AWS Security & Cloud Fundamentals

Bill Ohlson
Executive Security Advisor
Latin America, Canada & Caribbean
World Wide Public Sector, Amazon Web Services

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

1. Intro
2. Cloud Fundamentals
3. Design Patterns
4. Additional References, Resources and/or Questions

© 2022, Amazon Web Services, Inc. or its affiliates.

Intro

- Bill Ohlson
- ~2.5 years at AWS
- ~10 Information Security experience
- ~24 years IT experience
  - Including startups, investment banking, and payments

© 2020, Amazon Web Services, Inc. or its Affiliates.

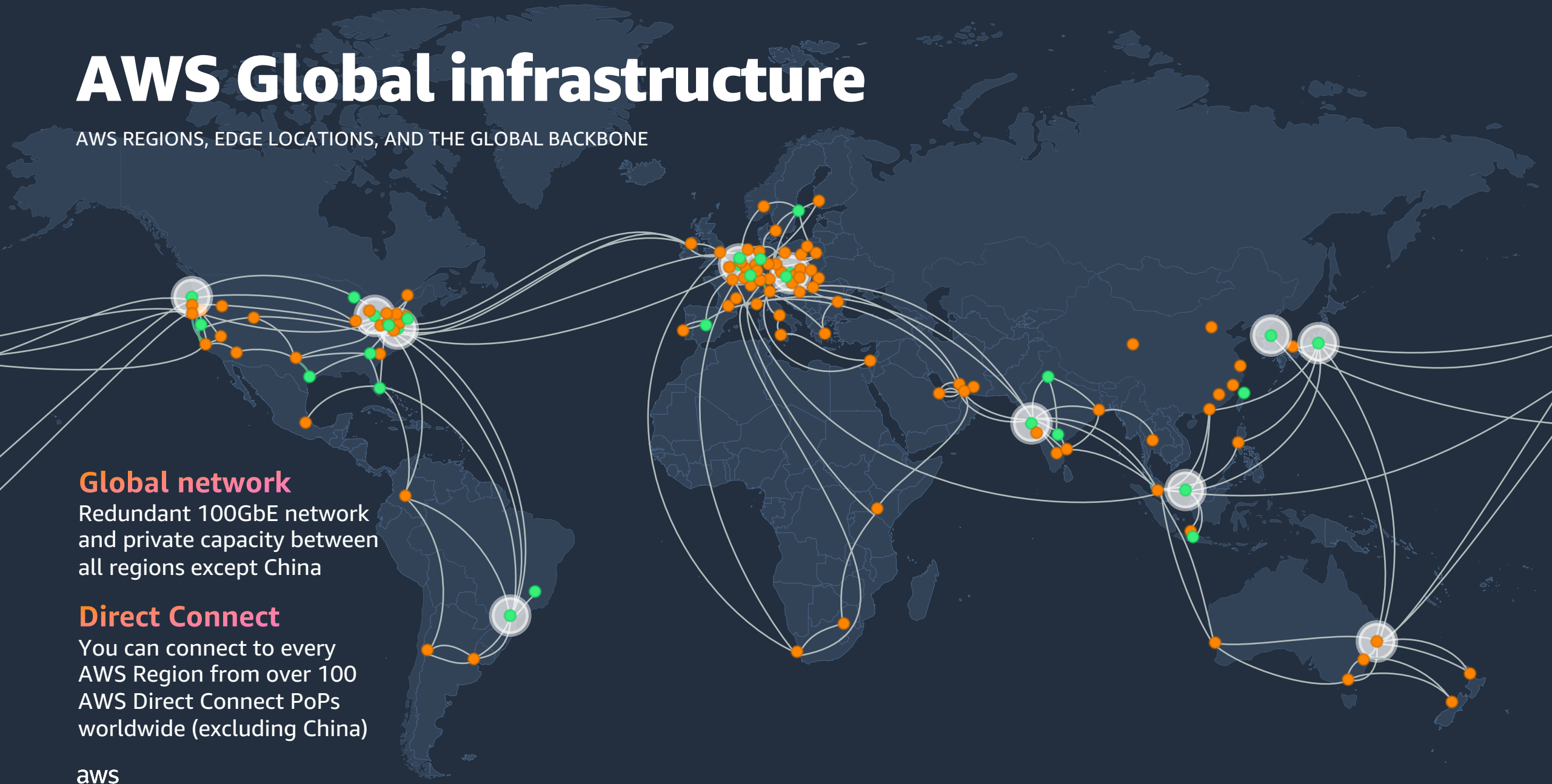
aws

Cloud Fundamentals

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

AWS Global infrastructure

AWS REGIONS, EDGE LOCATIONS, AND THE GLOBAL BACKBONE



Global network

Redundant 100GbE network and private capacity between all regions except China

Direct Connect

You can connect to every AWS Region from over 100 AWS Direct Connect PoPs worldwide (excluding China)

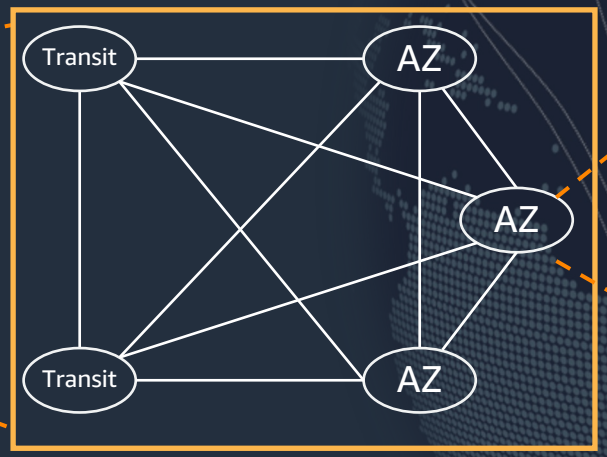
aws

© 2022, Amazon Web Services, Inc. or its affiliates.

AWS Region design

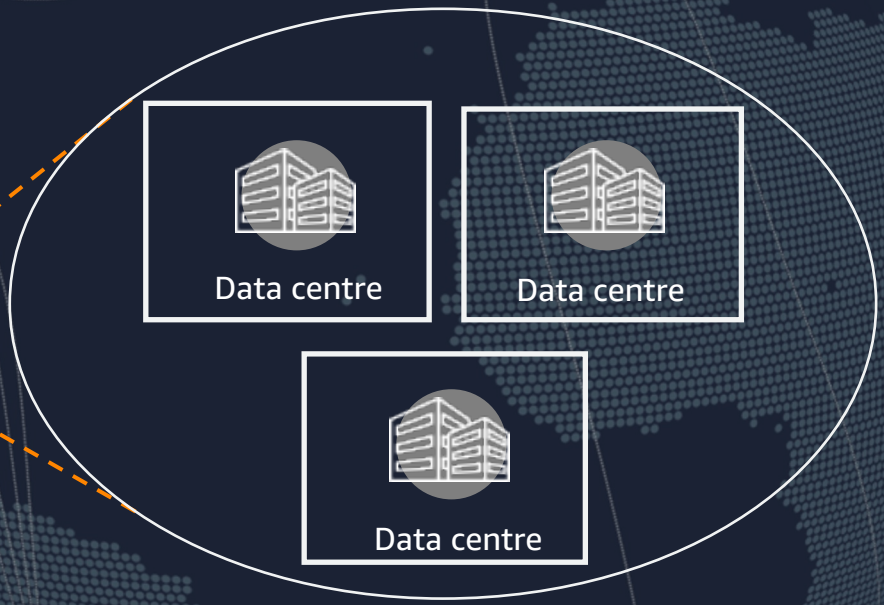
AWS Regions are comprised of multiple Availability Zones (AZs) for high availability, high scalability, and high fault tolerance. Applications and data are replicated in real time and consistent in the different AZs.

AWS Canada Region



A **Region** is a physical location in the world where we have multiple **AZs.**

AWS AZ



AZs consist of one or more discrete data centres, each with redundant power, networking, and connectivity, housed in separate facilities.

32 geographic Regions

102 AZs

600+ points of presence

aws

© 2022, Amazon Web Services, Inc. or its affiliates.

Calgary Region – On track for Q4 2023/Q1 2024

FULL REGION – 3 AVAILABILITY ZONES

CA$21 billion
data centre investment in Canada by 2037

CA$39 billion
increase in GDP due to construction and operation of our data centres by 2037

5,195
full-time equivalent (FTE) jobs supported through construction and operation of data centres by 2037

AWS locations in Canada

Amazon Offices
Vancouver, Winnipeg, and Toronto

AWS Regions
Montreal
Calgary (Coming Soon)

Amazon CloudFront Edge Locations
Vancouver, Toronto, and Montreal

Amazon Solar Farms
Newell, AB
Vulcan, AB

© 2022, Amazon Web Services, Inc. or its affiliates.

Why customers choose AWS

Most experience

16

years helping millions of customers

Global reach & high availability

102

availability zones spanning 32 geographic regions

Security & compliance

300+

security features

Customer obsession & innovation

200+

service offerings

AWS's Infrastructure is

3x **More Energy Efficient**

than the median of surveyed U.S. enterprise data centers

Improve TCO

111

price reductions since 2006

Machine learning

81%

of all deep learning is running on AWS[1]

Ecosystem

4,500

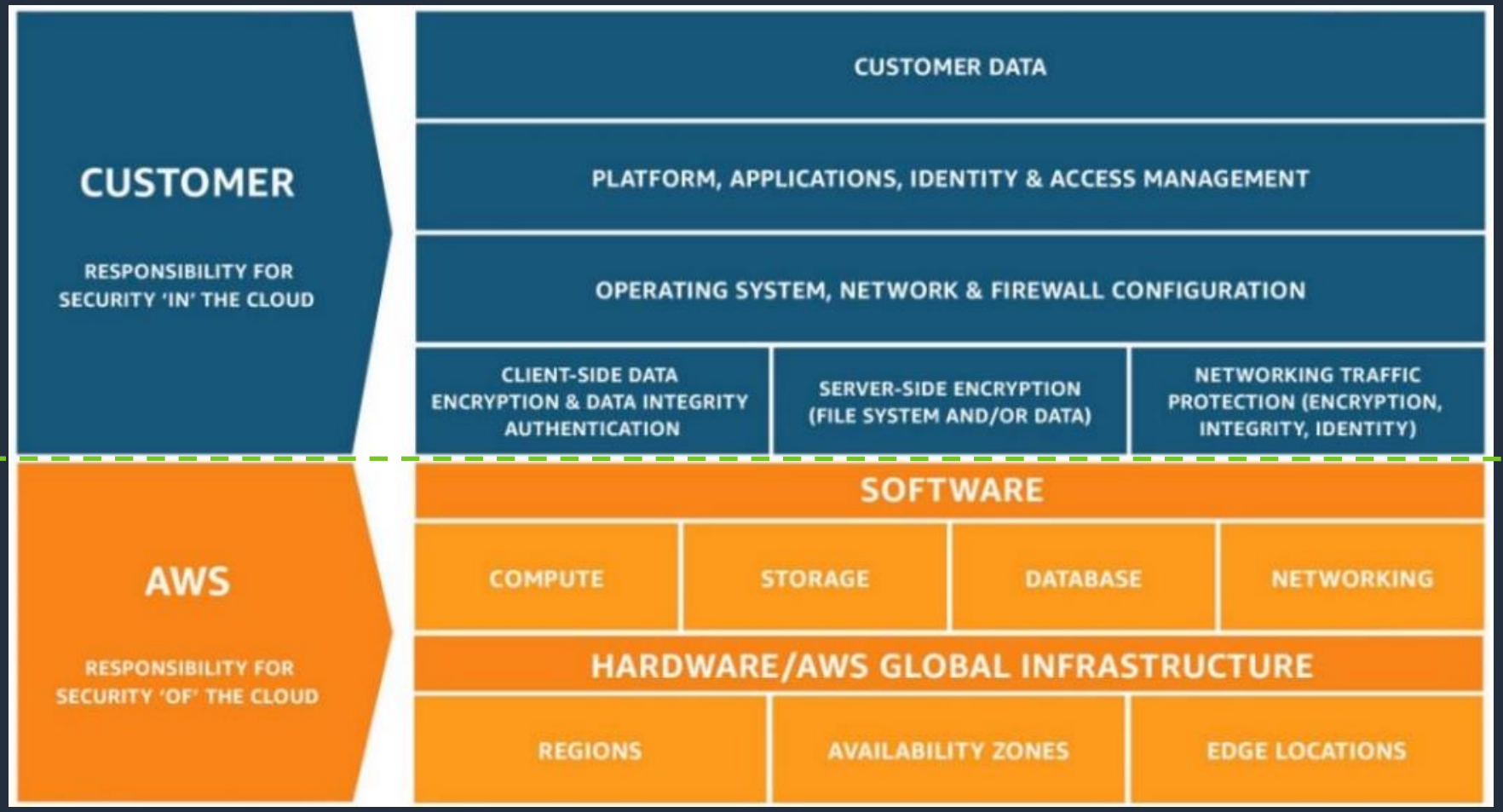
software listings from 1,400 ISVs

aws

© 2022, Amazon Web Services, Inc. or its affiliates.

Source: AWS Approved Public Stats

Understand the AWS Shared Responsibility Model



Security **IN** the Cloud

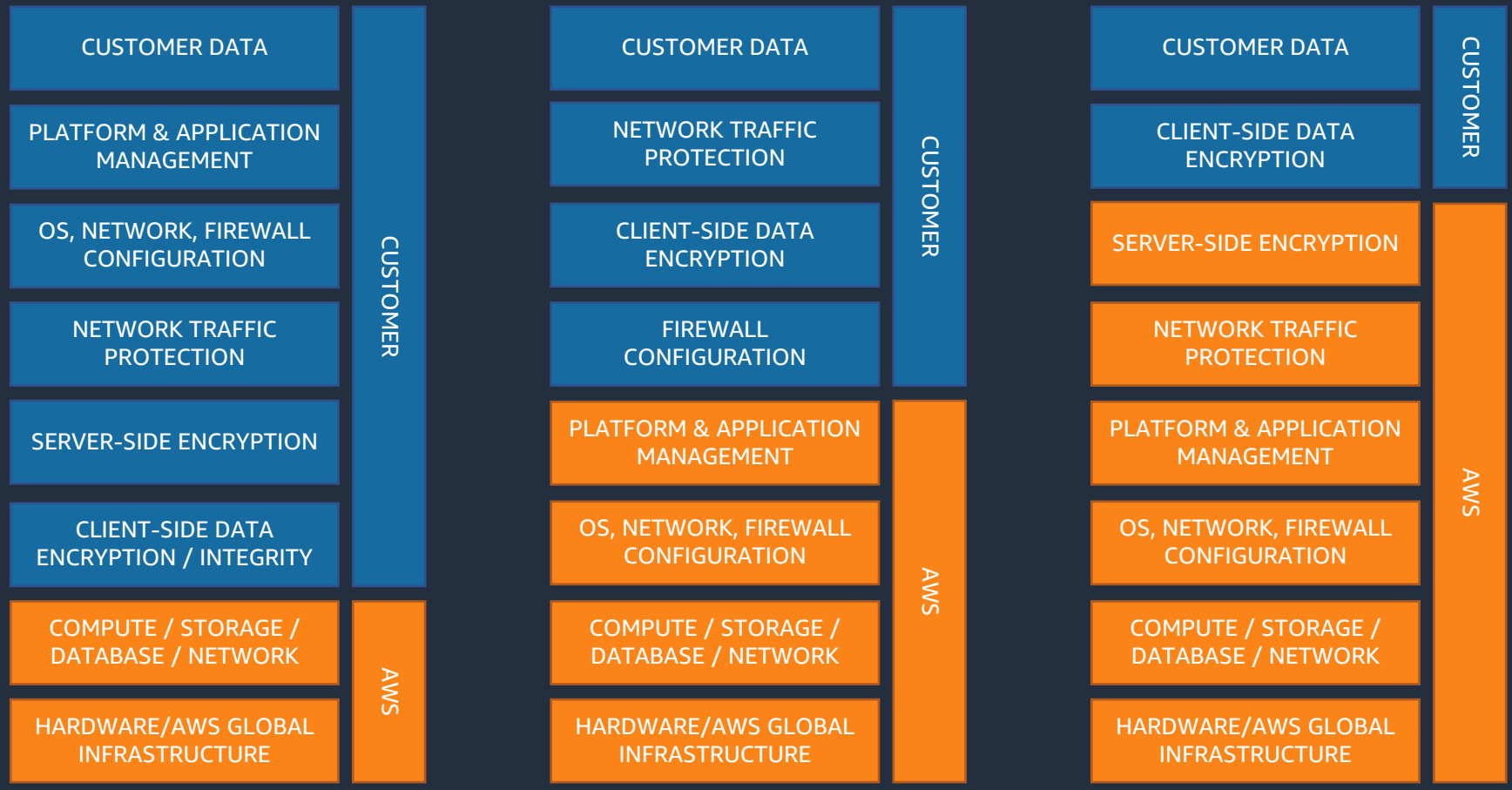
Managed by **customers**

Security **OF** the Cloud

Managed by **AWS**

© 2022, Amazon Web Services, Inc. or its affiliates.

Shared Responsibility Model is NOT static



More Customizable
+
More Customer Responsibility

Less Customizable
+
Less Customer Responsibility
+
More Best Practices built-in

© 2022, Amazon Web Services, Inc. or its affiliates.

Third Party Validation

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

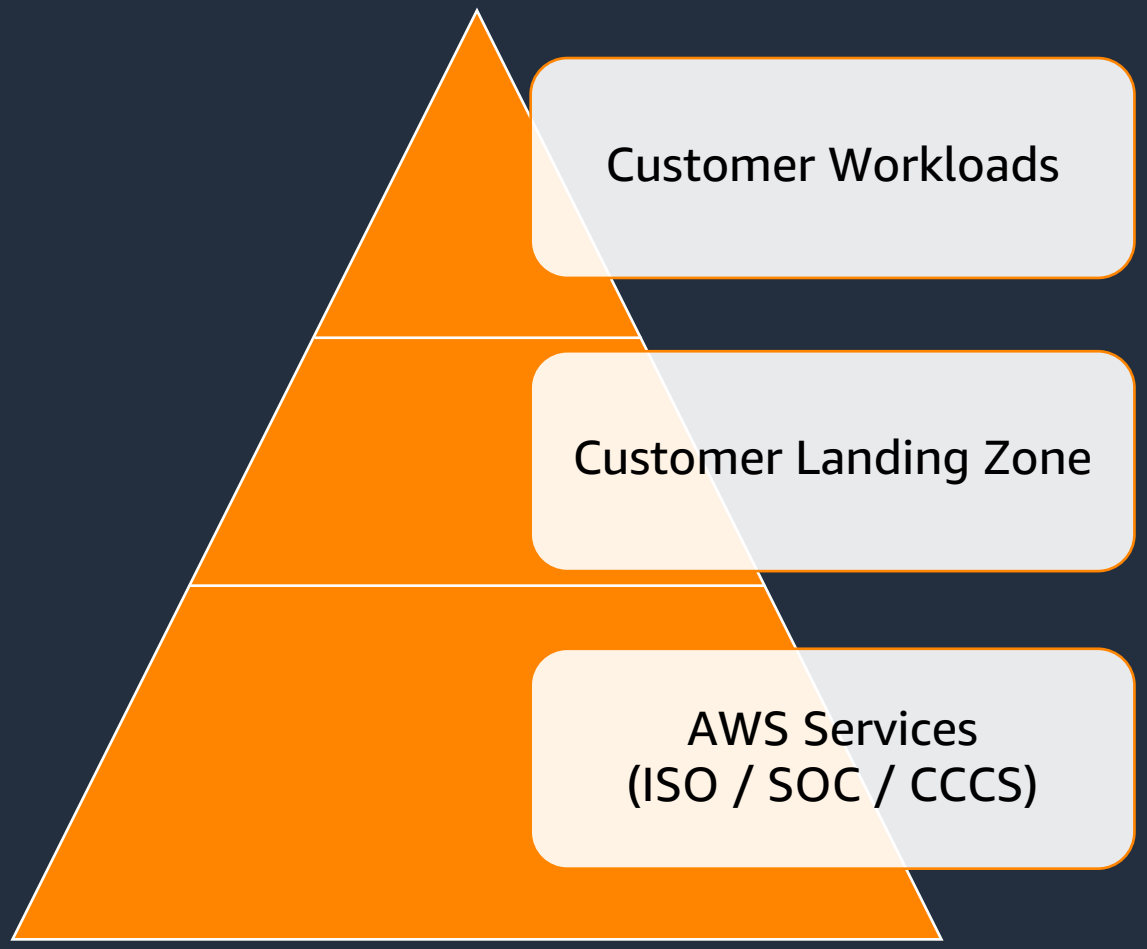
Global security and compliance standards

© 2020, Amazon Web Services, Inc. or its Affiliates.

aws

Stacked Assessment

- Controls can be inherited from underlying layers
- Landing zone provides organization-wide controls
- Many AWS services assessed by ISO, SOC, and CCCS

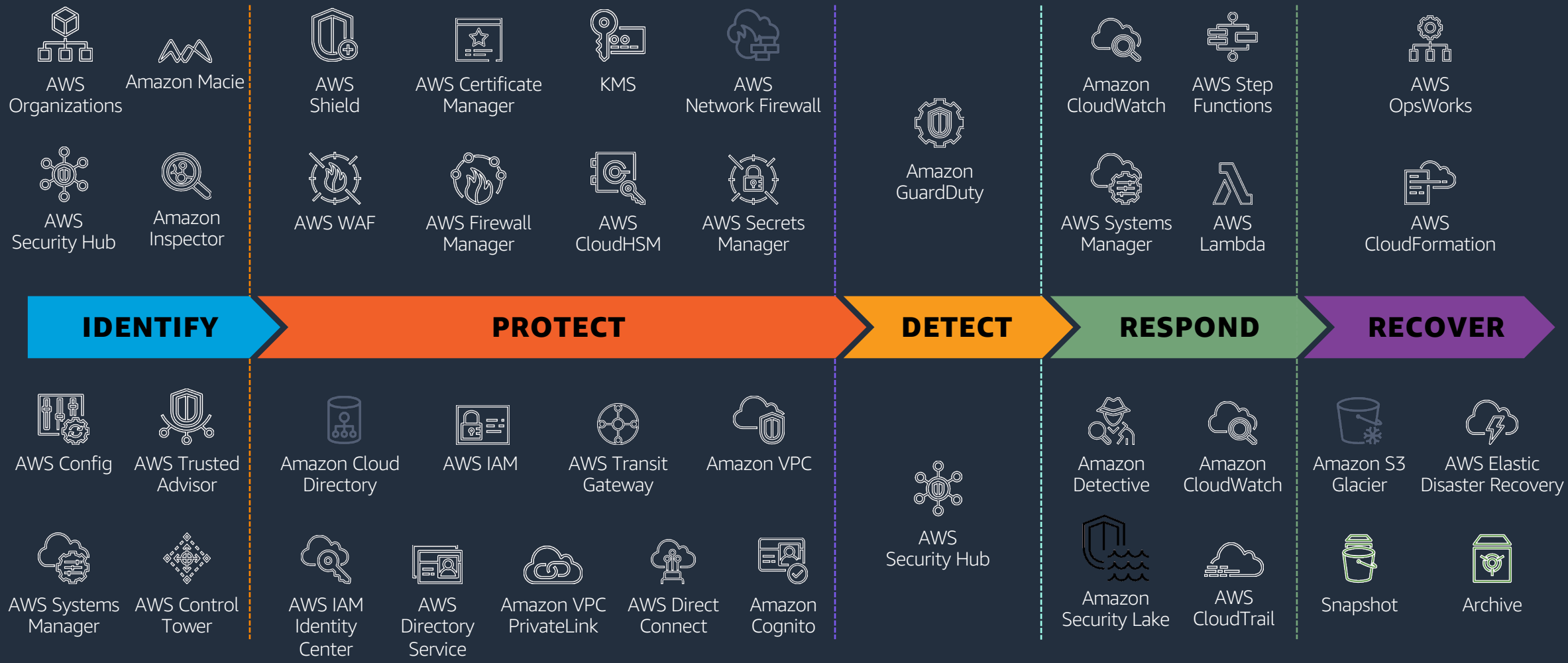


© 2022, Amazon Web Services, Inc. or its affiliates.

AWS Resources

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

Use AWS services to mitigate threats

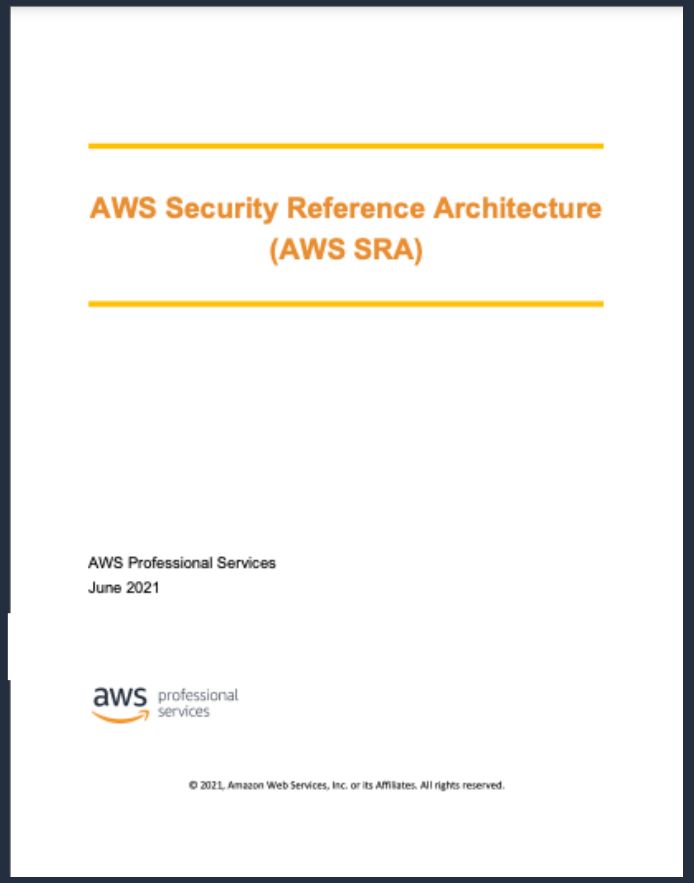


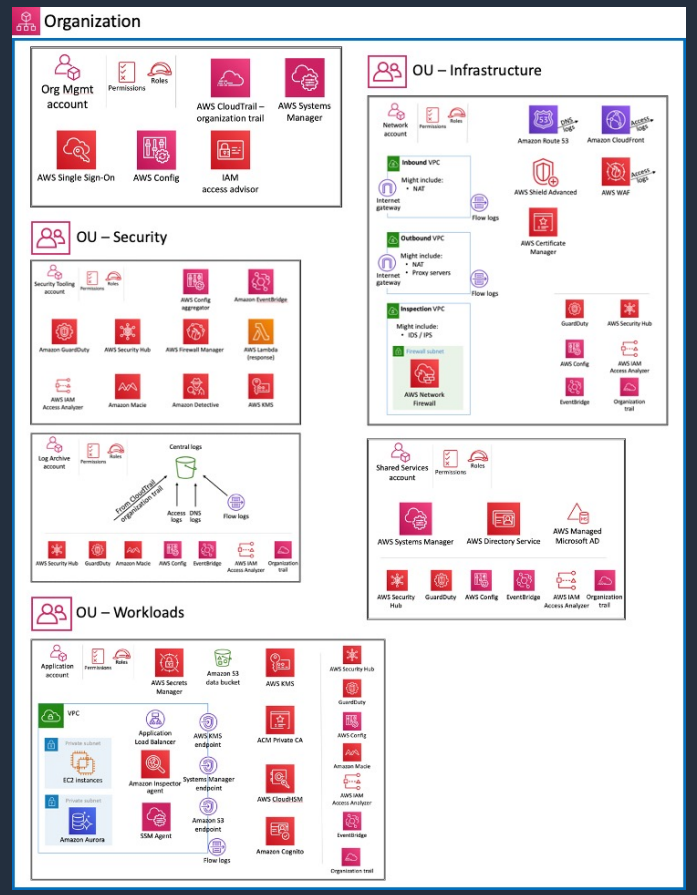
© 2022, Amazon Web Services, Inc. or its affiliates.

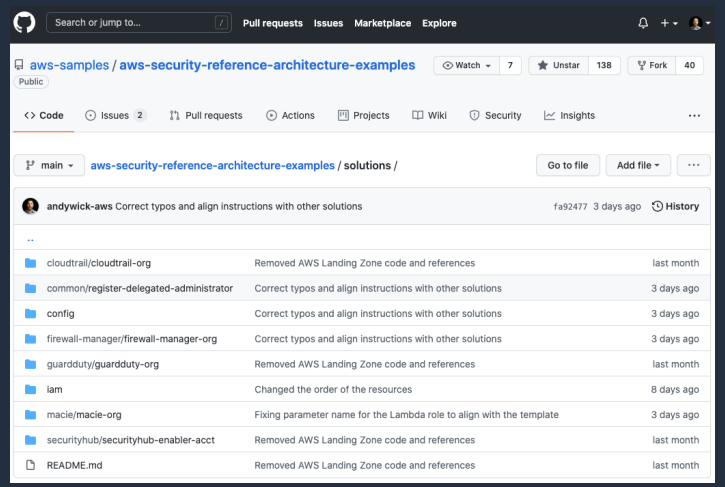
Perception?

© 2022, Amazon Web Services, Inc. or its affiliates.

AWS Security Reference Architecture (AWS SRA)







aws-samples/aws-security-reference-architecture-examples
https://github.com/aws-samples/aws-security-reference-architecture-examples

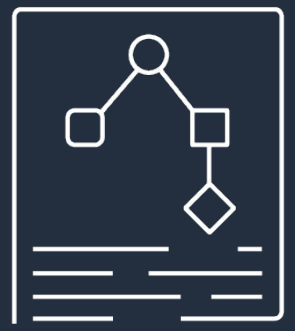
https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/welcome.html

© 2022, Amazon Web Services, Inc. or its affiliates.

Landing Zone Accelerator (LZA) on AWS

The Landing Zone Accelerator on AWS (LZA) is an open-source solution that accelerates the implementation of a customer's technical security controls and infrastructure foundation on AWS.

Automation



Data Security

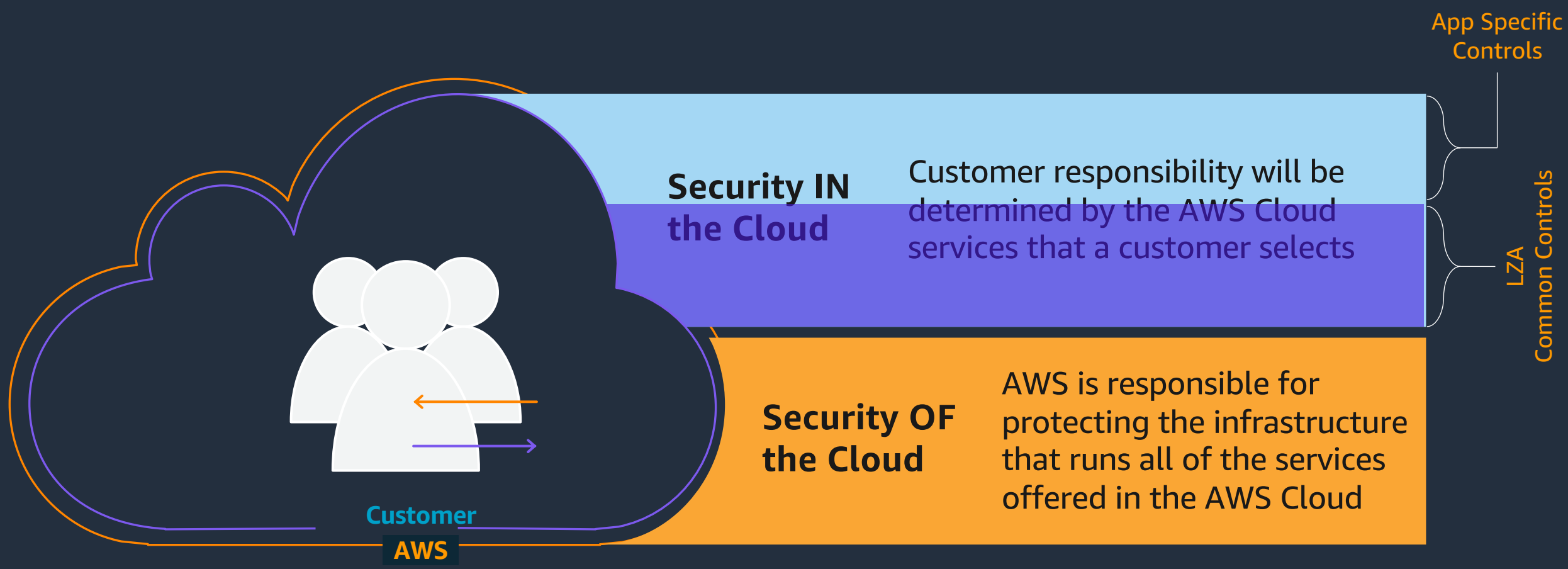
Compliance

Support

Learn more about the LZA and Deployment Guide in the [AWS Solutions Library]

© 2022, Amazon Web Services, Inc. or its affiliates.

Shared Responsibility Model

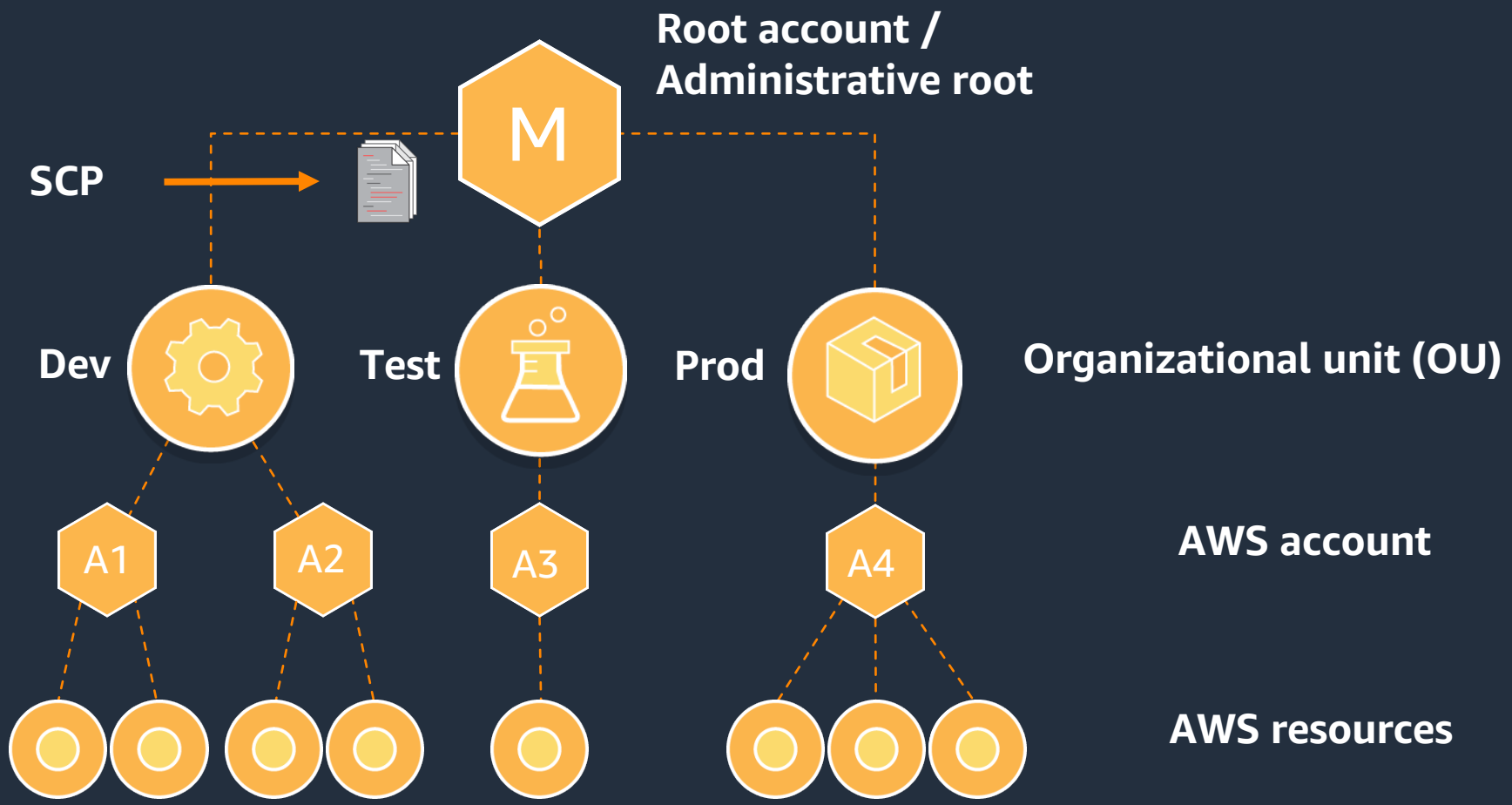


© 2022, Amazon Web Services, Inc. or its affiliates.

Design Patterns

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved. Amazon Confidential and Trademark.

Use a multi-account strategy and network segmentation



© 2022, Amazon Web Services, Inc. or its affiliates.

“Everything starts with a threat model”

- Characterizes what can (be made to) go wrong
    - Who causes it and how
- Is used in conjunction with a risk register
    - Characterizes probabilities and consequences
    - Material risks require compensating controls
    - Residual risks are accepted and signed off as part of “the risk of doing business”
- Informs controls (normally in a framework)
    - Which turn material risks into residual risks

aws

© 2022, Amazon Web Services, Inc. or its affiliates.

Why use a threat model

Identify security issues **early**

+

Understand security needs **early**

=

Build securely

© 2022, Amazon Web Services, Inc. or its affiliates.

Threat model developments

There are now threat analysis documents specifically focusing on ML from standards and advisory bodies and academia:

- Securing Artificial Intelligence (SAI)

- AI Accidents: An Emerging Threat

© 2022, Amazon Web Services, Inc. or its affiliates.

Shifting security left

Developer Workstations

Deployment Pipeline

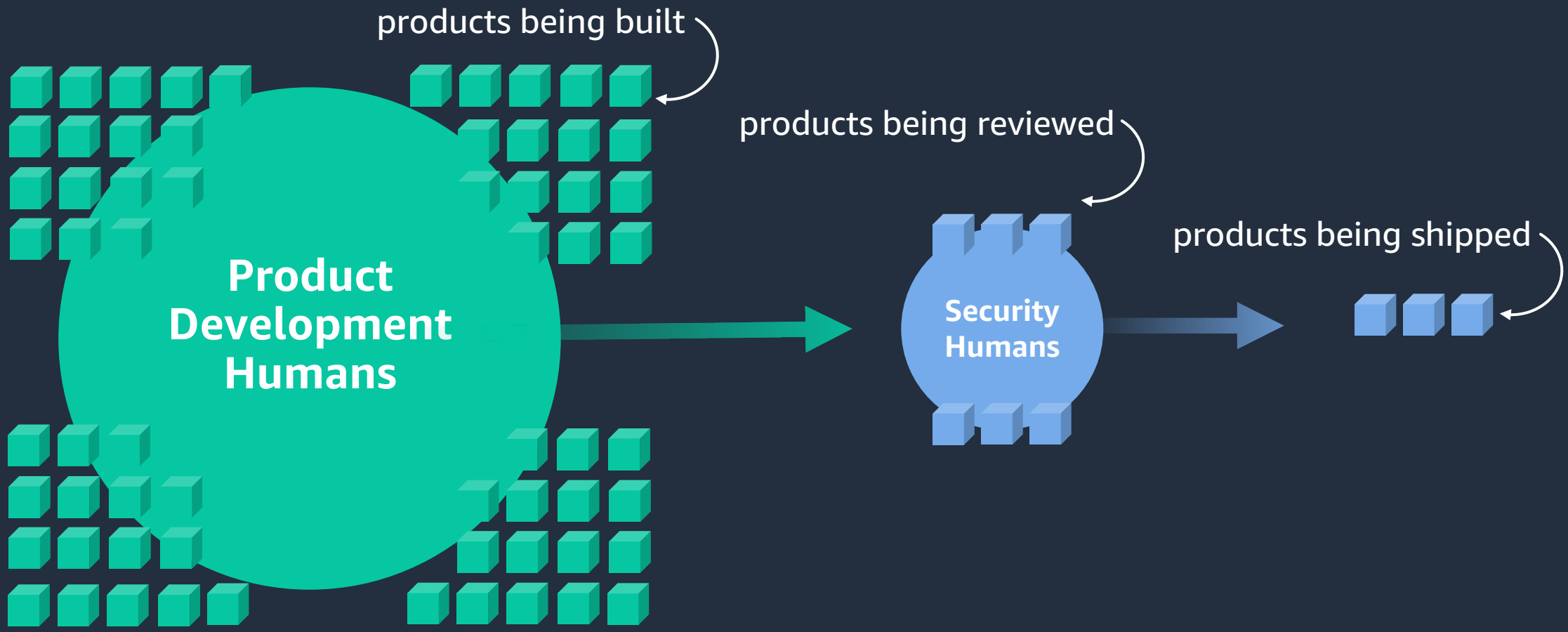
Assessment and Authorization

Monitoring

Address security sooner

© 2022, Amazon Web Services, Inc. or its affiliates.

How to build capability?

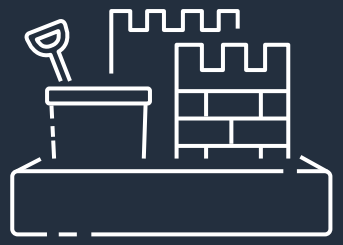


© 2022, Amazon Web Services, Inc. or its affiliates.

Security Guardians

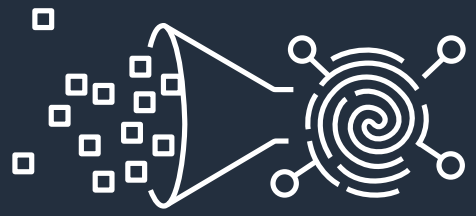
A human mechanism to scale security at AWS

Guardians are trained, security-minded Amazonians who volunteer to be a consistent champion for security on their team



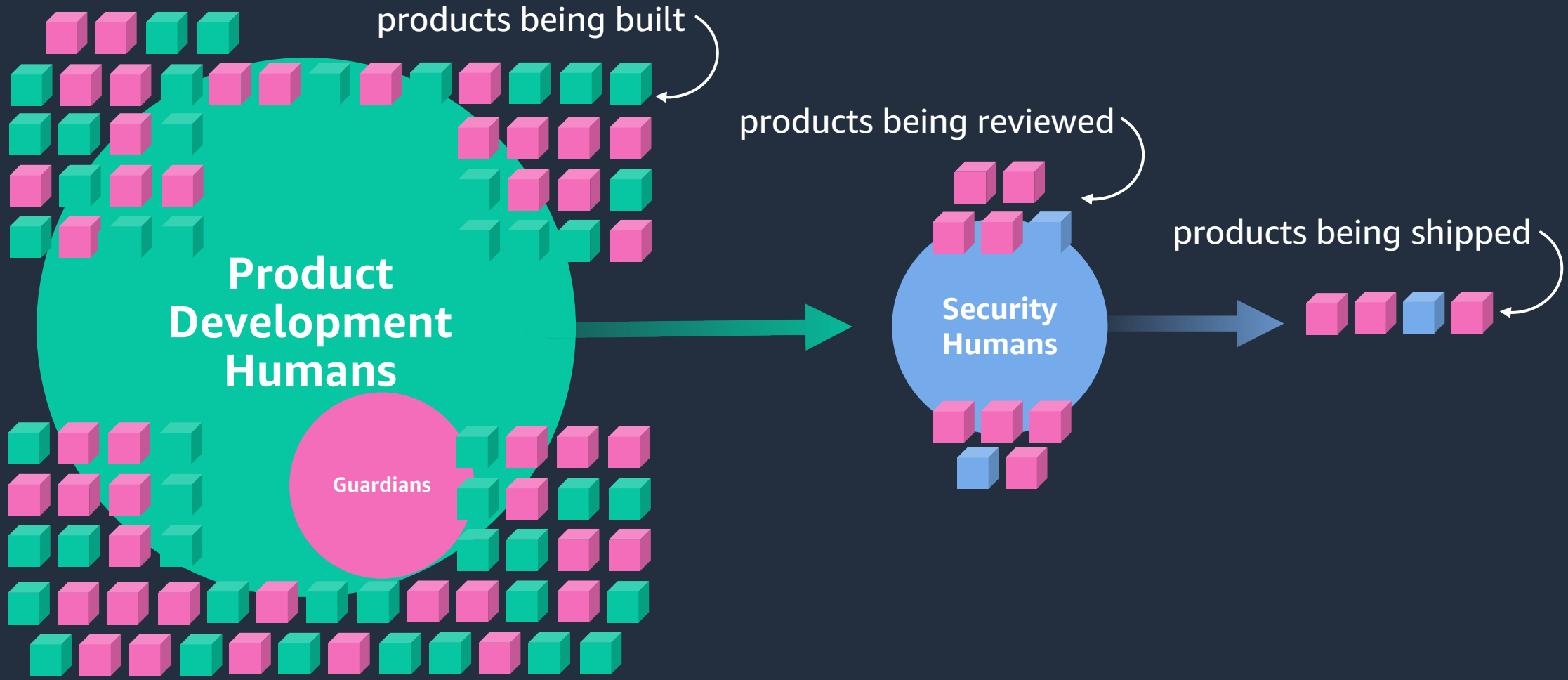
They partner with their fellow builders make informed security decisions that lead to more secure, on-time launches

They serve as an extension to the application security function, scaling security awareness and providing a strong feedback mechanism



© 2022, Amazon Web Services, Inc. or its affiliates.

Security embedded into builder teams



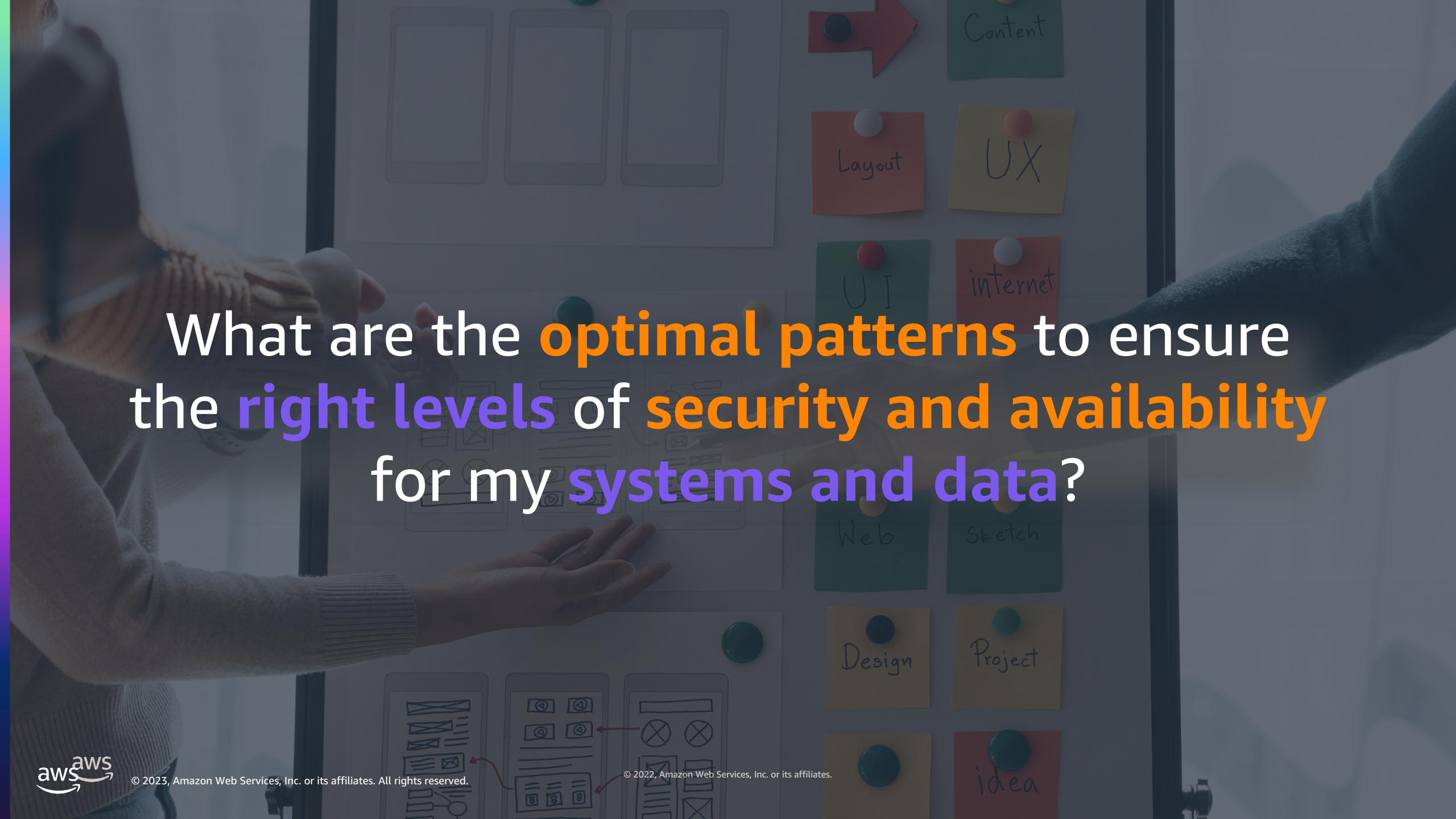
© 2022, Amazon Web Services, Inc. or its affiliates.

Security Guardian results

18.4% fewer launch-blocking findings

16.2% less time to complete a security review

© 2022, Amazon Web Services, Inc. or its affiliates.



What are the **optimal patterns** to ensure the **right levels** of **security and availability** for my **systems and data**?

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

© 2022, Amazon Web Services, Inc. or its affiliates.

Zero Trust defined

A conceptual **security model** and associated set of **mechanisms** that focus on providing security controls around digital assets that **do not solely or fundamentally depend on** traditional network controls or network perimeters

© 2022, Amazon Web Services, Inc. or its affiliates.

Guiding principles for Zero Trust

01

Avoid a binary choice

02

Work backwards from your use cases

03

One size doesn't fit all

© 2022, Amazon Web Services, Inc. or its affiliates.

What is a data perimeter?

Trusted identities

principals within your AWS accounts, or AWS services acting on your behalf

Trusted resources

resources owned by your AWS accounts or by AWS services acting on your behalf

Expected networks

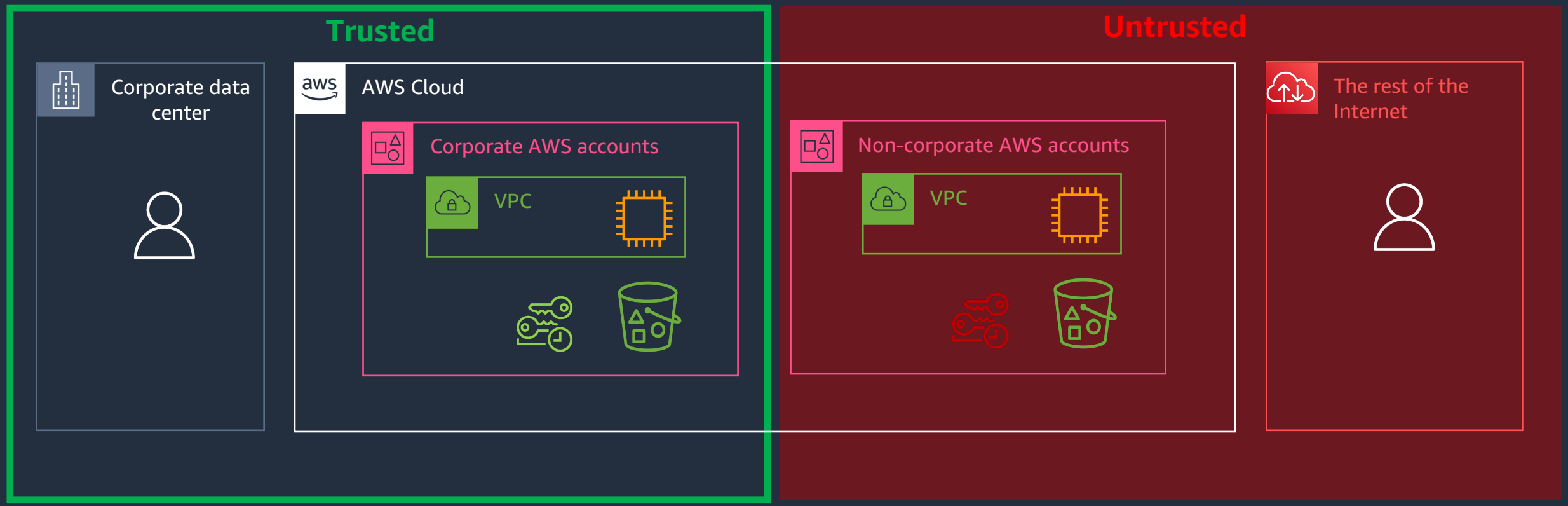
your on-premises data centers and virtual private clouds (VPCs), or networks of AWS services acting on your behalf

© 2022, Amazon Web Services, Inc. or its affiliates.

What is a data perimeter?

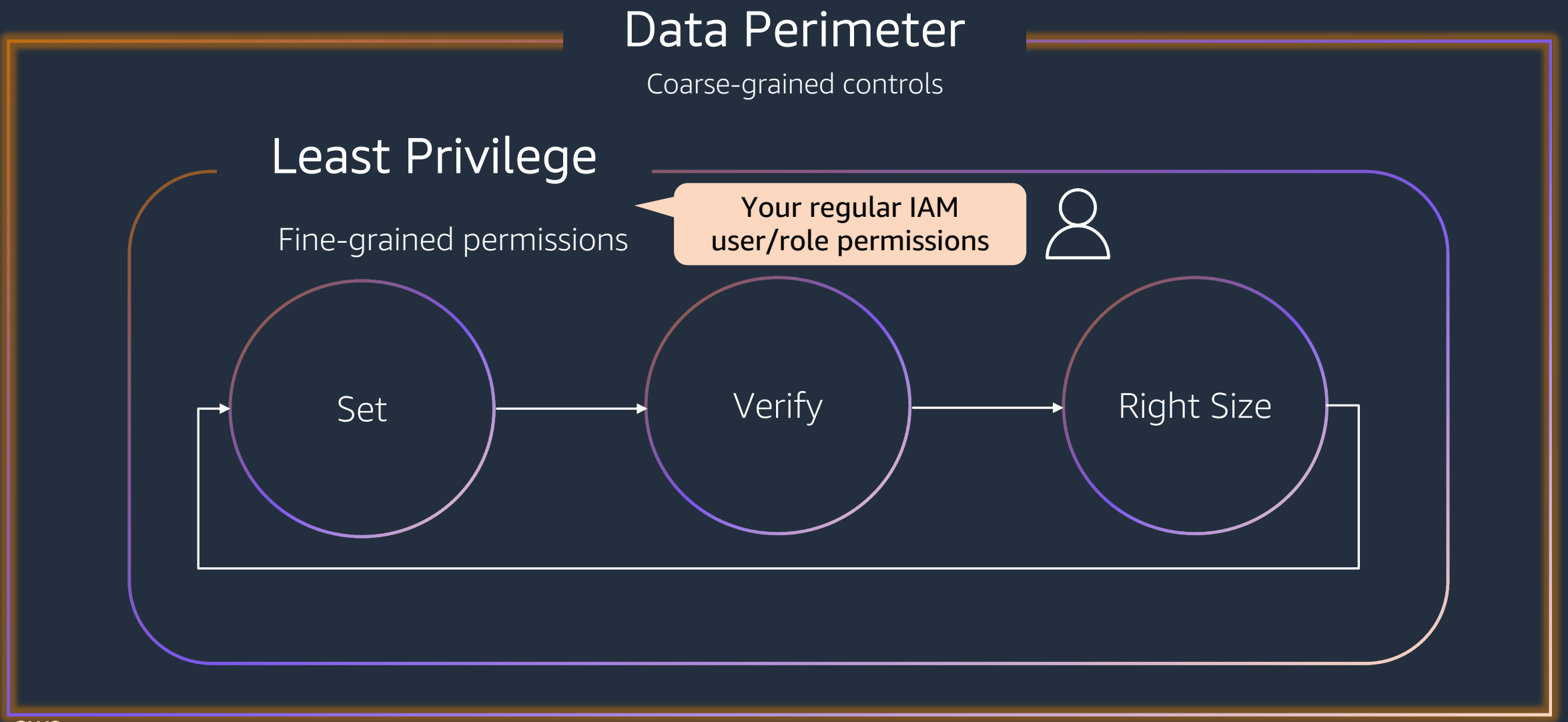
A set of **preventive guardrails**

- only your trusted identities
- are accessing trusted resources
- from expected networks



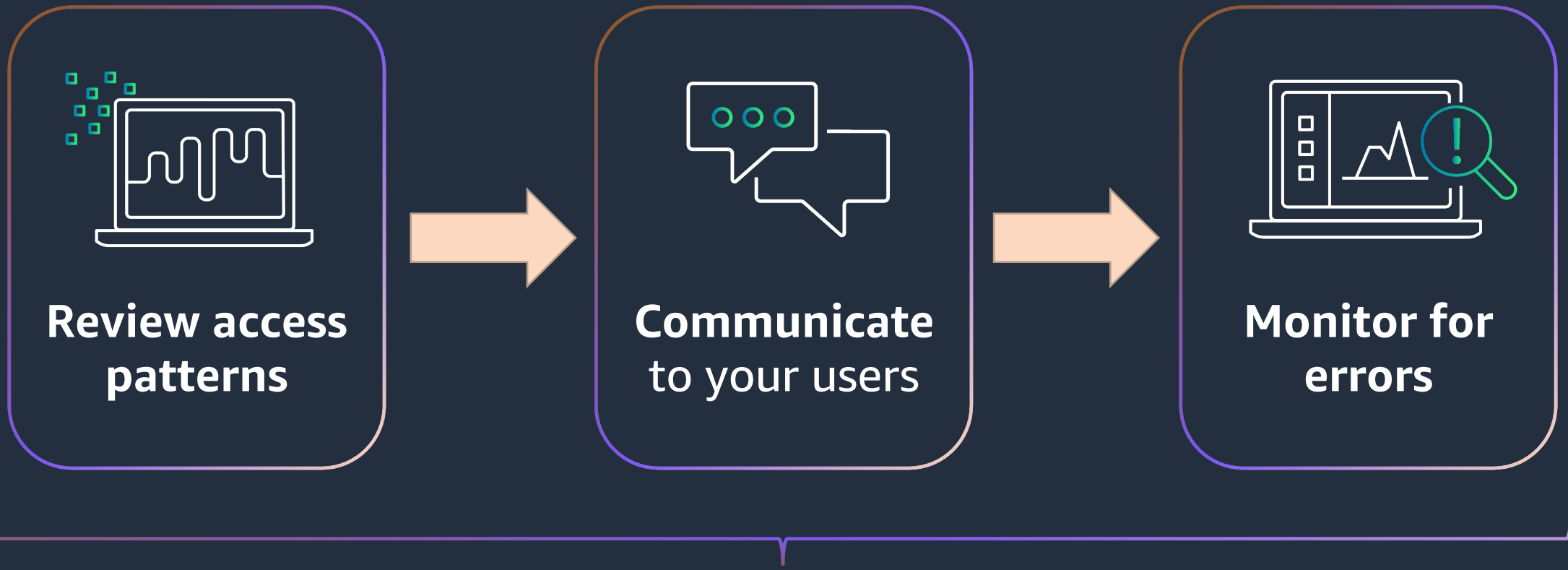
© 2022, Amazon Web Services, Inc. or its affiliates.

Access Management



© 2022, Amazon Web Services, Inc. or its affiliates.

Tips on implementation



© 2022, Amazon Web Services, Inc. or its affiliates.

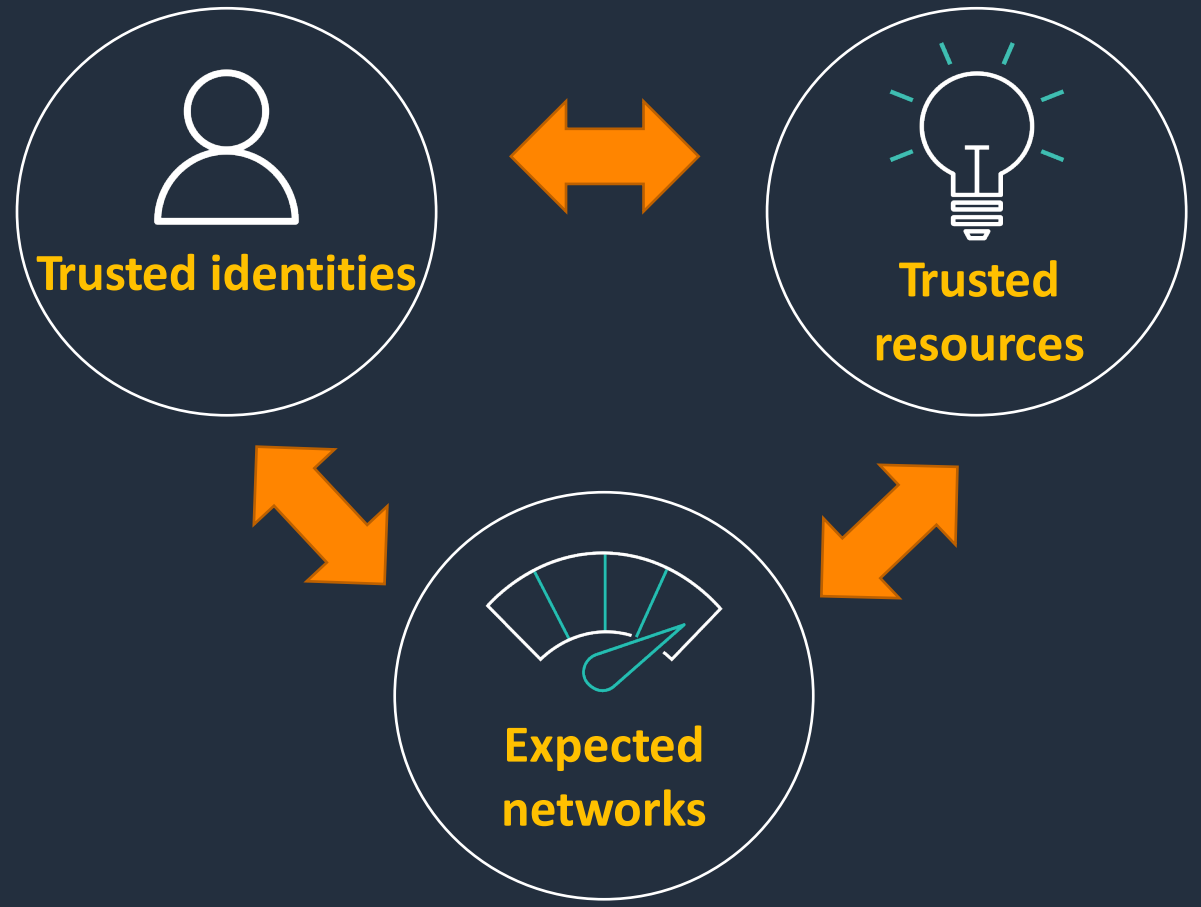
Key Takeaways

- Data perimeter provides **coarse-grained controls** to protect your organization as a whole

- How to implement
  - Service control policies
  - VPC endpoint policies
  - Resource-based policies

- Risk-based approach

- Always test before implementation



aws

© 2022, Amazon Web Services, Inc. or its affiliates.

Top 4 customer needs from data protection services

Data at rest

Storage encryption

Easily encrypt the data where it resides

Data in transit

Network encryption

Encrypt the data as it moves between networks – enforce data sovereignty

Application Credentials

Managed secrets

Encrypted secrets without the management overhead

Lifecycle Management

Automation

Make security easy and reduce human error

Customers don’t want to day-to-day management for cryptography or preventative controls

© 2022, Amazon Web Services, Inc. or its affiliates.

How does AWS help customers with data protection?

"How do we move our data to AWS securely?"

Client-side encryption to encrypt inbound data

AWS Certificate Manager for SSL/TLS certificates

"How do we keep data on AWS confidential?"

Server-side encryption to encrypt data at-rest

AWS KMS and CloudHSM for enterprise key management and FIPS 140 validated HSMs

"How do we securely share data and resources within the cloud?"

AWS Identity and Access Management – Cross-Account Access

"How do we manage authentication and authorization?"

AWS IAM and Secrets Manager for identity and credentials management

"How do I prove security and compliance to auditors?"

AWS Management & Governance integrations

"How do we optimize cost and performance?"

"How do we architect for availability?"

"How do we scale?"

- Well-Architected Guidance
- Available in all Regions
- Our services are used by all other AWS services
- Cryptographic SDKs for application encryption
- Multi-Region Keys for Disaster Recovery

© 2022, Amazon Web Services, Inc. or its affiliates.

Security assurance and provable data protection

Notify me if my desired encryption settings are modified

AWS Config

Utilize AWS Config Managed Rules to monitor encryption configuration changes in your AWS environment

Examples:

- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- cloud-trail-encryption-enabled

Monitor usage of ACM certificates and KMS keys

AWS CloudTrail

Use AWS CloudTrail to create detailed logs of API calls to the KMS and ACM services for audit purposes

A KMS API action was called:

- by who (user, account, IP)
- when (timestamp)
- where, why (KMS key, AWS resource)

Audit important lifecycle events for certificates and KMS keys

Amazon CloudWatch

Use Amazon CloudWatch Metrics and Events to monitor important events and API calls in your AWS accounts

Examples:

- Metrics: time until key/certificate expiration
- Events: key rotation, key deletion, imported key expiration, certificate renewal

© 2022, Amazon Web Services, Inc. or its affiliates.

Start with requirements

Identify applications to protect

Business impact analysis

Define RPO and RTO requirements

($ investment)

Compliance considerations

© 2022, Amazon Web Services, Inc. or its affiliates.

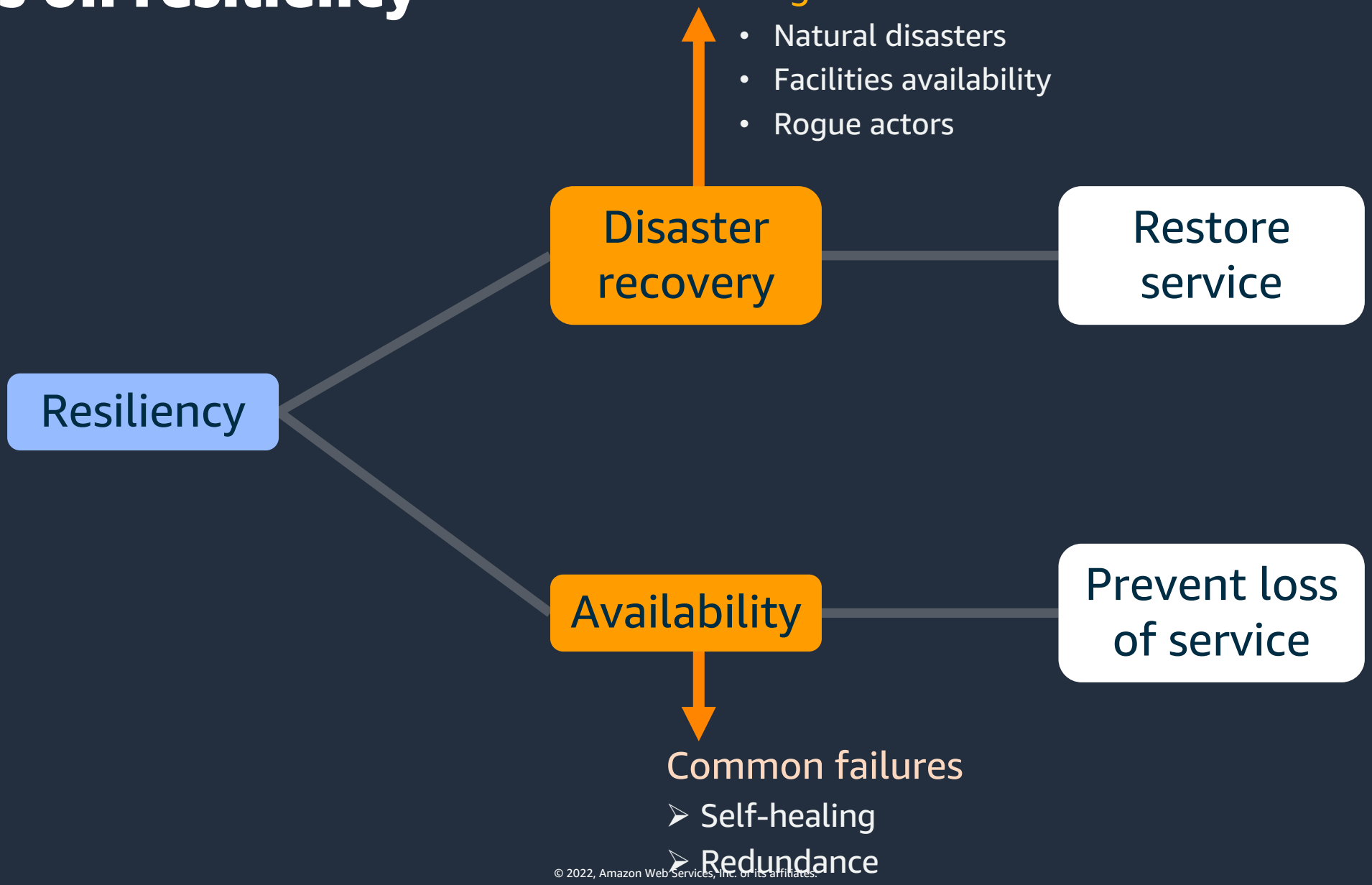
Objectives and impacts

How much data can you afford to recreate or lose?

How quickly must you recover? What is the cost of downtime?

© 2022, Amazon Web Services, Inc. or its affiliates.

Focus on resiliency



© 2022, Amazon Web Services, Inc. or its affiliates.

Categories of failures

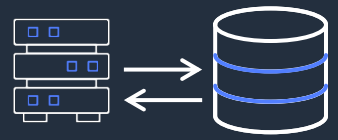
WHEN TO CHOOSE SINGLE REGION VS. MULTI-REGION

Code deployments and configuration

(e.g., bad deployment, cred expiration)

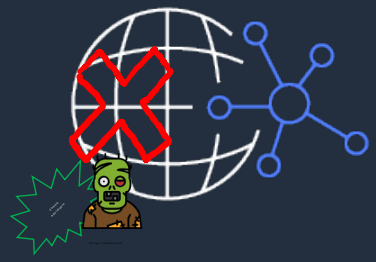
Core infrastructure

(e.g., data centre failure, host failure)



Data and state

(e.g., data corruption)



Highly unlikely scenarios

(e.g., all of internet failures, environmental disasters, supplier failures)

Likelihood

Probable — Rare

aws

© 2022, Amazon Web Services, Inc. or its affiliates.

AWS DR strategies (factors: complexity & time)

RPO/RTO: hours

- Lower priority use cases
- Solutions: Amazon S3, AWS Storage Gateway
- Cost: $

RPO/RTO: 10s of minutes

- Meeting lower RTO & RPO requirements
- Core services
- Scale AWS resources in response to a DR event
- Cost: $$

RPO/RTO: minutes

- Solutions that require RTO & RPO in minutes
- Business-critical services
- Cost: $$$

RPO/RTO: real time

- Auto-failover of your environment in AWS
- Cost: $$$$

© 2022, Amazon Web Services, Inc. or its affiliates.

Resiliency patterns and trade-offs

	P1	P2	P3	P4	P5
	Multi-AZ Deployment	Static Stability in Region	Application Portfolio Distribution	Multi-AZ Deployment [Regional DR]	Multi-Region Active-Active Deployment
Design Complexity	Low	Medium	Medium	High	Very High
Cost to Implement	Low	High	Medium	High	High
Operational Effort	Low	Medium	Medium	Medium	Very High
Effort to Secure	Low	Medium	Medium	High	High
Environmental Impact	Low	Medium	Medium	High	High

Lowest — Availability — Highest

© 2022, Amazon Web Services, Inc. or its affiliates.

Security resources

Developer information, articles and tutorials, security products, and whitepapers

http://aws.amazon.com/security/security-resources/

Security blog

Subscribe to the blog – it's a great way to stay up to date on AWS security and compliance

http://blogs.aws.amazon.com/security/

© 2022, Amazon Web Services, Inc. or its affiliates.

Thank you!

Bill Ohlson

billohl@amazon.com

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.