Zero Trust: The Foundation for Secure Business Enablement

CoAction
zscaler

IDC analysts recently examined the future of zero trust and shared their thoughts on how it will impact enterprice security.

The threat of landscape is rapidly accelerating.

80%
Increase in ransomware attacks in the last year

314%
Increase in attacks over encrypted channels

436%
Increase in phising attacks in retail and wholesale industries

Perimeter security architectures were designed for the past.

Perimeter-based secuirty was designed for a time when employees primarily worked in the office to access applications and resources in the data center.

Today's hybrid workplace is much more complex.

Users are working from everywhere, using multiple device, and accessing data and applications spread across SaaS, data centers, and public clouds.

Yesterday's defenses are insufficient.

Firewalls, virtual firewalls, VPNs, and other perimeter-oriented defenses are incapable of stopping dynamic and persistent threats.

FOUNDATIONAL ELEMENTS OF ZERO TRUST

- Granular authorization
- Strong identity and authentication
- Context-based policies
- Universal application of zero trust
- Continuous threat detection/protection
- "Need to know" access only

CoActionTech.com
Sales@CoActionTech.com

CoAction