

# 6

# KEY CLOUD

# SECURITY

# CONCENTRATIONS



# Identity and Access Management

## CAPABILITY: Groups, Roles, Policies, Permissions

- | AWS       | AZURE                | GCP                               |
|-----------|----------------------|-----------------------------------|
| ■ AWS IAM | ■ Microsoft Entra ID | ■ Cloud IAM<br>■ Resource Manager |

## CAPABILITY: Single Sign On (SSO)

- | AWS                   | AZURE                | GCP              | 3RD PARTY  |
|-----------------------|----------------------|------------------|--|
| ■ IAM Identity Center | ■ Microsoft Entra ID | ■ Cloud Identity | ■ Okta<br>■ Ping<br>■ Sailpoint<br>■ Oracle IDCS |

## CAPABILITY: Service Accounts

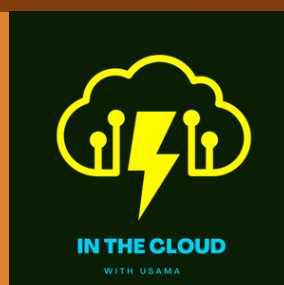
- | AWS                | AZURE   | GCP               |
|--------------------|---|-------------------|
| ■ Instance Profile | ■ Managed Identity<br>■ Service Principals<br>■ User-Based Service Accounts | ■ Service Account |

## CAPABILITY: Customer IAM (CIAM)

- | AWS                         | AZURE                    | GCP  |
|-----------------------------|--------------------------|--|
| ■ Amazon Cognito User Pools | ■ Entra ID for Customers | ■ Cloud Identity for Customers and Partners<br>■ Firebase Authentication<br>■ Managed Service for Microsoft Active Directory |

## CAPABILITY: Least Privilege

- | AWS                   | AZURE        | GCP         |
|-----------------------|--------------|-------------|
| ■ IAM Access Analyzer | ■ Azure RBAC | ■ Cloud IAM |



# DevSecOps

## CAPABILITY: CI/CD Security

AWS	AZURE	GCP
<ul style="list-style-type: none"><li>CodeBuild</li><li>CodePipeline</li></ul>	<ul style="list-style-type: none"><li>Azure DevOps</li><li>Azure Source Code Repositories</li><li>Azure Branch Policies</li><li>Azure Key Vault Secrets</li></ul>	<ul style="list-style-type: none"><li>Cloud Build</li></ul>

## CAPABILITY: Infrastructure as Code

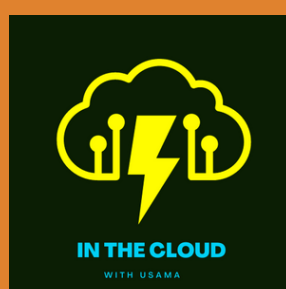
AWS	AZURE	GCP
<ul style="list-style-type: none"><li>AWS CloudFormation</li></ul>	<ul style="list-style-type: none"><li>Azure Resource Manager</li><li>BICEP</li></ul>	<ul style="list-style-type: none"><li>Cloud Resource Manager</li></ul>

## CAPABILITY: Configuration Management

AWS	AZURE	GCP
<ul style="list-style-type: none"><li>AWS OpsWorks</li></ul>	<ul style="list-style-type: none"><li>Configuration Manager on Azure</li><li>Azure Automation</li><li>Azure App Configuration</li></ul>	<ul style="list-style-type: none"><li>GCP – Anthos Config Management</li></ul>

## CAPABILITY: Content Delivery and Protection

AWS	AZURE	GCP
<ul style="list-style-type: none"><li>AWS CloudFront</li></ul>	<ul style="list-style-type: none"><li>Azure Content Delivery Network (CDN)</li></ul>	<ul style="list-style-type: none"><li>GCP Cloud CDN</li></ul>



# Application Security

## CAPABILITY: Static Application Security Testing

### >>> 3RD PARTY

- Veracode
- Synopsys
- Checkmarx
- GitHub Advanced Security

### OPEN SOURCE

- semgrep
- BetterScan
- Horusec
- Automated Security Helper

## CAPABILITY: Software Composition Analysis

### >>> 3RD PARTY

- Veracode
- Synopsys
- Checkmarx
- GitHub SCA
- Snyk

### OPEN SOURCE

- OWASP Dependency-Check
- retire.js
- OSS Review Toolkit

## CAPABILITY: Dynamic Application Security Testing

### >>> 3RD PARTY

- Veracode
- Synopsys
- Acunetix

### OPEN SOURCE

- ZAP
- w3af
- Nuclei

## CAPABILITY: Web Application Firewall

### AWS      AZURE      GCP      3RD PARTY      OPEN SOURCE

- AWS WAF
- Azure WAF
- Cloud WAF
- Akamai
- ModSecurity
- Cloudflare
- Imperva

## CAPABILITY: Web App and API Protection

### AWS      AZURE      GCP      3RD PARTY      OPEN SOURCE

- API Gateway
- API Management
- Application Gateway
- Web App Protection
- API Protection
- Akamai
- Cloudflare
- Imperva
- NoName
- Salt Security
- Curiefence

## CAPABILITY: Runtime Application Self-Protection

### >>> 3RD PARTY

- Imperva
- Signal Sciences
- Contrast Security

### OPEN SOURCE

- OpenRASP



# Data Protection

## CAPABILITY: Key Management

AWS	AZURE	GCP
<ul style="list-style-type: none"><li>■ Key Management Service (KMS)</li><li>■ Cloud HSM</li></ul>	<ul style="list-style-type: none"><li>■ Azure Key Vault</li><li>■ Azure Dedicated HSM</li></ul>	<ul style="list-style-type: none"><li>■ Cloud Key Management Service (KMS)</li><li>■ Google Cloud HSM</li></ul>

## CAPABILITY: Secrets Management

AWS	AZURE	GCP	3RD PARTY
<ul style="list-style-type: none"><li>■ AWS Secrets Manager</li><li>■ Parameter Store</li></ul>	<ul style="list-style-type: none"><li>■ Azure Key Vault</li></ul>	<ul style="list-style-type: none"><li>■ Secret Manager</li></ul>	<ul style="list-style-type: none"><li>■ HashiCorp Vault</li></ul>

## CAPABILITY: Encryption at Rest

AWS	AZURE	GCP
<ul style="list-style-type: none"><li>■ AWS KMS</li></ul>	<ul style="list-style-type: none"><li>■ Azure Key Vault</li></ul>	<ul style="list-style-type: none"><li>■ Google Cloud KMS</li></ul>

## CAPABILITY: Encryption in Transit

AWS	AZURE	GCP
<ul style="list-style-type: none"><li>■ AWS Certificate Manager</li></ul>	<ul style="list-style-type: none"><li>■ Azure Key Vault</li></ul>	<ul style="list-style-type: none"><li>■ Certificate Manager</li></ul>

## CAPABILITY: Certificate Management

AWS	AZURE	GCP
<ul style="list-style-type: none"><li>■ AWS Certificate Manager</li></ul>	<ul style="list-style-type: none"><li>■ Azure Key Vault</li></ul>	<ul style="list-style-type: none"><li>■ Certificate Authority Service</li><li>■ Certificate Manager</li></ul>

## CAPABILITY: Data Loss Prevention

AWS	AZURE	GCP
<ul style="list-style-type: none"><li>■ Amazon Macie</li></ul>	<ul style="list-style-type: none"><li>■ Microsoft Purview</li></ul>	<ul style="list-style-type: none"><li>■ Cloud Data Loss Prevention</li></ul>

## CAPABILITY: Cloud Access Security Broker

AZURE
<ul style="list-style-type: none"><li>■ Microsoft Defender for Cloud Apps</li></ul>

## CAPABILITY: Data Backup, Restore and Recovery

AWS	AZURE	GCP
<ul style="list-style-type: none"><li>■ AWS Backup</li></ul>	<ul style="list-style-type: none"><li>■ Azure Backup</li></ul>	<ul style="list-style-type: none"><li>■ GCP Backup &amp; Disaster Recovery</li></ul>



# Infrastructure Security

## CAPABILITY: Cloud Security Posture Management

AZURE	3RD PARTY	OPEN SOURCE
<ul style="list-style-type: none"><li>Microsoft Defender for Cloud</li></ul>	<ul style="list-style-type: none"><li>Palo Alto Prisma Cloud</li><li>Palo Alto – Prisma CSPM</li><li>Orca</li><li>Wiz</li></ul>	<ul style="list-style-type: none"><li>Cloud Custodian</li><li>GCP Config Validator</li><li>GCP Terraform Validator</li><li>Prowler</li></ul>

## CAPABILITY: Network Security

AWS	AZURE	GCP
<ul style="list-style-type: none"><li>Virtual Private Cloud<ul style="list-style-type: none"><li>AWS Firewall Manager</li></ul></li><li>Network Access Control Lists</li><li>Security Groups</li></ul>	<ul style="list-style-type: none"><li>Virtual Network<ul style="list-style-type: none"><li>Azure Firewall Manager</li></ul></li><li>Network Security Groups</li></ul>	<ul style="list-style-type: none"><li>Virtual Private Cloud<ul style="list-style-type: none"><li>GCP Firewall</li></ul></li></ul>

## CAPABILITY: Private Connectivity

AWS	AZURE	GCP
<ul style="list-style-type: none"><li>AWS Direct Connect</li><li>AWS PrivateLink</li></ul>	<ul style="list-style-type: none"><li>Azure Express Route</li><li>Azure Private Link</li></ul>	<ul style="list-style-type: none"><li>Cloud InterConnect</li><li>Private Service Connect</li></ul>

## CAPABILITY: Private Endpoints

AWS	AZURE	GCP
<ul style="list-style-type: none"><li>VPC Endpoints</li></ul>	<ul style="list-style-type: none"><li>Network Service Endpoints</li></ul>	<ul style="list-style-type: none"><li>VPC Service Controls</li></ul>

## CAPABILITY: Remote Access

AWS	AZURE	GCP
<ul style="list-style-type: none"><li>Session Manager</li><li>VPN</li></ul>	<ul style="list-style-type: none"><li>Serial Console</li><li>VPN Gateway</li></ul>	<ul style="list-style-type: none"><li>Cloud SSH</li><li>Cloud VPN</li></ul>

## CAPABILITY: DDoS Protection

AWS	AZURE	GCP
<ul style="list-style-type: none"><li>AWS Shield</li></ul>	<ul style="list-style-type: none"><li>Azure DDoS Protection</li></ul>	<ul style="list-style-type: none"><li>Cloud Armor</li></ul>



# Want to Learn More about Cloud Security

Leave a comment below

