
AWS
re:Invent

ENT308

Building the right foundation for your migration

Sam Elmalak

WW Tech Leader, Cloud Foundations

AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

What to think about

Why do it

How to build the right foundation



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

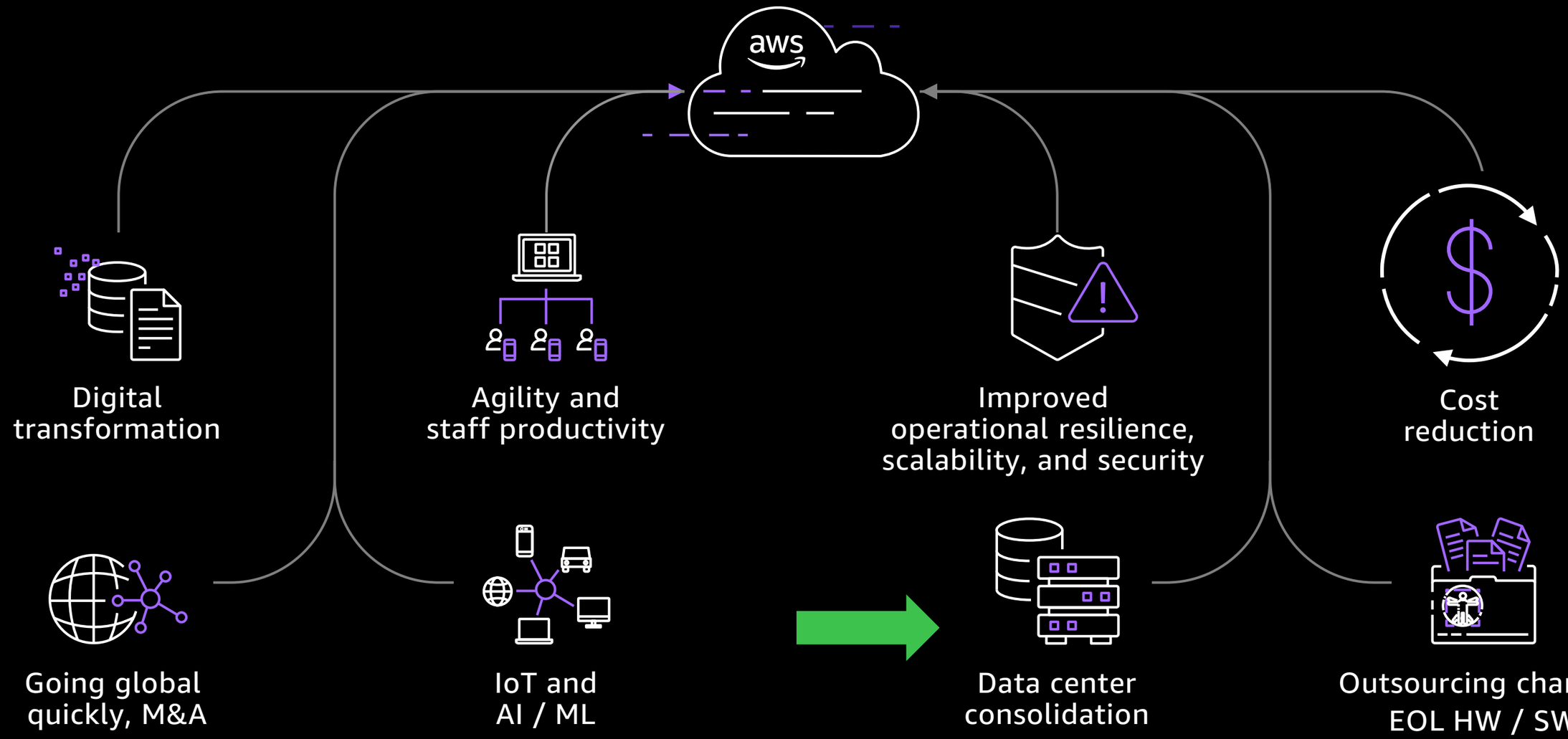
So you’ve decided to migrate something

Congratulations!

Let’s just copy the servers over and move it

3 weeks and we’re done

Business drivers for migrating to the cloud



Common questions

How do I create a business case?

How do I get started?

What workloads should I move first?

How do we manage workloads in the cloud?

What do I have in my environment?

What should I move to the cloud?

How do I migrate these workloads?

How do I get my team re-skilled?

What do I do!?



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Customer journey

Assess



Rapid discovery



TCO report



Migration readiness assessment



Briefings & workshops



Immersion day

Mobilize

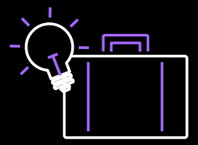
Portfolio



Discovery and planning



Migration plan

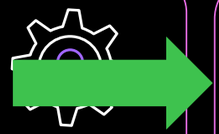


Business case / Mig. Evaluator

Migrate



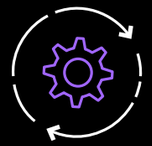
Migration and modernization experience



Skills / center of excellence



Landing zone



Operating model

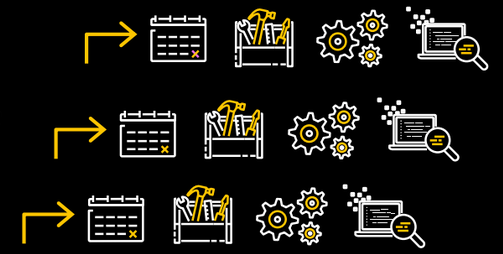


Security and compliance

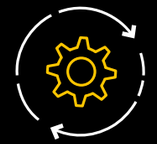
People

Platform

Migrate & Modernize



Migrate



Operate & optimize



Modernize

Create a case for change

Build readiness through experiences

Accelerate transformation at scale

Things to consider . . .



Access management



Service knowledge management



Change management



Provisioning



Automation



Configuration management



Log management



Host security



Continuity management (backup)



Patch management



Monitoring



Event incident service management



24x7 service desk coverage



Reporting



Compliance



Capacity management

Across these areas

Governance, risk, and compliance

Identity management & access control

Service management

Security management

Data protection

Asset management

Developer experience

Change & release management

Networking

Monitoring and event management

Business continuity



Governance, Risk, and Compliance

Immutable environment log storage
Resources isolation boundary
Financial mgmt (centralized)
Green lighting services
Governance
Vulnerability & threat management
Records management

Networking

Central network connectivity

- Ability to connect to on-premises resources
- Ability to interconnect resources in the cloud
- Ability to connect to internet
  - Serve content and product, etc.
  - Updates to software, patching, etc.

Identity Management and Access control

AWS access

- Access to AWS environment and AWS resources
- Identity for AWS services, for infrastructure, for applications on top
- Human-level access and joiners / leavers process
- Programmatic access

Instance-level access

- Operating system, databases, etc.

Application-level access

Service Management

Security incident response

Forensics

Support

Rollout / rollback

Centralized template management

Security Management

Security operational capabilities

Network security

Application security

Data Protection

Data / content Isolation

Encryption key management / crypto hierarchy

Secrets management

Business Continuity

Disaster recovery

Backups

Asset Management

Central sort / search for metadata

Tagging strategy (for resources)

Resource inventory management

Capabilities

Change & release management

- Patching

Monitoring and event management

- Centralized enterprise logging and monitoring

Developer experience

- Developer experience & tools

The Account Structure



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Disable service APIs you won't be using

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
      "Effect": "Deny",
      "Action": ”<Insert unwanted service prefix here>:*",
      "Resource": "*"
    }
  ]
}
```

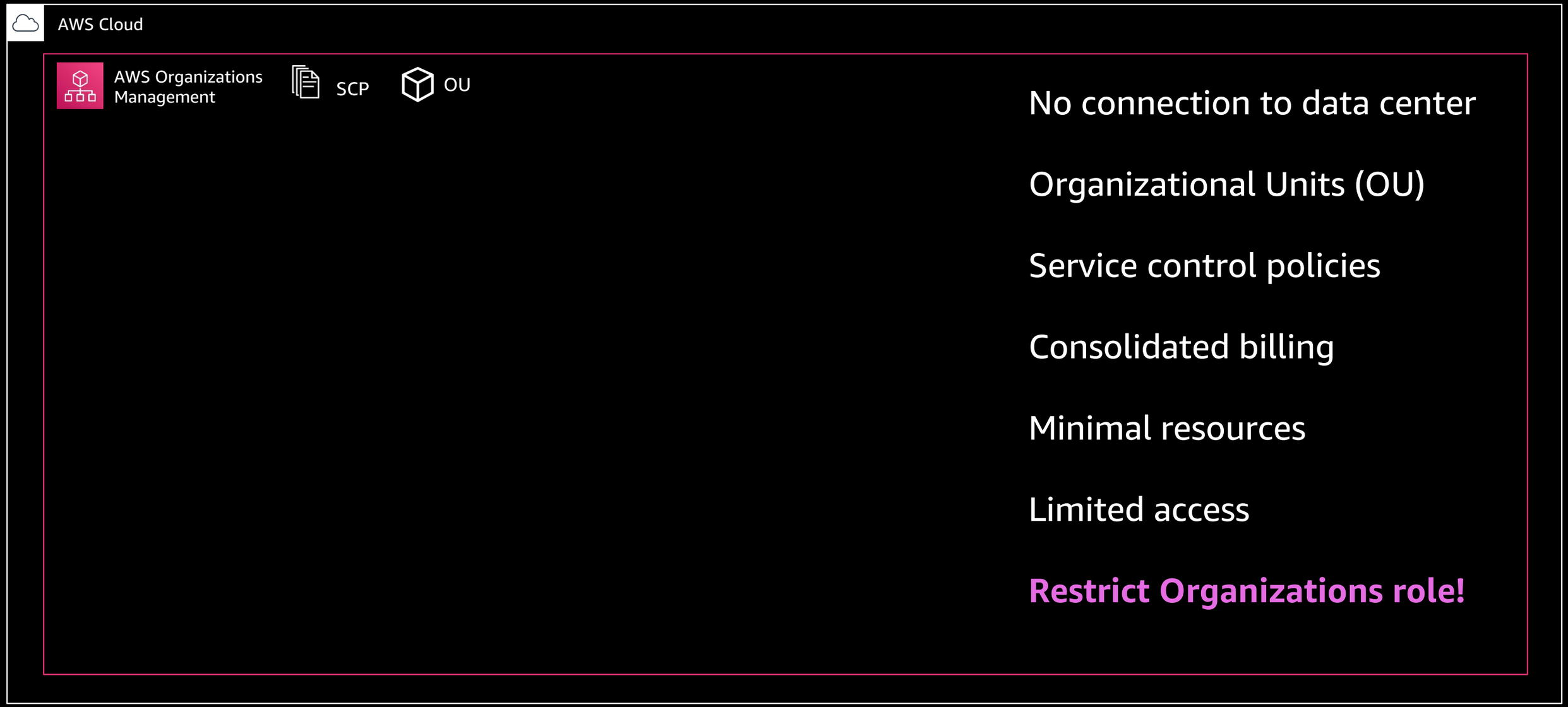
NotAction	(Optional) List the AWS actions exempt from the SCP. Used in place of the Action element.
Resource	List the AWS resources the SCP applies to.
Condition	(Optional) Specify conditions for when the statement is in effect.

Organizational Units

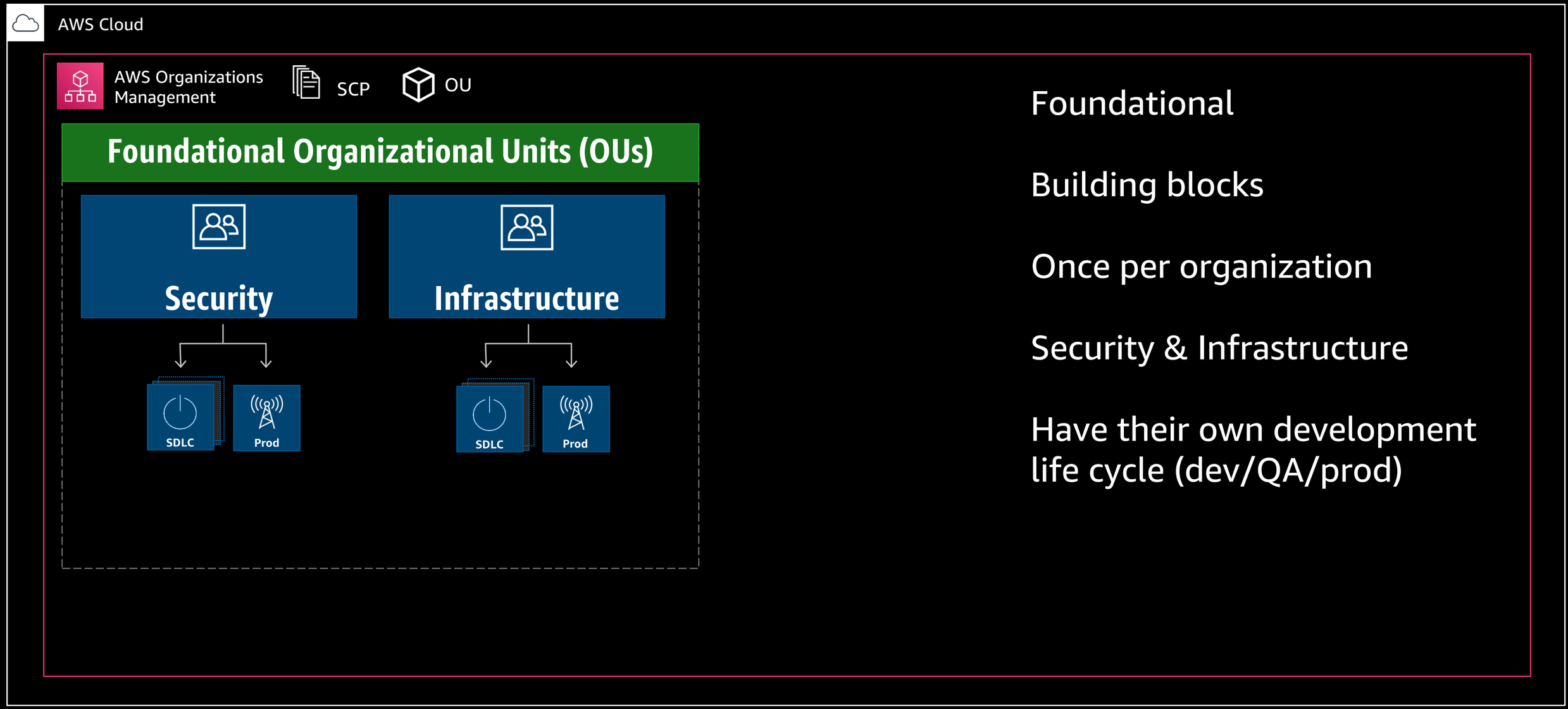
- Grouping of AWS Accounts
- Service Control Policies (SCP) to the groups
- Use permission grouping (NOT corporate structure)

How likely is the group to need a set of similar policies?

AWS Organizations Management



Foundational OUs



Foundational

Building blocks

Once per organization

Security & Infrastructure

Have their own development life cycle (dev/QA/prod)

Log Archive



Versioned Amazon S3 bucket
Restricted
MFA delete

AWS CloudTrail logs

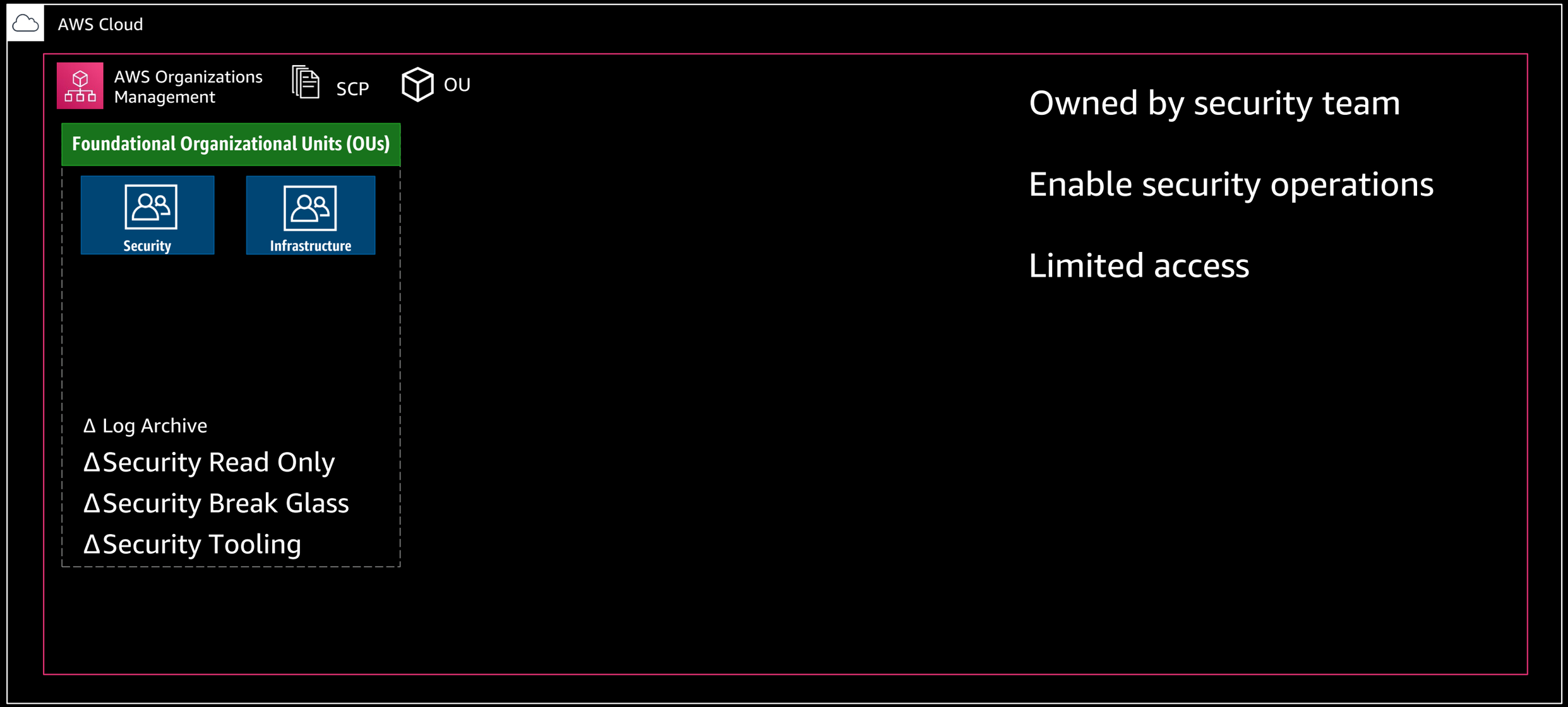
Security logs

Single source of truth

Alarm on user login

Limited access

Security Accounts



Security Accounts // Read Only



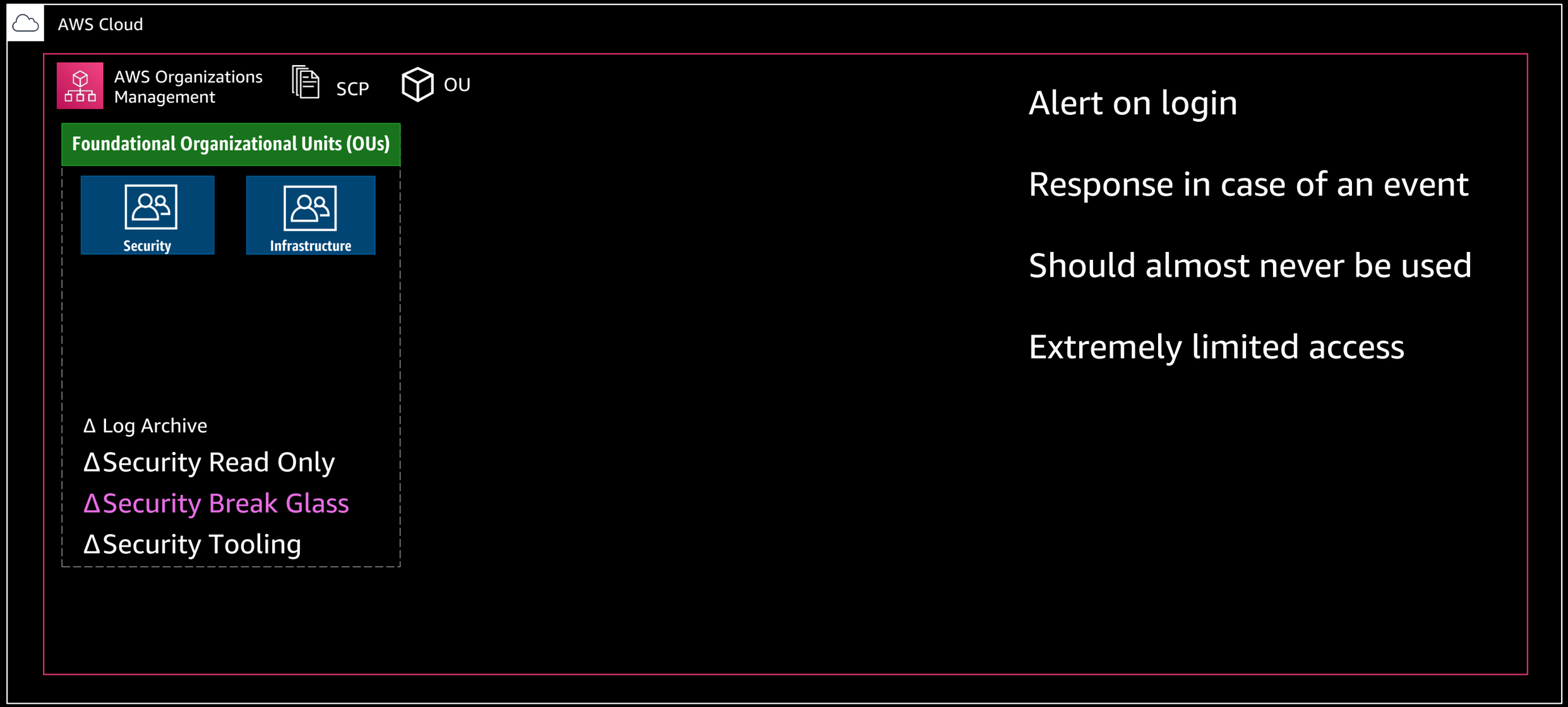
View/Scan resources in other accounts

Exploratory Security Testing

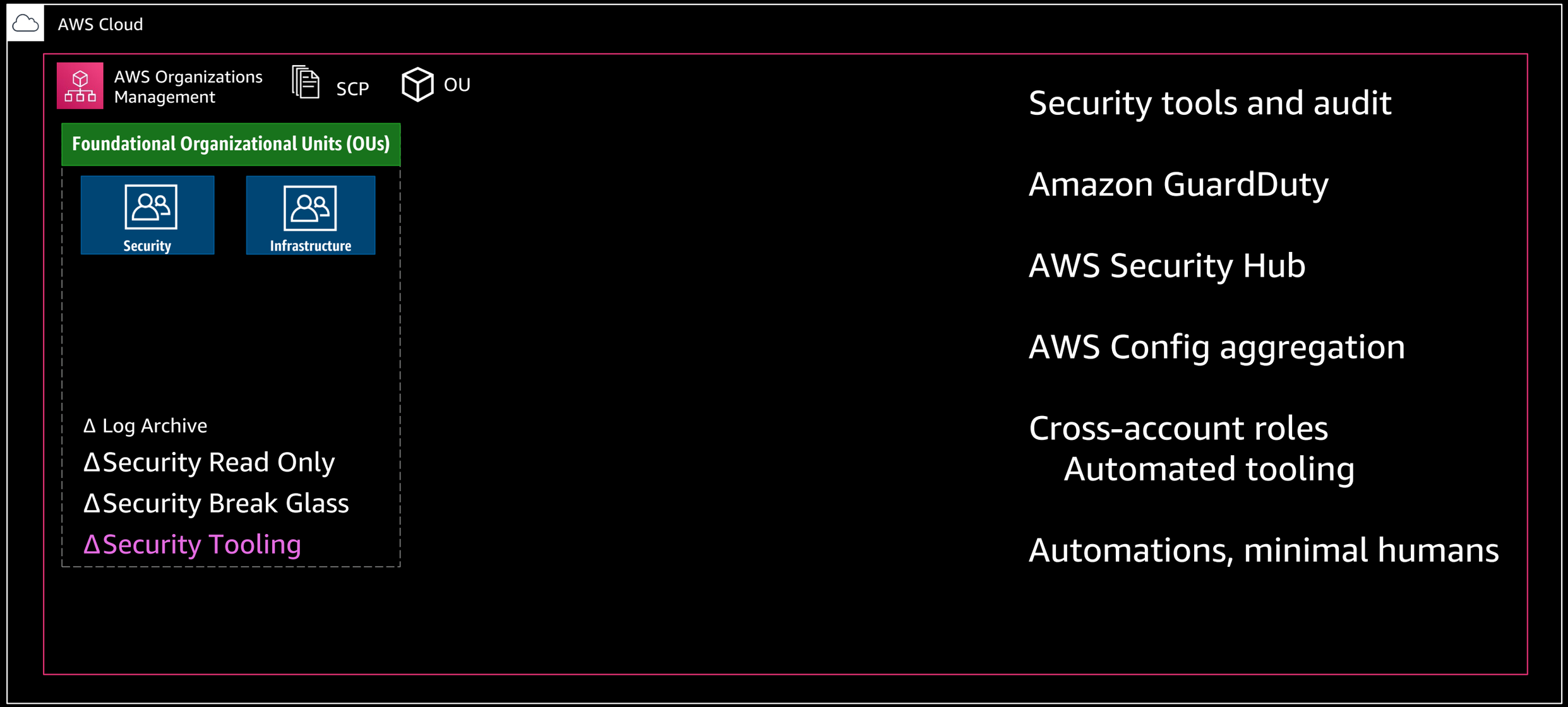
Cross account read-only (security Auditor)

Limited access

Security Accounts // Break Glass



Security Accounts // Tooling



Security tools and audit

Amazon GuardDuty

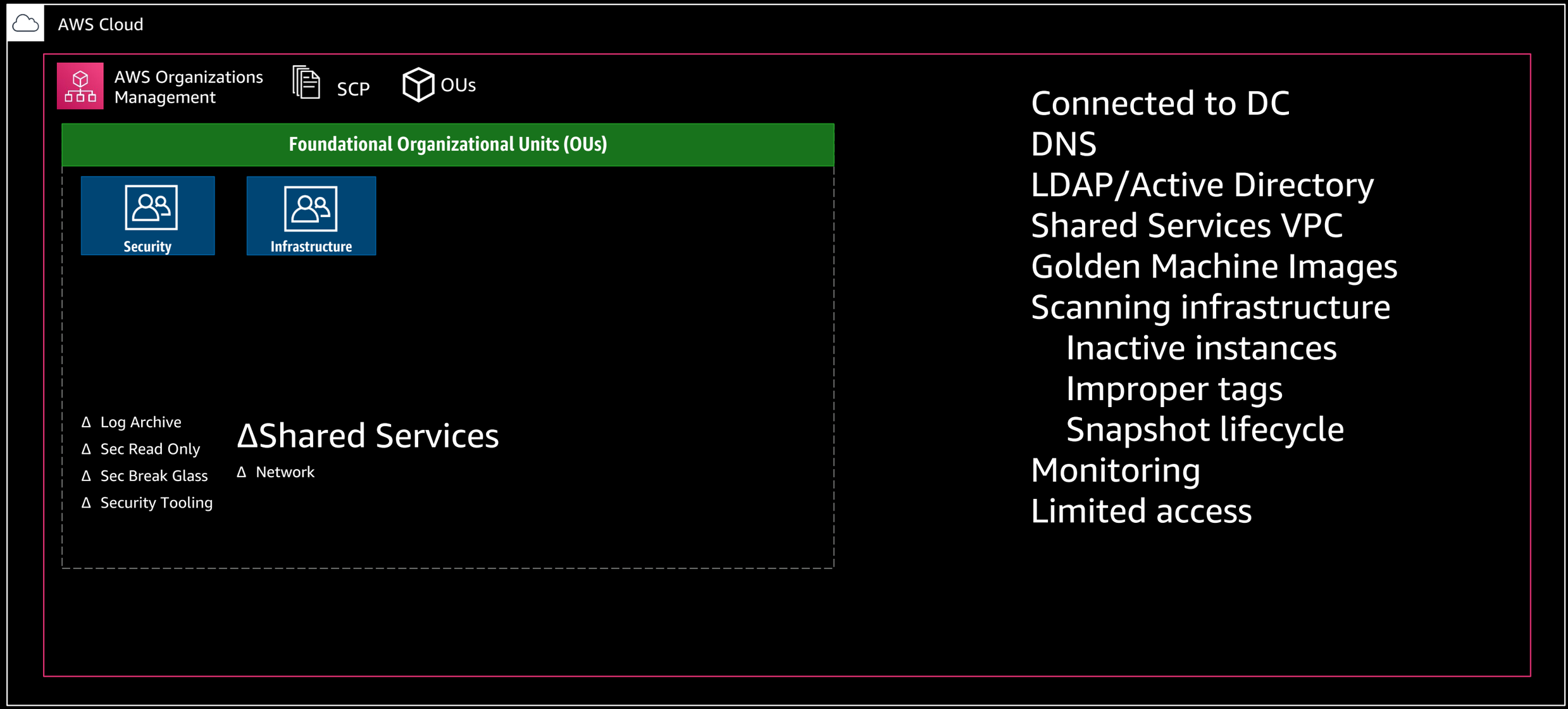
AWS Security Hub

AWS Config aggregation

Cross-account roles
Automated tooling

Automations, minimal humans

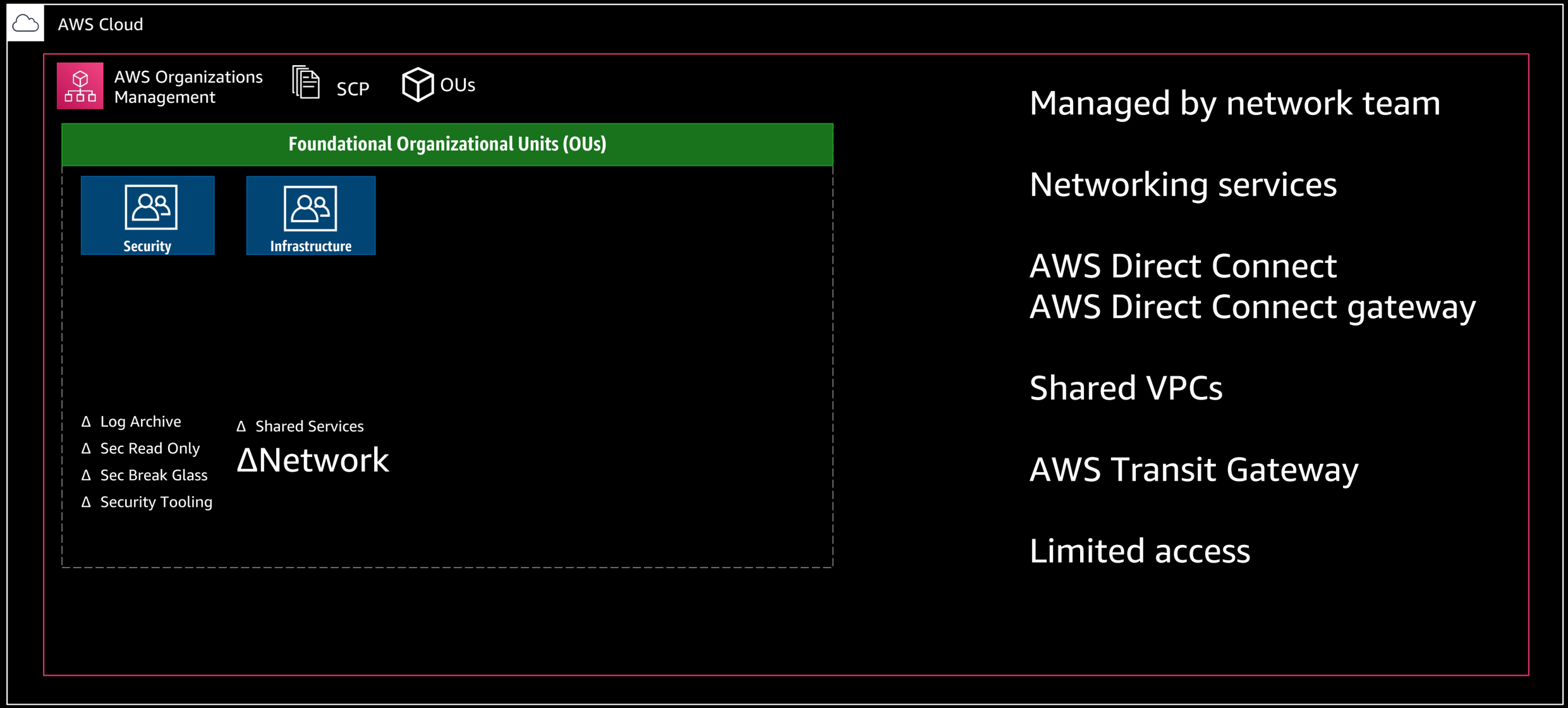
Shared Services



Connected to DC
DNS
LDAP/Active Directory
Shared Services VPC
Golden Machine Images
Scanning infrastructure
- Inactive instances
- Improper tags
- Snapshot lifecycle

Monitoring
Limited access

Network



Managed by network team

Networking services

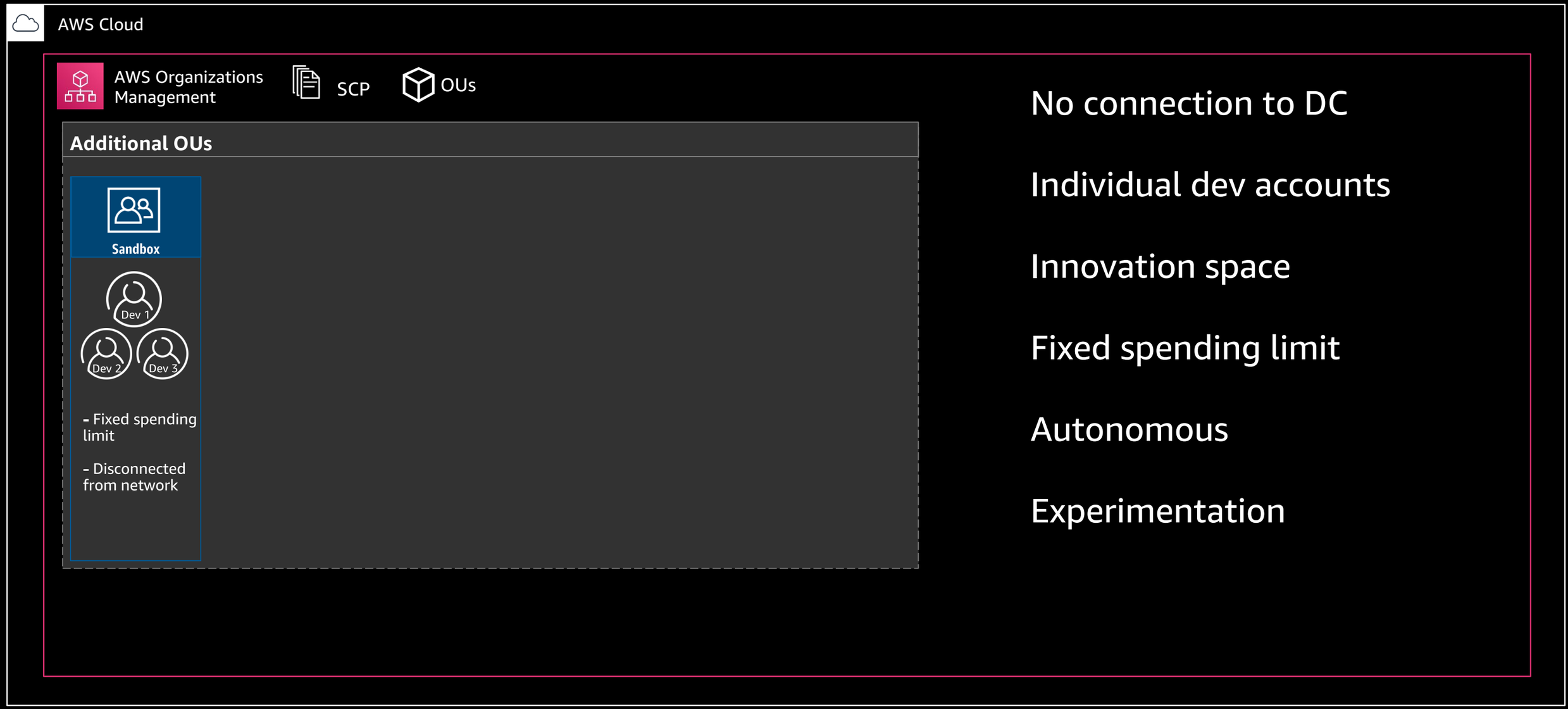
AWS Direct Connect
AWS Direct Connect gateway

Shared VPCs

AWS Transit Gateway

Limited access

Sandbox



No connection to DC

Individual dev accounts

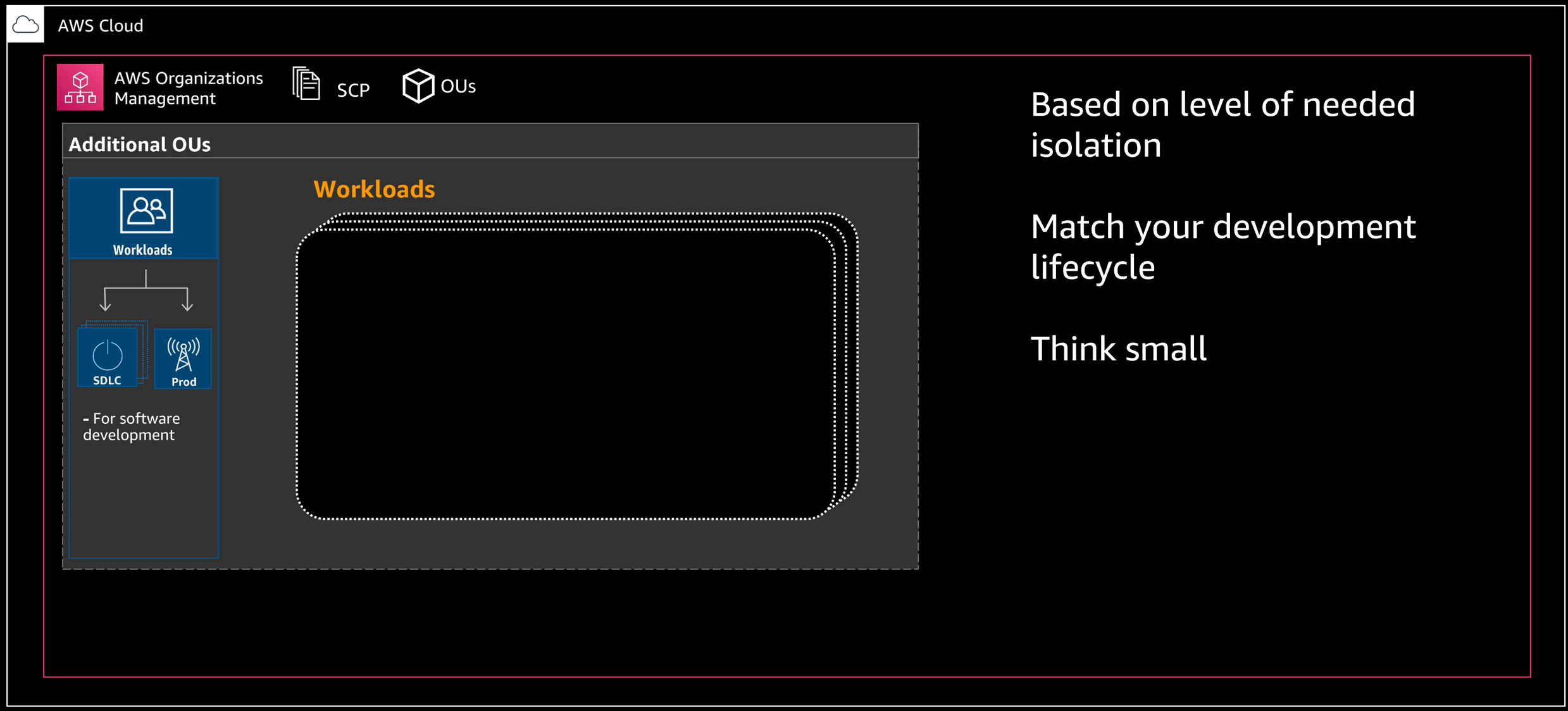
Innovation space

Fixed spending limit

Autonomous

Experimentation

Workloads

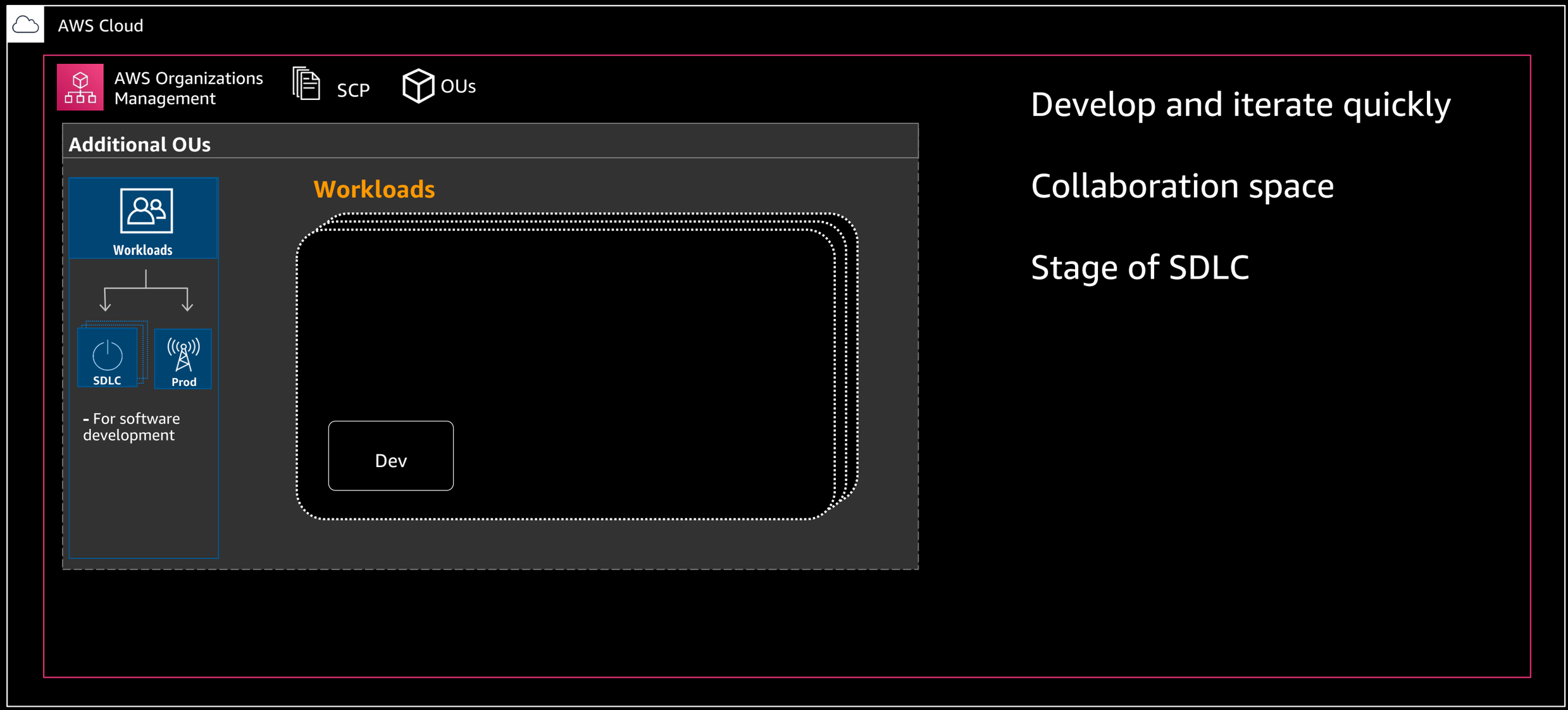


Based on level of needed isolation

Match your development lifecycle

Think small

Workloads // Dev

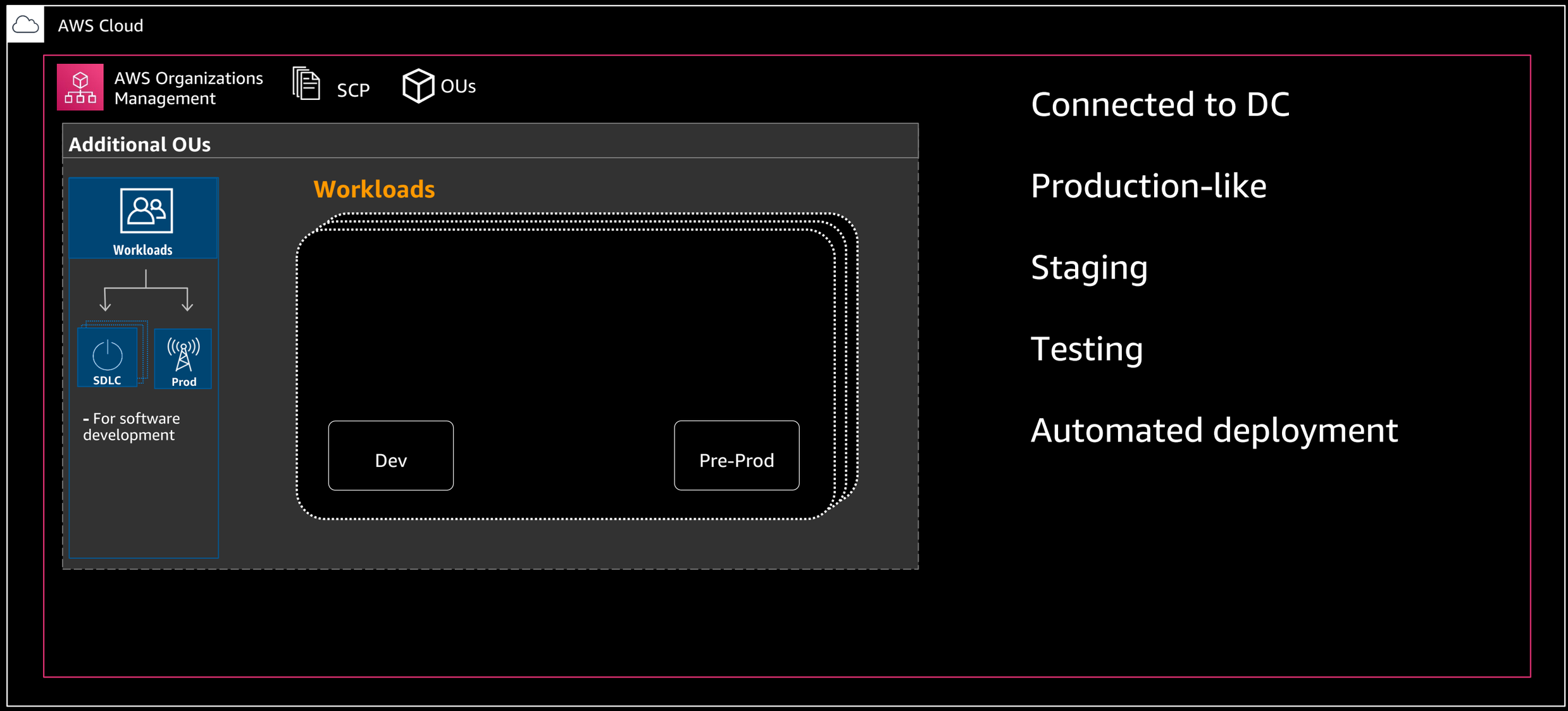


Develop and iterate quickly

Collaboration space

Stage of SDLC

Workloads // Pre-Prod



Connected to DC

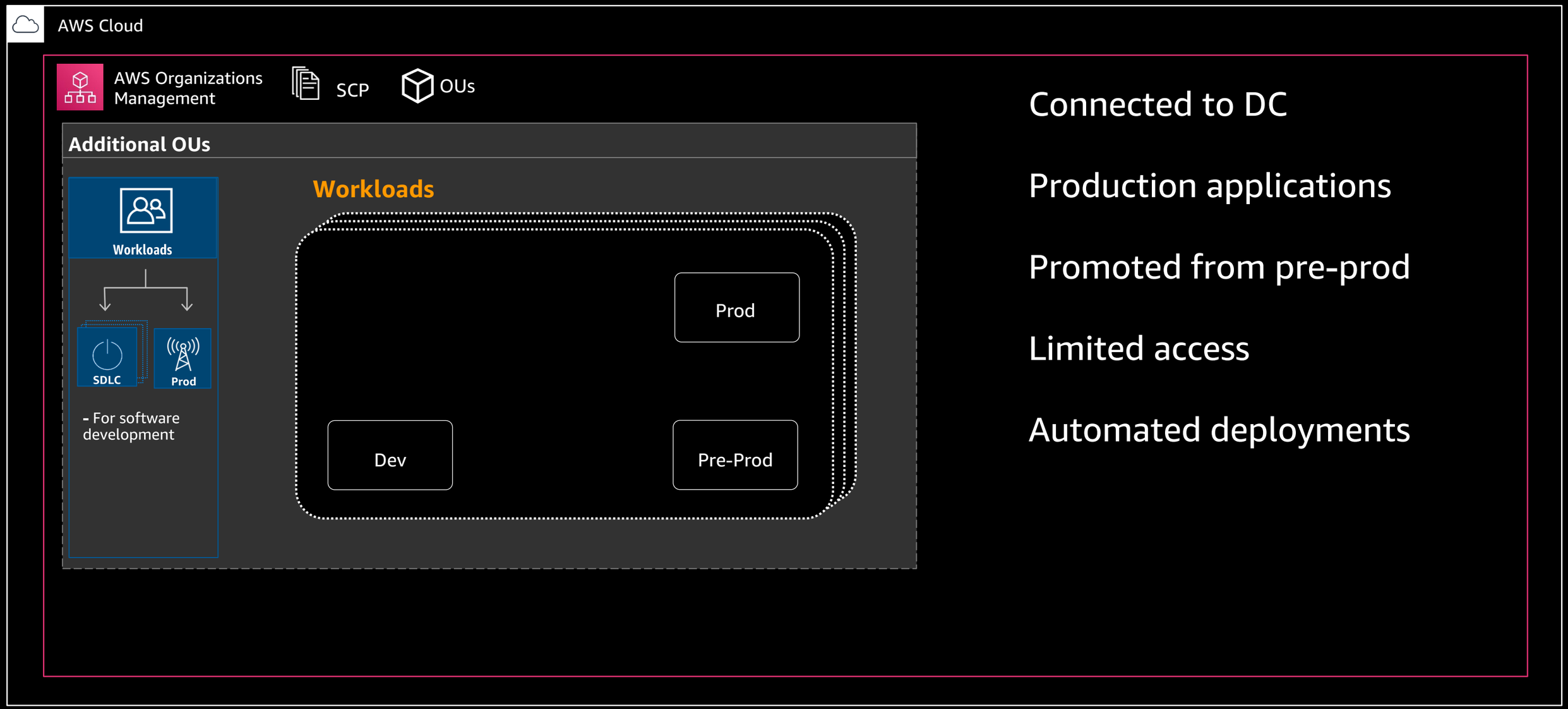
Production-like

Staging

Testing

Automated deployment

Workloads // Prod



Connected to DC

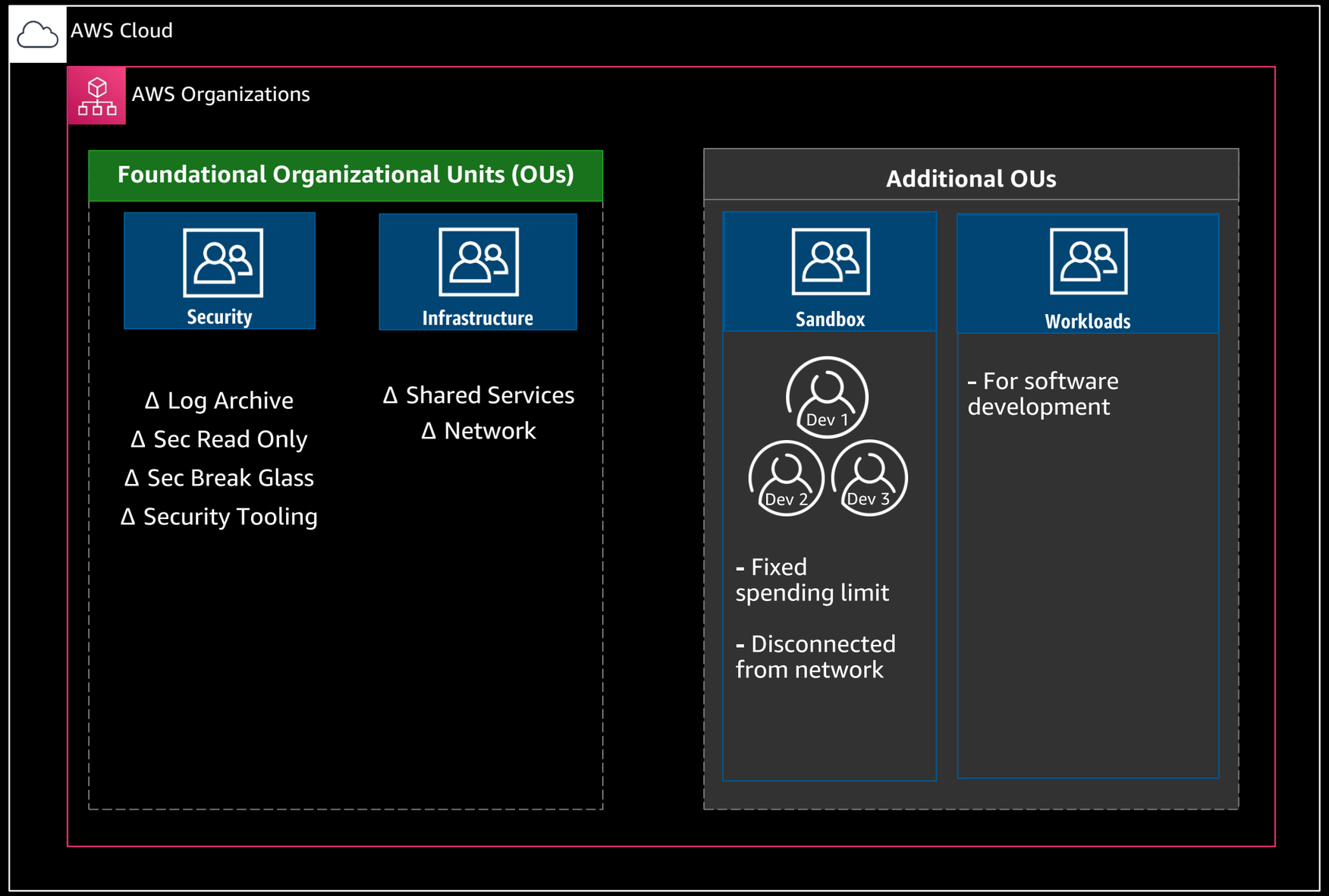
Production applications

Promoted from pre-prod

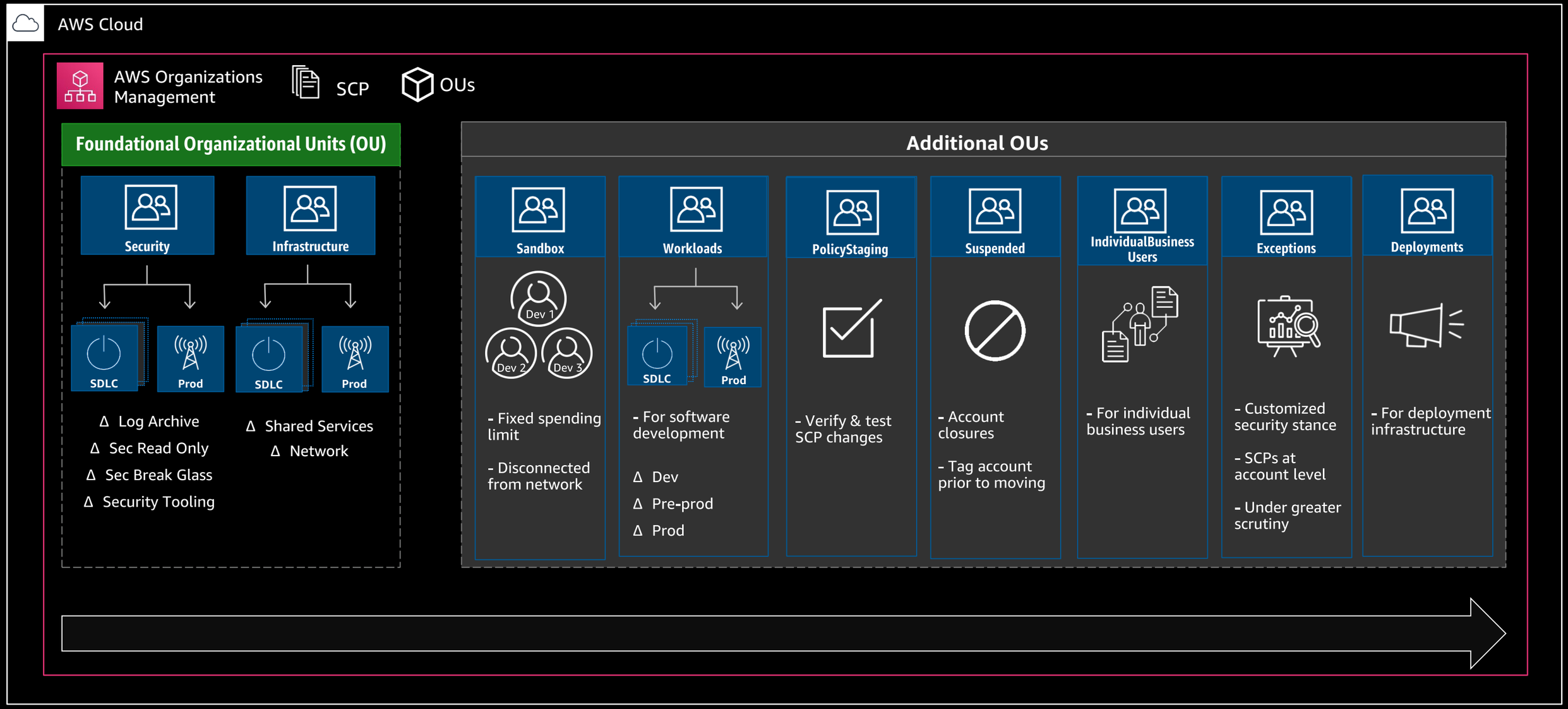
Limited access

Automated deployments

Starter AWS multi-account framework



Multi-account framework



v20191204

Summary



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Summary

- Look at holistic approach
- Consider capabilities
- Scope down to migration needs
- Build operational model

Capabilities to consider [focus area]

Immutable environment log storage

Identity management & access control

Security incident response

Forensics

Security operational capabilities

Account isolation (resource grouping)

Network security

Application security

Data / content isolation

Central network connectivity

Enterprise / core infrastructure shared services

Business unit shared services

Support

Rollout / rollback

Centralized template management

Centralized enterprise logging and monitoring

Financial mgmt (centralized)

Central sort / search for metadata

Disaster recovery

Backups

Encryption key management / crypto hierarchy

Secrets management

Developer experience & tools

Tagging strategy (for resources)

Green lighting services

Patching

Governance

Resource inventory management

Vulnerability & threat management

Records management

Resources

Cloud Migration Homepage: https://aws.amazon.com/cloud-migration/

Additional Migration Resources, AWS Prescriptive Guidance, AWS Enterprise Blog Collection:
https://aws.amazon.com/cloud-migration/resources/

Migration Immersion Day: https://migration-immersionday.workshop.aws/en

All AWS workshops available here: https://www.workshops.aws/

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.