



SUMMIT  
ONLINE

# Introduction to AWS security

Myles Hosford

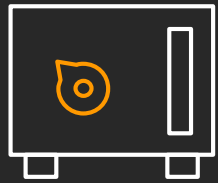
Principal, Security Architecture

Amazon Web Services

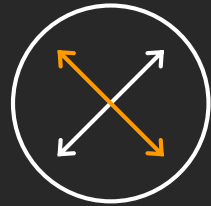
# Agenda

- Shared responsibility model
- Security *of* the cloud
- Security *in* the cloud
- Security governance
- Next steps

# Elevate your security with the AWS Cloud



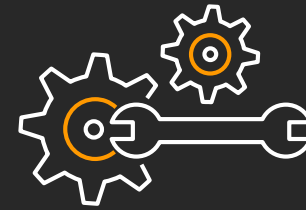
Inherit global  
security and  
compliance  
controls



Scale with  
superior visibility  
and control



Highest standards  
for privacy and  
data security

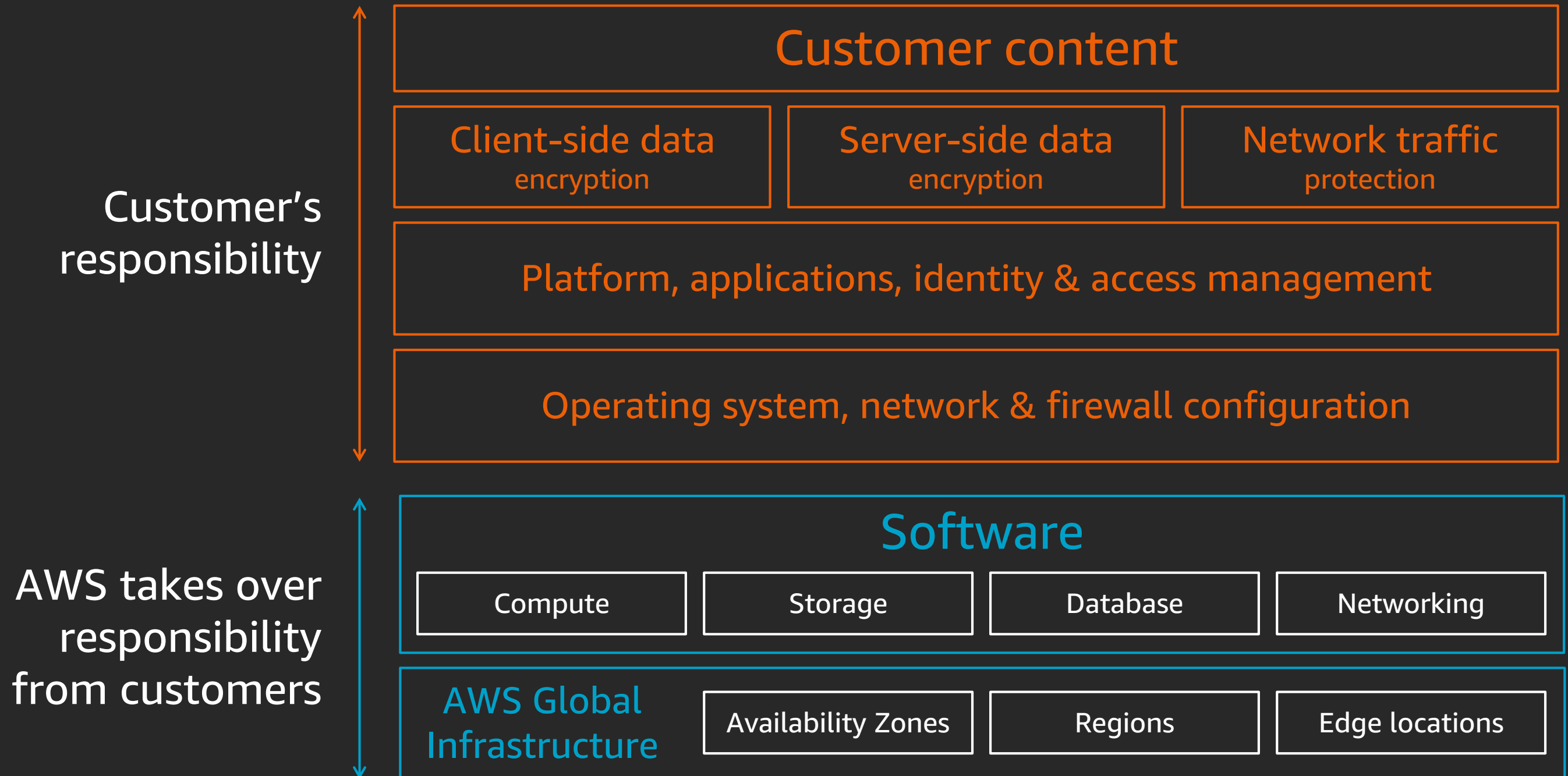


Automate with  
comprehensive,  
integrated  
security services



Largest network  
of security  
partners and  
solutions

# Shared responsibility between AWS and the customer

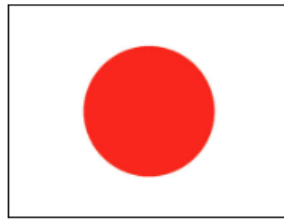


# Security *of* the cloud

# AWS Compliance Programs – Global

				
<b>CSA</b> Cloud Security Alliance Controls	<b>ISO 9001</b> Global Quality Standard	<b>ISO 27001</b> Security Management Controls	<b>ISO 27017</b> Cloud Specific Controls	<b>ISO 27018</b> Personal Data Protection
				
<b>PCI DSS Level 1</b> Payment Card Standards	<b>SOC 1</b> Audit Controls Report	<b>SOC 2</b> Security, Availability, & Confidentiality Report	<b>SOC 3</b> General Controls Report	

# AWS Compliance Programs – Regional



**FISC [Japan]**  
Financial Industry  
Information Systems



**IRAP [Australia]**  
Australian Security  
Standards



**K-ISMS [Korea]**  
Korean Information  
Security



**MTCS Tier 3  
[Singapore]**  
Multi-Tier Cloud  
Security Standard



**OSPAR  
[Singapore]**  
Outsourcing  
Guidelines



# AWS Artifact & AWS Compliance Center



## The AWS Artifact tool supports increased transparency

A portal that provides on-demand access to:

- **Information** on AWS policies, processes, and controls
- **Documentation** of controls relevant to specific AWS services
- **Validation** that AWS controls are operating effectively

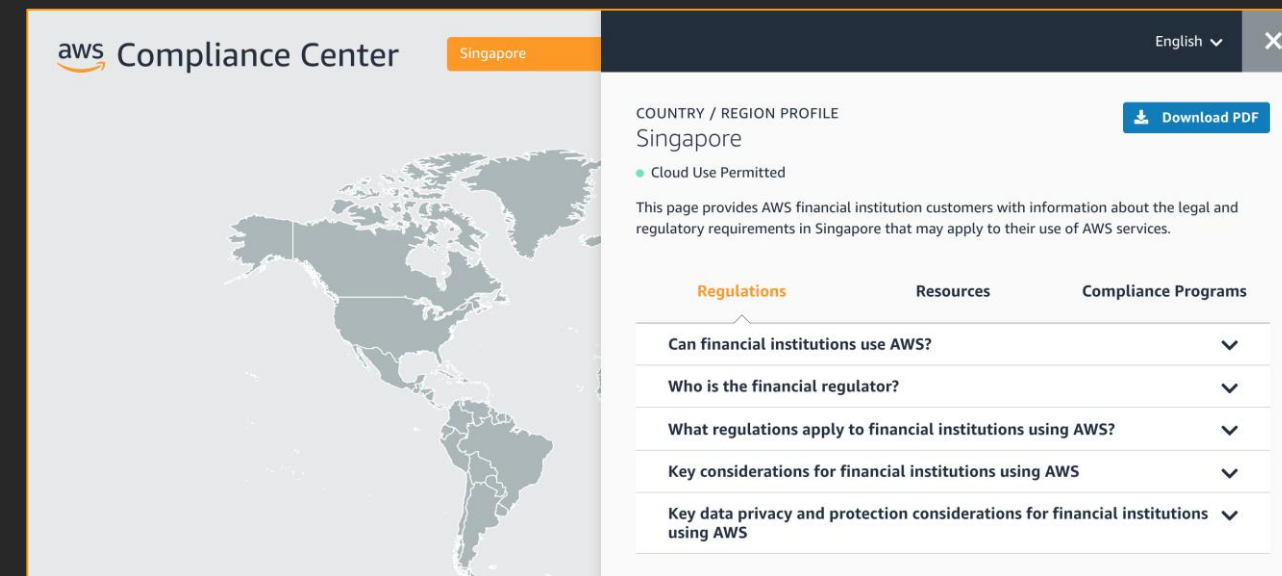
Customers can use the reports to align AWS controls to their own control frameworks, and verify that AWS controls are operating effectively



## The AWS Compliance Center provides research on cloud regulations

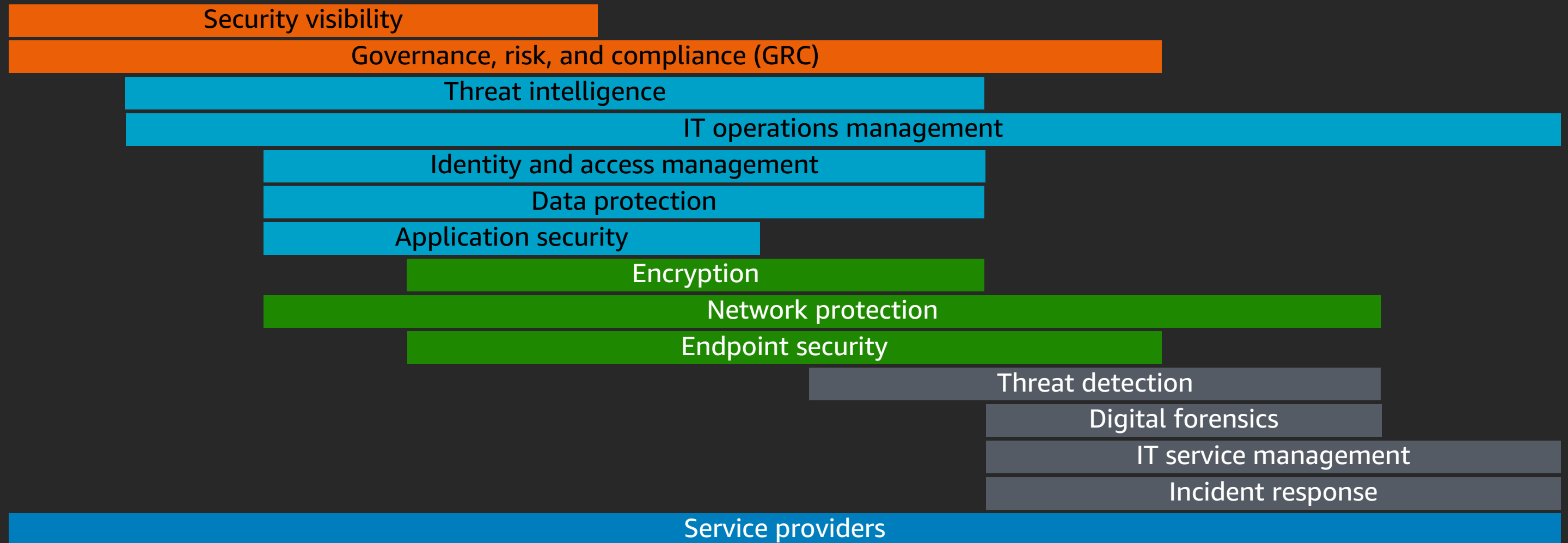
The AWS Compliance Center provides a central location to research cloud regulations in specific countries and learn about AWS Compliance programs

[www.atlas.aws](http://www.atlas.aws)



# Security *in* the cloud

# Security in the cloud



## Identify

Security fundamentally anchors on having sufficient knowledge of your world

## Protect

The best defense is a good offense, but ...

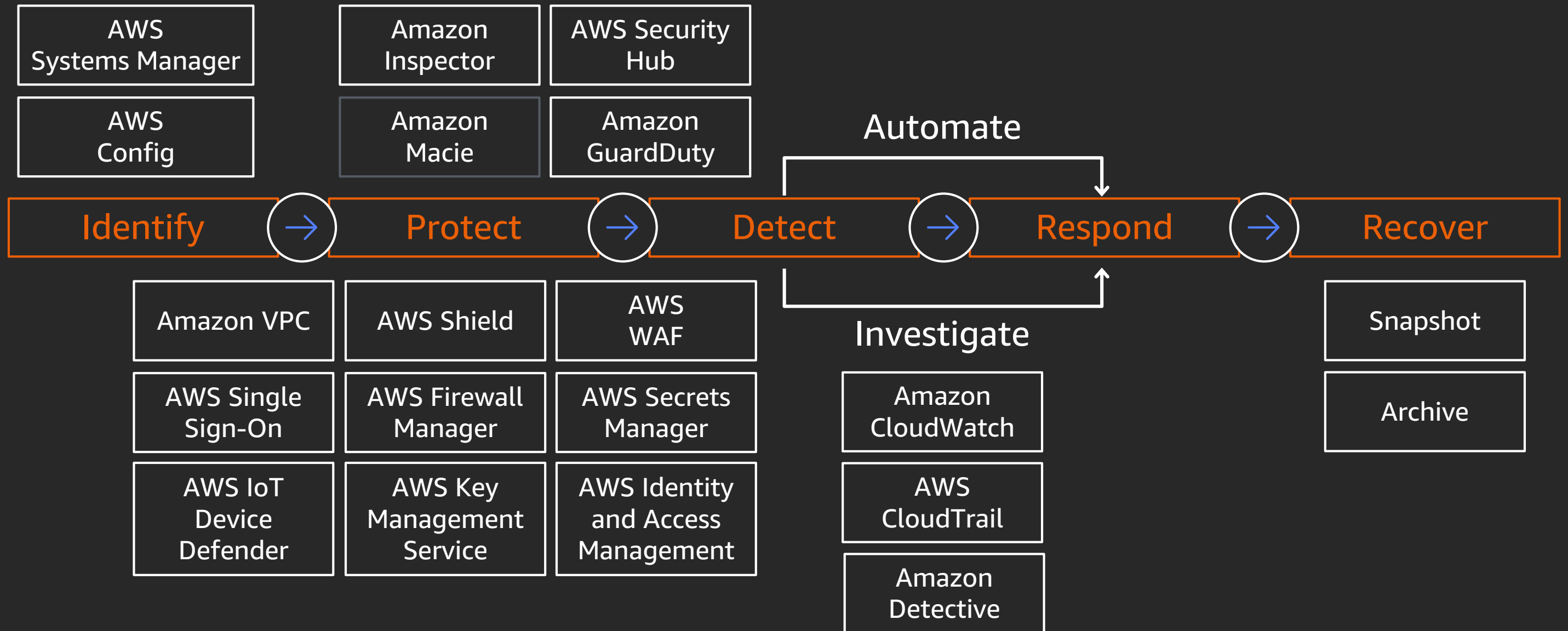
## Detect

One must "assume breach" and have a strong defense

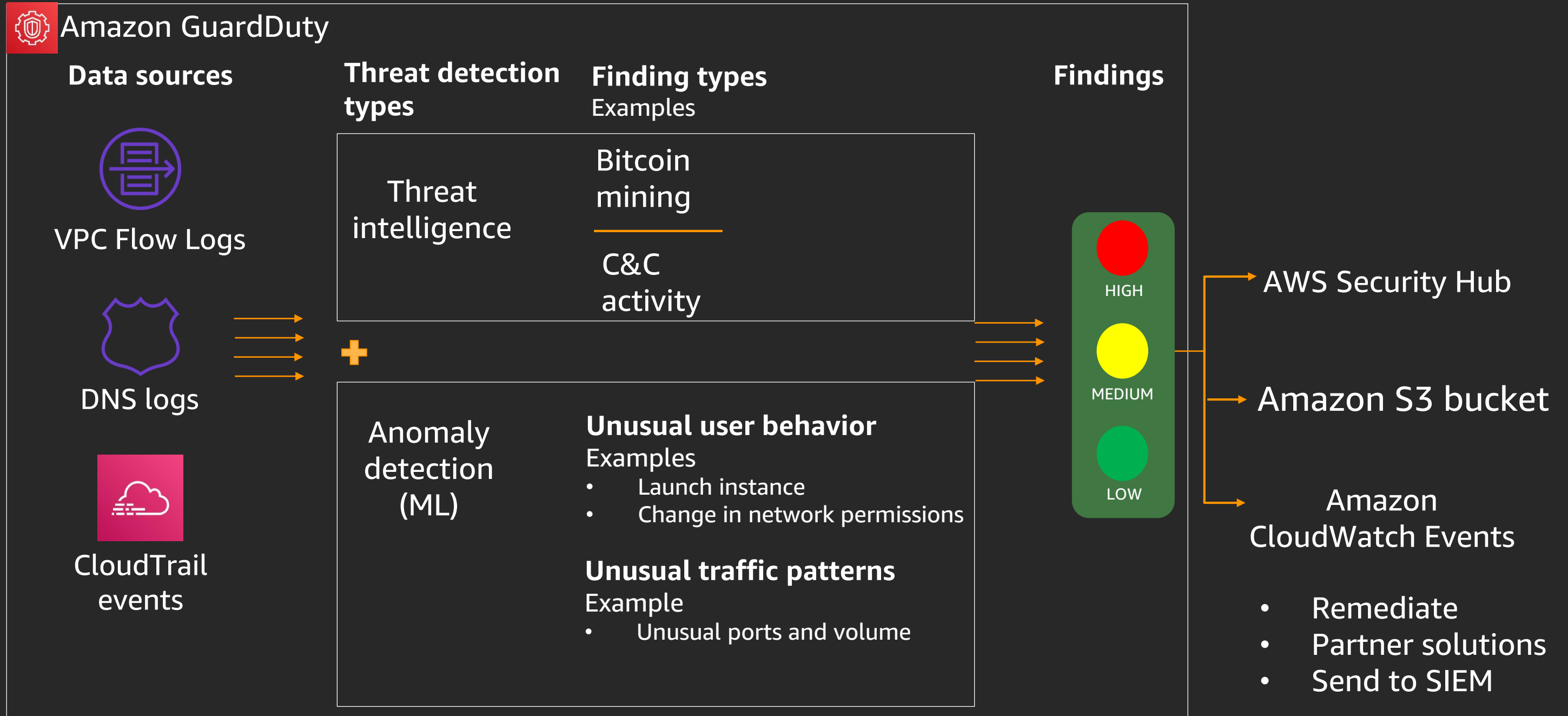
## Respond/Recover

Knowing and being able to act swiftly is key in the cloud

# AWS cloud-native security services

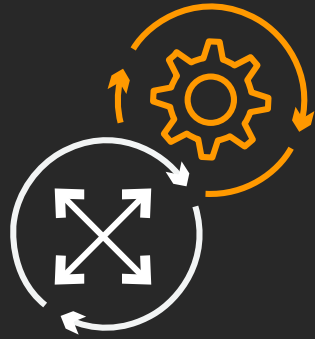


# Amazon GuardDuty



# Security governance

# More innovation and greater agility with control



Agility and control: Don't choose just one **or** the other



---

## Agility

Experiment

Be productive

Empower a distributed team

Customers want both

---

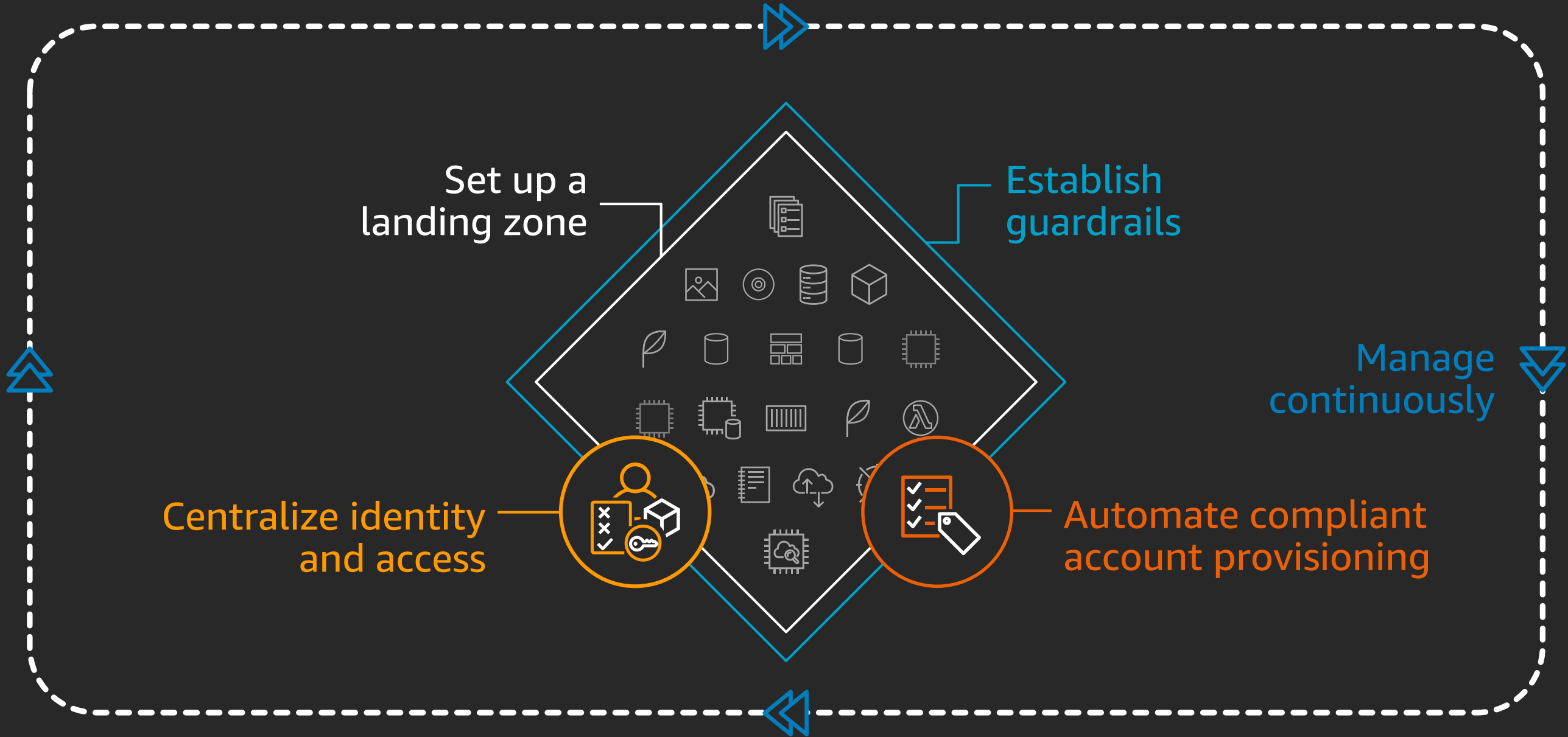
## Governance

Enable

Provision

Operate

# Governance at scale





# Governance at scale

 Enable



**Set up a best practice environment for control**

**AWS Control Tower**

**Manage accounts**

**AWS Organizations**

**Establish cost controls**

**AWS Budgets**

**AWS License Manager**

**AWS Marketplace: Private Marketplace**

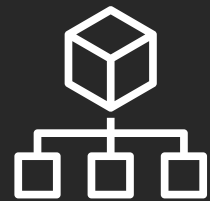
**Improve architecture over time**

**AWS Well-Architected Tool**

# Governance at scale



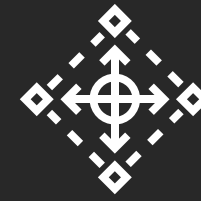
Enable



---

## AWS Organizations

Centrally govern resources in your  
multi-account AWS environment

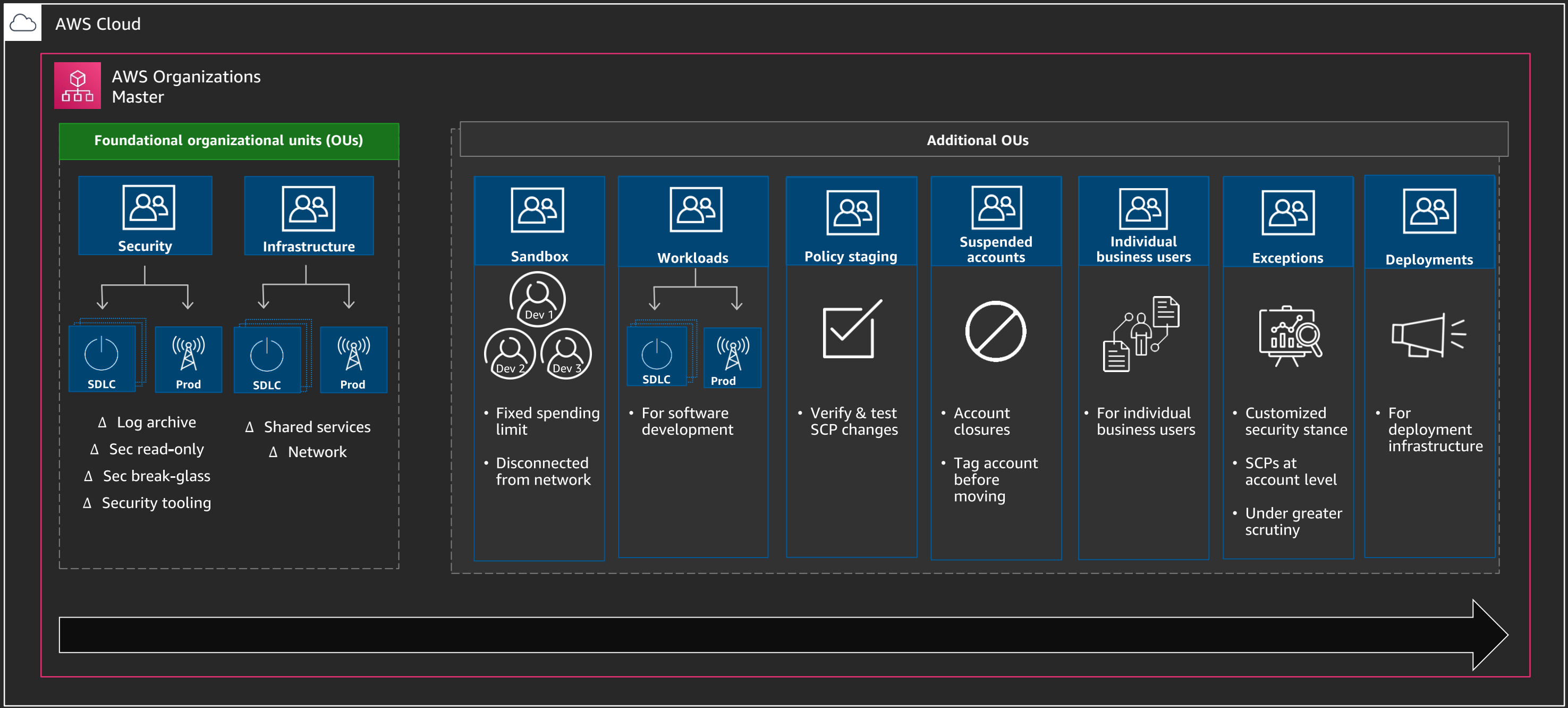


---

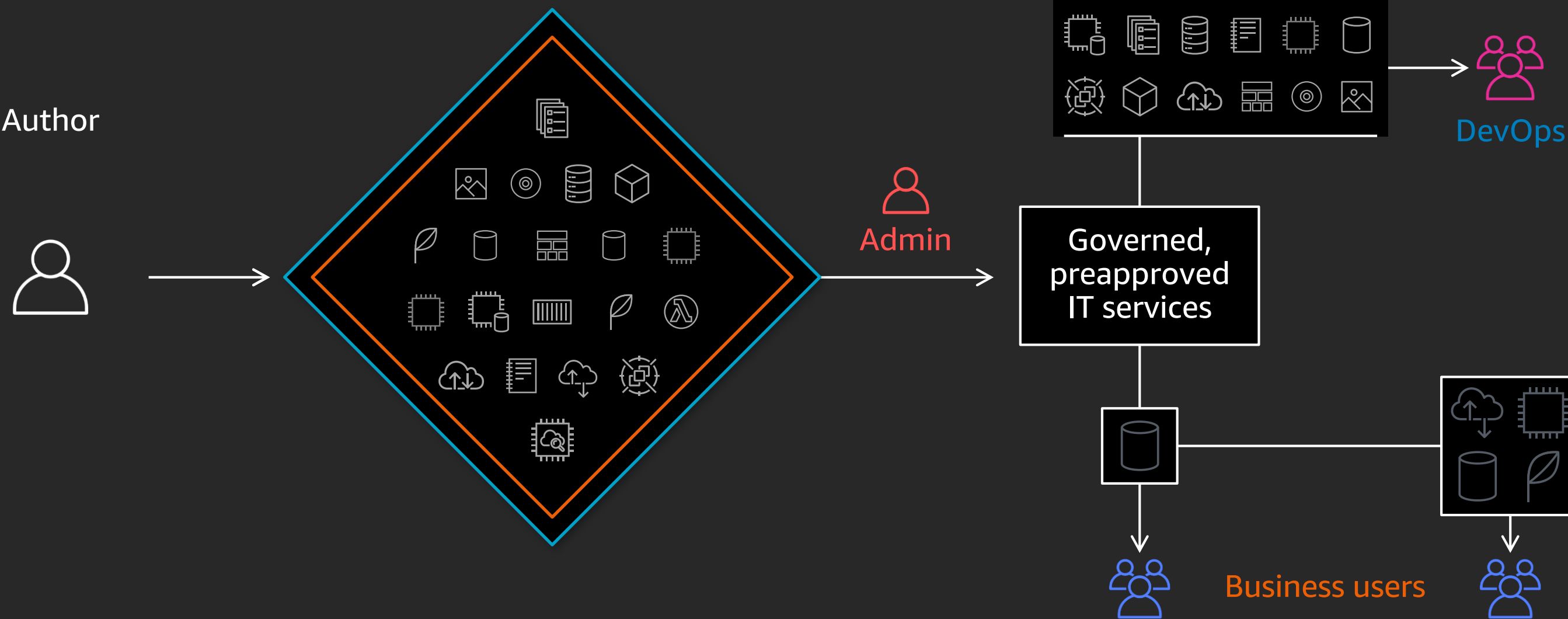
## AWS Control Tower

The easiest way to set up a multi-  
account AWS environment with  
built-in governance

# Recommended AWS multi-account framework



# Automate provisioning



# Automate provisioning



Provision



## DevOps

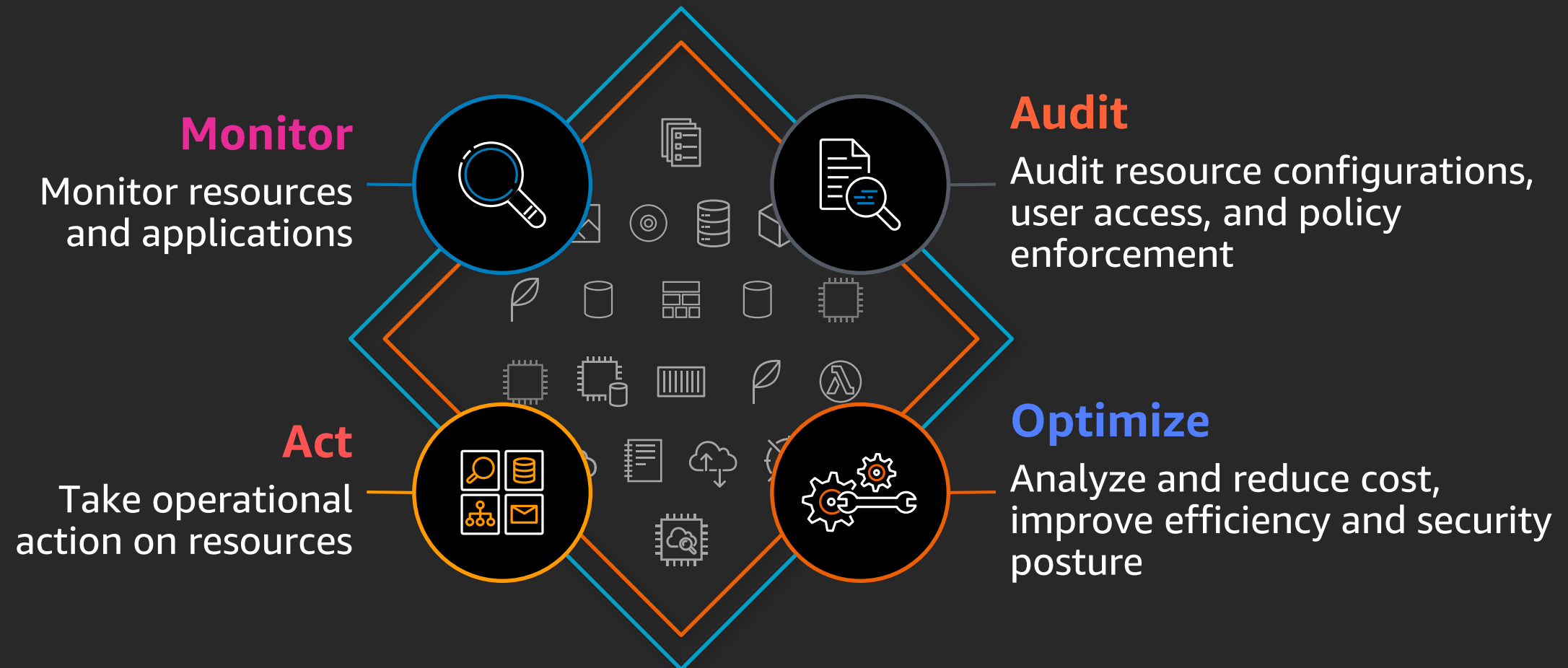
AWS CloudFormation  
AWS OpsWorks  
AWS Marketplace  
AWS Service Catalog

## Business users

AWS Service Catalog  
AWS Marketplace

# Operate with agility and control

 Operate



# Operate with agility and control



## Monitor resources and applications

Amazon CloudWatch

## Audit user activity and resource configurations

AWS CloudTrail

AWS Config

## Manage resources and take operational action

AWS Systems Manager

## Optimize to reduce cost and improve security posture

AWS Trusted Advisor

AWS Cost and Usage Reports

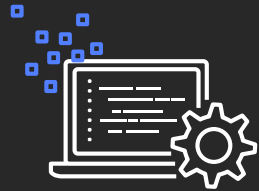
AWS Cost Explorer

# Current approach to security assessment

	A	B	C	D	E	F
1	3 OVERSIGHT OF TECHNOLOGY RISKS BY BOARD OF DIRECTORS AND					
2	Item	TRMG Section	Guideline Description	Full Compliance	Partial Compliance	Non-compliance
3	1	3.0.2	The board of directors and senior management have oversight of technology risks.			
4			The IT function is capable of supporting business strategies and objectives.			
5	2	3.1.1	A sound and robust technology risk management framework is established and maintained.			
6			The board of directors and senior management are involved in key IT decisions.			
7	3	3.1.2	The board of directors and senior management are fully responsible for ensuring that effective internal controls and risk management practices are implemented to achieve security, reliability, resiliency and recoverability.			
8	4	3.1.3	The board of directors and senior management have given due consideration to cost-benefit issues, including factors such as reputation, customer confidence, consequential impact and legal implications, with regard to investment in controls and security measures for computer systems, networks, data centres (DC), operations and backup facilities.			
9	5	3.2.1	IT policies, standards and procedures are established to manage technology risks and safeguard information system assets.			
10	6	3.2.2	IT policies, standards and procedures are regularly reviewed and updated.			
11	7	3.2.3	Compliance processes are implemented to verify that IT security standards and procedures are enforced.			



# AWS CloudTrail



---

## Capture

Record activity as  
CloudTrail events



---

## Store

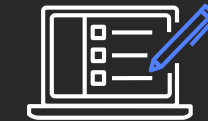
Retain events logs in a  
secure Amazon S3 bucket



---

## Act

Trigger actions  
when important  
events are detected



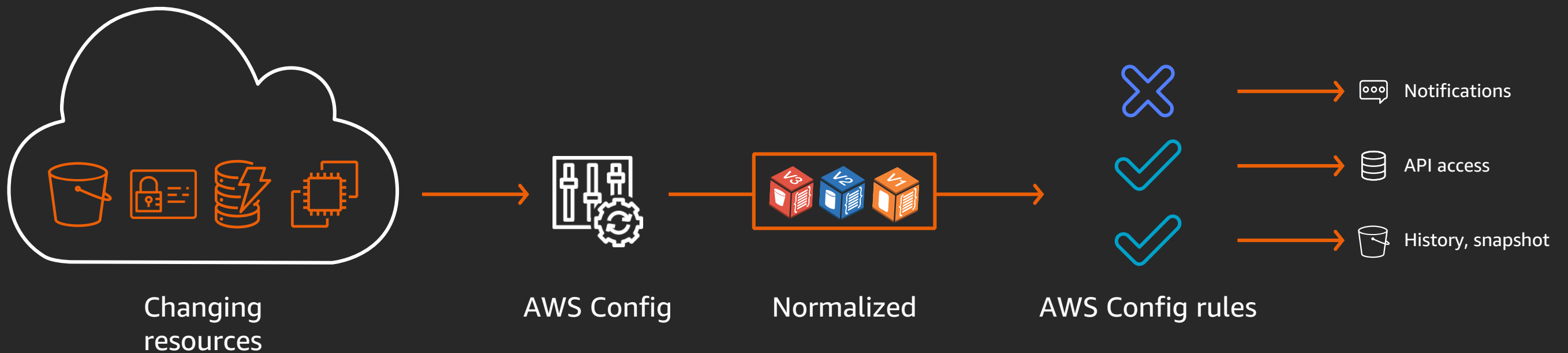
---

## Review

Analyze recent  
events and logs with  
Amazon Athena or  
Amazon CloudWatch  
Logs Insights

# AWS Config

- Continuous recording and continuous assessment service
- Tracks configuration changes to AWS resources
- Alerts you if the configuration is noncompliant with your policies
- Automated remediation of noncompliant resources
- Control and manage custom resources



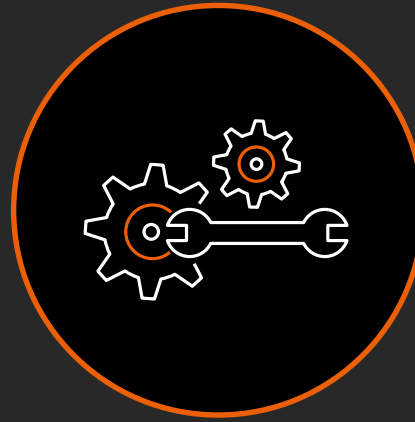
# Current approach to security assessment

	A	B		D	E	F
1	RIGHT OF TECHNOLOGY RISKS BY BOARD OF DIRECTORS AND					
2	Item	TRMG Section	Guideline Description	Full Compliance	Partial Compliance	Non-compliance
3	1	3.0.2	The board and senior management have oversight of technology risk.			
4			The board is capable of supporting business strategies and objectives.			
5	2	3.1.1	A robust technology risk management framework is maintained.			
6			The board and senior management are involved in decisions.			
7	3	3.1.2	The board and senior management are responsible for ensuring that effective internal controls are implemented to ensure reliability, resiliency and recoverability.			
8	4	3.1.3	The board and senior management give due consideration to cost-benefit issues, including reputational, confidential and legal implications, with regard to investment in security and security measures such as data centres (DC), operations and backup facilities.			
9	5	3.2.1	IT policies, standards and procedures are established to manage technology risks and safeguard system assets.			
10	6	3.2.2	IT policies, standards and procedures are regularly reviewed and updated.			
11	7	3.2.3	Compliance processes are in place and are enforced.			

# Continuous compliance on AWS



Unprecedented visibility



Near real-time automation

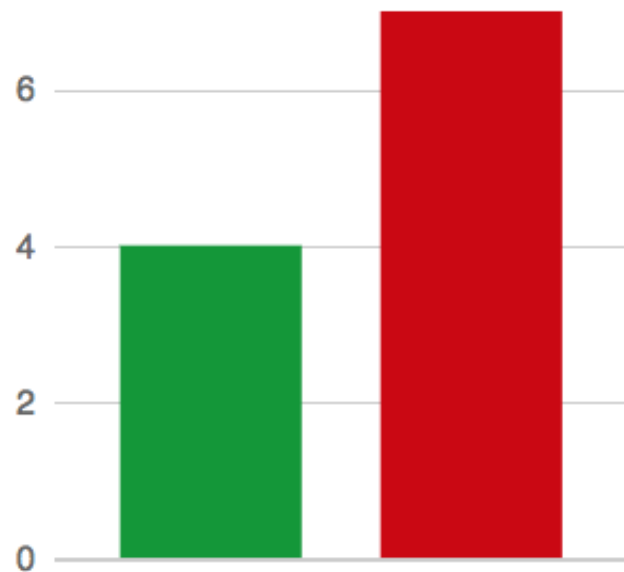


Continuous compliance

Having the visibility into **who** made **what** change from **where** in near real time enables financial institutions to **detect** misconfigurations and noncompliance and **respond** quickly to **prevent** risks from materializing

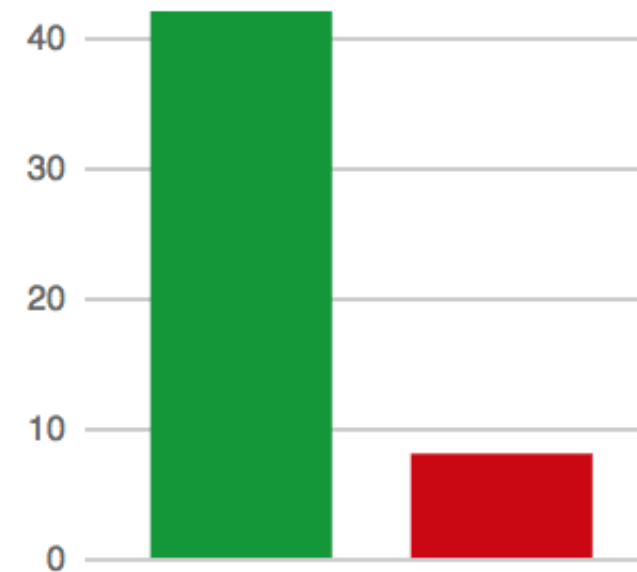
# AWS Config rules: Real-time compliance engine

## Config rule compliance



■ 7  
Noncompliant  
rule(s)

## Resource compliance

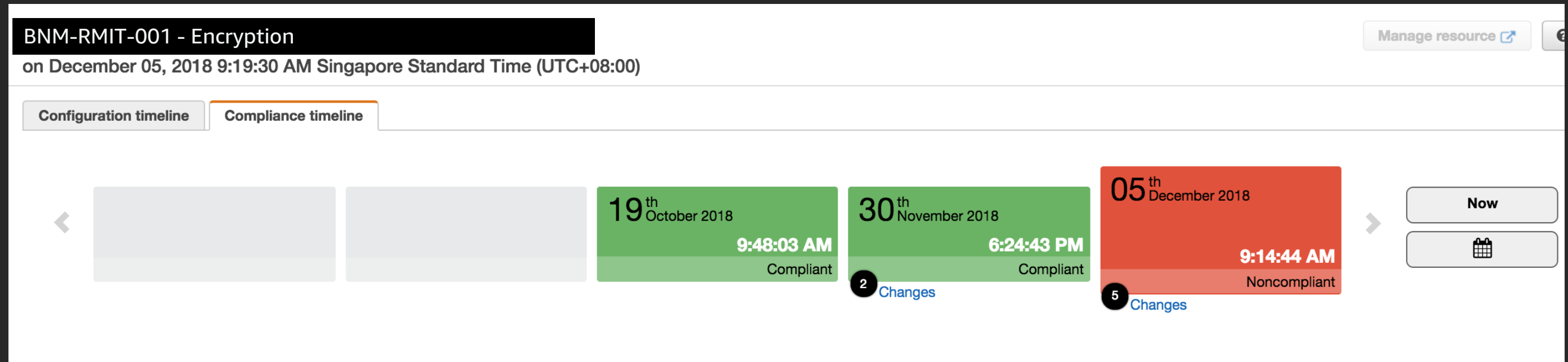


■ 8  
Noncompliant  
resource(s)

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

# Compliance timeline: Deep insight for audit



AWS Config enables you to record and retrieve the compliance status of a resource over time. This enables your risk and compliance teams to determine whether a resource always has been compliant or whether it has drifted in and out of compliance with ongoing changes.

# Automatic remediation

## Manage remediation: encrypted-volumes

Status ?

The execution of remediation actions is achieved using [AWS Systems Manager Automation](#). Choose from a set of AWS recommended remediation actions or custom remediation actions. To remediate a rule choose all the noncompliant resources in scope from table.

Rule name encrypted-volumes

Remediation action Remediation action

Resource ID parameter NA

**Parameters** Every parameter has either a static value or a dynamic value. By default, the dynamic value is no-resource type. Only when the dynamic value is no-resource type, you can enter a static value. Alternatively, you can choose a resource type from the dynamic value drop-down list. Upon choosing a dynamic value, the static value is cleared (if present) and grayed. Depending on the remediation action, you will see either specific parameters or no parameters.

\* Required fields

Delete remediation action

If remediation is in progress, the remediation action is not deleted.



Remediation action

AWS-DeleteEbsVolumeSnapshots

AWS-DeleteImage

AWS-DeleteSnapshot

AWS-DetachEBSVolume

AWS-DisablePublicAccessForSecurityGroup

AWS-DisableS3BucketPublicReadWrite

AWS-EnableCloudTrail

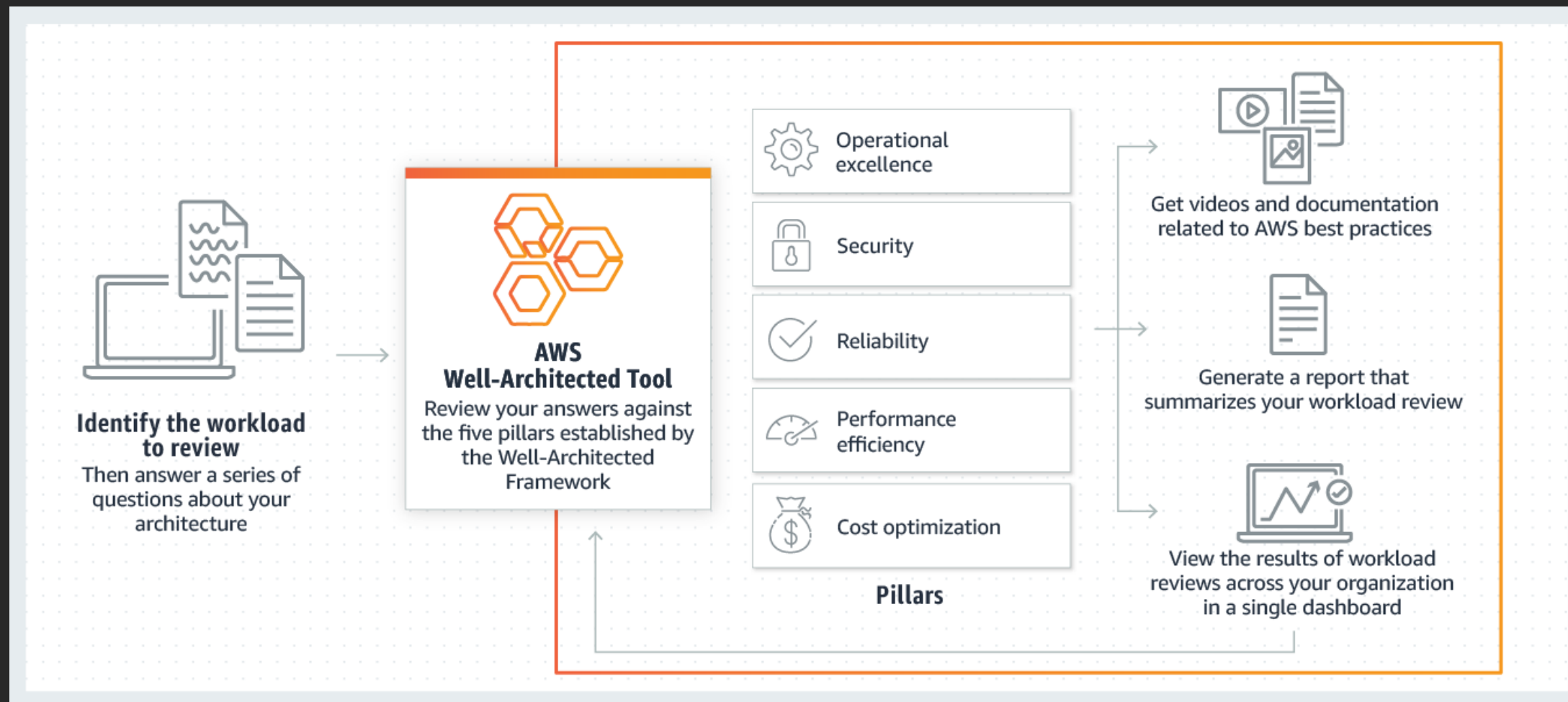
AWS-EnableS3BucketEncryption

# Next steps



# AWS Well-Architected Framework

The [Well-Architected Framework](#) has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on five pillars—operational excellence, security, reliability, performance efficiency, and cost optimization—the Framework provides a consistent approach for customers to evaluate architectures, and implement designs that will scale over time.



# AWS Well-Architected Framework

1. How do you manage credentials and authentication?
2. How do you control human access?
3. How do you control programmatic access?
4. How do you detect and investigate security events?
5. How do you defend against emerging security threats?
6. How do you protect your networks?
7. How do you protect your compute resources?
8. How do you classify your data?
9. How do you protect your data at rest?
10. How do you protect your data in transit?
11. How do you respond to an incident?

# AWS Well-Architected Framework

1. How do you manage credentials and authentication?
2. How do you control human access?
3. How do you control access to your data?
4. How do you detect and respond to security events?
5. How do you defend against attacks?
6. How do you protect your data at rest?
7. How do you protect your data in transit?
8. How do you classify and label your data?
9. How do you protect your data from unauthorized access?
10. How do you protect your data from loss?
11. How do you respond to security events?

## SEC 9. How do you protect your data at rest? [Info](#)

Save and exit

Protect your data at rest by defining your requirements and implementing controls, including encryption, to reduce the risk of unauthorized access or loss.

☒ Question does not apply to this workload [Info](#)

Select from the following

☐ Define data management and protection at rest requirements [Info](#)

☐ Implement secure key management [Info](#)

☐ Enforce encryption at rest [Info](#)

☐ Enforce access control [Info](#)

☐ Provide mechanisms to keep people away from data [Info](#)

☐ None of these [Info](#)

# AWS Well-Architected Framework

- 1. How do you manage credentials and authentication?
- 2. How do you control human access?
- 3. How do you control access to your data?
- 4. How do you detect and respond to unauthorized access?
- 5. How do you define and enforce security requirements?
- 6. How do you protect your data at rest?
- 7. How do you protect your data in transit?
- 8. How do you classify and label your data?
- 9. How do you protect your data from loss?
- 10. How do you protect your data from corruption?
- 11. How do you respond to data breaches?

SEC 9. How do you protect your data at rest?[Info](#)

Save and exit

Protect your data at rest by defining your requirements and implementing controls, including encryption, to reduce the risk of unauthorized access or loss.

☒ Question does not apply to this workload [Info](#)

Select from the following

☐ Define data management and protection controls

☐ Implement secure key management [Info](#)






☐ Enforce encryption at rest [Info](#)

☐ Enforce access control [Info](#)

☐ Provide mechanisms to keep people away from sensitive data

☐ None of these [Info](#)

## Question status

	High risk	1
	Medium risk	0
	No improvements identified	0
	Not Applicable	0
	Unanswered	10

# AWS Well-Architected Framework

1. How do you manage credentials and authentication?
2. How do you control human access?
3. How do you control access to your data?
4. How do you detect and respond to unauthorized access?
5. How do you define and enforce security requirements?
6. How do you protect your data at rest?
7. How do you protect your data in transit?
8. How do you classify and label your data?
9. How do you protect your data from unauthorized access?
10. How do you protect your data from loss?
11. How do you respond to security incidents?

SEC 9. How do you protect your data at rest?[Info](#)

Save and exit

Protect your data at rest by defining your requirements and implementing controls, including encryption, to reduce the risk of unauthorized access or loss.

☒ Question does not apply to this workload [Info](#)

Select from the following

☐ Define data management and protection

☐ Implement secure key management [Info](#)

☐ Enforce encryption at rest [Info](#)

☐ Enforce access control [Info](#)

☐ Provide mechanisms to keep people away from sensitive data

☐ None of these [Info](#)

## Question status



High risk

1



Medium risk

0



No issue



Not applicable



Unknown

## Pillars

Name	Questions answered	High risks
<a href="#">Operational Excellence</a>	0/9	0
<a href="#">Security</a>	1/11	1
<a href="#">Reliability</a>	0/9	0
<a href="#">Performance Efficiency</a>	0/8	0
<a href="#">Cost Optimization</a>	0/9	0

# Learn security with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate cloud security skills



30+ free digital courses cover topics related to cloud security, including Introduction to Amazon GuardDuty and Deep Dive on Container Security



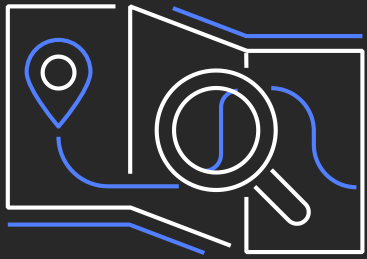
Classroom offerings, such as Security Engineering on AWS, feature AWS expert instructors and hands-on activities



Validate expertise with the AWS Certified Security – Specialty exam

Visit the security learning path at <https://aws.training/security>

# AWS Training and Certification



## Training for the whole team

Explore tailored learning paths for customers and partners



## Flexibility to learn your way

Build cloud skills with 550+ free digital training courses, or dive deep with classroom training



## Validate skills with AWS Certification

Demonstrate expertise with an industry-recognized credential



## Education programs

Find entry-level cloud talent with AWS Academy and AWS re/Start

[aws.amazon.com/training](https://aws.amazon.com/training)

# Thank you!

Myles Hosford