
aws
SUMMIT
OTTAWA | SEPTEMBER 8, 2022

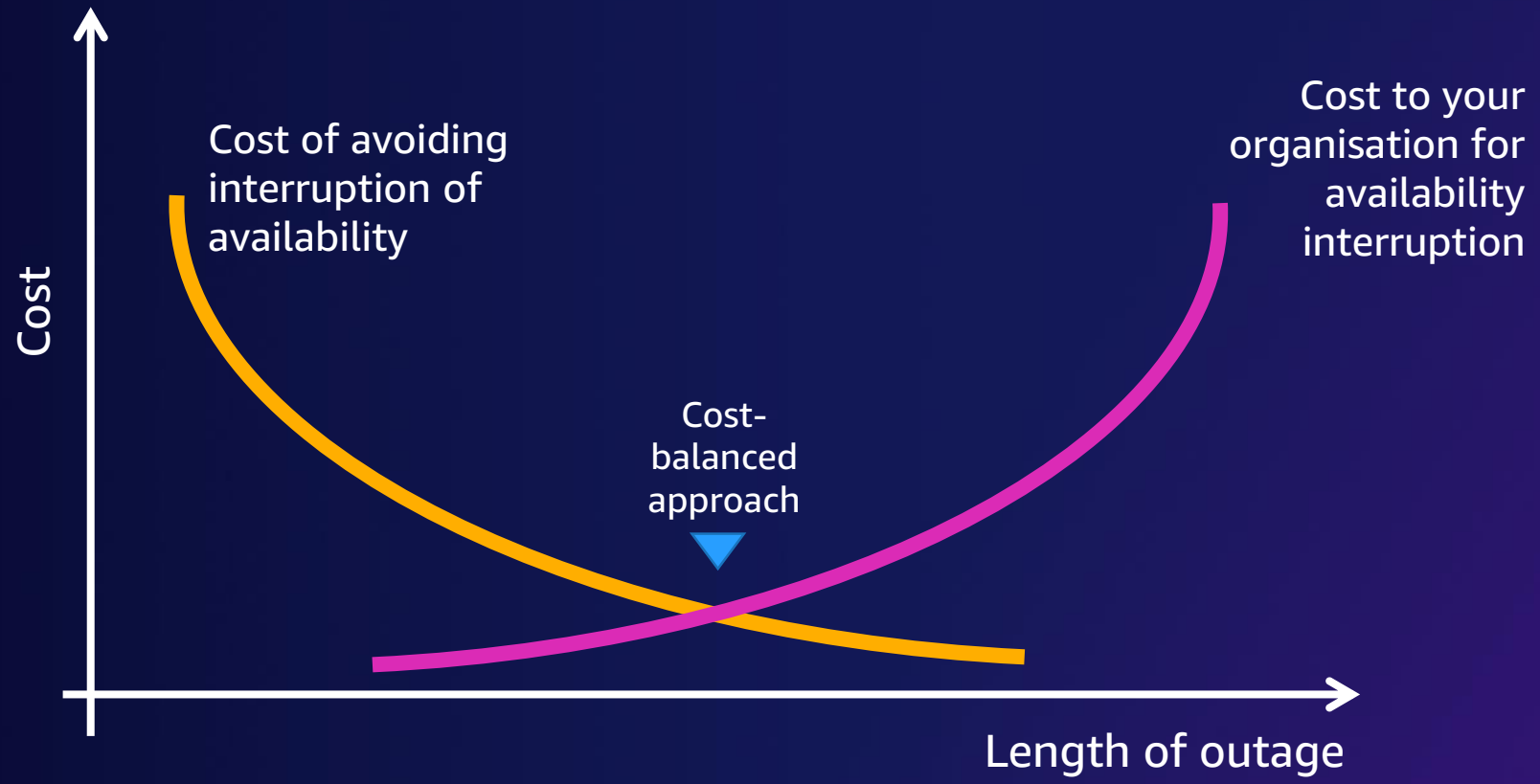
SEC201

# Disaster recovery and data residency in Canada

Scott Levac
Office of the Chief Information Officer
Treasury Board of Canada Secretariat

Bill Ohlson
Principal Security Leader
AWS WWPS LCC SA

# Availability is not free



# Focus on outcomes

Daily tape backups on magnetic tape stored offsite in two locations at least 10 km apart. Redundant servers hosted in data centres 50 km apart.

The business cannot tolerate more than one hour of lost services and should never lose more than 20 minutes of data. The service needs to be available 24 hours per day, seven days per week, with no more than one hour of lost productivity per month.

**Myth:** For cloud providers, we must specify how recovery is implemented.

**Busted:** Policy wants an outcomes-based approach.

# Clouds are made of cells

**Myth:** Availability Zones (AZs), or Zones, are all created equal across cloud providers

**Busted:** Understand each cloud provider's SLAs and design for AZs; look beyond the name

**Tip: In Canada, AZ is pronounced "eh zed," not "a zee"**

# Oh Canada

**Myth:** Government of Canada (GC) policy does not allow Protected B data to be stored outside of Canada

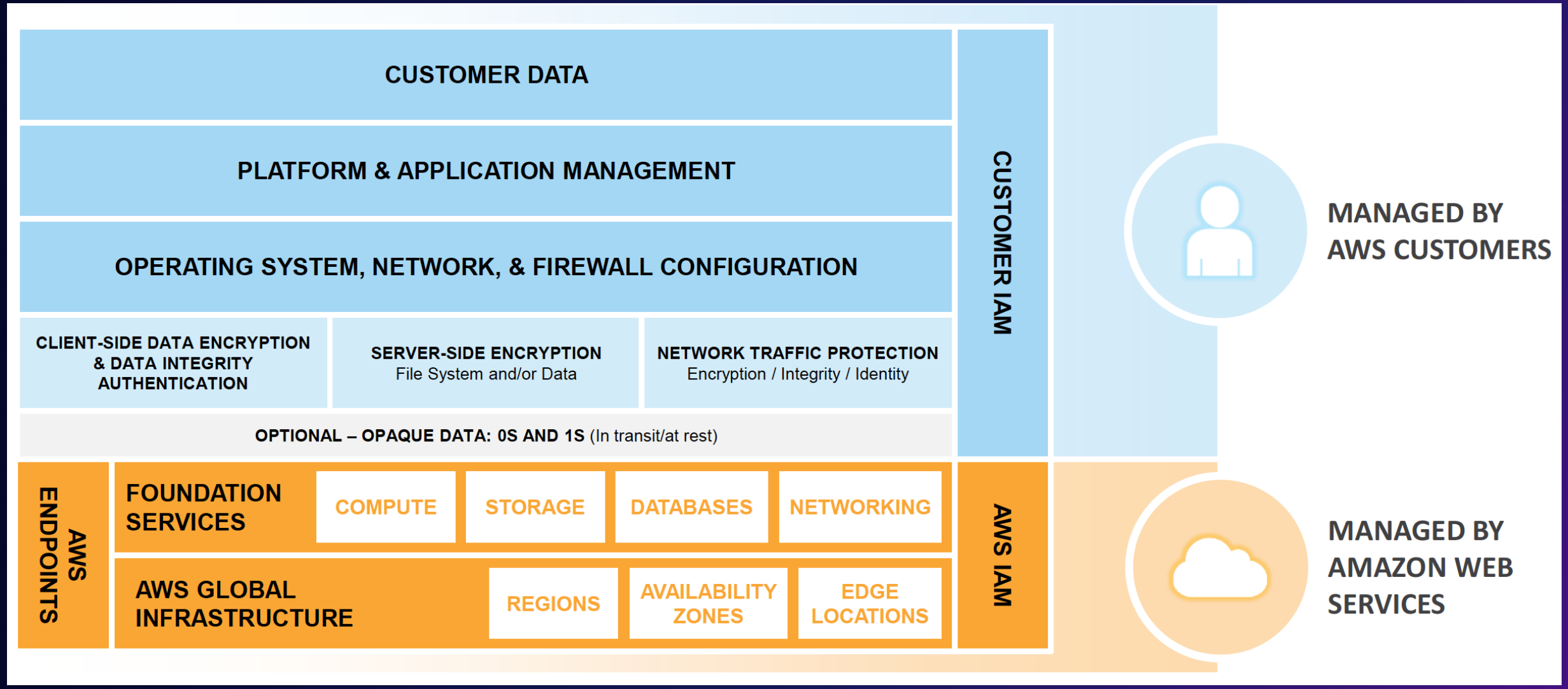
**Busted:** GC policy states Canada is the preferred location, but departmental CIOs can decide otherwise

# What is resiliency?

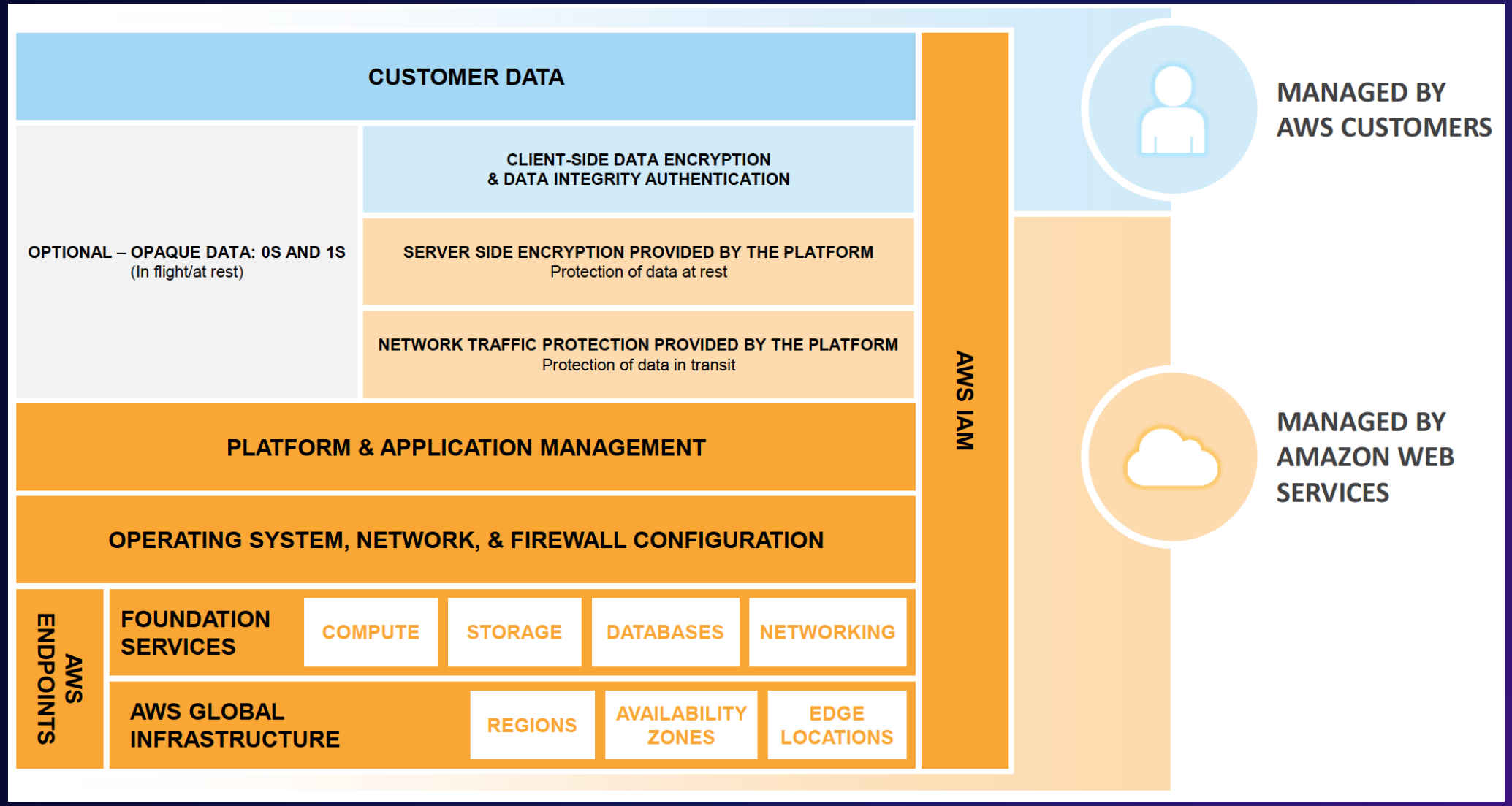
**“The ability for a system to continue operating during a failure induced by load, attacks, and failures, and recover quickly.”**

Resiliency Pillar
AWS Well-Architected Framework

# Understand the Shared Responsibility Model



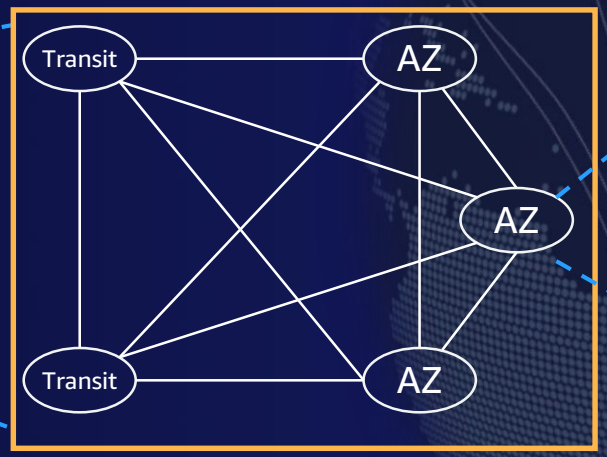
# Shared Responsibility Model is not static



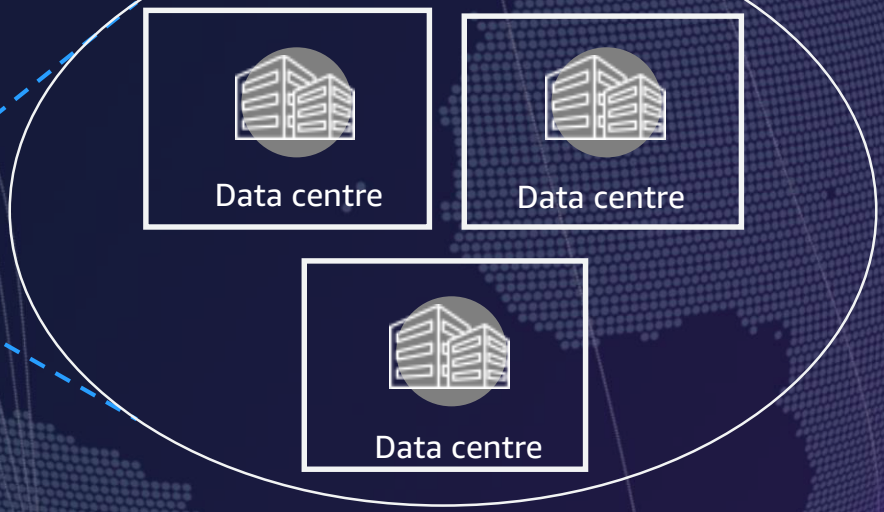
# AWS Region design

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




AWS AZ




**26** geographic Regions

**84** AZs

**230+** points of presence

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

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

**Canada West coming in 2023/2024!**

# Calgary Region – On track for Q4 2023

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*

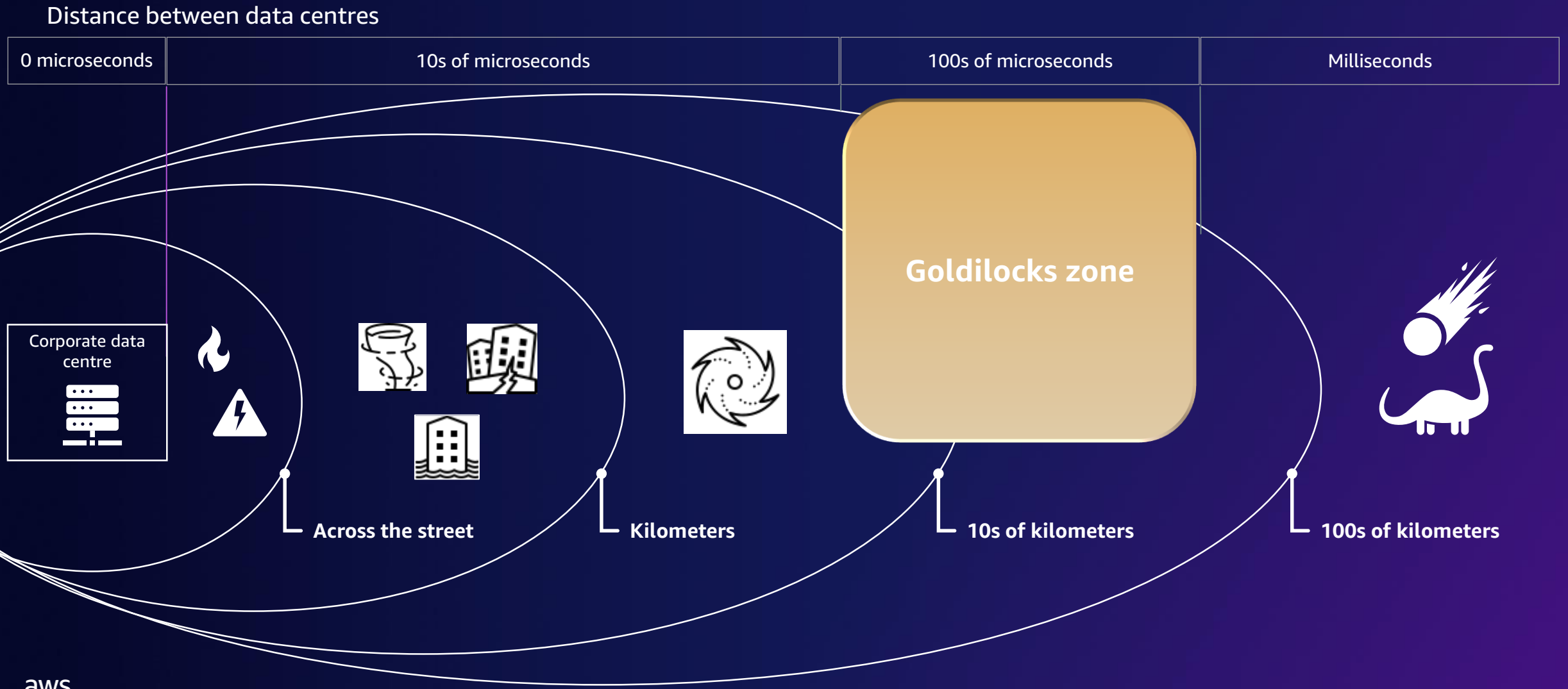
**AWS Regions**
*Montreal*
*Calgary (Coming Soon)*

**Amazon CloudFront Edge Locations**
*Vancouver, Toronto, and Montreal*

**Amazon Solar Farms**
*Newell, AB*
*Vulcan, AB*

# Goldilocks zone

NOT TOO CLOSE, AND NOT TOO FAR, BUT JUST RIGHT



# Inherit global security and compliance controls

CSA cloud security alliance SM

ISO 9001 International Organization for Standardization

ISO 27001 International Organization for Standardization

ISO 27017 International Organization for Standardization

ISO 27018 International Organization for Standardization

PCI Security Standards Council PARTICIPATING ORGANIZATION

AICPA SOC — SOC 1

AICPA SOC — SOC 2

AICPA SOC — SOC 3

CJIS

FIPS 140-2 CRYPTOGRAPHY

FISMA FEDERAL INFORMATION SECURITY MANAGEMENT ACT

DoD SRG

FR FedRAMP

FERPA

FFIEC Federal Financial Institutions Examination Council

C5

SEC Rule 17a-4(f)

GxP

HIPAA

Cloud Medium (formerly PBMM) CANADA

MPAA

iDA SINGAPORE

マイナンバー My Number Act

VPAT Section 508

FIEC

irap

ISMS

G-Cloud

TISAX ENX ASSOCIATION

ITAR International Traffic in Arms Regulations Compliant

CYBER ESSENTIALS PLUS

CERTIFICACIÓN DE CONFORMIDAD CON EL ens

CGP CANADA

# High-compliance environments

# Cloud disaster recovery benefits

## Traditional disaster recovery

- Massive upfront investment in hardware and high ongoing costs
- Data growth increases hardware and operational costs
- Hard to actually test without business disruption
- Management and infrastructure overhead for globally distributed businesses
- Vulnerable to cyber threats/hacking

## Disaster recovery in the cloud

- No upfront hardware investment needed
- Only pay for rightsized compute/storage when actually needed
- Lower IT management overhead
- (**Much**) More automation
- Easy and repeatable testing
- Systems up in minutes (not hours/days)

# Start with requirements

Identify applications to protect

Business impact analysis

Define RPO and RTO requirements

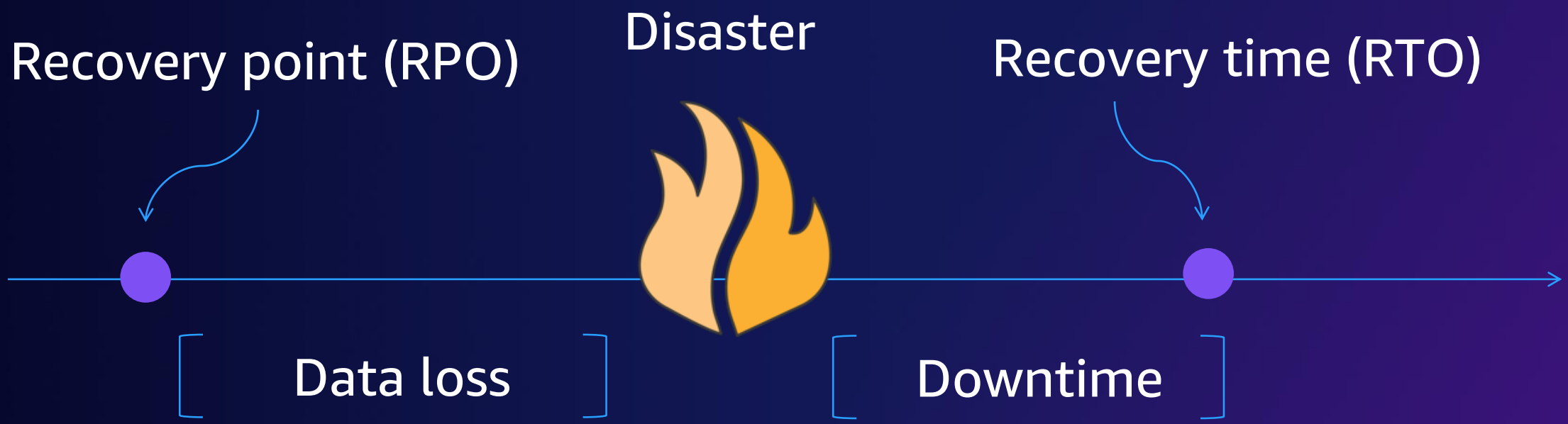
($ investment)

Compliance considerations

# Objectives and impacts

How much data can you afford to recreate or lose?

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



# What does policy tell us?

**Business impact assessment**
(Appendix D: Mandatory Procedures for Business Continuity Planning)

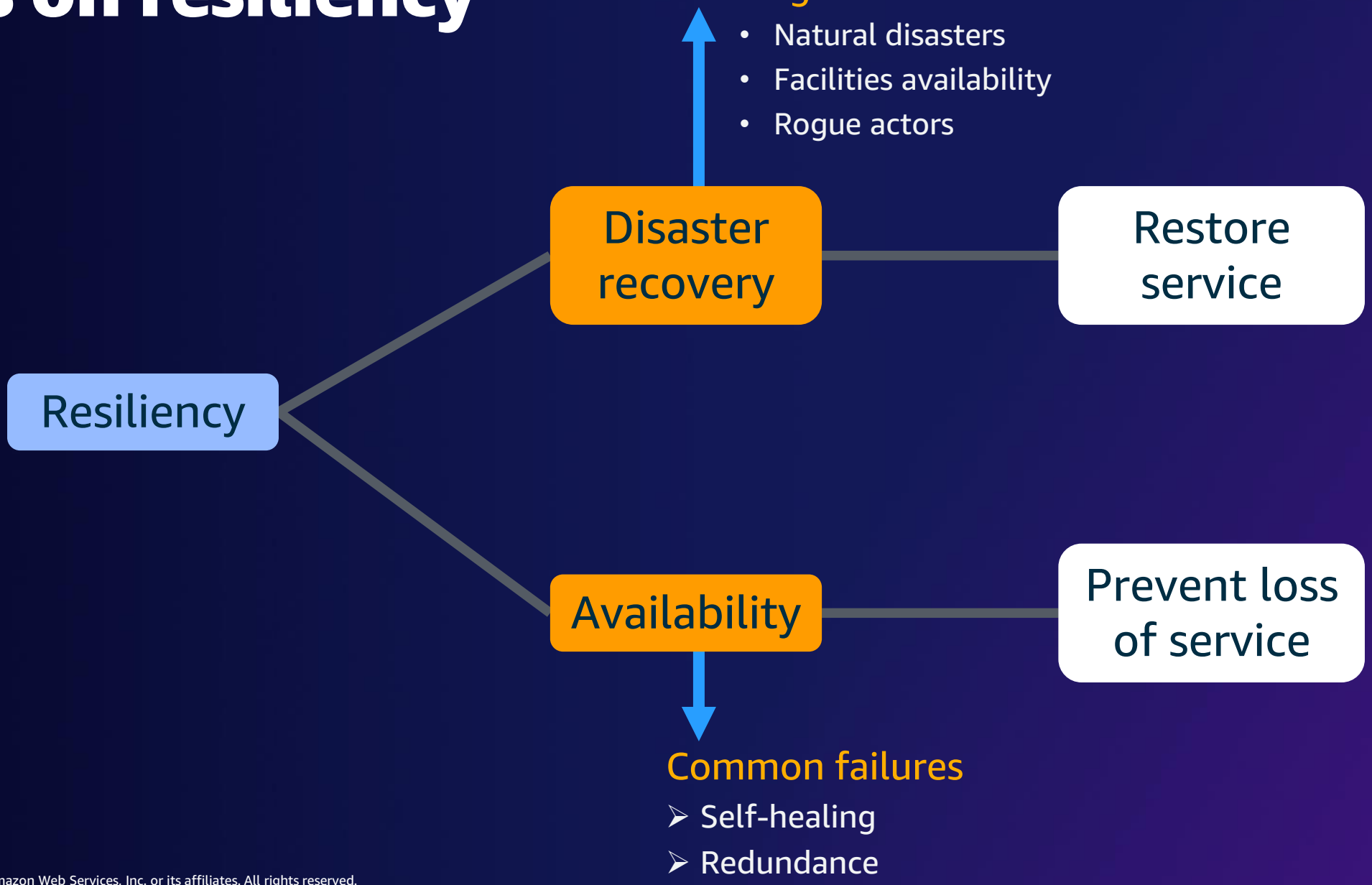
| Service | Potential impacts | Service RTO |
|---|---|---|
| Payroll | Operations – Cannot pay employees. Emergency checks can be issued for a period. | 24 hours |
| Staffing | Operations – Emergency staffing only. Letters of offer issued ad hoc. | 3 days |
| Personal tax processing | Reputation – Inability to perform core function of organization. 30,000 taxes processed daily. | 12 hours |
| Inquiries | Reputation – Public-facing service will be unavailable. 1,000 calls per day unanswered. | 24 hours |
| Payments | Operations – Inability to pay out $5M daily to small and medium businesses. | 8 hours |

**Data categorization**
(Appendix J: Standard on Security Categorization)

| Application | App. RTO | Injury assessment (ITSG-33) Conf | Int | Av |
|---|---|---|---|---|
| Financial system | 24 hours | PB | L | M |
| HR system | 3 days | PB | M | L |
| T4 system | 4 hours | PB | M | M |
| Call centre | 18 hours | PB | L | L |
| Banking | 4 hours | PB | M | M |

Security control profile

# Focus on resiliency



# Categories of failures

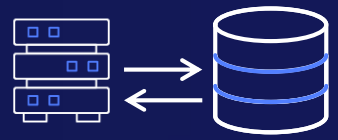
WHEN TO CHOOSE SINGLE REGION VS. MULTI-REGION

## Code deployments and configuration

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

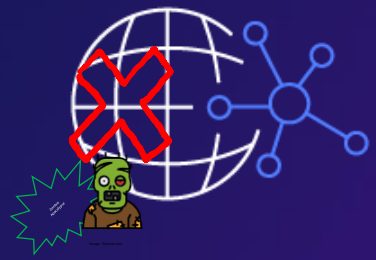
## Core infrastructure

(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 DR strategies (factors: complexity & time)


**Backup and restore**

RPO/RTO: hours

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

**Pilot light**

RPO/RTO: 10s of minutes

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

**Warm standby in AWS**

RPO/RTO: minutes

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

**Hot standby (with multi-site)**

RPO/RTO: real time

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

# Resiliency patterns and trade-offs

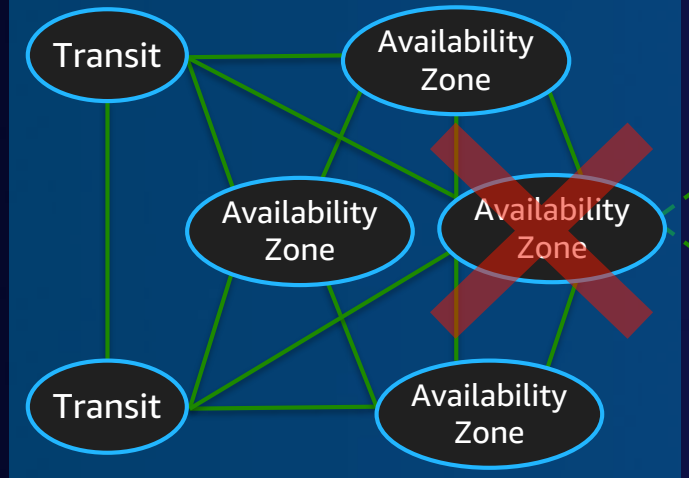
| | P1 | P2 | P3 | P4 | P5 |
|---|---|---|---|---|---|
| | Multi-AZ Deployment | Static Stability in Region | Application Portfolio Distribution | Multi-AZ Deployment [Regional DR] | Multi-Region Active-Active Deployment |
| Design Complexity | Low | Medium | Medium | High | Very High |
| Cost to Implement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

# Single Region

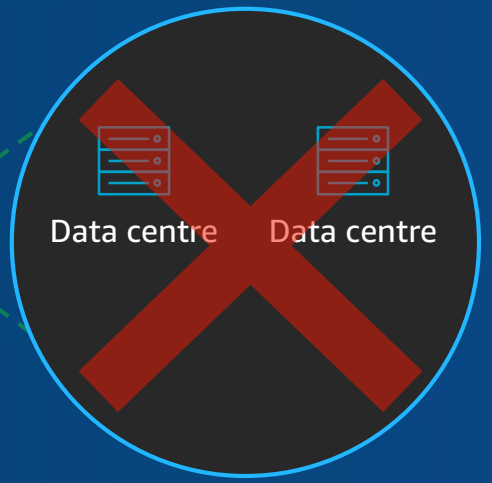
**DISASTER EVENT SCOPE: AVAILABILITY ZONE**

AWS Region
Multiple Availability Zones



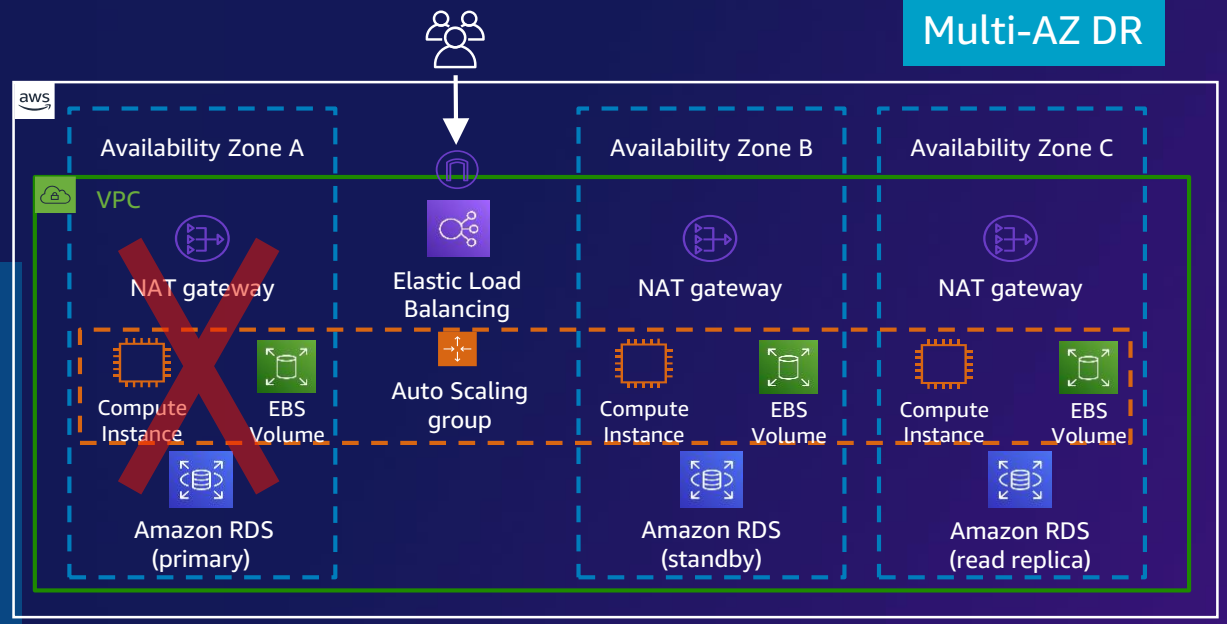

A **Region** is a physical location in the world

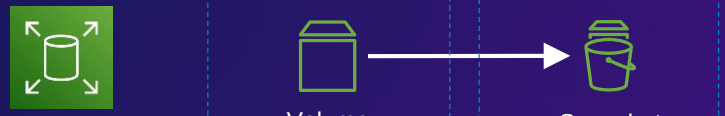
Availability Zone
One or more data centres




Data centres, each with redundant power, networking, and connectivity, housed in separate facilities

Multi-AZ DR




Amazon Elastic Block Store (Amazon EBS)

Amazon DynamoDB

Continuous backup with PITR


Amazon Simple Storage Service (Amazon S3)

# Develop & exercise your incident response plan

## People

- ✓ Train security operations staff on AWS

## Process

- ✓ Develop an incident response plan and strategy
- ✓ Run drills and automate simulations where possible

## Technology

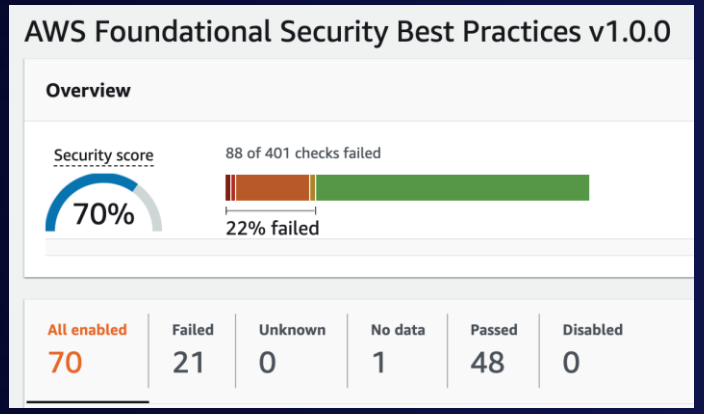
- ✓ Build AWS accounts for security operations and log archival
- ✓ Create read-only and break-glass roles for access to AWS accounts
- ✓ Set up security services like Amazon GuardDuty and AWS Security Hub to detect threats
- ✓ Use security services like Amazon Detective to help you investigate security findings

# Perform self-assessments

**AWS Well-Architected**

Learn, measure, and build using architectural best practices

## AWS Security Hub

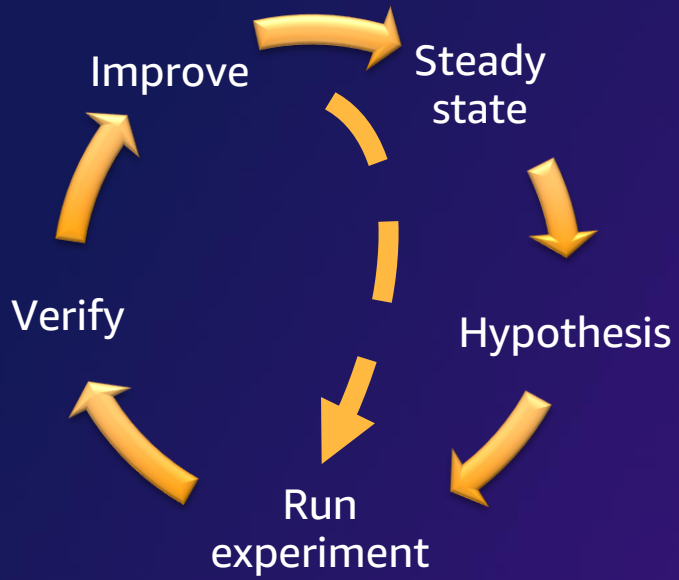



awslabs / aws-security-assessment-solution

These security assessments are from the open source projects "Prowler" and "ScoutSuite," which include custom modules that **check for ransomware-specific findings**

# AWS Fault Injection Simulator

FULLY MANAGED CHAOS ENGINEERING SERVICE ON AWS




Improve application performance and resiliency

Safely run chaos experiments with fine-grained controls

Test complex, real-world failure scenarios

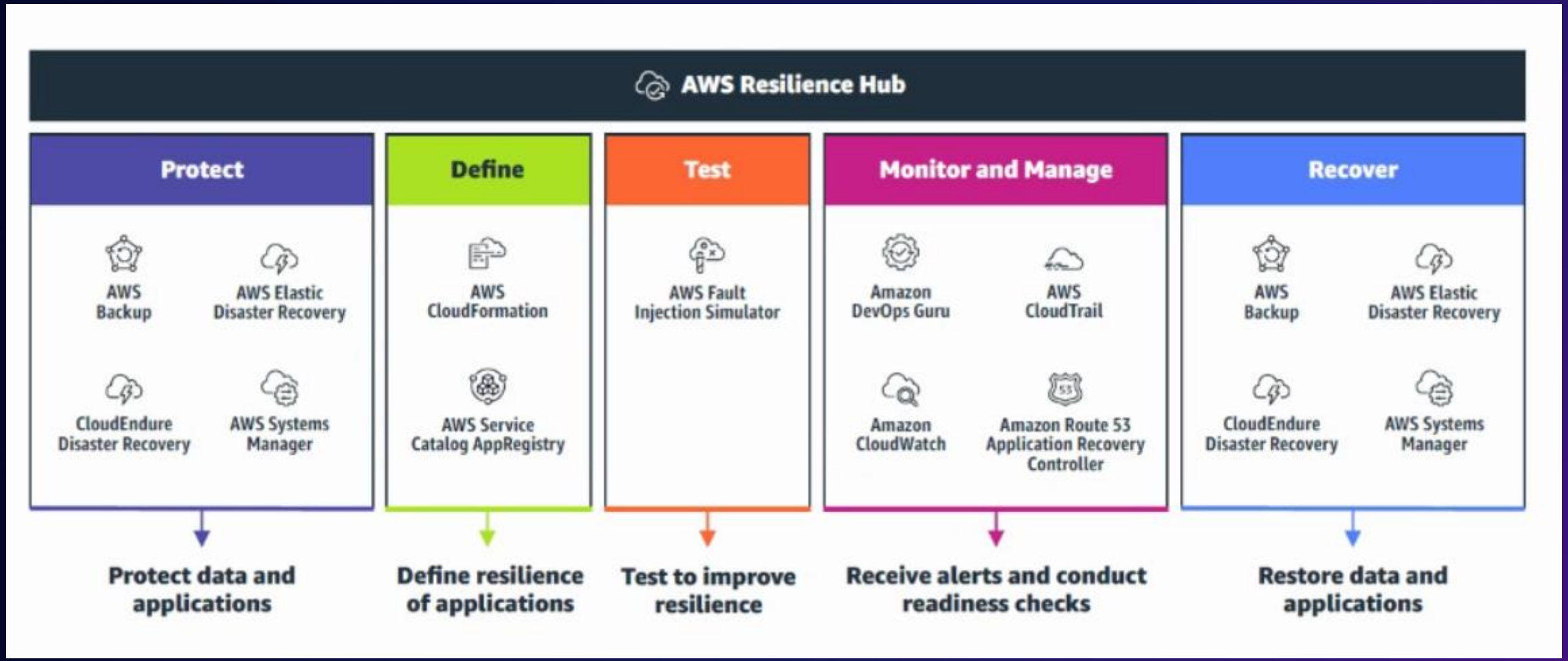
# Key takeaways

- Availability and residency starts with the business
- State your requirements as objectives; avoid specifying solutions
- Understand, and explain, the optionality and impact of recovery choices
- Resiliency is not a pass/fail; it is something to work on continuously
- Make sure you have a plan
- TEST!

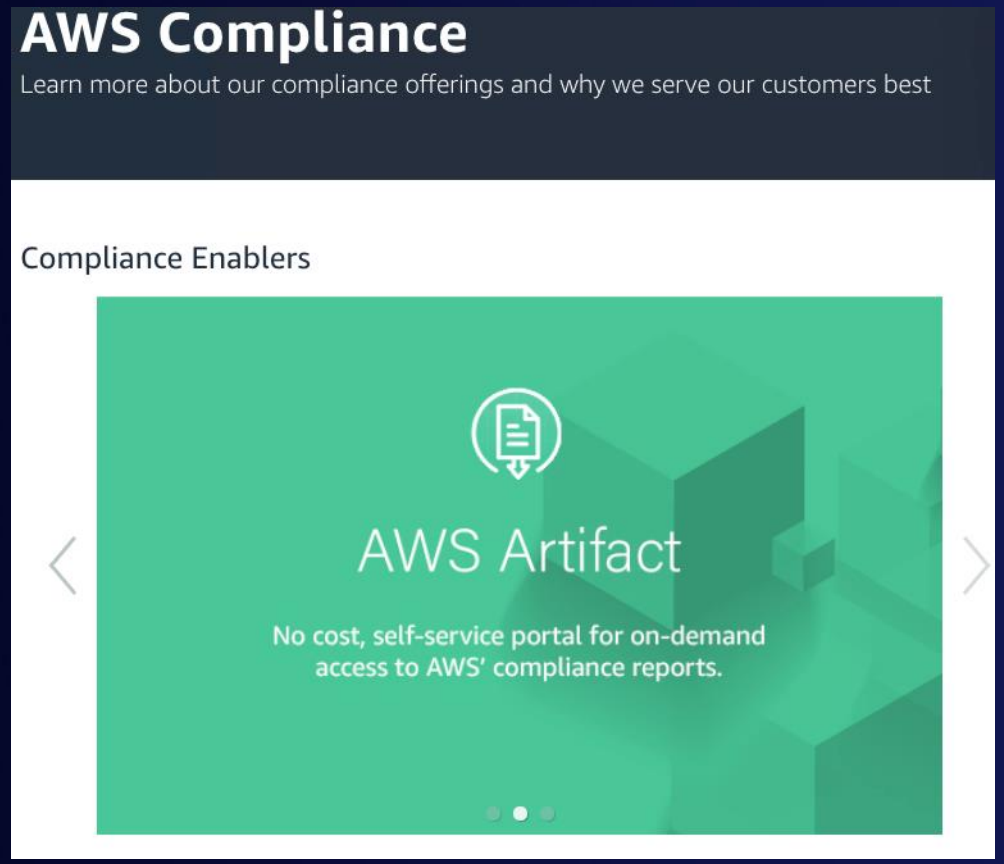
# Additional resources

# AWS resilience tools

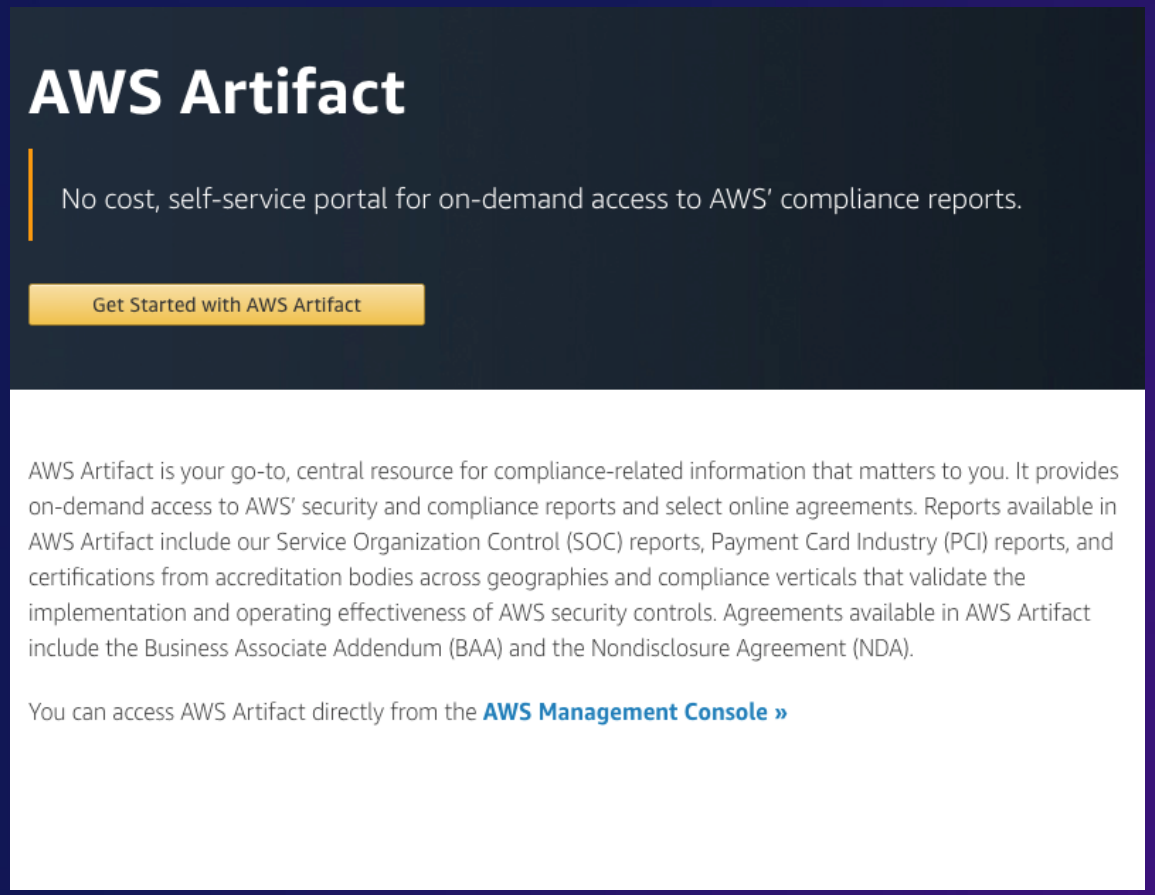
HOW AWS HELPS YOU DESIGN RESILIENT WORKLOADS



# Available reports



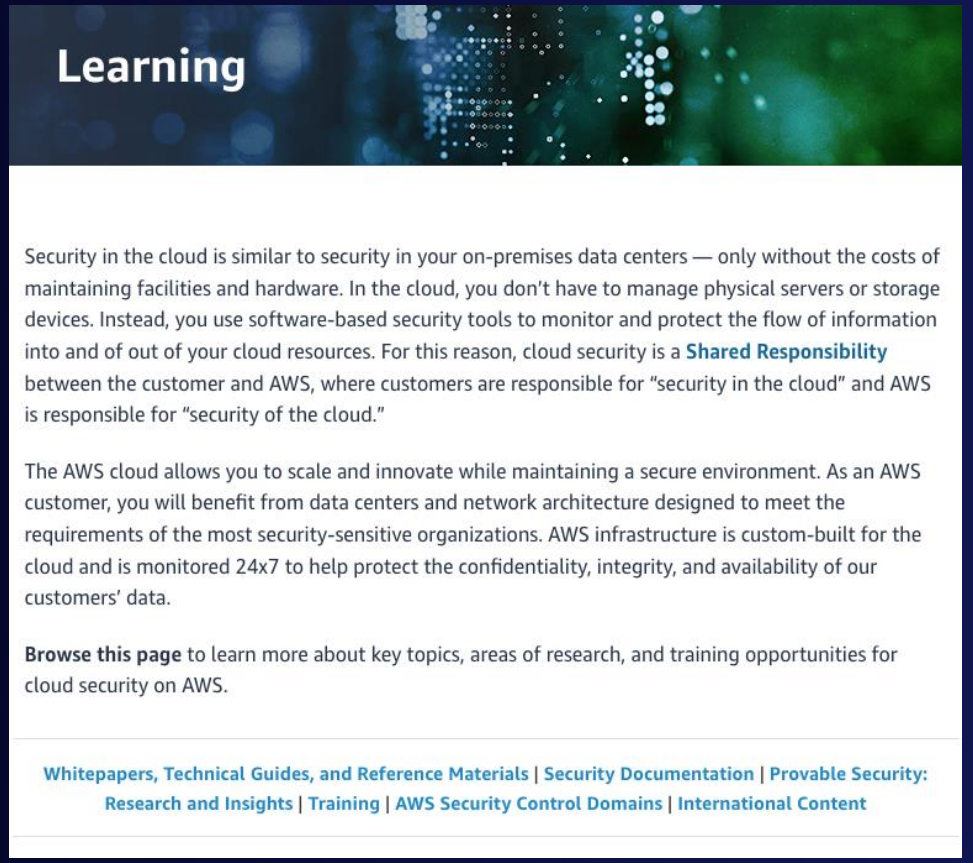

https://aws.amazon.com/compliance/




https://aws.amazon.com/artifact/

# Security resources

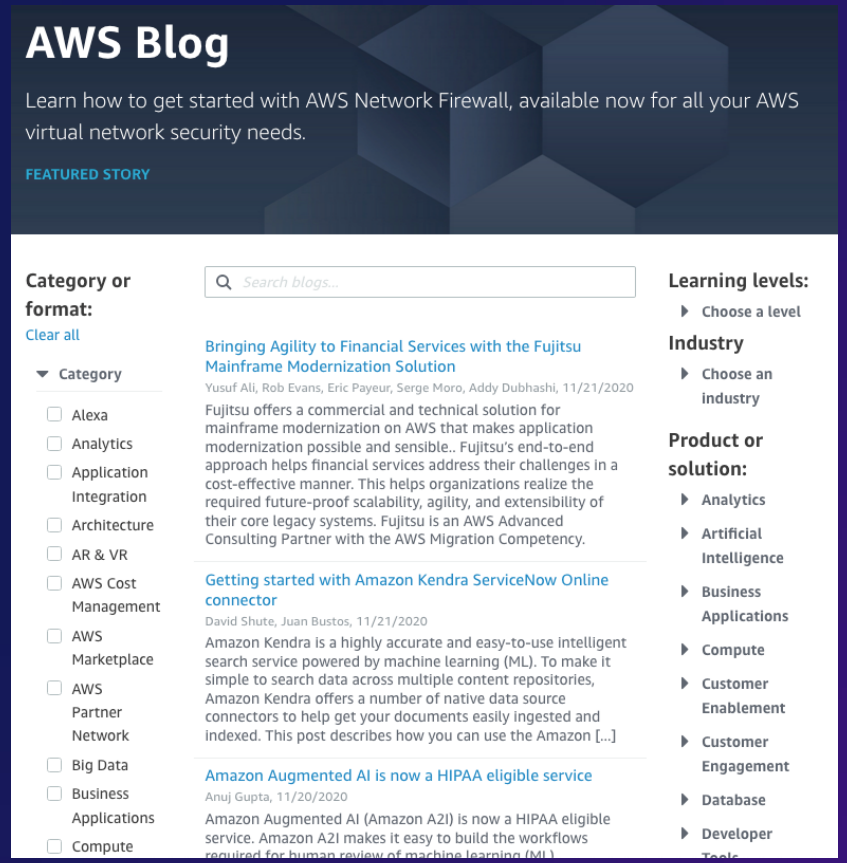
Developer information, articles and tutorials, security products, and whitepapers




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/

# Learn in-demand AWS Cloud skills

## AWS Skill Builder

Access **500+ free** digital courses and Learning Plans

Explore resources with a variety of skill levels and **16+** languages to meet your learning needs

Deepen your skills with digital learning on demand

Train now

## AWS Certifications

Earn an industry-recognised credential

Receive Foundational, Associate, Professional, and Specialty certifications

Join the **AWS Certified community** and get exclusive benefits

Access **new** exam guides

# Thank you!

# Please complete the session survey in the mobile app

Android

iOS