# Security Immersion Day

Kuala Lumpur 2020

Andrei Lizarraga-Cardenas
Partner Solutions Architect
jrliz@amazon.com

Kimberly Chow
Specialist Security Solutions Architect
kimbchow@amazon.com

# Agenda

0900 - 0930 AWS Security Services

0930 – 1030 Essential Security Patterns and Security Best Practices

1030 – 1100 Break

1100 – 1230 Builders session Part 1: Identify vulnerabilities and fix them / AWS Labs

1230 – 1330 Lunch

1330 – 1400 Builders session Part 2: Analysing CloudTrail logs using Serverless Services

1400 – 1430 Break

1430 – 1600 Security FAQ

# Labs / Challenge

2 Tracks Hands-on for security services:

1. Security Workshop

http://bit.ly/aws-sec-workshop

## Feeling adventurous?

2. Security Challenge

http://bit.ly/aws-sec-challenge

Discover the 10 security mistakes and if you are the fasters one, win some awesome AWS Swag

# Common Security Questions

## Security teams often ask the following questions:

- Do I have adequate security to protect my workloads and data?
- How ‘good’ is good enough?
- What security controls do I need?
- Do I have validation that the right controls were built?
- Do I have verification that the controls work as planned?

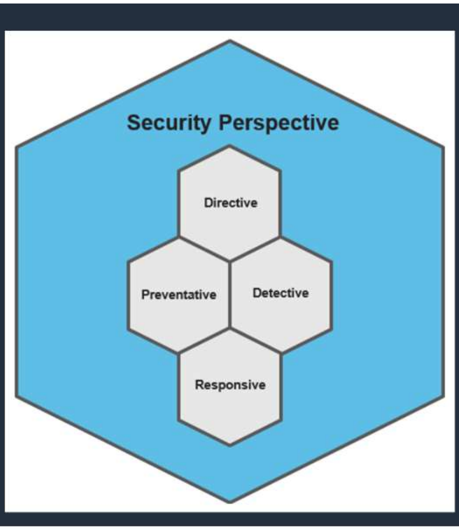
# AWS Security Perspective

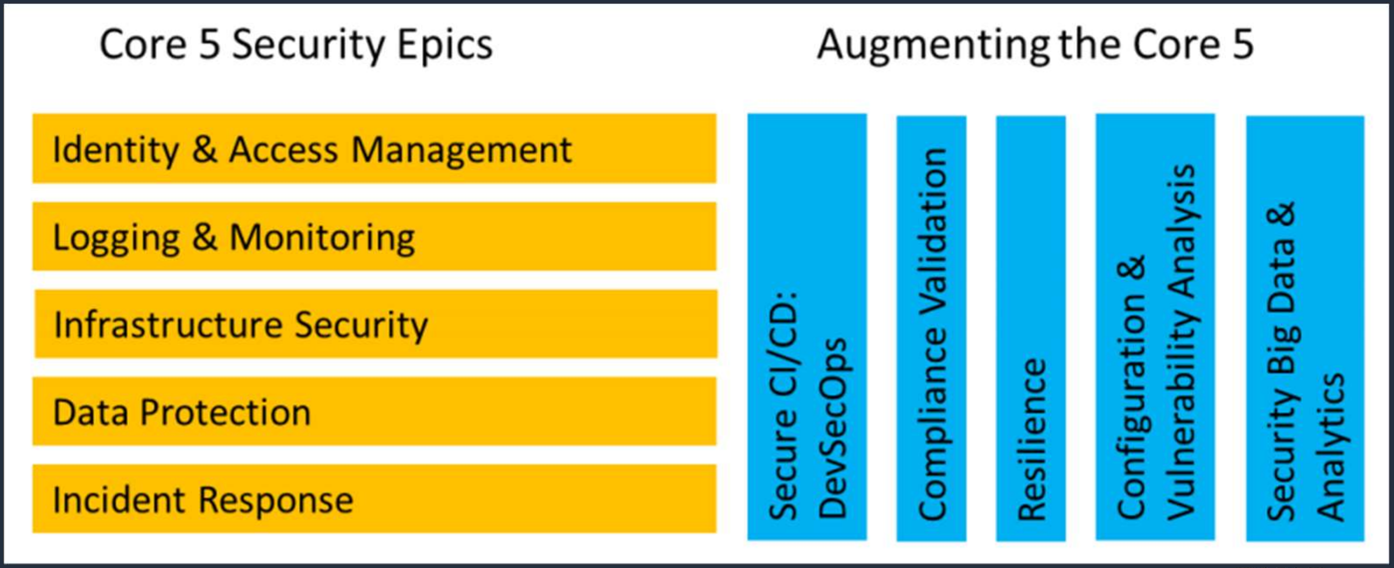
**Directive** controls establish the governance, risk, and compliance models the environment will operate within.

**Preventive** controls protect your workloads and mitigate threats and vulnerabilities.

**Detective** controls provide full visibility and transparency over the operation of your deployments in AWS.

**Responsive** controls drive remediation of potential deviations from your security baselines.





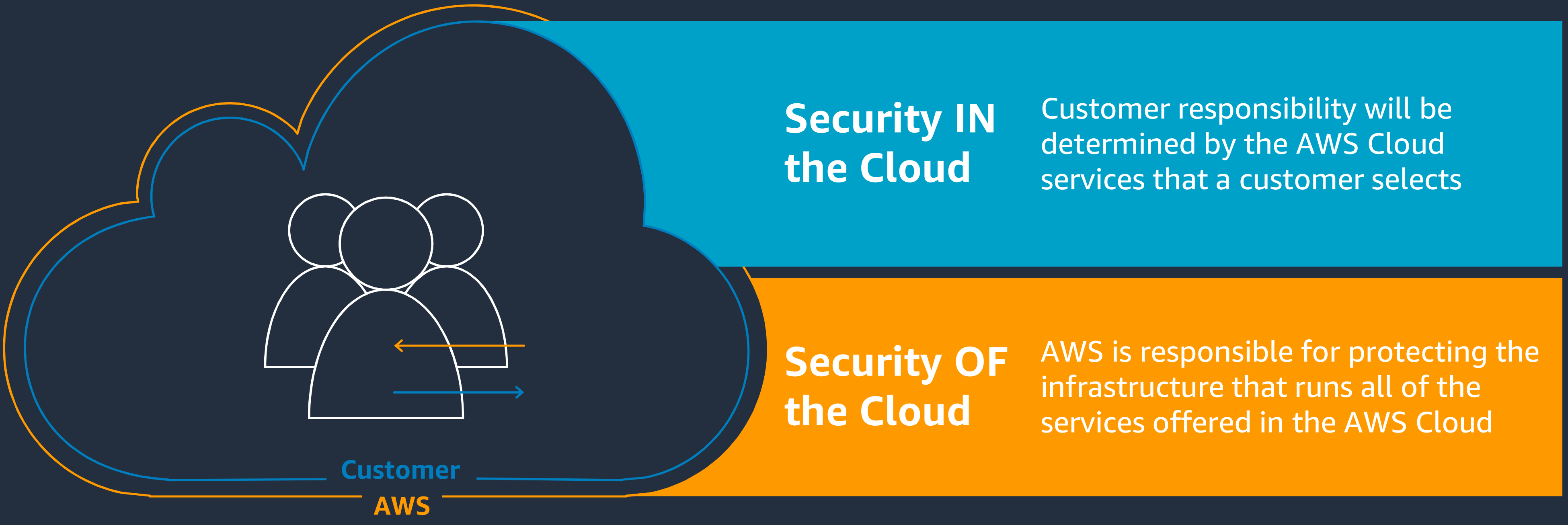
Core 5 Security Epics

- Identity & Access Management
- Logging & Monitoring
- Infrastructure Security
- Data Protection
- Incident Response

Augmenting the Core 5

- Secure CI/CD: DevSecOps
- Compliance Validation
- Resilience
- Configuration & Vulnerability Analysis
- Security Big Data & Analytics

# Shared responsibility model



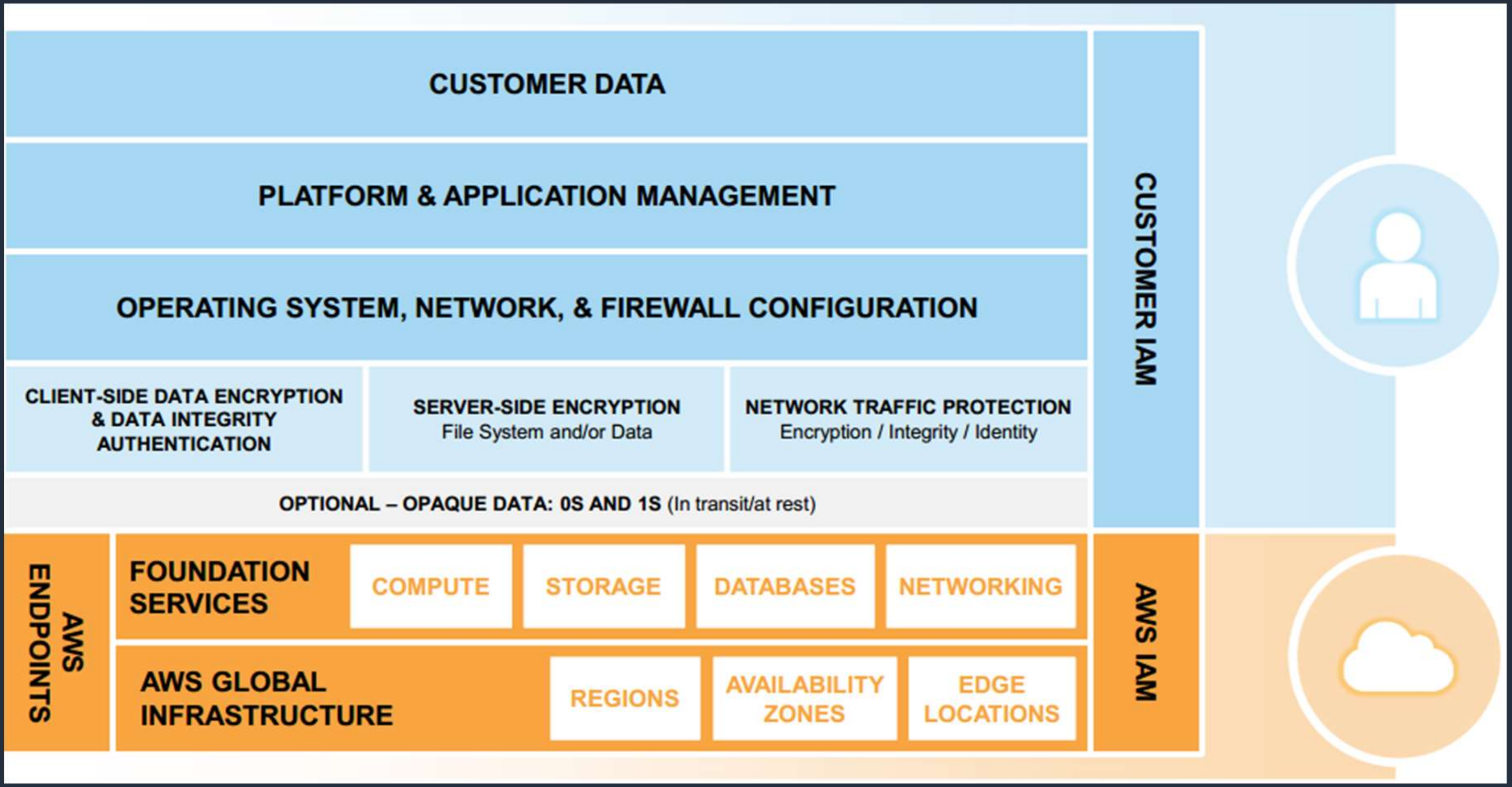
**Security IN the Cloud**

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

# Infrastructure Services – e.g. EC2



CUSTOMER DATA

PLATFORM & APPLICATION MANAGEMENT

OPERATING SYSTEM, NETWORK, & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION File System and/or Data

NETWORK TRAFFIC PROTECTION Encryption / Integrity / Identity

OPTIONAL – OPAQUE DATA: 0S AND 1S (In transit/at rest)

CUSTOMER IAM

AWS ENDPOINTS

FOUNDATION SERVICES: COMPUTE, STORAGE, DATABASES, NETWORKING

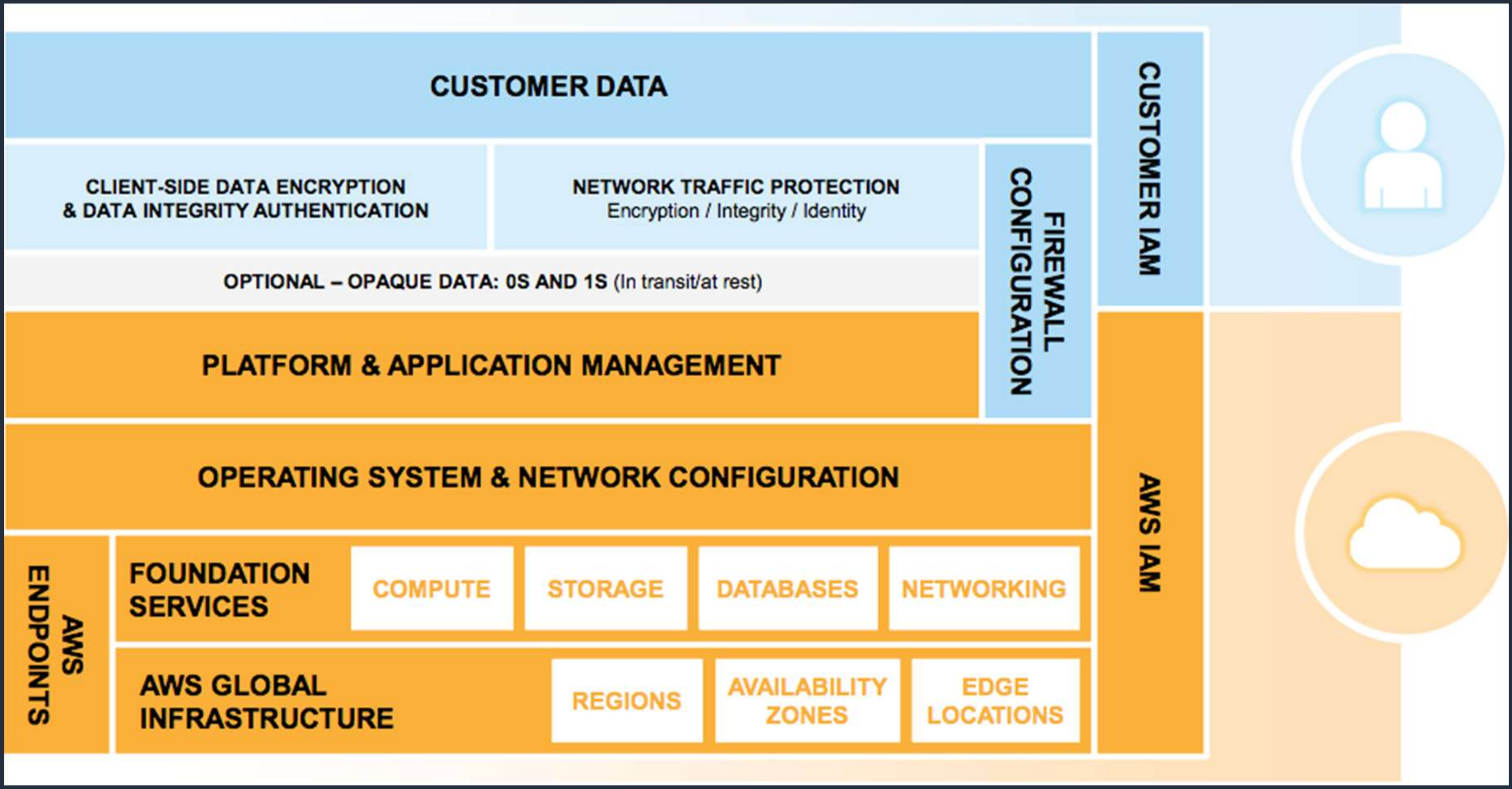
AWS GLOBAL INFRASTRUCTURE: REGIONS, AVAILABILITY ZONES, EDGE LOCATIONS

AWS IAM

Managed by AWS Customers

Managed by Amazon Web Services

# Container Services – e.g. RDS



CUSTOMER DATA

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

NETWORK TRAFFIC PROTECTION
Encryption / Integrity / Identity

OPTIONAL – OPAQUE DATA: 0S AND 1S (In transit/at rest)

FIREWALL CONFIGURATION

CUSTOMER IAM

PLATFORM & APPLICATION MANAGEMENT

OPERATING SYSTEM & NETWORK CONFIGURATION

AWS IAM

AWS ENDPOINTS

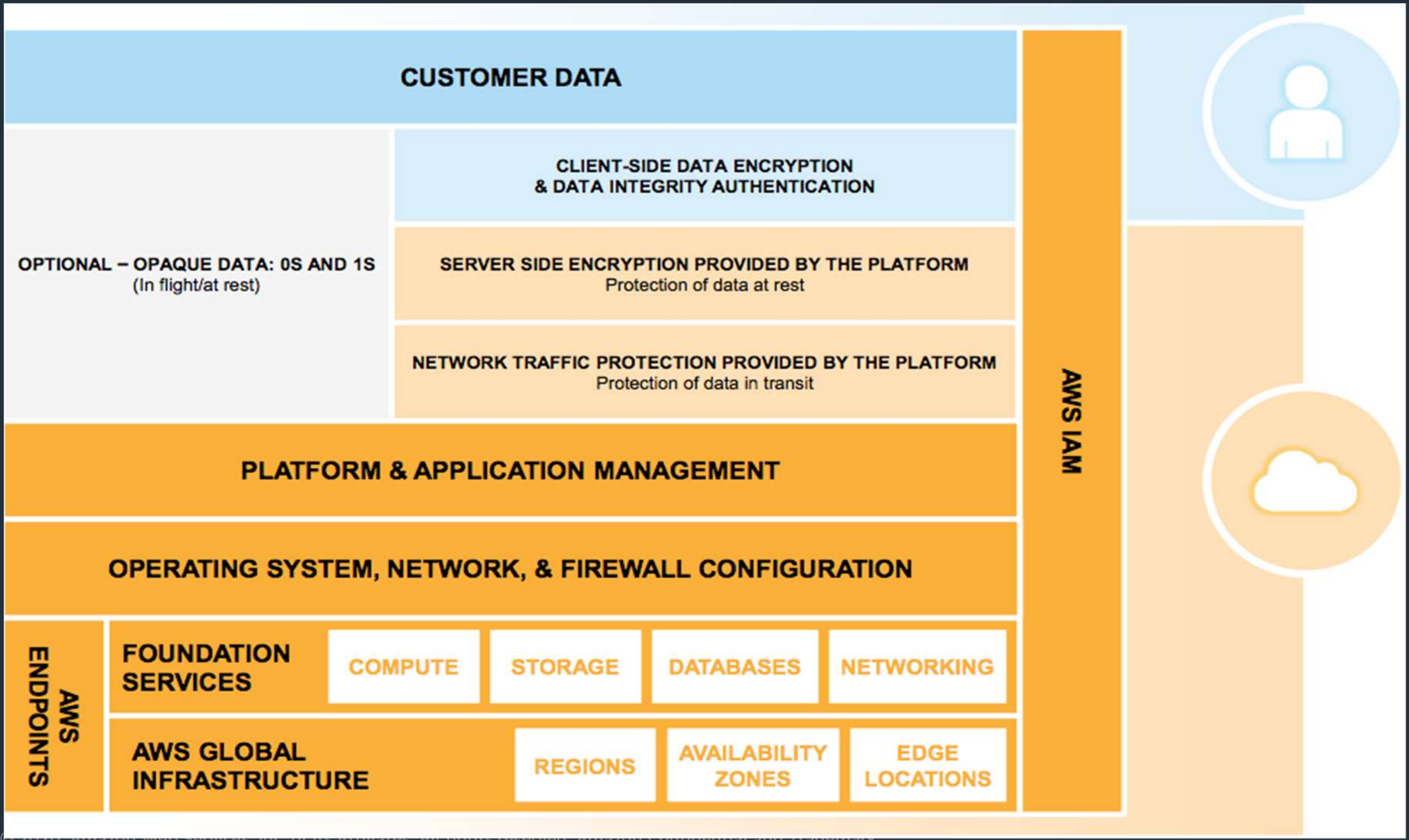
FOUNDATION SERVICES: COMPUTE, STORAGE, DATABASES, NETWORKING

AWS GLOBAL INFRASTRUCTURE: REGIONS, AVAILABILITY ZONES, EDGE LOCATIONS

Managed by AWS Customers

Managed by Amazon Web Services

# Abstracted Services - e.g. S3



CUSTOMER DATA

OPTIONAL – OPAQUE DATA: 0S AND 1S
(In flight/at rest)

CLIENT-SIDE DATA ENCRYPTION
& DATA INTEGRITY AUTHENTICATION

SERVER SIDE ENCRYPTION PROVIDED BY THE PLATFORM
Protection of data at rest

NETWORK TRAFFIC PROTECTION PROVIDED BY THE PLATFORM
Protection of data in transit

PLATFORM & APPLICATION MANAGEMENT

OPERATING SYSTEM, NETWORK, & FIREWALL CONFIGURATION

AWS ENDPOINTS

FOUNDATION SERVICES: COMPUTE, STORAGE, DATABASES, NETWORKING

AWS GLOBAL INFRASTRUCTURE: REGIONS, AVAILABILITY ZONES, EDGE LOCATIONS

AWS IAM

Managed by AWS Customers

Managed by Amazon Web Services

# The things you have to configure on AWS

Protect your customer data and applications with

- Configuration of access controls
- Configuring encryption
- Application monitoring
- Intrusion detection/prevention
- Backups
- Disaster Recovery

# AWS security solutions

## Identity & access management

AWS Identity & Access Management (IAM)

AWS Single Sign-On

AWS Directory Service

Amazon Cognito

AWS Organizations

AWS Secrets Manager

AWS Resource Access Manager

## Detective controls

AWS Security Hub

Amazon GuardDuty

AWS Config

AWS CloudTrail

Amazon CloudWatch

VPC Flow Logs

## Infrastructure protection

AWS Systems Manager

AWS Shield

AWS WAF – Web application firewall

AWS Firewall Manager

Amazon Inspector

Amazon Virtual Private Cloud (VPC)

## Data protection

AWS Key Management Service (KMS)

AWS CloudHSM

AWS Certificate Manager

Amazon Macie

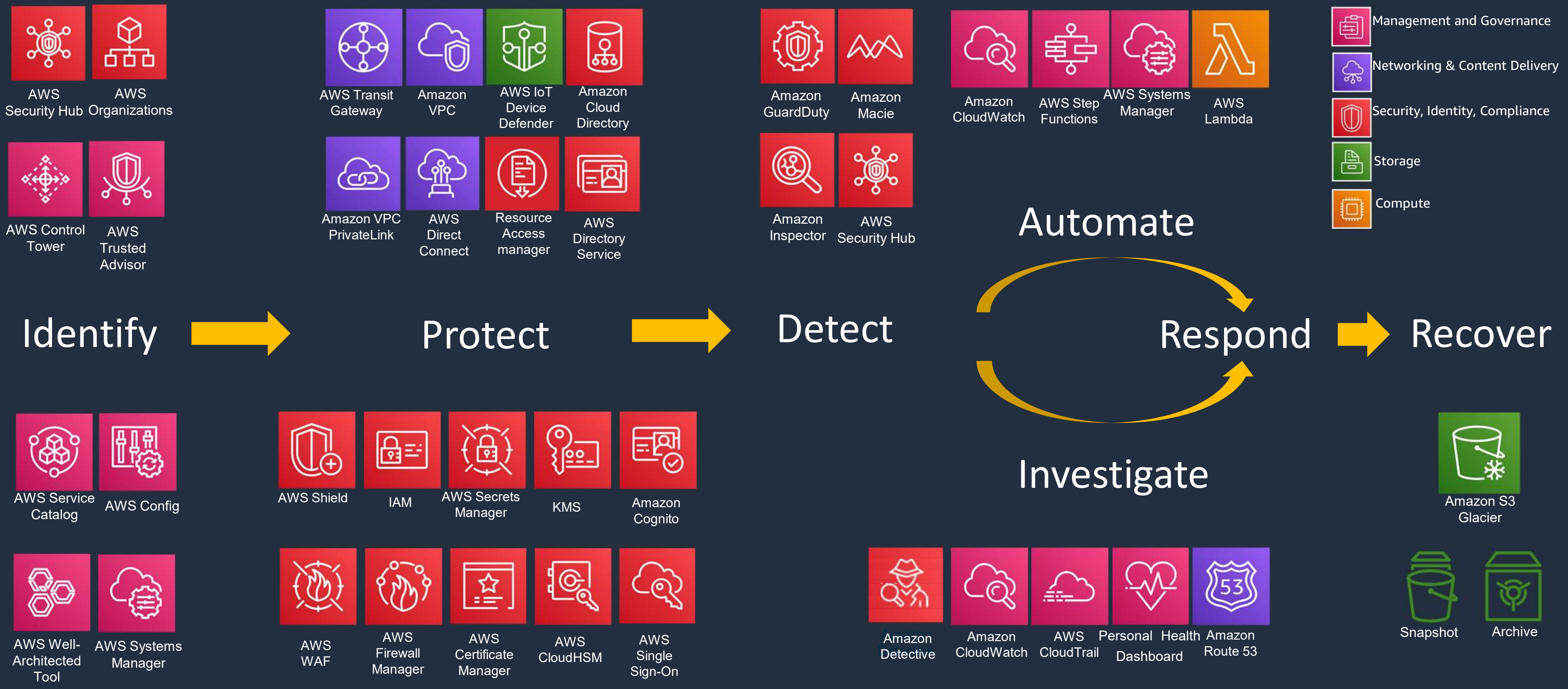
Server-Side Encryption

## Incident response

AWS Config Rules

AWS Lambda

# Foundational and Layered Services against NIST CSF



AWS Security Hub

AWS Organizations

AWS Control Tower

AWS Trusted Advisor

Identify

AWS Service Catalog

AWS Config

AWS Well-Architected Tool

AWS Systems Manager

AWS Transit Gateway

Amazon VPC

AWS IoT Device Defender

Amazon Cloud Directory

Amazon VPC PrivateLink

AWS Direct Connect

Resource Access manager

AWS Directory Service

Protect

AWS Shield

IAM

AWS Secrets Manager

KMS

Amazon Cognito

AWS WAF

AWS Firewall Manager

AWS Certificate Manager

AWS CloudHSM

AWS Single Sign-On

Amazon GuardDuty

Amazon Macie

Amazon Inspector

AWS Security Hub

Detect

Amazon CloudWatch

AWS Step Functions

AWS Systems Manager

AWS Lambda

Automate

Respond

Investigate

Amazon Detective

Amazon CloudWatch

AWS CloudTrail

Personal Health Dashboard

Amazon Route 53

Recover

Amazon S3 Glacier

Snapshot

Archive

🟪 Management and Governance

🟪 Networking & Content Delivery

🟥 Security, Identity, Compliance

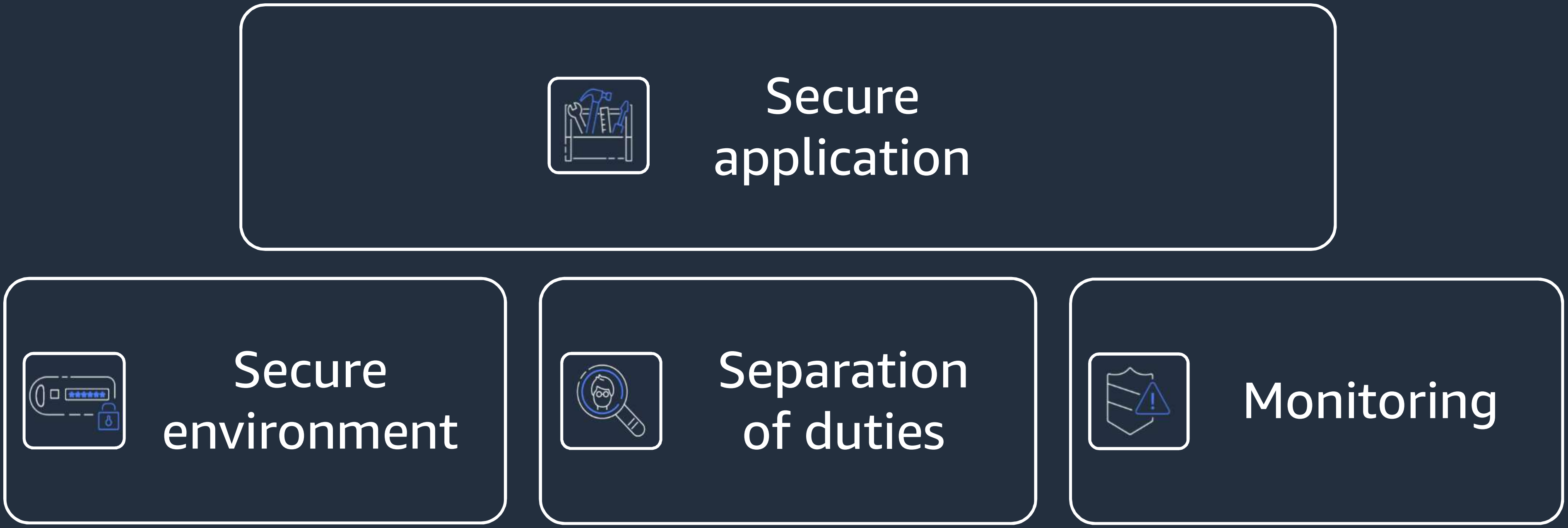
🟩 Storage

🟧 Compute

# Well Architected Security Pillar – Design Principles

- Implement a strong identity foundation
- Enable traceability
- Apply security at all layers
- Automate security best practices
- Protect data in transit and at rest
- Keep people away from data
- Prepare for security events

# Security considerations



Secure application

Secure environment

Separation of duties

Monitoring

# Secure environment – Bare Minimum

Enable MFA

Don’t use root

Federate Identity

Least privilege

Disable public buckets

# Security considerations

Secure application

Secure environment

Separation of duties

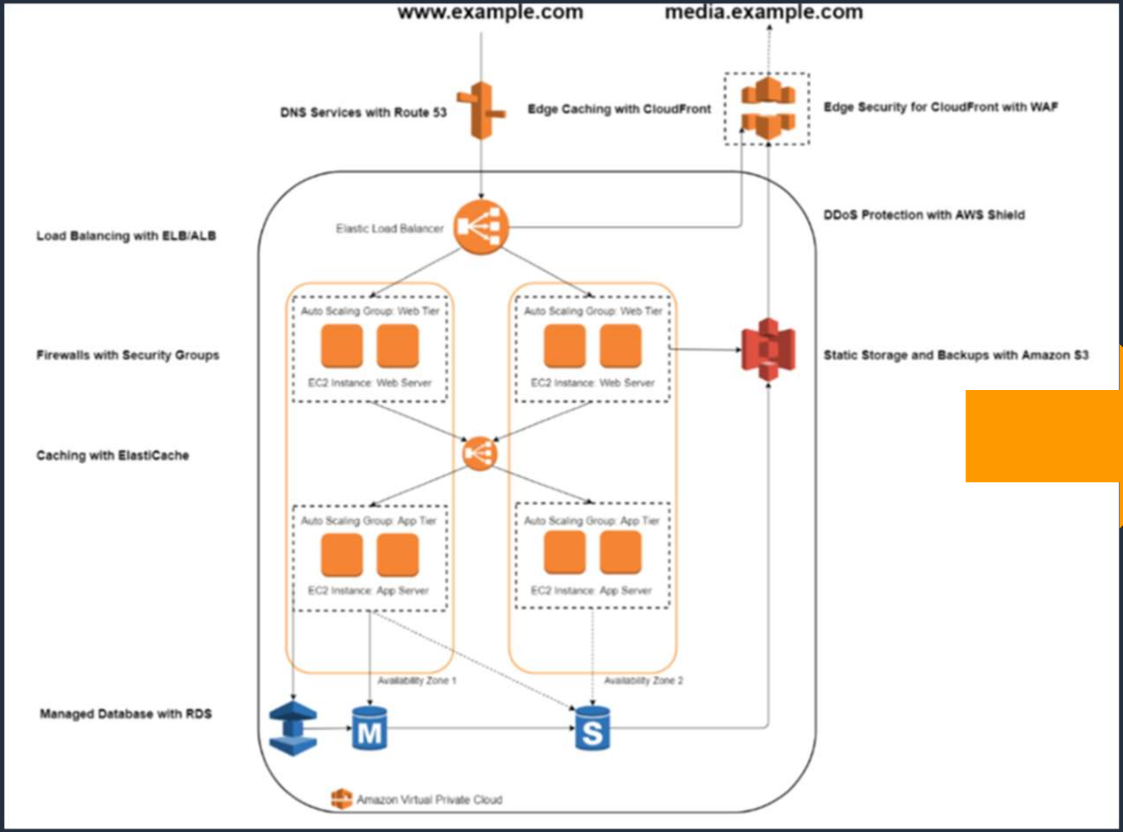
Monitoring

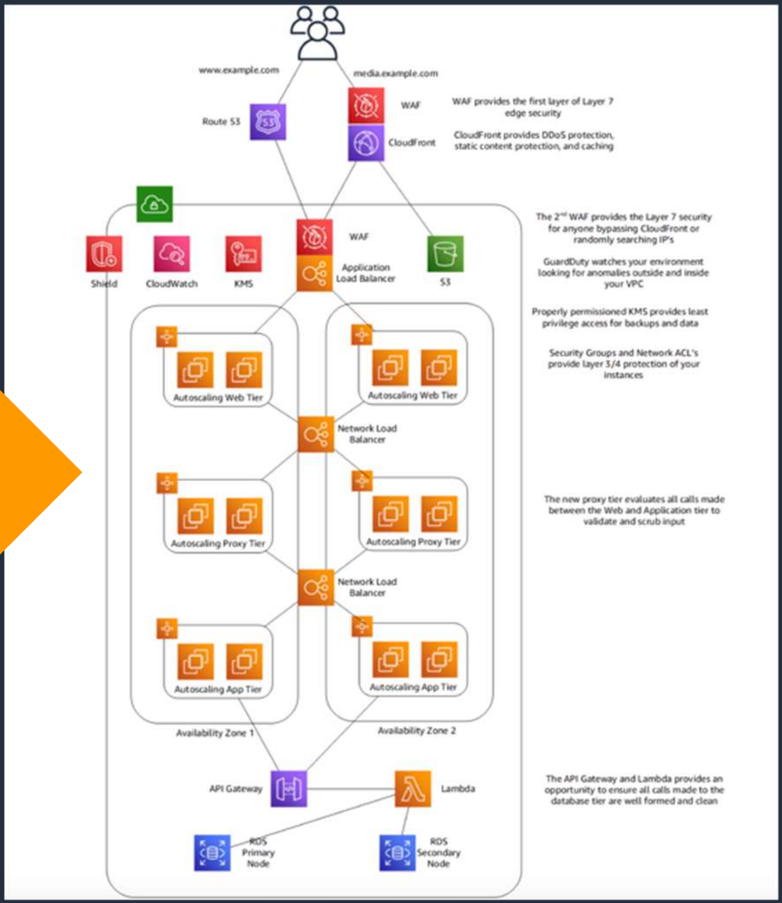
# Security Best Practices

# Common Security Requirements and Use Cases

- I want to ensure my environment can support multiple applications and teams without compromising on security.
- I want to control access to my environment, as well as know if somebody external has access to my data.
- I want to protect against cyber attacks, DDoS attacks and application layer exploits.
- I want to encrypt all my data using strong encryption. I also want to have control over the key.
- I want the ability to automatically detect security mis-configurations and respond in real-time.
- I want to be able to enforce guardrails in all my AWS accounts to ensure that my employees only do what I allow them to do.

# Zero Trust Reference Architecture


www.example.com
media.example.com
DNS Services with Route 53
Edge Caching with CloudFront
Edge Security for CloudFront with WAF
Load Balancing with ELB/ALB
Elastic Load Balancer
DDoS Protection with AWS Shield
Auto Scaling Group: Web Tier
EC2 Instance: Web Server
Auto Scaling Group: Web Tier
EC2 Instance: Web Server
Firewalls with Security Groups
Static Storage and Backups with Amazon S3
Caching with ElastiCache
Auto Scaling Group: App Tier
EC2 Instance: App Server
Auto Scaling Group: App Tier
EC2 Instance: App Server
Availability Zone 1
Availability Zone 2
Managed Database with RDS
M
S
Amazon Virtual Private Cloud



WAF provides the first layer of Layer 7 edge security

CloudFront provides DDoS protection, static content protection, and caching

The 2nd WAF provides the Layer 7 security for anyone bypassing CloudFront or randomly searching IP's

GuardDuty watches your environment looking for anomalies outside and inside your VPC

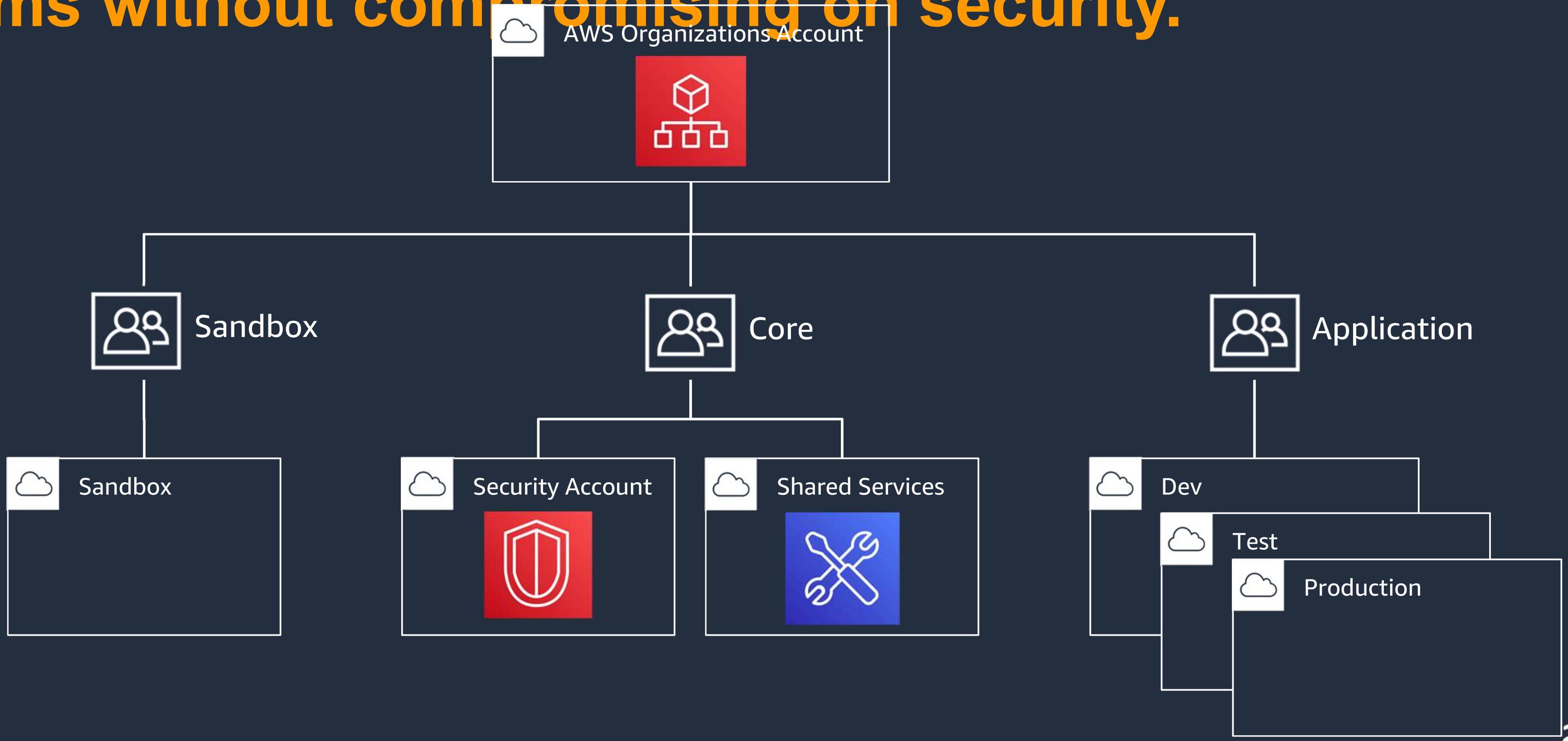
Properly permissioned KMS provides least privilege access for backups and data

Security Groups and Network ACL's provide layer 3/4 protection of your instances

The new proxy tier evaluates all calls made between the Web and Application tier to validate and scrub input

The API Gateway and Lambda provides an opportunity to ensure all calls made to the database tier are well formed and clean

# Multi-Account Strategy - “I want to ensure my environment can support multiple applications and teams without compromising on security.”



# Demo – Service Control Policy on AWS Organisations

## AWS IAM Best Practices - “I want to control access to my environment, as well as know if somebody external has access to my data.”

1. **Users** – Create individual users.
2. **Permissions** – Grant least privilege.
3. **Groups** – Manage permissions with groups.
4. **Auditing** – Enable AWS CloudTrail
5. **Password** – Configure a strong password policy.
6. **Rotate** – Rotate security credentials regularly.
7. **MFA** – Enable MFA for all users.
8. **Roles and Attributes** – Use IAM roles for Amazon EC2 instances.
9. **Root** – Reduce or remove use of root.

# Managing Credentials and Authentication with AWS

## 1) Create individual users

IAM

Creating individual users ensures the auditability of accounts.

## 2) Grant least Privilege

IAM

IAM Roles

Secrets Manager

Least privilege at every layer limits the blast radius in the event of a compromise.

Use access advisor to check for last accessed date for each user and limit permissions.

## 3) Enable CloudTrail

CloudTrail

Enabling CloudTrail allows you to monitor and log API calls in your AWS environment.

Practice log diving frequently so that in the event of a compromise you are able to investigate and respond quickly.

# Managing Credentials and Authentication with AWS

4) Use **multiple AWS accounts** to reduce blast radius

Production

Staging

AWS accounts provide administrative isolation between workloads across different lines of business, regions, stages of production and types of data classification.

5) Use **limited roles** and grant **temporary security credentials**

IAM

IAM Roles

Secrets Manager

IAM roles and temporary security credentials mean you don't always have to manage long-term credentials and IAM users for each entity that requires access to a resource.

Rotate security credentials regularly.

6) **Federate** to an existing identity service

IAM

MFA token

AWS SSO

Cognito

Control access to AWS resources, and manage the authentication and authorisation process without needing to re-create all your corporate users as IAM users.

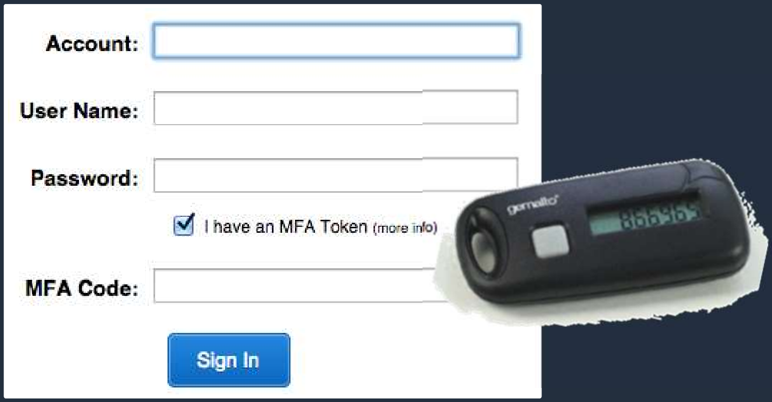
# IAM - Continued

- Integration with workforce management – movers, leavers joiners.
- Access keys in github ☺

# AWS Identity Authentication - “I want to control access to my environment, as well as know if somebody external has access to my data.”

## AWS Management Console

Login with **Username/Password** with optional **MFA** (recommended)



Account:

User Name:

Password:

☑ I have an MFA Token (more info)

MFA Code:

Sign In

For time-limited access: **a Signed URL in Amazon CloudFront can** provide temporary access to the Console

## API access

Access API using **Access Key + Secret Key**, with optional MFA

**ACCESS KEY ID**

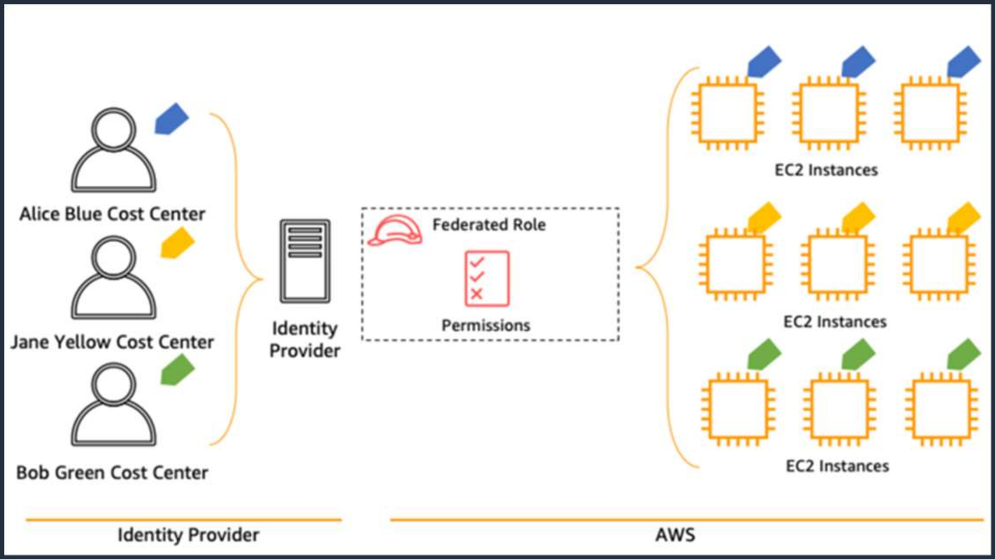
Ex: `AKIAIOSFODNN7EXAMPLE`

**SECRET KEY**

Ex: `UtnFEMI/K7MDENG/bPxRfiCYEX`

For time-limited access: Call the AWS Security Token Service (STS) to get a temporary AccessKey + SecretKey + session token

# Attribute Based Access Control (ABAC) - “I want to control access to my environment, as well as know if somebody external has access to my data.”



https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_attribute-based-access-control.html

# IAM Access Analyzer - “I want to control access to my environment, as well as know if somebody external has access to my data.”

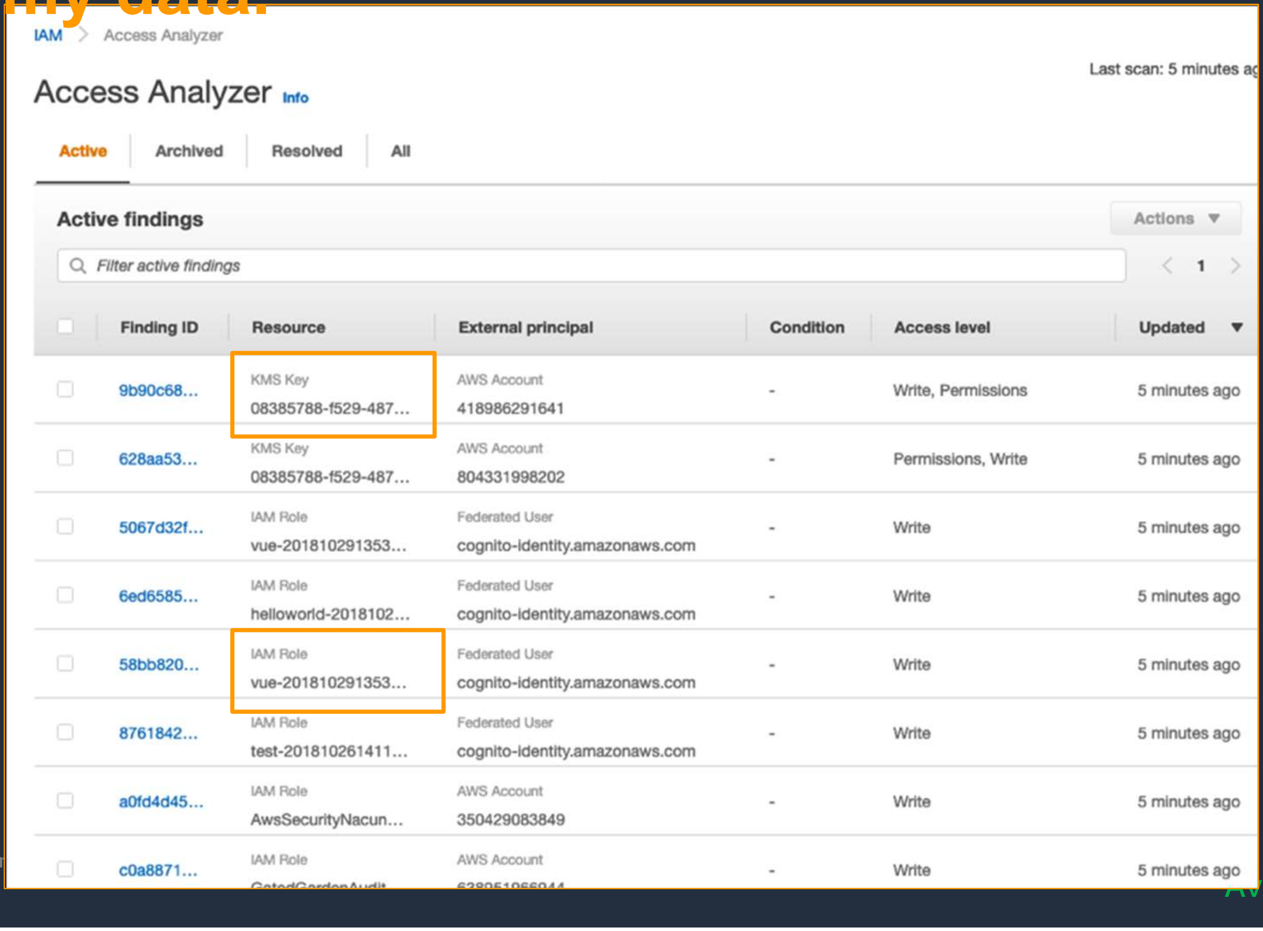
**AWS Identity and Access Management Access Analyzer**

Continuously generate comprehensive findings if your resource policies grant **public or cross-account access.**

**Useful for vendor management.**

Available in Singapore region

# IAM Access Analyzer - "I want to control access to my environment, as well as know if somebody external has access to my data."



IAM > Access Analyzer

Last scan: 5 minutes ag

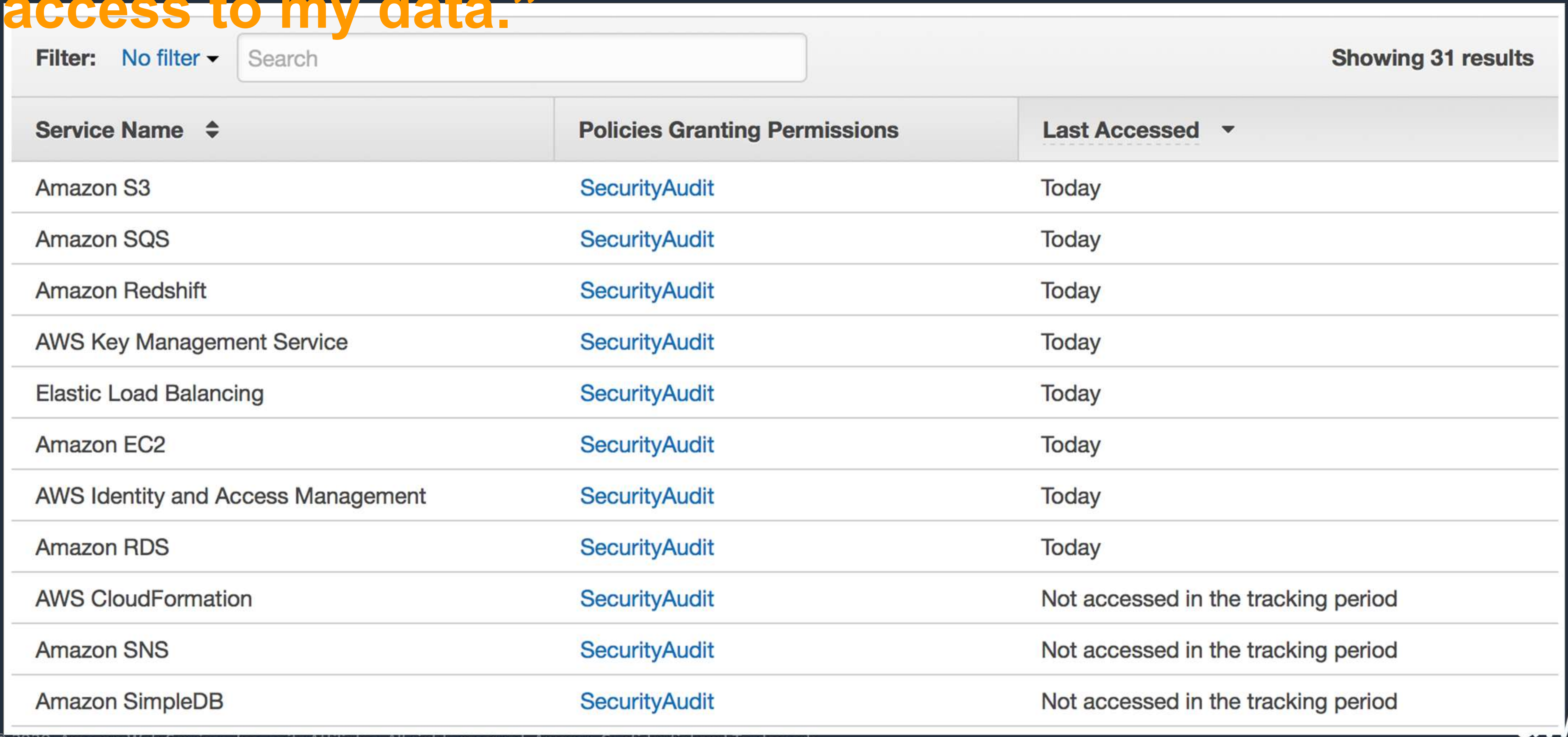
## Access Analyzer Info

### Active findings

| □ | Finding ID | Resource | External principal | Condition | Access level | Updated ▼ |
|---|---|---|---|---|---|---|
| □ | 9b90c68... | KMS Key<br>08385788-f529-487... | AWS Account<br>418986291641 | - | Write, Permissions | 5 minutes ago |
| □ | 628aa53... | KMS Key<br>08385788-f529-487... | AWS Account<br>804331998202 | - | Permissions, Write | 5 minutes ago |
| □ | 5067d32f... | IAM Role<br>vue-201810291353... | Federated User<br>cognito-identity.amazonaws.com | - | Write | 5 minutes ago |
| □ | 6ed6585... | IAM Role<br>helloworld-2018102... | Federated User<br>cognito-identity.amazonaws.com | - | Write | 5 minutes ago |
| □ | 58bb820... | IAM Role<br>vue-201810291353... | Federated User<br>cognito-identity.amazonaws.com | - | Write | 5 minutes ago |
| □ | 8761842... | IAM Role<br>test-201810261411... | Federated User<br>cognito-identity.amazonaws.com | - | Write | 5 minutes ago |
| □ | a0fd4d45... | IAM Role<br>AwsSecurityNacun... | AWS Account<br>350429083849 | - | Write | 5 minutes ago |
| □ | c0a8871... | IAM Role<br>GatedGardenAudit | AWS Account<br>628951966944 | - | Write | 5 minutes ago |

Available in Singapore region

# IAM Access Advisor - "I want to control access to my environment, as well as know if somebody external has access to my data."



Filter: No filter ▾ Search | Showing 31 results

| Service Name ⬍ | Policies Granting Permissions | Last Accessed ▾ |
|---|---|---|
| Amazon S3 | SecurityAudit | Today |
| Amazon SQS | SecurityAudit | Today |
| Amazon Redshift | SecurityAudit | Today |
| AWS Key Management Service | SecurityAudit | Today |
| Elastic Load Balancing | SecurityAudit | Today |
| Amazon EC2 | SecurityAudit | Today |
| AWS Identity and Access Management | SecurityAudit | Today |
| Amazon RDS | SecurityAudit | Today |
| AWS CloudFormation | SecurityAudit | Not accessed in the tracking period |
| Amazon SNS | SecurityAudit | Not accessed in the tracking period |
| Amazon SimpleDB | SecurityAudit | Not accessed in the tracking period |

# Detective Controls Best Practices- "I want the ability to automatically detect security mis-configurations and respond in real-time"

1. Enable Cloudtrail in all regions
2. Aggregate all logs from all parts of the stack
3. Now you actually need to review/monitor logs
4. Turn on Cloudwatch Alarms and Events
5. VPC Flow logs
6. Use an SIEM tool (such as AWS Security Hub)
7. Security Operations / Managed SOC
8. Consider a segregated account for logs and security tools only accessible to security teams
9. Enable GuardDuty, Config and Security Hub

# Best of the Best Practices: Logging and Monitoring

1) **Turn on logging** in all accounts, for all services, in all regions

AWS CloudTrail

Amazon GuardDuty

The AWS API history in CloudTrail enables security analysis, resource change tracking, and compliance auditing. GuardDuty provides managed threat intelligence & findings.

2) Use the AWS platform's built-in **monitoring and alerting** features

Security Hub

AWS Config

VPC Flow Logs

Cloud Watch

Monitoring a broad range of sources will ensure that unexpected occurrences are detected. Establish alarms and notifications for anomalous or sensitive account activity.

3) Use a separate AWS account to fetch and **store copies of all logs**

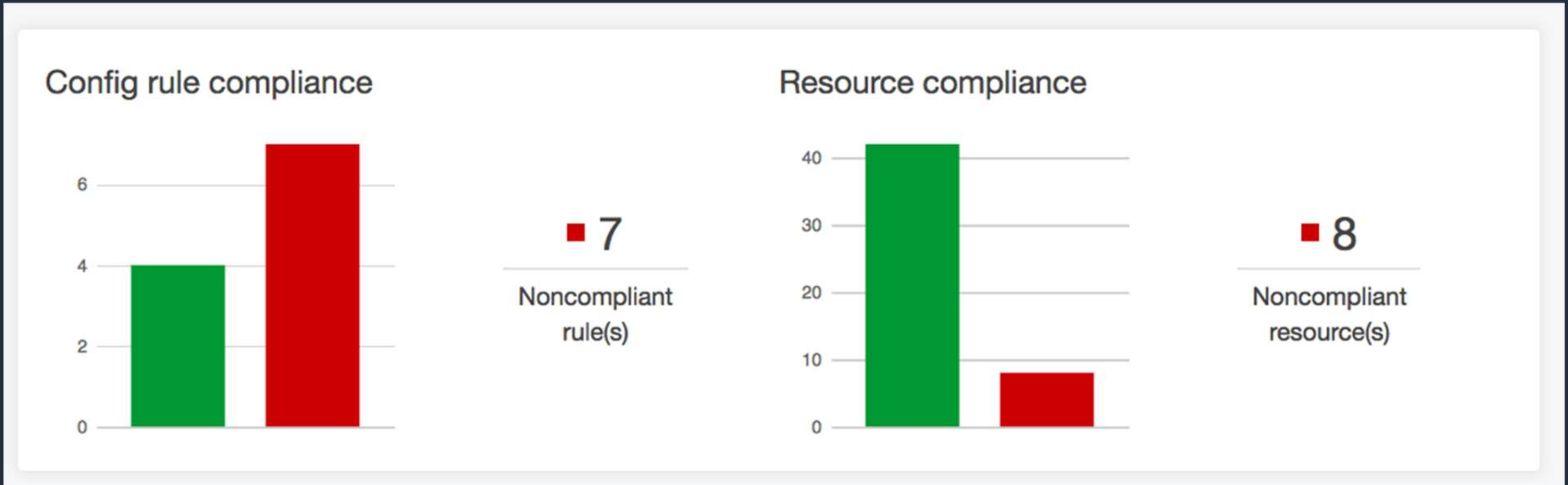
Production

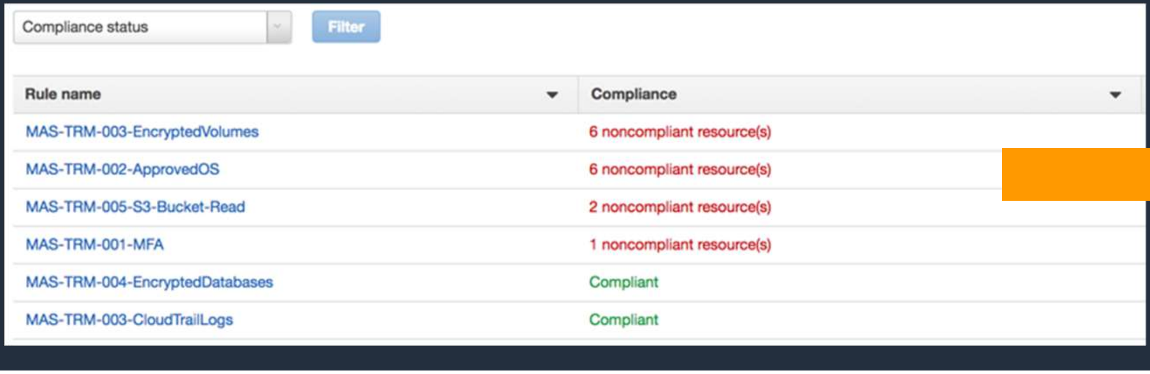
Security

Organisations

Configuring a security account to copy logs to a separate bucket ensures access to information which can be useful in security incident response workflows.

# AWS Config Rules -"I want the ability to automatically detect security mis-configurations and respond in real-time"





| Rule name | Compliance |
|---|---|
| MAS-TRM-003-EncryptedVolumes | 6 noncompliant resource(s) |
| MAS-TRM-002-ApprovedOS | 6 noncompliant resource(s) |
| MAS-TRM-005-S3-Bucket-Read | 2 noncompliant resource(s) |
| MAS-TRM-001-MFA | 1 noncompliant resource(s) |
| MAS-TRM-004-EncryptedDatabases | Compliant |
| MAS-TRM-003-CloudTrailLogs | Compliant |

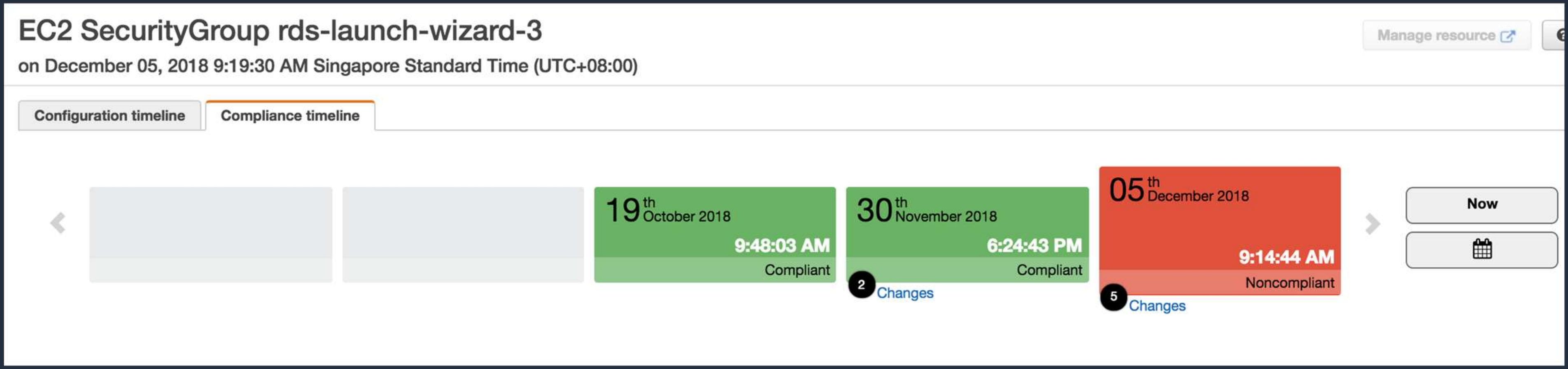
Automatic email to security teams when controls fail in real-time

Execute automatic remediation based on desired security outcome

# AWS Config Rules

| Compliance guideline | Action if non-compliance |
|---|---|
| All EBS volumes should be encrypted | Encrypt volumes and alert operations team |
| Instances must be from a specific approved AMI | Terminate instance and notify build team |
| Instances must be tagged with environment type | Flag as non-compliant but take no further action |

# Compliance Timeline – Deep Insight for Audit



EC2 SecurityGroup rds-launch-wizard-3

on December 05, 2018 9:19:30 AM Singapore Standard Time (UTC+08:00)

AWS Config allows you to record and retrieve the compliance status of a resource over time. This allows your risk and compliance teams to determine if a resource always has been compliant or has drifted in and out of compliance with on-going changes.

# Infrastructure Security Best Practices - “I want to protect against cyber attacks, DDoS attacks and application layer exploits”

1. Implement tight security groups (nothing to 0.0.0.0/0!!)
2. Environment (prod/dev) segregation (account versus VPC )
3. Web application firewall (GeoBlock, SQL injection, XSS)
4. Use a Bastion host OR AWS Systems Manager Session Manager (preferred option)
5. DDoS Resilient Architecture
6. IPS/IDS – e.g. Palo Alto
7. Host based agents (Trend Micro, vulnerability detection, malware)
8. Penetration Testing / Continuous VA
9. AMI Patching – If building your AMI use ec2 Image Builder

# Best of the Best Practices: Infrastructure Security

## 1) Create a **threat prevention layer** using AWS edge services

Amazon CloudFront

AWS Shield

AWS WAF

Use the 100s of worldwide points of presence in the AWS edge network to provide scalability, protect from denial of service attacks, and protect from web application attacks.

## 2) Create **network zones** with Virtual Private Clouds (VPCs) and security groups

VPC

Security Group

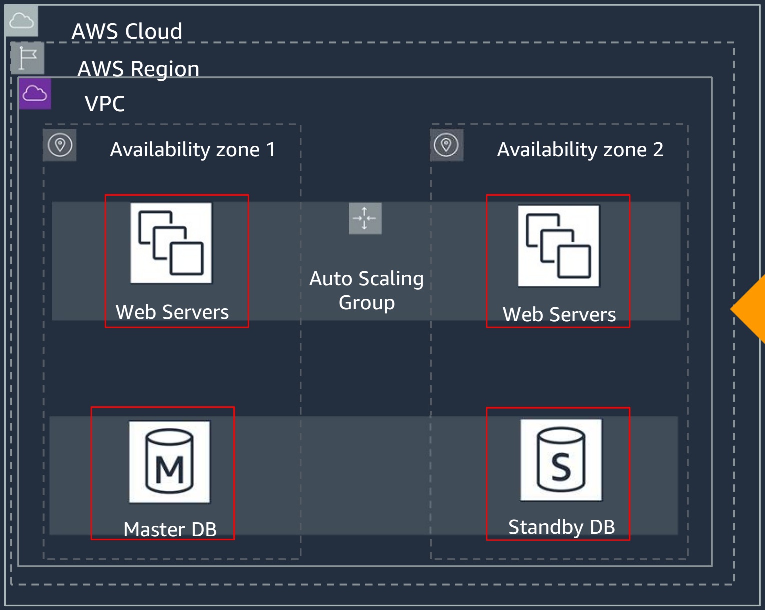
Implement security controls at the boundaries of hosts and virtual networks within the cloud environment to enforce access policy.

## 3) Manage vulnerabilities through **patching and scanning**

Systems Manager

AWS Systems Manager Patch Manager automates the process of patching managed instances with both security related and other types of updates.

# Network Security – “I want to protect against cyber attacks, DDoS attacks and application layer exploits”



AWS PrivateLink

Traffic Mirroring

AWS Direct Connect

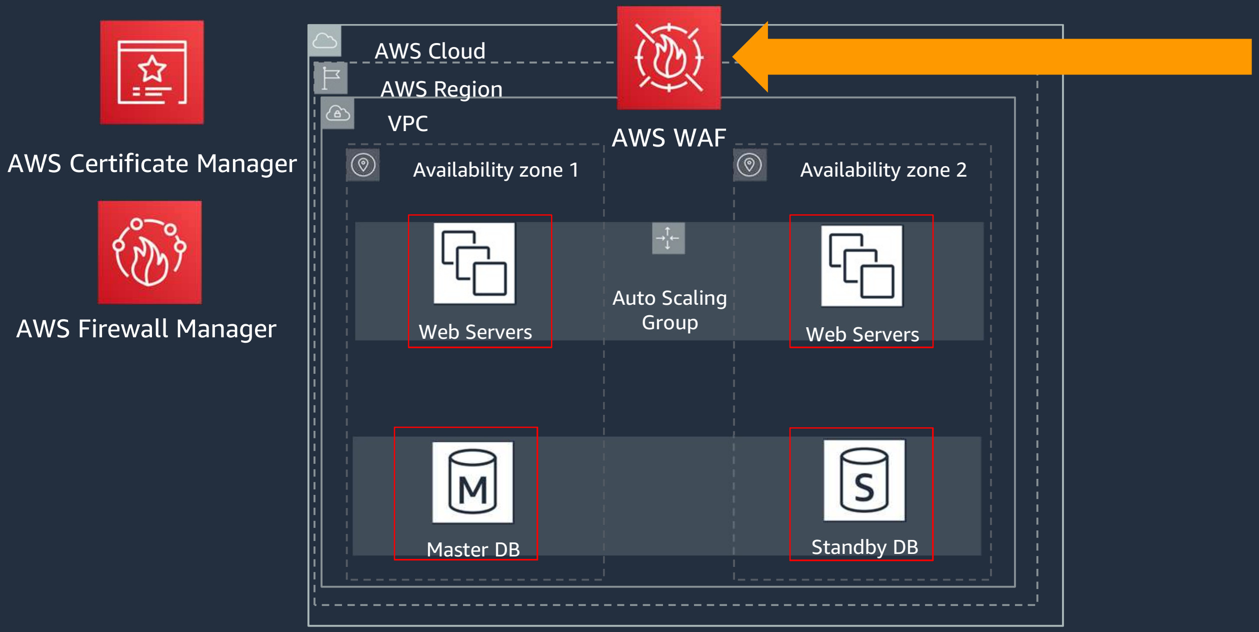
Security Groups are stateful host based firewalls that run on every single host inside your network. You can enforce encryption by ensuring only SSL / HTTPS connections via security groups

AWS Certificate Manager

Application Load Balancer

Amazon CloudFront

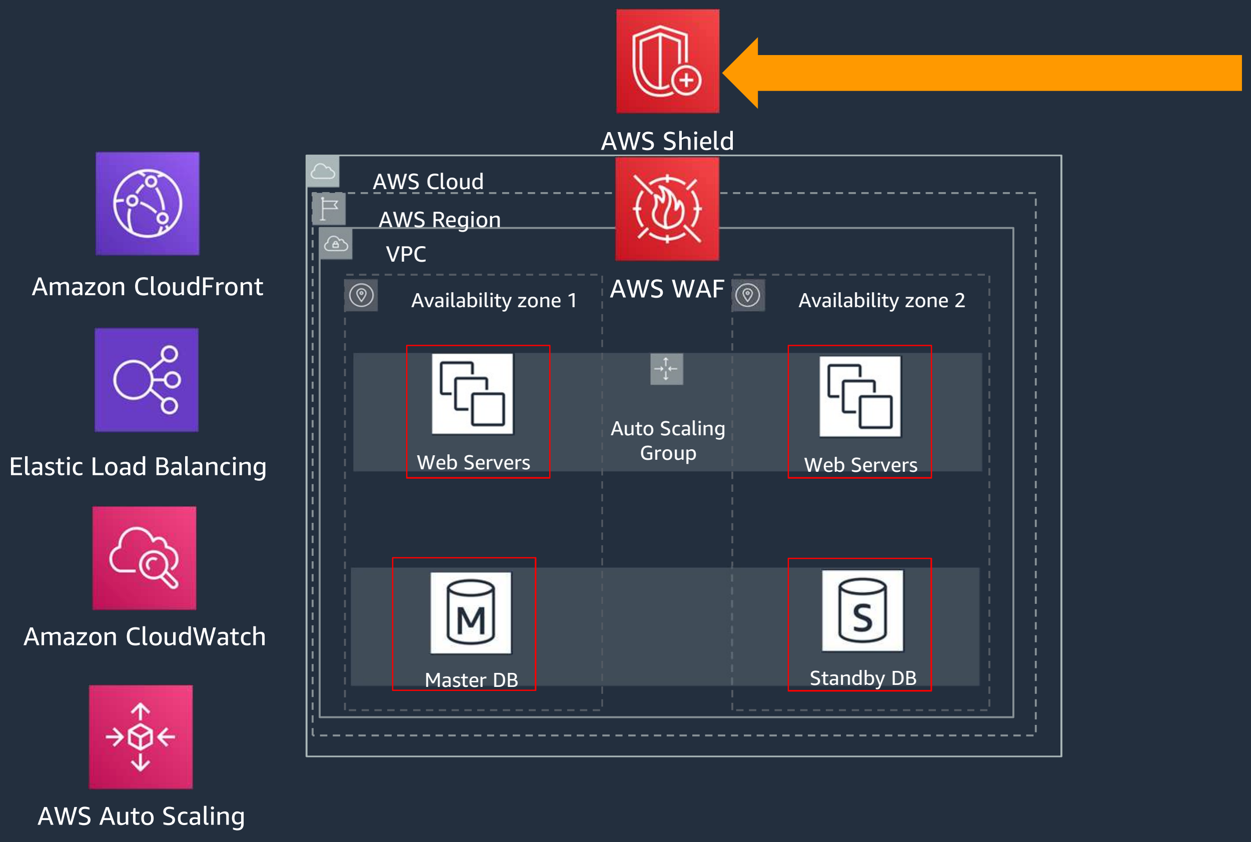
# Web Application Firewall - “I want to protect against cyber attacks, DDoS attacks and application layer exploits”



AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

SQL Injection
Cross-Site Scripting
Brute forcing
Etc…

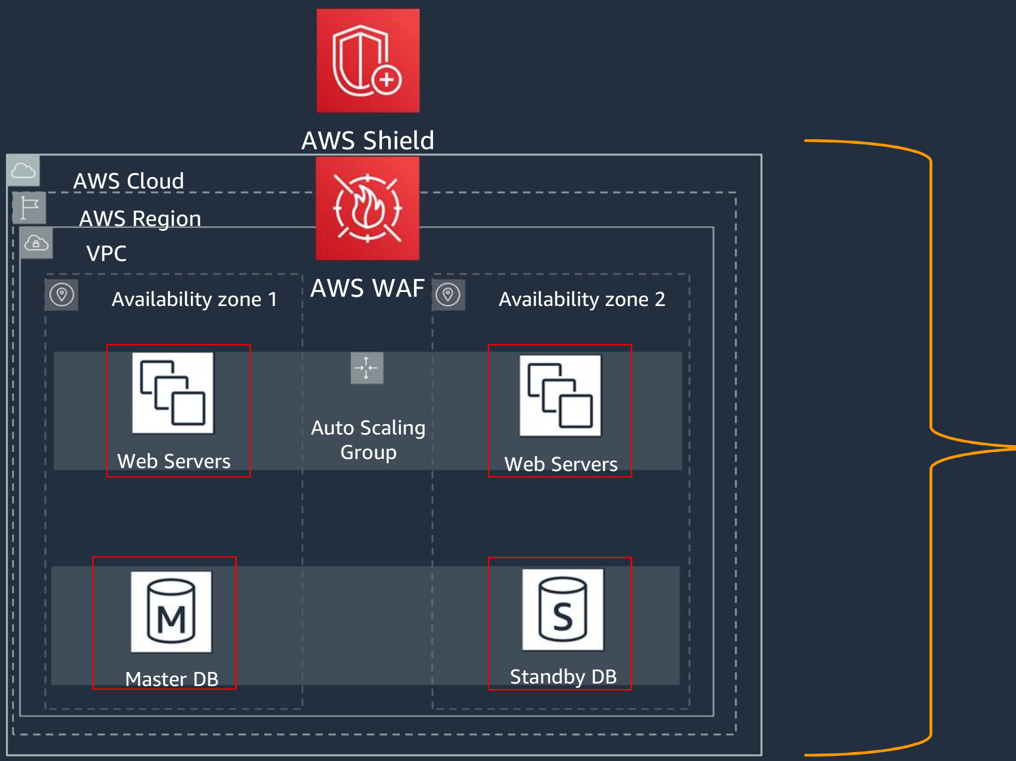
# DDoS Protection - "I want to protect against cyber attacks, DDoS attacks and application layer exploits"

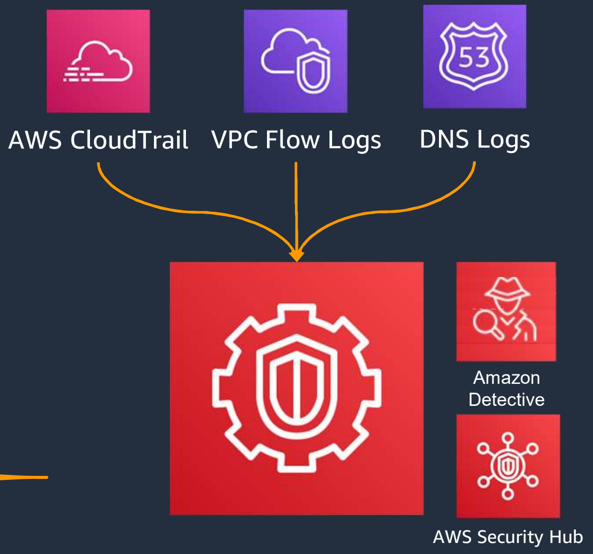


AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS.

AWS Shield defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications.

# Cyber Threat "I want to protect against cyber attacks, DDoS attacks and application layer exploits"





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

# Data Protection Best Practices “I want to encrypt all my data using strong encryption. I also want to have control over the key.”

1. Encryption in transit (ACM, TLS, ELB)
2. Encryption at rest (KMS, S3, RDS), Application layer encryption
3. Instance termination protection (EC2)
4. Backup / snapshots (EBS, RDS, Data, S3, Logs)
5. Do not expose data stores to the internet (S3, RDS, DynamoDB etc.)

# Best of the Best Practices: Data Protection

1) Encrypt **data at rest (**with occasional exceptions)

AWS KMS

Amazon S3

Enabling encryption at rest helps ensure the confidentiality and integrity of data. Consider encrypting everything that is not public.

2) Use **server-side encryption** with provider managed keys

AWS KMS

Data Encryption Key

AWS Key Management Service (KMS) is seamlessly integrated with 18 other AWS services. You can use a default master key or select a custom master key, both managed by AWS.

3) Encrypt **data in transit** (with no exceptions)

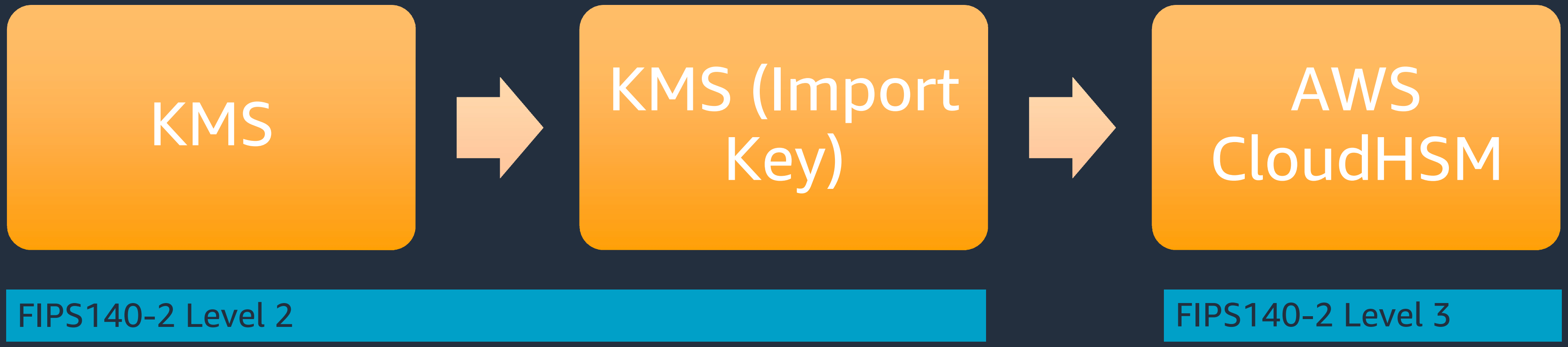
Amazon CloudFront

ACM

SSL / TLS / HTTPS

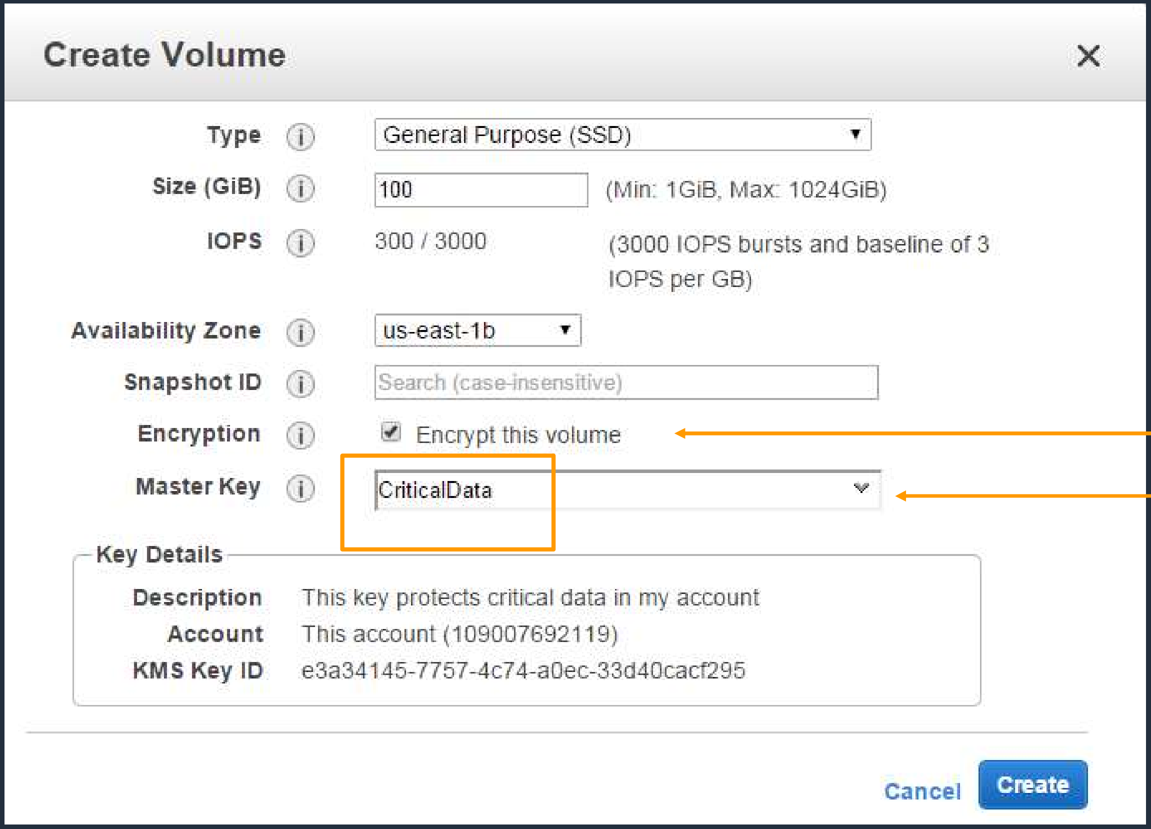
Encryption of data in transit provides protection from accidental disclosure, verifies the integrity of the data, and can be used to validate the remote connection.

# Data Protection – Encryption “I want to encrypt all my data using strong encryption. I also want to have control over the key.”



The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.

# AWS KMS Usage - Encryption “I want to encrypt all my data using strong encryption. I also want to have control over the key.”



Create Volume

| | |
|---|---|
| Type | General Purpose (SSD) |
| Size (GiB) | 100 (Min: 1GiB, Max: 1024GiB) |
| IOPS | 300 / 3000 (3000 IOPS bursts and baseline of 3 IOPS per GB) |
| Availability Zone | us-east-1b |
| Snapshot ID | Search (case-insensitive) |
| Encryption | ☑ Encrypt this volume |
| Master Key | CriticalData |

Key Details

| | |
|---|---|
| Description | This key protects critical data in my account |
| Account | This account (109007692119) |
| KMS Key ID | e3a34145-7757-4c74-a0ec-33d40cacf295 |

Key Admin

Key User

Single click, AES256 symmetric encryption

Protect data using a customer master key fully under the control of the AWS customer. Segregation of duties allow customers to have ‘key administrators’ and ‘key users’ that specifies who can use the key on a given data set.

# Incident Response

1. Enable Logging (Cloudtrail, Alarm, Events, Notifications to admins)
2. Monitor SOC for potential compromises
3. Playbooks / runbooks
4. Forensic capability
5. Automated recovery

# Next Steps: Path to Production

1. Identify & Engage Stakeholders

2. Capability & Enablement

3. Operational Model

4. Security of the Cloud

**5. Security in the Cloud**

6. FSI Regulations

7. Legal Agreements

8. Establish Security Controls (Prevent, Detect, Respond, Recover)

9. Internal & External Assessment

10. Regulator Approval or Notification

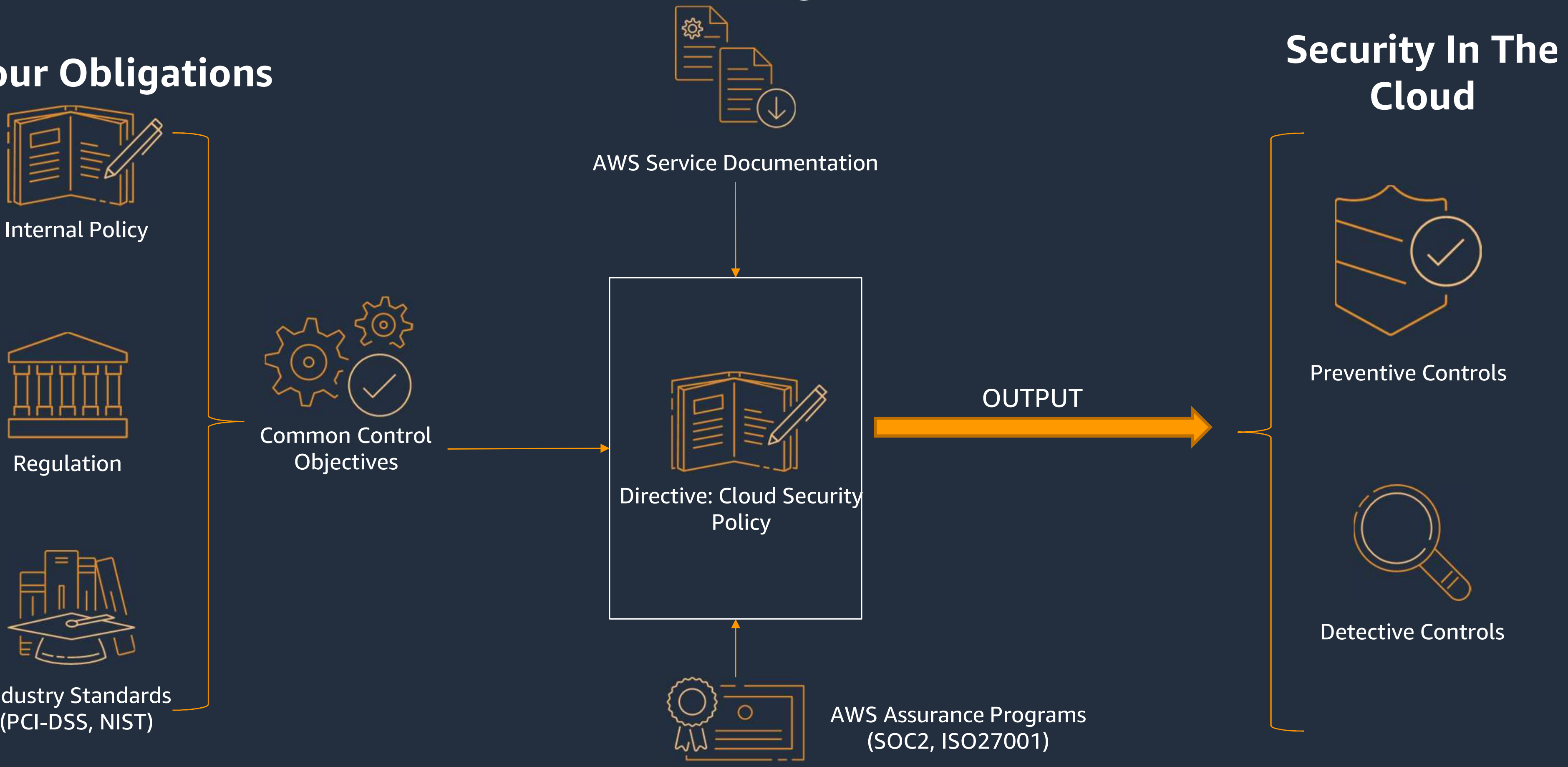
# Next Steps: Cloud Security Policy

Create a AWS usage policy Leverage existing where possible, create new ones where required

Communicate policy with AWS users and development teams that will be using AWS.

Aim for a high degree of automation for implementing policy

# Next Steps: Establish Security Controls



## Your Obligations

Internal Policy

Regulation

Industry Standards (PCI-DSS, NIST)

Common Control Objectives

AWS Service Documentation

Directive: Cloud Security Policy

AWS Assurance Programs (SOC2, ISO27001)

OUTPUT

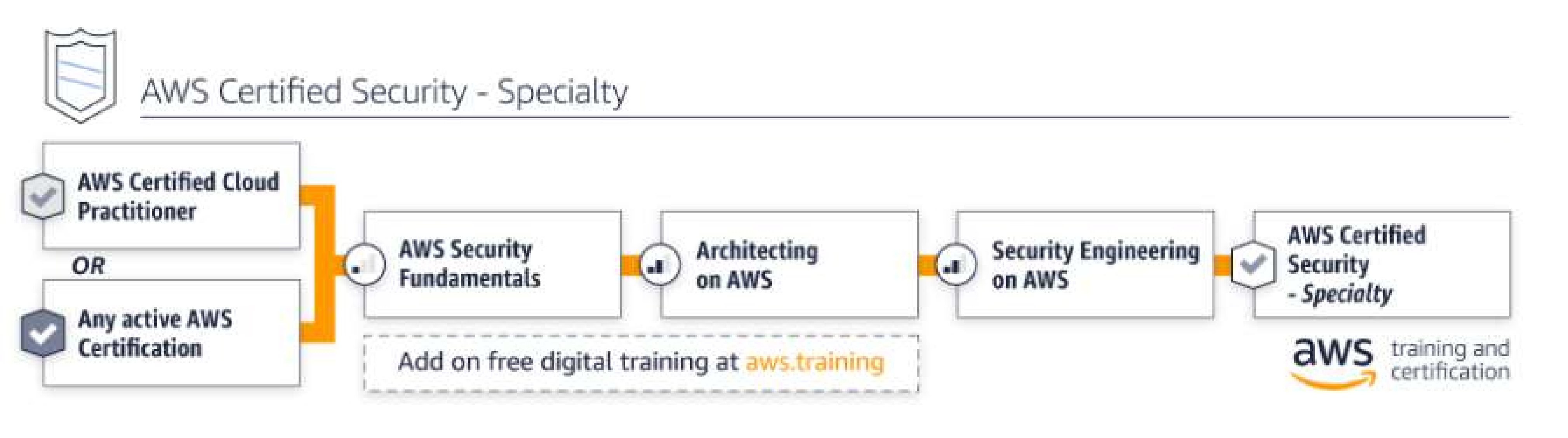
## Security In The Cloud

Preventive Controls

Detective Controls

# Next Steps

## Educate:
AWS Security Curriculum



AWS Certified Security - Specialty

AWS Certified Cloud Practitioner

OR

Any active AWS Certification

AWS Security Fundamentals

Architecting on AWS

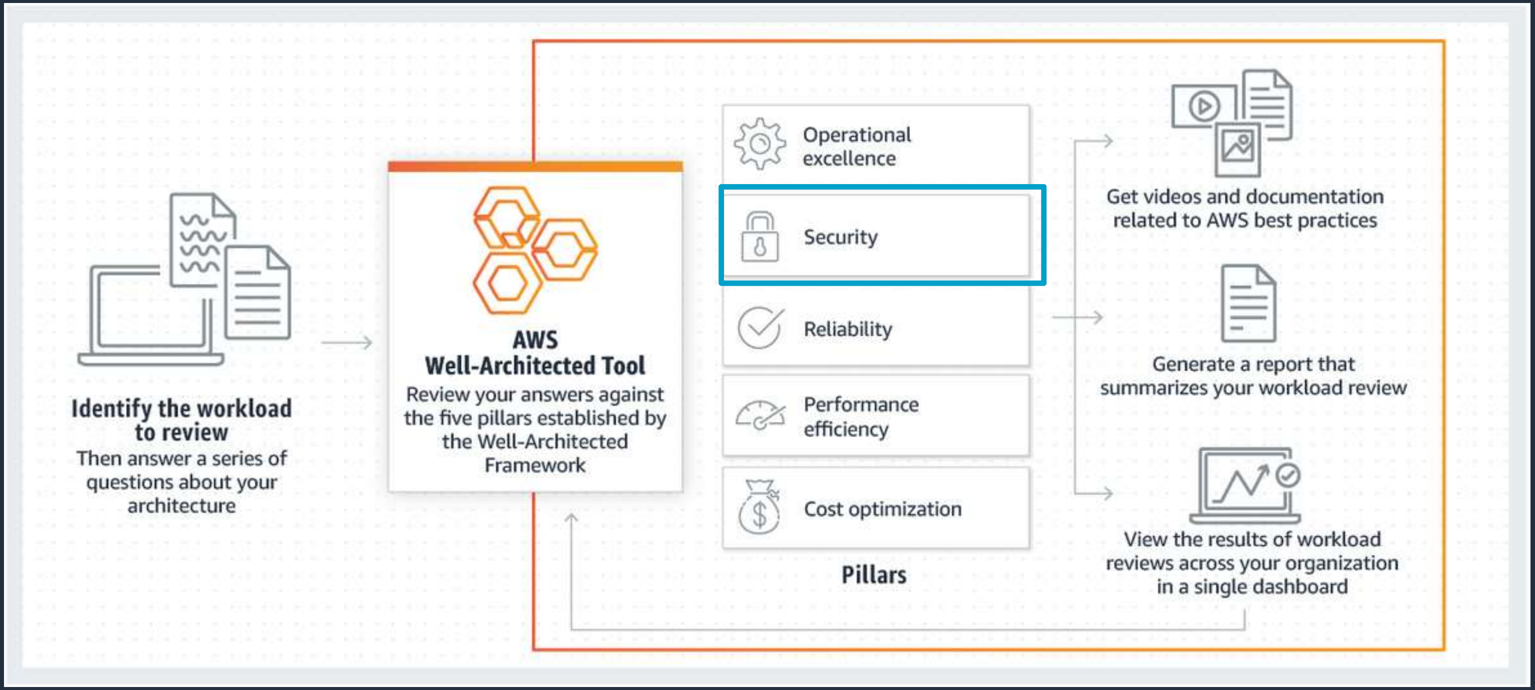
Security Engineering on AWS

AWS Certified Security - *Specialty*

Add on free digital training at aws.training

# Next Steps

## Assess:
## AWS Well Architected



**Identify the workload to review**
Then answer a series of questions about your architecture

**AWS Well-Architected Tool**
Review your answers against the five pillars established by the Well-Architected Framework

**Pillars**

- Operational excellence
- Security
- Reliability
- Performance efficiency
- Cost optimization

Get videos and documentation related to AWS best practices

Generate a report that summarizes your workload review

View the results of workload reviews across your organization in a single dashboard

# Builders Session – Identify vulnerabilities and fix them

# Hints

1. Has the principle of least privilege been applied?
2. Secure your data stores (all of them!)
3. Think about what should and should NOT be exposed to the public
4. How many services do we have for monitoring and logging?

# Bit.ly/aws-bkk-survey

# Thank You