# urity Immersion Day

npur 2020

aga-Cardenas

ions Architect

n.com

ow

curity Solutions Architect

mazon.com

# a

0 AWS Security Services

0 Essential Security Patterns and Security Best Practices

0 Break

0 Builders session Part 1: Identify vulnerabilities and fix them / AWS L

0 Lunch

0 Builders session Part 2: Analysing CloudTrail logs using Serverless

0 Break

0 Security FAQ

# Challenge

ands-on for security services:

/ Workshop

aws-sec-workshop

## g adventurous?

Challenge

aws-sec-challenge

e 10 security mistakes and if you are the fasters one, win some awes

# non Security Questions

## teams often ask the following questions:

- Do I have adequate security to protect my workloads and d
- 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?

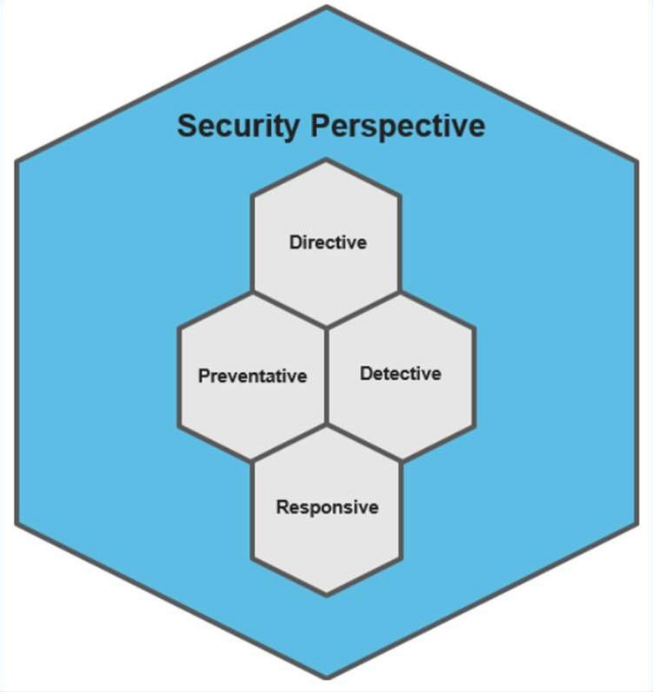
# ecurity ctive

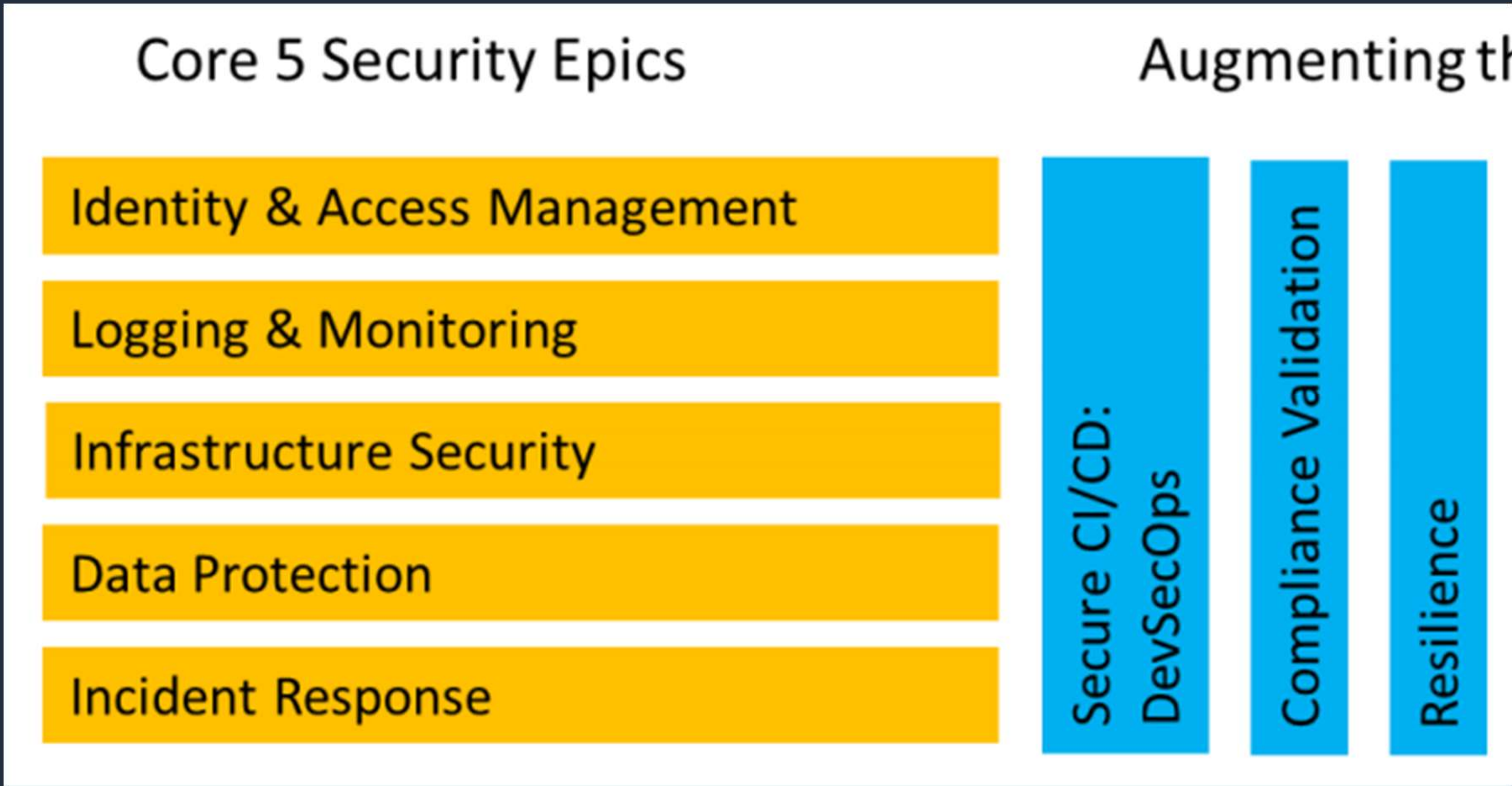
rols establish the sk, and odels the vill operate

ntrols protect s and mitigate lnerabilities.

trols provide full ransparency over of your n AWS.

ntrols drive f potential m your security





Core 5 Security Epics

Augmenting th

Identity & Access Management

Logging & Monitoring

Infrastructure Security

Data Protection

Incident Response

Secure CI/CD: DevSecOps

Compliance Validation

Resilience

# l responsibility model

Customer
AWS

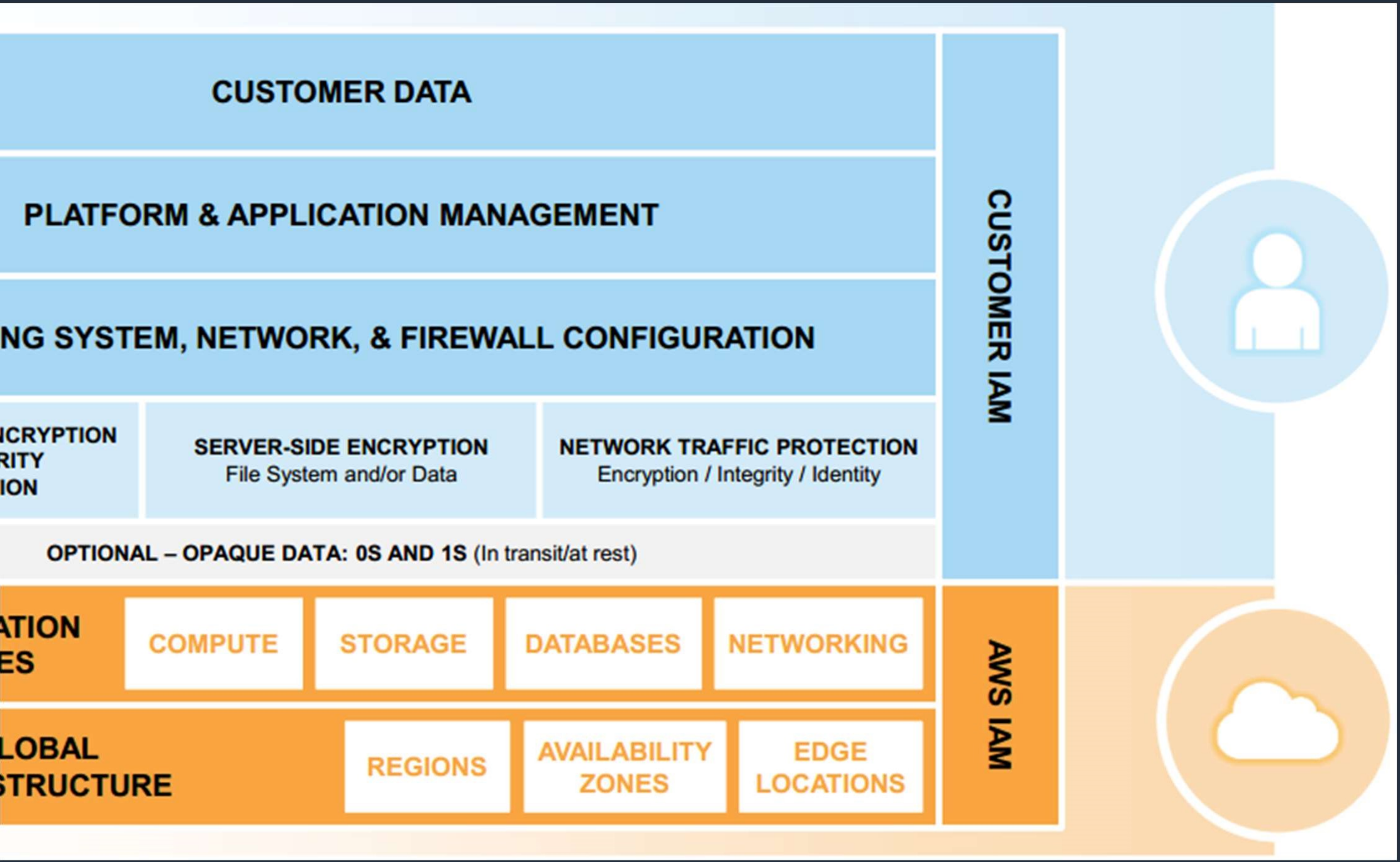
**Security IN the Cloud**

Customer responsibility v
determined by the AWS
services that a customer

**Security OF the Cloud**

AWS is responsible for pr
infrastructure that runs a
services offered in the AV

# ucture Services – e.g. EC2



CUSTOMER DATA

PLATFORM & APPLICATION MANAGEMENT

NG SYSTEM, NETWORK, & FIREWALL CONFIGURATION

CRYPTION
RITY
ION

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

ATION
ES

COMPUTE

STORAGE

DATABASES

NETWORKING

LOBAL
STRUCTURE

REGIONS

AVAILABILITY
ZONES

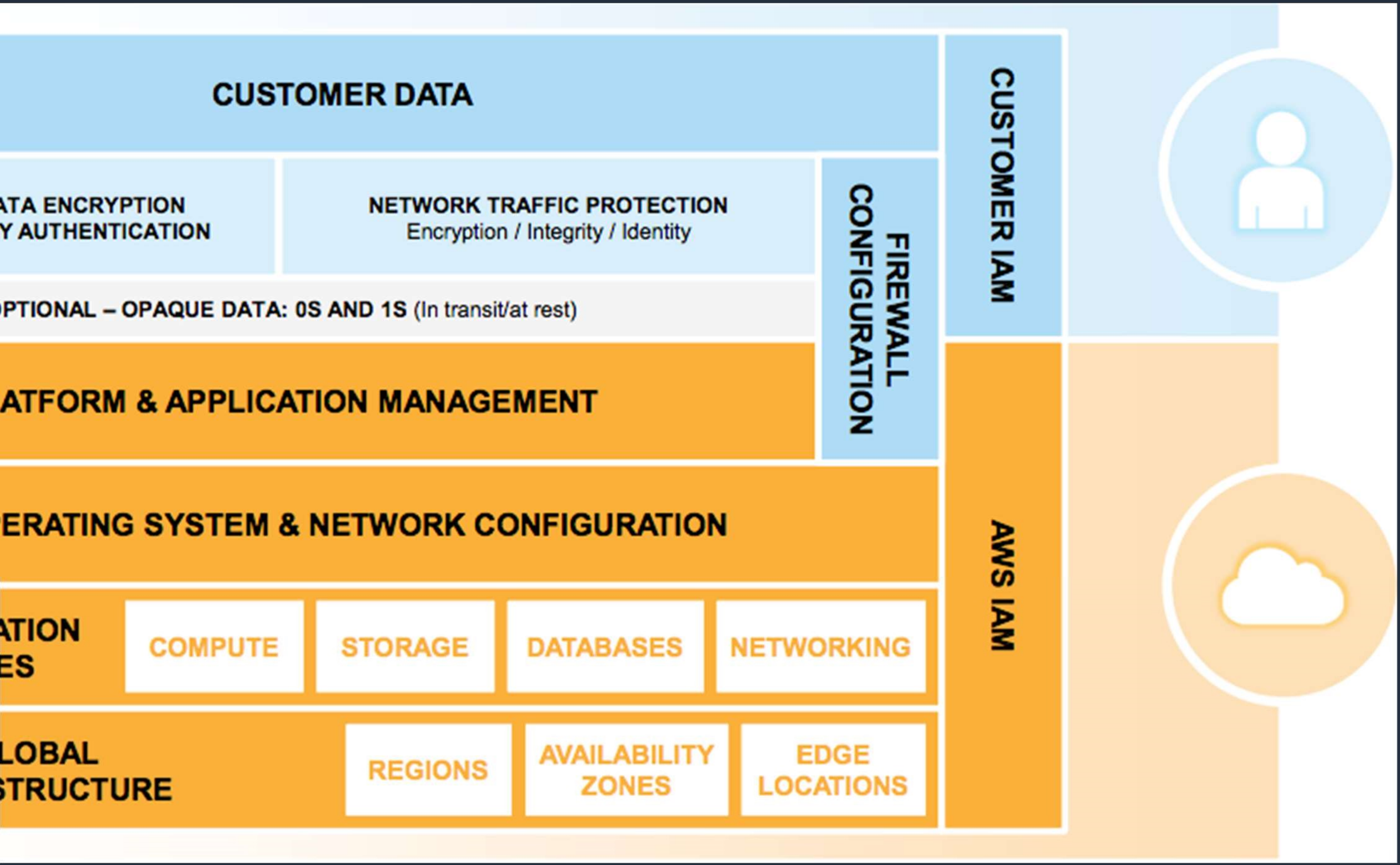
EDGE
LOCATIONS

AWS IAM

Mar
Cus

Mar
Ama
Serv

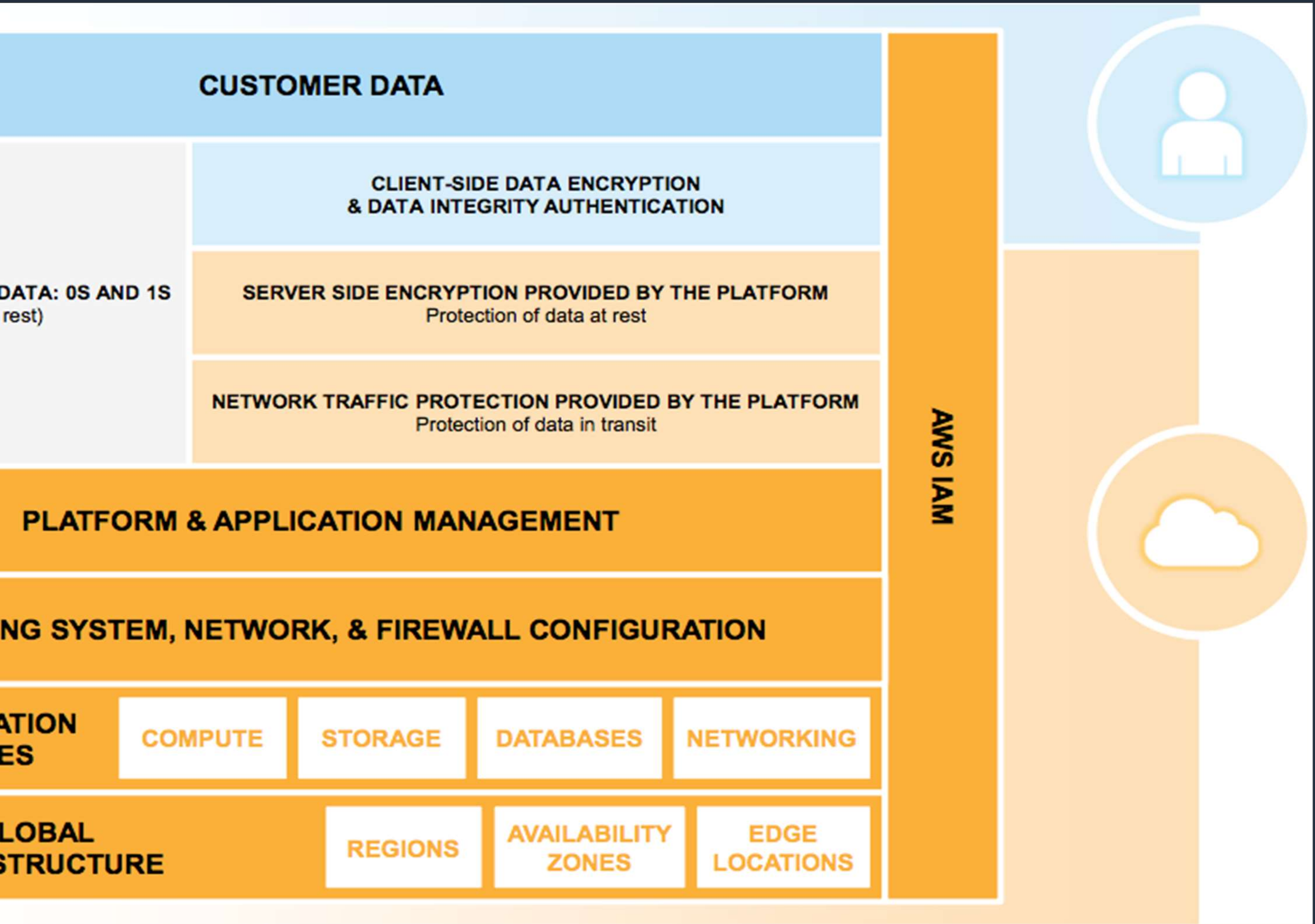
# ner Services – e.g. RDS


CUSTOMER DATA
ATA ENCRYPTION
Y AUTHENTICATION
NETWORK TRAFFIC PROTECTION
Encryption / Integrity / Identity
PTIONAL – OPAQUE DATA: 0S AND 1S (In transit/at rest)
FIREWALL CONFIGURATION
CUSTOMER IAM
ATFORM & APPLICATION MANAGEMENT
ERATING SYSTEM & NETWORK CONFIGURATION
ATION
ES
COMPUTE
STORAGE
DATABASES
NETWORKING
LOBAL
STRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS
AWS IAM

Mar
Cust

Mar
Ama
Serv

# cted Services - e.g. S3



CUSTOMER DATA

CLIENT-SIDE DATA ENCRYPTION
& DATA INTEGRITY AUTHENTICATION

DATA: 0S AND 1S
rest)

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

NG SYSTEM, NETWORK, & FIREWALL CONFIGURATION

ATION
ES

COMPUTE

STORAGE

DATABASES

NETWORKING

LOBAL
STRUCTURE

REGIONS

AVAILABILITY
ZONES

EDGE
LOCATIONS

AWS IAM

Mar
Cus

Mar
Ama
Serv

# ngs you have to configure on AWS

our customer data and applications with

uration of access controls
uring encryption
ation monitoring
on detection/prevention
os
er Recovery

# ecurity solutions

## access ment

- Access (IAM)
- ign-On
- Service
- gnito
- ations
- lanager
- Access r

## 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)

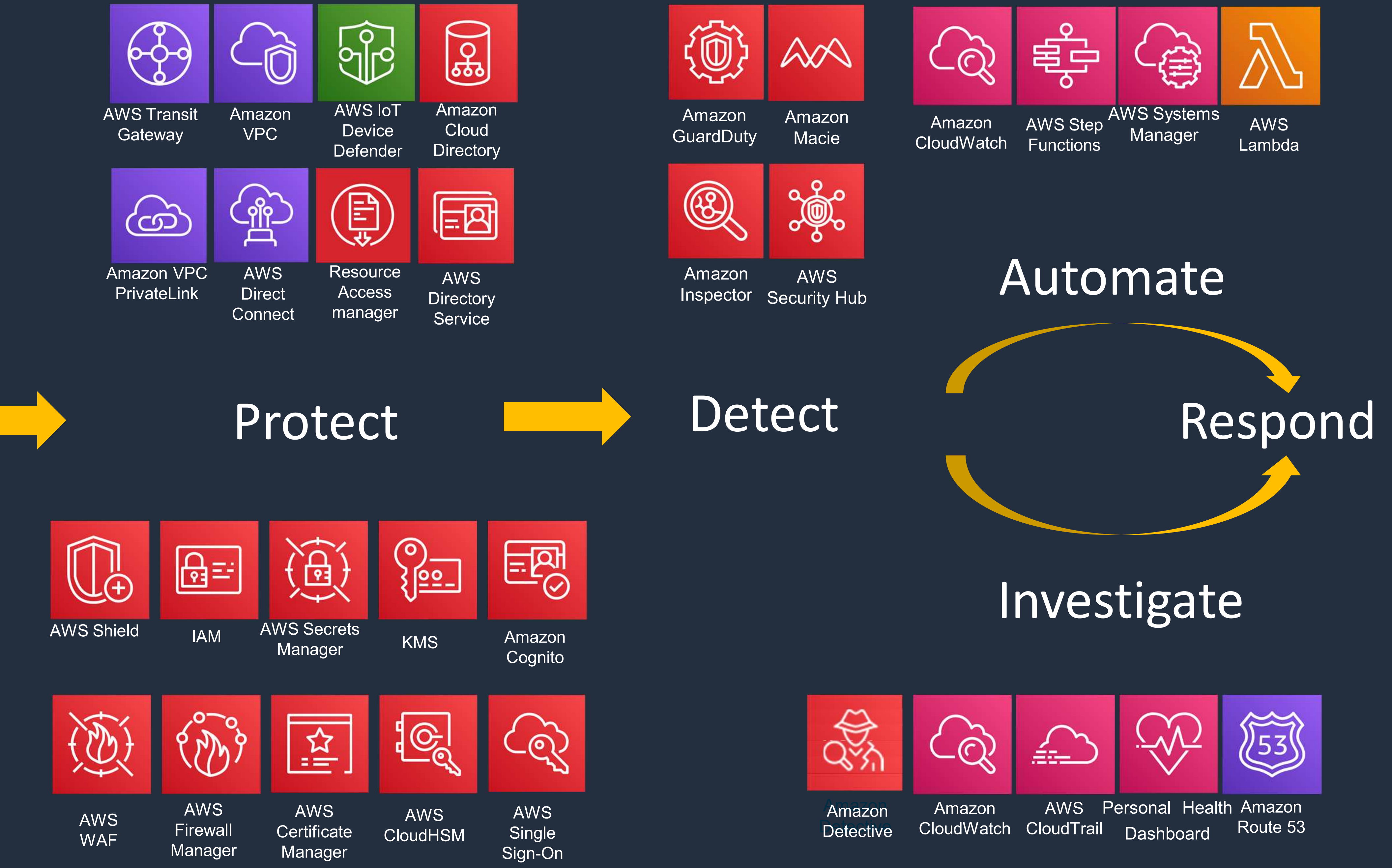
## Data protection

- AWS Key Management Service (KMS)
- AWS CloudHSM
- AWS Certificate Manager
- Amazon Macie
- Server-Side Encryption

## I r

- AW
- A

# onal and Layered Services against NIST CSF



Protect

AWS Transit Gateway

Amazon VPC

AWS IoT Device Defender

Amazon Cloud Directory

Amazon VPC PrivateLink

AWS Direct Connect

Resource Access manager

AWS Directory Service

AWS Shield

IAM

AWS Secrets Manager

KMS

Amazon Cognito

AWS WAF

AWS Firewall Manager

AWS Certificate Manager

AWS CloudHSM

AWS Single Sign-On

Detect

Amazon GuardDuty

Amazon Macie

Amazon Inspector

AWS Security Hub

Automate

Amazon CloudWatch

AWS Step Functions

AWS Systems Manager

AWS Lambda

Respond

Investigate

Amazon Detective

Amazon CloudWatch

AWS CloudTrail

Personal Health Dashboard

Amazon Route 53

# chitected Security Pillar – Design Principles

nent a strong identity foundation

traceability

security at all layers

ate security best practices

t data in transit and at rest

people away from data

e for security events

# y considerations

Secure application

Secure nvironment

Separation of duties

Monito

# environment – Bare Minimum

Enable MFA

Don’t use root

derate Identity

Least privilege

Disable public bu

# y considerations

Secure application

Secure nvironment

Separation of duties

Monito

# urity Best Practices

# en Security Requirements and Use Cases

o ensure my environment can support multiple applications and compromising on security.

o control access to my environment, as well as know if somebo has access to my data.

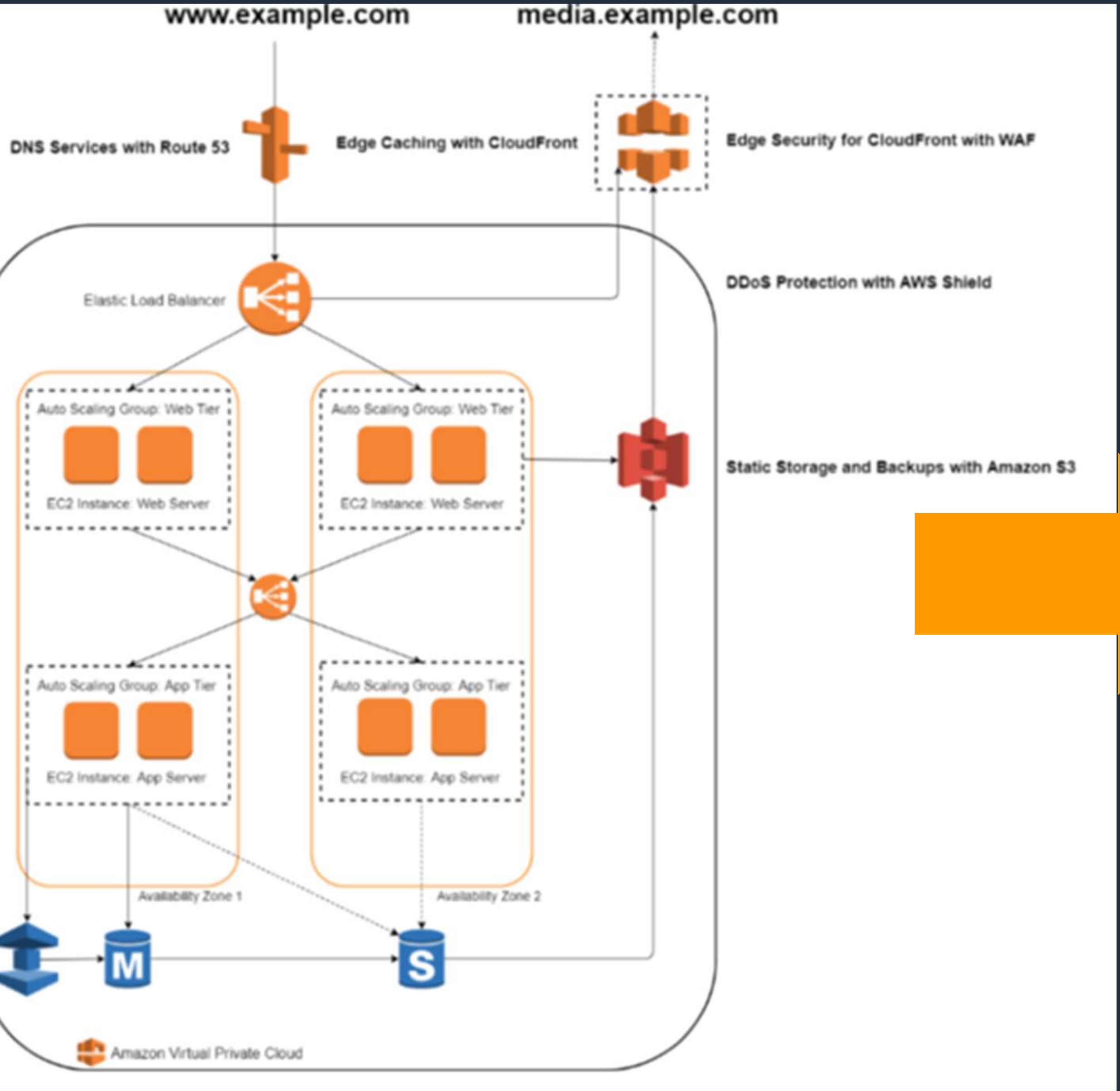
o protect against cyber attacks, DDoS attacks and application l .

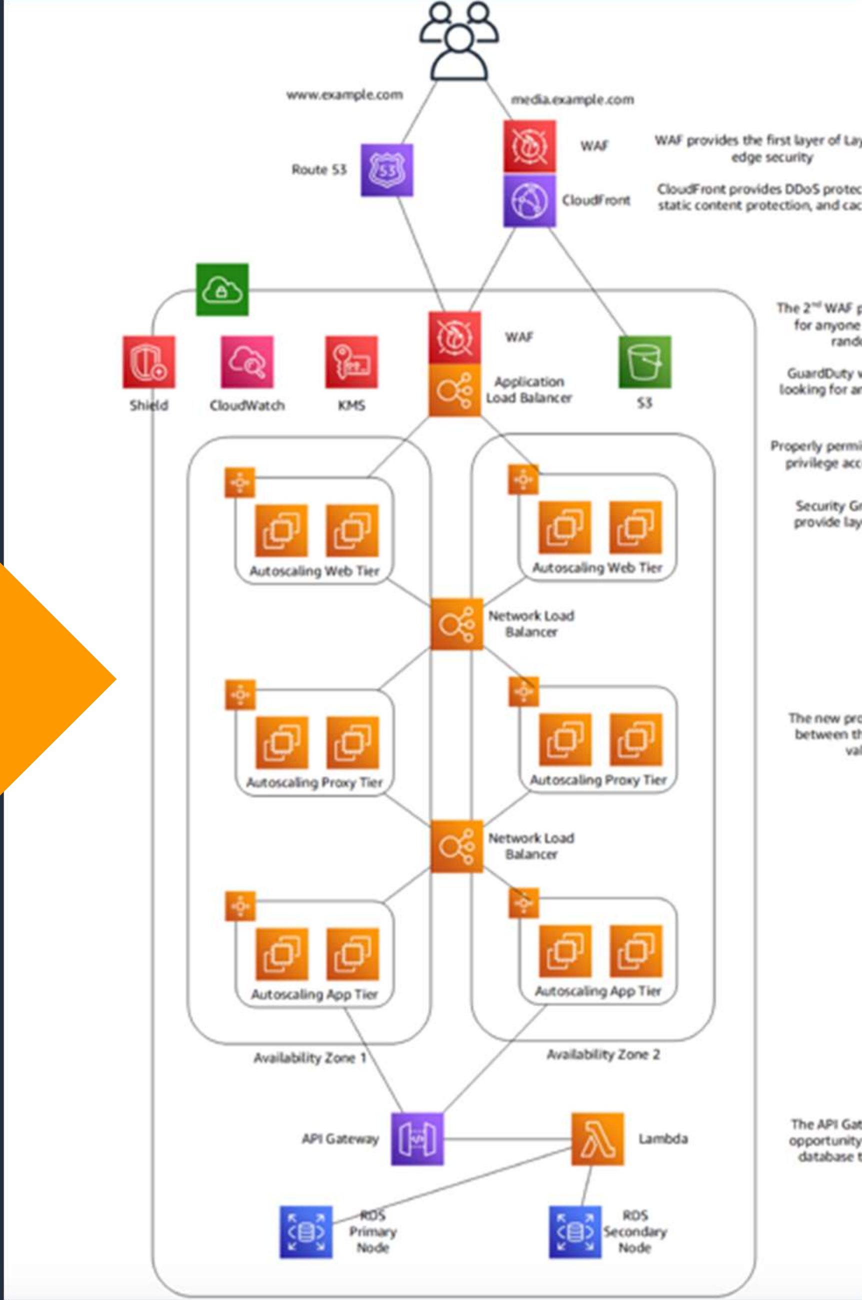
o encrypt all my data using strong encryption. I also want to ha key.

he ability to automatically detect security mis-configurations an me.

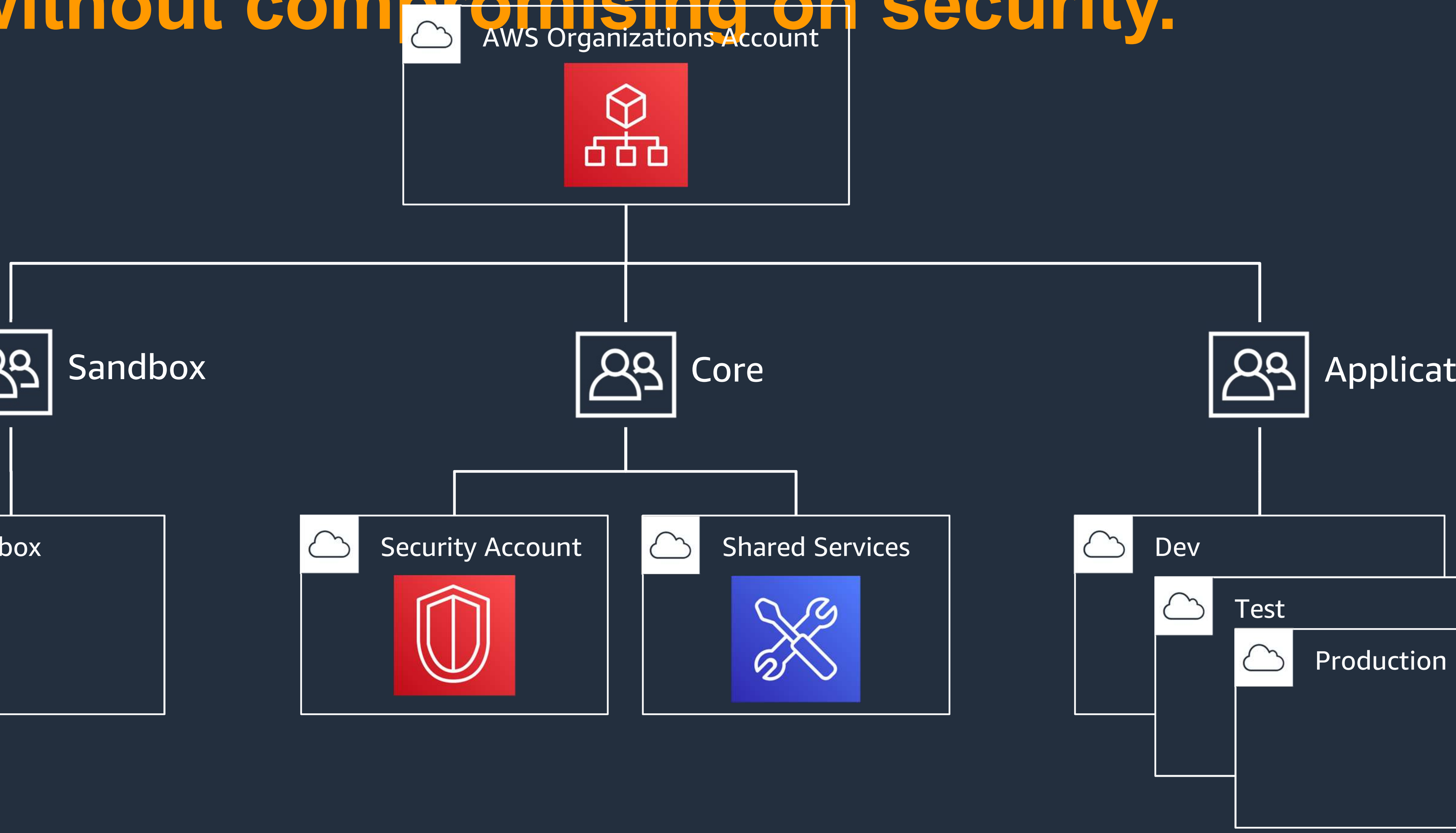
o be able to enforce guardrails in all my AWS accounts to ensu ees only do what I allow them to do.

# ust Reference Architecture


www.example.com
media.example.com
DNS Services with Route 53
Edge Caching with CloudFront
Edge Security for CloudFront with WAF
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
Static Storage and Backups with Amazon S3
Auto Scaling Group: App Tier
EC2 Instance: App Server
Auto Scaling Group: App Tier
EC2 Instance: App Server
Availability Zone 1
Availability Zone 2
M
S
Amazon Virtual Private Cloud



# ccount Strategy - “I want to ensure my ment can support multiple applications an vithout compromising on security.”



# no – Service Control Policy
# AWS Organisations

# M Best Practices - “I want to control access to my ment, as well as know if somebody external has a ”

**s** – Create individual users.

**nissions** – Grant least privilege.

**ps** – Manage permissions with groups.

**ting** – Enable AWS CloudTrail

**word** – Configure a strong password policy.

**te** – Rotate security credentials regularly.

– Enable MFA for all users.

**s and Attributes** – Use IAM roles for Amazon EC2 nces.

– Reduce or remove use of root.

# ng Credentials and Authentication with AWS

ividual users

AM

vidual users
auditability of

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 CloudTra**

**CloudTrail**

Enabling CloudTrai
to monitor and log
your AWS environn

Practice log diving
so that in the event
compromise you ar
investigate and res
quickly.

# ng Credentials and Authentication with AWS

**ple AWS**
reduce blast

Staging

ts provide
e isolation
rkloads across
s of business,
jes of
nd types of data
.

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 e
identity service

IAM

MFA token

AW

Control access to A
resources, and ma
authentication and
authorisation proce
without needing to
all your corporate u
IAM users.

# Continued

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

# entity Authentication - "I want to control access t ment, as well as know if somebody external ha to my data."

## Management Console

n **Username/Password** with **MFA** (recommended)

ted access: **a Signed URL in Amazon can** provide temporary access to the

## API access

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

**ACCESS KEY ID**

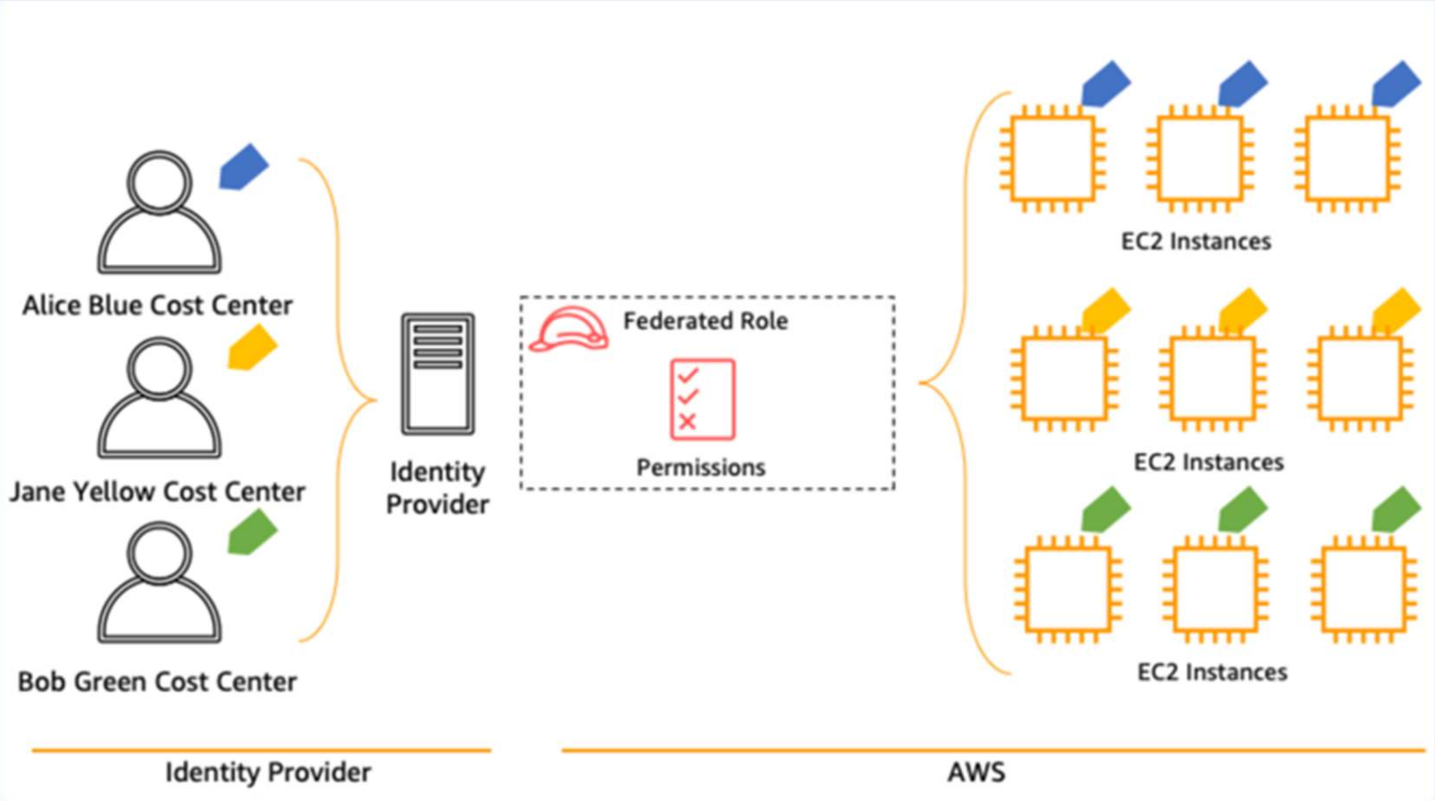
Ex: `AKIAIOSFODNN7EXAMPLE`

**SECRET KEY**

Ex: `UtnFEMI/K7MDENG/bPxRfiCYEX`

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

# te Based Access Control (ABAC) - "I want to access to my environment, as well as know if ody external has access to my data."



ws.amazon.com/IAM/latest/UserGuide/tutorial_attribute-based-access-c

# ccess Analyzer - “I want to control access to m nment, as well as know if somebody external ha to my data.”

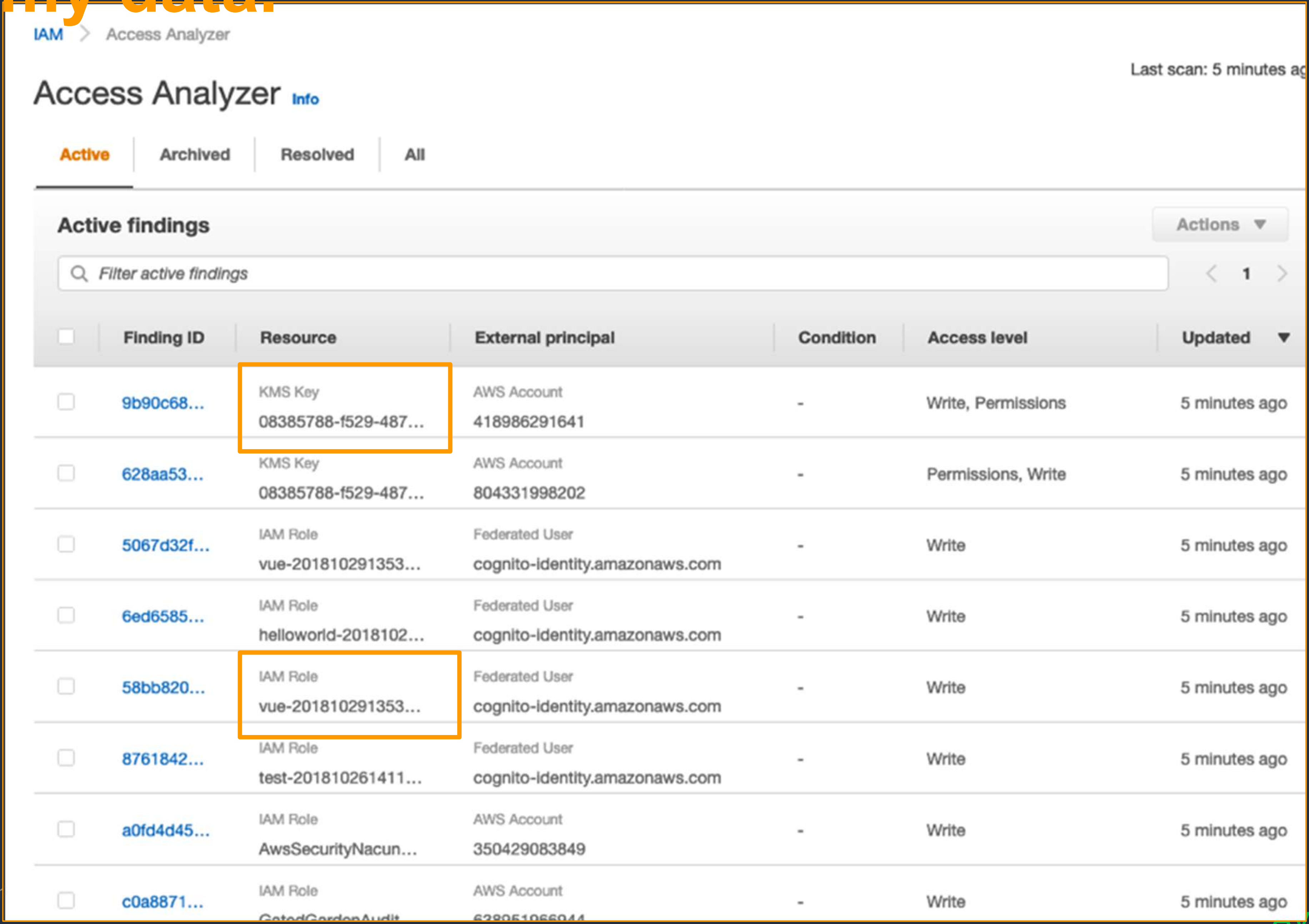
lentity and
Management
s Analyzer

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

**Useful for vendor management.**

Available

# ccess Analyzer - “I want to control access to m nment, as well as know if somebody external ha to my data.”



IAM > Access Analyzer

Last scan: 5 minutes ag

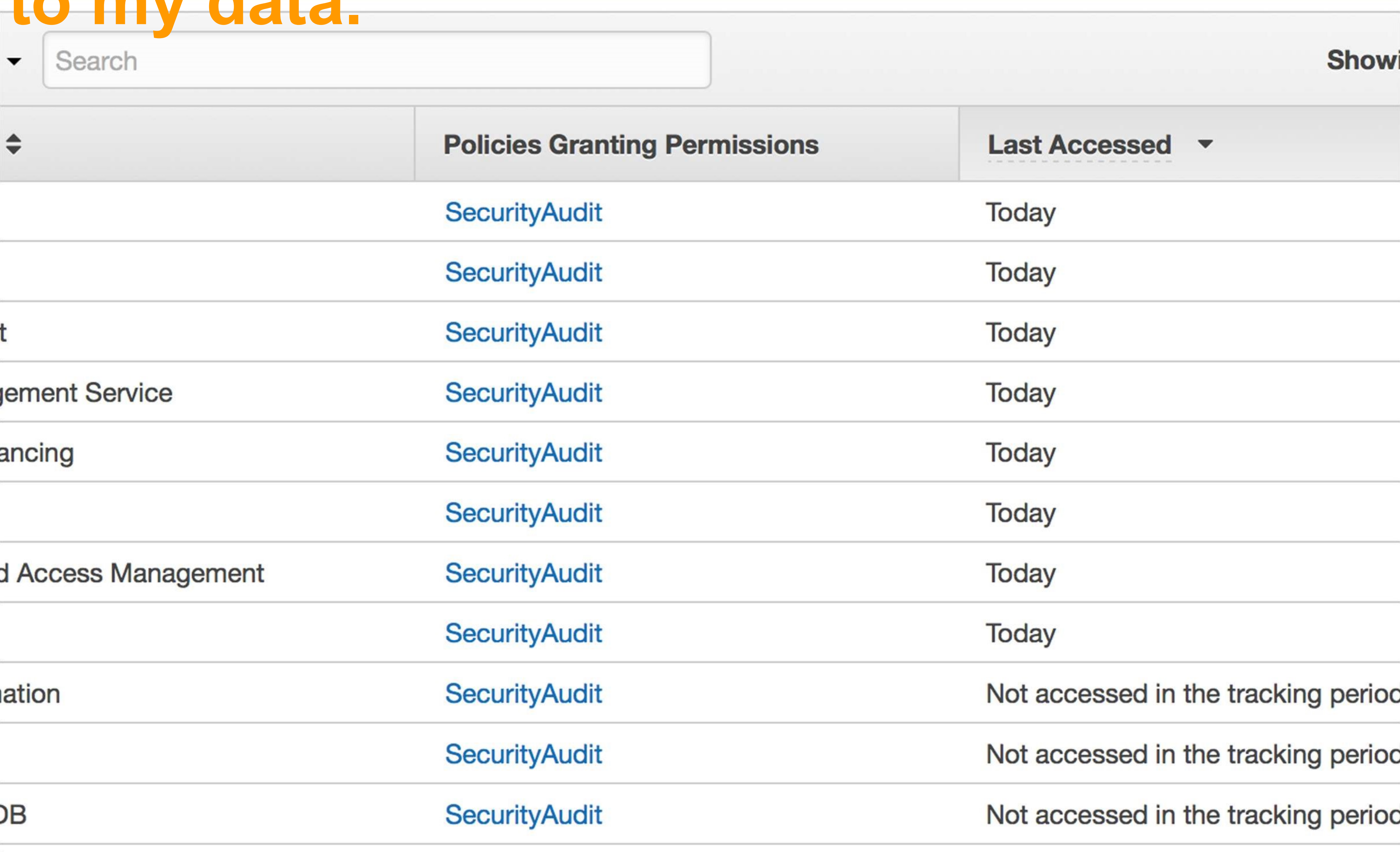
## Access Analyzer Info

### 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>638951966944 | - | Write | 5 minutes ago |

Available

# cess Advisor - "I want to control access to m ment, as well as know if somebody external to my data."



| | Policies Granting Permissions | Last Accessed |
|---|---|---|
| | SecurityAudit | Today |
| | SecurityAudit | Today |
| t | SecurityAudit | Today |
| gement Service | SecurityAudit | Today |
| ancing | SecurityAudit | Today |
| | SecurityAudit | Today |
| d Access Management | SecurityAudit | Today |
| | SecurityAudit | Today |
| ation | SecurityAudit | Not accessed in the tracking perioc |
| | SecurityAudit | Not accessed in the tracking perioc |
| DB | SecurityAudit | Not accessed in the tracking perioc |

# e Controls Best Practices- “I want the ability tically detect security mis-configurations and l in real-time”

e Cloudtrail in all regions

gate all logs from all parts of the stack

you actually need to review/monitor logs

on Cloudwatch Alarms and Events

low logs

n SIEM tool (such as AWS Security Hub)

ity Operations / Managed SOC

der a segregated account for logs and security tools onl sible to security teams

e GuardDuty, Config and Security Hub

# the Best Practices: Logging and Monitoring

**ogging** in all
all services, in

Amazon GuardDuty

I history in
nables security
ource change
compliance
ardDuty
naged threat
& 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.

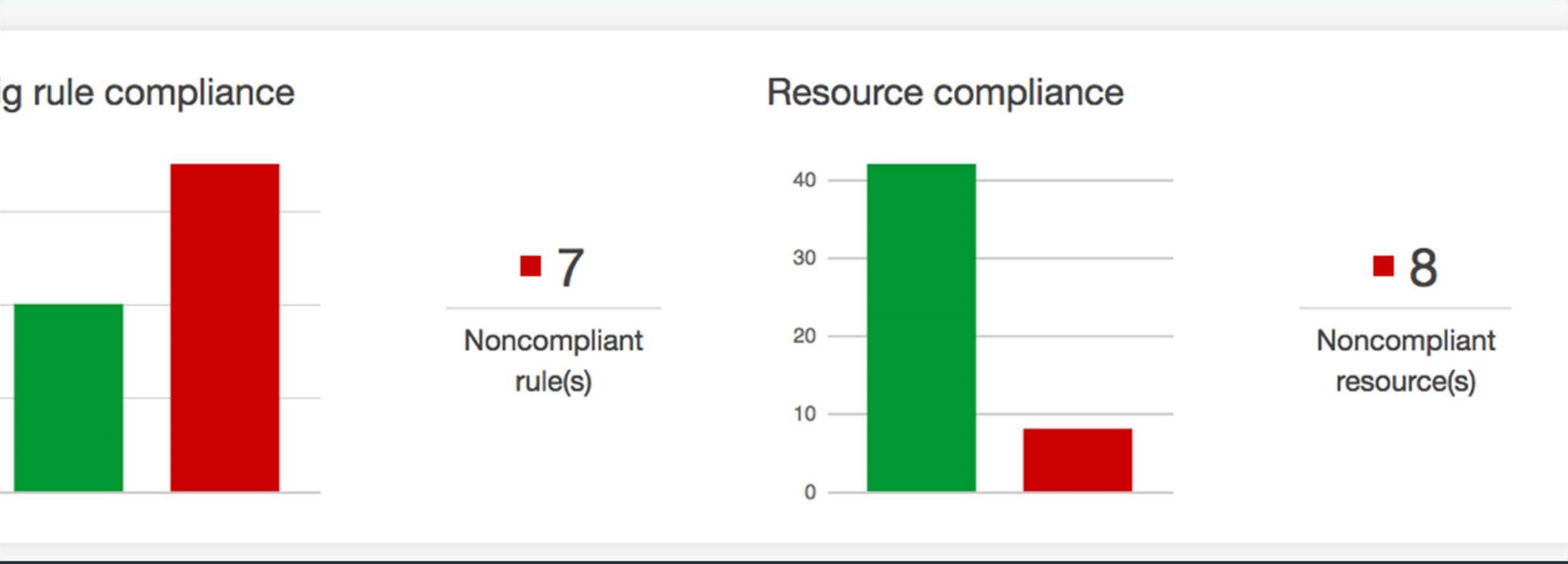
3) Use a separate A
account to fetch and
**copies of all logs**

Production

Security

Configuring a secu
account to copy log
separate bucket en
access to informati
can be useful in se
incident response
workflows.

# onfig Rules -“I want the ability to automatically mis-configurations and respond in real-time”



g rule compliance

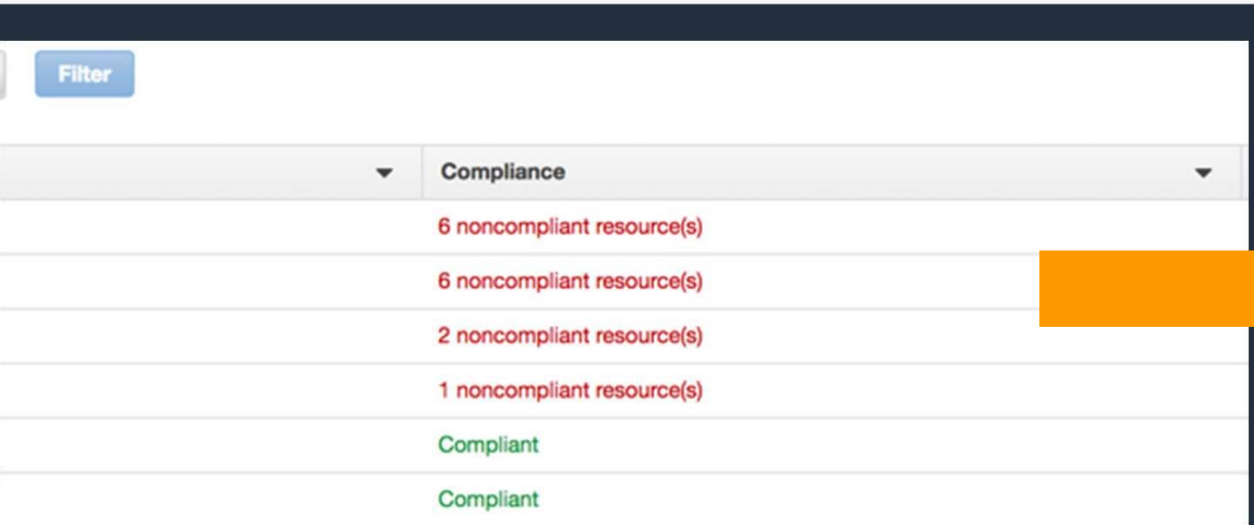
🟥 7

Noncompliant rule(s)

Resource compliance

🟥 8

Noncompliant resource(s)



| Compliance |
|---|
| 6 noncompliant resource(s) |
| 6 noncompliant resource(s) |
| 2 noncompliant resource(s) |
| 1 noncompliant resource(s) |
| Compliant |
| Compliant |

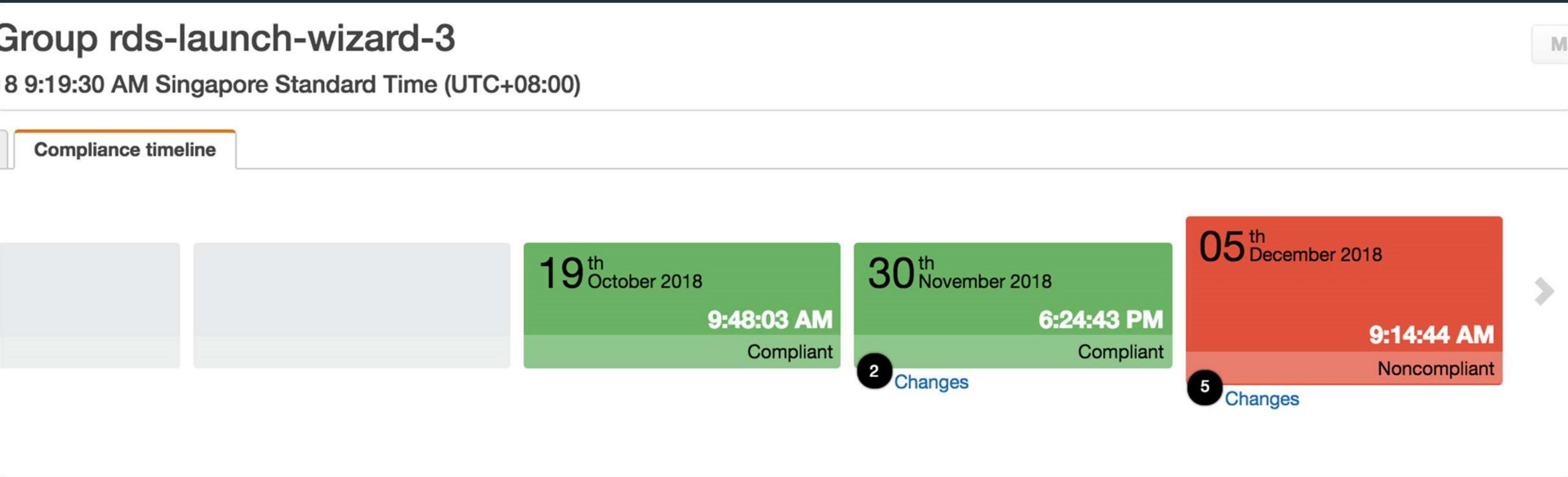
Automatic email to s when controls fail i

Execute automatic r based on desired outcome

# onfig Rules

| nce guideline | Action if non-compliance |
|---|---|
| olumes should be<br>ed | Encrypt volumes and alert operations team |
| s must be from a specific<br>d AMI | Terminate instance and notify team |
| s must be tagged with<br>nent type | Flag as non-compliant but take further action |

# ance Timeline – Deep Insight for Audit



Group rds-launch-wizard-3

8 9:19:30 AM Singapore Standard Time (UTC+08:00)

lows you to record and retrieve the compliance status of a resource over time. This a liance teams to determine if a resource always has been compliant or has drifted in a compliance with on-going changes.

# ructure Security Best Practices - "I want to p yber attacks, DDoS attacks and application layer exploit

- ment tight security groups (nothing to 0.0.0.0/0!!)
- onment (prod/dev) segregation (account versus VPC )
- pplication firewall (GeoBlock, SQL injection, XSS)
- Bastion host OR AWS Systems Manager Session Manag rred option)
- Resilient Architecture
- S – e.g. Palo Alto
- based agents (Trend Micro, vulnerability detection, malv
- ration Testing / Continuous VA
- atching – If building your AMI use ec2 Image Builder

# / the Best Practices: Infrastructure Security

**hreat**
**ayer** using AWS
s

VS Shield

AWS WAF

s of worldwide
sence in the
etwork to
ability, protect
of service
protect from
ion attacks.

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

VPC

Security Group

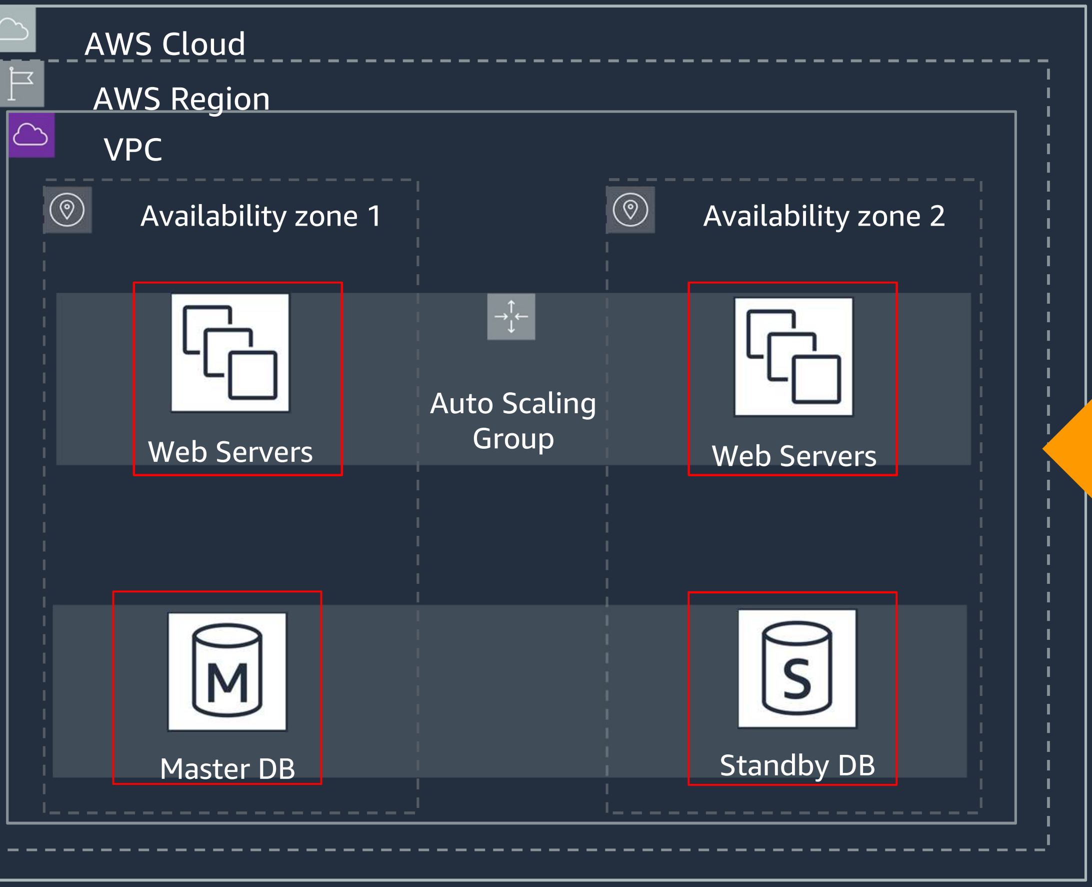
Implement security controls at the boundaries of hosts and virtual networks within the cloud environment to enforce access policy.

3) Manage vulnerab
through **patching a**
**scanning**

Systems Manage

AWS Systems Man
Patch Manager aut
the process of patc
managed instances
both security relate
other types of upda

# k Security – “I want to protect against cyber a ttacks and application layer exploits”



AWS PrivateLink

Traffic Mirroring

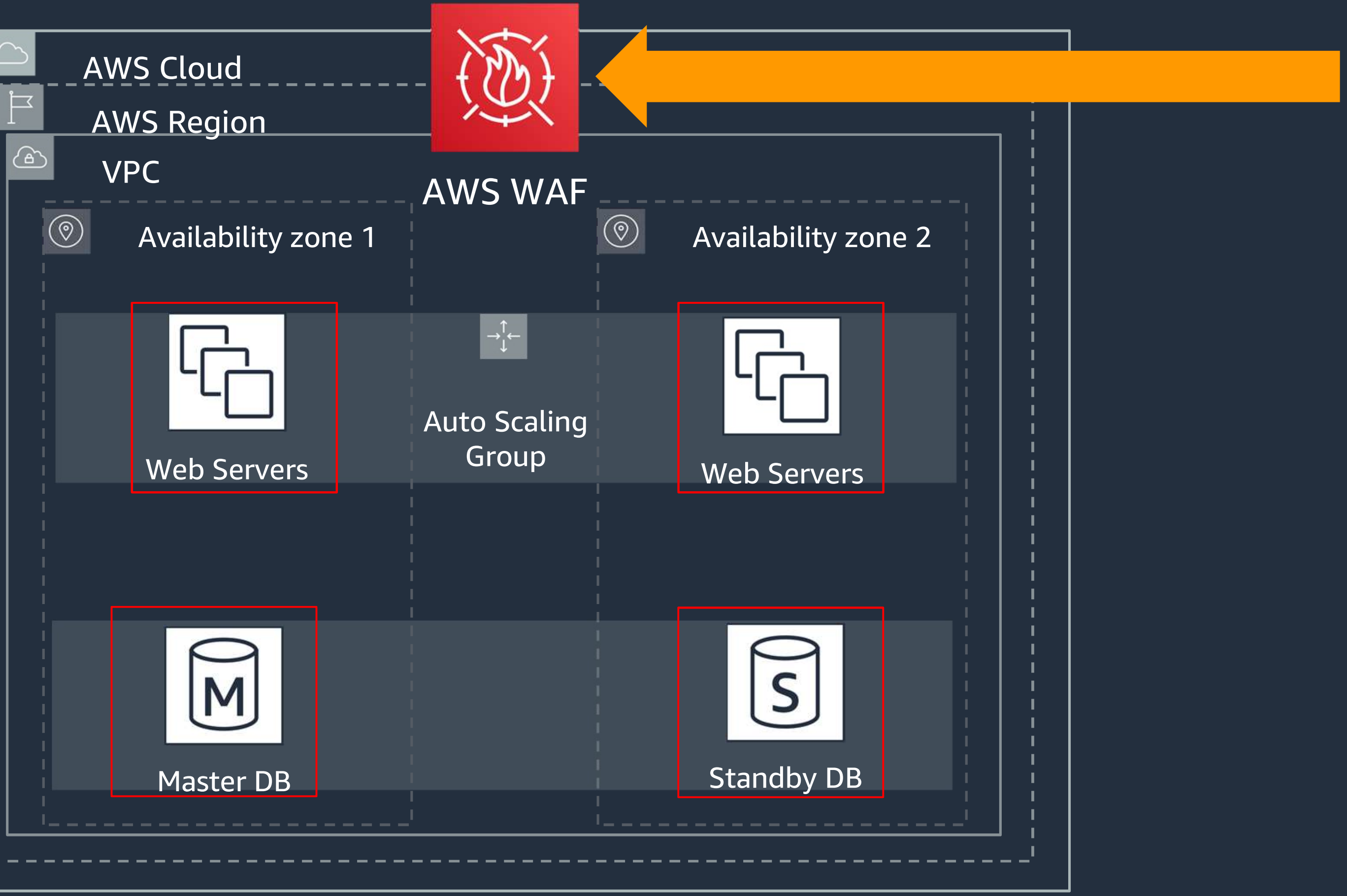
AWS Direct Conn

Security Groups are s
based firewalls that r
single host inside yo
You can enforce enc
ensuring only SSL
connections via secu

AWS Certificate Manager

Application Load Balancer

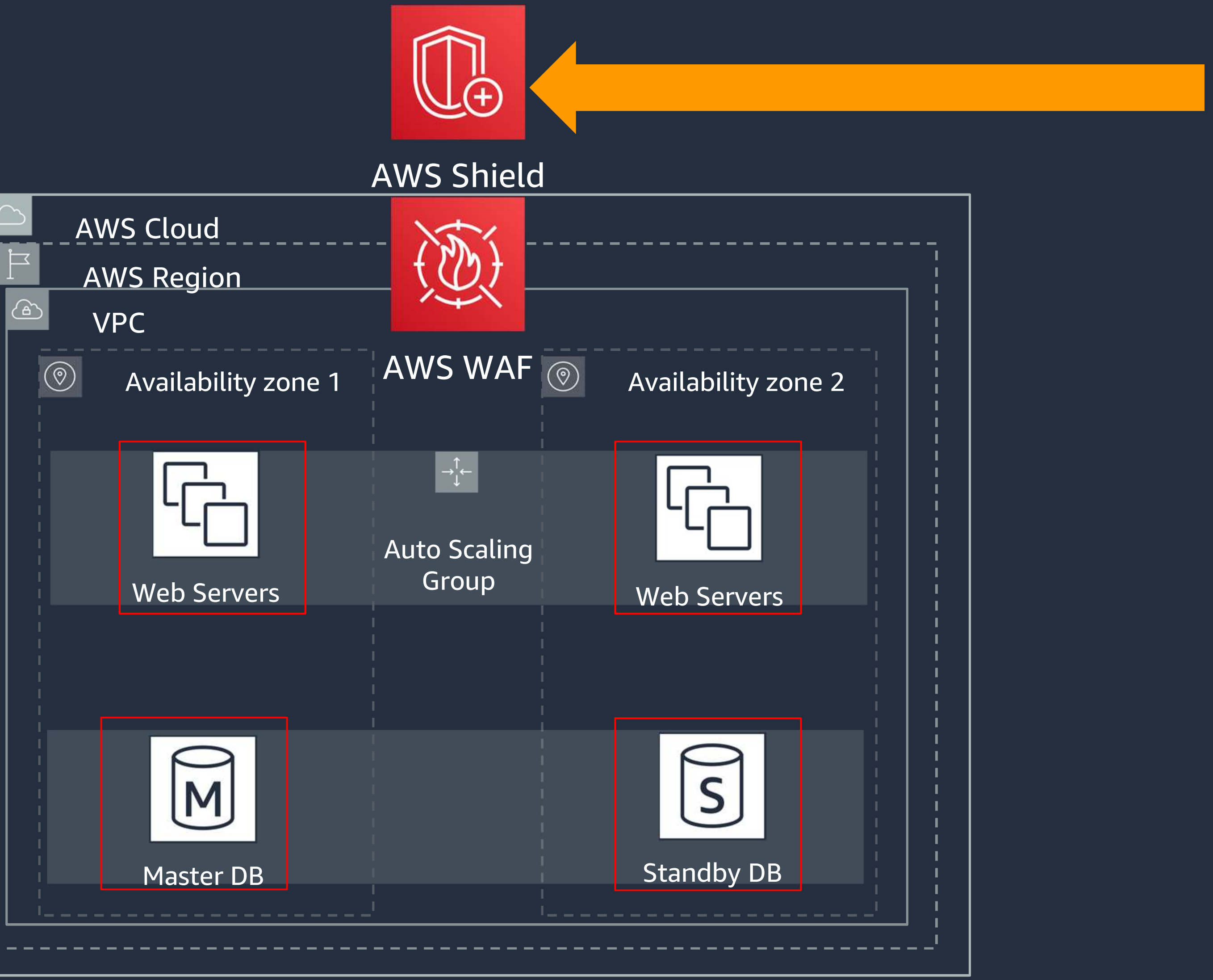
# pplication Firewall - “I want to protect against , DDoS attacks and application layer exploits”



AWS WAF is a we application firewall helps protect your applications fro common web exploit could affect applica availability, compro security, or consu excessive resourc

SQL Injection
Cross-Site Scripti
Brute forcing
Etc…

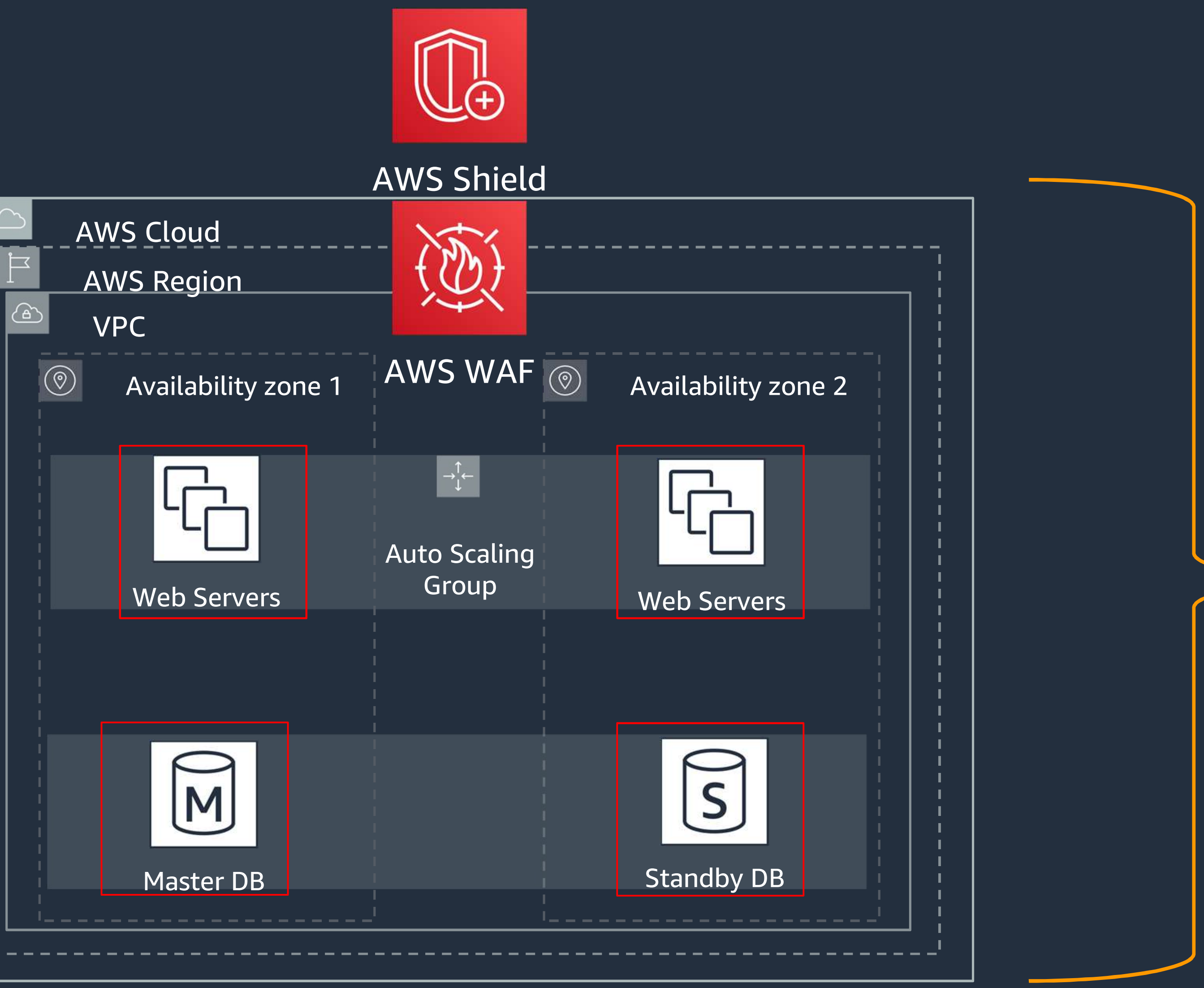
# Protection - “I want to protect against cyber att ttacks and application layer exploits”

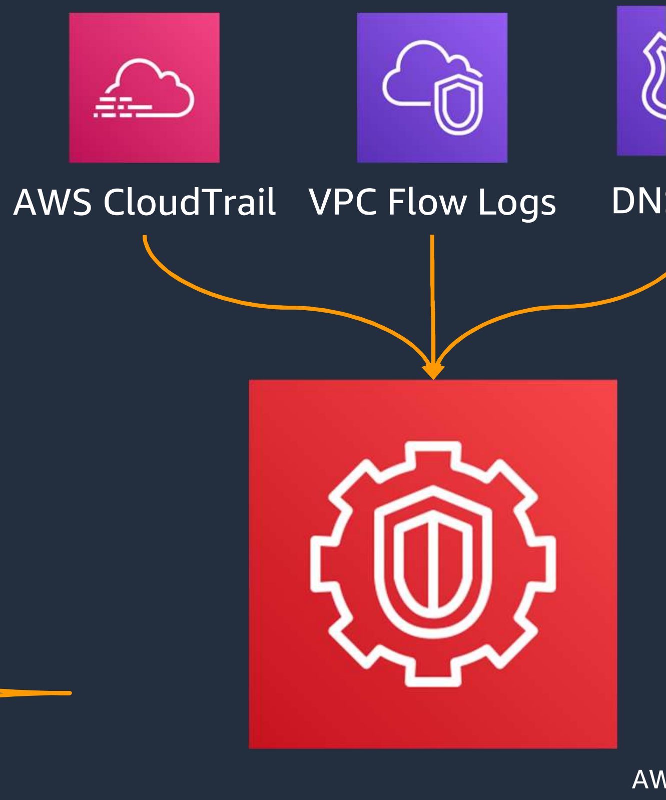


AWS Shield is a man Distributed Denia Service (DDoS) prote service that safegu applications runnin AWS.

AWS Shield defe against most comm frequently occurr network and trans layer DDoS attacks target your web sit applications.

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





**Amazon GuardDuty i** detection service continuously moni malicious activity unauthorized beha protect your AWS acc workloads

## otection Best Practices “I want to encrypt al strong encryption. I also want to have contro

- yption in transit (ACM, TLS, ELB)
- ryption at rest (KMS, S3, RDS), Applicatio r encryption
- ance termination protection (EC2)
- kup / snapshots (EBS, RDS, Data, S3, Log
- not expose data stores to the internet (S3 , DynamoDB etc.)

# the Best Practices: Data Protection

**ata at rest** (with
xceptions)

Amazon S3

cryption at rest
the
y and integrity
sider encrypting
at 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.

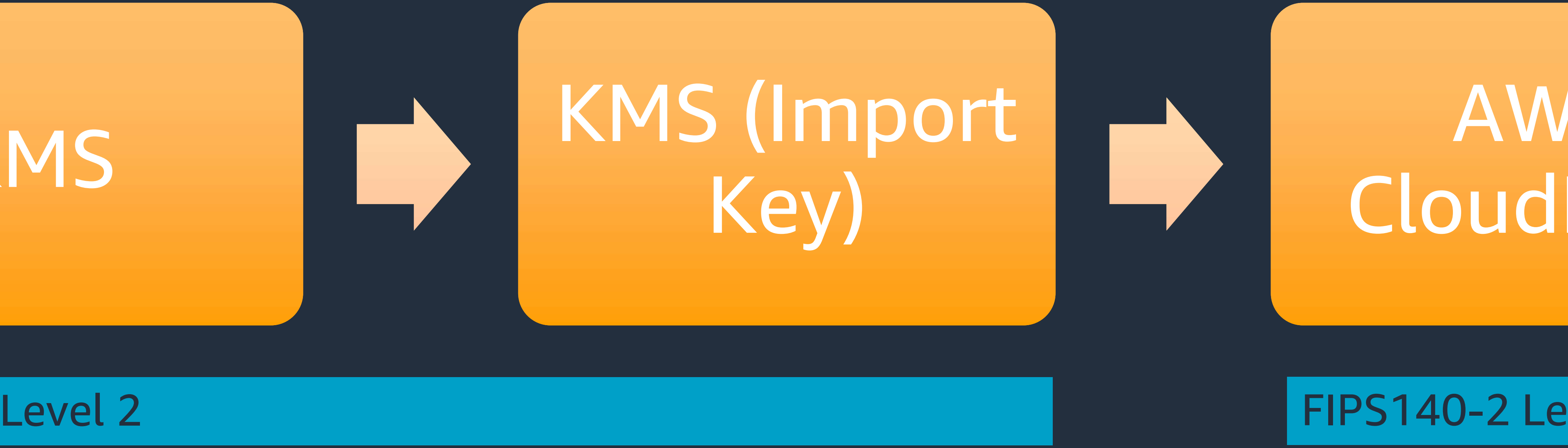
3) Encrypt **data in t**
(with no exceptions

Amazon CloudFront

ACM

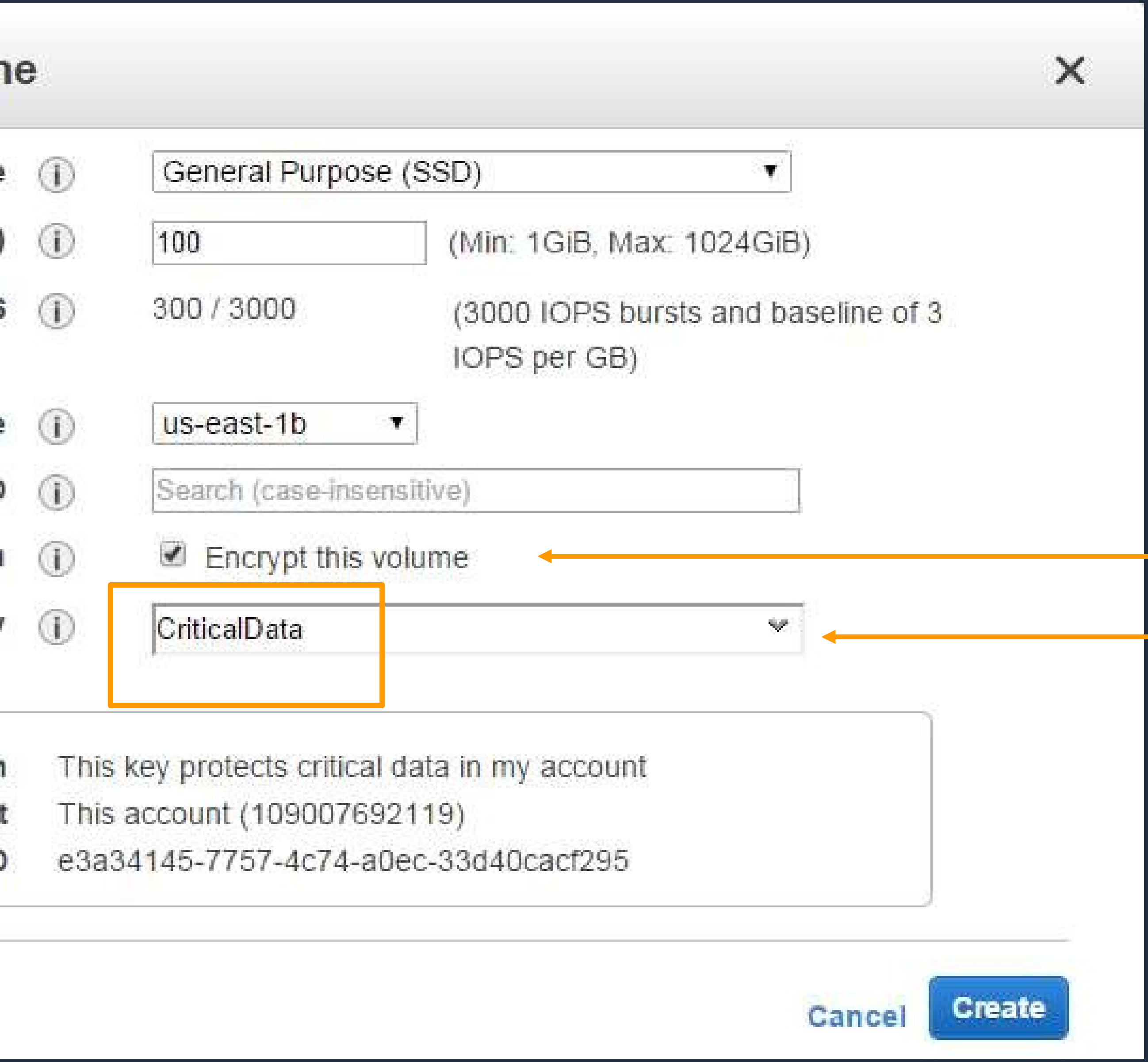
Encryption of data
provides protection
accidental disclosu
verifies the integrity
data, and can be us
validate the remote
connection.

# rotection – Encryption “I want to encrypt all m trong encryption. I also want to have control ov



eral Information Processing Standard (FIPS) Publicat FIPS PUB 140-2), is a U.S. government computer sec used to approve cryptographic modules.

# MS Usage - Encryption "I want to encrypt all m trong encryption. I also want to have control ov



ne

e General Purpose (SSD)

) 100 (Min: 1GiB, Max: 1024GiB)

s 300 / 3000 (3000 IOPS bursts and baseline of 3 IOPS per GB)

e us-east-1b

o Search (case-insensitive)

n ☑ Encrypt this volume

y CriticalData

n This key protects critical data in my account

t This account (109007692119)

D e3a34145-7757-4c74-a0ec-33d40cacf295

Key Admin Key

Single click, AES256 symm

Protect data using a custome
under the control of the
Segregation of duties allow
'key administrators' and
specifies who can use the ke
set.

# nt Response

- ble Logging (Cloudtrail, Alarm, Events, fications to admins)
- itor SOC for potential compromises
- books / runbooks
- nsic capability
- mated recovery

# teps: Path to Production

apability &
ablement

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 & Externa
Assessment

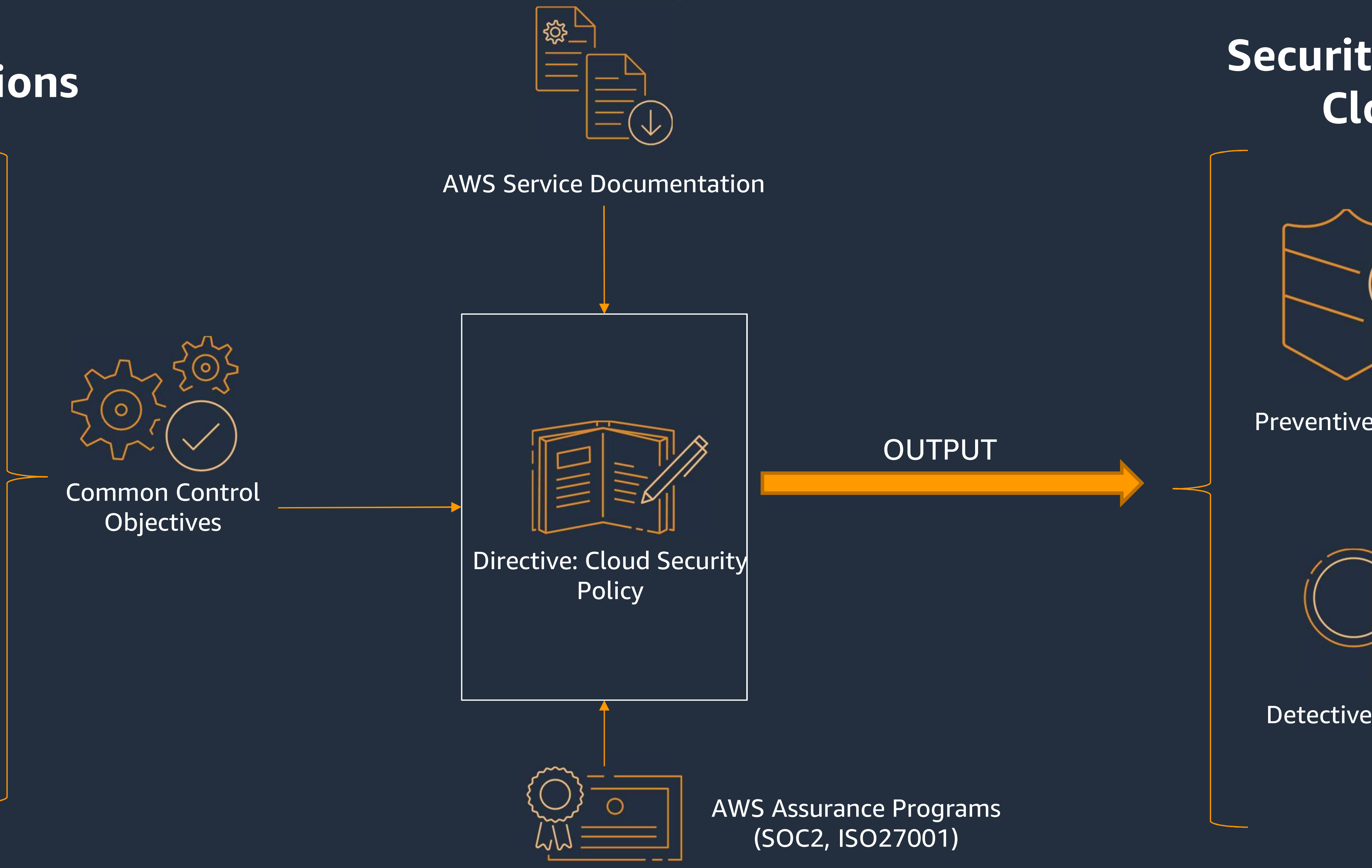
# teps: Cloud Security Policy

n AWS usage policy
ge existing where
e, create new ones
here required

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

Aim for a hig
degree of
automation f
implementing p

# eps: Establish Security Controls



ions

Securit
Cl

AWS Service Documentation

Common Control Objectives

Directive: Cloud Security Policy

OUTPUT

AWS Assurance Programs (SOC2, ISO27001)

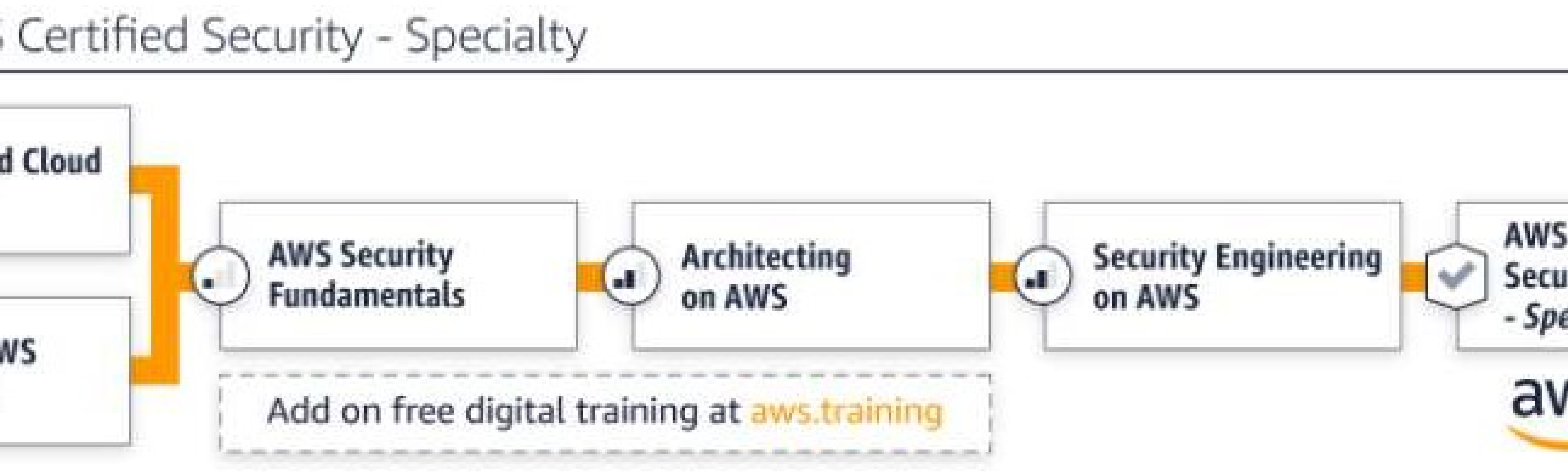
Preventive

Detective

# eps

e:

ecurity Curriculum



Certified Security - Specialty

d Cloud

WS

AWS Security Fundamentals

Architecting on AWS

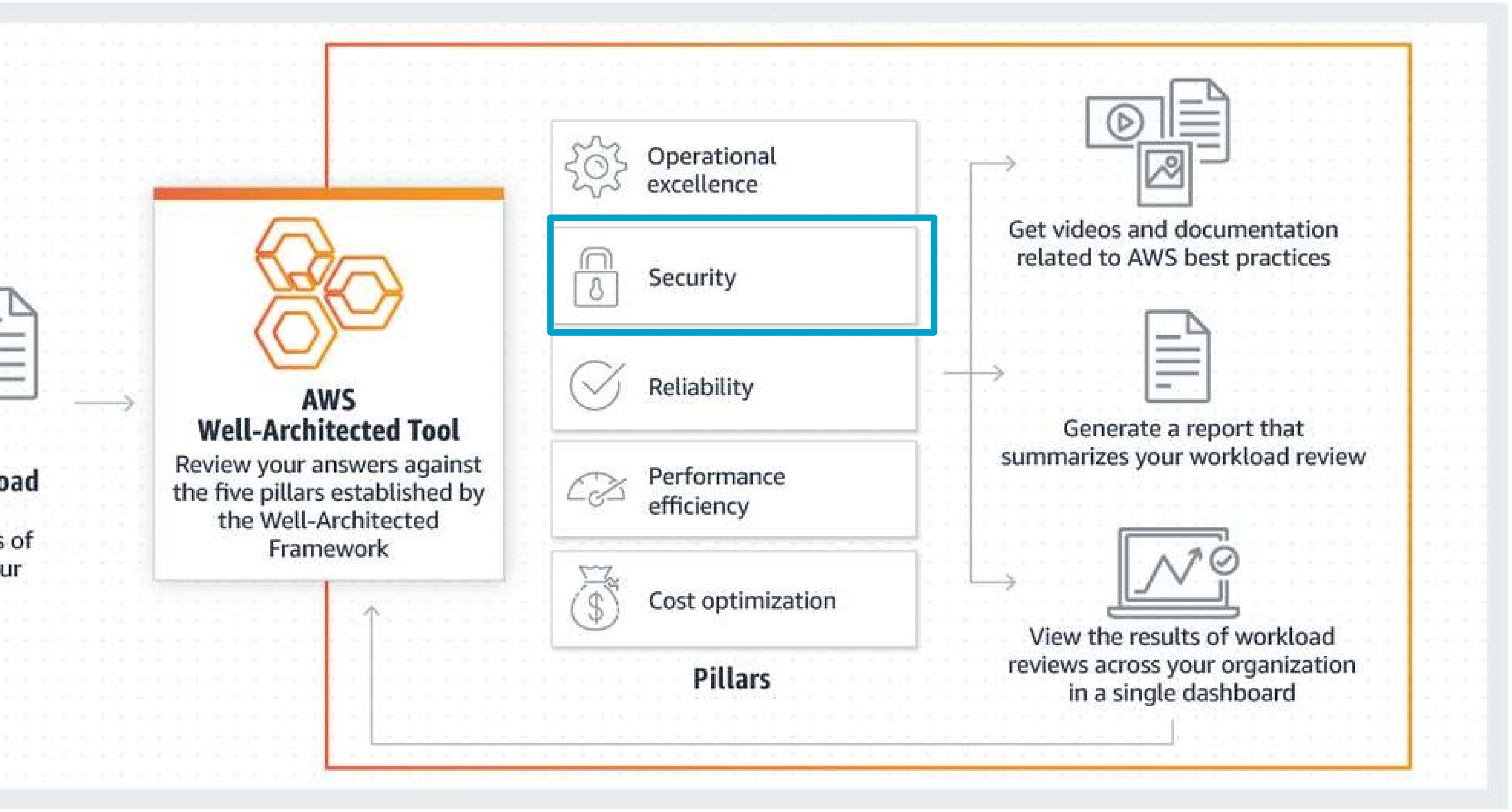
Security Engineering on AWS

AWS Secu - Spe

Add on free digital training at aws.training

# eps

## ell Architected



oad
s of
ur
AWS
Well-Architected Tool
Review your answers against the five pillars established by the Well-Architected Framework
Operational excellence
Security
Reliability
Performance efficiency
Cost optimization
Pillars
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

# ders Session – Identify erabilities and fix them

the principle of least privilege been appl

ure your data stores (all of them!)

k about what should and should NOT be
osed to the public

many services do we have for monitorin
logging?

# y/aws-bkk-survey

# nk You