AWS re:Invent

SEC319-R

Deep dive on security in Amazon S3

Sam Parmett
Software Development Engineer, Amazon S3
Amazon Web Services

Felix Davis
Principal Product Manager, Amazon S3
Amazon Web Services

AWS re:Invent

aws

Agenda

Amazon S3 access controls overview

Amazon S3 Block Public Access

Amazon S3 Access Points NEW

Encryption support in Amazon S3

Layers of protection for data at rest

Monitoring and audit security in Amazon S3

Building a secure data lake on Amazon S3

Related breakouts

Wednesday, December 4

What’s new with Amazon S3 and Amazon Glacier

4:45 – 5:45 PM | MGM, Level 3, Premier Ballroom 313

Thursday, December 5

Amazon S3 security settings and controls

11:30 – 1:45 PM | Mirage, Montego E

Friday, December 6

DOP310-R1, Amazon’s approach to security during development

10:45 – 11:45 AM, Venetian, Level 5, Palazzo O

Access controls

- AWS Identity and Access Management (IAM)
- Amazon S3 bucket policy
- Amazon S3 object tags
- Amazon S3 access control lists

Boundary enforcement

- AWS Organizations
  Service Control Policy (SCP)
- Amazon S3 VPC endpoint policy
- Amazon S3 Block Public Access

Amazon S3 Block Public Access

- Four security settings
- Applicable at the account level or on individual buckets
- Use AWS Organizations SCPs to prevent settings changes

Amazon S3 Block Public Access settings

1. Block new public ACLs and the uploading of public objects
2. Remove public access granted through public ACLs
3. Block new public bucket policies
4. Block public and cross-account access to buckets with public policies

Announcing S3 Access Points

NEW

Launched at re:Invent 2019

SIMPLIFIED CONTROL FOR

SHARED BUCKETS

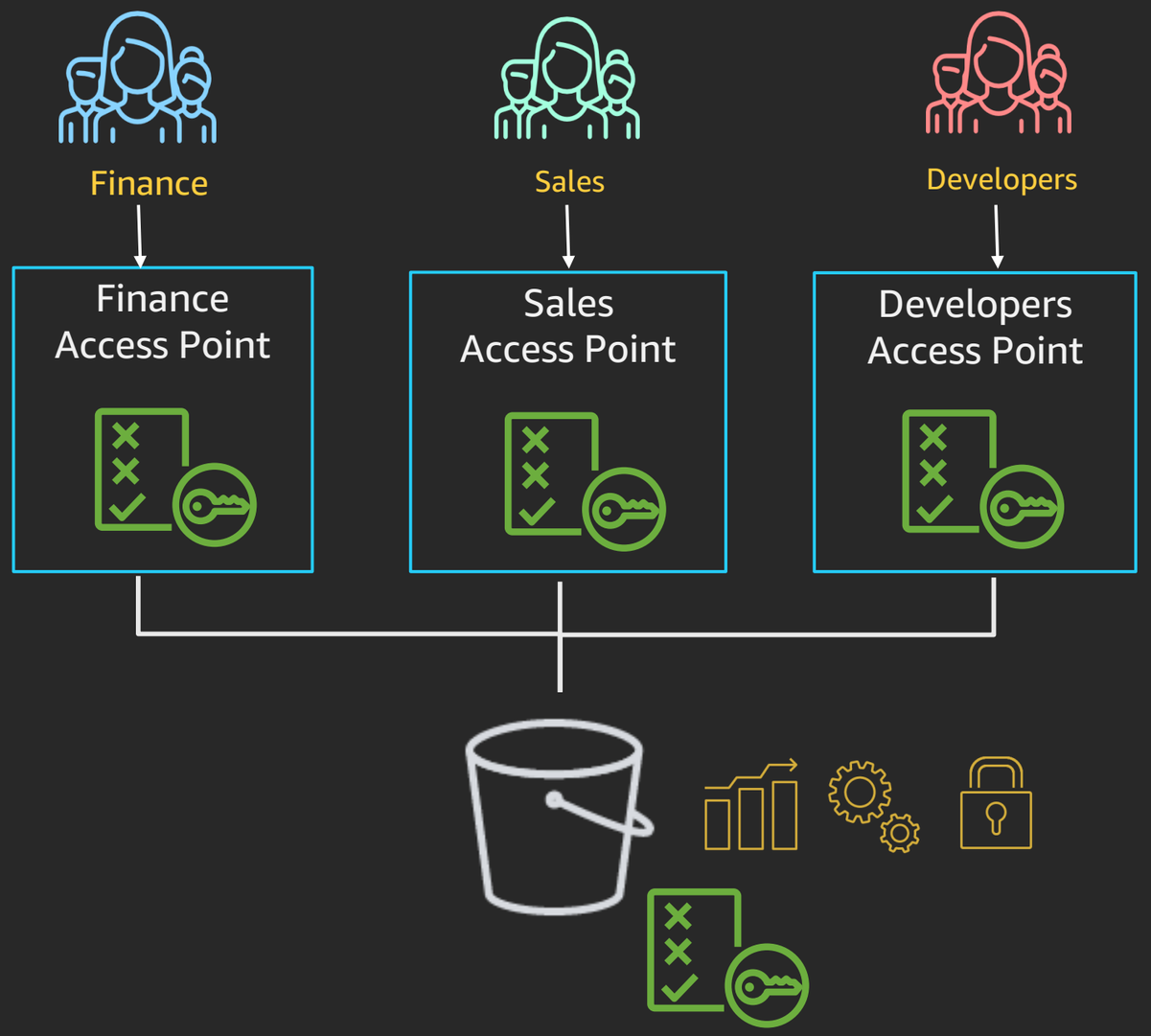
ACCESSED BY MANY TEAMS

USE CASES

DECENTRALIZED TEAMS

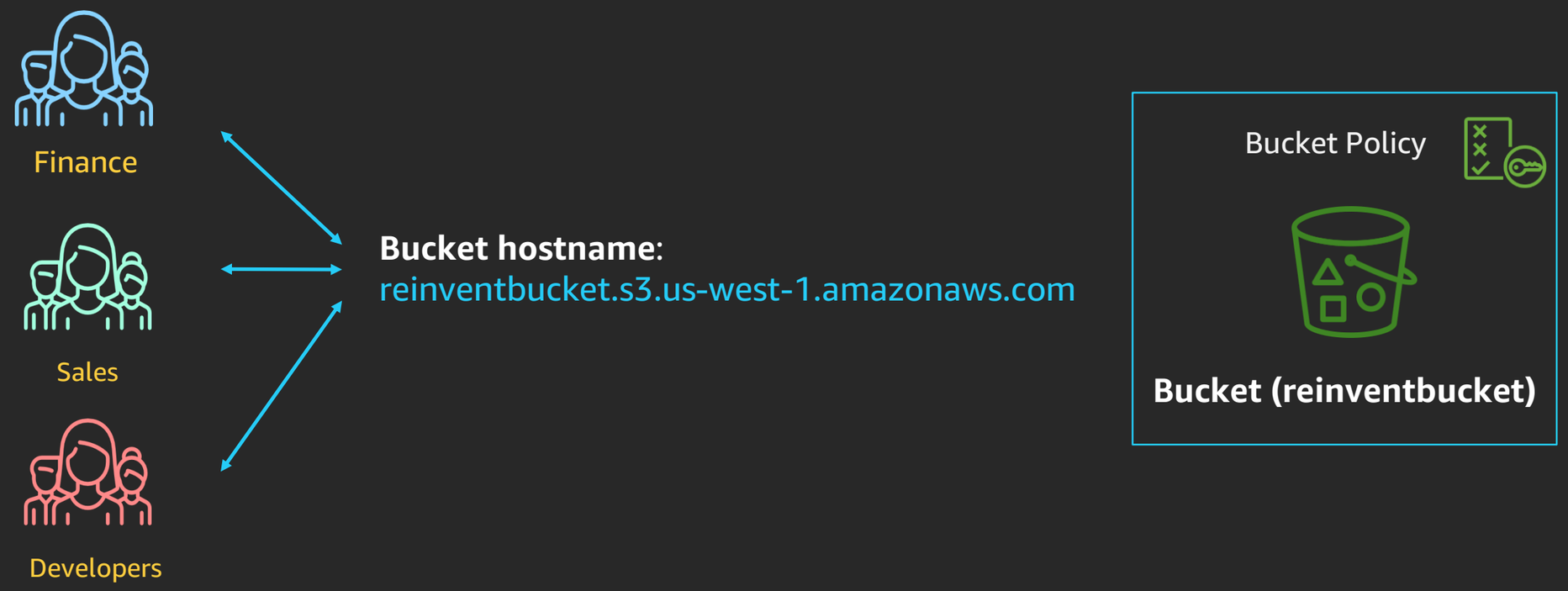
DATA LAKES

CROSS-ACCOUNT DATA EXCHANGE



Accessing objects in Amazon S3—Previously

All users would access objects directly through the bucket using the bucket hostname



What is an Amazon S3 Access Point?

A new Amazon S3 resource with a hostname, ARN, and resource policy

Access Point Name

S3 subdomain

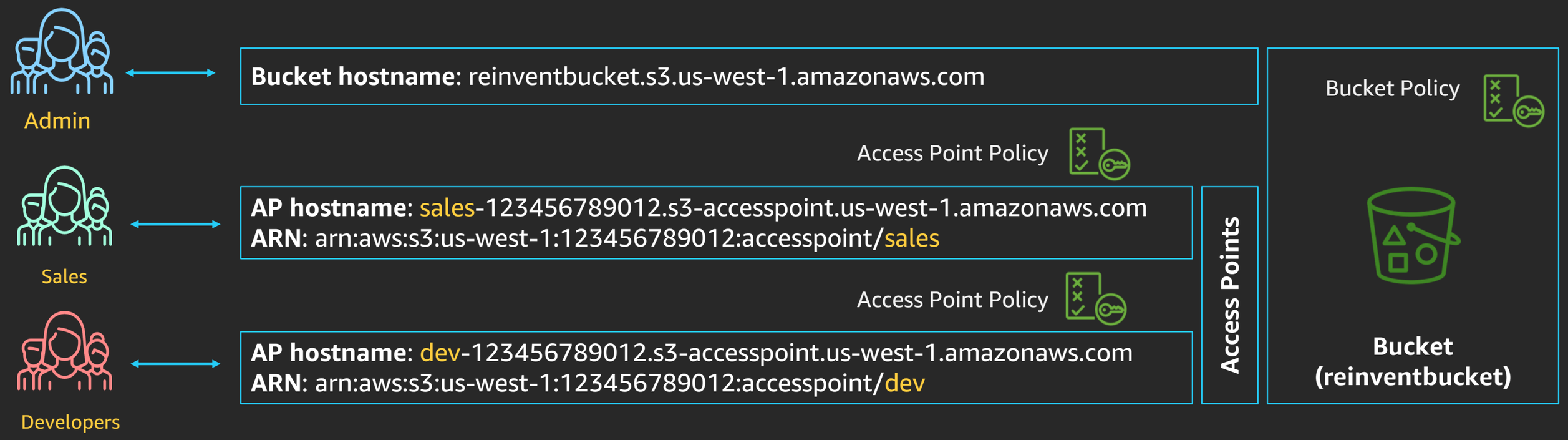
AP hostname: myap-123456789012.s3-accesspoint.us-west-1.amazonaws.com

AWS Account ID

ARN: arn:aws:s3:us-west-1:123456789012:accesspoint/myap

Accessing objects in Amazon S3 - Now

Users can access objects through dedicated Access Points in addition to the bucket directly



Amazon S3 encryption support

Encryption in transit — HTTPS/TLS

Encryption at rest

Server side
- SSE-S3 (Amazon S3 managed keys)
- SSE-KMS (AWS Key Management Service)
- SSE-C (customer-provided keys)

Client side
- Encrypt with the AWS Encryption SDK

Amazon S3 Default Encryption for S3 Buckets

One-time bucket-level setup

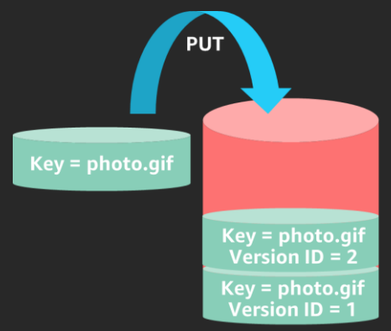
Automatically encrypts all new objects

Simplified compliance

Supports SSE-S3 and SSE-KMS

Layers of protection for your data

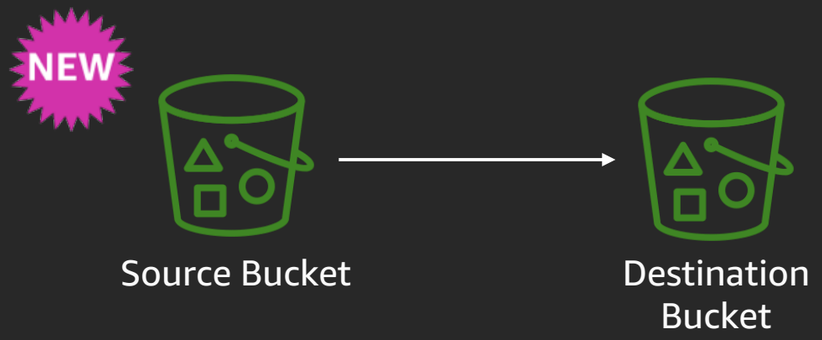
Best practices to prevent incidental and malicious data deletion



Versioning

Object Lock

Multi-Factor-Authentication



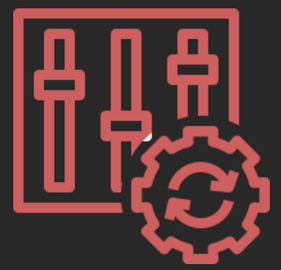
Replication (CRR, SRR)

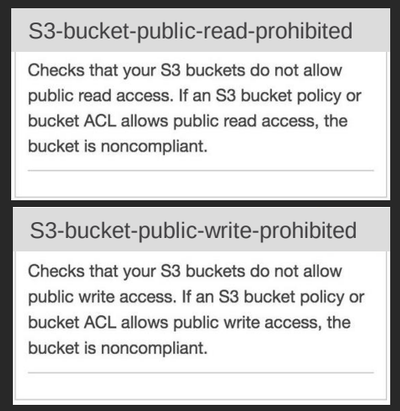
Monitoring Amazon S3 security settings

IAM Access Analyzer

AWS CloudTrail
Amazon S3 Server Access Logs

Object encryption status
Amazon S3 Inventory



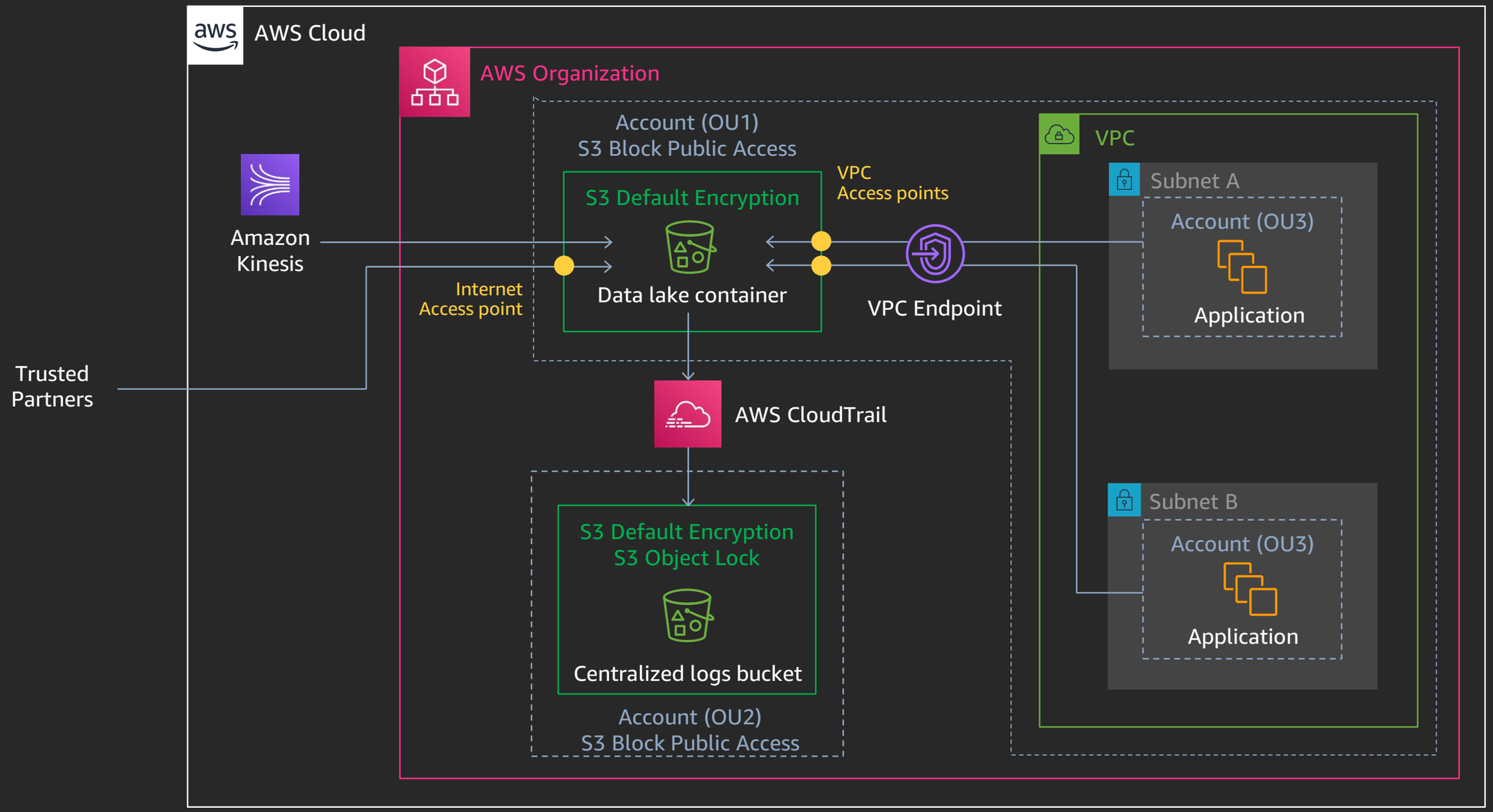


AWS Config rules

Data lake security model – First principles

- High cardinality set of users, ingestion & analysis pipelines
- Secure data at rest and in transit
- Principle of least privilege for data permissions
    - Deny as a default
    - Allow access where appropriate
- Monitor security controls and access patterns
    - Configuration drift
    - Anomalous access

Reference architecture



Takeaways - Amazon S3 security best practices

- Enable account-level Block Public Access
- Leverage Access Points to scope application permissions
- Send secure traffic with VPC endpoints
- Use bucket policy to enforce TLS
- Encrypt everything: SSE-KMS & SSE-S3
- Enable Object Lock, Versioning, MFA delete to protect data
- Monitor using AWS tools, such as AWS CloudTrail and AWS Config

Learn security with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate cloud security skills

30+ free digital courses cover topics related to cloud security, including Introduction to Amazon GuardDuty and Deep Dive on Container Security

Classroom offerings, like AWS Security Engineering on AWS, feature AWS expert instructors and hands-on activities

Validate expertise with the **AWS Certified Security - Specialty** exam

Visit aws.amazon.com/training/paths-specialty/

aws training and certification

Thank you!

Sam Parmett
sparmett@amazon.com

Felix Davis
felixdav@amazon.com

AWS re:Invent

aws

Please complete the session survey in the mobile app.

AWS re:Invent

aws