



PUBLIC SECTOR SYMPOSIUM

BRUSSELS | MARCH 28, 2023

BAT301

Keep your AWS environment safe from Ransomware attacks

Laura Verghote (she/her)

Solutions Architect

AWS

Rotem Agmon (he/him)

Solutions Architect

AWS



Agenda

- Evolution of Ransomware
- 7 best practices for Ransomware Protection
- AWS Backup - Deep dive
- AWS Backup - Demo

“75% of IT organisation will face one or more ransomware threats by 2025.”

Gartner, “[Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware](#)”

“Hackers are locking people out of their networks and demanding big payments to get back in. New data shows just how common and damaging the attacks have become.”

[The New York Times](#)

Scripps enters fourth week of ransomware attack

[The San Diego Union-Tribune](#)

DHS to issue first cybersecurity regulations for pipelines after Colonial hack

“Two directives will seek oversight of the industry after ransomware attack upended gas availability in the Southeast for 11 days”

[The Washington Post](#)

Ransomware attack on Bose exposes employee SSNs and financial information

“The company was forced to notify New Hampshire officials after employees in the state had their information accessed”

[ZDNet](#)

**Who here has experience
preventing or responding to
ransomware?**

Evolution of Ransomware



What is ransomware?



Wide range of technologies that unauthorized users use to extort money from entities

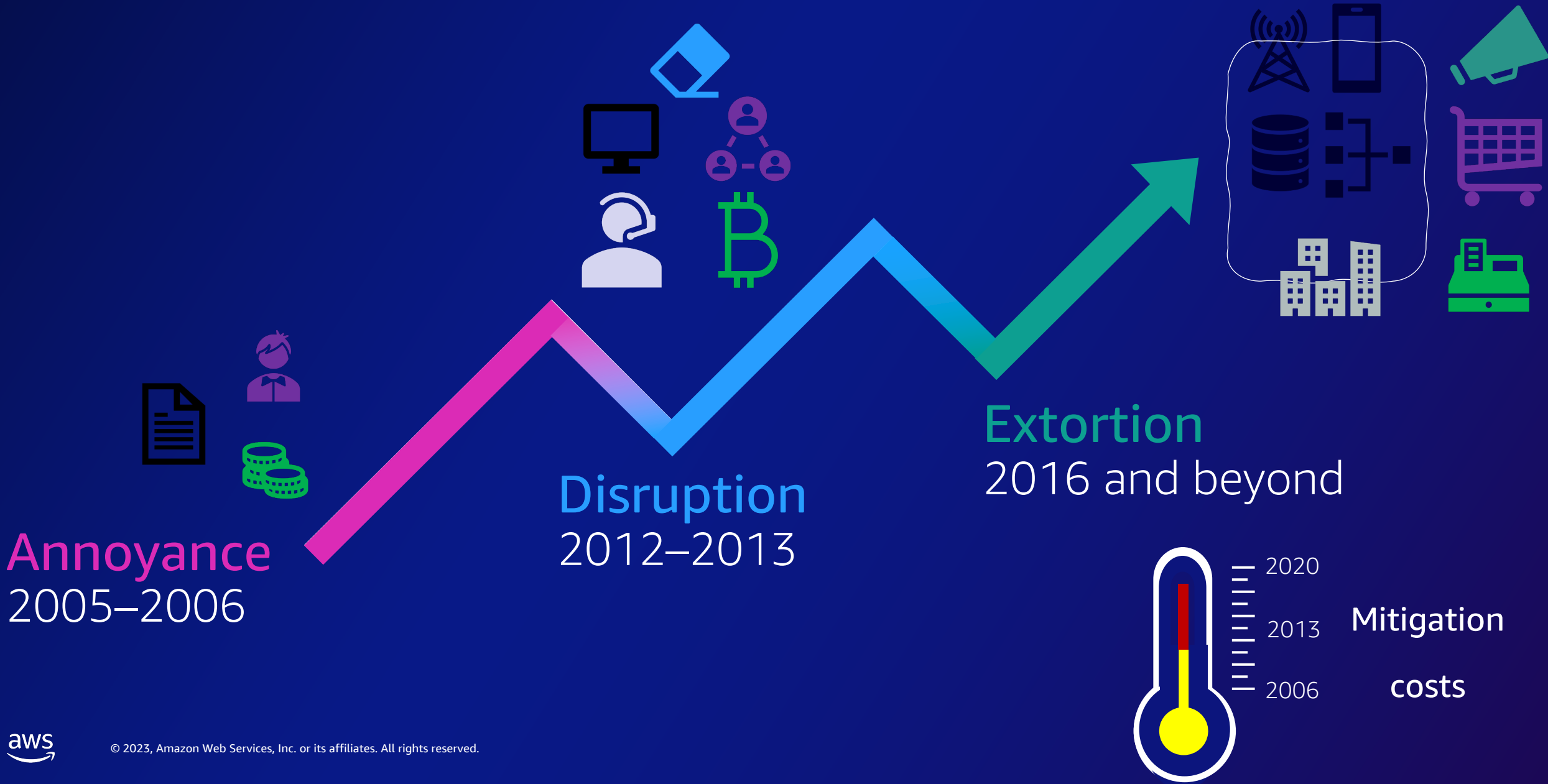


Unauthorized users use system vulnerabilities to access data and then restrict the rightful owner from accessing it



Unauthorized user **encrypts** data using actor-controlled encryption keys
OR uses access controls to **lock out** the rightful owner from a system
Unauthorized users may threaten to **reveal data or acts of exfiltration.**

Evolution of ransomware



Evolution taught us a few key lessons



Early detection is the key



Prevention is better than cure

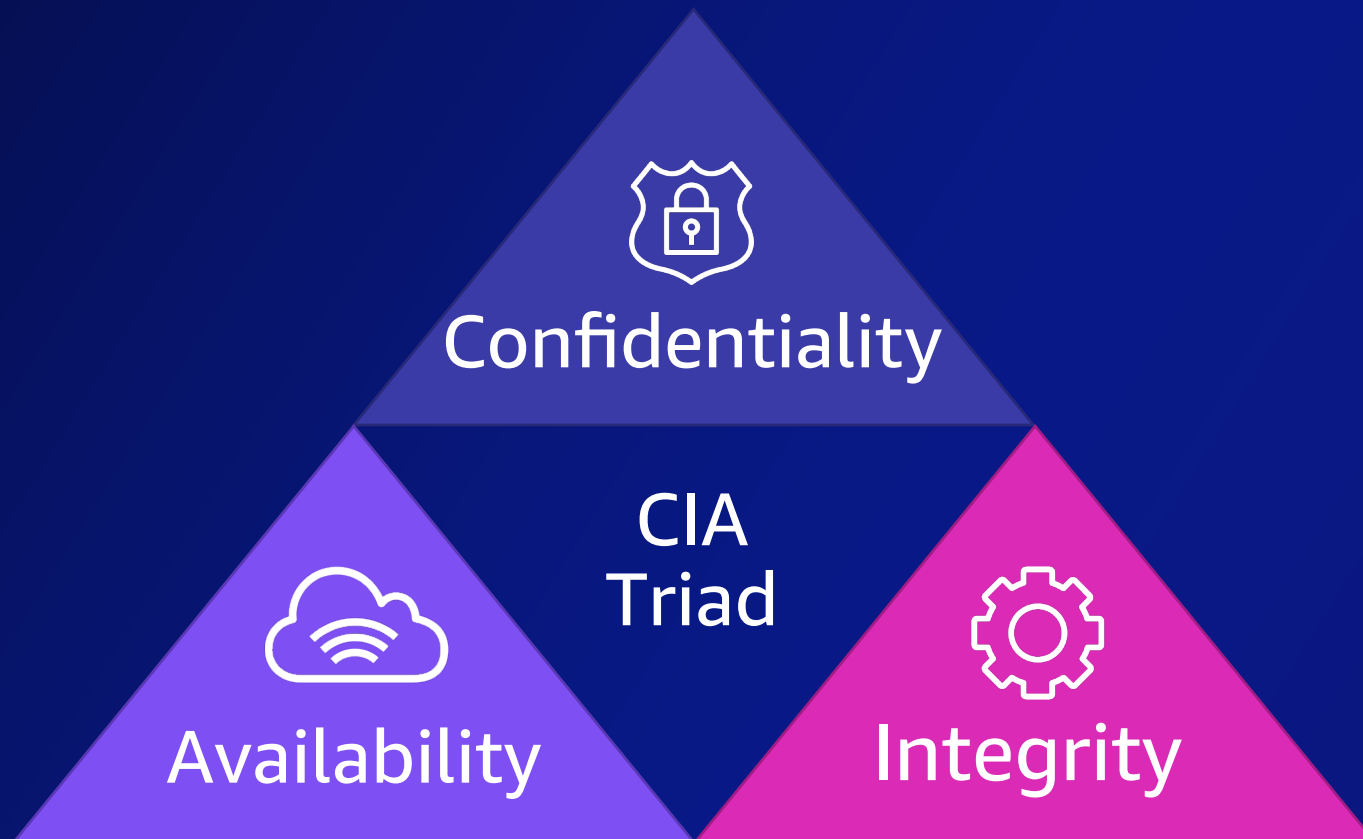


Automate assessments, recovery and response



Education and training become more important

Modern Ransomware targets the C, I & A of your data



Confidentiality

Leaking of stolen data

Integrity

Irreversible encryption of data

Availability

Downtime of mission critical services

7 best practices for Ransomware Protection



1. Use a security Framework



1. Use a security Framework

NIST Cyber Security Framework

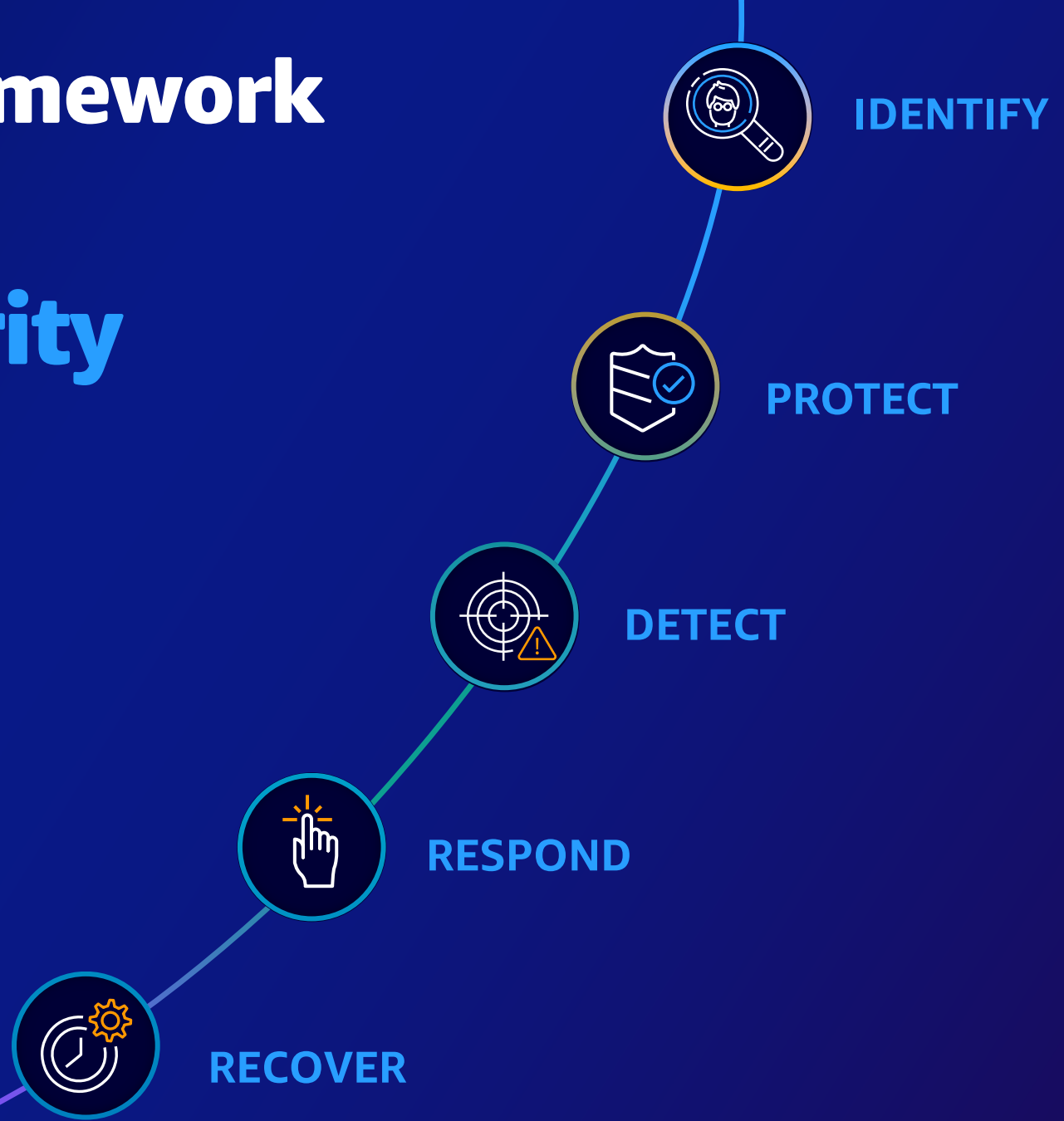
- is the industry standard,
- ... but most companies lack a reliable data protection and recovery strategy



1. Use a security Framework

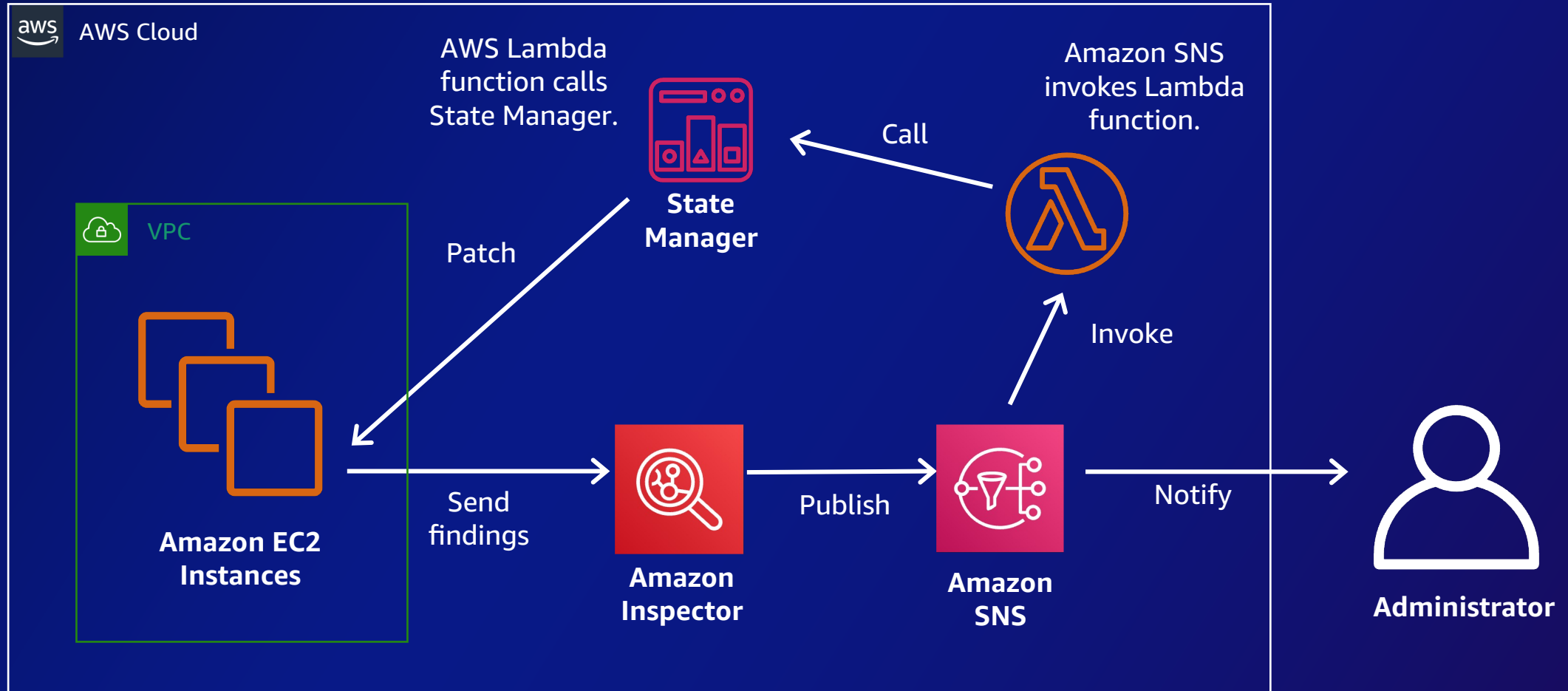
NIST Cyber Security Framework

- is the industry standard,
- ... but most companies lack a reliable data protection and recovery strategy

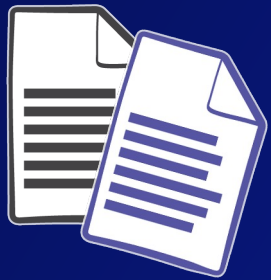


2. Apply critical patches and harden systems

UNPATCHED VULNERABILITIES ARE ONE OF THE MOST COMMON WAYS RANSOMWARE INFECTS AN ORGANIZATION'S ENVIRONMENT.



3. Eliminate long-lived credentials



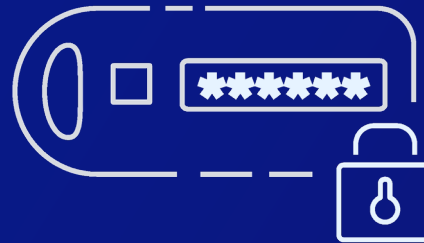
Credential report
and removal
unused credentials



Principle of
least privilege

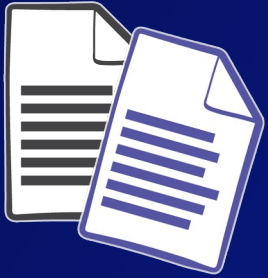


Credential
rotation

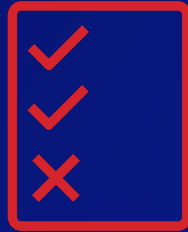


Multi-factor
authentication

3. Eliminate long-lived credentials



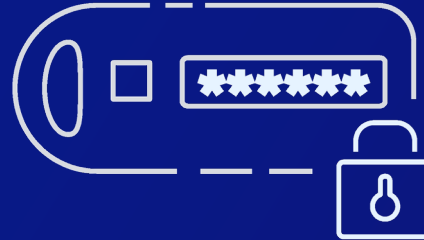
Credential report
and removal
unused credentials



Principle of
least privilege



Credential
rotation



Multi-factor
authentication



Role-based
Access controls

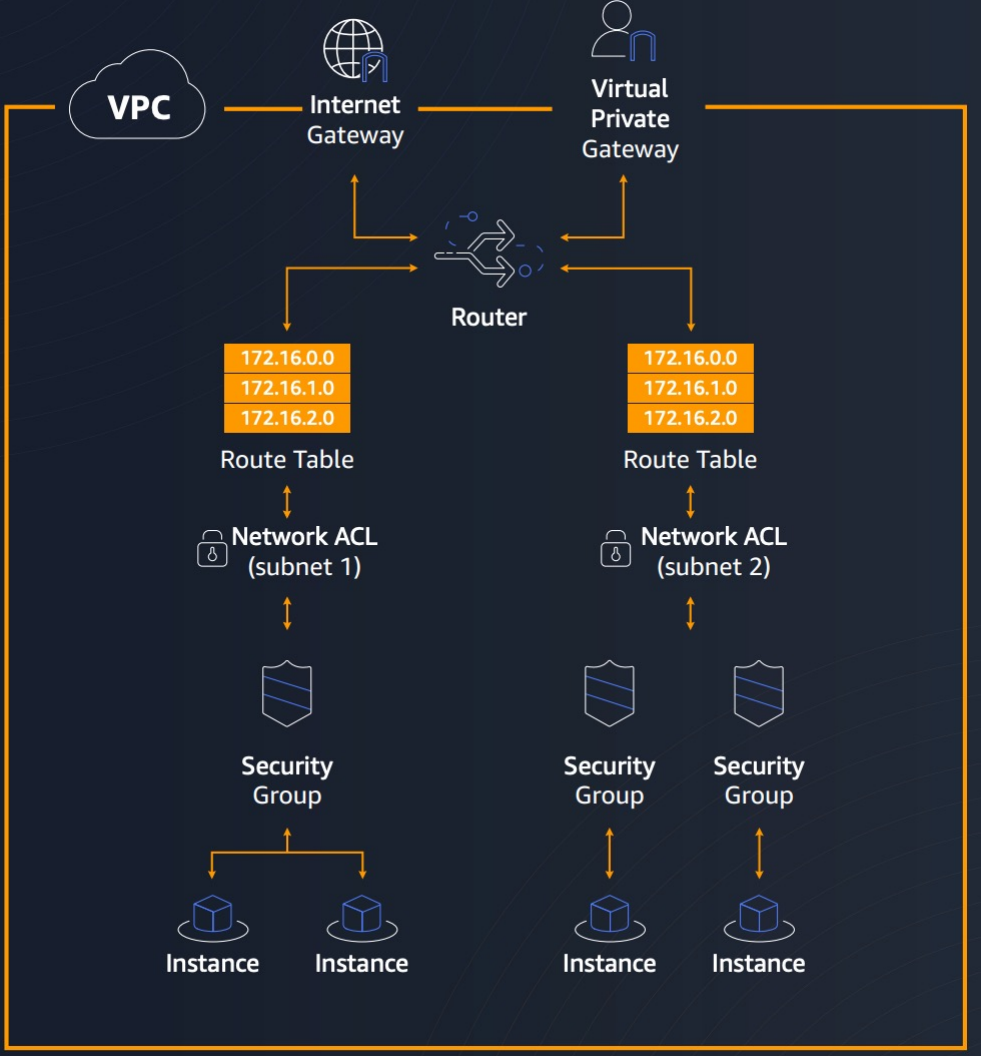
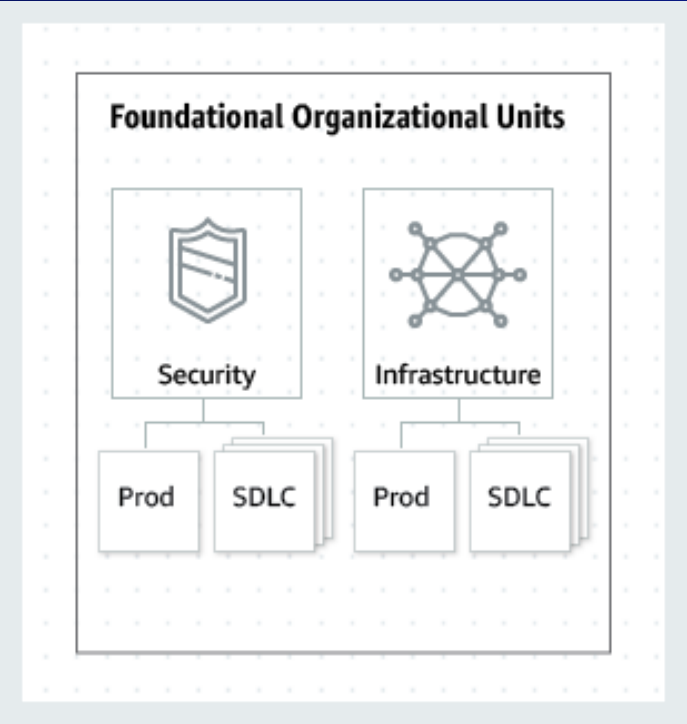


Identify resources
shared with
external entities

4. Use a multi-account strategy and network segmentation



4. Use a multi-account strategy and network segmentation

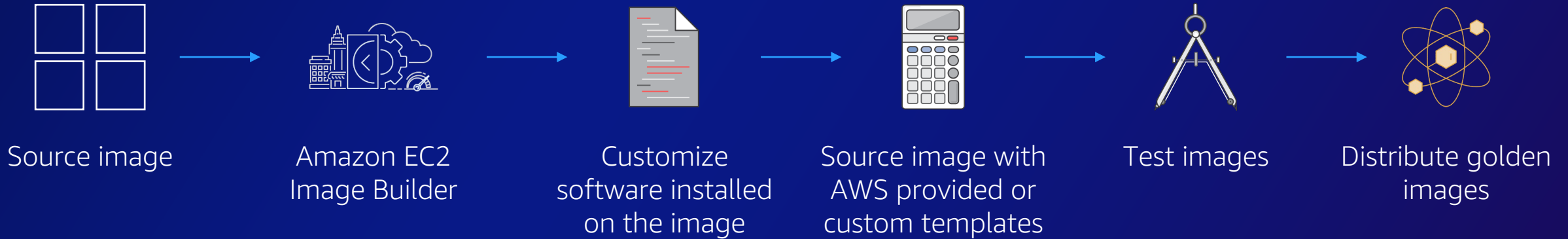


5. Use immutable infrastructure with no human access

AMAZON EC2 IMAGE BUILDER

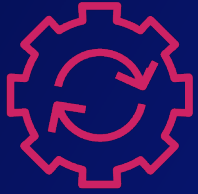


Amazon EC2 Image Builder simplifies the creation, maintenance, validation, sharing, and deployment of Linux or Windows Server images.



5. Use immutable infrastructure with no human access

AWS SYSTEMS MANAGER AUTOMATION



Safely automate common and repetitive IT operations and management tasks across AWS resources.

1



Create an Automation document.

2



Run the Automation document.

3



Monitor and test Automation.

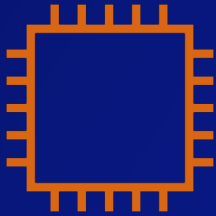
6. Implement centralized logging and monitoring

AWS CLOUDTRAIL



AWS CloudTrail helps you understand events in your accounts.

- Log and monitor account activity across your AWS infrastructure.
- Record API call interactions for most AWS services.
- Automatically push logs to Amazon S3.



Who **shut down** a specific instance



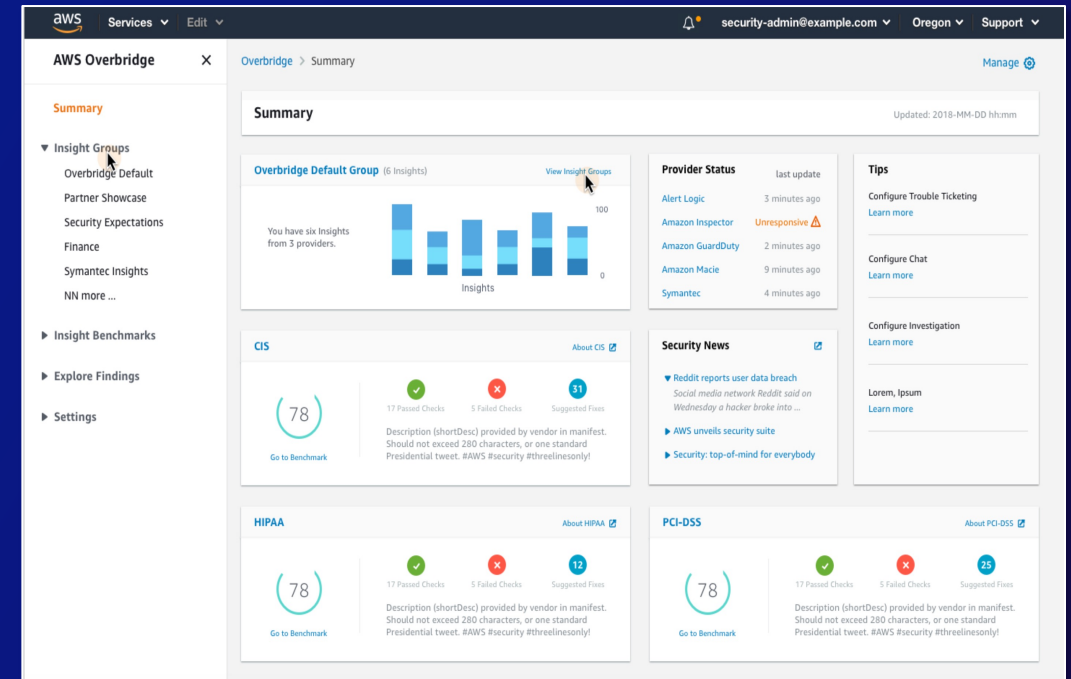
What activities were **denied** due to lack of permissions



Who **changed** a security group configuration

6. Implement centralized logging and monitoring

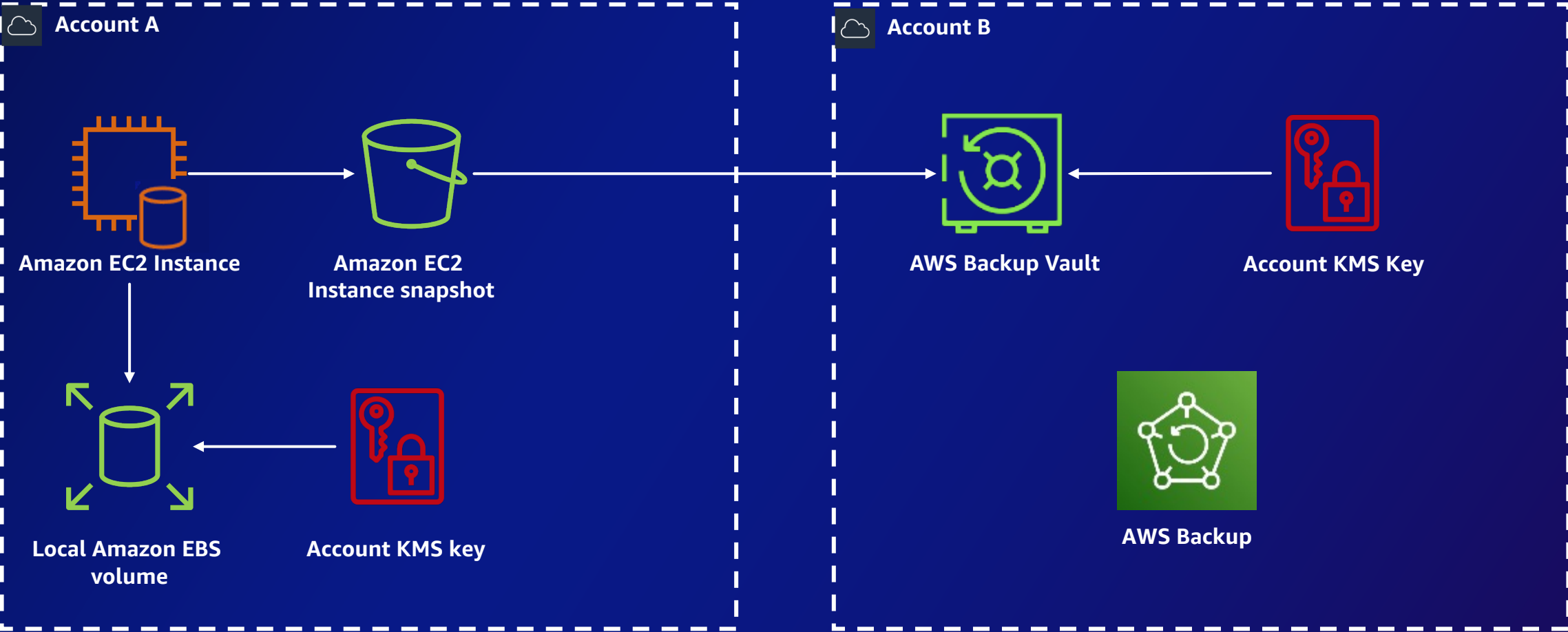
AWS SECURITY HUB



Investigate findings and take responsive/remediation actions.

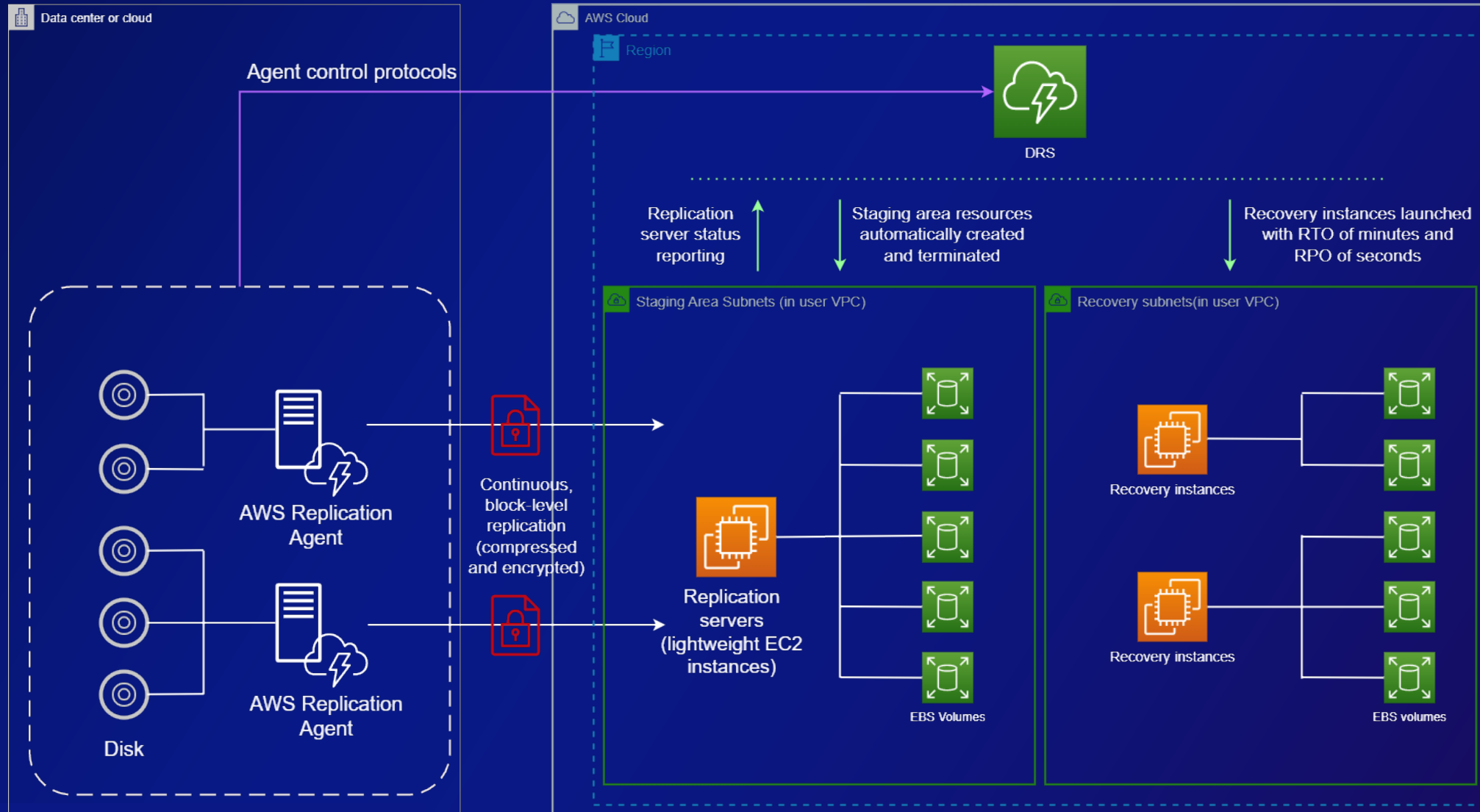
7. Set up the ability to backup and recover your apps and data

AWS BACKUP



7. Set up the ability to backup and recover your apps and data

AWS ELASTIC DISASTER RECOVERY



AWS Backup – Deep dive

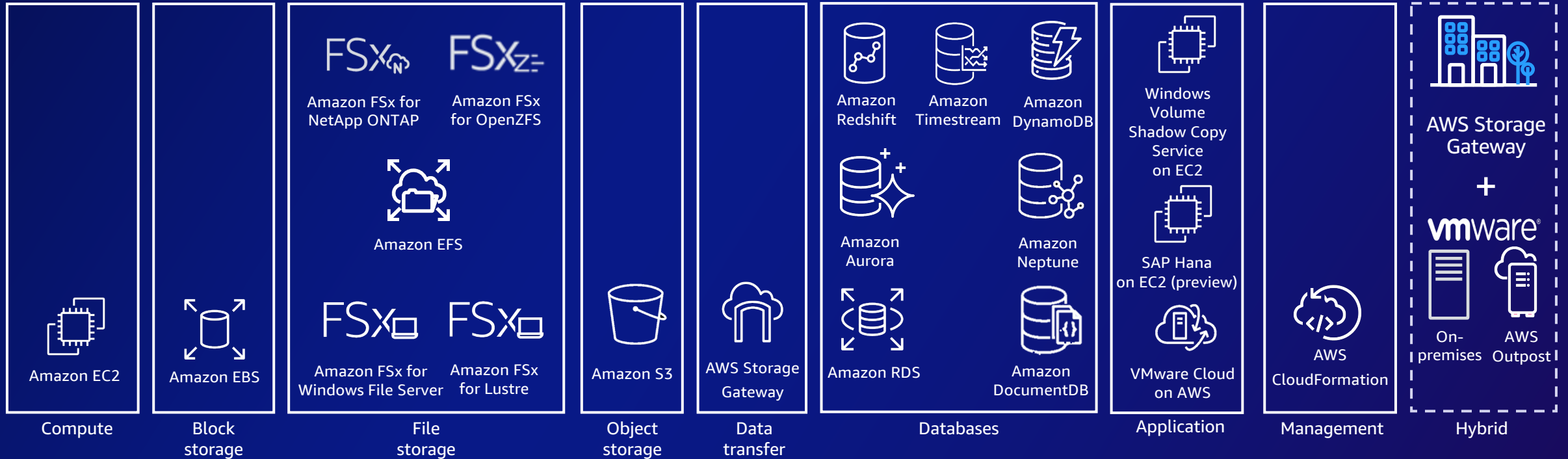


Overview of AWS Backup



AWS Backup

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



AWS Backup use cases



Cloud-native backups

Protect your critical data across AWS services



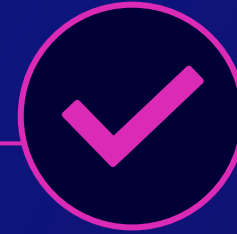
Compliance and governance

Simplify management and reporting of business & regulatory compliance



Disaster recovery

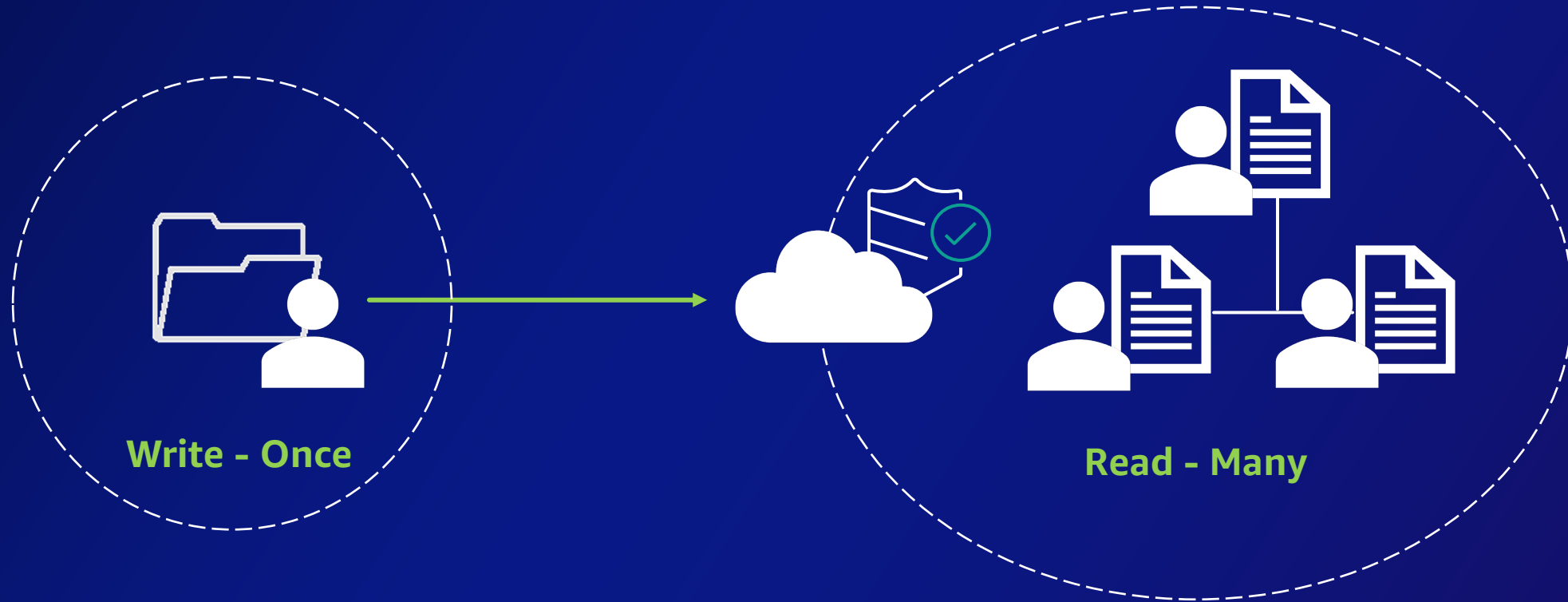
Reduce risk of downtime and build foundation for business continuity



Ransomware recovery

Protect and recover critical data from a ransomware events and account compromise

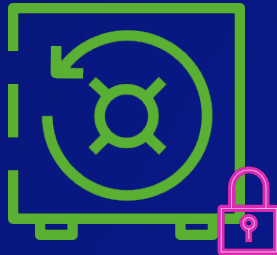
Leverage data immutability with WORM



Besides regulatory compliance, you can use WORM to protect your backup and archives from getting overwritten.

Leverage data immutability

AWS Backup Vault Lock



Fully managed policy-based
AWS-native service

Amazon S3 bucket

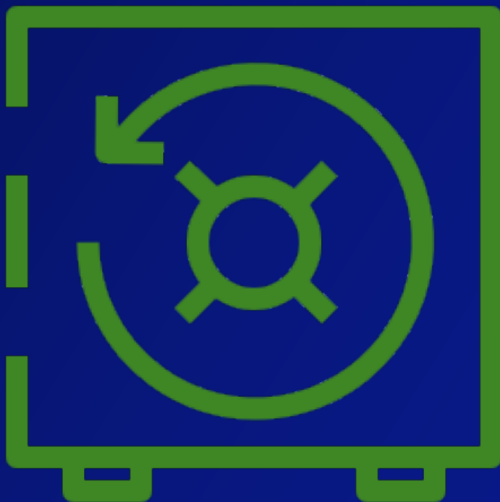


Primitive data types to build
customized solutions

AWS Backup Vault Lock protects your sensitive data backups against malicious actors



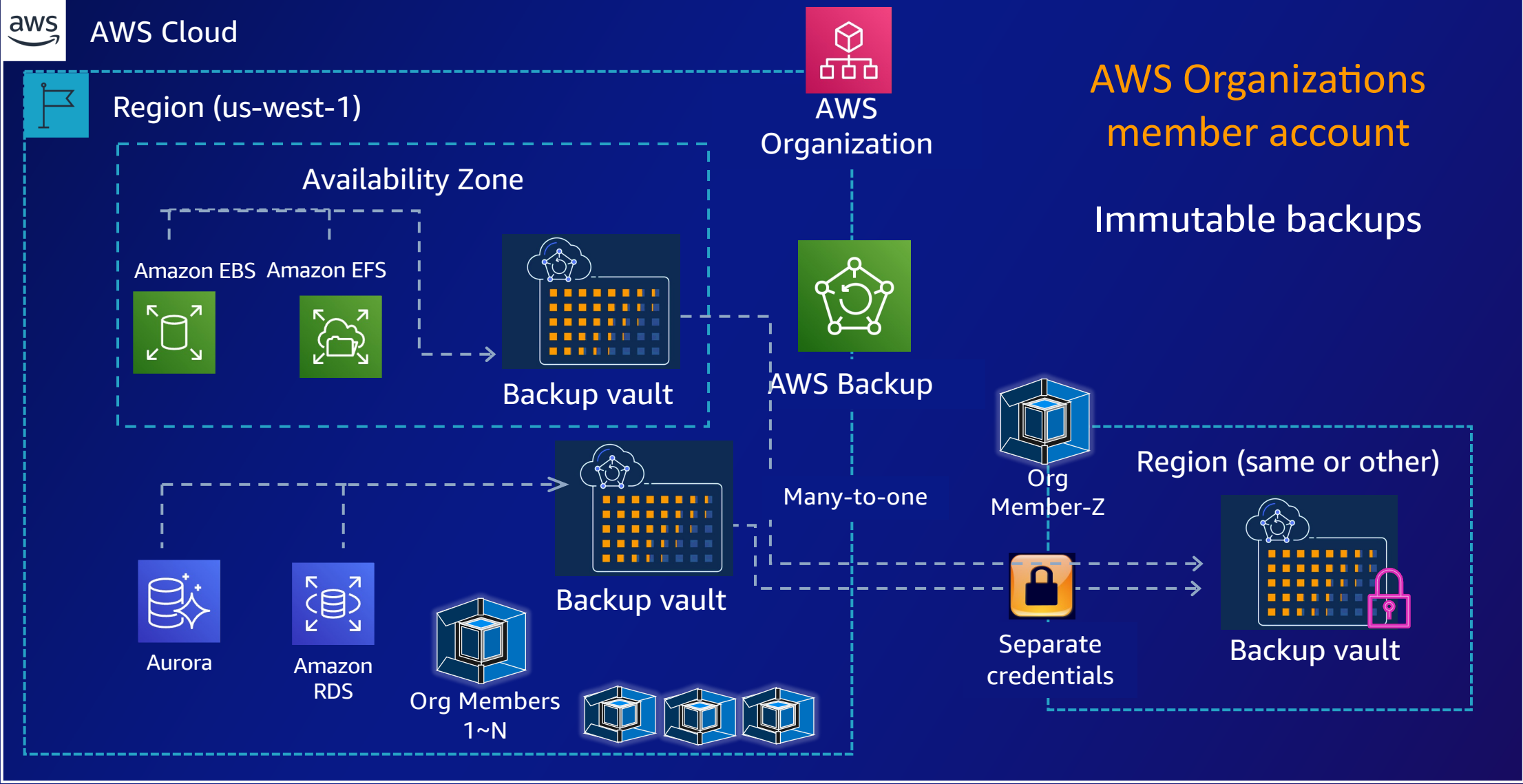
Vault Lock
configuration



AWS Backup Vault

- **Attached to a Backup vault** – You enable **AWS Backup Vault Lock** configuration at the AWS Backup Vault level
- **Protects against deletion** – No user, including the root account, can delete your backups
- **Protects against lifecycle changes** – No user, including the root account, can change your backups' retention periods or update backups transition to cold storage settings
- **Enable AWS Backup Vault Lock** using **AWS Backup API, CLI, or SDK**
- **AWS Backup Vault Lock** has been certified for **SEC 17a-4(f), FINRA 4511(c), and CFTC 1.31(c)-(d)**

Cross-account/cross-Region backups



AWS Backup - Demo



Console Home Info

Reset to default layout + Add widgets

Recently visited Info

- AWS Backup
- EC2
- Support
- S3
- RDS
- AWS Billing Conductor
- AWS Resource Explorer
- Resource Access Manager
- Amazon Interactive Video Service
- AWS Cost Explorer
- AWS Budgets
- CloudWatch

[View all services](#)

Welcome to AWS

- [Getting started with AWS](#)
Learn the fundamentals and find valuable information to get the most out of AWS.
- [Training and certification](#)
Learn from AWS experts and advance your skills and knowledge.
- [What's new with AWS?](#)
Discover new AWS services, features, and Regions.

AWS Health Info

Open issues
0 Past 7 days

Scheduled changes
0 Upcoming and past 7 days

Other notifications
0 Past 7 days

[Go to AWS Health](#)

Build a solution Info

Start building with simple wizards and automated workflows.

- [Launch a virtual machine](#)
With EC2 (2 mins)
- [Start a development project](#)
With CodeStar (5 mins)
- [Connect an IoT device](#)
With AWS IoT (5 mins)
- [Build using virtual servers](#)
With Lightsail (2 mins)
- [Host a static web app](#)
With AWS Amplify Console (2 mins)
- [Register a domain](#)
With Route 53 (3 mins)
- [Build a web app](#)
With AWS App Runner (5 mins)
- [Deploy a serverless microservice](#)
With API Gateway (2 mins)
- [Start migrating to AWS](#)
With AWS MGN (2 mins)
- [Build SQL Server on AWS](#)
With high availability (HA and FCI) (2 mins)

Trusted Advisor Info

No recommendations

This could be because you have not run Trusted Advisor checks, or you don't have AWS Business or AWS Enterprise support plans.

[Go to Trusted Advisor](#)

Explore AWS Info

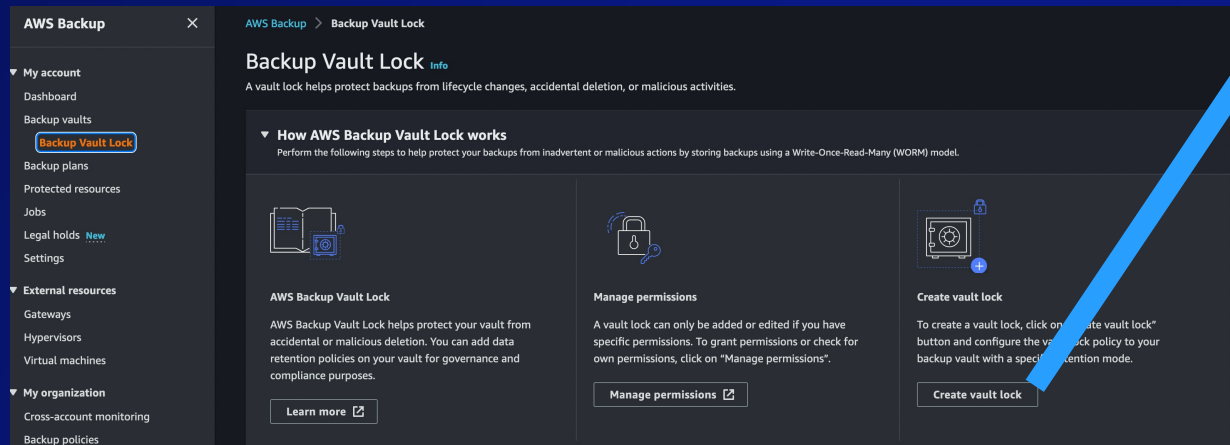
- [Free AWS Training](#)
Advance your career with AWS Cloud Practitioner Essentials—a free, six-hour, foundational course.
- [Free Digital Training](#)
Learn the AWS Cloud to create opportunities tomorrow.
- [Free eBook](#)
Get a complete overview of all things AWS Certification.
- [AWS Certification](#)
Propel your career with AWS Certification.

AWS Backup Vault Lock – How to enable it?

CLI

- `aws backup put-backup-vault-lock-configuration --backup-vault-name WORM_vault`
- `--changeable-for-days 3 --min-retention-days 7 --max-retention-days 30`

Console



Vault lock details

Protect your vault with your choice of retention mode.

Backup vault [Info](#)

The vault lock will apply to the contents of the selected vault.

Default

Vault lock mode [Info](#)

Governance mode
The lock can be managed or deleted by users with specific IAM permissions.

Compliance mode
The lock cannot be managed or deleted by any user, even by the root user (account owner) or AWS.

Retention period [Info](#)

Vault locks helps protect backups within the minimum and maximum retention periods.

Minimum retention period - optional [Info](#)

Backups with retention period equal to or greater than the entered value will be protected. 1 day is the default.

1 Days

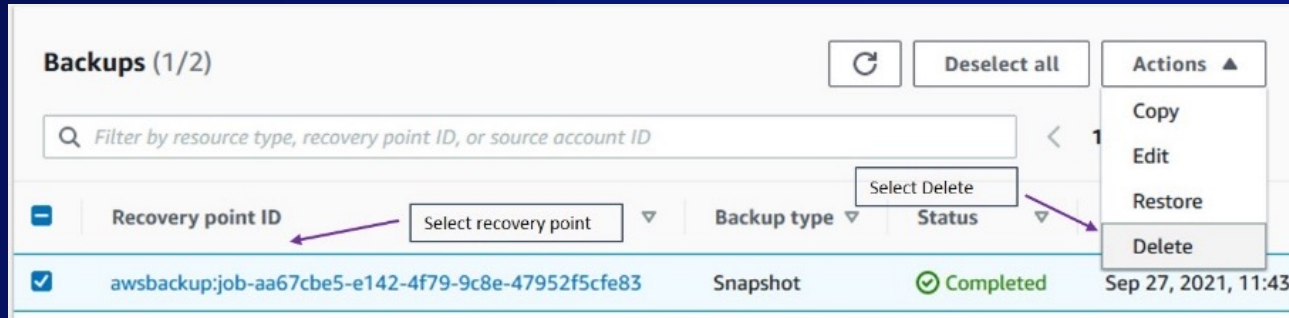
Maximum retention period - optional [Info](#)

Backups with a retention period equal to or less than the entered value will be protected.

Enter maximum retention period Days

! All existing backups in the vault and new backups or copy jobs added to the vault will be protected. This vault can be managed or deleted by only those users with specific IAM permissions. [Learn more](#)

AWS Backup **Vault Lock** – How to enable it?

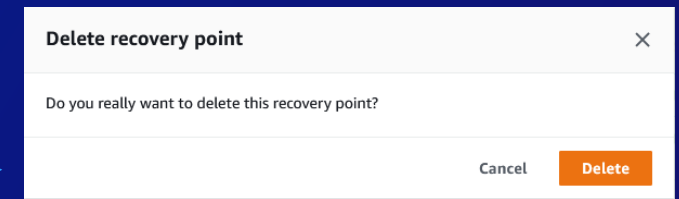


Backups (1/2)

Filter by resource type, recovery point ID, or source account ID

Recovery point ID	Backup type	Status	
awsbackup:job-aa67cbe5-e142-4f79-9c8e-47952f5cfe83	Snapshot	Completed	Sep 27, 2021, 11:43:...

Actions: Copy, Edit, Restore, Delete

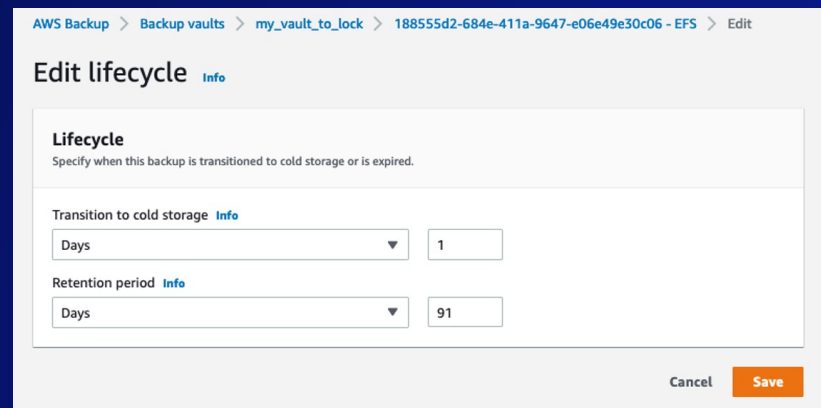


Delete recovery point

Do you really want to delete this recovery point?

Cancel Delete

RecoveryPoint cannot be deleted or updated (Backup vault configured with Lock.)



Edit lifecycle

Lifecycle

Specify when this backup is transitioned to cold storage or is expired.

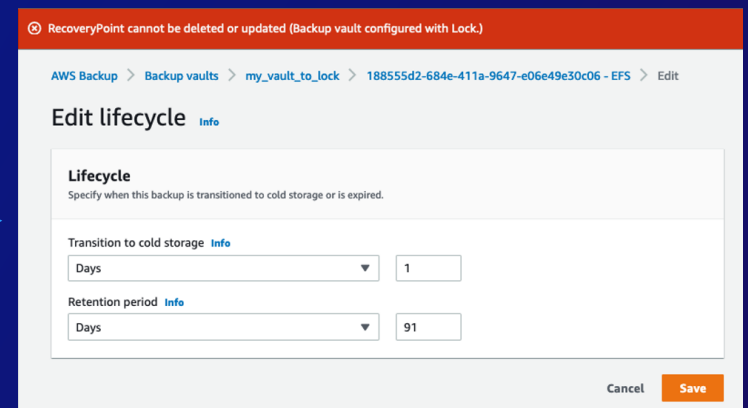
Transition to cold storage

Days 1

Retention period

Days 91

Cancel Save



RecoveryPoint cannot be deleted or updated (Backup vault configured with Lock.)

Edit lifecycle

Lifecycle

Specify when this backup is transitioned to cold storage or is expired.

Transition to cold storage

Days 1

Retention period

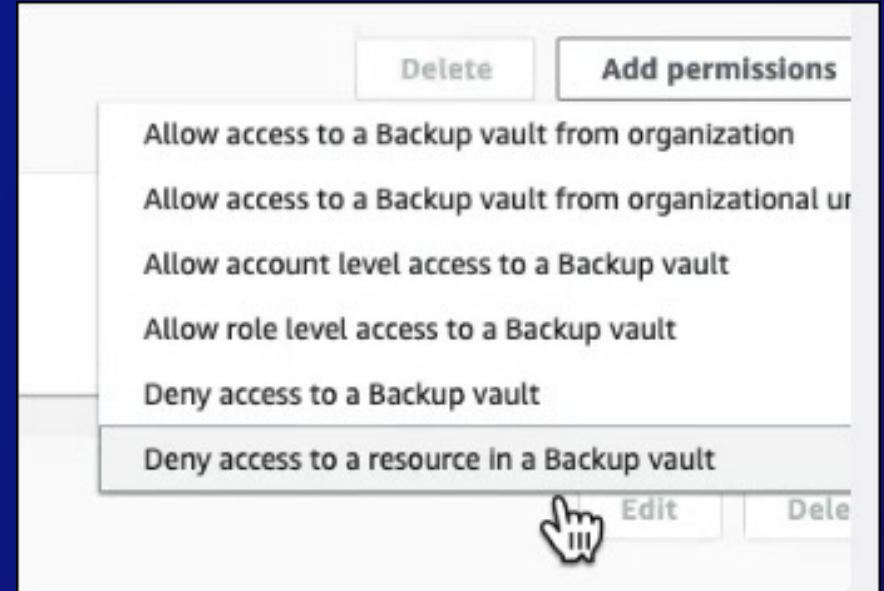
Days 91

Cancel Save

- **Delete Vault Lock configuration**
- `aws backup delete-backup-vault-lock-configuration --backup-vault-name WORM_vault`

How do AWS Backup vaults secure backups

- Limit who can **access recovery points** within an account
- Limit the ability to **destroy backups** from within a vault
- Many vaults can be used for **separation of permissions**, for example, development, test and production
- Backups **cannot be deleted** from the native services being protected.
- Each vault has its **own SNS notification** configuration



Summary

7 Best practices for Ransomware protection

1. Use a security Framework
2. Apply critical patches and harden systems
3. Eliminate long-lived credentials
4. Use a multi-account strategy and network segmentation
5. Use immutable infrastructure with no human access
6. Implement centralized logging and monitoring
7. Set up the ability to backup and recover your apps and data

AWS Backup

AWS Backup Vault Lock

Call to action

Reach out to your Account manager and/or Solutions Architect

Visit us at the booth!

Workshops

Ransomware detection workshop:

<https://catalog.us-east-1.prod.workshops.aws/workshops/6484b52f-39fa-45cf-937c-95af1ea29b6b/en-US>

AWS Backup workshop:

<https://catalog.us-east-1.prod.workshops.aws/workshops/74237958-77c8-4e7f-a02f-ae201a04d759/en-US/aws-backup-lab/02-backupplan>

Training and Certification

skillbuilder.aws 

AWS Backup and Ransomware documentation

<https://aws.amazon.com/blogs/storage/enhance-the-security-posture-of-your-backups-with-aws-backup-vault-lock/>

<https://aws.amazon.com/blogs/security/ransomware-mitigation-top-5-protections-and-recovery-preparation-actions/>

<https://d1.awsstatic.com/psc-digital/2022/qc-200/security-ransomware-ebook/Security-Ransomware-eBook.pdf>

Thank you!

Laura Verghote

Solutions Architect

 [linkedin.com/in/laura-verghote/](https://www.linkedin.com/in/laura-verghote/)

Rotem Agmon

Solutions Architect

 [linkedin.com/in/rotemagmon/](https://www.linkedin.com/in/rotemagmon/)



Please complete the session survey in the mobile app