WARSAW | 06 MAY 2026

AWS SUMMIT

STG401

Building resilience against ransomware using AWS Backup

Dragos Madarasan

Solutions Architect Manager

AWS

Adrian Bere

Senior Solutions Architect

AWS

Before we begin

400

This is a 400-level session, not entry level, but expert

We'll let you know when a buildout is complete for photos

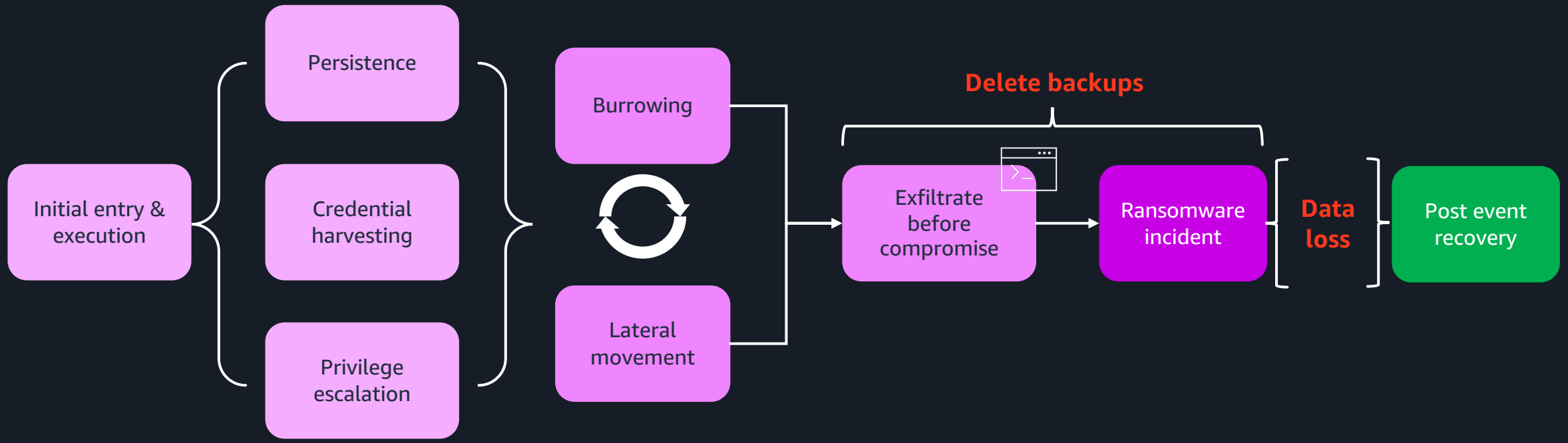
The key to cyber resilience is to have a robust plan in place to **recover quickly** and minimize the impact of any cyber events.

Agenda

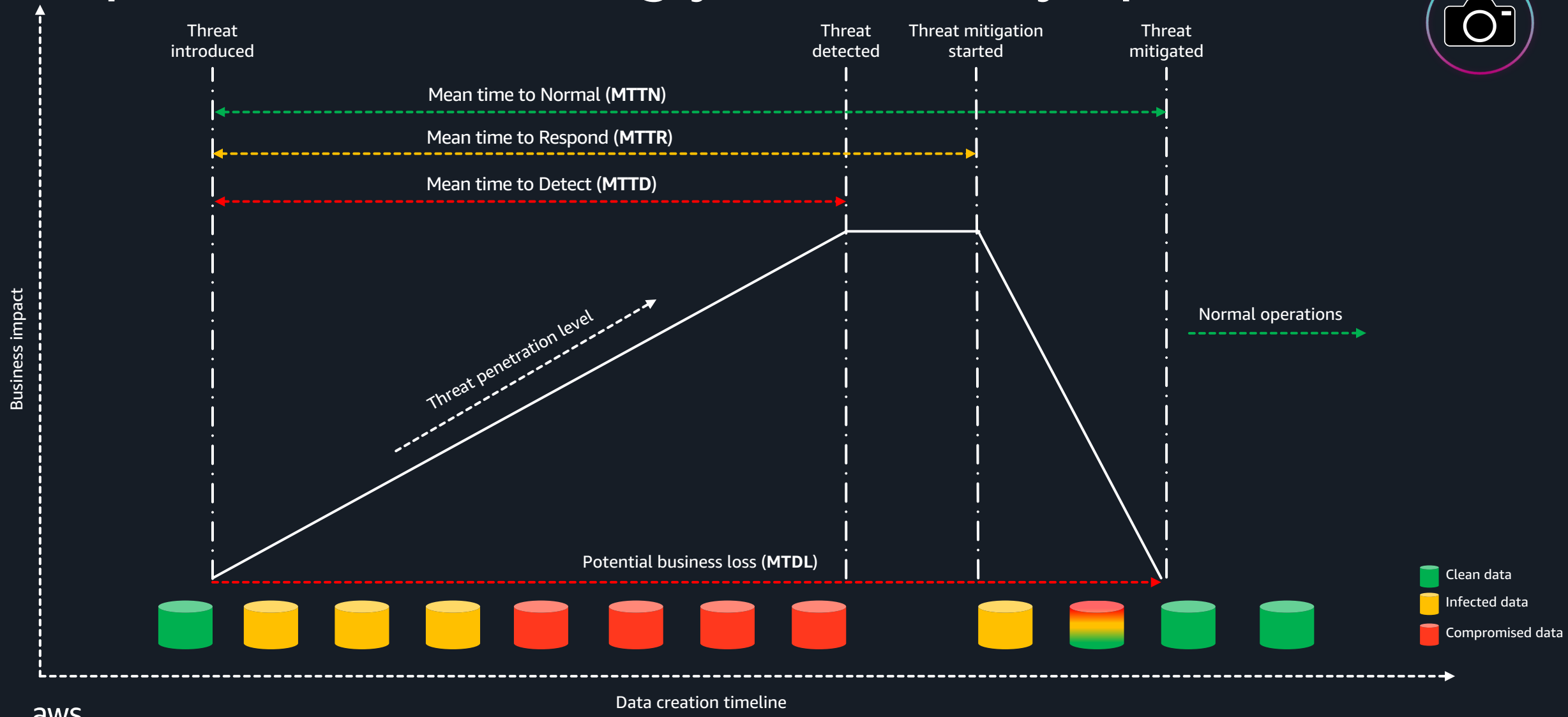
- The cyber threat landscape
- The role of backups in risk mitigation
- Building a resilient recovery strategy
- Reference Architecture
- Implementing effective recovery mechanisms
- Summary

The cyber threat landscape

Anatomy of a cyber attack



Importance of securing your recovery options



Key ransomware threats and trends

- Persistent threat landscape
- Organizational alignment challenges
- Comprehensive financial impact
- Backup systems targeted
- Evolving regulatory landscape

Heightened scrutiny for cyber resilience

NIS2 | **GDPR** | **CER**

Global focus

DORA | NYDFS | FINRA | MAS | FCA | JFSA | HKMA | SARB | APRA | GxP | HIPAA

Industry and country focused

Standards, guidelines, and best practices

(NIST CSF 2.0, HITRUST, PCI DSS, ISO 27001, SOC2, CMORG, MITRE ATT&CK, Essential 8)

Support mechanisms

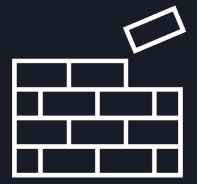
Regulators are now mandating cyber resilience and data protection as
essential business functions, not just IT concerns {even impacting SMBs and Startups}

The role of backups in risk mitigation

Threat Modelling for Recovery Resilience

What are we working on?

What can go wrong?



What are we going to do about it?

Did we do a good enough job?

Threat Model

Common Threat Vectors

A **threat vector**, also known as an **attack vector**, is a method that malicious actors can use to compromise the recoverability of a system or service which relies on data backups.

Some recovery challenges based on common threat vectors include

- Seamless recovery into a clean account
- Verifying the integrity of backup data
- Accessing data in the event of a breached cryptographic key
- Complying with regulatory recovery validation requirements

Strategies for Securing your Backups

3 different copies of the data including the source

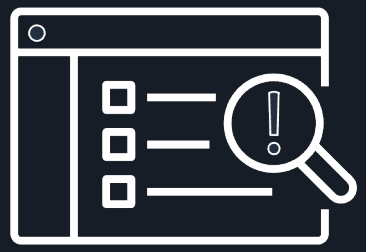
2 of these backups stored on different accounts

1 of these backups stored across regional boundaries

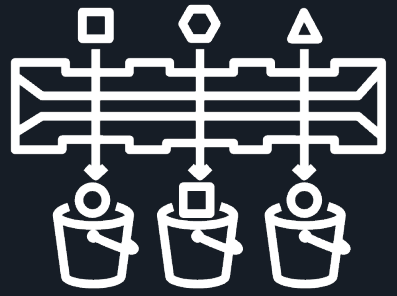
1 of the backup copies stored in an immutable vault

0 errors after automated backup and recoverability verification

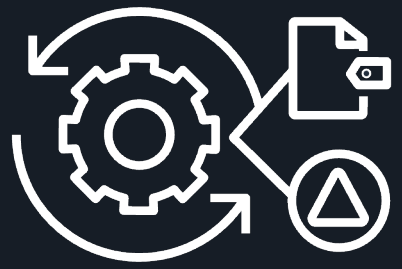
Starting Points



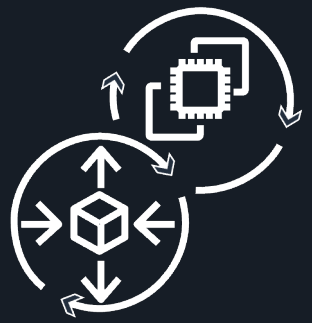
What needs to be vaulted



How will vaults be partitioned



Management of the Data Vault

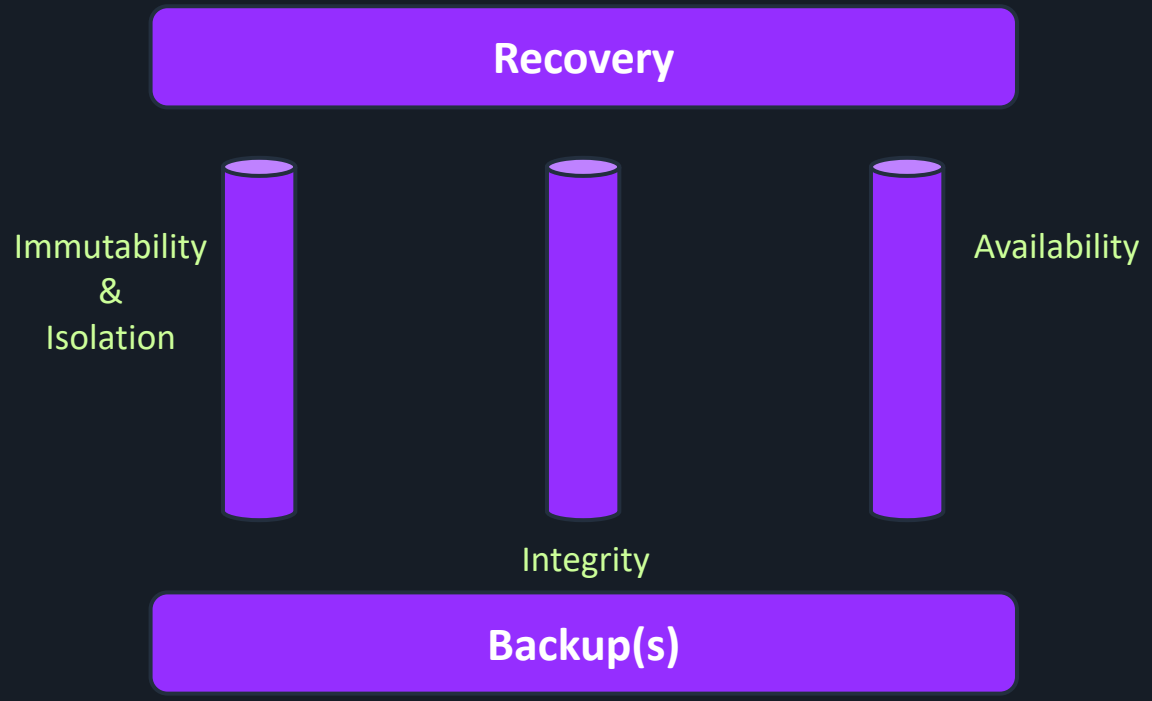


What does recovery look like

Building a resilient recovery strategy

Laying the foundation for a reliable recovery

- **Immutability & Isolation** : Ensure backups cannot be inadvertently or maliciously altered or deleted
- **Integrity** : Guarantee backups are complete and consistent
- **Availability** : Backups must be readily accessible and restorable



Backups are only good as their recoverability – ability to restore operational capability is the end objective

AWS Backup

AWS Backup is a fully managed service that centralizes and automates data protection across AWS services and hybrid workloads.

- Policy based data protection
- Search and item-level recovery
- Logically air-gapped vaults
- Restore testing
- Malware scanning
- Backup Audit Manager

Compute

- Amazon EC2

Containers

- Amazon EKS

Block Storage

- Amazon EBS

Object Storage

- Amazon S3

File storage

- Amazon FSx for NetApp ONTAP
- Amazon FSx for OpenZFS
- Amazon EFS
- Amazon FSx for Windows File Server
- Amazon FSx for Lustre

Databases

- Amazon Redshift
- Amazon Timestream
- Amazon DynamoDB
- Amazon Aurora
- Amazon Aurora DSQL
- Amazon Neptune
- Amazon RDS
- Amazon DocumentDB

Management

- AWS CloudFormation

Application

- Windows Volume Shadow Copy Service on Amazon EC2
- SAP Hana on Amazon EC2

Hybrid

- AWS Storage Gateway + vmware
- Hybrid

Importance of Isolation and Immutability

Ransomware actors target backup systems with the same vigor as production systems

A compromised credential can impact both production and backup if authentication boundaries are shared

Without immutability, threat actors can encrypt production data AND delete your recovery path

AWS Backup - Logically air-gapped vault

AWS Backup logically air-gapped vault, is a type of AWS Backup Vault that allows secure sharing of backups across accounts and organizations, supporting direct restore to help reduce recovery time from a data loss event.

Immutable by default

Compliance mode Vault Lock applied with Guardrails at creation.

Simplified Cross-account sharing

Flexible recovery or forensics with cross-account/cross organization sharing support with AWS Resource Access Manager (RAM) or **Multi-party Approval**.

Data isolation

Enhanced protection AWS Backup Service Owned KMS Key (with optional support for customer owned keys) to protect against KMS Key compromises.

Faster Restore Experience

Reduce time to recover with direct restores across accounts.

Importance of Integrity

Backups infected with malware are worse than no backups—they propagate the attack

Without integrity validation, you discover backup corruption during recovery (when it's too late)

Compliance and regulatory frameworks require proof of backup viability

AWS Backup Restore testing

AWS Backup Restore Testing (RT) can assess recoverability of business data against data loss events and prove the recovery posture for compliance using custom defined Restore Testing plans.

Setup restore testing plans to schedule test restores, and automatically clean-up all tested resources

Assess recoverability of business data against data loss events

Report on recovery readiness to meet compliance and audit requirements

Integration with custom built or partner solutions to extend validation

Importance of Availability

During a ransomware event, every minute of downtime costs money and reputation

Backups locked behind compromised credentials become unavailable at the moment of greatest need

Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are meaningless without guaranteed availability

Multi-party approval

Multi-party approval enables customers to guard critical operations with a distributed review process

Protect your AWS critical operations with approval of multiple people

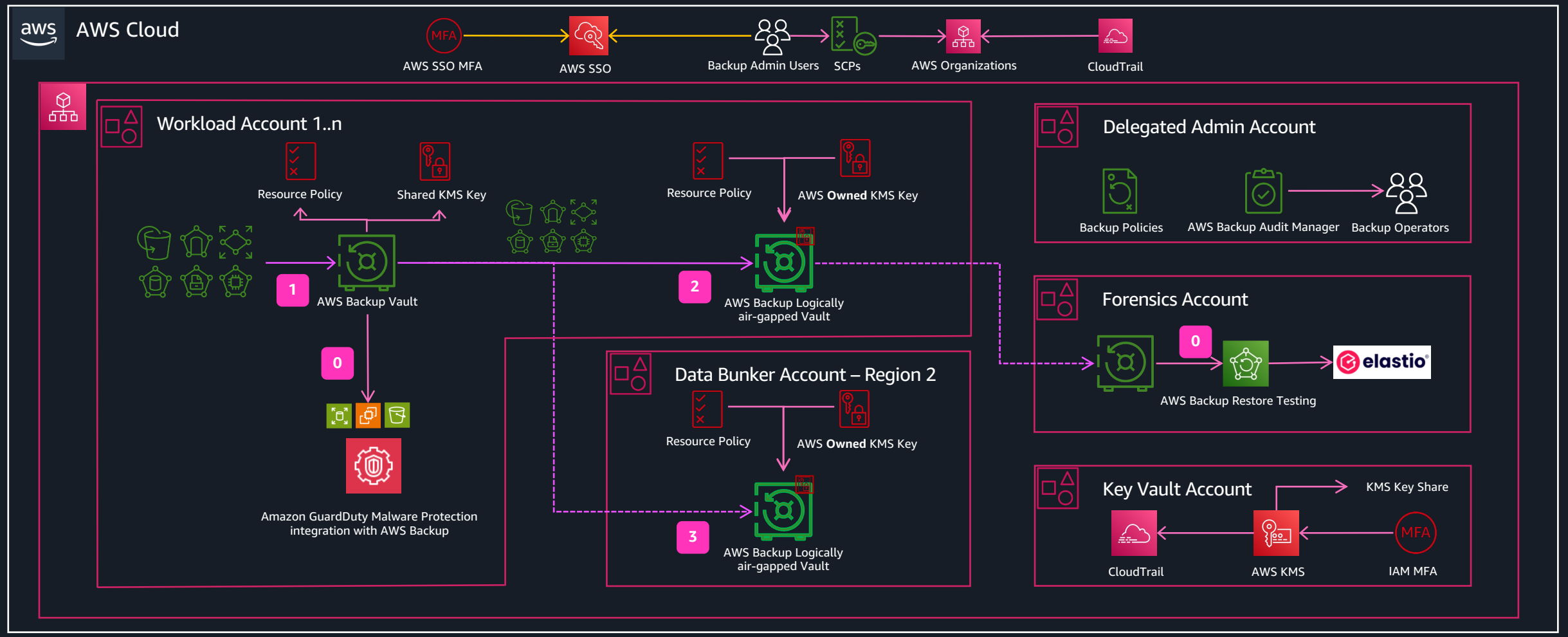
Additional layer of security for your AWS operations

Centralize and standardize approval workflows

Maintain clear **audit trails** for compliance

Reference Architecture

AWS Backup reference architecture



Backup Flow

Settings Flow

Authentication Flow

1 First Copy - Local

2 Second Copy – Vault – Same Region

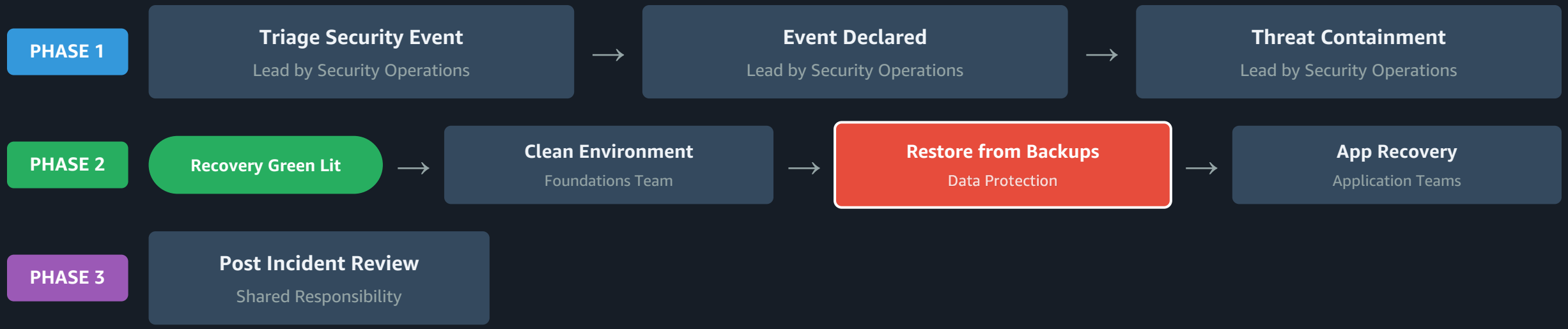
3 Third Copy – Vault – Second Region

0 Forensics and Recovery Validation(s)

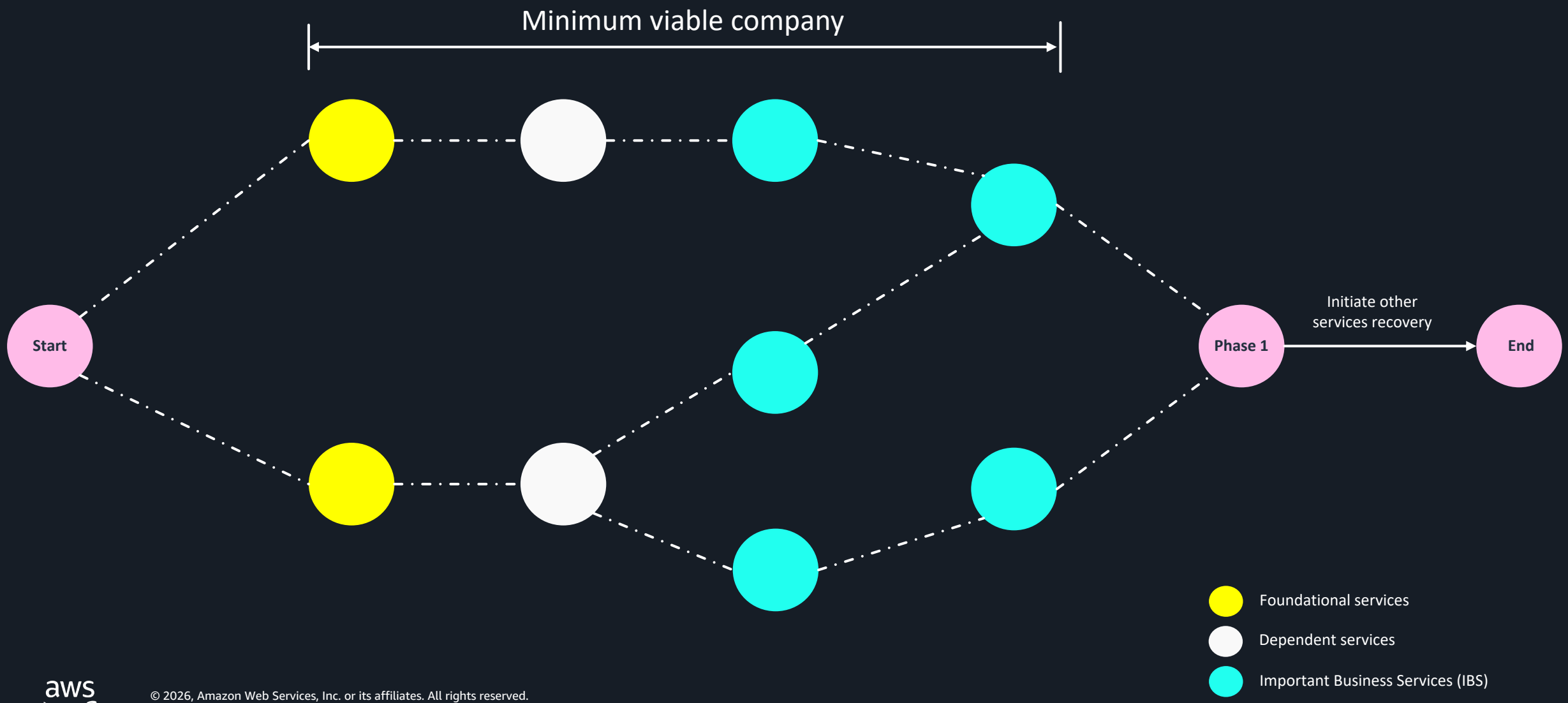
Implementing effective recovery mechanisms

Data recovery from a ransomware event

A successful ransomware recovery hinges on a well-defined and practiced plan that outlines the procedures and resources required to restore your systems and data after a cyber event



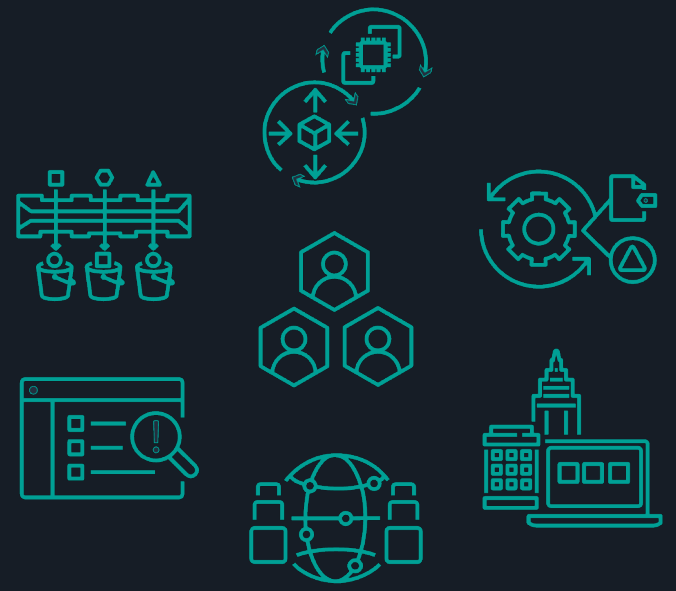
Important recovery concepts



Summary

Summary for building cyber event resilience

- Recovery is becoming a focus area
- Detection often relies on a critical mass
- Backups are targets and require testing
- Threat modelling helps to focus activity
- Operational resilience is not cyber resilience
- Cyber resilience is a business problem



Thank you

Please complete the session survey