1. EINES DE SEGURETAT EN AMAZON WEB SERVICES I GOOGLE CLOUD PLATFORM

Amazon Web Services (AWS) proporciona diferents tipus de mecanismes de seguretat en les aplicacions allotjades al núvol, a continuació podem observar les més representatives:

CAT. / DESCRIPCIÓ	SERVEI
1. Identitat i gestió d'accés	
1.1. Administració d'identitats per les aplicacions	Amazon Cognito
1.2. Microsoft Active Directory administrat	AWS Directory Service
1.3. Administració d'accés als usuaris i claus de xifratge	AWS Identity & Access Management (IAM)
1.4. Servei simple i segur per compartir recursos AWS	AWS Resource Access Manager
1.5. Administració i recuperació de dades confidencials	AWS Secrets Manager
1.6. Servei d'inici de sessió únic (SSO) en el núvol	AWS Single Sign-On
2. Controls de detecció	
2.1. Servei administrat de detecció d'amenaces	AWS GuardDuty
2.2. Centre unificat de seguretat i conformitat	AWS Security Hub
3. Protecció d'infraestructures	
3.1. Protecció a atacs DDoS	AWS Shield
3.2. Filtratge de tràfic malintencionat	AWS Web Application Firewall (WAF)
3.3. Administració central de regles de Firewall	AWS Firewall Manager
3.4. Analitzador de seguretat en les aplicacions	Amazon Inspector
4. Protecció de dades	
4.1. Administració i emmagatzematge clau	AWS Key Management Service (KMS)
4.2. Emmagatzematge de claus hardware	AWS CloudHSM
4.3. Gestió de certificats públic i privats SSL / TLS	AWS Certificate Manager
4.4. Classificació i protecció de les dades	Amazon Macie
5. Conformitat	
5.1. Informes de conformitat	AWS Artifact

Google Cloud Platform (GCP) també proporciona diferents tipus de mecanismes de seguretat en les aplicacions allotjades al núvol, a continuació podem observar les més representatives:

CAT. / DESCRIPCIÓ	SERVEI
1. Seguretat	
1.1. Plataforma de control de riscos de seguretat i dades	Cloud Security Command Center
1.2. Desp. de contenidors de confiança en Kubernetes	Autorització Binaria
1.3. Analitzador automàtic d'aplicacions en App Engine	Cloud Security Scanner
1.4. Enregistrament d'activitats dels usuaris en el núvol	Registres d'Auditoria en el Cloud

1.5. Detecció d'amenaces de seguretat	Event Threat Detection
1.6. Descobriment i ocultació de dades sensibles	Cloud Data Loss Prevention
1.7. Màquines virtuals endurides (Rootkits, Bootkits, etc.)	MV Blindades
1.8. Protecció de les claus criptogràfiques	Cloud HSM
1.9. Perímetres de seguretat virtuals	Controls de Servei de VPC
1.10. Gestió de les claus de xifratge	Cloud Key Management Service
2. Identitat i gestió d'accés	
2.1. Gestió d'identitats i d'accés als recursos	Cloud IAM
2.2. Servei que executa Microsoft Active Directory	Servei gestionat per Microsoft AD
2.3. Gestió d'identitats d'usuaris, dispositius i aplicacions	Cloud Identity
2.4. Control d'accés intel·ligent	Policy Intelligence
2.5. Gestiona l'accés a les aplicacions	Accés Contextual
2.6. Protecció d'accés a les aplicacions i MV	Cloud Identity-Aware Proxy
2.7. Gestió de recursos de forma jeràrquica	Resource Manager
2.8. Obligació de l'ús de claus de seguretat	Ús de Claus de Seguretat
2.9. Accessos propis de Google a les aplicacions	Identity Platform
3. Protecció d'usuaris	
3.1. Protecció a atacs de Phishing	Phishing Protection
3.2. Detecció de URL's malintencionades	API Web Risk
3.3. Protecció d'activitats fraudulentes i SPAM	ReCAPTCHA Enterprise

Com podem observar, les dues plataformes proporcionen una gran quantitat de mecanismes de protecció, a continuació es mostra una petita taula comparativa relacionant els serveis amb les instancies utilitzades en cada cas.

SERVEI	AMAZON WEB SERVICES	GOOGLE CLOUD PLATFORM
1. Autenticació i autorització	AWS Identity & Access Management (IAM)	Cloud IAM Cloud Identity-Aware Proxy
2. Protecció amb encriptació de dades	AWS Key Management Service (KMS)	Cloud Key Management Service
3. Firewall	AWS Web Application Firewall (WAF) AWS Firewall Manager	
4. Gestió d'identitats	Amazon Cognito	Cloud Identity
5. Analitzador de seguretat en les aplicacions	Amazon Inspector	Cloud Security Scanner

2. OPINIÓ PERSONAL

Amazon Web Services (AWS) i *Google Cloud Platform* (GCP) són plataformes tremendament complexes, utilitzen una gran quantitat de tecnologies per facilitar la gestió dels recursos de les organitzacions, proporcionen eines de desplegament, gestió dinàmica dels recursos, mecanismes de protecció, copies de seguretat, etc. Crec recordar, que actualment AWS suposa el 60% del benefici de la empresa *Amazon* i que per tant, es podria considerar un dels serveis més importants de l'organització. Segons la filosofia a seguir d'una organització, tindre les aplicacions i la informació allotjada al núvol pot suposar un clar benefici, utilitzant aquesta capa d'abstracció el client no s'ha de preocupar pels recursos hardware, degut a que aquests es van assignant dinàmicament segons la necessitat en cada moment, incrementant així la escalabilitat de les aplicacions i garantint la seva disponibilitat. Els mecanismes de protecció que utilitzen són tremendament útils per evitar els atacs DoS, Phishing, XSS, Rootkits, etc. Cal dir, que moltes de les empreses *d'Inditex* (*Zara*, *Pull&Bear*, *Massimo Dutti*, *Cortefiel*, etc.) utilitzen *Akamai Technologies*, i que aquesta conté un llistat actualitzat de direccions IP malicioses o “Black List” que poden suposar un risc pels seus clients, per tant, quan aquest ho detecta, talla immediatament la comunicació sense que el client pugui sol·licitar cap tipus d'informació sobre les organitzacions que gestiona.

3. FONTS D'INFORMACIÓ

Amazon

Pàgina oficial - Amazon Web Services.

https://aws.amazon.com

Google

Pàgina oficial - Google Cloud Platform.

https://cloud.google.com