Security & Compliance section

AWS Shared Responsibility Model.

1) AWS Responsibility - Security OF the cloud.
Protecting infrastructure (hw, sw, facilities and networking)
S3, DynamoDB, RDS.

2) Customer Responsibility - Security IN the cloud.
EC2, OS, firewall & network config
IAM
Encryption appln data

3) Shared control:
Patch Management, config management, awareness & Training.

What is DDoS Attack?

Attackers → Bots → Application server

Not accessible
Not responsive

Normal users

DDoS Protection on AWS.

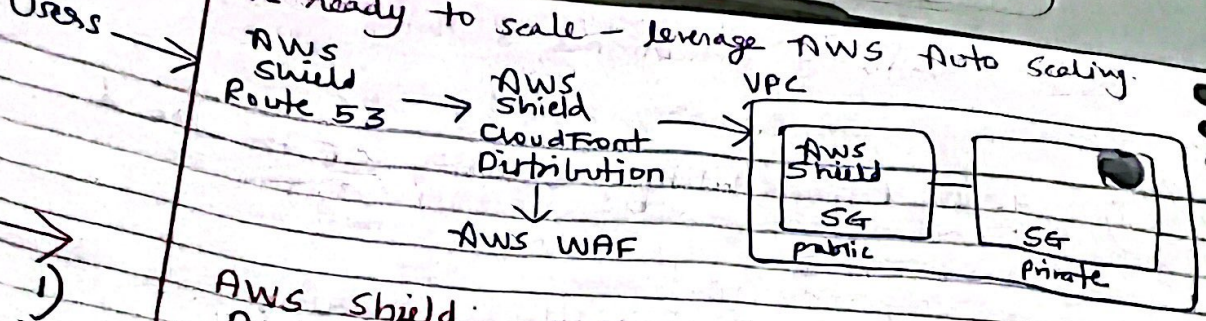
1) AWS Shield Standard: Protects against DDoS attack for your website and applications, for all customers at no additional costs

2) AWS Shield Advanced: 24/7 premium DDoS protection

3) AWS WAF: Filter specific requests based on rules.

4) CloudFront & Route 53: Availability protection using global edge network, Combined with AWS Shield, provides attack mitigation at the edge.

Be ready to scale – leverage AWS Auto Scaling.



1) AWS Shield:
   AWS Shield Standard:
   Free service
   Every AWS customer
   Protection – SYN / UDP floods, Reflection attacks and other layer 3 / layer 4 attacks.
2) AWS Shield Advanced:
   Optional DDoS mitigation service
   Protect against more sophisticated attack on EC2, ELB, CloudFront, Global Accelerator, Route 53
   24/7 access to AWS DDoS response team (DRP)
   Protect against higher fees during usage spikes due to DDoS.

AWS WAF – Web Application Firewall.
Protects your web application from common web exploits. (Layer 7)
Layer 7 is HTTP. (vs layer 4 is TCP)
Deploy on ALB, API Gateway, CloudFront
Define web ACL (Web Access Control List)
1) Rules can include IP addresses; HTTP headers, HTTP body, or URI strings
2) Protects from common attack - SQL injection and Cross-Site Scripting (XSS)
3) Size constraints, geo-match
4) Rate-based rules (to count occurrences of events) – for DDoS protection.

→ Penetration Testing on AWS cloud.

AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval.

1) Prohibited Activities
   DNS zone Walking via Amazon Route 53 Hosted zones.
2) DoS, DDoS, Simulated DoS, Simulated DDoS.
3) Port flooding
4) Protocol flooding
5) Request flooding (login request flooding, API request flooding).

→ Data at rest vs Data in transit.

Encrypted at rest on EFS	Encrypted in transit while uploading →

- At rest: Data stored or archived on a device on a hard disk, on a RDS instance, in S3 Glacier Deep archive.
- In transit (in motion): Moving data
  eg: Data transfer from on-premises to AWS, EC2 to DynamoDB
- Data transferred on the network
- Encryption keys: Keep data encrypt in both states to protect it.

⇒ AWS KMS (Key Management Service)

- AWS manages encryption keys for us.
- Encryption opt-in
  1) EBS Volumes
  2) S3 Buckets
  3) Redshift DB
  4) RDS DB
  5) EFS drives

1) Encryption Automatically enabled:
2) CloudTrail logs
S3 Glacier
3) Storage Gateway.

CloudHSM (Hardware Security Module)
Encryption hw
HSM - Dedicated HW
Manage your own encryption keys entirely.
Tamper resistant

CloudHSM Client

SSL connection
User manages the key

AWS CloudHSM

AWS manages the hw

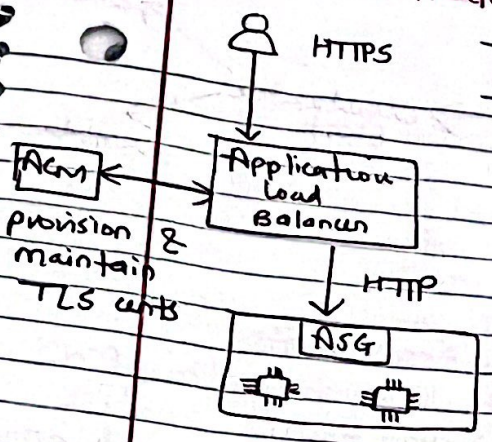
Types of Customer Master keys : CMK
Customer Managed CMK:
1) Create, manage and used by customers
2) Can enable / disable
3) Rotation policy
4) Bring your own key.

AWS managed CMK:
1) Create, manage and used on the customer's behalf by AWS.
2) Used by AWS services - S3, EBS, Redshift.

AWS owned CMK:
1) Collection of CMKs that an AWS service owns and manages to use in multiple accounts.
2) Protect resources in your account.

CloudHSM keys (Custom keystore):
1) Keys generated from your own CloudHSM hardware device.
2) Cryptographic operations are performed within the CloudHSM cluster.

AWS Certificate Manager (ACM).



provision & maintain TLS certs

- Let's you easily provision, manage and deploy TLS/SSL certificates.
- Provide in-flight encryption for websites.
- Both public & private TLS certificates.
- Free of charge for public TLS.
- Automatic TLS certificate renewal.
- Integrations with (load TLS certificates on)
  1) ELB
  2) CloudFront distributions
  3) APIs.

AWS Secret Manager:

- Meant for storing secrets.
- Force rotation of secrets every x days.
- Automate generation of secrets on rotation (uses Lambda)
- Integration with Amazon RDS (MySQL, PostgreSQL, Aurora).
- Encrypted using KMS.
- Meant for RDS integration.

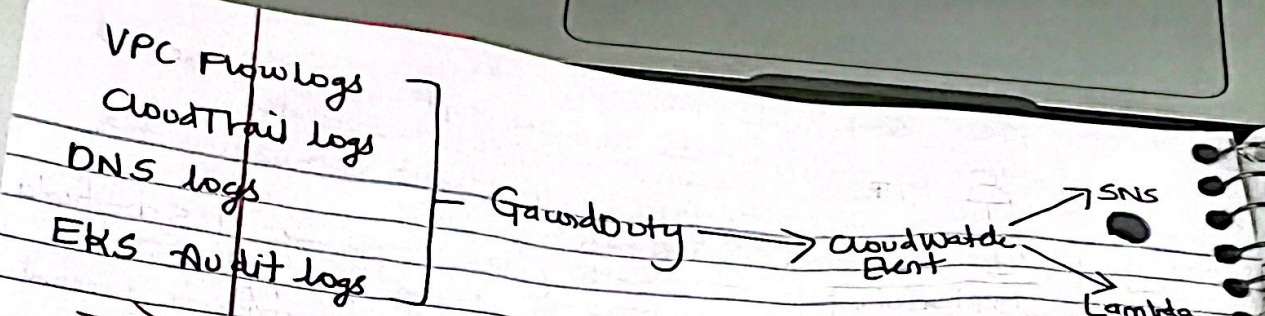
AWS Artifact:

Portal: Provides customers with on-demand access to AWS compliance and documentation and AWS agreements.

- Artifact Reports
- Artifact Agreements.
- Used to support internal audit or compliance.

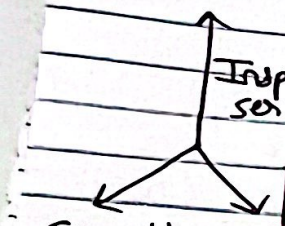
Amazon GuardDuty.

- Intelligent Threat Discovery
- ML algo., anomaly detection
- Setup Cloudwatch event rules
- Protect against cryptocurrency attacks.



Amazon Inspector:

- Automated security assessments.
- For EC2 instances: Leveraging the AWS System Manager (SSM) agent, analyze the unintended network accessibility, running OS against known vulnerabilities.
- For containers push to Amazon ECR: Assessment of containers.
- Reporting & integration with AWS security Hub
- Send findings to Amazon Event Bridge



What does AWS Inspector Evaluate?

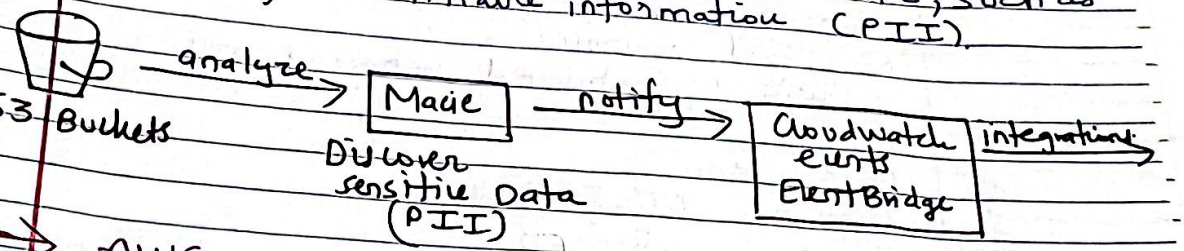
- only EC2 instances and containes infrastructure.
- Continuous scanning of the infra, only when needed.
- Package vulnerabilities (EC2, ECR)
- Network reachability (EC2)
- Risk score

AWS Config:

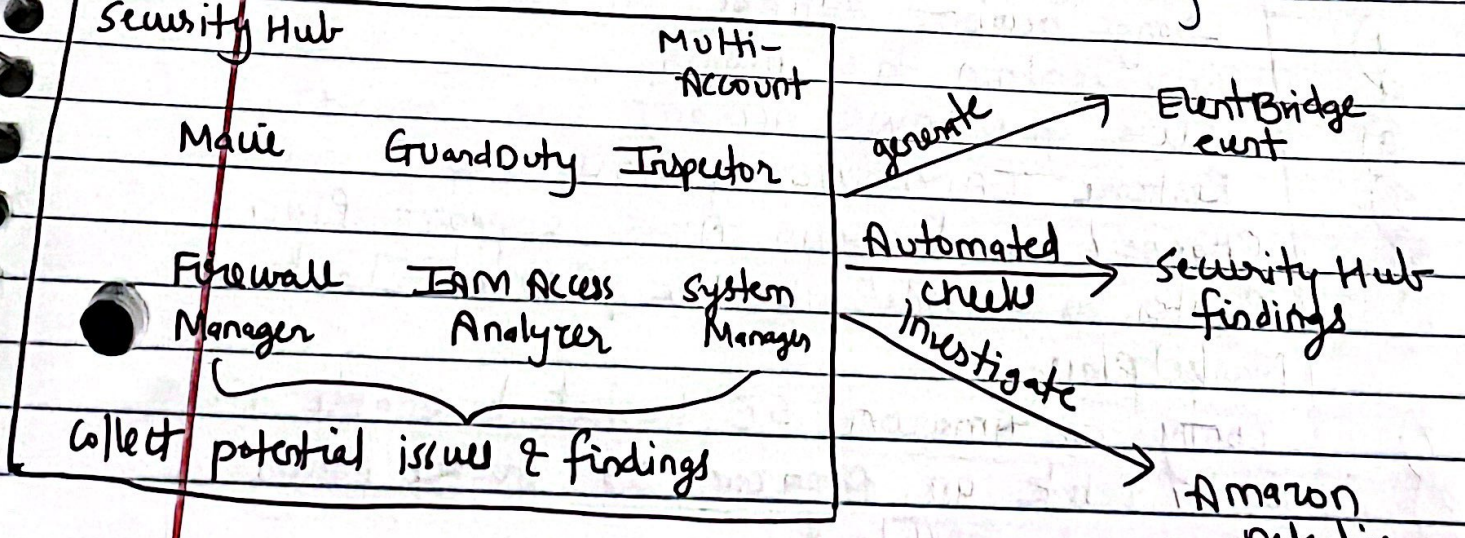
- Auditing & recording compliance of your AWS resources.
- Record configurations and changes over time.
- Send alerts for any changes
- Per-region service
- Can be aggregated across regions and accounts

AWS Config resource:
View compliance of a resource over time
View config of a resource over time
View CloudTrail API calls if enabled

Amazon Macie:
Data security & data privacy service
ML & pattern matching to discover and protect your sensitive data.
Identify and alert you to sensitive data, such as personally identifiable information (PII).



AWS Security Hub:
Central security tool to manage security across several AWS accounts and automate security checks.
Integrated dashboards: Current security, compliance status.
Automatically aggregates alerts in predefined or personal findings format.
Must first enable the AWS config service.



Amazon Detective
GuardDuty, Macie, SecurityHub : Identify potential security issues

Analyzes, investigates and quickly identifies the root cause of security issues or suspicious activities (using ML & graphs).
Automatically collects and processes events
Produces visualizations.

AWS Abuse:
Report suspected AWS resources used for abusive or illegal purposes.
Abusive & prohibited behaviors are:
1) Spam
2) Port scanning
3) DoS or DDoS attacks
4) Intrusion attempts
5) Hosting objectionable or copyrighted content
6) Distributing malware.

Root User privileges
Root user = Account owner
Complete access to all AWS services & resources.
Lock away your AWS account root user Access keys!
Actions performed (can be) by root user only:
1) Change account settings
2) View certain tax invoices
3) Close your AWS account
4) Restore IAM user permissions
5) Change / Cancel your AWS support Plan
6) Register as a seller in the Reserved Instance Marketplace.
7) Config an Amazon S3 bucket to enable MFA.
8) Edit / Delete an Amazon S3 bucket policy
Sign up for GovCloud

Security & Compliance Summary *

- Shared responsibility on AWS
- Shield: Automatic DDoS Protection + 24/7 support
- WAF: Firewall to filter incoming requests based on rules.
- KMS: Encryption keys managed by AWS.
- Cloud HSM: Hardware encryption we manage encryption keys.
- AWS Certificate Manager: Provision, Manage and deploy SSL/TLS certificates.
- Artifact = Get access to compliance reports.
- GuardDuty - Find malicious behavior with VPC, DNS & CloudTrail logs.
- Inspector: For EC2 only, install agent and find vulnerabilities.
- Config: Track config changes and compliance against rules.
- Macie: Find sensitive data (ex. PII data) in Amazon S3 buckets.
- CloudTrail: Track API calls made by users with account
- AWS Security Hub: Gather security findings from multiple AWS accounts.
- Amazon Detective: Find the root cause of security issue or suspicious activities.
- Amazon Abuse: Report AWS resources used for abusive or illegal purposes.
- Root User privileges:

1) Change account settings
2) Close your AWS account
3) Change / cancel your AWS support plan.
4) Register as a seller at Reserved Instance Marketplace