
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

STG-208

Protect against ransomware with a Zero Trust architecture

Nancy Wang

Director / General Manager, AWS Data Protection
She / hers

Neha Rungta

Director, AWS Automated Reasoning for Identity
She / hers

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

1. Why a Zero Trust architecture is key for ransomware protection
2. Provable security and immutability with Zero Trust Architecture
3. Case Study: Amazon Consumer Payments
4. Protecting your data with Zero Trust Architecture on AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ransomware in the cloud

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

Colonial Pipeline



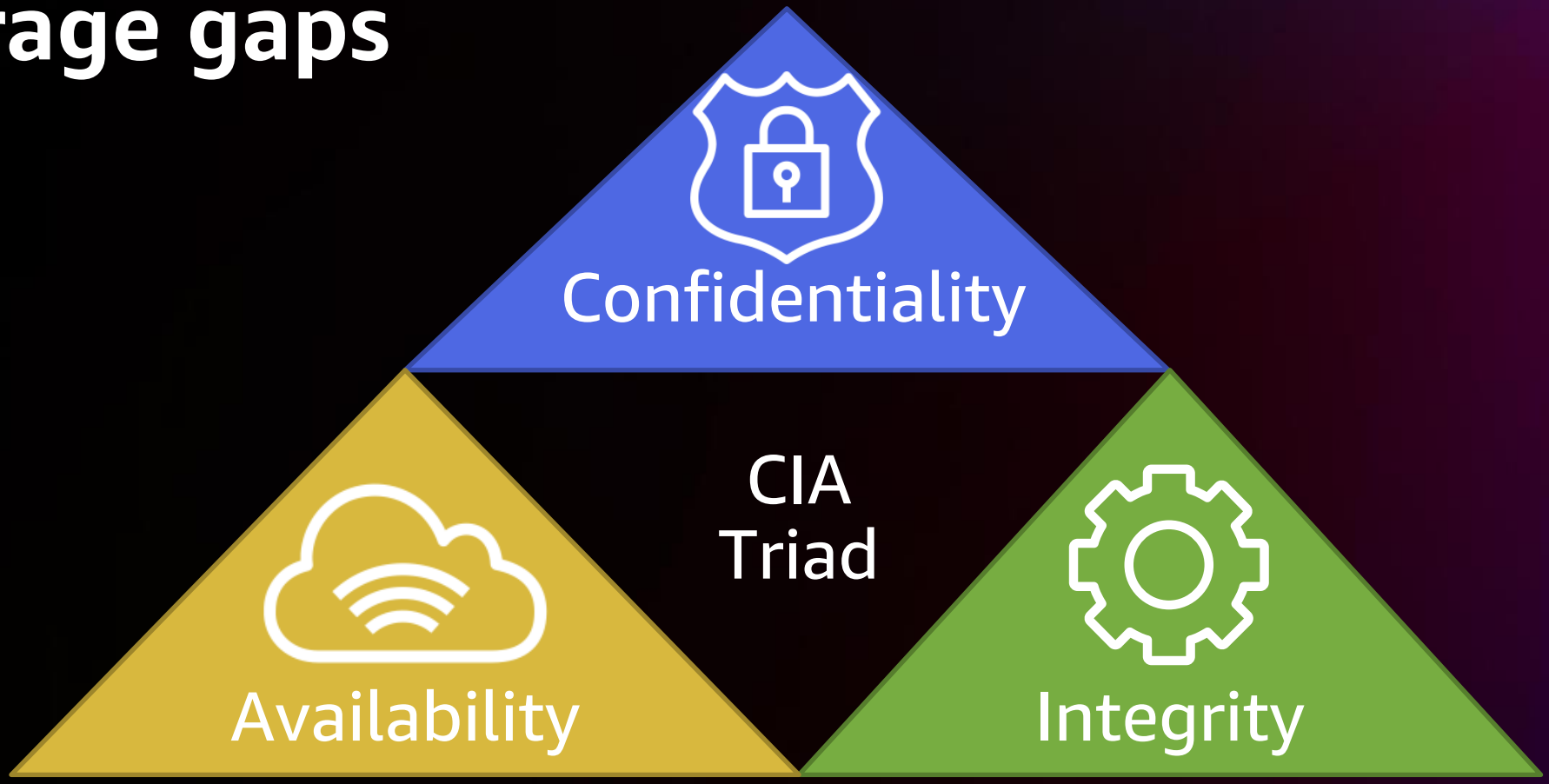
JBS



aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ransomware exploits access and coverage gaps



How do we know we're protecting the CIA of our crown jewels?

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is Zero Trust on AWS?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Changing our intuition on ransomware



If an actor is already in your environment, how do you make it hard for them to further progress toward your crown jewels?

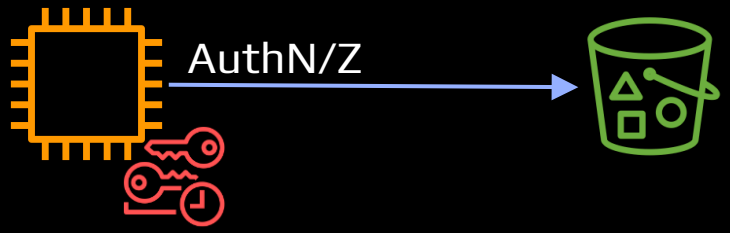
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

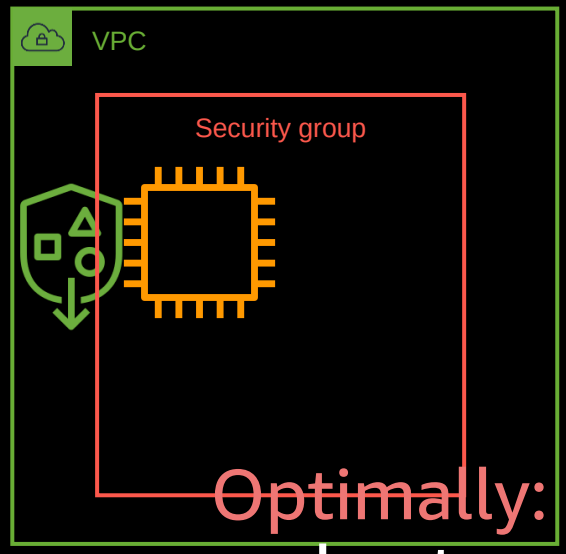
Defining Zero Trust

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Zero Trust

Identity-centric AND Network-centric





~~Optimally:~~ Identity-centric and network-centric controls aware of each other

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved. Amazon Confidential and Trademark.

The Zero Trust stance toward ransomware

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

To stop ransomware, start with the data

KNOW → PROTECT → HARDEN → PATCH

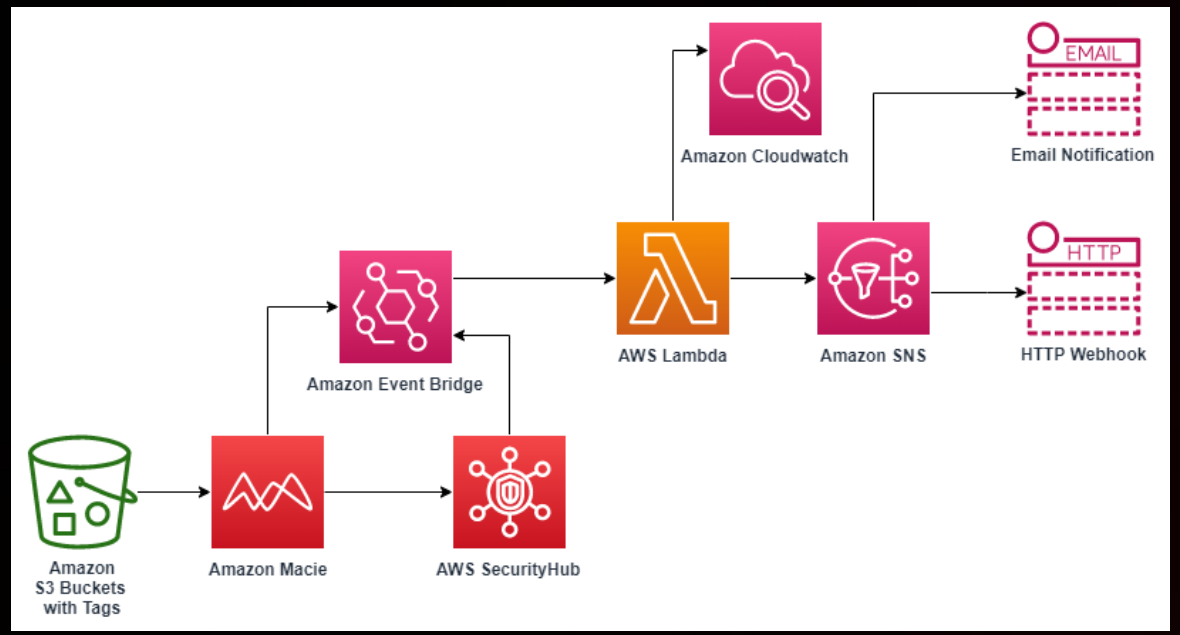
1. **Know** where your crown jewels live
2. **Protect** your crown jewels with the right configurations and policies
3. **Harden** all paths to your crown jewels
4. **Patch** your services regularly

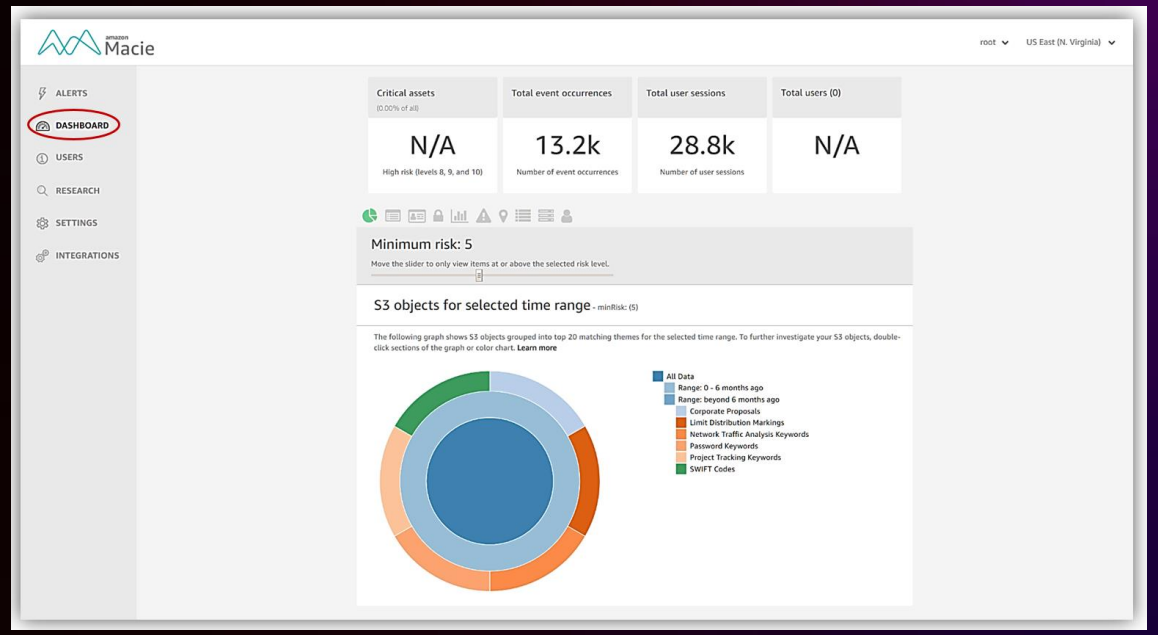
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step one: Know where your data lives

- Data is created and copied constantly
- Identify your organization's crown jewels and establish a tagging/isolation practice

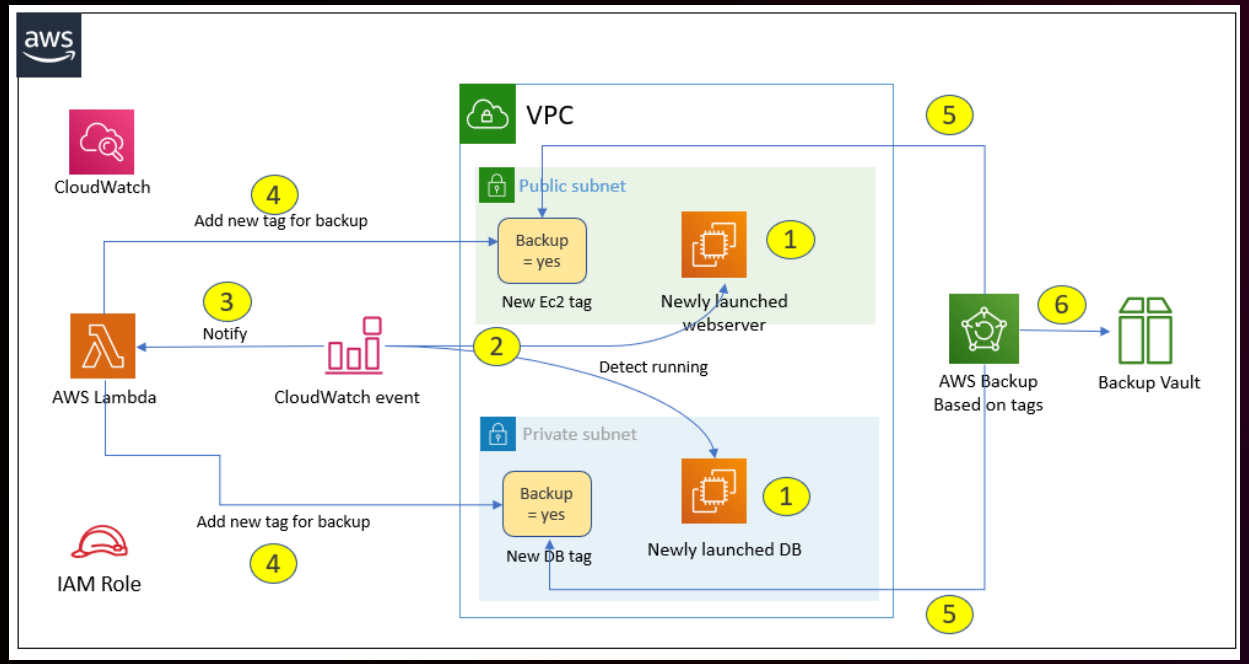




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step two: Protect your data

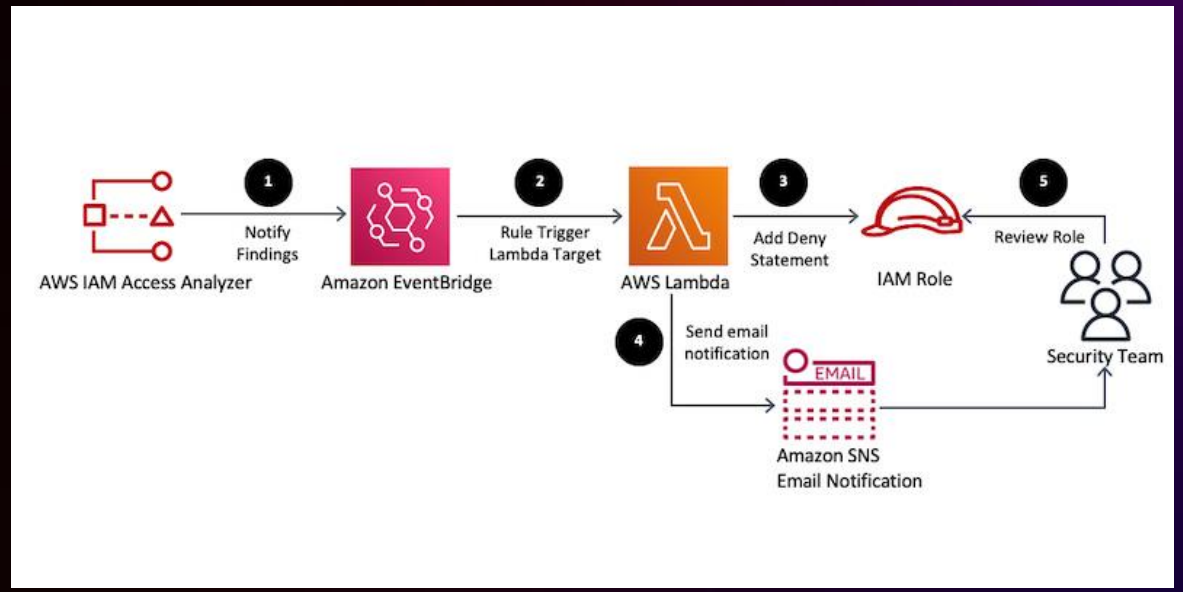
- Ensure proper configurations of your crown jewels services + data
- Protect your crown jewels and data by taking regular backups



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step three: Employ zero trust to harden paths to crown jewels

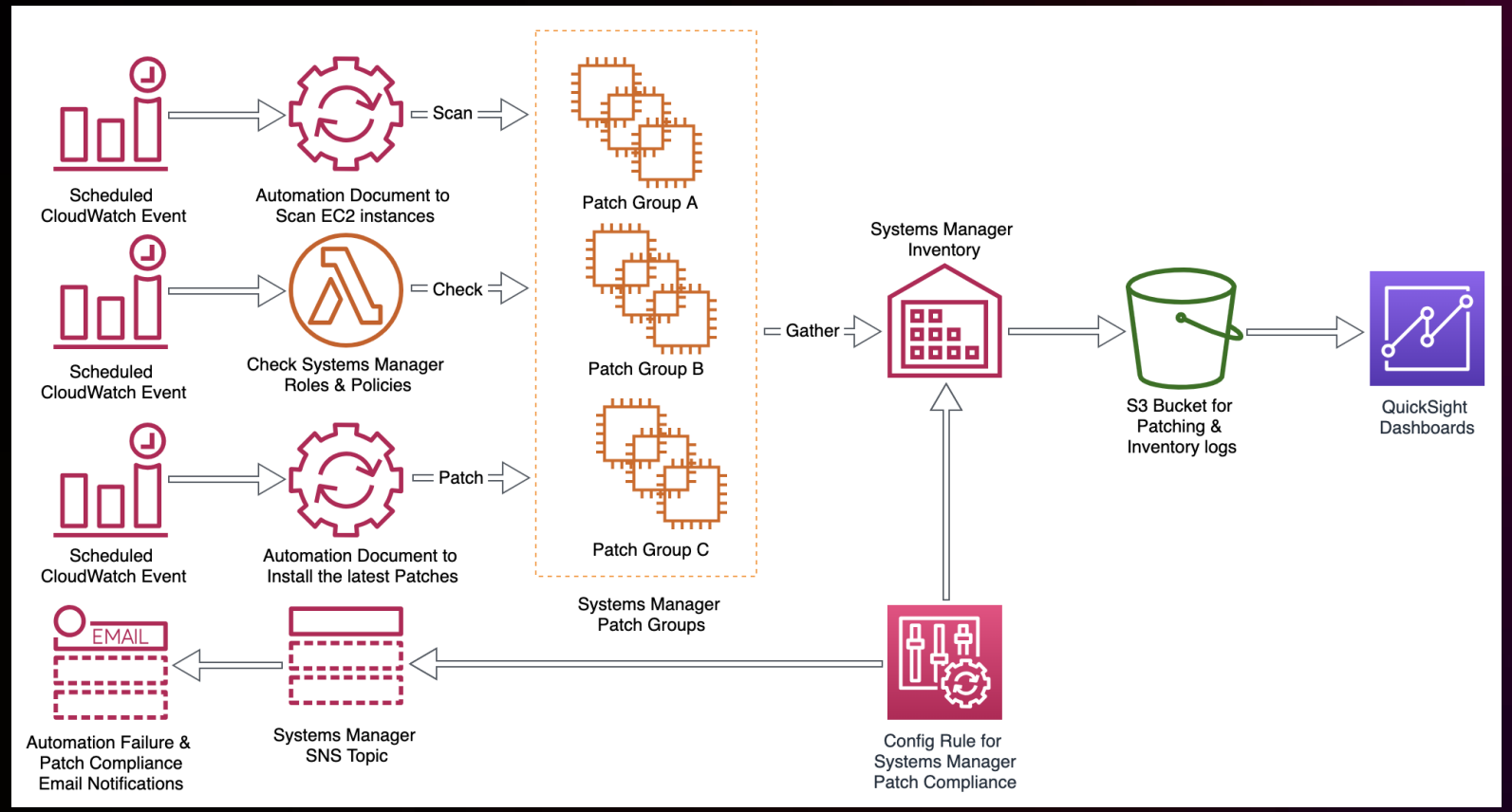
- **Evaluate** IAM and network paths leading to crown jewel data, services and backups
- **Identify** high risk roles, users and network routes
- **Rightsize** access and network reach



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step four: Have a regular patching cadence

- For the crown jewel services you've identified, make sure you have a **regular patching cadence**



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How AWS can help you

- Many of the steps I just went through to defend against ransomware relied on an analysis of what is possible given current configurations
- Here at AWS, we're building these analytical capabilities using techniques in symbolic analysis

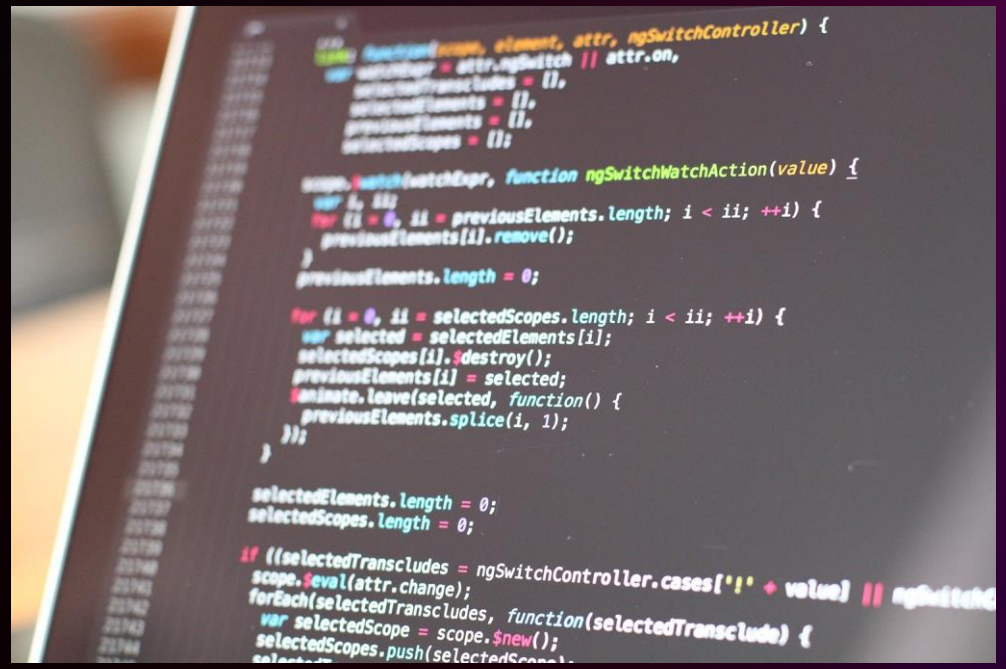
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Provable Security

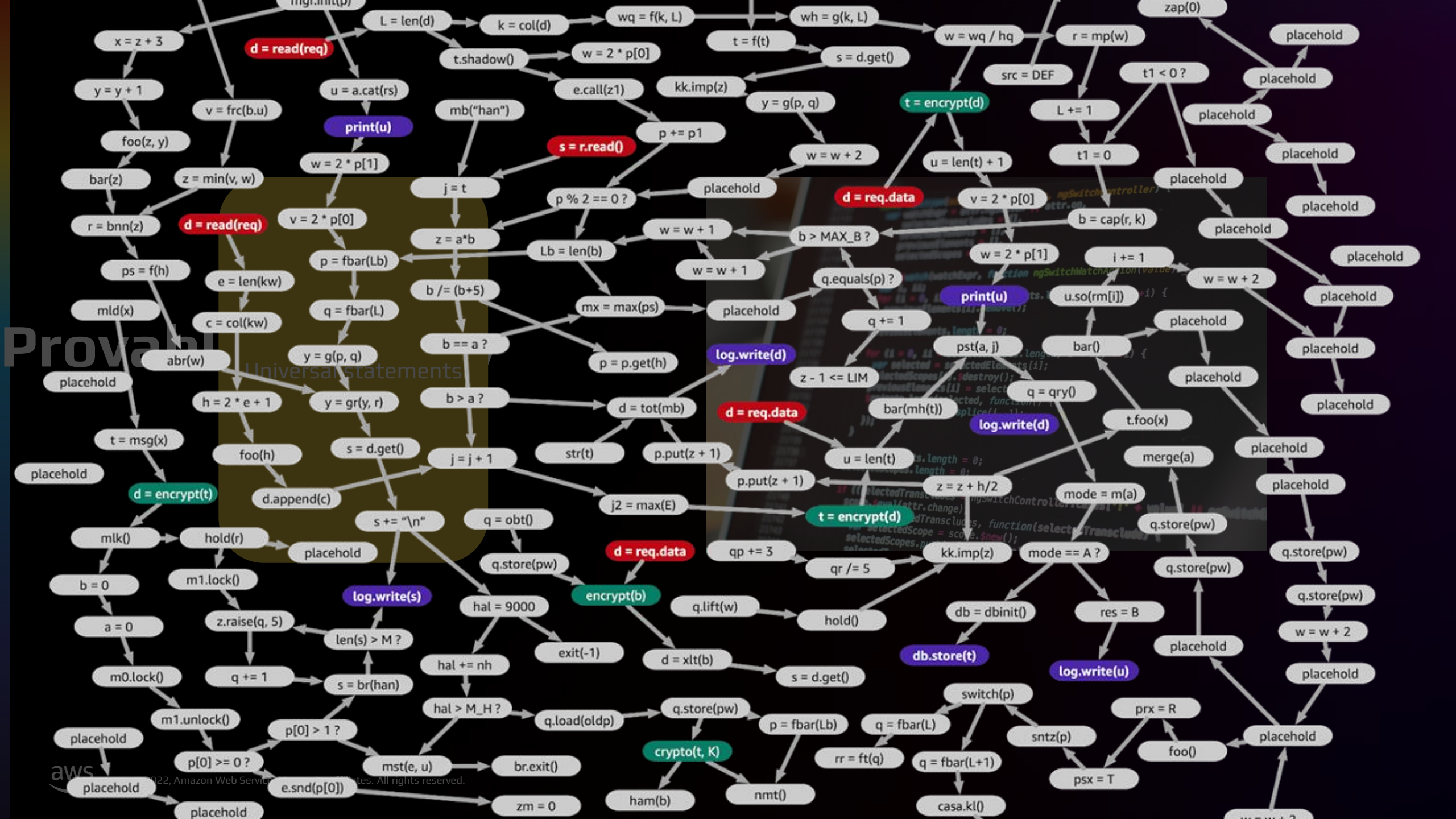
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Provable Security

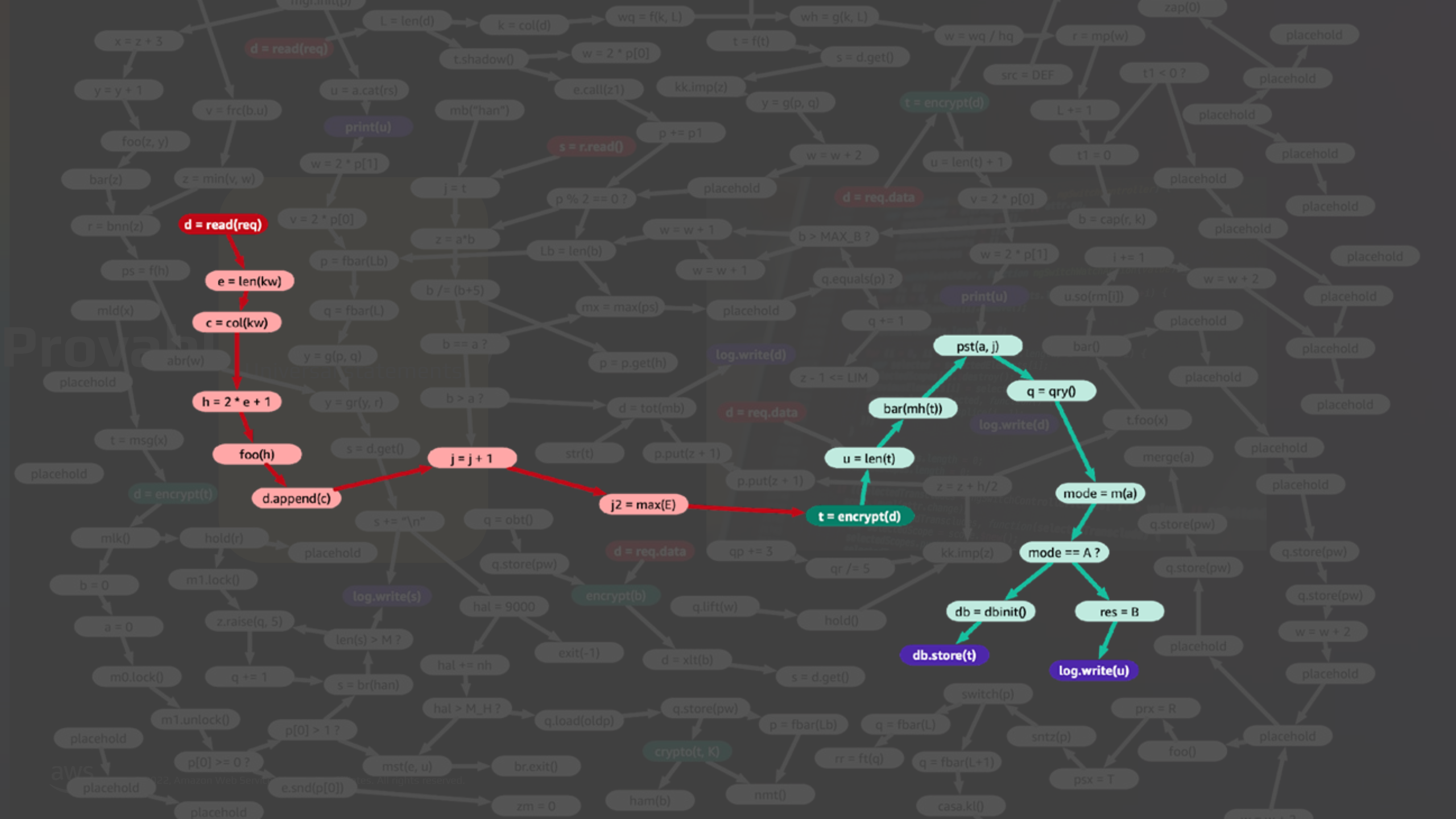
Universal Statements



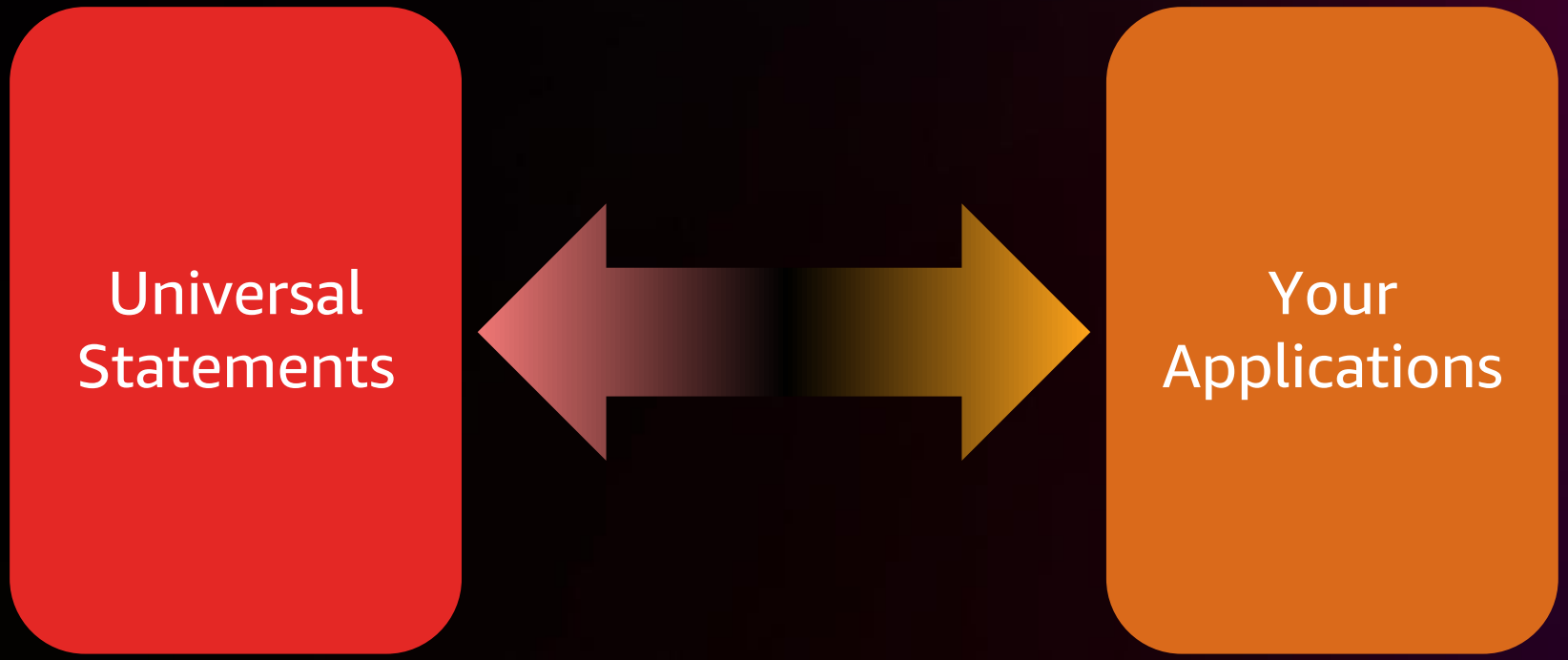
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Provable
Universal statements
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.


d = read(req)
e = len(kw)
c = col(kw)
h = 2 * e + 1
foo(h)
d.append(c)
j = j + 1
j2 = max(E)
t = encrypt(d)
u = len(t)
bar(mh(t))
pst(a, j)
q = qry()
mode = m(a)
mode == A ?
db = dbinit()
res = B
db.store(t)
log.write(u)

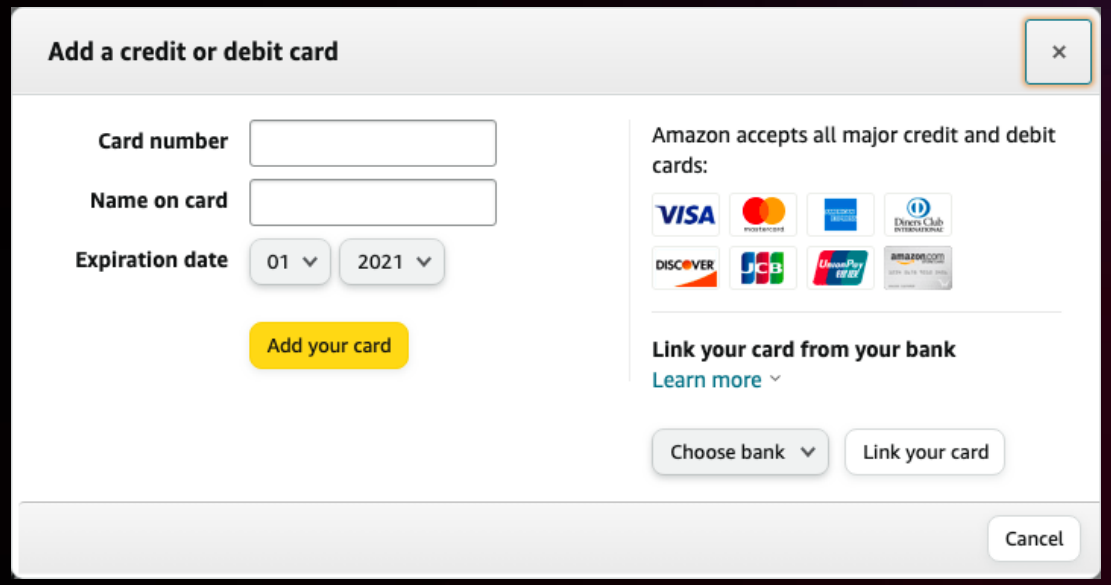
Provable Security



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Case study:
Amazon consumer payments

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

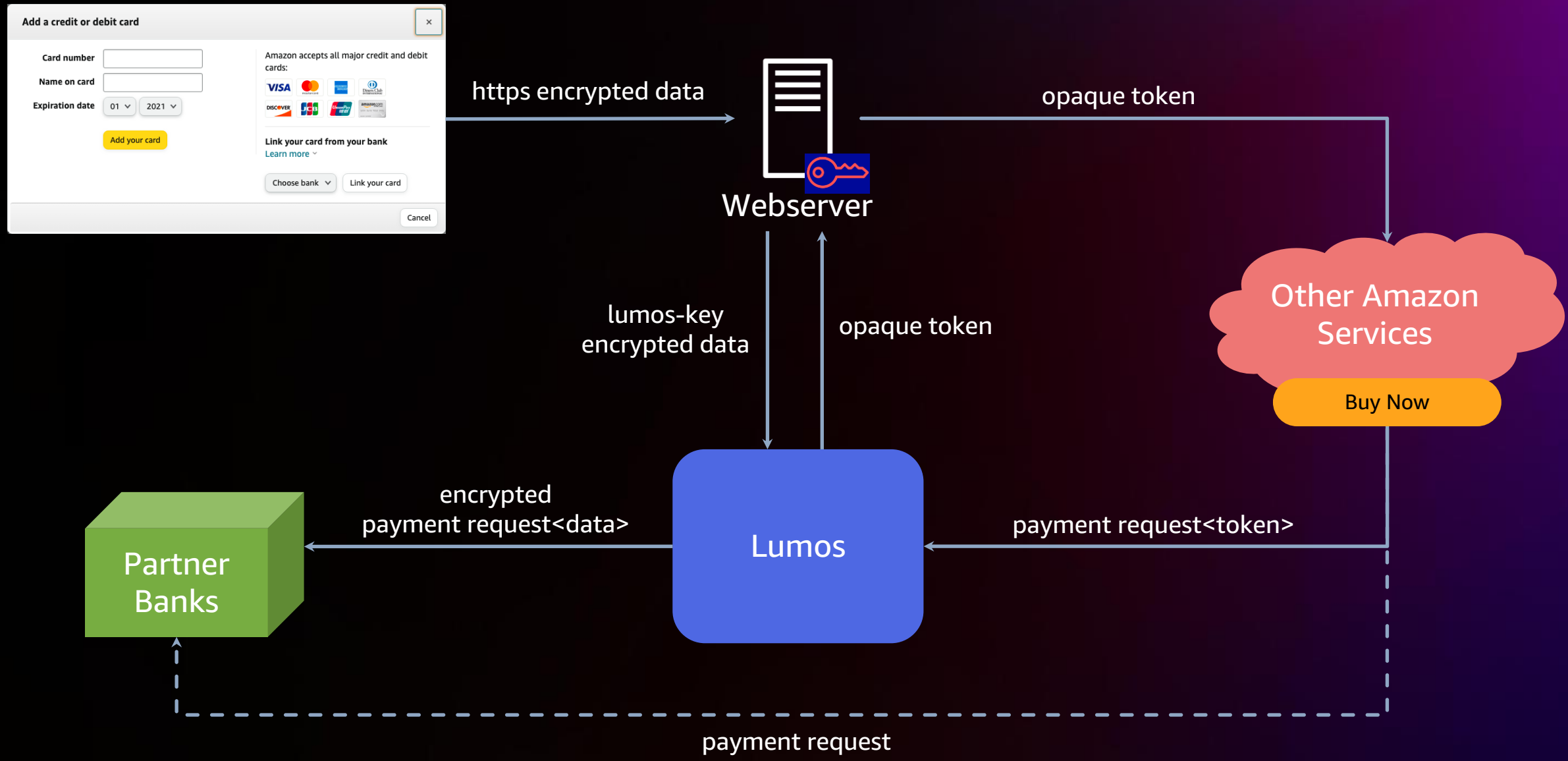


Custom, on-prem, isolated

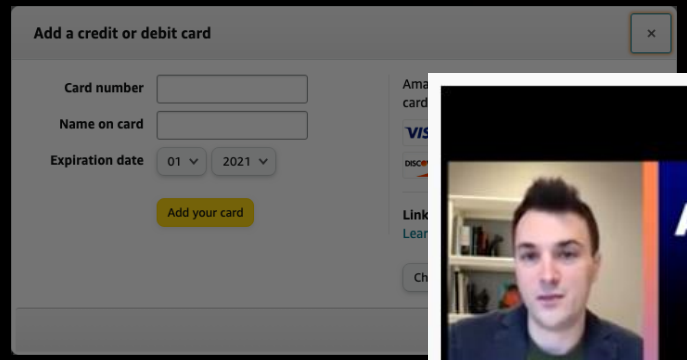


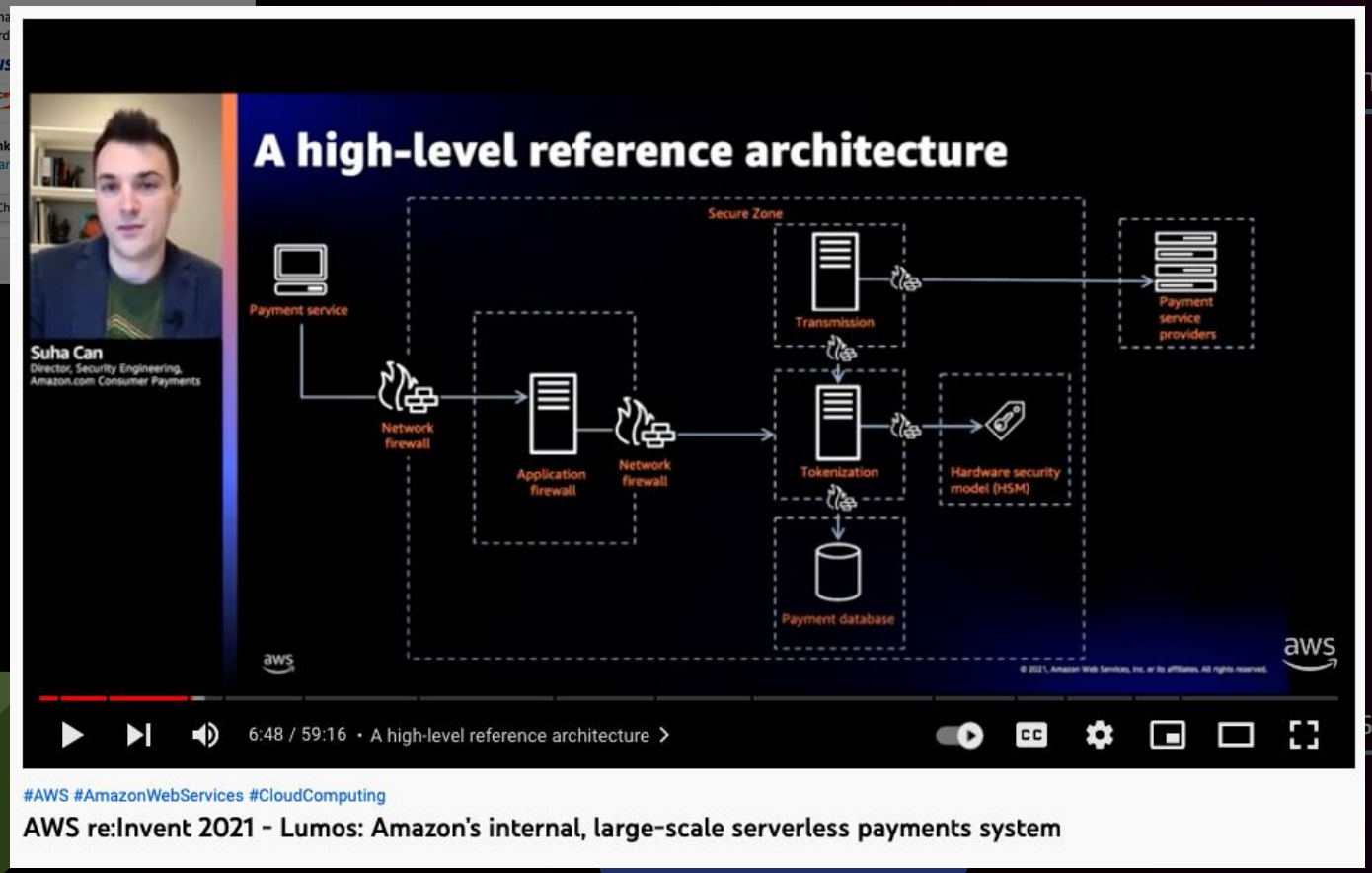
Lumos

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.





Other Amazon Services

Buy Now

Partner Banks

st<token>

payment request

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Customer data



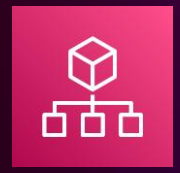
1. Treat customer data like it’s radioactive
2. Build a containment unit out of AWS



AWS Identity and Access Management (IAM)



Amazon Virtual Private Cloud (Amazon VPC)



AWS Organizations

1. Ensure exposure is not even theoretically possible

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

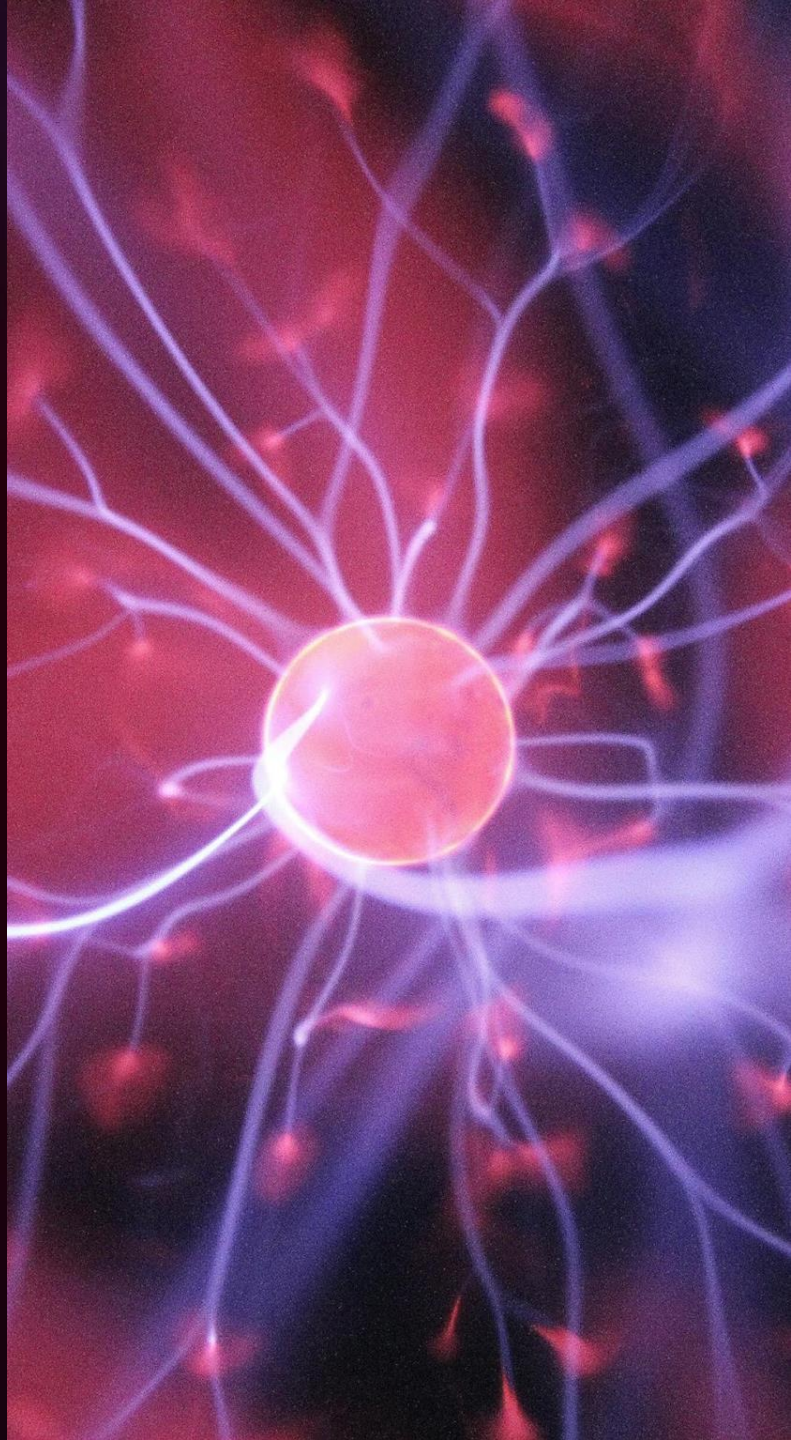
“We are never unintentionally exposed to customer data”

- Amazon Consumer Payments

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Critical zone

- Need to know where all the critical data is
- Need to know where it can go
- Need to know where it can *never* go



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

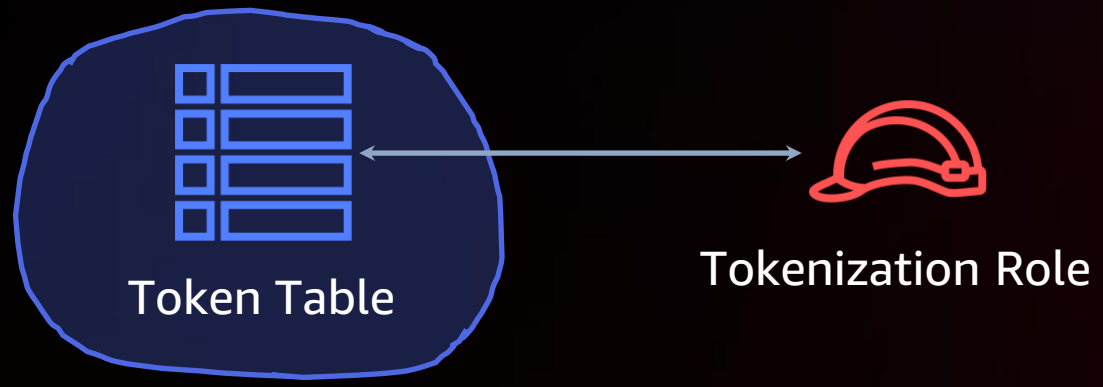


Token Table

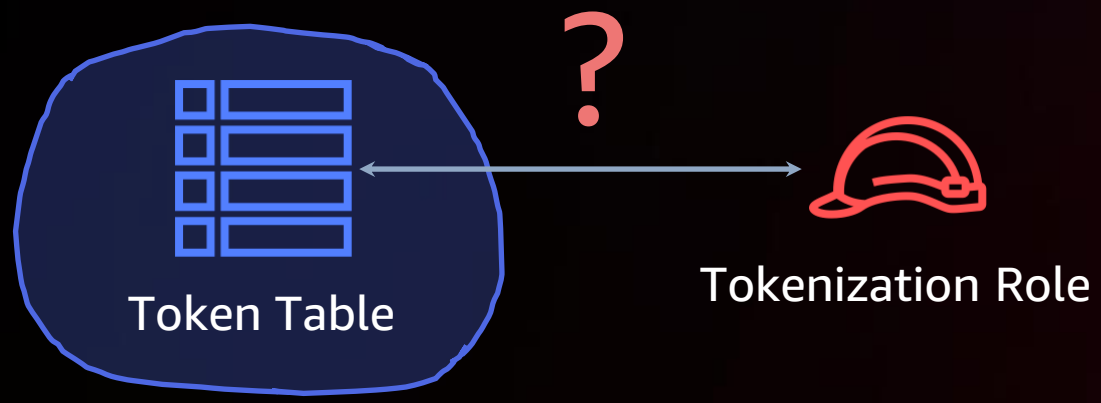
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



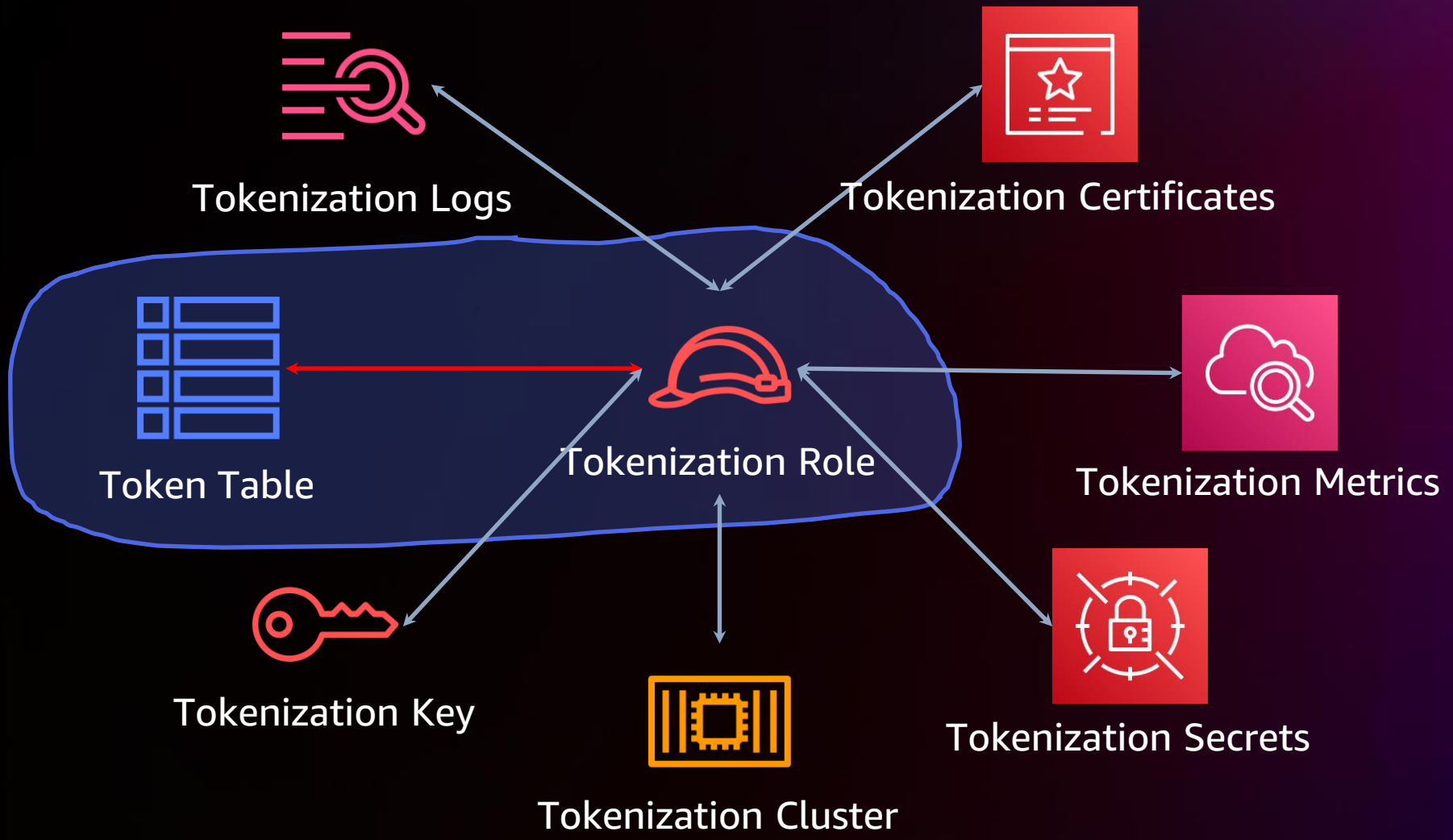
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



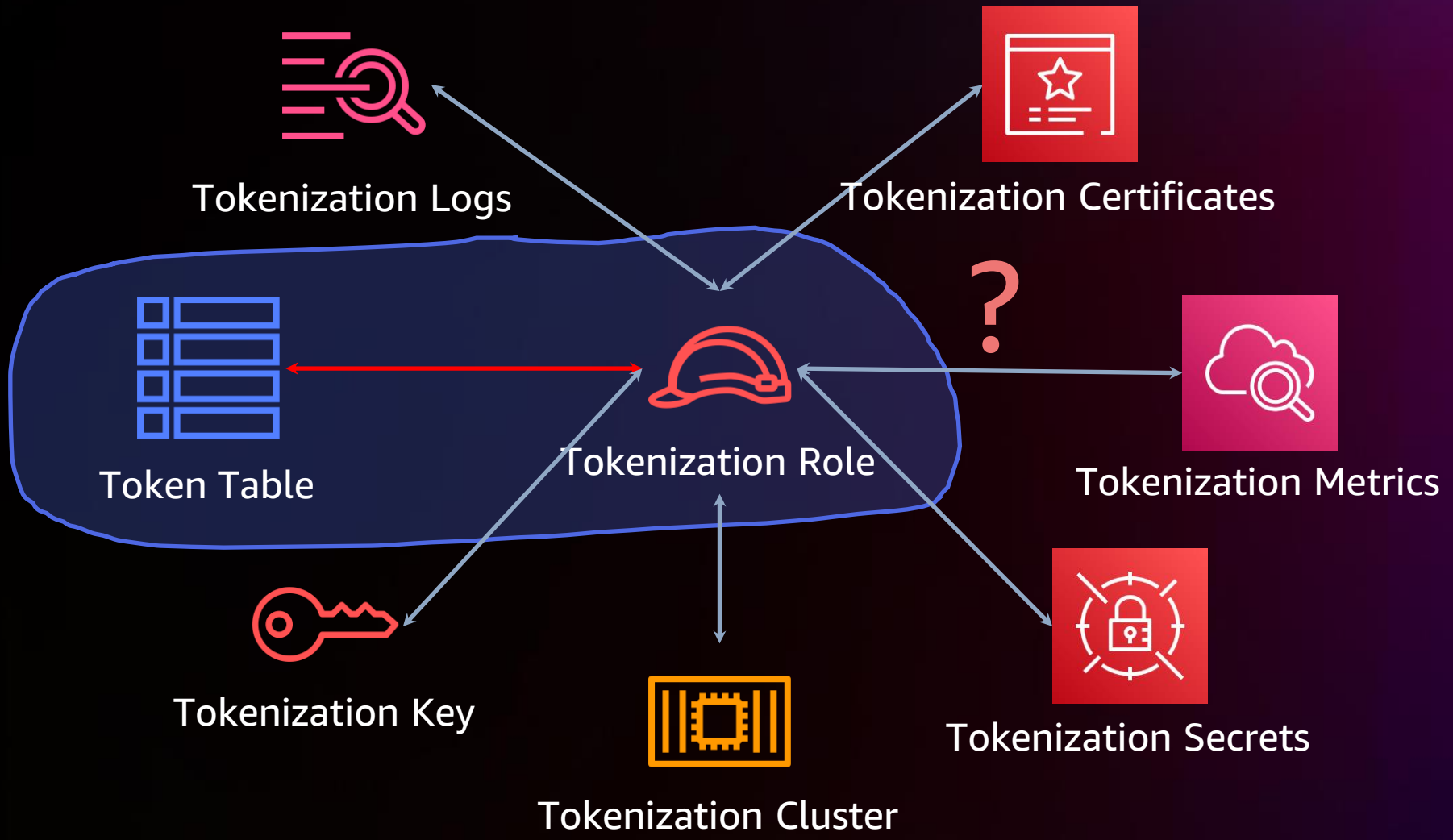
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



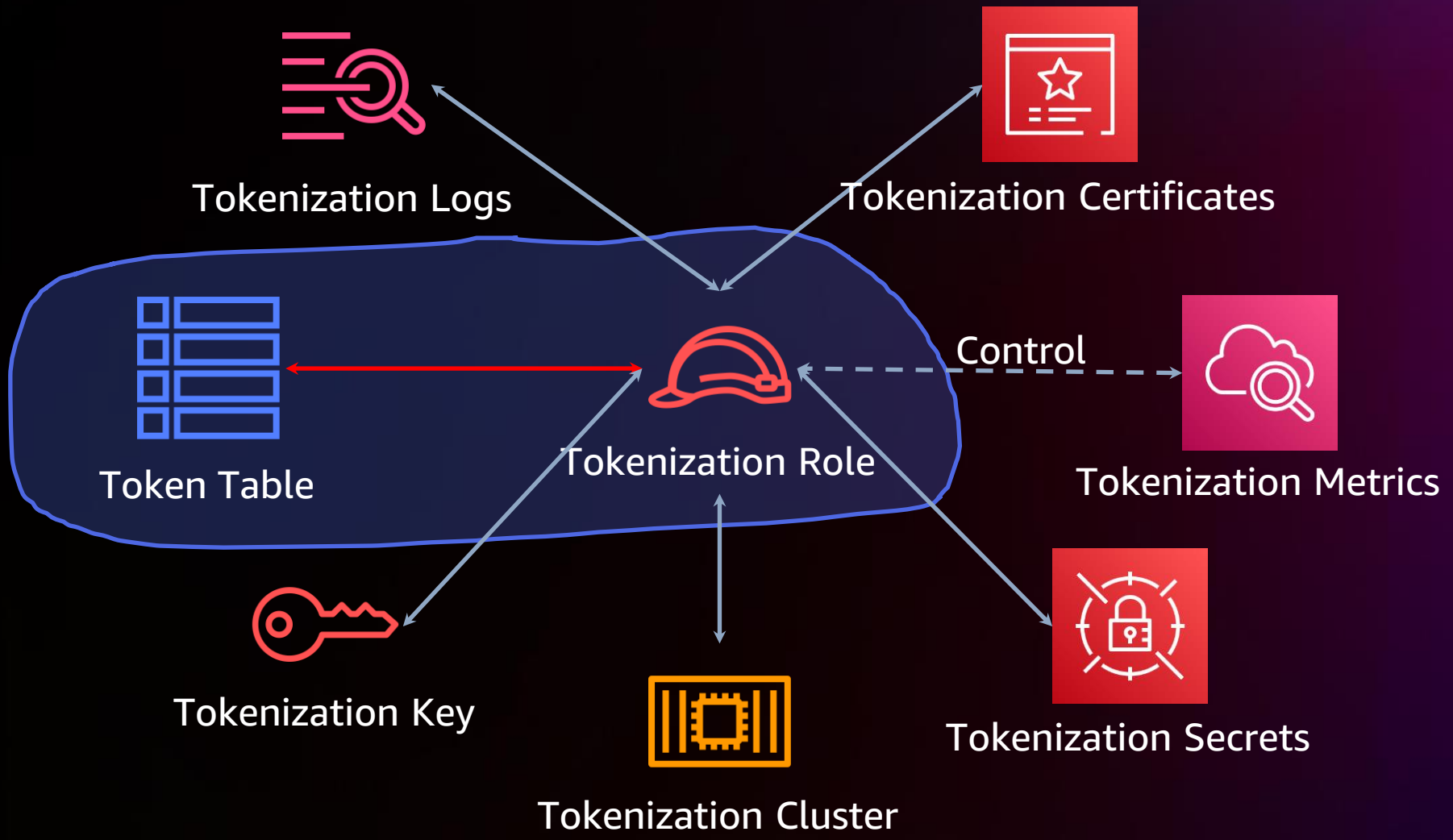
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



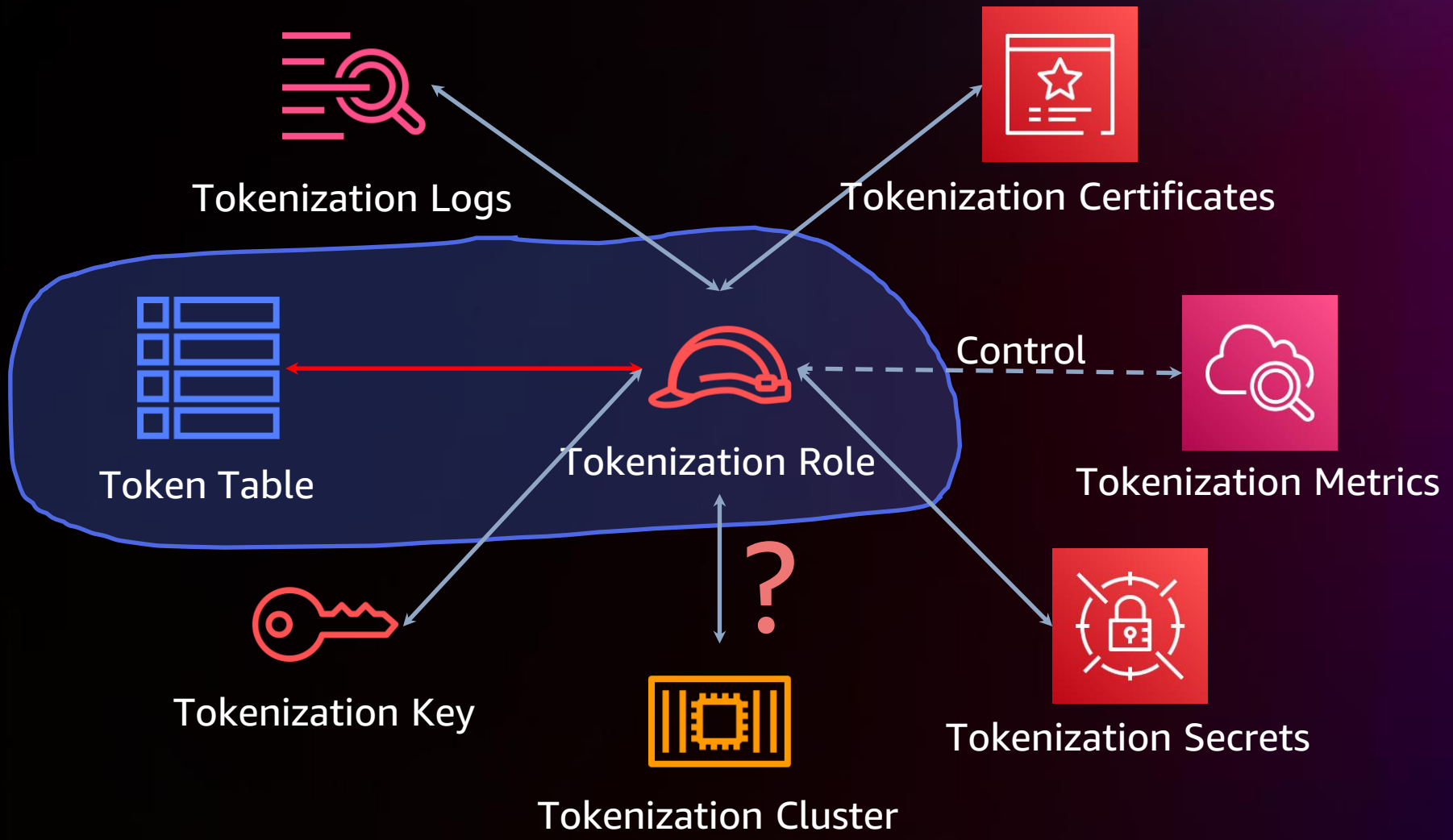
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



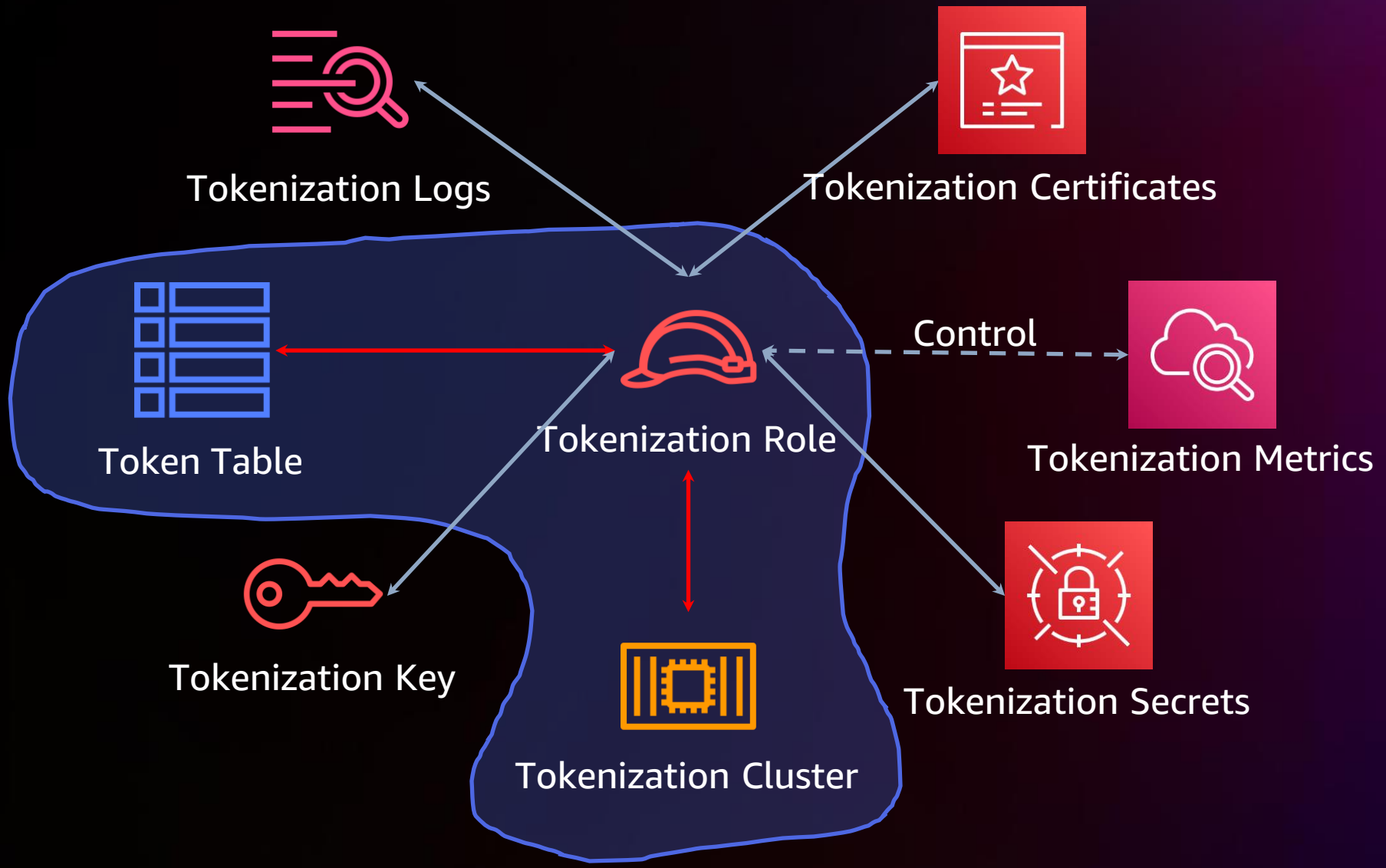
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



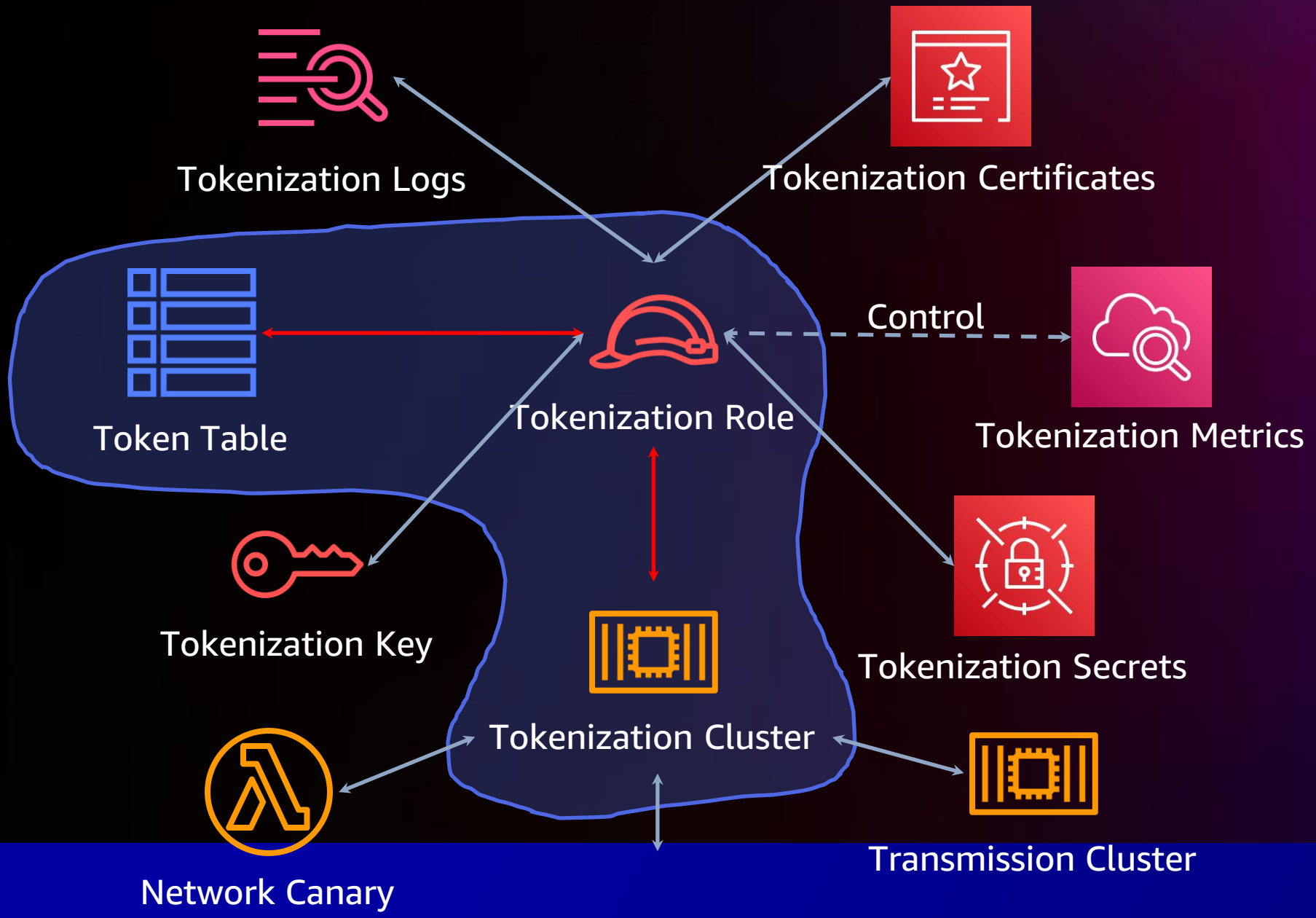
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

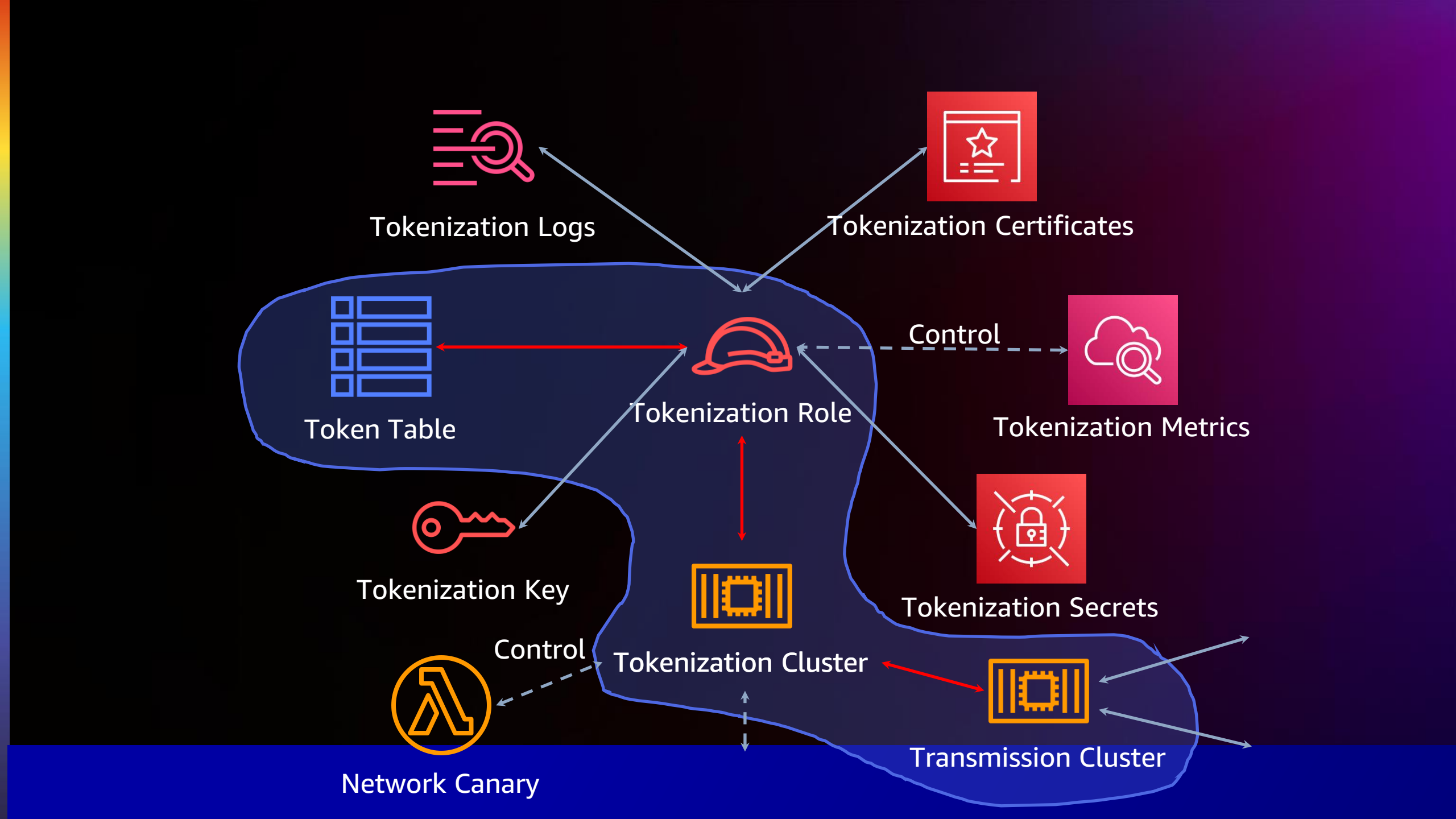


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

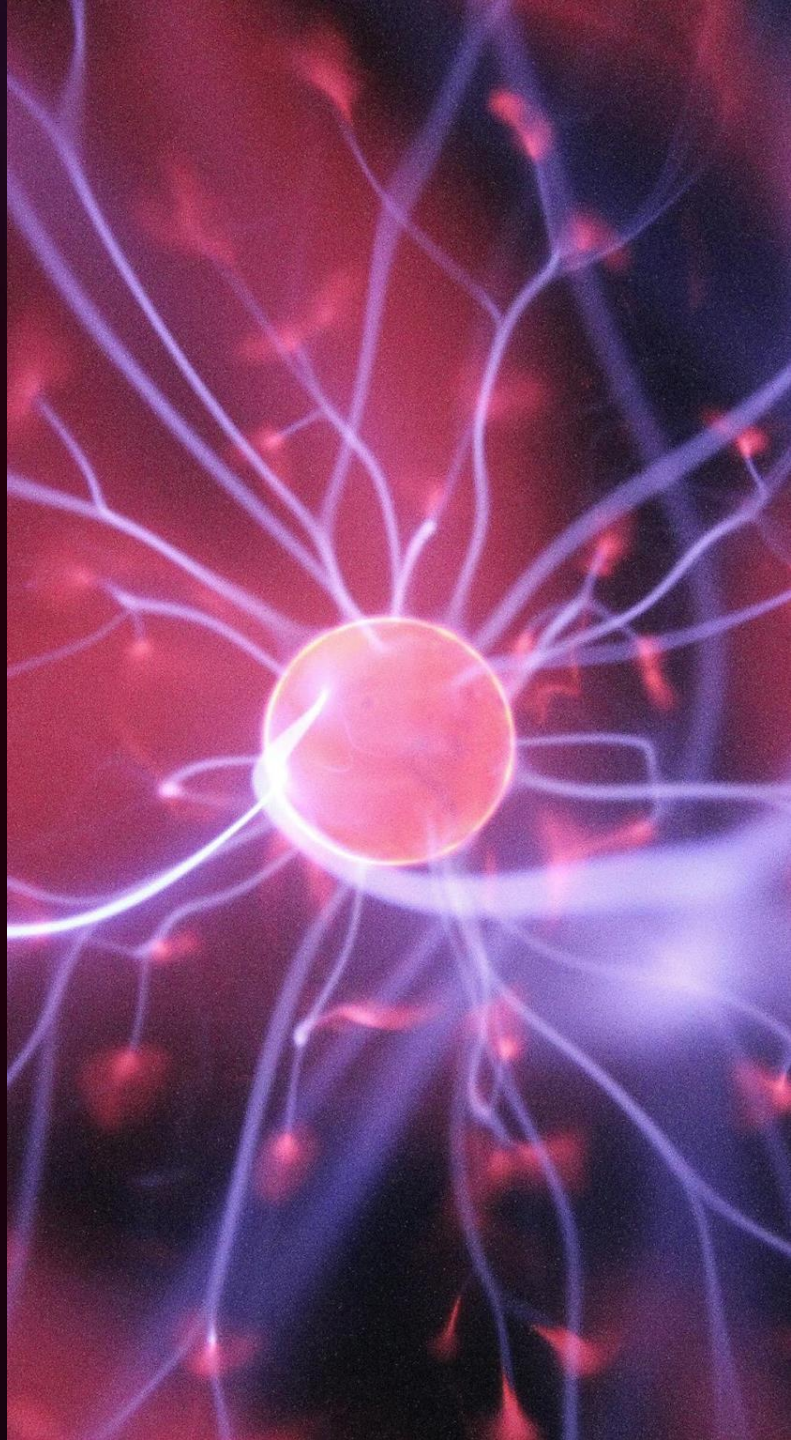

Tokenization Logs
Tokenization Certificates
Control
Token Table
Tokenization Role
Tokenization Metrics
Tokenization Key
Tokenization Secrets
Tokenization Cluster
Transmission Cluster
Network Canary


Tokenization Logs
Tokenization Certificates
Control
Token Table
Tokenization Role
Tokenization Metrics
Tokenization Key
Tokenization Secrets
Control
Tokenization Cluster
Transmission Cluster
Network Canary

Critical zone

- Know where all the critical data is
- Know where it can go
- Know where it can *never* go

"We are *never* unintentionally exposed to customer data"



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Universal statements

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Universal security statements



"My S3 buckets are not publicly accessible"



"There is no unknown external access to my S3 buckets"



"All SSH traffic to my instances goes through a firewall"

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

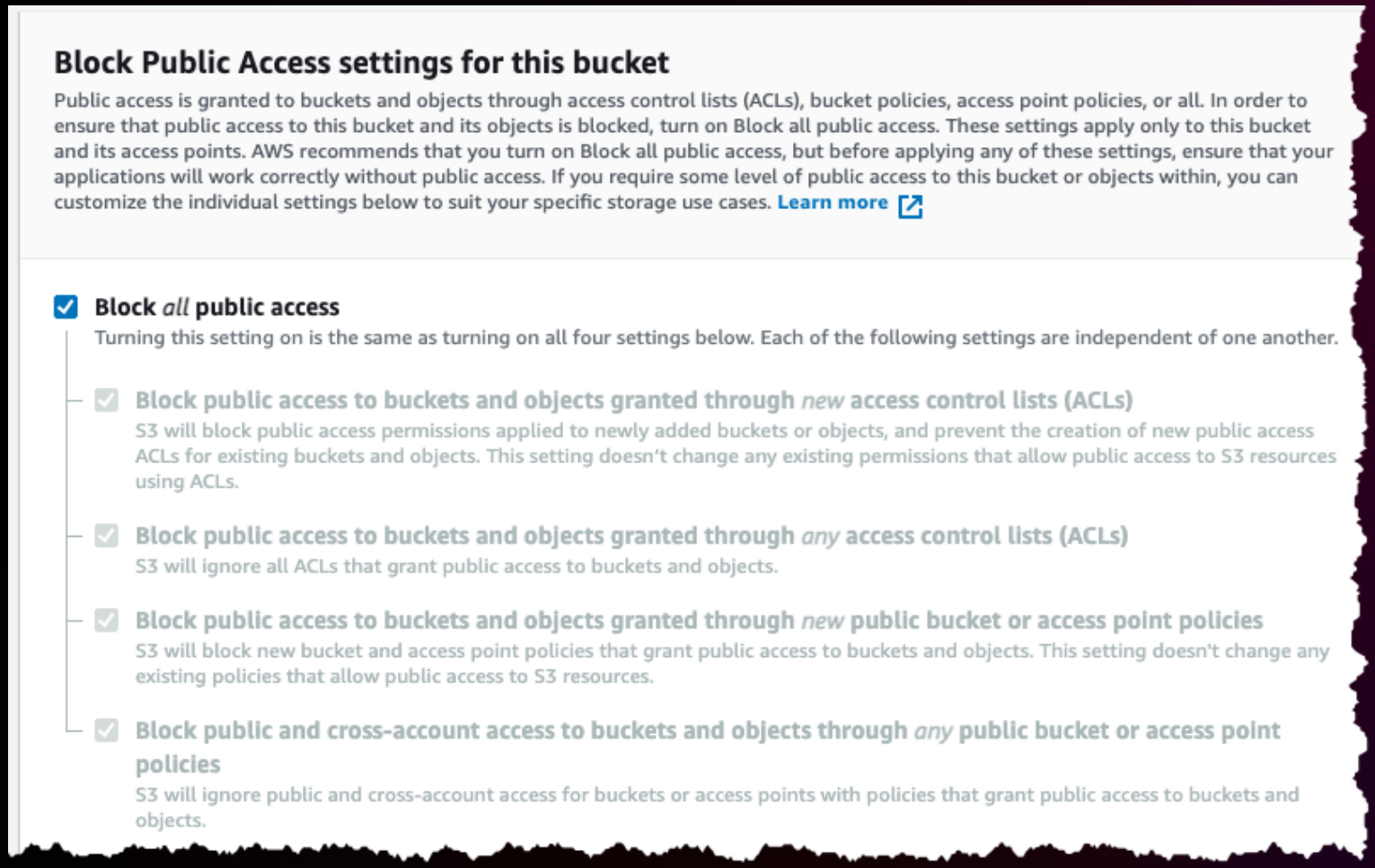
“My S3 buckets are not publicly accessible”

You

After using S3 Block Public Access

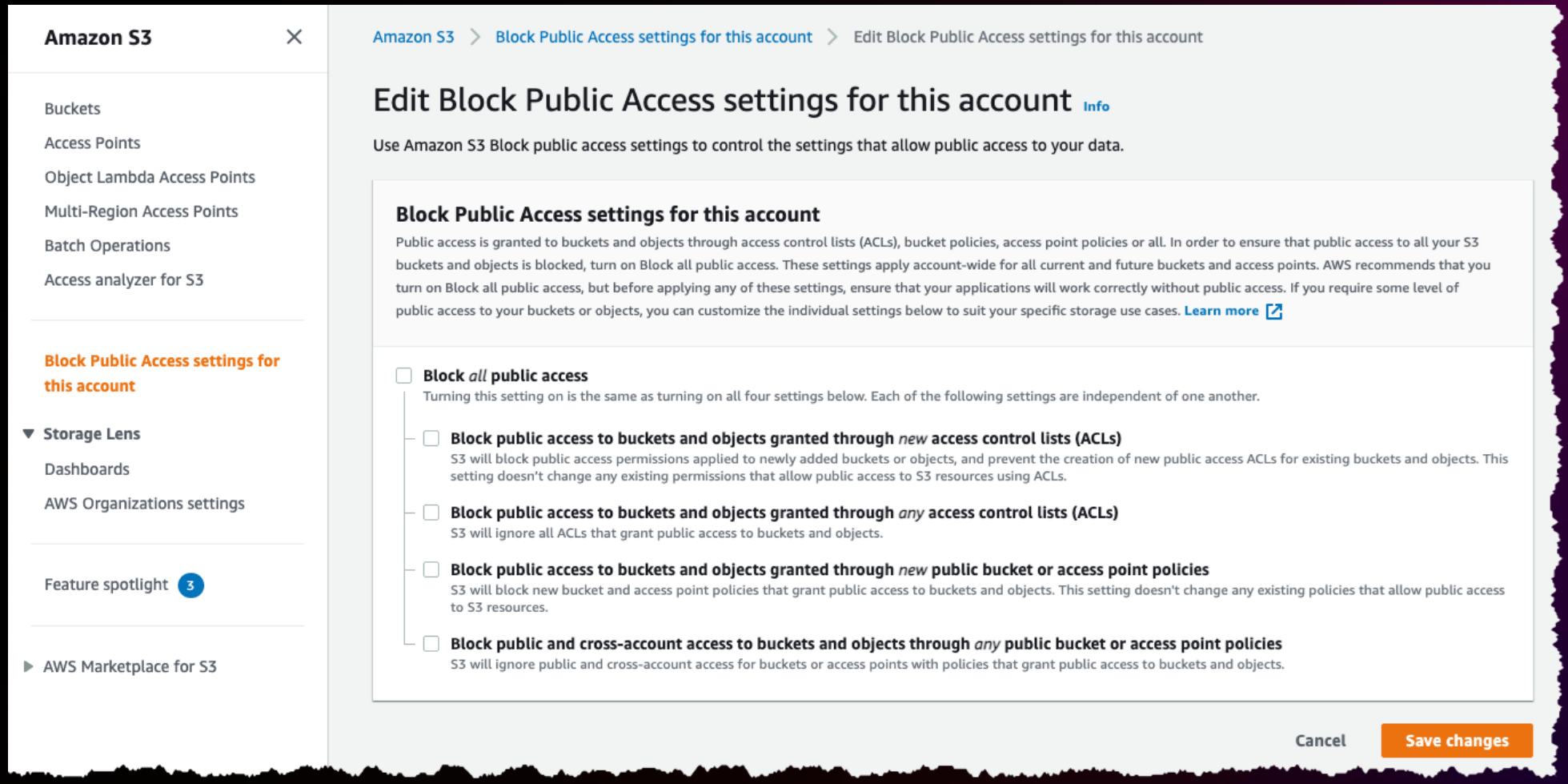
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

S3: Block Public Access



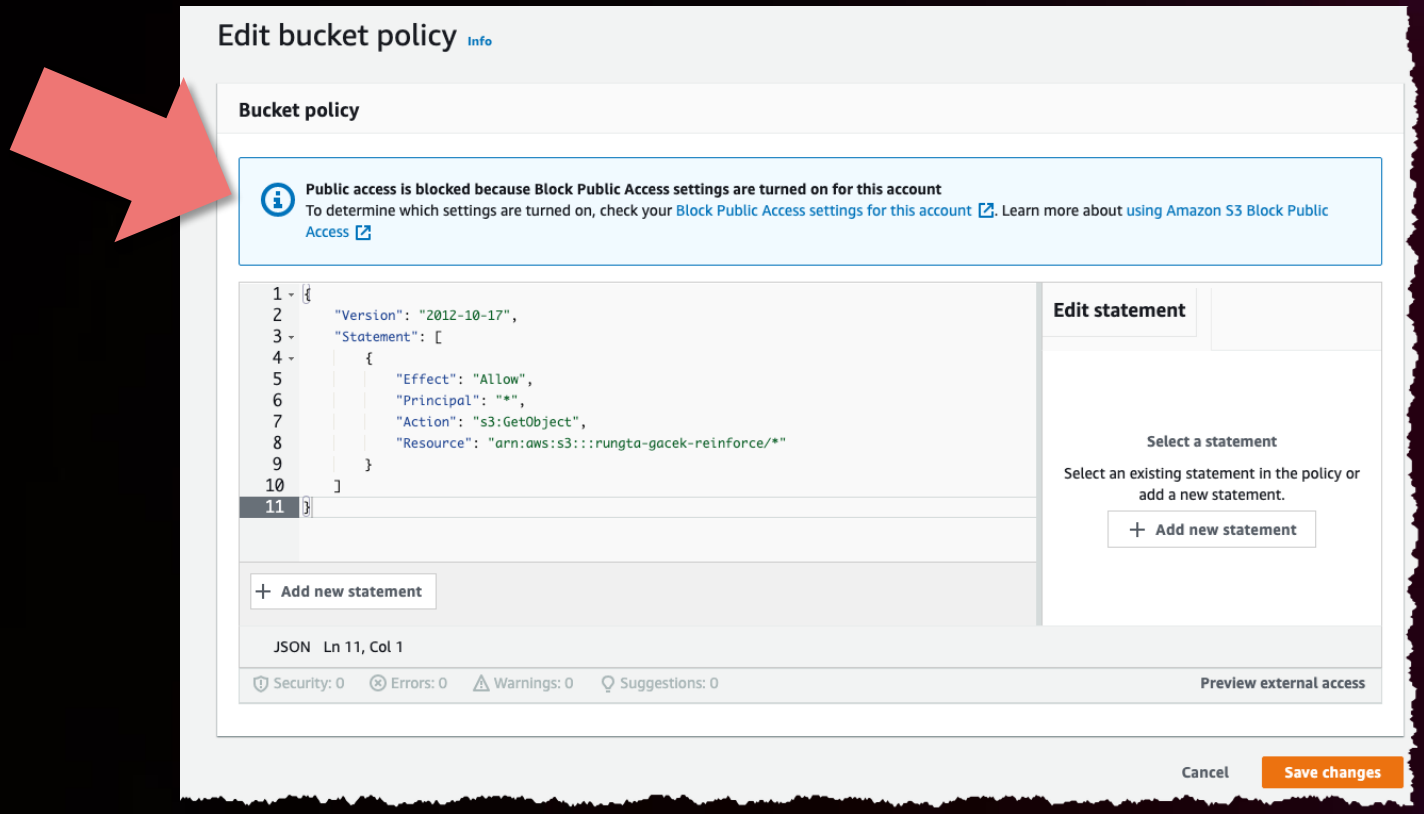
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

S3: Block Public Access



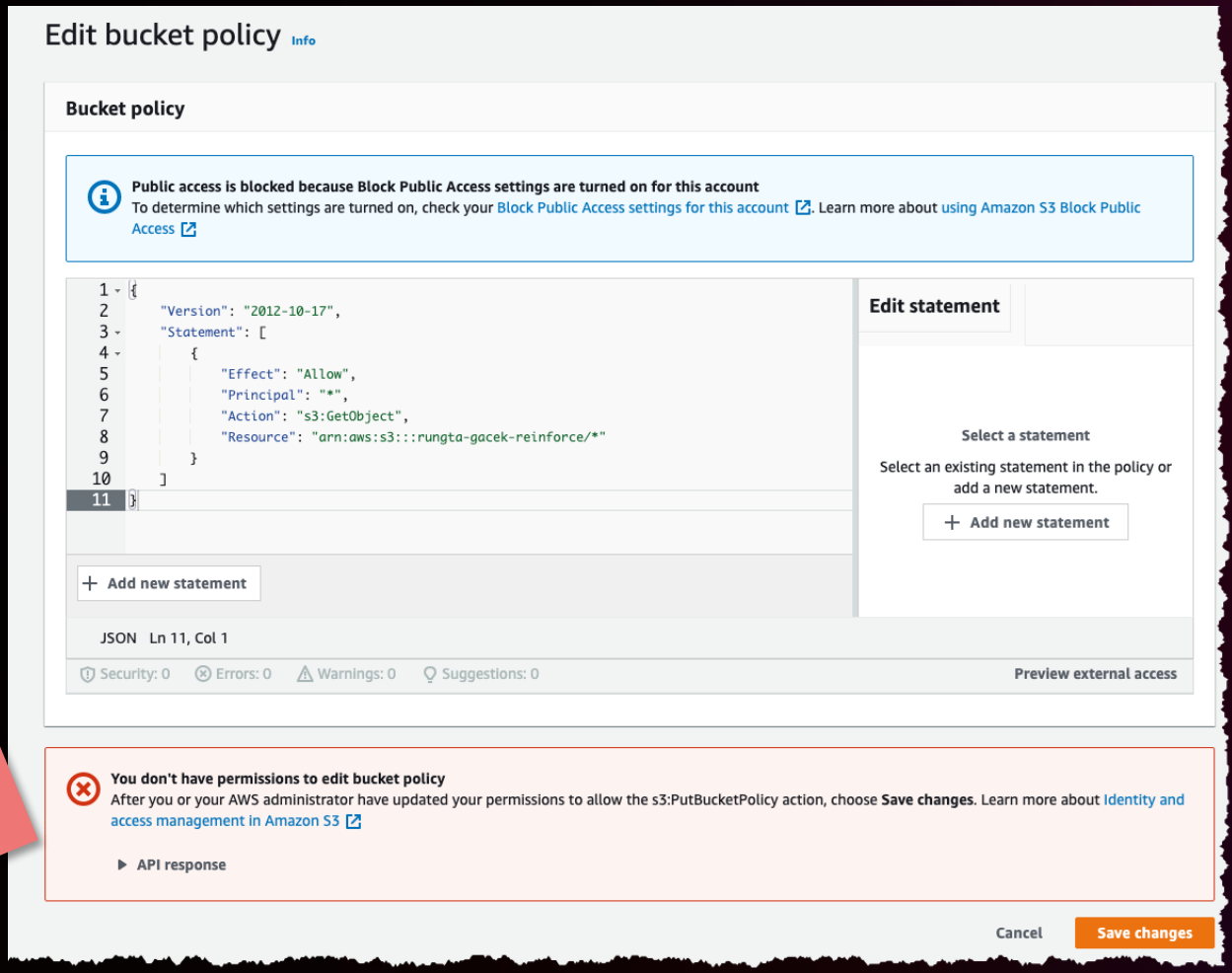
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

S3: Block Public Access



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

S3: Block Public Access



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

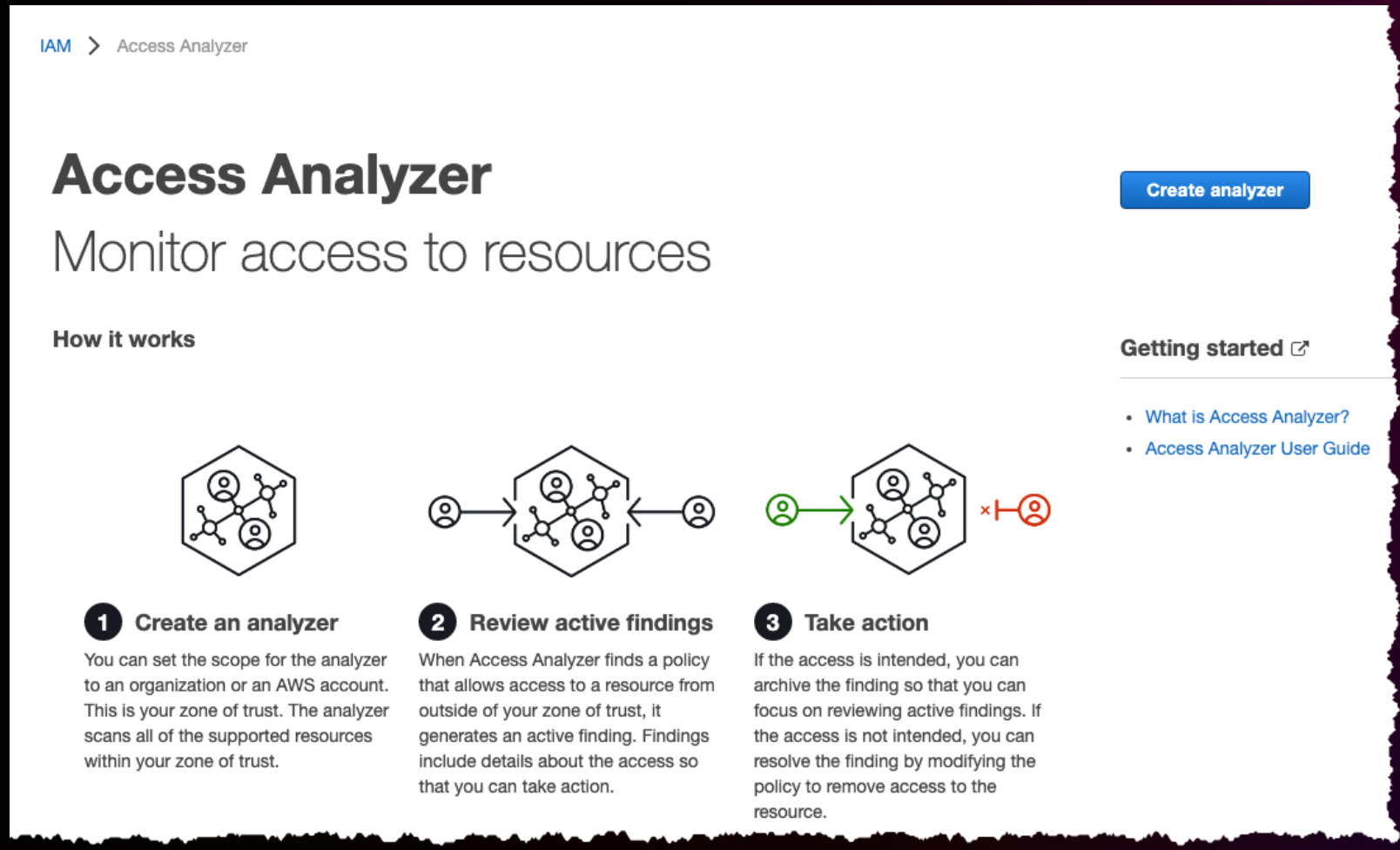
“There is no unknown external access to my S3 buckets”

You

After using IAM Access Analyzer

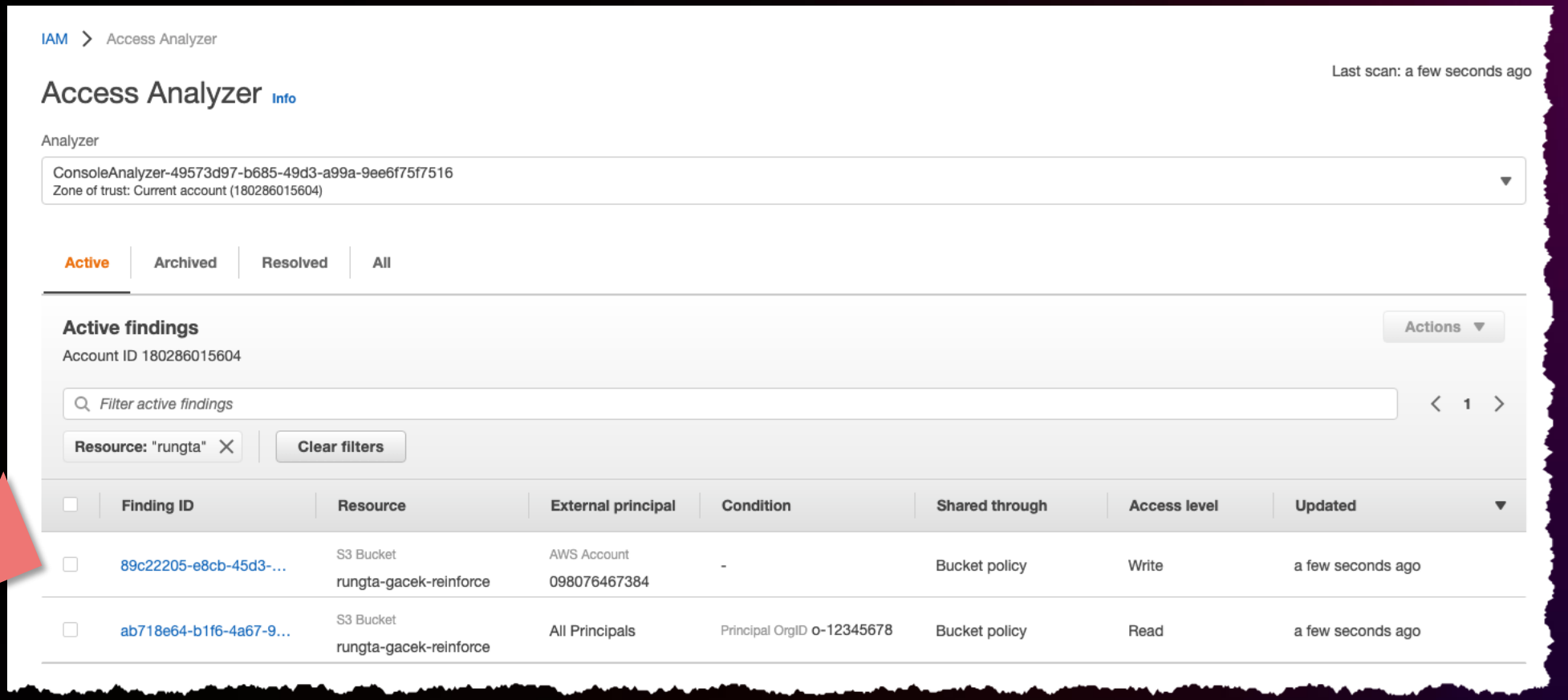
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IAM Access Analyzer



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

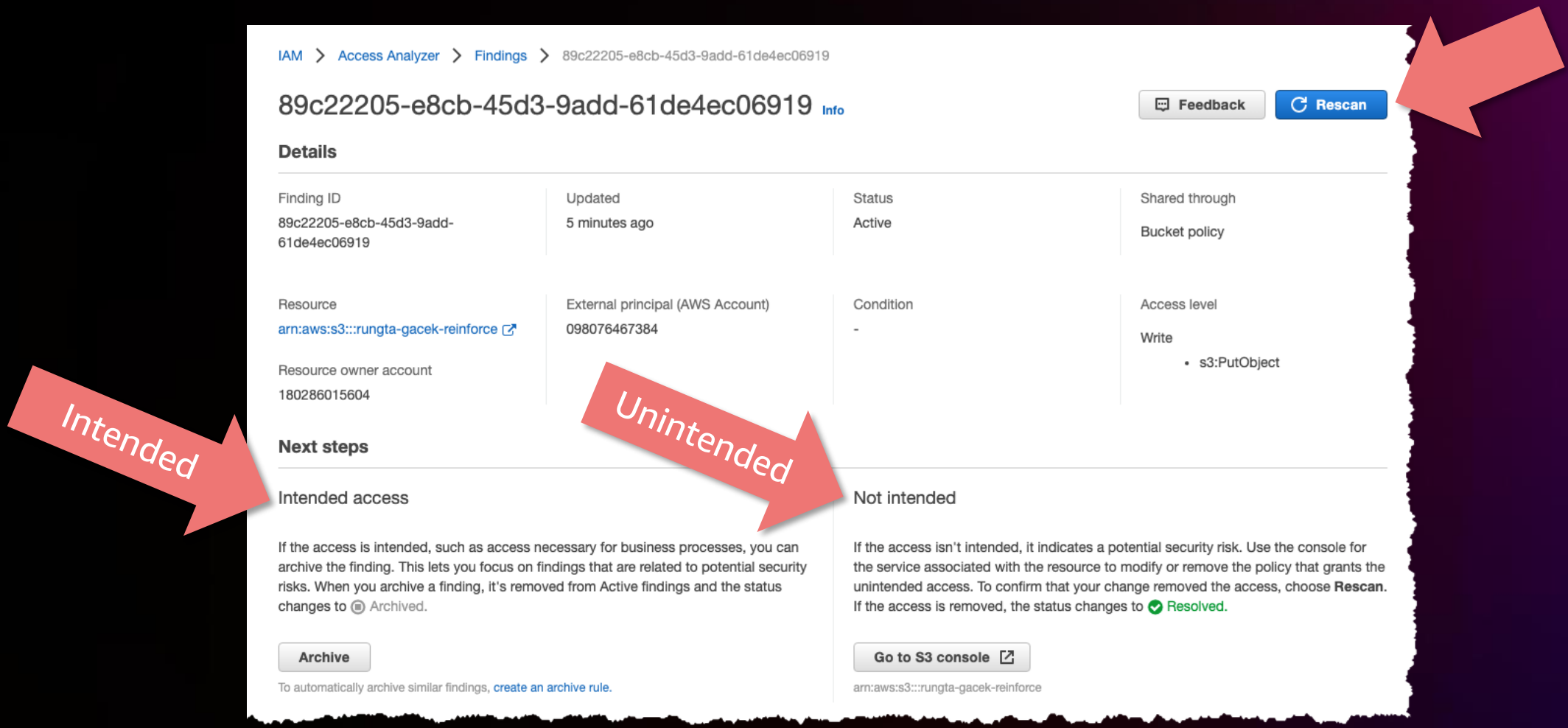
IAM Access Analyzer



2 findings

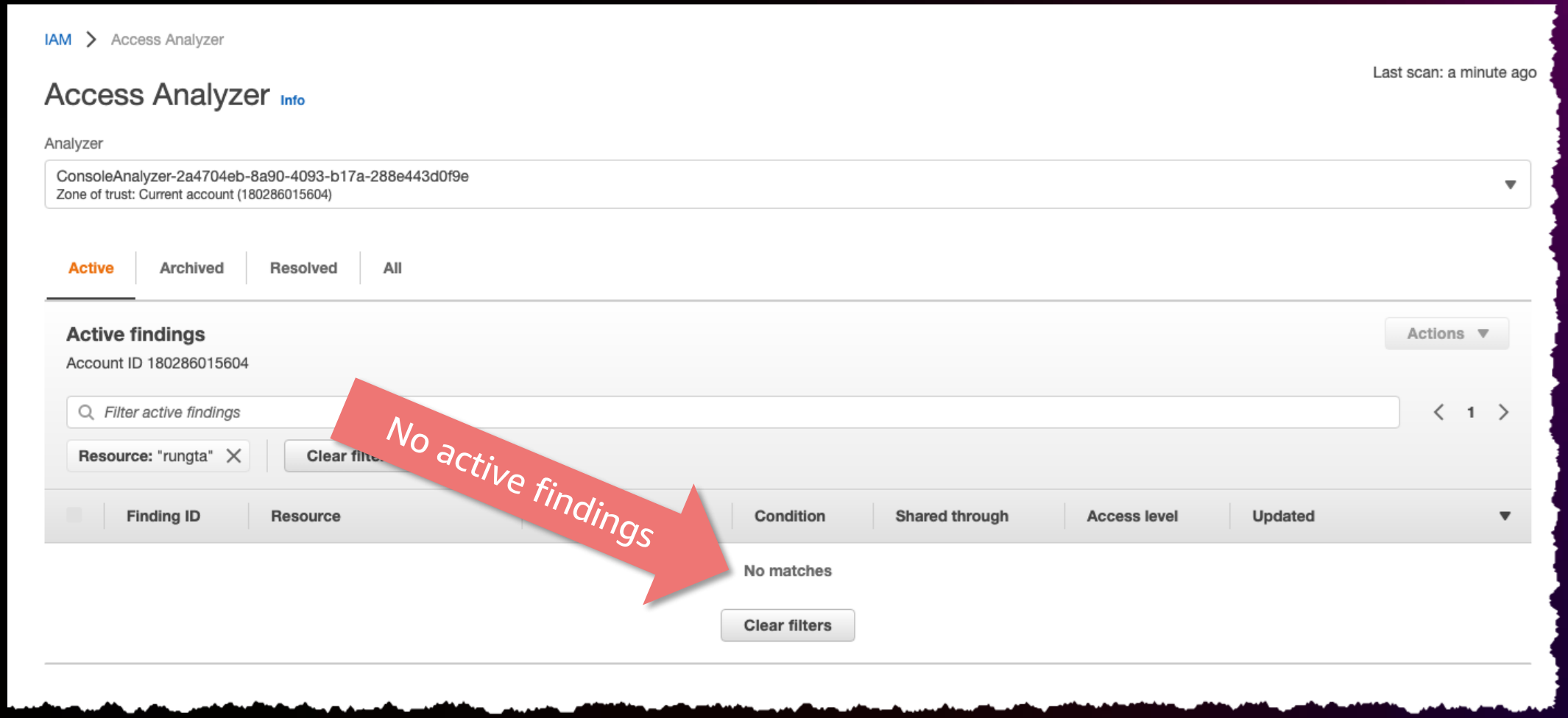
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IAM Access Analyzer



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IAM Access Analyzer



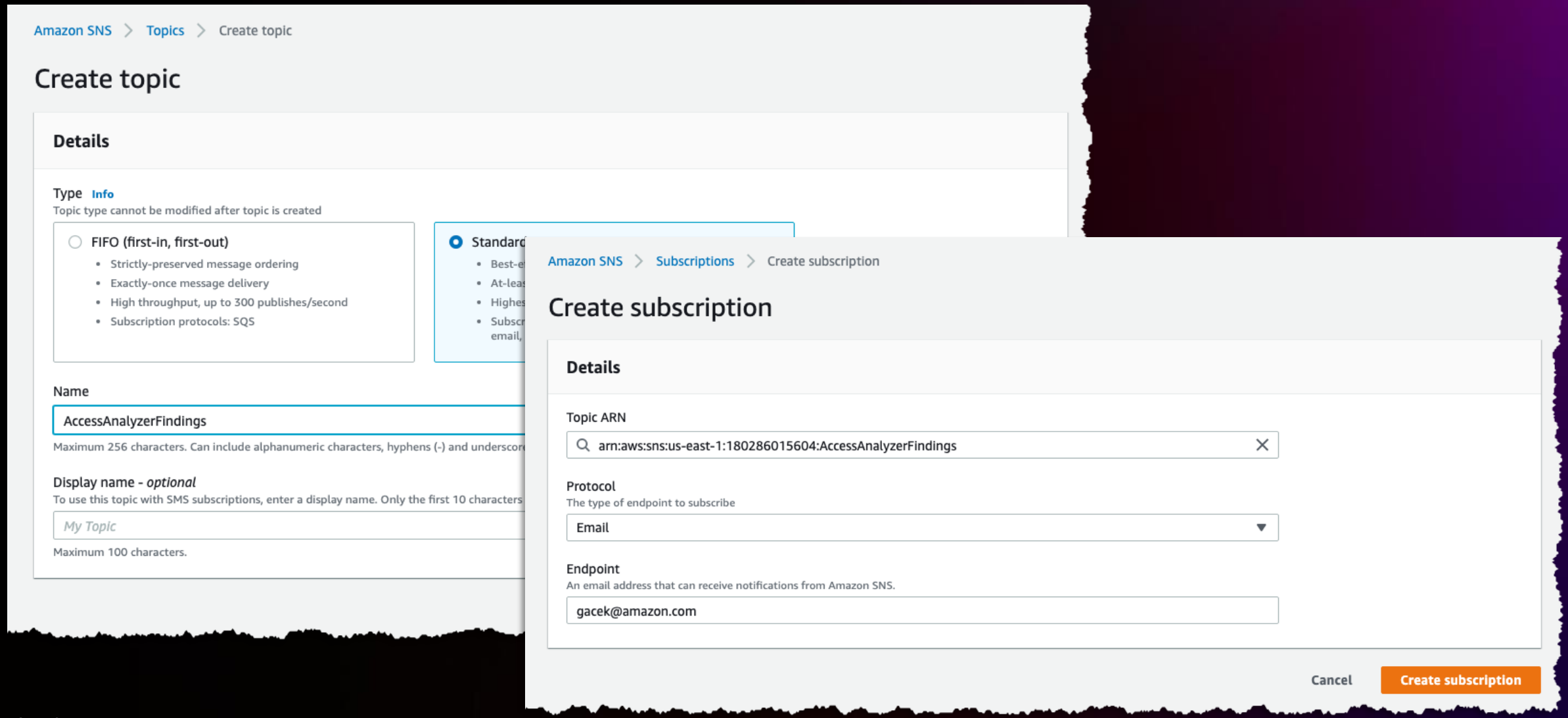
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IAM Access Analyzer: Alerts



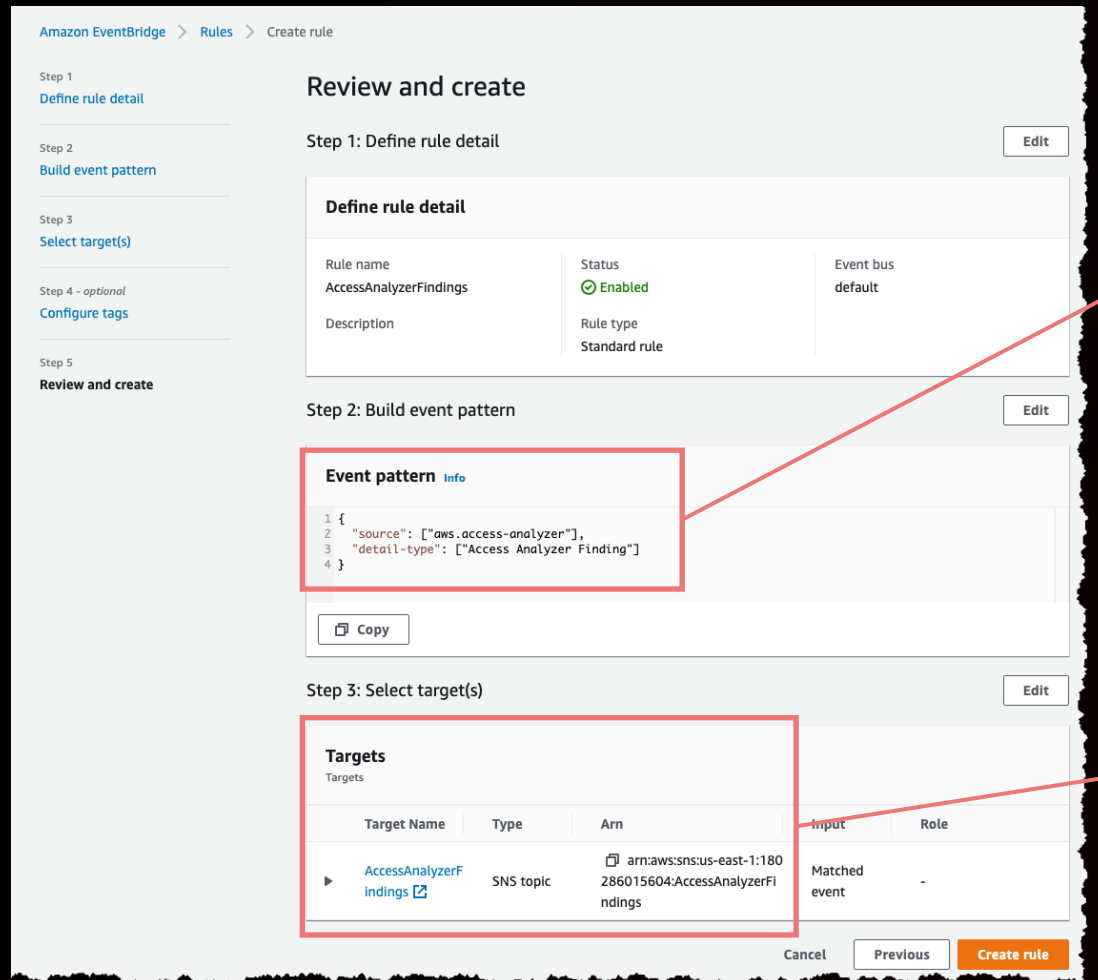
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

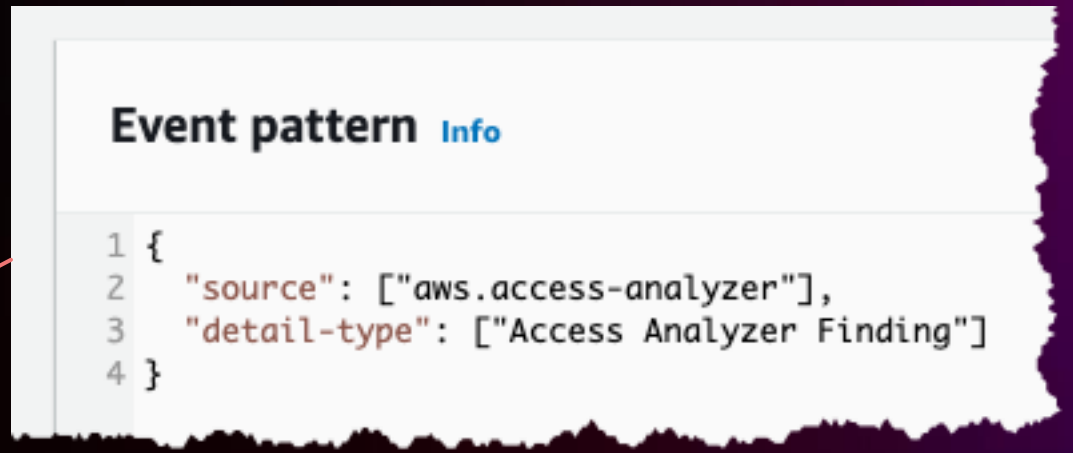
SNS Topic

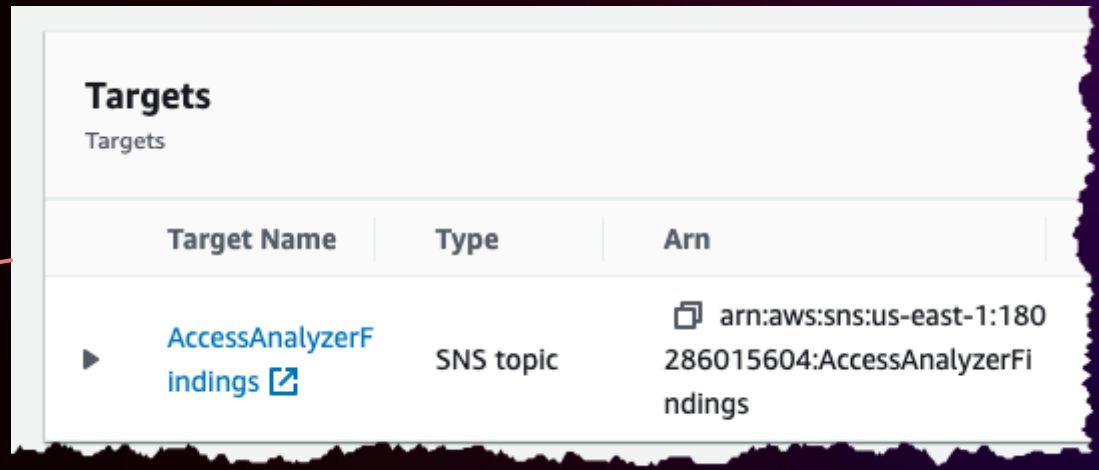


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

EventBridge Rule







© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

S3: Update Policy

Bucket ARN

arn:aws:s3:::rungta-gacek-reinforce

Policy

```
{
    "Effect": "Allow",
    "Principal": "*",
    "Action": [
        "s3:GetObject",
        "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::rungta-gacek-rei
    "Condition": {
        "StringEquals": {
            "aws:SourceVpc": "vpc-12345678"
        }
    }
}
```

+ Add new statement

JSON Ln 36, Col 3

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Message

Delete Reply Reply All Forward

AWS Notificatio

AWS Notifications <

To: Gacek, Andrew

{"version":"0","id":"5c9b7151-5f31-8d2f-
analyzer","account":"180286015604","tim
1:180286015604:analyzer/ConsoleAnalyz
f0a78093210d","status":"ACTIVE","resou
14T16:24:30.468Z","analyzedAt":"2022-0
{"AWS":"*"},"action":["s3:GetObject","s3

--

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe.

gacek@amazon.com">https://sns.us-east-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-1:180286015604:AccessAnalyzerFindings:e39769c1-1178-49b7-8b22-a751ffdd7a97&Endpoint=gacek@amazon.com

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.amazon.com/support


```
{
  "version": "1.0",
  "id": "71985311-83c3-4a8f-b939-f0a78093210d",
  "status": "ACTIVE",
  "resourceType": "AWS::S3::Bucket",
  "resource": "arn:aws:s3:::rungta-gacek-reinforce",
  "createdAt": "2022-06-14T16:24:30.468Z",
  "analyzedAt": "2022-06-14T16:24:30.468Z",
  "updatedAt": "2022-06-14T16:24:30.468Z",
  "accountId": "180286015604",
  "region": "us-east-1",
  "principal": {
    "AWS": "*"
  },
  "action": [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "condition": {
    "aws:SourceVpc": "vpc-12345678"
  },
  "isDeleted": false,
  "isPublic": false
}
```


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

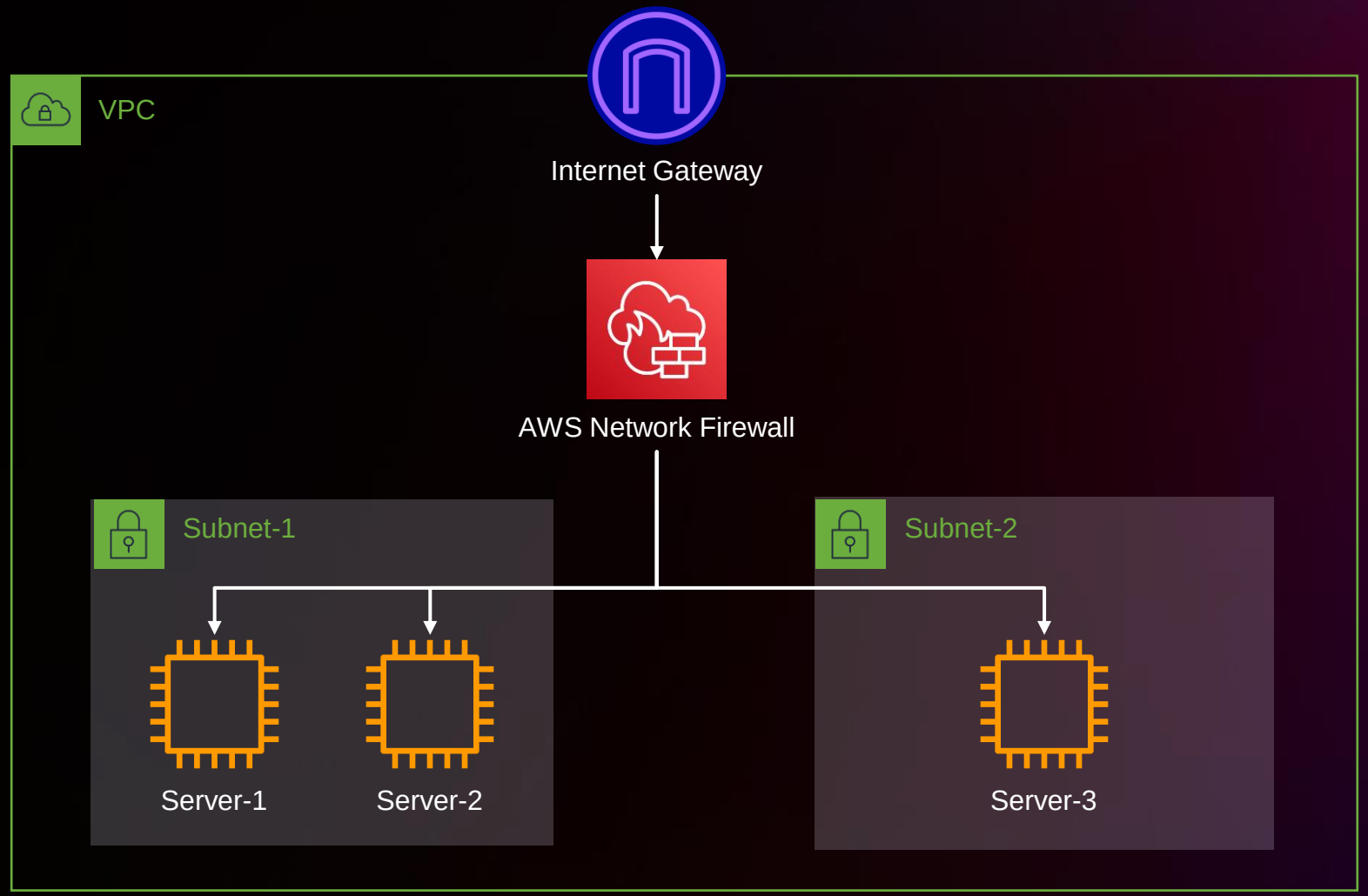
“All SSH traffic to my instances goes through a firewall”

You

After using VPC Network Access Analyzer

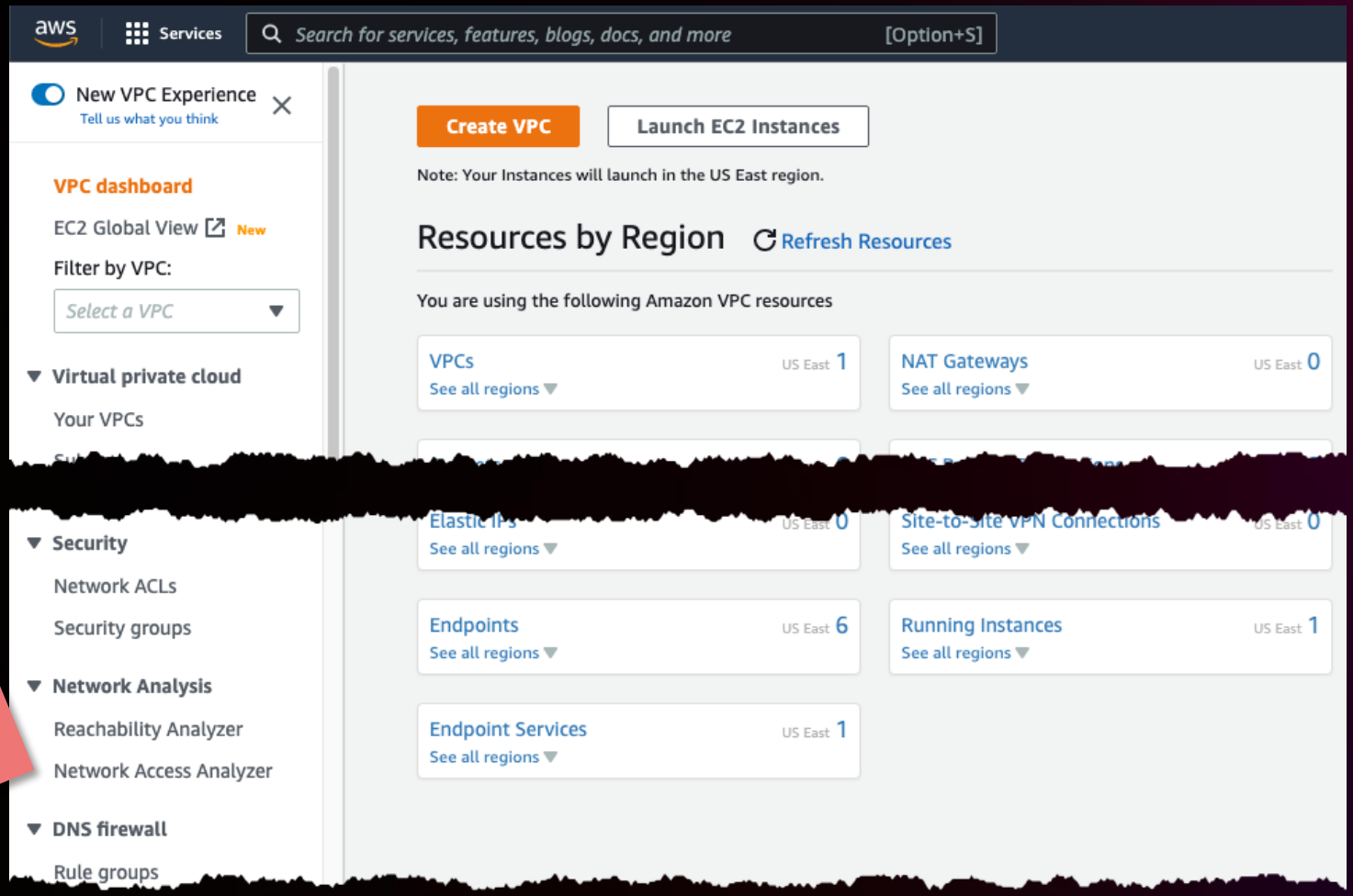
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Intended network



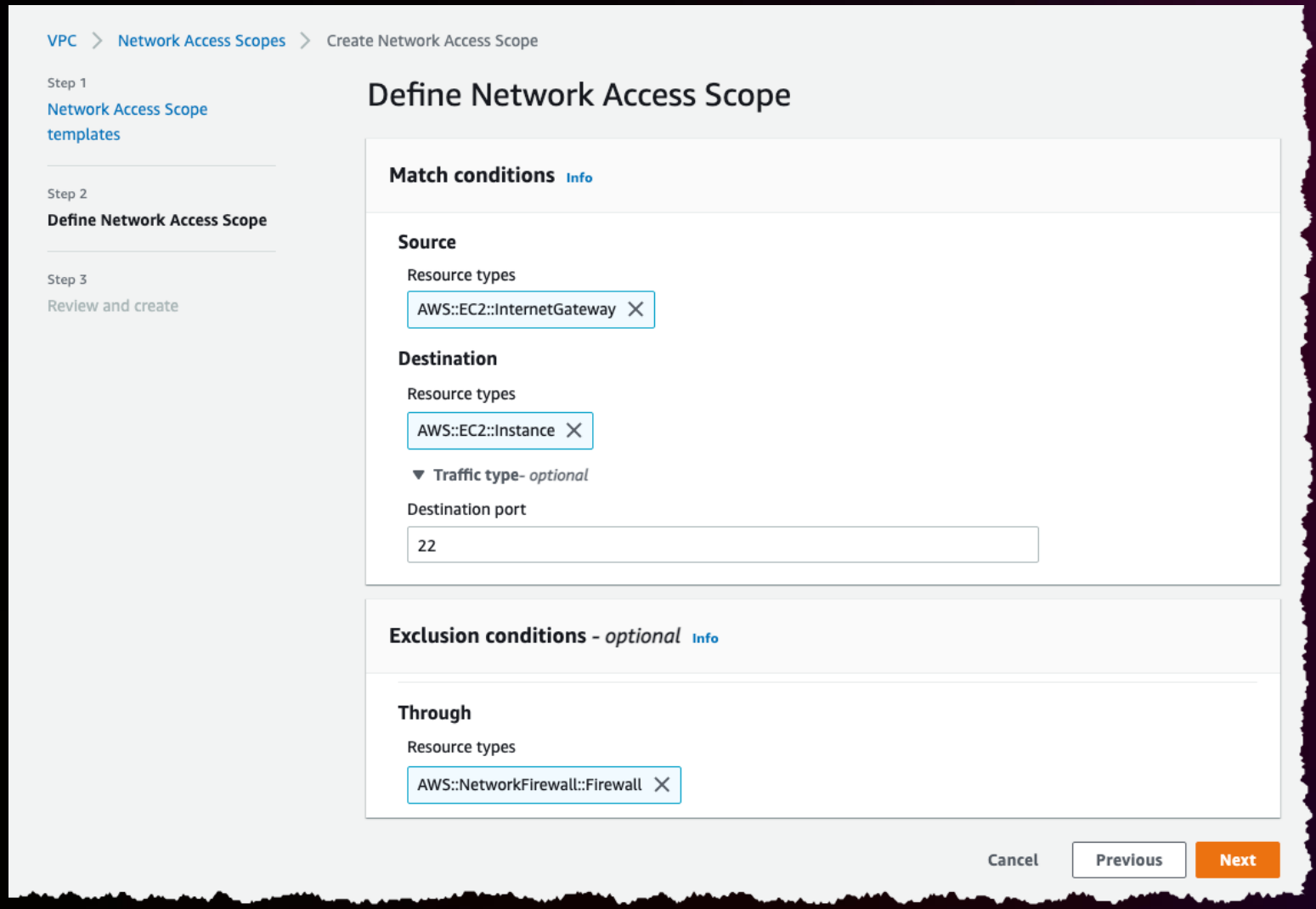
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Access Analyzer



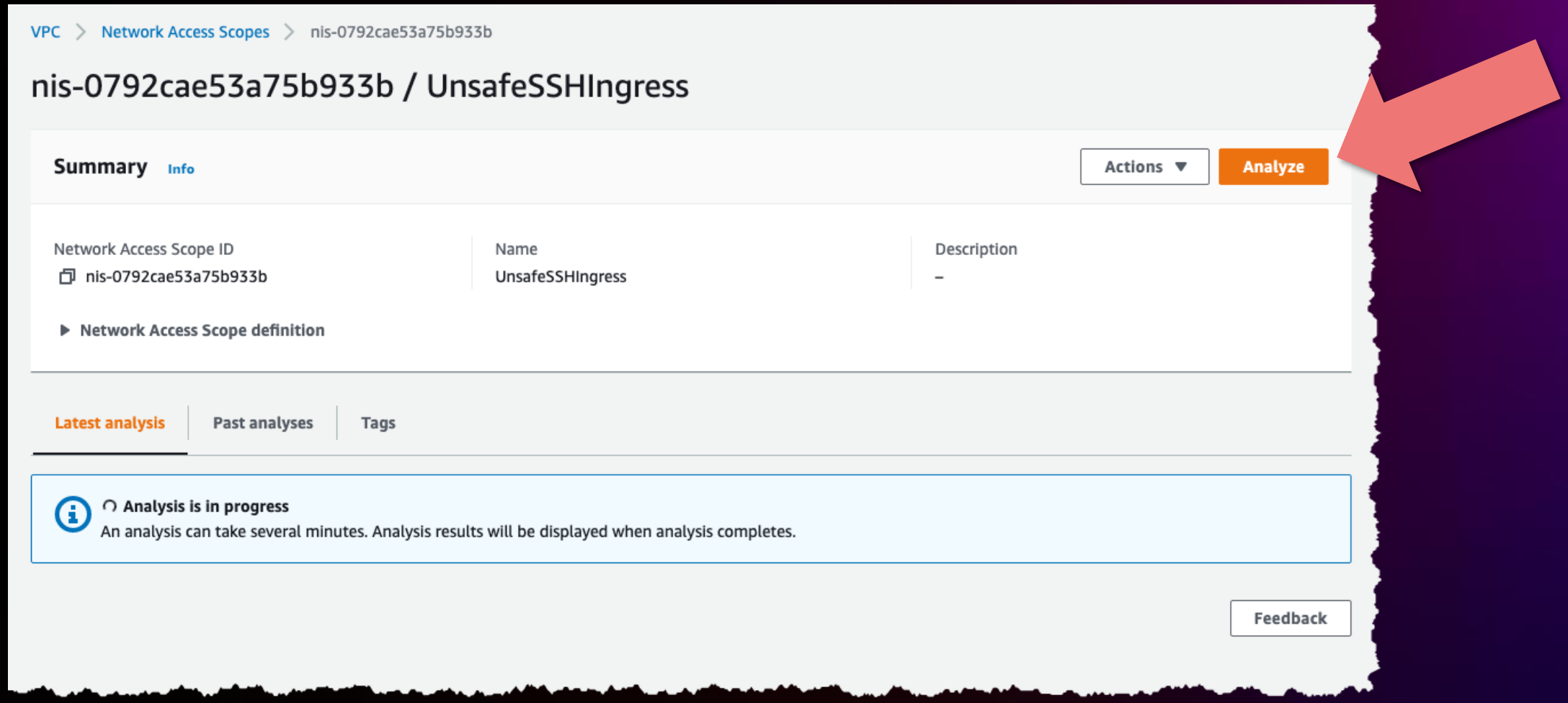
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Access Analyzer



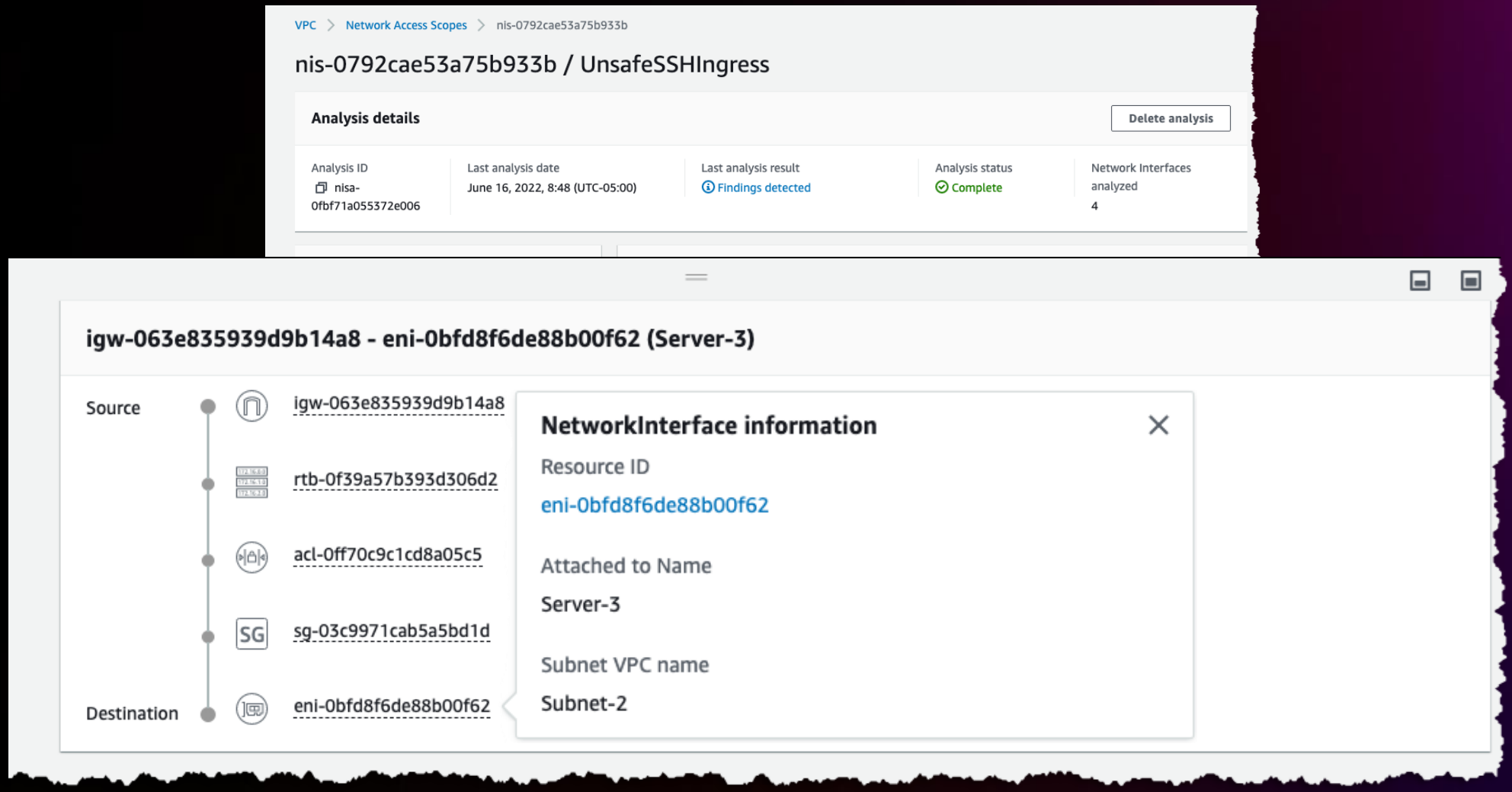
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Access Analyzer



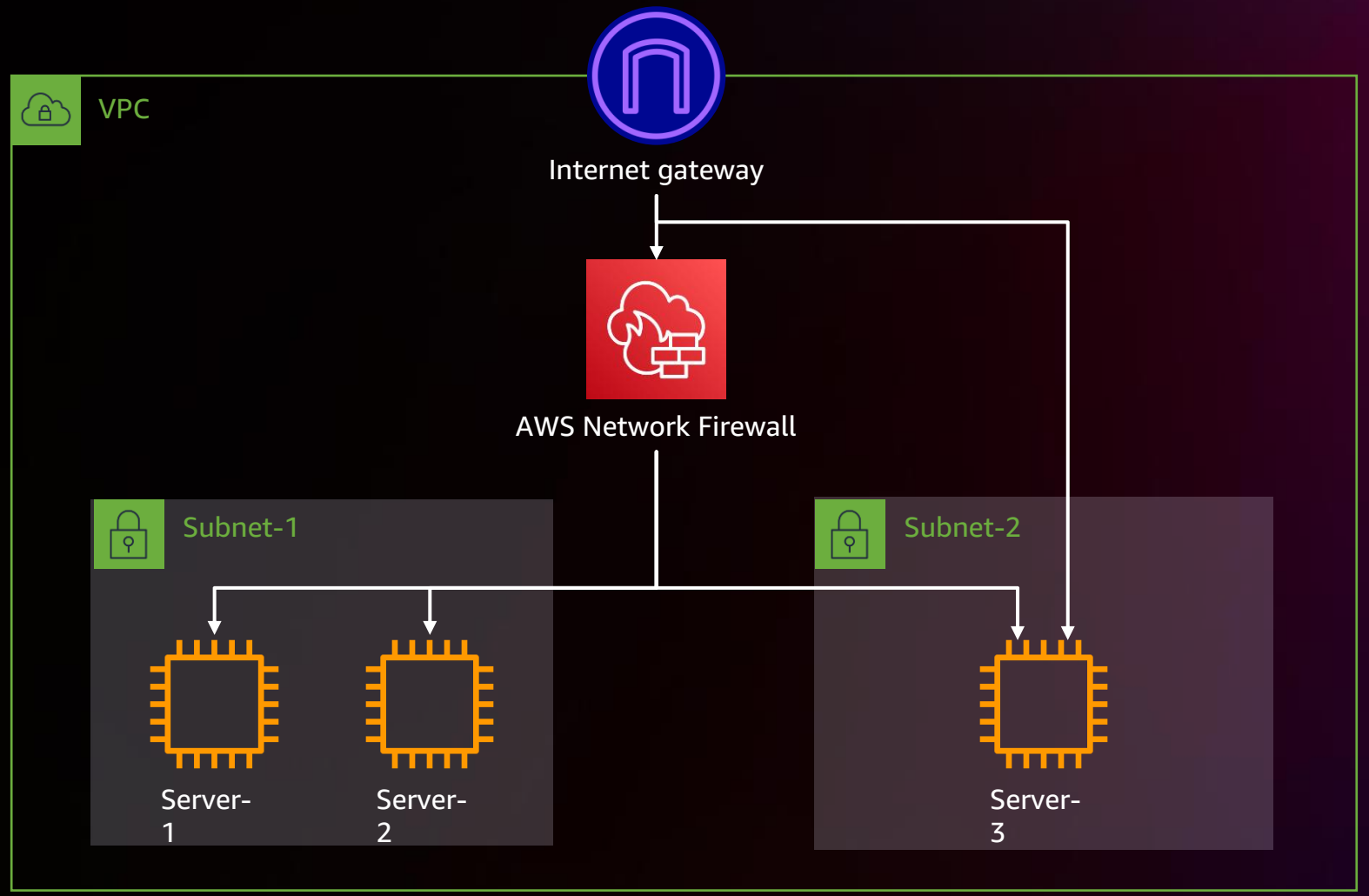
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Access Analyzer



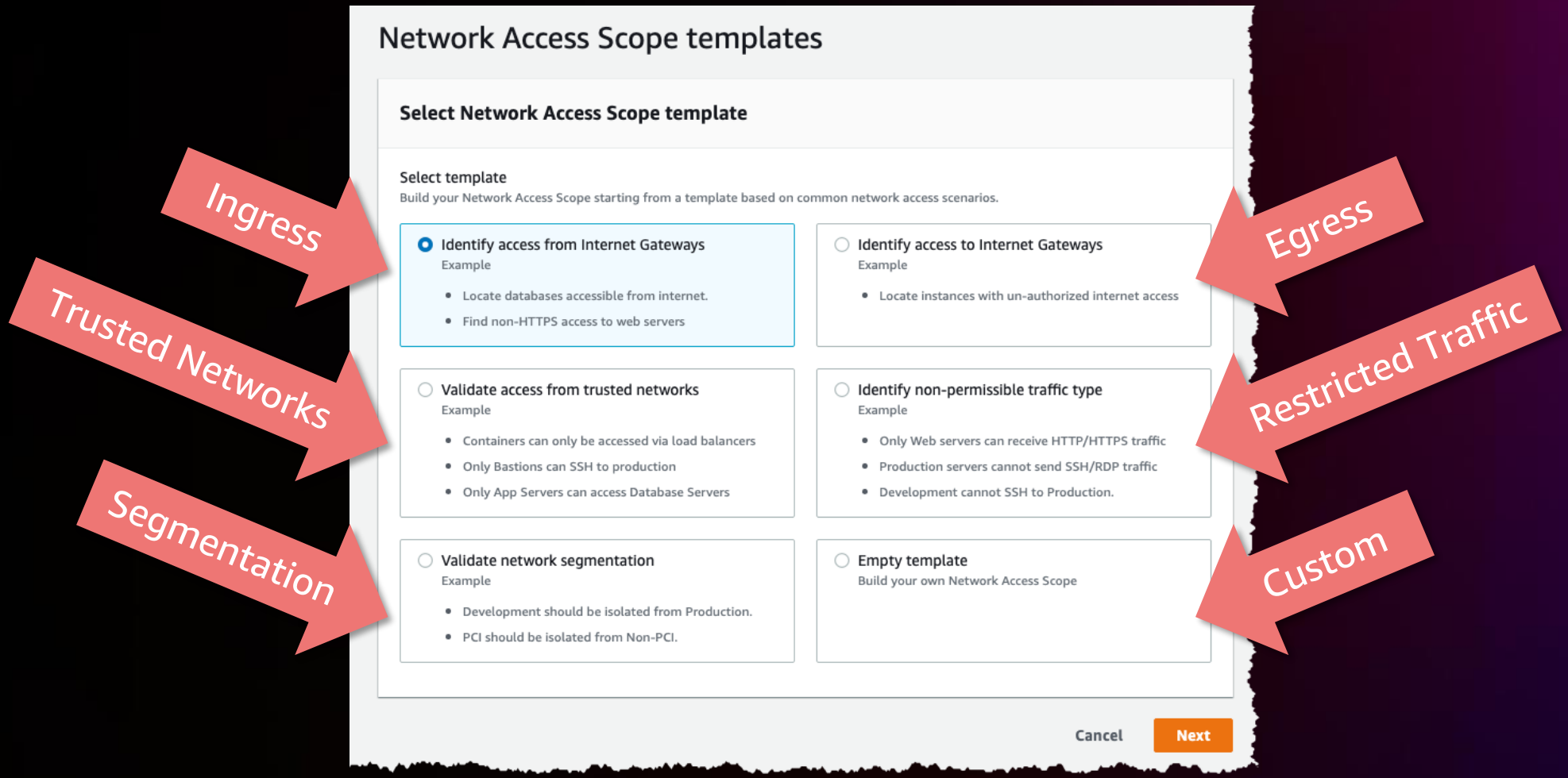
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Actual Network



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Access Analyzer



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Protecting your data by creating an immutable ”golden image”

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Backup provides broadest support for AWS resources

AWS Backup

Compute
- VMware Cloud on AWS
- Amazon EC2

Block Storage
- Amazon EBS

File Storage
- Amazon FSx for NetApp ONTAP
- Amazon FSx for OpenZFS
- Amazon EFS
- Amazon FSx for Windows File Server
- Amazon FSx for Lustre

Databases
- Amazon DynamoDB
- Amazon RedShift
- Amazon Aurora
- Amazon Neptune
- Amazon RDS
- Amazon DocumentDB

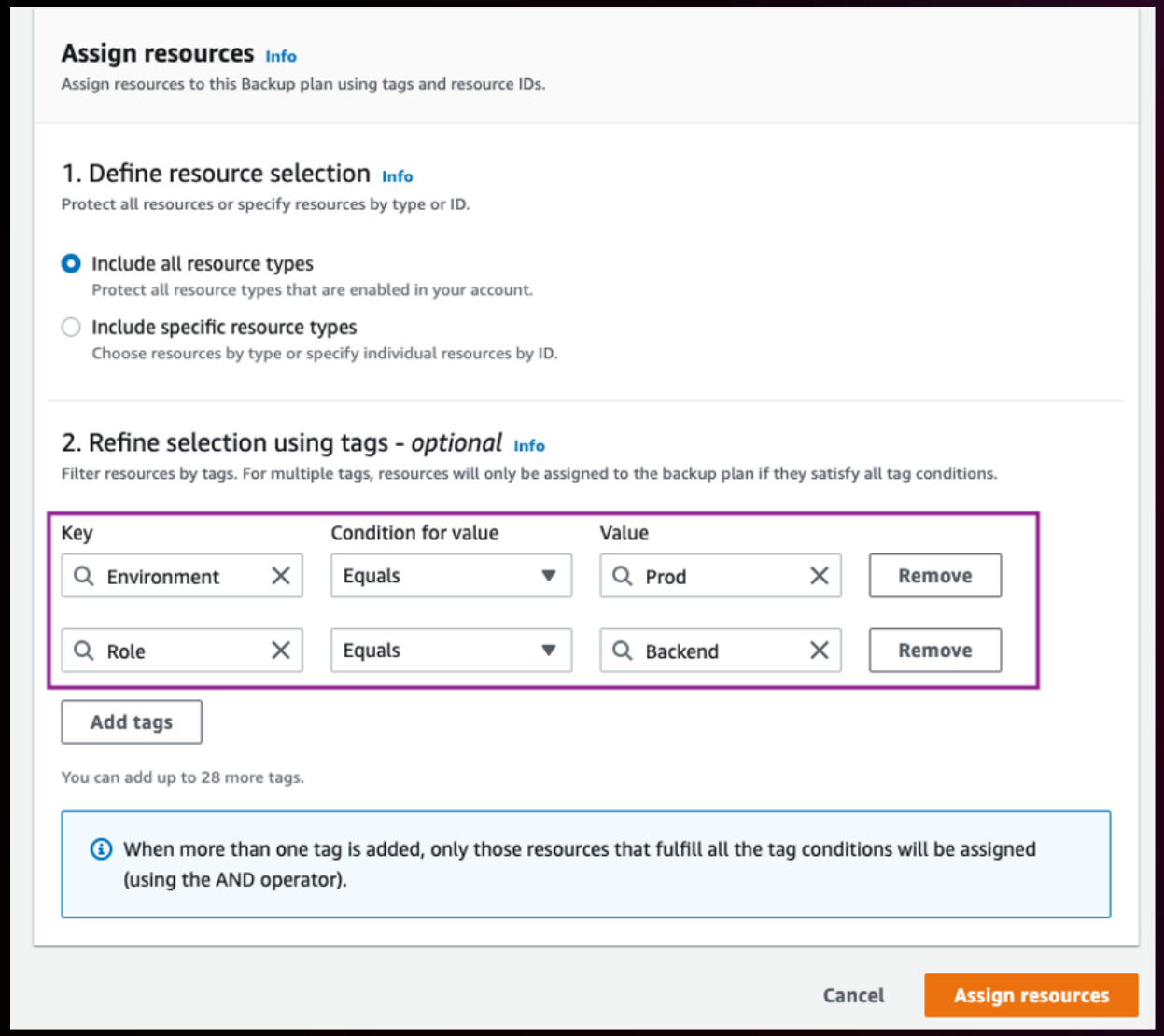
Object Storage
- Amazon S3

Data Transfer
- AWS Storage Gateway

Hybrid Workloads
- AWS Storage Gateway
- \+
- vmware

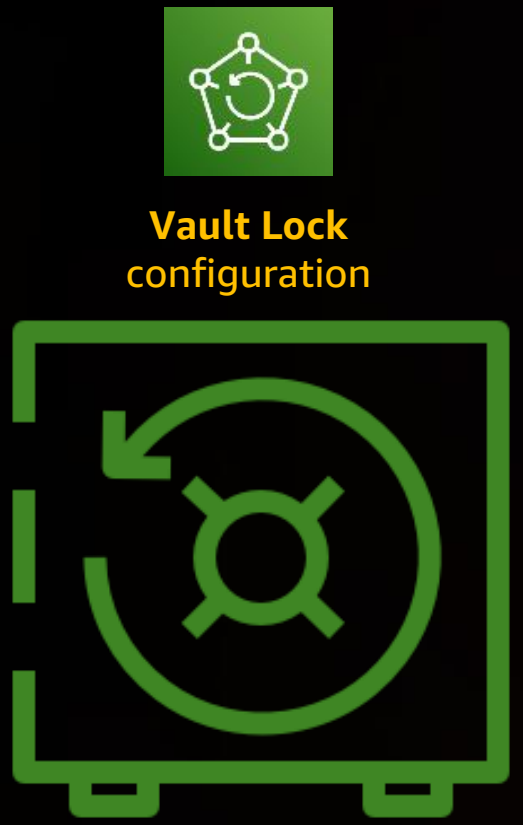
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Back up your critical assets by using tags



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

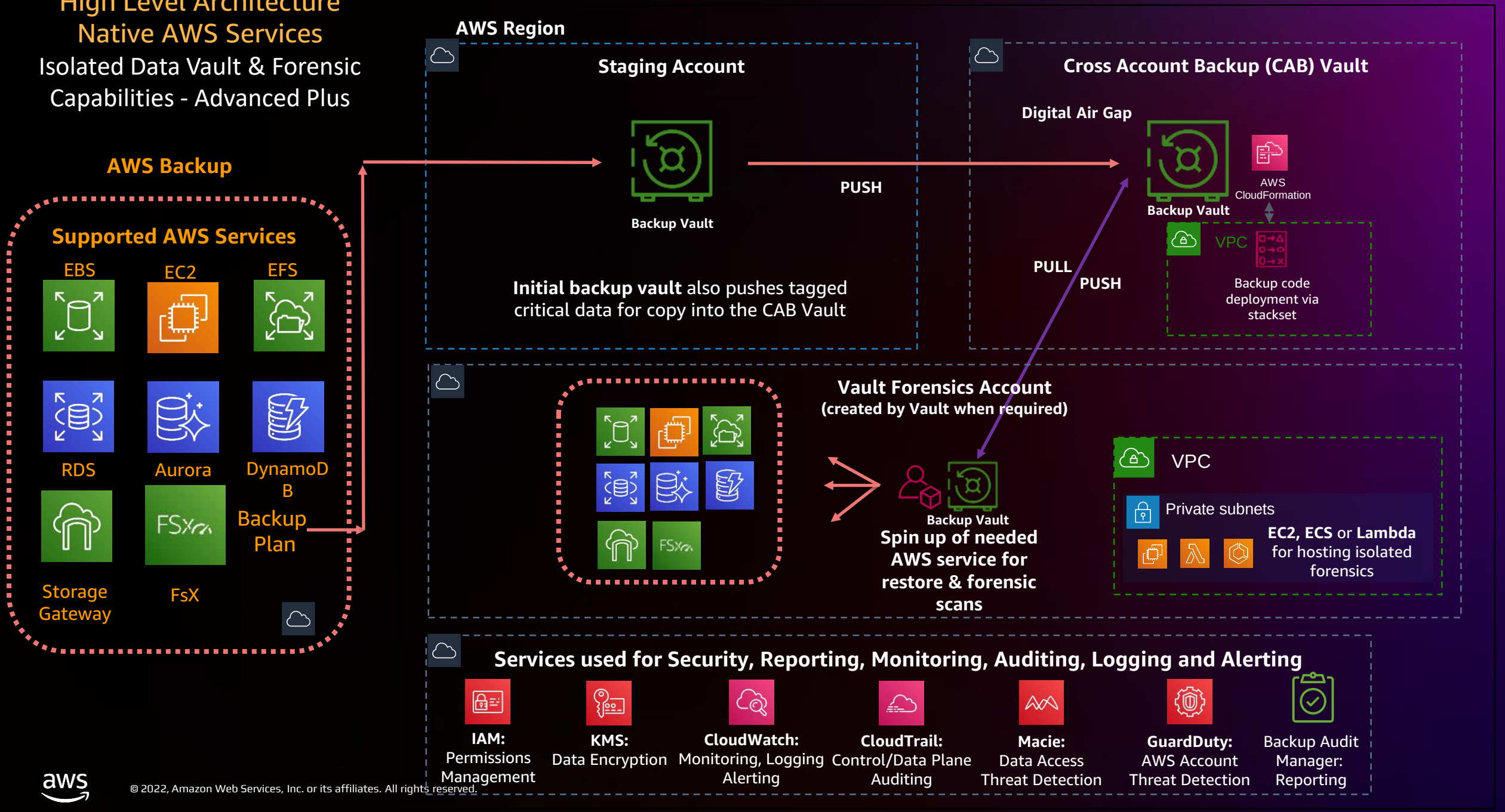
AWS Backup Vault Lock protects your sensitive data backups against malicious actors



- 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)

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

High Level Architecture
Native AWS Services
Isolated Data Vault & Forensic Capabilities - Advanced Plus



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

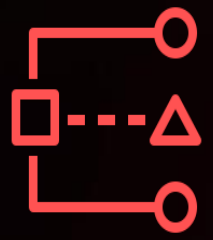
Universal security statements



Amazon S3 Block Public Access

"My S3 buckets are not publicly accessible"

AWS IAM Access Analyzer



"There is no unknown external access to my S3 buckets"



AWS Backup

"All my sensitive data is backed up and protected from malicious actors."



Amazon Inspector Network Reachability

"My EC2 instances are not publicly accessible"



Amazon VPC Network Access Analyzer

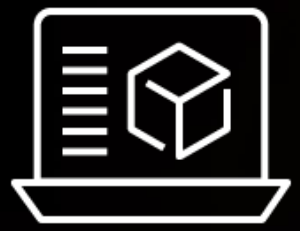
"All SSH traffic to my instances goes through a firewall"

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Continue your AWS Storage learning

Build a learning plan



Create your AWS Storage Learning Plans via **AWS Skill Builder**

Increase your knowledge



Use our **Ramp-Up Guides** to build your storage knowledge

Earn AWS Storage badges



Demonstrate your knowledge by achieving **digital badges**

aws.training/storage

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sessions from the AWS Data Protection team

Breakout sessions

- STG206 (11/28)
  - Data resiliency design patterns with AWS
- STG207 (11/30)
  - Data protection and governance on AWS
- STG208 (11/29)
  - Protect against ransomware with a Zero Trust architecture

Builders' sessions

- STG324-R (11/28)
- STG324-R1 (11/30)
  - Protect AWS resources with AWS Backup

Chalk talks

- STG304-R (11/28)
- STG304-R1 (12/2)
  - Using AWS Backup to protect your cloud resources and hybrid environments
- STG305-R (11/29)
- STG305-R1 (12/1)
  - Data protection and application recovery strategies for ransomware events
- STG341 (11/30)
  - Proactively protect critical applications

Workshops

- STG312-R (12/1)
- STG312-R1 (11/30)
  - Build a disaster recovery solution with AWS storage services
- STG313 (11/30)
  - Backup for applications running on the AWS Cloud

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Nancy Wang
@nancyzwang

Neha Rungta
@neharungta



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.