Zero Trust (ZT)

Return to Glossary

Definition 1

Zero Trust (ZT) also **Zero-Trust**, provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

Source: NIST: SP 800-207: Zero Trust Architecture (ZTA)

Definition 2

Zero Trust (ZT) is a data-centric Cybersecurity strategy for enterprise computing that assumes no end-user, Network Device, Mobile Device, Peripheral Device, or Storage Device, Web Service, or network connection can be trusted – even when an access request originates from within the organization's own network perimeter.

The Zero Trust Security Model has evolved to take into account distributed computing and an ever-expanding attack surface. Unlike a Single Sign-On (SSO) strategy that allows users to log in once and access multiple network services without re-entering authentication factors, **Zero Trust** requires authentication factors to be verified – and re-verified – each time a network resource is requested.

Because untrusted threat actors exist both internally and external to a network, **Zero Trust** supports the following principles:

- Never Trust
- Always Verify
- Enforce Least Privilege

An important goal of the Zero Trust Model is to prevent malicious actors from using a compromised account to move laterally across a target network.

Source: https://www.techopedia.com/definition/34572/zero-trust-zt