Security on AWS

Infrastructure and Services to elevate your security in the cloud

Isha Doshi
Associate Solutions Architect

Agenda – Security on AWS

- How AWS thinks about Security
- The AWS Shared Responsibility Model
- Foundational Controls
- The Well Architected Framework – The Security Pillar
    - Identity and Access Management
    - Detection
    - Infrastructure Protection
    - Data Protection
    - Incident Response

aws

How AWS thinks about Security

Security is the top priority

Security is
everyone's responsibility

Guardrails, not gates

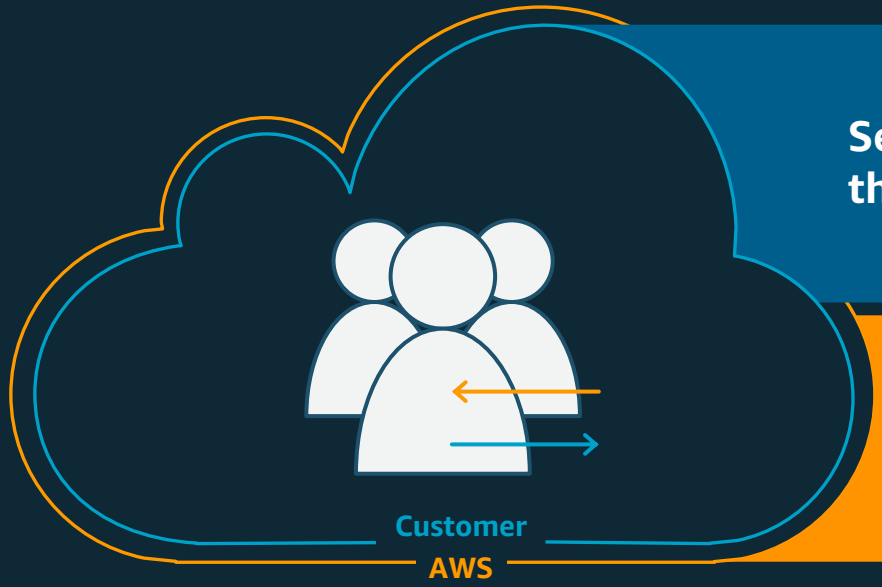
Security is a journey

aws

The AWS Shared Responsibility Model

aws

Shared responsibility model



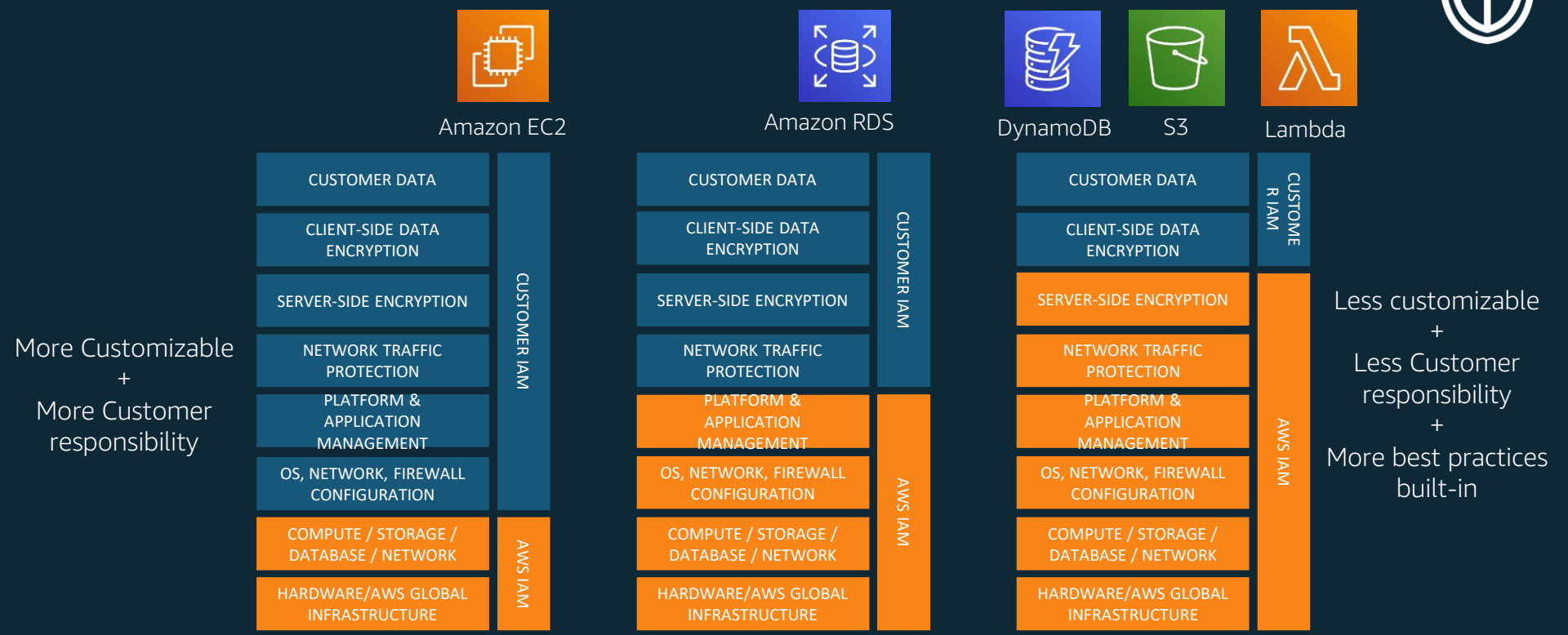
Security IN the Cloud

Customer responsibility will be determined by the AWS Cloud services that a customer selects

Security OF the Cloud

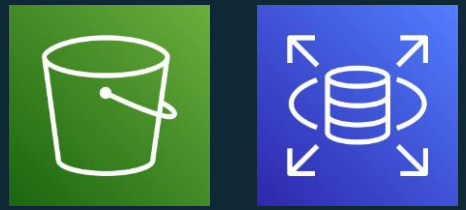
AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud

The line varies …

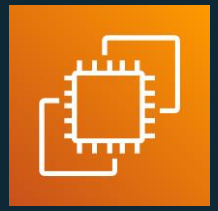


Your AWS Account is precious

AWS Account



Sensitive customer data



Running workloads

Payment information

Foundational Security controls

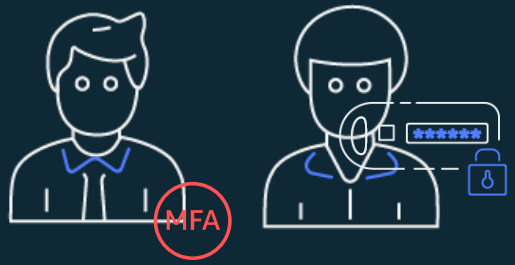
- Accurate account information
- Protecting your Root User
- Using IAM Users
- Configuring alarms
- Turning CloudTrail ON
- Using AWS Config
- Using Trusted Advisor

aws

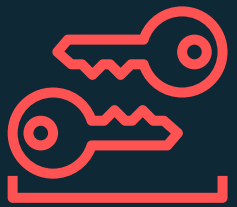
Protect your Root User

Use a complex password

Turn on MFA



Separate password and MFA holder



Delete access keys

Set up alarms

AWS CloudTrail

AWS CloudTrail – Auditing, Governance and Compliance

Record Activity – actions taken by user, role or AWS service

Simplify compliance by automatically recording and storing activity logs

Gain visibility – view, search, download, analyze, respond

Troubleshoot – who/what took which action and when?

Build security automation by tracking and responding to threats

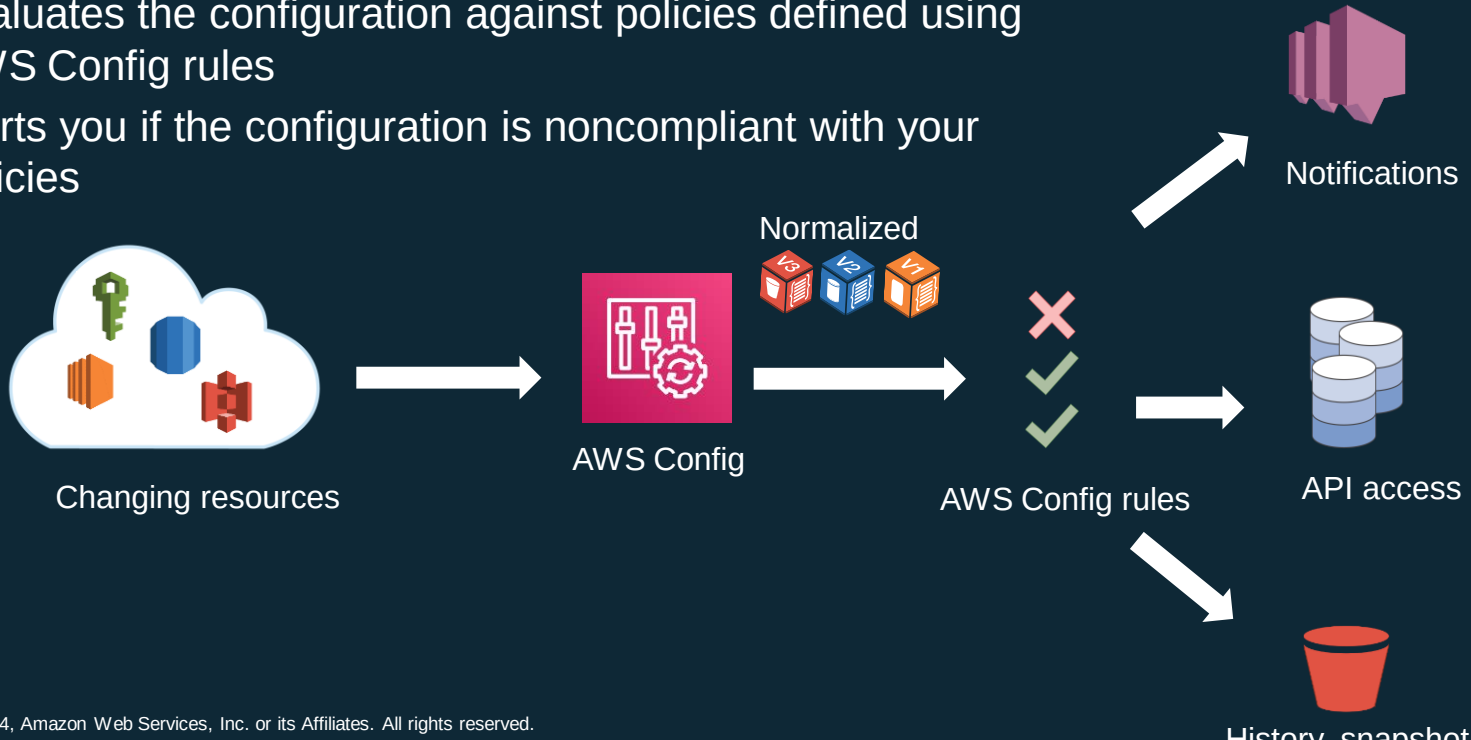
Features - CloudTrail Insights, CloudTrail Lake, Log Encryption, File Integrity Validation

aws

AWS Config

AWS Config

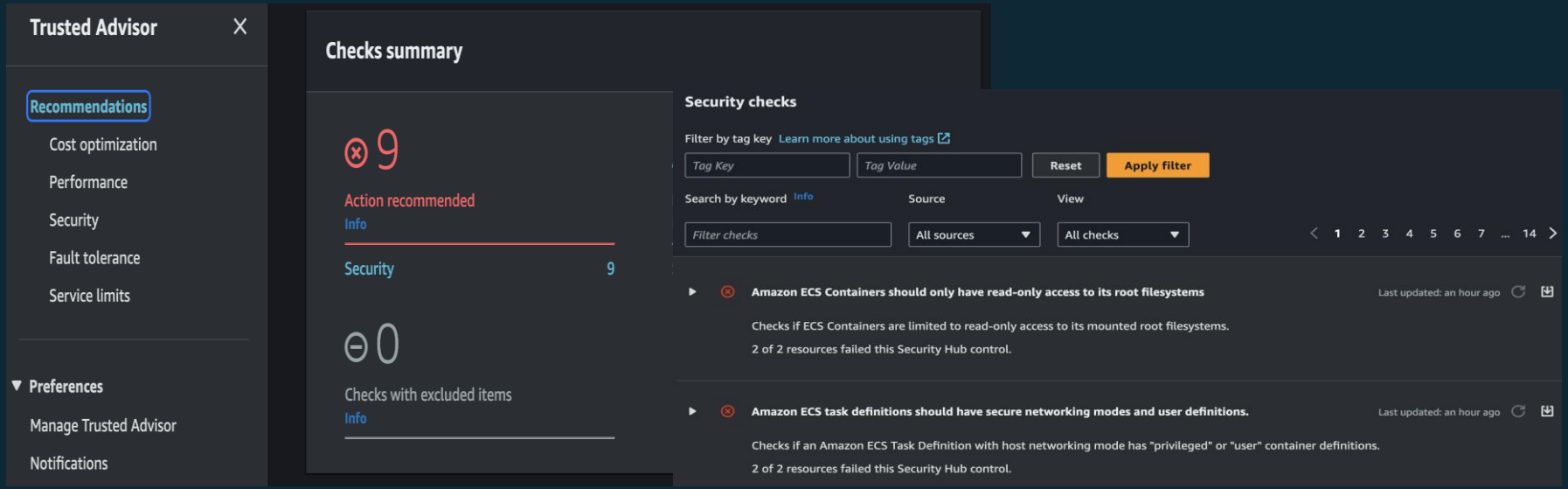
- Configuration auditor
- Monitors configuration changes over time
- Evaluates the configuration against policies defined using AWS Config rules
- Alerts you if the configuration is noncompliant with your policies



AWS Trusted Advisor

AWS Trusted Advisor

Leverage Trusted Advisor to analyze your AWS resources for best practices for availability, cost, performance and security.



The AWS Well Architected Framework

aws

AWS W-A Security Pillar

Identity and access management

Detective controls

Infrastructure protection

Data protection

Incident response

aws

Identity and Access Management

aws

Who can access what

Who

Developers and applications

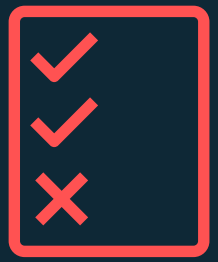
can access

Permissions

what

Resources

aws



Policy Authorization

Policy Guardrails

Goal: Least privileged access

aws

Identity and access management

Define, enforce, and audit user permissions across AWS services, actions, and resources

AWS Identity and Access Management (IAM)
Securely manage access to AWS services and resources

AWS IAM Identity Center
Centrally manage SSO access to multiple AWS accounts and business apps

AWS Directory Service
Managed Microsoft Active Directory in AWS

Amazon Cognito
Add user sign-up, sign-in, and access control to your web and mobile apps

AWS Organizations
Policy-based management for multiple AWS accounts

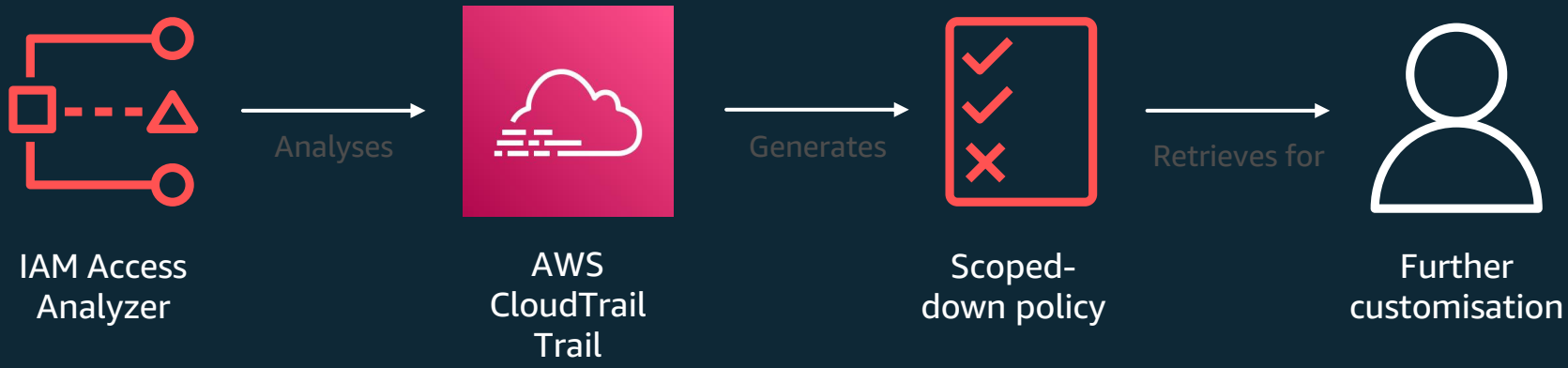
AWS Resource Access Manager
Simple, secure service for sharing AWS resources

Amazon Verified Permissions
Fine-grained permissions and authorization for your applications

aws

IAM Access Analyzer - Generate Policies based on Access Activity

IAM Access Analyzer reviews your AWS CloudTrail logs and generates a policy template that contains the permissions that have been used by the entity in your specified time frame.



Detection

aws

Detective controls

Gain the visibility you need to spot issues before they impact your business, improve your security posture, and reduce the risk profile of your environment

AWS Security Hub
Automate AWS security checks and centralize security alerts.

Amazon GuardDuty
Protect your AWS accounts with intelligent threat detection.

Amazon Inspector
Automated and continual vulnerability management at scale.

Amazon CloudWatch
Observe and monitor resources and applications on AWS, on premises, and on other clouds.

AWS Config
Assess, audit, and evaluate configurations of your resources.

AWS CloudTrail
Track user activity and API.

VPC Flow Logs
Capture info about IP traffic going to and from network interfaces in your VPC.

Amazon Security Lake
Automatically centralize your security data in a few steps.

Amazon GuardDuty

What is Amazon GuardDuty?

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.

Threat detection using two methods:

- Threat Intelligence
- Machine Learning

aws

Amazon Inspector

Amazon Inspector

AUTOMATED AND CONTINUAL VULNERABILITY MANAGEMENT AT SCALE

Amazon Inspector is an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure.

- AMAZON ELASTIC COMPUTE CLOUD (EC2)
- CONTAINER IMAGES RESIDING IN AMAZON ELASTIC CONTAINER REGISTRY (AMAZON ECR)
- AWS LAMBDA FUNCTIONS

AWS Security Hub

What is AWS Security Hub?

AWS Security Hub is the compliance and security center for AWS customers

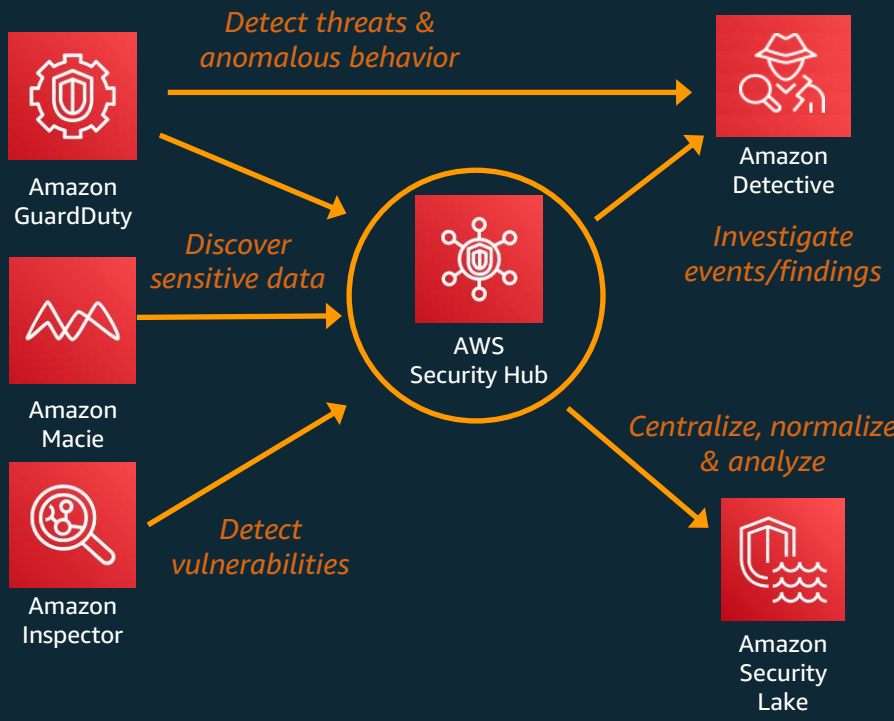
- One part automated checks against compliance standards
- One part SIEM-like aggregation for AWS-related “findings”

aws

Threat detection, monitoring, and response

Security Monitoring and Threat Detection

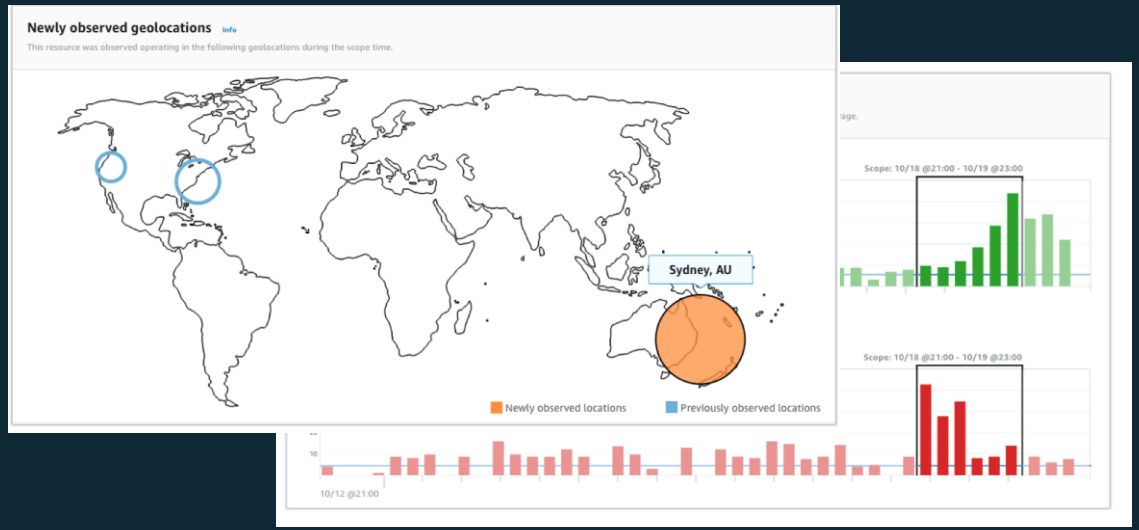
Integrated with AWS Workloads in an AWS Account, along with identities and network activity



Amazon Detective

Introducing Amazon Detective

Analyze and visualize security data to rapidly get to the root cause of potential security issues



Infrastructure Security

aws

Infrastructure protection

Reduce surface area to manage and increase privacy for and control of your overall infrastructure on AWS

AWS Firewall Manager
Centrally configure and manage firewall rules across your accounts.

AWS Network Firewall
Deploy network firewall security across your VPCs.

AWS Shield
Maximize application availability and responsiveness with managed DDoS protection.

AWS WAF (Web Access Firewall)
Protects your web applications from common exploits.

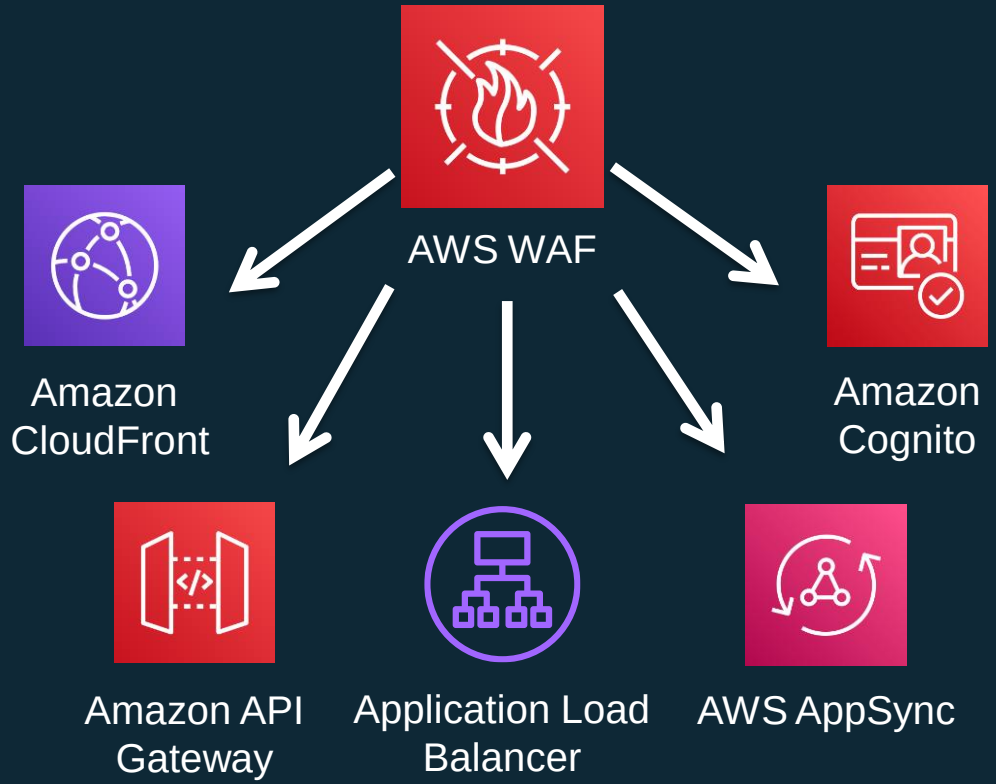
Amazon Virtual Private Cloud
Define and launch AWS resources in a logically isolated virtual network.

AWS PrivateLink
Establish connectivity between VPCs and AWS services without exposing data to the internet.

AWS Systems Manager
Gain operational insights into AWS and on-premises resources.

AWS Verified Access
Provide secure access to corporate applications without a VPN.

AWS WAF - Layer 7 Protection



- Managed, Elastic, and **Integrated** WAF
- Pay-as-you-go
- Rules Managed by AWS
  + Custom Rules.
  + Provided by partners

DDoS protection with AWS Shield

Standard

Available to all AWS customers at no additional cost

- Protection against the most common attacks (SYN/UDP Floods, Reflection Attacks, etc. Layer 3/4)
- Automatic detection and mitigation

Advanced

Paid service that provides additional protection against sophisticated attacks

+ Protection against advanced attacks (Layer 7)
+ 24x7 DDoS Response Team (Proactive/Reactive)
+ Cost protection
+ Faster Mitigation/Better Visualization
+ Includes WAF and Firewall Manager

aws

AWS Network Firewall: Native Firewall

Automatically scale, managed AWS infrastructure

Highly flexible, high-capacity rule engine with managed IPS rules

Centrally manage policies, real-time monitoring

There are no upfront commitments and you only pay for what you use

aws

Data protection

aws

Data protection

A suite of services designed to automate and simplify many data protection and security tasks ranging from key management and storage to credential management.

Amazon Macie
Discover and protect your sensitive data at scale.

AWS Key Management Service (AWS KMS)
Create and control keys used to encrypt or digitally sign your data.

AWS CloudHSM
Manage single-tenant hardware security modules (HSMs) on AWS.

AWS Certificate Manager
Provision and manage SSL/TLS certificates with AWS services and connected resources.

AWS Secrets Manager
Centrally manage the lifecycle of secrets.

AWS VPN
Connect your on-premises networks and remote workers to the cloud.

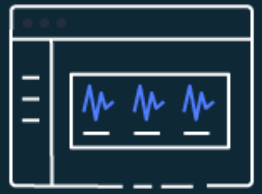
Server-Side Encryption
Flexible data encryption options using AWS service managed keys, AWS managed keys via AWS KMS, or customer managed keys.

AWS Private CA
Create private certificates to identify resources and protect data.

Amazon Macie

Amazon Macie

- *Discover and protect your sensitive data at scale*



Gain visibility and evaluate

- Bucket inventory
- Bucket policies

Discover sensitive data

- Inspection jobs
- Flexible scope

Centrally manage at scale

- AWS Organizations
- Managed & custom data detections

Automate and take actions

- Detailed findings
- Management APIs

Amazon Macie – Data Identifiers

- Fully managed sensitive data types
- Amazon Macie maintains a growing list of sensitive data types that include common personally identifiable information (PII) and other sensitive data types as defined by data privacy regulations, such as GDPR, PCI-DSS, CCPA and HIPAA.

Data identifiers

- *Financial (card, bank account numbers…)*
- *Personal (names, address, contact…)*
- *National (passport, ID, driver license…)*
- *Medical (healthcare, drug agency …)*
- *Credentials & secrets (AWS secret keys, private keys …)*
- *Custom – regex, keywords*
- *Allow Lists*

Amazon Macie – Supported File Formats

- Supported file and storage formats in Amazon Macie
- When Amazon Macie analyzes data in an S3 bucket, it performs a deep inspection that factors the file or storage format for the data. Macie can analyze and detect sensitive data in many different formats, including commonly used compression and archive formats.

File and storage formats

Big Data - Apache Avro object containers and Apache Parquet files
Compression or archive - .gz, .gzip, .tar, .zip
Document - .doc, .docx, .pdf, .xls, .xlsx
Text - .csv, .htm, .html, .json, .tsv, .txt, .xml, and others (depending on the type of non-binary text file)

Incident Response

aws

Incident response

During an incident, containing the event and returning to a known good state are important elements of a response plan. AWS provides the following tools to automate aspects of this best practice.

Amazon Detective

Analysis and visualization of security data to get to the root cause of potential security issues quickly

Amazon EventBridge

Serverless event bus that makes it easier to build event-driven applications to scale your programmed, automated response to incidents

AWS Backup

Centrally manage and automate backups across AWS services to simplify data protection at scale

AWS Security Hub

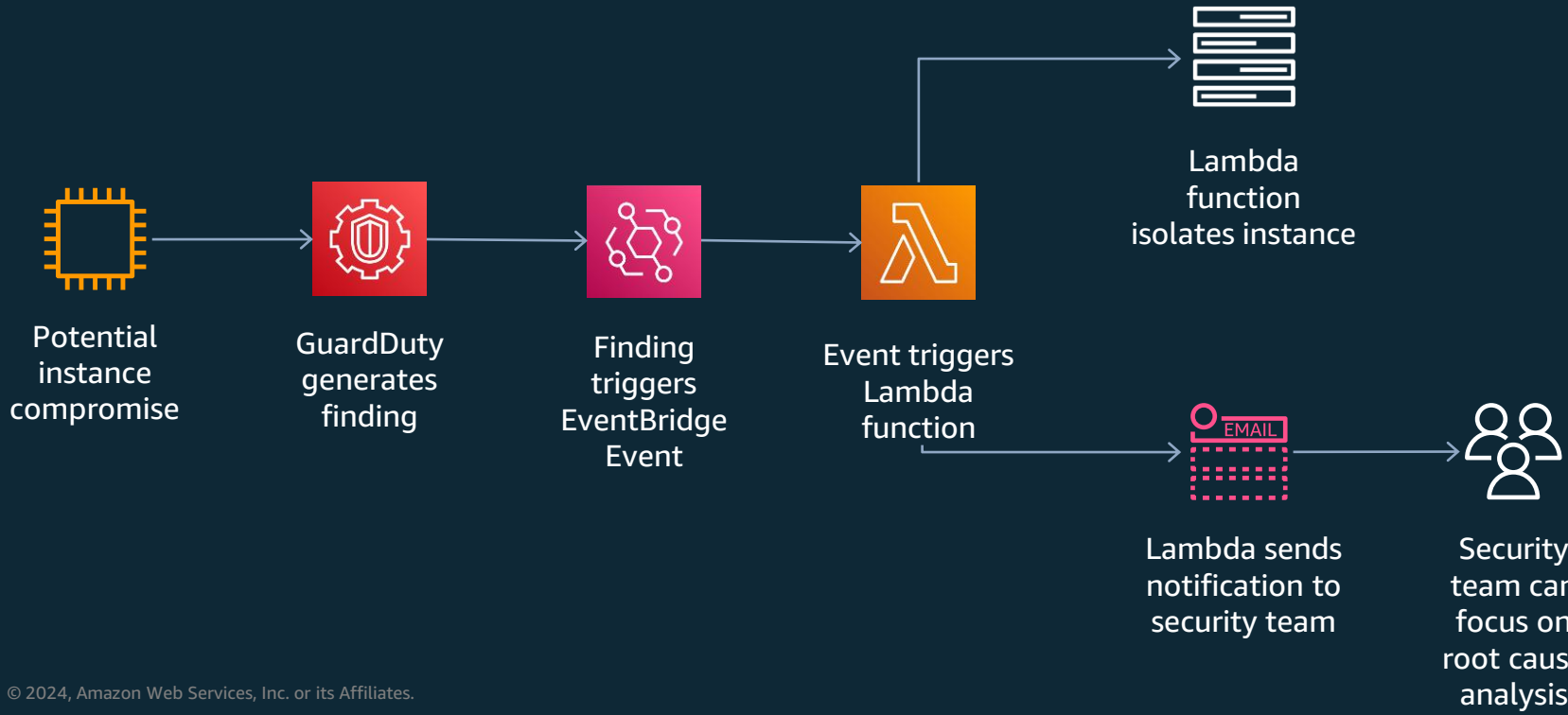
Out-of-the-box integrations with ticketing, chat, SIEM, SOAR, threat investigation, incident management, and GRC tools to support your security operations workflows

AWS Elastic Disaster Recovery

Fast, automated, cost-effective disaster recovery

Automated Incident Response – simple example

Automated process



aws

Recap

- How AWS thinks about Security
- The AWS Shared Responsibility Model
- Foundational controls
- The Well Architected Framework – The Security Pillar
    - Identity and Access Management
    - Detection
    - Infrastructure protection
    - Data protection
    - Incident response

aws

Useful Resources

- AWS Security Portal
- AWS Startup Security Baseline (SSB)
- AWS Security Solutions Library
- Security Pillar of AWS Well-Architected Framework – Design cloud architectures with security in mind.
- Security Reference Architecture
- AWS Architecture Center
- AWS Security Services
- Best Practices for Security, Identity and Compliance – Whitepapers, blogs, videos, workshops
- Customer Success Stories
- Security Competency Partners
- Security Learning

Thank you!

Isha Doshi| irdoshi@amazon.com