Track 5 | Session 2

多重帳戶安全策略與方針

Young Yang

Machine Learning Specialist SA

Amazon Web Services

aws SUMMIT ONLINE

Agenda

- Multi-Account Strategy and Guidance
- Architecting Multi-Account
- Control Tower Overview

Why one account isn’t enough

Many teams

Isolation

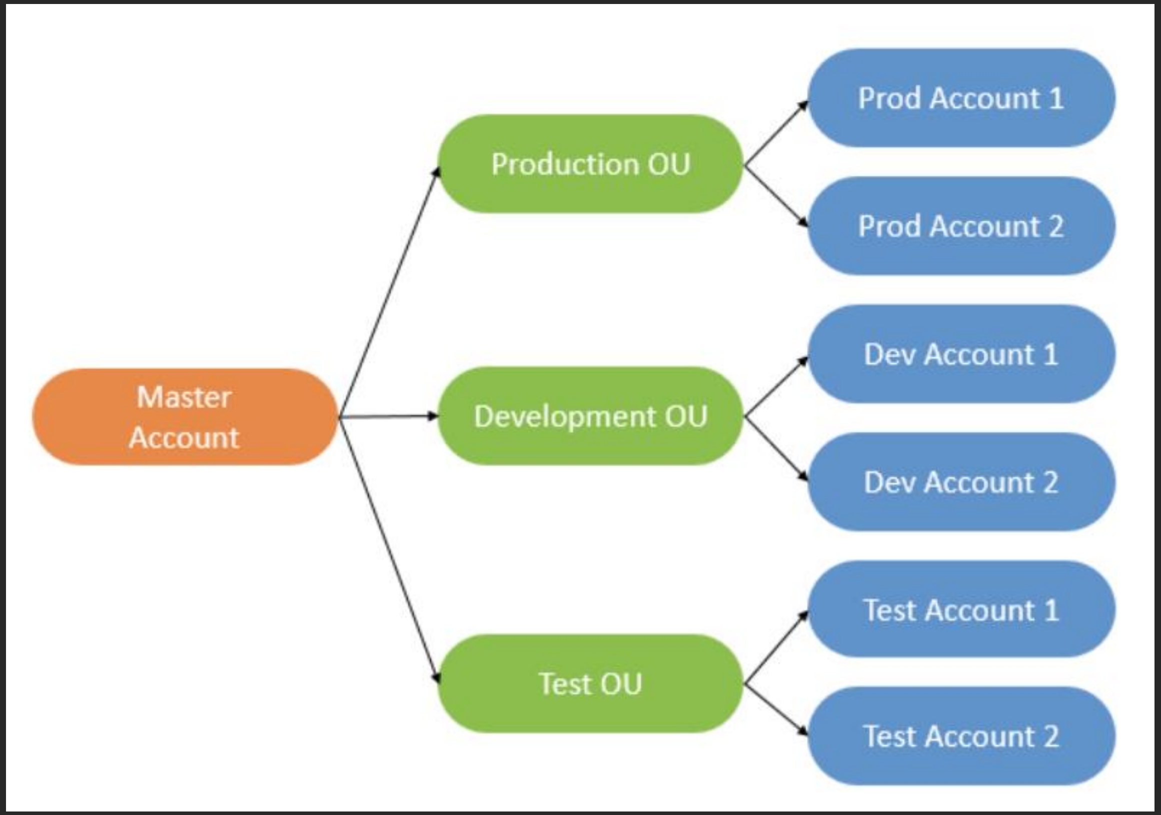
Billing

Security/compliance controls

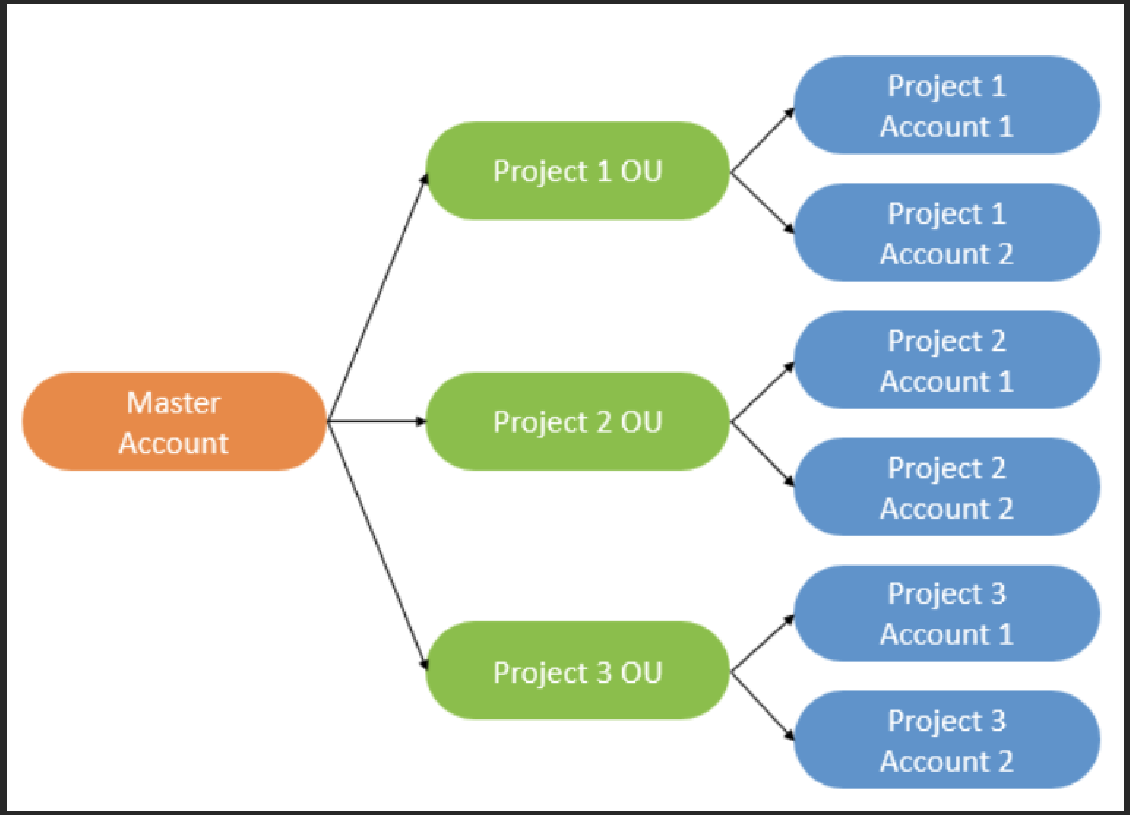
Business process

Architecting AWS accounts

Isolation



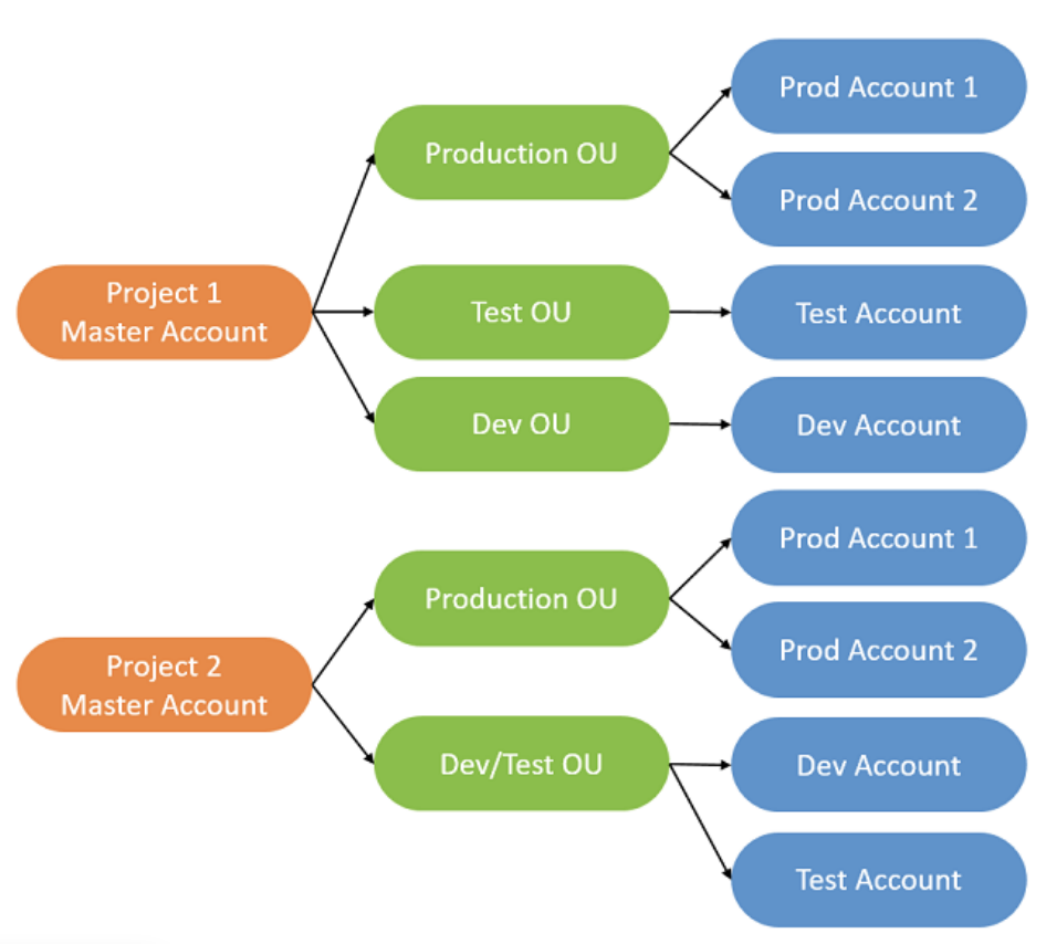
Environment Lifecycle
Account Structure



Project-Based
Account Structure

Architecting AWS accounts

Hybrid architecture: Project + Environment



Segmentation reasons

There are multiple reasons for segmenting by accounts or Amazon VPCs; these generally include:

Environmental

Separation among development, test, and production for security, governance, or regulatory reasons, e.g., PCI workloads

Segmentation reasons

There are multiple reasons for segmenting by accounts or Amazon VPCs; these generally include:

Environmental

Separation among development, test, and production for security, governance, or regulatory reasons, e.g., PCI workloads

Financial

Provide cost visibility, accountability, or control on a per account basis; this may also be related to a line of business

Segmentation reasons

There are multiple reasons for segmenting by accounts or Amazon VPCs; these generally include:

Environmental	Financial	Business
Separation among development, test, and production for security, governance, or regulatory reasons, e.g., PCI workloads	Provide cost visibility, accountability, or control on a per account basis; this may also be related to a line of business	Delegated control to particular business unit to be able to leverage AWS environment within pre-defined governance framework

Segmentation reasons

There are multiple reasons for segmenting by accounts or Amazon VPCs; these generally include:

Environmental

Separation among development, test, and production for security, governance, or regulatory reasons, e.g., PCI workloads

Financial

Provide cost visibility, accountability, or control on a per account basis; this may also be related to a line of business

Business

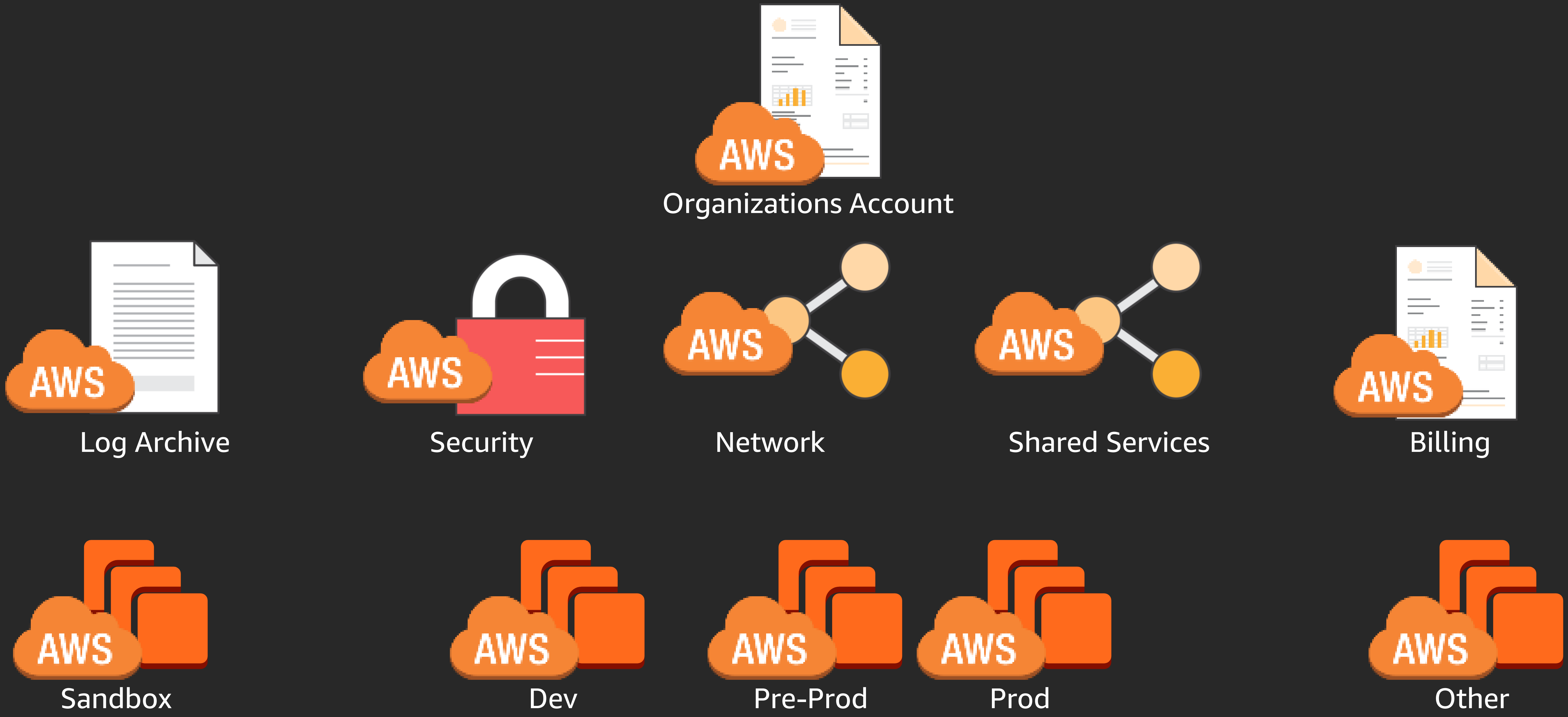
Delegated control to particular business unit to be able to leverage AWS environment within pre-defined governance framework

Workload

Segregation of public or private-facing services, differing risk profiles, data classification, consumer of service, etc.

Architecting Multi-Account

What Accounts Should I Create?



Organizations Account

Log Archive

Security

Network

Shared Services

Billing

Sandbox

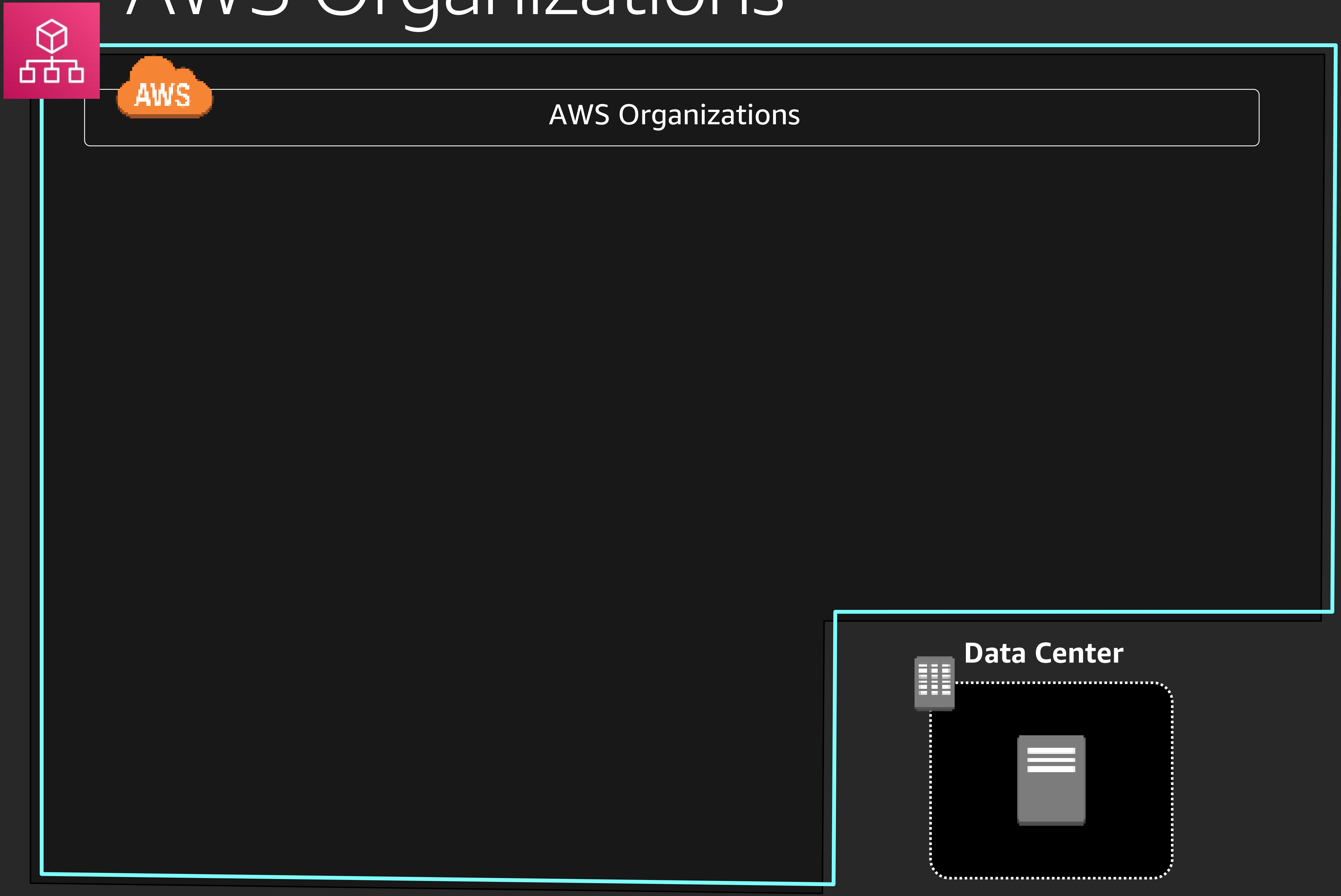
Dev

Pre-Prod

Prod

Other

AWS Organizations



No connection to DC

Service control policies

Consolidated billing

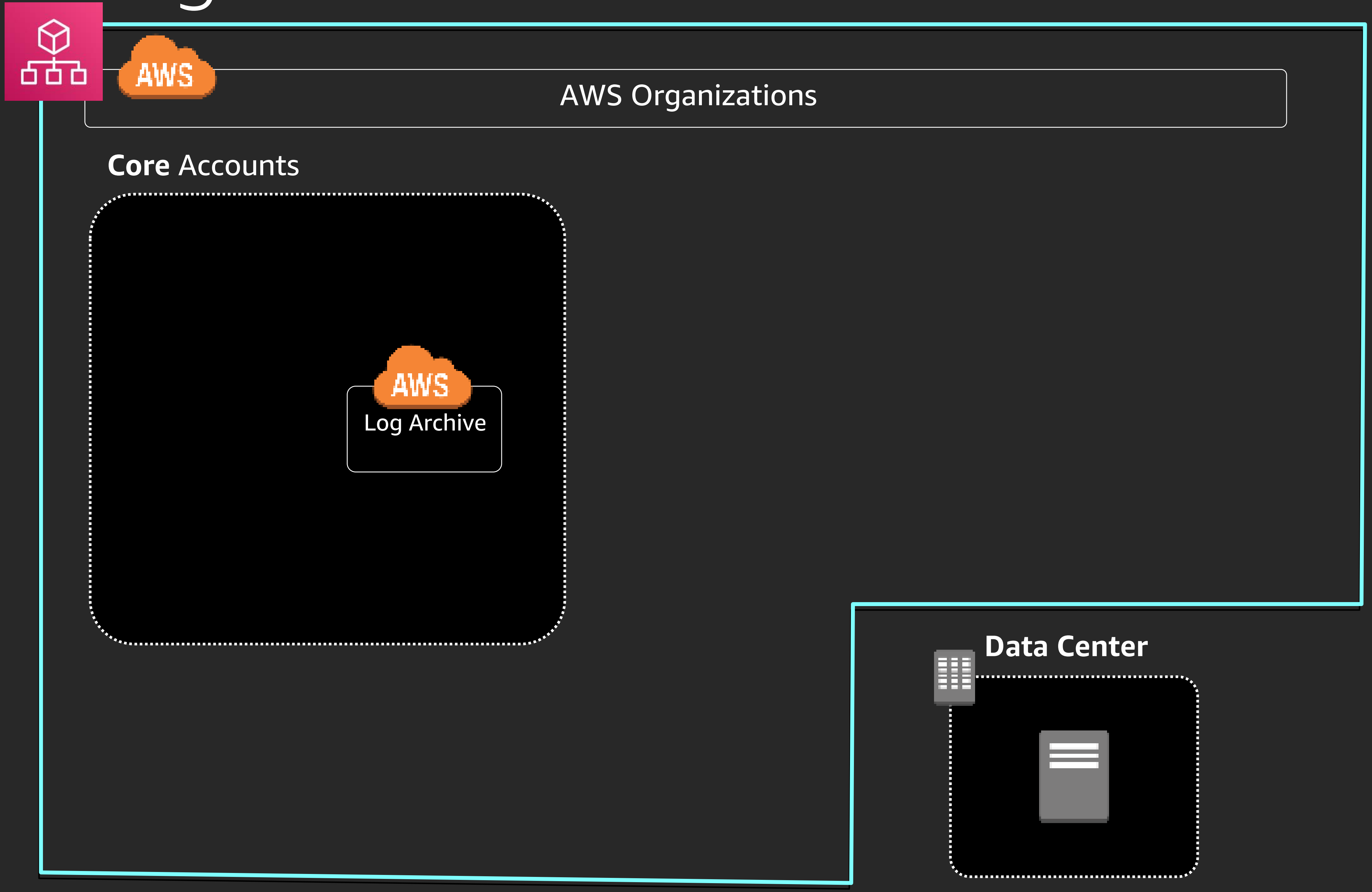
Volume discount

Minimal resources

Limited access

Restrict Orgs role!

Log Archive Account



Versioned Amazon S3 bucket

- Restricted
- MFA delete

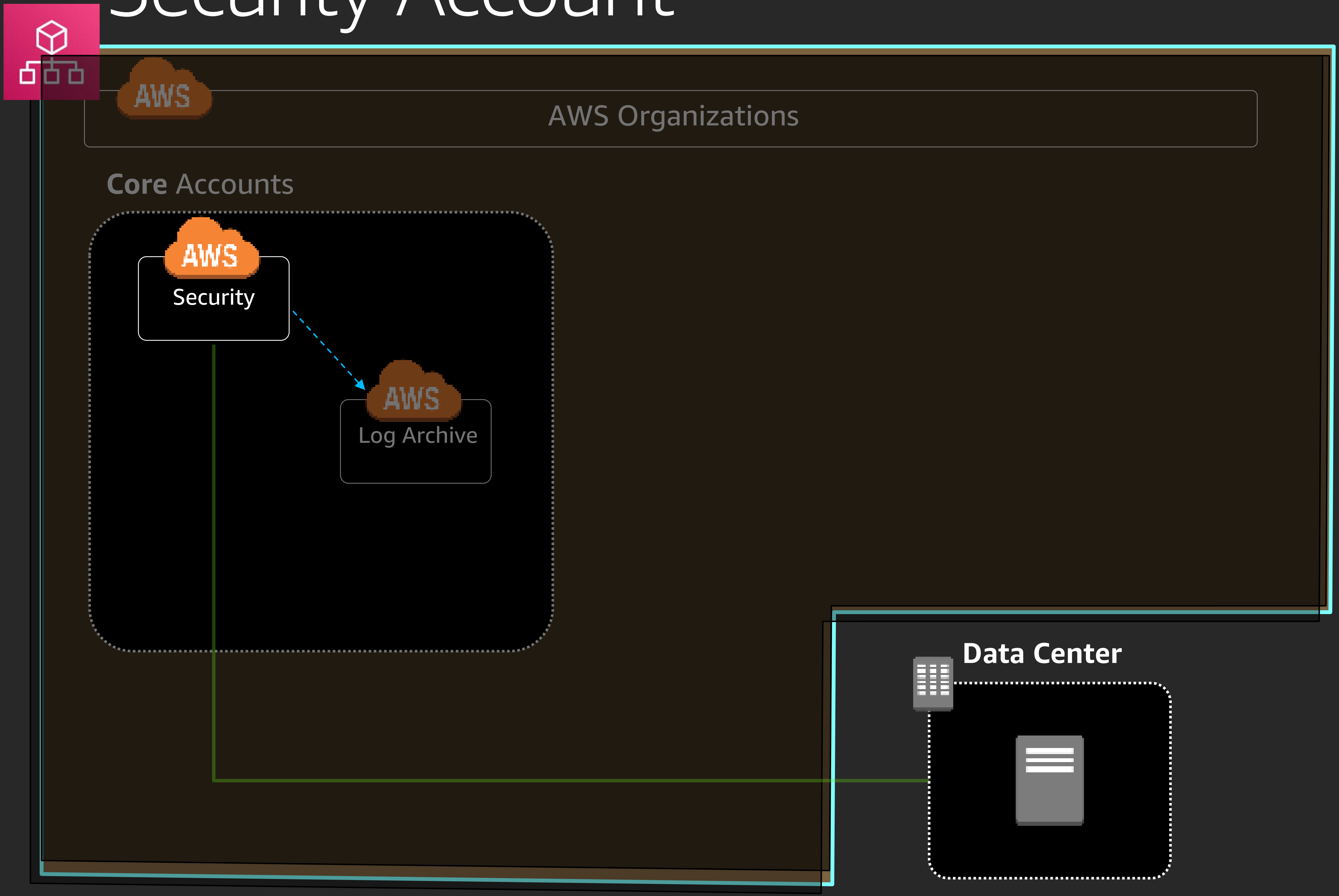
CloudTrail logs

Security logs

Single source of truth

Limited access

Security Account



Optional data center connectivity

Security tools and audit

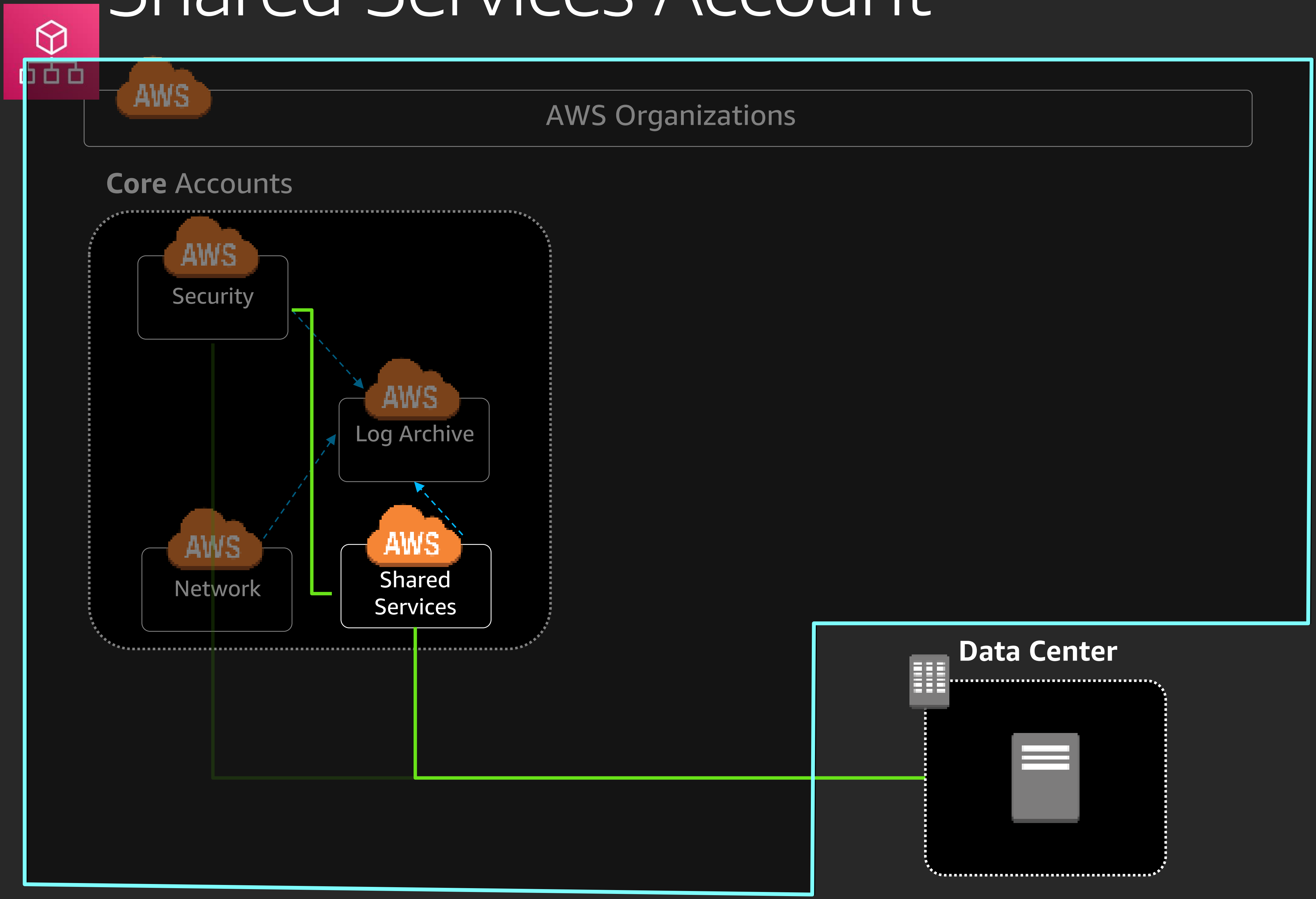
Cross-account read/write

Limited access

AWS CloudTrail

AWS Config

Shared Services Account



Connected to DC

DNS

LDAP/Active Directory

Shared Services VPC

Deployment tools

- Golden AMI
- Pipeline

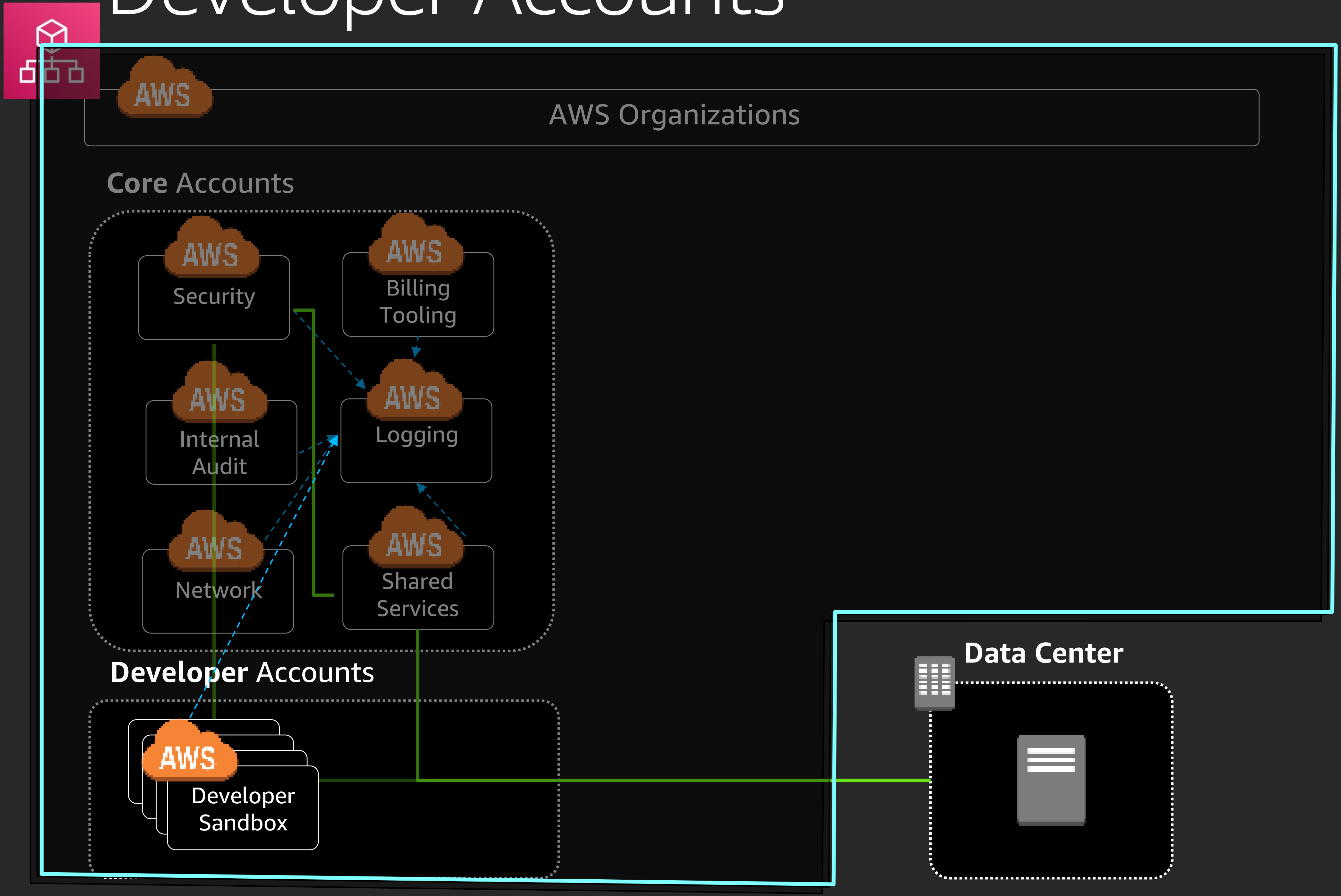
Scanning infrastructure

- Inactive instances
- Improper tags
- Snapshot lifecycle

Monitoring

Limited access

Developer Accounts



No connection to DC

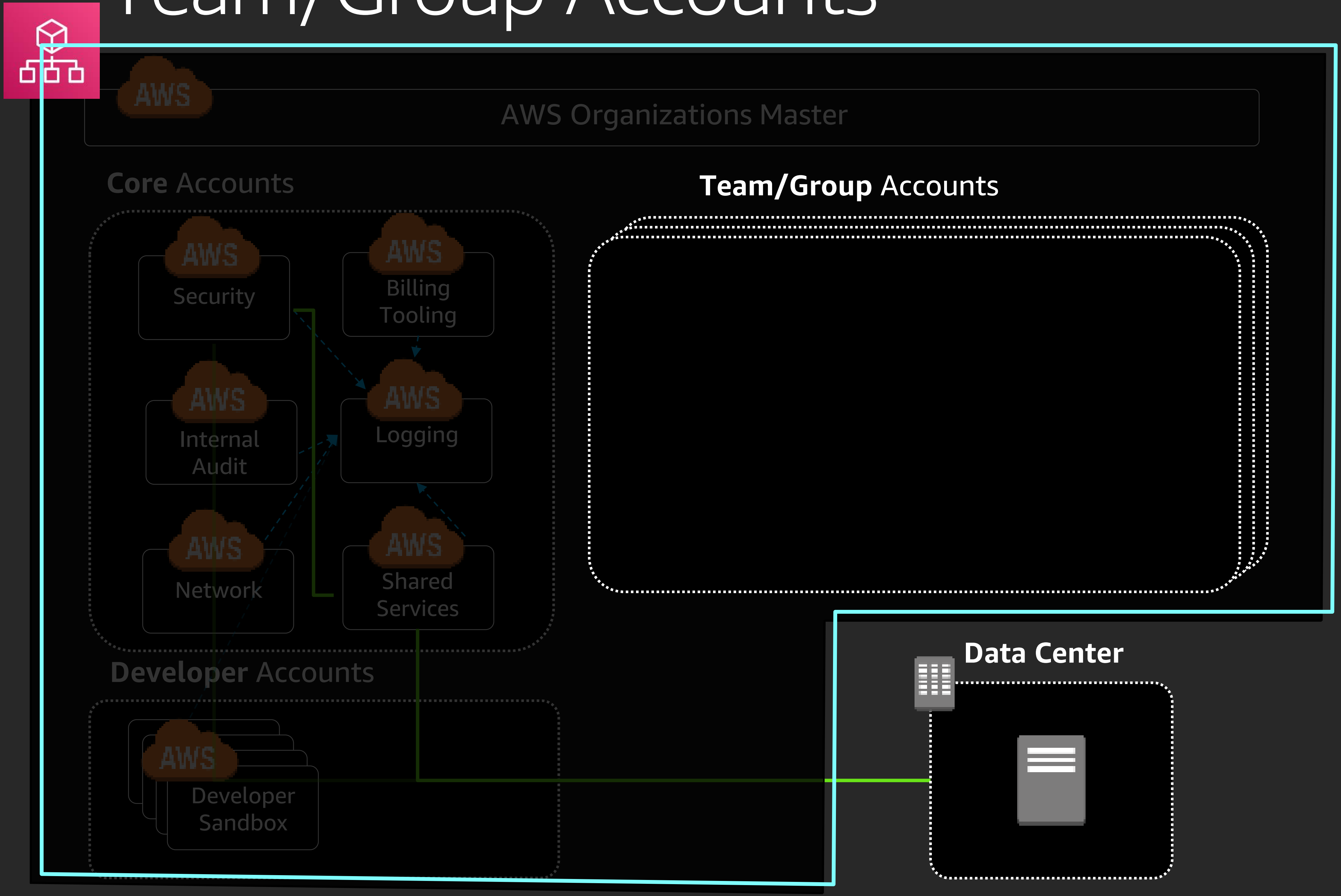
Innovation space

Fixed spending limit

Autonomous

Experimentation

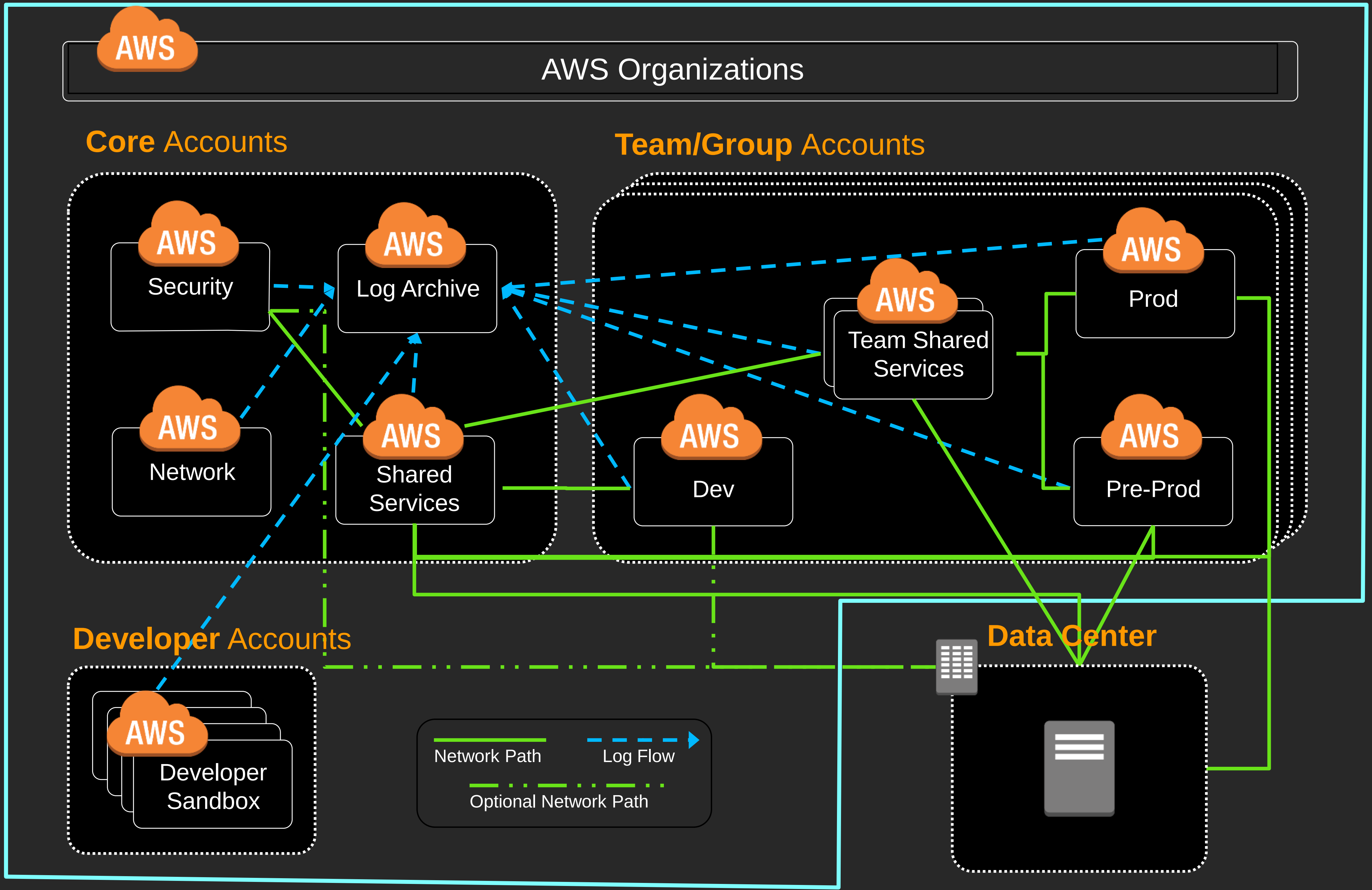
Team/Group Accounts



Based on level of needed isolation

Match your development lifecycle

Multi-Account Recommended 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

Control Tower Overview

Customers end up with Multi-account Challenges

Paradox of Choice

Too many design decisions

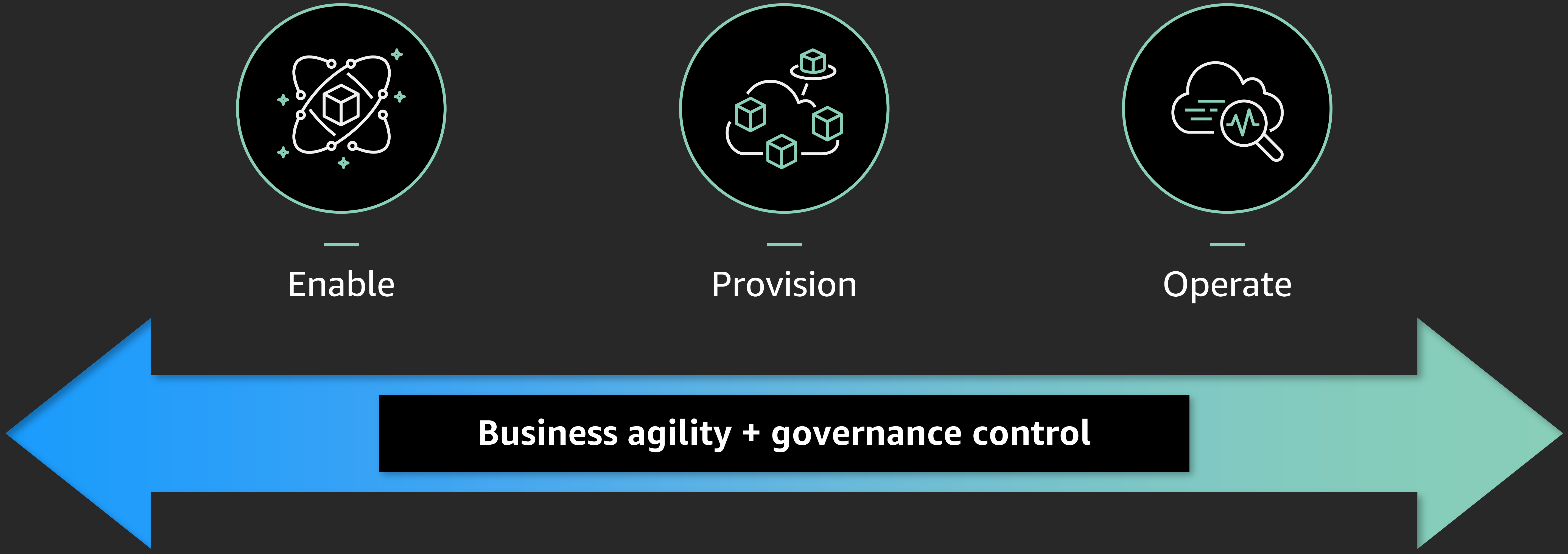
Setup Complexity

Granular AWS policies across multiple accounts & services

Ongoing management

Centrally managing compliance and security of multiple accounts

AWS Control Tower: Easiest way to set up and govern AWS at scale



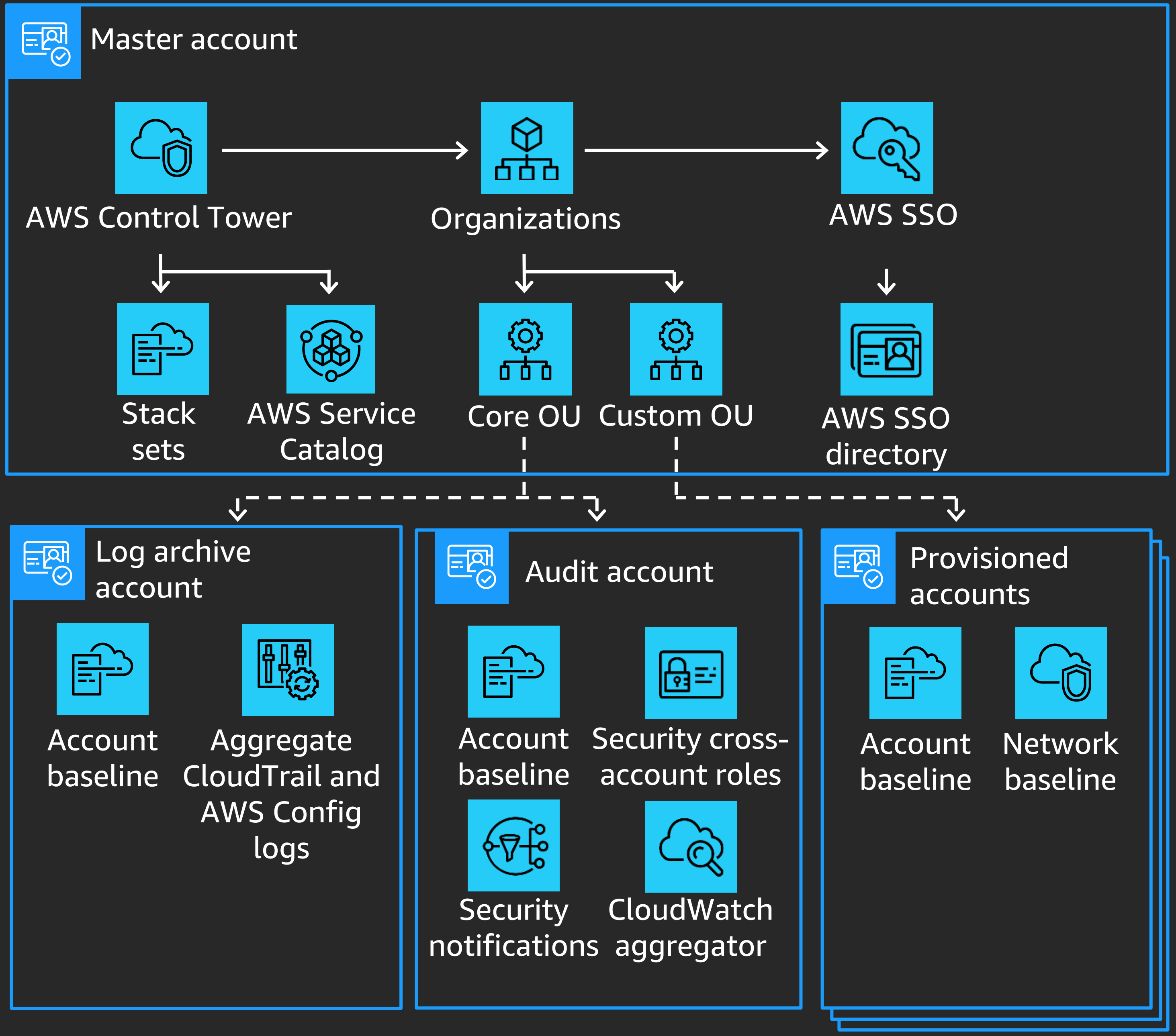
Enable

Provision

Operate

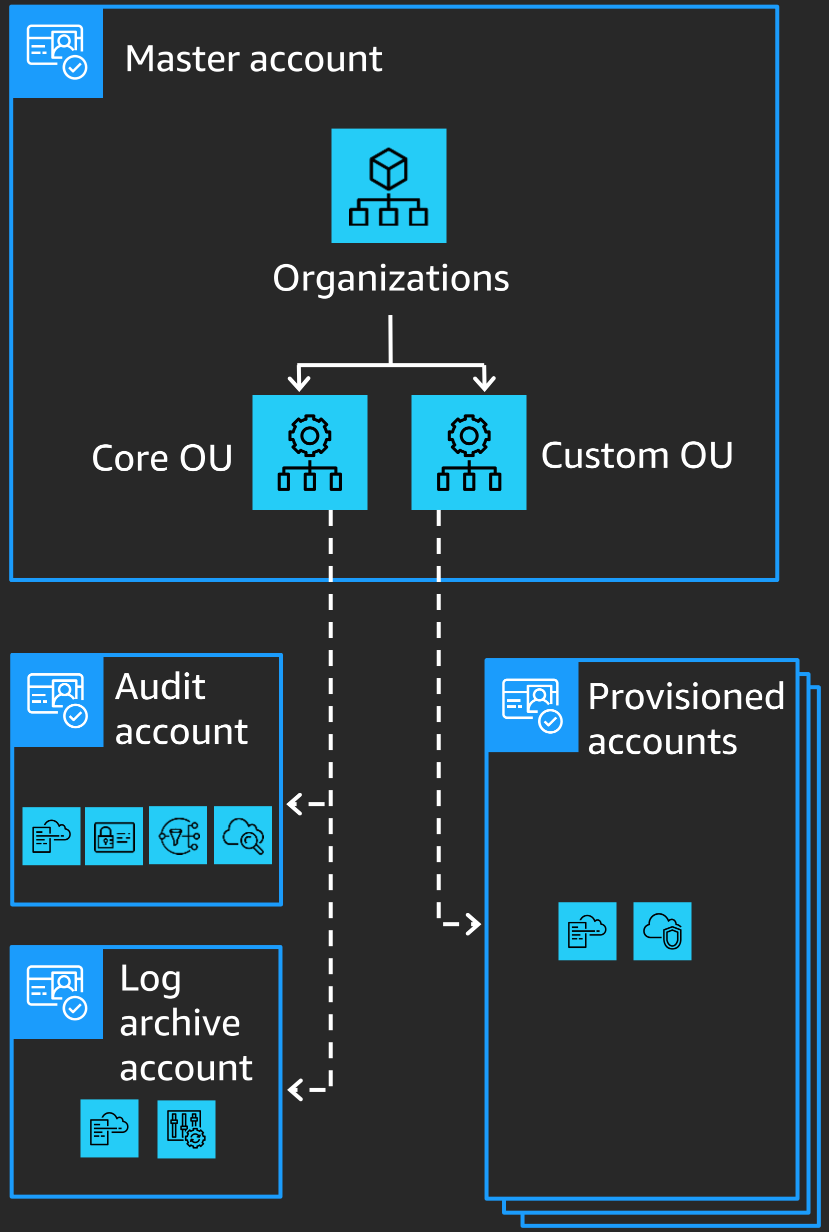
Business agility + governance control

Set up an AWS landing zone



- Landing zone—a preconfigured, secure, scalable, multi-account AWS environment based on best practice blueprints
- Multi-account management using Organizations
- Identity and federated access management using AWS SSO
- Centralized log archive using CloudTrail and AWS Config
- Cross-account audit access using AWS SSO and IAM
- End-user account provisioning through AWS Service Catalog
- Centralized monitoring and notifications using Amazon CloudWatch and Amazon SNS

Multi-account architecture

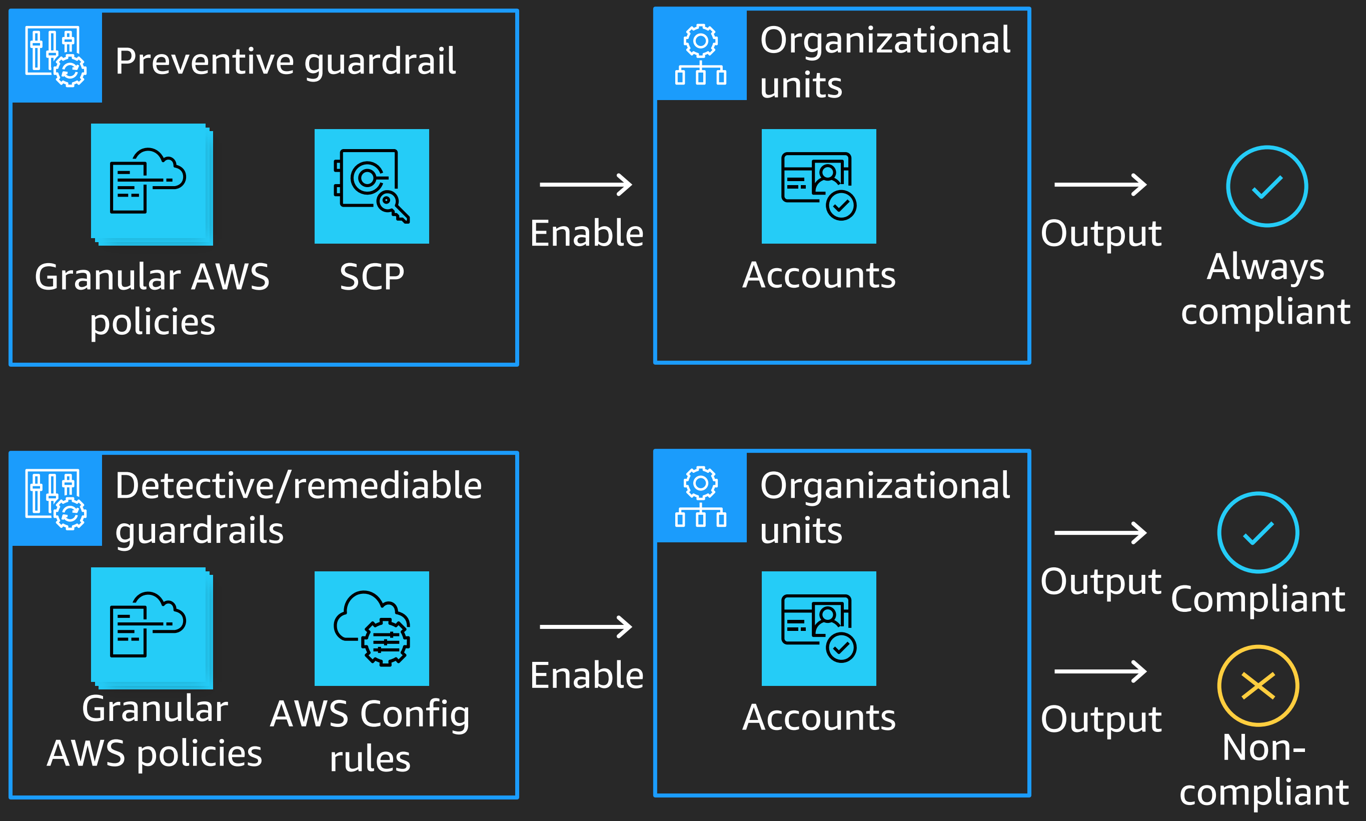


- Master account: Designation of your existing account to create a new organization. Also your master payer account.
- Organization consists of 2 OUs with pre-configured accounts—
  - Core OU: AWS Control Tower–created accounts, i.e., audit account and log archive account
  - Custom OU: Your provisioned accounts

Centralize identity and access

- AWS SSO provides default directory for identity
- AWS SSO also enables federated access management across all accounts in your organization
- Preconfigured groups (e.g., AWS Control Tower administrators, auditors, AWS Service Catalog end users)
- Preconfigured permission sets (e.g., admin, read-only, write)
- Option to integrate with your managed or on-premises Active Directory (AD)

Establish guardrails

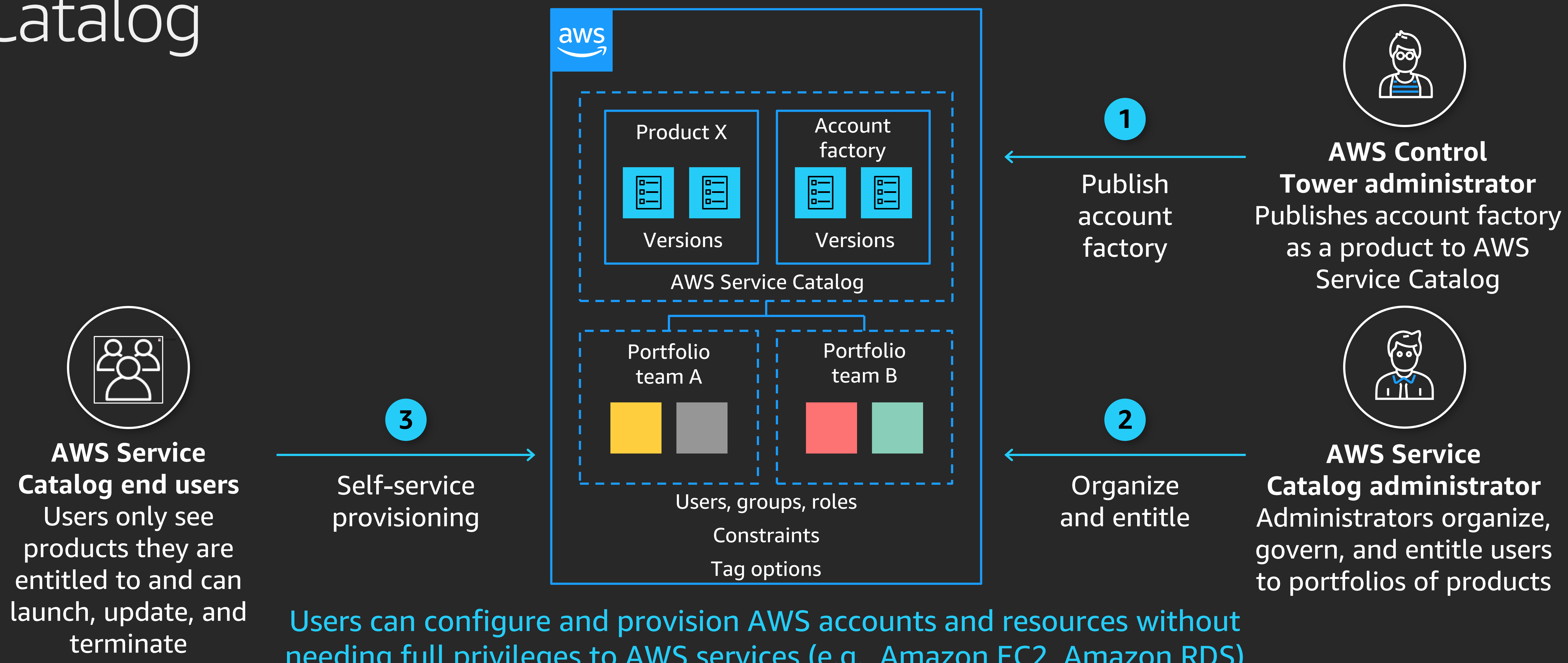


- Guardrails are preconfigured governance rules for security, compliance, and operations
- Expressed in plain English to provide abstraction over granular AWS policies
- Preventive guardrails: prevent policy violations through enforcement; implemented using AWS CloudFormation and SCPs
- Detective guardrails: detect policy violations and alert in the dashboard; implemented using AWS Config rules
- Mandatory and strongly recommended guardrails for prescriptive guidance
- Easy selection and enablement on organizational units

Guardrail examples

Goal/category	Example
IAM security	Require MFA for root user
Data security	Disallow public read access to Amazon S3 buckets
Network security	Disallow internet connection via Remote Desktop Protocol (RDP)
Audit logs	Enable AWS CloudTrail and AWS Config
Monitoring	Enable AWS CloudTrail integration with Amazon CloudWatch
Encryption	Ensure encryption of Amazon EBS volumes attached to Amazon EC2 instances
Drift	Disallow changes to AWS Config rules set up by AWS Control Tower

Self-service account provisioning in AWS Service Catalog



AWS Control Tower administrator
Publishes account factory as a product to AWS Service Catalog

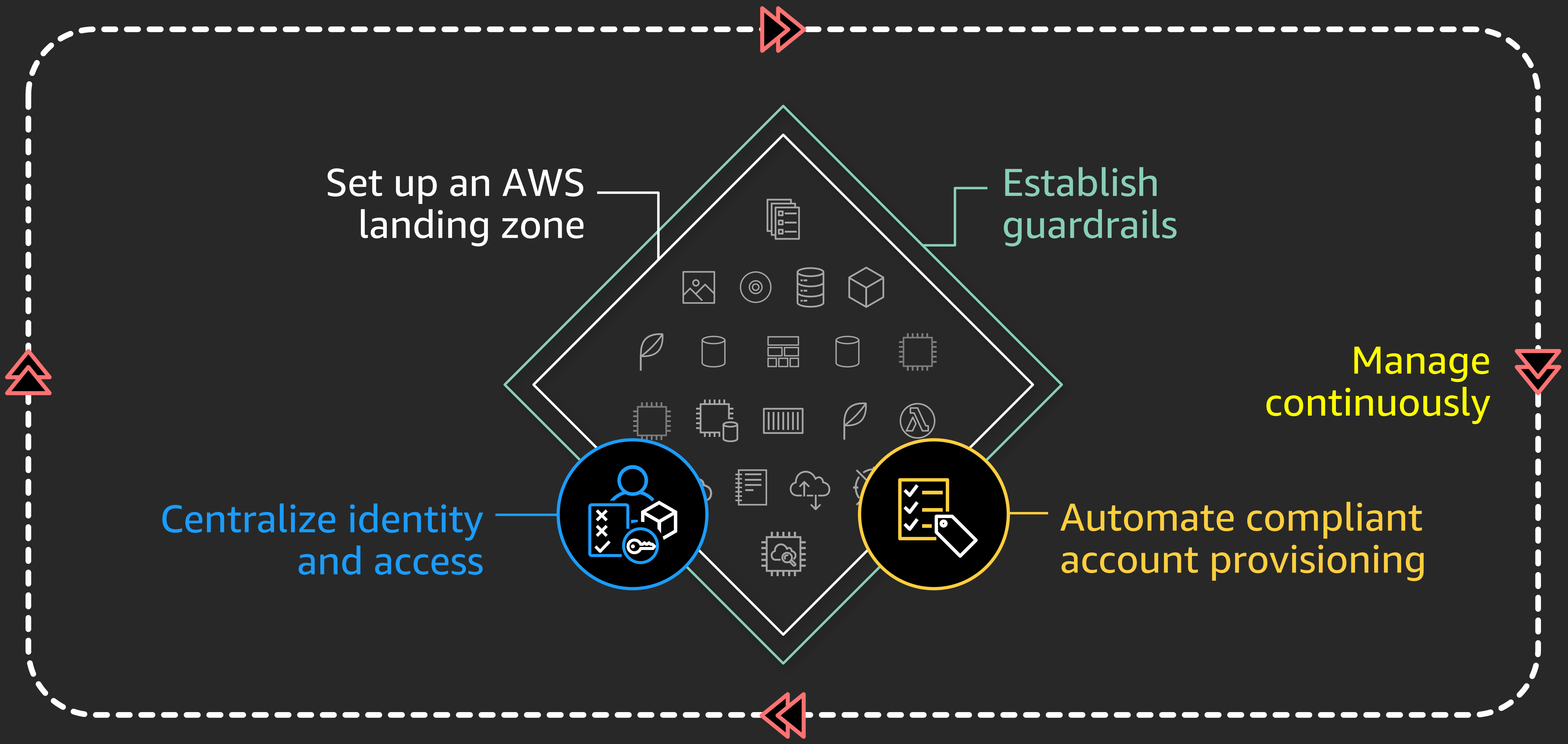
AWS Service Catalog administrator
Administrators organize, govern, and entitle users to portfolios of products

AWS Service Catalog end users
Users only see products they are entitled to and can launch, update, and terminate

Users can configure and provision AWS accounts and resources without needing full privileges to AWS services (e.g., Amazon EC2, Amazon RDS)

Enable governance

Enable



Set up an AWS landing zone

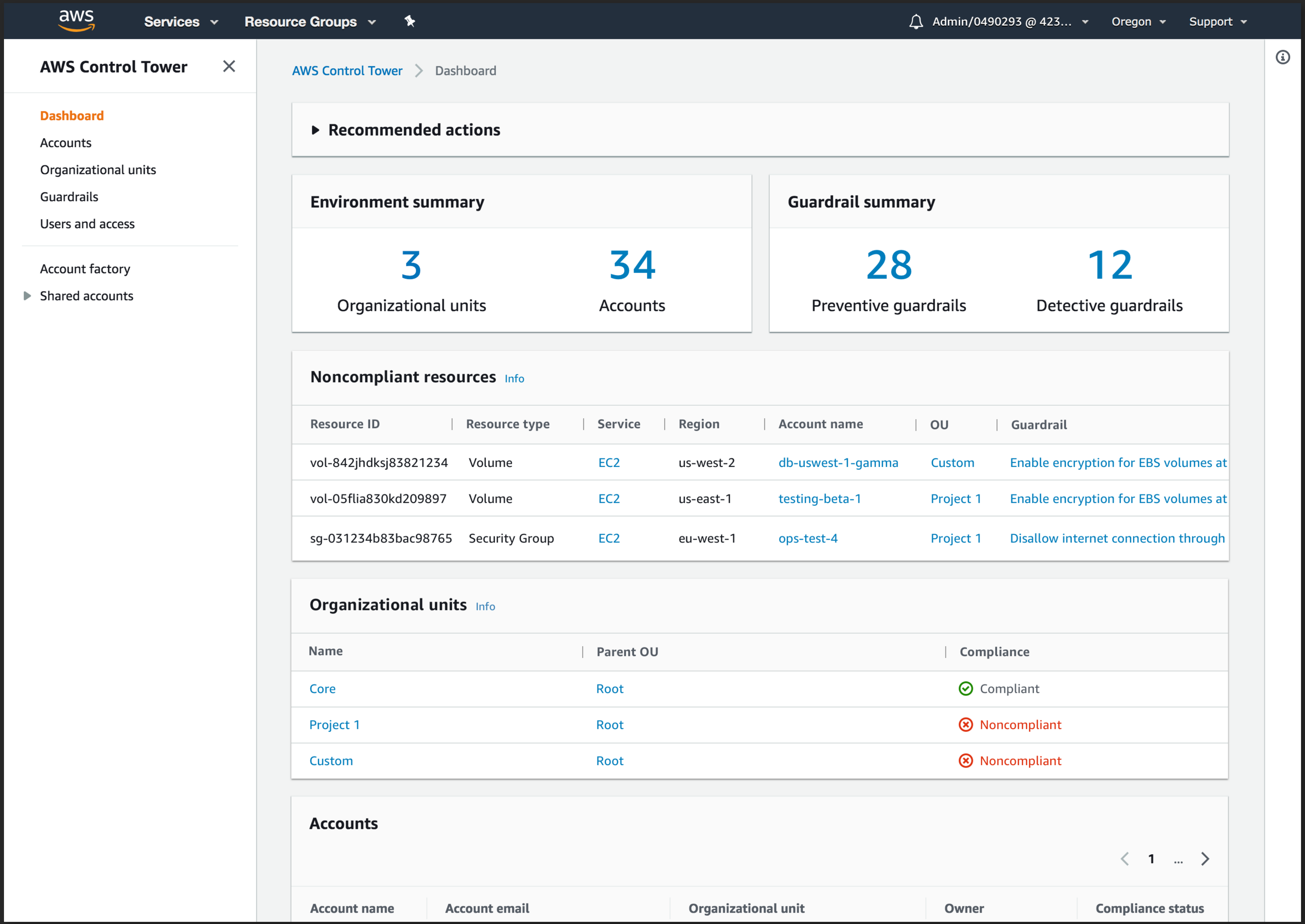
Establish guardrails

Manage continuously

Automate compliant account provisioning

Centralize identity and access

Dashboard for oversight



AWS Control Tower > Dashboard

▶ Recommended actions

Environment summary

3 Organizational units

34 Accounts

Guardrail summary

28 Preventive guardrails

12 Detective guardrails

Noncompliant resources Info

Resource ID	Resource type	Service	Region	Account name	OU	Guardrail
vol-842jhdksj83821234	Volume	EC2	us-west-2	db-uswest-1-gamma	Custom	Enable encryption for EBS volumes at
vol-05flia830kd209897	Volume	EC2	us-east-1	testing-beta-1	Project 1	Enable encryption for EBS volumes at
sg-031234b83bac98765	Security Group	EC2	eu-west-1	ops-test-4	Project 1	Disallow internet connection through

Organizational units Info

Name	Parent OU	Compliance
Core	Root	✓ Compliant
Project 1	Root	⊗ Noncompliant
Custom	Root	⊗ Noncompliant

Accounts

< 1 ... >

Account name	Account email	Organizational unit	Owner	Compliance status

Summary of key features

- Automated landing zone with best practice blueprints
- Guardrails for policy management
- Account factory for account provisioning
- Dashboard for visibility and actions
- Built-in identity and access management
- Preconfigured log archive and audit access to accounts
- Built-in monitoring and notifications
- Automatic updates

Learn security with AWS Training and Certification

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

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

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

Validate expertise with the AWS Certified Security – Specialty exam

Visit the security learning path at https://aws.training/security