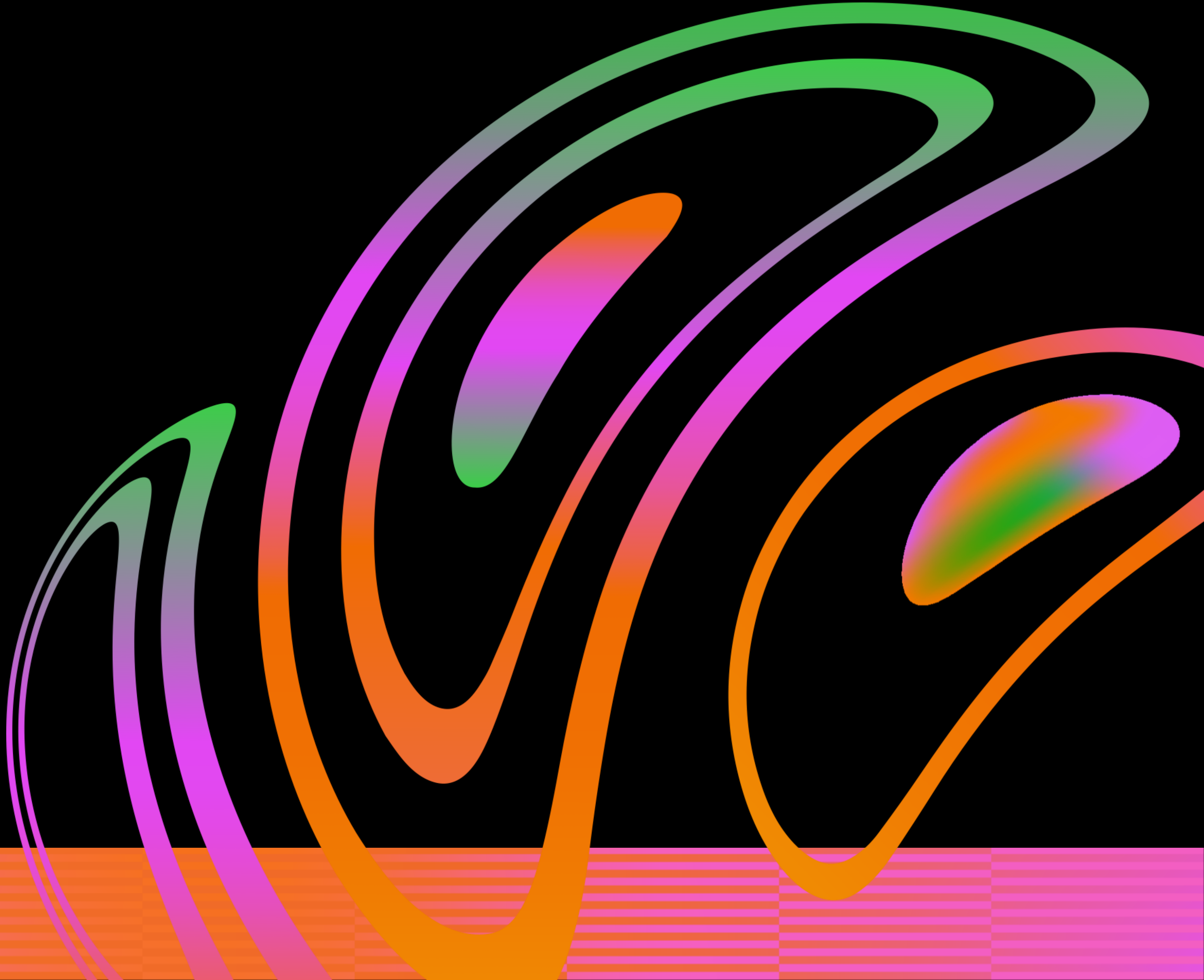
AWS re:Invent



STG305

# A defense-in-depth approach to Amazon S3 security and access

Paul Meighan

Product Manager, Amazon S3
AWS

AWS re:Invent

# What is defense-in-depth

Access Controls

Block Public Access

Encryption

Data protection

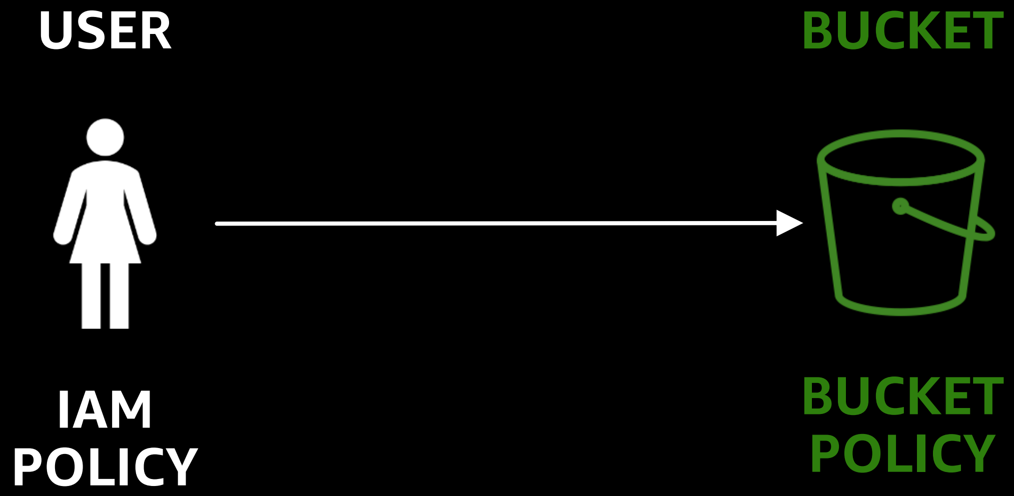
Access Controls

Block Public Access

Encryption

Data protection

# Starting simple: IAM and bucket policies



# IAM policy example

*A simple policy to allow a user to read and write to a bucket called reinvent-bucket*

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::/reinvent-bucket/*"
        }
    ]
}
```

# IAM policy example

*A simple policy to allow a user to read and write to a bucket called reinvent-bucket*

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "s3:PutObject",
            "s3:GetObject"
         ],
         "Resource": "arn:aws:s3:::/reinvent-bucket/*"
      }
   ]
}
```

**Effect – specifies whether the statement results in an allow or an explicit deny**

# IAM policy example

*A simple policy to allow a user to read and write to a bucket called reinvent-bucket*

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::/reinvent-bucket/*"
        }
    ]
}
```

**Action – specifies the action** that will be allowed or denied

*(An S3 GET or PUT request, in this case)*

# IAM policy example

*A simple policy to allow a user to read and write to a bucket called reinvent-bucket*

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::/reinvent-bucket/*"
        }
    ]
}
```

**Resource – specifies what** the statement covers

*(A bucket named reinvent-bucket, in this case)*

# Starting simple: IAM and bucket policies

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::/reinvent-bucket/*"
        }
    ]
}
```

*“These users are allowed to read and write objects to that bucket”*

403 ACCESS DENIED

PRIVATE BY DEFAULT

# Bucket policy example

*Same syntax and language, with one additional required element*

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "s3:PutObject",
            "s3:GetObject"
         ],
         "Resource": "arn:aws:s3:::/reinvent-bucket/*”,
         ”Principal”: {"AWS":"1111111111"} ←
      }
   ]
}
```

**<u>Principal</u> – specifies who** the statement covers

*(Fake AWS Account ID 1111111111, in this case)*

# Bucket policy example

Valid principals for your bucket policies include:

- AWS account and root user
- IAM users
- Federated users (using web identity or SAML federation)
- IAM roles
- Assumed-role sessions
- AWS services
- Anonymous users (not recommended)

# Starting simple: IAM and bucket policies

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::/reinvent-bucket/*"
        }
    ]
}
```

*“These users can read and write objects to that bucket”*

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::/reinvent-bucket/*”,
            ”Principal”:{"AWS":"1111111111"}
        }
    ]
}
```

*“This bucket can be read and written to by that account”*

# Adding granularity with condition keys

## S3 bucket policies

*Who can access the contents of this bucket?*

*Limit the scope of access to objects that have a Project:reInvent tag*

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
       "Effect":”Allow",
       "Action":[
               "s3:PutObject",
               "s3:GetObject"
         ],
       "Resource":"arn:aws:s3:::reinvent-bucket/*”,
       ”Principal”:{"AWS":"1111111111"},
       "Condition": {
               "StringEquals":{"s3:ExistingObjectTag/Project":”reInvent"}
       }
      }
   ]
}
```

# Adding granularity with condition keys

## A condition key for every occasion:

aws:RequestTag/${TagKey}
s3:object-lock-legal-hold
aws:ResourceTag/${TagKey}
s3:object-lock-mode
aws:TagKeys
s3:object-lock-remaining-retention-days
s3:AccessPointNetworkOrigin
s3:object-lock-retain-until-date
s3:DataAccessPointAccount
s3:prefix
s3:DataAccessPointArn
s3:signatureAge
s3:ExistingJobOperation
s3:signatureversion
s3:ExistingJobPriority
s3:versionid
s3:locationconstraint
s3:max-keys
s3:x-amz-website-redirect-location

s3:ExistingObjectTag/<key>
s3:x-amz-acl
s3:JobSuspendedCause
s3:x-amz-content-sha256
s3:LocationConstraint
s3:x-amz-copy-source
s3:RequestJobOperation
s3:x-amz-grant-full-control
s3:RequestJobPriority
s3:x-amz-grant-read
s3:RequestObjectTag/<key>
s3:x-amz-grant-read-acp
s3:RequestObjectTagKeys
s3:x-amz-grant-write
s3:VersionId
s3:x-amz-grant-write-acp
s3:authType
s3:x-amz-metadata-directive
s3:x-amz-server-side-encryption-aws-kms-key-id
s3:x-amz-storage-class

For detailed descriptions and non-tiny text:
*https://docs.aws.amazon.com/IAM/latest/UserGuide/list_amazons3.html*

I’m allowed to write to that bucket, *but should I?*

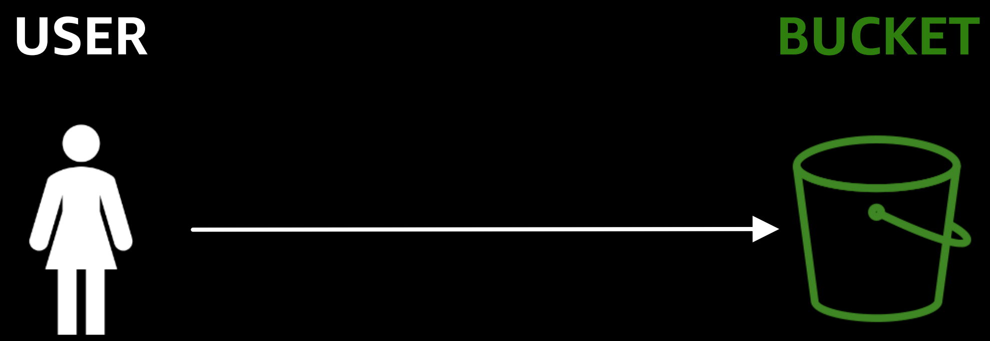
# Enforcing bucket ownership controls

NEW

Bucket owner condition

```
x-amz-expected-bucket-owner
=
111111111111
```

*“This request will only succeed against buckets in that account”*



USER

BUCKET

```
Bucket: reinvent-bucket
Owner: 111111111111
```

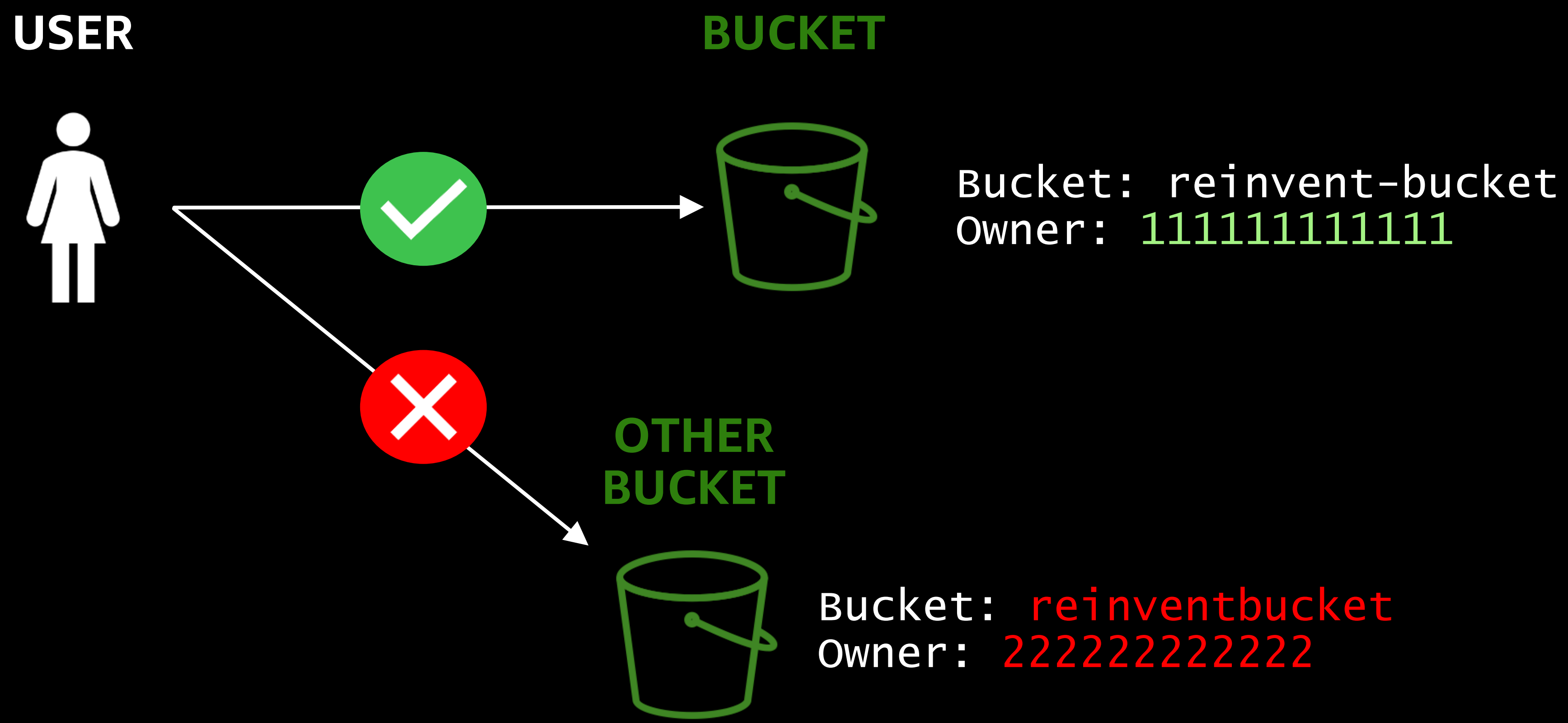
# Enforcing bucket ownership controls

NEW

Bucket owner condition

```
x-amz-expected-bucket-owner
=
111111111111
```

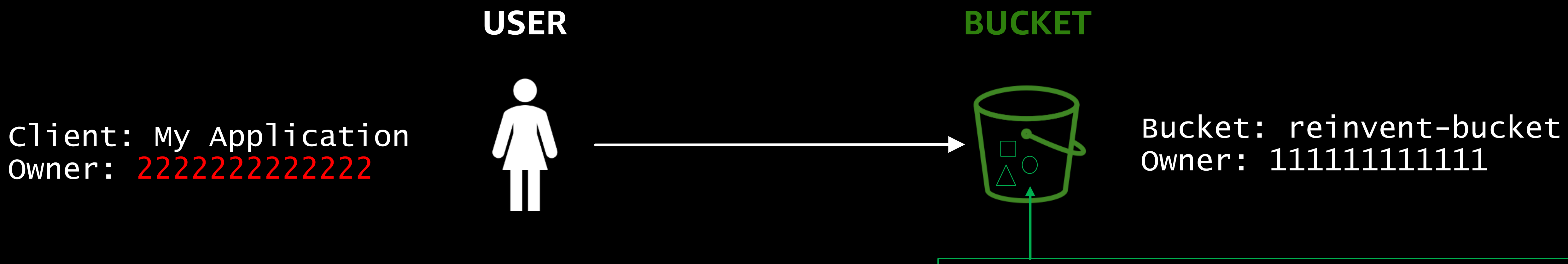
*“This request will only succeed against buckets in that account”*



```
Bucket: reinvent-bucket
Owner: 111111111111
```

```
Bucket: reinventbucket
Owner: 222222222222
```

# Enforcing object ownership controls



Client: My Application
Owner: 2222222222222

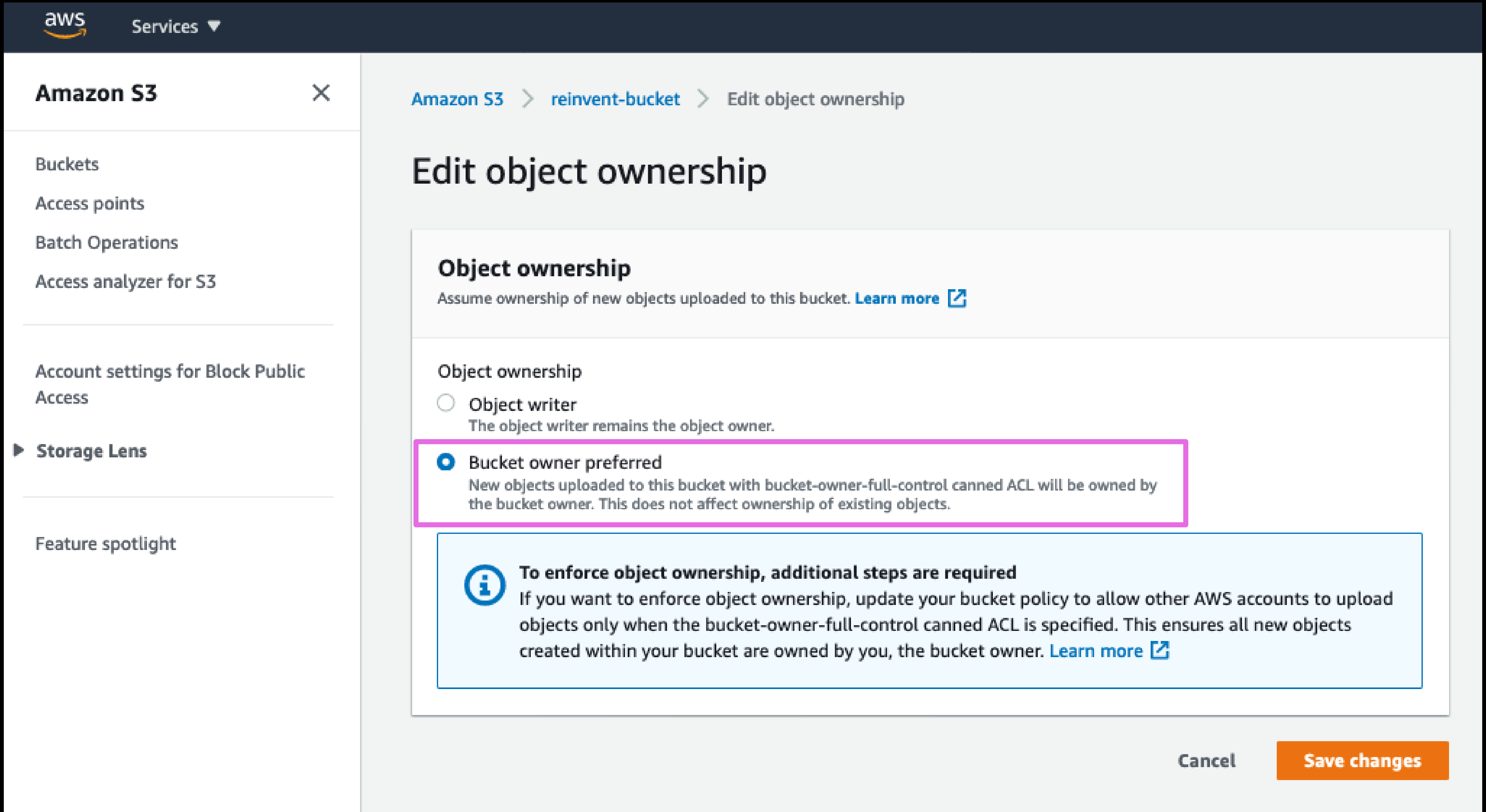
Bucket: reinvent-bucket
Owner: 111111111111

By default, these objects:

- Are owned by the writer (222222222222)
- Can't be read by the bucket owner
- Can never be shared with other accounts

# Enforcing object ownership controls

NEW



## Edit object ownership

### Object ownership

Assume ownership of new objects uploaded to this bucket. Learn more

Object ownership

○ Object writer
The object writer remains the object owner.

● Bucket owner preferred
New objects uploaded to this bucket with bucket-owner-full-control canned ACL will be owned by the bucket owner. This does not affect ownership of existing objects.

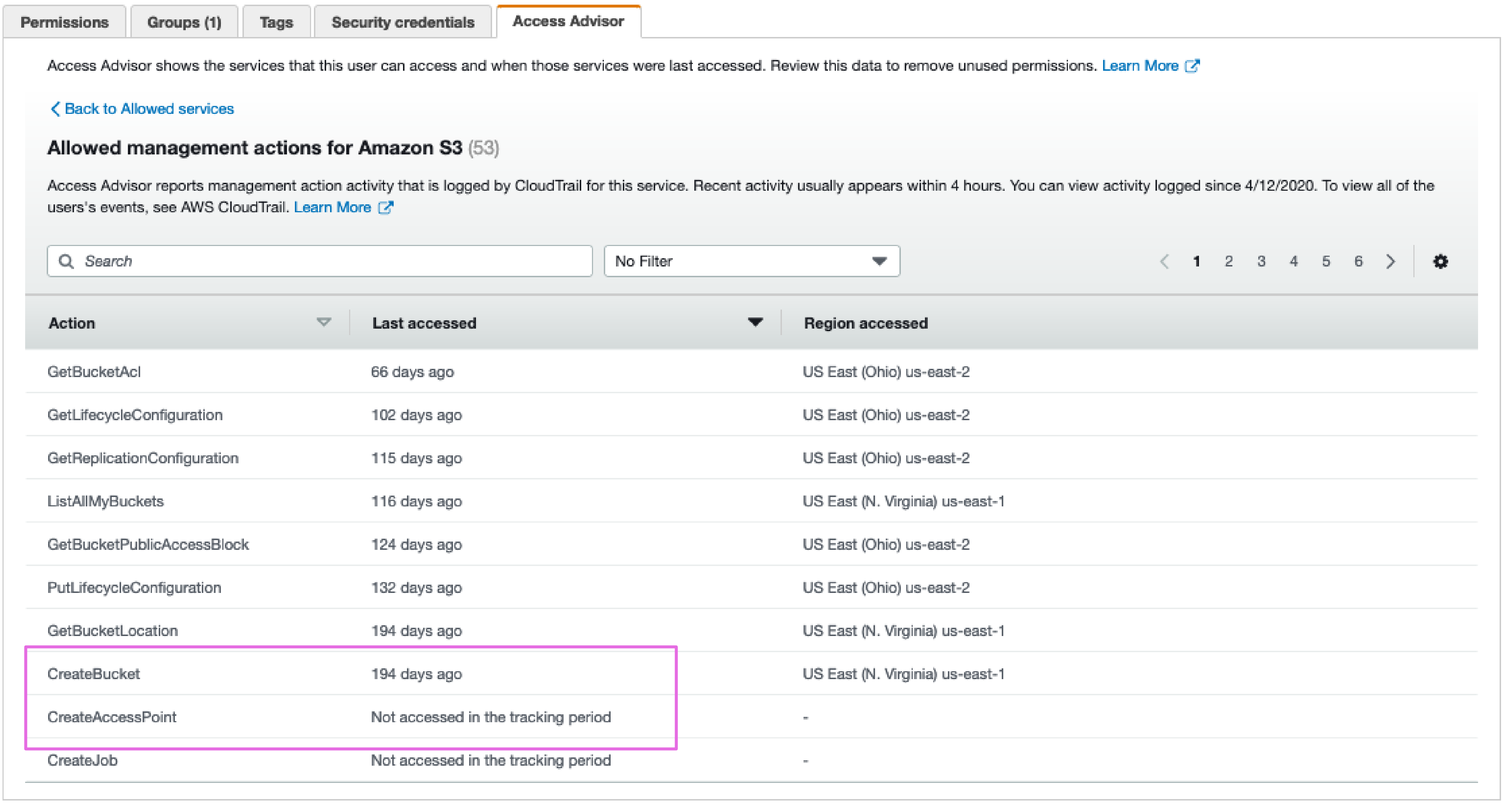
**To enforce object ownership, additional steps are required**
If you want to enforce object ownership, update your bucket policy to allow other AWS accounts to upload objects only when the bucket-owner-full-control canned ACL is specified. This ensures all new objects created within your bucket are owned by you, the bucket owner. Learn more

# Limiting the privileges of a user

USER
root please.
BUCKET

# S3 last action accessed

NEW



Access Advisor shows the services that this user can access and when those services were last accessed. Review this data to remove unused permissions. Learn More

< Back to Allowed services

**Allowed management actions for Amazon S3** (53)

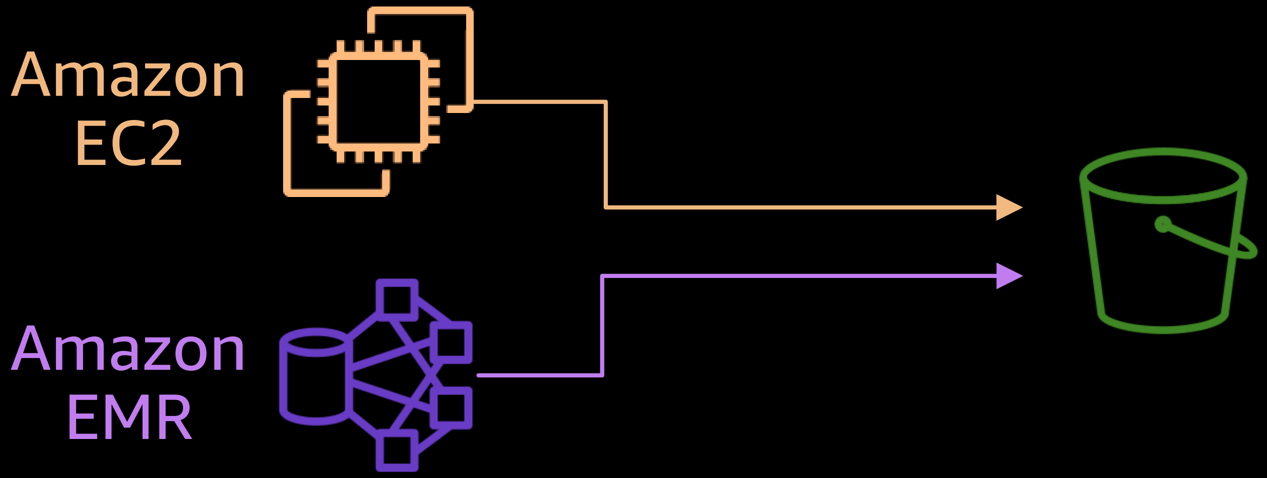
Access Advisor reports management action activity that is logged by CloudTrail for this service. Recent activity usually appears within 4 hours. You can view activity logged since 4/12/2020. To view all of the users's events, see AWS CloudTrail. Learn More

| Action | Last accessed | Region accessed |
|---|---|---|
| GetBucketAcl | 66 days ago | US East (Ohio) us-east-2 |
| GetLifecycleConfiguration | 102 days ago | US East (Ohio) us-east-2 |
| GetReplicationConfiguration | 115 days ago | US East (Ohio) us-east-2 |
| ListAllMyBuckets | 116 days ago | US East (N. Virginia) us-east-1 |
| GetBucketPublicAccessBlock | 124 days ago | US East (Ohio) us-east-2 |
| PutLifecycleConfiguration | 132 days ago | US East (Ohio) us-east-2 |
| GetBucketLocation | 194 days ago | US East (N. Virginia) us-east-1 |
| CreateBucket | 194 days ago | US East (N. Virginia) us-east-1 |
| CreateAccessPoint | Not accessed in the tracking period | - |
| CreateJob | Not accessed in the tracking period | - |

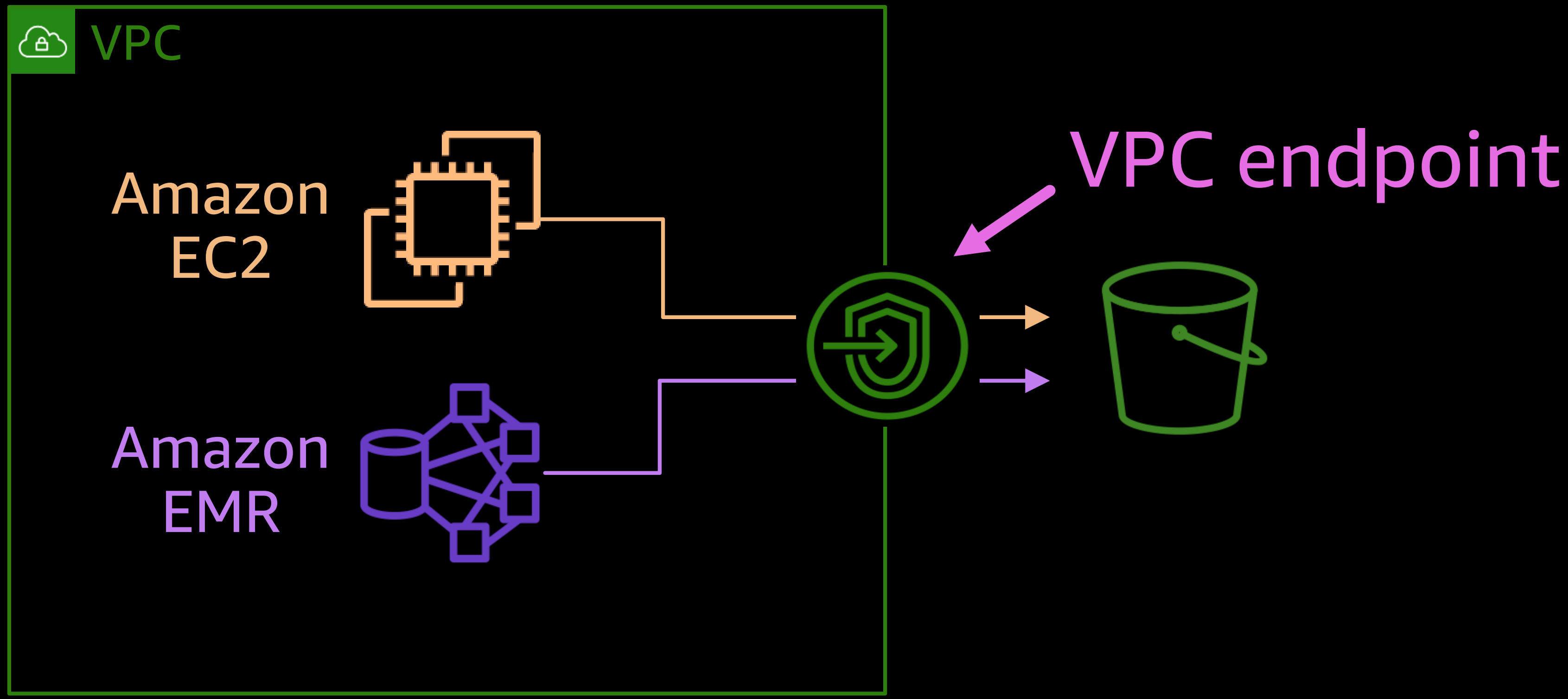
This user hasn’t created a bucket in 194 days and has never created an Access Point

*Do they need those permissions?*

# More, higher-end applications

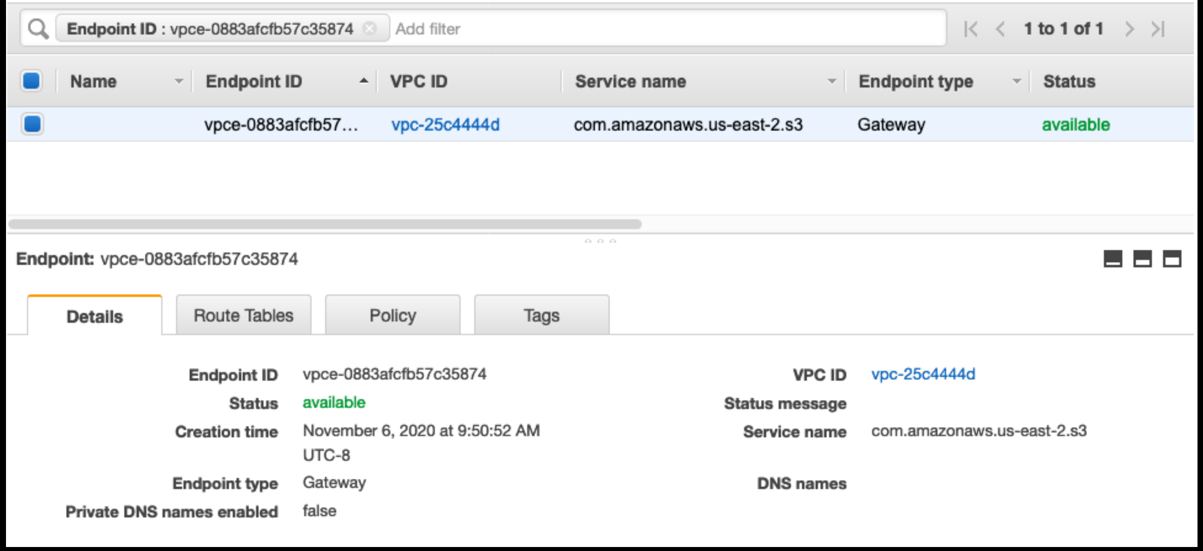


# Enter the network



# VPC endpoints

## Gateway endpoints



| Name | Endpoint ID | VPC ID | Service name | Endpoint type | Status |
|---|---|---|---|---|---|
|  | vpce-0883afcfb57… | vpc-25c4444d | com.amazonaws.us-east-2.s3 | Gateway | available |

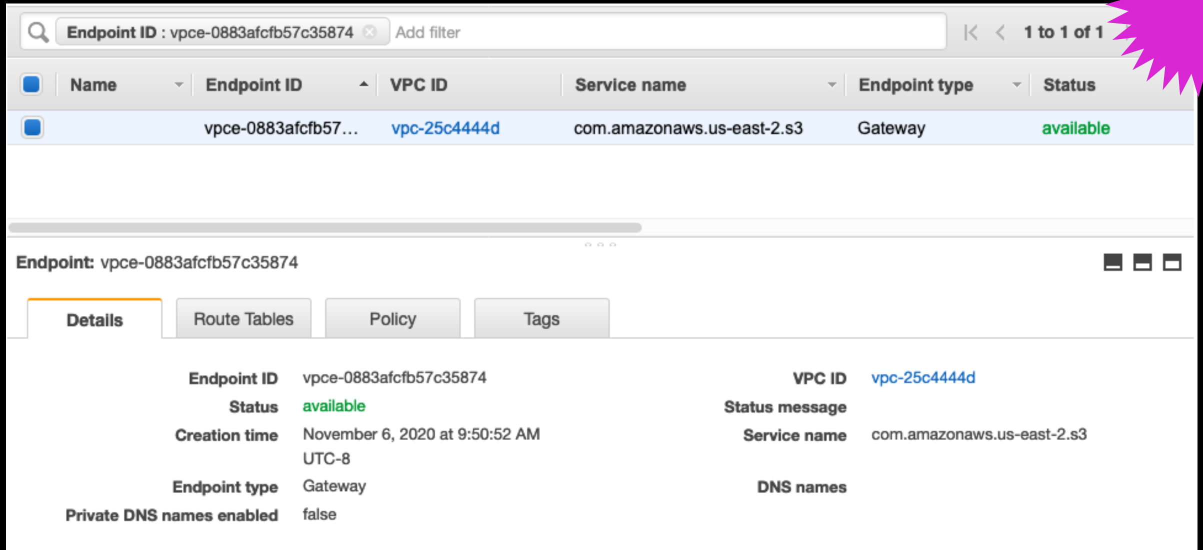
Endpoint: vpce-0883afcfb57c35874

Endpoint ID vpce-0883afcfb57c35874
Status available
Creation time November 6, 2020 at 9:50:52 AM UTC-8
Endpoint type Gateway
Private DNS names enabled false
VPC ID vpc-25c4444d
Status message
Service name com.amazonaws.us-east-2.s3
DNS names

- Clients use public S3 IP addresses
- The route table for your VPC is updated so that all S3 requests go through the endpoint
- No support for on-premises applications or cross-region requests
- Free of charge

## Interface endpoints

*Based on AWS PrivateLink*



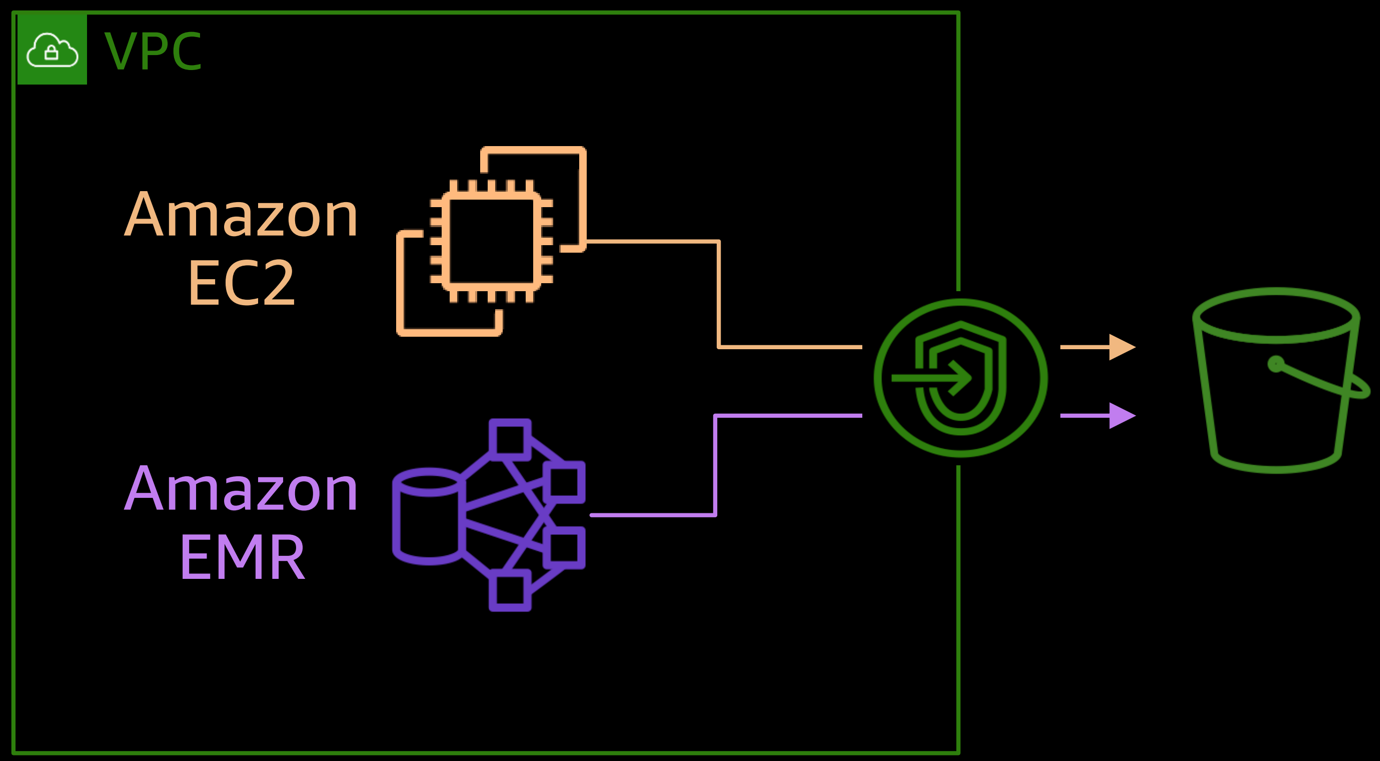
| Name | Endpoint ID | VPC ID | Service name | Endpoint type | Status |
|---|---|---|---|---|---|
|  | vpce-0883afcfb57… | vpc-25c4444d | com.amazonaws.us-east-2.s3 | Gateway | available |

Endpoint: vpce-0883afcfb57c35874

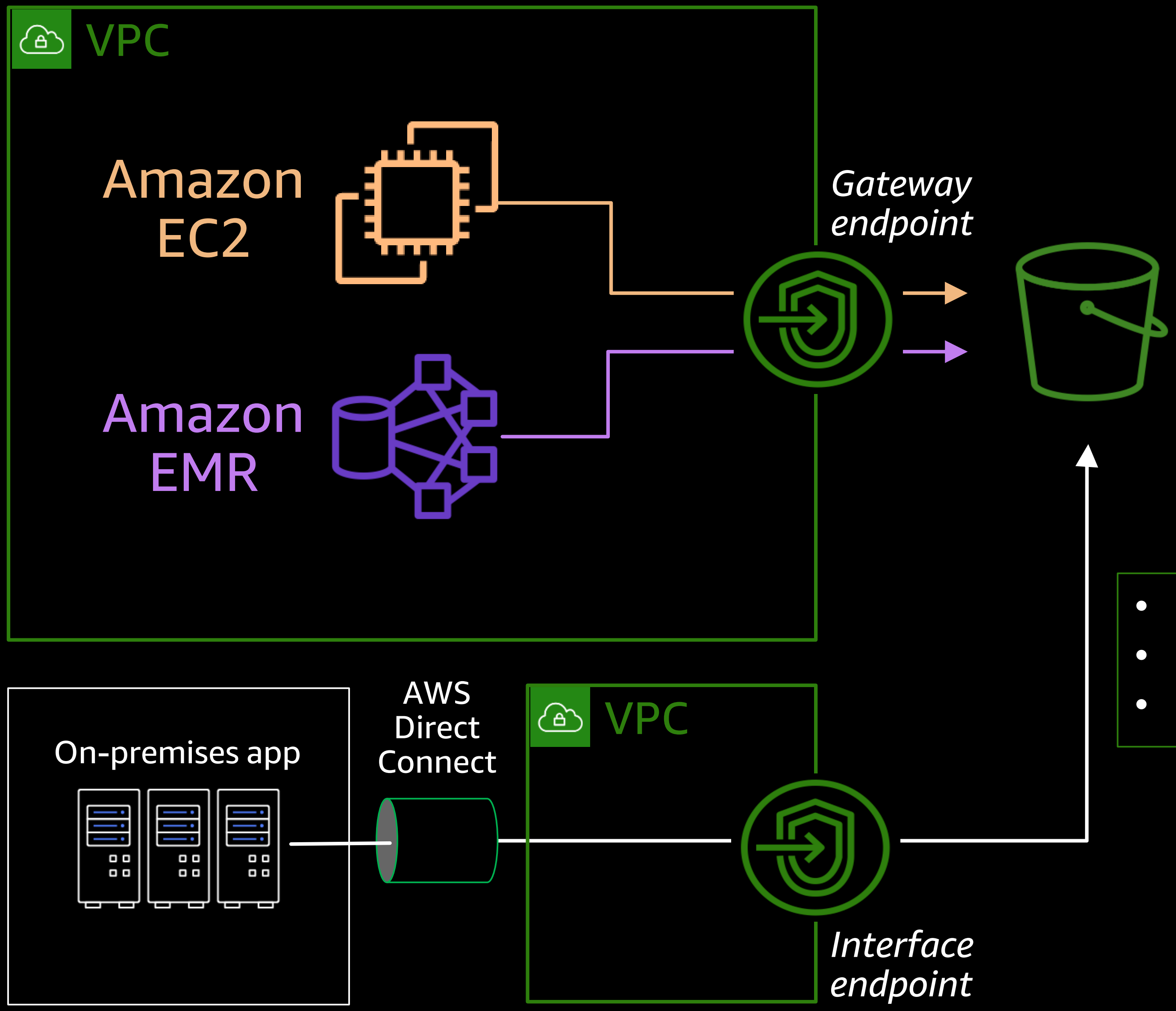
Endpoint ID vpce-0883afcfb57c35874
Status available
Creation time November 6, 2020 at 9:50:52 AM UTC-8
Endpoint type Gateway
Private DNS names enabled false
VPC ID vpc-25c4444d
Status message
Service name com.amazonaws.us-east-2.s3
DNS names

- Clients use IP addresses from your VPC
- DNS records in your VPC are updated so that all S3 requests go through the endpoint
- Support for on-premises applications and cross-region requests
- Paid feature

# Coming soon: Amazon S3 support for AWS PrivateLink

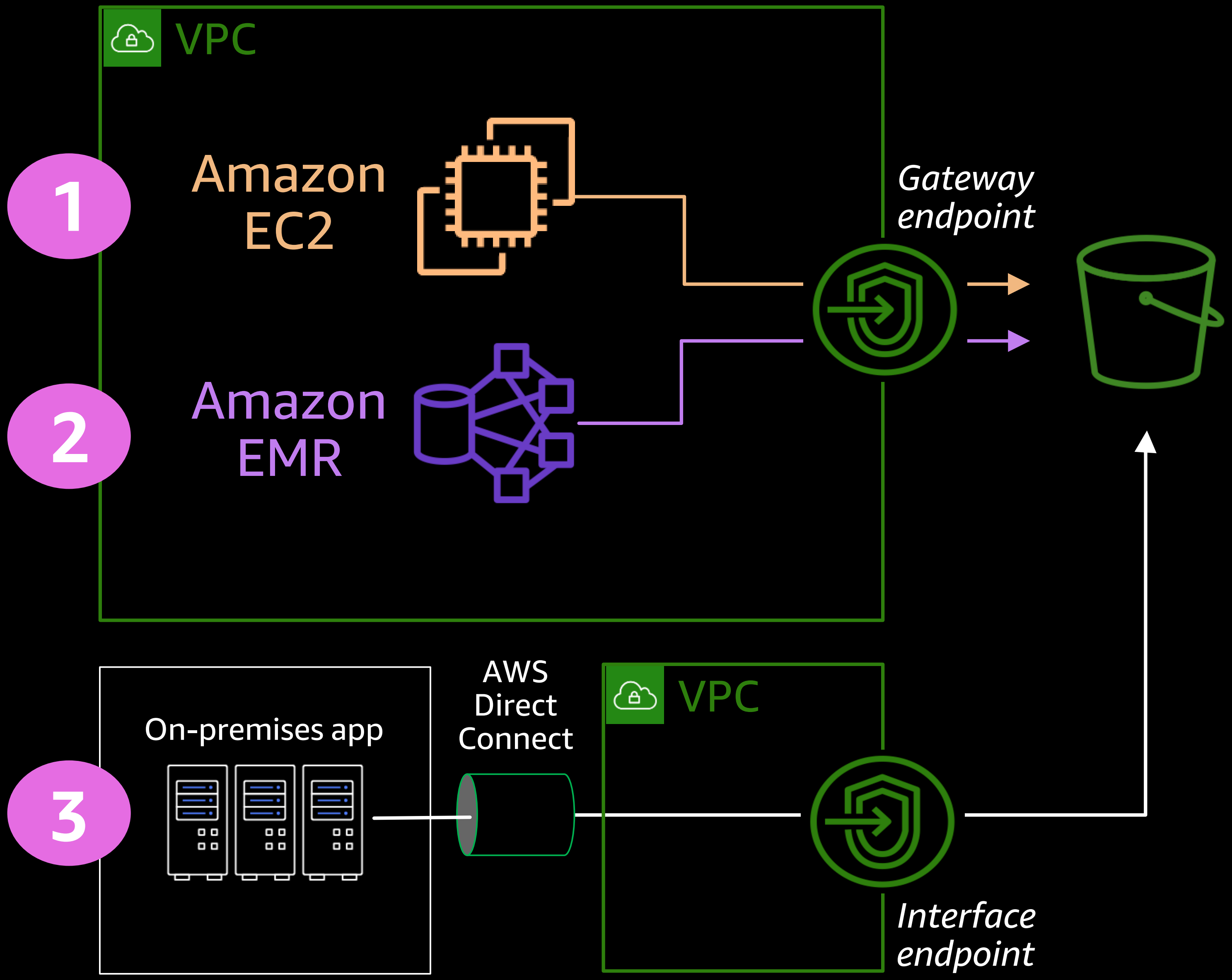


# Coming soon: Amazon S3 support for AWS PrivateLink

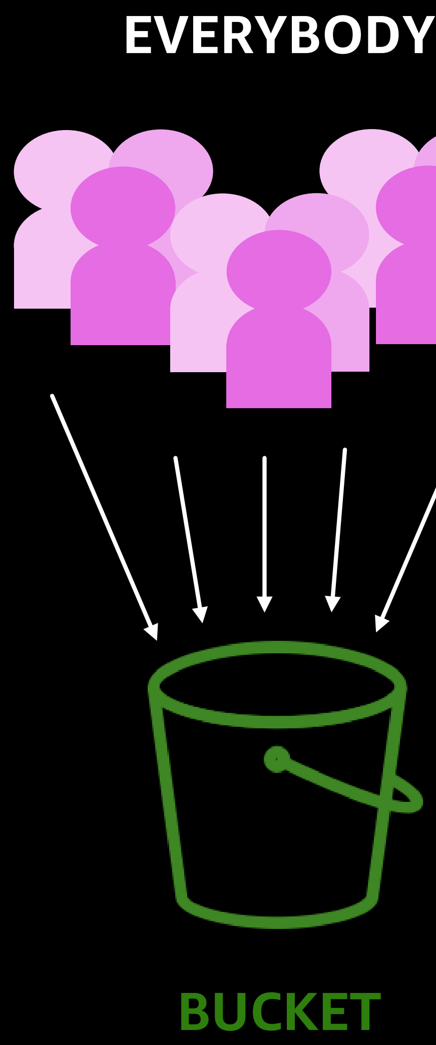


- Simple network architecture
- Connections avoid the public internet
- Additional visibility and access control

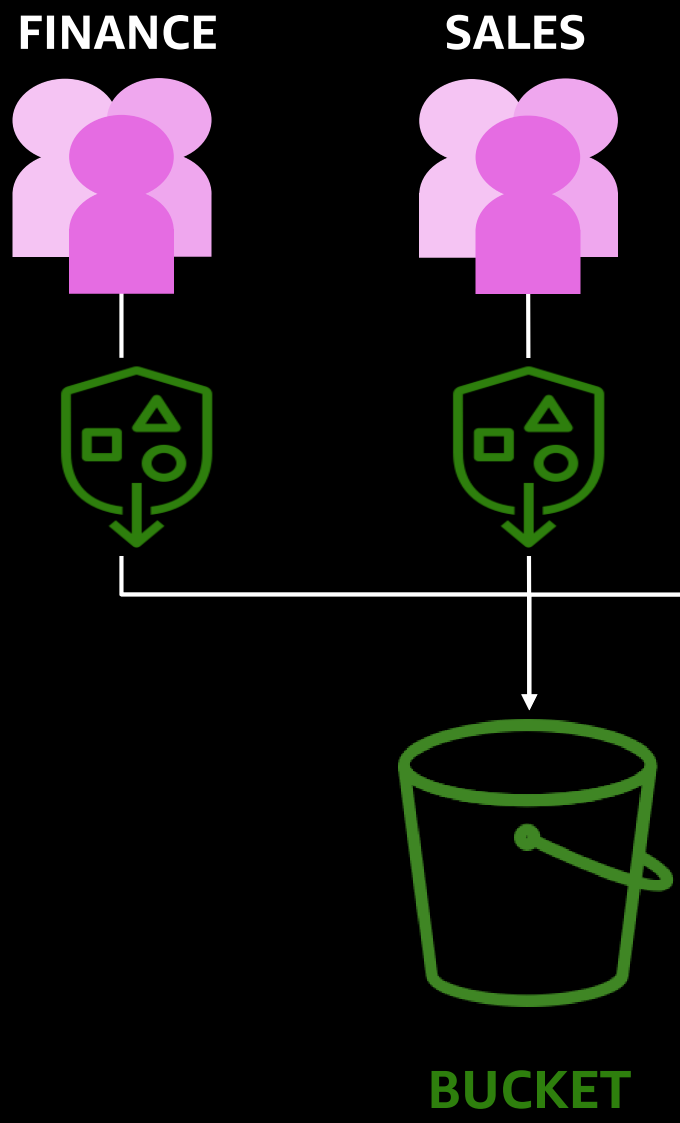
# Access controls for shared datasets



# Access controls for shared datasets

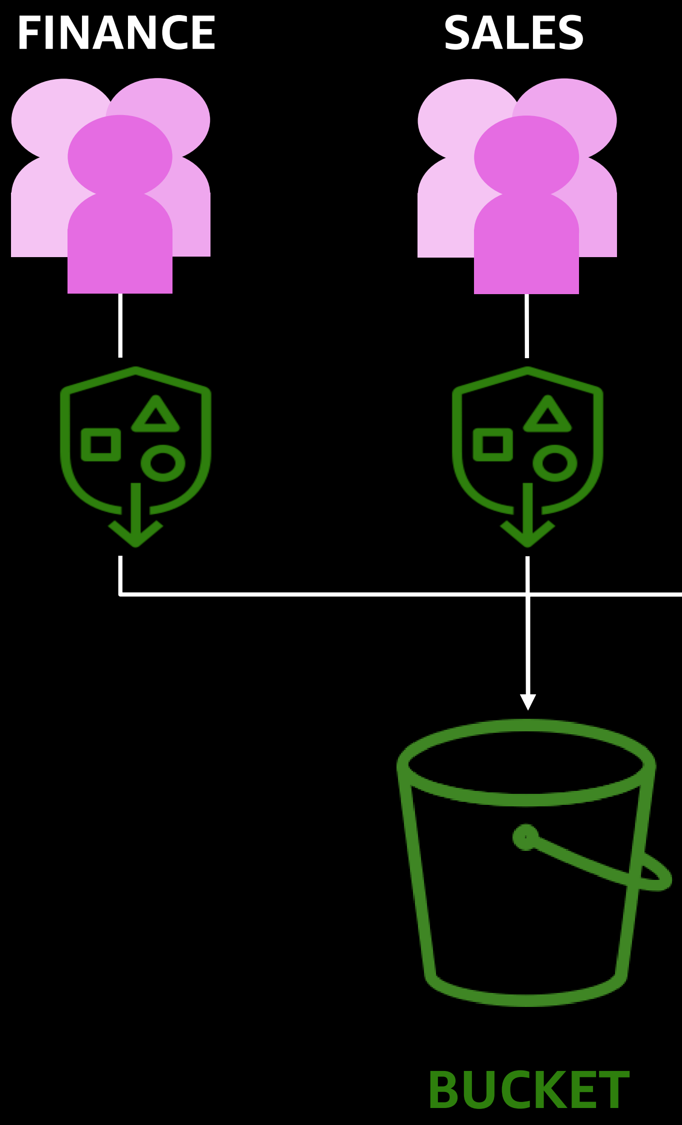


# S3 Access Points

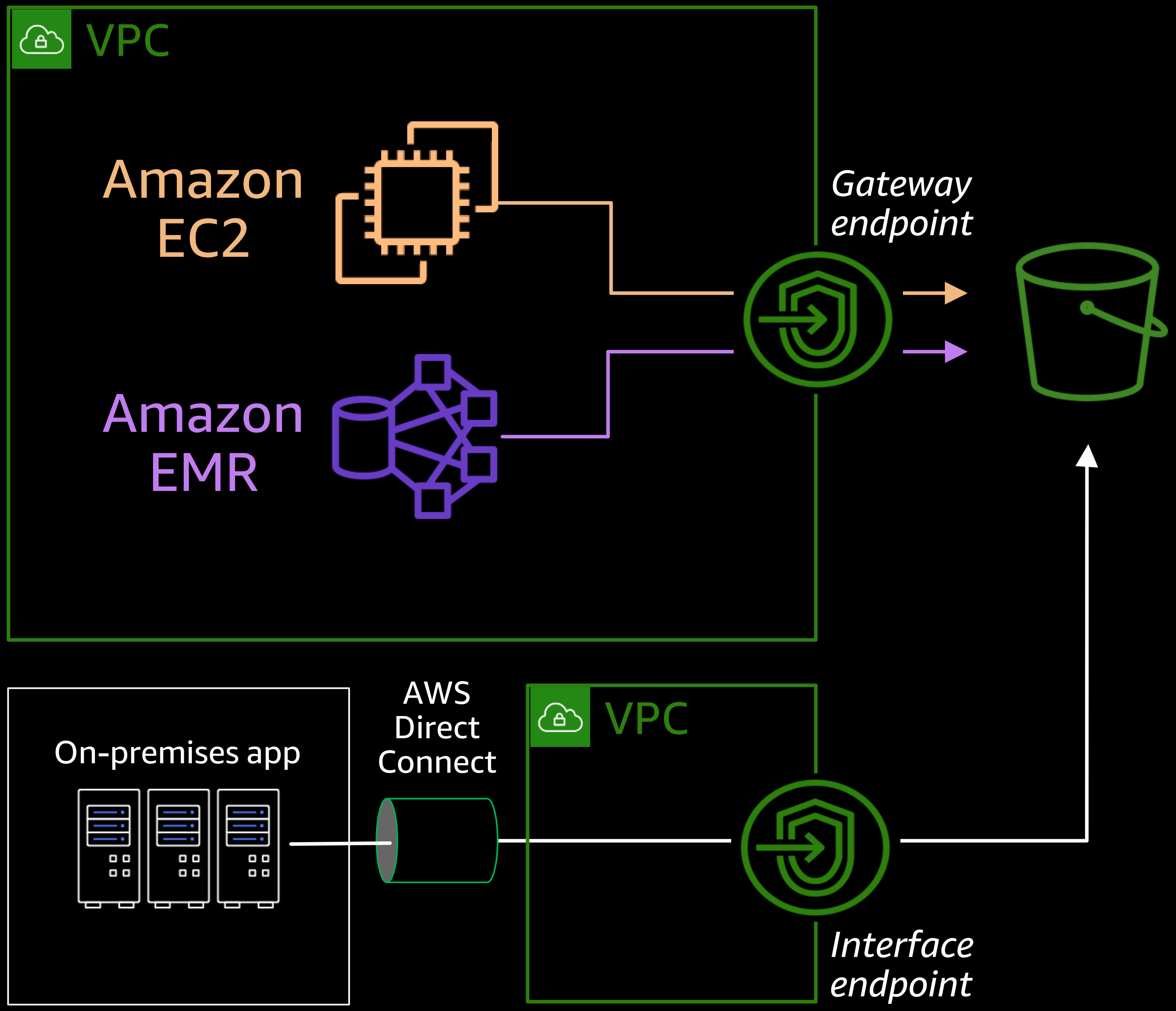


# S3 Access Points

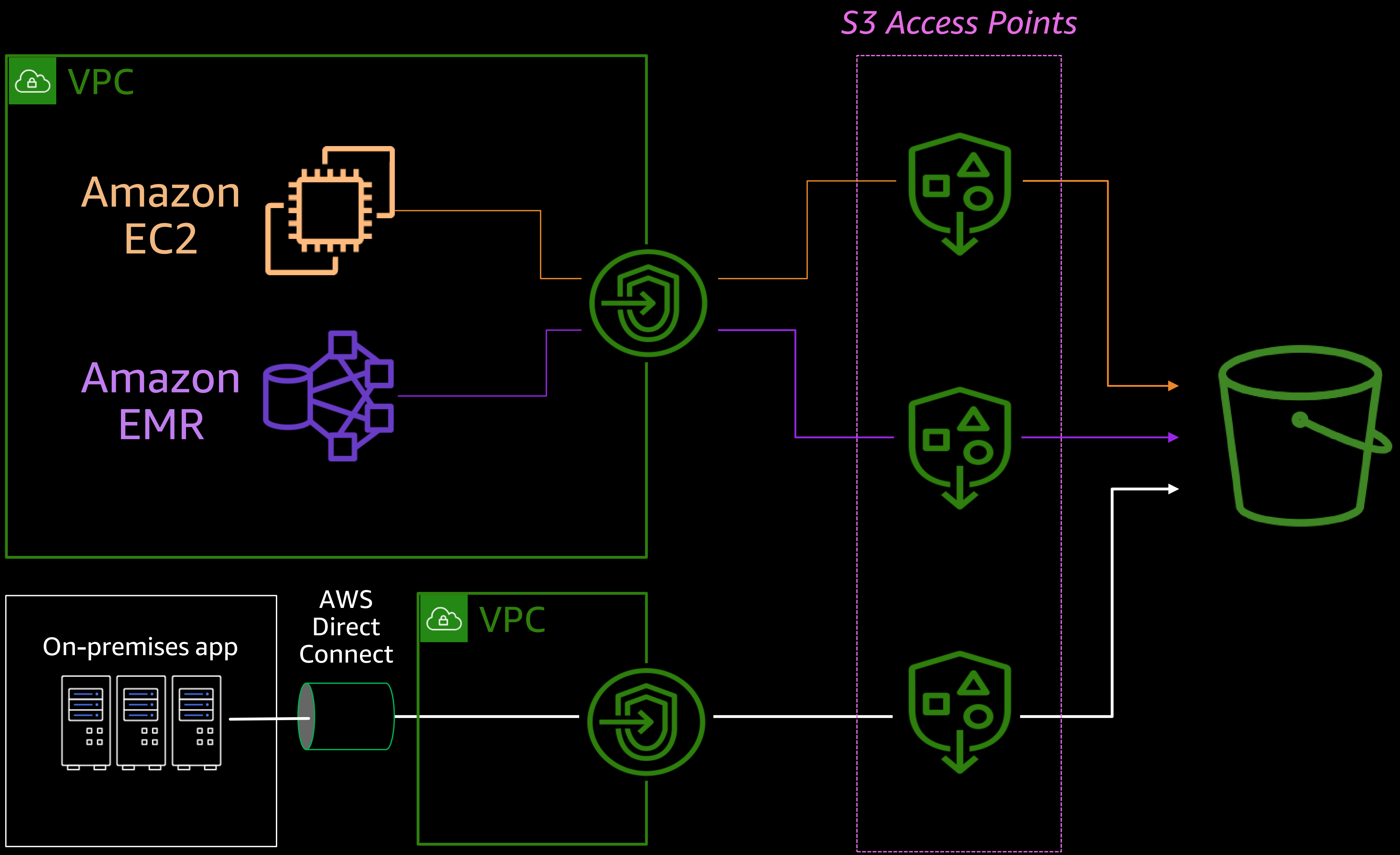
1. Simplify access management for shared buckets
2. Establish a new namespace that prevents naming conflicts
3. Restrict network traffic to specific VPCs



# S3 Access Points

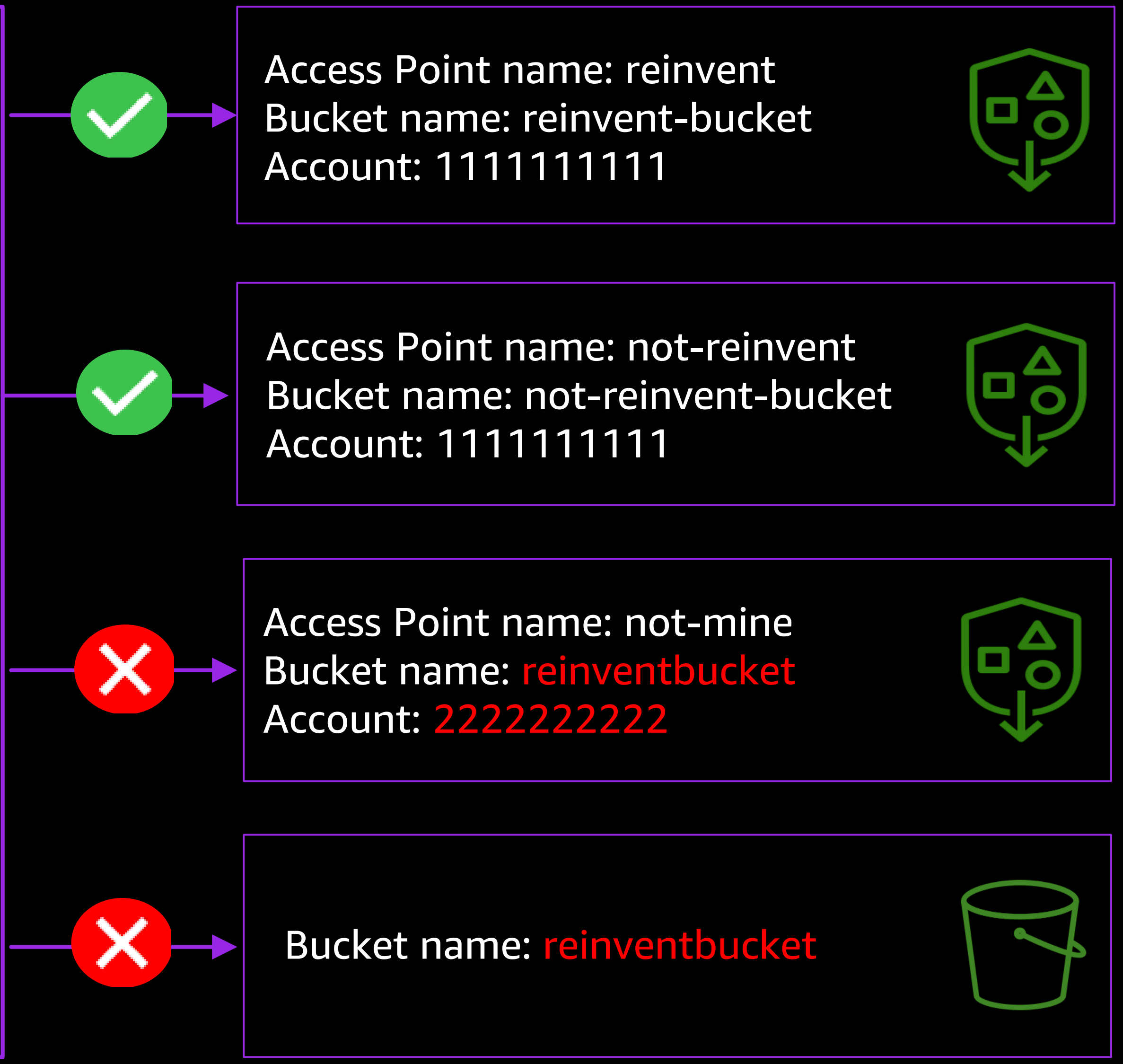


# S3 Access Points



# Limit resources to be accessed from your VPC

```
{ "Version": "2012-10-17",
"Id": "Policy1415115909152",
"Statement": [
 { "Sid": "Access-to-specific-bucket-only",
   "Principal": {"AWS":"1111111111"},
   "Action": [ "s3:GetObject, s3:PutObject",
   "Effect": "Allow",
  "Resource": ["arn:aws:s3:us-west-1:1111111111:accesspoint/*"
                ],
} ] }
```



✓ Access Point name: reinvent
Bucket name: reinvent-bucket
Account: 1111111111

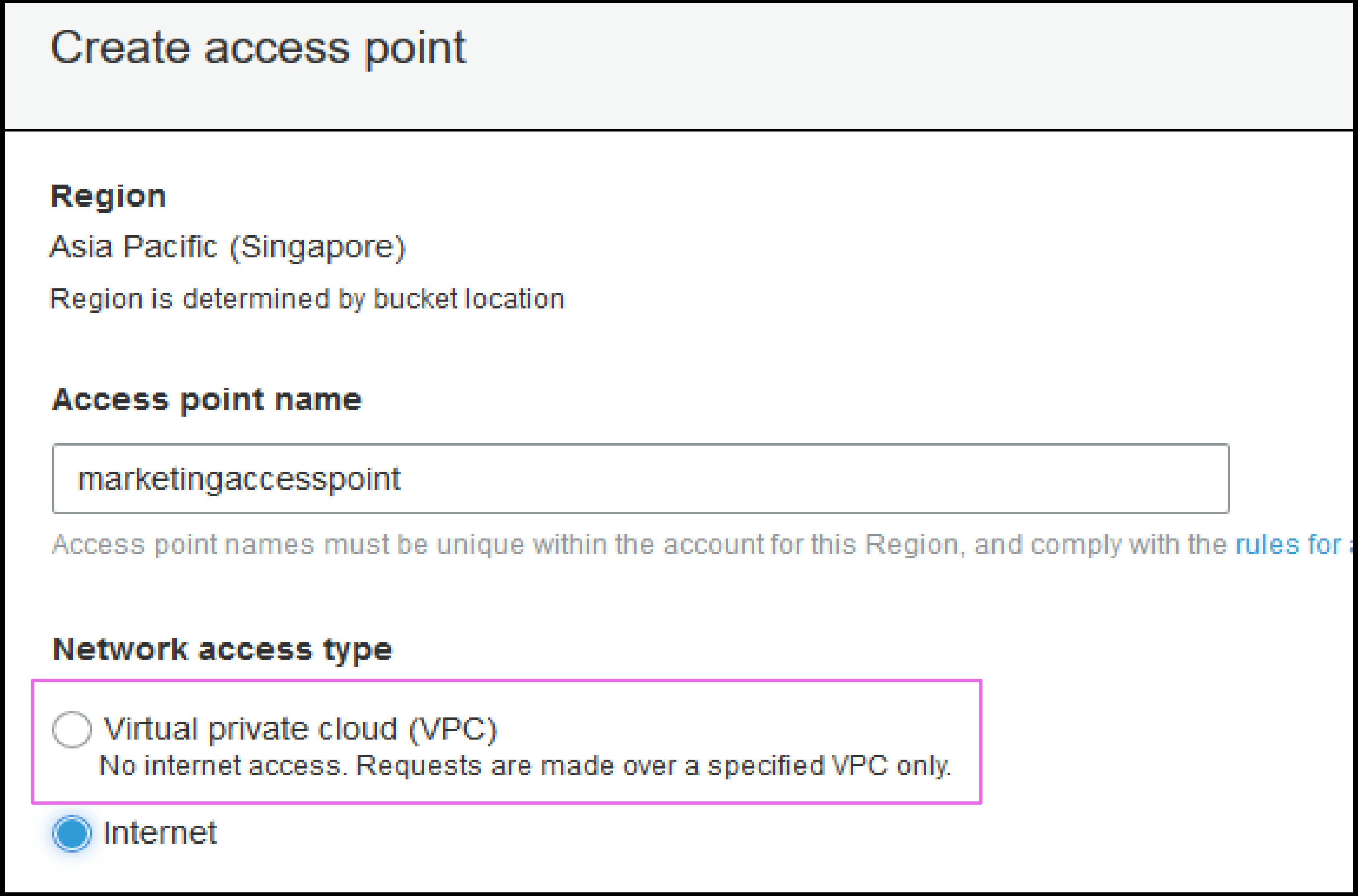
✓ Access Point name: not-reinvent
Bucket name: not-reinvent-bucket
Account: 1111111111

✗ Access Point name: not-mine
Bucket name: reinventbucket
Account: 2222222222

✗ Bucket name: reinventbucket

*“Clients in this VPC can use*
*Access Points in that AWS Account”*

# Limit VPCs that can access your resources



Create access point

**Region**

Asia Pacific (Singapore)

Region is determined by bucket location

**Access point name**

marketingaccesspoint

Access point names must be unique within the account for this Region, and comply with the rules for

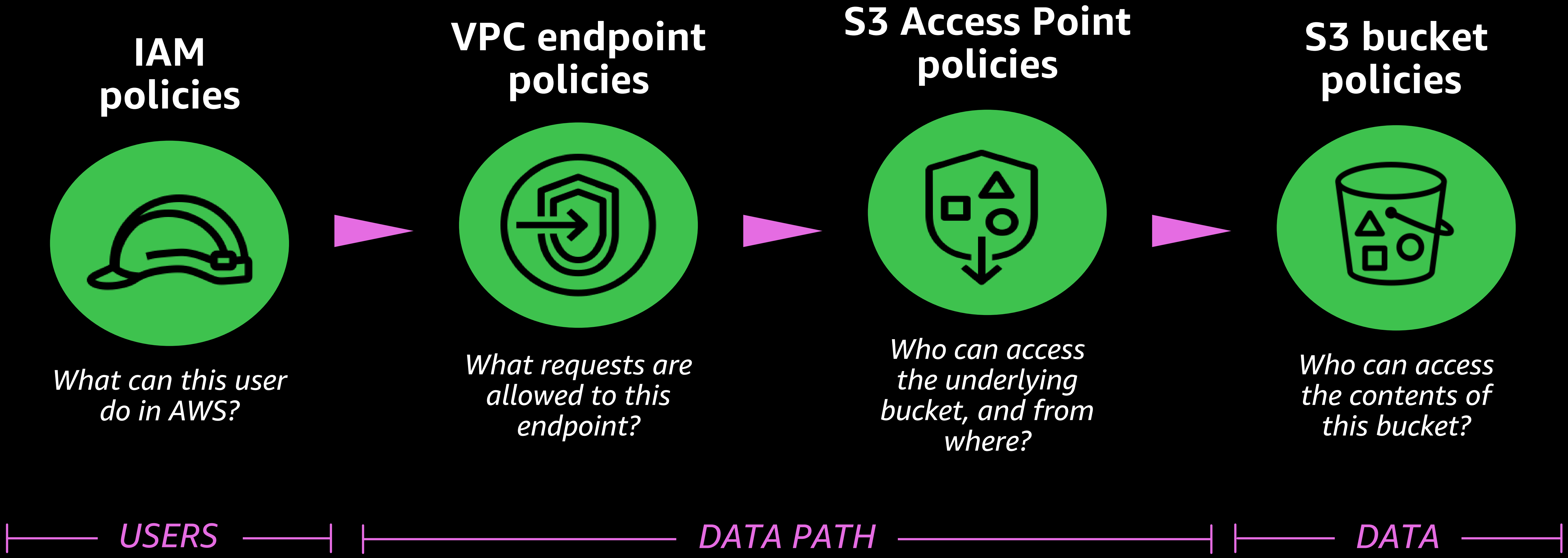
**Network access type**

○ Virtual private cloud (VPC)
No internet access. Requests are made over a specified VPC only.

● Internet

- Enforce VPC-only data access for a bucket
- Disable direct data access to the bucket
- Couple with Amazon VPC endpoint policies to prevent traffic that leaves an account

# Access controls all along the data path



**IAM policies**

*What can this user do in AWS?*

**VPC endpoint policies**

*What requests are allowed to this endpoint?*

**S3 Access Point policies**

*Who can access the underlying bucket, and from where?*

**S3 bucket policies**

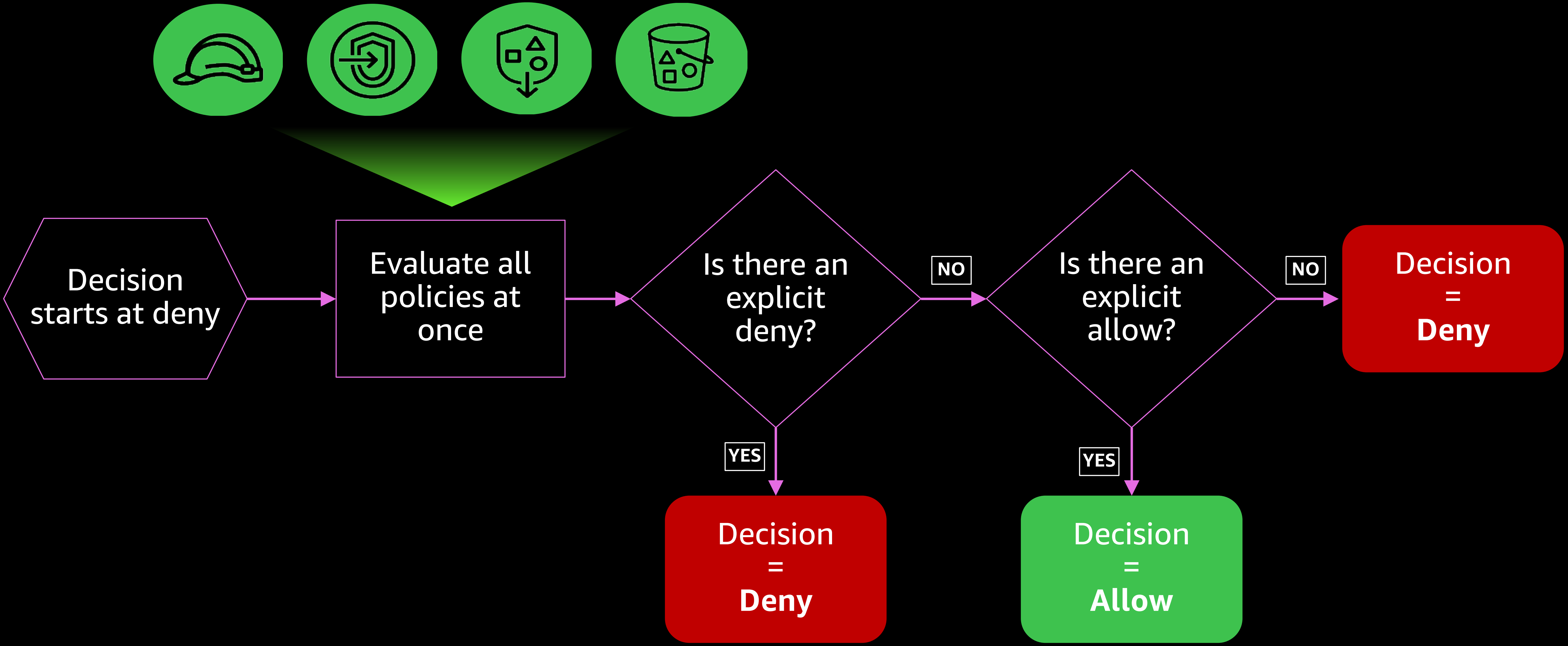
*Who can access the contents of this bucket?*

*USERS*

*DATA PATH*

*DATA*

# How policy evaluation works



Access Controls

Block Public Access

Encryption

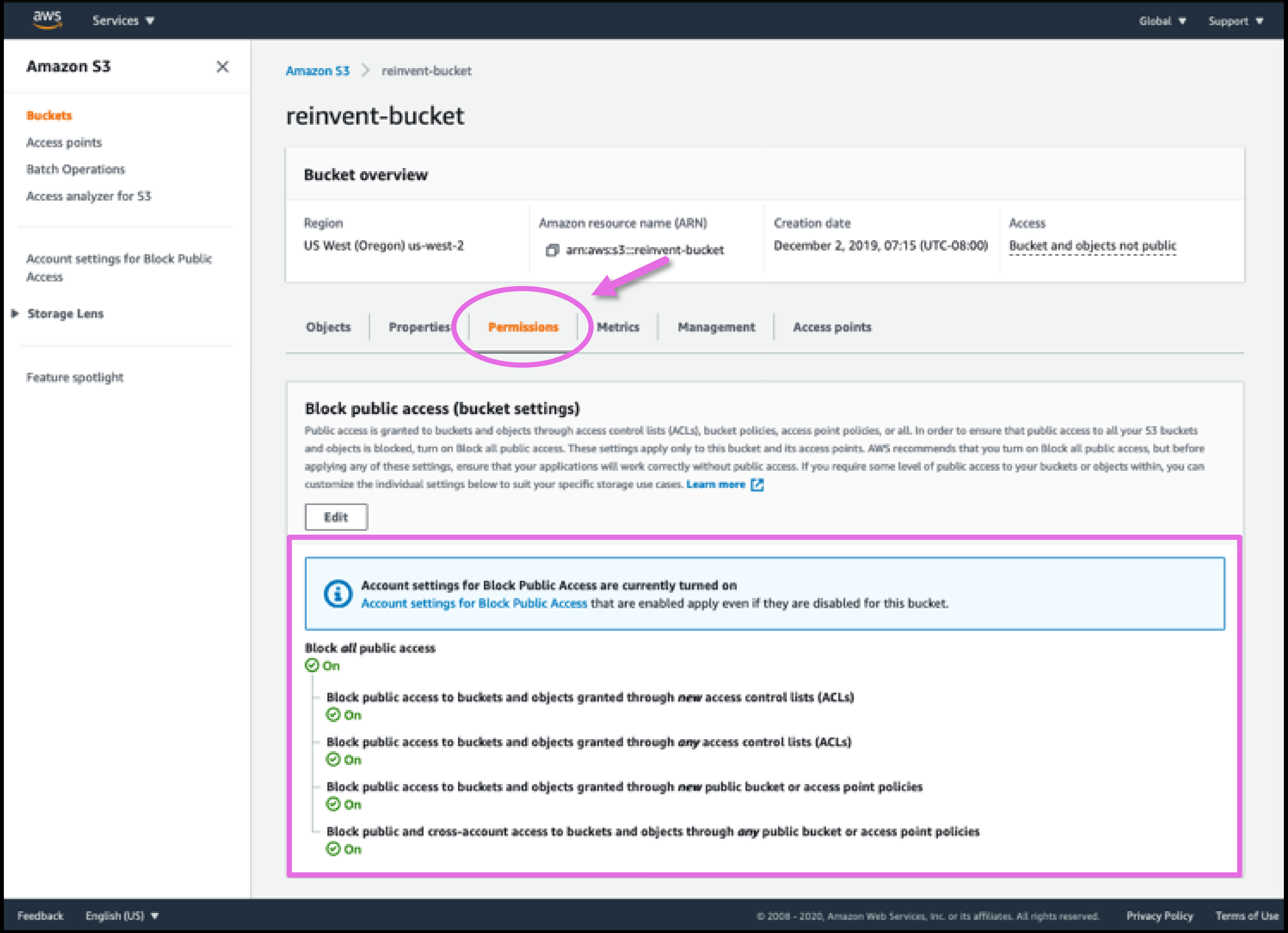
Data protection

# Managing public access

## Block Public Access

- Applies blanket protection against accidental public access
- Set at the bucket or the account level
- Can be applied to ACL access, bucket policy access, or both

# Managing public access



## reinvent-bucket

### Bucket overview

Region
US West (Oregon) us-west-2

Amazon resource name (ARN)
arn:aws:s3:::reinvent-bucket

Creation date
December 2, 2019, 07:15 (UTC-08:00)

Access
Bucket and objects not public

### Block public access (bucket settings)

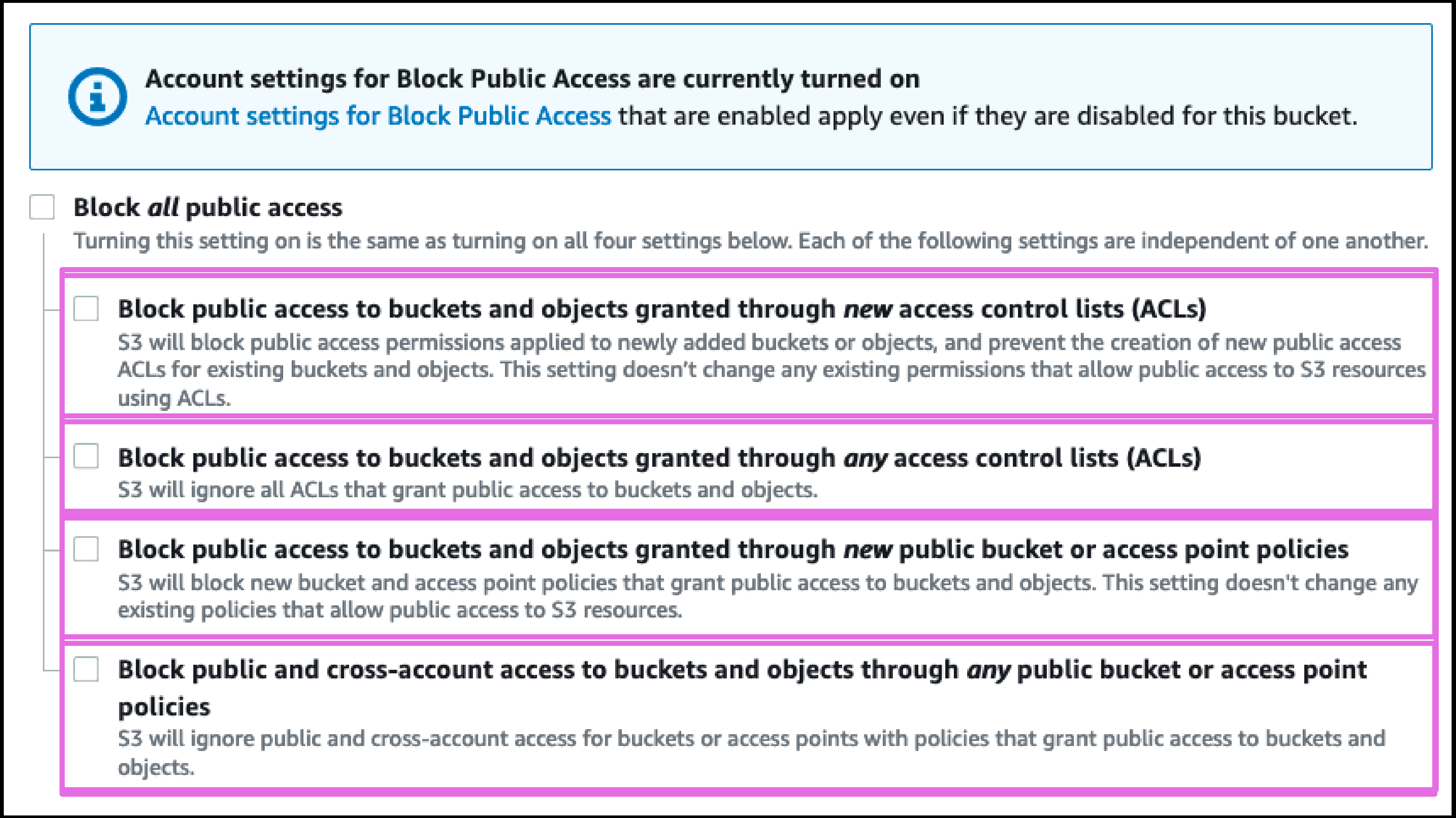
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

**Account settings for Block Public Access are currently turned on**
Account settings for Block Public Access that are enabled apply even if they are disabled for this bucket.

Block *all* public access
✓ On

- Block public access to buckets and objects granted through *new* access control lists (ACLs)
  ✓ On
- Block public access to buckets and objects granted through *any* access control lists (ACLs)
  ✓ On
- Block public access to buckets and objects granted through *new* public bucket or access point policies
  ✓ On
- Block public and cross-account access to buckets and objects through *any* public bucket or access point policies
  ✓ On

# Managing public access

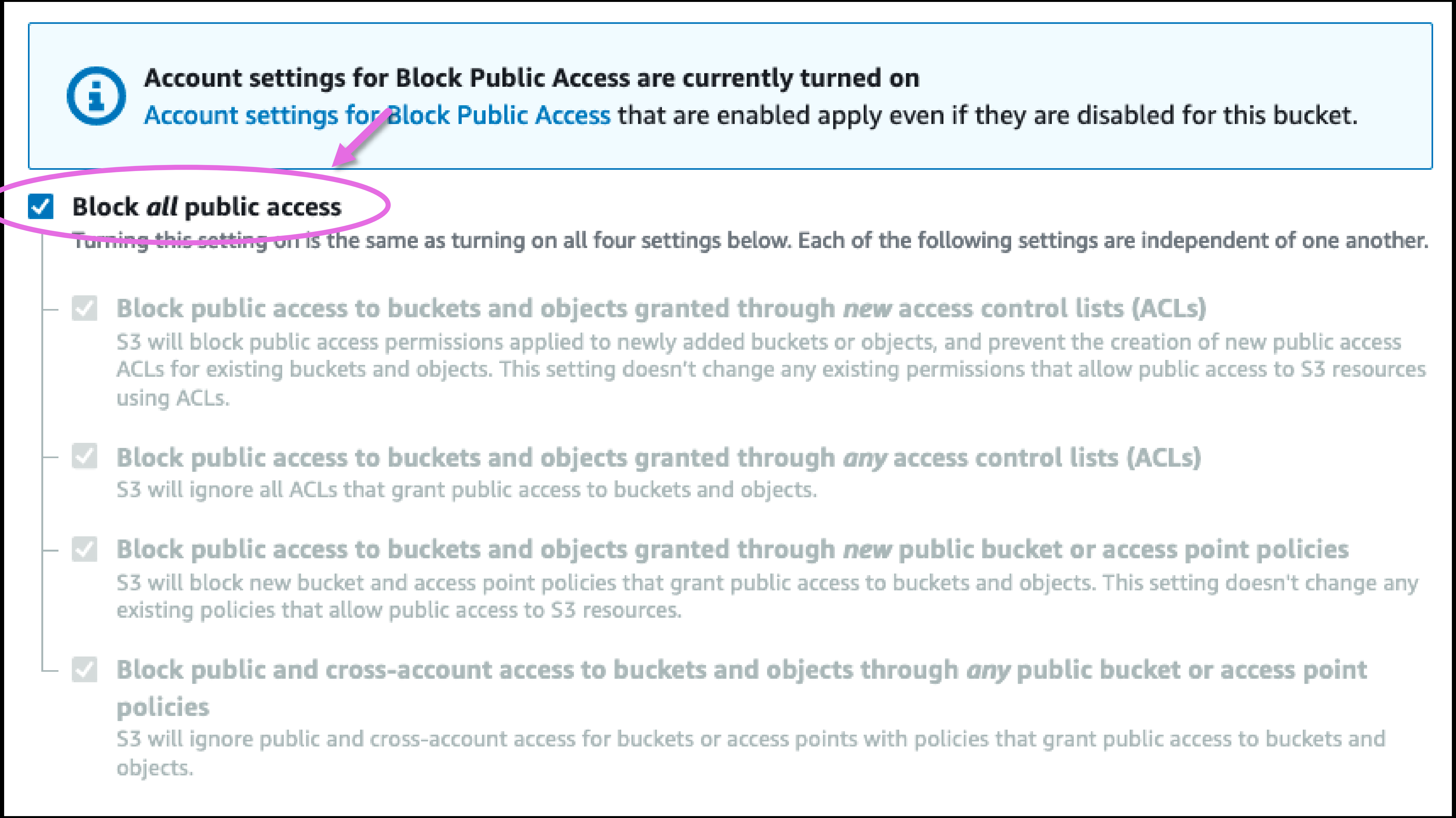


**Account settings for Block Public Access are currently turned on**
Account settings for Block Public Access that are enabled apply even if they are disabled for this bucket.

□ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- □ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- □ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.
- □ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- □ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

# Managing public access



**Account settings for Block Public Access are currently turned on**
Account settings for Block Public Access that are enabled apply even if they are disabled for this bucket.

☑ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

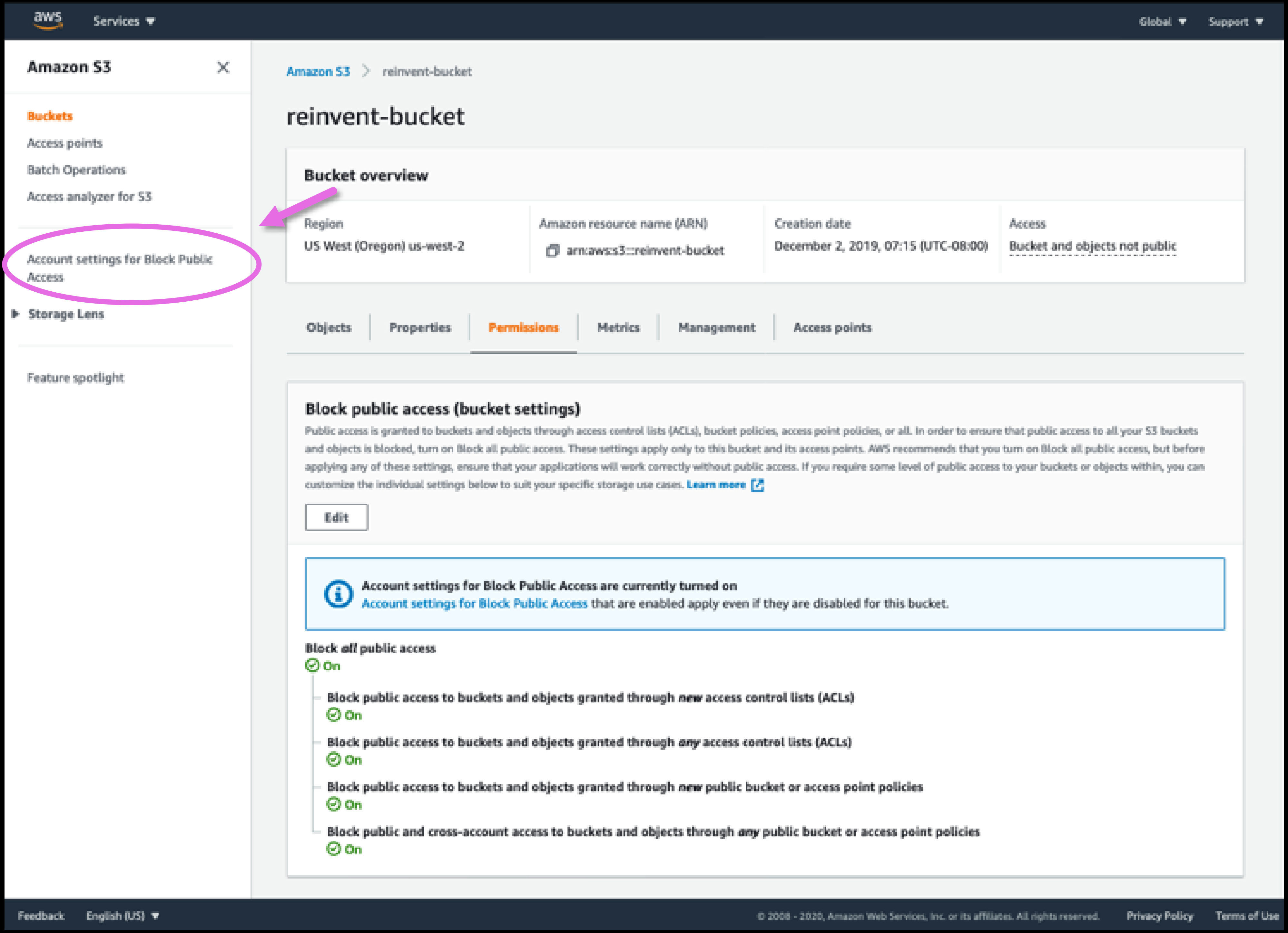
- ☑ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

- ☑ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.

- ☑ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

- ☑ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

# Managing public access



## reinvent-bucket

### Bucket overview

| Region | Amazon resource name (ARN) | Creation date | Access |
|---|---|---|---|
| US West (Oregon) us-west-2 | arn:aws:s3:::reinvent-bucket | December 2, 2019, 07:15 (UTC-08:00) | Bucket and objects not public |

### Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

**Account settings for Block Public Access are currently turned on**
Account settings for Block Public Access that are enabled apply even if they are disabled for this bucket.

Block *all* public access
✓ On

- Block public access to buckets and objects granted through *new* access control lists (ACLs)
  ✓ On
- Block public access to buckets and objects granted through *any* access control lists (ACLs)
  ✓ On
- Block public access to buckets and objects granted through *new* public bucket or access point policies
  ✓ On
- Block public and cross-account access to buckets and objects through *any* public bucket or access point policies
  ✓ On

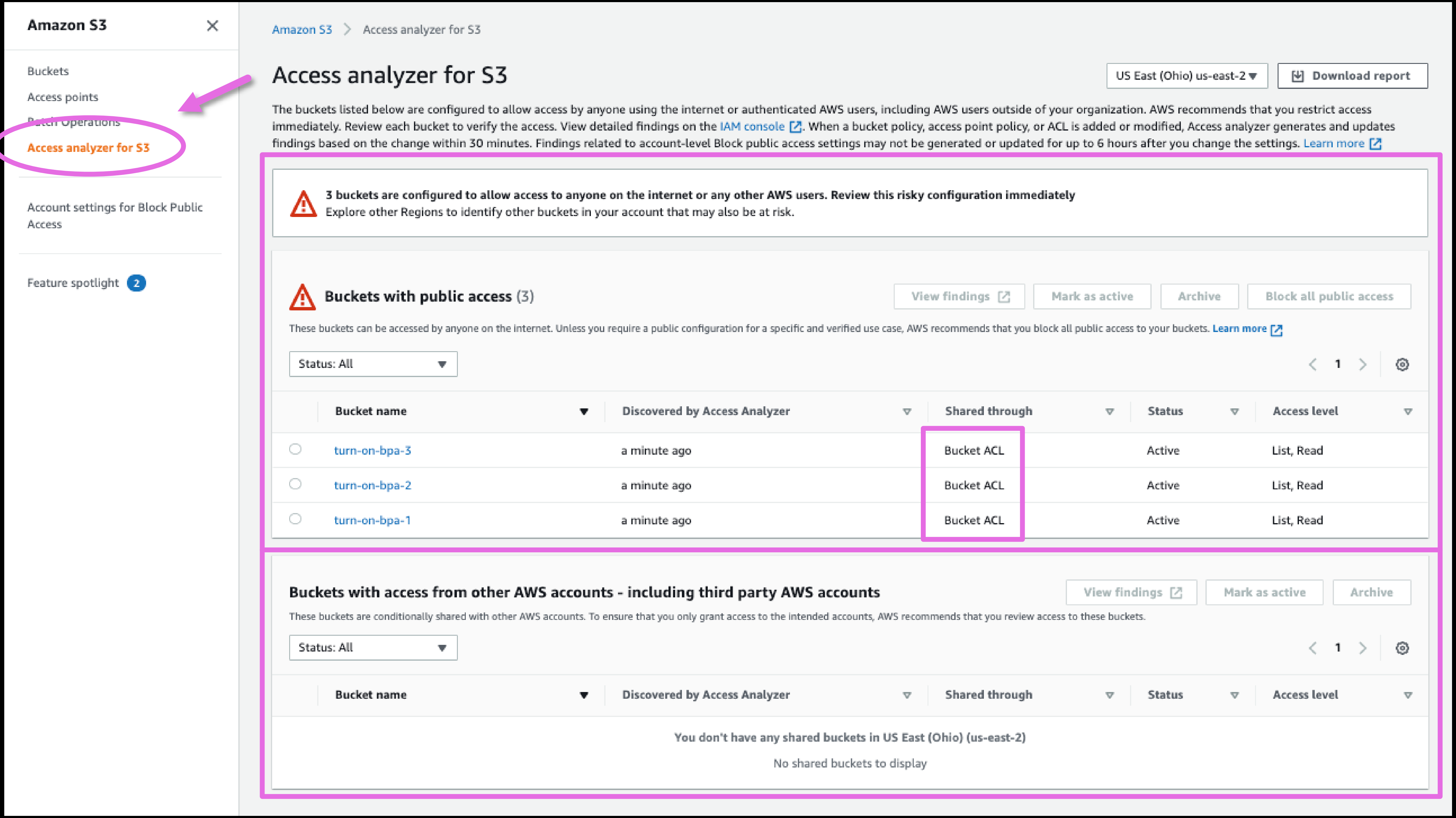
Feedback
English (US) ▼
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

# Managing public access

## Access Analyzer for S3

- Analyzes permissions for all buckets in an AWS Region
- Provides a simple dashboard to show public buckets
- 1-click Block Public Access

# Managing public access



Amazon S3 > Access analyzer for S3

## Access analyzer for S3

The buckets listed below are configured to allow access by anyone using the internet or authenticated AWS users, including AWS users outside of your organization. AWS recommends that you restrict access immediately. Review each bucket to verify the access. View detailed findings on the IAM console. When a bucket policy, access point policy, or ACL is added or modified, Access analyzer generates and updates findings based on the change within 30 minutes. Findings related to account-level Block public access settings may not be generated or updated for up to 6 hours after you change the settings. Learn more

**3 buckets are configured to allow access to anyone on the internet or any other AWS users. Review this risky configuration immediately**
Explore other Regions to identify other buckets in your account that may also be at risk.

### Buckets with public access (3)

These buckets can be accessed by anyone on the internet. Unless you require a public configuration for a specific and verified use case, AWS recommends that you block all public access to your buckets. Learn more

Status: All

|  | Bucket name | Discovered by Access Analyzer | Shared through | Status | Access level |
|---|---|---|---|---|---|
| ○ | turn-on-bpa-3 | a minute ago | Bucket ACL | Active | List, Read |
| ○ | turn-on-bpa-2 | a minute ago | Bucket ACL | Active | List, Read |
| ○ | turn-on-bpa-1 | a minute ago | Bucket ACL | Active | List, Read |

### Buckets with access from other AWS accounts - including third party AWS accounts

These buckets are conditionally shared with other AWS accounts. To ensure that you only grant access to the intended accounts, AWS recommends that you review access to these buckets.

Status: All

|  | Bucket name | Discovered by Access Analyzer | Shared through | Status | Access level |
|---|---|---|---|---|---|

You don't have any shared buckets in US East (Ohio) (us-east-2)

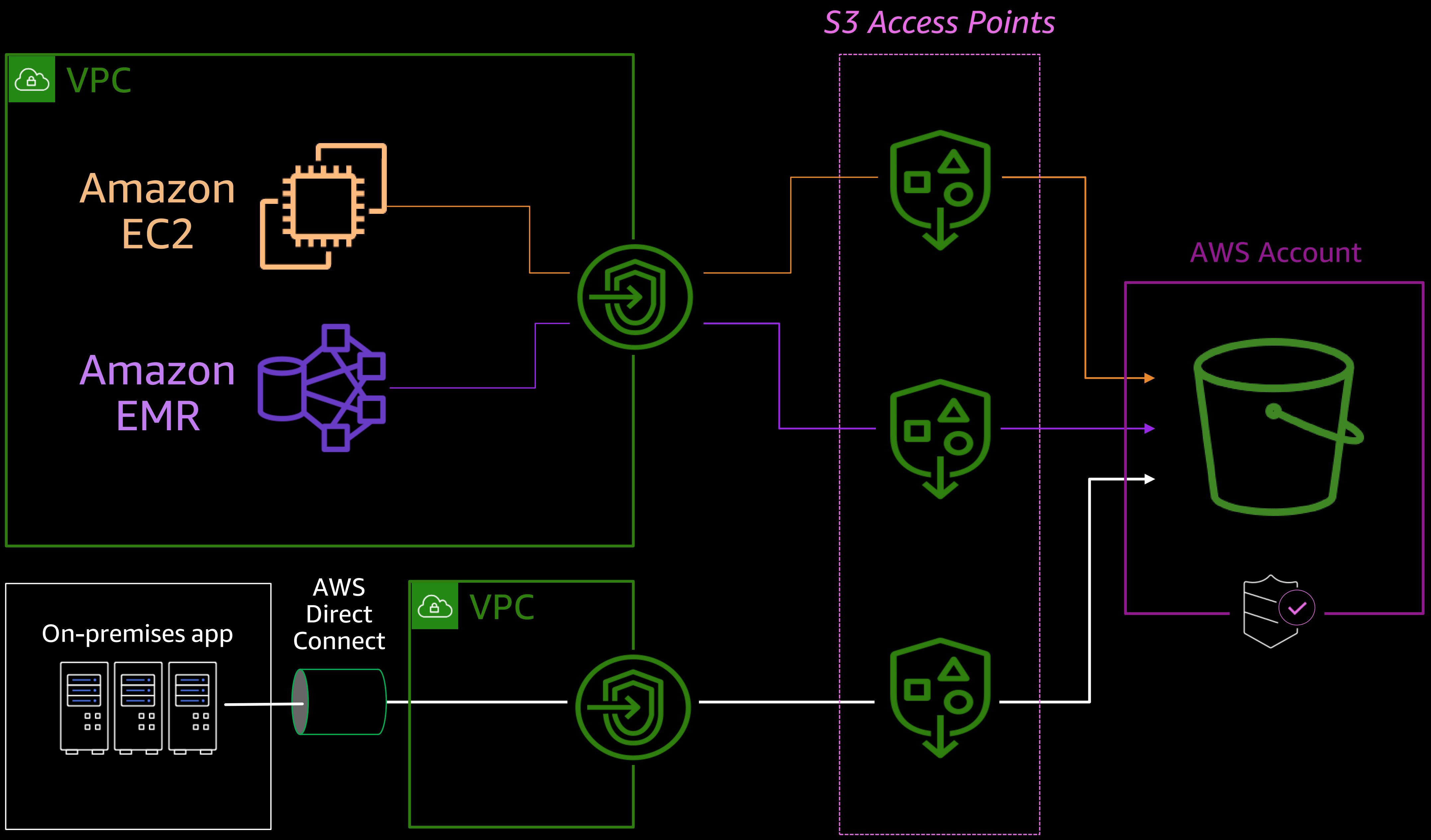
No shared buckets to display

# Managing public access

## 3 key best practices

1. Run Access Analyzer – understand how your buckets are being shared
2. Keep public buckets in a dedicated AWS Account, so you can enable Block Public Access at the account level everywhere else
3. Bucket policies > ACLs

# Managing public access



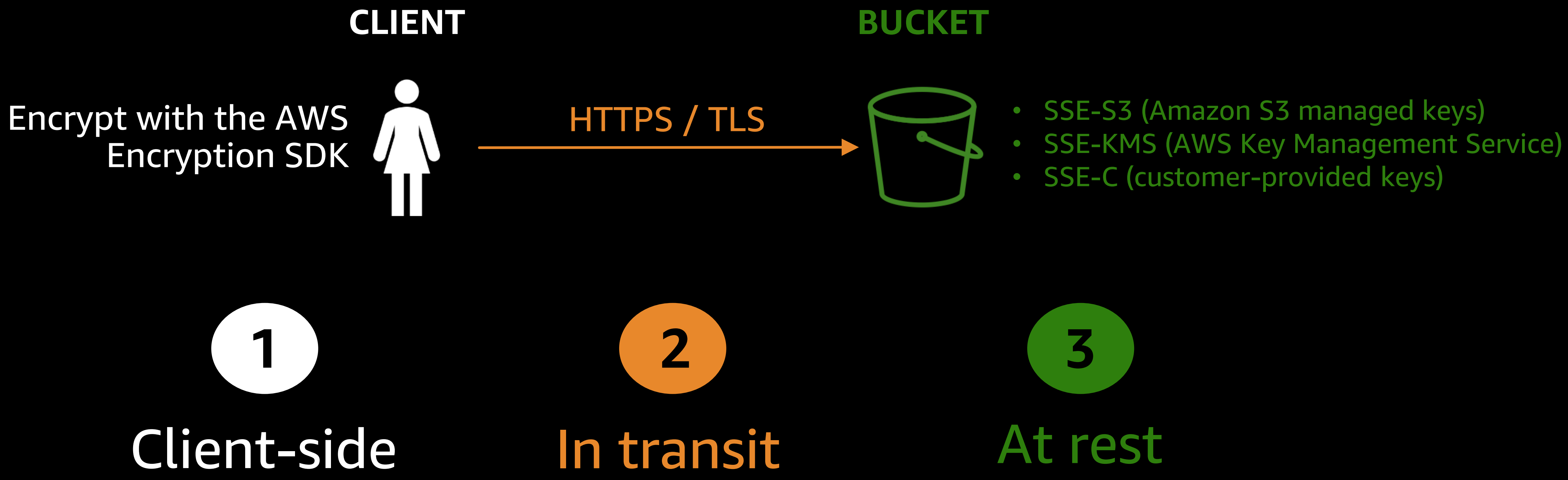
Access Controls

Block Public Access

Encryption

Data protection

# Amazon S3 encryption support



CLIENT

Encrypt with the AWS Encryption SDK

HTTPS / TLS

BUCKET

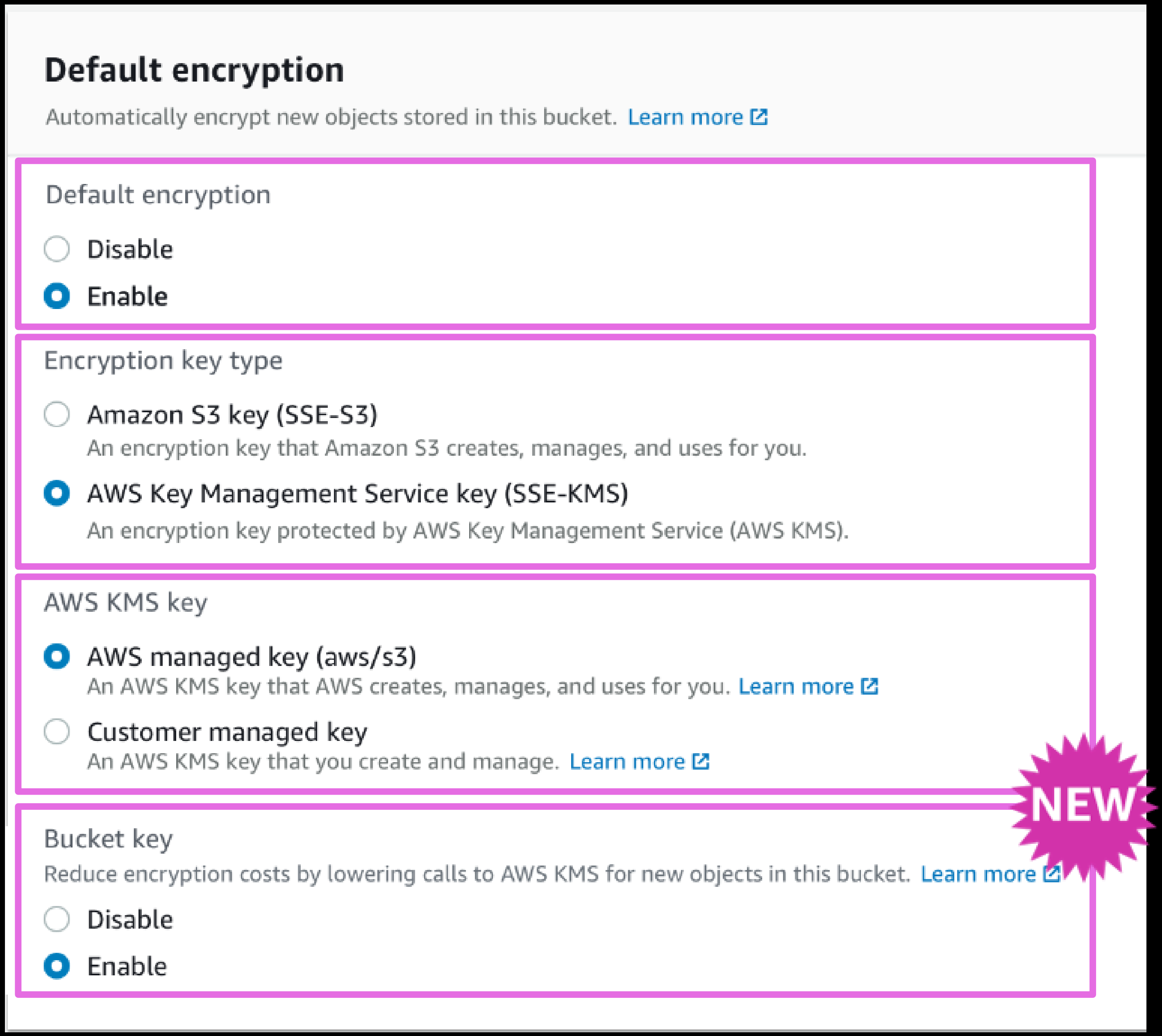
- SSE-S3 (Amazon S3 managed keys)
- SSE-KMS (AWS Key Management Service)
- SSE-C (customer-provided keys)

1 Client-side

2 In transit

3 At rest

# Amazon S3 default encryption



**Default encryption**

Automatically encrypt new objects stored in this bucket. Learn more

Default encryption

○ Disable

● Enable

Encryption key type

○ Amazon S3 key (SSE-S3)
An encryption key that Amazon S3 creates, manages, and uses for you.

● AWS Key Management Service key (SSE-KMS)
An encryption key protected by AWS Key Management Service (AWS KMS).

AWS KMS key

● AWS managed key (aws/s3)
An AWS KMS key that AWS creates, manages, and uses for you. Learn more

○ Customer managed key
An AWS KMS key that you create and manage. Learn more

NEW

Bucket key

Reduce encryption costs by lowering calls to AWS KMS for new objects in this bucket. Learn more

○ Disable

● Enable

- One-time bucket-level setup
- Automatically encrypts all new objects

- Specify key management strategy
- You manage keys or offload to S3

- If KMS, then specify a key
- Use your own or a service-managed key

- Reduce KMS costs with a bucket key
- Results in up to 99% fewer KMS requests

# Amazon S3 Bucket Keys

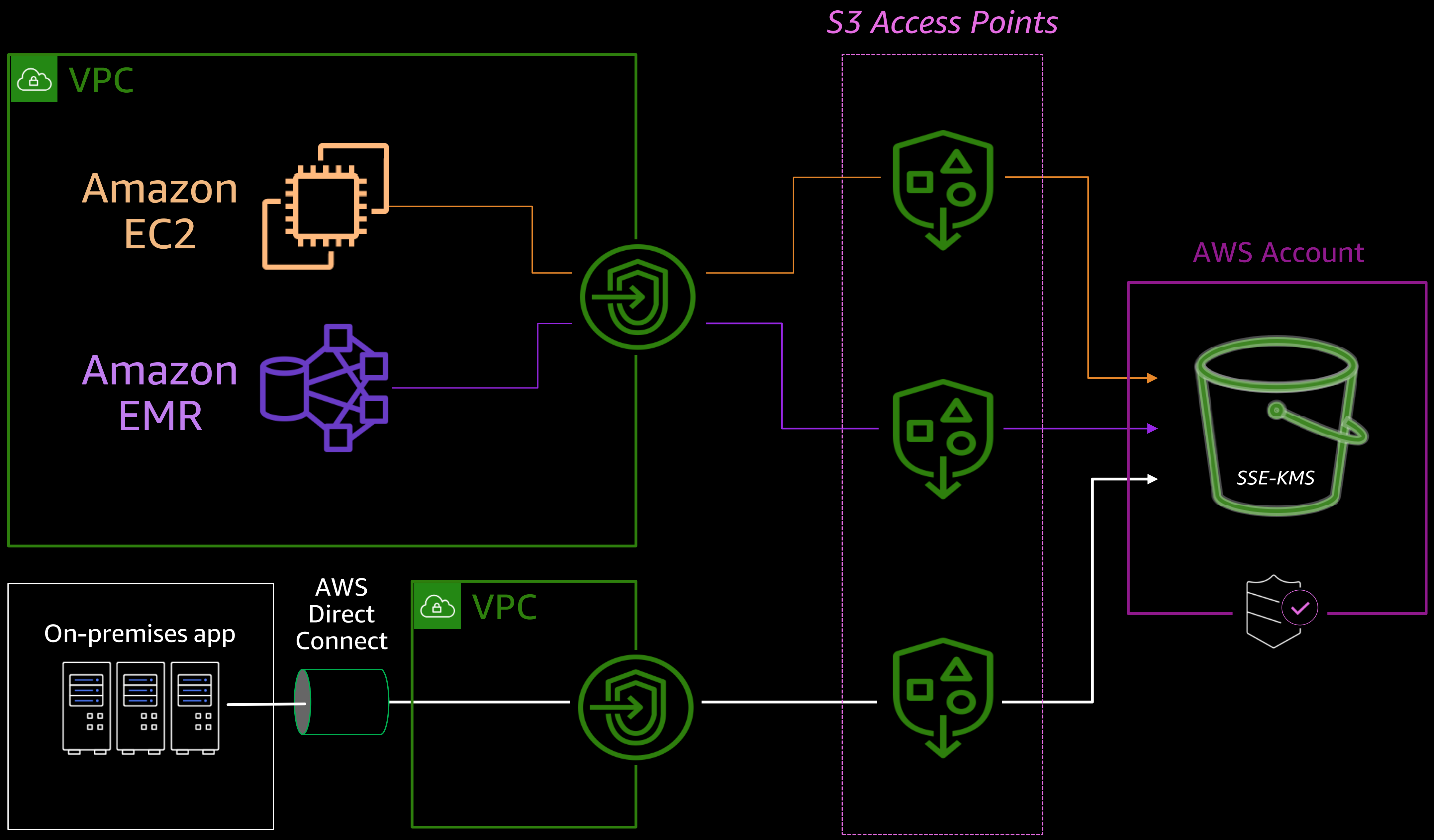
NEW

Increase performance for encryption

Reduce request costs for KMS-backed server-side encryption by up to

99%

# Amazon S3 default encryption



Access Controls

Block Public Access

Encryption

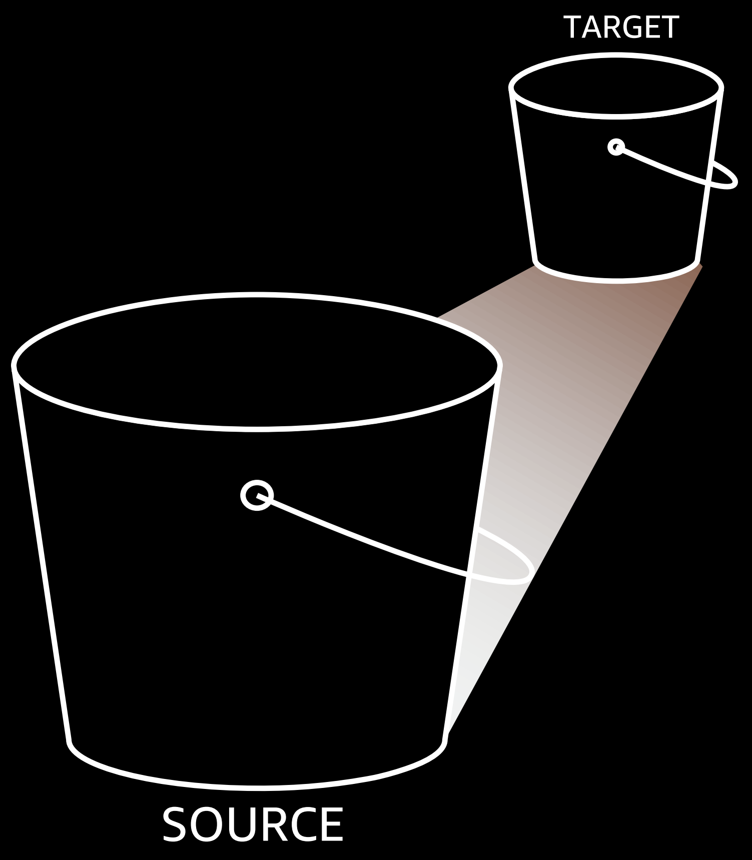
Data protection

# Amazon S3 object versioning

*VERSION STACK*

| | | Key | LastModified | VersionId | |
|---|---|---|---|---|---|
| PUT 4 → | ◆ | **EXAMPLE.JPG** | **2018**-11-05T18:44:56 | ex5e6GzmPcAzEmJLEZ6KihZYzZGw8eVq | GET: ◆ |
| DELETE → | DELETE<br>MARKER | **EXAMPLE.JPG** | **2017**-11-05T18:44:56 | yLAuNvayJMTvtJY2Eat6GZJgvQdPHaAG | GET: 404 |
| PUT 3 → | ▲ | **EXAMPLE.JPG** | **2016**-11-05T18:44:56 | JA4myYTL9eh9TK.dhTIgYonqBKa6Mfjd | GET: ▲ |
| PUT 2 → | ● | **EXAMPLE.JPG** | **2015**-11-05T18:44:56 | OqSso_2kQhdyg5GGyW61gQlrQY1YT503 | |
| PUT 1 → | ■ | **EXAMPLE.JPG** | **2014**-11-05T18:44:56 | ekT1wA4fPyQgVaMKDQSmpJk4GUEzbX0K | |

# S3 Replication: More than a second copy



SELECT

**Select data**

Replicate the whole bucket
… or based on a prefix
… or based on object tags

PROTECT

**In or across Regions**

Replicate any second S3 bucket
Continuous replication as your data changes
**Automatically generate and maintain a second copy**

**Change ownership & account**

Replicate into a second account
Automatically change owner of replica objects
**Protect against AWS Account compromise**

OPTIMIZE

**Set storage class**

Maintain production access characteristics
… or Land and Lifecycle
… or replicate straight to S3 Glacier

# S3 Object Lock

### Immutable objects in S3

Assessed for SEC Compliance by Cohasset Associates

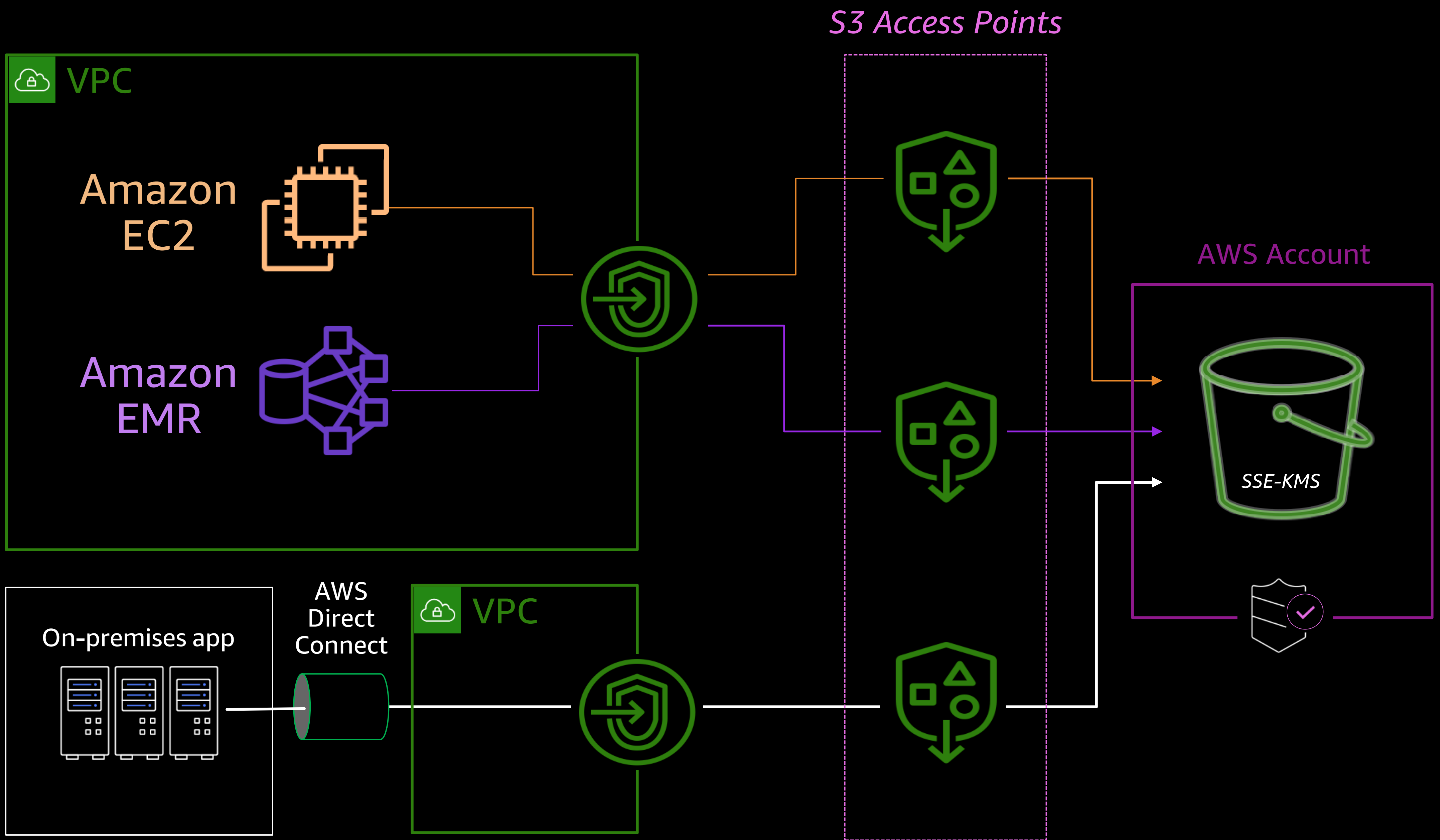
### Retention controls

Down to the object and object version levels

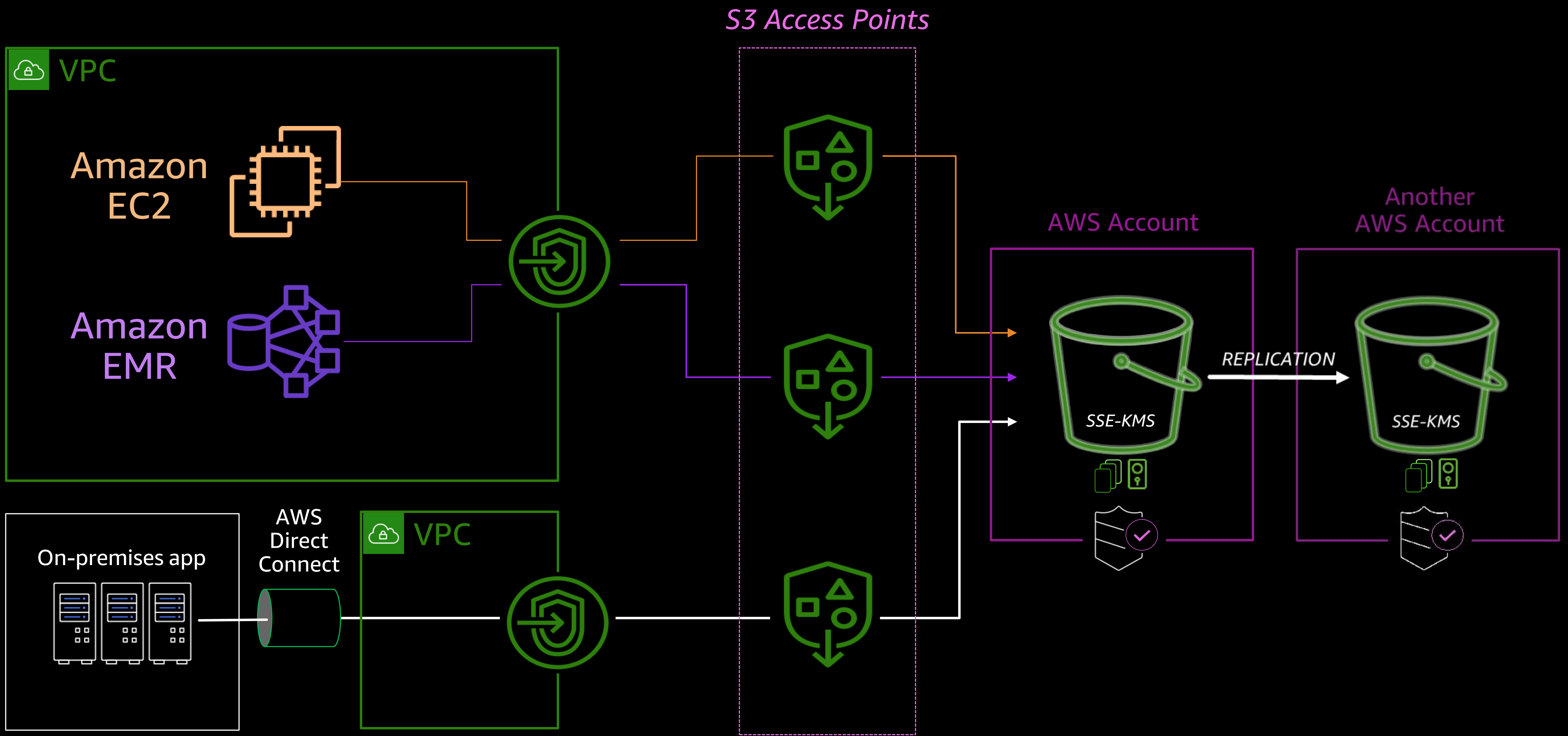
### Auditing and visibility

Track, report, and alert on access and retention changes

# Adding in data protection



# Adding in data protection



Access Controls

Block Public Access

Encryption

Data protection

# Thank you!

Paul Meighan

@paulmeighan

Product Manager
Amazon S3

AWS re:Invent

Please complete the session survey