K-12 BLUEPRINT

A Phishing Expedition | Sponsored by CDW Education

May 2023 | Prepared by Clarity Innovations, Inc.

Establishing a Zero Trust Ecosystem

The security needs of education are every bit as unique as each student in the classroom...and there are several elements necessary to create a "perfect storm" of security, one that is commonly referred to as a Zero Trust Ecosystem.

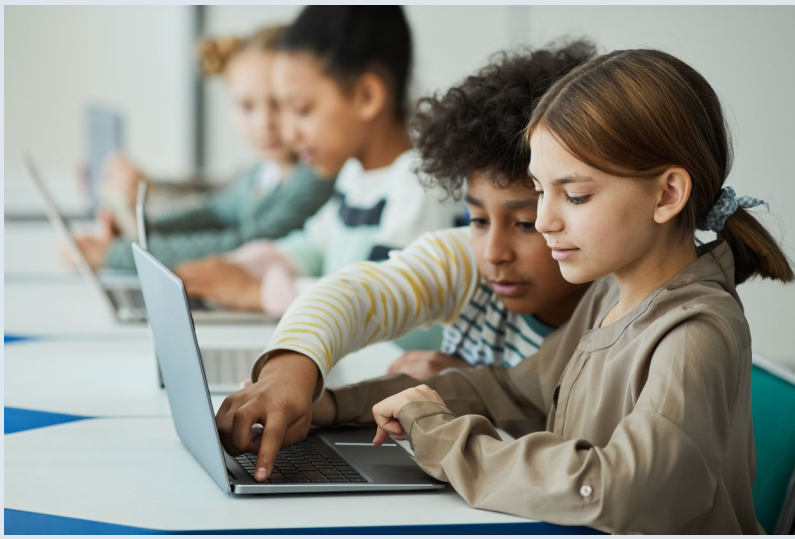
What is Zero Trust?

Zero trust is exactly that: having no trust in anyone or anything that could possibly breach data security. This bold approach requires an integrated defense strategy that takes into account such threats to security as the cloud, where sensitive data is shuttled back and forth (oftentimes between an on-premises school network and outside locations), making seamless protections "must haves" not "nice-to-haves."

A Zero Trust model forges a data-centric perimeter around school information comprised of powerful encryption methods—as well as stringent authentication techniques—as sloppy user access protocols undermine any security strategy. Modern security requires visibility into who has the potential to access data, while only allowing access when all risk factors are properly evaluated.

In a school or district's data ecosystem, users, email and cloud application can all be exploited as potential entry points. The Zero Trust model is based upon intelligent authentication and strict network controls that segment and isolate data.

Zero Trust assumes that a network must verify anyone and anything trying to connect before granting access. Connectivity is only granted after identity is authenticated, the security posture of the connected device is verified, and the user is authorized to access the desired application, service or information.



Practice Makes Perfect

The following practices work together to ensure Zero Trust. They include:

- **Leadership Practices**: Education leaders who embody and promote a security-first outlook
- **Professional Development Practices**: Comprehensive staff training on the latest security practices
- **Business Practices**: Ensuring that administrators and support staff follow sound security protocols
- **Classroom Practices**: Safeguards and strategies to protect student data in the classroom
- **Data Security Practices**: School-and district-wide protocols implemented by IT.

People Make (and Break) a Zero Trust Environment

Safeguarding school data with strong user authentication and strict access management is vital to a Zero Trust ecosystem. Schools need to accurately control who gets what access, to which data—and when—all the while protecting users from phishing attacks and credential theft. And this level of defense extends to every device in a school's network, requiring the vetting of every device (ensuring it's trustworthy) before granting access then isolating, securing, and controlling every device touching the network at all times.

Cloud computing and hybrid IT environments are now the norm. To ensure appropriate and protected connectivity to applications and information, schools need solutions that can extend proven data center security to the cloud. Then there are risks posed by common peripherals such as printers, smart TVs, security cameras, and others. The security of these systems, from changing default passwords to installing patches, is often an afterthought and many school IT professionals are unaware of the many ways these devices are connecting to internal systems and data.

> **"A Zero Trust security solution must account for user experience, endpoint diversity and threats, hybrid cloud migration, platform and policy unification and ecosystem interoperability."**

An effective Zero Trust solution simplifies the secure use of mobile devices by offering automated, self-service onboarding of a variety of these devices. Mobility enablement also requires the ability to ensure compliance by isolating work applications and data from private applications in BYOD (Bring Your Own Device) scenarios.

New Threats. New Solutions.

Cyberthreats and security breaches are becoming ever-more sophisticated, such as hiding in encrypted traffic to evade detection for one. The key is to grant visibility to these attacks while aiding in detection and response if already exposed. It is also vital to provide a seamless, simple user experience that users will actually use, because if the experience is non-intuitive, users will seek risky workarounds to do what they need to do.

For instance, end users might want the convenience of Single Sign On (SSO) to applications across devices, operating systems and application infrastructures, while IT administrators might demand an intuitive way to orchestrate all elements of access security.

The balance of ensuring security while granting accessibility, mobility and flexibility is a precarious one, especially in the face of evolving data threats. A Zero Trust security solution must account for user experience, endpoint diversity and threats, hybrid cloud migration, platform and policy unification and ecosystem interoperability. With all of these elements in place, administrators, teachers and students can enjoy productivity and freedom while school IT can better mitigate risks such as malware and data loss.

Learn more about configuring and managing Zero Trust Ecosystems at CDW.