**# Cloud Services Alternative Report**

In the course, we learn a lot of different services in Azure cloud that uses for implementing security in our architecture. Now, I will explain the comparisons to the resources we use in Azure to resources to other cloud services such as AWS (Amazon Web Services) and GCP (Google Cloud Platform).

**## Azure Active Directory (SSO, IAM)**

| Azure Service | AWS | Google Cloud |

| --- | --- | --- |

| Azure AD | AWS IAM Identity | Google Cloud Identity |

**### Overview**

-   **\*\*Azure AD\*\***: It is a built in identify and access management service that use SSO, MFA, and role-based access control (RBAC)

-   **\*\*AWS IAM Identity\*\***: An AWS’s solution for SSO and multi account management.

-   **\*\*Google Cloud Identity\*\***: Google IAM service for managing users, groups, and policies

**### Core Features**

| **\*\***Feature**\*\*** | **\*\***Azure AD**\*\*** | **\*\***AWS IAM Identity**\*\*** | **\*\***Google Cloud Identity**\*\*** |

| --- | --- | --- | --- |

| **\*\***SSO**\*\*** | have | have | have |

| **\*\***MFA**\*\*** | have | have | have |

| **\*\***RBAC**\*\*** | have | have | have |

| **\*\***Directory Sync**\*\*** | Azure AD Connect | AWS Directory Service | Google Cloud Directory Sync |

**### Security & Compliance**

-   All support SOC 2, ISO 27001 and GDPR

-   \*\*Azure AD\*\*: Deep integration with Microsoft 365.

-   \*\*Azure IAM\*\*: integrates with AWS Organizations.

-   \*\*Google Cloud Identity\*\*: supports BeyondCorp Zero Trust.

**### Pricing Model**

-   **\*\***Azure AD**\*\***: Free tier and premium tier with $6 per month

-   **\*\***AWS IAM Identity Center**\*\***: Free

-   **\*\***Google Cloud Identity**\*\***: with $6 per month

**### Integration with DevSecOps**

-   All support CI/CD integration

-   All use Terraform and Ansible modules for automation

**## Azure Monitor & Log Analytics**

| Azure Service | AWS | Google Cloud |

| --- | --- | --- |

| Azure Monitor and Log Analytics | Amazon CloudWatch | Google Cloud Operations Suite |

**### Overview**

- **\*\*Azure Monitor\*\***: Full-stack monitoring for apps, infrastructure, and networks.

- **\*\*CloudWatch\*\***: AWS’s monitoring and observability service.

- **\*\*Google Cloud Operations\*\***: GCP’s unified monitoring, logging, and diagnostics.

**### Core Features**

| \*\*Feature\*\* | \*\*Azure Monitor\*\* | \*\*CloudWatch\*\* | \*\*Google Cloud Operations\*\* |

| --- | --- | --- | --- |

| \*\*Log Analytics\*\* | have | CloudWatch Logs | Cloud Logging |

| \*\*Metrics & Alerts\*\* | have | have | have |

| \*\*Distributed Tracing\*\* | Application Insights | X-Ray | Cloud Trace |

**### Security & Compliance**

- All support encryption at rest and in transit.

- HIPAA, PCI DSS compliant.

**### Pricing Model**

- \*\*Azure Monitor\*\*: Pay-as-you-go (~$2.30/GB for logs).

- \*\*CloudWatch\*\*: Free tier; Log storage at $0.50/GB/month.

- \*\*Google Operations\*\*: Free tier; Logging at $0.50/GB/month.

**### Integration for DevSecOps**

- All integrate with Kubernetes, serverless, and CI/CD pipelines.

- Prometheus/Grafana support in all three.

**## Azure Policy**

| \*\*Azure Service\*\* | \*\*AWS Equivalent\*\* | \*\*Google Cloud\*\* |

| --- | --- | --- |

| Azure Policy | AWS Config | Google Cloud Security Command Center (SCC) |

**### Overview**

- \*\*Azure Policy\*\*: Enforces compliance rules across Azure resources.

- \*\*AWS Config\*\*: Tracks resource configurations and compliance.

- \*\*GCP SCC\*\*: Security and risk management platform.

**### Core Features**

| \*\*Feature\*\* | \*\*Azure Policy\*\* | \*\*AWS Config\*\* | \*\*SCC\*\* |

| --- | --- | --- | --- |

| \*\*Compliance Checks\*\* | have | have | have |

| \*\*Auto-Remediation\*\* | have | AWS System Manager | have |

| \*\*Custom Policies\*\* | have | have | have |

**### Security & Compliance**

- All support CIS Benchmarks, NIST, HIPAA.

**### Pricing Model**

- \*\*Azure Policy\*\*: Free for basic policies.

- \*\*AWS Config\*\*: $0.003 per configuration item.

- \*\*GCP SCC\*\*: $0.0025/resource/hour.

**### Integration for DevSecOps**

- All support Terraform, CLI, and API automation.

**## Microsoft Defender for Cloud**

| \*\*Azure Service\*\* | \*\*AWS Equivalent\*\* | \*\*GCP Equivalent\*\* |

| --- | --- | --- |

| Defender for Cloud | AWS Security Hub | Google Cloud Security Command Center (SCC) |

**### Overview**

- \*\*Defender for Cloud\*\*: Cloud security posture management (CSPM) and threat protection.

- \*\*AWS Security Hub\*\*: Centralized security alerts and compliance checks.

- \*\*GCP SCC\*\*: Unified security and threat detection.

**### Core Features**

| \*\*Feature\*\* | \*\*Defender for Cloud\*\* | \*\*AWS Security Hub\*\* | \*\*GCP SCC\*\* |

| --- | --- | --- | --- |

| \*\*Vulnerability Scanning\*\* | have | have | have |

| \*\*Threat Detection\*\* | have | have | have |

| \*\*Compliance Dashboards\*\* | have | have | have |

### **Security & Compliance**

* \*\*Defender for Cloud\*\*: Contain protection tools such as Threat Detection, Vulnerability Scanning, and Network access that can enforce compliance and auto-remediate threats using Azure Policy.
* \*\*AWS Security Hub\*\*: detect threats by using GuardDuty, Inspector, and Macie and then trigger lambda function when threats detected.
* \*\*GCP SCC\*\*: Go though all the GCP resources and use Google’s threat intelligence to analyze data and scan Google Kubernetes Engine.

**### Pricing Model**

- \*\*Defender for Cloud\*\*: Starts at $15/server/month.

- \*\*AWS Security Hub\*\*: $0.001 per finding.

- \*\*GCP SCC\*\*: $0.0025/resource/hour.

**### Integration for DevSecOps**

* \*\*Defender for Cloud\*\*: Supports automated security enforcement, compliance-as-code, and CI/CD pipeline integration for shift-left security
* \*\*AWS Security Hub\*\*: Centralized security compliance dashboard (CSPM)
* \*\*GCP SCC\*\*: have a unified CSPM and vulnerability scanning

**## Microsoft Sentinel (SIEM/SOAR)**

| \*\*Service\*\* | \*\*AWS Equivalent\*\* | \*\*GCP Equivalent\*\* |

| --- | --- | --- |

| Azure Sentinel | Amazon Guard Duty | Google Chronicle |

**### Overview**

- \*\*Azure Sentinel\*\*: Cloud-native SIEM with SOAR capabilities.

- \*\*Amazon Guard Duty\*\*: Threat detection service.

- \*\*Google Chronicle\*\*: Google’s security analytics platform.

### Core Features

* \*\*Azure Sentinel\*\*: Centralized threat detection, investigation, and automated response across hybrid environments.
* \*\*Amazon Guard Duty\*\*: Analyzed AWS logs from VPC Flow, CloudTrail, DNS for strange activity.
* \*\*Google Chronicle (GCP)\*\*: Large-scale log analysis and threat hunting with Google’s infrastructure.

### **Security & Compliance**

* \*\*Azure Sentinel\*\*: gather logs from Azure resources, Office 365 and third-party systems from Microsoft and use AI for threat detection with pre-built playbooks for automated response
* \*\*Amazon Guard Duty\*\*: analyzes VPC, DNS, and cloud Trail logs with machine learning to find compromised instances, crypto-mining and suspicious API calls.
* \*\*Google Chronicle (GCP)\*\*: it is a large-scale security analytics platform that is build on Big Query the enables fast threat hunting across massive datasets with Virus Total integration and YARA-L detection rules

**### Pricing Model**

- \*\*Microsoft Sentinel\*\*: $4.50/GB log ingestion.

- \*\*Amazon Guard Duty\*\*: $1.00 per 1M events.

- \*\*Google Chronicle\*\*: Custom pricing.

**### Integration for DevSecOps**

* \*\*Microsoft Sentinel\*\*: enables automated threat detection, incident response, and security orchestration in DevSecOps workflow.
* \*\*Amazon Guard Duty\*\*: Threat detection such as malware and strange API calls.
* \*\*Google Chronicle\*\*: SIEM for threat detection using log analysis

**## Summary table**

| \*\*Azure AD\*\* | \*\*AWS IAM Identity\*\* | \*\*Google Cloud Identity\*\* |

| --- | --- | --- |

| Azure Monitor | Amazon CloudWatch | Google Cloud Operations Suite |

| Azure Policy | AWS Config | Google Cloud Security Command Center (SCC) |

| Defender for Cloud | AWS Security Hub | Google Cloud Security Command Center (SCC) |

| Microsoft Sentinel | Amazon GuardDuty and AWS Detective | Google Chronicle |