Demystifying Cloud Security With AWS

Fundamentals and Best Practices

Vishal Alhat

SSE, Forcepoint

https://www.linkedin.com/in/vishalalhat

@WeShallAWS
Agenda

✓ Introduction
✓ AWS Shared Responsibility model
✓ Security Best Practices
✓ AWS Data Security
✓ AWS Servers Security
✓ AWS Applications Security
✓ Monitoring with AWS
Shared Responsibility Model
Shared Responsibility Model and Service Categories

Amazon EC2
- Customer Data
- Platform & Application Management
- OS, Network, Firewall Configuration
- Network Traffic Protection
- Server-Side Encryption
- Client-Side Data Encryption / Integrity
- Compute / Storage / Database / Network
- Hardware/AWS Global Infrastructure

Amazon RDS
- Customer Data
- Network Traffic Protection
- Client-Side Data Encryption
- Firewall Configuration
- Platform & Application Management
- OS, Network, Firewall Configuration
- Compute / Storage / Database / Network
- Hardware/AWS Global Infrastructure

AWS S3
- Customer Data
- Client-Side Data Encryption
- Server-Side Encryption
- Network Traffic Protection
- Platform & Application Management
- OS, Network, Firewall Configuration
- Compute / Storage / Database / Network
- Hardware/AWS Global Infrastructure

AWS KMS
- Customer Data
- Client-Side Data Encryption
- Network Traffic Protection
- Platform & Application Management
- OS, Network, Firewall Configuration
- Compute / Storage / Database / Network
- Hardware/AWS Global Infrastructure

DynamoDB
- Customer Data
- Client-Side Data Encryption
- Network Traffic Protection
- Platform & Application Management
- OS, Network, Firewall Configuration
- Compute / Storage / Database / Network
- Hardware/AWS Global Infrastructure

Infrastructure Services
- More Customer Responsibility
- More Customizable

Container Services
- Customer Services
- Less Customizable

Managed Services
- Less Customer Responsibility
- Less Customizable
<table>
<thead>
<tr>
<th>AWS security best practices by service</th>
<th>AWS IAM</th>
<th>Medium Risk</th>
<th>Low Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High Risk</strong></td>
<td>IAM policies should not allow full &quot;*&quot; administrative privileges</td>
<td>IAM users’ access keys should be rotated every 90 days or less</td>
<td>IAM users should not have IAM policies attached</td>
</tr>
<tr>
<td><strong>Medium Risk</strong></td>
<td>IAM root user access key should not exist</td>
<td>MFA should be enabled for all IAM users that have a console password</td>
<td></td>
</tr>
<tr>
<td><strong>Low Risk</strong></td>
<td>Hardware MFA should be enabled for the root user</td>
<td>Password policies for IAM users should have strong configurations</td>
<td></td>
</tr>
<tr>
<td><strong>Low Risk</strong></td>
<td>IAM users should not have IAM policies attached</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IAM policies should not allow full "*" administrative privileges.
IAM root user access key should not exist.
Hardware MFA should be enabled for the root user.
IAM users’ access keys should be rotated every 90 days or less.
MFA should be enabled for all IAM users that have a console password.
Password policies for IAM users should have strong configurations.
Unused IAM user credentials should be removed.
IAM users should not have IAM policies attached.
<table>
<thead>
<tr>
<th>Category</th>
<th>What is it</th>
<th>AWS service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity and access management</td>
<td>Securely manage access to services and resources</td>
<td>AWS Identity and Access Management (IAM)</td>
</tr>
<tr>
<td></td>
<td>Manage workforce access across AWS accounts and apps</td>
<td>AWS IAM Identity Center (successor to SSO)</td>
</tr>
<tr>
<td></td>
<td>Identity management for your apps</td>
<td>Amazon Cognito</td>
</tr>
<tr>
<td></td>
<td>Managed Microsoft Active Directory</td>
<td>AWS Directory Service</td>
</tr>
<tr>
<td></td>
<td>Simple, secure service to share AWS resources</td>
<td>AWS Resource Access Manager</td>
</tr>
<tr>
<td></td>
<td>Central governance and management across AWS accounts</td>
<td>AWS Organizations</td>
</tr>
</tbody>
</table>
AWS security best practices

- Permissions granted vs. Permissions used over time
- Using multi-factor authentication (MFA) with YubiKey
- Revoking IAM policies
- Rotating API keys every 90 days
AWS security best practices

73% of cloud accounts contain publicly exposed S3 buckets
## AWS security best practices by service

<table>
<thead>
<tr>
<th>AWS S3</th>
<th>High Risk</th>
<th>Medium Risk</th>
<th>Low Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="images/red_square.png" alt="Red Square" /> <img src="images/red_square.png" alt="Red Square" /> <img src="images/red_square.png" alt="Red Square" /></td>
<td><img src="images/yellow_square.png" alt="Yellow Square" /> <img src="images/yellow_square.png" alt="Yellow Square" /></td>
<td><img src="images/green_square.png" alt="Green Square" /></td>
</tr>
</tbody>
</table>

### AWS S3

- **S3 buckets should have server-side encryption enabled** - configure your buckets with server-side encryption
- **S3 Block Public Access setting should be enabled** using ACLs
- **S3 Block Public Access setting should be enabled** at the bucket level using bucket level policies
## AWS security best practices by service

<table>
<thead>
<tr>
<th>Service</th>
<th>High Risk</th>
<th>Medium Risk</th>
<th>Low Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS CloudTrail</td>
<td>CloudTrail should be enabled and configured with at least one multi-Region trail</td>
<td>CloudTrail should have encryption at rest enabled</td>
<td>Ensure CloudTrail log file validation is enabled</td>
</tr>
<tr>
<td>AWS Config</td>
<td>AWS Config should be enabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# AWS security best practices

## AWS security best practices by service

<table>
<thead>
<tr>
<th>Service</th>
<th>High Risk</th>
<th>Medium Risk</th>
<th>Low Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Amazon EC2</strong></td>
<td>Attached EBS volumes should be encrypted at rest</td>
<td>EBS default encryption should be enabled</td>
<td>VPC flow logging should be enabled in all VPCs</td>
</tr>
<tr>
<td></td>
<td>EBS default encryption should be enabled</td>
<td></td>
<td>The VPC default security group should not allow inbound and outbound traffic</td>
</tr>
<tr>
<td><strong>AWS DMS</strong></td>
<td>AWS Database Migration Service replication instances should not be public</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AWS security best practices

The Internet

ATTACKER

SSH PORT 22

YOUR VPC

0.0.0.0/0:22

NO ENCRYPTION

SSH WORLD-ACCESSIBLE

NON-STANDARD AMI

EC2 INSTANCE

EBS

CUSTOM AMI

AWS

User Groups
<table>
<thead>
<tr>
<th>Service</th>
<th>High Risk</th>
<th>Medium Risk</th>
<th>Low Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon EBS</td>
<td><img src="#" alt="High Risk" /> <img src="#" alt="High Risk" /> <img src="#" alt="High Risk" /></td>
<td><img src="#" alt="Medium Risk" /> <img src="#" alt="Medium Risk" /></td>
<td><img src="#" alt="Low Risk" /></td>
</tr>
<tr>
<td>Amazon EBS snapshots should not be public, determined by the ability to be restorable by anyone</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon OpenSearch Service-(successor to Elasticsearch)</td>
<td><img src="#" alt="Medium Risk" /> <img src="#" alt="Medium Risk" /></td>
<td><img src="#" alt="Low Risk" /></td>
<td></td>
</tr>
<tr>
<td>Elasticsearch domains should have encryption at rest enabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon SageMaker</td>
<td><img src="#" alt="Medium Risk" /> <img src="#" alt="Medium Risk" /></td>
<td><img src="#" alt="Low Risk" /></td>
<td></td>
</tr>
<tr>
<td>SageMaker notebook instances should not have direct internet access</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## AWS security best practices

### AWS Lambda
- **High Risk**: Lambda functions should use supported runtimes

### AWS KMS
- **Medium Risk**: AWS KMS keys should not be unintentionally deleted

### Amazon GuardDuty
- **Low Risk**: GuardDuty should be enabled
Data Security Best Practices

✓ Encryption
✓ Use KMS
✓ Rotate your keys
✓ Classify your data
✓ Secure data in transit
✓ S3 bucket permissions
Servers Security Best Practices

✓ Use IAM roles for EC2
✓ Use ELB
✓ Security group configuration
✓ Use Web Application Firewall (WAF)
✓ Secured access
✓ Backup and recovery
✓ EC2 termination protection
Application Security Best Practices

✓ Use web application firewall
✓ Amazon Inspector
✓ Penetration testing
✓ Utilize AWS security tools
Application Security Best Practices

✓ Use web application firewall
✓ Amazon Inspector – vulnerability management service
✓ Penetration testing
✓ Utilize AWS security tools
Monitoring in Cloud

ALL I KNOW IS THE BOSS SAID WE HAD TO MONITOR THE CLOUD.
Monitoring With AWS

AWS Allows you to monitor all your resources in cloud, such as your servers and your AWS services, along with applications running with these services through its fully managed monitoring service – AWS CloudWatch.

AWS CloudWatch provides

✓ Metrics
✓ Dashboard
✓ Events
✓ Alarms
✓ Log monitoring

Resources Monitored By CloudWatch
Thank you!

Q & A
Please complete the session survey