Cloud Security on AWS

Bob Rotsted

Carlos Armas

Agenda

- Guiding principles of cloud security on AWS
- AWS-specific security services and tools
- Case studies in cloud security breaches
- Best practices to prevent breaches using AWS

Guiding Principles of AWS Cloud Security

1. **Minimize attack surface:** Use AWS Security Groups, NACLs, WAF, and regular penetration tests
2. **IAM best practices:** Enforce least-privilege policies, use IAM roles over access keys
3. **Encrypt data:** Use AWS KMS, enforce encryption at rest (S3, EBS, RDS) and in transit (TLS)
4. **Monitor & audit:** Enable AWS CloudTrail, Amazon GuardDuty, and AWS Config continuously
5. **Zero Trust:** Verify every request with IAM policies, VPC endpoints, and AWS Verified Access
6. **Patch & backup:** Use AWS Systems Manager for patching, AWS Backup for recovery

It's Okay to Delete!

Data are liabilities, not assets.

Delete early. Delete often (*)

You don't need to protect data you don't have.

Use S3 Lifecycle Policies and S3 Object Lock to automate data retention and deletion.

** Subject to regulatory requirements.*

Reduce Cloud Attack Surface

NSRC
Network Startup Resource Center

Best Practices

- Use layered security: Security Groups, NACLs, AWS WAF, and Shield
- Run AWS Inspector for automated vulnerability scanning of EC2 and ECR
- Use Amazon Macie to discover and protect sensitive data in S3
- Conduct regular penetration tests (AWS permits this without approval for most services)
- Enable AWS Trusted Advisor for security checks and recommendations

IAM & Authentication on AWS

Best Practices

- Never use the root account for daily tasks; secure it with hardware MFA
- Enforce least-privilege IAM policies; use IAM Access Analyzer to audit permissions
- Use IAM Roles (not long-lived access keys) for services and EC2 instances
- Centralize authentication with AWS IAM Identity Center (successor to AWS SSO) and SAML
- Enable MFA for all human users; require MFA for sensitive API operations
- Use AWS Secrets Manager or Parameter Store for credentials
- Scan code repositories for leaked secrets

Network & Environment Isolation

Best Practices

- Use separate AWS accounts for dev, staging, and production
  - (consider using AWS Organizations, and Service Control Policies)
- Dev environments should never access production data or resources
- Use VPCs with private subnets; expose only what must be public
- Gate services behind AWS PrivateLink, VPN, or VPC endpoints
- Use AWS Transit Gateway for controlled cross-account networking

Preventing Insider Issues

Best Practices

- Require managed devices for access to AWS Console and sensitive resources
- Use IAM Identity Center to centrally manage and revoke access on offboarding
- Time account termination with offboarding conversations
- Revoke all active sessions and federated access tokens immediately
- Rotate or deactivate any access keys associated with departing users
- Collect and deactivate all devices affiliated with de-credentialed users
- Use AWS CloudTrail to audit any actions taken by departing personnel

Logging, Monitoring & Response

Best Practices

- Enable AWS CloudTrail in all regions; send logs to a centralized, immutable S3 bucket
- Use Amazon GuardDuty for intelligent threat detection across accounts
- Enable AWS Config to continuously track resource configuration changes
- Set up Amazon CloudWatch Alarms for anomalous activity (e.g., unusual API calls)
- Use AWS Security Hub as a single dashboard for security findings
- Ensure logging credentials are write-only; compromised admin should not erase logs
- Maintain an incident response plan and test it

Staff Security Awareness

Best Practices

- Make training fun: frequent, short, and engaging sessions increase awareness
- Create a supportive environment: encourage reporting errors without fear of reprimand
- Simulate real threats: run realistic phishing simulations to identify vulnerable areas
- Incentivize participation: reward good security-minded behavior

Protect Secrets

TruffleHog

github.com/trufflesecurity/trufflehog

- Finds credentials in git, GitHub, Docker, S3, GCS, filesystem, CI/CD
- Integrate into CI pipelines to catch secrets before they ship

GitGuardian

www.gitguardian.com

- Automated secret detection in repos, Jira, Slack, and more
- Free tier available for teams up to 25 members

AWS Secrets Manager + IAM Access Analyzer

- Store and rotate credentials automatically with AWS Secrets Manager
- Use IAM Access Analyzer to find resources shared with external entities
- Detect exposed access keys with AWS Health and automated remediation via EventBridge

Stay Informed

NSRC
Network Startup Resource Center

AWS Security Blog

aws.amazon.com/blogs/security/

AWS Security Bulletins

aws.amazon.com/security/security-bulletins/

Dark Reading

www.darkreading.com/cyberattacks-data-breaches

DataBreachToday

www.databreachtoday.com

Tech.co Security

tech.co/tag/privacy-security

Backdoors & Breaches

Tabletop Security Exercises

- Build your own tabletop security exercises at bnb.silverday.de
- Free account required (disposable email works, e.g., sharklasers.com)
- Developed by Black Hills Security (blackhillsinfosec.com)
- Physical card game also available for purchase
- Great for AWS incident response planning and team readiness

NSRC
Network Startup Resource Center

Discussion / Questions