Using AWS Control Tower to govern multi-account AWS environments at scale

NAME
TITLE
AWS
DATE

Balancing the needs of builders and central cloud IT

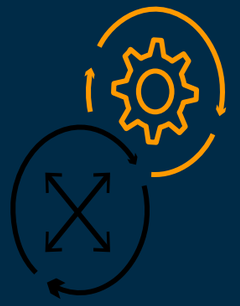
Builders: Stay agile

Innovate with the speed and agility of AWS

Cloud IT: Establish governance

Govern at scale with central controls

More innovation, greater agility, with control



Agility

Experiment

Be productive
Empower distributed teams
Self-service access

Respond quickly to change

Don’t choose between Agility or Control

You need and want both

Governance

Enable

Provision

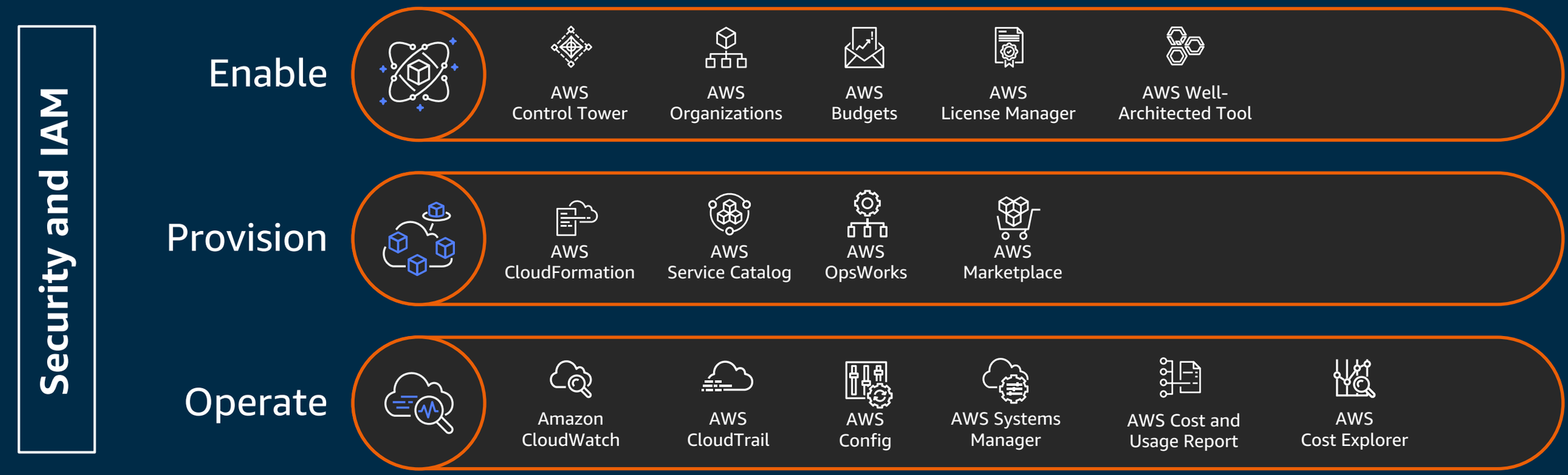
Operate

Secure & Compliant

Operations & Spend Management

aws

AWS management and governance services



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

Enable

Provision

Operate

Business agility + governance control

Why use AWS Control Tower?

- Set up a best-practices AWS environment in a few clicks
- Standardize account provisioning
- Centralize policy management
- Enforce governance and compliance proactively
- Enable end user self-service
- Get continuous visibility into your AWS environment
- Gain peace of mind

What is 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

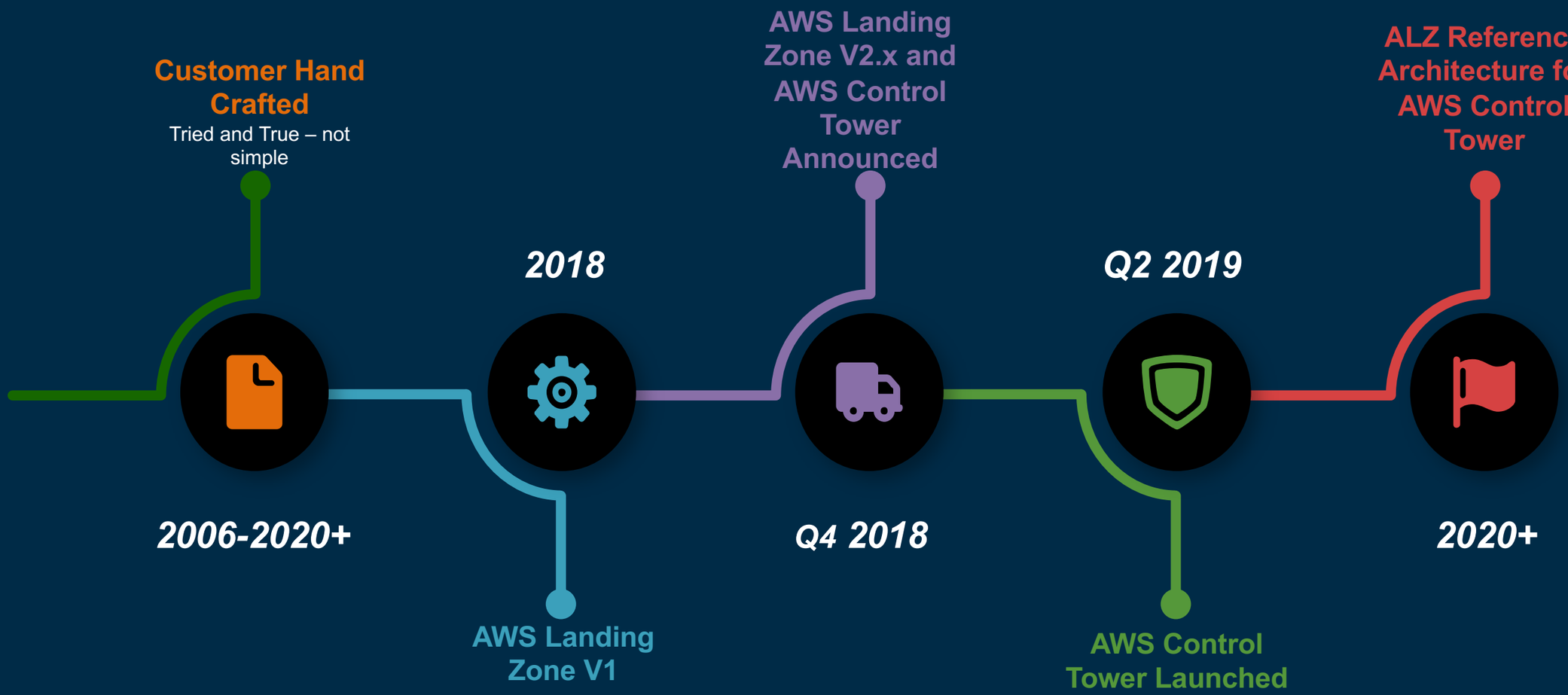
AWS Landing Zone Solution:

- Implementation of a landing zone based on multi-account strategy guidance
- Customers get code that they will need to manage & maintain
- Solution will no longer receive updates by EOY 2020

AWS Control Tower:

- AWS Managed Service version of AWS Landing Zone

Landing Zones – how we got here



Enable governance

Enable

aws

AWS Control Tower

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

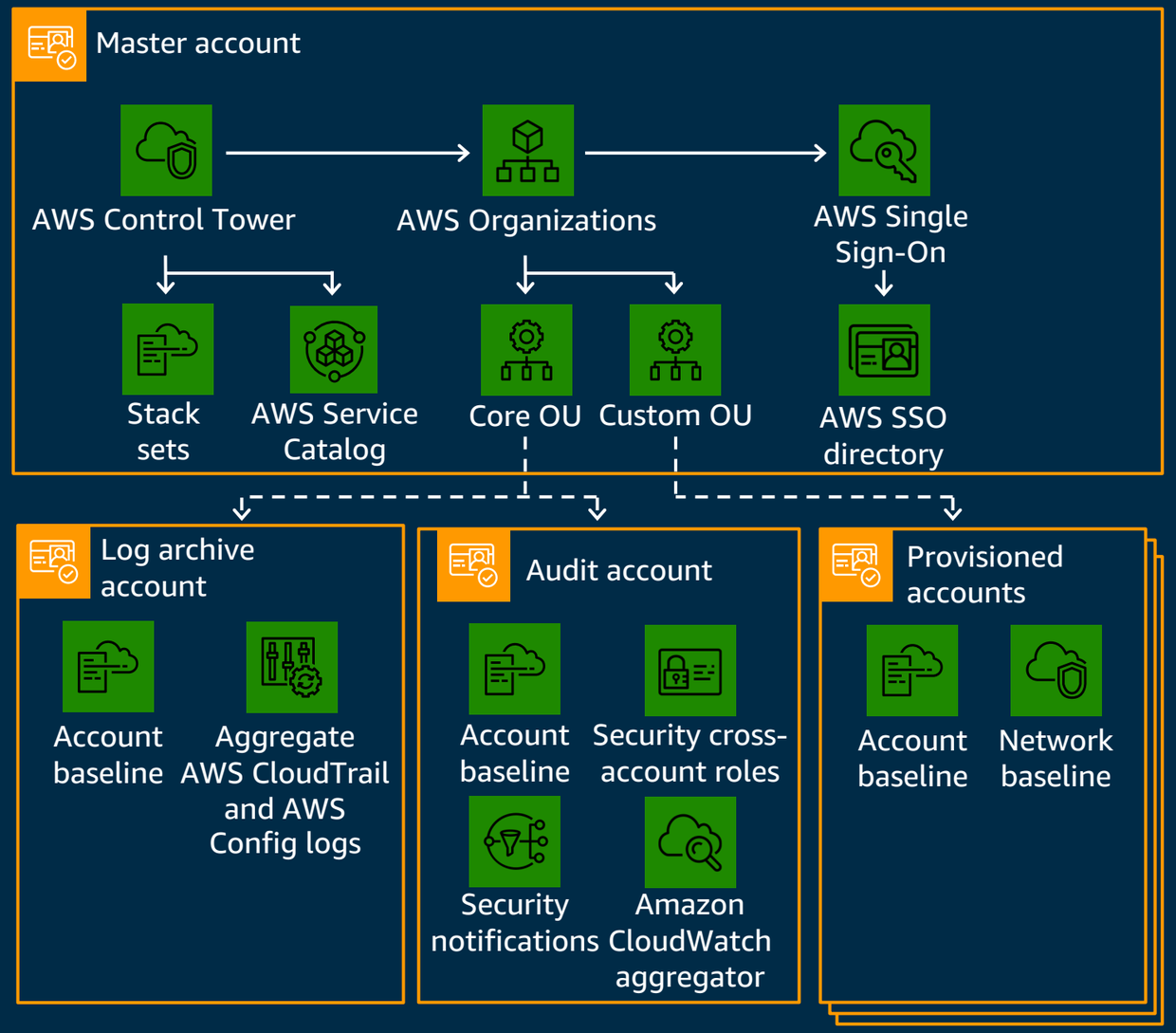
An AWS service offering account creation based on AWS best practices

Deployment of AWS best practice Blueprints and Guardrails

Baseline fundamental accounts to provide standardization of best practices

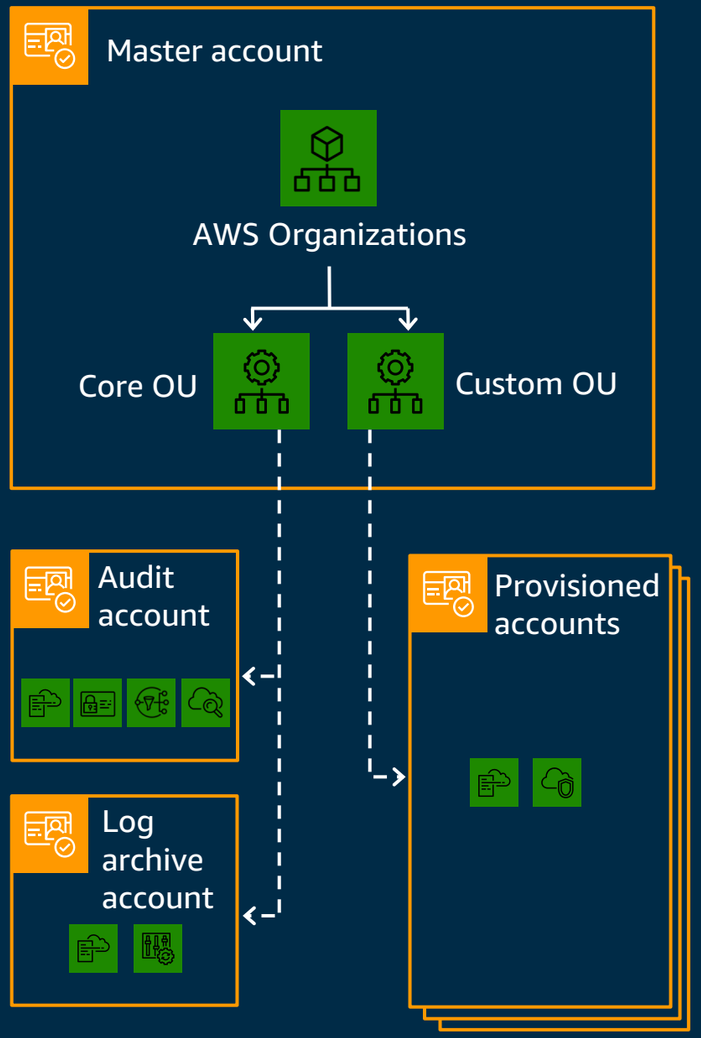
Single pane of glass for monitoring compliance to guardrails

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 AWS Organizations
- Identity and federated access management using AWS SSO
- Centralized log archive using AWS CloudTrail and AWS Config
- Cross-account audit access using AWS SSO and AWS IAM
- End user account provisioning through AWS Service Catalog
- Centralized monitoring and notifications using Amazon CloudWatch and Amazon SNS

Multi-account architecture

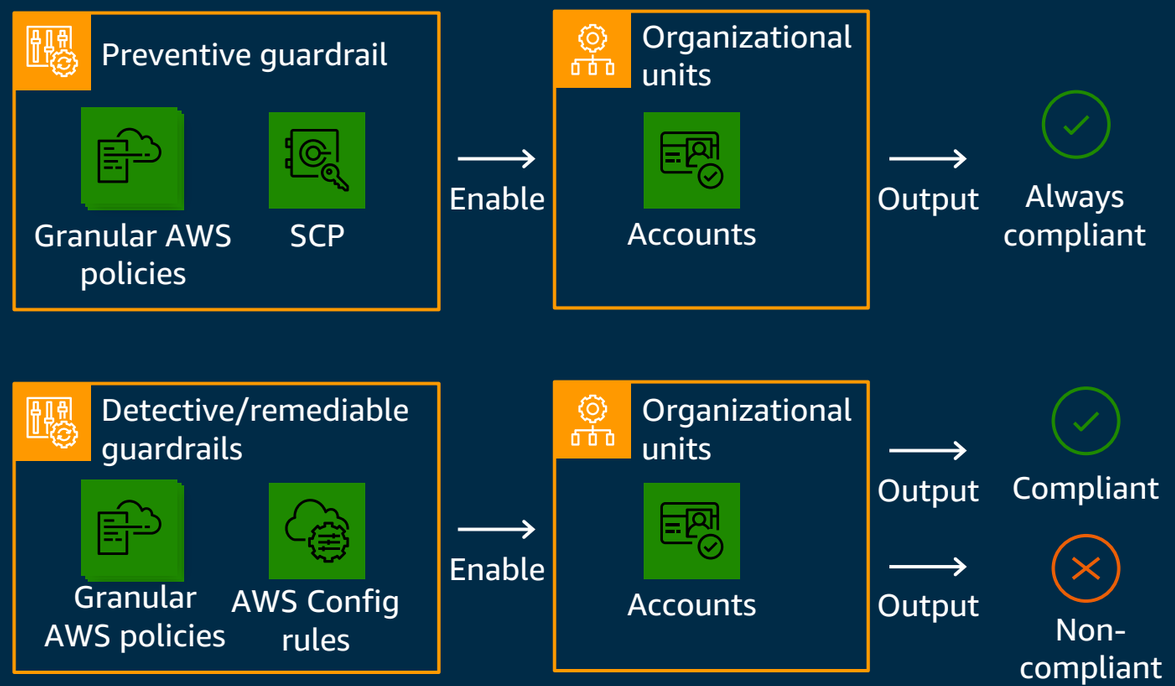


- Master account: designation of your existing account to create a new organization. Also your master payer account
- Organization consists of 2 OUs with pre-configured accounts -
  - Core OU: AWS Control Tower-created accounts, i.e., Audit account and Log archive account
  - Custom OU: Your provisioned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

Establish guardrails

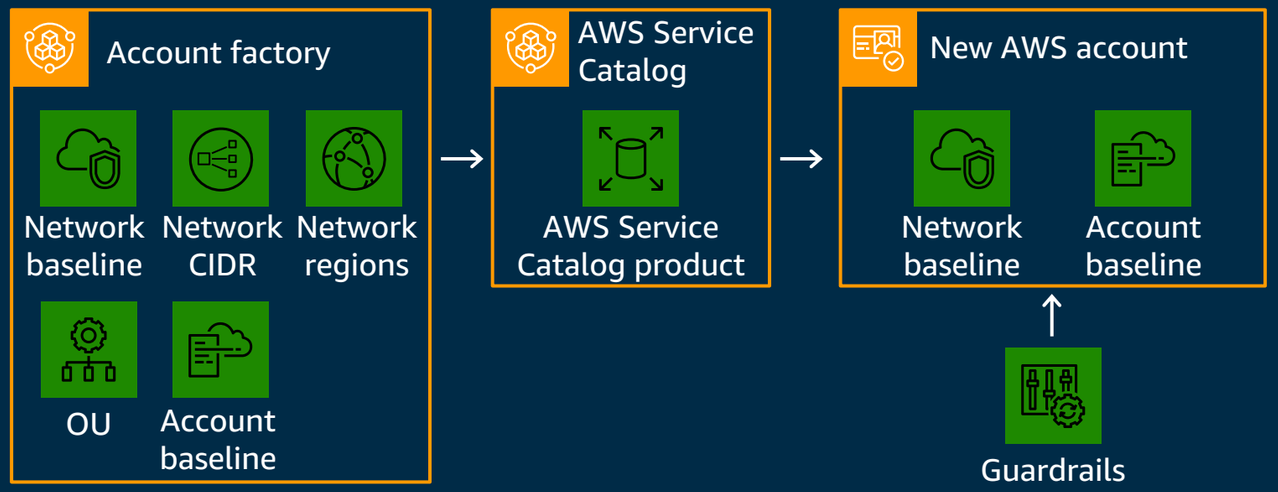


- Guardrails are preconfigured governance rules for security, compliance, and operations
- Expressed in plain English to provide abstraction over granular AWS policies
- Preventive guardrails: prevent policy violations through enforcement; implemented using AWS CloudFormation and SCPs
- Detective guardrails: 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

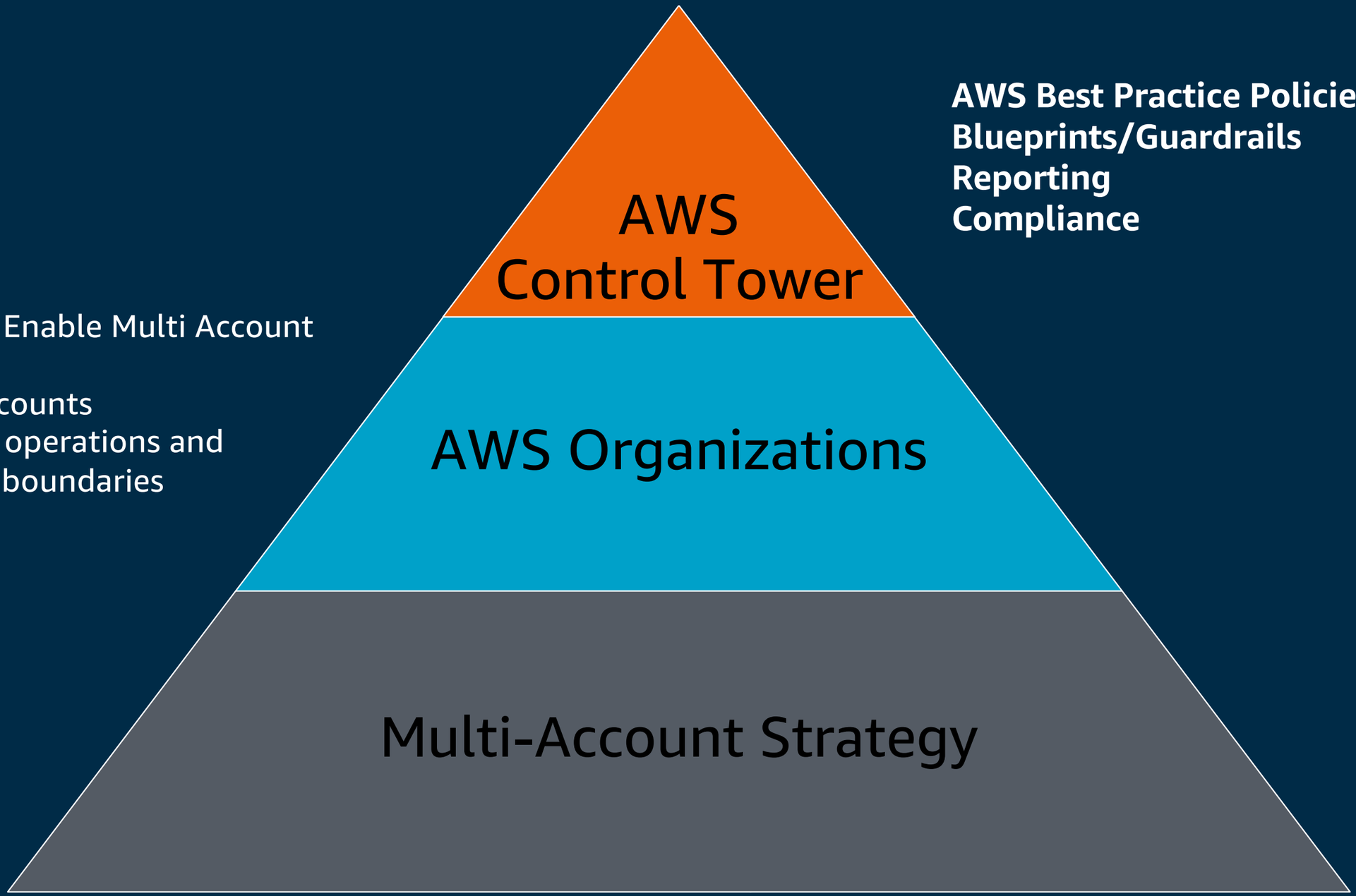
Guardrail examples

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

Automate compliant account provisioning



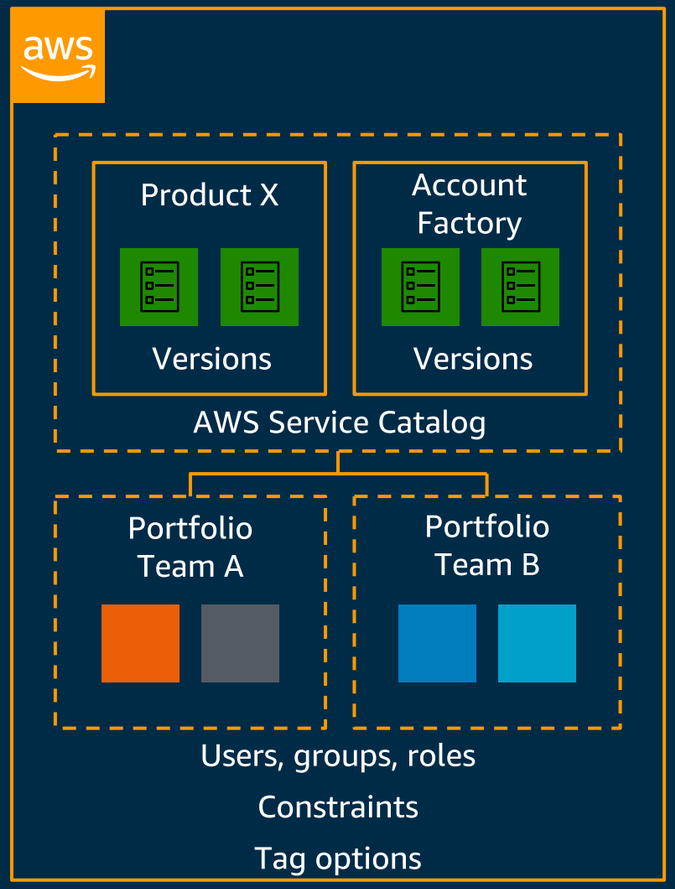
- Built-in account factory provides a template to standardize account provisioning
- Configurable network settings (e.g., subnets, IP addresses)
- Automatic enforcement of account baselines and guardrails
- Published to AWS Service Catalog



AWS Best Practice Policies
Blueprints/Guardrails
Reporting
Compliance

Define and Enable Multi Account Strategy
Manage Accounts
Implement operations and functional boundaries

Self-service account provisioning in AWS Service Catalog



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

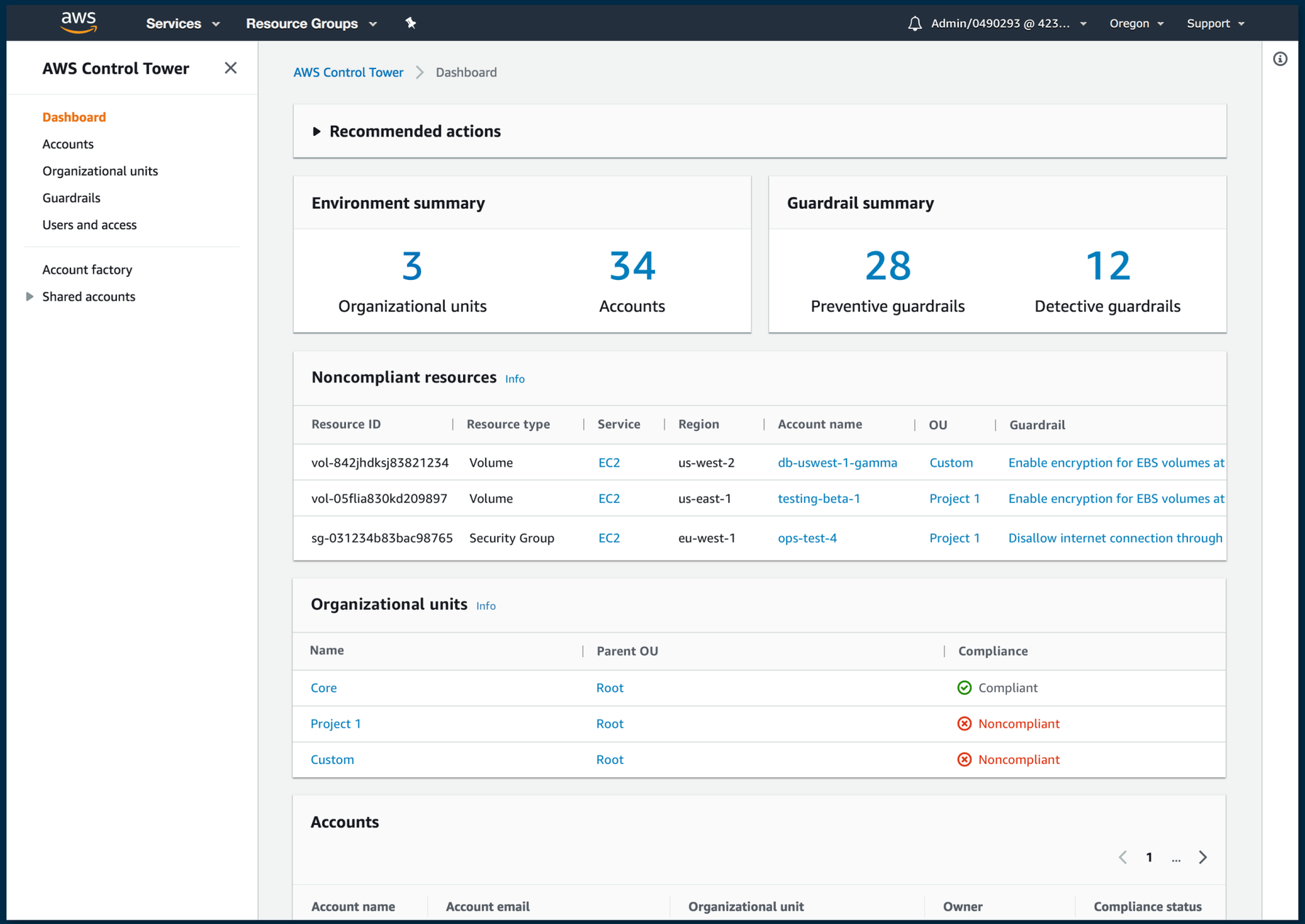
Take operational action on resources

Dashboard

Continuous visibility into your multi-account environment

aws

Dashboard for oversight



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 • Integration options with other 3rd party SSO providers (PING/OKTA, Azure AD – native support) • Cross-account roles enable centralized management
Security & Governance	• Multiple accounts enable separation of duties • Initial account security and AWS Config rules baseline • Network baseline

Summary of key features

Automated landing zone with best practice blueprints

Built-in identity and access management

Guardrails for policy management

Preconfigured log archive and audit access to accounts

Account factory for account provisioning

Built-in monitoring and notifications

Dashboard for visibility and actions

Automatic updates

aws

Pricing and availability

Generally available in US East (N. Virginia), US East (Ohio), US West (Oregon), and EU (Ireland), AP Southeast (Sydney)

No additional charge for using AWS Control Tower

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

How do I get started?

Management & Governance AWS Blog

AWS Organizations website

AWS Control Tower Getting Started

AWS Well-Architected website

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

Customer Immersion Day Material : https://dev.immersionday.com/control-tower/

AWS Control Tower blogs:

- Guardrail Mitigation: **https://tinyurl.com/y56dsalz**
- Self-Service Provisioning: **https://tinyurl.com/y3fk3fpk**
- Migrating workloads with AWS Control Tower and CloudEndure : **https://tinyurl.com/CTMigrate**

Getting started (re:Inforce 2019): **https://tinyurl.com/y2gtzf9c**
How-to videos (Management & Governance): **https://tinyurl.com/y3yeohkm**