AWS re:Invent

SEC204-S

Strong security made simple: Putting all the pieces together



Mark Nunnikhoven
Vice President, Cloud Research at Trend Micro
@marknca

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

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

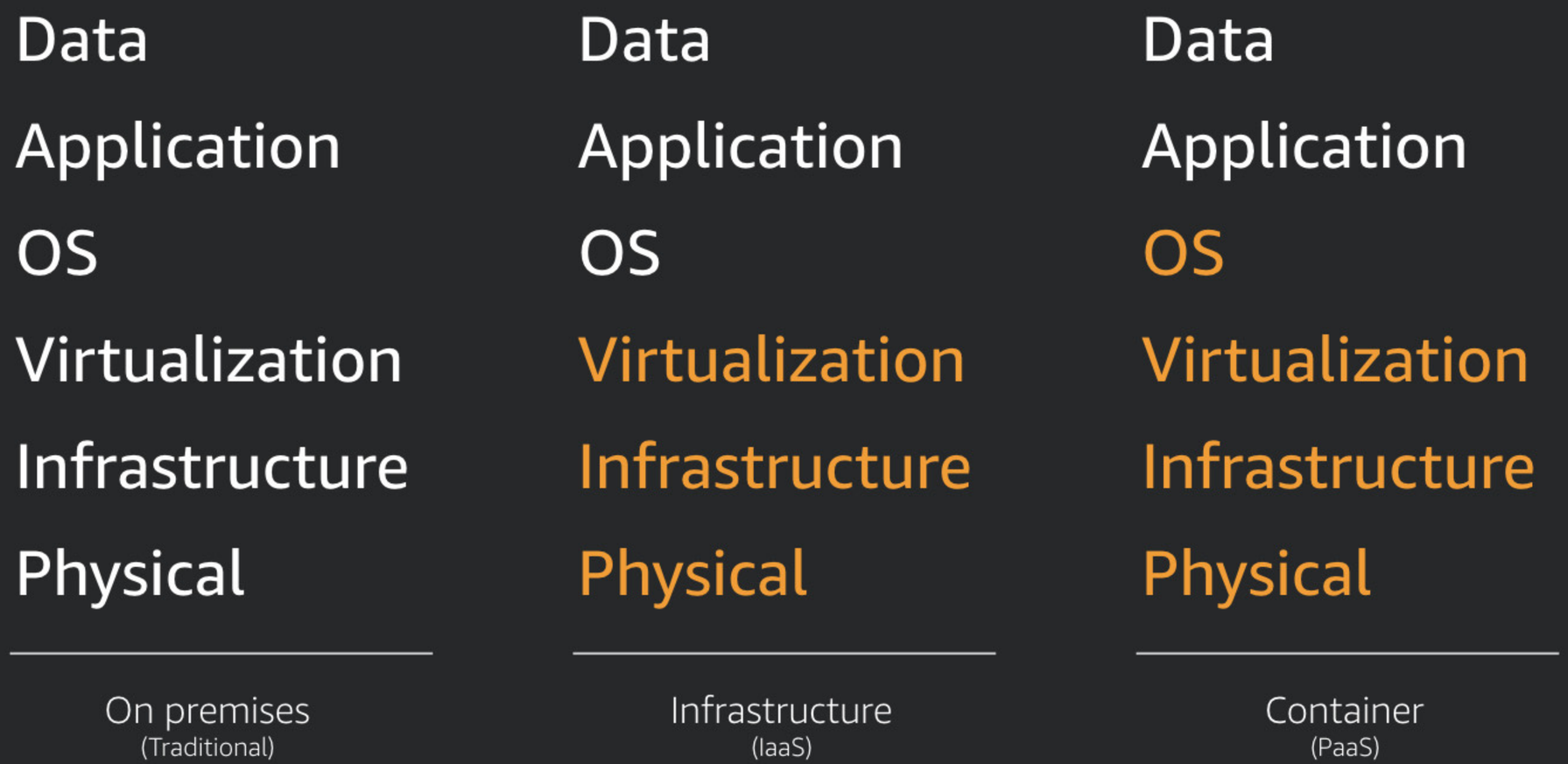
On premises
(Traditional)

The Shared Responsibility Model

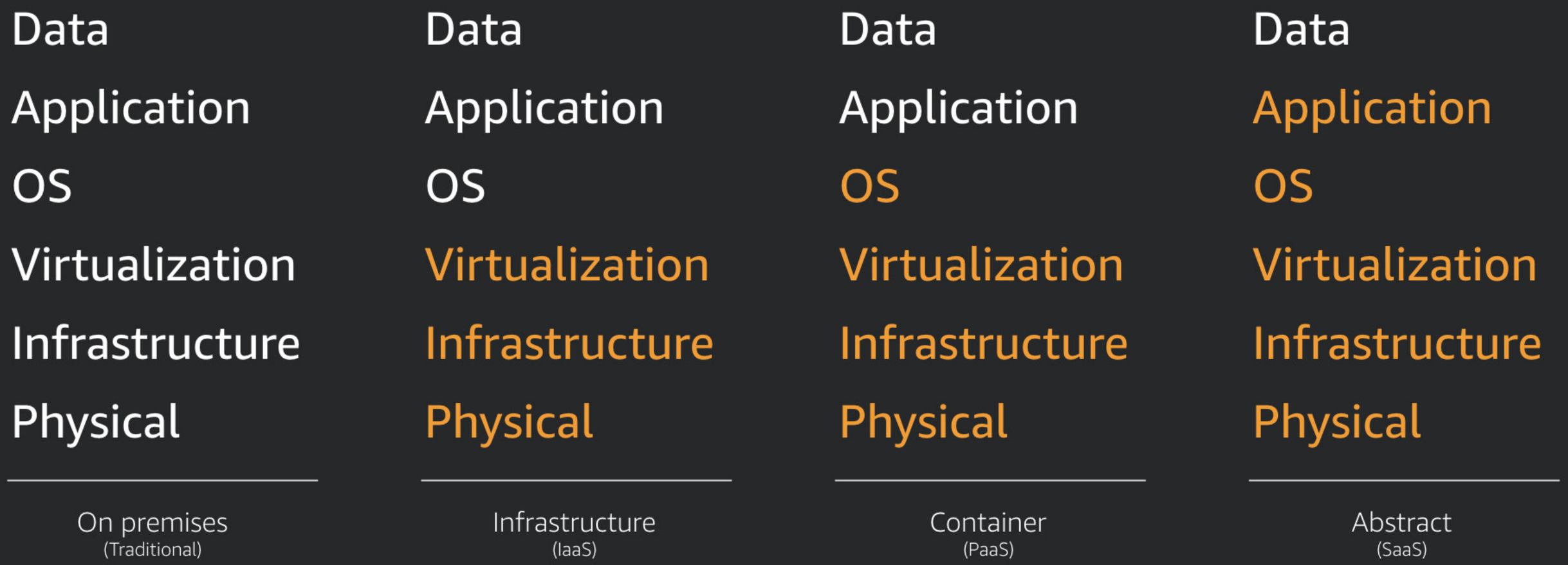
On premises (Traditional)	Infrastructure (IaaS)
Data	Data
Application	Application
OS	OS
Virtualization	Virtualization
Infrastructure	Infrastructure
Physical	Physical

Your responsibility AWS' responsibility

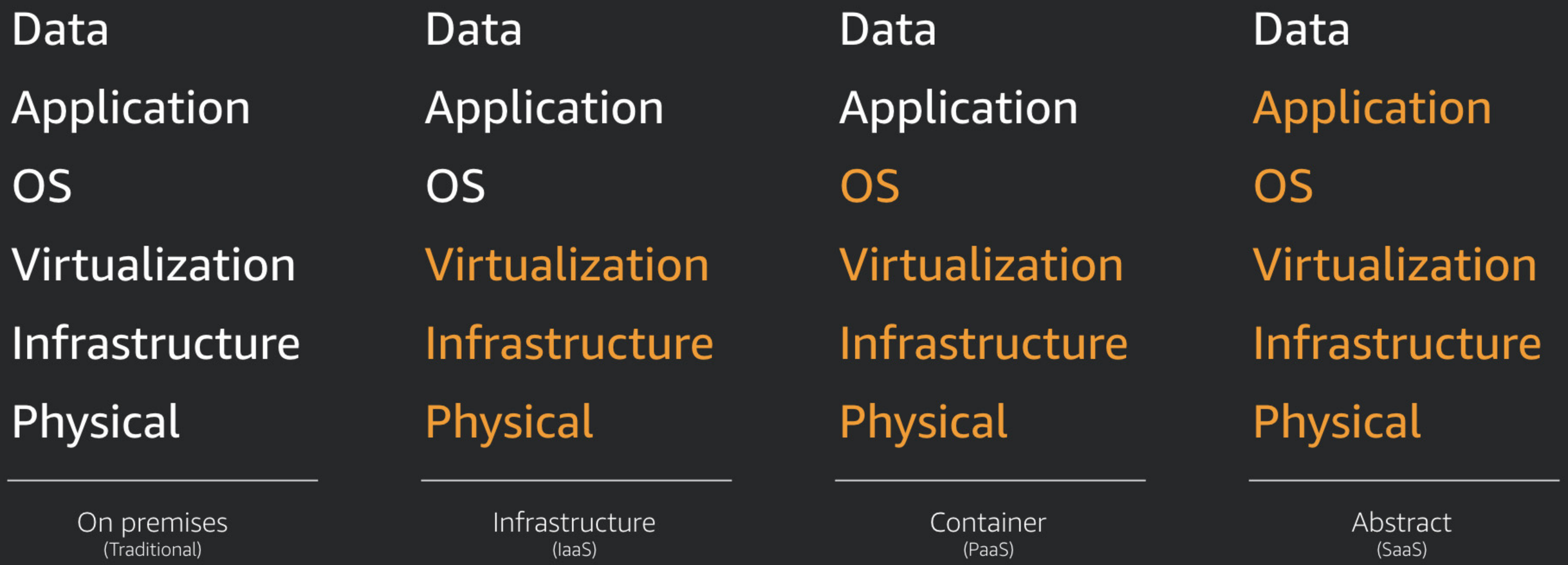
The Shared Responsibility Model



The Shared Responsibility Model



The Shared Responsibility Model







AWS Compliance Programs

Global

CSA ISO 9001 ISO 27001 ISO 27017 ISO 27018

CSA ISO 9001 ISO 27001 ISO 27017 ISO 27018

Global

United States

Canada

Asia Pacific

Europe

Privacy



AWS Compliance Programs

Global

Global

United States

Canada

Asia Pacific

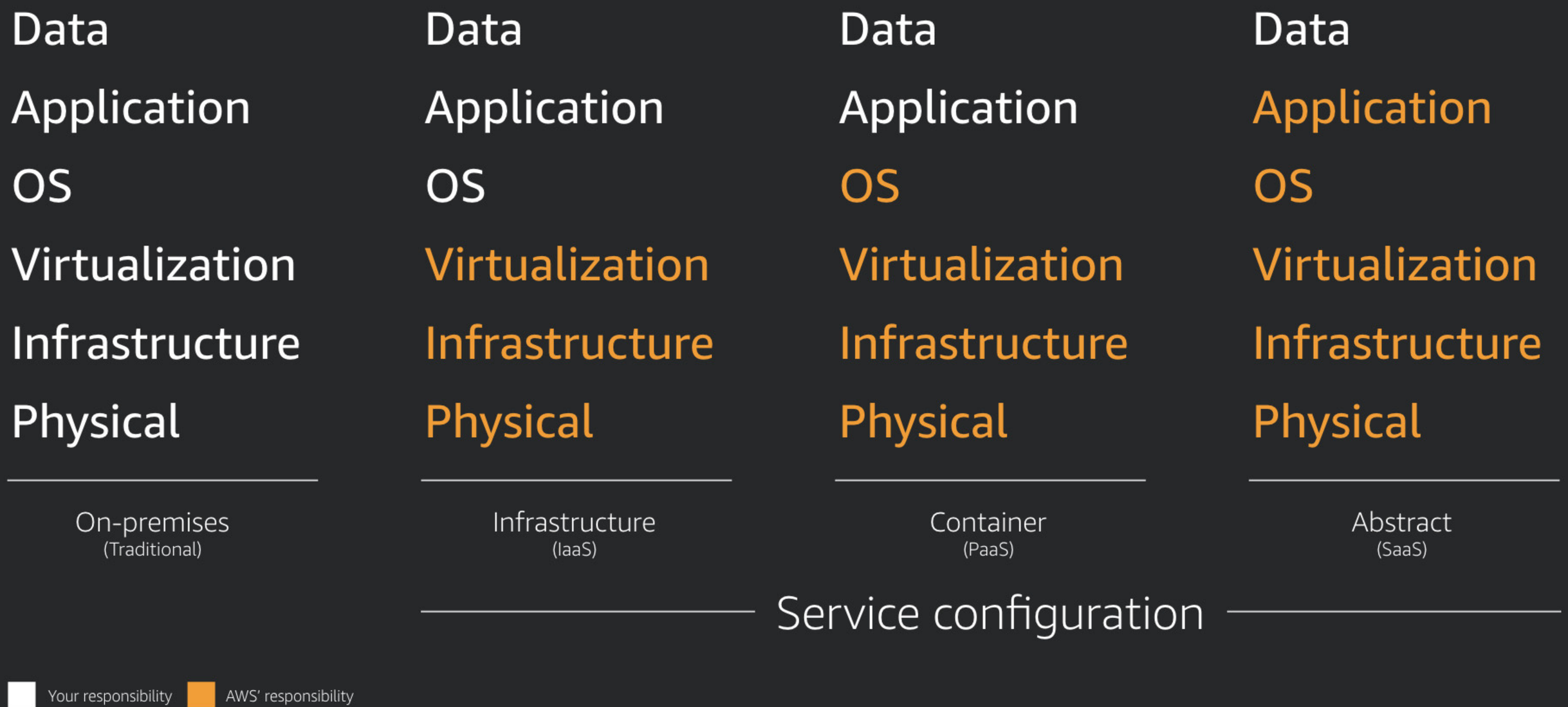
Europe

Privacy

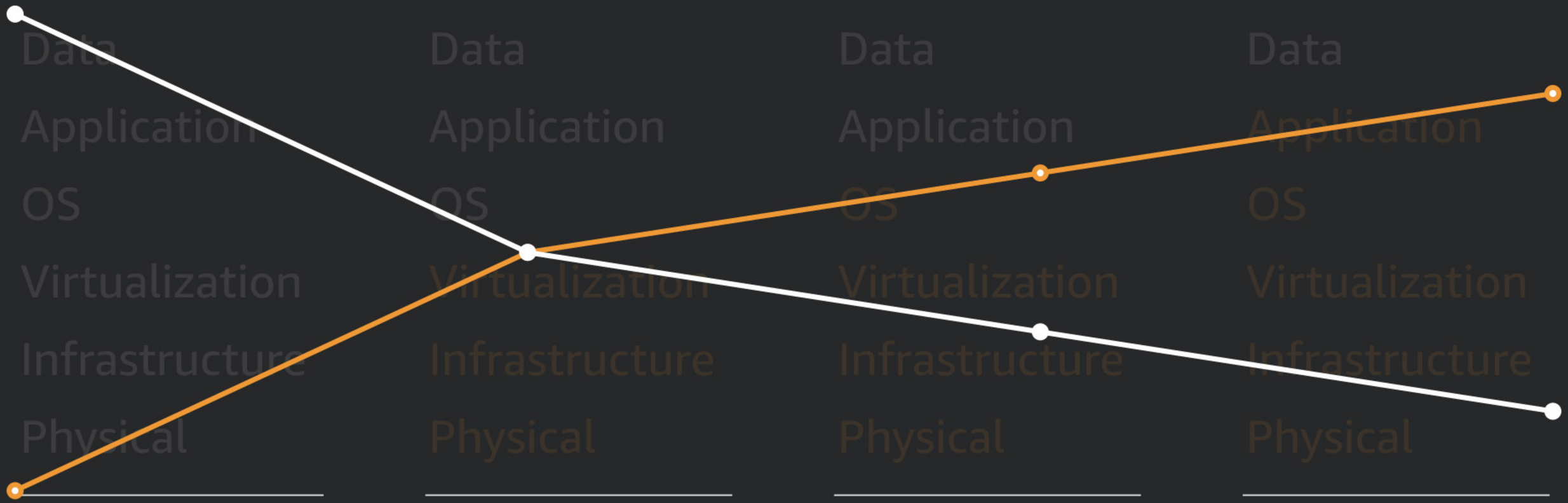
aws.amazon.com/compliance

CSA ISO 9001 ISO 27001 ISO 27017 ISO 27018

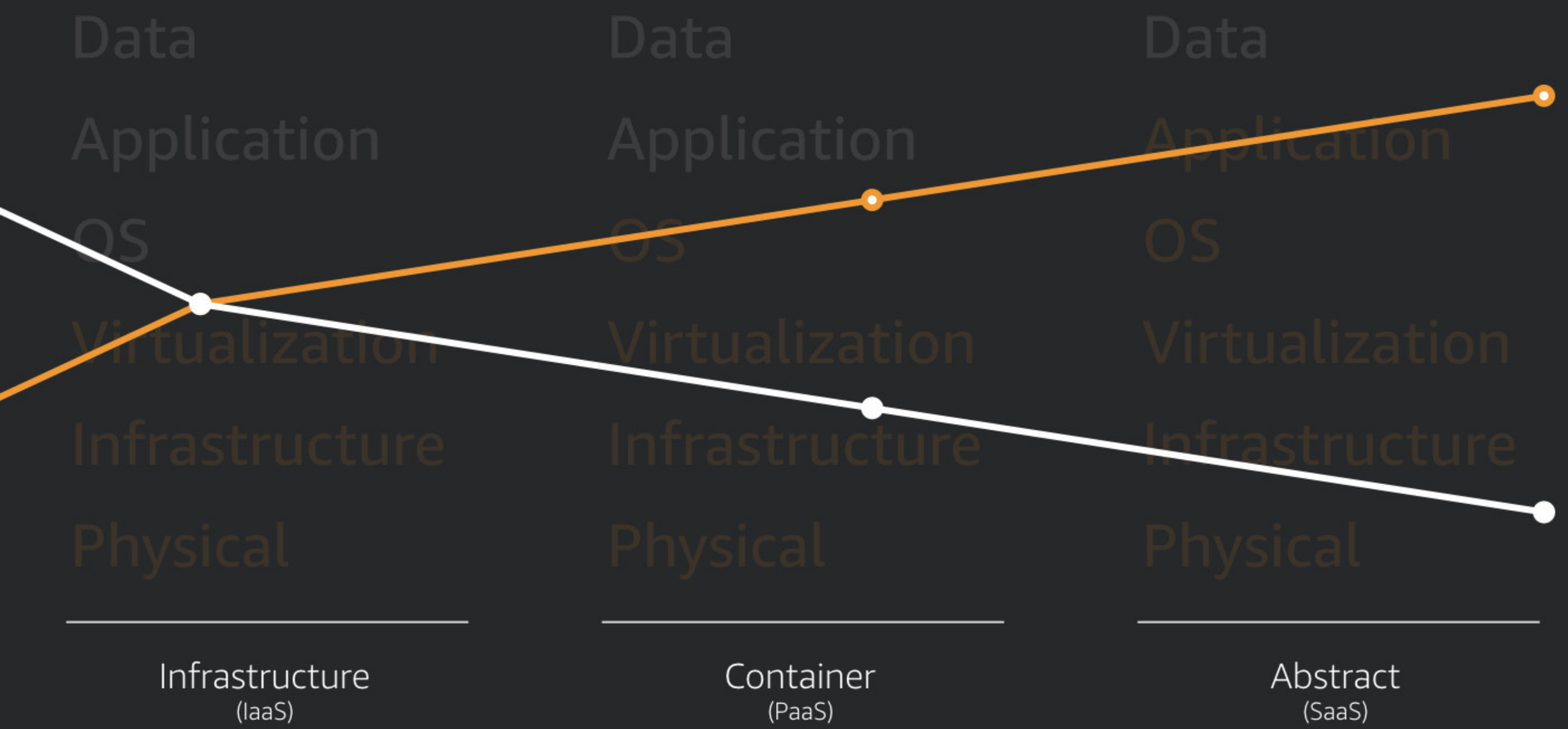
The Shared Responsibility Model



The Shared Responsibility Model



The Shared Responsibility Model



Infrastructure
(IaaS)

Container
(PaaS)

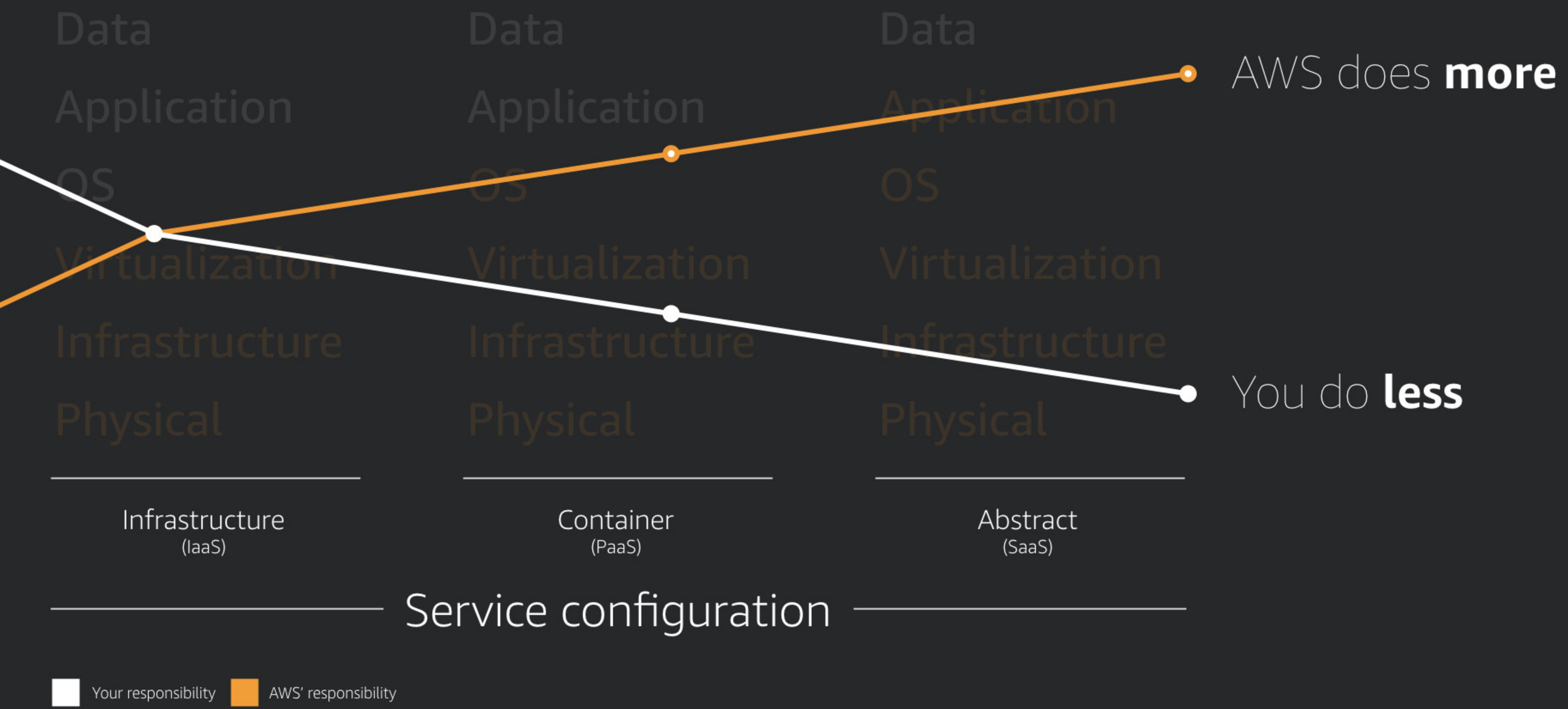
Abstract
(SaaS)

Service configuration

Your responsibility

AWS' responsibility

The Shared Responsibility Model



What’s stopping us?

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.


Hackers

Nation State



Insider Threats



Courtesy of the fantastic @quinnypig


STOP


Mistakes & Misconfigurations

Our goal

Make sure that systems work as intended and only as intended

Largest risk

Mistakes & misconfigurations

Can I learn from others?

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cloud Adoption Framework

Cloud Adoption Framework



Business



People



Governance

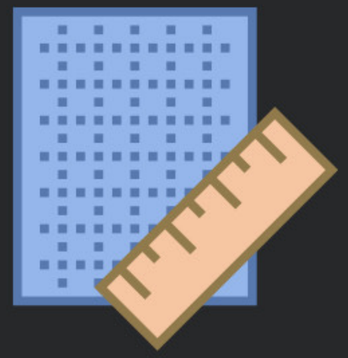
Cloud Adoption Framework



Business



People



Platform



Security



Governance



Operations

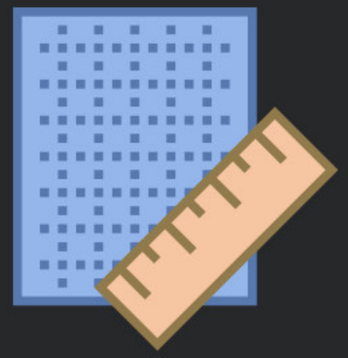
Cloud Adoption Framework



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



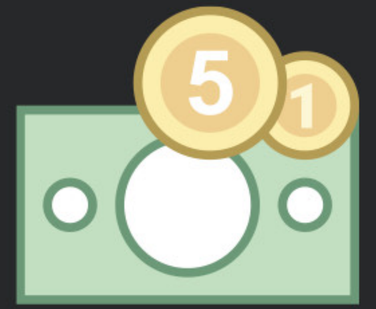
Security



Reliability



Performance Efficiency



Cost Optimization

AWS Well-Architected Framework



Operational Excellence



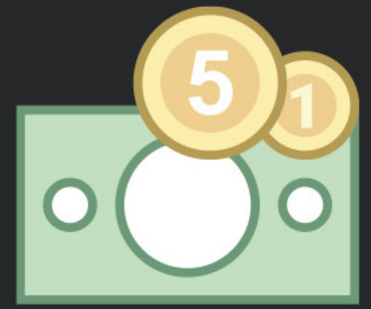
Security



Reliability



Performance Efficiency



Cost Optimization

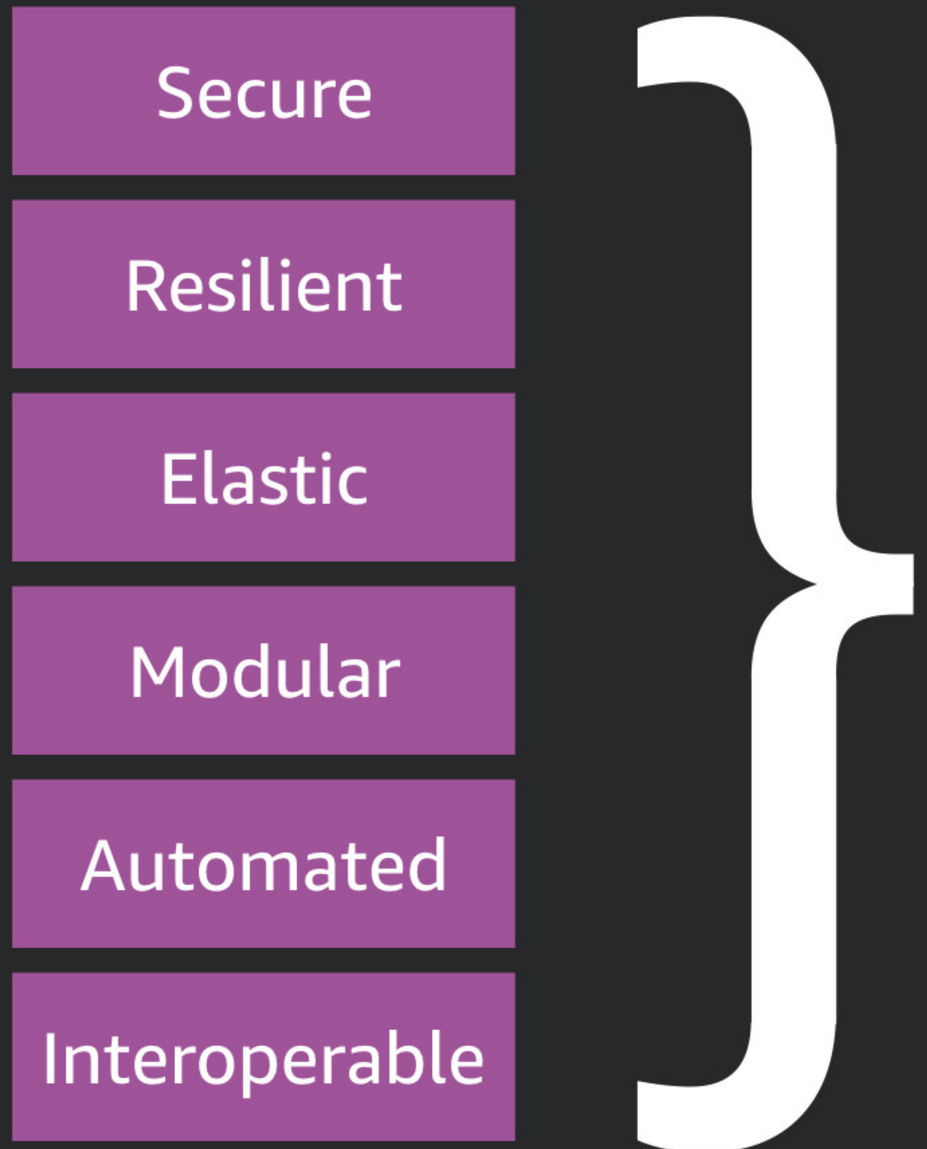
Helps you make smart trade-offs

Modern Application Design

Modern Application Design

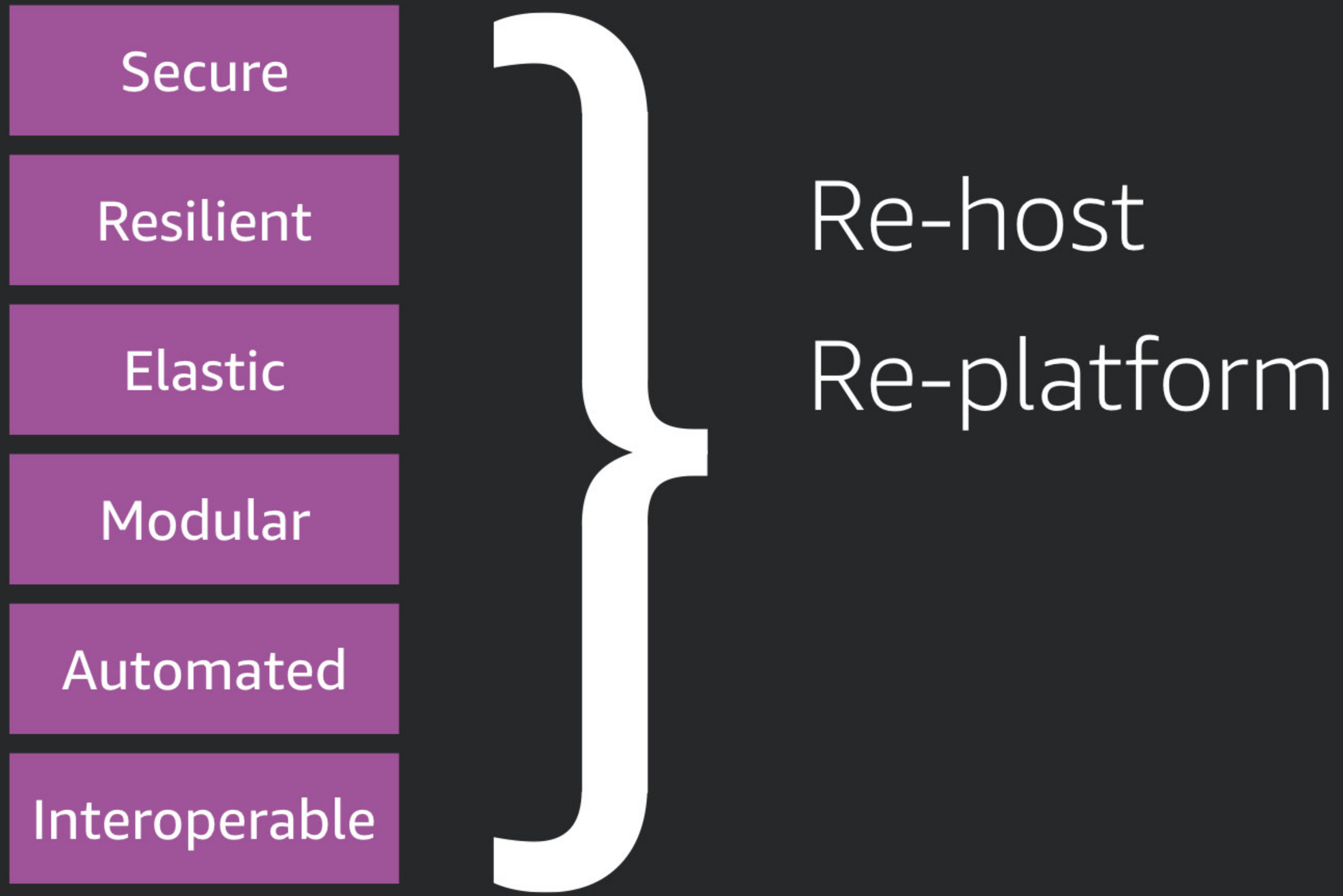
- Secure
- Resilient
- Elastic
- Modular
- Automated
- Interoperable

Modern Application Design

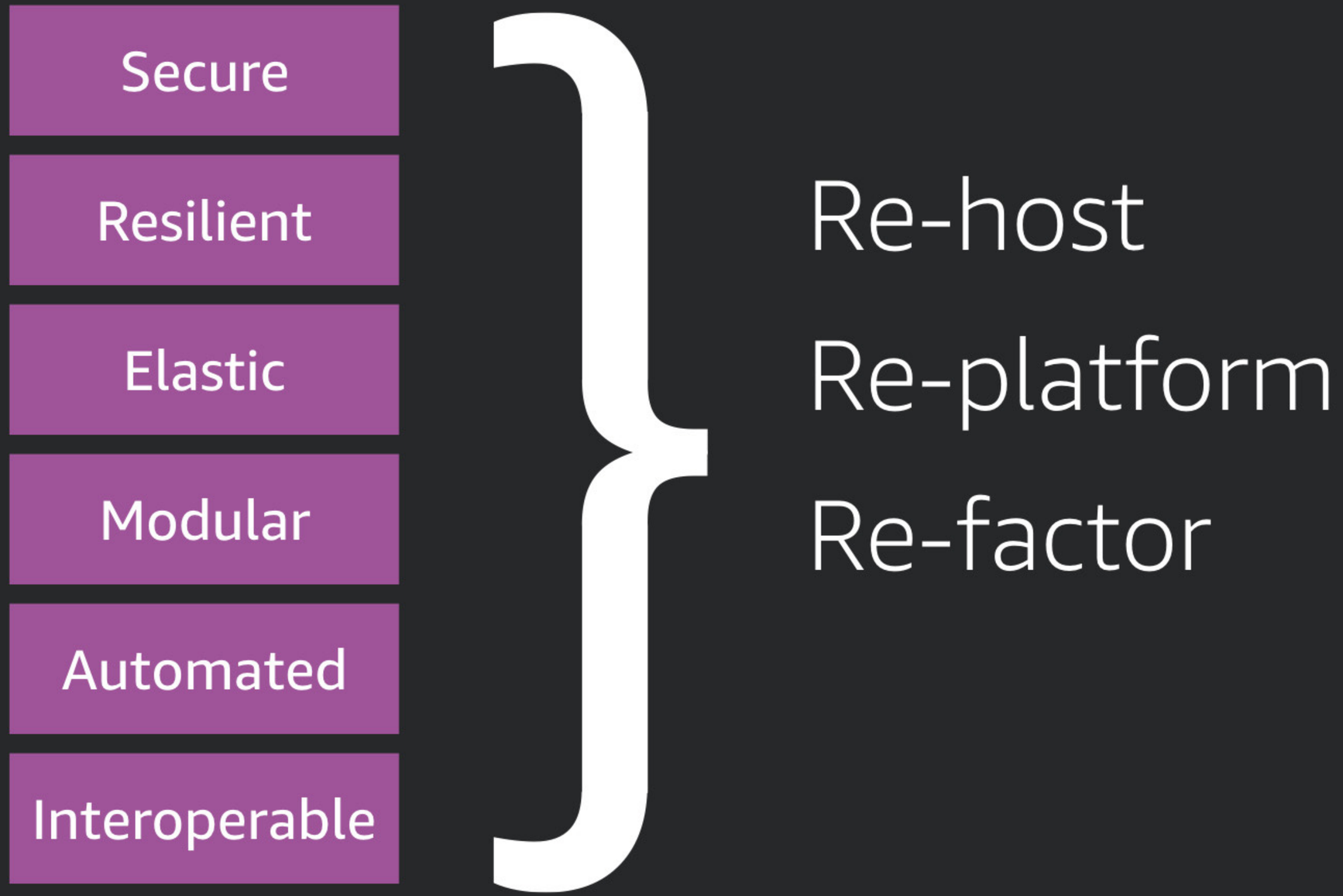


Re-host

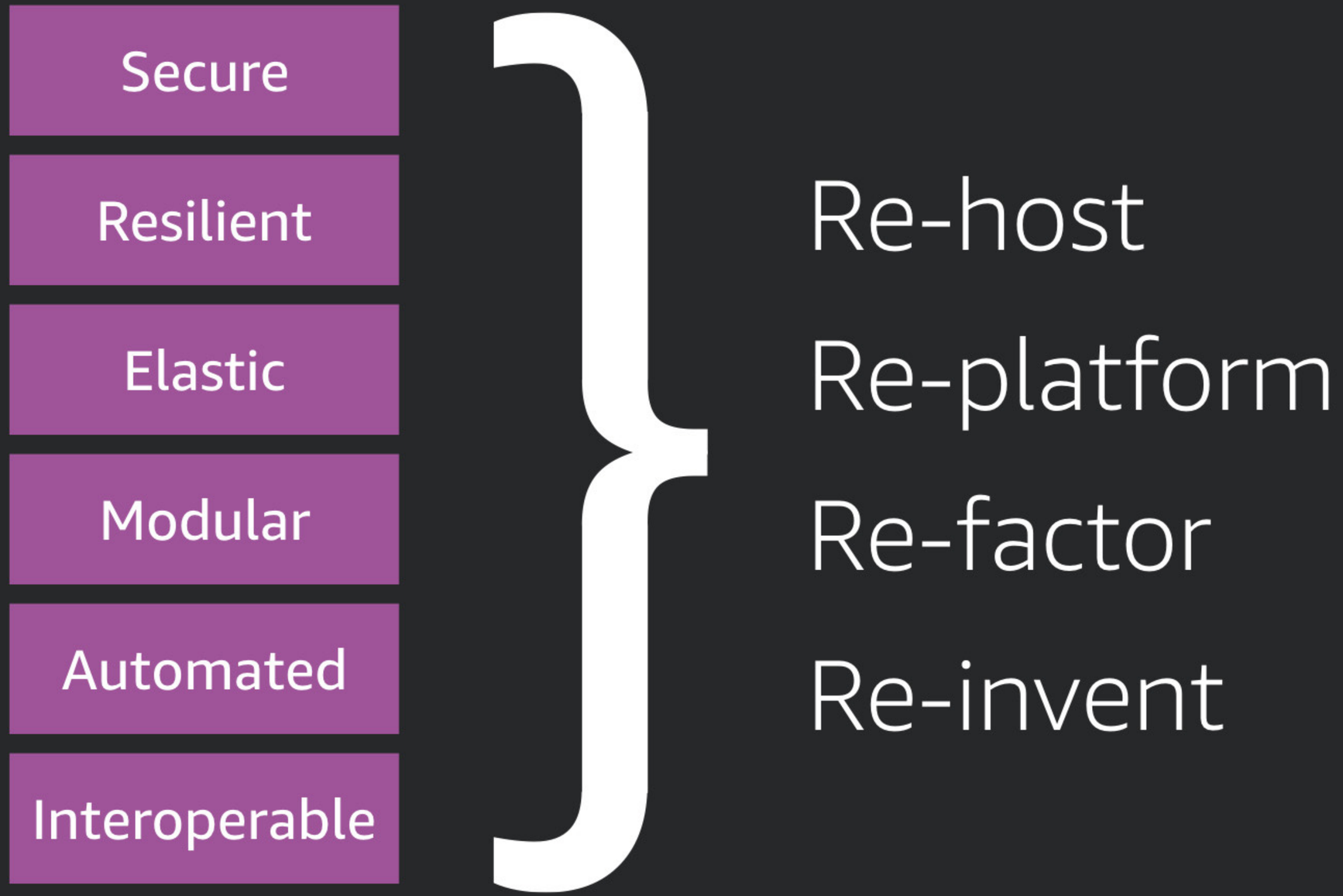
Modern Application Design



Modern Application Design



Modern Application Design



CIS AWS Foundations

CIS AWS Foundations



CIS AWS Foundations



Prescriptive guidance

CIS AWS Foundations



Prescriptive guidance

Strong baseline

CIS AWS Foundations



Prescriptive guidance

Strong baseline

Checklist of tasks

What happened?

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.


Auditing



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?

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.


Identity
PASSPORT
Visas
Sorties / Salidas
LFT LUNDRES
A 138
Canada
104
SEP 07 2008
CALGARY
701
DEPARTMENT OF HOMELAND SECURITY
JAN 1

The Principle of Least Privilege



The Principle of Least Privilege



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



AWS Identity and Access Management



AWS Identity and Access Management

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

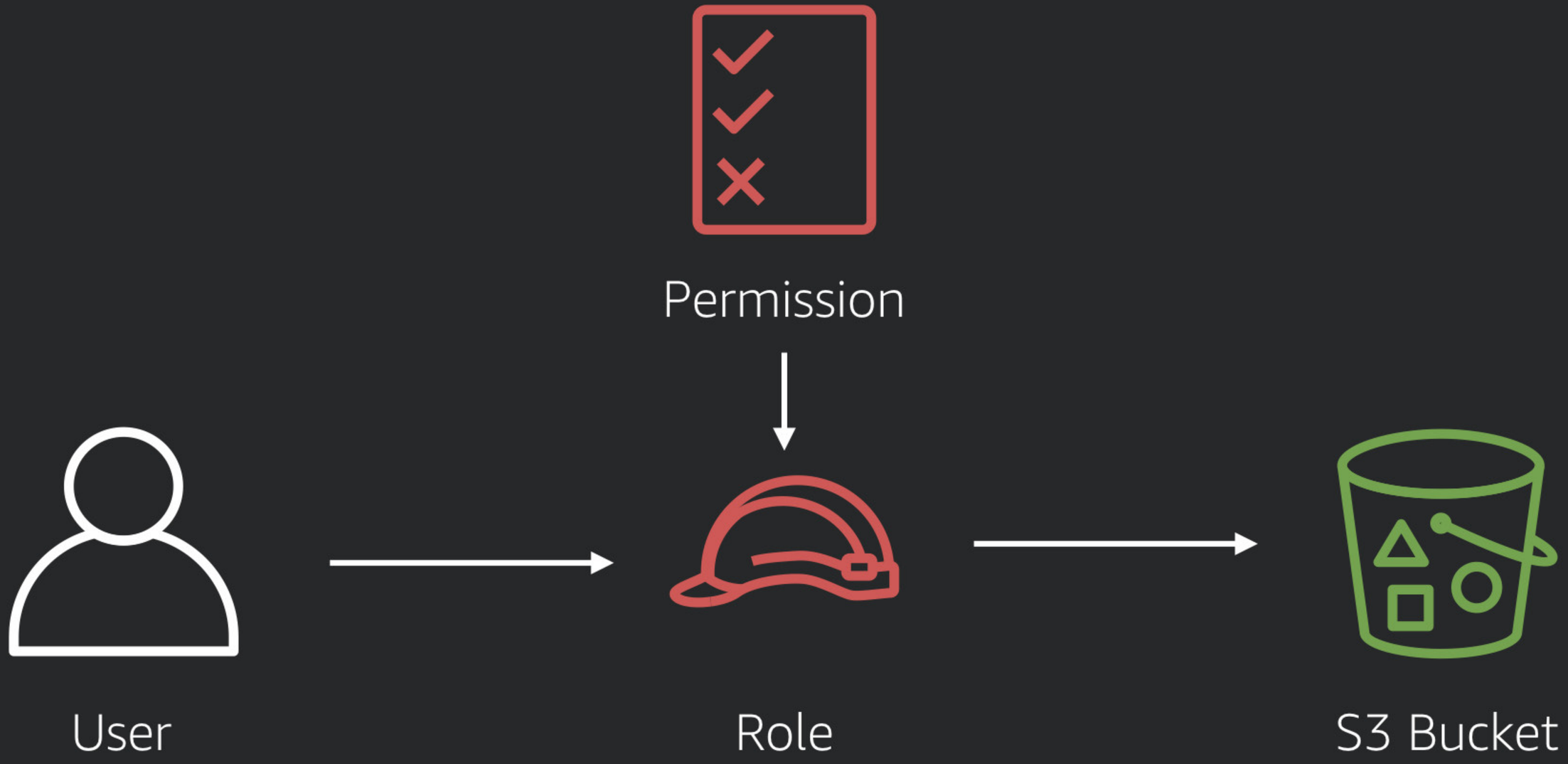
Works fine
Unmanageable a scale
Not granular enough



User

Permission

S3 Bucket


Permission
User
Role
S3 Bucket



AWS IAM



AWS IAM

SEC209

Getting started with AWS Identity



AWS IAM

SEC209

Getting started with AWS Identity

SEC316

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

Website

IAM Best Practices

https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

How can I protect my network?

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.



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 allow access to AWS services



Your own slice of the AWS Cloud

- Controllable routing, IP space, subnetting, and access control
- VPC Endpoints allow access to AWS services
- AWS PrivateLink connects to third party SaaS



Your own slice of the AWS Cloud

- Controllable routing, IP space, subnetting, and access control
- VPC Endpoints allow access to AWS services
- AWS PrivateLink connects to third 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, AWS Transit Gateway is a simpler way to connect



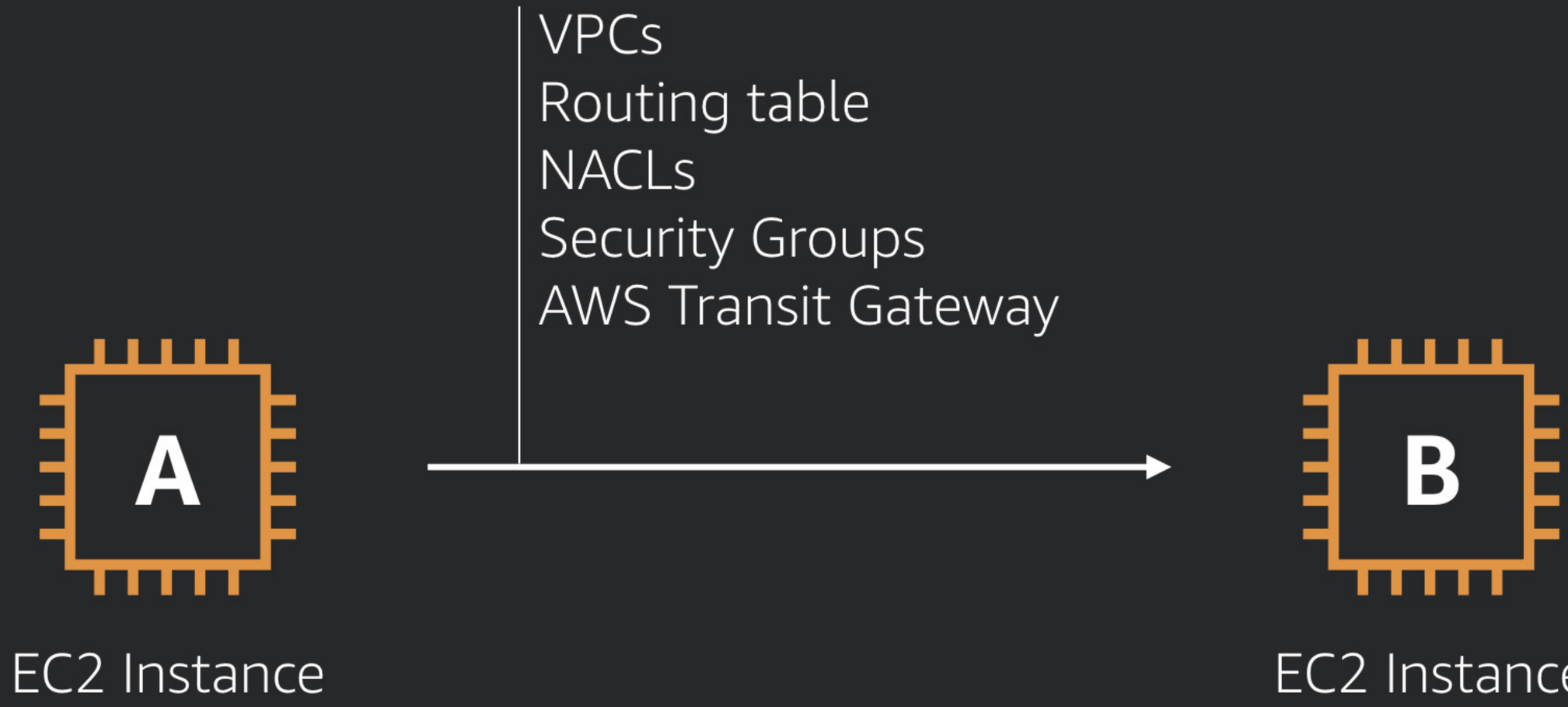
Make connecting everything easier

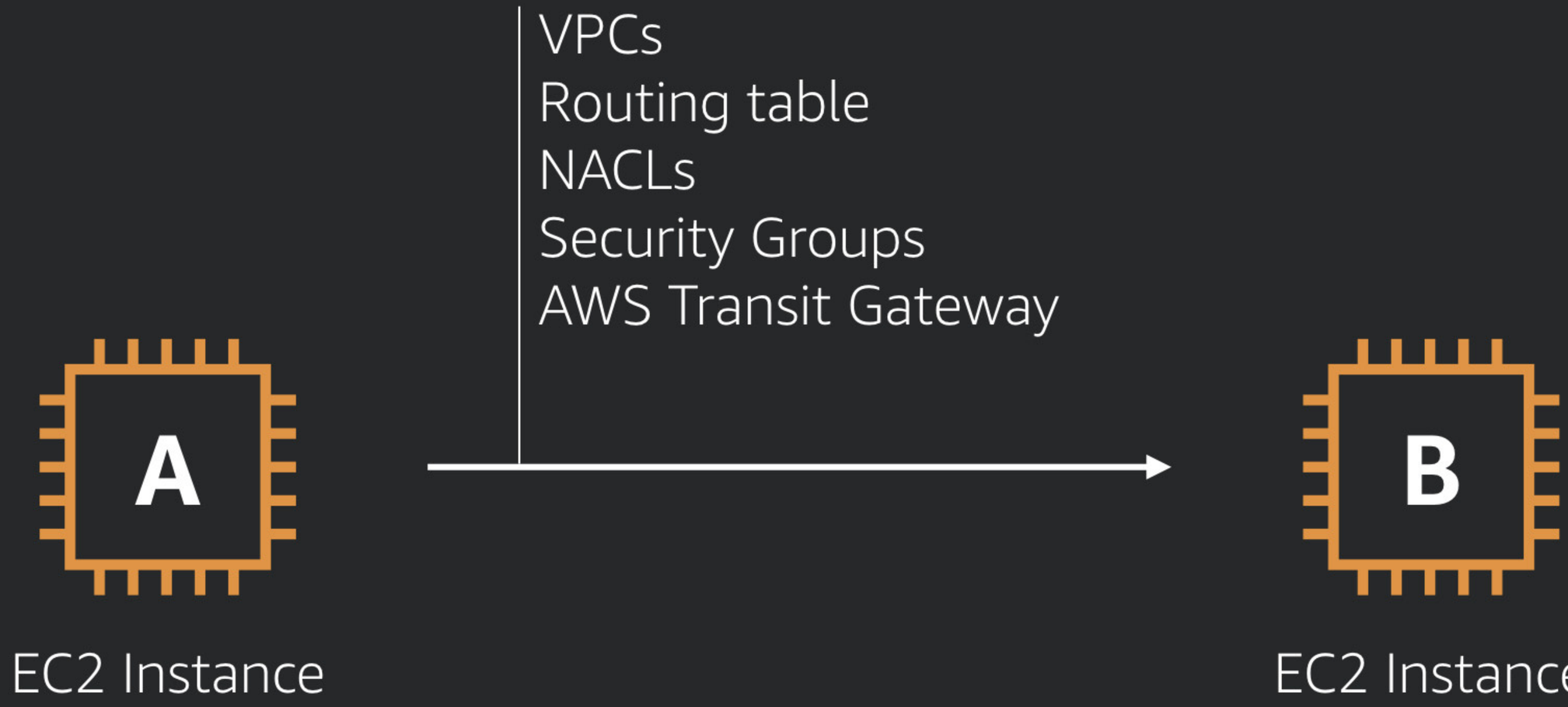
- If you have multiple VPCs or will soon, AWS Transit Gateway is a simpler way to connect
- Simplified advanced network design



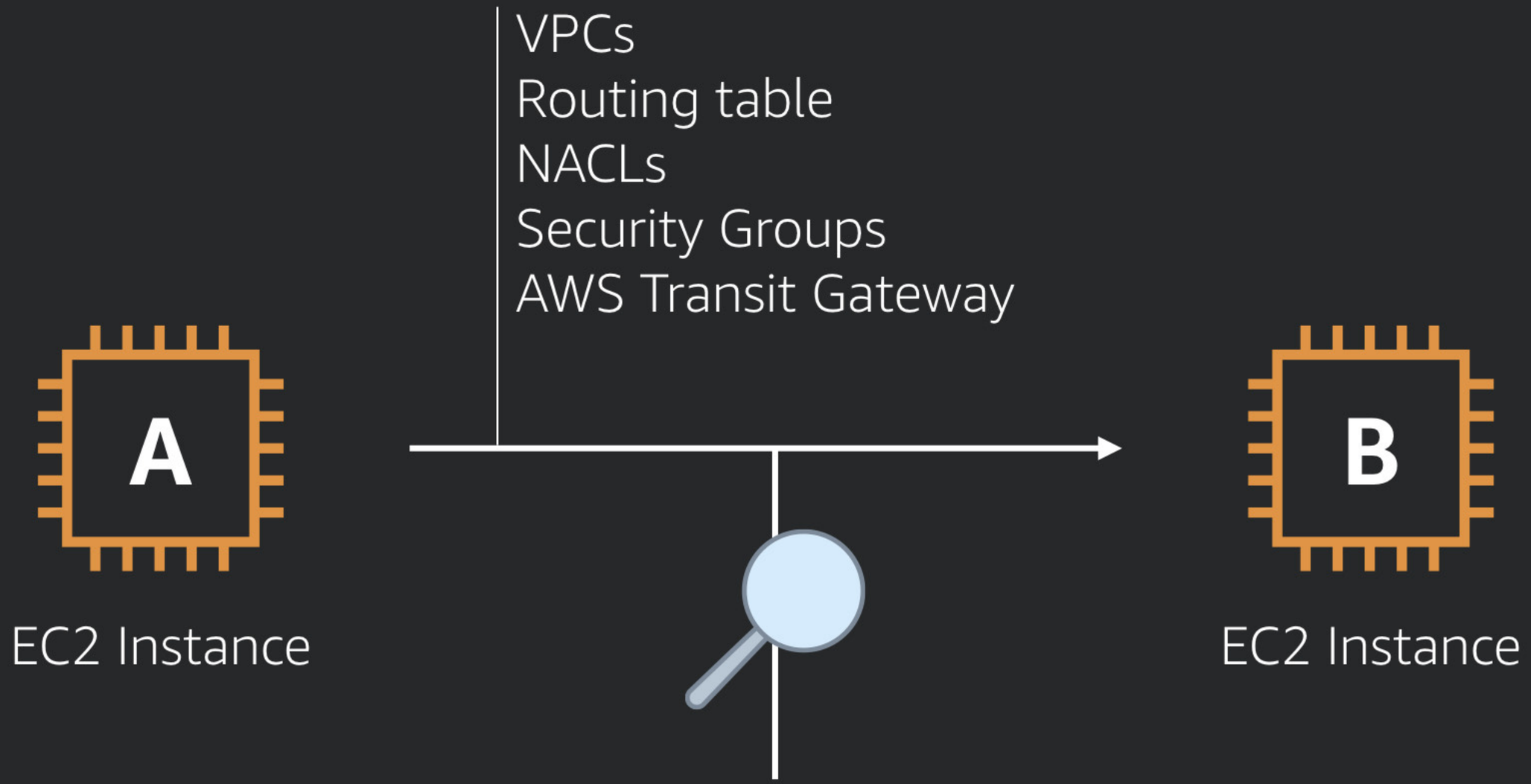
Make connecting everything easier

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


VPCs
Routing table
NACLs
Security Groups
AWS Transit Gateway
A
B
EC2 Instance
EC2 Instance



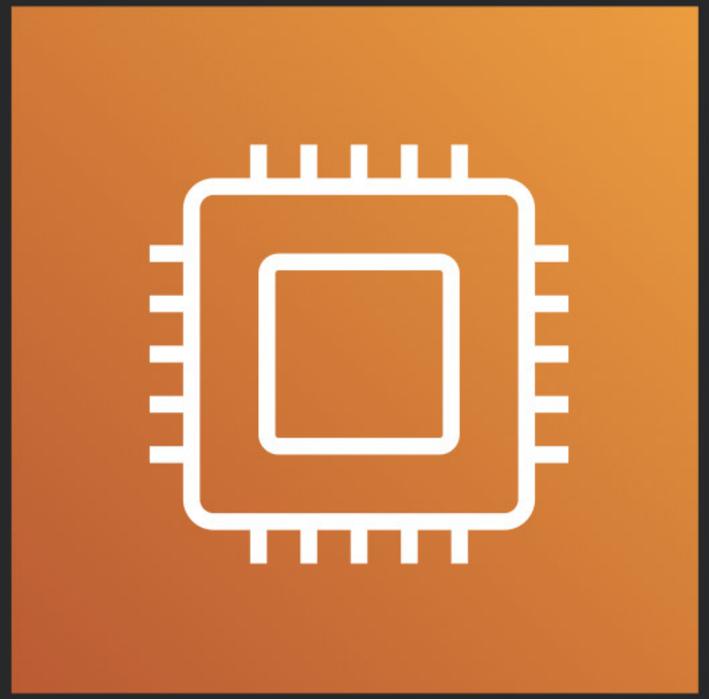
Is **A** allowed to talk to **B**?



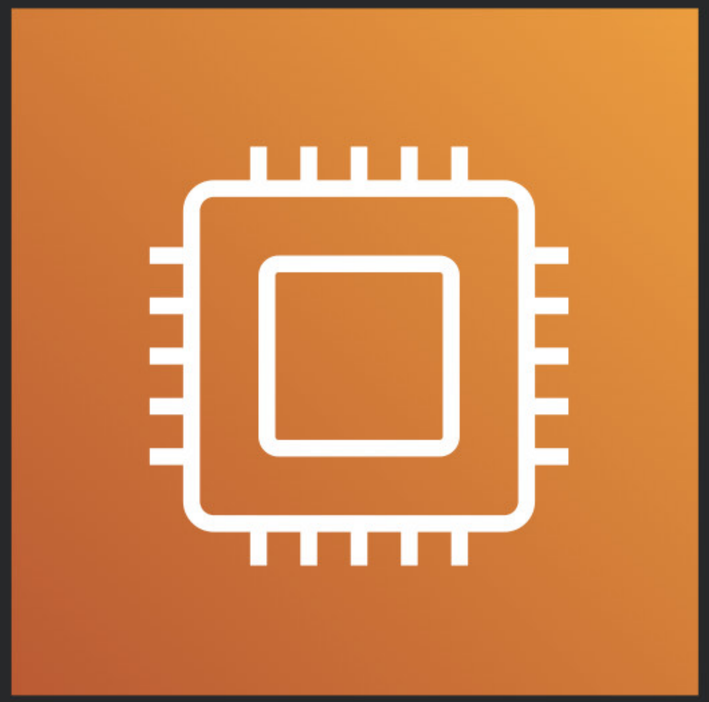
What are they saying? **IPS**

How do I protect compute?

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

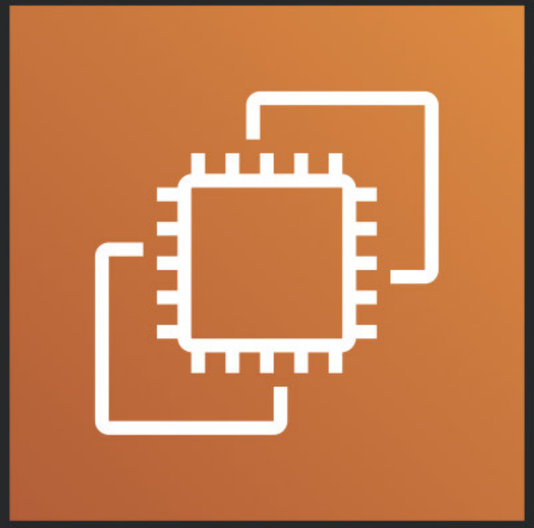


Compute



Compute

Running code in the cloud



Amazon EC2

Instances

Data

Application

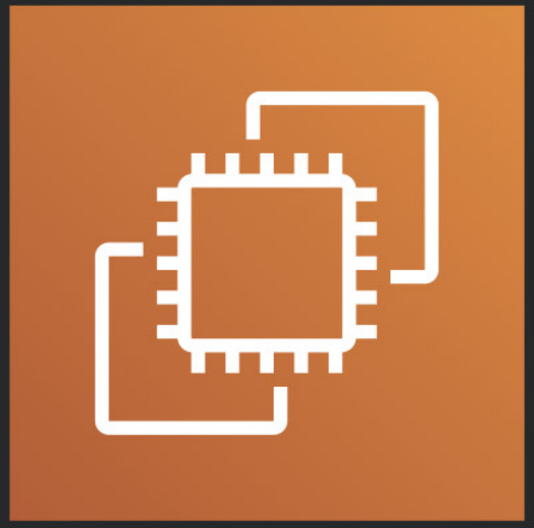
OS

Virtualization

Infrastructure

Physical

Infrastructure
(IaaS)



Amazon EC2

Instances

Data
Application
OS
Virtualization
Infrastructure
Physical

Infrastructure
(IaaS)

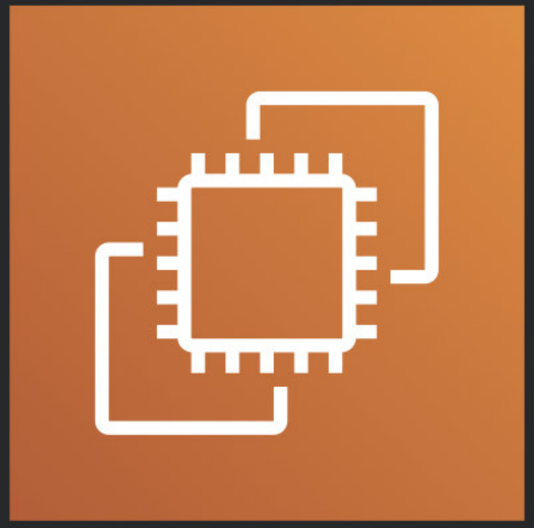


Amazon ECS

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)

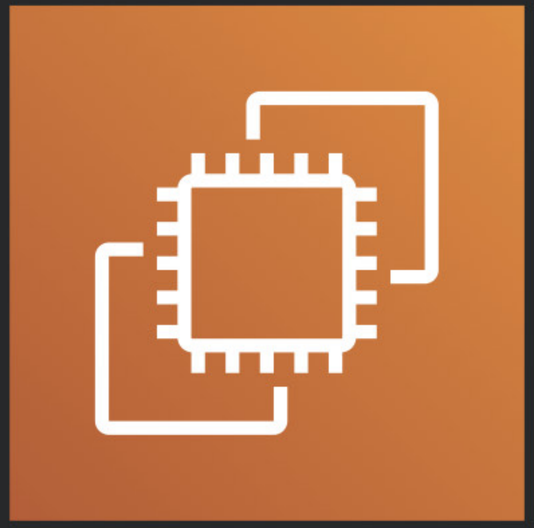


AWS Fargate

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)

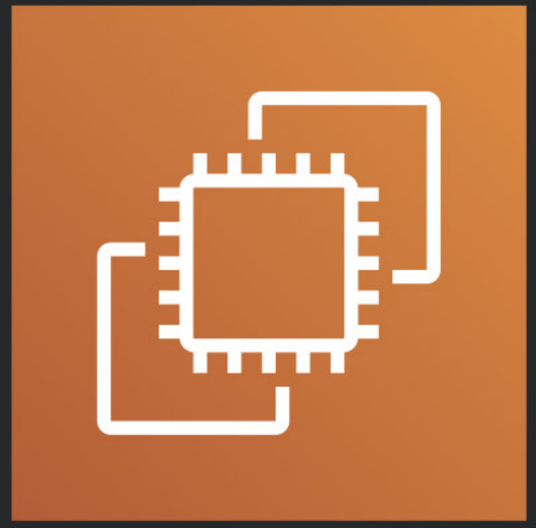


AWS Lambda

Functions

Data
Application
OS
Virtualization
Infrastructure
Physical

Abstract
(SaaS)



Amazon EC2

Instances



Amazon ECS

Containers + Host



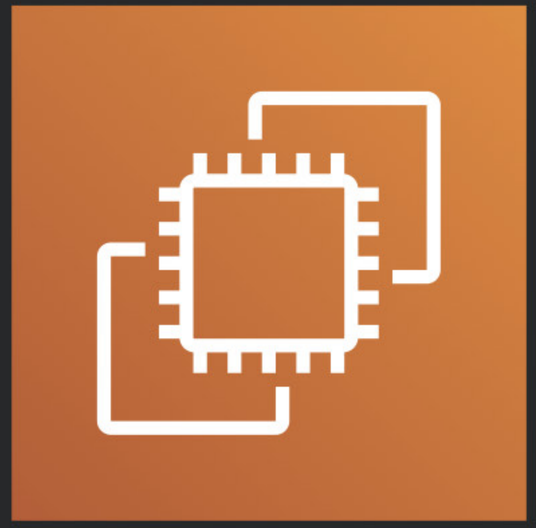
AWS Fargate

Managed Containers



AWS Lambda

Functions



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

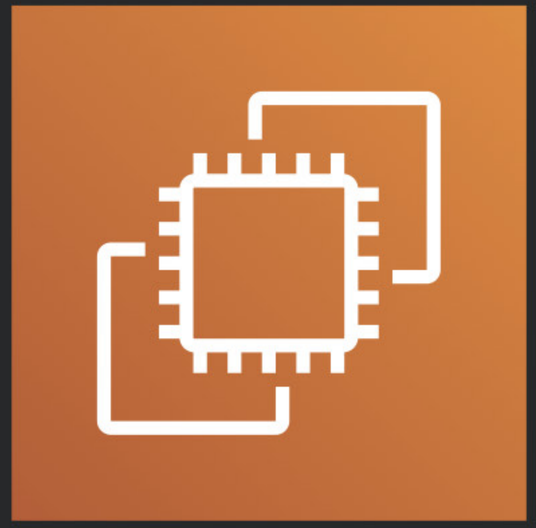
Managed Containers



AWS Lambda

Functions

- Harden the OS configuration



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

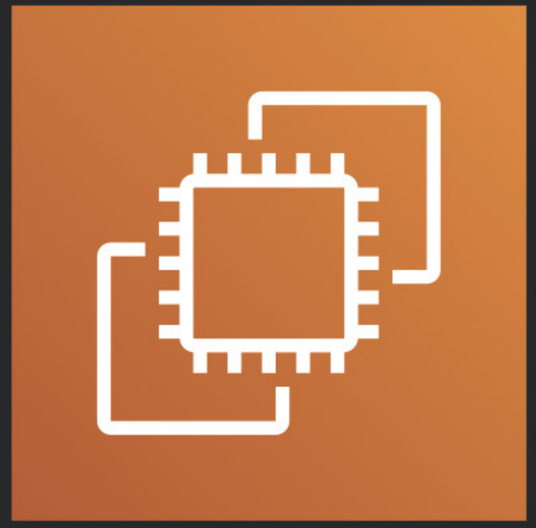
Managed Containers



AWS Lambda

Functions

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



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

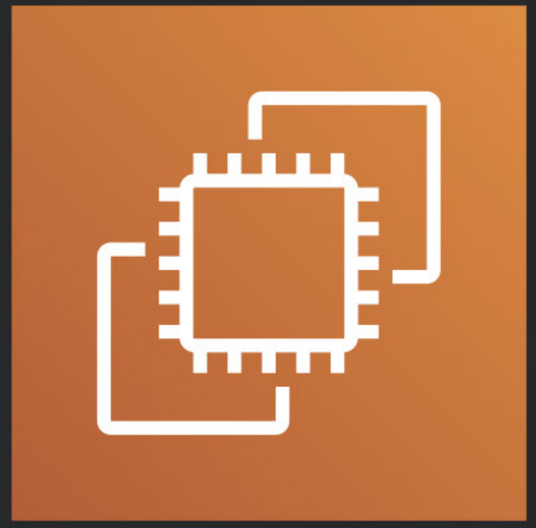
Managed Containers



AWS Lambda

Functions

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



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

Managed Containers

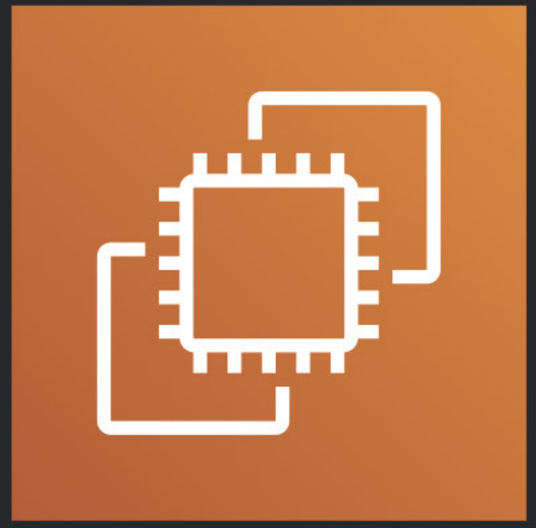


AWS Lambda

Functions

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

- Code quality is a priority



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

Managed Containers

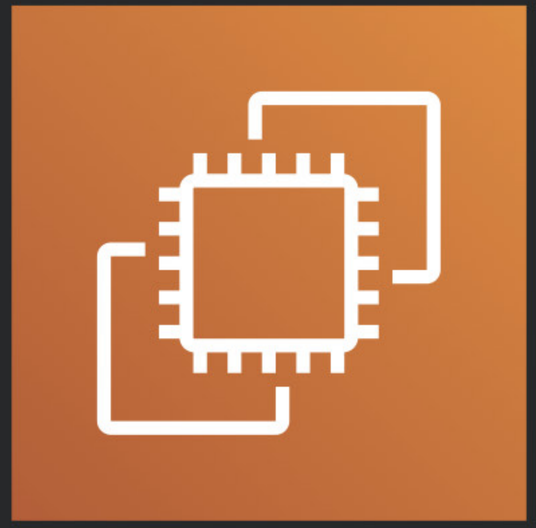


AWS Lambda

Functions

- Harden the OS configuration
- Controls like integrity monitoring, intrusion prevention, anti-malware
- Don’t patch or log in 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

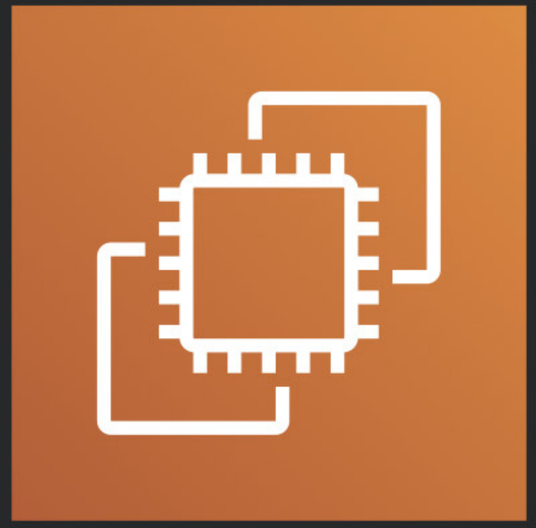


AWS Lambda

Functions

- Harden the OS configuration
- Controls like integrity monitoring, intrusion prevention, anti-malware
- Don’t patch or log in 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



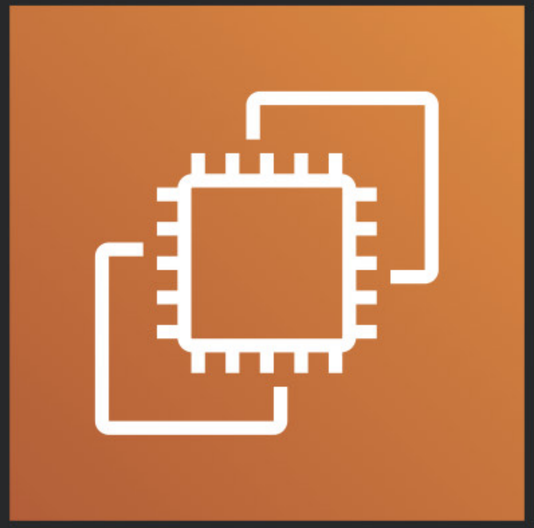
AWS Fargate

Managed Containers



AWS Lambda

Functions



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

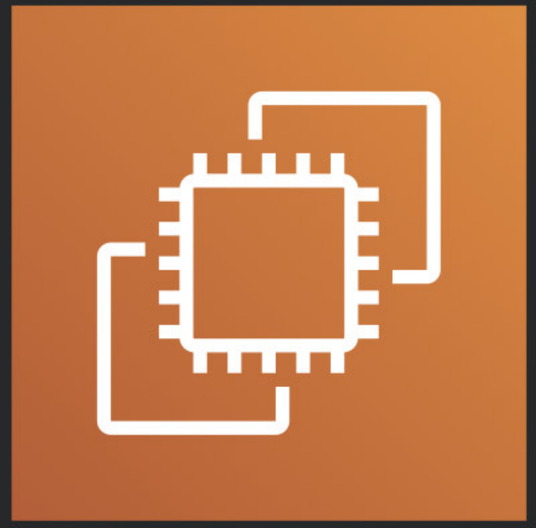
Managed Containers



AWS Lambda

Functions

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



Amazon EC2

Instances



Amazon ECS

Containers + Host



AWS Fargate

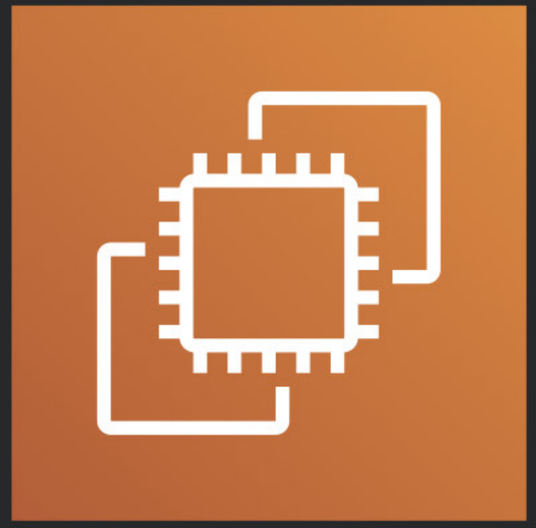
Managed Containers



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

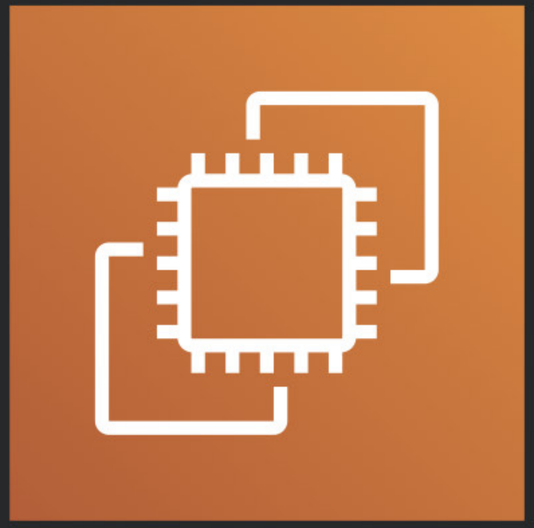
Managed Containers



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

How do I protect my data?

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.



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
- Back up 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 S3 Glacier, Amazon Elastic File System, etc.



Structured, accessible data but in files

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

- Encrypt the data at rest



Structured, accessible data but in files

Amazon Elastic Block Store, Amazon FSx, Amazon S3, Amazon S3 Glacier, Amazon Elastic 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 S3 Glacier, Amazon Elastic 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?

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Observability



Traceability

Traceability

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

Traceability

Traceability

Where did this come from?
Who can access it?
When?

Observability

Observability

The ability to infer internal states from external outputs

Observability

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 are an excellent trigger for automation via AWS Lambda

Automation

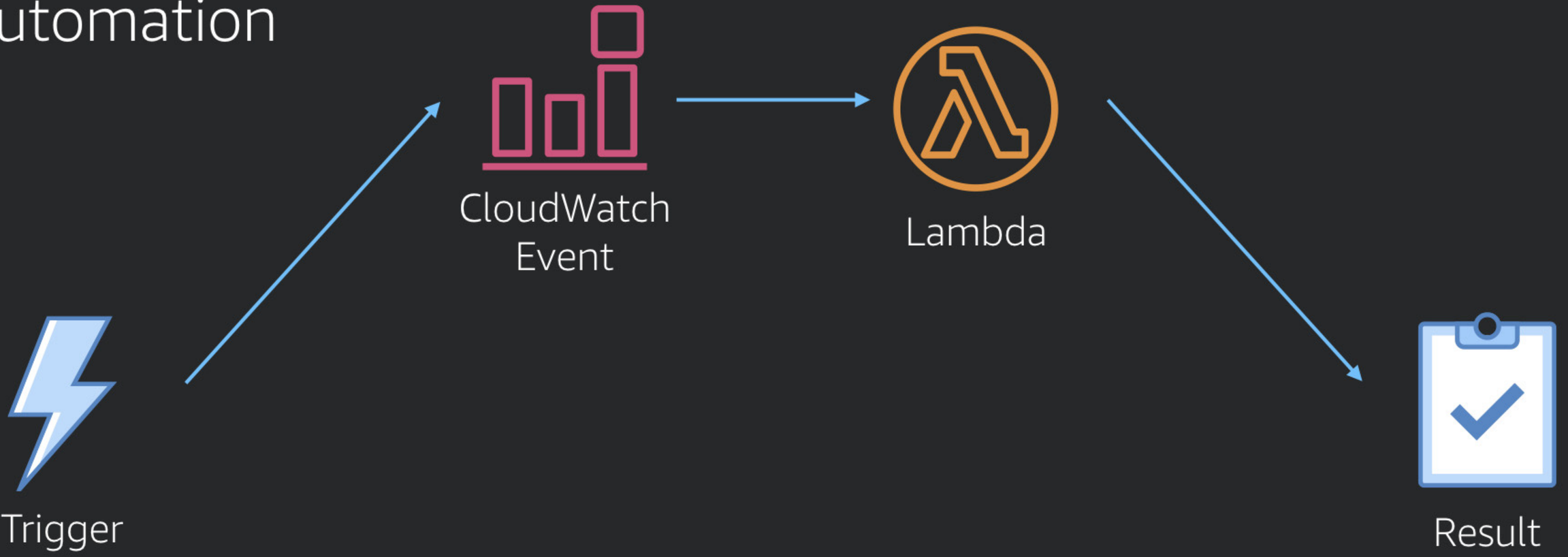


Trigger

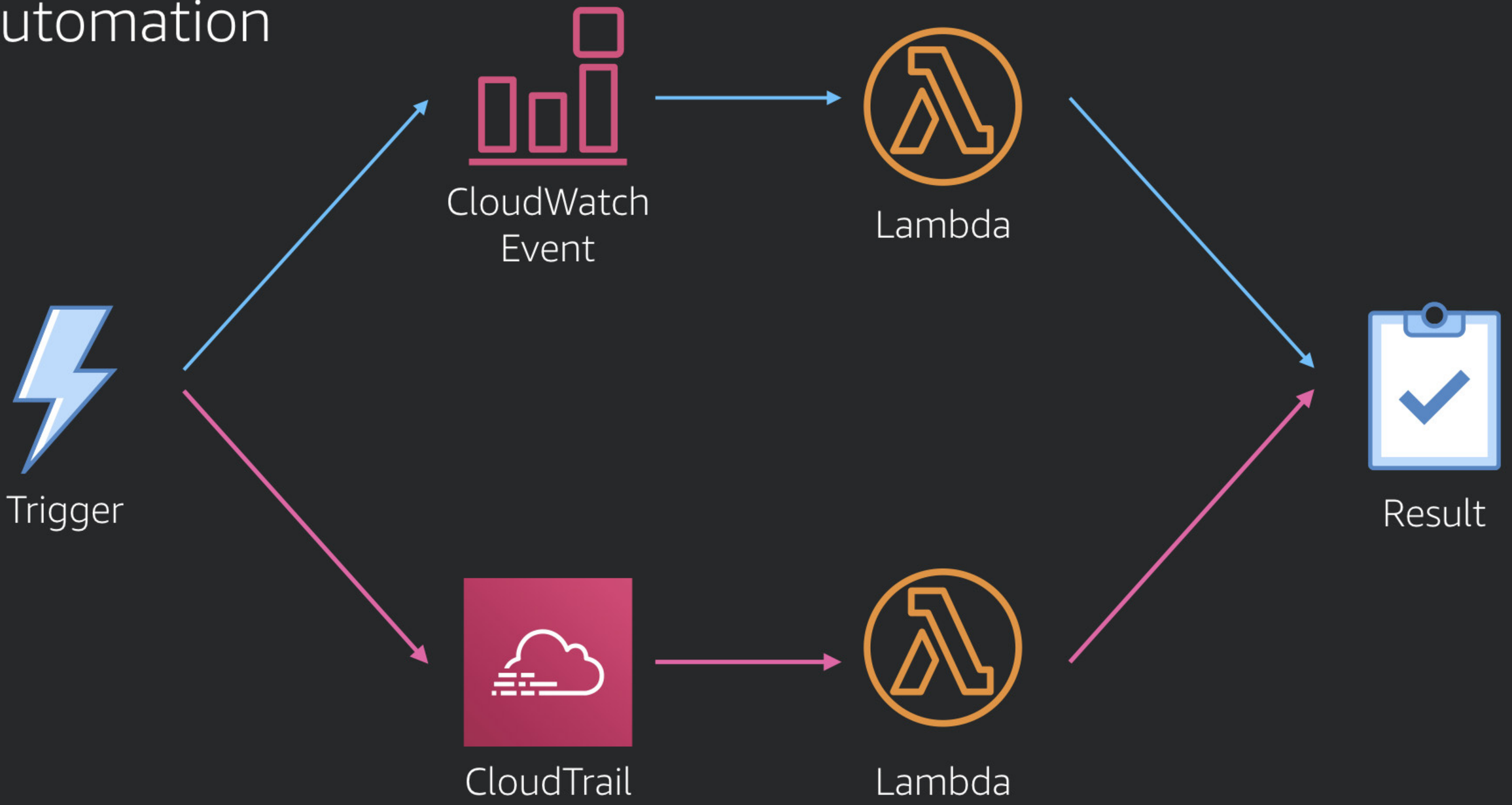


Result

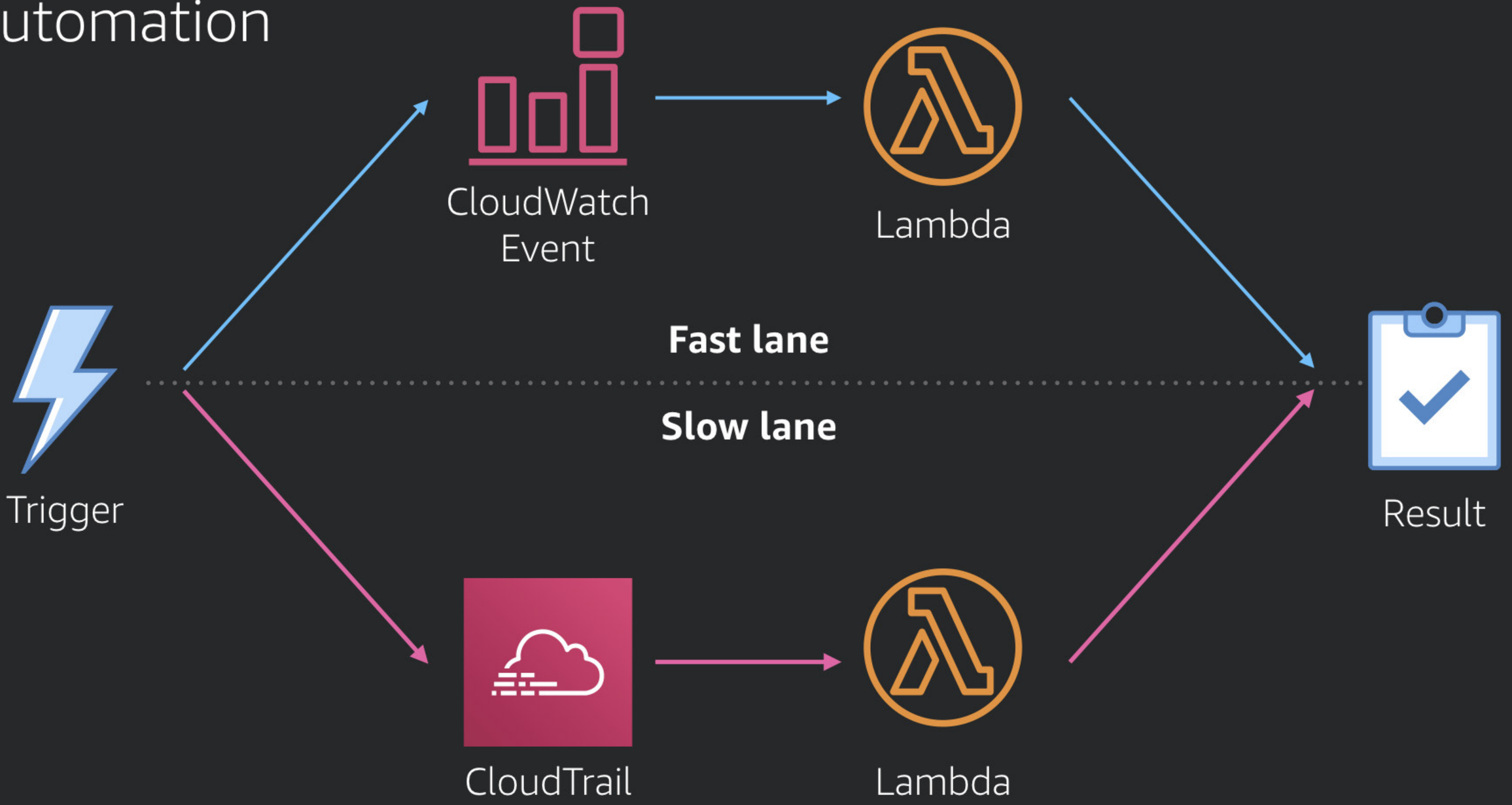
Automation



Automation


CloudWatch
Event
Lambda
Trigger
Result
CloudTrail
Lambda

Automation


CloudWatch Event
Lambda
Fast lane
Slow lane
Trigger
Result
CloudTrail
Lambda

Keys to success

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

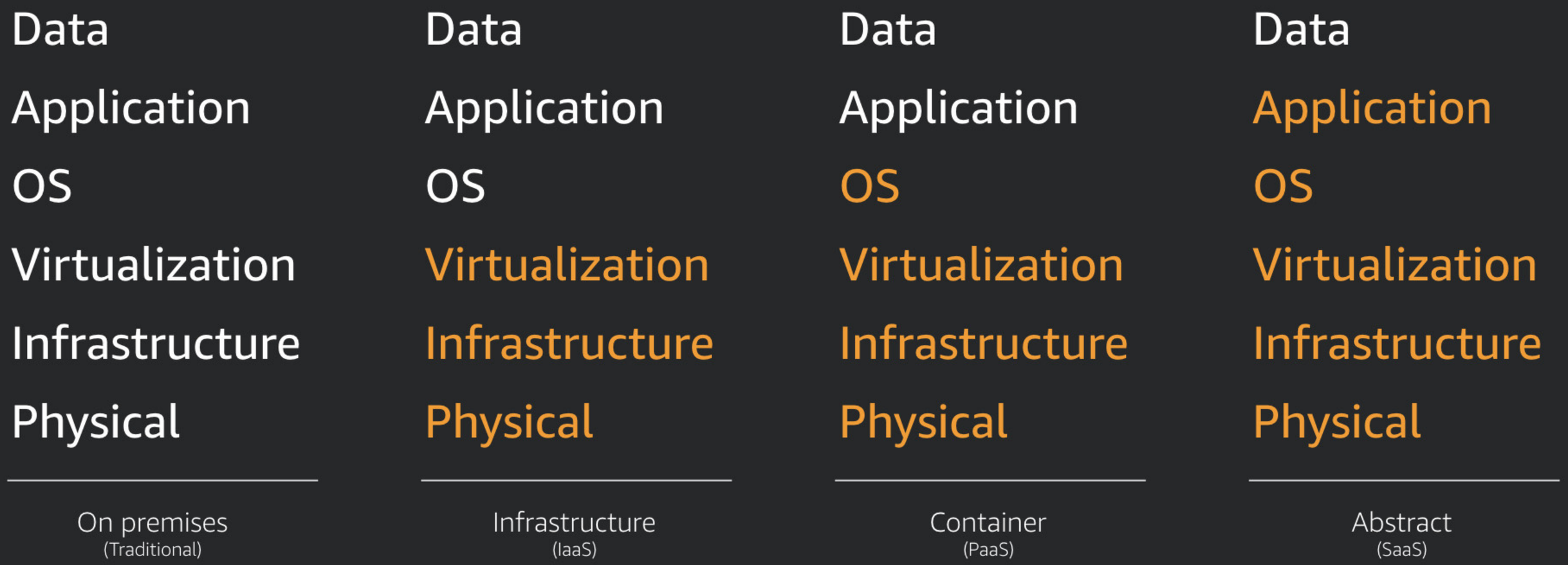
The cloud simplifies security.

* 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 MICRO™

Cloud security simplified

Visit Trend Micro in booth #2820

Thank you!



Mark Nunnikhoven
Vice President, Cloud Research at Trend Micro
@marknca

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey in the mobile app.

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.