

What is True Zero Trust?

Businesses are embracing zero trust to accelerate secure digital transformation. But navigating the sea of “zero trust” solutions can be a challenge. It’s important to know what differentiates a true zero trust solution from one that merely uses the name.

True Zero Trust

DOES NOT

Use perimeter-based firewalls and VPNs to extend a flat network to remote users, which increases the attack surface.

✗ Trust implicitly

Assume known users, apps, and devices are trustworthy

✗ Put users on a network

Make use of a routable network for user and app traffic, which facilitates lateral movement

✗ Allow passthrough traffic

Allow encrypted traffic without inspecting for threats and sensitive data

DOES

Assume that everything is hostile or compromised, only granting access based on whether it can:

✓ Verify identity and context

Terminate the connection and verify identity and context by understanding the ‘who’, ‘what’, and ‘where’ of the request

✓ Control content and access

Evaluate the risk associated with connection requests and inspect traffic for cyberthreats and sensitive data

✓ Enforce policy per-session decision, and enforcement

Enforce policy before connecting to internal or external applications

Discover the One True Zero Trust: The Zscaler Zero Trust Exchange



Experience zero trust without compromise and let your business achieve a seamless, secure, cost effective zero trust architecture that turns your IT infrastructure into a digital transformation accelerator.