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