

Zero Trust Security:

Zero Trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

Traditional IT network security trusts anyone and anything inside the network. A Zero Trust architecture trusts no one and nothing.

Think of Zero Trust Security like a high-security building. Even if you're inside, you still need to show your ID and get permission to enter different rooms.

Zero Trust security means that no one is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources on the network.

- o Verify Identity
- o Continuous monitoring and validation
- o Least privilege
- o Device access control
- o Micro segmentation
- o Multi-factor authentication (MFA)
- o Access Controls
- o Encryption
- o Device Health Verification

A zero trust architecture follows the maxim "Never Trust, Always Verify."

