Sergio Cambelo
BLOG

AWS Security Checklist for Production

A practical, opinionated checklist for teams running production workloads on AWS

cambelo.com

Practical AWS networking and security content

IAM & Identity

Root Account

- [ ] MFA hardware token (YubiKey) on all root users
- [ ] No access keys on root accounts
- [ ] Root email is a distribution list, not a personal inbox
- [ ] Centralized root access management enabled (AWS Organizations)
- [ ] Root usage monitored via CloudTrail alerts

Access Management

- [ ] IAM Identity Center (SSO) as single entry point
- [ ] Permission sets follow least-privilege (no AdministratorAccess in prod)
- [ ] Just-In-Time (JIT) access for elevated permissions — time-boxed, audited
- [ ] Service-linked roles preferred over custom roles where available
- [ ] No long-lived access keys — use IAM roles + temporary credentials

Preventive Controls

- [ ] SCPs enforcing guardrails at Organization level
- [ ] Deny regions not in use
- [ ] Deny disabling CloudTrail / GuardDuty / Config
- [ ] Deny public S3 buckets at org level
- [ ] Deny leaving the Organization

Networking

VPC Design

- [ ] Multi-AZ deployment for all production workloads
- [ ] Private subnets for compute, public only for ALB/NLB
- [ ] No IGW in workload accounts (egress via centralized inspection VPC)
- [ ] VPC Flow Logs enabled (at least REJECT, sent to S3 or CloudWatch)
- [ ] DNS resolution and DNS hostnames enabled

Connectivity

- [ ] Transit Gateway or Cloud WAN for multi-account connectivity
- [ ] Centralized egress with NAT Gateway in shared VPC
- [ ] PrivateLink for AWS service access (no public endpoints)
- [ ] VPN/Direct Connect with redundancy (2 tunnels, 2 DX connections)
- [ ] Third-party connectivity isolated (VPC Lattice or dedicated VPCs)

Security

- [ ] Security Groups: default deny, allow by application port only
- [ ] NACLs as secondary defense (stateless, subnet-level)
- [ ] Network Firewall or third-party IDS/IPS in inspection VPC
- [ ] DNS Firewall rules blocking known malicious domains
- [ ] IPv6 considered and explicitly allowed or blocked (no accidental exposure)

Data Protection

Encryption at Rest

- [ ] Default EBS encryption enabled per account (account-level setting)
- [ ] S3 buckets with SSE-KMS or SSE-S3 (bucket policy enforcing encryption)
- [ ] RDS/Aurora encryption enabled (cannot be enabled after creation)
- [ ] DynamoDB encryption with CMK where required
- [ ] Secrets in Secrets Manager or Parameter Store, never in code

Encryption in Transit

- [ ] TLS 1.2+ enforced on all public endpoints
- [ ] ACM certificates with auto-renewal
- [ ] Internal traffic encrypted (ALB → target TLS, or service mesh)
- [ ] S3 bucket policy denying non-HTTPS requests

Key Management

- [ ] KMS keys with automatic rotation enabled (annual)
- [ ] Key policies follow least-privilege (separate encrypt/decrypt grants)
- [ ] Multi-region keys for DR scenarios
- [ ] Deletion protection: 30-day waiting period, CloudWatch alarm on scheduled deletion

Logging & Monitoring

Audit Trail

- [ ] CloudTrail enabled in all regions, all accounts (Organization trail)
- [ ] CloudTrail log file validation enabled
- [ ] CloudTrail logs in dedicated logging account (cross-account S3)
- [ ] S3 access logging for sensitive buckets
- [ ] VPC Flow Logs retained >= 90 days

Threat Detection

- [ ] GuardDuty enabled in all accounts and regions
- [ ] GuardDuty findings aggregated to delegated admin account
- [ ] Security Hub enabled with CIS and AWS Foundational benchmarks
- [ ] Automated response for critical findings (Lambda/EventBridge)

Operational Monitoring

- [ ] CloudWatch alarms for: billing anomalies, failed logins, root usage
- [ ] AWS Config rules for compliance (encrypted volumes, public access, etc.)
- [ ] Config conformance packs for organizational standards
- [ ] Centralized log aggregation (CloudWatch Logs, S3, or third-party SIEM)
- [ ] Amazon Inspector enabled for continuous vulnerability scanning (EC2, Lambda, ECR)

Account Structure

Multi-Account Strategy

- [ ] AWS Organizations with OUs: Security, Workloads (prod/dev), Sandbox, Shared
- [ ] Dedicated accounts: Log Archive, Security Tooling, Network Hub
- [ ] Account Factory (Control Tower or custom) for consistent provisioning
- [ ] Billing alerts per account and consolidated

Incident Readiness

- [ ] Incident response runbook documented
- [ ] Break-glass procedure for emergency access (tested quarterly)
- [ ] Backup strategy: cross-region, cross-account, tested restores
- [ ] Contact information updated in AWS account settings

⚡ Quick Wins — Do These First

1. Enable GuardDuty everywhere (5 minutes, zero config)
2. Enable default EBS encryption (account setting, one click)
3. Organization CloudTrail (single trail, all accounts)
4. SCP: deny root access keys + deny leaving org
5. MFA on all root users + IAM Identity Center for humans

📚 References

Well-Architected Framework — Security Pillar
AWS Security Reference Architecture (SRA)
AWS SRA — Identity Management
AWS SRA — Perimeter Security
Service Control Policies (SCPs)
AWS Control Tower
Amazon GuardDuty
AWS Security Hub