ENTERPRISE CYBERSECURITY STRATEGY

Zero Trust Architecture

Moving Beyond the Perimeter: From "Trust but Verify" to "Never Trust, Always Verify".

Identity First

Micro-Segmentation

Continuous Auth

Core Principles of Zero Trust

Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location.

Verify Explicitly

Always authenticate and authorize based on all available data points: user identity, location, device health, service or workload, and data classification.

Use Least Privilege

Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive polices, and data protection to secure data and productivity.

Assume Breach

Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

Authentication Models: The Front Door

Multi-Factor Authentication (MFA)

MFA requires the user to provide two or more verification factors to gain access.

- ✓ **Something you know:** Password or PIN.
- ✓ **Something you have:** Smartphone, hardware token, smart card.
- ✓ **Something you are:** Biometrics (Fingerprint, FaceID).

Role-Based Access Control (RBAC)

Access is restricted based on a person's role within the organization, enforcing least privilege.

- ✓ **Roles:** Define job functions (e.g., HR, Admin, Dev).
- ✓ **Permissions:** Define what access the role has (Read, Write, Execute).
- ✓ **Scalability:** Administrators assign roles, not individual permissions.

Designing the Zero Trust Framework

1. Identity Verification

The foundation of the framework. We move the perimeter from the network edge to the identity itself.

- ✓ IAM Integration (Okta/Azure AD)
- ✓ Single Sign-On (SSO)
- ✓ Context-Aware Access Policies

2. Micro-Segmentation

Prevents lateral movement. Even if an attacker enters the network, they are trapped in a small segment.

- ✓ VLANs & Subnets
- ✓ Software-Defined Perimeters (SDP)
- ✓ East-West Traffic Inspection

3. Encryption & Data

Protecting the asset itself. Data must be unreadable to unauthorized entities at all times.

- ✓ Encryption at Rest (AES-256)
- ✓ Encryption in Transit (TLS 1.3)
- ✓ Data Loss Prevention (DLP)

Simulation & Implementation

Building the Environment

We simulate a corporate network using virtualization tools to test policies safely.

01 **Virtualization Layer**

Using VMware or VirtualBox to create isolated segments (HR, Finance, IT).

02 **Containerization**

Deploying services via Docker to simulate application workloads.

Applying IAM Policies

Configuring the logic that decides who gets in and who stays out.

```
// Pseudocode Policy Example

IF user.group == "Finance"
AND device.isManaged == TRUE
AND location == "Office_VPN"
AND auth.mfa == "Verified"
THEN allow.access(Finance_DB)
ELSE deny.access
```

Threat Testing & Validation

Scenario A: The Insider Threat

A user in "Marketing" attempts to access "Engineering" blueprints via lateral movement.

Attack Simulation
Compromised credential attempts SSH connection to Engineering Server IP.

Zero Trust Response
Blocked. Network Micro-segmentation firewall rules drop traffic. IAM verifies user role does not match resource required role.

Scenario B: External Credential Theft

Attacker steals valid username/password via phishing and attempts remote login.

Attack Simulation
Login attempt from unrecognized device/IP address using correct password.

Zero Trust Response
Blocked. Conditional Access Policy fails. Device is unmanaged, and MFA challenge is triggered but not completed.

Results & Continuous Improvement

Documented Success

- ✓ 100% of unauthorized lateral movement attempts blocked by micro-segmentation.
- ✓ Credential theft rendered ineffective without MFA token.
- ✓ Full audit trail visibility achieved.

Challenges Identified

- ✓ Legacy applications may not support modern IAM protocols (SAML/OIDC).
- ✓ User friction increased initially due to aggressive MFA prompts.

Future Improvements

- ✓ **Adaptive Auth:** Use AI to reduce MFA prompts for low-risk behavior.
- ✓ **SIEM Integration:** Automate response to detected anomalies.
- ✓ **Passwordless:** Move to FIDO2 hardware keys.