
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

STG305-R

Data protection & application recovery strategies for ransomware events

Fathima Kamal

Principal Storage SA
AWS

Vivek Mishra

Sr. Product Manager – AWS Data Protection
AWS

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

Agenda

01 Ransomware threats

02 AWS ransomware protection & recovery

03 Whiteboarding

04 Q&A session

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

What is ransomware?

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



Locker ransomware

Does not encrypt files, instead attackers lock the victims out of their devices and prevent them from having access; criminals then demand a ransom to unlock the device



Crypto ransomware

Prevents users from accessing important files by encrypting their data; attackers make money by demanding that victims pay a ransom to get their files back, normally through cryptocurrency-based transactions

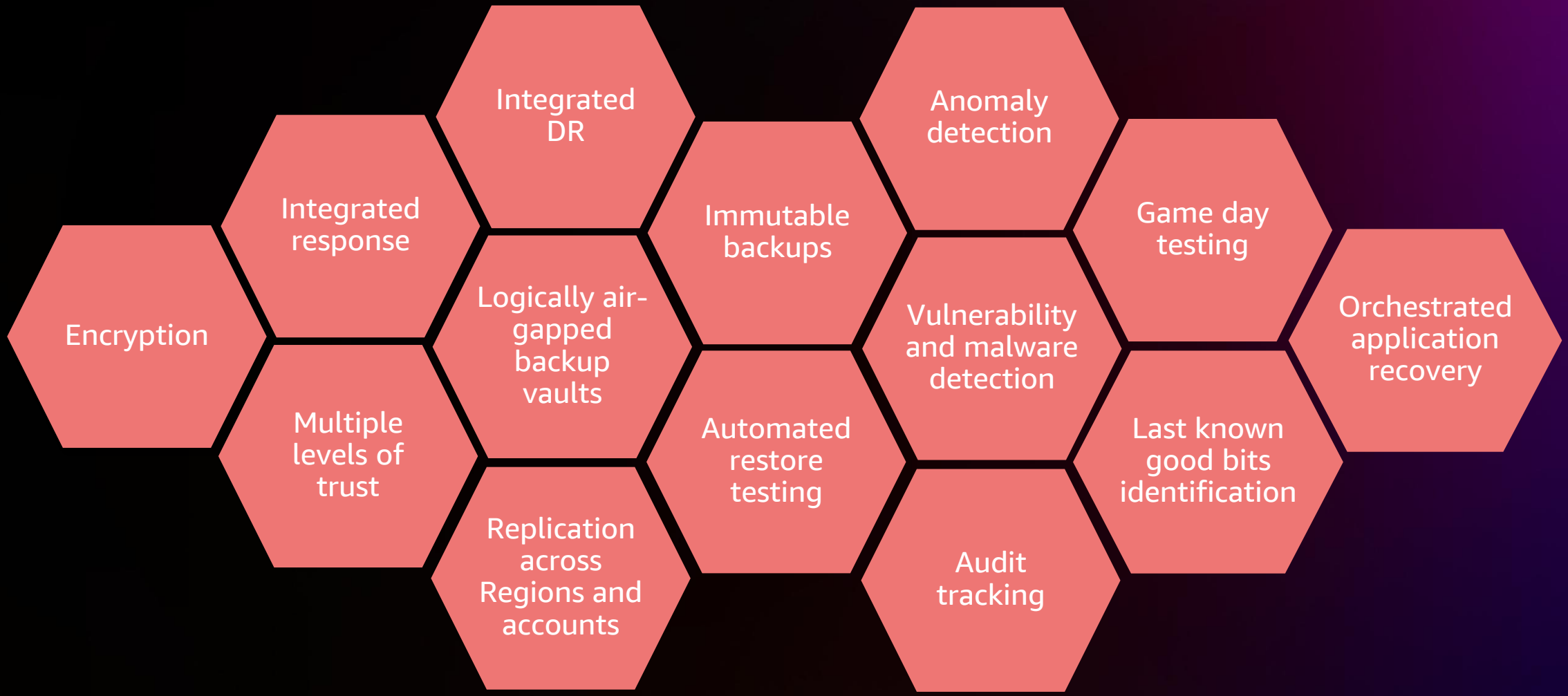
Why are they so effective? Think people, process, and technology

aws

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

Ransomware protection and recovery

Automation of a defense-in-depth approach

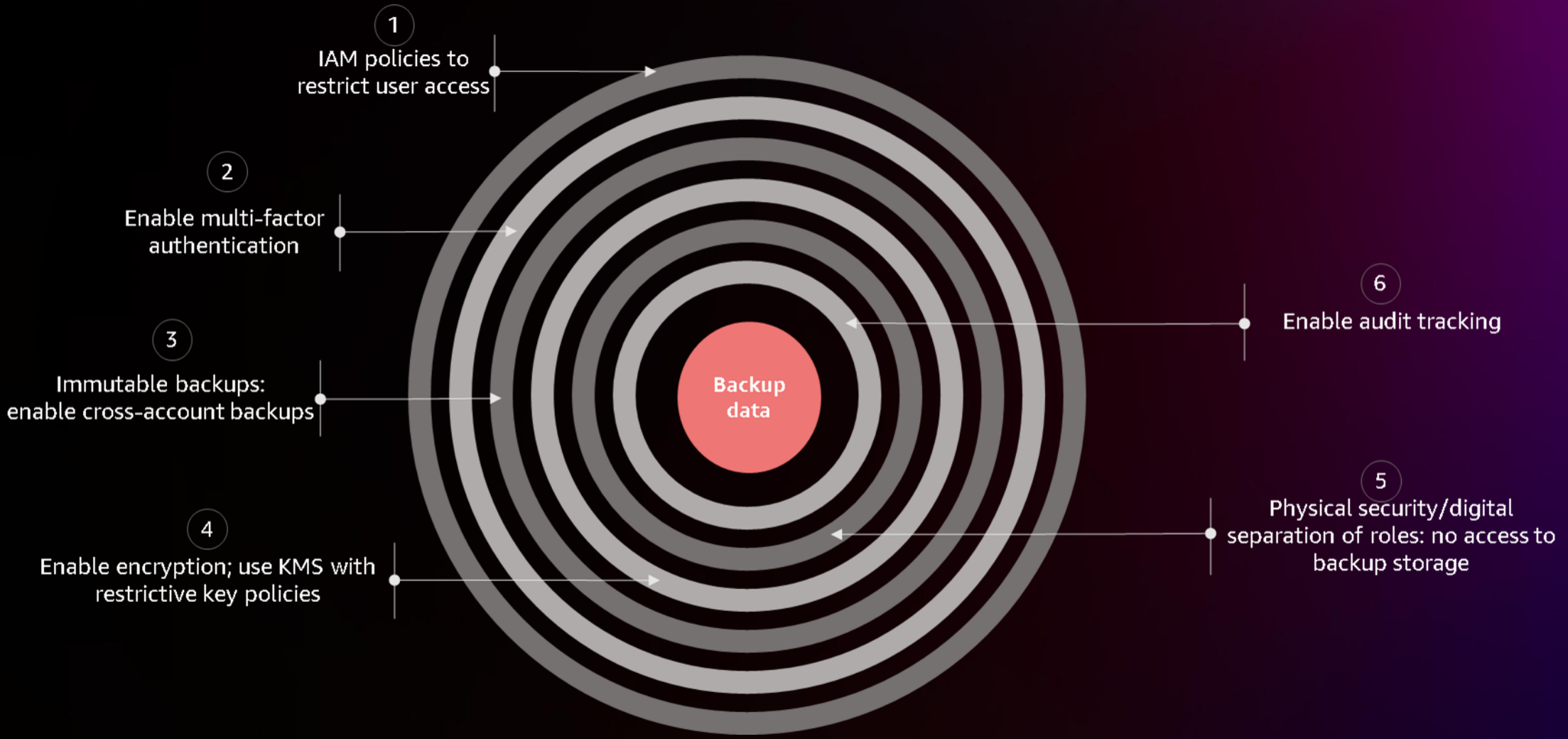


aws

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

AWS multi-layer security

PROTECT DATA WITH MULTIPLE LAYERS OF SECURITY



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

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 and hybrid workloads

Compute
- VMware Cloud on AWS
- Amazon EC2

Block storage
- Amazon EBS

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 DynamoDB
- Amazon Aurora
- Amazon Neptune
- Amazon RDS
- Amazon DocumentDB

Object storage
- Amazon S3

Data transfer
- AWS Storage Gateway

Hybrid workloads
- AWS Storage Gateway
- +
- VMware

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

AWS Backup enables you to create an immutable copy of your data

AWS Backup Vault Lock features and capabilities – write once, read many (WORM)

Control plane security
Isolated from all other customer AWS accounts (entirely segregated entity)

Vault model scalability
The AWS Vault solution allows the creation of multiple dedicated vaults

Data plane security – ingress data flow
Vaulted data is always pulled into the vault and never pushed by an external entity

Protecting data with AWS Backup Vault Lock



AWS Backup **vault**

AWS Backup Vault Lock – WORM Compatibility
Meets write-once, read-many (WORM) requirements for electronically stored information (ESI)

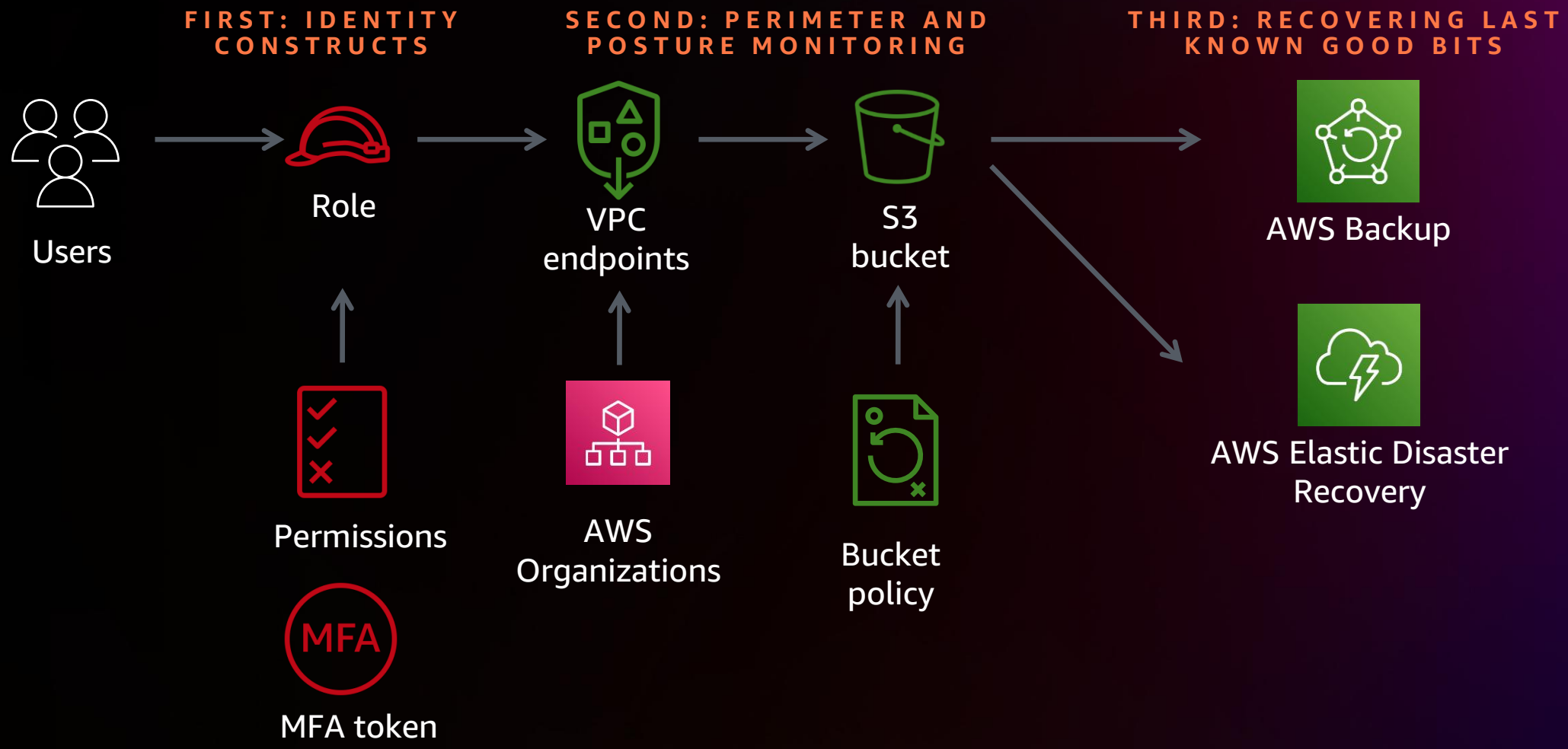
Data immutability – data retention
The capability for vaulted data artifacts to be immutably stored and subject to bounded or unbounded retention periods

Vault performance
Highly performant vault that caters to elastic needs of data protection

Audit and compliance
Best security, compliance, vault monitoring, and audit capability

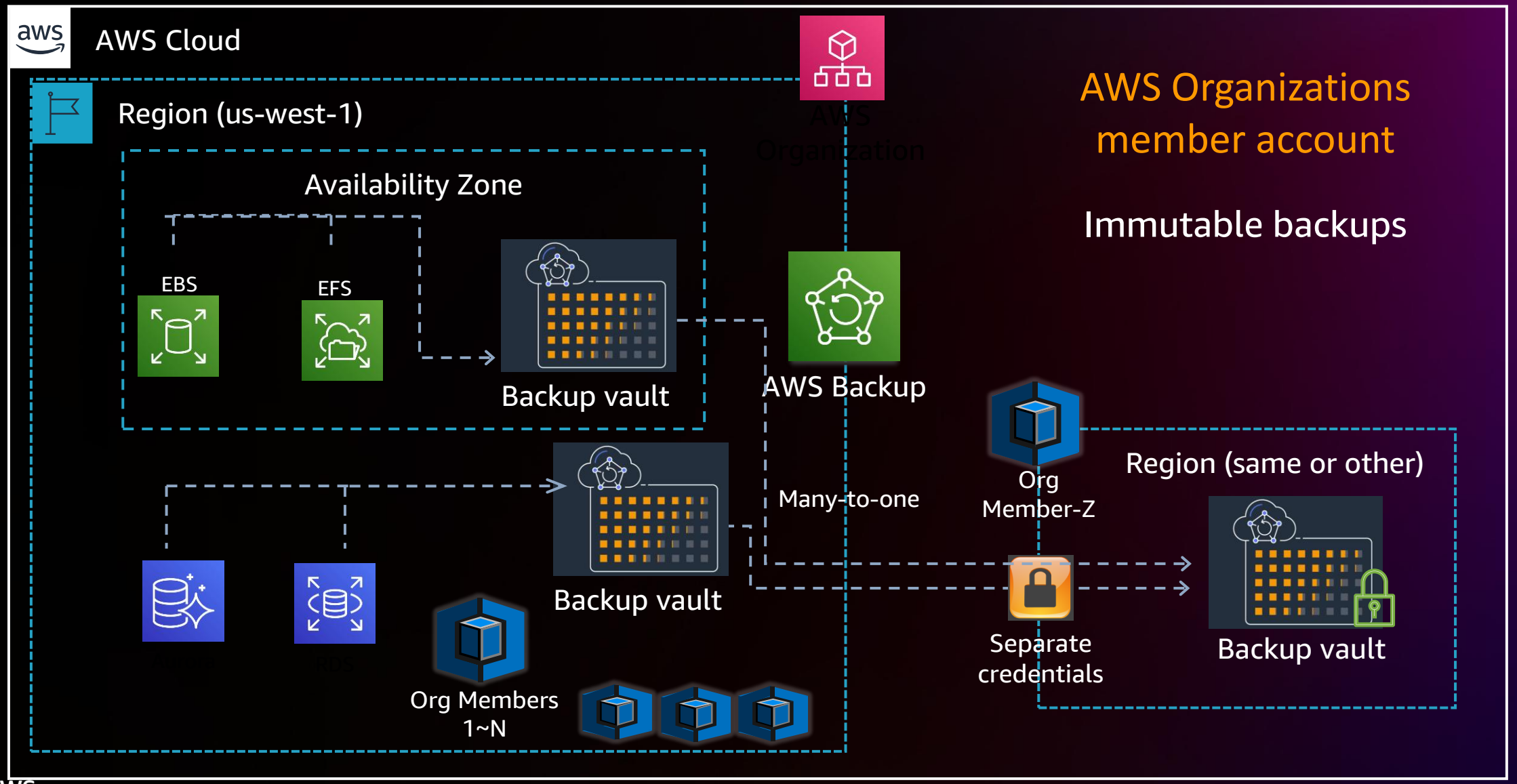
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Implement multiple levels of protection



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

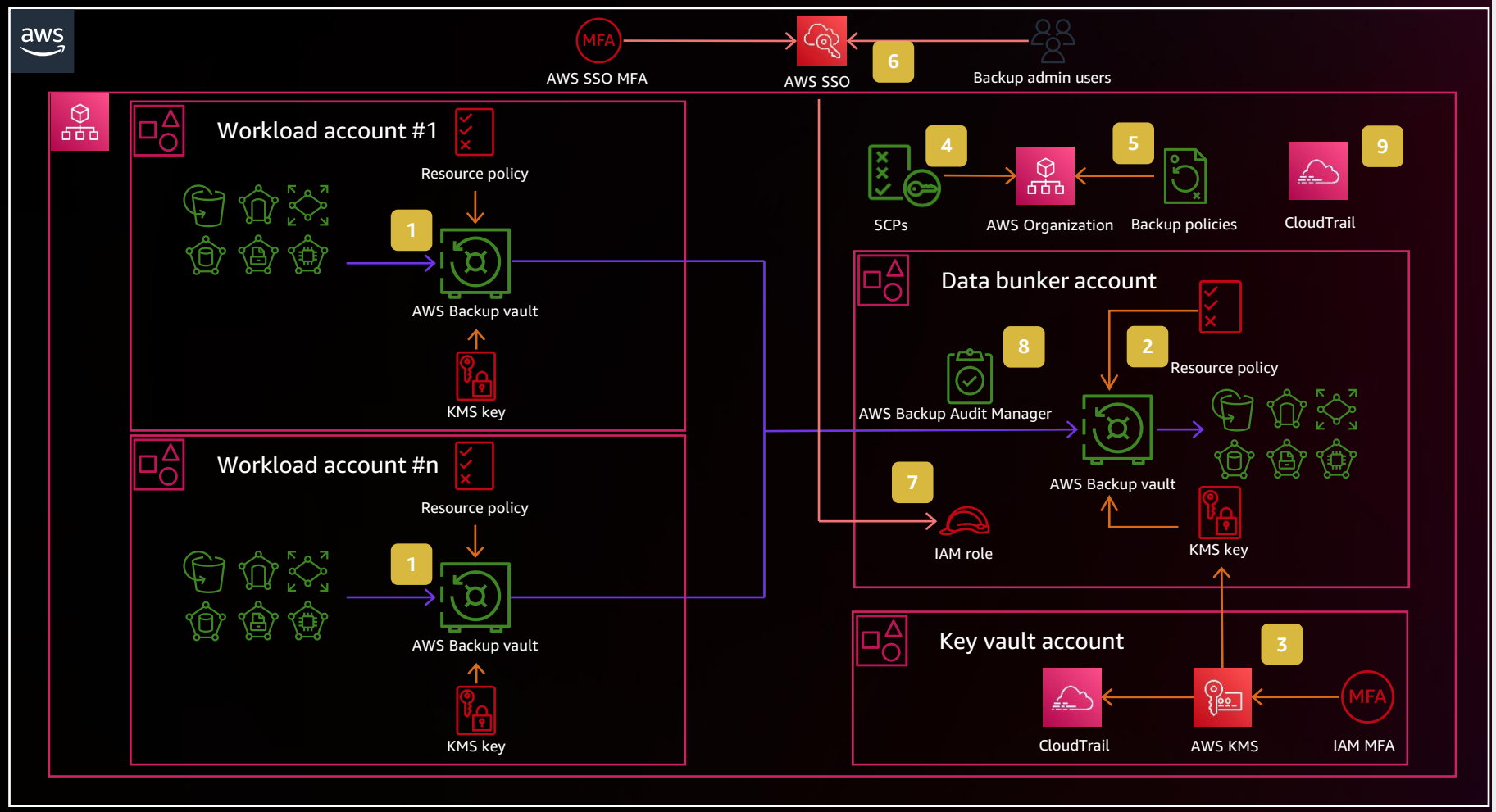
Cross-account/cross-Region backups



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

Centralized AWS Backup data bunker

This architecture details the key steps involved in setting up a central immutable backup data bunker that follows the principles of least privileges in a multi-account AWS Organization



1. Create a **resource policy** that limits *CopyFromBackupVault* to the backup data bunker account and apply to the **AWS Backup vault**(s) in each member account. Create customer managed KMS key and apply to the AWS Backup vault(s) in each member account.

2. Set up a backup data bunker account and create an **AWS Backup vault** and set up **Vault Lock** to it. Create a resource policy that limits *CopyIntoBackupVault* actions from specific organizational units (OUs) or accounts and apply to this AWS Backup vault.

3. Create a **customer managed KMS key** in a separate key vault account and share the KMS key to the central vault account. Implement additional security controls including MFA on critical KMS API calls like **ScheduleKeyDeletion**.

4. Create a **service control policy** that restricts access to the appropriate IAM roles to create backups to create boundaries on the copy operations into the backup data bunker account and apply to the member accounts.

5. Create an AWS Backup policy with a copy operation into the backup data bunker account applied to the member accounts.

6. Restrict the access to the backup data bunker account to specific userbase via **AWS SSO and MFA** that will follow a break-glass workflow.

7. The authenticated user is granted AWS **STS** temporary credentials through federation with specific access to the backup data bunker.

8. Create audit reporting using **AWS Backup Audit Manager (BAM)**.

9. Create an Organizational **CloudTrail** for recording and monitoring of policy changes and central backup vault access patterns.

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

AWS Partner Network



























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

This is not a complete list. To view all AWS Partners for this category, visit AWS Partner Solutions Finder. This list of partners is current as of July 2022.

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

Call to action



Learn

aws.amazon.com/security
aws.amazon.com/backup

- Ransomware protection
- Product information
- Product documentation



Execute

aws.amazon.com/console

- Create a backup plan
- Start protecting your critical AWS workloads
- Create compliance reports



Get help

forums.aws.amazon.com

- Community help
- Your AWS account team
- AWS Support

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

Thank you!

Fathima Kamal
fkamal@amazon.com
@fathimakg

Vivek Mishra
vivekmsh@amazon.com
@mishra_vivek



Please complete the session survey in the **mobile app**

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