AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

STG203

Backup, disaster recovery, and ransomware protection with AWS

Rajesh Vijayaraghavan (he, his)
Sr. Business Development Manager, AWS Storage
AWS

Aditya Kalyanakrishnan (he, his)
Sr. Product Manager, AWS Storage
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Data protection trends and the customer journey

AWS key data protection features

Backup and archive using AWS

Ransomware recovery using AWS

Disaster recovery using AWS

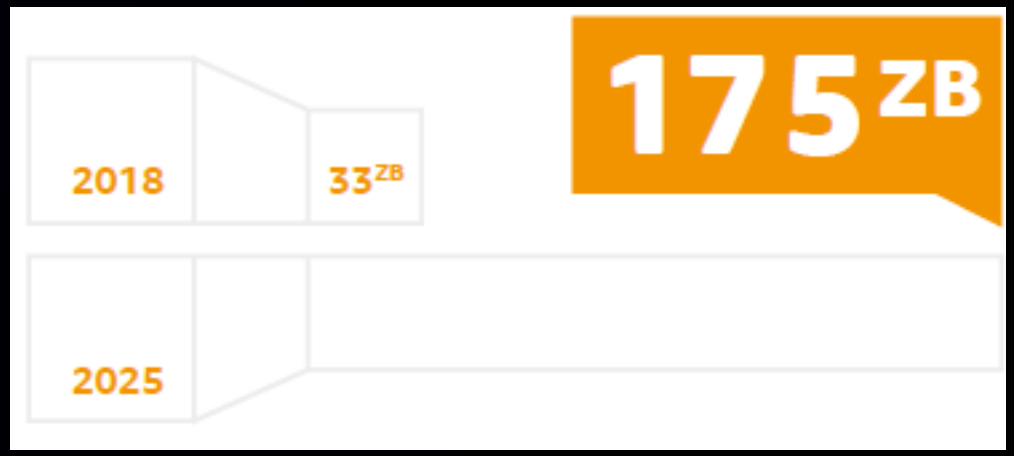
Summary

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data growth is exponential

2018–2025

5.3x



Global data will grow to 175 zettabytes by 2025*

Due to the exponential growth of data worldwide, designing and deploying backup solutions is more complicated than before

Source: *Data Age 2025, IDC and Seagate, April 2017, https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf

aws

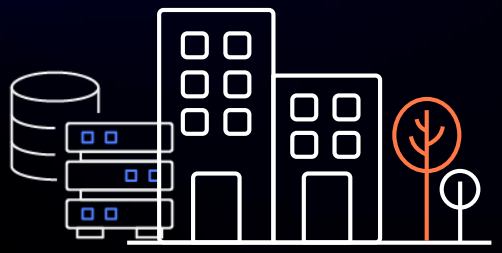
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Customer data protection journey



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Modernize your data protection strategies



With on-premises environment, you:

- Procure, set up, manage, monitor your storage
- Prepay for your storage with no ability to easily scale up or down
- Settle for <11 9s of data durability
- Manage daily maintenance tasks
- Buy two or more appliances for higher availability and redundancy with no SLAs



With AWS storage, you do NOT:

- Pay for fixed storage costs up front
- Worry about running out of space
- Settle for <11 9s of data durability
- Manage daily or weekly maintenance tasks
- Settle for <99.5% data availability or buy multiple backup appliances to increase availability

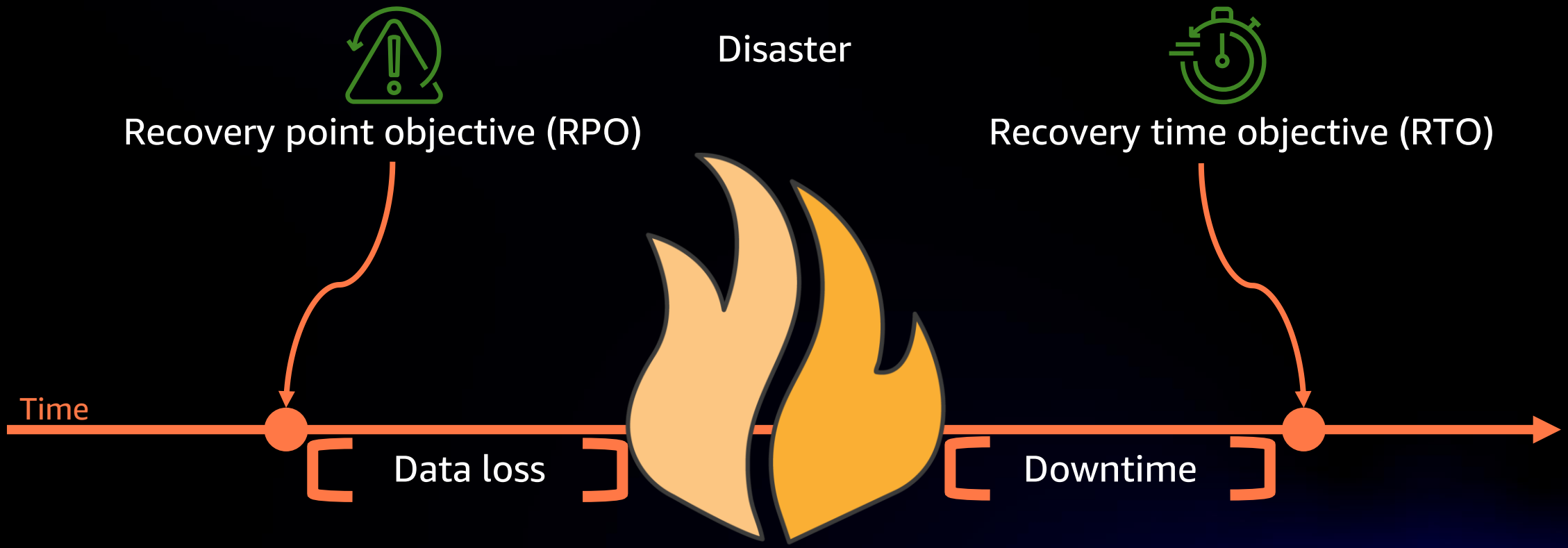
aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data protection key metrics

How much data can you afford to re-create or lose?

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



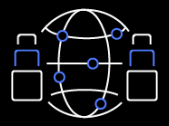
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data protection objectives

Goal



Protect data from accidental deletes



Replicate data for resiliency and bad actor protection



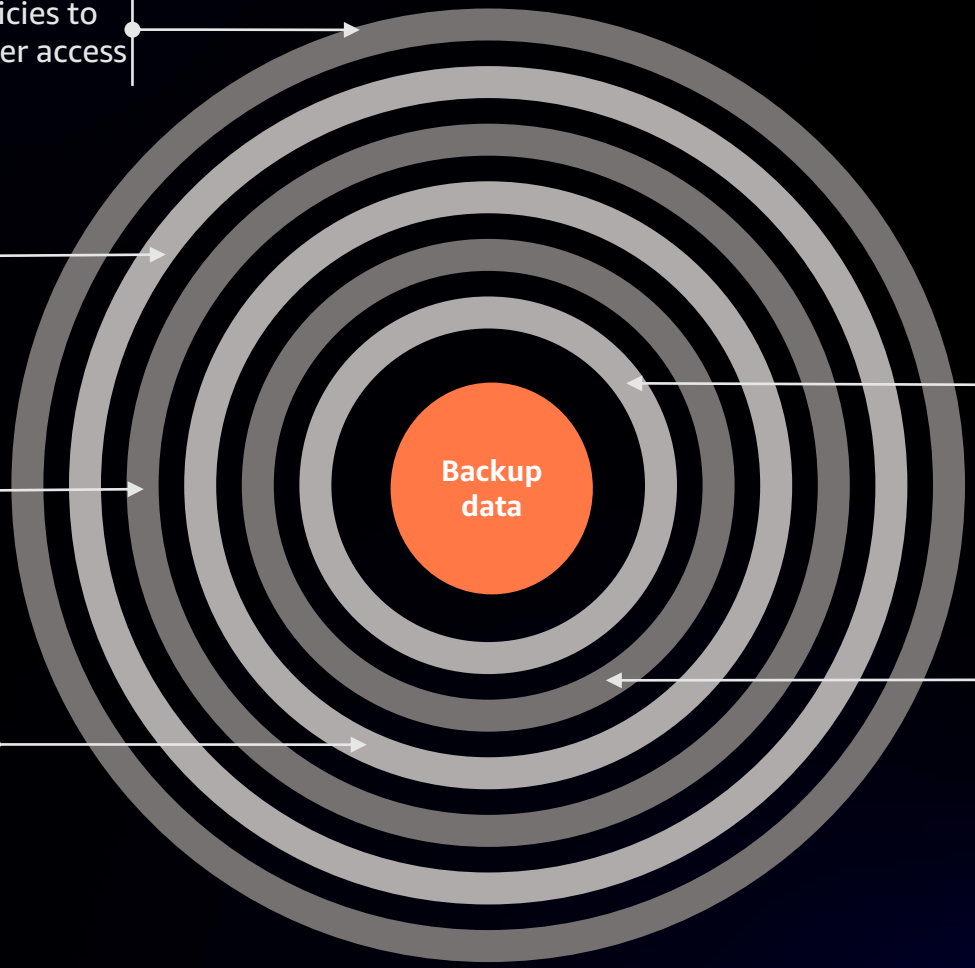
Protect data for governance and compliance purposes



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS multi-layer security

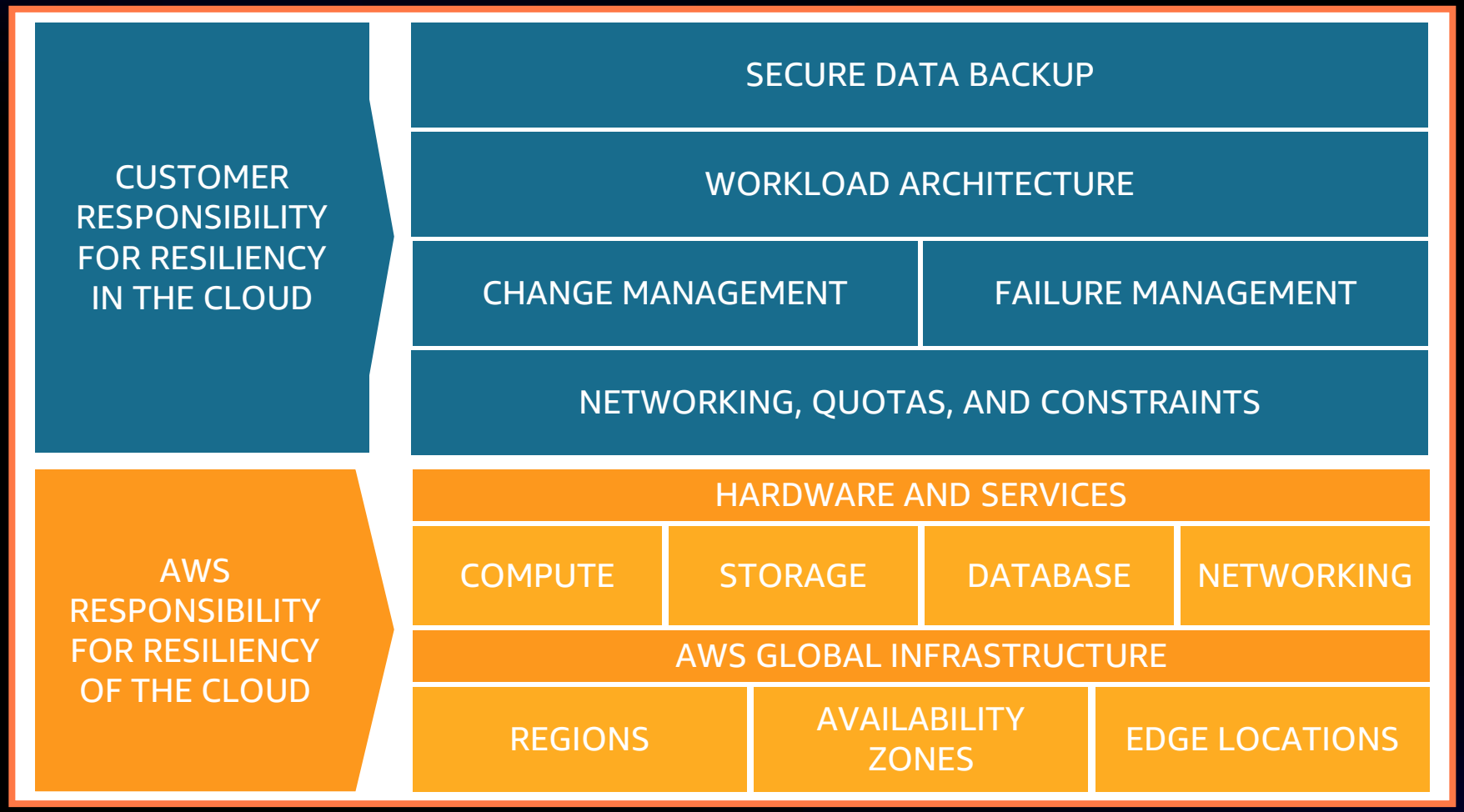
PROTECT DATA WITH MULTIPLE LAYERS OF SECURITY



1. IAM policies to restrict user access
2. Enable multi-factor authentication
3. Immutable backups: enable cross-account backups
4. Enable encryption; use KMS with restrictive key policies
5. Physical security/ digital separation of roles: no access to backup storage
6. Enable audit tracking

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shared responsibility model for resiliency



Reliability Pillar
AWS Well-Architected

http://bit.ly/reliability-pillar

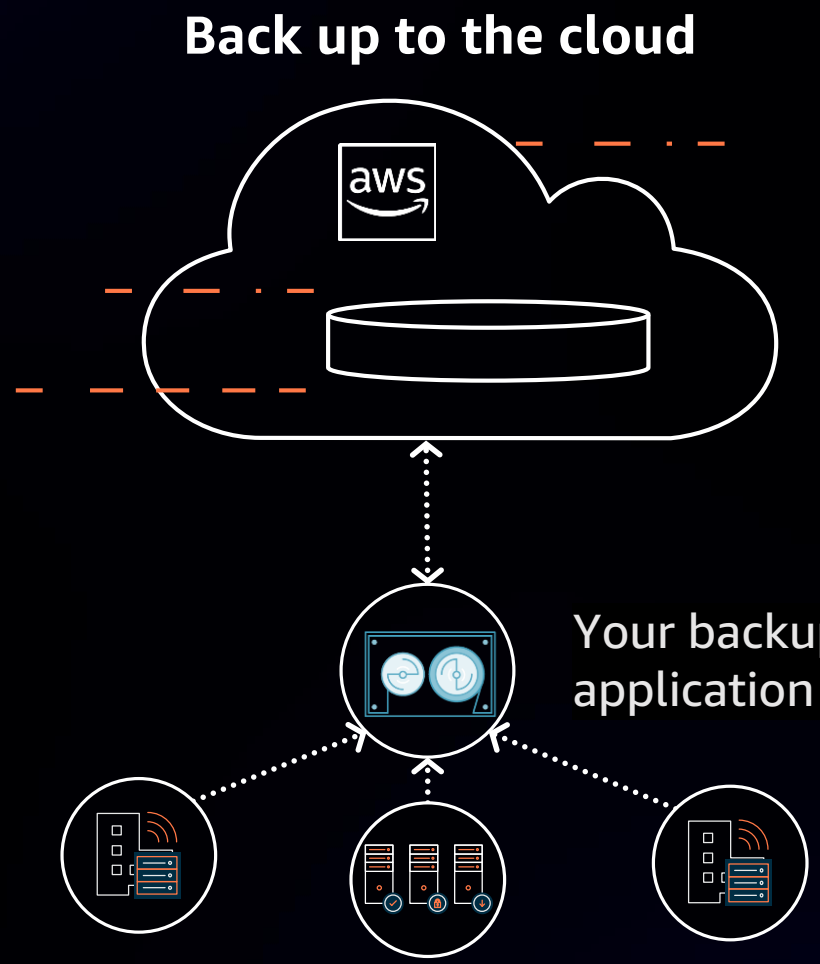
aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS data protection features

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data protection with AWS

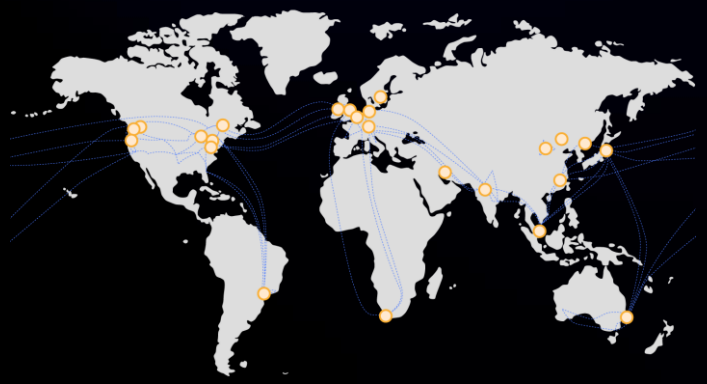


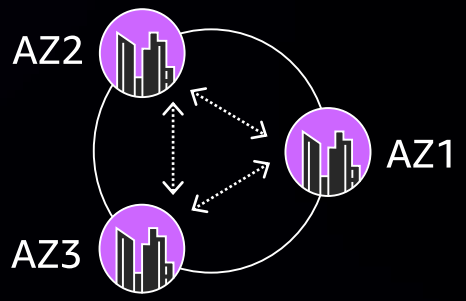
You have on-premises data and applications to protect

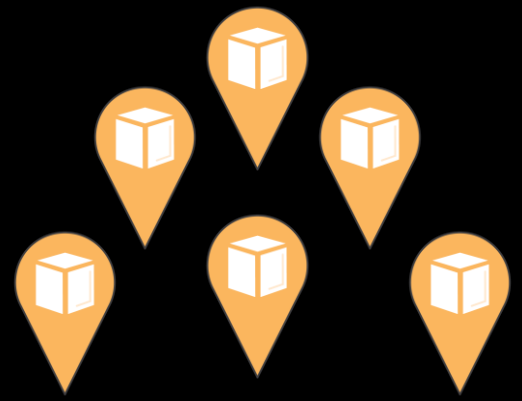
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Operate at scale with Amazon S3

DESIGNED FOR 11 9S OF DURABILITY







25 Regions

Geographic locations with multiple AZs, separated physically by miles and isolated

81 Availability Zones (AZs)

Objects stored across multiple devices spanning a minimum of 3 AZs

Multi-AZ storage classes function normally if an AZ is lost

Highly durable

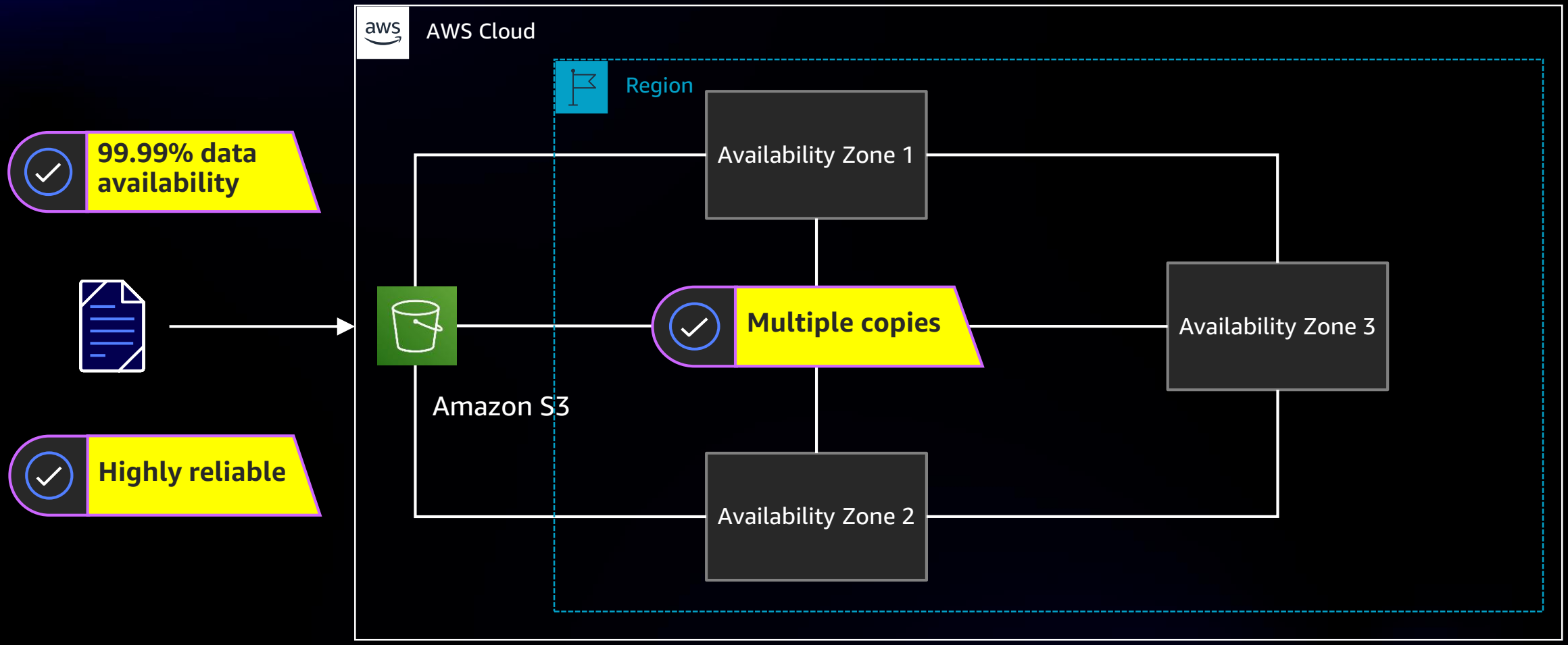
Designed to sustain concurrent device failures and data in the event of an entire AZ loss

Operational performance is second only to security

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Higher availability for your backup data



99.99% availability in S3 Standard and IA classes

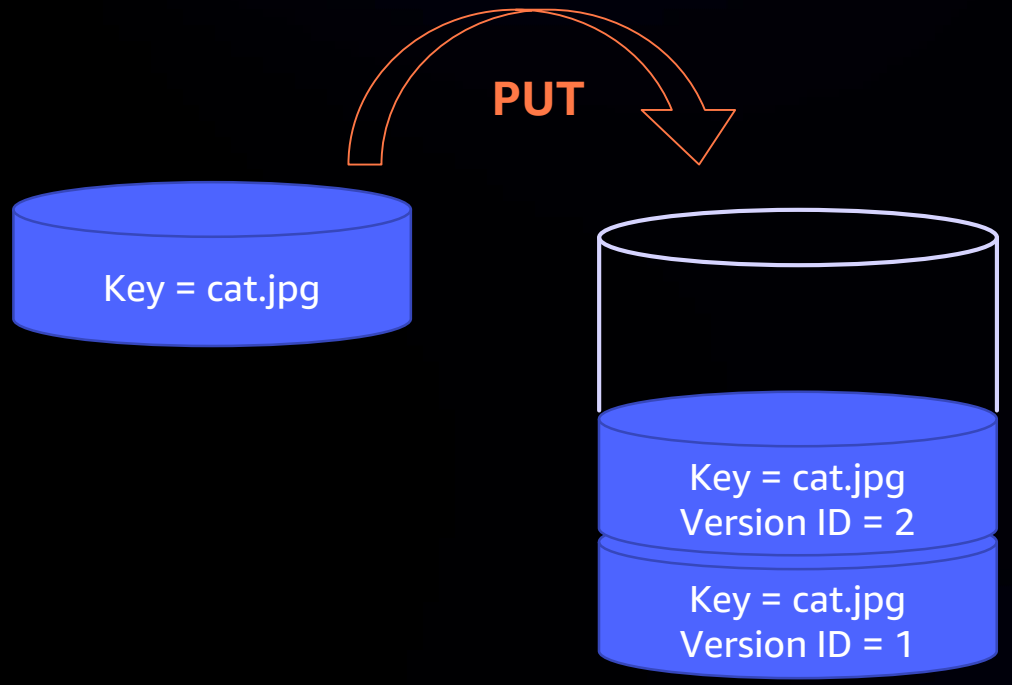
Designed for 99.999999999% durability

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 bucket versioning

PROTECT YOUR DATA FROM ACCIDENTAL DELETION



Create a new version with every upload
Previous versions are retained, not overwritten

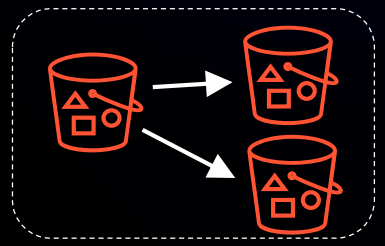
Protect from unintended user delete
Delete requests without version ID removes access to object but keeps the data

Manage previous versions with lifecycle
Transition or expire objects a specified number of days after they are no longer the current version

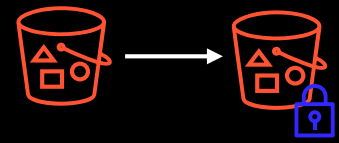
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 replication

Replicate to 1 or more buckets within the same AWS Region



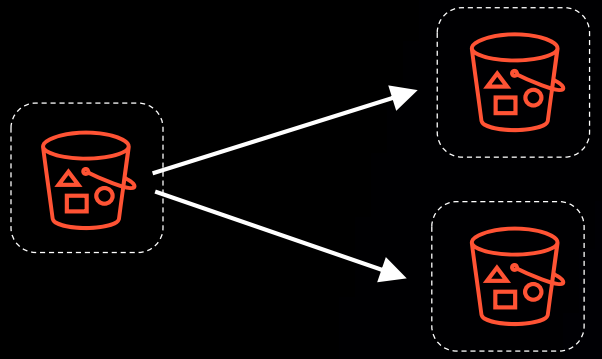
Replicate to a bucket with retention controls (in the same or different AWS Region)



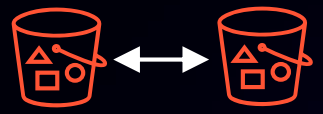


Amazon S3

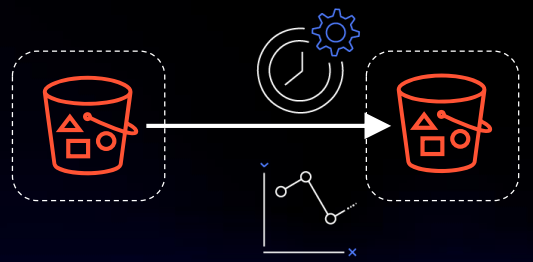
Replicate to one or more bucket in different AWS Regions



Bidirectional replication (in the same or different AWS Region)



Replicate faster to a different AWS Region, backed by an SLA plus replication metrics



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 Object Lock



Ingest

Add retention controls to the object on PUT,
or use bucket defaults to set retention on all new objects



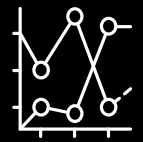
Lock

WORM enforced based on Retain Until Date
Versioning protects against overwrite, deletes are blocked



Retain

Use APIs to extend retention, or for legal holds



Audit

Review and audit retention information using S3 inventory
and object-level events

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 Object Lock modes

Use **Object Lock** to safely store backups against ransomware

Retention period

Compliance mode

Store compliant data

Governance mode

Store data in WORM format; privileged users can modify retention controls

Legal hold

If you're unsure how long you want your objects to stay immutable

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon S3 storage class options

Low RTO ideal for primary copies



S3 Standard

- Active, frequently accessed data
- Millisecond access



S3 Standard-IA

- Infrequently accessed data
- Millisecond access
- Retrieval fee per GB
- Minimum storage duration
- Minimum object size

Archive storage classes for secondary/tertiary copies



S3 Glacier

- Archive data
- In minutes and hours
- Retrieval fee per GB
- Minimum storage duration
- Minimum object size



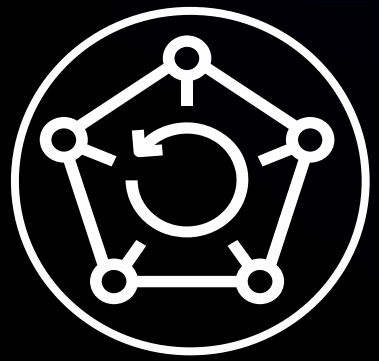
S3 Glacier Deep Archive

- Long-term archive data
- Select hours
- Retrieval fee per GB
- Minimum storage duration
- Minimum object size

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Back up in the cloud using AWS Backup

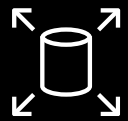


AWS Backup

A fully managed, policy-based backup service that makes it easy to centrally manage and automate the backup of data across AWS services



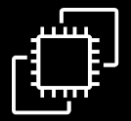
Amazon RDS



Amazon EBS



Amazon EFS



Amazon EC2



AWS Storage Gateway



Amazon DynamoDB



Amazon FSx for Lustre



Amazon FSx for Windows File Server

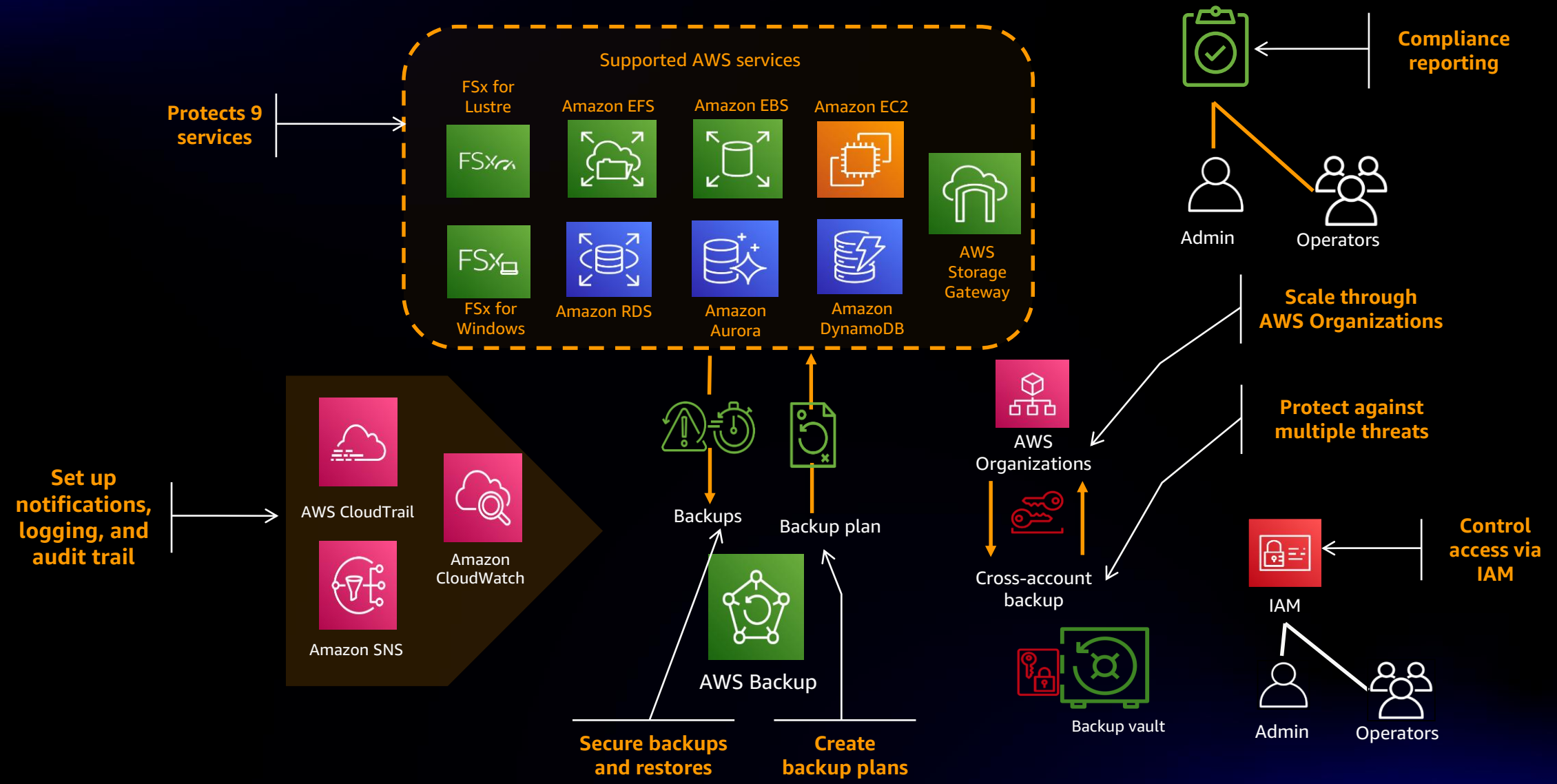


Amazon Aurora

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How AWS Backup works



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup Vault Lock

Vault Lock makes your backups immutable to protect them against inadvertent or malicious actions such as ransomware events



Vault Lock configuration



AWS Backup vault

- Attach a lock to a vault (WORM)
- Protects against deletion and lifecycle changes, even by privileged users
- Enable Vault Lock using AWS Backup API, CLI, or SDK

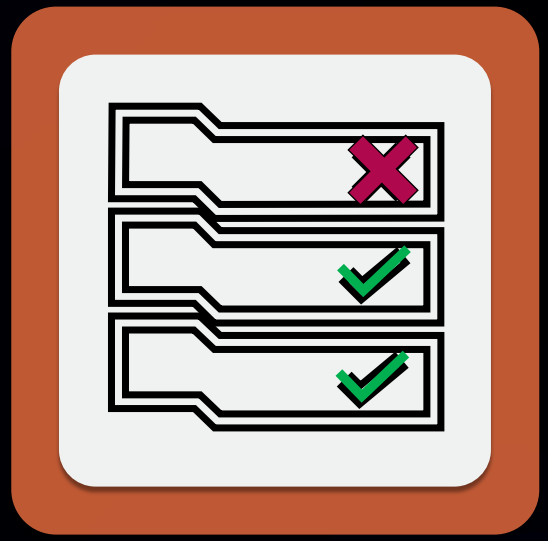
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup Audit Manager

MONITOR, EVALUATE, AND DEMONSTRATE YOUR BACKUP COMPLIANCE POSTURE



Continuously track your backup activities



Automatically audit your backup practices

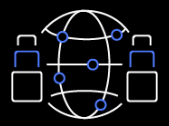


Generate periodic and on-demand audit reports

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data protection objectives

Goal	AWS capabilities
 Protect data from accidental deletes	Use S3 bucket versioning to roll back to a previous versions Create backup policies with AWS Backup
 Replicate data for resiliency and bad actor protection	Replication across accounts and Regions S3 Replication Time Control for SLA-backed replication
 Protect data for governance and compliance purposes	Use S3 Object Lock and AWS Backup Vault Lock to store write-once-read-many (WORM) data

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data protection solutions

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

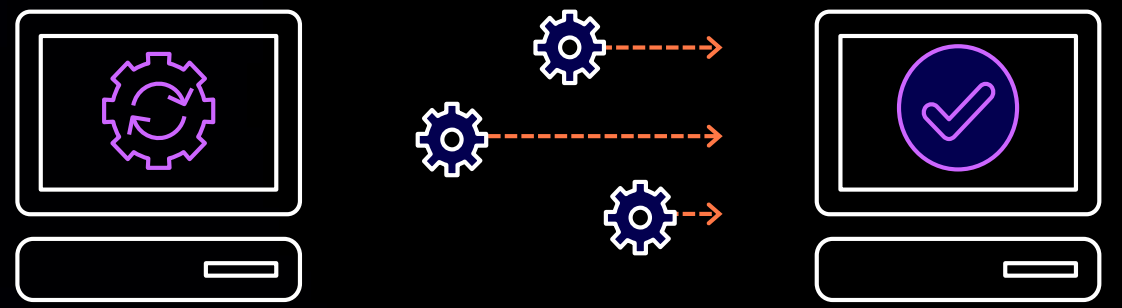
Customer data protection journey

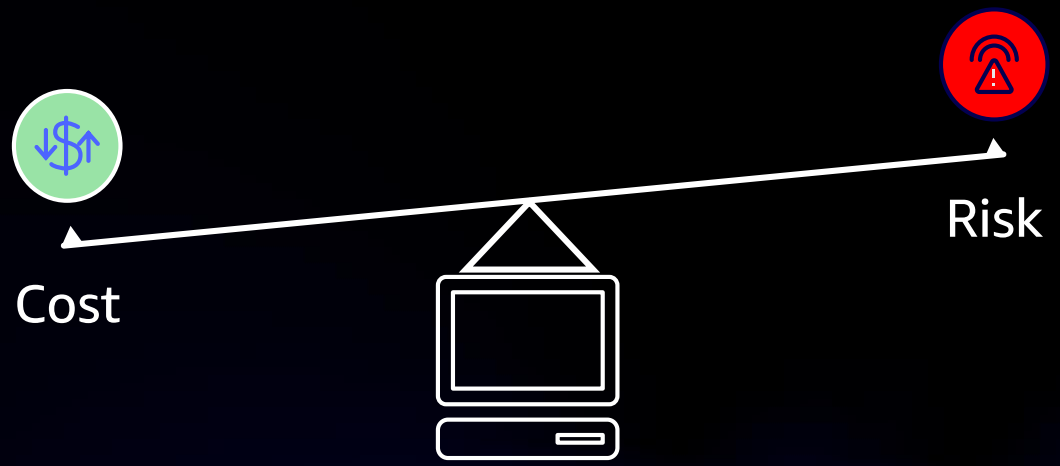


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key considerations for backup

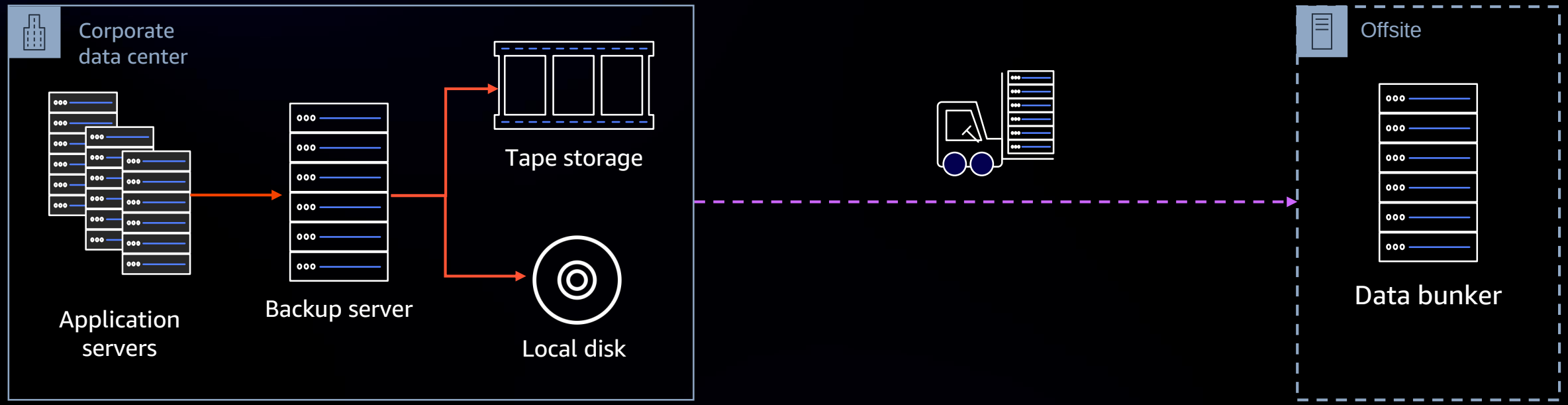
- Minimize time to recover
- Minimize data loss
- Balance cost with business risk





© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Traditional backup environment



Too much data

Vulnerable

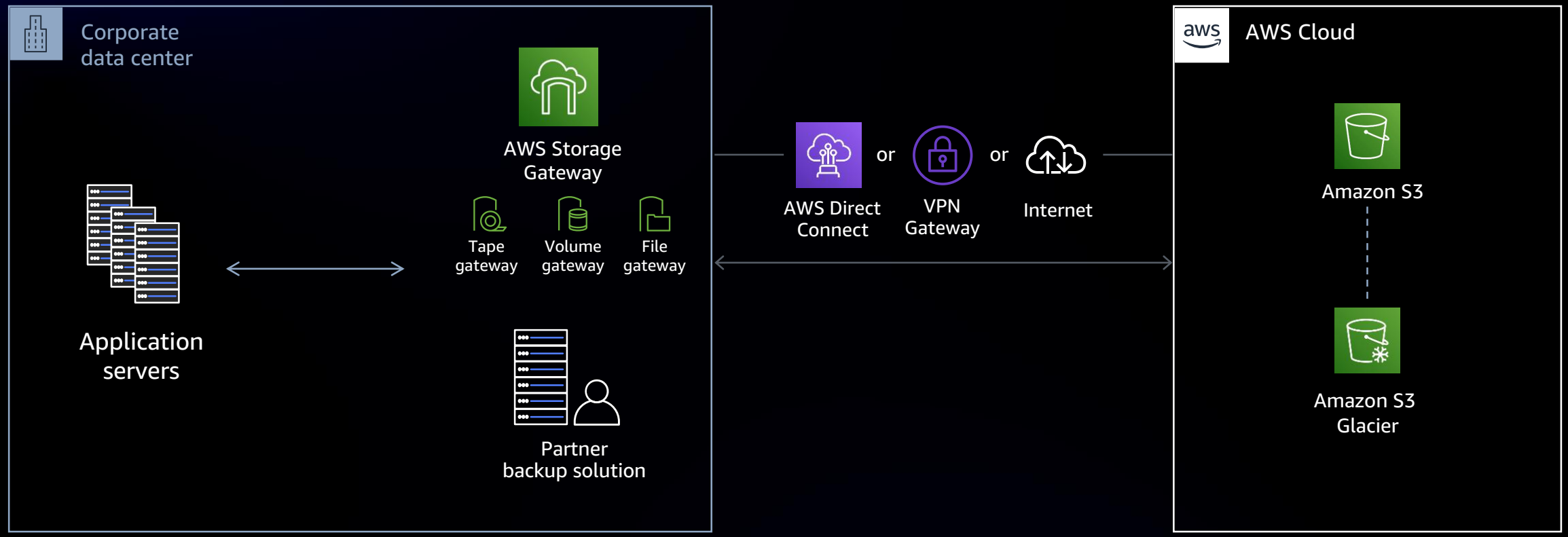
Fragile

Expensive

Complicated

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Modernizing backup with AWS



- Backup from on premises to AWS
- Use AWS Storage Gateway to Amazon S3
- Use backup partner to Amazon S3

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ways to back up with AWS

Backup vendors | Backup on premises and in the cloud, advanced backup functionality, ability to use AWS Backup APIs to integrate with AWS services



AWS Backup

API | Backup for AWS services, API access to multiple AWS services



Amazon EFS



AWS SGW



Amazon RDS



Amazon DynamoDB



Amazon EBS



Amazon S3



Amazon S3 Glacier

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Partners for backup

CLUMIO
COHESITY
COMMVAULT
ctera
DELL EMC
druva
IBM
MSP360 #1 MSP BACKUP
N2WS
NetApp
rubrik
VEEAM
VERITAS

www.aws.amazon.com/backup-recovery/partner-solutions/

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Customer data protection journey



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cybersecurity is increasingly important

75% of IT organizations will face one or more ransomware events **by 2025**

Source: Gartner 2021 study, gtnr.it/3vR5oKh

Analysts are estimating that ransomware events could occur every **11 seconds** in 2021 and result in financial loss of up to **$20B**

Source: Cybercrime Magazine, cybersecurityventures.com/cybersecurity-market-report/

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is ransomware?

Ransomware is a form of malware that threatens to publish victim's data, delete, or perpetually block access to business-critical information unless a ransom is paid off

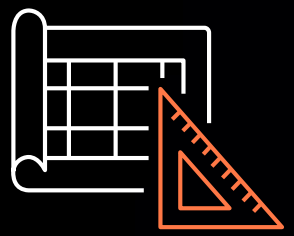


Mass delete ransomware

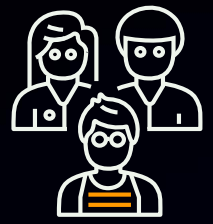


Mass re-encrypt ransomware

Ransomware attacks most likely when



Technical maintenance is behind schedule



Employee behavior creates security risks



Security strategy doesn't prepare for attacks

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Anatomy of an actual ransomware event

First 12 hours

+21 days post-event (millions lost per day)

Infiltrate/access

- Employee hit by social engineering
- application_agent.exe <click-here>
- Gain Windows OS login/Active Directory admin rights
- Push malicious code via Windows update

Event/issue

- Full event begins/users report pop-up to IT
- IP phones down
- AD destroyed/Windows logins disabled
- No email access

Isolate

- Personal email used
- Cell phones for comms

FBI engaged

Cybersecurity consultant

PO issued

Recover

- Local backups not impacted/restores initiated
- No NAS backups; only snapshots
  - Snapshot rollback initiated
  - Dangerously high IOPS/extreme latency

Scrap

- New hardware ordered
- 4,000 laptops /$3+ million in servers

Rebuild/restore

- New hardware/rack and stack of new servers
- Manual rebuild of DNS
- Restores resume/Active Directory restored
- New laptops, reimaging begins
- 3+ weeks manual recovery to roll back snapshots

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NIST Cybersecurity Framework

Industries are now prioritizing recovery



IDENTIFY
Identify an organization's critical functions, assets, and processes and how cybersecurity risks could disrupt them



PROTECT
Define safeguards necessary to protect critical infrastructure services



DETECT
Implement the right measures to identify threats and cyber risks promptly



RESPOND
Define the measures necessary to react to an identified threat



RECOVER
Strategic plans to restore and recover any capabilities damaged during a cybersecurity event

Strategy formation

- What is the most important data that you want to protect?
- Should the recovery of some data be prioritized over others?
- What is an acceptable recovery time?
- What tradeoffs should be made among budget, time, and data completeness?

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key requirements of ransomware recovery

Immutable
Store objects in a state that cannot be modified after creation

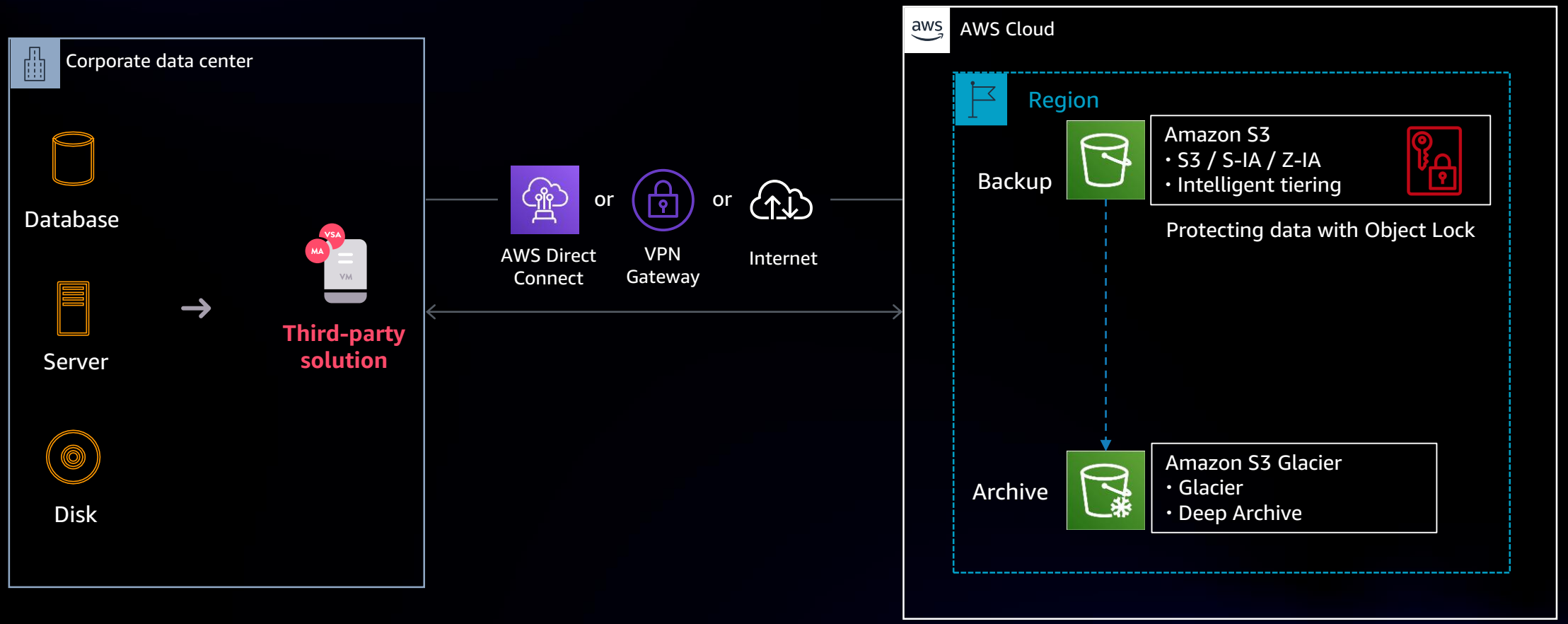
Isolation
Physically and logically isolating copies of infrastructure templates, files, and applications required to bring back mission-critical business processes

Intelligence
Machine learning and content analytics scanning data offers insight into how the data has changed and can alert to signs of corruption



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

On premises to AWS ransomware recovery



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Partner ransomware recovery

COMMVAULT

VEEAM

VERITAS

Zerto

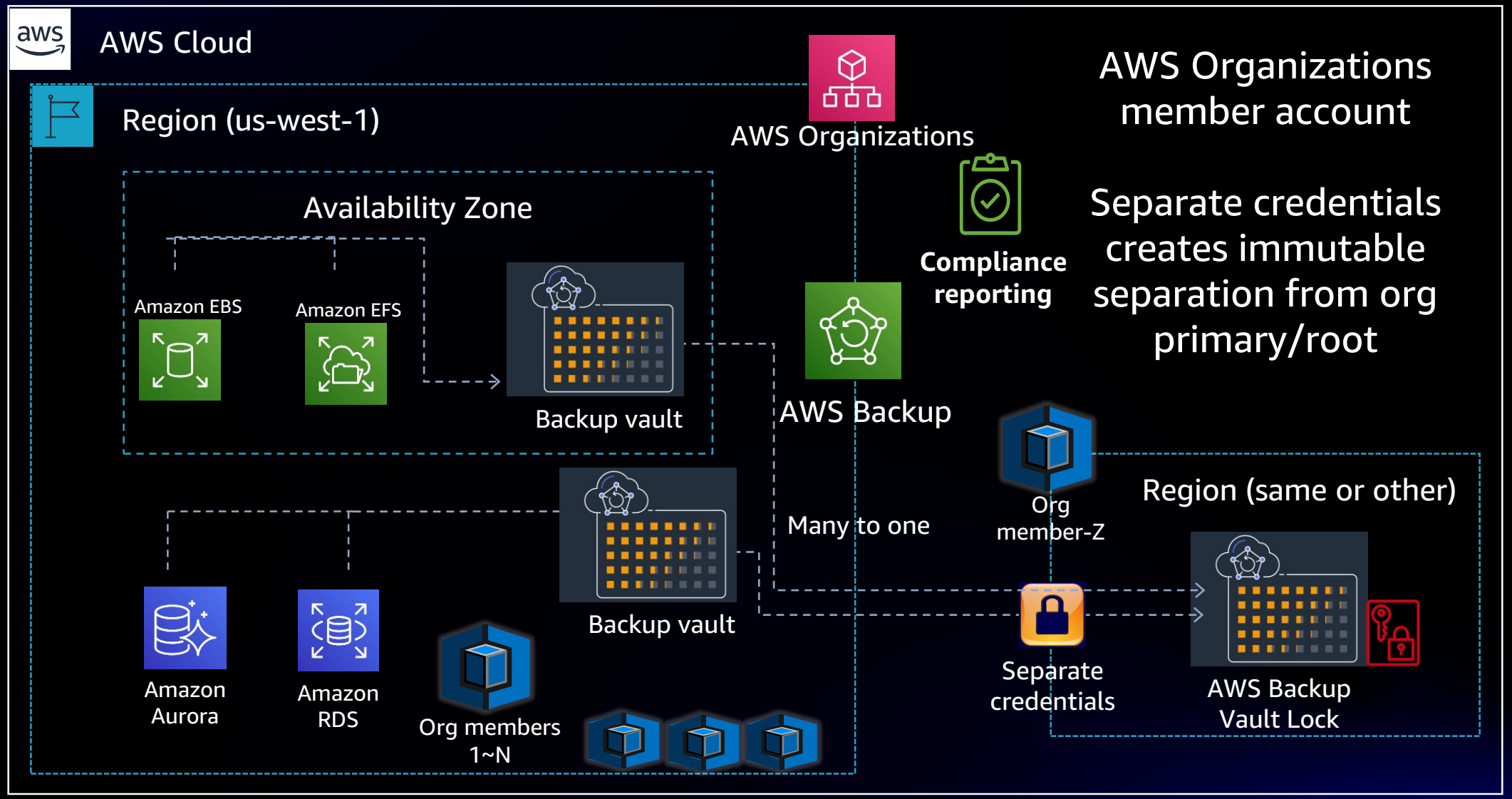
- Supports **Amazon S3 Object Lock** for immutable object storage
- Store backups in Amazon S3 using **write-once-read-many (WORM)** model
- Prevent delete, modify, or overwrite of data
- Protect against ransomware and rogue actors

www.aws.amazon.com/backup-recovery/partner-solutions/

aws

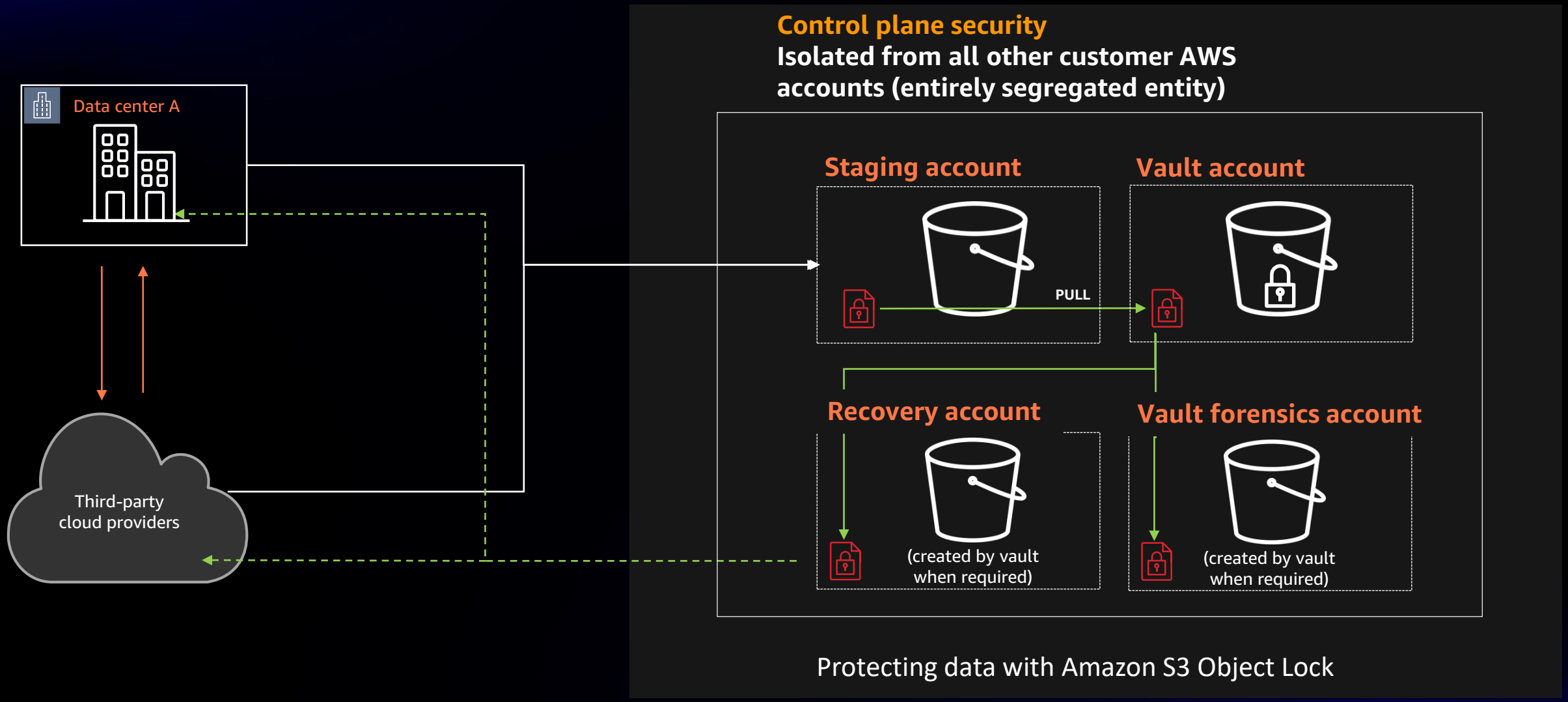
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS to AWS protection with AWS Backup



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS ransomware recovery solution



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Customer data protection journey



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Types of disaster

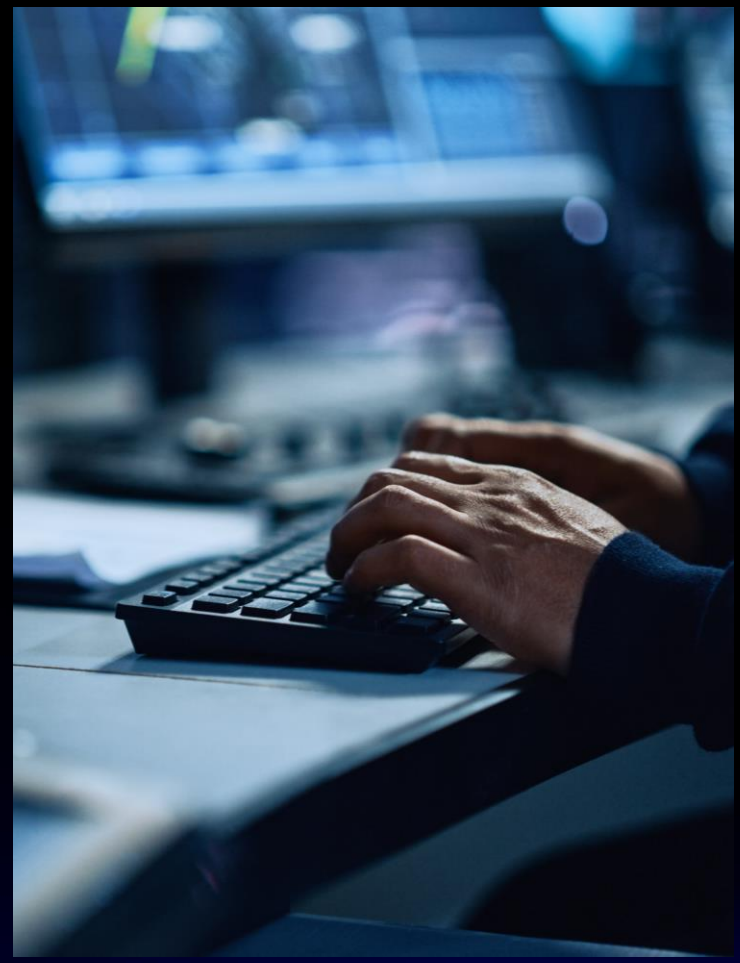
Natural disaster



Technical failure

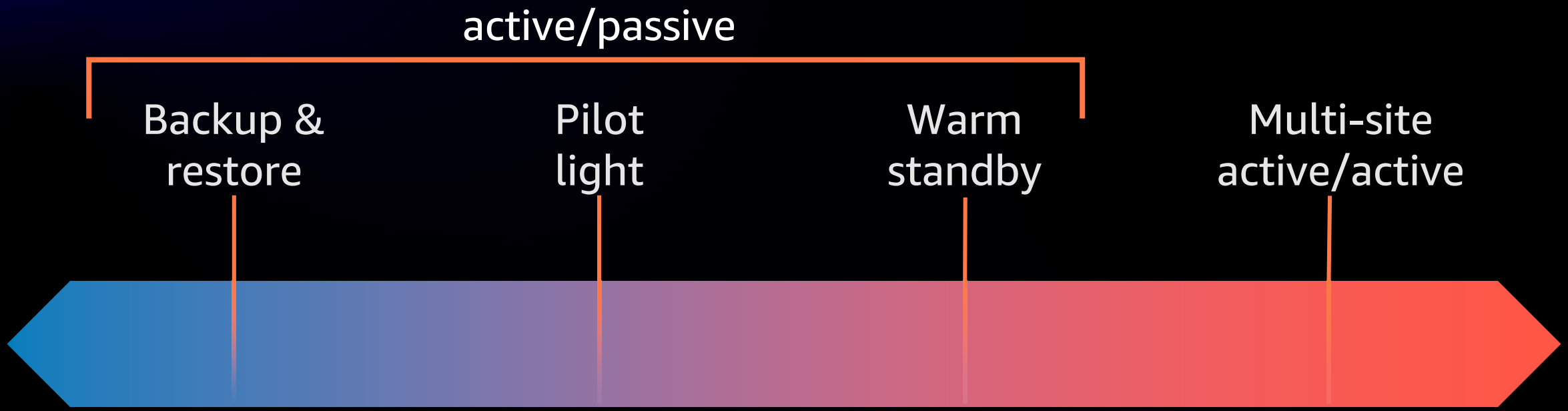


Human actions



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Strategies for disaster recovery



RPO/RTO: hours

- Lower-priority use cases
- Provision all AWS resources after event
- Restore backups after event
- Cost: $

RPO/RTO: 10s of minutes

- Data live
- Services idle
- Provision some AWS resources and scale after event
- Cost: $$

RPO/RTO: minutes

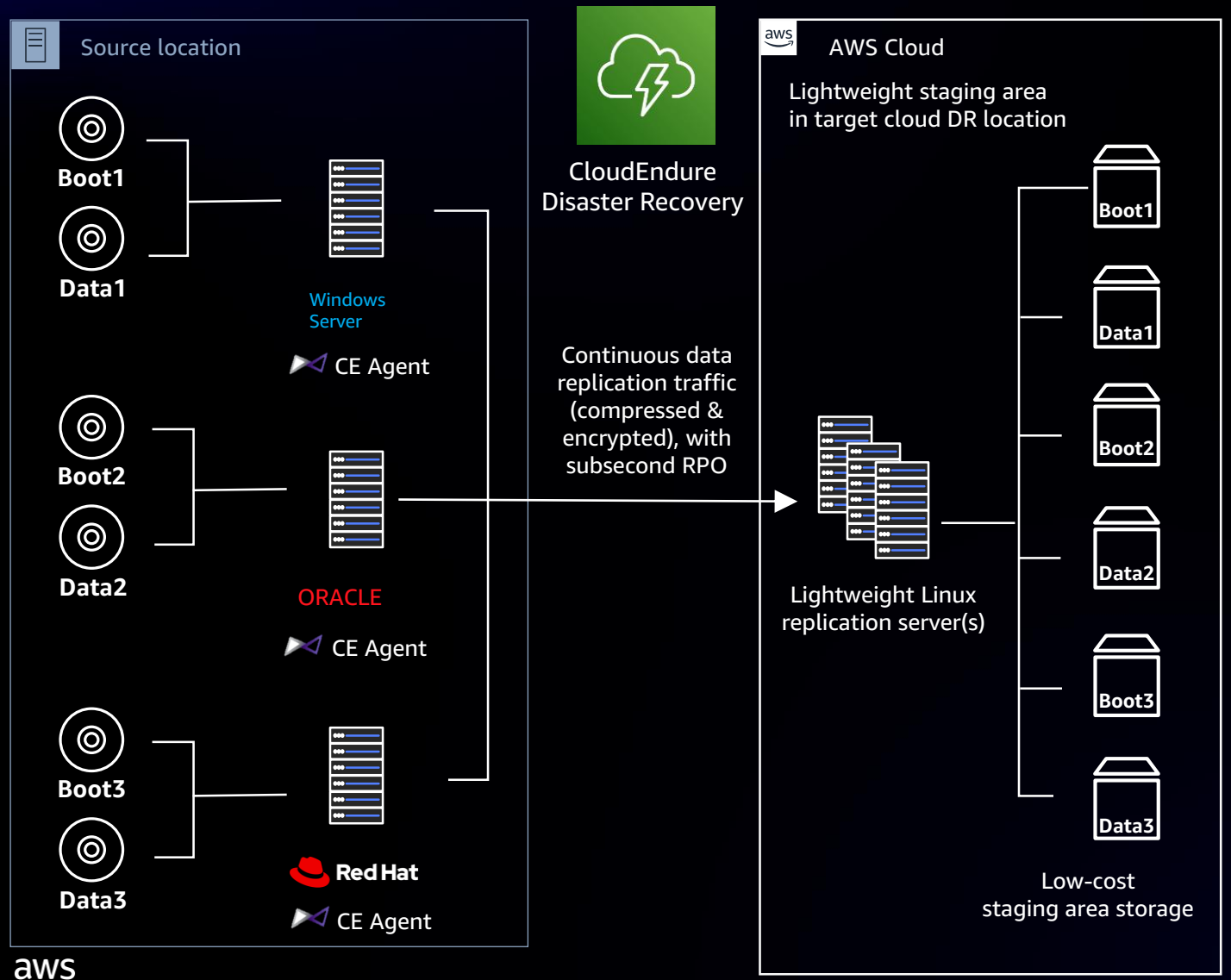
- Always running, but smaller
- Business-critical
- Scale AWS resources after event
- Cost $$$

RPO/RTO: real time

- Zero downtime
- Near-zero data loss
- Mission-critical services
- Cost $$$$

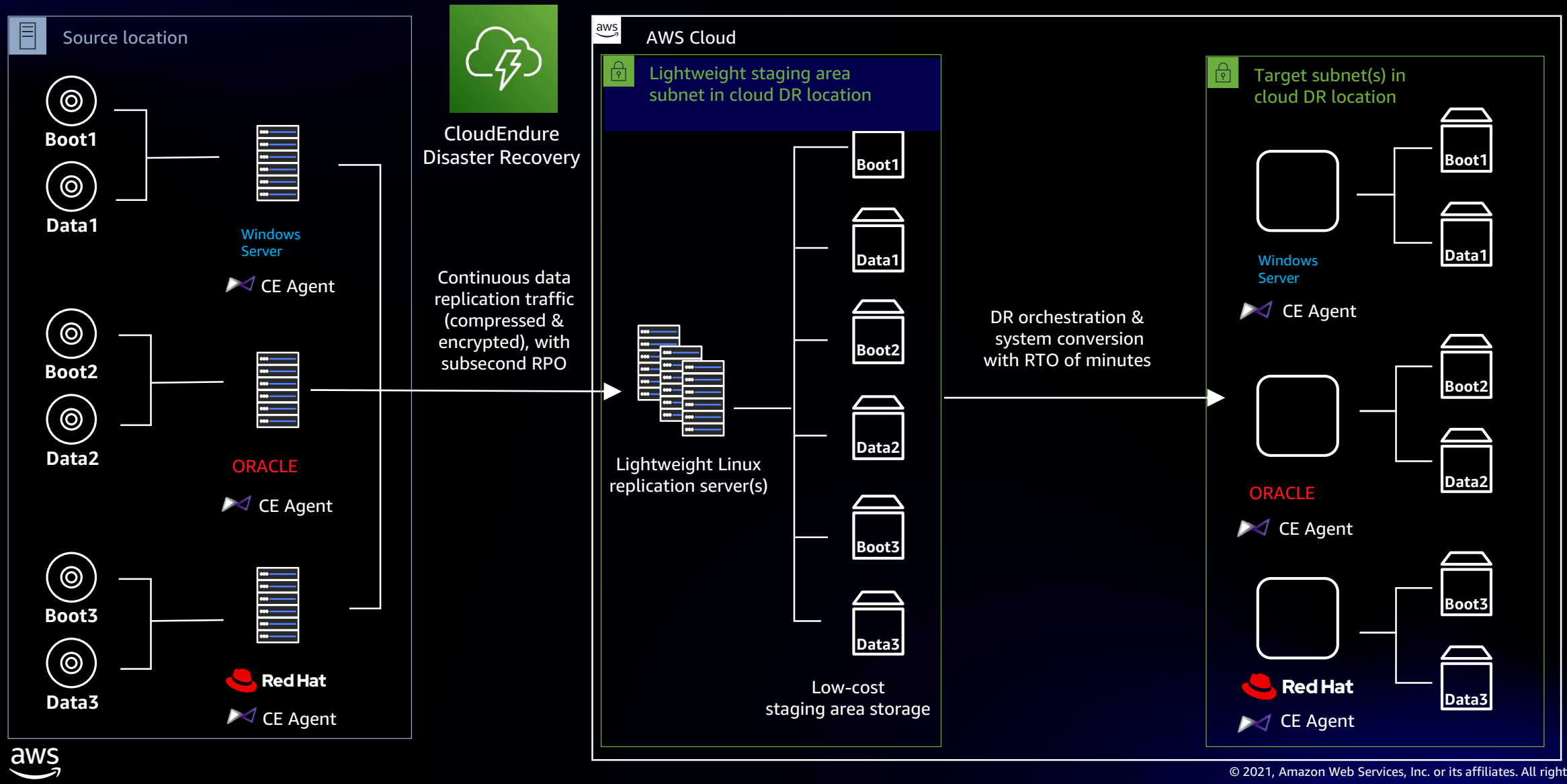
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pilot light (CloudEndure) lightweight staging



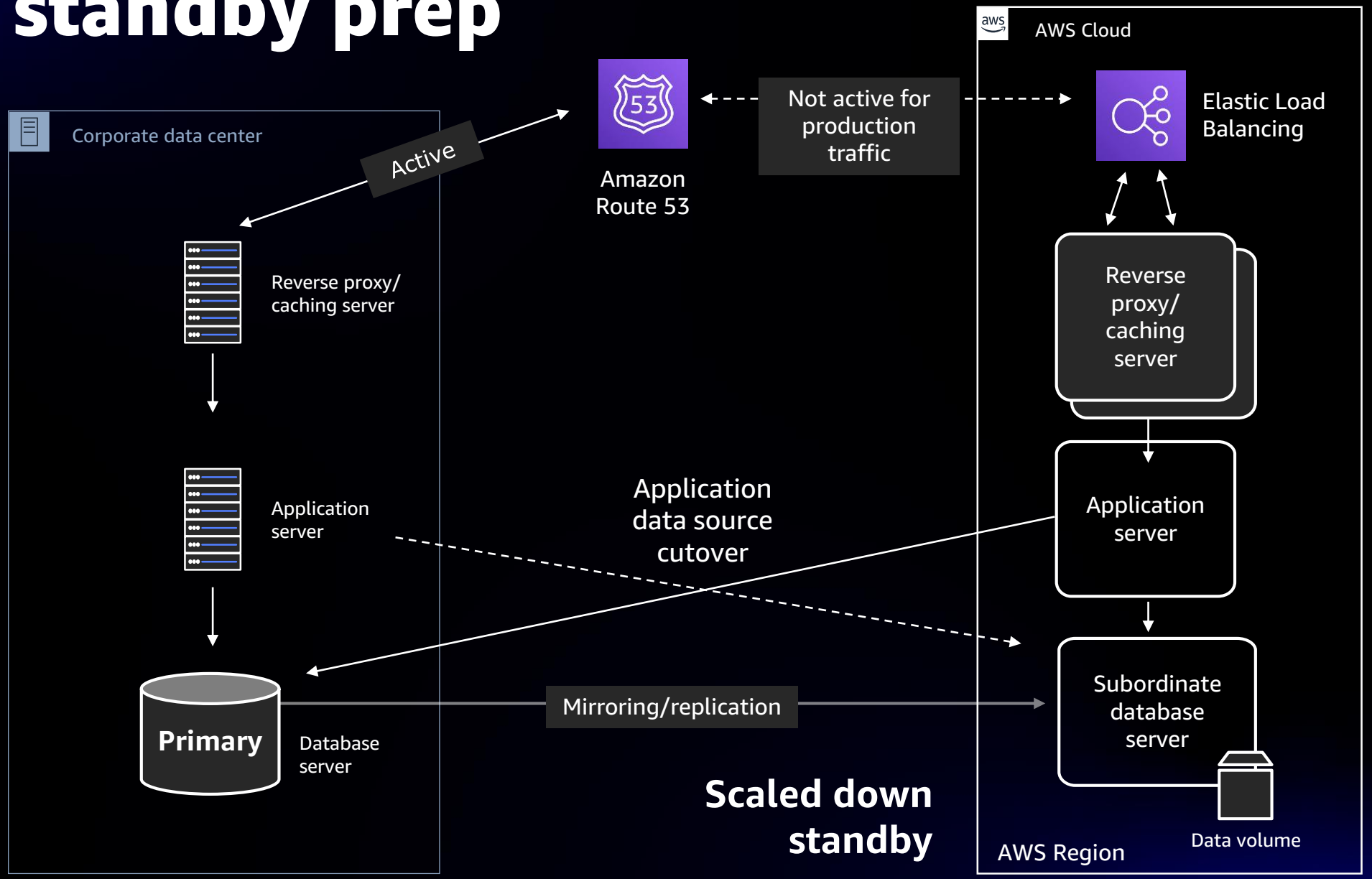
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pilot light (CloudEndure) failover scenario



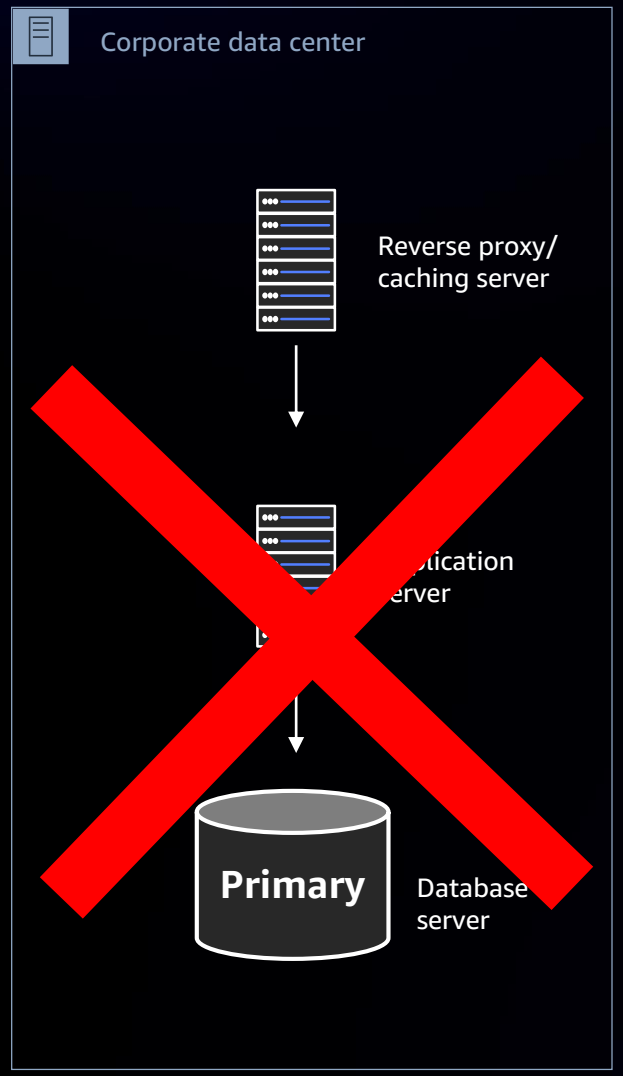
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

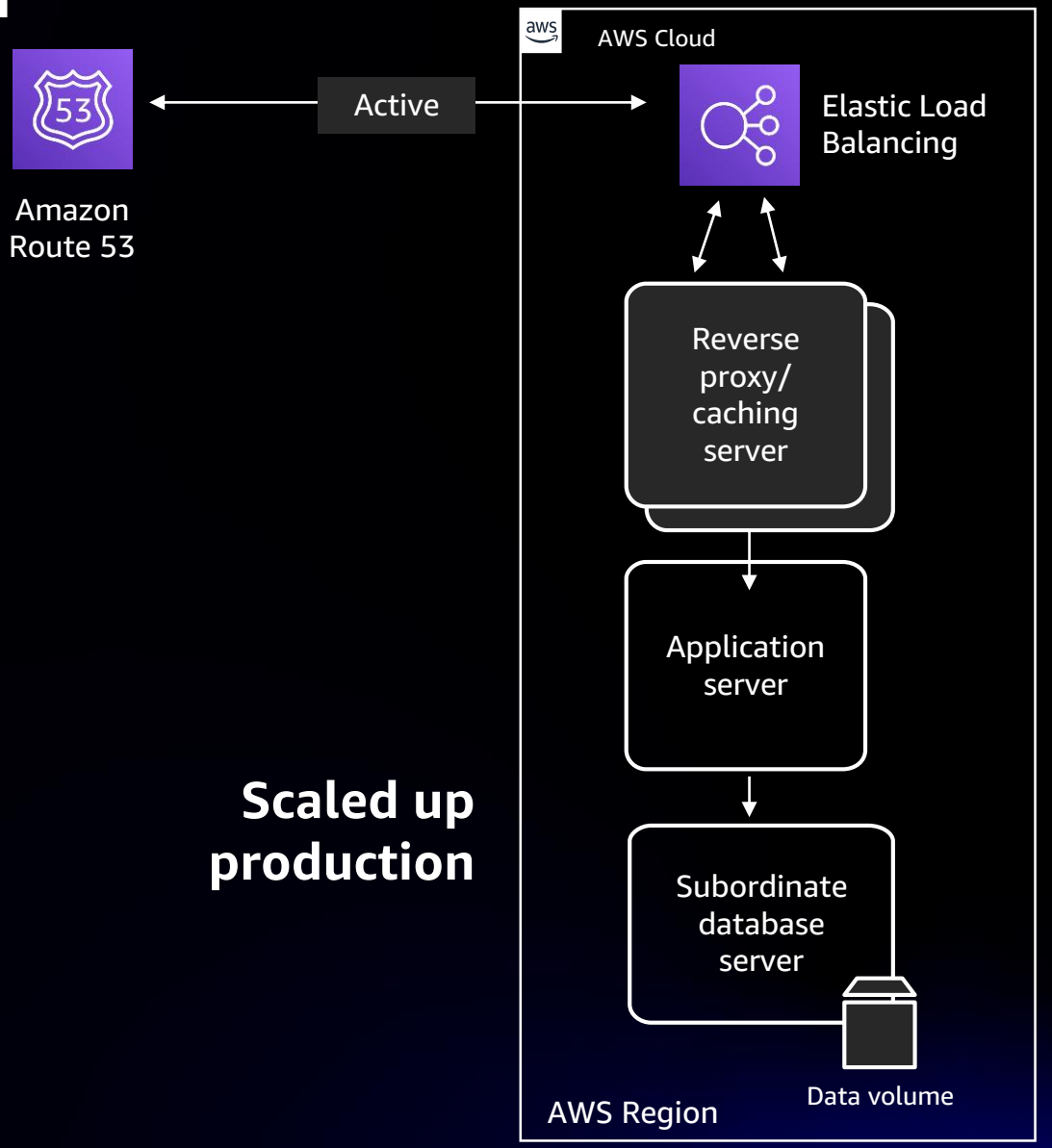
Warm standby prep



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Warm standby recover

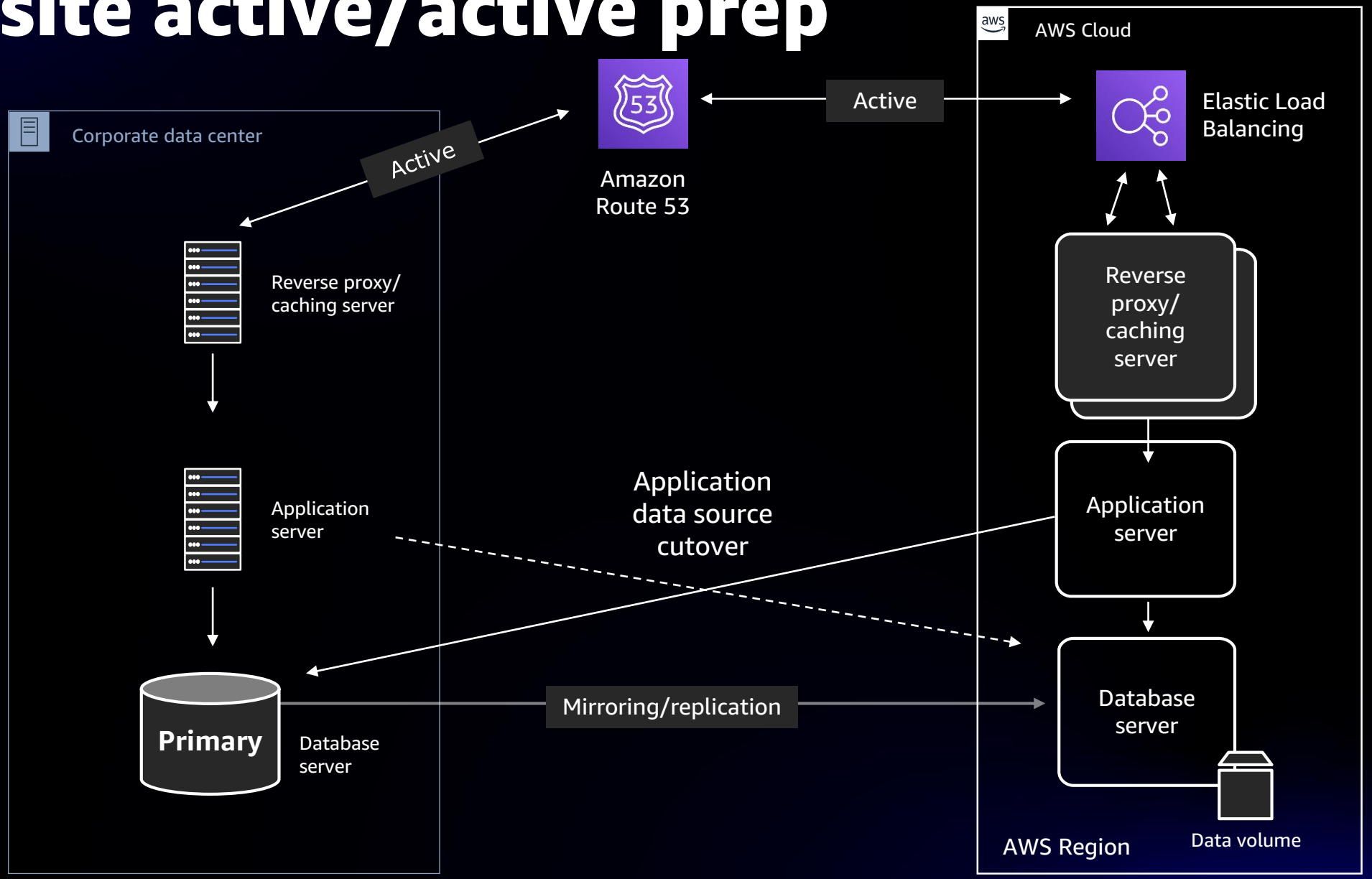




Scaled up production

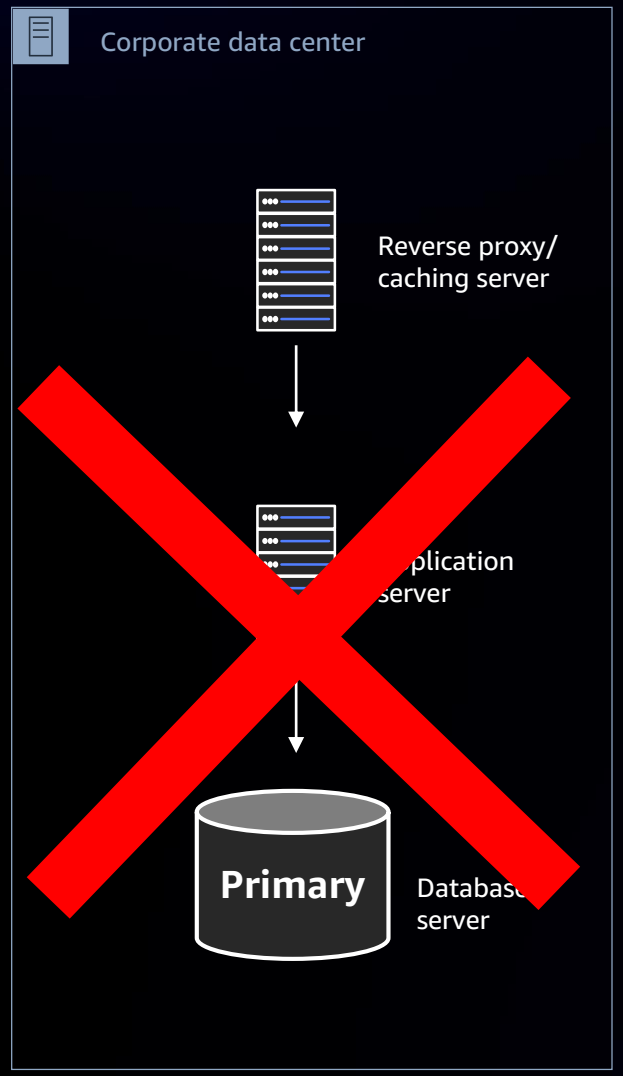
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

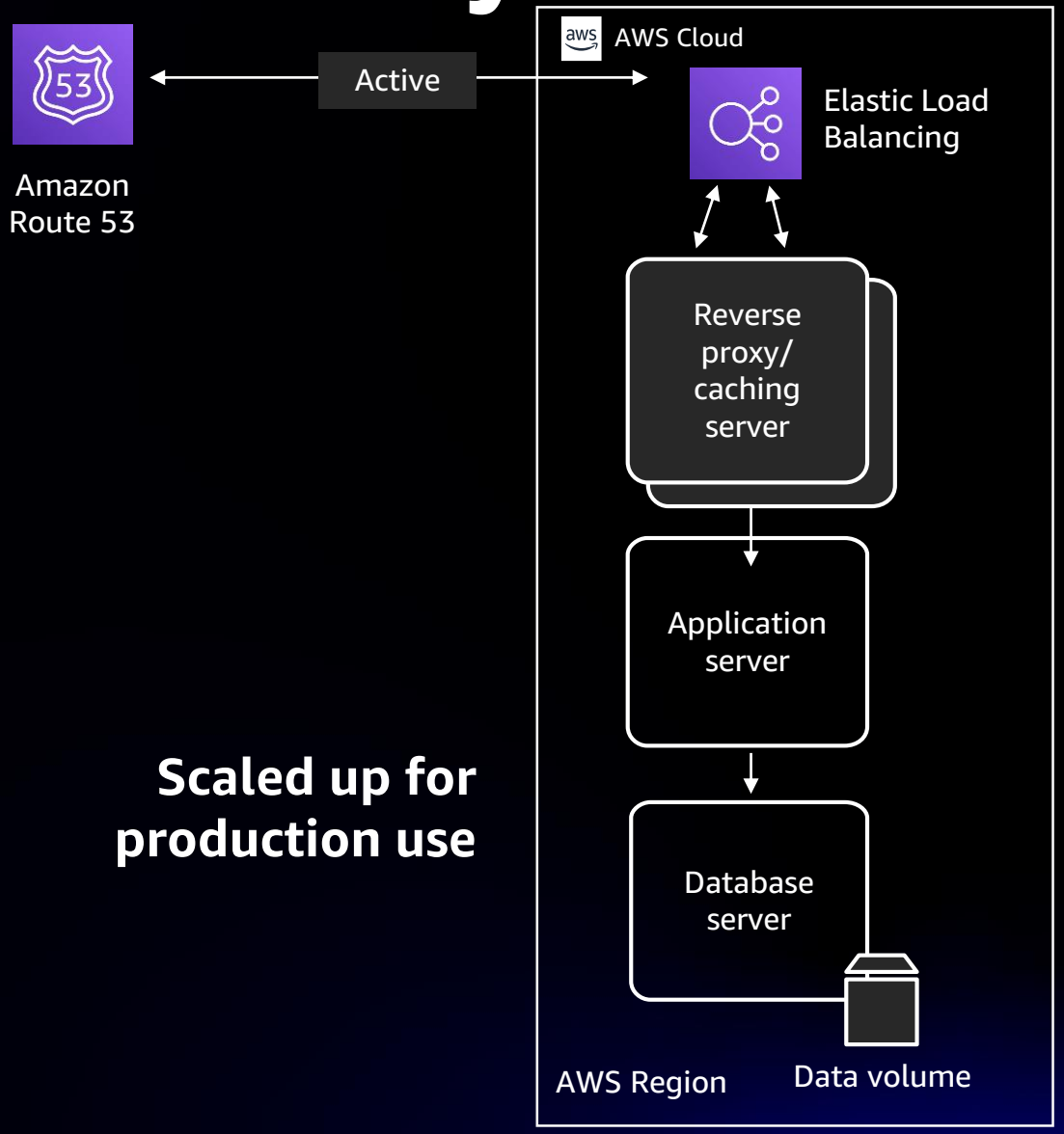
Multi-site active/active prep



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multi-site active/active recovery





Scaled up for production use

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Summary

Backup, restore, and archive

re:Invent sessions

ARC318: Designing a multi-account environment for disaster recovery

STG341: AWS Backup to protect cloud-native resources and hybrid environments

Ransomware recovery

re:Invent sessions

STG332: Data protection and recovery strategies from ransomware events

GPS212: Working with AWS Partners for anti-ransomware solutions

SEC308: Use AWS to improve your security posture against ransomware

Disaster recovery

re:Invent sessions

ARC202: Learn to build disaster recovery solutions for AWS workloads

ARC317: Best practices for disaster recovery of workloads on AWS

ARC316: Well-architected reliability: Best practices you can use now

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.