AWS Zero-Trust Implementation Roadmap

Implementing a Zero-Trust security model using AWS requires careful planning and execution across multiple phases,
including identity and access management, network segmentation, encryption, monitoring, and response.
Below is a detailed roadmap and plan of action with timelines for each phase, tailored for a beginner or small team environment.

Phase 1: Identity and Access Management

Timeline: Week 1–2

Objective: Set up centralized identity management and authentication using AWS IAM and related services.

Action Items:
• Deploy AWS IAM Identity Center (SSO) for workforce authentication and single sign-on access.
• Configure IAM policies with least privilege and MFA enforcement.
• Use Amazon Cognito for application-level user authentication and JWT token issuance.
• Implement conditional access through IAM context keys and device posture checks (via Verified Access).

Tasks:
Week 1:
• Set up AWS Organizations and enable AWS IAM Identity Center (SSO).
• Create user groups and permission sets aligned with roles (Admin, Developer, Auditor).
• Enable MFA for all users in IAM Identity Center.

Week 2:
• Configure IAM policies using ABAC (attribute-based access control).
• Set up Cognito user pool and enable MFA for application users.
• Test access flows and validate least privilege policies.

Phase 2: Network Segmentation

Timeline: Week 3–4

Objective: Implement network segmentation using Amazon VPC and Security Groups.

Action Items:
• Create separate VPC subnets for frontend, application, and database tiers.
• Configure Security Groups (SGs) and AWS Network Firewall to control traffic flow.
• Use VPC Flow Logs for visibility into allowed/denied traffic.

Tasks:
Week 3:
• Create VPC with subnets (Public for ALB, Private for App/DB).
• Associate Security Groups with each subnet and set initial ingress/egress rules.

Week 4:
• Refine Security Group rules based on application needs (e.g., ALB:443 → App:8443, App → DB:5432).
• Deploy AWS Network Firewall for east-west traffic inspection.
• Enable VPC Flow Logs and review traffic metrics in CloudWatch.

Phase 3: Encryption and Data Protection

Timeline: Week 5–6

Objective: Secure data at rest and in transit using AWS KMS and encryption services.

Action Items:
• Set up AWS Key Management Service (KMS) for centralized key management.
• Encrypt data at rest across S3, RDS, and EBS volumes.
• Manage credentials and secrets securely using AWS Secrets Manager.
• Enforce TLS (1.2+) for all in-transit communications with certificates from AWS Certificate Manager (ACM).

Tasks:
Week 5:
• Create AWS KMS Customer Managed Keys (CMKs) and define key policies.
• Integrate KMS with S3, RDS, and EBS encryption configurations.

Week 6:
• Enable automatic key rotation and enforce encryption policies.
• Configure AWS Secrets Manager for API keys and DB credentials.
• Verify encryption compliance using AWS Config rules.

Phase 4: Monitoring and Response

Timeline: Week 7–8

Objective: Establish continuous security monitoring and automated incident response using AWS services.

Action Items:
• Enable AWS CloudTrail for activity logging across all accounts and regions.
• Configure AWS GuardDuty for anomaly and threat detection.
• Integrate AWS Security Hub and AWS Detective for centralized investigation and correlation.
• Create CloudWatch dashboards and alarms for critical events.
• Automate incident response with EventBridge and AWS Systems Manager.

Tasks:
Week 7:
• Enable CloudTrail organization trail and connect GuardDuty to Security Hub.
• Configure Config rules for compliance checks (e.g., public S3 buckets, unencrypted EBS).

Week 8:
• Create CloudWatch metrics and alarms for high-risk activities.
• Set automated remediation via Lambda or SSM runbooks.
• Test detection and response workflows using simulated incidents.

Phase 5: Ongoing Maintenance and Review

Timeline: Week 9 onwards

Objective: Maintain continuous monitoring, policy improvement, and staff training for Zero-Trust posture.

Action Items:
• Conduct regular security assessments using AWS Security Hub, Inspector, and Prowler.
• Review IAM roles, SCPs, and SG rules quarterly for compliance.
• Update configurations based on AWS best practices and threat intelligence.
• Provide recurring security awareness training for users via AWS Skill Builder and internal sessions.

Tasks:

Ongoing:
• Review GuardDuty and Security Hub findings weekly.
• Update IAM and Security Group configurations as environment evolves.
• Apply patches promptly using AWS Systems Manager Patch Manager.
• Continuously monitor AWS Health Dashboard and security bulletins.

Summary

By following this AWS Zero-Trust roadmap, organizations can systematically implement security controls across identity,
network, data protection, and monitoring layers. The roadmap ensures alignment with AWS Well-Architected Security Pillar
principles and promotes continuous improvement of the Zero-Trust posture.