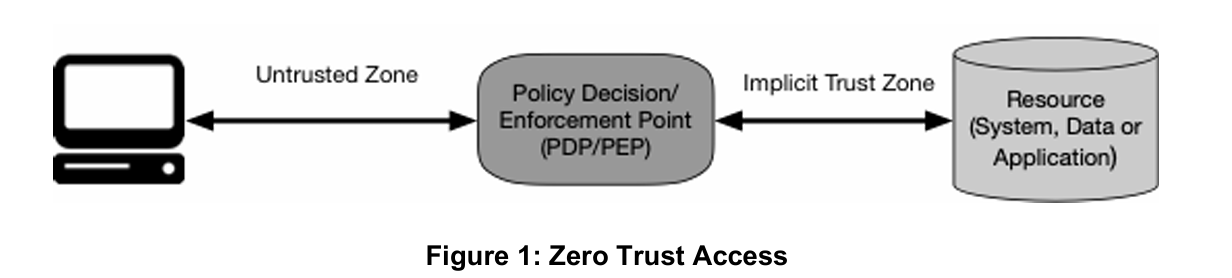
ZT is not a single architecture but a set of guiding principles for workflow, system design and operations that can be used to improve the security posture of any classification or sensitivity level

An operative definition of zero trust and zero trust architecture is as follows: Zero trust (ZT) 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. Zero trust architecture (ZTA) is an enterprise’s cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.



All data sources and computing services are considered resources.

All communication is secured regardless of network location.

Access to individual enterprise resources is granted on a per-session basis.

Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.

The enterprise monitors and measures the integrity and security posture of all owned and associated assets.

All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

The entire enterprise private network is not considered an implicit trust zone.

Devices on the network may not be owned or configurable by the enterprise.

No resource is inherently trusted.

Not all enterprise resources are on enterprise-owned infrastructure.

Remote enterprise subjects and assets cannot fully trust their local network connection.

Assets and workflows moving between enterprise and nonenterprise infrastructure should have a consistent security policy and posture.