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.

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

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.

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.