Zero Trust Architecture

A Comprehensive Guide to understand Zero Trust Architecture.

Authored by: Khushi Malhotra

Introduction to Zero Trust

- Zero Trust is a cybersecurity framework that assumes no user or device should be trusted by default, even if inside the network perimeter.
- It challenges the outdated concept of trusting users within a corporate network.
- Adopted to counter modern threats like insider attacks and lateral movement within networks.

Why Zero Trust is Needed

EVOLVING CYBER THREATS

- Modern attackers exploit trusted systems.
- **Example:** SolarWinds attack infiltrated through legitimate software updates.

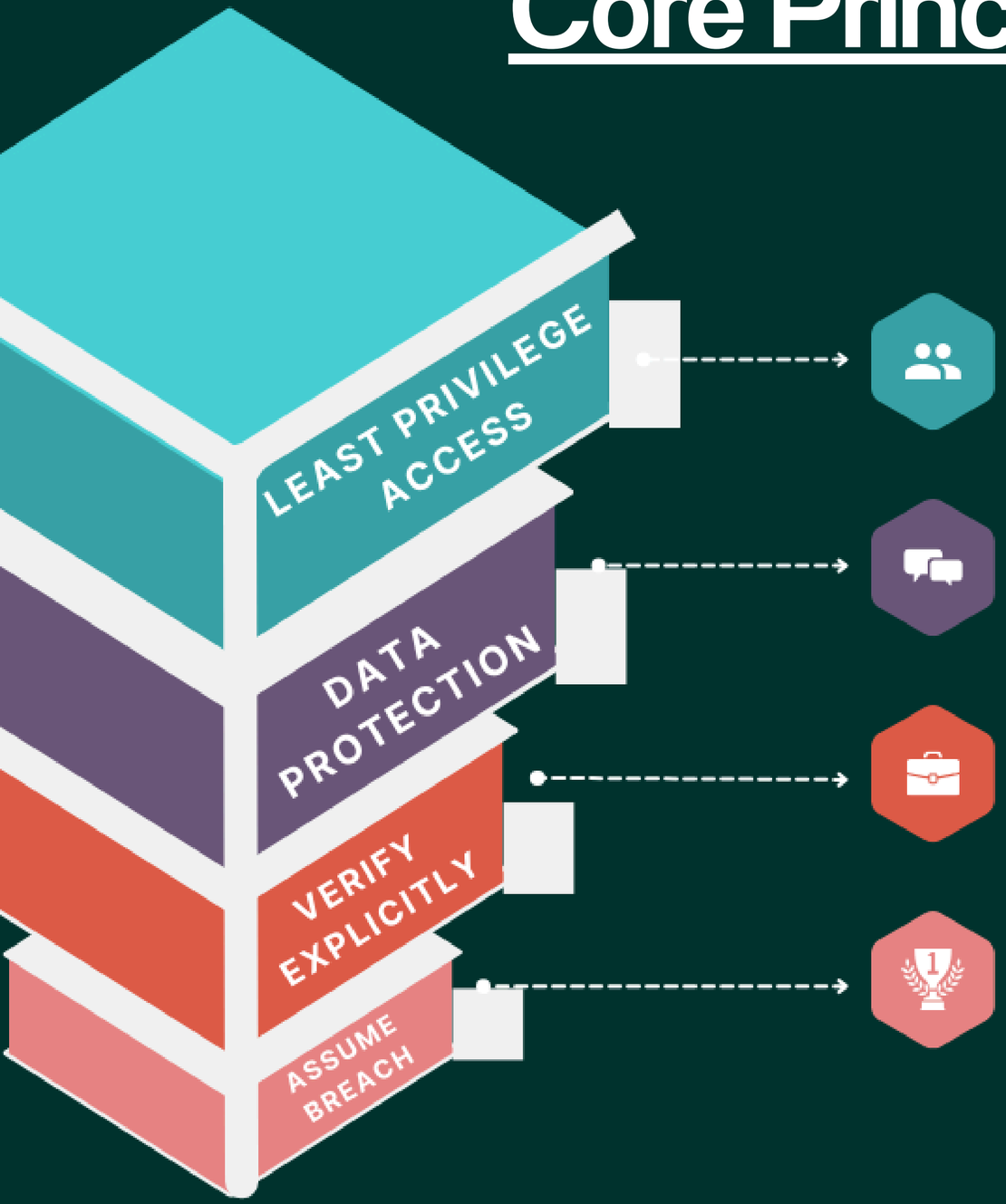
REGULATORY COMPLIANCE

- Meets security standards like GDPR and HIPAA.
- **Example:** Healthcare organizations protecting patient records across locations.

MINIMIZING BREACH IMPACT

- Segmented access limits attackers' movement.
- **Example:** Ransomware contained to one system instead of spreading network-wide.

Core Principles of Zero Trust



- Limit access to only what's necessary for a specific task or role.
- Example: An intern only accesses files relevant to their project, not the entire database.

- Encrypt and classify data to restrict unauthorized access and sharing.
- Example: Sensitive files requiring encryption keys to view or edit.

- Always authenticate and authorize based on available data points.
- Example: MFA required even for internal systems.

- Operate under the assumption that a breach has already occurred.
- Example: Continuous monitoring to detect anomalies, like unusual login times.

Zero Trust vs. Traditional Security

Zero Trust	Traditional Security
Continuous verification of users/devices	Trusts devices/users once inside the network.
Least privilege access for all users.	Grants broad access after initial authentication.
No network perimeter; security enforced everywhere.	Focused on perimeter defense (firewalls, VPNs).
Uses multi-factor authentication (MFA).	Relies mainly on firewalls and VPNs.

Components of Zero Trust

Identity and Access Management (IAM)

Multifactor authentication, Single Sign-On (SSO).

Device Security

Endpoint detection, regular device health checks.

Micro-Segmentation

Dividing the network into isolated zones.

Data Protection

Encryption, classification, and monitoring.

Threat Detection and Response

Continuous monitoring for anomalies.

How Zero Trust Works

1

User or Device Requests Access

A user or device attempts to access a resource or network.

2

Authentication via Multi-Factor Authentication (MFA)

A robust authentication process is triggered,quirinultiple factors (e.g., pas)

3

Access is Granted Based on Roles and Permissions

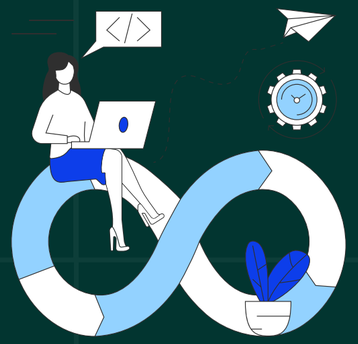
Users are granted access only to the specific resources they need.

4

Dynamic Access Control

Access permissions are continuously re-evaluated based on real-time information.

Benefits of Zero Trust

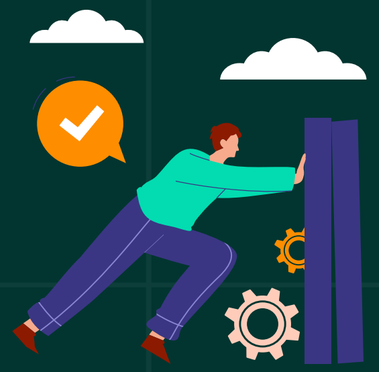


Better Visibility

Continuous monitoring of users and devices.

Compliance-Friendly

Aligns with GDPR, HIPAA, and other regulations.



Resilience

Limits damage even if a breach occurs.

Challenges to Implementation

Complexity

Requires a complete overhaul of legacy systems.

Cultural Resistance

Employees may resist additional authentication steps.

Integration

Ensuring compatibility with existing systems.

Real-Life Case Study

Overview: Google adopted Zero Trust with BeyondCorp to secure access to internal resources for remote employees, eliminating reliance on traditional network perimeter security.

Challenge

Securing access to internal resources for remote employees without relying on traditional security perimeters.

Solution

Google implemented BeyondCorp, a Zero Trust model that focuses on continuous verification of users and devices.

How it Works

- MFA and device health checks authenticate users.
- Least-privilege access is enforced for better control.

Outcome

- Improved security for remote work.
- Simplified access without relying on VPNs.

Future Trends in Zero Trust

01

AI Security

Automates access and threat detection.

02

IoT Protection

Secures all connected devices.

03

Cloud Integration

Ensures Zero Trust for multi-cloud systems.

Zero Trust in Everyday Life

ID Verification (Authentication)

Just like you need an ID to enter a building, Zero Trust requires users and devices to verify their identity.

Restricted Floors (Least Privilege)

Access is given only to necessary resources, just like restricted building floors.

Security Guards Monitoring (Continuous Monitoring)

It ensures security, like guards watching for unauthorized.

Conclusion

01 Eliminates Implicit Trust

Shifts from trust-based to verification-based security.

02 Future-Ready

Adapts to evolving technologies and security needs.

03 Enhances Resilience

Minimizes damage even in case of a breach.

04 Strengthens Security

Protects against modern threats like insider attacks.

THANK YOU

Never Trust, Always Verify:
Redefining Security in the Digital Age

Authored by: Khushi Malhotra