Zero Trust Architecture:

Zero trust is a cybersecurity strategy wherein security policy is applied based on context established through least-privileged access controls and strict user authentication—not assumed trust. A well-tuned zero trust architecture leads to simpler network infrastructure, a better user experience, and improved cyber threat defense.

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

Execution of this framework combines advanced technologies such as risk based multi-factor authentication, identity protection, next-generation endpoint security, and robust cloud workload technology to verify a user or systems identity, consideration of access at that moment in time, and the maintenance of system security. Zero Trust also requires consideration of encryption of data, securing email, and verifying the hygiene of assets and endpoints before they connect to applications.

Zero trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access.

A Zero Trust architecture works seamlessly for users, helps protect against cyberattacks, and simplifies infrastructure requirements.

Zero trust is a cybersecurity strategy for verifying every user, device, application and transaction in the belief that no user or process should be trusted. Zero trust is not a single technique or product, but a set of principles for a modern security policy.