
Pillars of Zero Trust
Users
Devices
Network/Platform
Applicatio nand Data Protection
Workload Protection
Continus Monitoring and Risk Assessment
Automation and Continus Improvement
Continuous Authentication
Zero Trust Policies Enforcement

# Zero Trust Framework

In today's evolving threat landscape, traditional security models are no longer enough. As cyber threats grow in sophistication, conventional security models that rely on perimeter defenses are no longer sufficient. This is where the concepts of Zero Trust and the Principle of Least Privilege come into play.

**Zero Trust** is a set of principles or a framework for introducing least privilege and access control, ensuring that when someone or something interacts with the environment, they have only the access they need to perform their job. In general, the Zero Trust model is based on the principle of "never trust, always verify." Unlike traditional security models that assume trust within a network perimeter, Zero Trust requires strict identity verification for every user, device, and application attempting to access resources—regardless of location (inside or outside the network).

Key components of Zero Trust include identity verification and multifactor authentication (MFA), network segmentation, data encryption, and real-time monitoring.

Complementing Zero Trust is the **Principle of Least Privilege (PoLP**). This principle dictates that users and systems should have the minimum level of access necessary to perform their functions—nothing more, nothing less.

As we move forward in an era where data is one of our most valuable assets, adopting Zero Trust and the Principle of Least Privilege is not just an option—it's a Mandatory security requirement.

# Zero Trust Framework

## Core Pillars of Zero Trust:

- **Identity Verification**
  - Every user, device, and service must be **authenticated and authorized** before accessing resources.
  - Uses **Multi-Factor Authentication (MFA), biometrics, and behavioral analytics** to ensure legitimacy.
- **Least Privilege Access**
  - Users and systems get **only the minimum access necessary** to perform their tasks.
  - **Just-In-Time (JIT) and Just-Enough-Access (JEA)** reduce exposure to threats.
- **Micro-Segmentation**
  - Breaks networks into **small, isolated zones** to prevent lateral movement by attackers.
  - Applies strict access controls between segments (e.g., separating finance from HR networks).
- **Continuous Monitoring & Risk Assessment**
  - **Real-time analytics** detect anomalies in user behavior, device health, and traffic patterns.
  - **Adaptive access policies** adjust based on risk (e.g., blocking logins from unusual locations).
- **Device Security & Compliance**
  - Ensures **endpoints (laptops, IoT, mobile)** meet security standards (patches, encryption, EDR).
  - **Zero Trust requires verifying device trustworthiness**, not just user credentials.
- **Data Protection**
  - **Encrypts data** in transit and at rest.
  - Uses **Data Loss Prevention (DLP)** to prevent unauthorized sharing.
  - Classifies data sensitivity to enforce stricter controls.
- **Zero Trust Network Access (ZTNA)**
  - Replaces traditional VPNs with **granular, app-level access**.
  - Users connect directly to apps (not the whole network), reducing attack surfaces.

# Least Privilege Principle (PoLP):

**Least Privilege Principle (PoLP): Users, systems, or processes should have only the minimum permissions necessary to perform their tasks—nothing more.**

- **Granular Access Control: Limits rights to only what's essential.**
- **Reduces Attack Surface: If an account is compromised, damage is contained.**
- **Applies to Humans & Machines: Both user accounts and software/services.**

- **Examples:**
  - **A regular employee cannot install software (requires admin rights).**
  - **A database analyst has read-only access to customer data (not write/delete).**
  - **A web server runs under a limited user account, not root/admin.**

- **Implementation Methods:**
  - **Role-Based Access Control (RBAC) – Assign permissions based on job function.**
  - **Just-In-Time (JIT) Access – Temporary elevation of privileges when needed.**
  - **Regular Permission Audits – Remove unnecessary access over time.**