Zero-Trust Architecture Scenario using AWS Services

1. Introduction

This scenario outlines the implementation of a Zero-Trust security architecture for a cloud-based web application hosted on AWS.
The goal is to protect corporate and customer resources through continuous authentication, least-privilege access control,
micro-segmentation, encryption, and continuous monitoring and response. The design leverages AWS native security services to
create a scalable and compliant Zero-Trust environment.

2. Identity and Access Management

• Objective: Strengthen identity verification and enforce least privilege across all access points.

• Action Items:
- Implement AWS IAM Identity Center (SSO) for workforce authentication with enforced MFA and role-based access.
- Use AWS IAM policies with context-based conditions (ABAC) and Service Control Policies (SCPs) for account-level control.
- Manage application users with Amazon Cognito for user registration, MFA, and secure JWT-based authentication.
- Rotate access keys automatically with AWS Secrets Manager and eliminate long-lived credentials.

3. Network Segmentation

• Objective: Isolate workloads and control network communication between application tiers.

• Action Items:
- Build multi-tier architecture within Amazon VPC using public, private, and database subnets.
- Control east-west and north-south traffic using AWS Network Firewall and Security

Groups.
- Enable private service connectivity via AWS PrivateLink and enforce endpoint policies.
- Deploy AWS Verified Access or Client VPN for secure, identity-based remote access.

4. Data Protection and Encryption

• Objective: Ensure that all data is protected both in transit and at rest.

• Action Items:
- Encrypt data at rest using AWS Key Management Service (KMS) for S3, EBS, and RDS resources.
- Use TLS 1.2+ for all data in transit with certificates managed by AWS Certificate Manager (ACM).
- Manage and rotate credentials with AWS Secrets Manager and enforce encryption in all storage layers.
- Enable S3 Block Public Access and enforce bucket policies tied to VPC endpoints.

5. Monitoring and Threat Detection

• Objective: Continuously monitor, detect, and respond to security events across the AWS environment.

• Action Items:
- Enable AWS CloudTrail for auditing all API and console activities across accounts.
- Deploy AWS GuardDuty for threat detection and AWS Security Hub for centralized findings aggregation.
- Configure AWS Config for compliance monitoring and AWS CloudWatch for metrics, logs, and alarms.
- Automate incident response using AWS Lambda and Systems Manager runbooks triggered via EventBridge.

6. User Education and Awareness

• Objective: Promote security awareness and ensure users understand Zero-Trust principles and best practices.

• Action Items:
 - Conduct periodic security awareness training using AWS Well-Architected Labs and AWS Skill Builder.
 - Provide guidance on MFA usage, phishing detection, and secure password management.
 - Establish clear communication channels for incident reporting and suspicious activity notifications.

7. Regular Security Assessments and Updates

• Objective: Maintain and enhance Zero-Trust security posture through continuous assessments and updates.

• Action Items:
 - Perform regular vulnerability scans and compliance audits using Amazon Inspector, Prowler, and Security Hub standards.
 - Stay updated with AWS security advisories and apply patching to EC2, EKS, and RDS resources promptly.
 - Continuously review IAM roles, SCPs, and GuardDuty findings to ensure compliance with least privilege and Zero-Trust goals.

8. Collaboration and Governance

• Objective: Foster collaboration between IT, Security, and Compliance teams to maintain alignment with Zero-Trust principles.

• Action Items:
 - Implement AWS Control Tower and AWS Organizations for multi-account governance.
 - Use Service Control Policies (SCPs) and tagging standards for unified compliance enforcement.
 - Integrate dashboards via AWS Security Hub and Amazon QuickSight for executive-level visibility.
 - Encourage cross-team collaboration for incident response, risk assessment, and continuous improvement.