AWS re:Invent

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

STG332-R2

Data protection and recovery strategies from ransomware events

Mohammed Sabunchi
Principal - Storage Specialist
AWS - Canada

Fathima Kamal
Sr. Specialist SA – Storage
AWS

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

Agenda

01 The state of ransomware threats

02 The industry standard (NIST)

03 AWS ransomware recovery solution

04 Next steps

05 Q/A session

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

Ransomware threats are rampant

75% of IT organizations will face one or more **RANSOMWARE THREATS** by 2025

Gartner, 2021

RANSOMWARE ATTACKS will occur every 11 seconds in 2021 and will result in financial loss of **$20B**

Source: Sophos the state of Ransomware 2020 Report—Independent study of 5,000 IT managers

The New York Times

TECHNOLOGY

Ransomware Attacks Grow, Crippling Cities and Businesses

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 Colonial Pipeline attack should be a wake-up call for hardening our cyber defenses

THE HILL

The Washington Post

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

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

The San Diego Union-Tribune

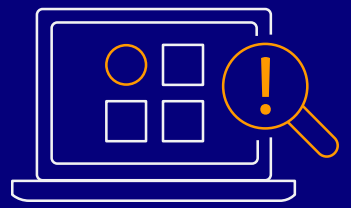
Scripps enters fourth week of ransomware attack

The ransomware surge ruining lives

BBC NEWS

What is ransomware?

Ransomware is a form of malware that threatens to publish victim's 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 victims to pay a ransom to get their files back, normally through cryptocurrency-based transactions

aws

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

Ransomware attacks are more likely when...

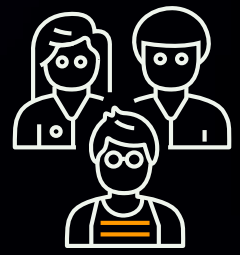
Technical element



Lacking in technical competency

- Patching not up to date
- Irregular untested data backups
- Manual time-consuming processes

Educational element



There is social unawareness

- Low security and data protection awareness
- Vulnerable to social engineering
- Employee behavior creates security risks

Governance element



No established governance body

- Overly permissive credentials
- Open trust model allows malware to spread
- No clear governance model

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

NIST Cyber Security Framework

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



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 incident

aws

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

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 incident

Strategy formation

- What is the most important data that we want to protect?
- Should the recovery of some data be prioritized over others?
- What is an acceptable recovery time?



AWS Backup



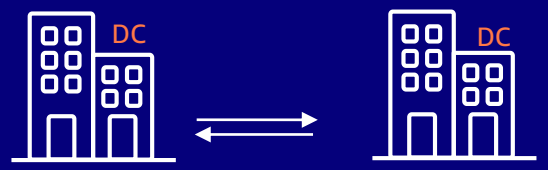
Amazon S3

Disaster recovery vs. ransomware recovery

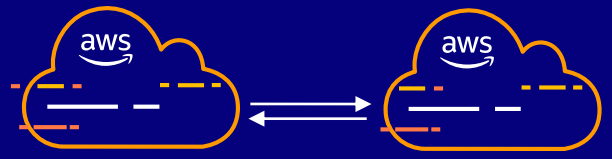
EXPANDING ON DISASTER RECOVERY

Disaster recovery

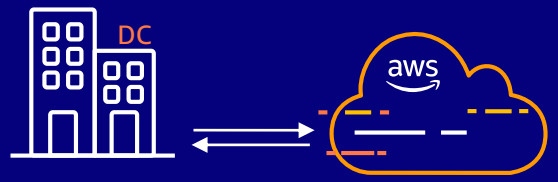
Recovery time objective (RTO)



Option 1: On premises to AWS



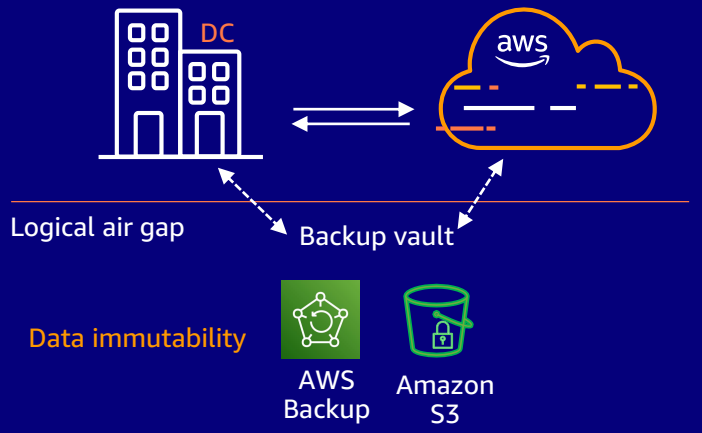
Option 2: Cross-Region or Availability Zone

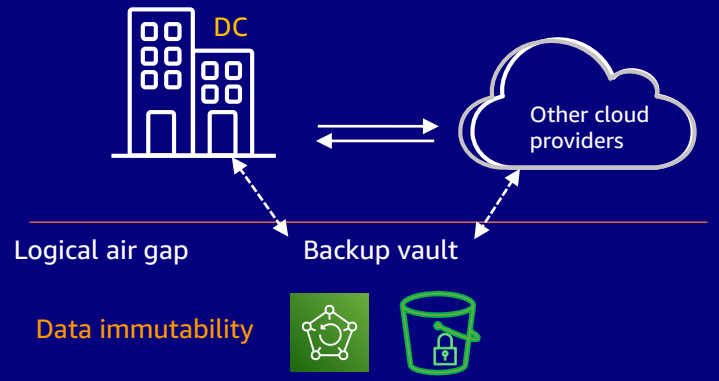


Option 3: Hybrid

Ransomware recovery

Recovery solution





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

Main benefits of the backup vault in the cloud

Data immutability

- Secure environment that prevents modification or deletion of important data with the tools to create the desired solution

Isolation – Separate credentials

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

Agility & speed

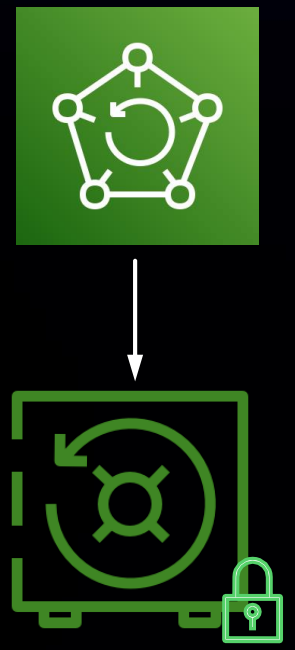
- The ability to deploy and implement ransomware solutions on the cloud providing security, agility, and speed in execution



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

Ransomware recovery options based on your needs

AWS Backup vault



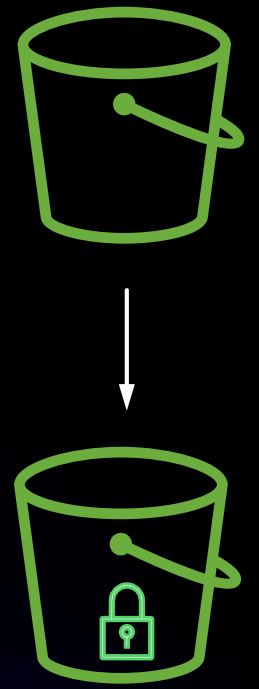
Backup vault

Robust standard configuration (AWS Managed Services [AMS])

Technical features

- Data immutability
- Logical air gap
- Forensic analysis
- Pinholing / Pull only vault
- Control plane security
- Fully managed services
- Flexible and customizable solution
- Replication across organizations
- Multiple roots of trust

Amazon S3

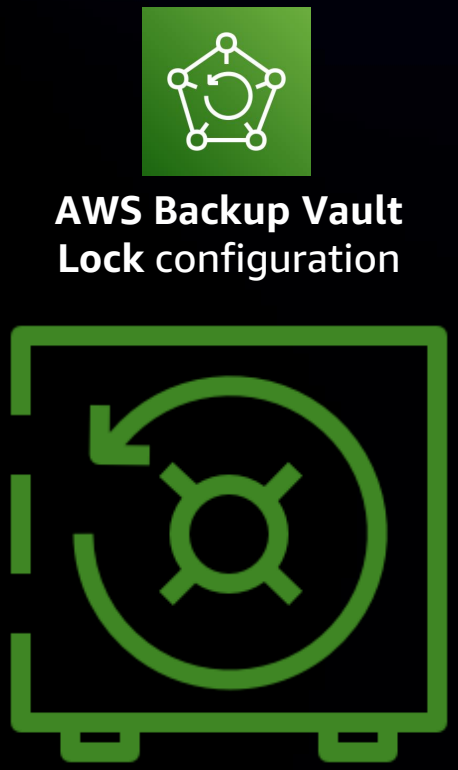


Powerful & customizable

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

AWS Backup Vault Lock

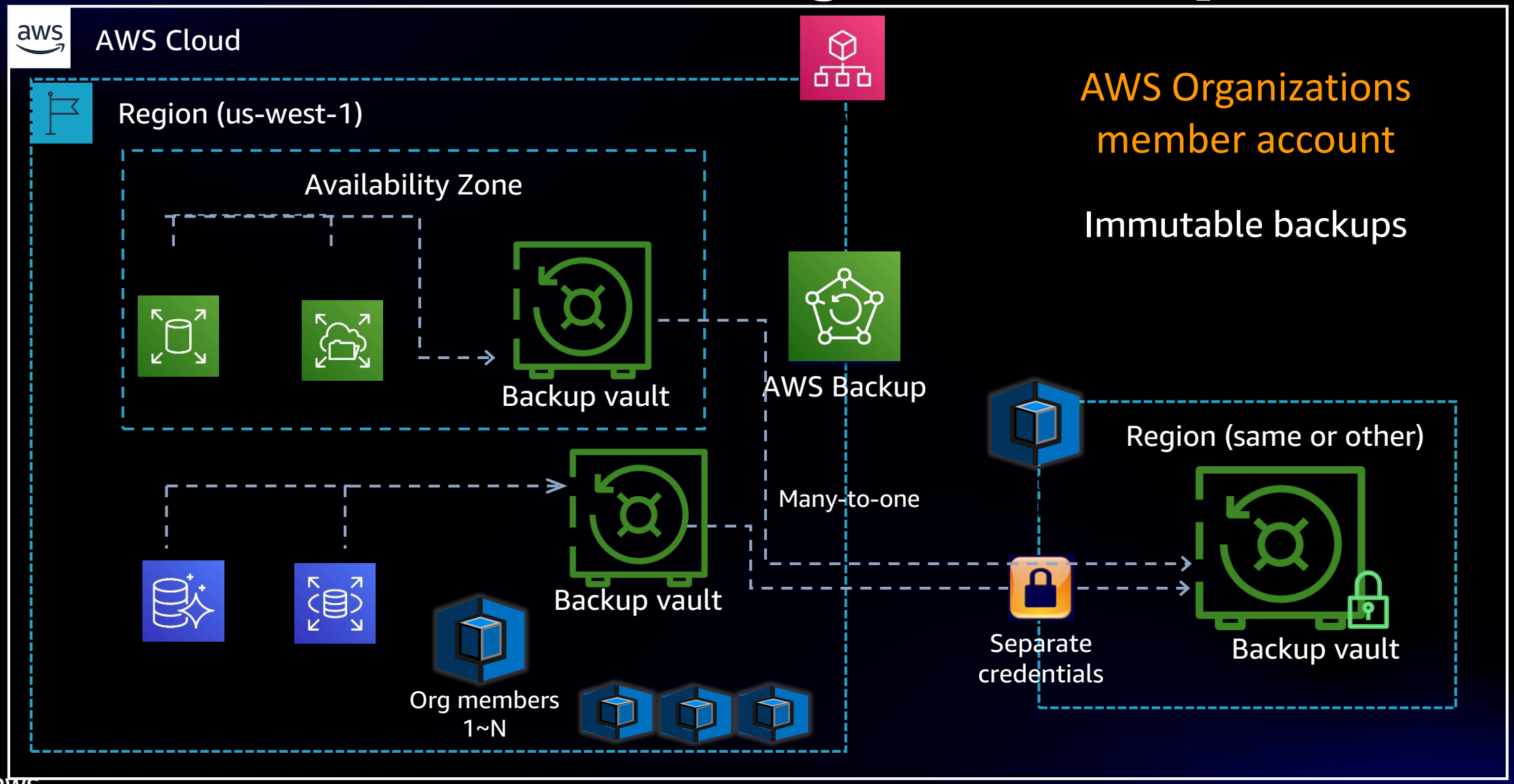
AWS Backup Vault Lock protects your backups against malicious or accidental actions



- Attached to the backup vault – you enable AWS Backup Vault Lock configuration at the 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

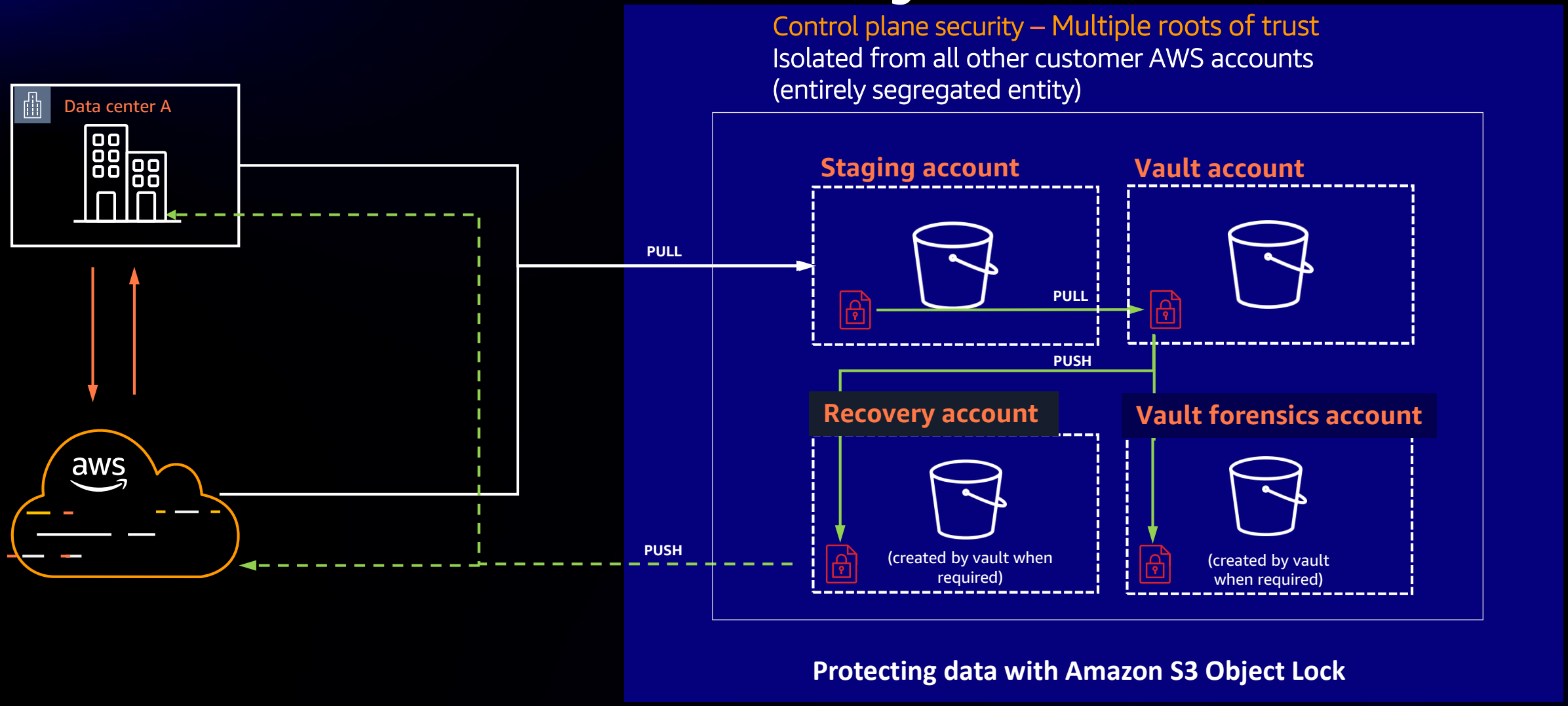
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cross-account/cross-Region backups



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

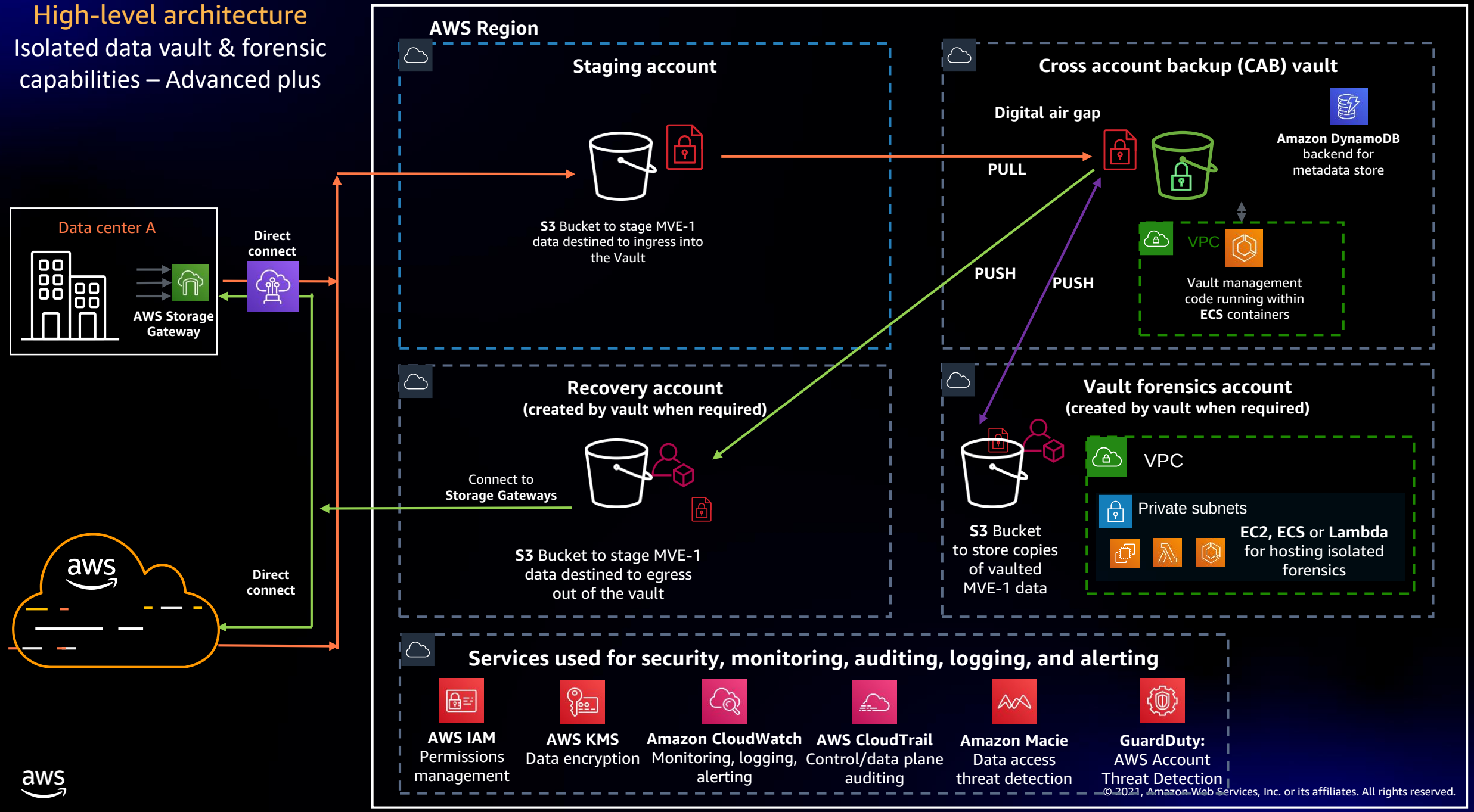
AWS ransomware recovery solution



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

High-level architecture

Isolated data vault & forensic capabilities – Advanced plus



aws

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

Next steps

Recovery strategy session with AWS

- Highlight the importance of Ransomware recovery solution
- Start the process to identify critical data in your organization!

Start with the assessment

- Time: 1 month assessment on data processes and current system capabilities
- Participation from business stakeholders, cyber security and IT Infrastructure teams

Outcome: Recommended recovery strategy

- Defined internal business requirements
- Internal capabilities, tools, and technologies to be included in strategy
- Partner identification
- High-level timeline

aws

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

Thank you!

Mohammed Sabunchi

Sabunchi@amazon.com
Twitter: @sabunchi_m

Fathima Kamal

fkamal@amazon.com
Twitter: @fathimakg

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