AWS re:Invent

SEC325

Architecting security & governance across your landing zone

Sam Elmalak

WW Tech Leader, Enterprise Greenfield
Amazon Web Services

AWS re:Invent

aws

Agenda

Why a landing zone?

How to think about it?

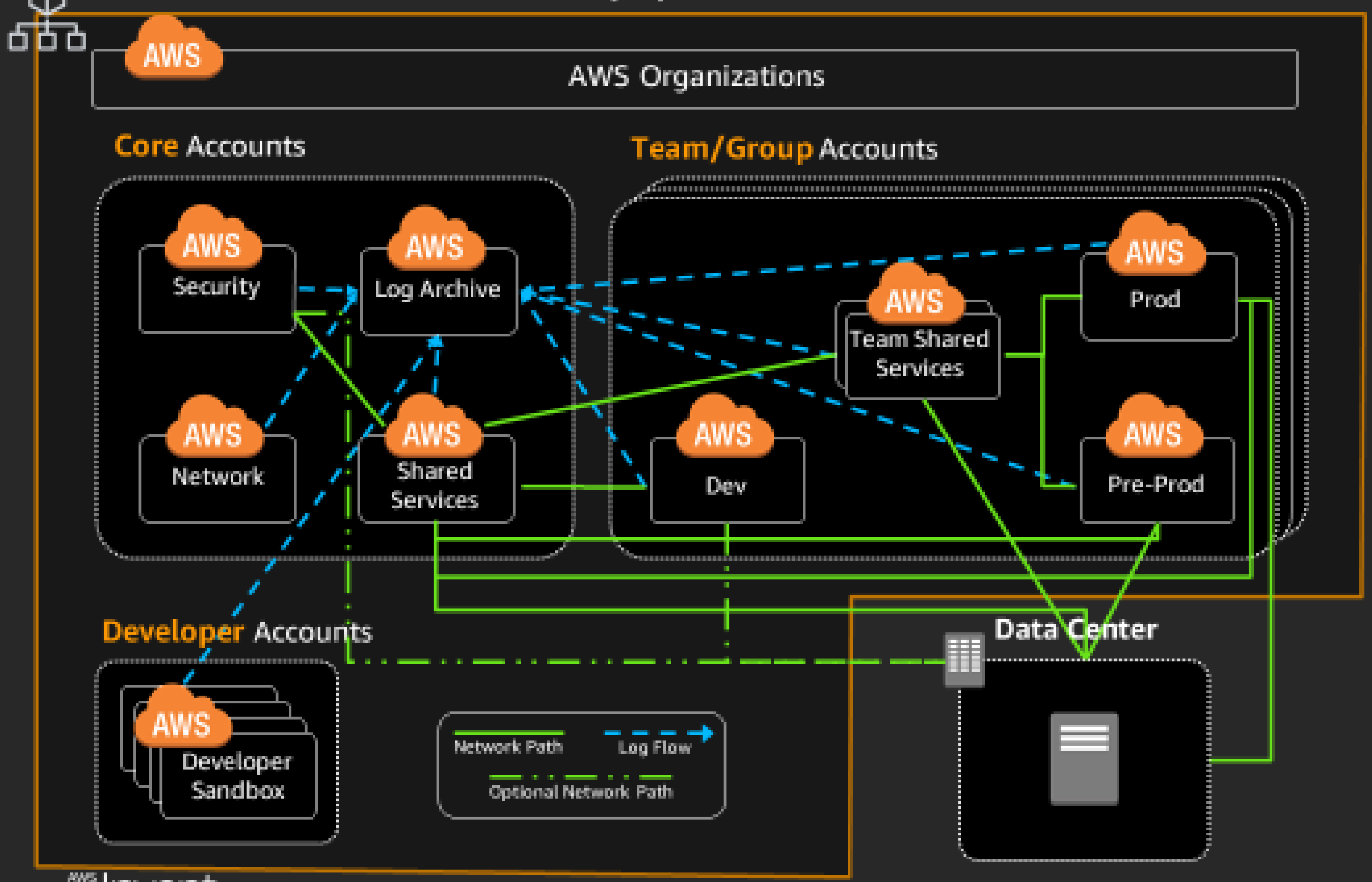
The framework

The services

How does it all fit together?

Have you seen this before? // reinvent 2018

Multi-account approach



AWS Organizations

Core Accounts

AWS Security

AWS Log Archive

AWS Network

AWS Shared Services

Team/Group Accounts

AWS Team Shared Services

AWS Prod

AWS Dev

AWS Pre-Prod

Developer Accounts

AWS Developer Sandbox

Network Path

Log Flow

Optional Network Path

Data Center

Orgs: Account management

Log Archive: Security logs

Security: Security tools, AWS Config rules

Shared services: Directory, limit monitoring

Network: Direct Connect

Dev Sandbox: Experiments, Learning

Dev: Development

Pre-Prod: Staging

Prod: Production

Team SS: Team Shared Services, Data Lake

What do customers want to do on AWS?

Build

focus on what differentiates

Move Fast

ideation to instantiation

Stay Secure

secure and compliant environment

Customers need an environment that is

Secure & compliant

Meets the organization's security and auditing requirements

Scalable & resilient

Ready to support highly available and scalable workloads

Adaptable & flexible

Configurable to support evolving business requirements

Why?

Many teams

Isolation

Billing

Security / compliance controls

Business process

Customers Need

Resource Container

AWS Account

Security/Resource Boundary

API Limits/Throttling

Billing Separation

Isolation with IAM and VPC in one account?

Everything

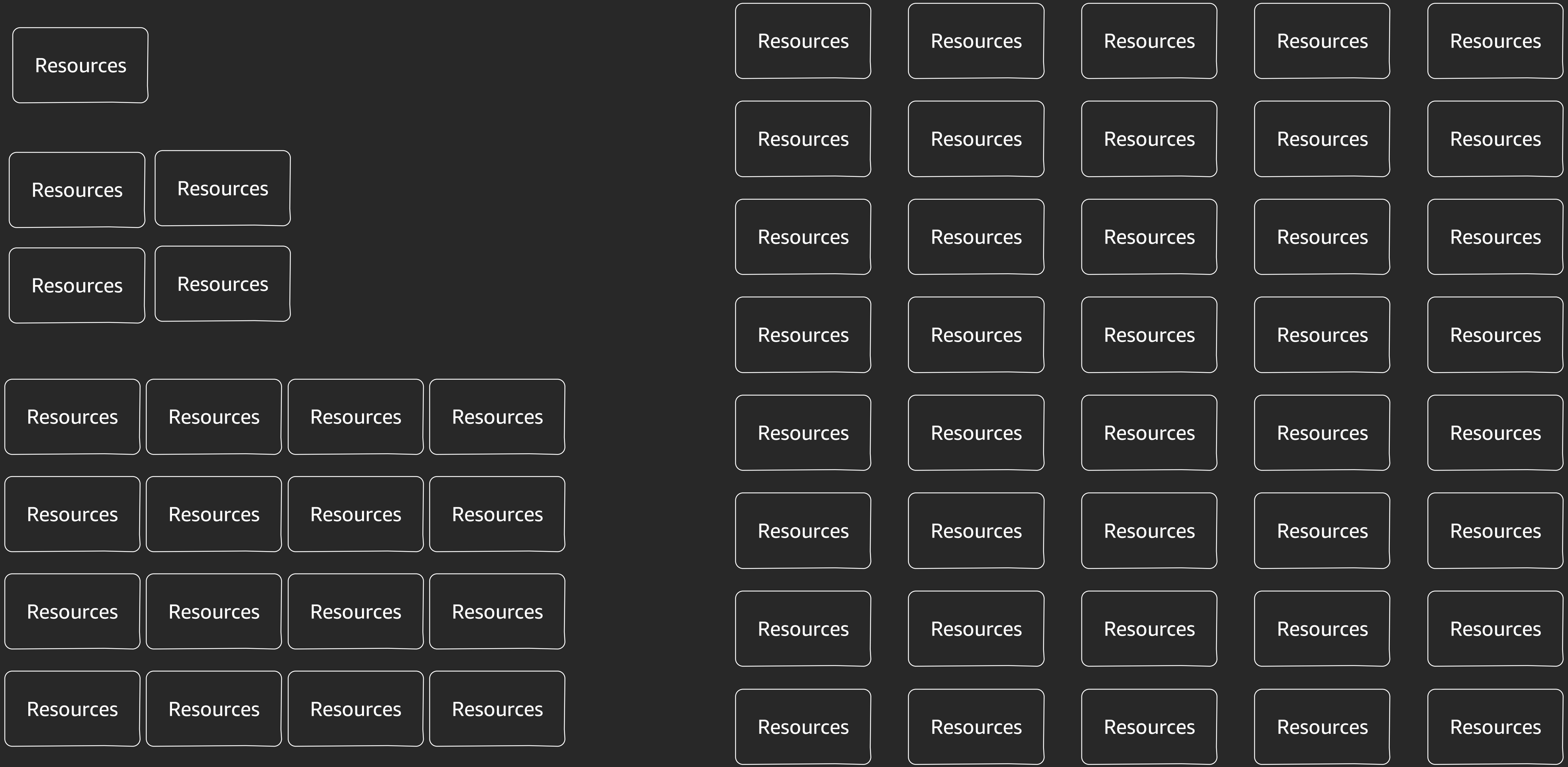
"Gray" boundaries

Complicated and messy over time

Difficult to track resources

People stepping on each other

Resource containers over time



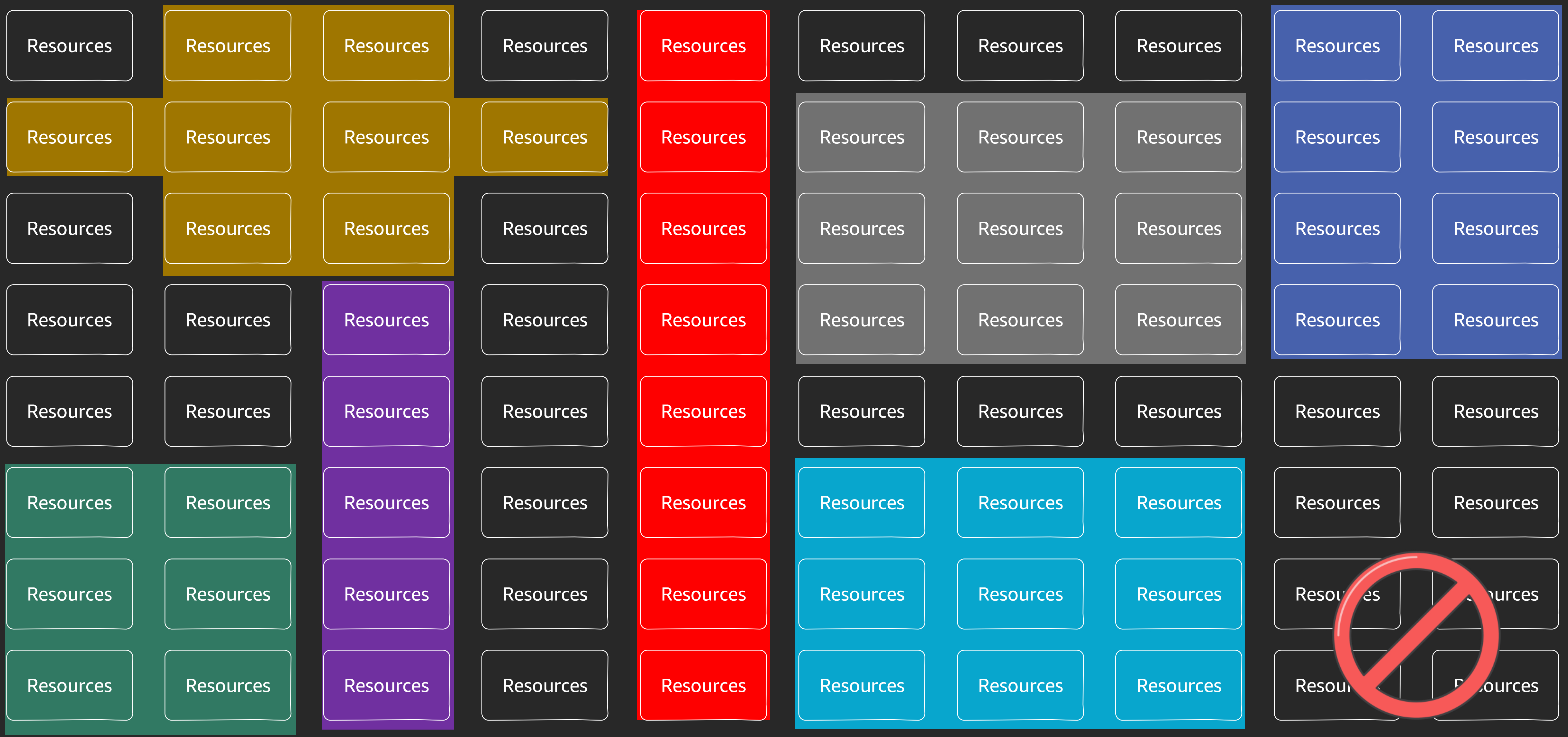
Resources

Resources Resources
Resources Resources

Resources Resources Resources Resources
Resources Resources Resources Resources
Resources Resources Resources Resources
Resources Resources Resources Resources

Resources Resources Resources Resources Resources
Resources Resources Resources Resources Resources
Resources Resources Resources Resources Resources
Resources Resources Resources Resources Resources
Resources Resources Resources Resources Resources
Resources Resources Resources Resources Resources
Resources Resources Resources Resources Resources
Resources Resources Resources Resources Resources

Resource Containers Grouping



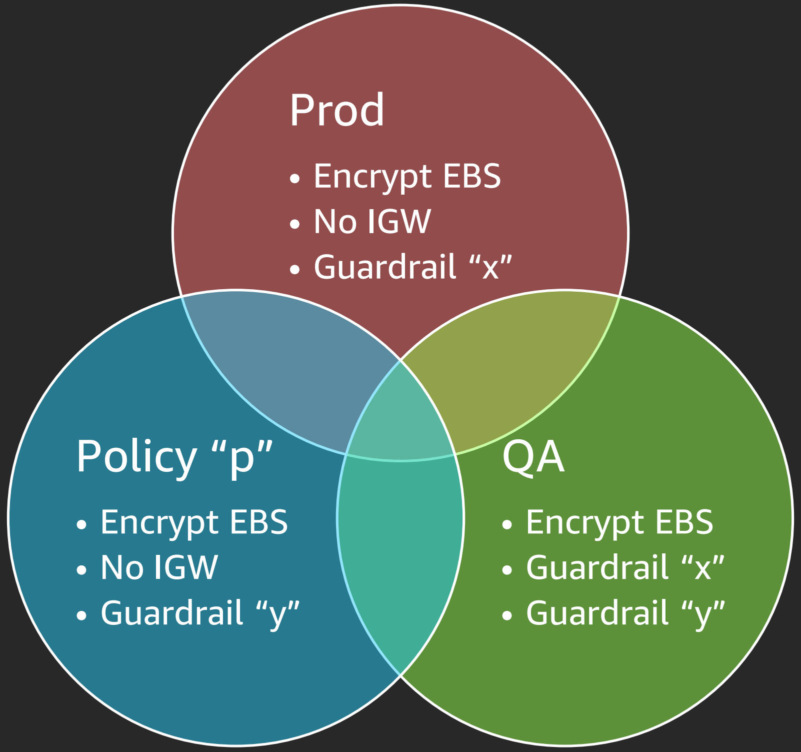
Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources
Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources
Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources
Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources
Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources
Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources
Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources
Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources	Resources

You Need… Orchestration Framework

account management

Notification

Account Metadata: Owner, function, policies, BU, SDLC, cost center, etc …



policy deployment

policy enforcement

Remediation

With capabilities…

Billing Management

Identity and Access Management

Immutable Security Logs

Shared Infrastructure

Resource Isolation

Support Dev Lifecycle

Central Network Connectivity

Security Tooling

Goals

Automated

Scalable

Self-service

Guardrails NOT blockers

Auditable

Flexible

You need a “landing zone”

- A configured, secure, scalable, multi-account (multiple resource containers) AWS environment based on AWS best practices
- A starting point for net new development and experimentation
- A starting point for migrating applications
- An environment that allows for iteration and extension over time

landing zone, AWS Landing Zone, AWS Control Tower

landing zone:

- Secure pre-configured environment for your AWS presence
- Scalable and flexible
- Enables agility and innovation

AWS Landing Zone Solution:

- Implementation of a landing zone based on multi-account strategy guidance

AWS Control Tower:

- AWS Service version of AWS Landing Zone

The Architecture

Service Control Policies (SCPs)

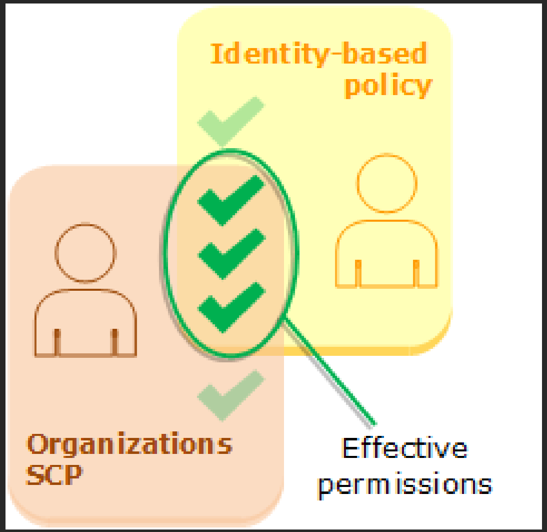
- Enables you to control which AWS service APIs are accessible
  - Define the list of APIs that are allowed – <u>whitelisting</u>
  - Define the list of APIs that must be blocked – <u>blacklisting</u>
- SCPs are:

  Invisible to all users in the child account, <u>including root</u>

  Applied to all users in the child account, <u>including root</u>
- Permission:

  intersection between the SCP and IAM permissions

  IAM policy simulator is SCP aware



Disable Service APIs you Won’t be Using

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

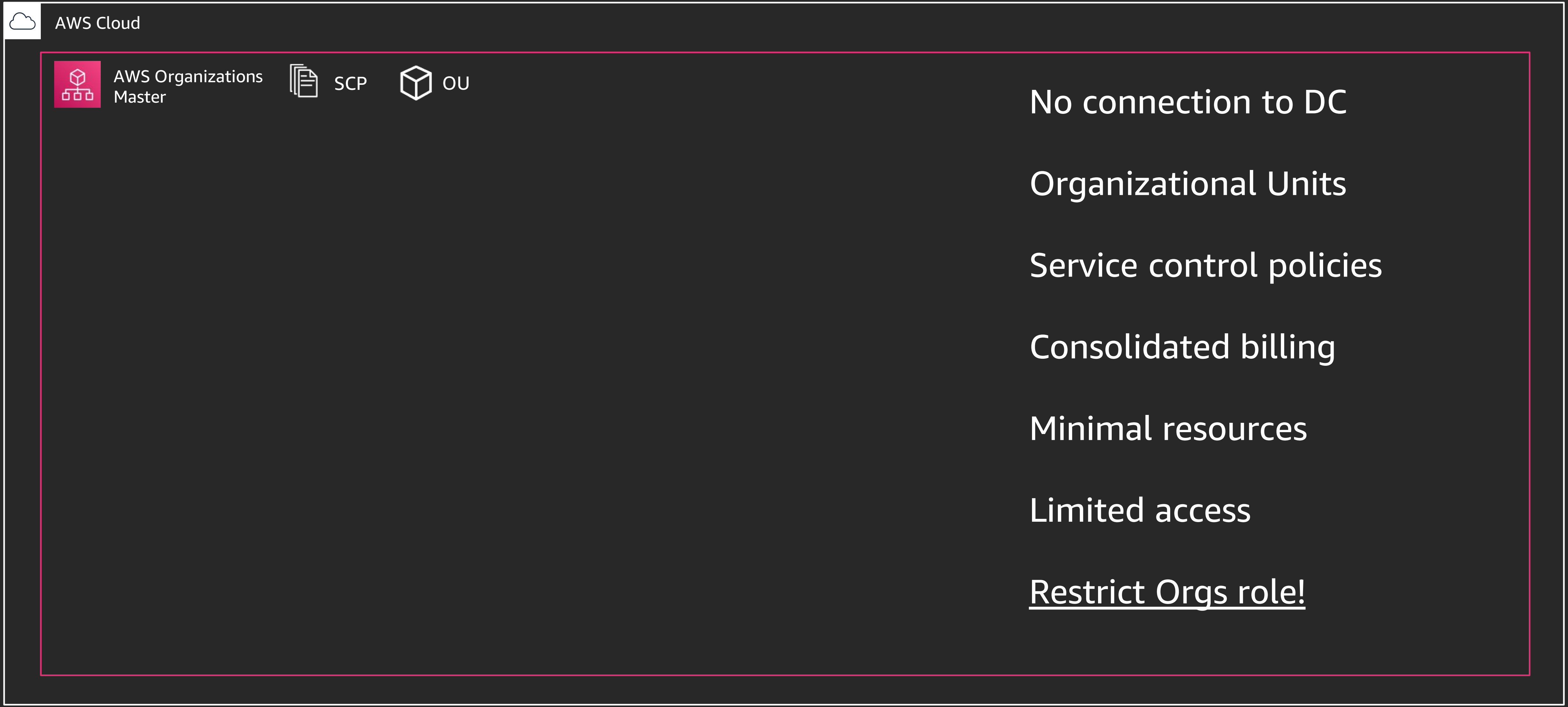
NotAction	(Optional) List the AWS actions exempt from the SCP. Used in place of the Action element.
Resource	List the AWS resources the SCP applies to.
Condition	(Optional) Specify conditions for when the statement is in effect.

Organizational Units

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

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

AWS Organizations Master



AWS Cloud

AWS Organizations Master

SCP

OU

No connection to DC

Organizational Units

Service control policies

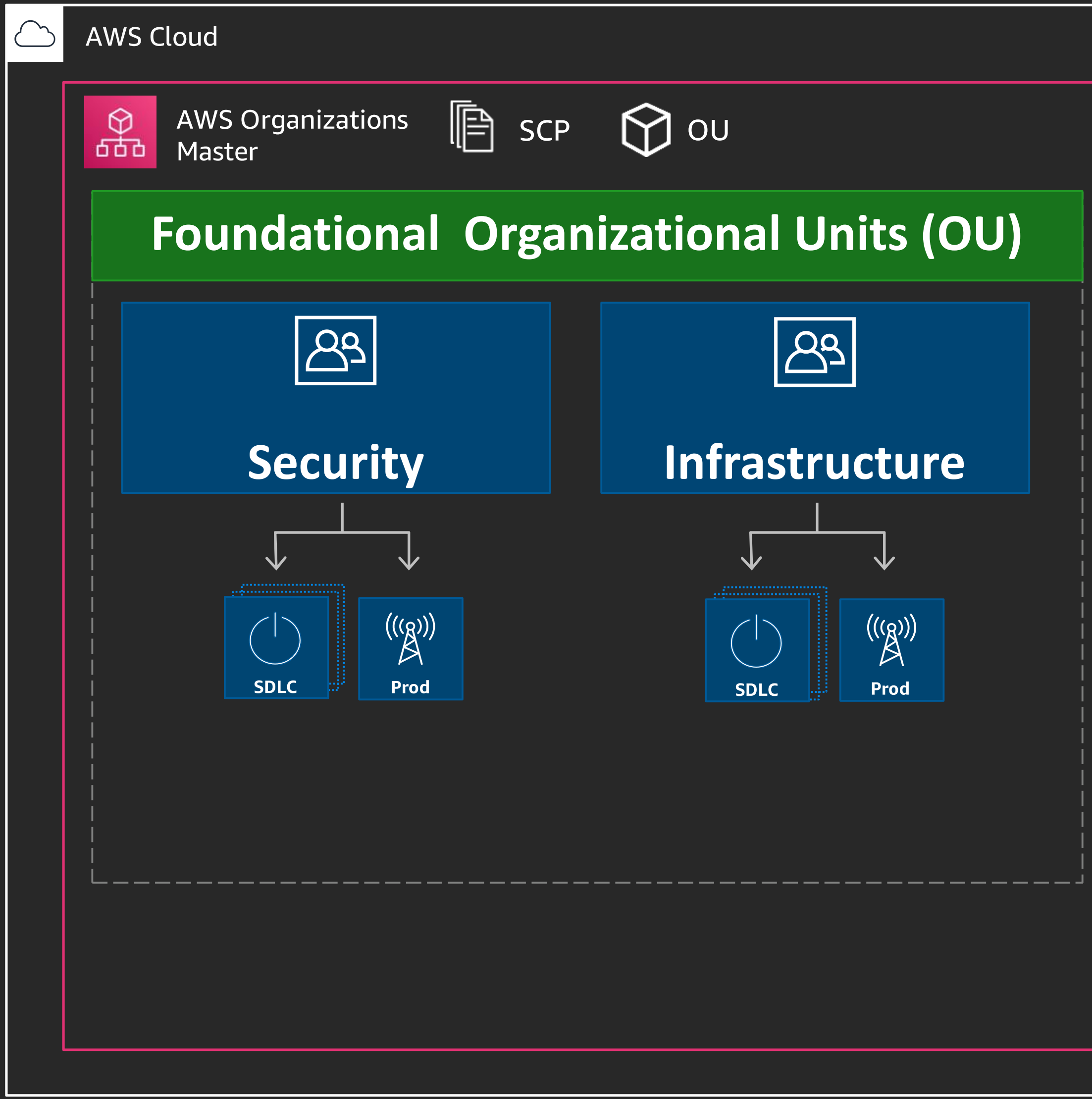
Consolidated billing

Minimal resources

Limited access

Restrict Orgs role!

Foundational OUs



Foundational

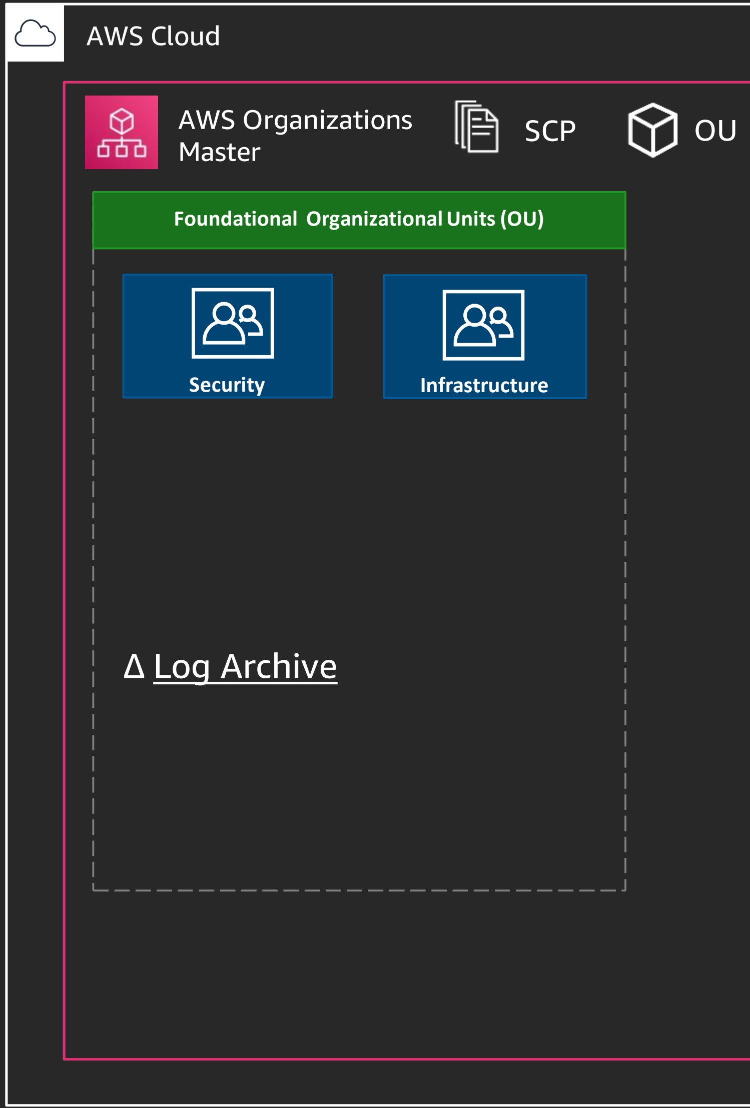
Building blocks

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

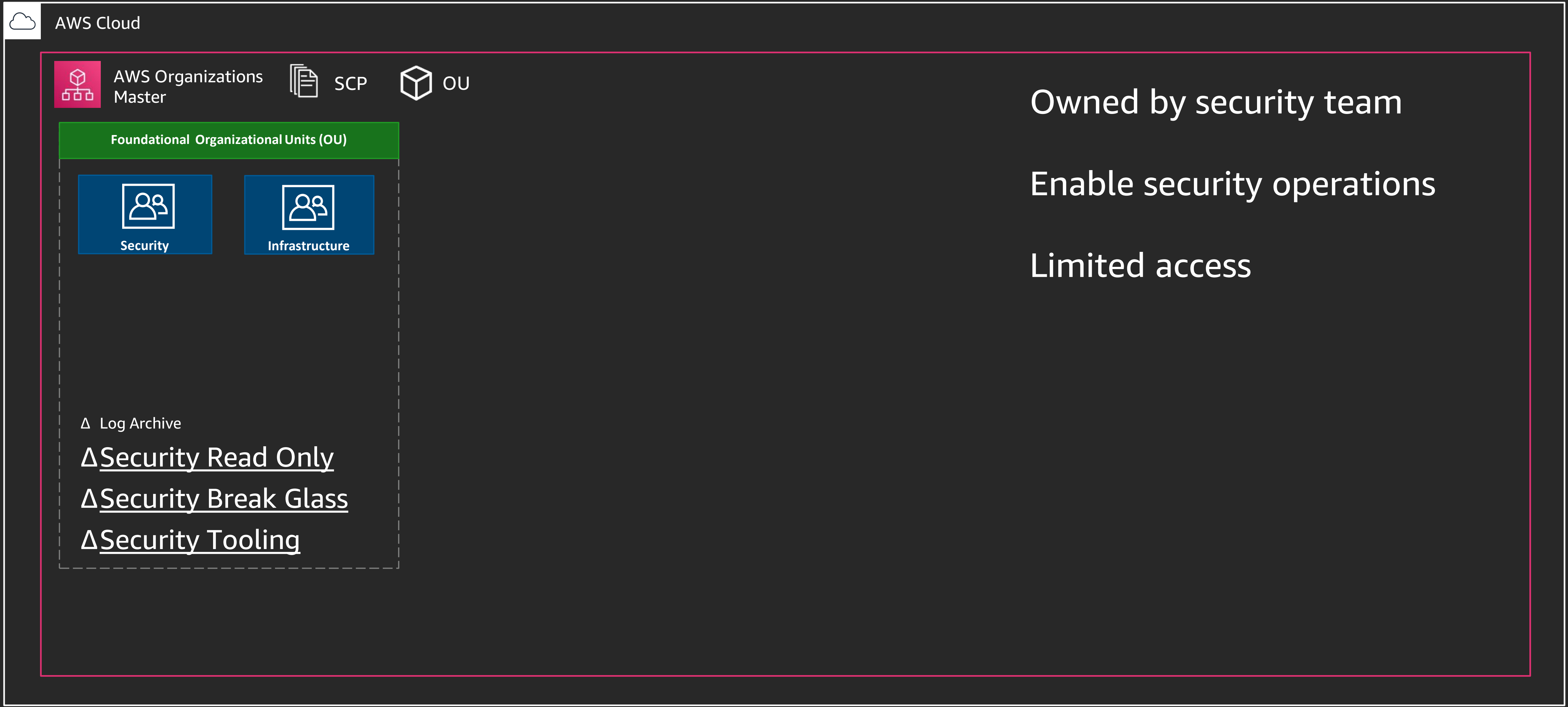
Security logs

Single source of truth

Alarm on user login

Limited access

Security Accounts



AWS Cloud

AWS Organizations Master

SCP

OU

Foundational Organizational Units (OU)

Security

Infrastructure

Δ Log Archive

Δ Security Read Only

Δ Security Break Glass

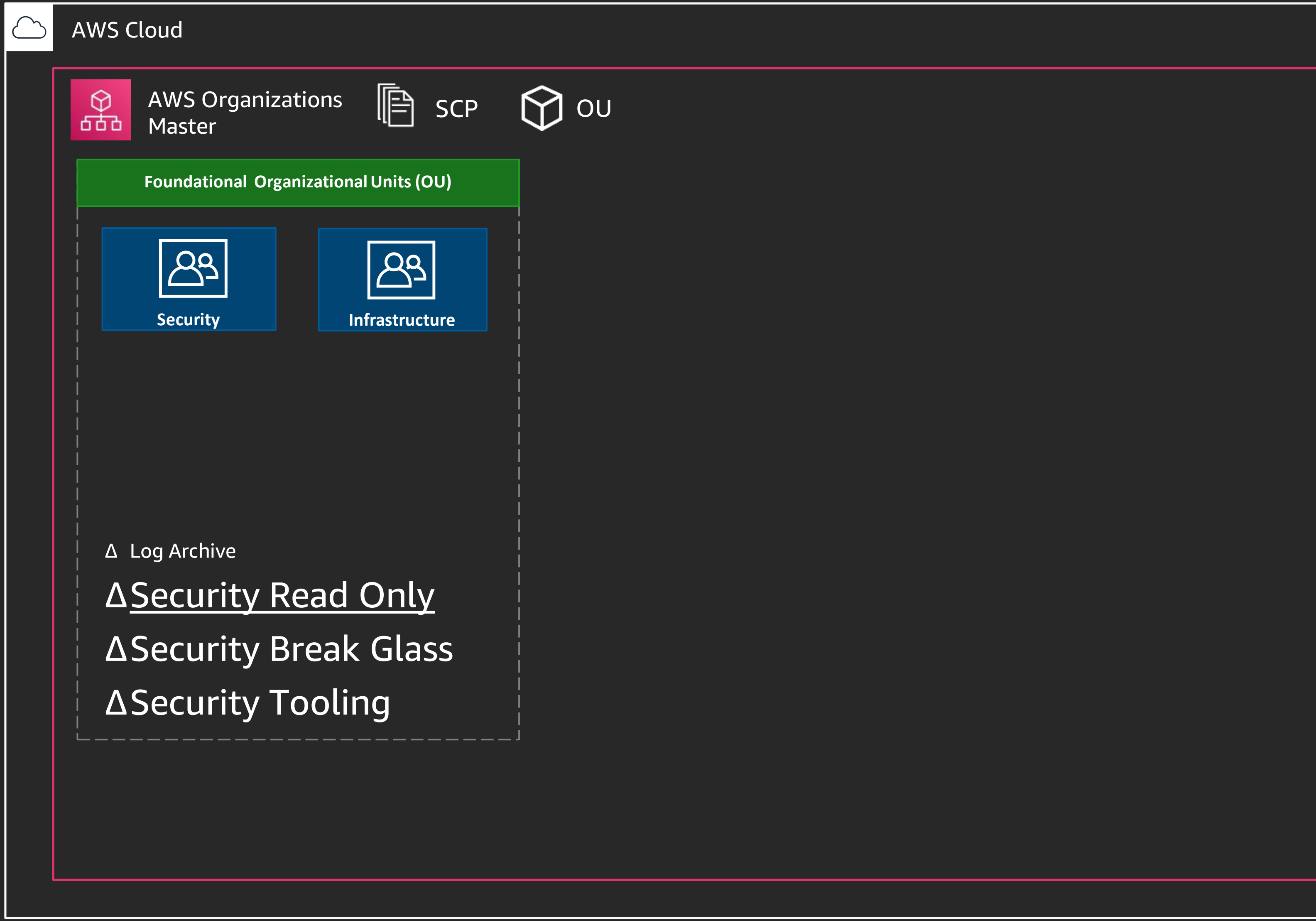
Δ Security Tooling

Owned by security team

Enable security operations

Limited access

Security Accounts // Read Only



Δ Log Archive

Δ Security Read Only

Δ Security Break Glass

Δ Security Tooling

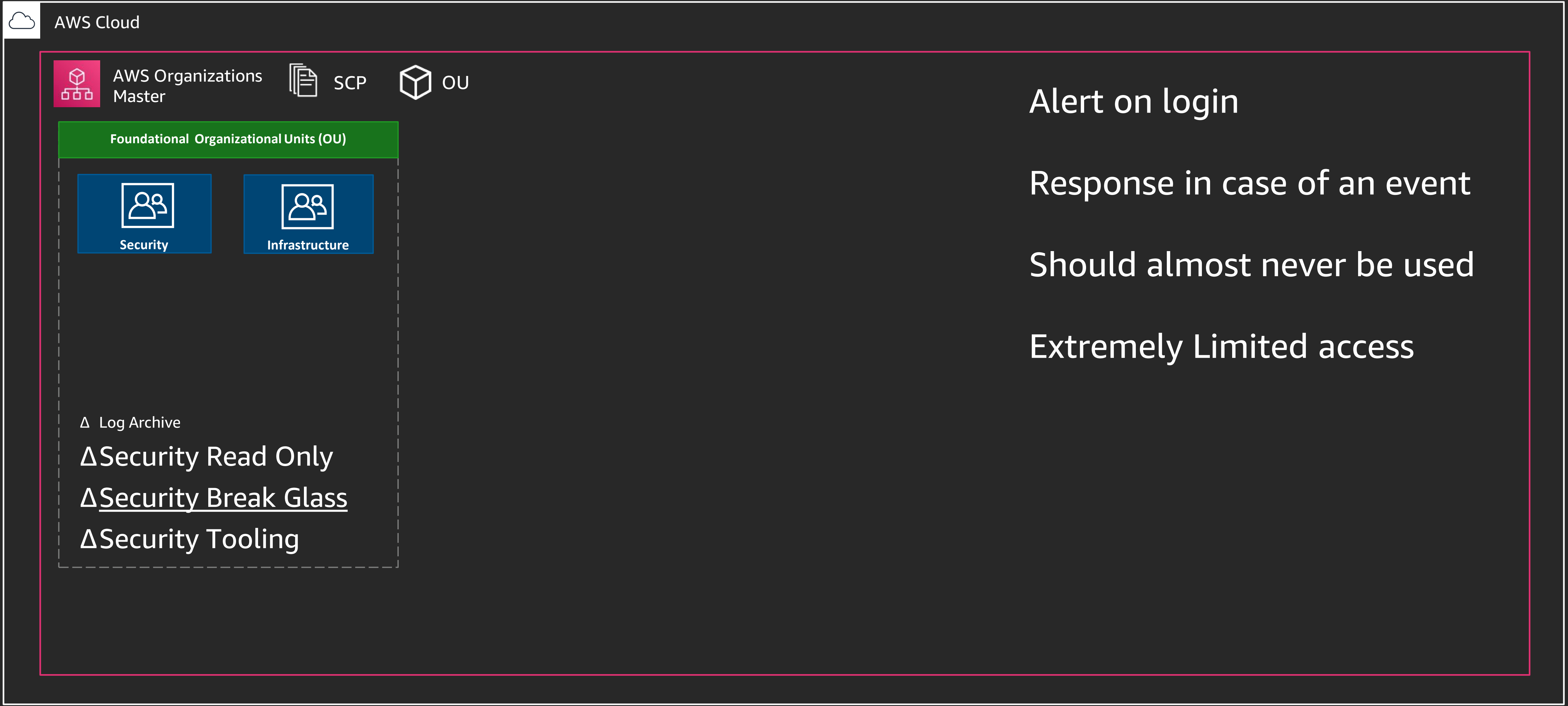
View/Scan resources in other accounts

Exploratory Security Testing

Cross account read-only (security Auditor)

Limited access

Security Accounts // Break Glass



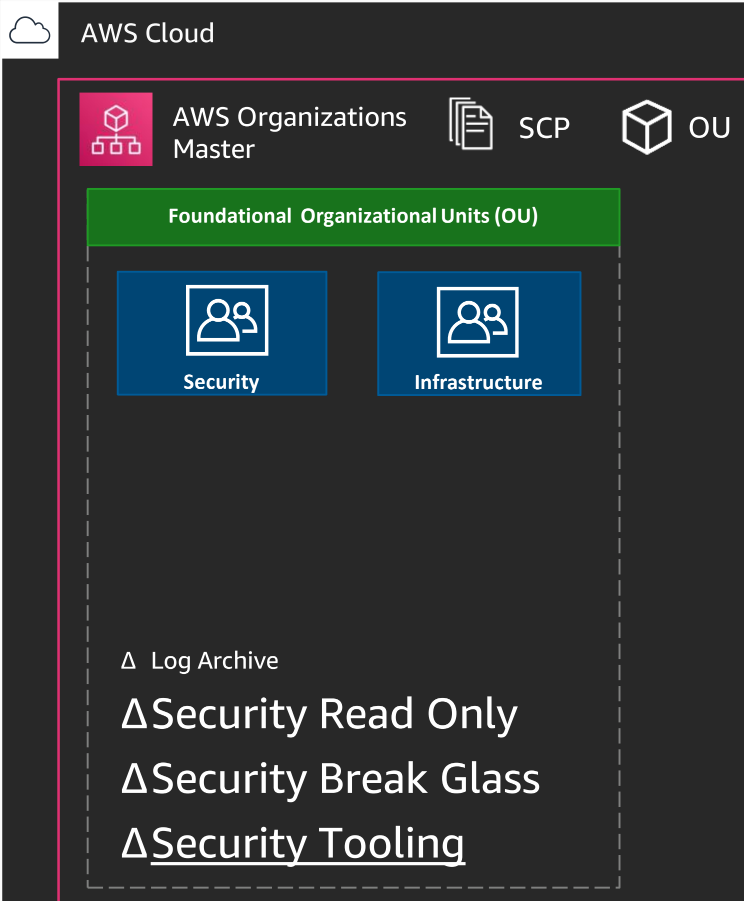
Alert on login

Response in case of an event

Should almost never be used

Extremely Limited access

Security Accounts // Tooling



AWS Cloud

AWS Organizations Master

SCP

OU

Foundational Organizational Units (OU)

Security

Infrastructure

Δ Log Archive

ΔSecurity Read Only

ΔSecurity Break Glass

ΔSecurity Tooling

Security tools and audit

Amazon GuardDuty

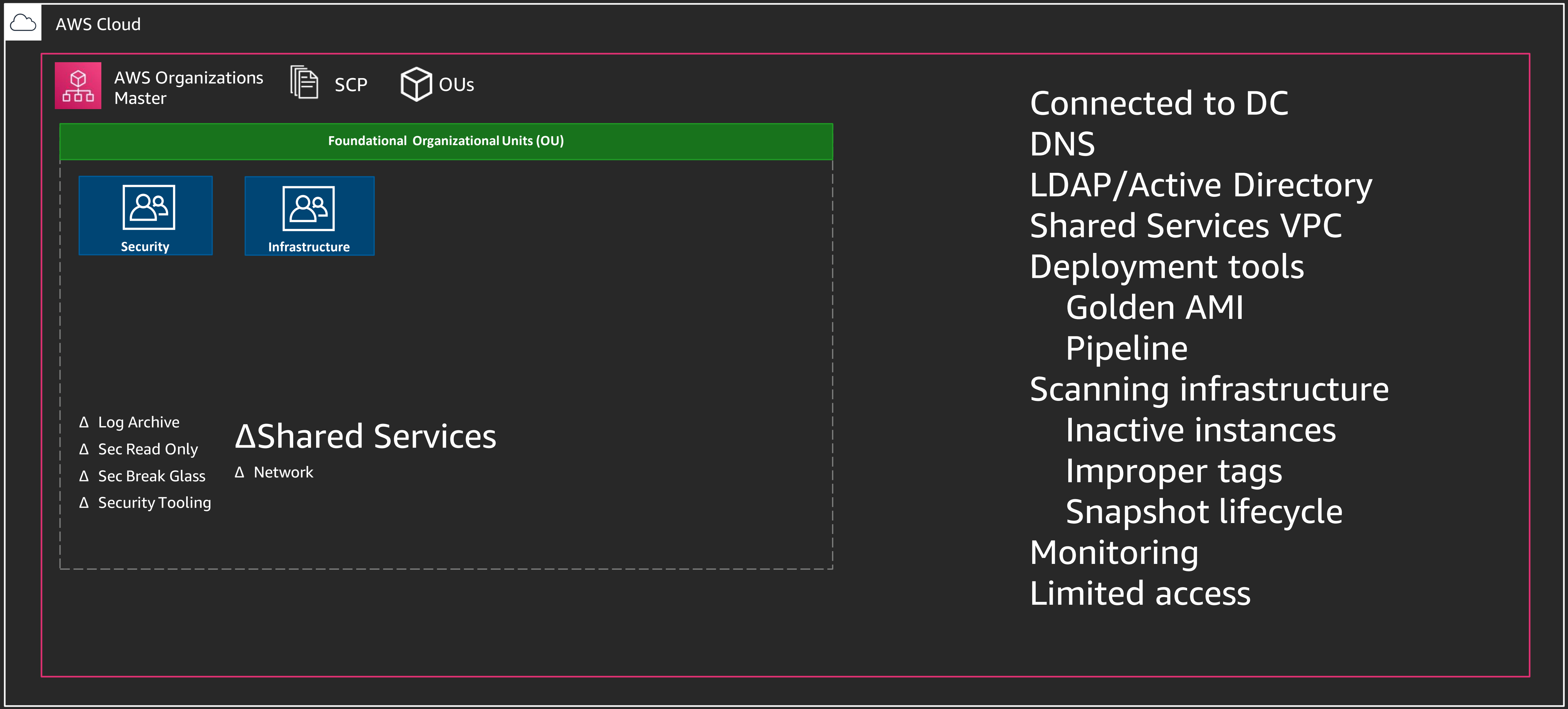
AWS Security Hub

AWS Config Aggregation

Cross-account roles
Automated Tooling

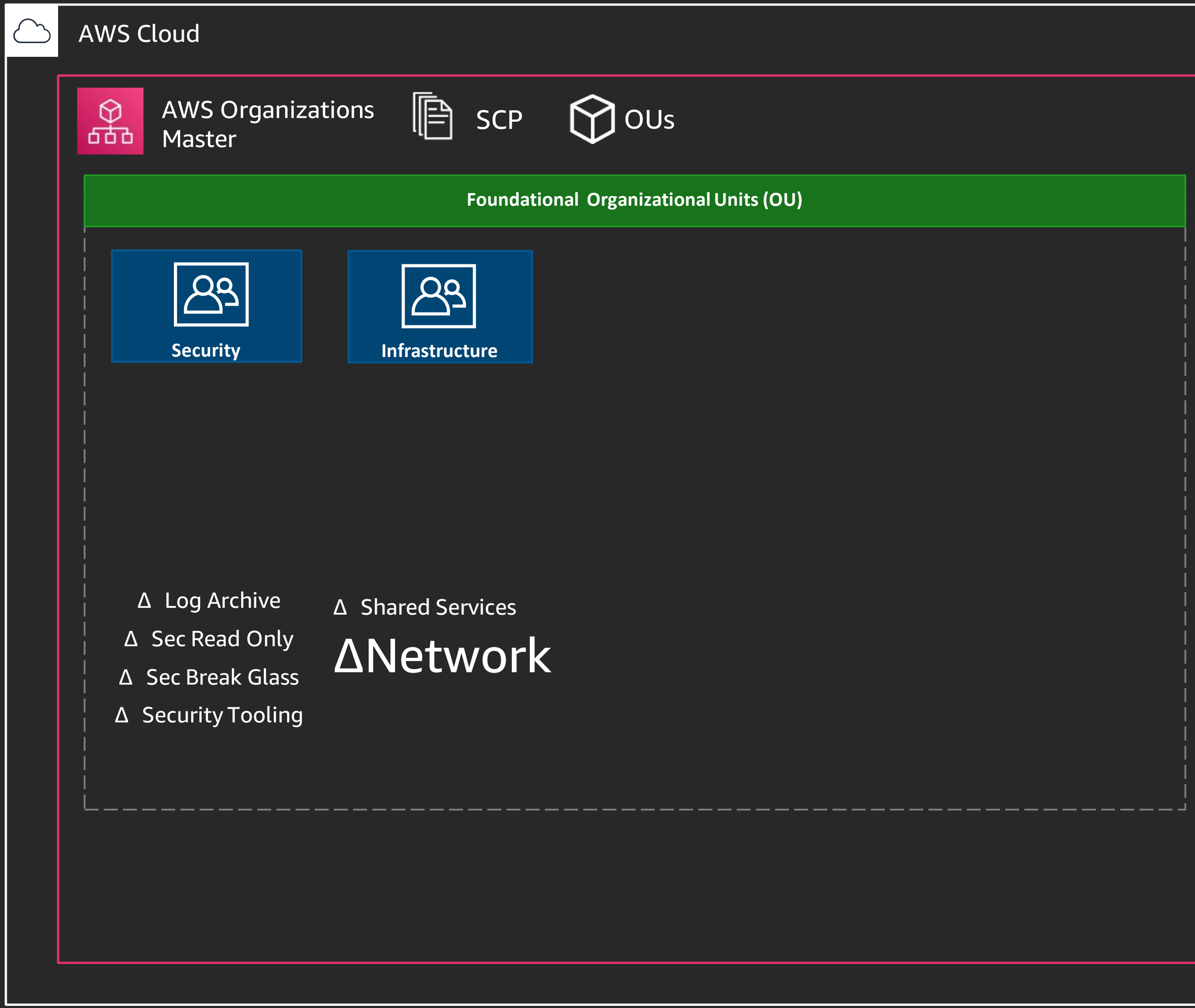
Automations, not humans

Shared Services



Connected to DC
DNS
LDAP/Active Directory
Shared Services VPC
Deployment tools
Golden AMI
Pipeline
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

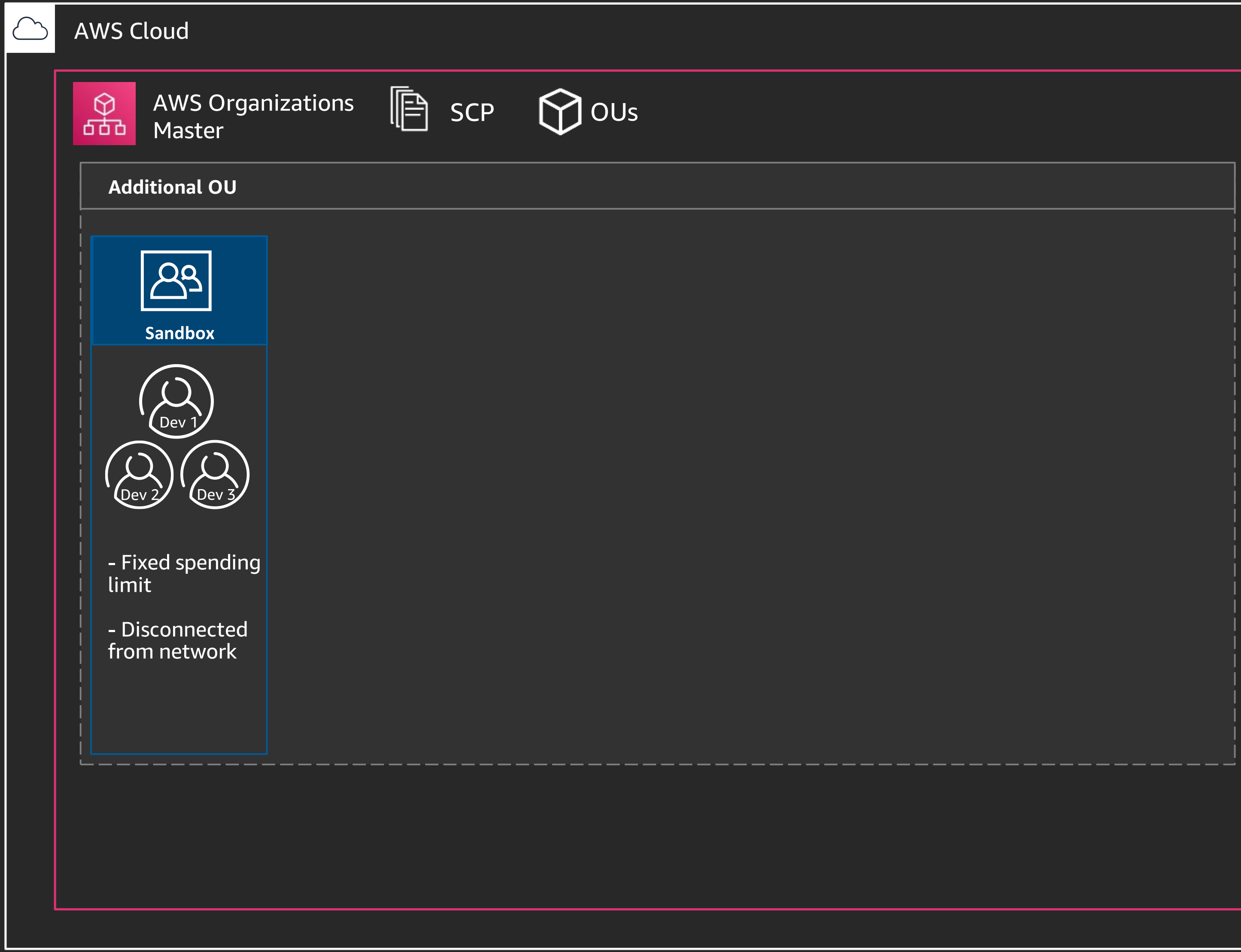
Shared VPCs

AWS Transit Gateway

Limited access

Additional organizational units

Developer Sandbox



No connection to DC

Individual Dev Accounts

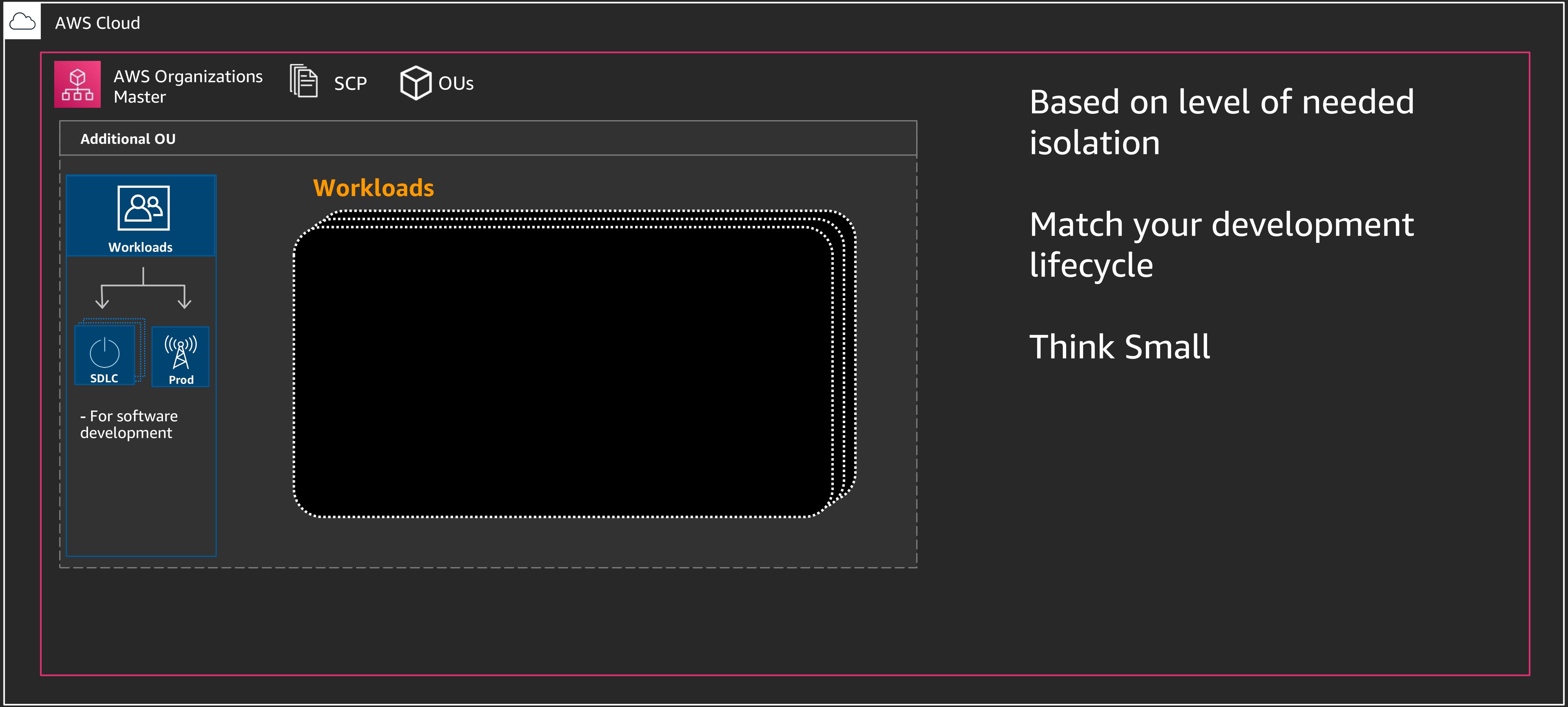
Innovation space

Fixed spending limit

Autonomous

Experimentation

Workloads

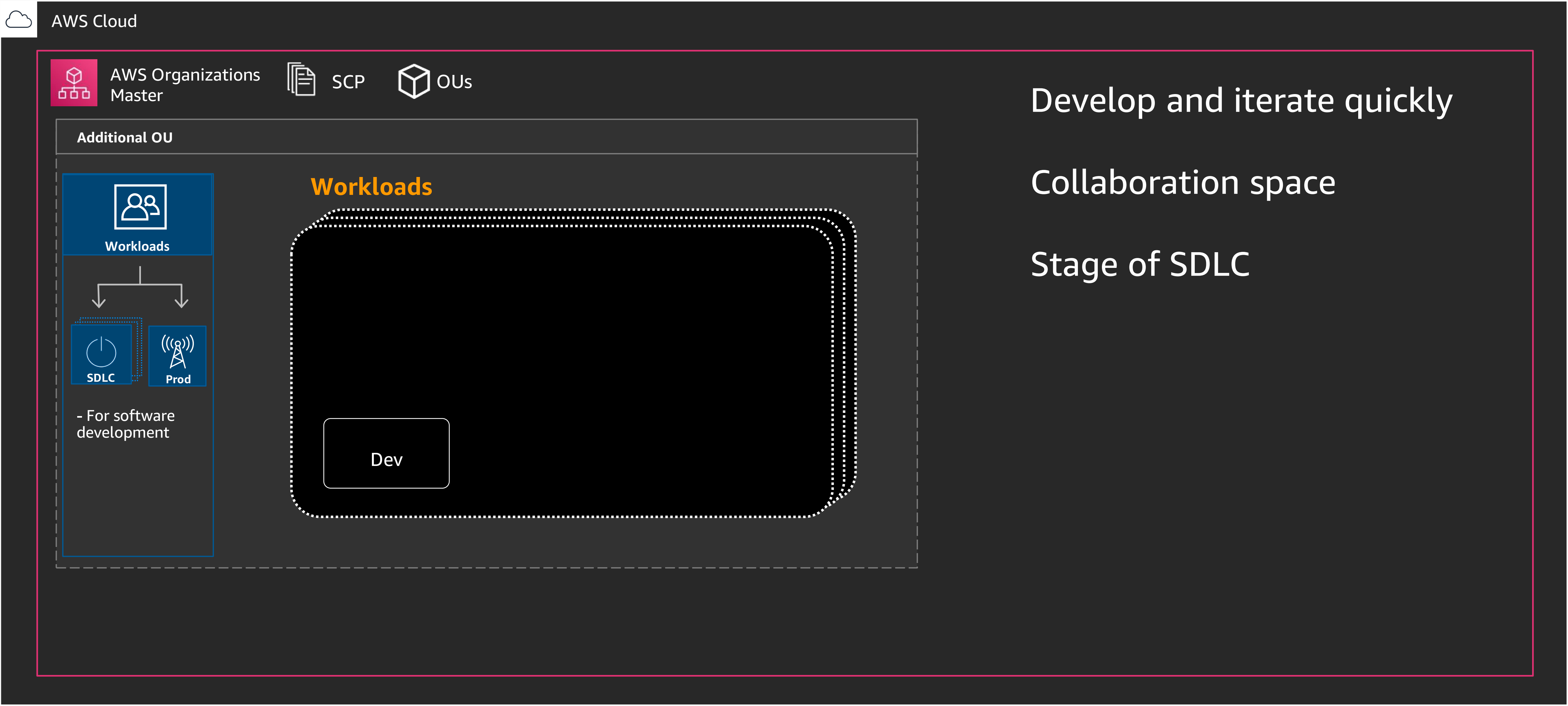


Based on level of needed isolation

Match your development lifecycle

Think Small

Workloads // Dev

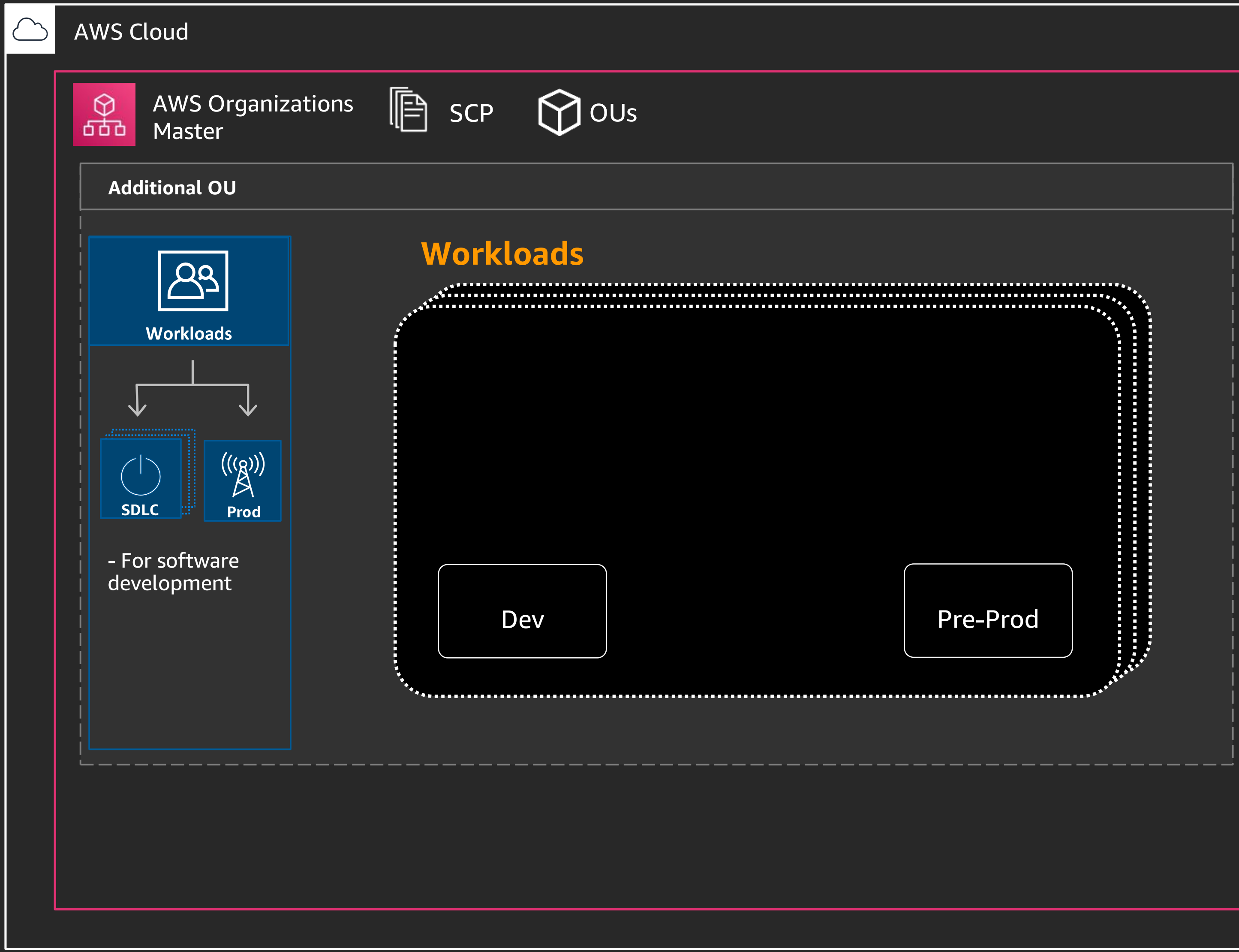


Develop and iterate quickly

Collaboration space

Stage of SDLC

Workloads // Pre-Prod



Connected to DC

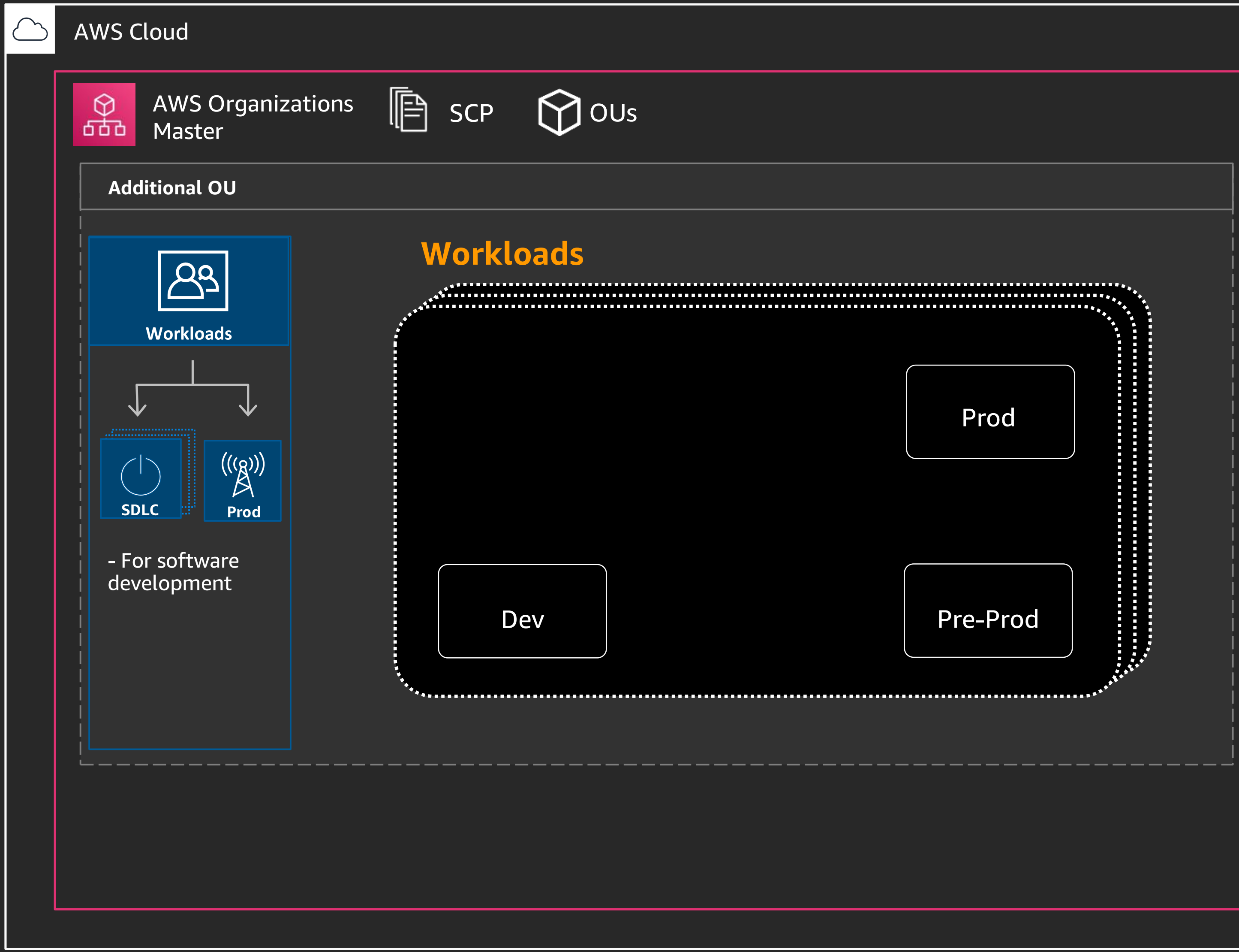
Production-like

Staging

Testing

Automated deployment

Workloads // Prod



Connected to DC

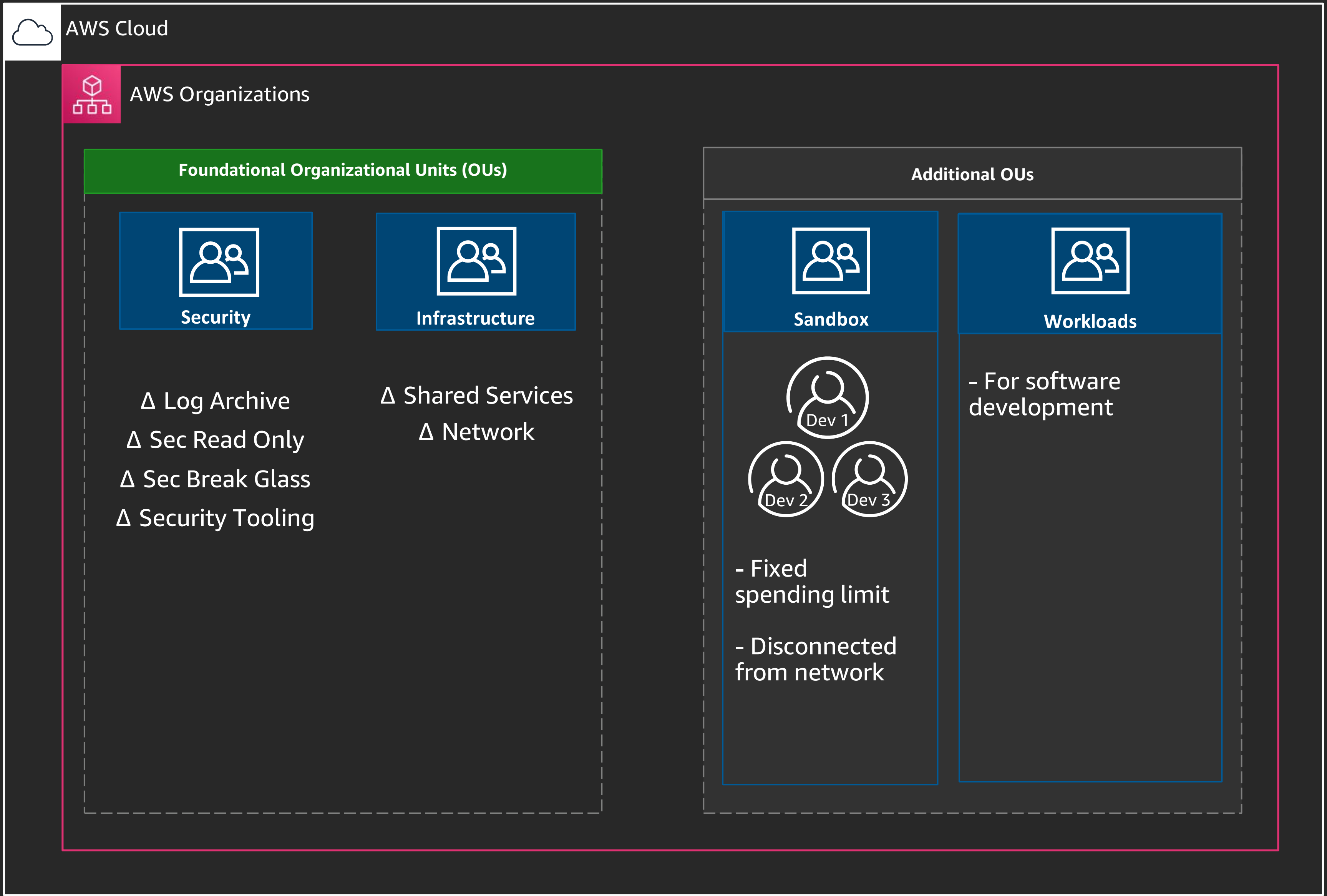
Production applications

Promoted from Pre-Prod

Limited access

Automated deployments

Starter AWS multi-account framework



AWS Cloud

AWS Organizations

Foundational Organizational Units (OUs)

Security

Δ Log Archive
Δ Sec Read Only
Δ Sec Break Glass
Δ Security Tooling

Infrastructure

Δ Shared Services
Δ Network

Additional OUs

Sandbox

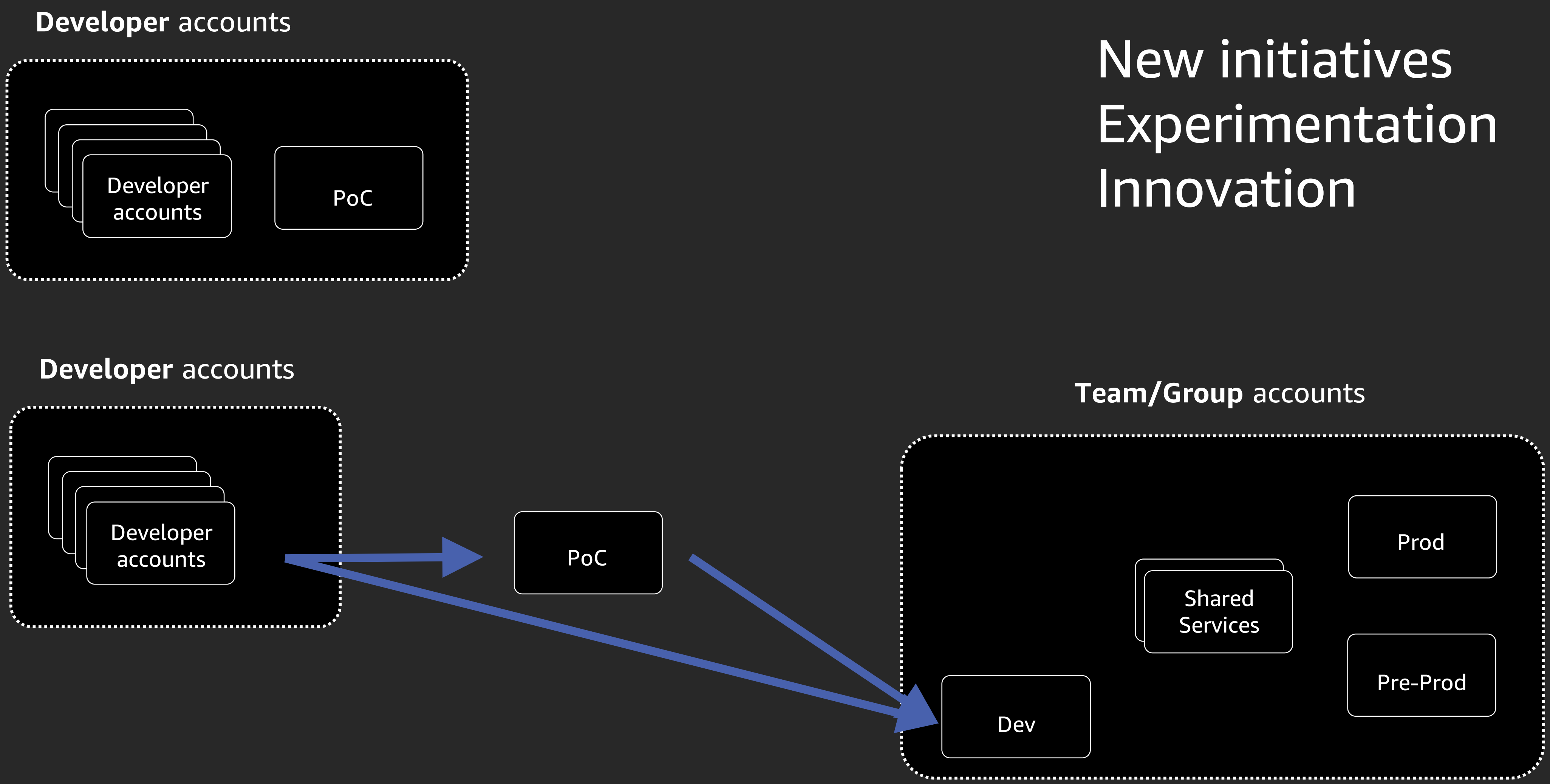
- Fixed spending limit
- Disconnected from network

Workloads

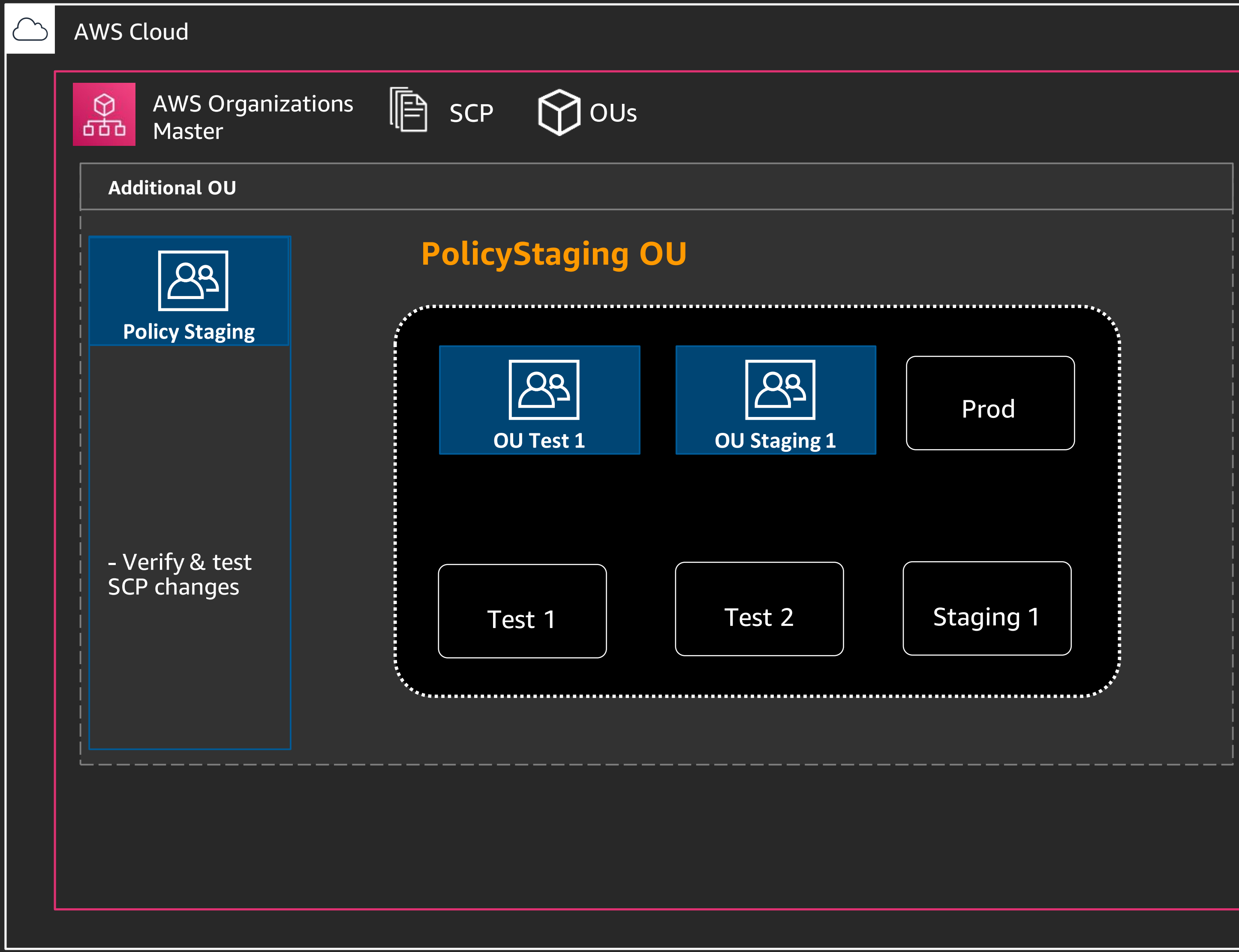
- For software development

Innovation pipeline

New initiatives
Experimentation
Innovation



PolicyStaging OU



Safely test policy changes

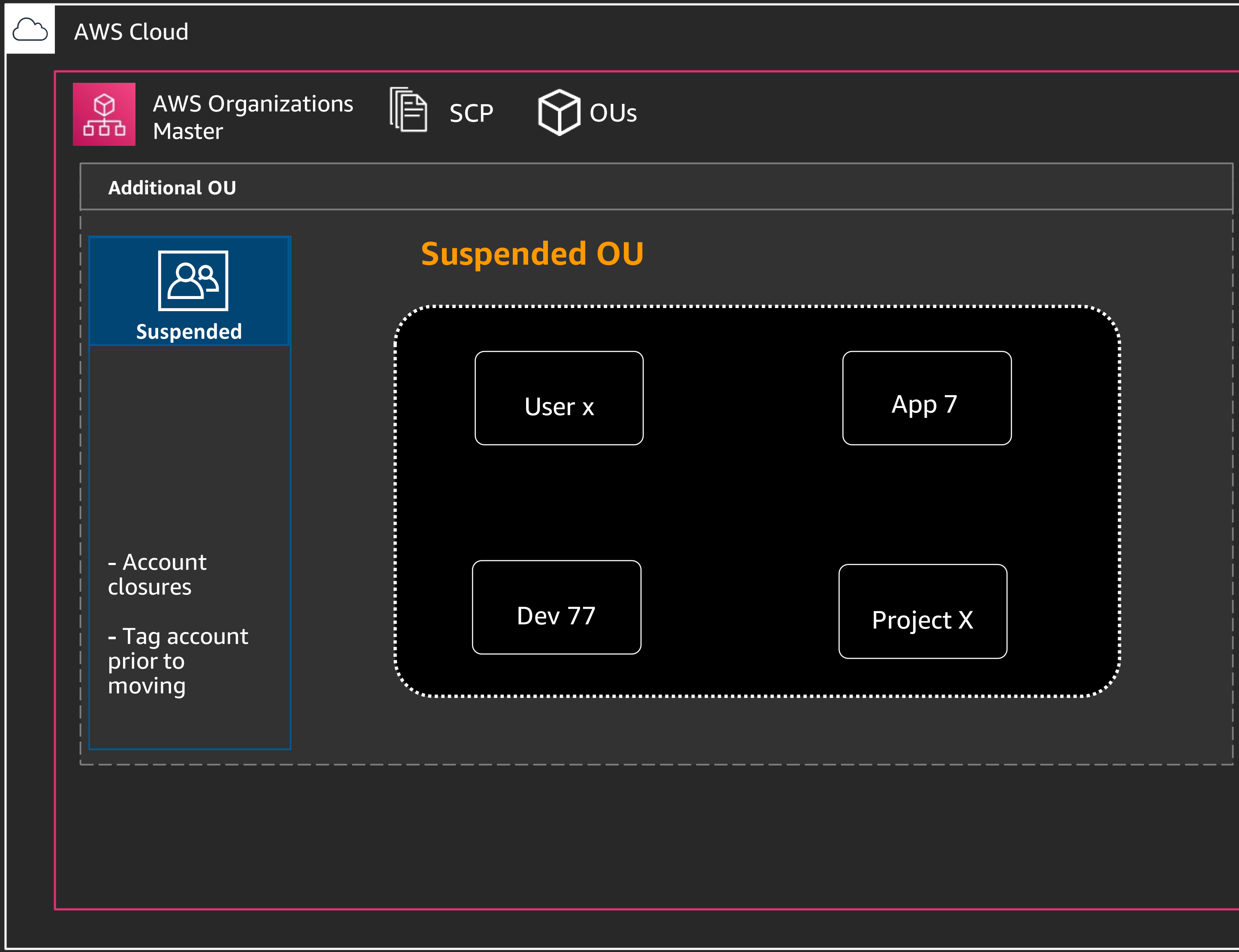
Test Single Account

Promote to an OU

Promote to final target OU

Reduces need for 2nd Org

Suspended OU



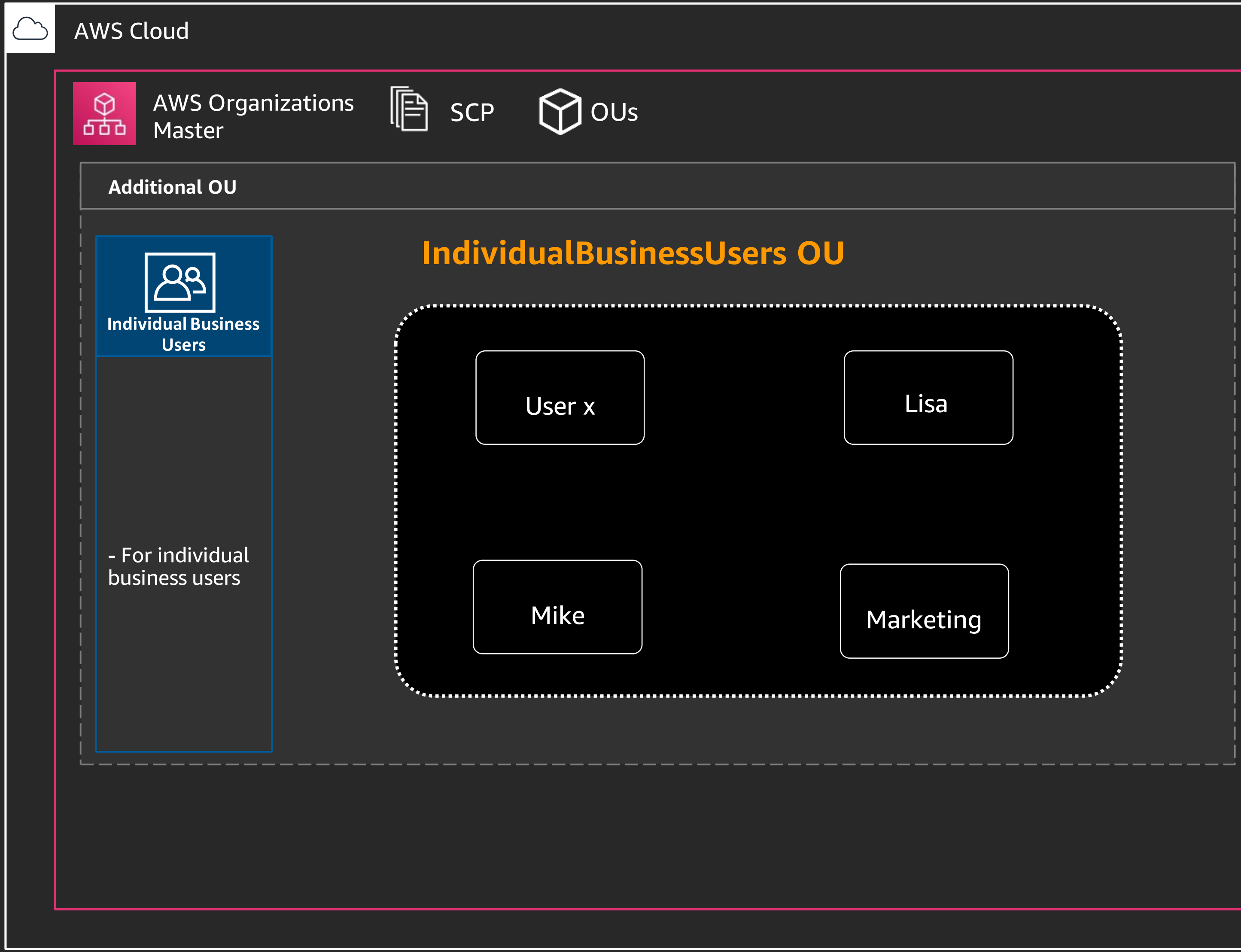
Deny All SCP

Account Closure

Departures

Tag Account prior to moving

IndividualBusinessUsers OU


AWS Cloud
AWS Organizations Master
SCP
OUs
Additional OU
Individual Business Users
- For individual business users
IndividualBusinessUsers OU
User x
Lisa
Mike
Marketing

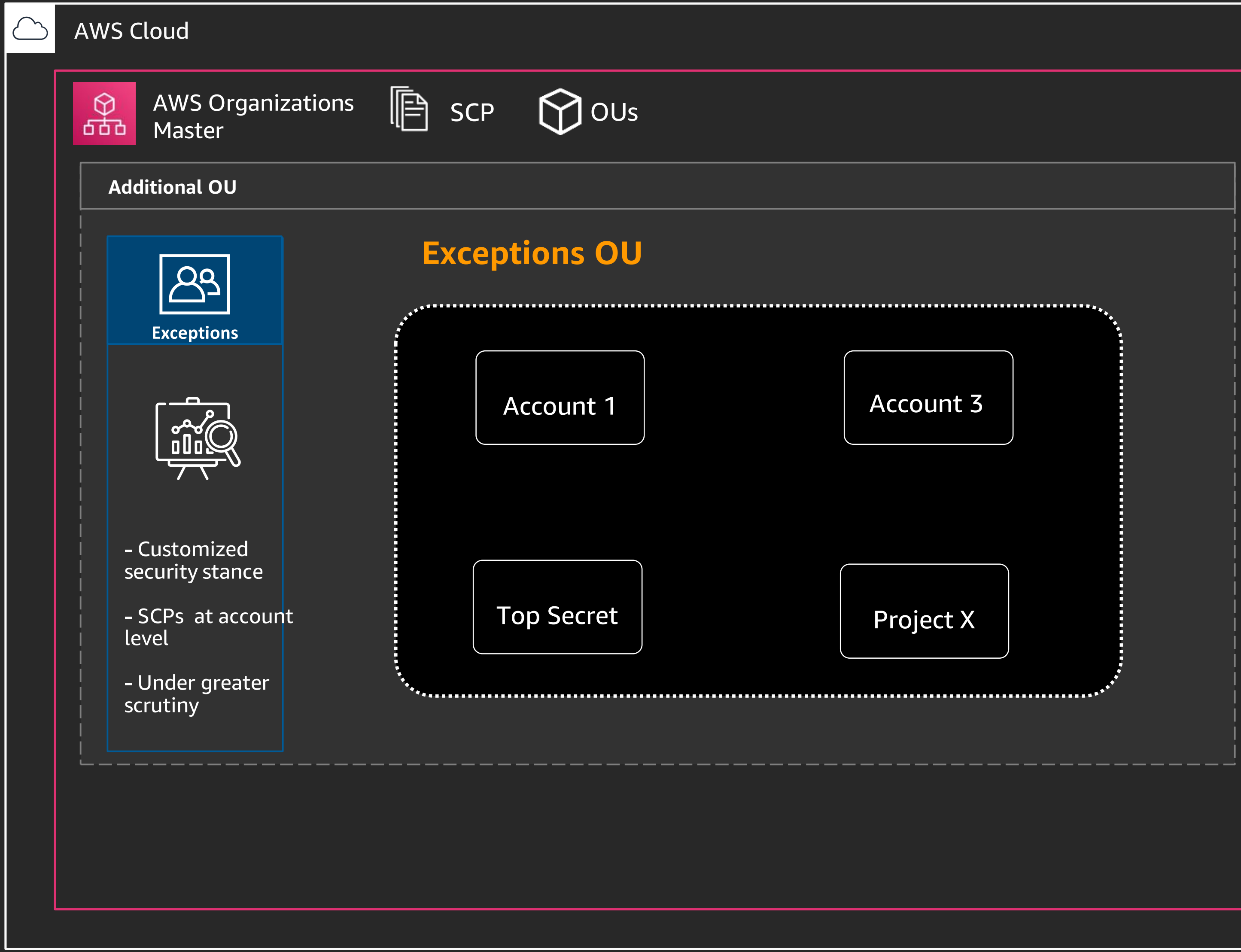
Need access for business reasons

Reporting access

S3 bucket to share marketing videos/data

Case by case and pre authorized

Exceptions OU



- Customized security stance
- SCPs at account level
- Under greater scrutiny

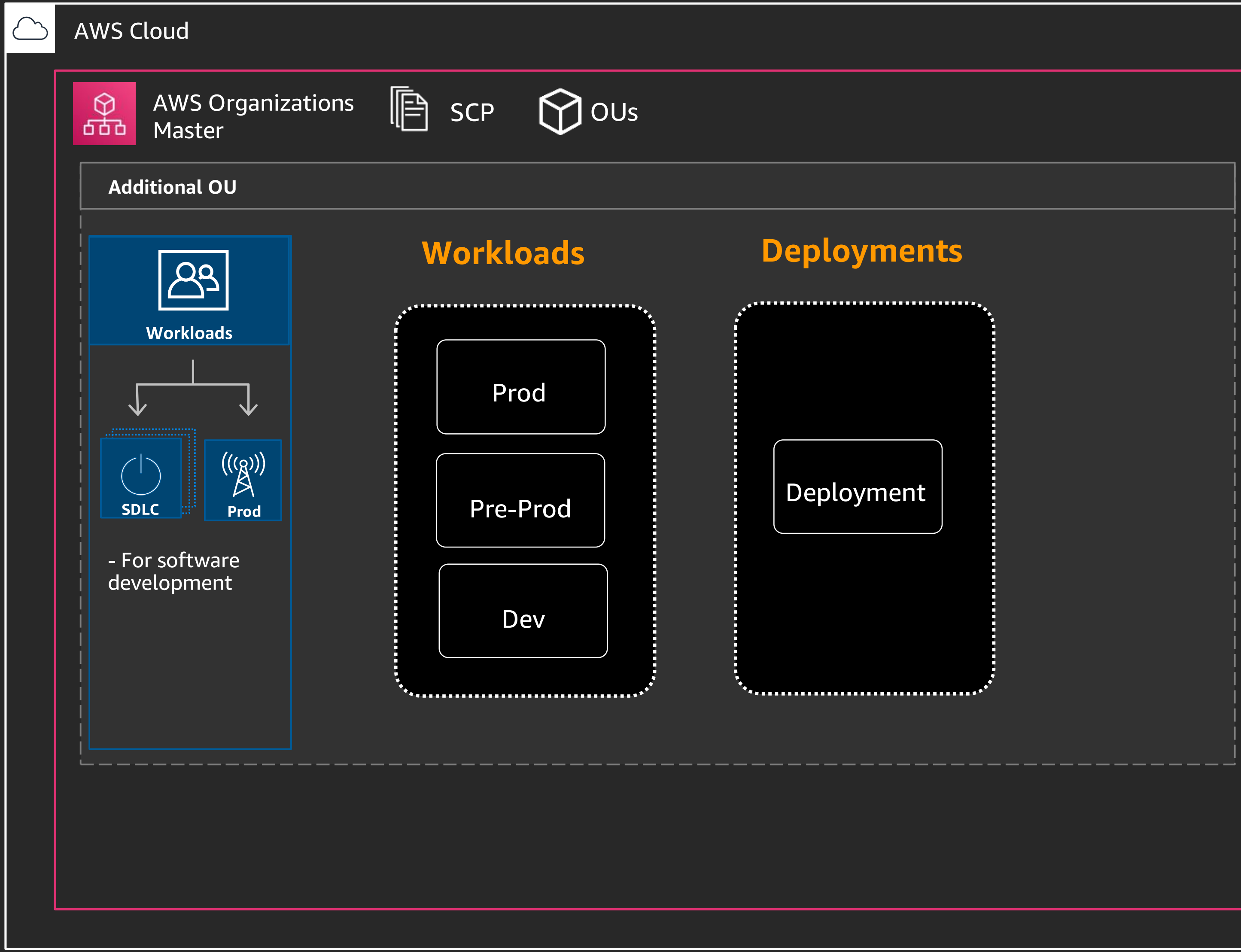
No SCP on OU

SCP on accounts

Strict approval process

SCPs applied to accounts

Deployments OU



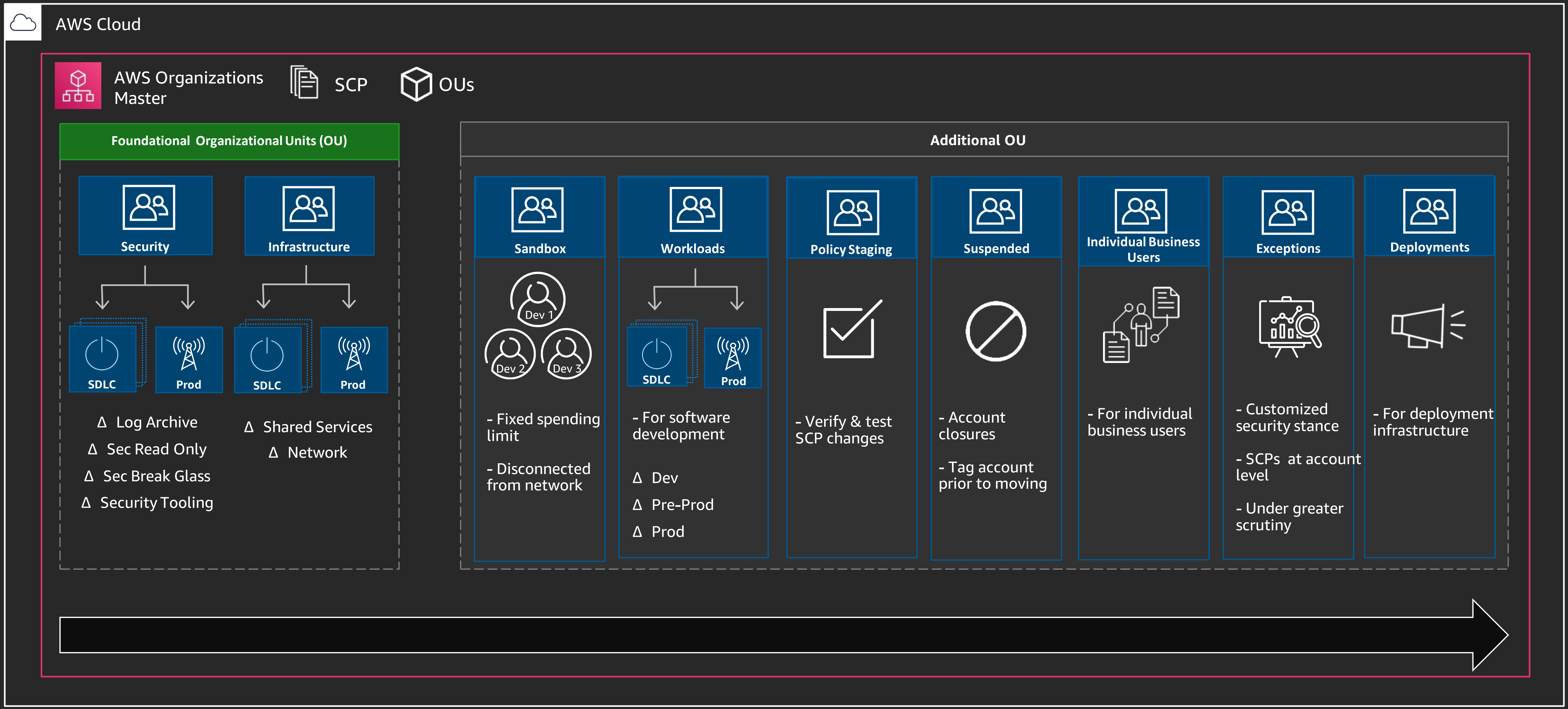
Build Pipelines

One Account for each Workload

Highly secured

Extremely Limited access

Multi-account framework



AWS Cloud

AWS Organizations Master

SCP

OUs

Foundational Organizational Units (OU)

Security

SDLC

Prod

- Δ Log Archive
- Δ Sec Read Only
- Δ Sec Break Glass
- Δ Security Tooling

Infrastructure

SDLC

Prod

- Δ Shared Services
- Δ Network

Additional OU

Sandbox

Dev 1

Dev 2

Dev 3

- Fixed spending limit

- Disconnected from network

Workloads

SDLC

Prod

- For software development

- Δ Dev
- Δ Pre-Prod
- Δ Prod

Policy Staging

- Verify & test SCP changes

Suspended

- Account closures

- Tag account prior to moving

Individual Business Users

- For individual business users

Exceptions

- Customized security stance

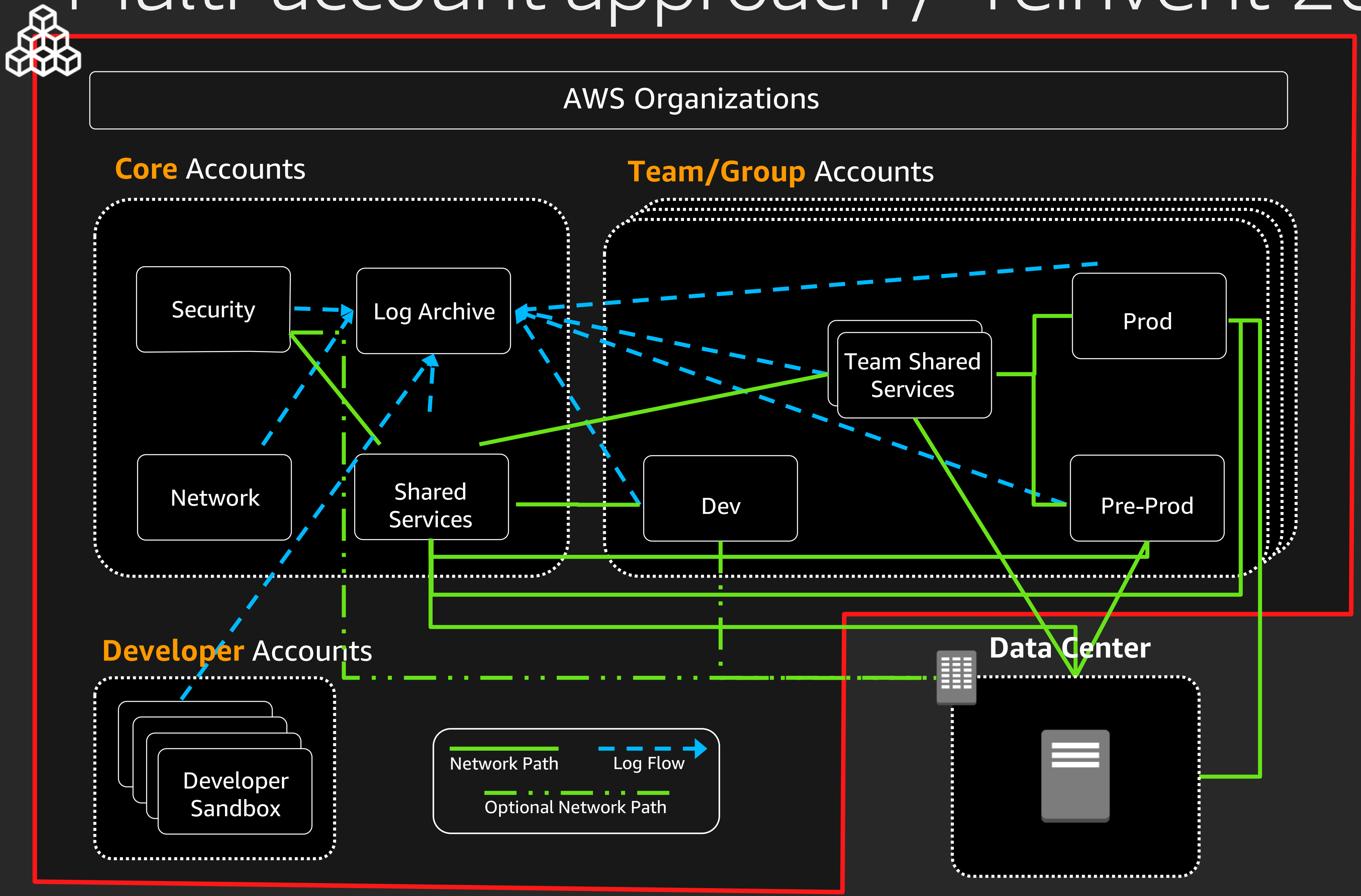
- SCPs at account level

- Under greater scrutiny

Deployments

- For deployment infrastructure

Multi-account approach / reinvent 2018 (old)



Orgs: Account management

Log Archive: Security logs

Security: Security tools, AWS Config rules

Shared services: Directory, limit monitoring

Network: AWS Direct Connect

Dev Sandbox: Experiments, Learning

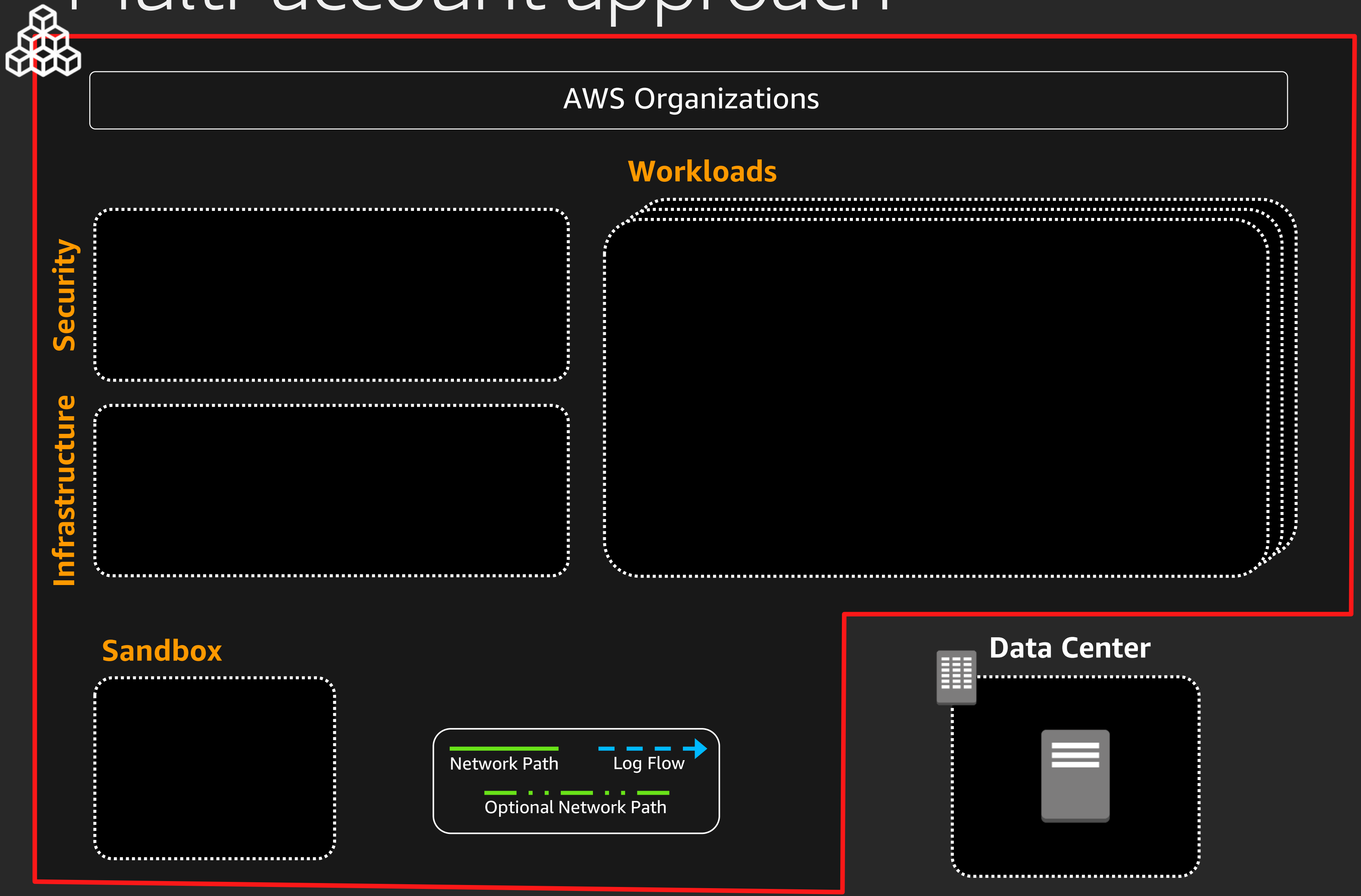
Dev: Development

Pre-Prod: Staging

Prod: Production

Team SS: Team Shared Services, Data Lake

Multi-account approach



Orgs: Account management

Log Archive: Security logs

Security: Security tools, AWS Config rules

Shared services: Directory, limit monitoring

Network: AWS Direct Connect

Dev Sandbox: Experiments, Learning

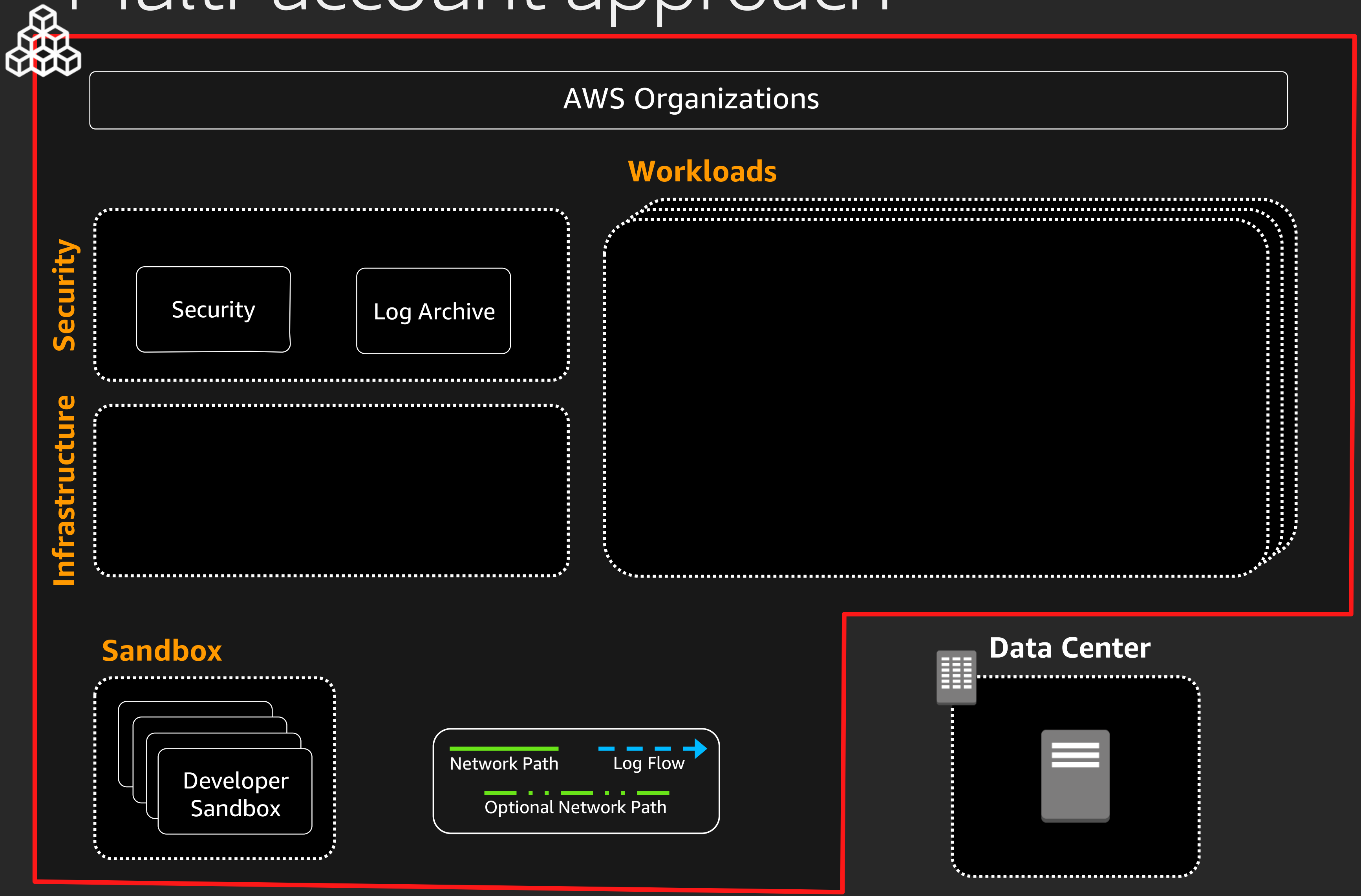
Dev: Development

Pre-Prod: Staging

Prod: Production

Team SS: Team Shared Services, Data Lake

Multi-account approach



Orgs: Account management

Log Archive: Security logs

Security: Security tools, AWS Config rules

Shared services: Directory, limit monitoring

Network: AWS Direct Connect

Dev Sandbox: Experiments, Learning

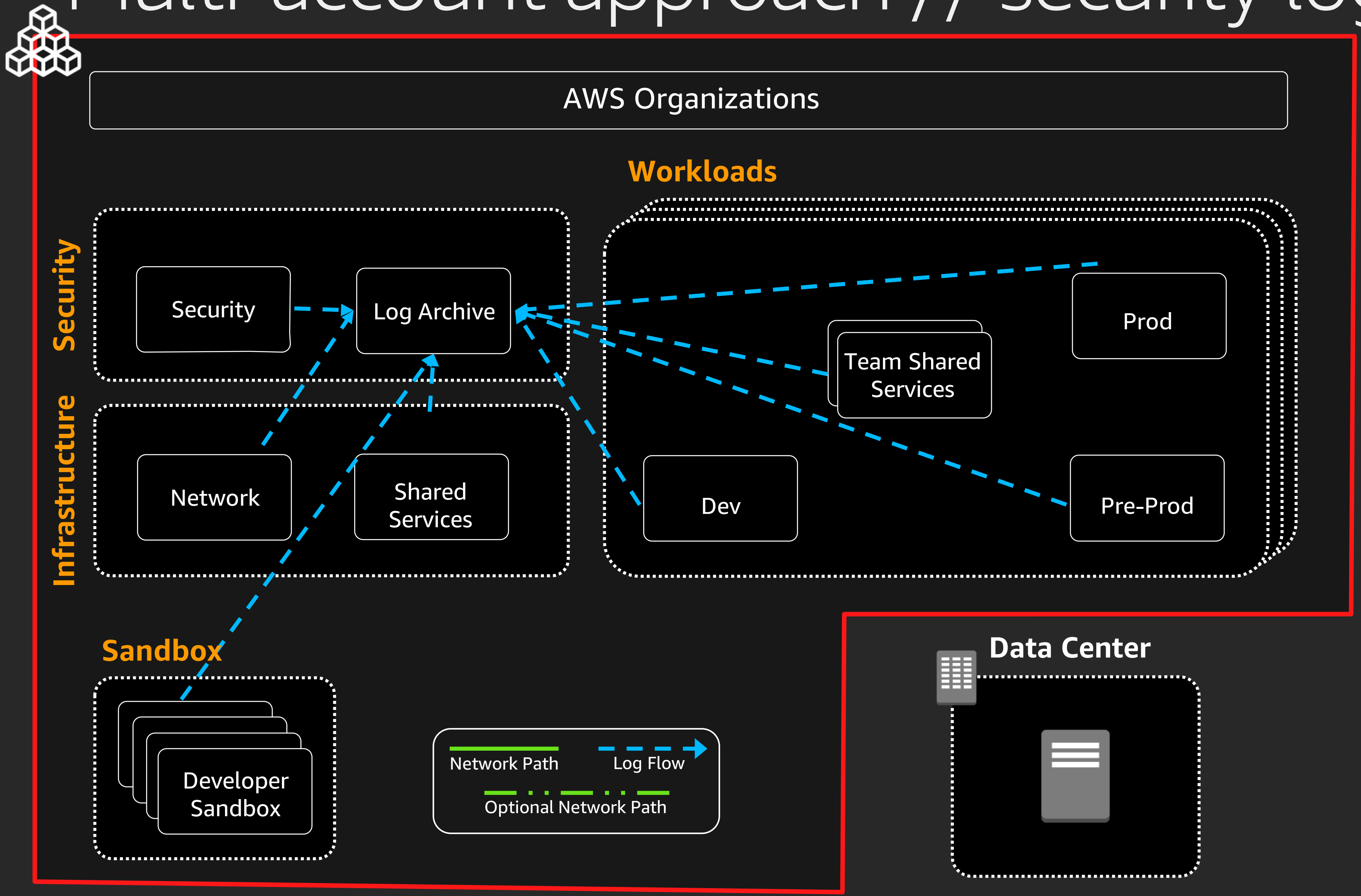
Dev: Development

Pre-Prod: Staging

Prod: Production

Team SS: Team Shared Services, Data Lake

Multi-account approach // security log flow



Orgs: Account management

Log Archive: Security logs

Security: Security tools, AWS Config rules

Shared services: Directory, limit monitoring

Network: AWS Direct Connect

Dev Sandbox: Experiments, Learning

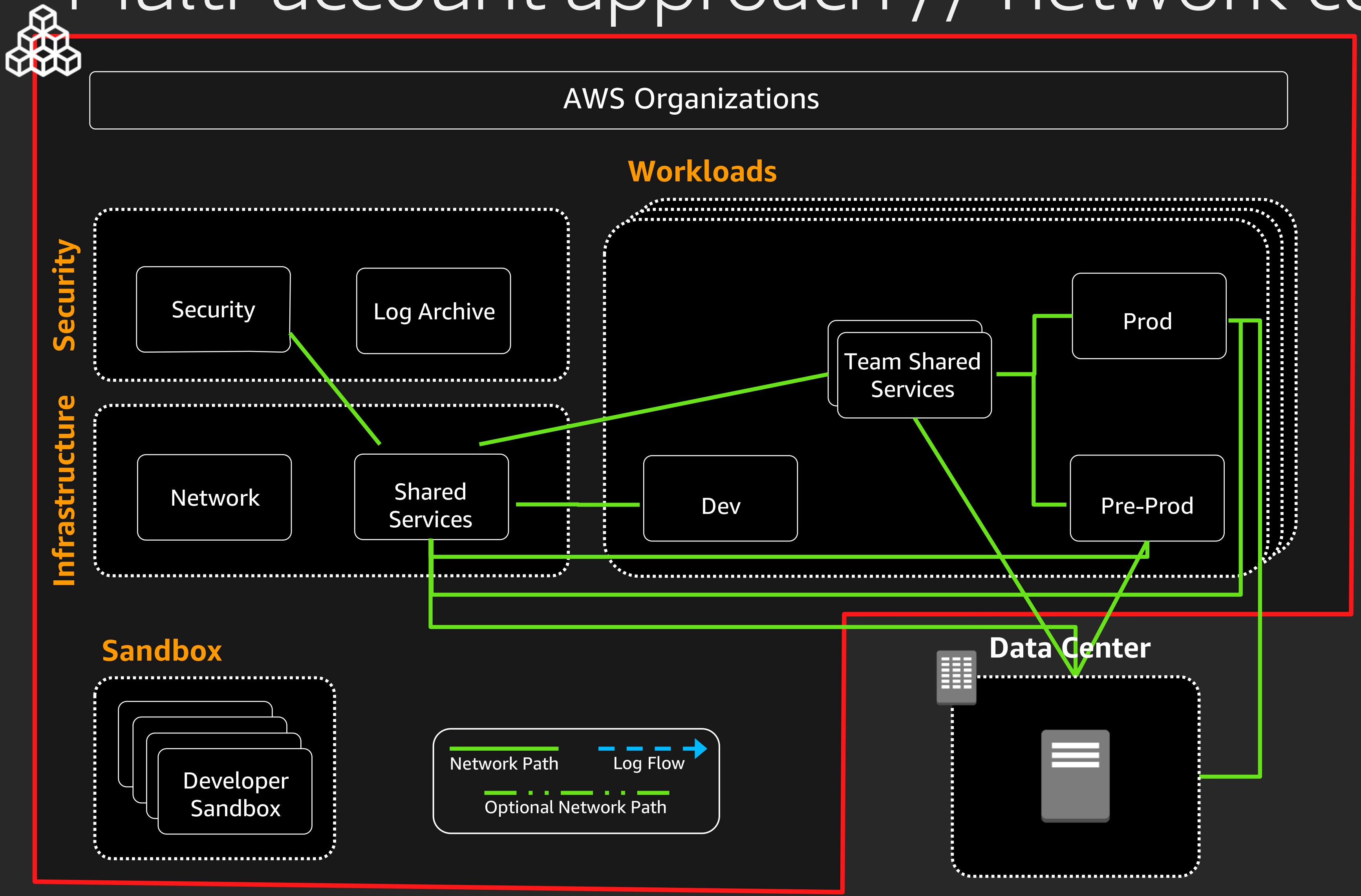
Dev: Development

Pre-Prod: Staging

Prod: Production

Team SS: Team Shared Services, Data Lake

Multi-account approach // network connectivity



Orgs: Account management

Log Archive: Security logs

Security: Security tools, AWS Config rules

Shared services: Directory, limit monitoring

Network: AWS Direct Connect

Dev Sandbox: Experiments, Learning

Dev: Development

Pre-Prod: Staging

Prod: Production

Team SS: Team Shared Services, Data Lake

Implementation

AWS solutions that enable agility + governance

Set up multi-account AWS environments

AWS Control Tower
AWS Organizations
AWS Service Catalog

Establish cost controls

AWS Budgets
AWS License Manager
AWS Marketplace (Private Marketplace)

Monitor/Manage policies and security configurations

AWS CloudTrail
AWS Config
AWS Security Hub
Amazon CloudWatch

Improve over time – operate and optimize

AWS Well-Architected Tool

AWS Organizations

Central governance and management across AWS accounts for **a comprehensive multi-account AWS environment**

- Manage and define your organization and accounts
- Control access and permissions
- Audit, monitor, and secure your environment for compliance
- Share resources across accounts
- Centrally manage costs and billing

Powers AWS Control Tower and AWS Landing Zone

AWS Control Tower

Self-service solution to automate the setup of **new AWS multi-account environments**

An AWS service offering account creation based on AWS best practices

Deployment of AWS best practice Blueprints and Guardrails

Baseline fundamental accounts to provide standardization of best practices

Single pane of glass for monitoring compliance to guardrails

AWS Control Tower capabilities

Account Management

- Framework for creating and baselining a multi-account environment using AWS Organizations
- Initial multi-account structure including security, audit, & shared service requirements
- An account vending machine that enables automated deployment of additional accounts with a set of managed and monitored security baselines
- A management console that shows compliance status of accounts
- The ability to apply AWS best practice guardrails and Blueprints to accounts at account creation
- The ability to detect and report on any drift / changes that have occurred that deviate from initial configuration options

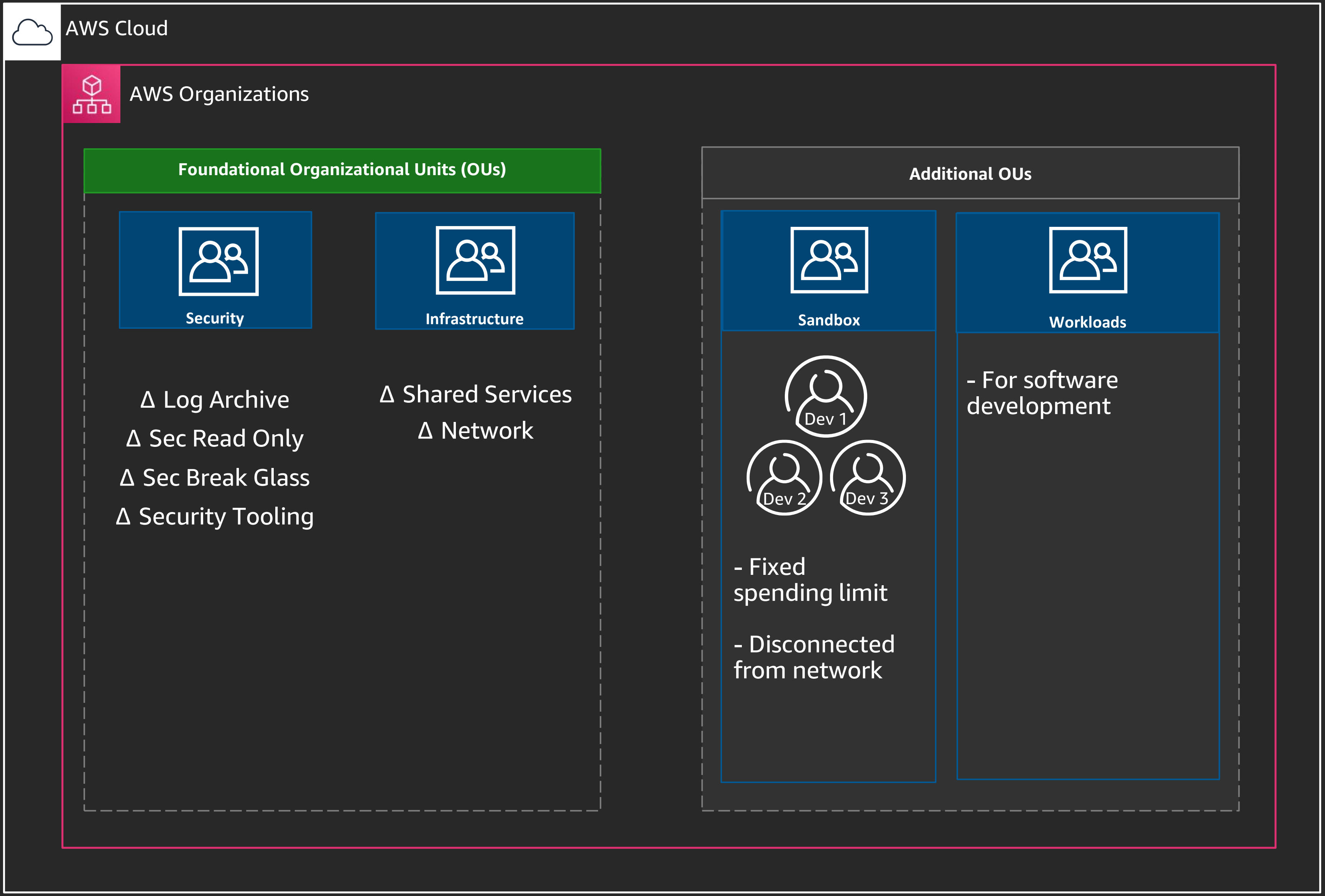
Identity & Access Management

- User account access managed through AWS SSO federation
- NEW! Integration options with other 3rd party SSO providers
- Cross-account roles enable centralized management

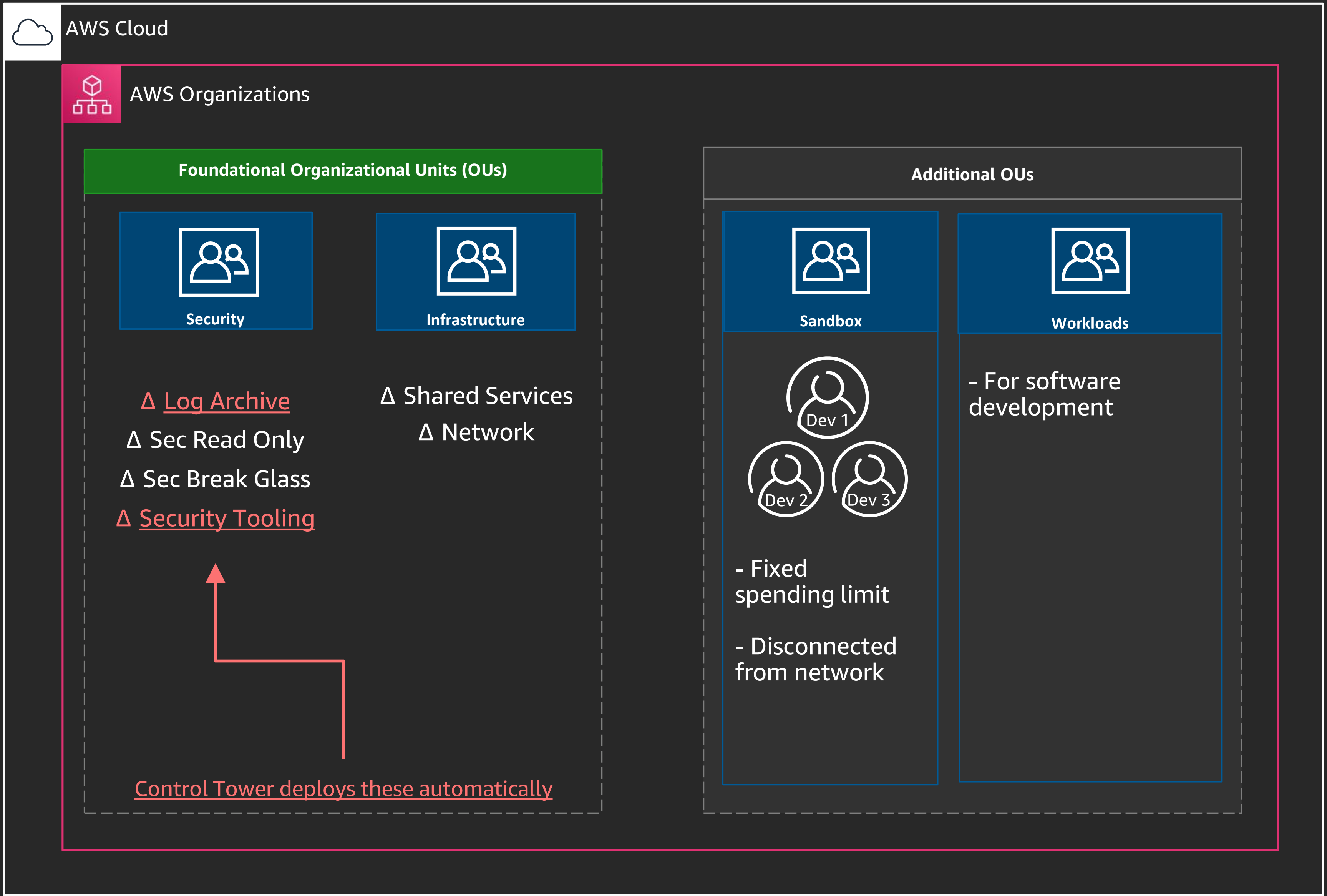
Security & Governance

- Multiple accounts enable separation of duties
- Initial account security and AWS Config rules baseline
- Network baseline

Starter AWS multi-account framework



Starter AWS multi-account framework



AWS Cloud

AWS Organizations

Foundational Organizational Units (OUs)

Security

Δ Log Archive

Δ Sec Read Only

Δ Sec Break Glass

Δ Security Tooling

Infrastructure

Δ Shared Services

Δ Network

Control Tower deploys these automatically

Additional OUs

Sandbox

- Fixed spending limit

- Disconnected from network

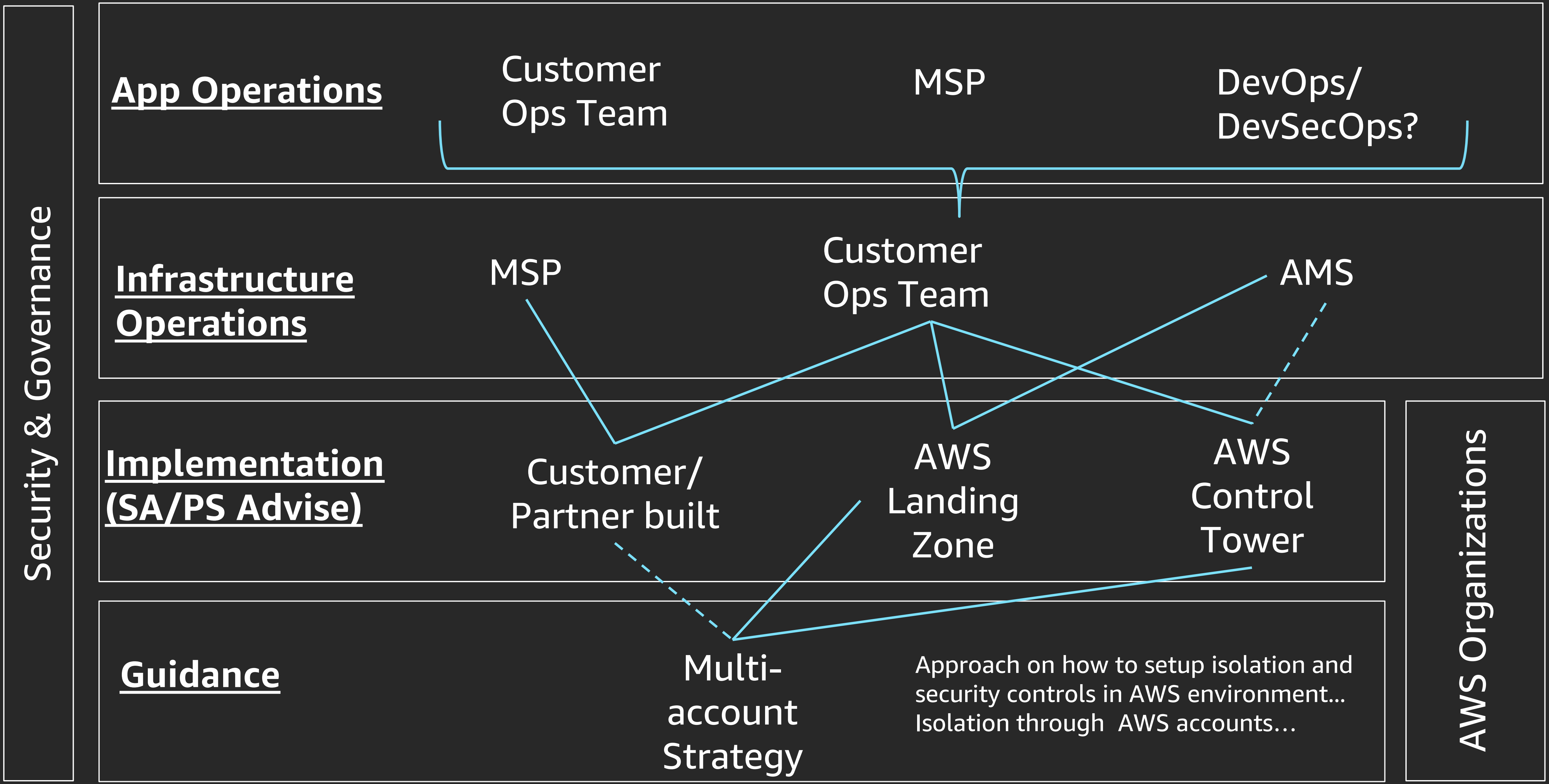
Workloads

- For software development

AWS Organizations
or
AWS Control Tower
or
AWS Landing Zone
or ...?

We thought we did this…

But…



Security & Governance

App Operations

Customer Ops Team

MSP

DevOps/ DevSecOps?

Infrastructure Operations

MSP

Customer Ops Team

AMS

Implementation (SA/PS Advise)

Customer/ Partner built

AWS Landing Zone

AWS Control Tower

Guidance

Multi-account Strategy

Approach on how to setup isolation and security controls in AWS environment…
Isolation through AWS accounts…

AWS Organizations

Recommendations

New customer:

- Evaluate AWS Control Tower (CT)
- Use out-of-box guardrails and blueprints
- Use CT Account Factory

Existing customer:

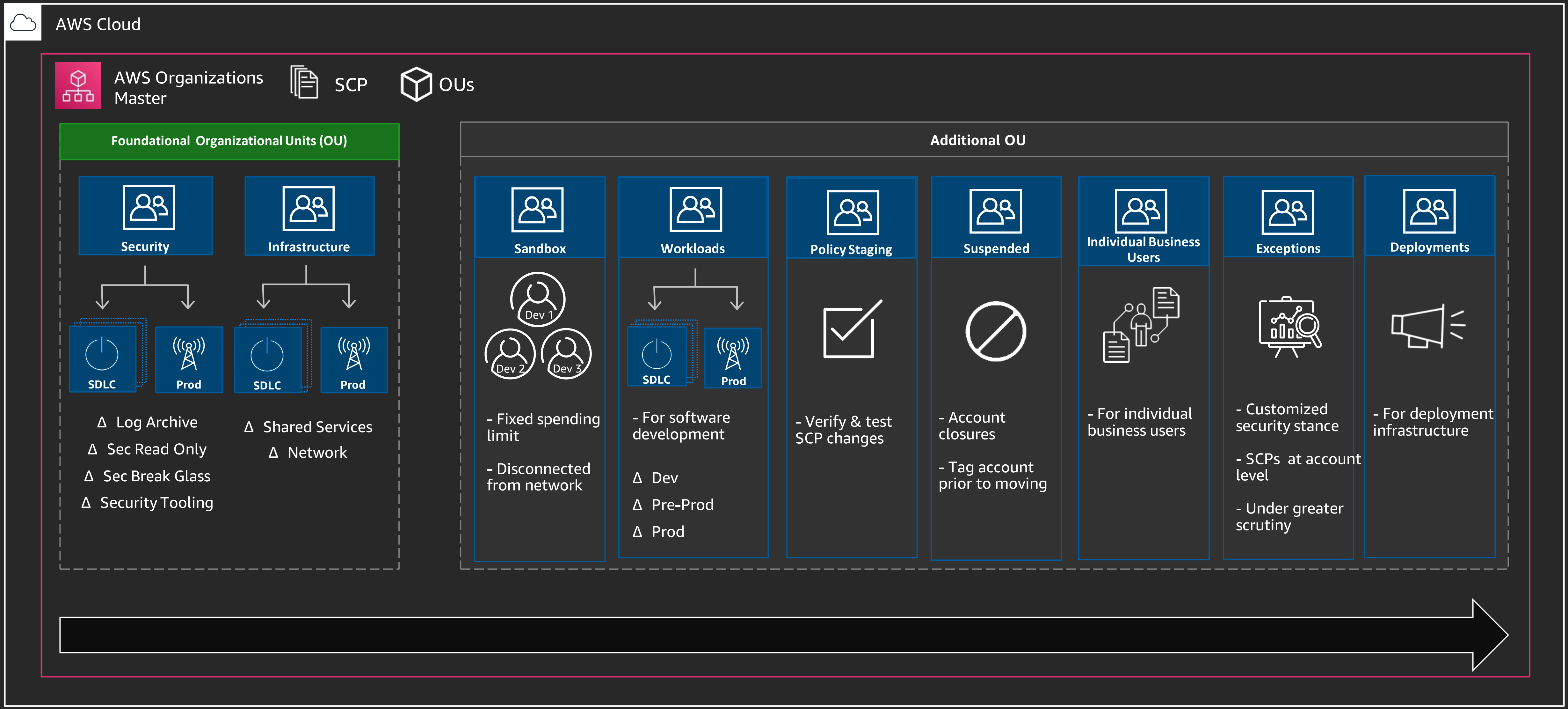
- Native CT AWS CloudWatch events and reference implementation
- Beta to use CT in existing AWS Organizations

Current AWS Landing Zone (ALZ) customers:

- New version to upgrade
- Replaces ALZ code with CT functionality
- Extensibility framework with CT

Summary

Multi-account framework



AWS Cloud

AWS Organizations Master

SCP

OUs

Foundational Organizational Units (OU)

Security

Δ Log Archive
Δ Sec Read Only
Δ Sec Break Glass
Δ Security Tooling

Infrastructure

Δ Shared Services
Δ Network

Additional OU

Sandbox

- Fixed spending limit

- Disconnected from network

Workloads

- For software development

Δ Dev
Δ Pre-Prod
Δ Prod

Policy Staging

- Verify & test SCP changes

Suspended

- Account closures

- Tag account prior to moving

Individual Business Users

- For individual business users

Exceptions

- Customized security stance

- SCPs at account level

- Under greater scrutiny

Deployments

- For deployment infrastructure

How many landing zones?

Primary production: Yes

Dev/QA/test deployment: Yes

- Test out new CT/Orgs features
- Test out orchestration framework/services

Always running pre-prod deployment: Maybe

Forensics: Maybe

Landing zone sessions

search: “landing zone”

Architecture

SEC325 – Architecting security & governance across your landing zone (Session)
ARC344 – Understanding the landing zone journey (Chalk Talk)
GPSTEC203 – Control Tower versus AWS Landing Zone (Chalk Talk)

Implementation

MGT313 – Architect governance at enterprise scale with Goldman Sachs
MGT307 – Governance at scale: AWS Control Tower, AWS Organizations, and more (Chalk Talk)
MGT302 – Enable AWS adoption at scale with automation and governance (Session)
SEC335 – How to deploy secure workloads with AWS Control Tower (Chalk Talk)
GPSTEC324 – Automating ISV product deployment in AWS Landing Zone (Chalk Talk)
GPSTEC325 – Control Tower in a nutshell and practice enablement for APN Partners

Operations

ENT214 – Cloud migration in the face of data-center eviction (Session)
ENT215 – Five steps AMS leverages to accelerate cloud adoption (Session)

Discussion /Feedback

SEC324 – Deep dive into AWS multi-account strategies (Chalk Talk)

Hands on

ARC315 – Build end-to-end governance with AWS Control Tower (Workshop)
SEC347 – DNS across a multi-account environment (Builder session)

Ideas and guidance // Multi-account Strategy

- Service control policies strategies and recommendations
- Identify Federation best practices and details
- Steps to migrate into a multi-account environment
- Networking recommendations (Transit gateway, Shared Amazon VPC, Private Link, peering, etc …)
- Security specific tooling and where to run/how e.g. Firewalls, IDS/IPS
- Alerting and alarming recommendations
- Forensics landing zone
- QA/Staging landing zone
- Backup/disaster recovery recommendations at account level
- Cost implications of many accounts vs. few
- CI/CD in a multi-account environment

Thank you!

AWS re:Invent

aws

Please complete the session survey in the mobile app.

AWS re:Invent

aws

Ideas and guidance // Multi-account Strategy

- Service control policies strategies and recommendations
- Identify Federation best practices and details
- Steps to migrate into a multi-account environment
- Networking recommendations (Transit gateway, Shared Amazon VPC, Private Link, peering, etc …)
- Security specific tooling and where to run/how e.g. Firewalls, IDS/IPS
- Alerting and alarming recommendations
- Forensics landing zone
- QA/Staging landing zone
- Backup/disaster recovery recommendations at account level
- Cost implications of many accounts vs. few
- CI/CD in a multi-account environment