AWS Control Tower

Activation Day

5-26-2021

Agenda

All times Central US *(GMT -05:00)*

09:00 AM	09:15 AM	Introductions
09:15 AM	10:00 AM	AWS Control tower Overview
10:00 AM	10:50 AM	Multi-Account Governance / OU Structure
10:50 AM	11:00 AM	Break
11:00 AM	11:30 AM	AWS Control Tower Demo
11:30 AM	12:00 PM	AWS Control Tower Customizations
12:00 PM	01:00 PM	CloudCheckr Presentation / Lunch Break
01:00 PM	04:00 PM	Introduction to our labs

Presenters Introduction

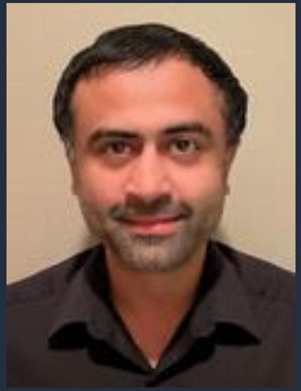
Jarrid Kleinfelter
Sr. Solutions Architect
Wisconsin

Andrew Timpone
Solutions Architect
Ohio

Roguen Keller
Sr. Customer Delivery Architect
Illinois

Support Introduction

Dan Ullom
Solutions Architect
Missouri



Jimmy Thanki
Sr. Solutions Architect
Iowa

David McElligott
Solutions Architect
Nebraska

Lijan Kuniyil
Solutions Architect
Massachusetts

Sahil Saini
Cloud Infra Architect
New York

Sushanth Mangalore
Solutions Architect
Illinois

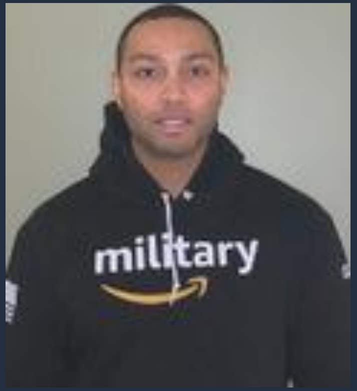
Jayapradha Krishnan
Sr. Solutions Architect
California

Johanna Wood
Sr. Migration Specialist
Massachusetts

Support Introduction

Charles Proctor
Demand Gen Rep
Virginia

Fernanda Machado
Solutions Architect
Amsterdam



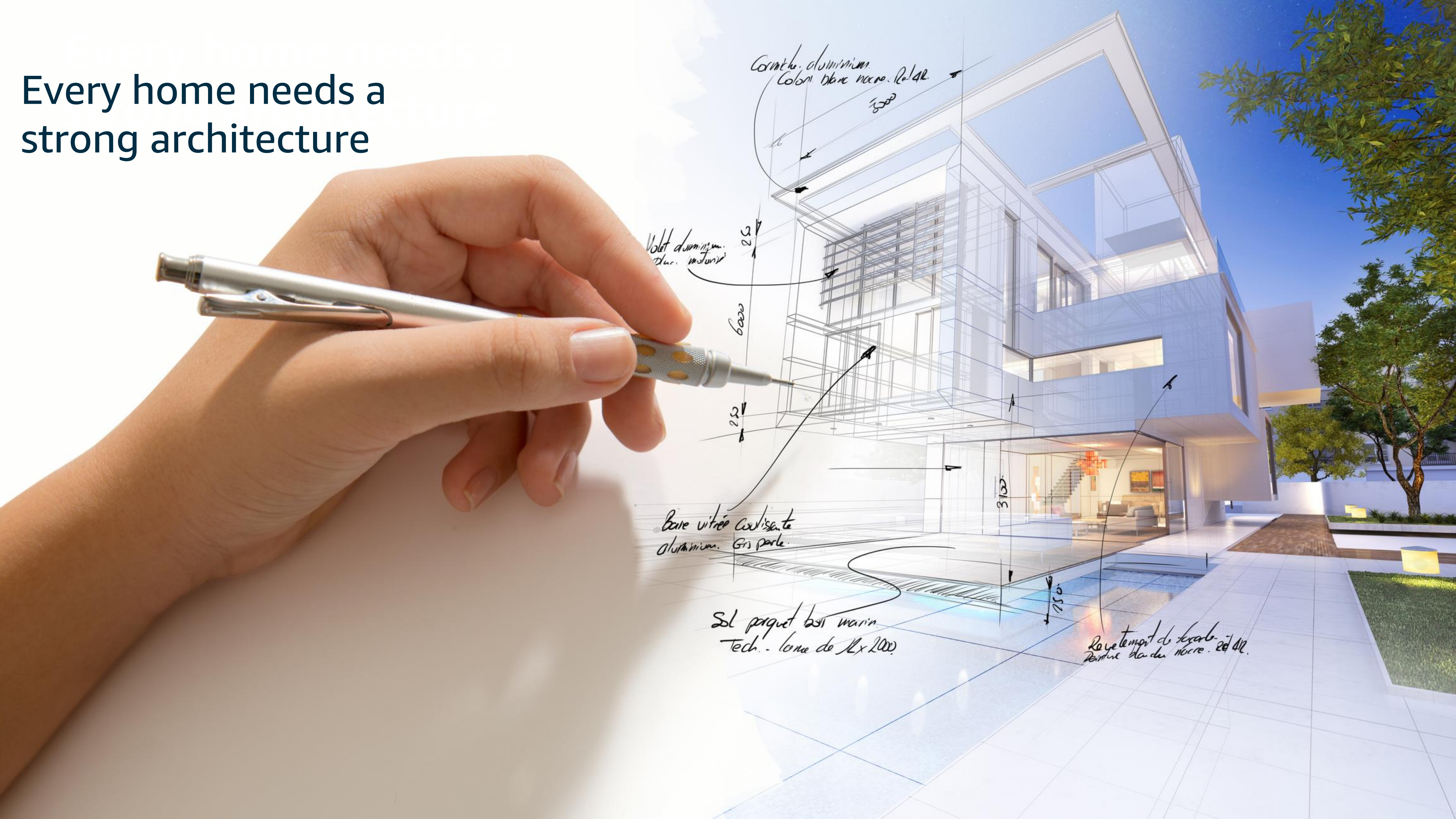
Craig Edwards
Solutions Architect
Virginia

Vijay Kumar
Solutions Architect
North Carolina

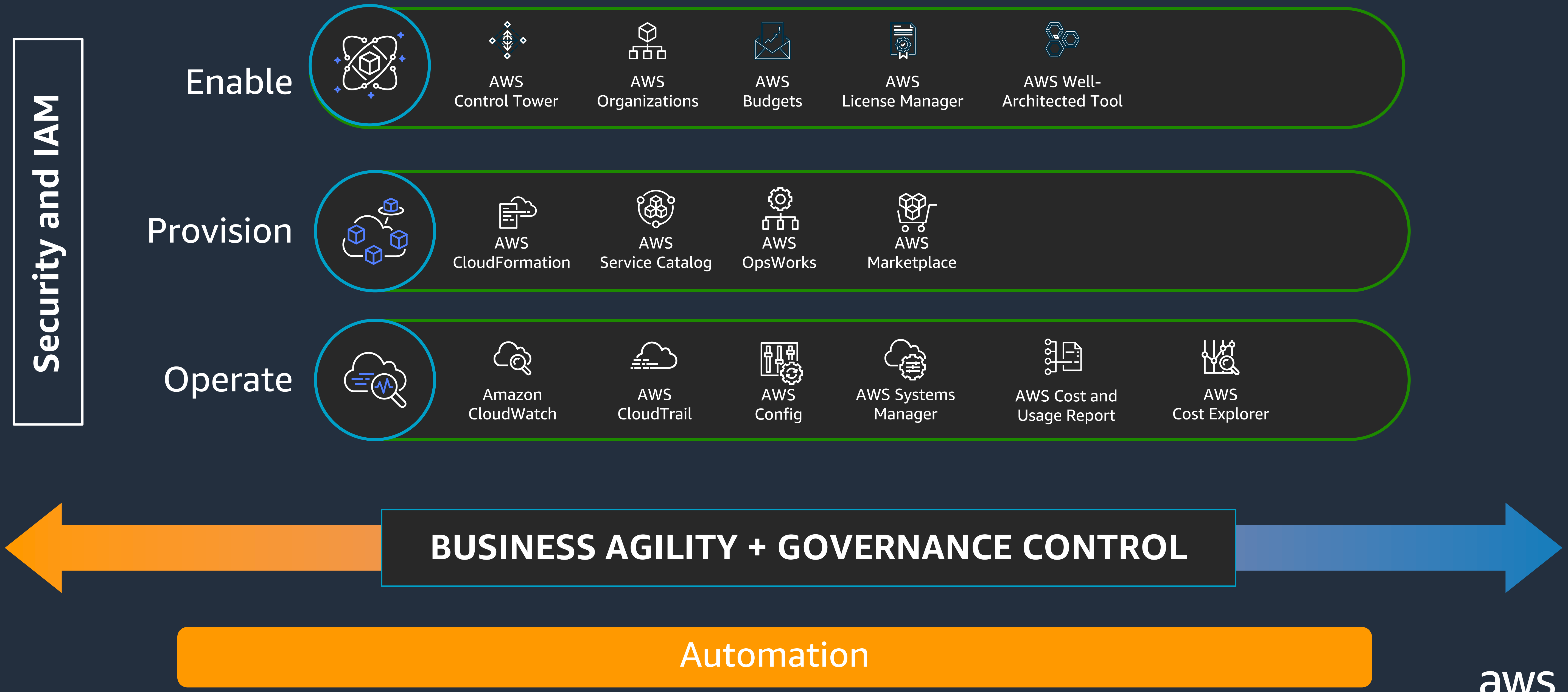
Introduction Poll

https://pollev.com/jarridkleinf831

Every home needs a strong architecture



AWS management and governance services



Security and IAM

Enable

AWS Control Tower

AWS Organizations

AWS Budgets

AWS License Manager

AWS Well-Architected Tool

Provision

AWS CloudFormation

AWS Service Catalog

AWS OpsWorks

AWS Marketplace

Operate

Amazon CloudWatch

AWS CloudTrail

AWS Config

AWS Systems Manager

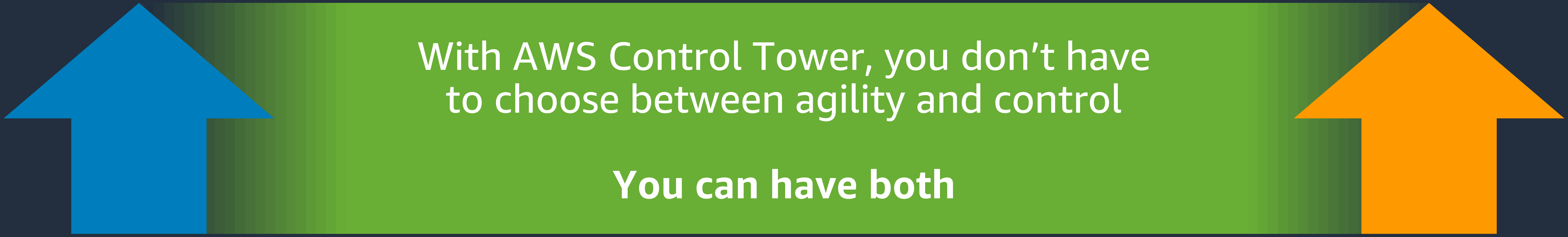
AWS Cost and Usage Report

AWS Cost Explorer

BUSINESS AGILITY + GOVERNANCE CONTROL

Automation

Business agility *and* governance control



With AWS Control Tower, you don’t have to choose between agility and control

You can have both

Governance

Security

Compliance

Operations

Spend Management

Agility

Self-service access

Experiment fast

Respond quickly to change

What is a landing zone?

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
- Customers get code that they will need to manage & maintain

AWS Control Tower:

- AWS Managed Service version of AWS Landing Zone

AWS Control Tower

The easiest self-service solution to automate the setup of **new AWS multi-account environments**

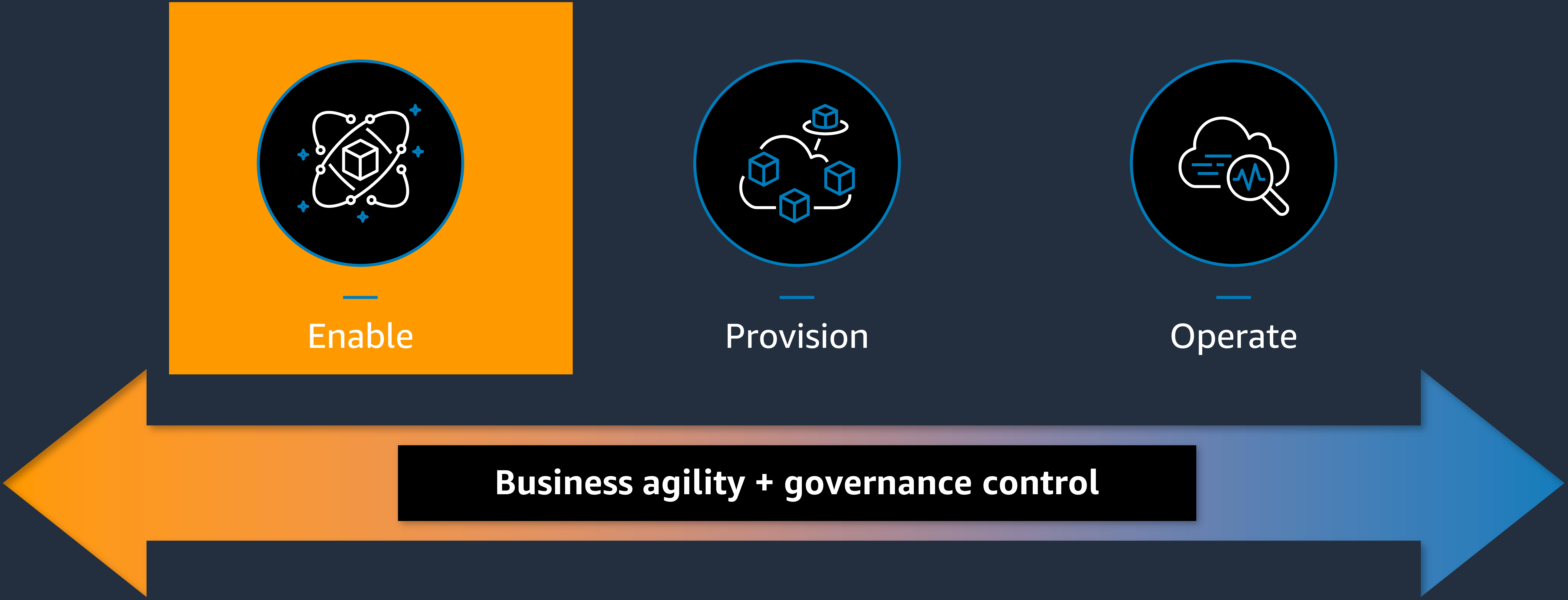
AWS Managed Service version of multi account environment

Deployment of AWS best practice Blueprints and Guardrails

An AWS service, offering automated account creation based on AWS best practices

Dashboard for monitoring compliance status

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



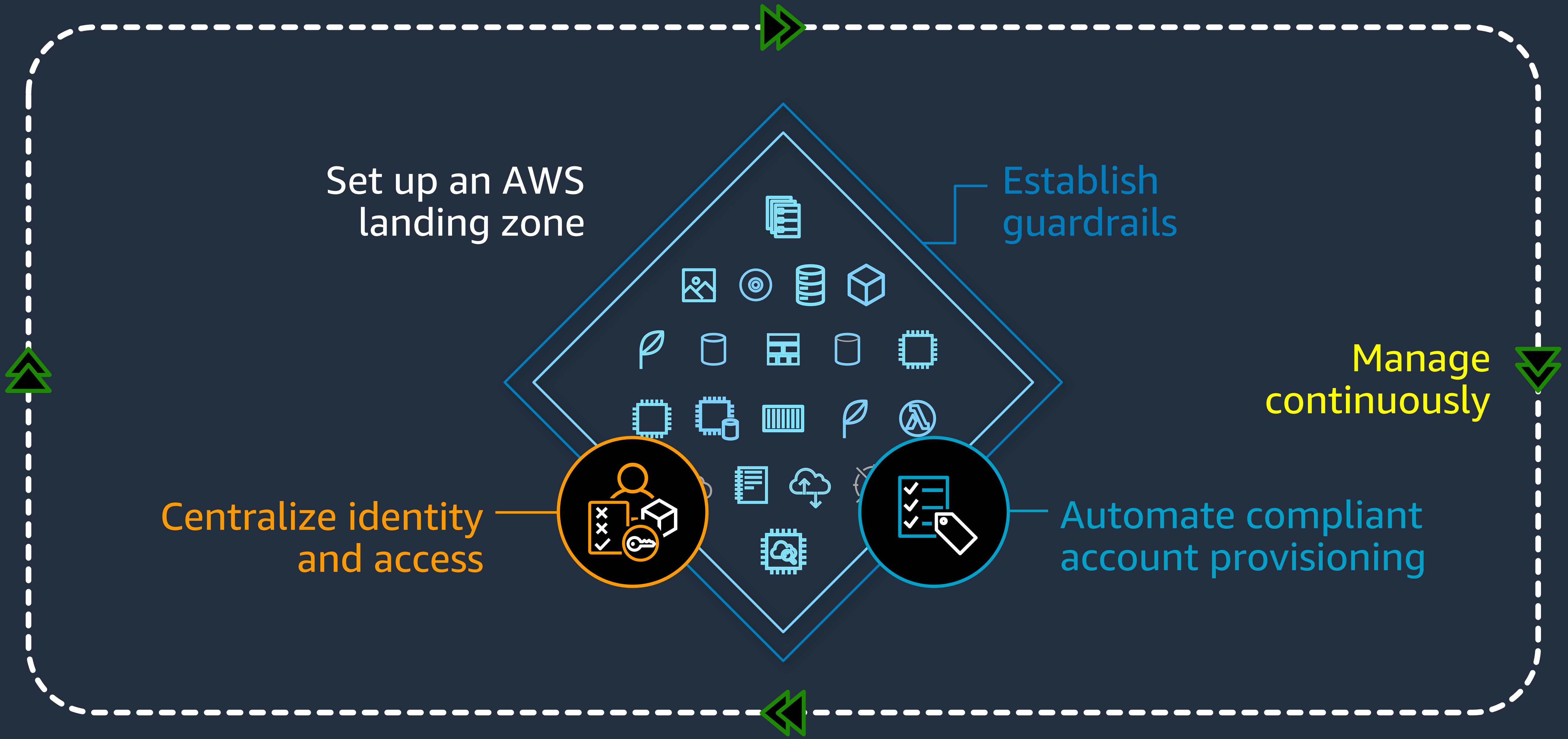
Enable

Provision

Operate

Business agility + governance control

Enable governance



Set up an AWS landing zone

Establish guardrails

Manage continuously

Centralize identity and access

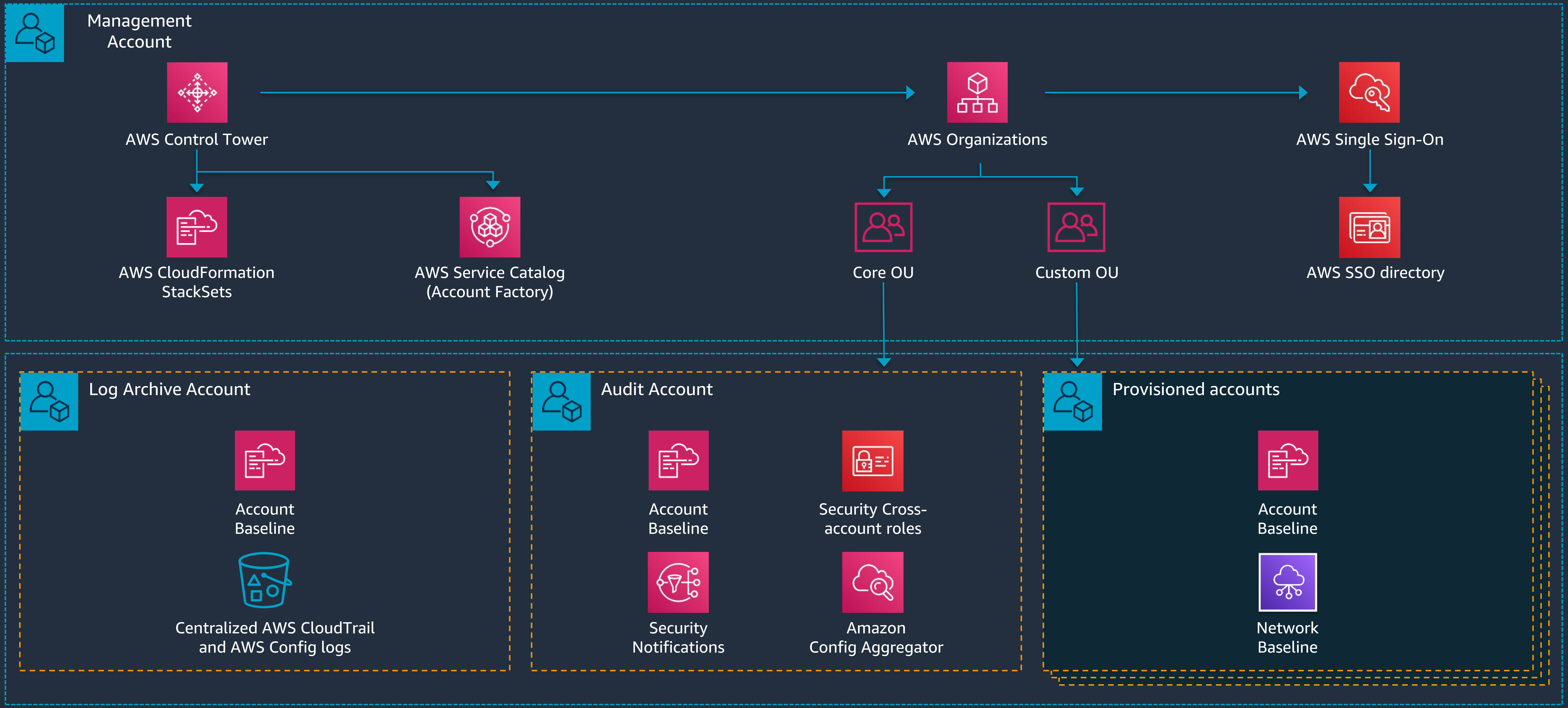
Automate compliant account provisioning

Out of the Box in < 1 Hr…ZERO lines of code written
2 email addresses and 2 mouse clicks

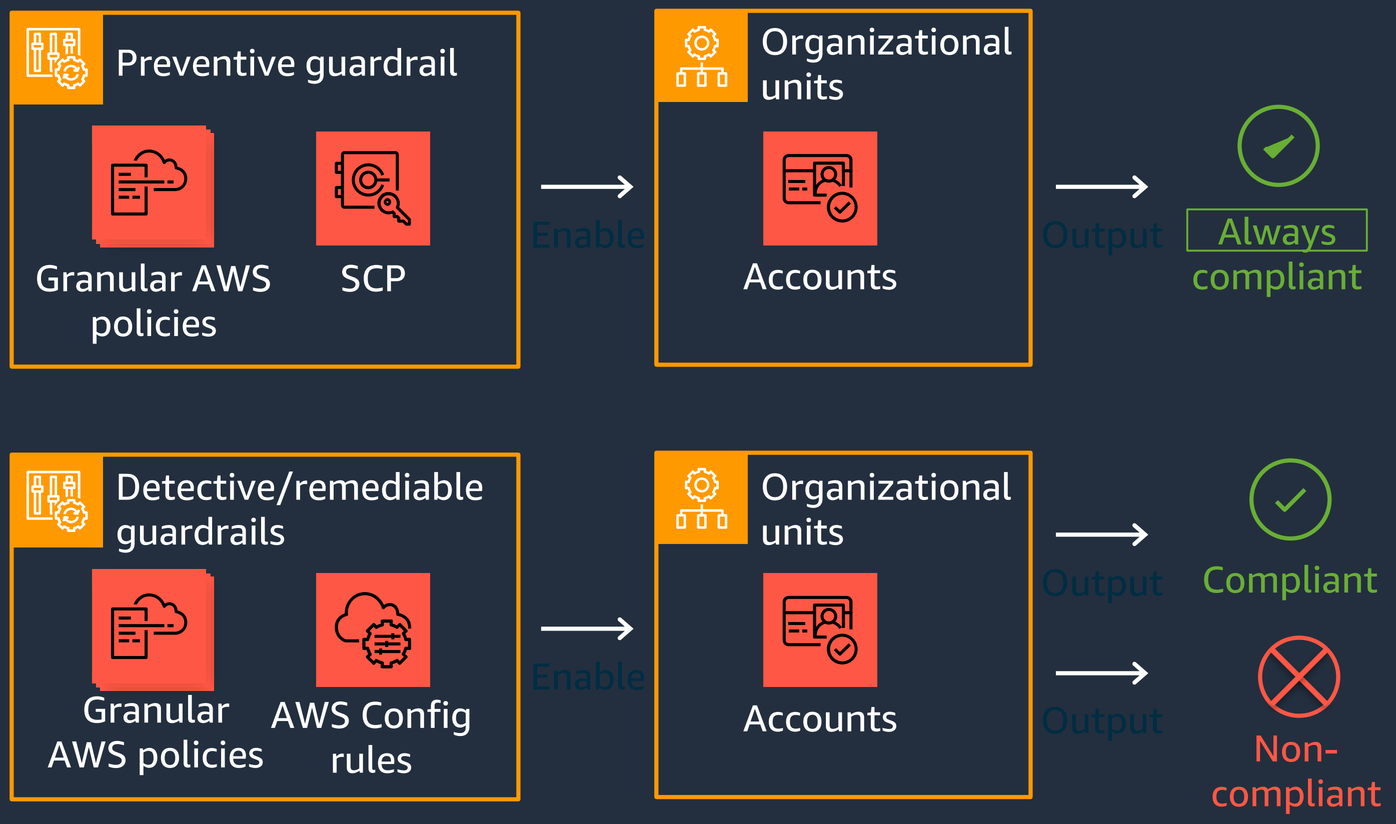
- Automated landing zone
- Account factory
- Guardrails
- Dashboard for visibility
- Built-in identity and access
- Preconfigured log archive and audit access to accounts
- Built-in monitoring and notificatior
- Automatic updates

https://tinyurl.com/setuplaunch

Landing Zone provisioned by AWS Control Tower



Establish guardrails



Guardrail Examples

Guardrail	Type	Requirement
Enable MFA for the Root User	Detective	Strongly Recommended
Disallow public read access to S3	Detective	Strongly Recommended
Enable AWS Config in All Available Regions	Preventive	Mandatory
Disallow Policy Changes to Log Archive	Preventive	Mandatory
Integrate CloudTrail Events with CloudWatch Logs	Preventive	Mandatory
Disallow Amazon S3 Buckets That Are Not Versioning Enabled	Detective	Elective
Disallow Delete Actions on Amazon S3 Buckets Without MFA	Detective	Elective

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)
- AWS SSO integrates with 3rd party IDP (Microsoft Azure AD, PING, OKTA)

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

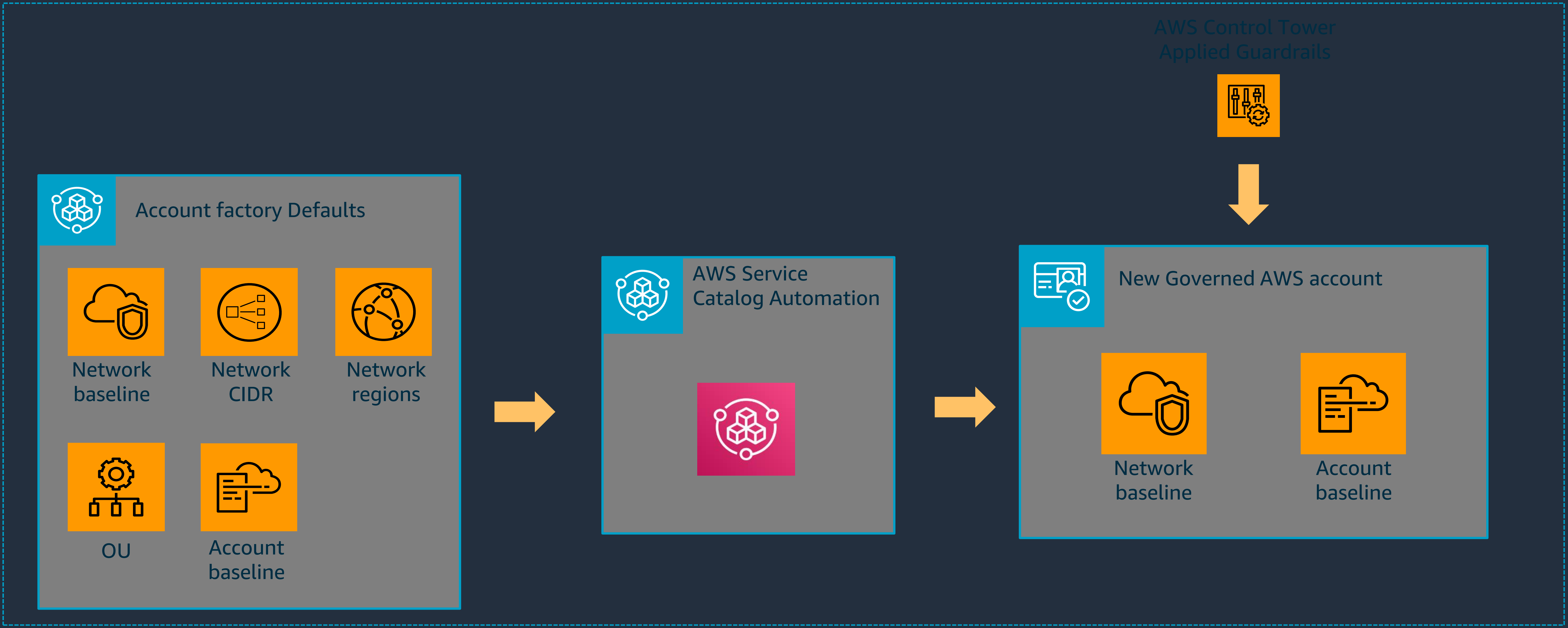
Enable

Provision

Operate

Business agility + governance control

Automate Compliant Account Provisioning



AWS Control Tower
Applied Guardrails

Account factory Defaults

Network baseline

Network CIDR

Network regions

OU

Account baseline

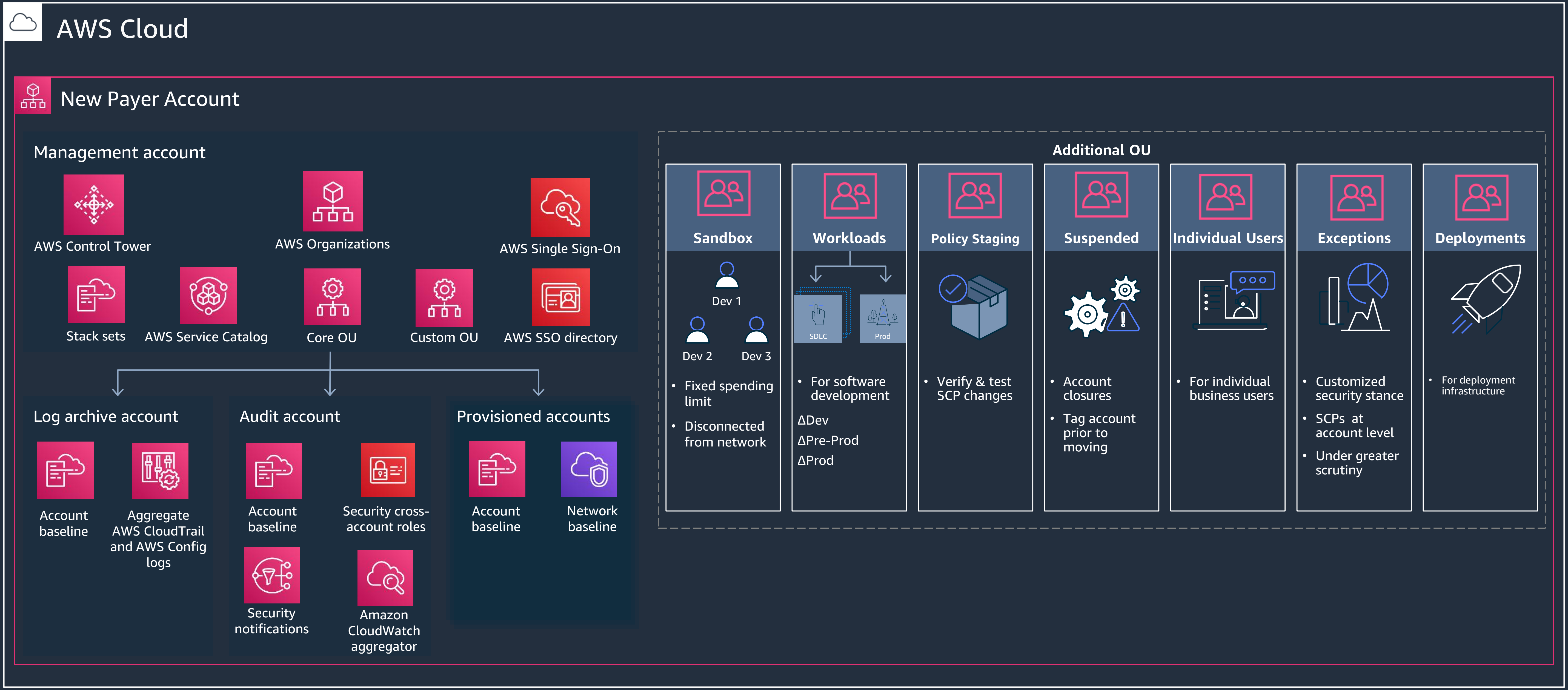
AWS Service
Catalog Automation

New Governed AWS account

Network baseline

Account baseline

New customer journey



AWS Cloud

New Payer Account

Management account

AWS Control Tower

AWS Organizations

AWS Single Sign-On

Stack sets

AWS Service Catalog

Core OU

Custom OU

AWS SSO directory

Log archive account

Account baseline

Aggregate AWS CloudTrail and AWS Config logs

Audit account

Account baseline

Security cross-account roles

Security notifications

Amazon CloudWatch aggregator

Provisioned accounts

Account baseline

Network baseline

Additional OU

Sandbox

Dev 1

Dev 2

Dev 3

- Fixed spending limit
- Disconnected from network

Workloads

- For software development

ΔDev

ΔPre-Prod

ΔProd

Policy Staging

- Verify & test SCP changes

Suspended

- Account closures
- Tag account prior to moving

Individual Users

- For individual business users

Exceptions

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

Deployments

- For deployment infrastructure

Existing customer journey

Jump start your Organization

Service Catalog

SCPs

with

AWS SSO

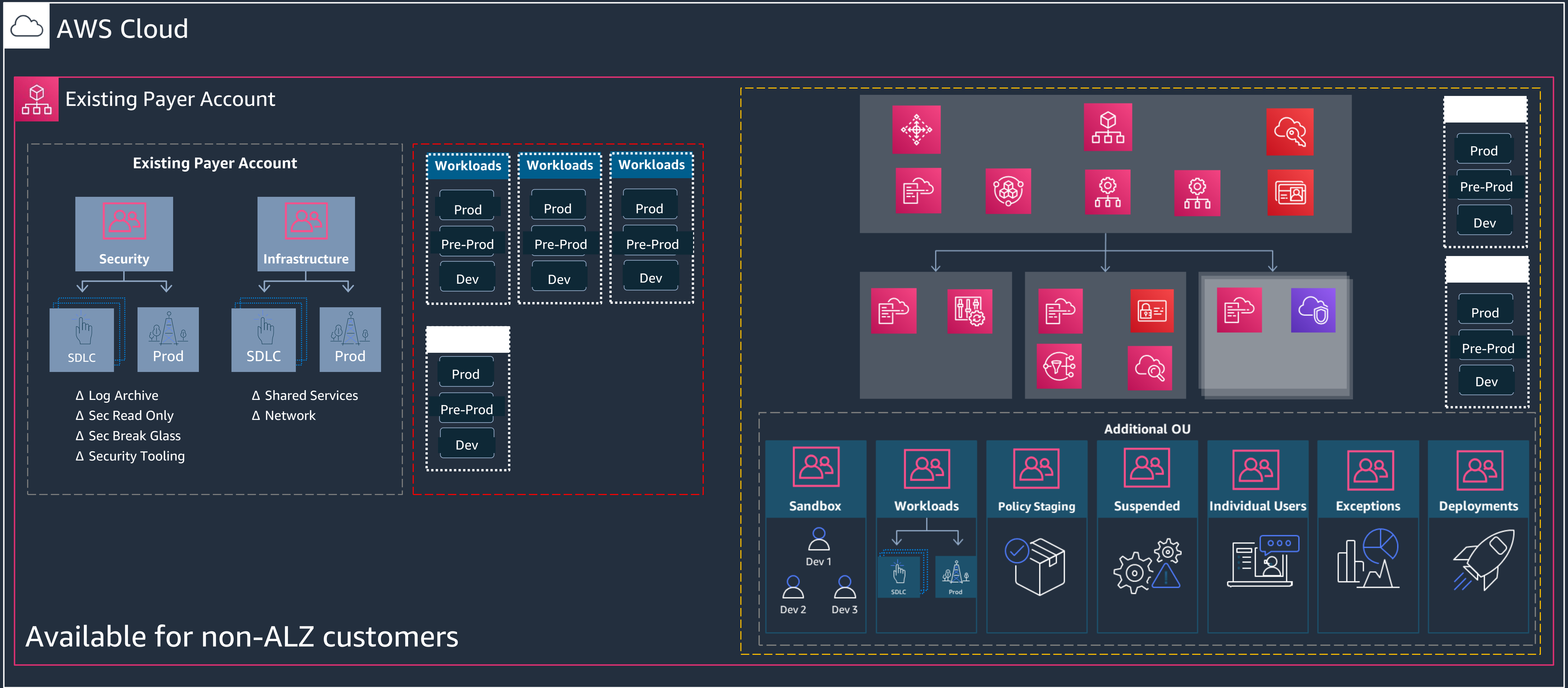
AWS Config

AWS Control Tower

Review and test requirements:

- Single Sign-On
- Secure Token Service - STS
- Service Control Policies (SCP)
- AWS Config
- CloudTrail
- CloudFormation Stack Sets

Existing customer journey



Available for non-ALZ customers

Extend central governance with AWS Organizations

Centrally provision resources in a multi-account environment

- AWS CloudFormation
- AWS Systems Manager
- AWS Service Catalog

Share resources and control access to accounts, regions, and services

- AWS Personal Health Dashboard
- AWS Resource Access Manager
- AWS Backup & Backup Policies
- Tag Policies

Optimize costs and identify cost-saving measures

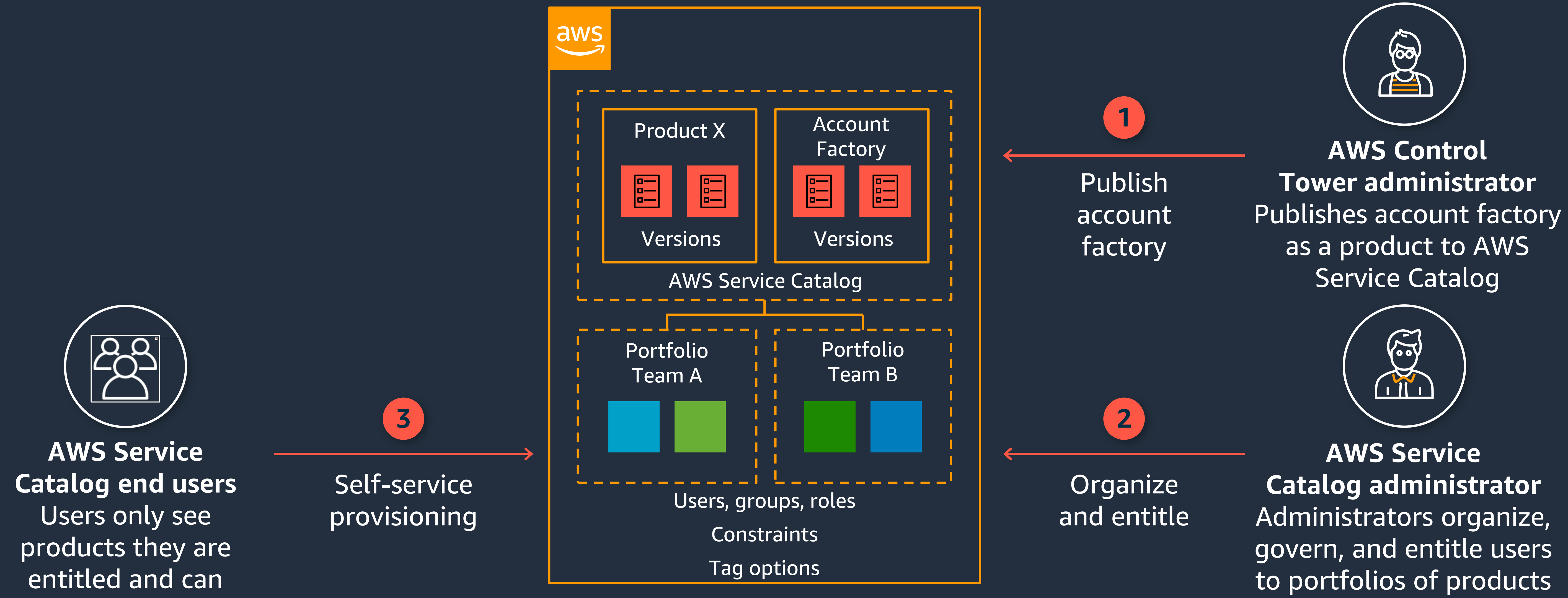
- AWS Trusted Advisor
- AWS Compute Optimizer
- AWS Cost Explorer
- AWS License Manager
- S3 Storage Lens

Seamless integration with AWS security services

- AWS Audit Manager
- Amazon GuardDuty
- Amazon Cloud Directory
- AWS Firewall Manager
- Amazon Macie
- AWS Security Hub
- AWS IAM Access Analyzer
- AI/ML Policies

https://docs.aws.amazon.com/organizations/

Self-service account provisioning in AWS Service Catalog



Product X

Versions

Account Factory

Versions

AWS Service Catalog

Portfolio Team A

Portfolio Team B

Users, groups, roles

Constraints

Tag options

1 Publish account factory

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

2 Organize and entitle

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

3 Self-service provisioning

AWS Service Catalog end users
Users only see products they are entitled 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)

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

Enable

Provision

Operate

Business agility + governance control

Operate with agility + control

Operate

Monitor

Monitor resources and workloads

Audit

Audit resource configurations, user access, and policy enforcement

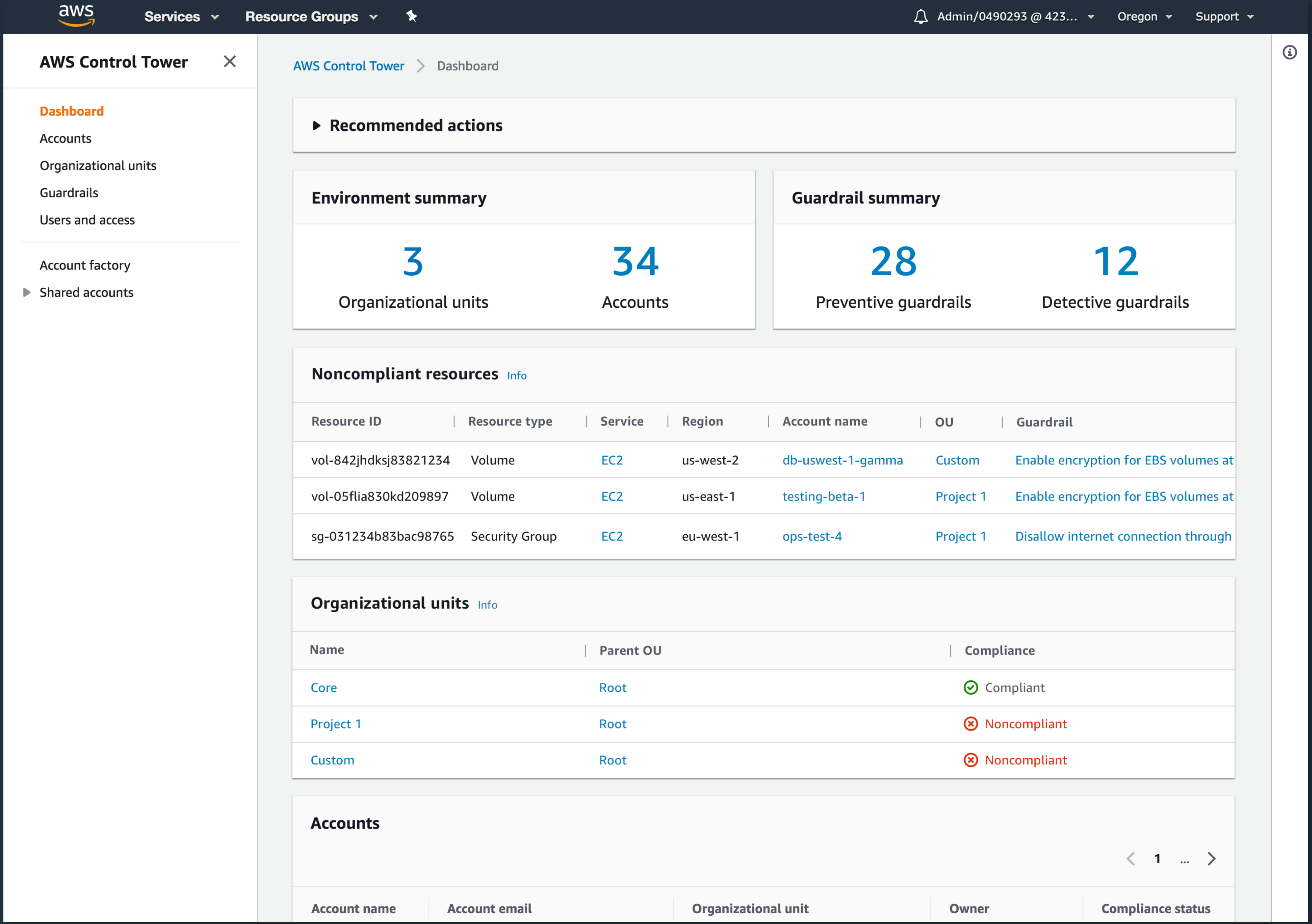
Act

Take operational action on resources

Dashboard

Continuous visibility into your multi-account environment

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

Pricing and availability

Generally available in Americas (Canada, N. Virginia & Ohio, Oregon), APAC (Sydney, Singapore) and EU (Ireland, Frankfurt, London, Stockholm)

No additional charge for using AWS Control Tower

Pay only for underlying AWS services (e.g., AWS Config rules, AWS CloudTrail) that are enabled

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

Questions?

AWS Control Tower customizations

Lifecycle events

Benefits:

- Amazon EventBridge Integration
- Operation Status

Events supported:

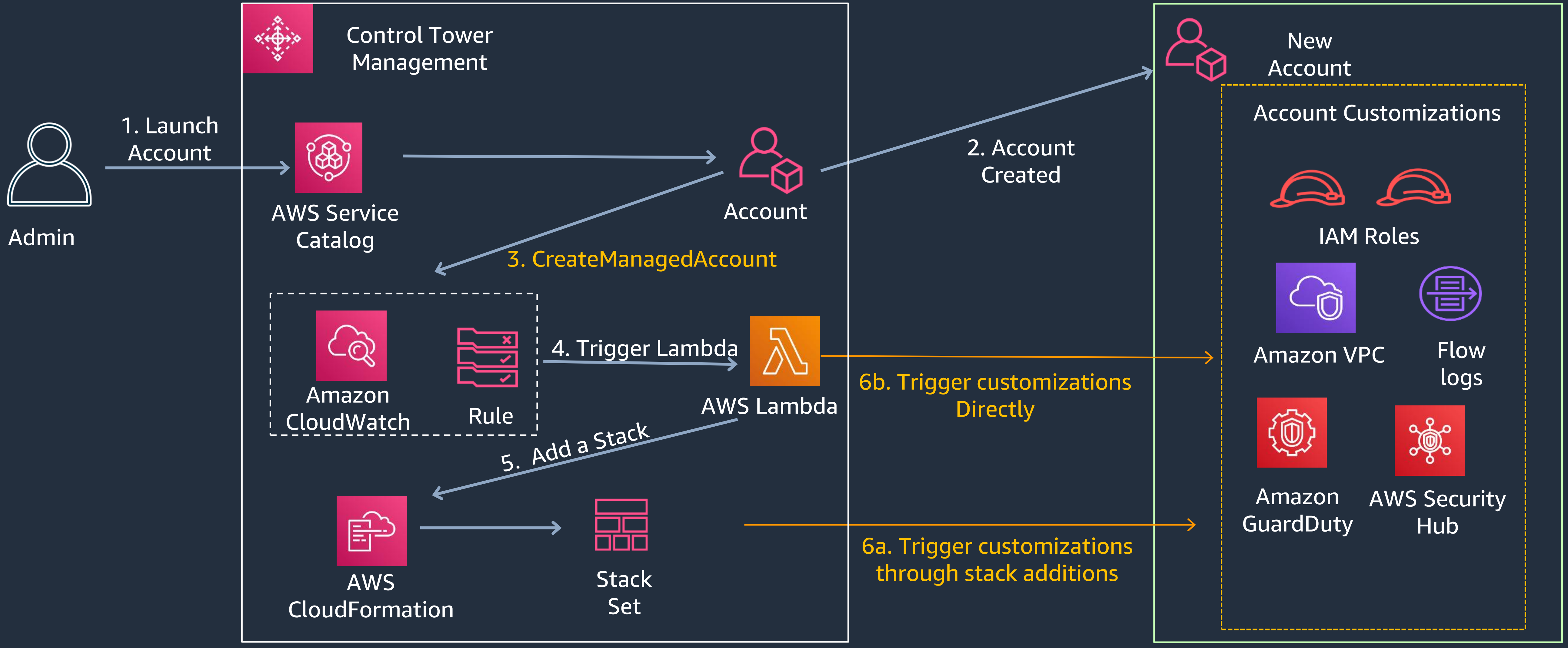
1. CreateManagedAccount
2. UpdateManagedAccount
3. EnableGuardrail
4. DisableGuardrail
5. SetupLandingZone
6. UpdateLandingZone
7. RegisterOrganizationalUnit
8. DeregisterOrganizationalUnit

Life Cycle Events

- CreateManagedAccount:
  - Creates and provisions a new account using account factory.
- UpdateManagedAccount:
  - Updates a provisioned product that is associated with an account you created using account factory.
- EnableGuardrail:Enables a guardrail on an OU that was created by Control Tower.
- DisableGuardrail: Disables a guardrail on an account that was created by Control Tower.
- SetupLandingZone: Sets up a landing zone.
- UpdateLandingZone: Updates a landing zone.
- RegisterOrganizationalUnit: Creates a new OU.
- DeregisterOrganizationalUnit: Deletes an OU that was created by Control Tower.

Configure/Trigger Customizations with LifeCycle Events

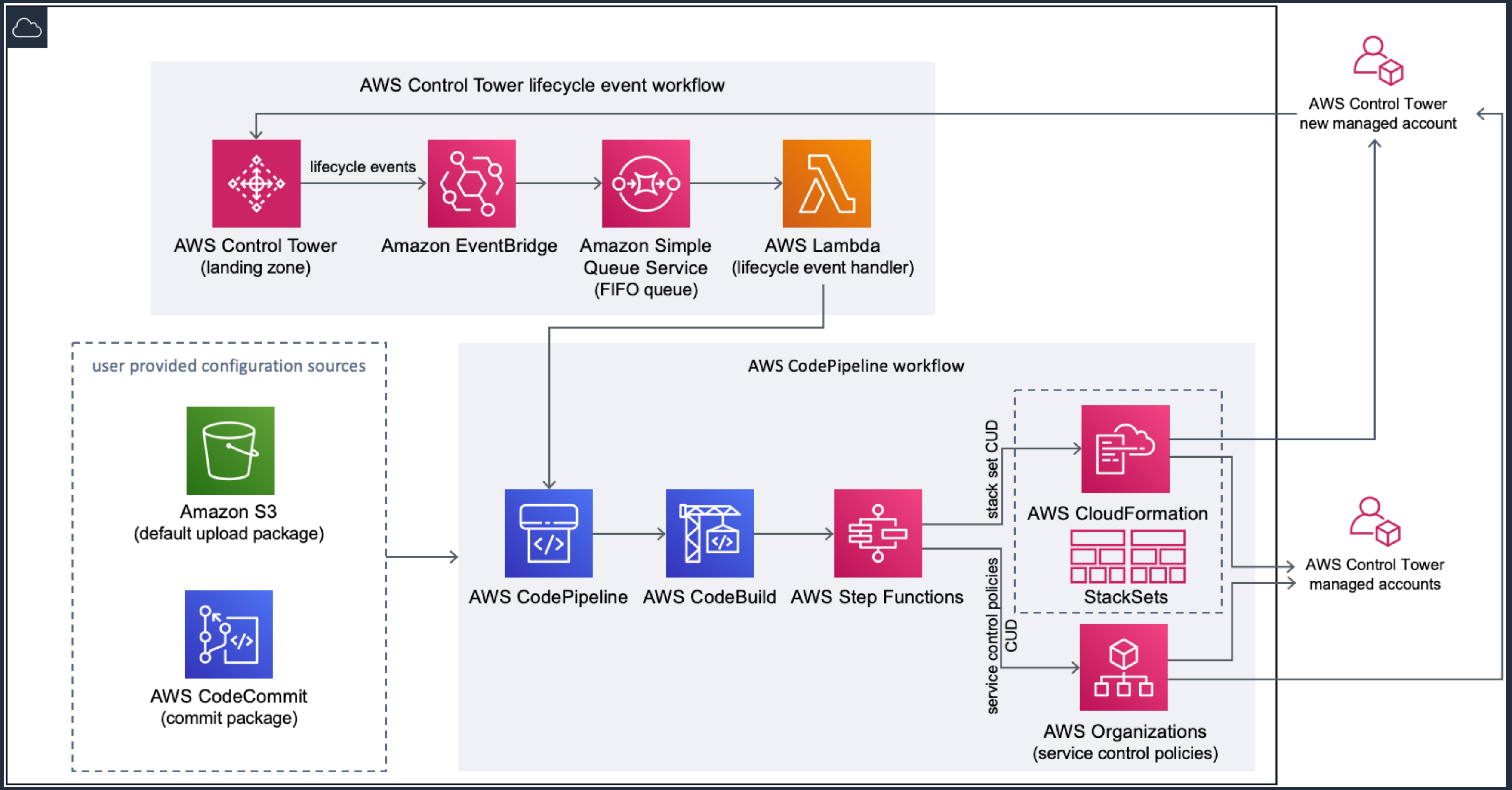
CreateManagedAccount: The log records whether AWS Control Tower successfully completed every action to create and provision a new account using account factory.



How to customize AWS CT today?

- Automate post-account creation tasks
- Extend your Control Tower Landing Zone
- Attach resources to accounts
- Deploy SCP's & Config rules

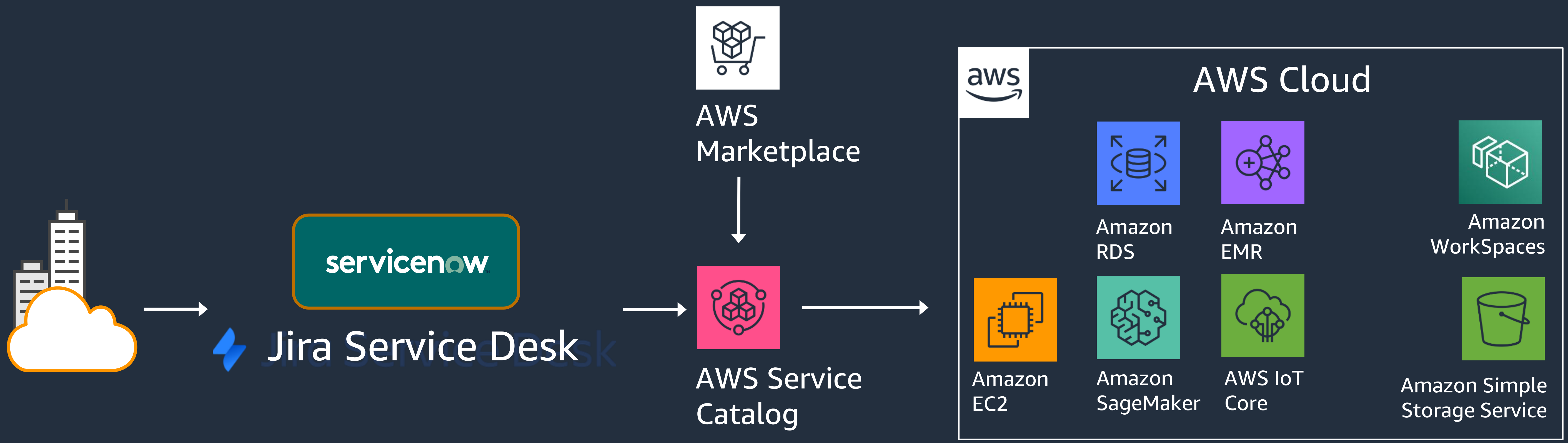
Customization Reference Solution



AWS Control Tower lifecycle event workflow
lifecycle events
AWS Control Tower (landing zone)
Amazon EventBridge
Amazon Simple Queue Service (FIFO queue)
AWS Lambda (lifecycle event handler)
AWS Control Tower new managed account
user provided configuration sources
Amazon S3 (default upload package)
AWS CodeCommit (commit package)
AWS CodePipeline workflow
AWS CodePipeline
AWS CodeBuild
AWS Step Functions
stack set CUD
service control policies CUD
AWS CloudFormation
StackSets
AWS Organizations (service control policies)
AWS Control Tower managed accounts

https://aws.amazon.com/solutions/customizations-for-aws-control-tower/

Enabling self-service via AWS & ITSM Tools



1 Users browse and request AWS services

2 Administrators procure, publish, and govern AWS services

3 Operators monitor and manage AWS services

Use cases for Control Tower solutions on AWS Marketplace

https://aws.amazon.com/marketplace/solutions/control-tower/

Operational Readiness

Establish centralized infrastructure software and services to manage a multi-account environment and deliver enhanced performance and security.

Multi-account security

Multi-account security

Identity management

Network management

Operational Excellence

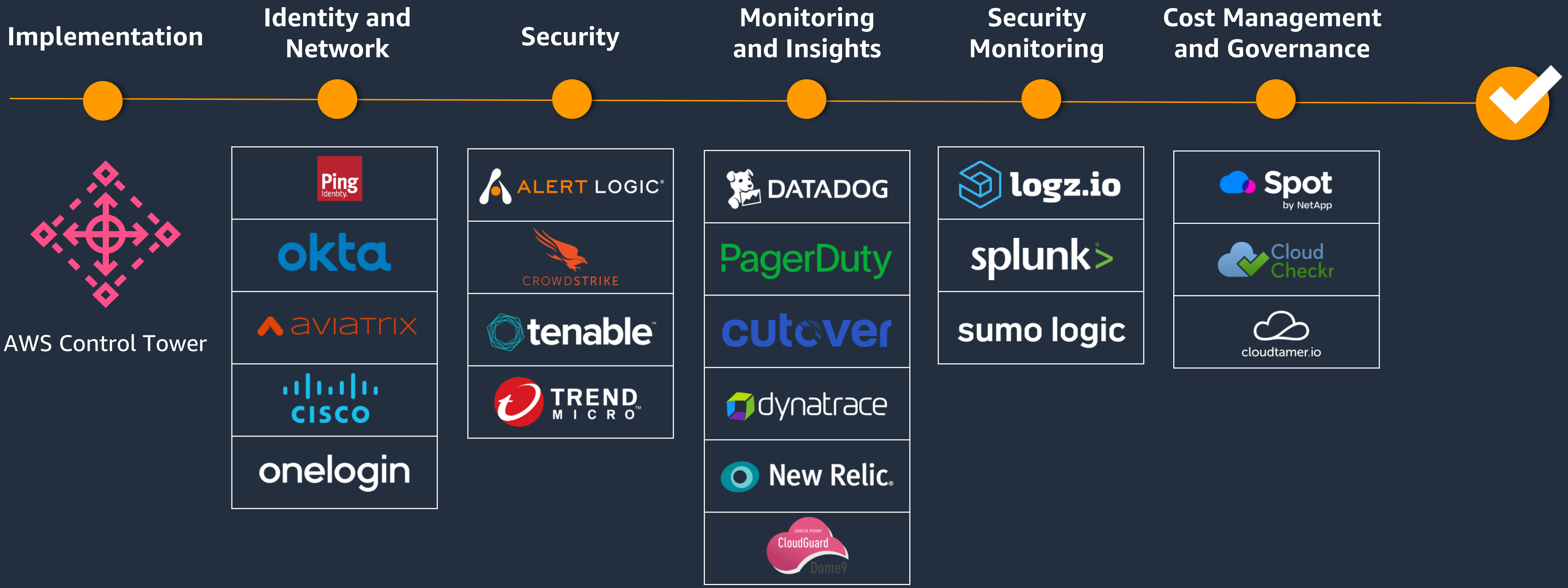
Elevate your multi-account environment by detecting the occurrence of security events, enabling faster responses, and making security improvements.

SIEM

Operational intelligence

Cost management and governance

Journey from zero to hero



Implementation

Identity and Network

Security

Monitoring and Insights

Security Monitoring

Cost Management and Governance

AWS Control Tower

Knowledge Check

https://pollev.com/jarridkleinf831

Session survey

https://survey.immersionday.com/F_3kSP3Gg

Session reference material

https://github.com/jarridkleinfelter/awsctactivationday526/blob/main/README.md

How do I get started?

Getting started : https://tinyurl.com/y2gtzf9c

AWS Control Tower labs: https://controltower.aws-management.tools/

How-to videos (Management & Governance): https://tinyurl.com/y3yeohkm

SCAN ME

Management & Governance AWS Blog

SCAN ME

AWS Organizations website

SCAN ME

AWS Control Tower Getting Started

SCAN ME

AWS Well-Architected website

Thank you

aws-cs-bd@amazon.com