

AWS
re:Invent

SEC204-S

Strong security made simple: Putting all the pieces together



Mark Nunnikhoven

Vice President, Cloud Research at Trend Micro

[@marknca](#)

The cloud simplifies security.

The cloud simplifies security.

* When you understand how it works

The cloud simplifies security.

* When you understand how it works

** Compared to traditional environments

The cloud simplifies security.

* When you understand how it works

** Compared to traditional environments

*** Depending on how much you pay attention for the next 60m

The goal of cybersecurity

**Make sure that systems
work as intended**

The goal of cybersecurity

**Make sure that systems
work as intended
...and only as intended**

The Shared Responsibility Model

Data

Application

OS

Virtualization

Infrastructure

Physical

On-premises
(Traditional)

The Shared Responsibility Model

Data

Data

Application

Application

OS

OS

Virtualization

Virtualization

Infrastructure

Infrastructure

Physical

Physical

On-premises
(Traditional)

Infrastructure
(IaaS)

The Shared Responsibility Model

Data
Application
OS
Virtualization
Infrastructure
Physical

On-premises
(Traditional)

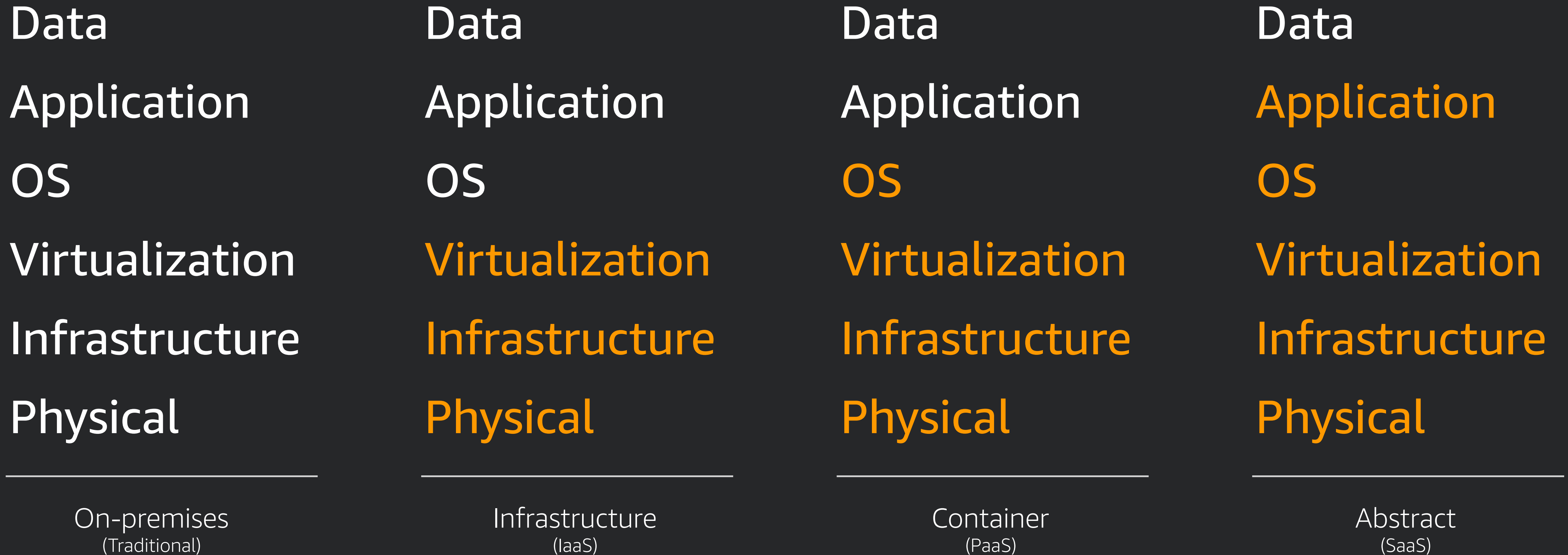
Data
Application
OS
Virtualization
Infrastructure
Physical

Infrastructure
(IaaS)

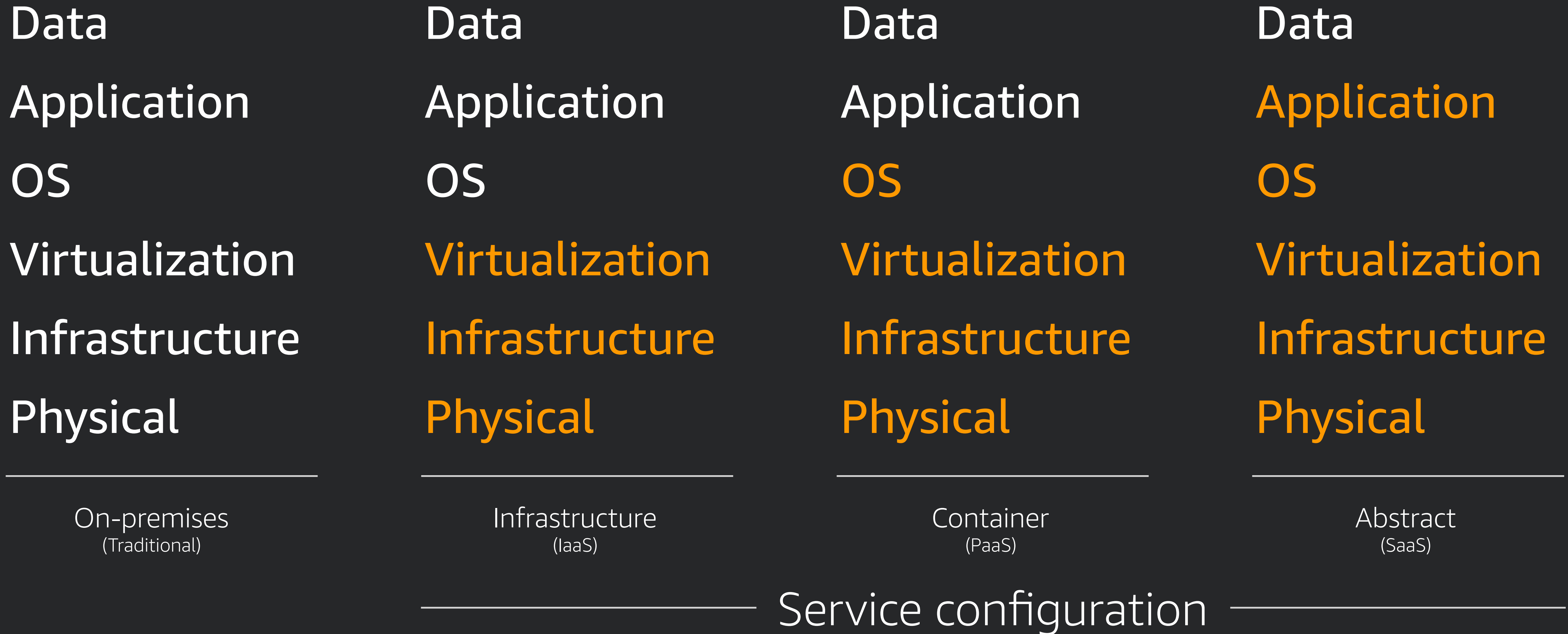
Data
Application
OS
Virtualization
Infrastructure
Physical

Container
(PaaS)

The Shared Responsibility Model



The Shared Responsibility Model







AWS Compliance Programs

Global

Global

United States

Canada

Asia Pacific

Europe

Privacy



CSA



ISO 9001



ISO 27001



ISO 27017



ISO 27018



AWS Compliance Programs

Global

Global

United States

Canada

Asia Pacific

Europe

Privacy



aws.amazon.com/compliance

CSA

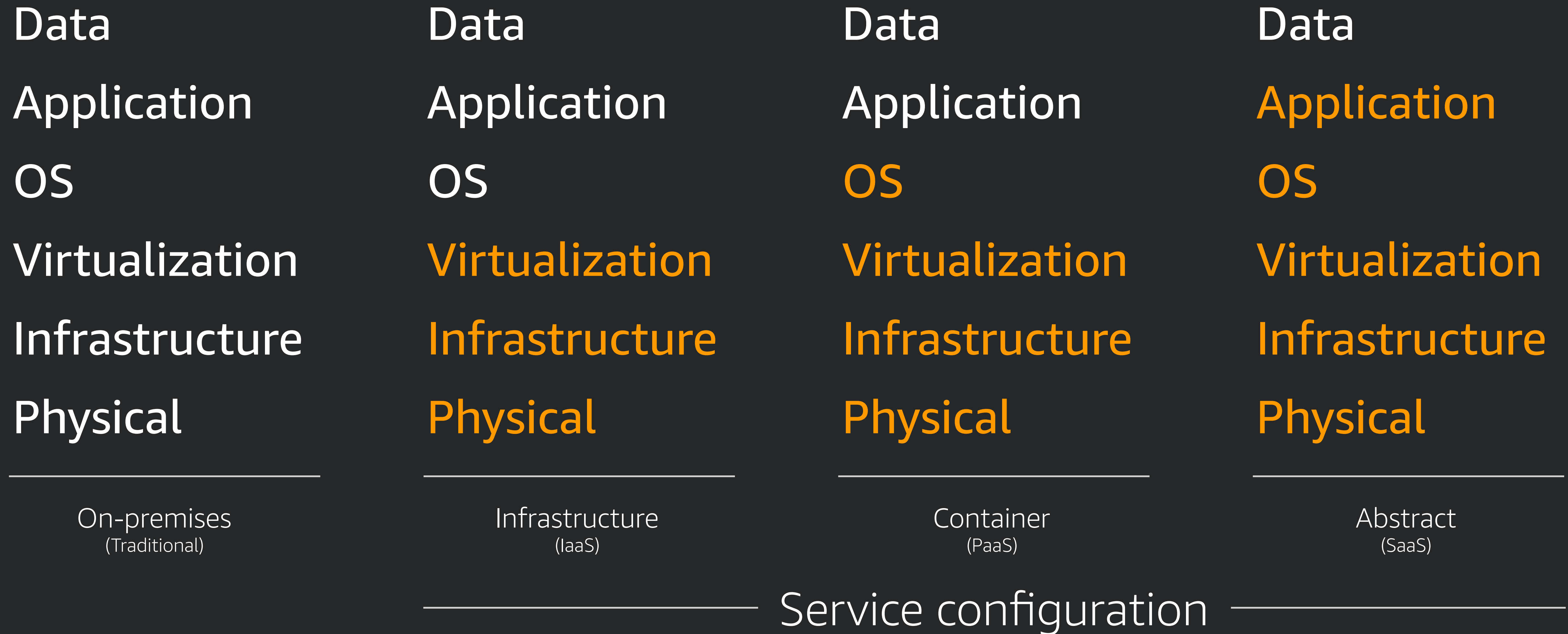
ISO 9001

ISO 27001

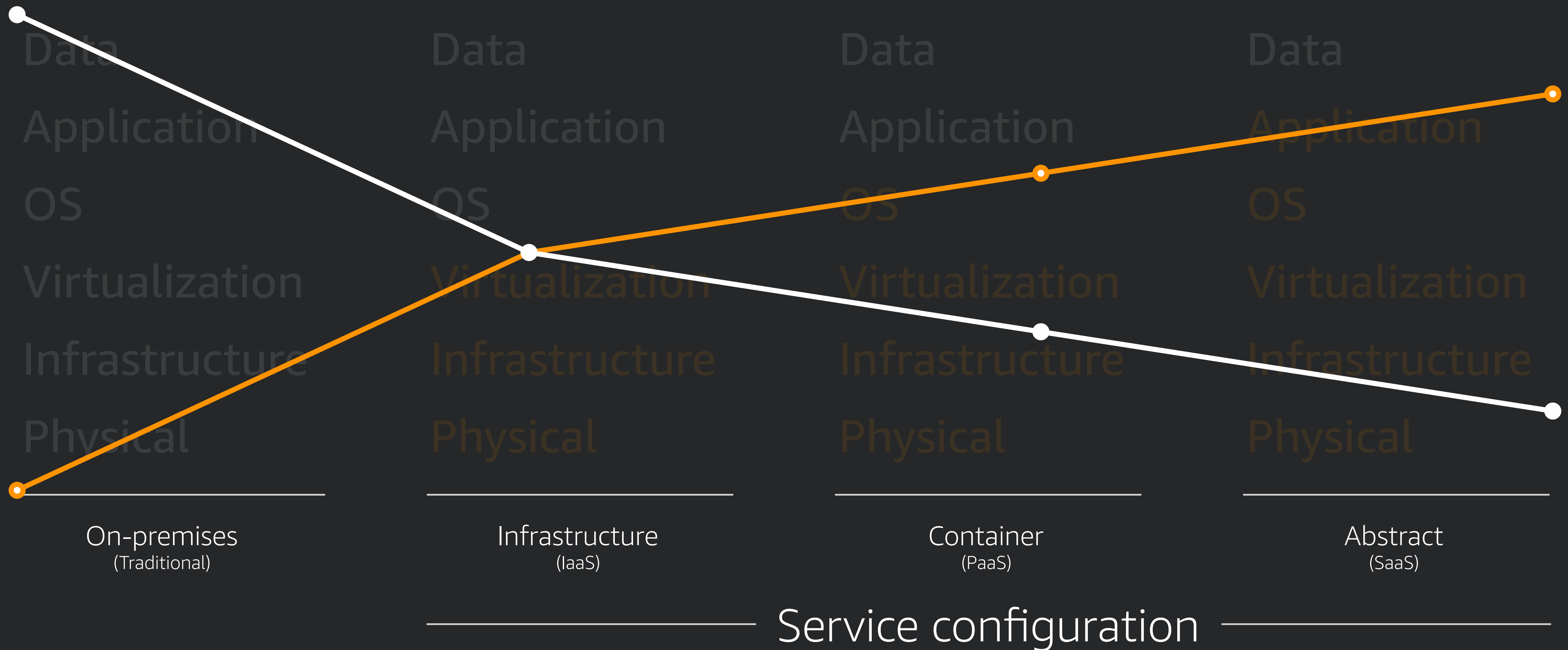
ISO 27017

ISO 27018

The Shared Responsibility Model

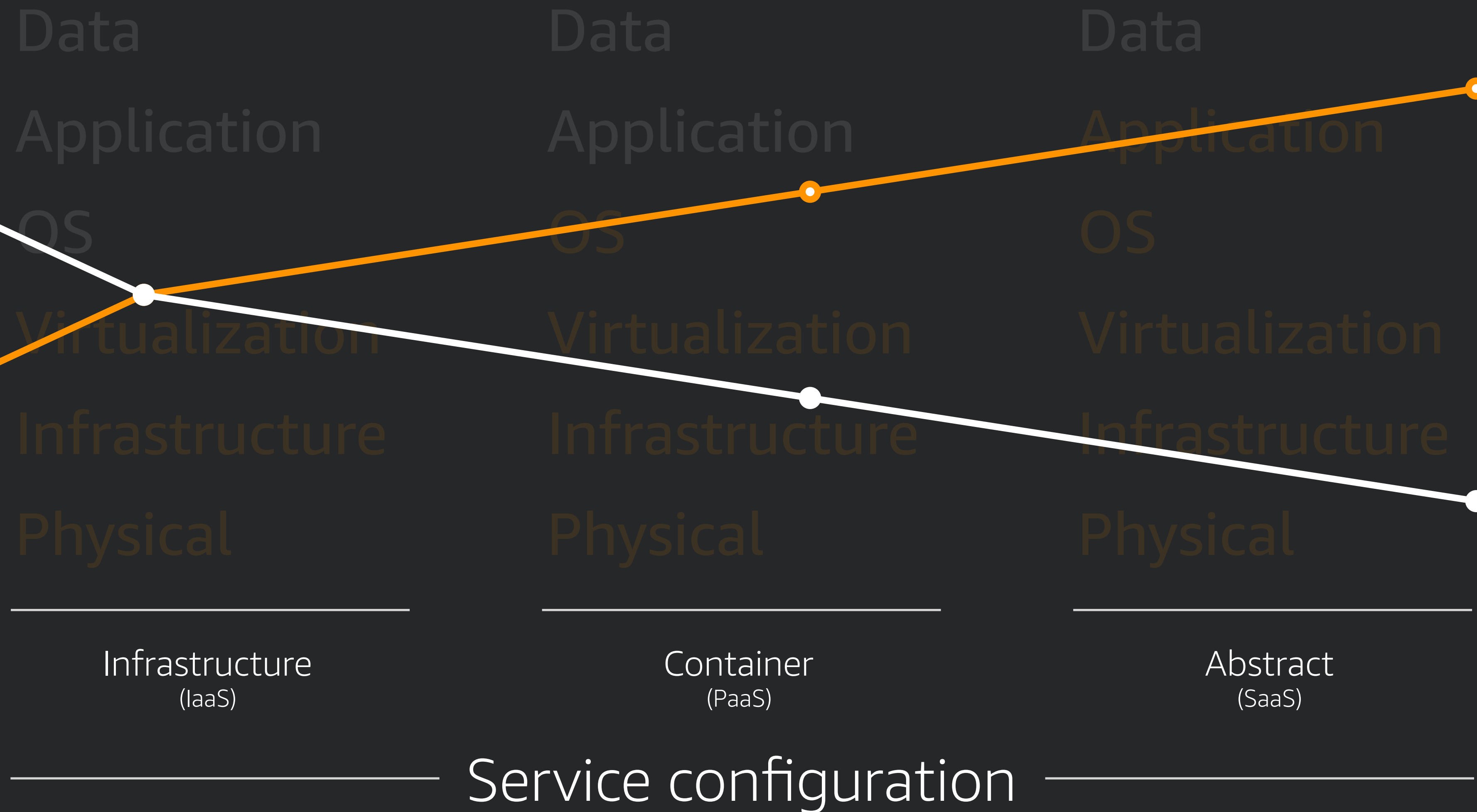


The Shared Responsibility Model



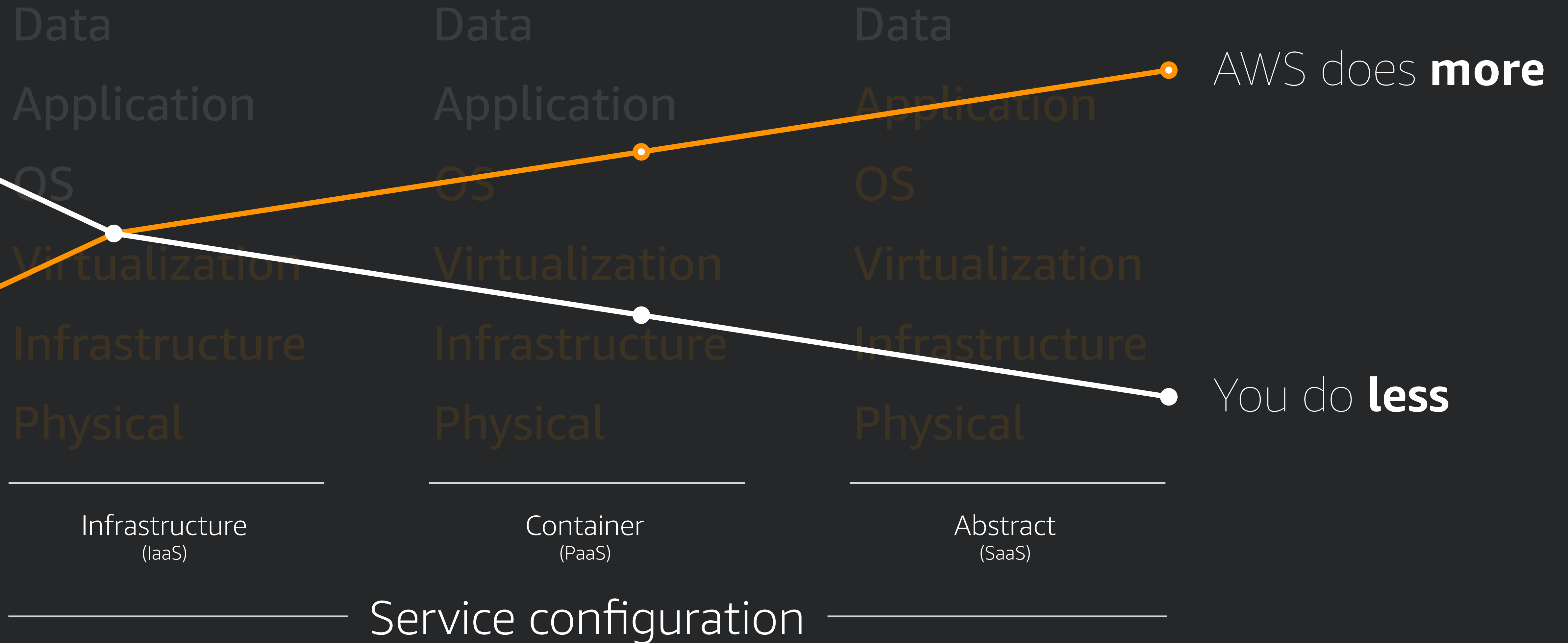
■ Your responsibility ■ AWS' responsibility

The Shared Responsibility Model



■ Your responsibility ■ AWS' responsibility

The Shared Responsibility Model



■ Your responsibility ■ AWS' responsibility

What's stopping us?

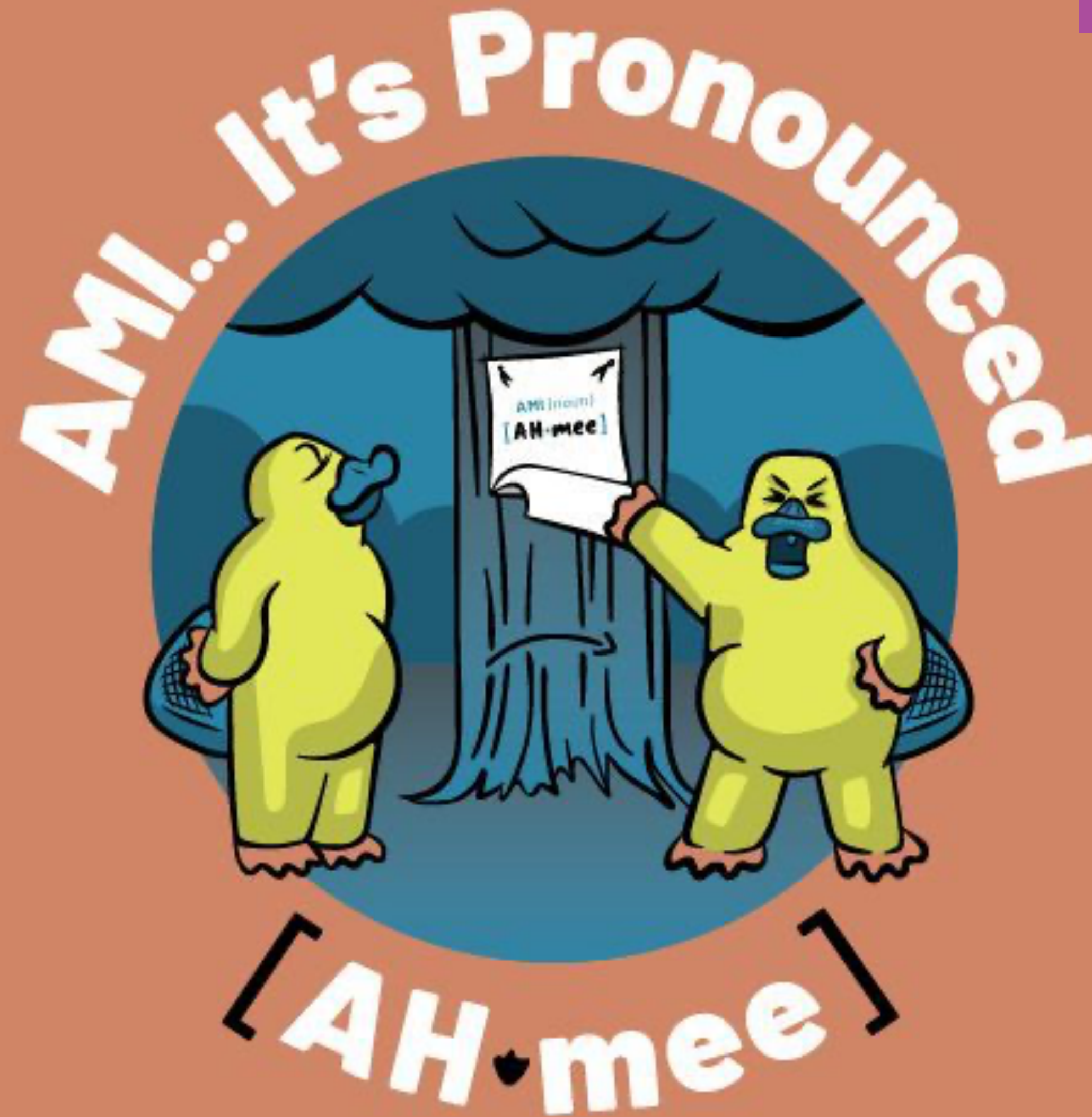
Hackers



Nation State



Insider Threats





Mistakes & misconfigurations



Our goal

**Make sure that systems
work as intended and
only as intended**

Largest risk

**Mistakes &
misconfigurations**

Can I learn from others?

Cloud Adoption Framework

Cloud Adoption Framework



Business



People



Governance

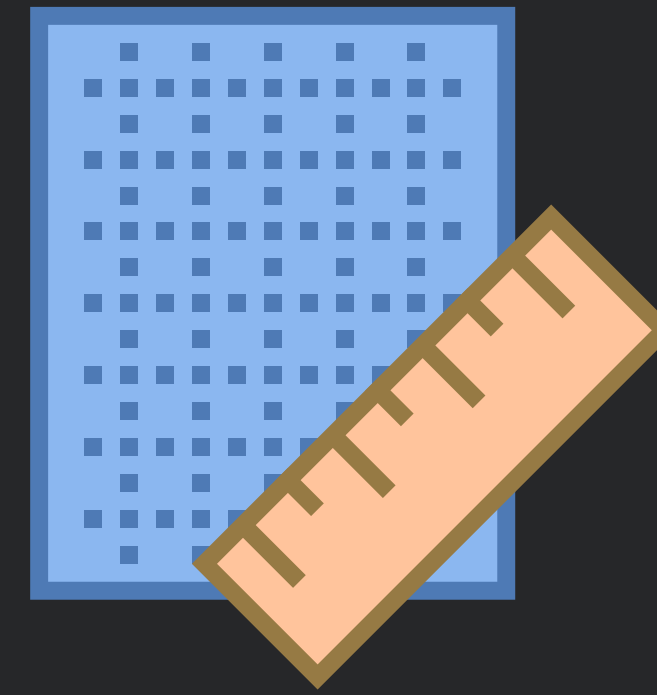
Cloud Adoption Framework



Business



People



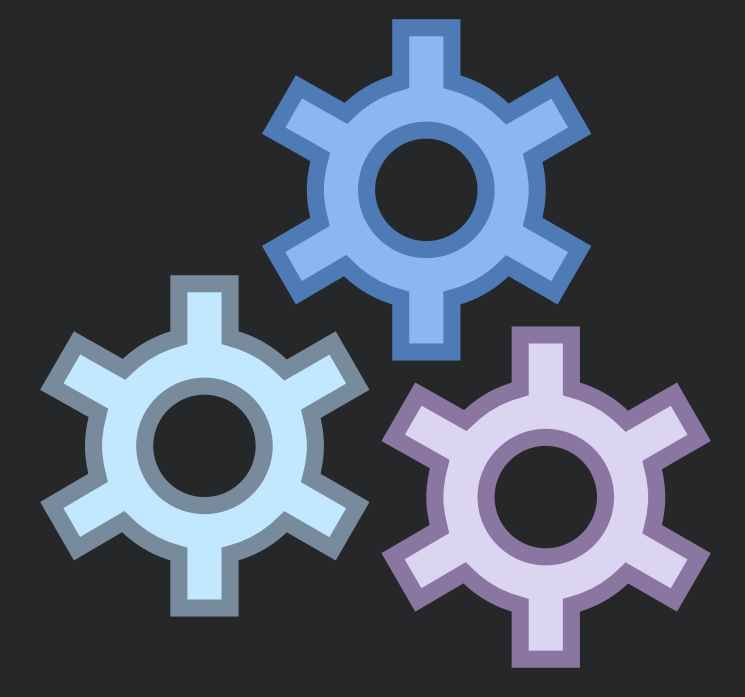
Platform



Security



Governance



Operations

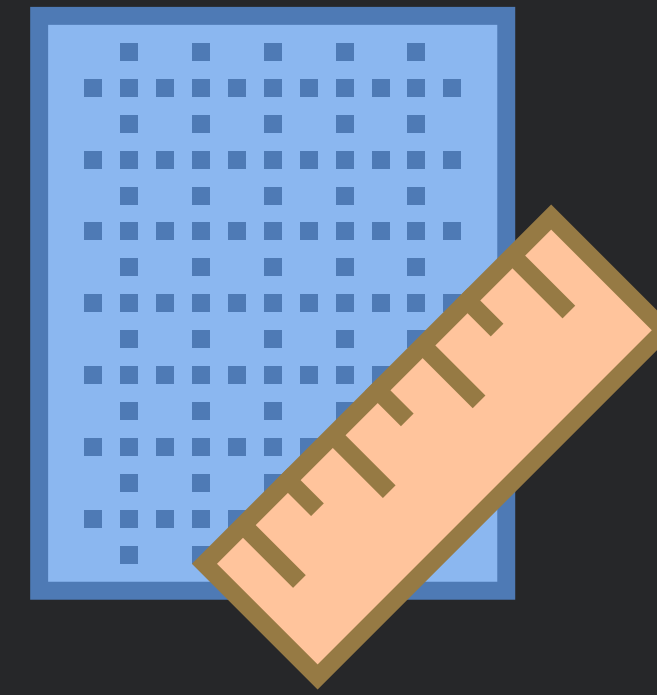
Cloud Adoption Framework



Business



People



Platform

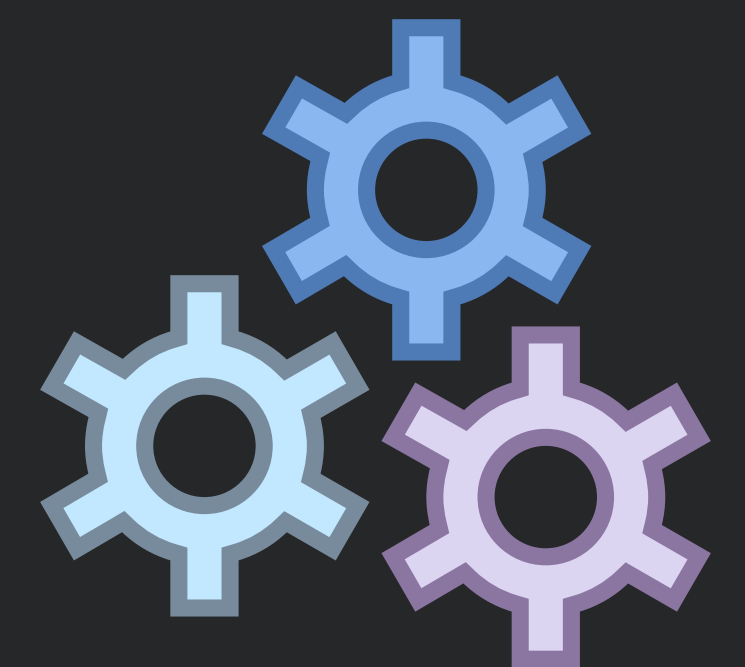


Security



Governance

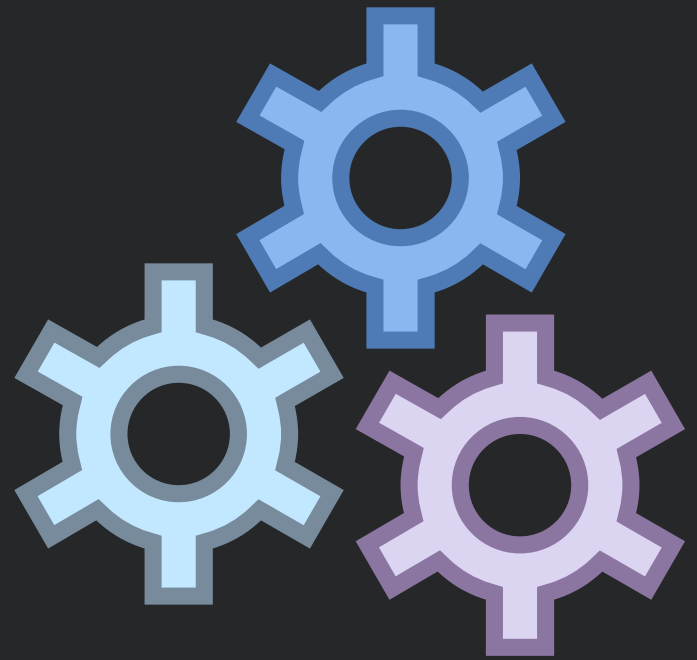
Builds an action plan



Operations

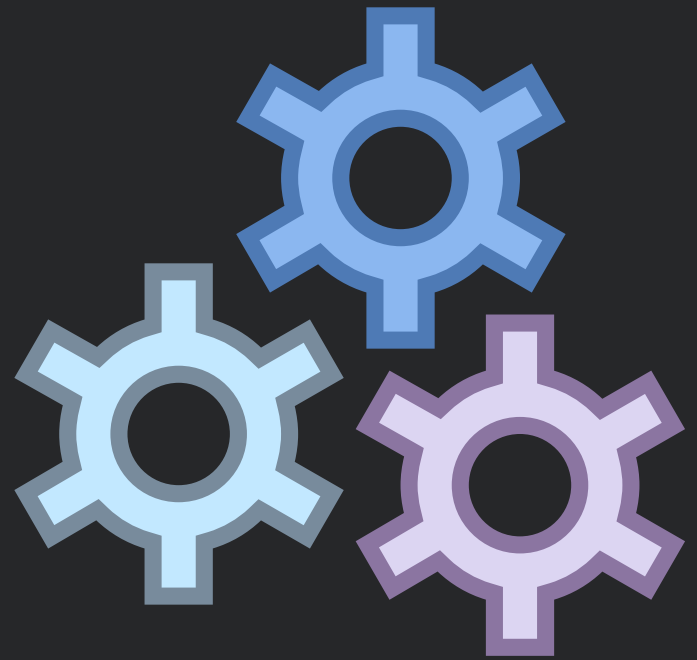
AWS Well-Architected Framework

AWS Well-Architected Framework



Operational
Excellence

AWS Well-Architected Framework

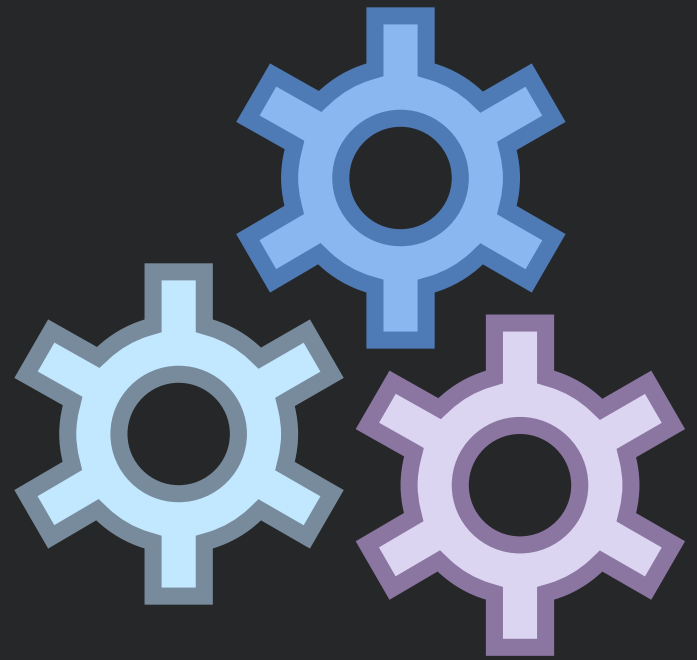


Operational
Excellence



Security

AWS Well-Architected Framework



Operational
Excellence

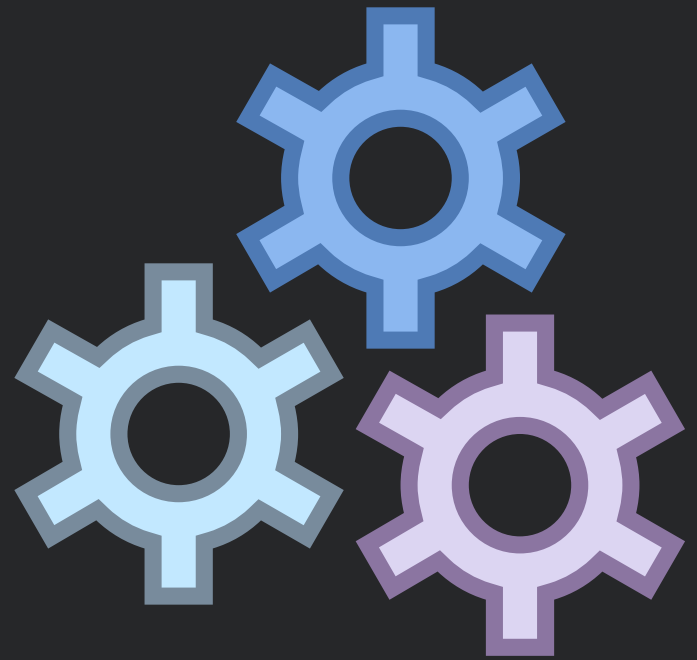


Security



Reliability

AWS Well-Architected Framework



Operational
Excellence



Security

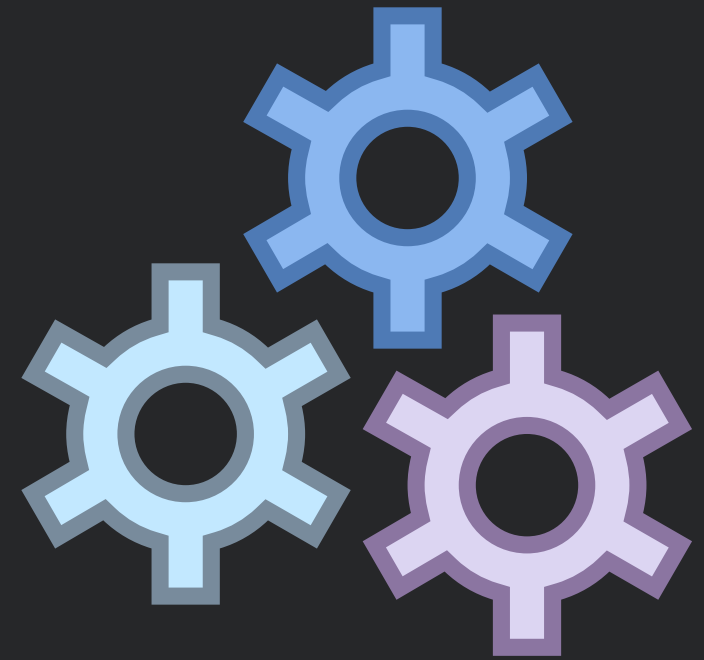


Reliability



Performance
Efficiency

AWS Well-Architected Framework



Operational
Excellence



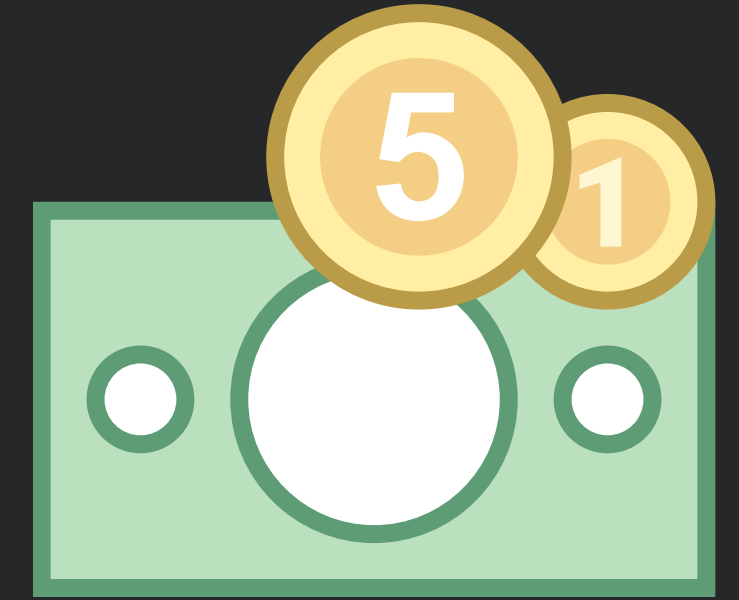
Security



Reliability

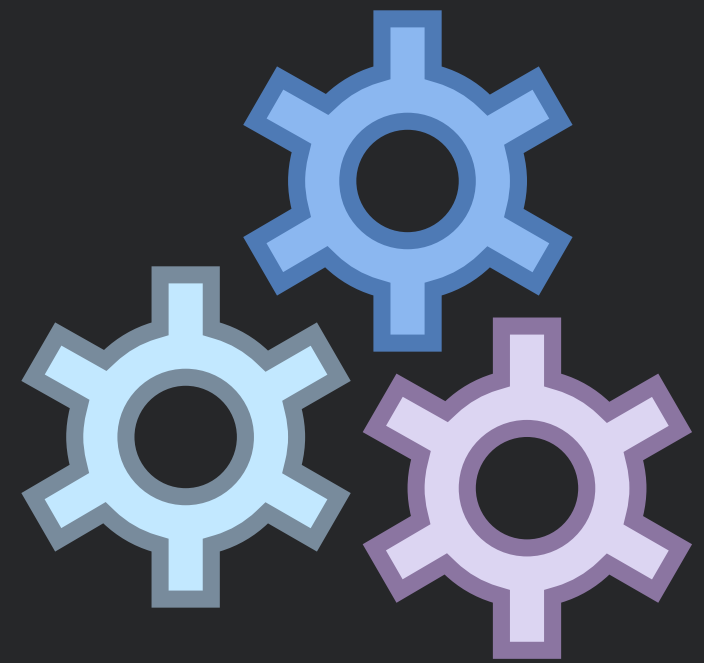


Performance
Efficiency



Cost
Optimization

AWS Well-Architected Framework



Operational
Excellence



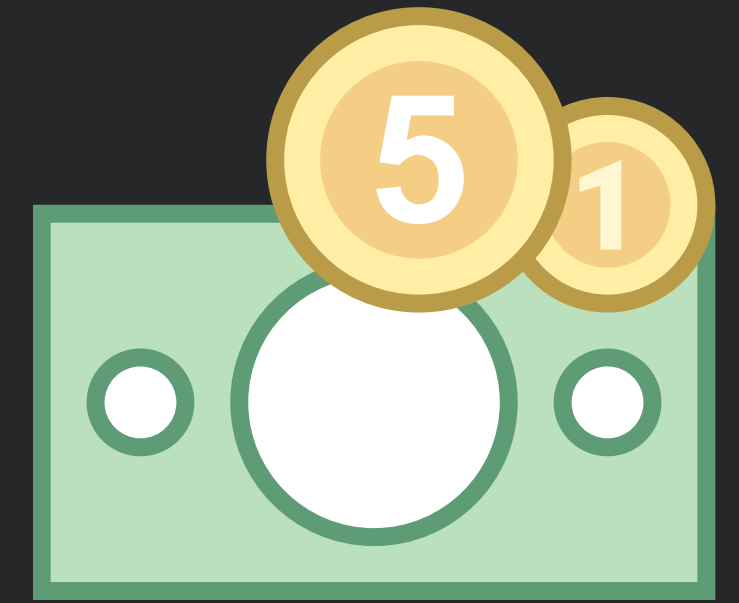
Security



Reliability



Performance
Efficiency



Cost
Optimization

Helps you make smart trade-offs

Modern Application Design

Modern Application Design

Secure

Resilient

Elastic

Modular

Automated

Interoperable

Modern Application Design

Secure

Resilient

Elastic

Modular

Automated

Interoperable



Re-host

Modern Application Design

Secure

Resilient

Elastic

Modular

Automated

Interoperable



Re-host

Re-platform

Modern Application Design

Secure

Resilient

Elastic

Modular

Automated

Interoperable



Re-host

Re-platform

Re-factor

Modern Application Design

Secure

Resilient

Elastic

Modular

Automated

Interoperable



Re-host

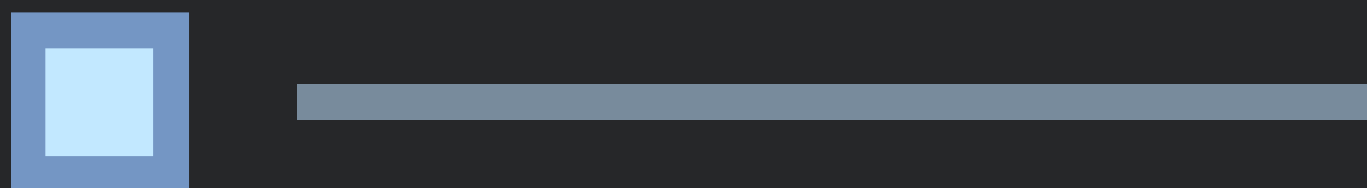
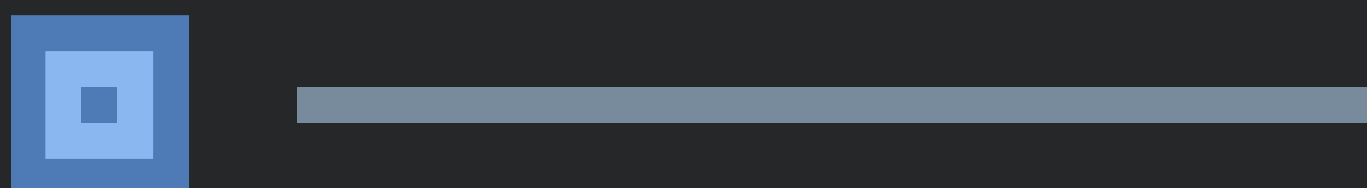
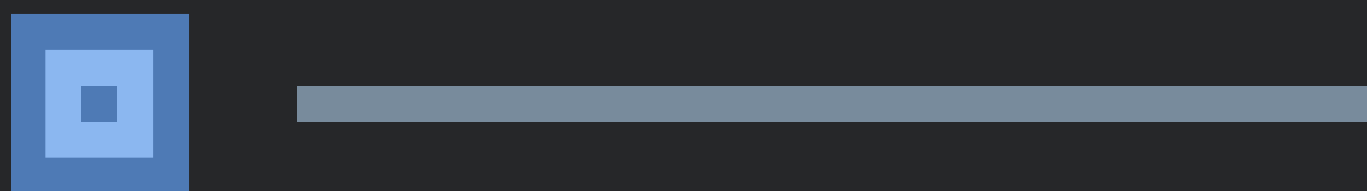
Re-platform

Re-factor

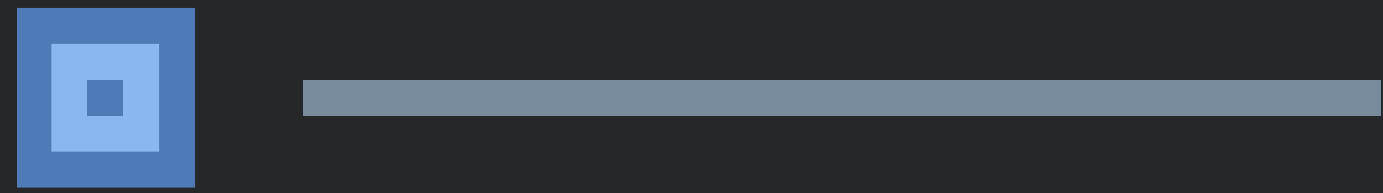
Re-invent

CIS AWS Foundations

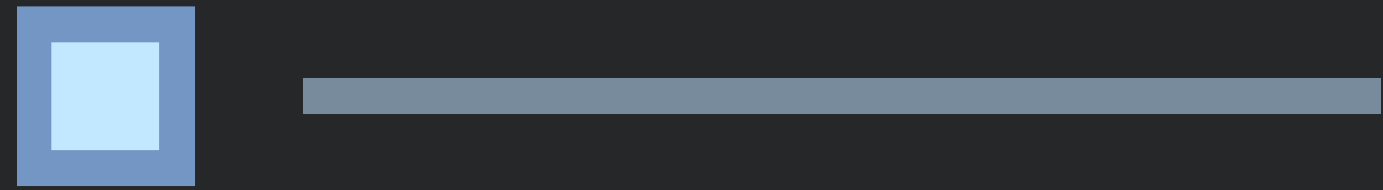
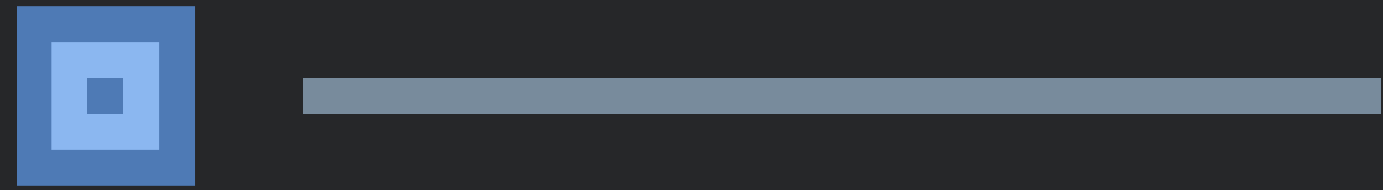
CIS AWS Foundations



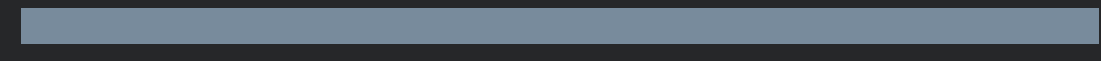
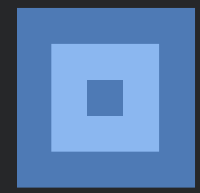
CIS AWS Foundations



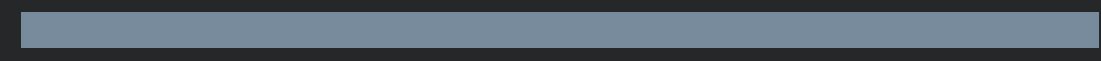
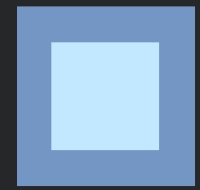
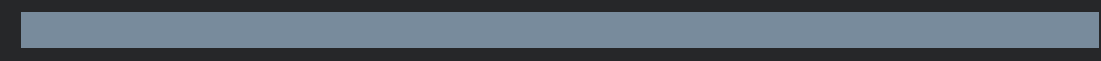
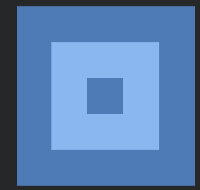
Prescriptive guidance



CIS AWS Foundations



Prescriptive guidance



Checklist of @TODOs

What happened?

Auditing



	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov
	7.02	18.44	20.77	5.86	3.96	6.6	1	0	11.2
	0	3	1.5	4	0.37	0	0.5		
	3.11	0	0.5	0	0.3	1.21	0		
	3.13	2.7	53.32	2.36	0.3	1.21	0	22.06	2.24
	3.81	9964.9	9964.76	11065	13945.79	14851.18	17625.9	19138.99	20234.06
	9.96	149.99	211.18	54.91	453.65	229.93	59.97	139.96	299.93
Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	
2.65	13359.77	14016.76	1094.89	12901.21	12625.01	13686.73	213.05	12941.58	1
5.57	925.61	1232.46	1046.6	1152.52	1210.19	2180.86	2100	1938.61	
1.89	2990.29	3408.59	445.21	3400	2956.12	3779.39	325.32	3003.2	
2.52	340.83	445.02	491.75	442.9	443.92	603	774.39	696.84	
4.23	8953.85	8323.28	228.76	5744.81	4654.11	6468.39	6983.6	6088.4	
92.9	1675.65	1859.25	78.12	1914.77	1830.85	2268.69	5165.45	2480.94	
1.67	911.7	860.27	53.35	979.59	847.94	1067.62	1163.01	1107.32	
7.45	482.46	561	583	515.79	558.06	645.75	549	589.68	
5.55	419.47	390.96	392	403.78	402.73	329.75	367.56	313.65	
59.8	57.72	80.6	47	87.88	35.36	74	85.28	56.68	
4.08	1.24	0.99		17.86	1.88	37	1.3	0.71	
0.75	1	0.75		0.25	3.70	2.5	0	2.5	
4.74	196.66	313.82	14	52		710.8	794.06	738.56	
9.24	173.81	308	22.03	191.87	172.88	153.71	119.41	121.48	
0.2	0.2		14.44	0	20.7	0.19	0	7.47	
2.35	30.8		16.55	23.4	30.25	28.35	45.7	28.85	



AWS CloudTrail



AWS CloudTrail

What happened in your account
+
Who/what made it happen



What happened in your account

+

Who/what made it happen



What happened in your account

+

Who/what made it happen

- Signed audit trail of API calls




What happened in your account

+

Who/what made it happen

- Signed audit trail of API calls
- Data source for other key services



What happened in your account
+

Who/what made it happen

- Signed audit trail of API calls
- Data source for other key services
- On by default



What happened in your account
+

Who/what made it happen

- Signed audit trail of API calls
- Data source for other key services
- On by default
- Log delivery in ~2–4m but no guarantee

Who's there?

Identity

Visas Sorties / Salidas

← LFT LONDRES
A 138

↑

Canada
104

SEP 07 2008

CALGARY
701

DEPARTMENT OF HOMELAND SECURITY
CLASS
UNMI

JAN 1

6E

Entrées / Entradas Visas Sorties / Salidas

Immigration Canada

2008

PASSPORT



The Principle of Least Privilege



The Principle of Least Privilege



Grant **only** those privileges which are **essential** to perform the intended function



AWS IAM



AWS IAM

Who are you?

+

What are you allowed to do?



Who are you?

+

What are you allowed to do?



Who are you?

+

What are you allowed to do?

- Managed users and roles



Who are you?

+

What are you allowed to do?

- Managed users and roles
- Assign permissions to policies, users, or roles



Who are you?

+

What are you allowed to do?

- Managed users and roles
- Assign permissions to policies, users, or roles
- Granular permissions for each service



Who are you?

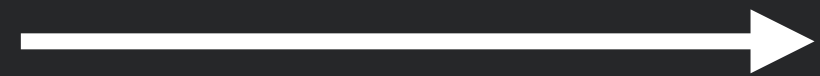
+

What are you allowed to do?

- Managed users and roles
- Assign permissions to policies, users, or roles
- Granular permissions for each service
- Federation with existing directories available



User



Permission



S3 Bucket

Works fine
Unmanageable a scale
Not granular enough



User



Permission



S3 Bucket



User



Role

Permission



S3 Bucket



AWS Identity and Access Management (IAM)



AWS Identity and Access Management (IAM)

SEC209

Getting started with AWS Identity



AWS Identity and Access Management (IAM)

SEC209

Getting started with AWS Identity

SEC316

Access control confidence: Grant the right access to the right things

Website

IAM Best Practices

How can I protect my network?



Amazon VPC



Amazon VPC

Your own slice of the AWS Cloud



Your own slice of the *AWS* Cloud



Your own slice of the AWS Cloud

- Controllable routing, IP space, subnetting, and access control



Your own slice of the AWS Cloud

- Controllable routing, IP space, subnetting, and access control
- VPC Endpoints allows access to AWS services



Your own slice of the AWS Cloud

- Controllable routing, IP space, subnetting, and access control
- VPC Endpoints allows access to AWS services
- AWS PrivateLink connects to 3rd party SaaS'



Your own slice of the AWS Cloud

- Controllable routing, IP space, subnetting, and access control
- VPC Endpoints allows access to AWS services
- AWS PrivateLink connects to 3rd party SaaS'
- AWS Direct Connect connects to on-premises



AWS Transit Gateway



AWS Transit Gateway

Make connecting everything easier



Make connecting everything easier



Make connecting everything easier

- If you have multiple VPCs or will soon, Transit Gateway is a simpler way to connect



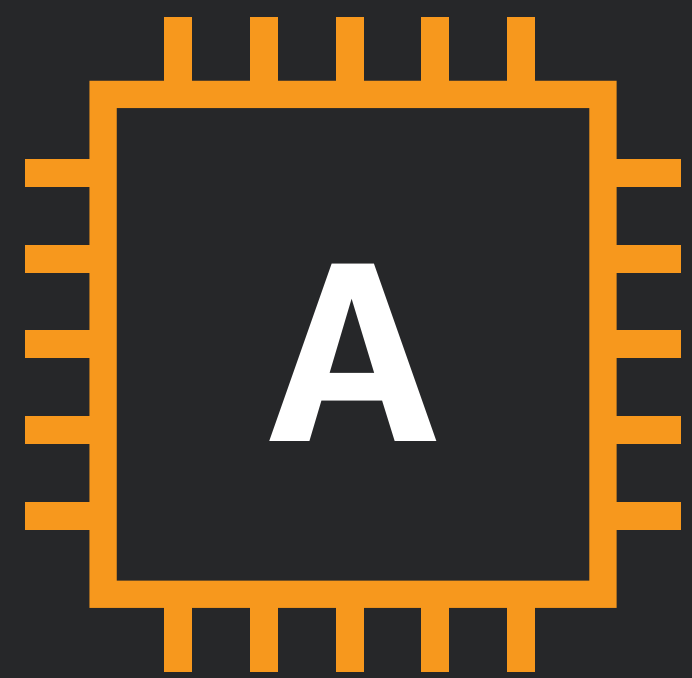
Make connecting everything easier

- If you have multiple VPCs or will soon, Transit Gateway is a simpler way to connect
- Simplified advanced network design

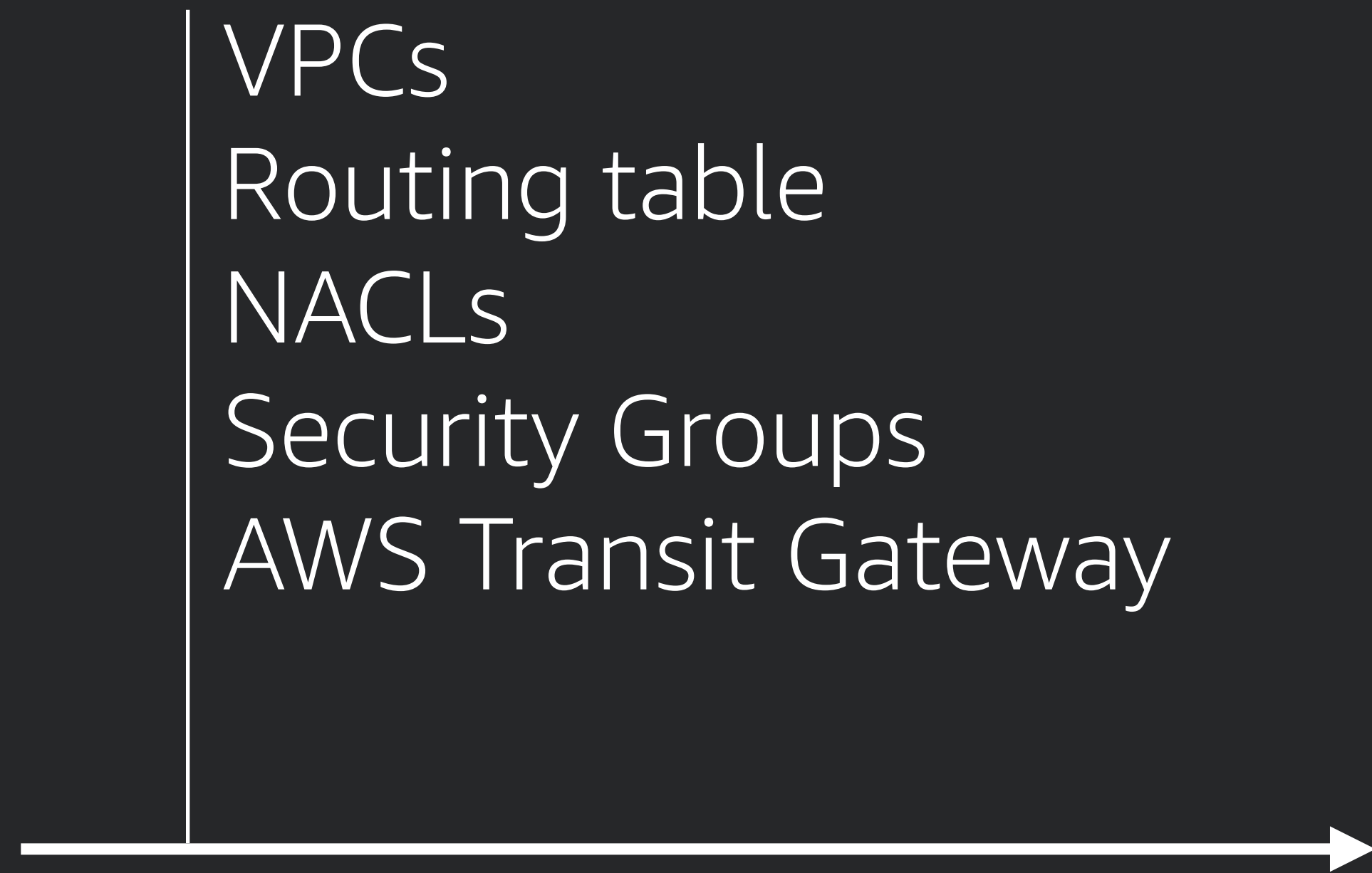


Make connecting everything easier

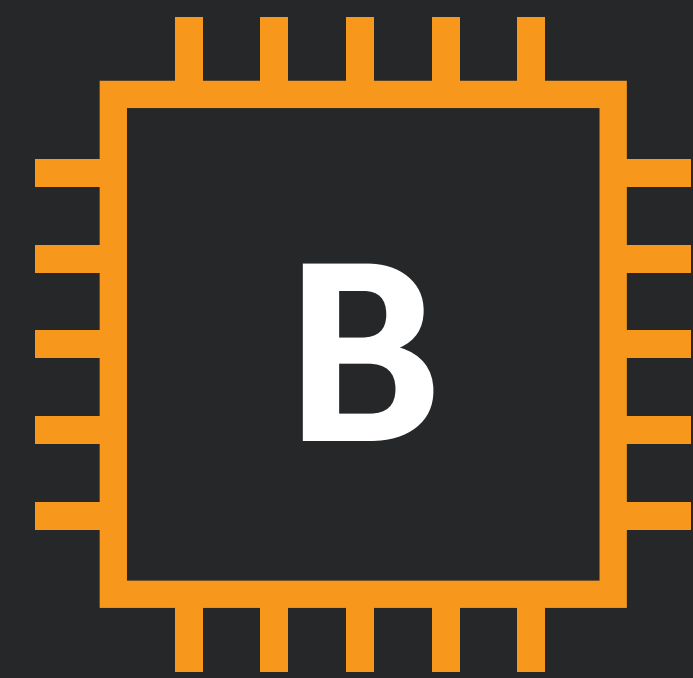
- If you have multiple VPCs or will soon, Transit Gateway is a simpler way to connect
- Simplified advanced network design
- Use VPC Peering at small scale



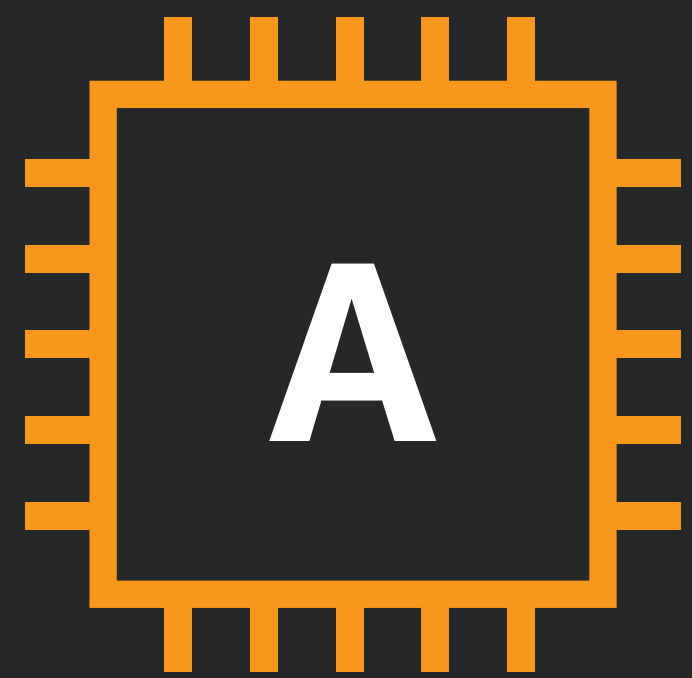
EC2 Instance



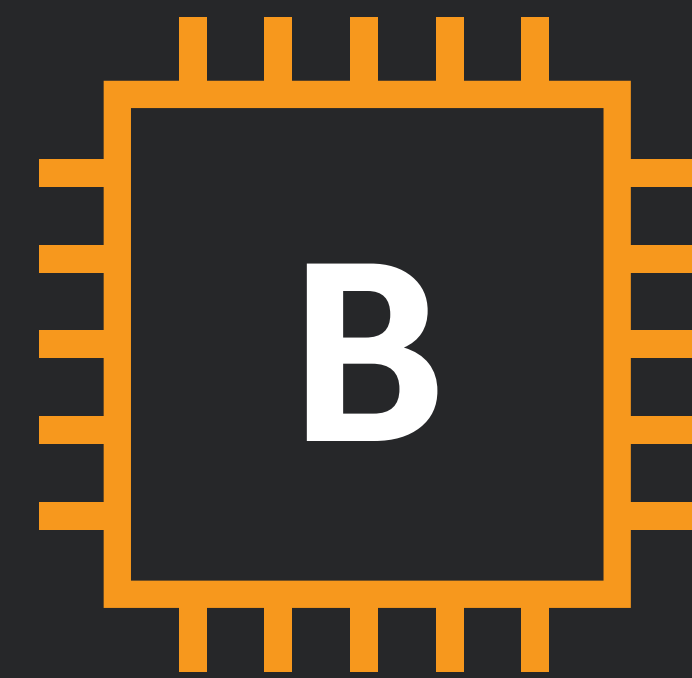
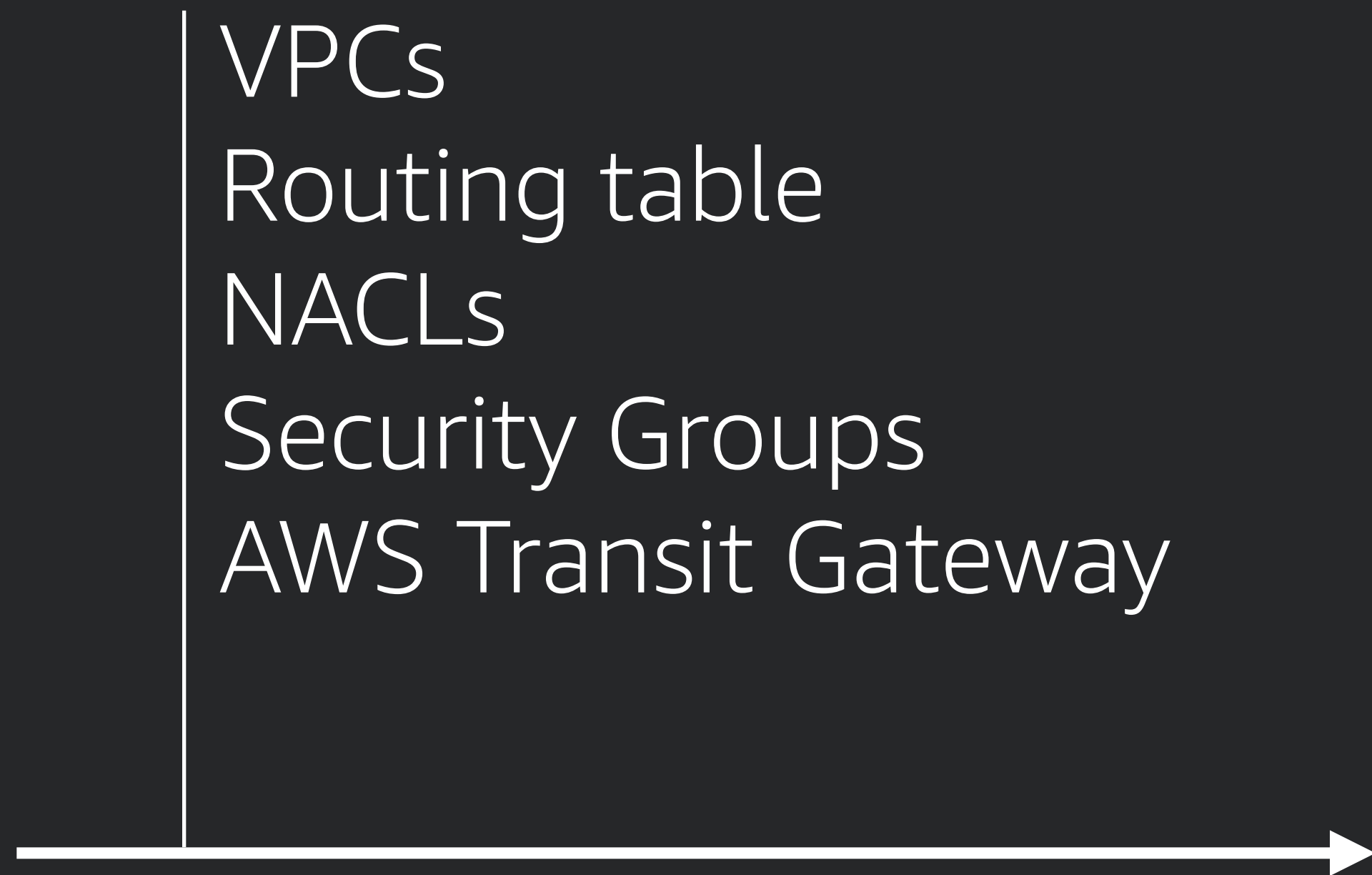
VPCs
Routing table
NACLs
Security Groups
AWS Transit Gateway



EC2 Instance



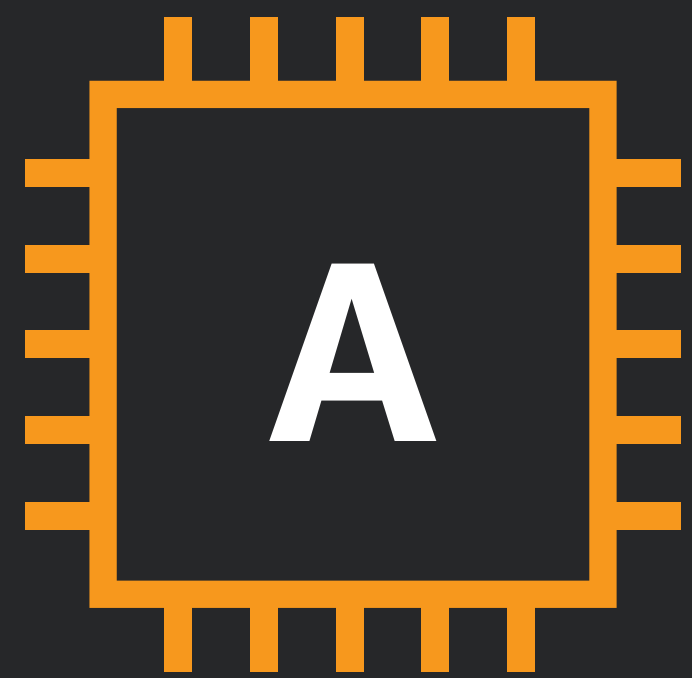
EC2 Instance



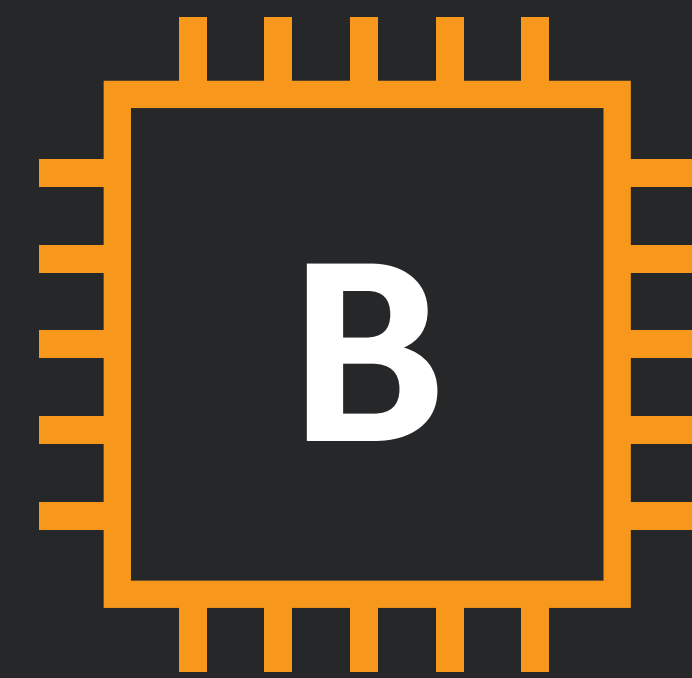
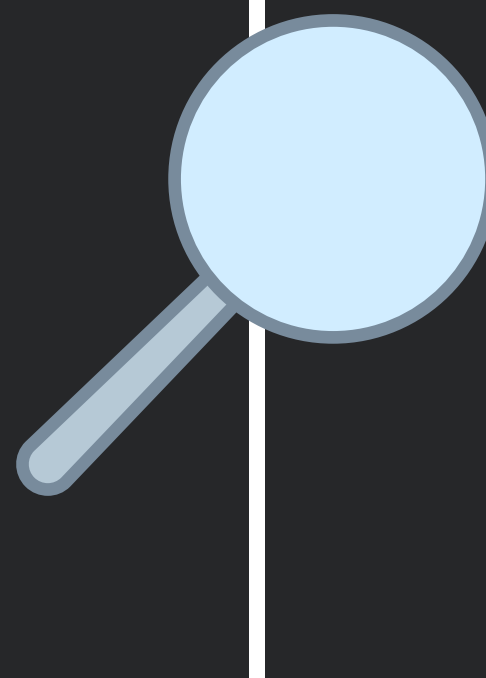
EC2 Instance

Is **A** allowed to talk to **B**?

VPCs
Routing table
NACLs
Security Groups
AWS Transit Gateway



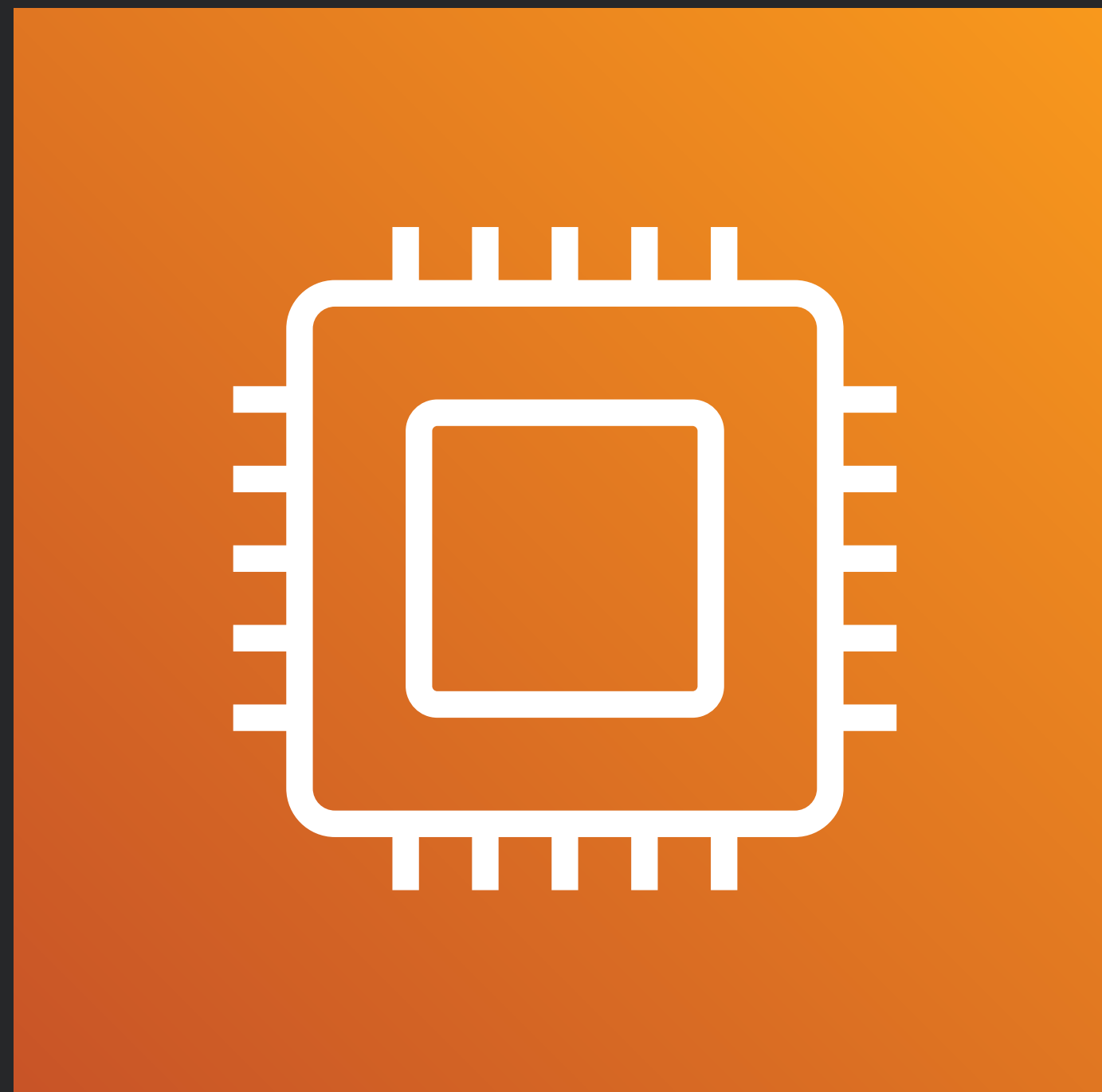
EC2 Instance



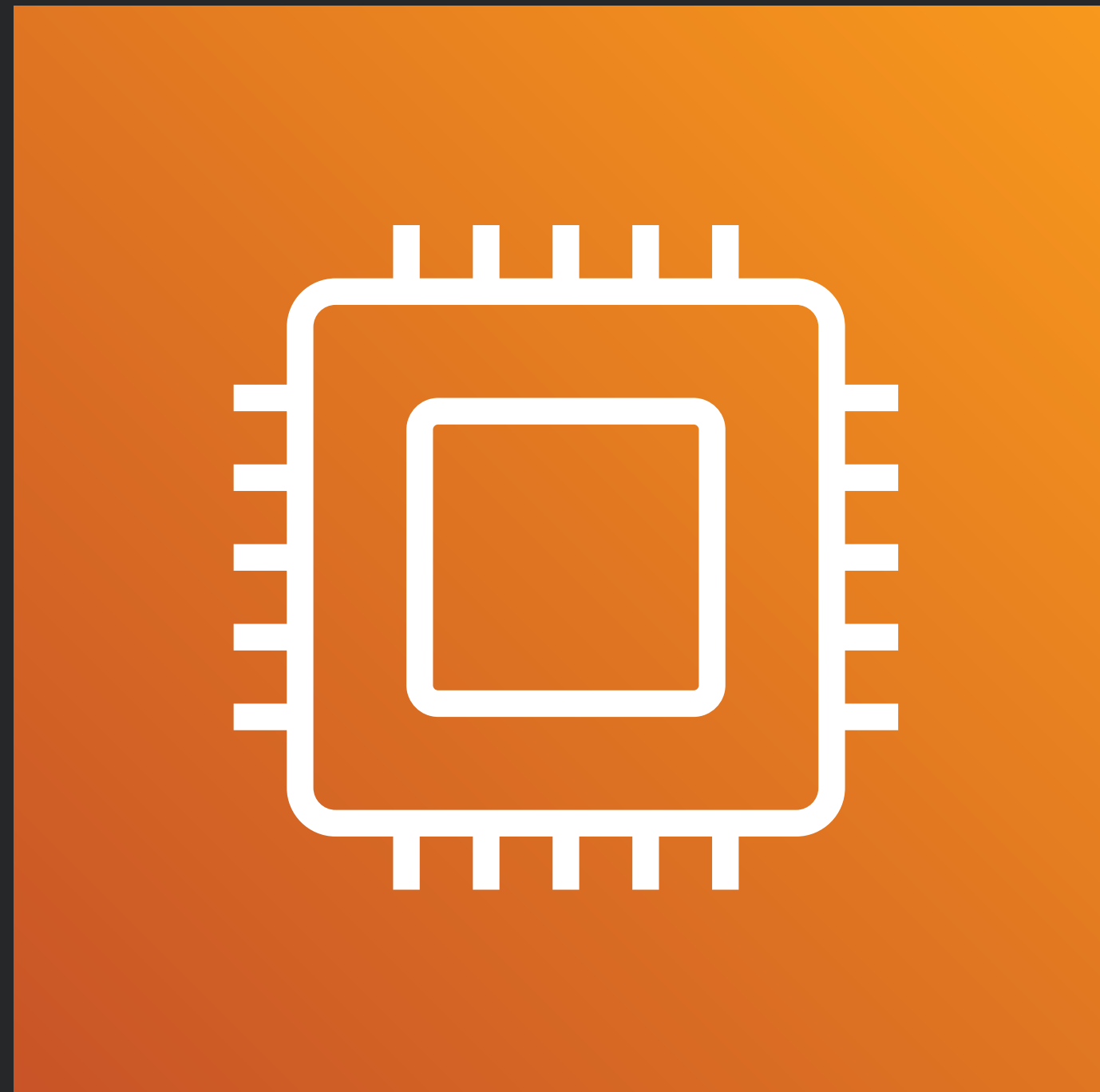
EC2 Instance

What are they saying? **IPS**

Compute

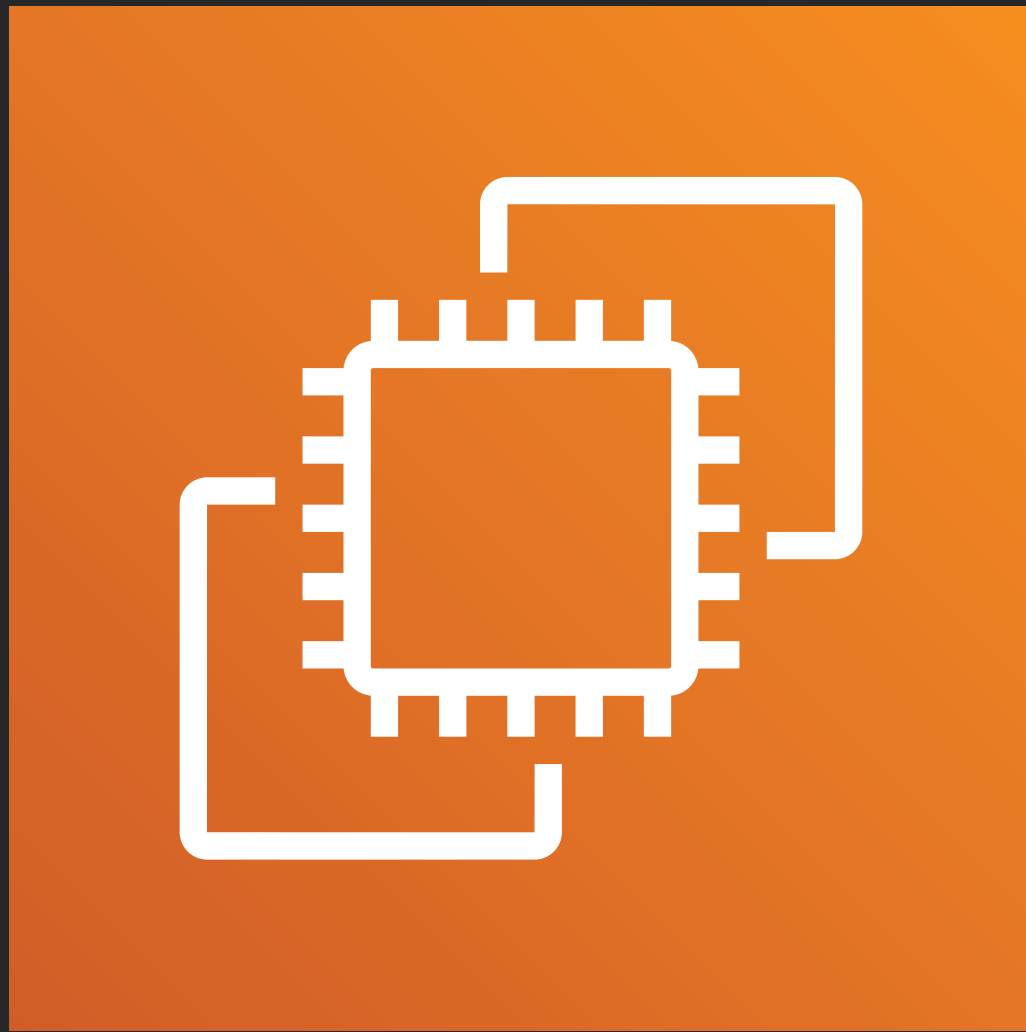


Compute



Compute

Running code in the cloud



Amazon EC2

.....
Instances

Data

Application

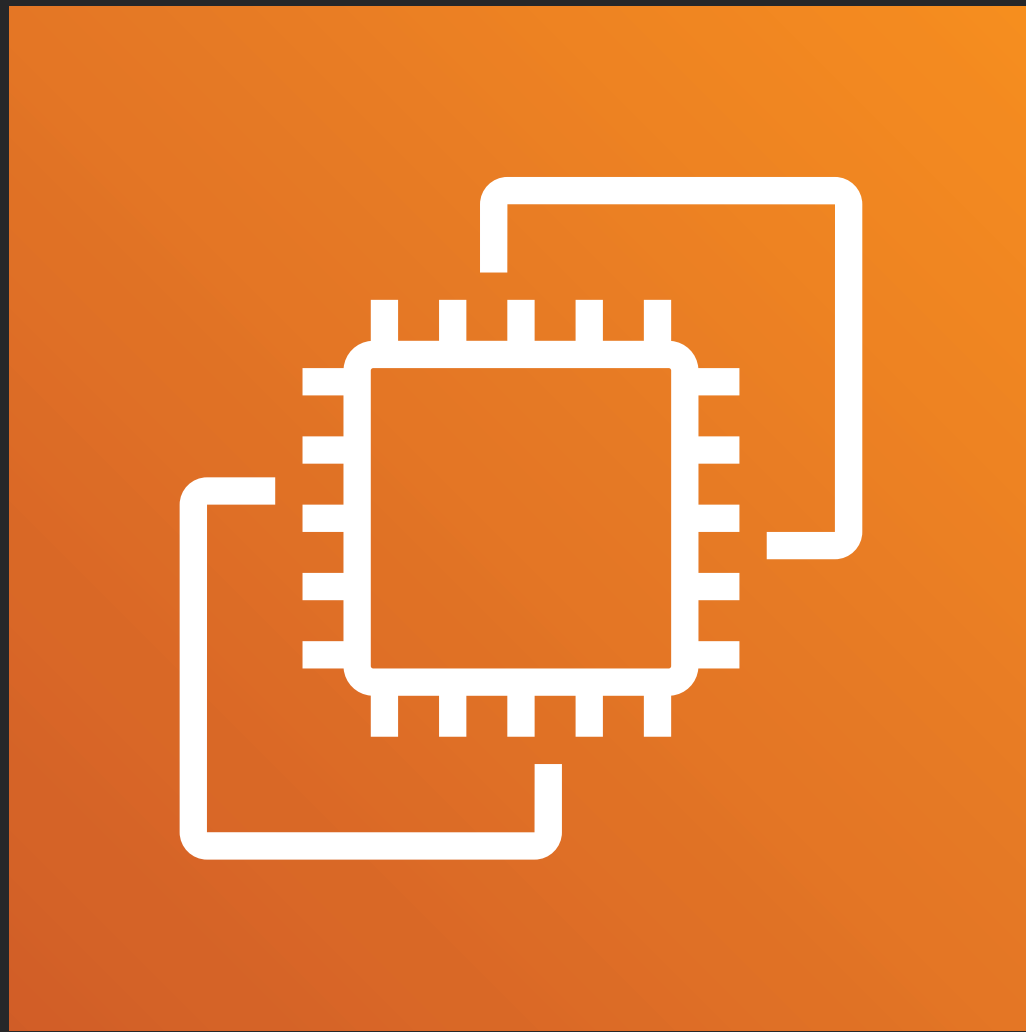
OS

Virtualization

Infrastructure

Physical

Infrastructure
(IaaS)



Amazon EC2

Instances

Data

Application

OS

Virtualization

Infrastructure

Physical

Infrastructure
(IaaS)



Amazon ECS

Containers + Host

Data

Application

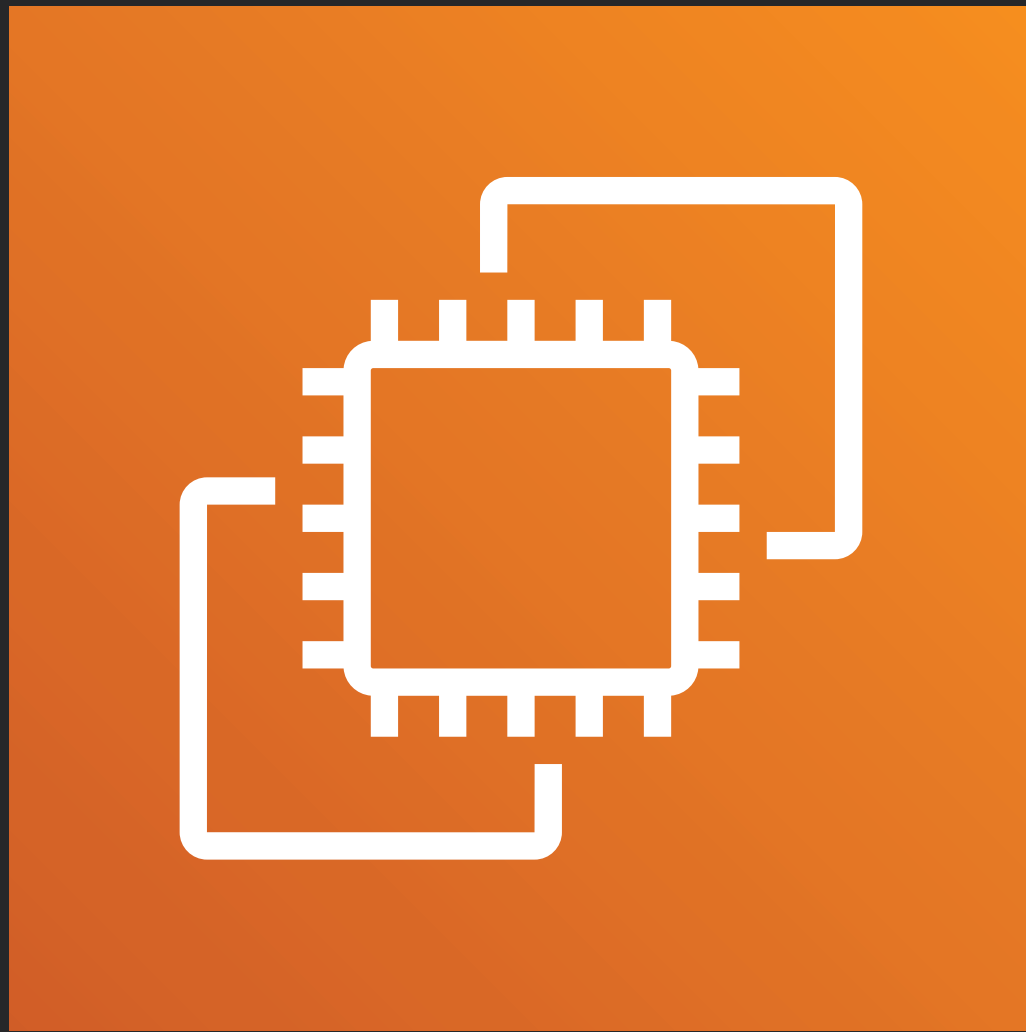
OS

Virtualization

Infrastructure

Physical

Infrastructure
(IaaS)



Amazon EC2

Instances

Data
Application
OS
Virtualization
Infrastructure
Physical

Infrastructure
(IaaS)



Amazon ECS

Containers + Host

Data
Application
OS
Virtualization
Infrastructure
Physical

Infrastructure
(IaaS)

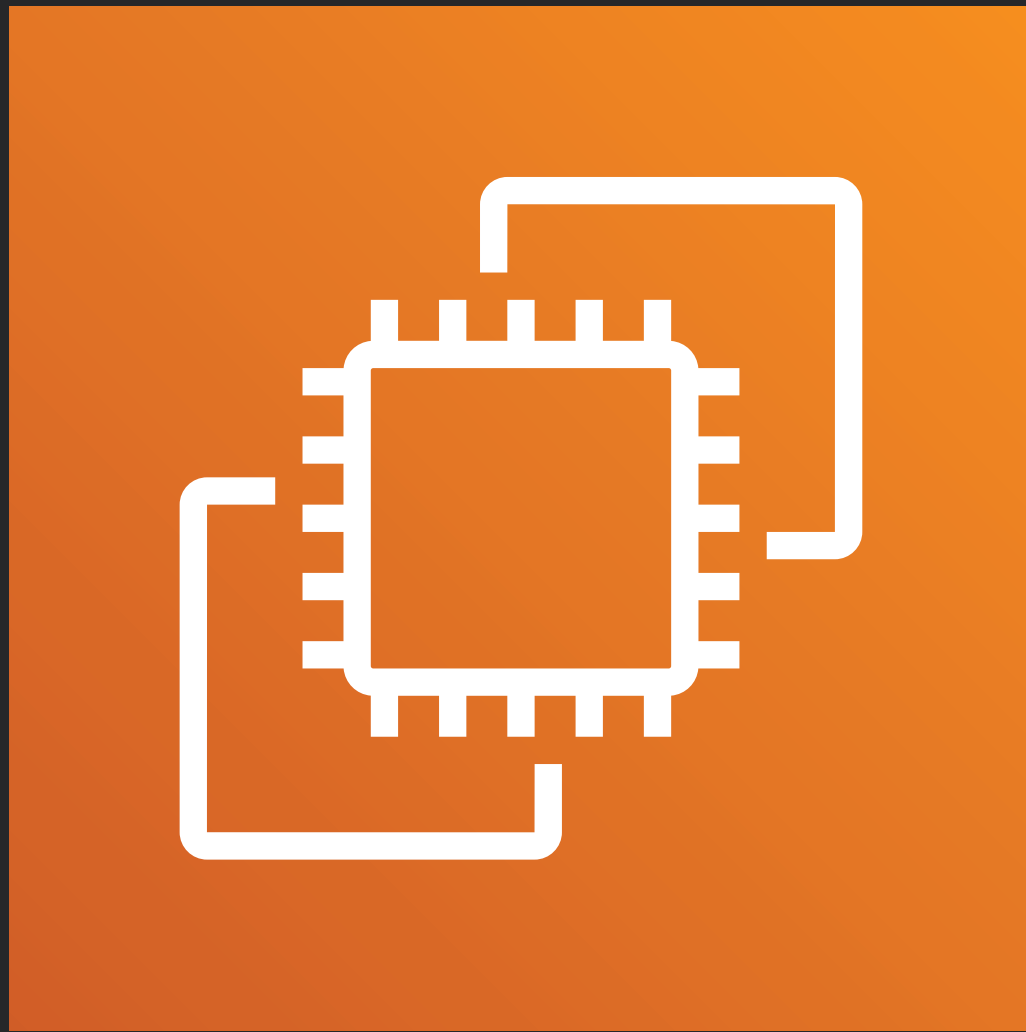


AWS Fargate

Managed Containers

Data
Application
OS
Virtualization
Infrastructure
Physical

Container
(PaaS)



Amazon EC2

Instances

Data
Application
OS
Virtualization
Infrastructure
Physical

Infrastructure
(IaaS)



Amazon ECS

Containers + Host

Data
Application
OS
Virtualization
Infrastructure
Physical

Infrastructure
(IaaS)



AWS Fargate

Managed Containers

Data
Application
OS
Virtualization
Infrastructure
Physical

Container
(PaaS)

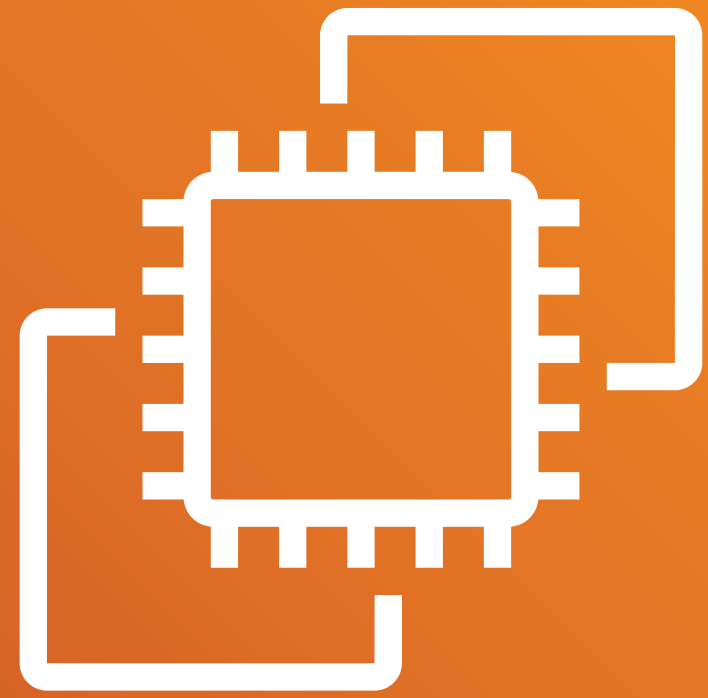


AWS Lambda

Functions

Data
Application
OS
Virtualization
Infrastructure
Physical

Abstract
(SaaS)



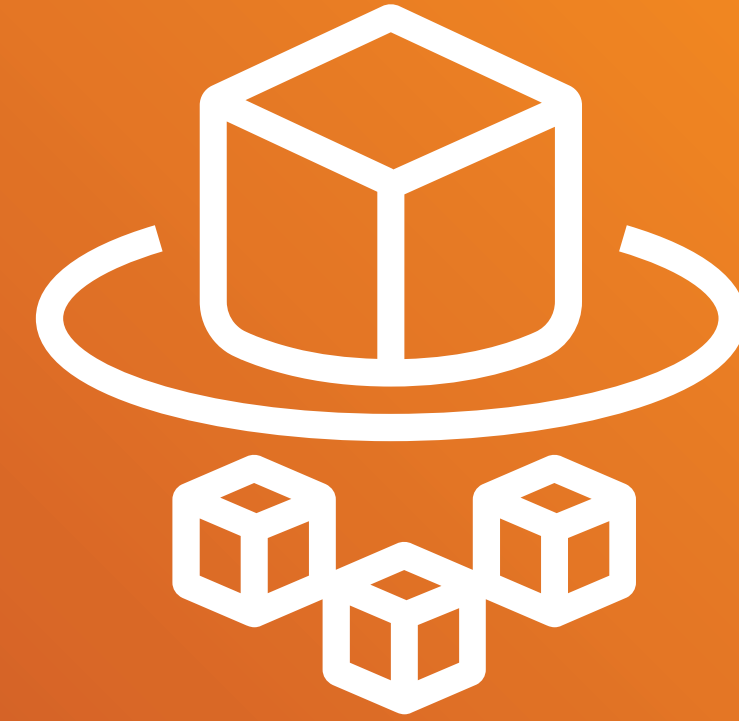
Amazon EC2

Instances



Amazon ECS

Containers + Host



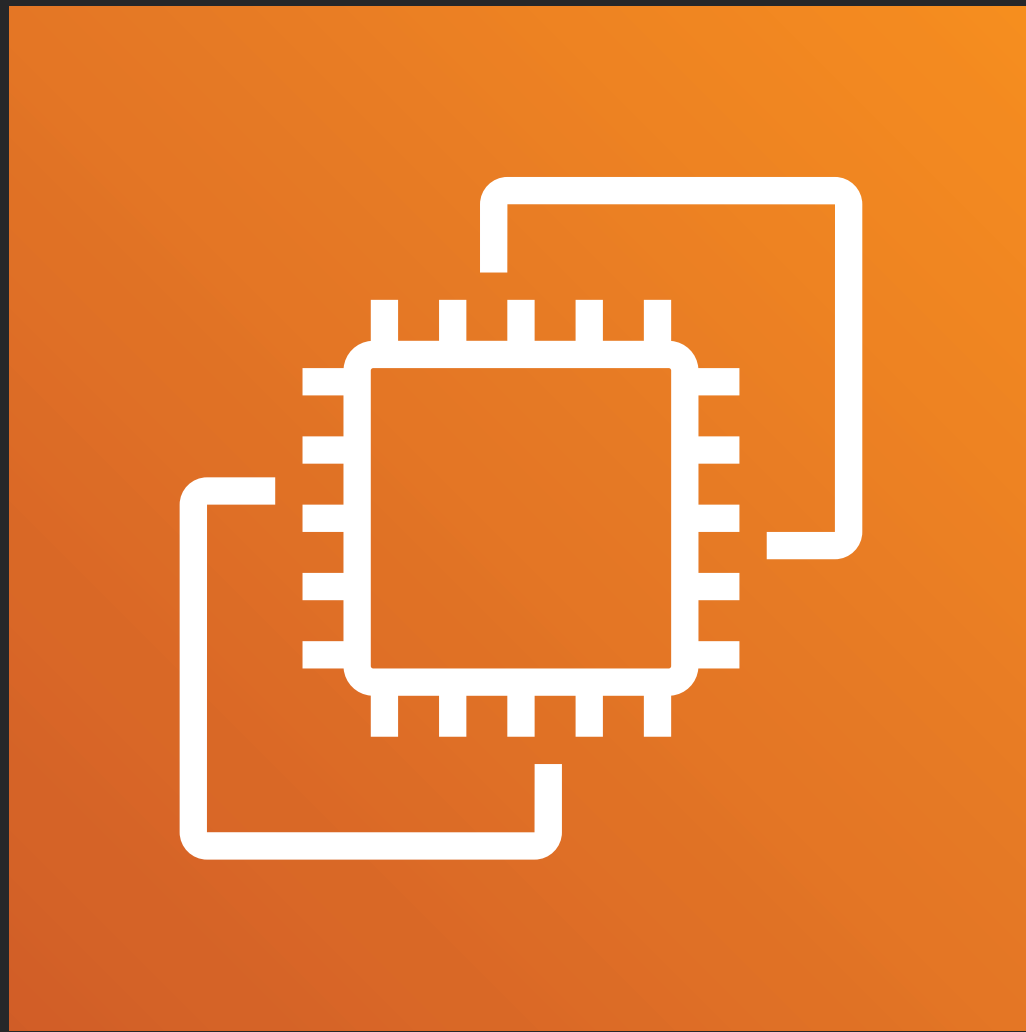
AWS Fargate

Managed Containers



AWS Lambda

Functions



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

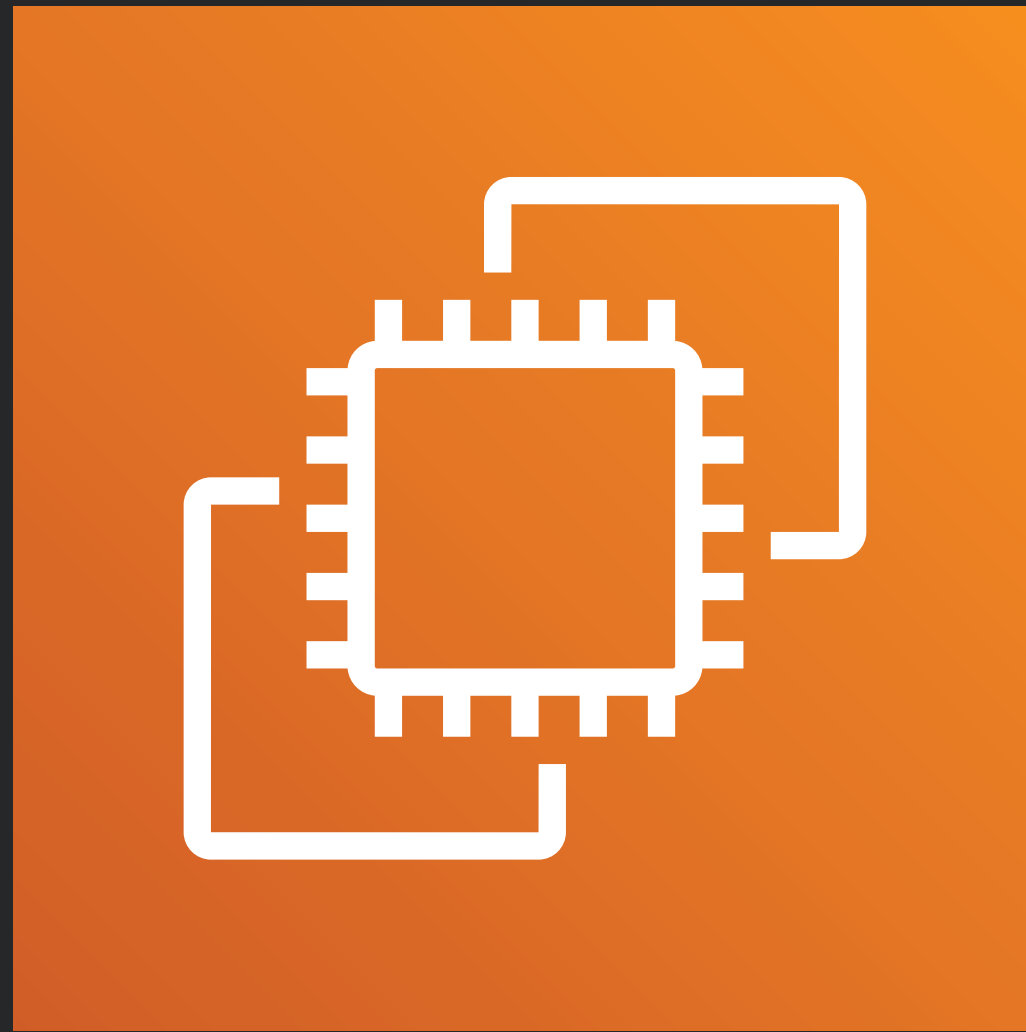
Managed Containers



AWS Lambda

Functions

- **Harden the OS configuration**



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

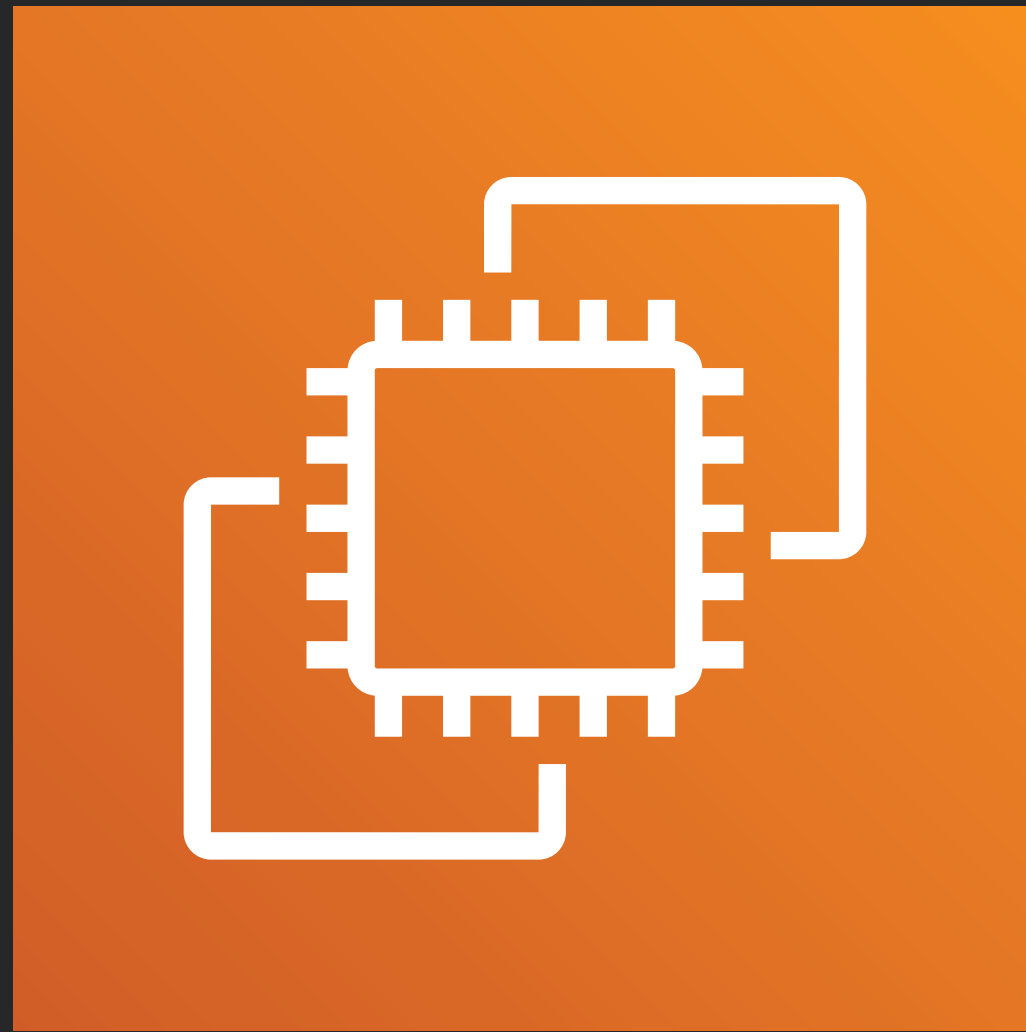
Managed Containers



AWS Lambda

Functions

- Harden the OS configuration
- Controls like integrity monitoring, intrusion prevention, anti-malware



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

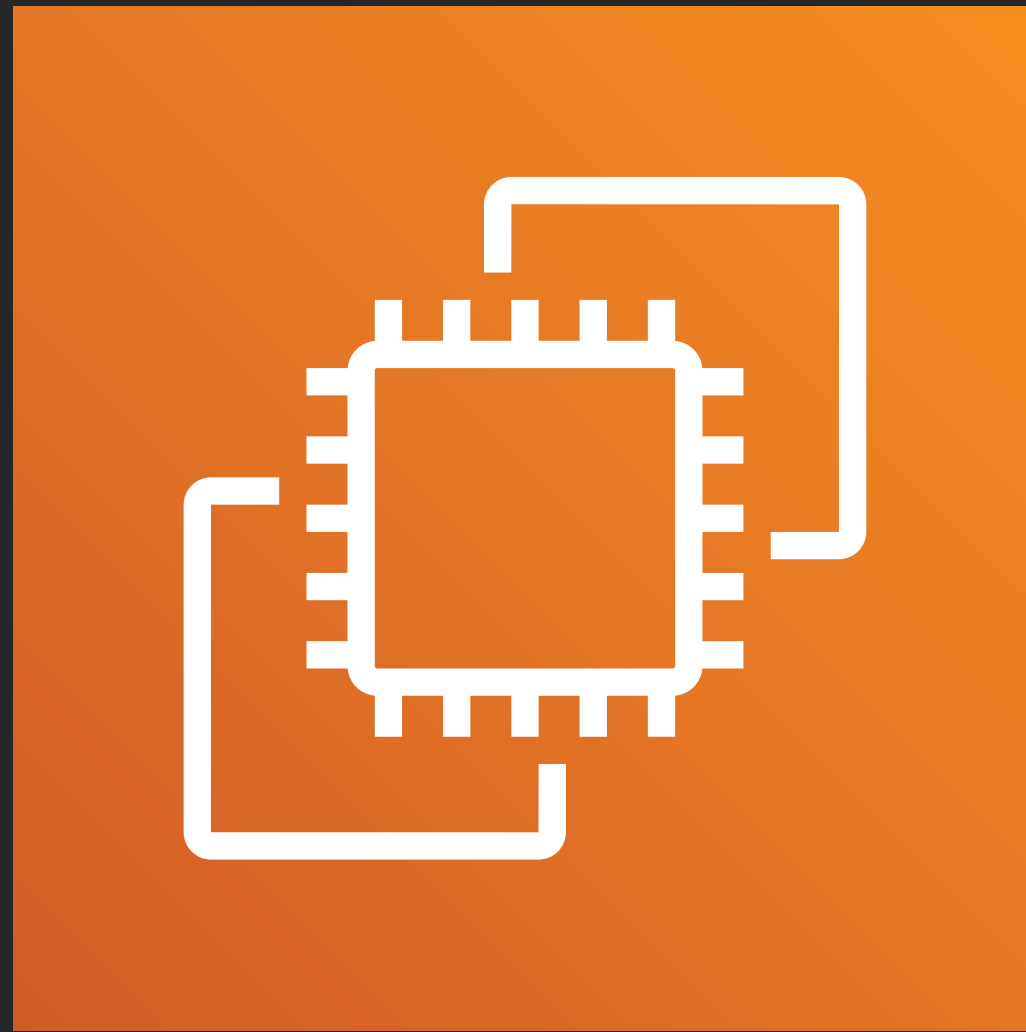
Managed Containers



AWS Lambda

Functions

- Harden the OS configuration
- Controls like integrity monitoring, intrusion prevention, anti-malware
- Don't patch or login to production



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

Managed Containers

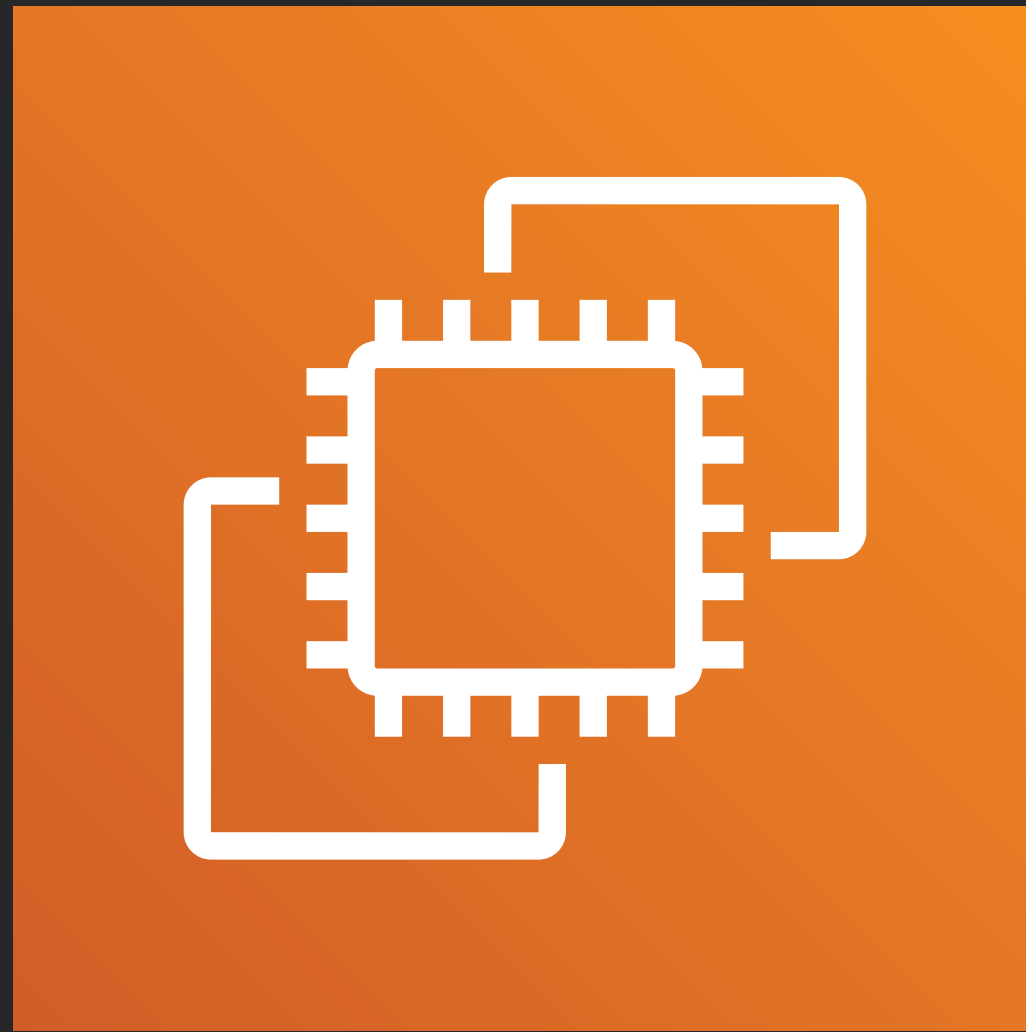


AWS Lambda

Functions

- Harden the OS configuration
- Controls like integrity monitoring, intrusion prevention, anti-malware
- Don't patch or login to production

- Code quality is a priority



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

Managed Containers

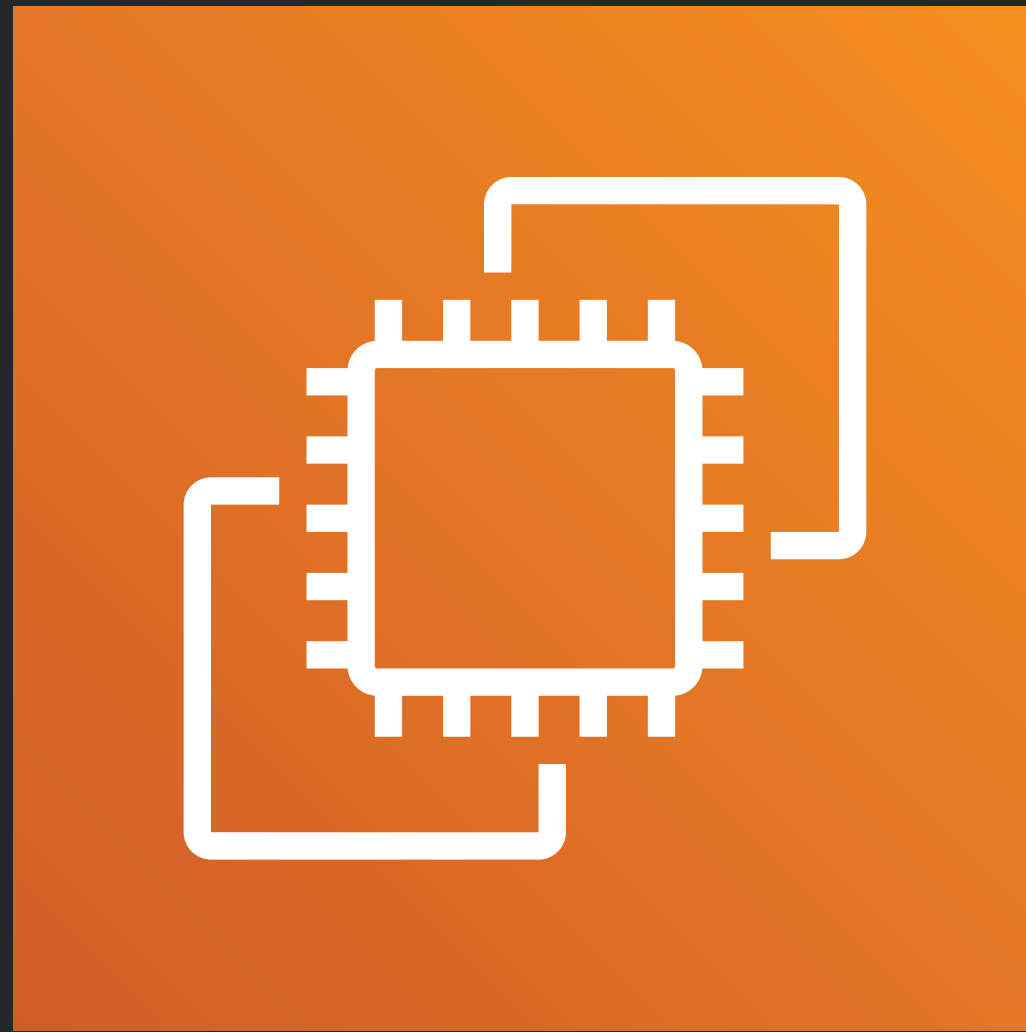


AWS Lambda

Functions

- Harden the OS configuration
- Controls like integrity monitoring, intrusion prevention, anti-malware
- Don't patch or login to production

- Code quality is a priority
- Controls like real-time application protection are key



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

Managed Containers

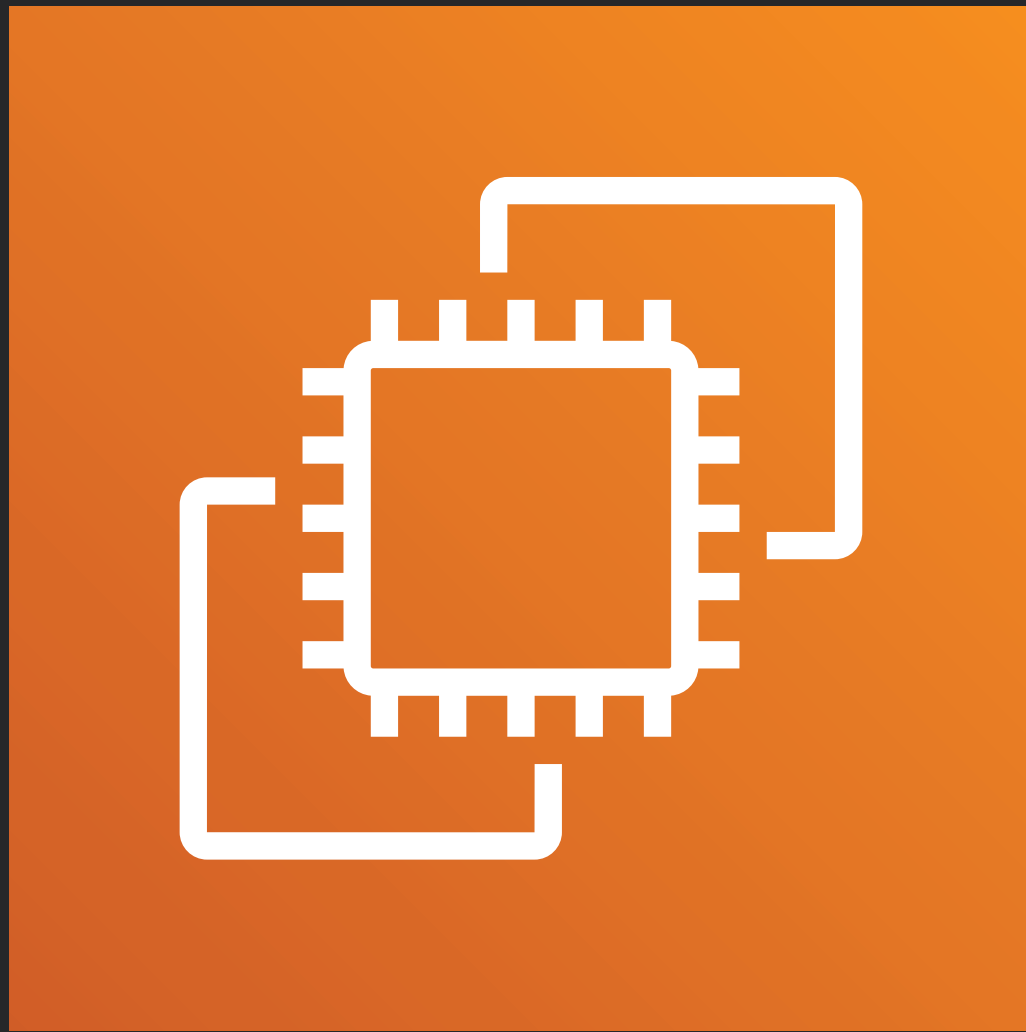


AWS Lambda

Functions

- Harden the OS configuration
- Controls like integrity monitoring, intrusion prevention, anti-malware
- Don't patch or login to production

- Code quality is a priority
- Controls like real-time application protection are key
- Dependency verification and validation is critical



Amazon EC2

Instances



Amazon ECS

Containers + Host



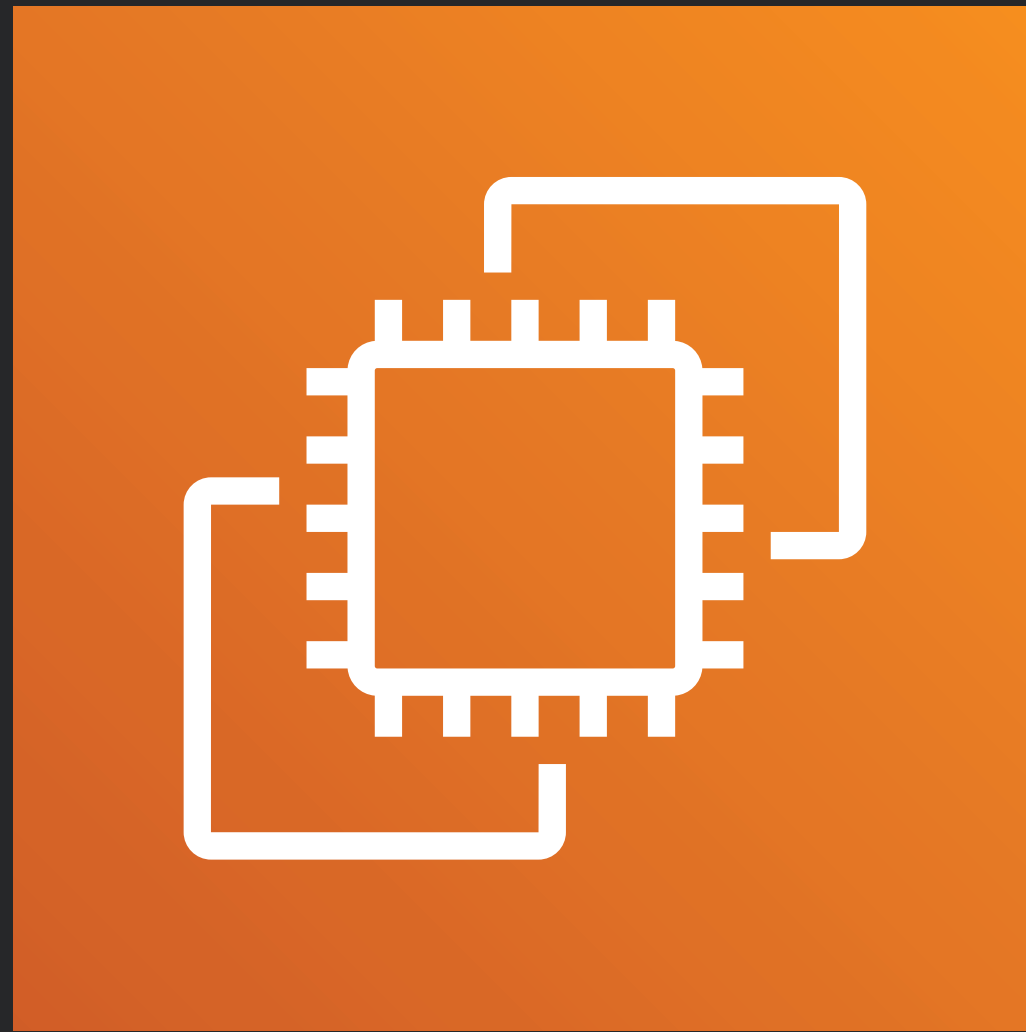
AWS Fargate

Managed Containers



AWS Lambda

Functions



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

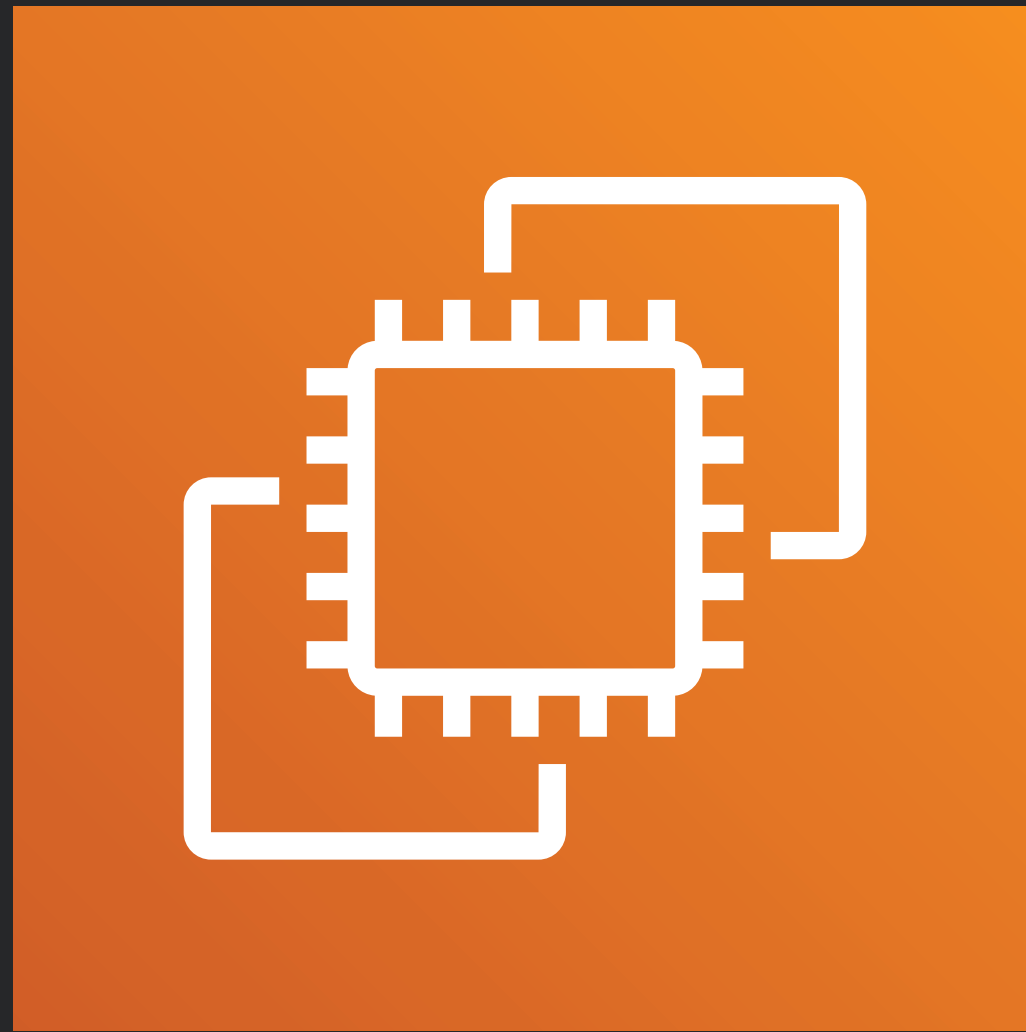
Managed Containers



AWS Lambda

Functions

- **Fix issues in the build pipeline and redeploy (blue/green)**



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

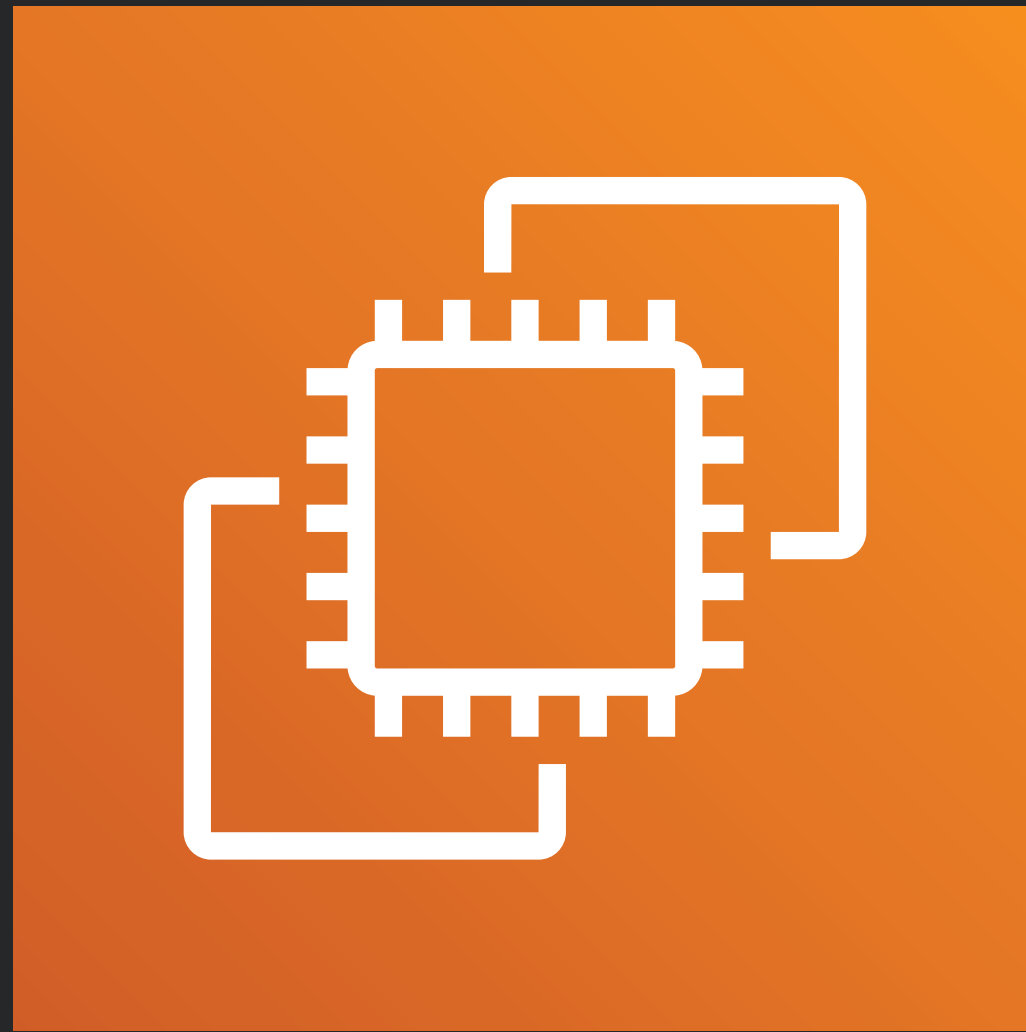
Managed Containers



AWS Lambda

Functions

- **Fix issues in the build pipeline and redeploy (blue/green)**
- **Automated controls and verification with security testing**



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

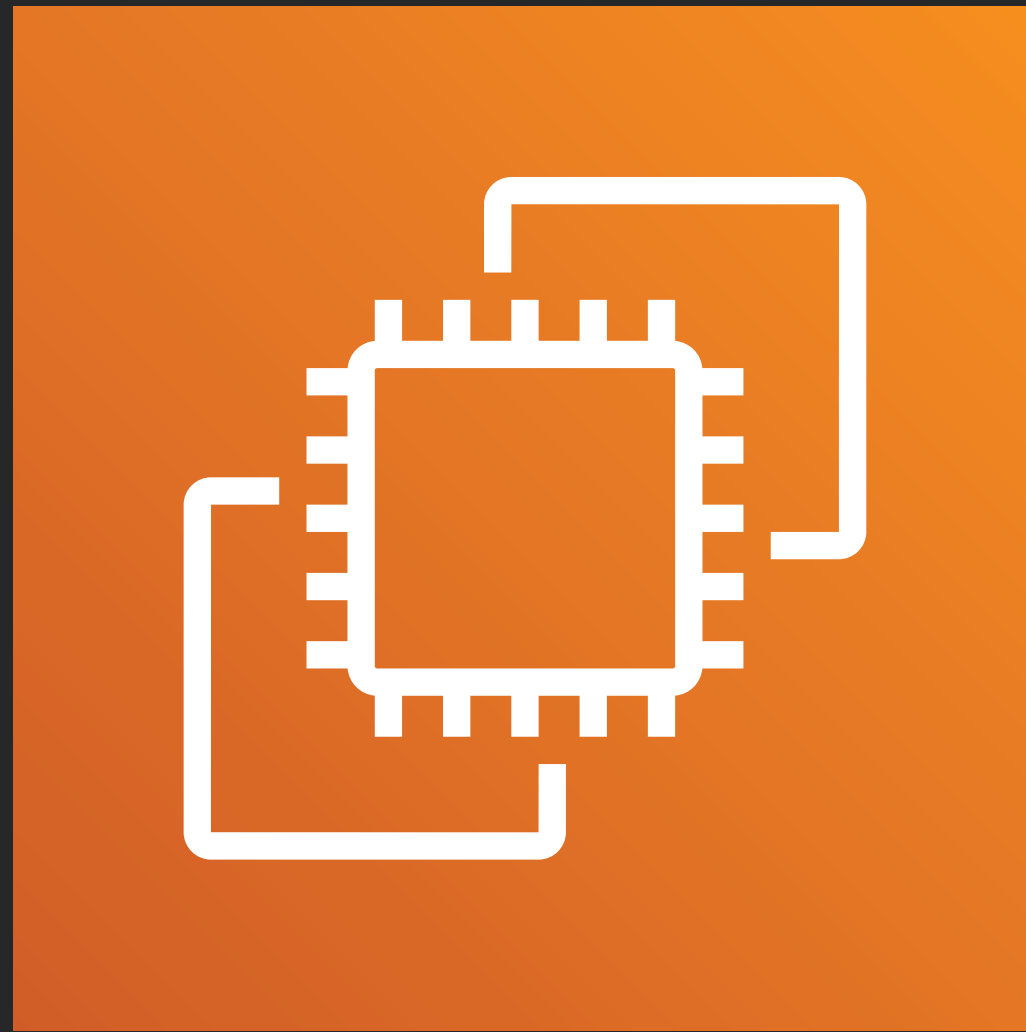
Managed Containers



AWS Lambda

Functions

- Fix issues in the build pipeline and redeploy (blue/green)
- Automated controls and verification with security testing
- Builder's workstations are a weak point (opsec is critical!)



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

Managed Containers

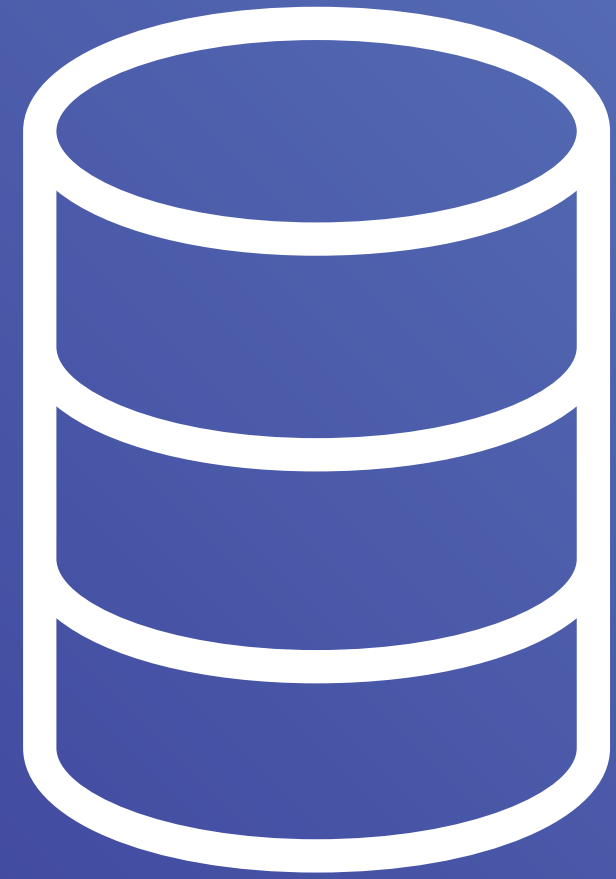


AWS Lambda

Functions

- Fix issues in the build pipeline and redeploy (blue/green)
- Automated controls and verification with security testing
- Builder's workstations are a weak point (opsec is critical!)
- Systems over people

Data



Databases



Databases

Structured, accessible data



Structured, accessible data

Amazon DynamoDB, Amazon DocumentDB, Amazon RDS, Amazon Timestream, Amazon Neptune, etc.



Structured, accessible data

Amazon DynamoDB, Amazon DocumentDB, Amazon RDS, Amazon Timestream, Amazon Neptune, etc.

- **Encrypt the data at rest**



Structured, accessible data

Amazon DynamoDB, Amazon DocumentDB, Amazon RDS, Amazon Timestream, Amazon Neptune, etc.

- **Encrypt the data at rest**
- **Use IAM permissions to restrict access**



Structured, accessible data

Amazon DynamoDB, Amazon DocumentDB, Amazon RDS, Amazon Timestream, Amazon Neptune, etc.

- Encrypt the data at rest
- Use IAM permissions to restrict access
- Backup everything, all the time, test that backup regularly



Storage



Storage

Structured, accessible data **but** in files



Structured, accessible data but in files

Amazon Elastic Block Store, Amazon FSx, Amazon S3, Amazon Glacier, Amazon File System, etc.



Structured, accessible data but in files

Amazon Elastic Block Store, Amazon FSx, Amazon S3, Amazon Glacier, Amazon File System, etc.

- **Encrypt the data at rest**



Structured, accessible data but in files

Amazon Elastic Block Store, Amazon FSx, Amazon S3, Amazon Glacier, Amazon File System, etc.

- **Encrypt the data at rest**
- **Use IAM permissions to restrict access**



Structured, accessible data but in files

Amazon Elastic Block Store, Amazon FSx, Amazon S3, Amazon Glacier, Amazon File System, etc.

- Encrypt the data at rest
- Use IAM permissions to restrict access
- Use lifecycle strategies to reduce costs and optimize usage

Is this working?

Observability



Traceability

Verify the history, location,
and application of a specific
data point or action

Traceability

Where did this come from?

Who can access it?

When?

Observability

The ability to infer internal states from external outputs

Observability

What's going on?

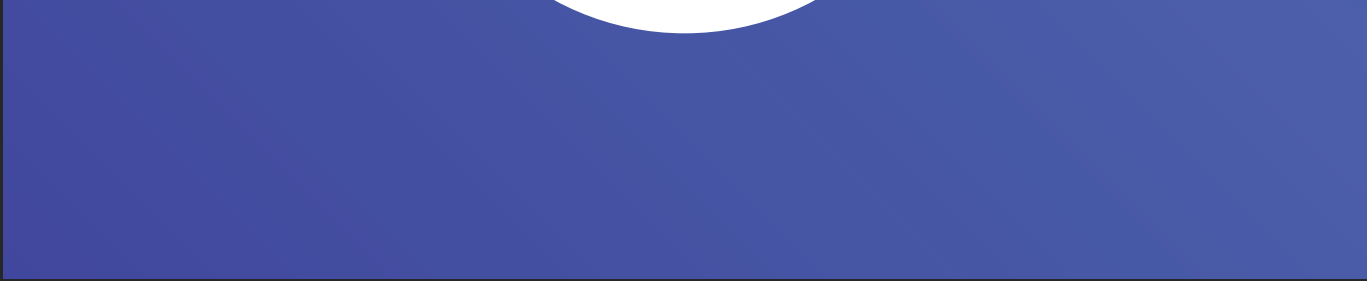


AWS X-Ray

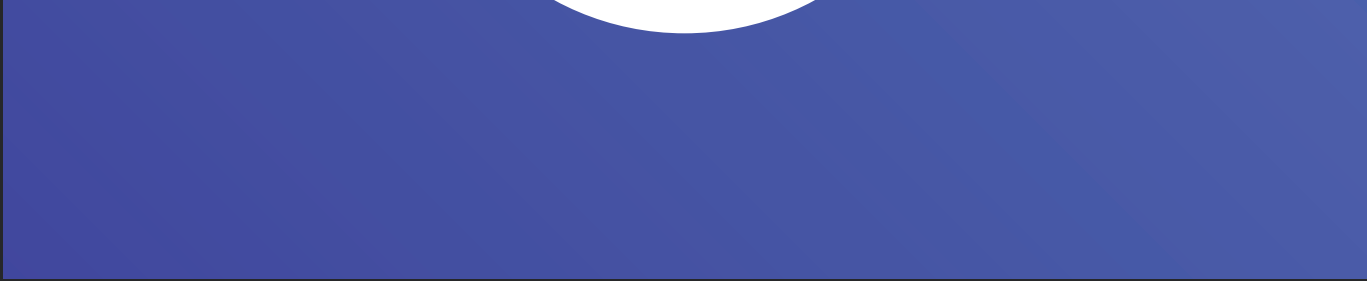


AWS X-Ray

Understand the behaviour of distributed applications

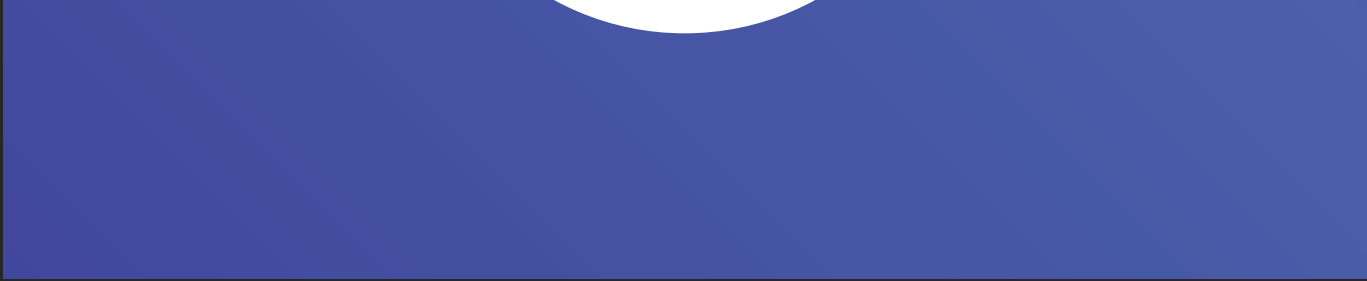


Understand the behaviour of distributed applications



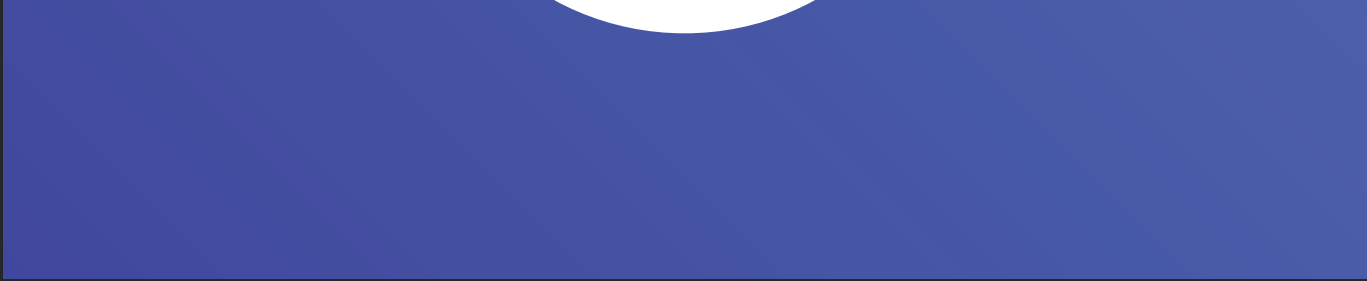
Understand the behaviour of distributed applications

- Provides a cross-service view of your application



Understand the behaviour of distributed applications

- Provides a cross-service view of your application
- Helps map out the service usage



Understand the behaviour of distributed applications

- Provides a cross-service view of your application
- Helps map out the service usage
- Limited language support but getting better quickly



Amazon CloudWatch



Amazon CloudWatch

Metrics, events, and logs



Metrics, events, and logs



Metrics, events, and logs

- 3 services disguised as one



Metrics, events, and logs

- 3 services disguised as one
- Metrics for basic operational health



Metrics, events, and logs

- 3 services disguised as one
- Metrics for basic operational health
- Logs for system and application events



Metrics, events, and logs

- 3 services disguised as one
- Metrics for basic operational health
- Logs for system and application events
- Events for AWS account events is an excellent trigger for automation via AWS Lambda

Automation



Trigger

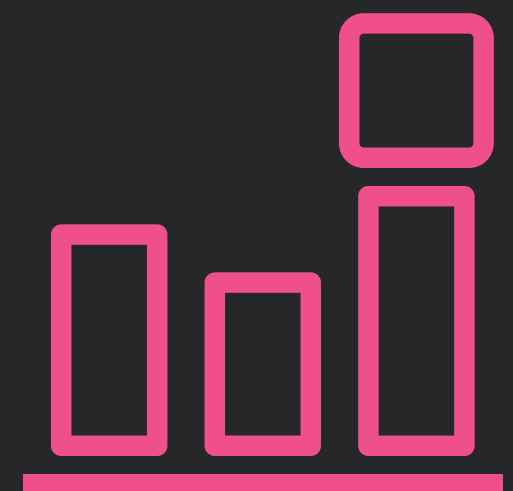
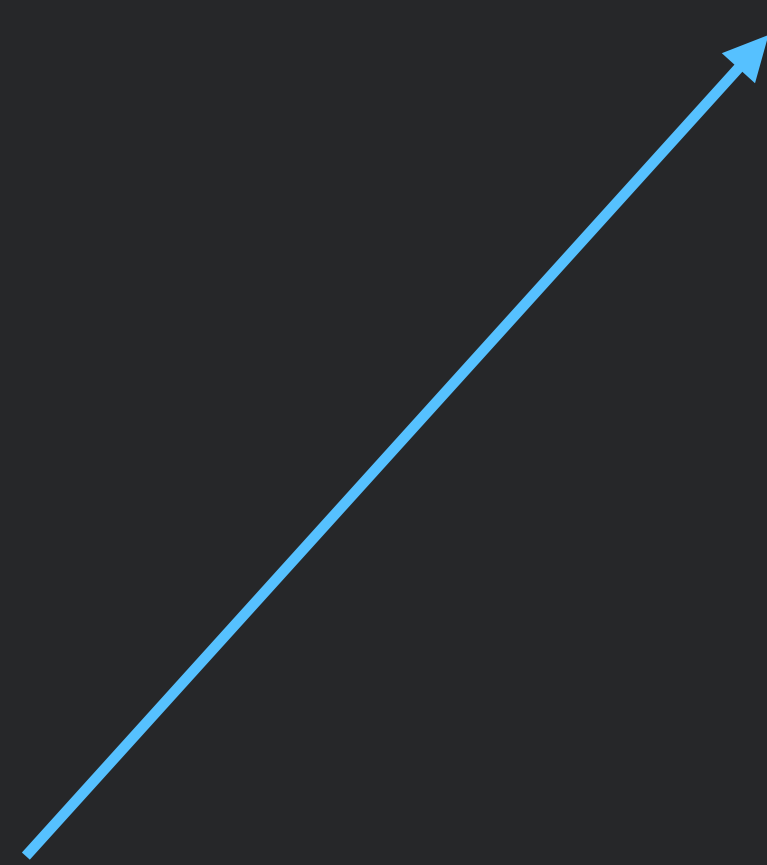


Result

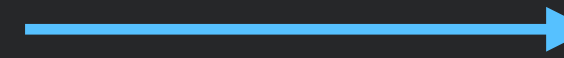
Automation



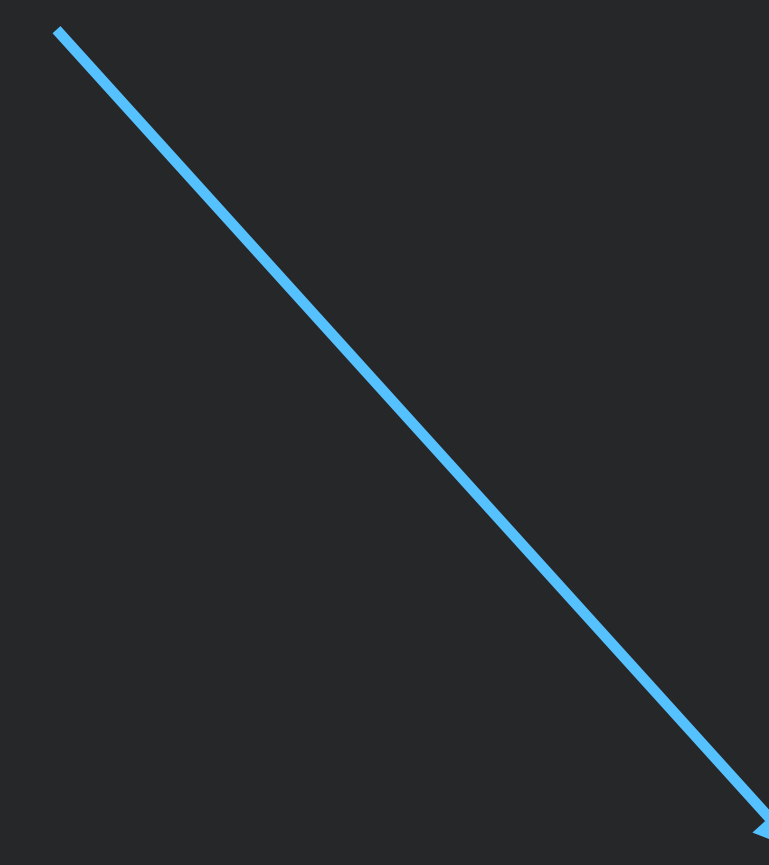
Trigger



CloudWatch
Event



Lambda



Result

Automation



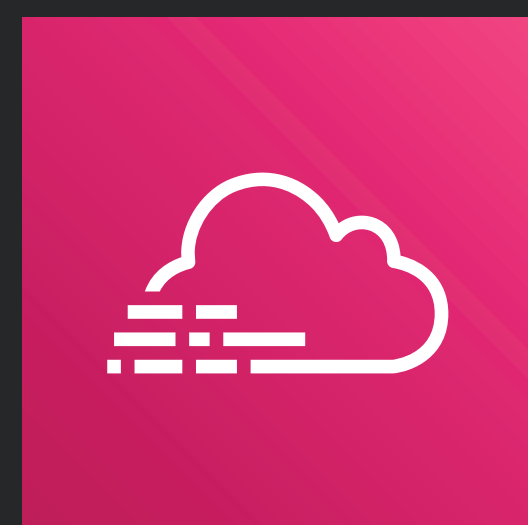
Trigger



Lambda



Result



CloudTrail

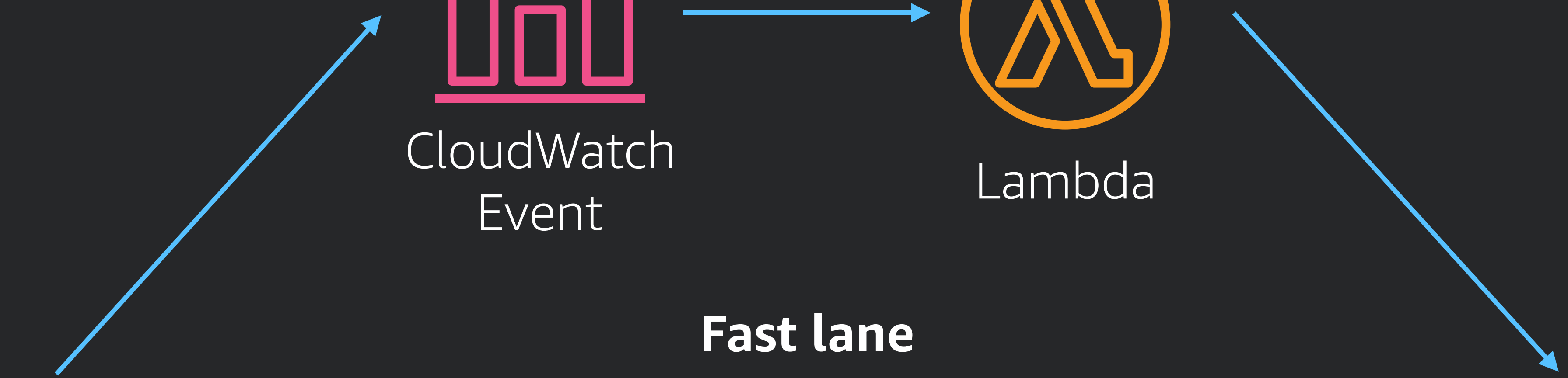


Lambda

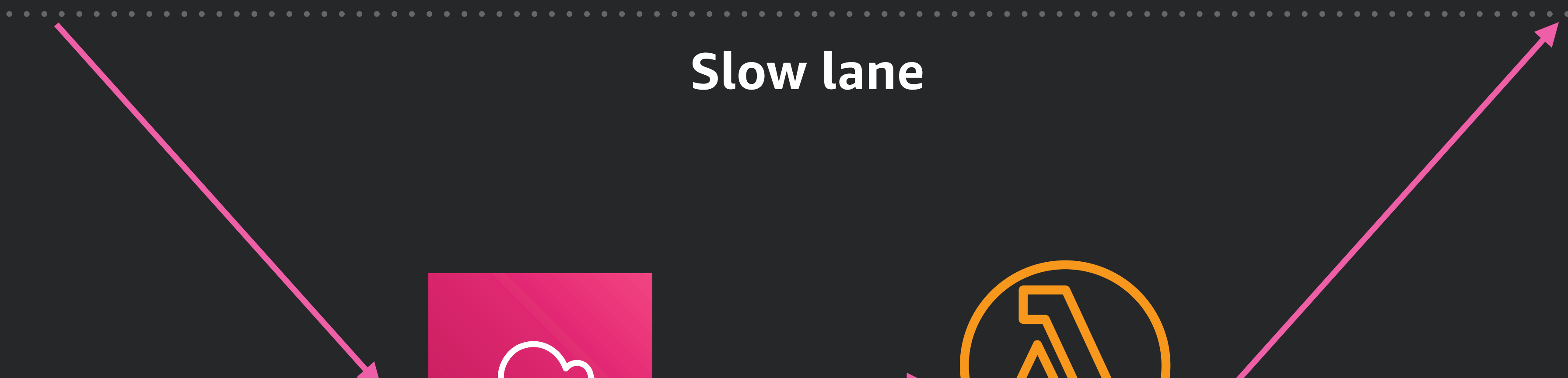
Automation



Trigger



Fast lane



Slow lane



Result

Keys to success

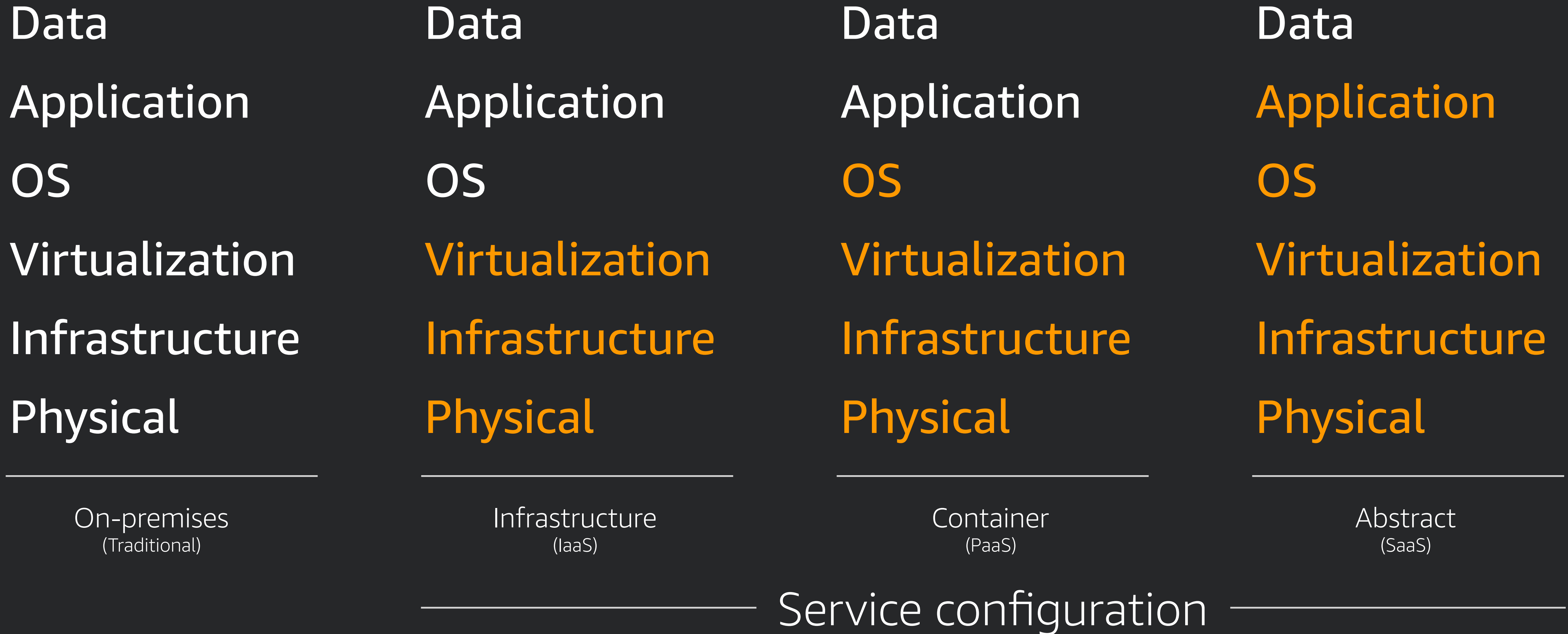
The cloud simplifies security.

* When you understand how it works

** Compared to traditional environments

*** Depending on how much you pay attention for the next 60m

The Shared Responsibility Model



Our goal

**Make sure that systems
work as intended and
only as intended**

Largest risk

**Mistakes &
misconfigurations**



Keys To Success



Keys To Success

Have a plan



Cloud Adoption Framework



Keys To Success

Have a plan Cloud Adoption Framework

Build well Well-Architected Framework



Keys To Success

Have a plan Cloud Adoption Framework

Build well Well-Architected Framework

Systems over people The right controls & tools



Keys To Success

Have a plan Cloud Adoption Framework

Build well Well-Architected Framework

Systems over people The right controls & tools

Observe & react Be vigilant & practice



TREND
M I C R OTM

Cloud security simplified
Visit Trend Micro in booth #2820

Thank you!



Mark Nunnikhoven

Vice President, Cloud Research at Trend Micro

[@marknca](#)



Please complete the session survey in the mobile app.