WE GET YOU CAN'T TRUST EVERYONE ON YOUR NETWORK

Security Services and Solutions

Many enterprises have watched their network infrastructure grow increasingly complex, employing a multitude of internal networks, cloud services and even remote offices. This forces many businesses to operate in a threat-conducive environment as the traditional methods of perimeter-based network security become increasingly irrelevant.

Achieving stronger data protection in today's complex architectures requires a new approach to network security: zero-trust architecture (ZTA).

THE BASICS OF ZERO-TRUST

Zero-trust works under the assumption that a network is innately hostile, and that users and devices must prove their identities to gain trust.

Transitioning to a ZTA often involves a paradigm shift and cannot be accomplished without implementing effective information security and resiliency practices.

WHY CDW FOR ZTA?

With a broad portfolio of partner solutions surrounding device, user, session, application and data trust, CDW is uniquely positioned to help you through the entirety of your ZTA journey.

A partnership with CDW can help you roadmap, design and implement zero-trust across your enterprise's entire network, bringing your organization:

- **Enhanced visibility through analytics:** Gather credible insights into who is accessing your information and when.

- **Reduced risk:** Cut down on the possibility of insider threats and maintain business continuity and agility.

- **Permission controls:** Have the ability to grant access from anywhere and allow partner connections with limited access (if any) to mission-critical systems.

- **Ensured security:** Gain greater control over your entire cloud environment.

WHO BENEFIT FROM ZERO-TRUST?

This set of guiding principles in network infrastructure design and operation can be used to improve the security of any organization. And while a full instance of zero-trust cannot be achieved without an infrastructure rebuild, many modern organizations already have elements in place that can bring some of the advantages of a ZTA to legacy environments.

When paired with existing cybersecurity practices — identity and access management, security policies, continuous monitoring — a zero-trust philosophy can help mitigate risk by minimizing threats through network segmentation and reinforcing an organization's overall security posture.

Contact your CDW account team to speak with a solutions architect about zero-trust.

CDW · PEOPLE WHO GET IT