What is zero trust security?

1 November 2026 · 5 min read · blogs.iictp.org/what-is-zero-trust

Zero trust is a security approach that gives no request automatic trust because of where it comes from. Every access is checked against identity, device and context, and each user or service gets only the access it needs.

TL;DR The short version

- Zero trust gives no request automatic trust because of where it comes from; every access is checked against identity, device and context.
- It answers the old model's flaw, where an attacker inside the network could move freely.
- It is an approach, not a product: start with identity by removing shared accounts and long-lived keys and adding multi-factor authentication.

Read online, listen to it, or change the text size: https://blogs.iictp.org/what-is-zero-trust

What problem does zero trust solve?

The older model trusted anything inside the company network, so once an attacker was inside they could move freely. Remote work, cloud services and stolen credentials made the network edge a poor place to put all the trust.

What are the core principles?

Verify explicitly, meaning authenticate and authorise each request using all available signals. Grant least privilege, meaning the smallest access that does the job for the shortest time. Assume breach, meaning design so that one compromised account or workload cannot reach everything.

What does it look like in practice?

People use strong authentication, including multi-factor. Services use identity-based access with short-lived credentials. The network is segmented so systems can only reach what they must, and every access decision is logged and monitored.

Is zero trust a product you can buy?

No. It is an approach that combines several controls. Vendors sell tools that help, but no single purchase delivers it.

Where should you begin?

Start with identity: remove shared accounts and long-lived keys, add multi-factor authentication, and then restrict access to the most sensitive systems first. Widen the programme as you learn what your traffic actually looks like.

Related credential: Certified Technical Practitioner. Explore the exam facts and syllabus.

Sources and further reading

1. NIST. SP 800-207, Zero Trust Architecture. csrc.nist.gov/pubs/sp/800/207/final.
2. CISA. Zero Trust Maturity Model. cisa.gov/zero-trust-maturity-model.

Published by IICTP, an independent technical credential body, on 1 November 2026. The current version of this post is at https://blogs.iictp.org/what-is-zero-trust. More guides: blogs.iictp.org.