AWS re:Invent

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

SEC308

Use AWS to improve your security posture against ransomware

Merritt Baer
merrbaer@amazon.com
Principal, Office of the CISO
AWS

Megan O'Neil
megoneil@amazon.com
Sr. Security Specialist Solutions Architecture
AWS

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

What is ransomware?

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

What is ransomware?



Ransomware refers to a business model and a wide range of associated technologies that unauthorized users use to extort money from entities

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

What is ransomware?

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



Accomplished by unauthorized user who **encrypts** data using actor-controlled encryption keys, using access controls to **lock out** the rightful owner from a system

Or, unauthorized users may threaten to **reveal data or facts of exfiltration**, which can result in large monetary fines from data privacy authorities and/or litigation from affected parties

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

How did we get here?



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

White House guidance

"We urge you to take these critical steps to protect your organizations and the American public."

- Back up data and test regularly
- Update and patch systems promptly
- Test incident response plan
- Check your work – use third-party pen testing
- Segment networks



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

Level up your security (an invitation!)

1.0 Minimize human access

2.0 Translate security policies into code

3.0 Build mechanisms/tooling and measure them

4.0 Streamline the use of environments and infrastructure

5.0 Utilize advanced data/database services features



Outcomes: innovation and security at scale

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

1.0 Minimize human access

- Use federation, and require MFA for human access
- Reduce, as much as possible, the use of long-term credentials
- Use service control policies (SCPs) to set key boundaries
- Use AWS IAM Access Analyzer to scope-down privileges

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

Use federation, and require MFA for human access



Easy management

Easily manage AWS account and role access at scale



AWS CLI

Single sign-on from AWS Command Line Interface (AWS CLI)



One logon

One sign-in experience for cloud business applications



Existing identity provider

Bring your own identities, or create them natively

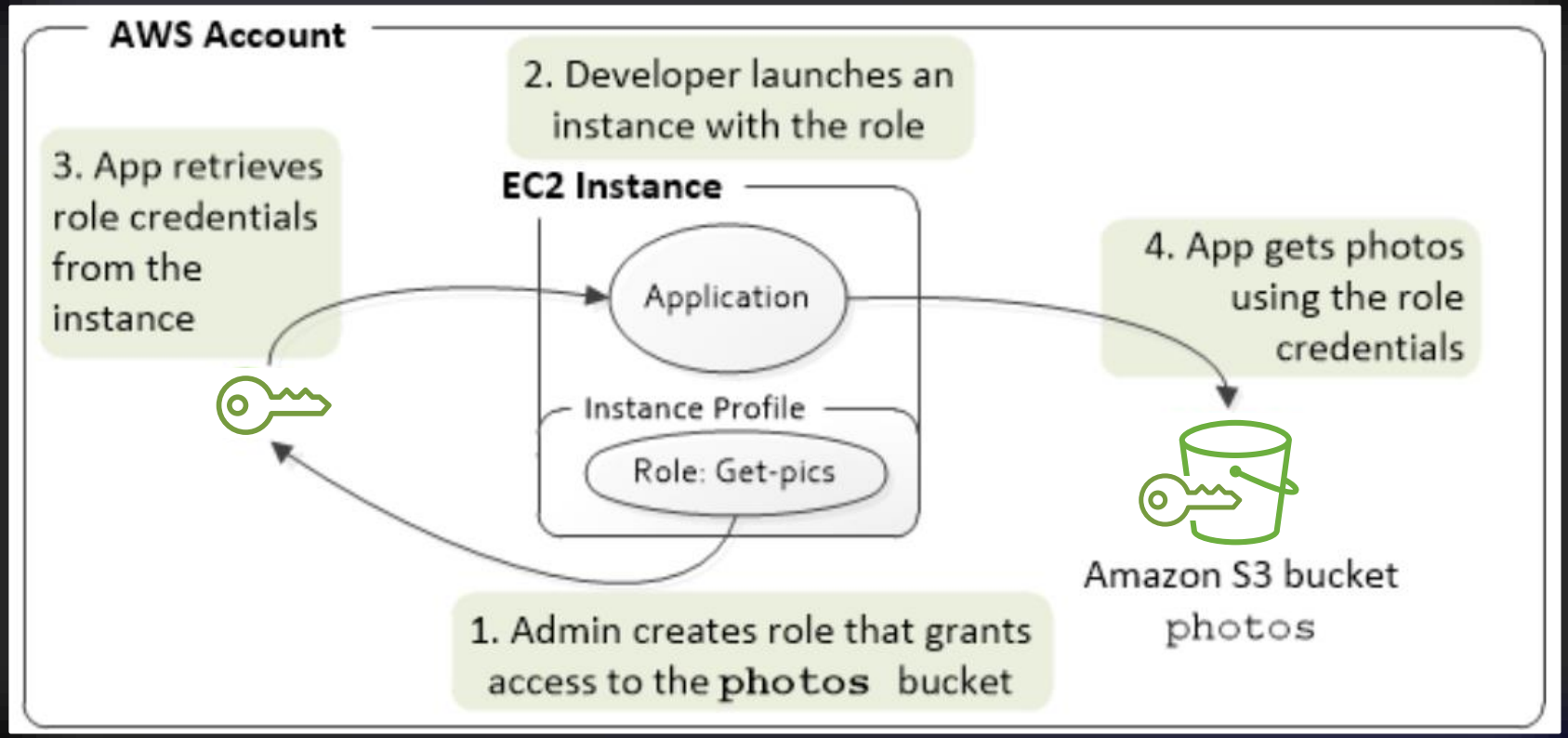


First-party application integration

One sign-in for integrated applications; AWS IoT SiteWise Monitor, Amazon SageMaker notebooks

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

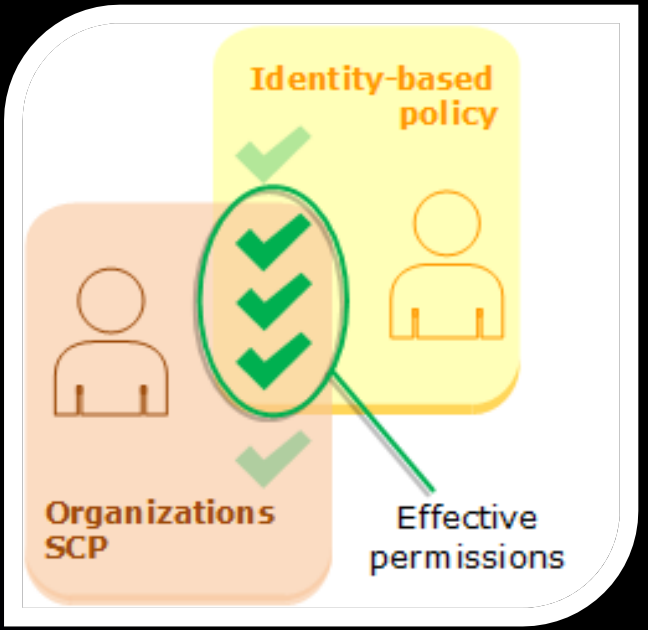
Reduce, as much as possible, the use of long-term credentials



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

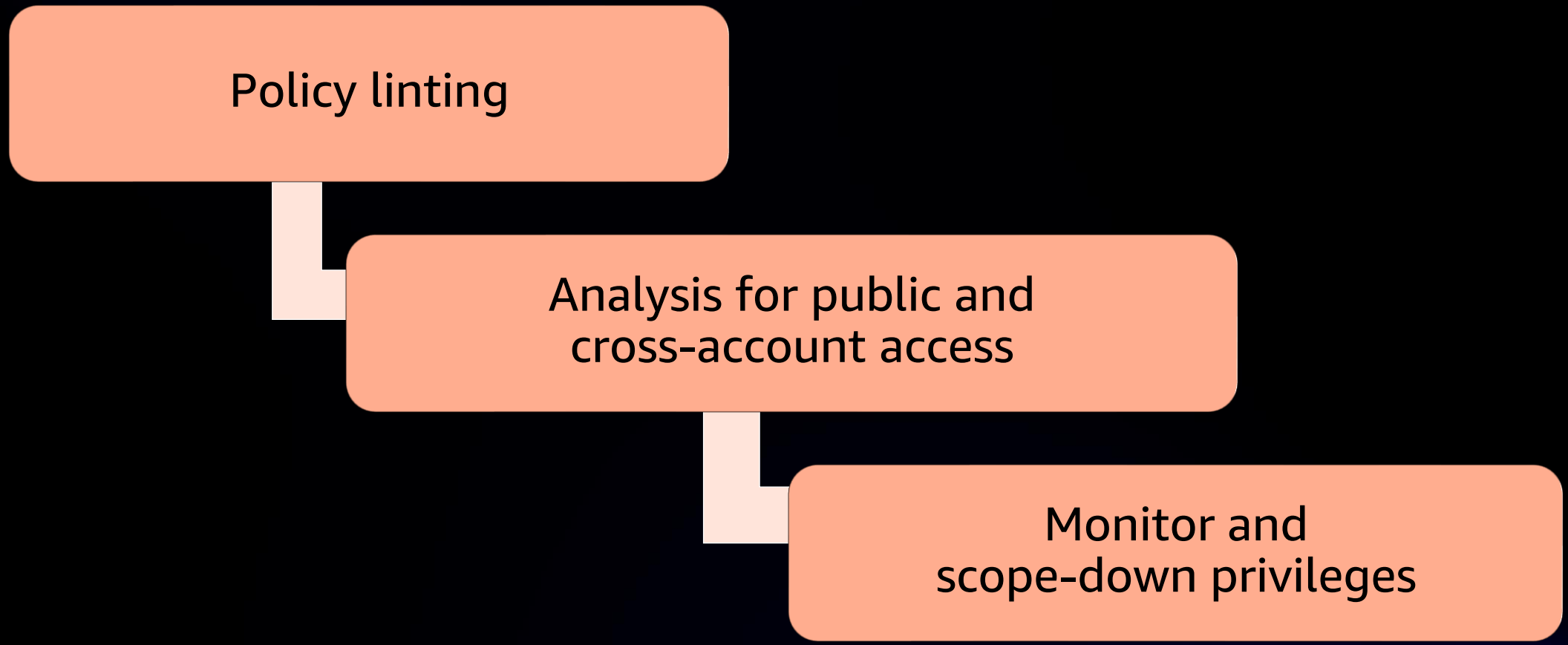
Use service control policies (SCPs) to set key boundaries

- **Control which AWS service APIs are accessible**
  - Define list of APIs that are granted – **grant**
  - Define list of APIs that must be denied – **deny**
- **SCPs**
  - Remove privileges; never add them
  - Are invisible to all users in the child account, including root
  - Can be applied to all users in the child account, including root
- **Permission**
  - Intersection between SCP and IAM permissions
  - IAM policy simulator is SCP-aware



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

Use AWS IAM Access Analyzer to scope-down privileges



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



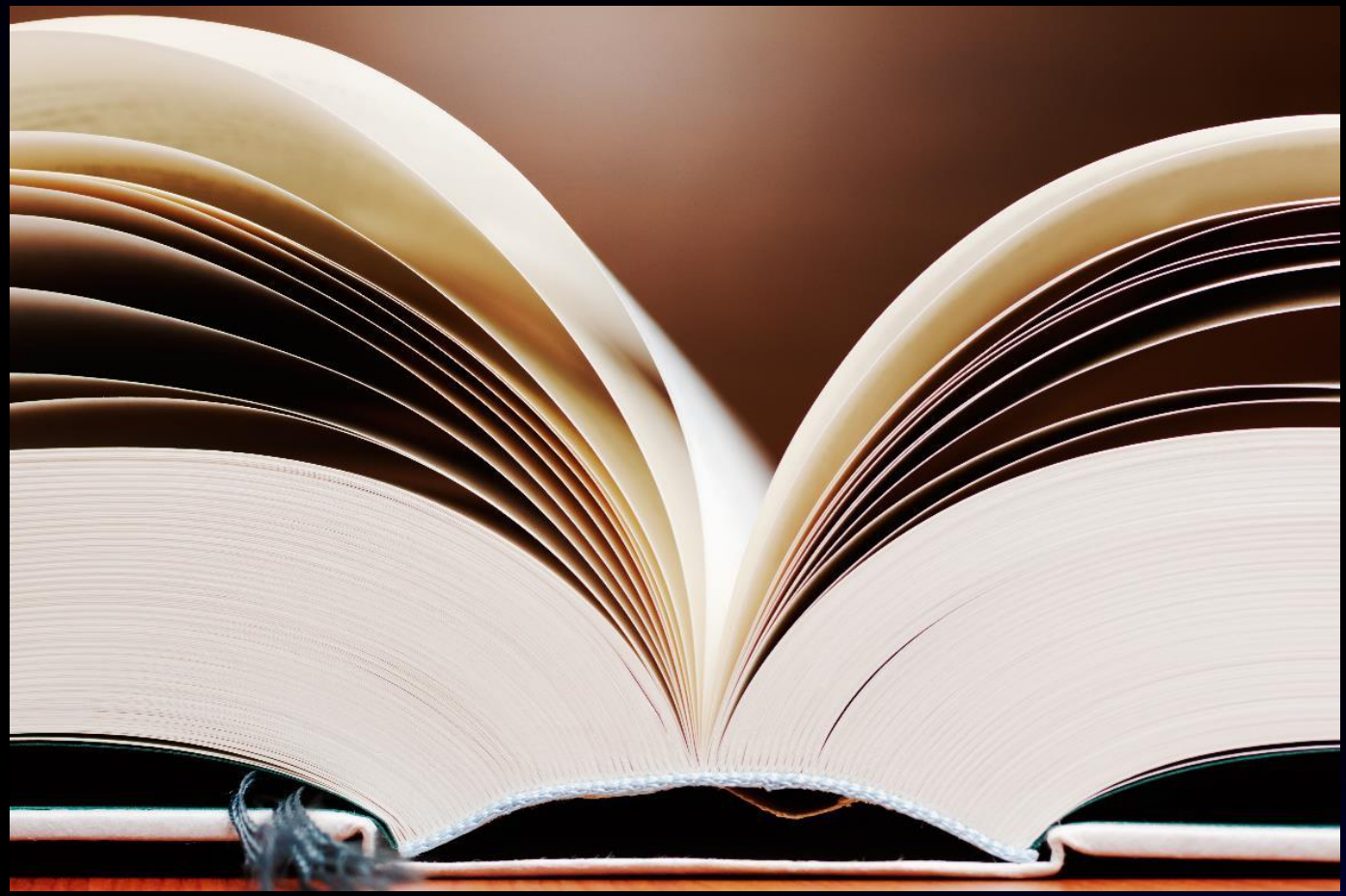
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

2.0 Translate security policies into code

- Translate your security requirements into user stories and then code
- AWS CloudFormation Guard 2.0
- Democratize your security responsibility

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

Translate your security requirements into user stories and then code



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

AWS CloudFormation Guard 2.0

Example rule: This rule checks that AWS KMS server-side encryption is enabled on Amazon S3 buckets

```
let s3_buckets = Resources.*[ Type == 'AWS::S3::Bucket' ]
let allowed_algos = ["aws:kms"]

rule s3_buckets_allowed_sse_algorithm when %s3_buckets !empty {
    let encryption = %s3_buckets.Properties.BucketEncryption
    %encryption exists
    %encryption.ServerSideEncryptionConfiguration[*].ServerSideEncryptionByDefault.SSEAlgorithm in %allowed_algos

}
```

github.com/aws-cloudformation/cloudformation-guard

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

Make the secure thing to do, the easy thing to do

Democratize down



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

3.0 Build mechanisms/tooling and measure them

- Implement and monitor AWS security services
- Start somewhere
- Patch and harden systems
- IR is different in the cloud
- Practice your IR with tabletop exercises

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

“If it’s not someone’s job then it’s a hope. And a hope is not a plan.”

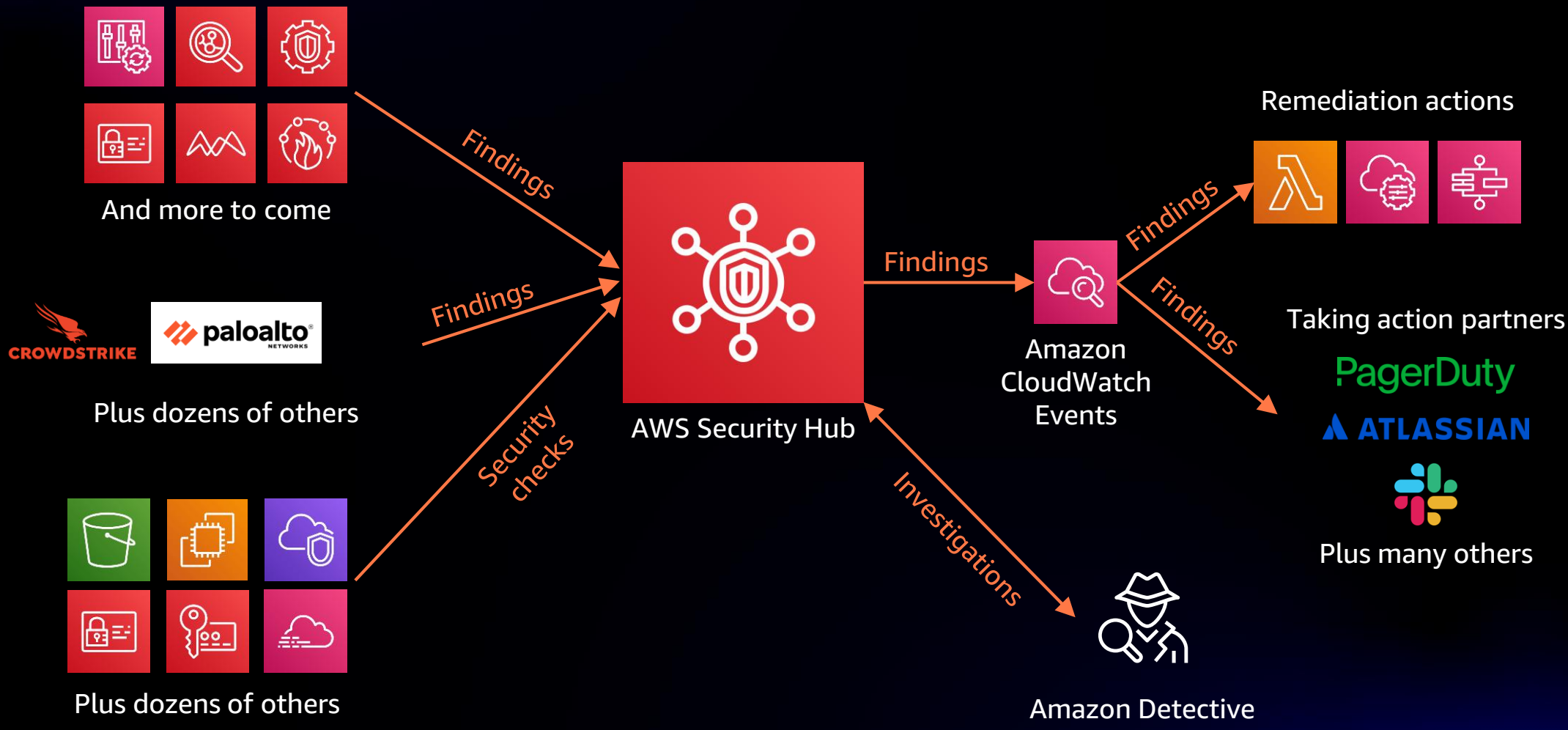
Eric Brandwine

VP/Distinguished Engineer, AWS Security

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

Use AWS security services for monitoring

"Good intentions are not enough." – Eric Brandwine, VP/Distinguished Engineer, AWS Security



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

Start somewhere

"There are two ways to learn incident response. One will be chosen for you (responding to a real incident)."

Beetle@
AWS Security



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

Patch and harden systems



- Use **Amazon Inspector** to identify vulnerabilities and assess instances against security benchmarks
- Use **Amazon ECR image scanning** to identify vulnerabilities and assess your container images
- **AWS Systems Manager Patch Manager** to deploy OS and software patches automatically
- Endpoint detection software and OS/software hardening
- Phishing as a primary vector

CIS. aws marketplace

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

IR in the cloud

Forensics looks different (logging)

Working at scale (security data lake)

Preparation as fundamental to success (it's knowable)

Enable your teams to get the data they need to do IR



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

Develop and exercise your incident response plan

People

- ✓ Train security operations staff on AWS

Process

- ✓ Develop an incident response plan and strategy
- ✓ Run drills and automate simulations where possible

Technology

- ✓ Build AWS accounts for: security operations and log archival
- ✓ Create read only and break glass roles for access to AWS accounts
- ✓ Setup security services like Amazon GuardDuty, AWS Security Hub to detect threats
- ✓ Use security services like Amazon Detective to help you investigate security findings

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

4.0 Utilize advance features of data/database services

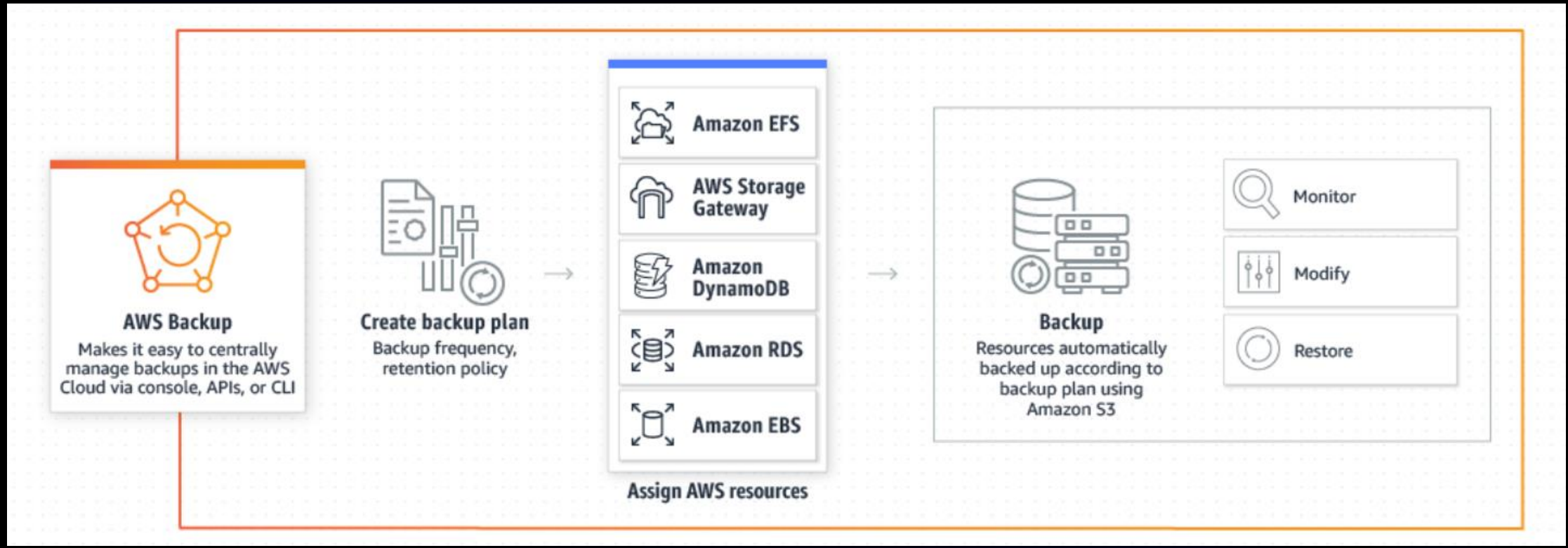
USE VAULTS AND LOCKS

- AWS Backup Vault Lock
- Amazon S3 Object Lock and S3 Glacier Vault Lock
- Point-in-time recovery (PITR) for Amazon DynamoDB for Amazon RDS
- Amazon Aurora database cloning

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

AWS Backup with Vault Lock

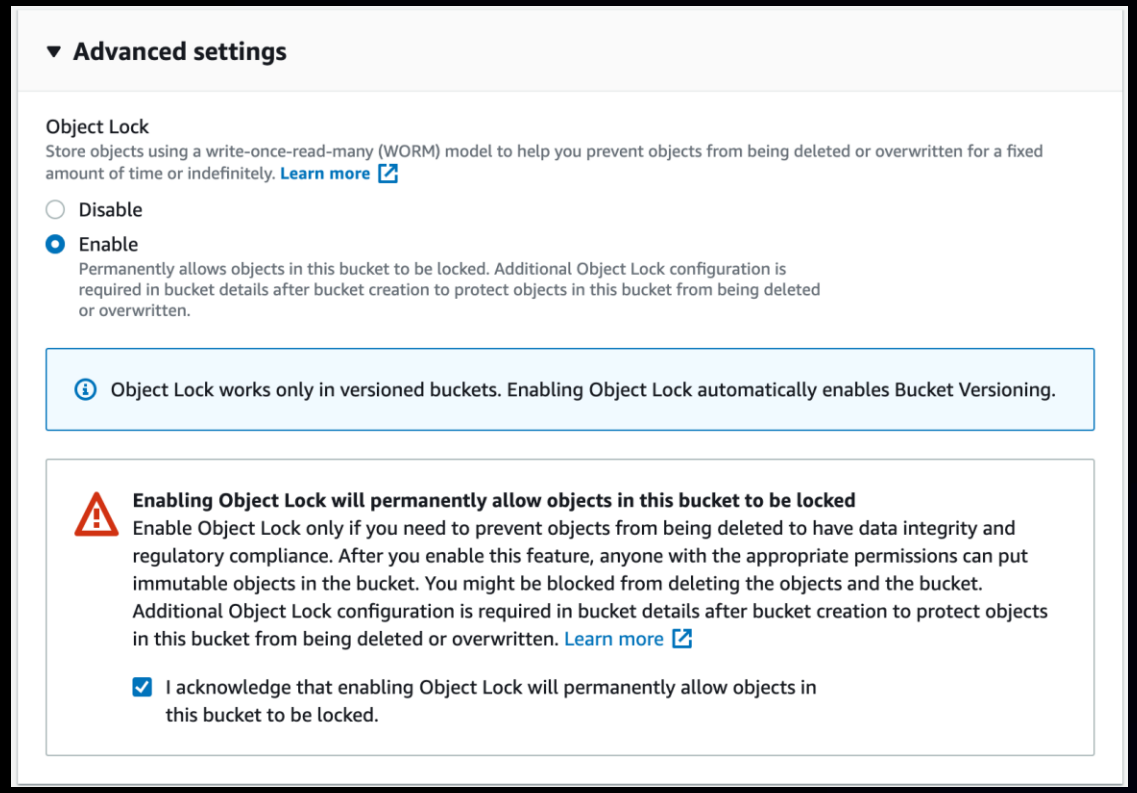
USE VAULTS AND LOCKS



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

Amazon S3 Object Lock and S3 Glacier Vault Lock

USE VAULTS AND LOCKS

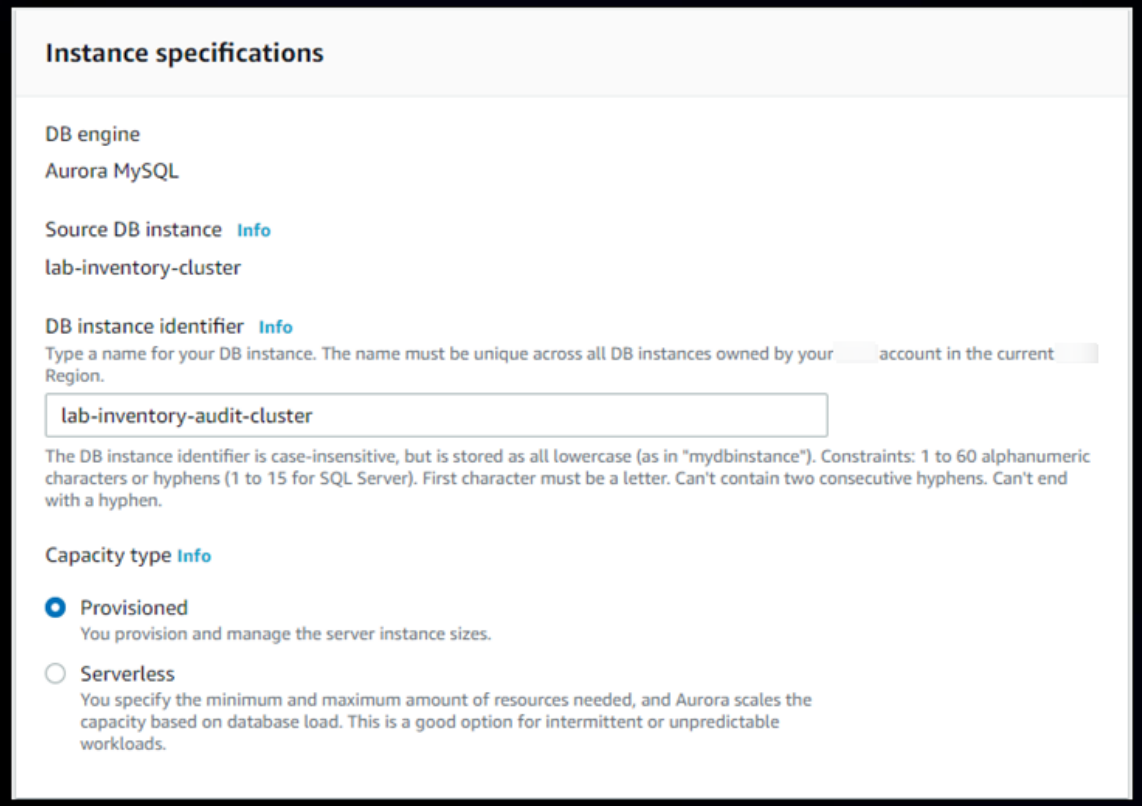


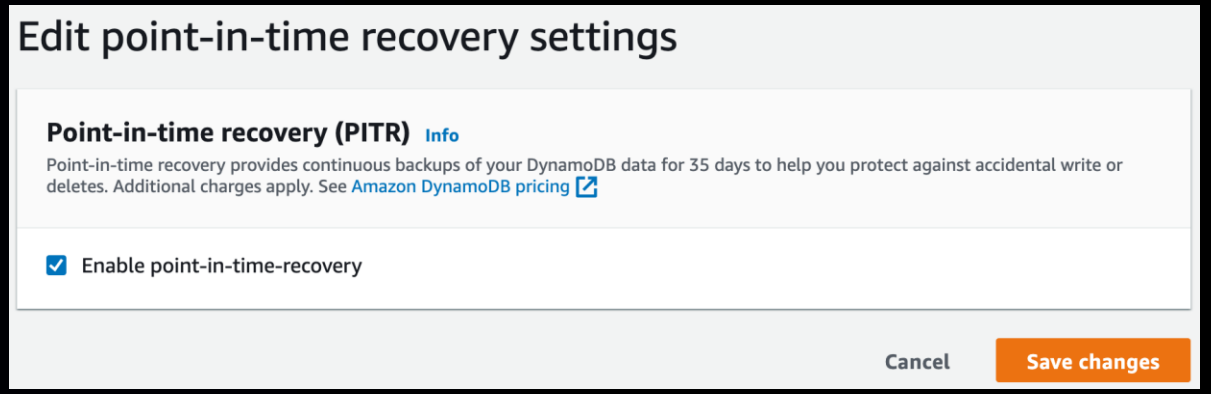

```
{
    "Version":"2012-10-17",
    "Statement":[
     {
        "Sid": "d
        "Principal": "*",
        "Effect": "Deny",
        "Action": "glacier:DeleteArchive",
        "Resource": [
           "arn:aws:glacier:us-west-2:123456789012:vaults/examplevault"
        ],
        "Condition": {
            "NumericLessThan" : {
                "glacier:ArchiveAgeInDays" : "365"
            }
        }
     }
   ]
}
```

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

Aurora Database Cloning and DynamoDB PITR

ADVANCED RECOVERY FEATURES





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

5.0 Streamline the use of environments and infrastructure

- Use managed services
- Use CI/CD & AMIs and rebuild systems frequently
- Utilize air-gap-like secure backup account architecture

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

Use managed services

THE BEST PATCHING IS PATCHING YOU DON'T HAVE TO DO

Managed by customers



Management protocols

API calls

Customer data

Client-side data encryption and data integrity authentication

Network traffic protection (encryption, integrity, identity)

Opaque data (Optional): 1s and 0s (in transit/at rest)

Firewall configuration

Customer IAM

IAM

Platform and applications management

Operating system, network configuration

AWS foundation services

Compute | Storage | Database | Networking

AWS Global Cloud Infrastructure

Availability Zones

Regions

Edge locations

API endpoints

Managed by aws

aws

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

Use CI/CD & AMIs and rebuild systems frequently

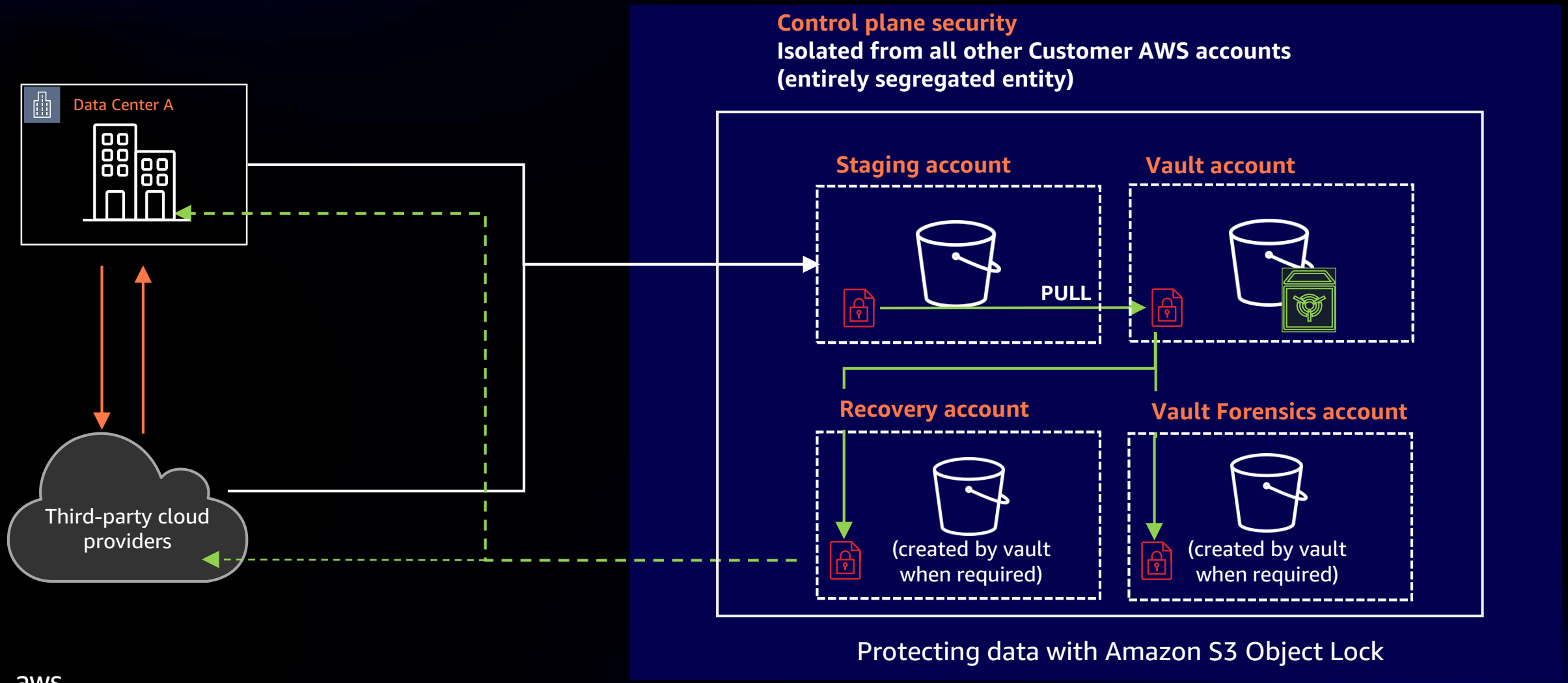
NOT PETS . . .





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

Utilize air-gap-like secure backup account architecture



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

That’s everything, right?

. . . not exactly.

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

Where can I go to learn more?

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

Resources

A FEW TO HIGHLIGHT

AWS

- AWS Cloud Security Resources Hub
  amzn.to/3gcnv6W
- Aligning to the NIST CSF in the AWS Cloud
  bit.ly/3AQc3WC
- AWS Well-Architected Framework – Security Pillar
  amzn.to/3m9bfI3
- Building a Threat Detection Strategy on AWS
  bit.ly/3k1GNNl
- AWS Security Incident Response Guide
  bit.ly/3sq7mj6
- AWS Compliance
  amzn.to/3srWEsD

Community

nomoreransom.org/en/index.html

U.S. federal government

- FBI IC3 – File a complaint
  www.ic3.gov
- The Cybersecurity and Infrastructure Security Agency (CISA) publications
  www.cisa.gov/stopransomware

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

Thank you!

Merritt Baer

merrbaer@amazon.com
@merrittbaer (Twitter)

Megan O'Neil

megoneil@amazon.com

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



Please complete the session survey

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