Backup and disaster recovery strategies for increased resilience

Nick Kniveton
Solutions Architect
Amazon Web Services

John Haghighi
Sr. Solutions Architect
Amazon Web Services

Agenda

01 Resilience on Amazon Web Services (AWS)

02 Backup and disaster recovery strategies

03 AWS Backup

04 Elastic Disaster Recovery service

Resilience

Ability of a workload to recover from infrastructure or service disruptions

The mental model

High availability

Resistance to common failures through design and operational mechanisms at a primary site

Core services, design goals to meet availability goals

Disaster recovery

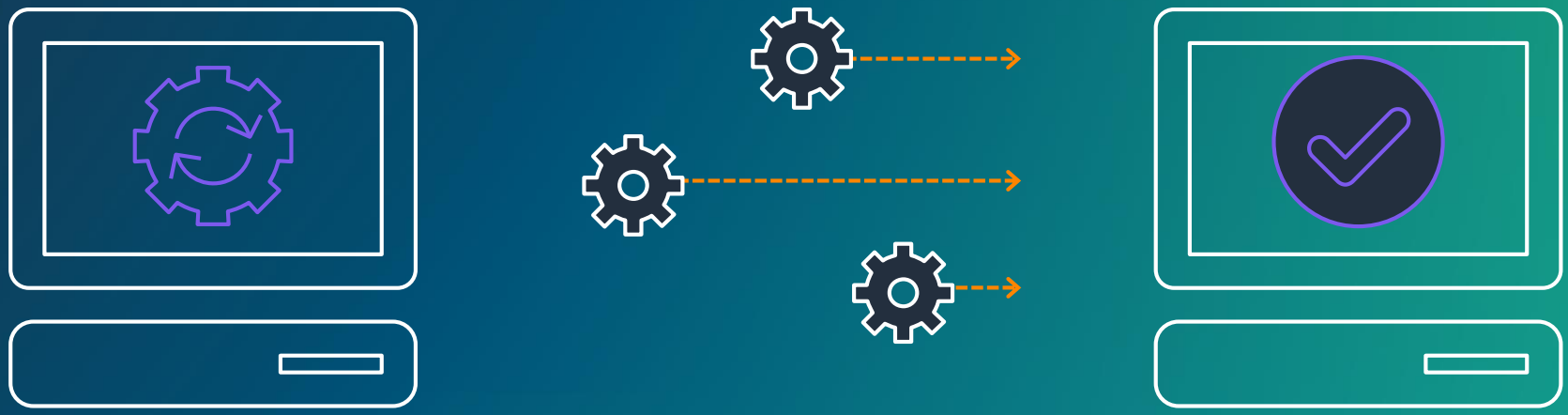
Returning to normal operation within specific targets at a recovery site for failures that cannot be handled by HA

Backup and recovery, data bunkering, managed recovery objectives

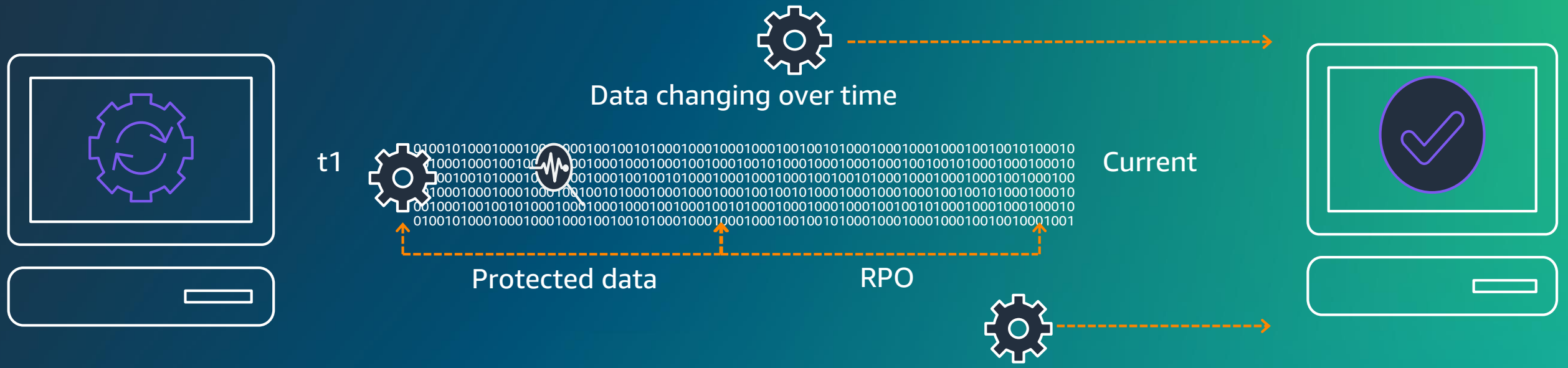
Continuous improvement

CI/CD, observability, moving beyond pre-deployment testing towards chaos engineering patterns

Why do we backup data?
Minimize time to recover



Why do we backup data?
Minimize data loss



Initial questions to answer

How important are the applications to your business?

What is the associated recovery point and time for these applications?

How are you storing the data?

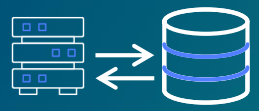
Where are you storing the data?

How are you restoring the application?

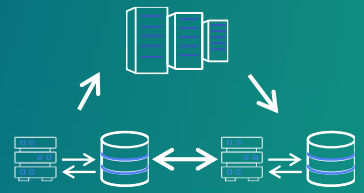
Categories of failure

Code deployments and configuration
e.g. bad deployment, cred expiration

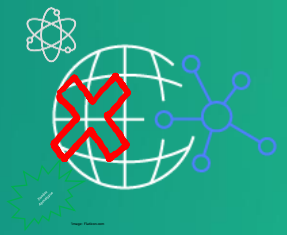
Core infrastructure
e.g. datacenter failure, host failure



Data and state
e.g. data corruption



Dependencies
e.g. infrastructure, external APIs



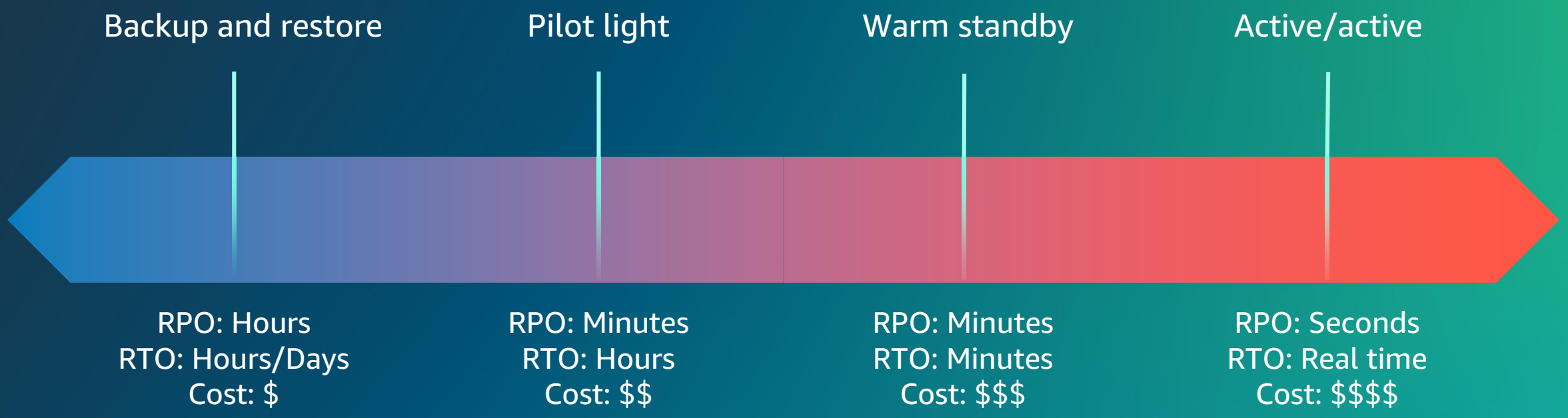
Highly unlikely scenarios
e.g. All of internet failure, environmental disasters,

Determining your recovery objectives: RPO and RTO

How much data can you afford to recreate or lose?

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

Data resilience options in the cloud



Apply the right protection for your resources

AWS Backup

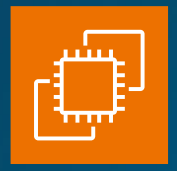
AWS Elastic Disaster Recovery

Amazon EBS

Amazon S3 & Amazon S3 Glacier

Amazon FSx

Amazon EFS



Amazon EC2

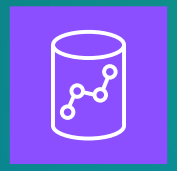
VMware Cloud on AWS

Anywhere to AWS

Amazon Aurora

Amazon DynamoDB

Amazon RDS



Amazon Redshift

AWS Backup: Centralize compliance, automate backup, and work across services

AWS Backup

1. Simplified backup scheduling and lifecycle management across AWS services
2. Centrally manage backup activities, security, and reporting
3. Achieve consistency and meet compliance requirements

Amazon EBS

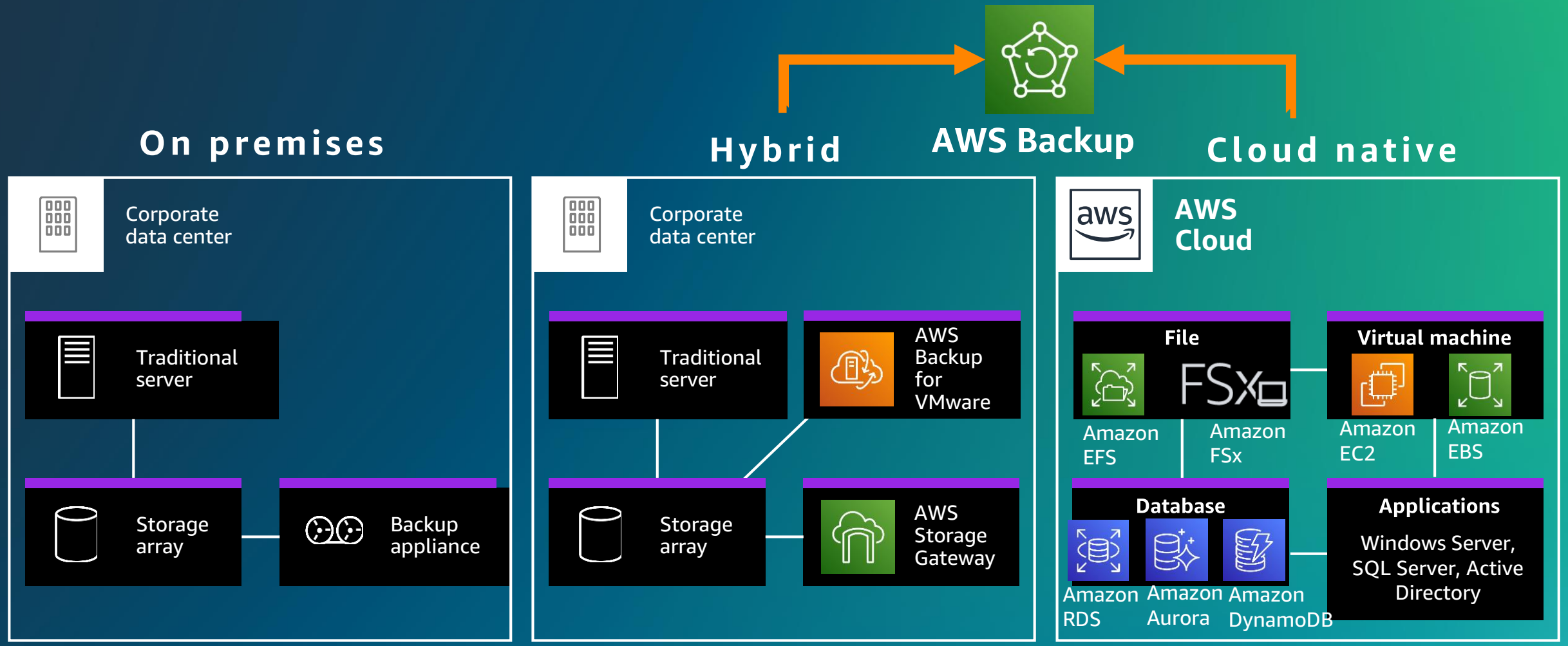
Amazon EFS

Amazon RDS

Amazon DynamoDB

AWS Storage Gateway

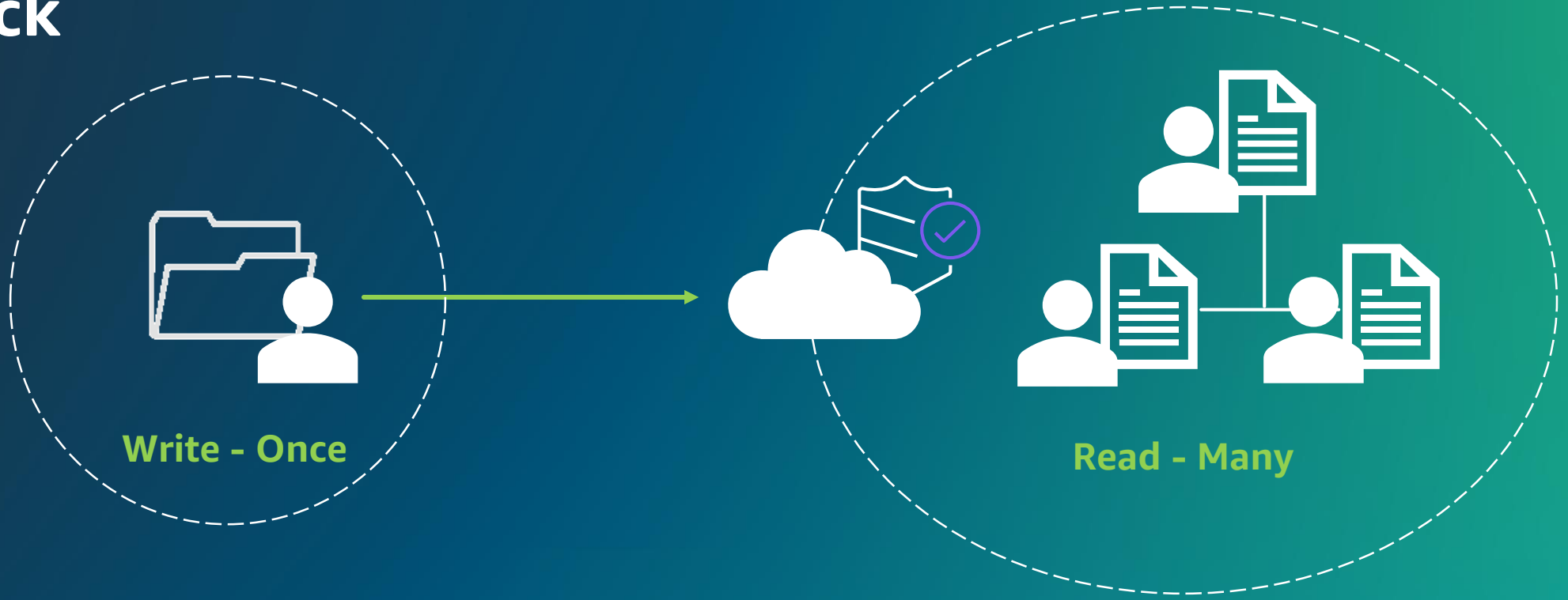
AWS Backup deployment patterns



Determining your backup policies

- Retention policy
- Backup frequency
- Cross-Region vs in-Region
- Object lock
- Accounts

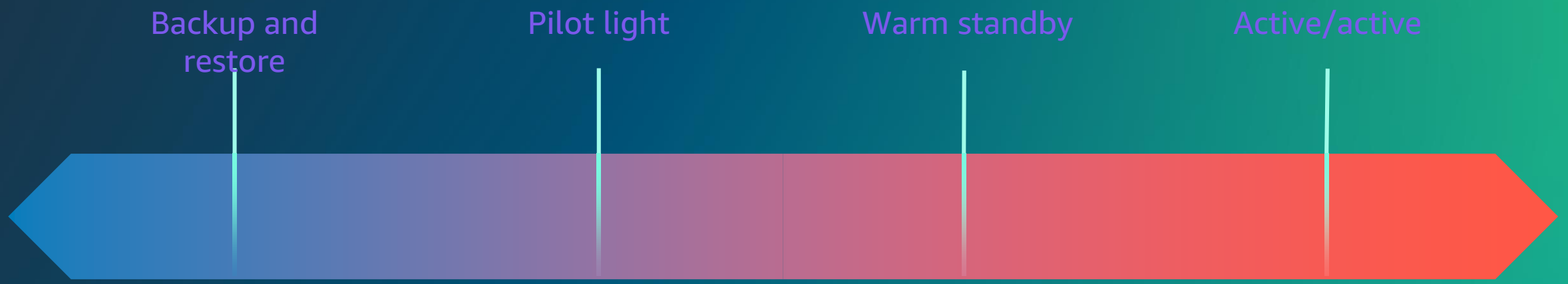
Protect against ransomware with Vault Lock



Besides regulatory compliance, you can use Vault Lock, a WORM design to protect your backups from getting overwritten

AWS Elastic Disaster Recovery

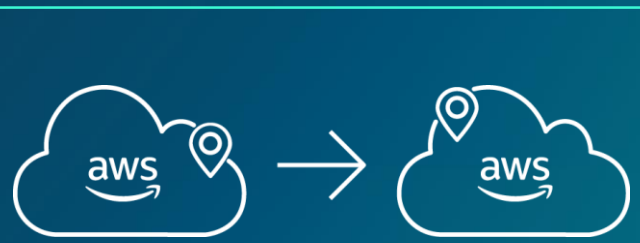
- Get the RPOs of active/active and the RTOs of warm standby at the cost of pilot light



AWS Elastic Disaster Recovery patterns

On premises to AWS

Other cloud to AWS



AWS Region to AWS Region

AWS Availability Zone to
AWS Availability Zone

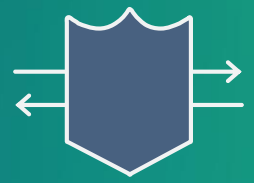
AWS Elastic Disaster Recovery key benefits

Faster recovery

Recovery time objectives (RTOs) of minutes

Lower costs

No need to pay for idle recovery site resources



Data protection

Recovery point objectives (RPOs) of seconds

Easy testing

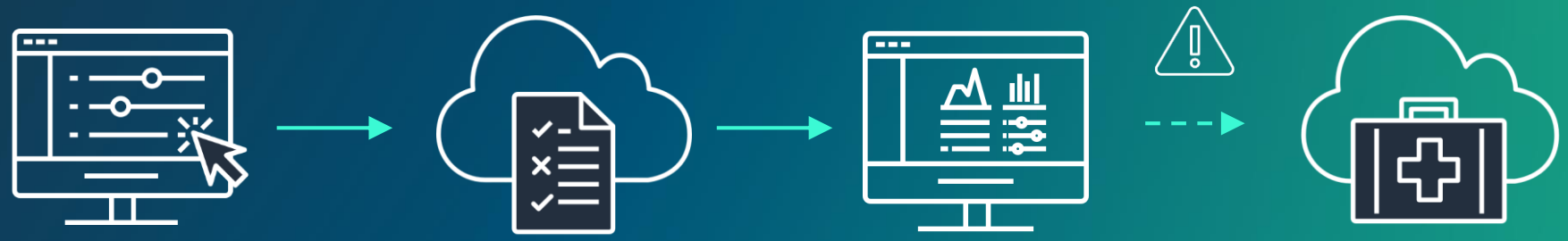
Conduct non-disruptive drills to verify readiness

Ransomware recovery

Launch unlocked and unencrypted versions of your applications

AWS Elastic Disaster Recovery lifecycle

Use a single process to recover applications across all supported infrastructure and OS



Set up
Define settings and initiate continuous data replication

Test
Launch instances for non-disruptive tests

Operate
Maintain readiness with monitoring and periodic drills

Failover
Launch recovery instances on AWS within minutes

Failback
Initiate replication and return to primary site

Ransomware mitigation – Low RPO

Use AWS Elastic Disaster Recovery for ransomware protection, detection, response, and recovery

Account isolation

Protect your workloads by isolating your staging account from your production and recovery accounts

Immutable snapshots

Keep your data safe with immutable snapshots that can’t be altered or overwritten

Endpoint detection and response (EDR)

Detect and eliminate threats using integrated solutions from AWS Partners

Point-in-time recovery

Recover your servers by using unlocked and unencrypted point-in-time snapshots

Please provide your feedback

Step 1: Select: **Security, governance, and resilience**
Step 2: Select: **Backup and disaster recovery strategies for increased resilience**