toward zero trust. "There's not one single product or approach," Snyder asserts.

A HIGH-LEVEL VIEW OF CISA'S ZERO TRUST MATURITY MODEL

PILLAR	TRADITIONAL	ADVANCED	OPTIMAL
IDENTITY	Password or multi-factor authentication (MFA) Limited risk assessment	MFA Some identity federation with cloud and on-premises systems	Continuous validation Real-time machine learning analysis
DEVICES	Limited visibility into compliance Simple inventory	Compliance enforcement employed Data access depends on device posture upon first access	Constant device security monitoring and validation Data access depends on real-time risk analytics
NETWORK ENVIRONMENT	Large macro-segmentation Minimal internal or external traffic encryption	Defined by ingress/egress micro-perimeters Basic analytics	Fully distributed ingress/egress micro-perimeters Machine learning-based threat protection All traffic is encrypted
APPLICATION WORKLOAD	Access based on local authorization Minimal integration with application workflow Some cloud accessibility	Access based on centralized authorization Basic integration into application workflow	Access is authorized continuously Strong integration into application workflow
DATA	Not well inventoried Static control Unencrypted	Least privilege controls Data stored in cloud or remote environments are encrypted at rest	Dynamic support All data are encrypted

Source: CISA

Securing the Network Edge

Here's what to look for in an authentication solution.

ZERO TRUST ACKNOWLEDGES THERE IS no longer a traditional network perimeter to be defended because applications now exist in the cloud and users can log into the network from any location. Basically, the network edge extends to each user, and security is achieved by authenticating users' identities.

To secure the network edge under this new paradigm, school districts need better visibility and control of who's using the network and what resources they have permission to access.

Zero trust involves authenticating users or devices whenever they try to gain access, verifying their identity and tracking their network use at every step. Once someone is granted access, their network activity is monitored to make sure they remain compliant with security policies.

Top Criteria

School districts need a robust identity and access management (IAM) solution to manage these tasks. Ideally, the platform that districts choose should employ single sign-on (SSO) technology, streamlining users' access to multiple applications with a single network login. This eliminates the bad habits that users often fall into with their passwords, such as forgetting or reusing them. For IT departments, SSO serves

as a single, unified point of visibility for network authentication and access logs.

An effective IAM solution also uses multi-factor authentication (MFA) to ensure that users really are who they say they are. Aside from a network password, authentication factors might include a specific device or location, a security key or a fingerprint, for example.

To help K–12 leaders choose a high-quality IAM solution that meets their needs, here are some key questions to ask:

- **Does the solution ensure secure logins from any location, on or off premises, using FIDO-based security keys? (FIDO stands for Fast ID Online, an open industry standard for strong authentication.)**
- **Can the solution provide access control for both managed and unmanaged devices?**
- **Can the solution verify the security posture of all devices trying to access the network? For instance, can it ensure that these devices have critical software patches or endpoint security software installed?**
- **Does the solution alert you to unusual or suspicious login activity? Can it detect and automatically alert administrators to risky behaviors or events, such as enrollment of a new device or a device logging in from an unexpected location?**
- **Can you create and enforce stricter policies and controls for environments or applications with highly sensitive data, such as financial information?**
- **Does the solution provide adaptive policies and controls for different user groups or situations? (For instance, allowing users to authenticate less often when using the same device or letting users access certain applications only from district-managed devices.)**

Zero trust acknowledges there is no longer a traditional network perimeter to be defended, because applications now exist in the cloud and users can log into the network from any location.

A high-quality IAM solution reduces the risk of a data breach by verifying users' identities using multiple factors. It gives you full visibility into all devices to make sure they meet your security standards before logging on. It lets you enforce access and security policies based on various user groups, devices and application risks. And it streamlines the workflow for users with an SSO dashboard for accessing all applications.

4 Keys to Success with Zero Trust

These strategies will help K–12 schools navigate the zero trust journey.

WHILE ZERO TRUST CAN BE CHALLENGING TO implement, its potential for reducing risks and improving network security is significant. Here are four keys to success when moving ahead with a zero-trust approach.

1: Focus on change management.

When embarking on any large-scale IT initiative, school districts sometimes focus too much on the technology and not enough on the people and processes behind it. Taking a human-centered approach will greatly increase the likelihood of success.

To ensure a smooth transition, IT staff should anticipate the impact that zero trust might have on various school district operations and should plan accordingly. For instance, a business department that is processing payments might be sensitive to changes that could create problems for users.

"Zero trust is as much a cultural innovation as a technological one," consulting firm Deloitte **observes**. "Getting people to change their behavior requires communication and training." School district IT departments should lead a training and awareness campaign before

Not only are network users coming and going all the time, but their roles within the district frequently change as well.

implementing zero trust, so students, employees, and other stakeholders understand the purpose of this approach, how zero trust works, and where to get help if they encounter any problems.

2: Have good inventory control.

For zero trust to work well, "you have to get rid of applications that provide implicit trust," says IT consultant Joel Snyder, "or you have to segment them off from the other parts of your network." This requires having good visibility into the applications running on your network and a system for cataloging what these applications are and what ports they're using.

3: Keep user profiles up to date.

Under a zero-trust approach, permission to access data and resources is granted based on factors such as a user's role at the institution. This can be challenging to manage, especially within a K–12 setting — where student turnover happens every year and substitute teachers and volunteers frequently come and go.

Not only are network users coming and going all the time, but their roles within the district frequently change as well. These changes might require updates to their network permissions.

"Identity management can be an incredibly laborious and tedious process," says Doug Levin, national director for K12 SIX. "It involves close coordination with human resources departments." For zero trust to work effectively, school districts will need to invest sufficient time and resources in keeping user profiles up to date.

4: Make sure vendors are on board.

K–12 districts have transitioned to more cloud-based software in recent years, and IT leaders must make sure the cloud services they're using support a zero-trust model.

"All of your software-as-a-service vendors have to be on board with whatever you're doing for zero trust," Snyder says. "If a vendor is not going to be participating in the central authentication store you're using for identity and access management, then you've got a problem."

Snyder says he's working with a school district that's using a cloud-based administrative system from a small service provider. "I can tell from talking to the vendor that they don't really care about security," he notes. "Having your SaaS vendors and your IT department on the same page and at the same level of concern about security is critical."