Complete List of AWS Security Options

1. Identity & Access Security

- AWS IAM (Identity and Access Management): Create fine-grained roles/policies, apply least privilege, enable MFA.
- AWS IAM Identity Center (formerly SSO): Centralized access management across AWS accounts.
- AWS Organizations & SCPs: Enforce security policies across multiple accounts.
- AWS Directory Service / Cognito: Manage user identity and authentication for applications.

2. Network Security

- Amazon VPC: Network isolation, private/public subnets, NAT gateways.
- Security Groups & NACLs: Instance- and subnet-level firewalls.
- AWS WAF (Web Application Firewall): Protect web apps from SQL injection, XSS, bots.
- AWS Shield (Standard & Advanced): DDoS protection.
- AWS Firewall Manager: Centralized management of WAF, Shield, security groups across accounts.
- PrivateLink, VPN, Direct Connect: Secure hybrid connectivity.

3. Data Protection

- AWS KMS (Key Management Service): Centralized encryption key management.
- AWS CloudHSM: Dedicated hardware security module for regulatory compliance.
- S3 Security: Block public access, encryption (SSE-S3, SSE-KMS), versioning, MFA delete.
- AWS Secrets Manager & Systems Manager Parameter Store: Secure storage and rotation of secrets.
- AWS Certificate Manager (ACM): Manage SSL/TLS certificates.

4. Threat Detection & Monitoring

- Amazon Inspector: Automated vulnerability scanning for EC2, Lambda, and ECR containers.
- Amazon GuardDuty: Threat detection using VPC flow logs, DNS logs, CloudTrail events.
- Amazon Detective: Investigate and analyze GuardDuty findings with graphs and link analysis.
- AWS Security Hub: Central dashboard for all security findings (GuardDuty, Inspector, IAM Access Analyzer, etc.).
- AWS Macie: Detects and protects sensitive data in S3 (e.g., PII, PHI).
- CloudTrail: Full audit logs of API calls and activities across AWS.
- CloudWatch & CloudWatch Logs: Monitoring, alarms, metric analysis, anomaly detection.
- AWS Config: Tracks configuration changes, enforces compliance rules, detects drift.
- AWS IAM Access Analyzer: Detects overly permissive IAM roles, S3 buckets, and KMS keys.

5. Infrastructure & Application Security

- AWS Systems Manager Patch Manager: Automates patching of EC2 and on-prem servers.
- Amazon Inspector: Continuous vulnerability management.
- AWS CodeGuru Security: Scan application code for security flaws.
- ECR Image Scanning (via Inspector): Find vulnerabilities in container images.
- AWS Proton / ECS / EKS security best practices: Secure container orchestration.

6. Resilience, Backup & Recovery

- AWS Backup: Centralized, automated backup across AWS services.
- Multi-AZ & Multi-Region Architectures: High availability & disaster recovery.
- S3 Cross-Region Replication & Versioning: Data resilience.
- Auto Scaling & Load Balancing: Reduce downtime during attacks/incidents.

7. Compliance & Governance

- AWS Artifact: Access compliance reports (SOC, PCI, HIPAA).
- AWS Audit Manager: Automates evidence collection for audits.
- AWS Well-Architected Framework (Security Pillar): Blueprint for security best practices.