# ZERO TRUST SECURITY FRAMEWORK DESIGN

**Zero Trust Security Framework Design**

1. Core Zero Trust Principles

1. **Least Privilege Access**
    - Users and applications have only the minimum permissions needed and not more than necessary.
    - Dynamic adjustments are made based on role, location, and device posture.
2. **Continuous Verification**
    - Each and Every access request is verified.
    - That includes MFA, device checks, and risk scoring.
3. **Micro-Segmentation**
    - Network divided into isolated zones to minimize lateral movement.
4. **Assume Breach**
    - Monitor and log all activities continuously.
    - Design as if attackers may already exist.
5. **Device and Endpoint Security**
    - Enforce security hygiene before granting access.
    - Use EDR and patch management.

## 2. Architecture Components Mapping

| Component | Function in Zero Trust | Tools / Services |
|---|---|---|
| IAM | Central identity repository, role-based access, policy enforcement | AWS IAM, Azure AD |
| MFA | Strengthens identity verification | Azure MFA, AWS MFA, Duo Security |
| Network Micro-Segmentation | Controls lateral movement, isolates applications | VMware NSX, Cisco Tetration |
| Continuous Monitoring & Analytics | Detect anomalies and breaches | Splunk, Azure Sentinel, AWS GuardDuty |
| Endpoint Security | Ensures device compliance and integrity | Microsoft Defender, CrowdStrike, SentinelOne |
| Policy Engine / Enforcement Point | Evaluates access requests dynamically | Zscaler, Palo Alto Prisma, Cloudflare Access |
| Access Gateway / VPN Replacement | Secure remote access | ZTNA solutions |

## 3. Layered Zero Trust Network Model

**Layer 1: User & Device Identity Layer** - Verify identity and device health. - Tools: Azure AD, AWS IAM, MFA, EDR.

**Layer 2: Policy Enforcement Layer** - Apply dynamic policies (RBAC, ABAC). - Conditional access based on user, device, location, risk.

**Layer 3: Network Segmentation Layer** - Micro-segment applications and workloads. - East-West traffic strictly controlled.

**Layer 4: Application & Data Layer** - Data access encrypted and restricted. - Monitor and log all interactions.

**Layer 5: Analytics & Continuous Monitoring Layer** - Centralized SIEM for logs. - Risk scoring, anomaly detection, automated response.

## 4. Continuous Authentication & Access Control

- **Adaptive authentication**: Step-up authentication for unusual activity.
- **Policy-based access control**: Combine RBAC and ABAC.
- Consider device posture, location, and time in access decisions.

## 5. Strategic Implementation Plan

**Phase 1: Assessment & Planning** - Map current network, users, devices, and applications. - Identify critical assets and data flows.

**Phase 2: Identity & Access Hardening** - Deploy MFA across users. - Integrate IAM with centralized directory.

**Phase 3: Network Segmentation** - Identify trust zones. - Apply micro-segmentation and firewall rules.

**Phase 4: Endpoint Security Enforcement** - Deploy EDR across endpoints. - Ensure device security posture.

**Phase 5: Policy Enforcement & Continuous Verification** - Implement ZTNA or Policy Enforcement Points. - Enable continuous monitoring and risk scoring.

**Phase 6: Monitoring & Analytics** - Integrate SIEM for centralized logging and detection. - Set up automated response for suspicious activity.

**Phase 7: Continuous Improvement** - Regular audits and red-teaming. - Adjust policies dynamically based on threat landscape.

## 6. Conceptual Diagram Layout