AWS Control Tower

Simple, Consistent and Central Cloud Governance

AWS Control Tower

What do customers want to do on AWS?

Empower Builders

Decentralized model, self-service for builders

Move Fast

Innovate without sacrificing speed & agility of AWS

Stay Secure & Compliant

Govern at scale using central security and compliance rules

Challenges with multi-account environments

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

Introducing AWS Control Tower

Consistent and simple multi account management.

Automated AWS Setup

Launch an automated landing zone with best-practices blueprints

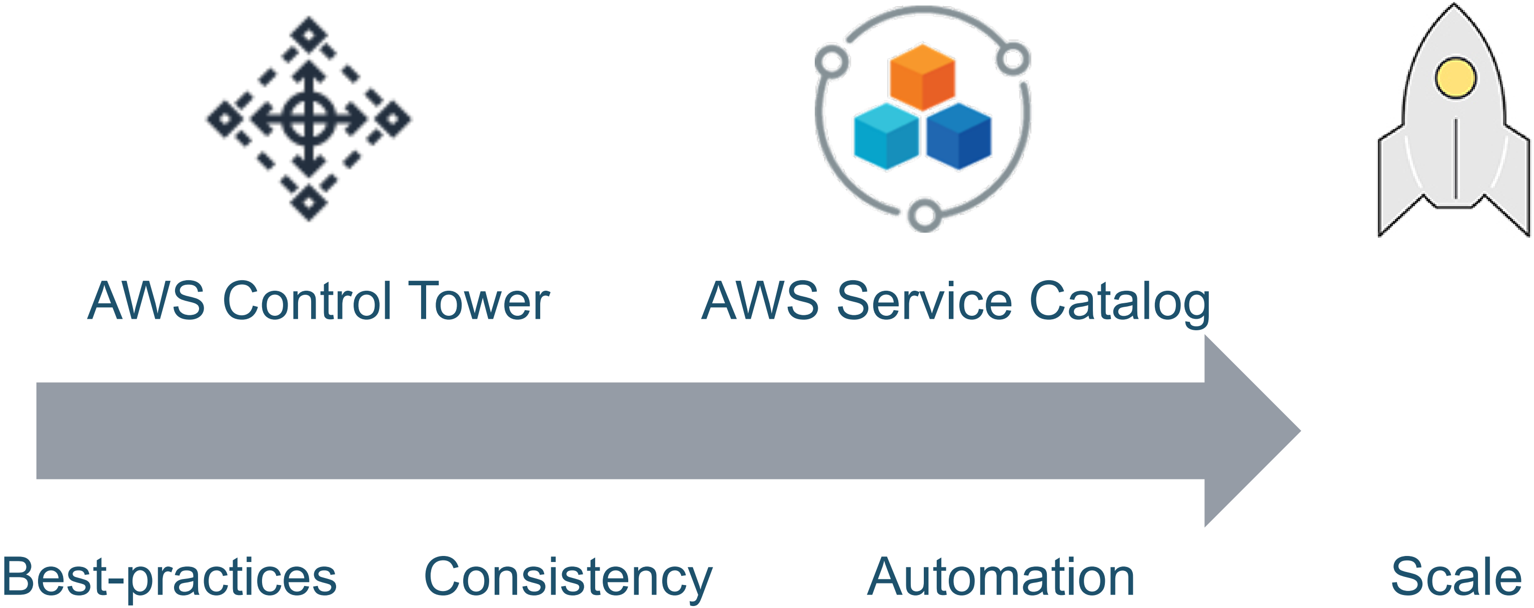
Policy Enforcement

Pre-packaged guardrails to enforce policies or detect violations

Dashboard for Oversight

Continuous visibility into workload compliance with controls

Enterprise Self-Service



AWS Control Tower

AWS Service Catalog

Best-practices

Consistency

Automation

Scale

Key Features / Benefits

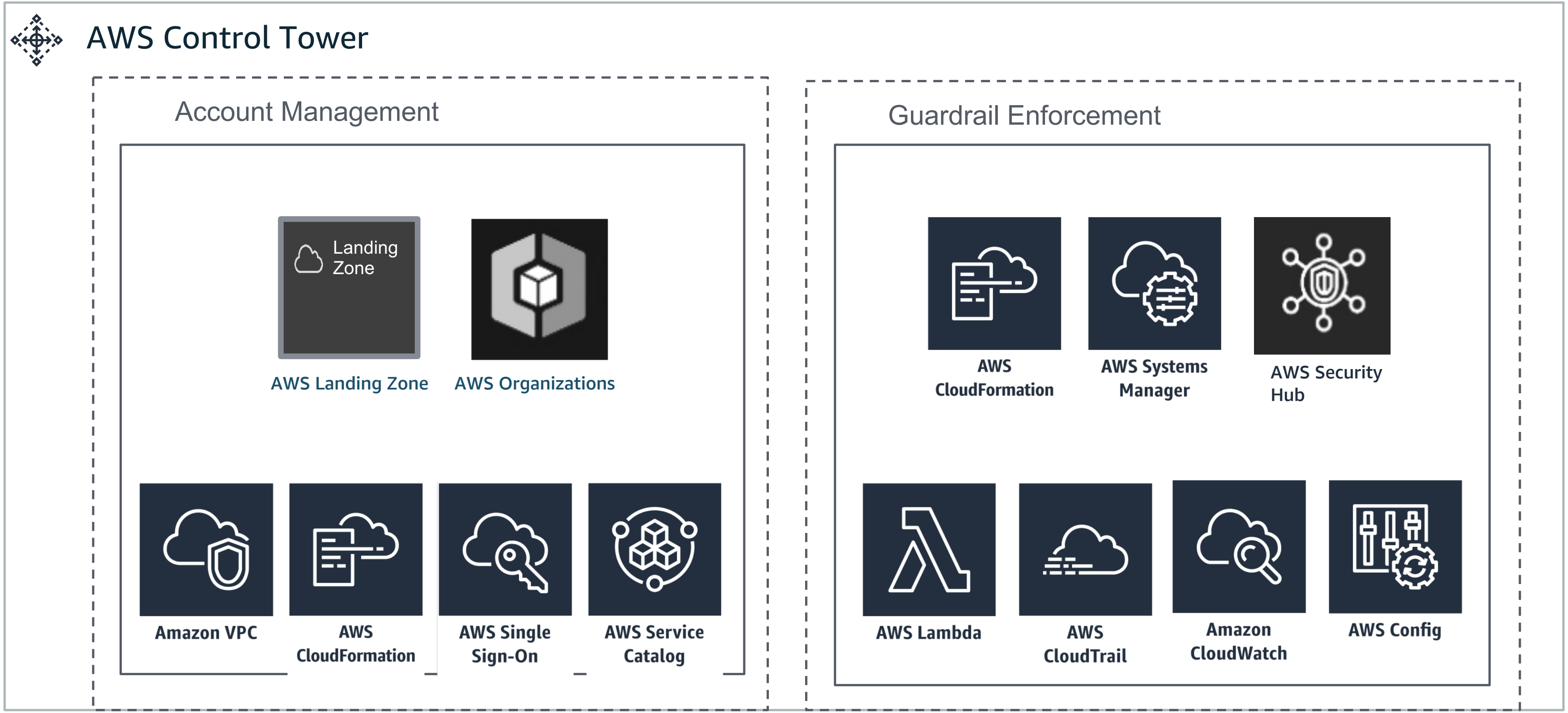
Account Setup

- Automated secure and scalable landing zone
- Multi-account management using AWS Organizations
- Account provisioning wizard
- Central Logging and Multi-account configuration consistency

Guardrails

- Built-in best practices
- Multi-account Preventive and detective guardrails
- Curated rules in plain English
- Easy to use Dashboard and notifications

AWS Service Integration



AWS Control Tower

Account Management

AWS Landing Zone

AWS Organizations

Amazon VPC

AWS CloudFormation

AWS Single Sign-On

AWS Service Catalog

Guardrail Enforcement

AWS CloudFormation

AWS Systems Manager

AWS Security Hub

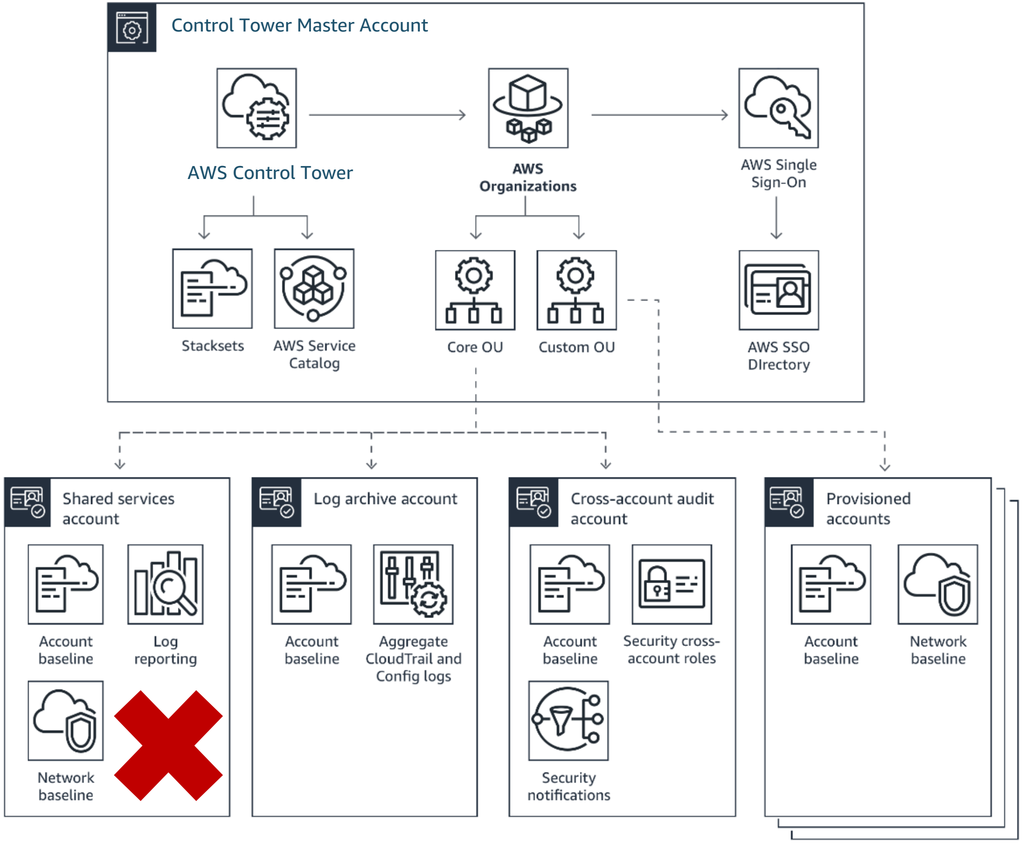
AWS Lambda

AWS CloudTrail

Amazon CloudWatch

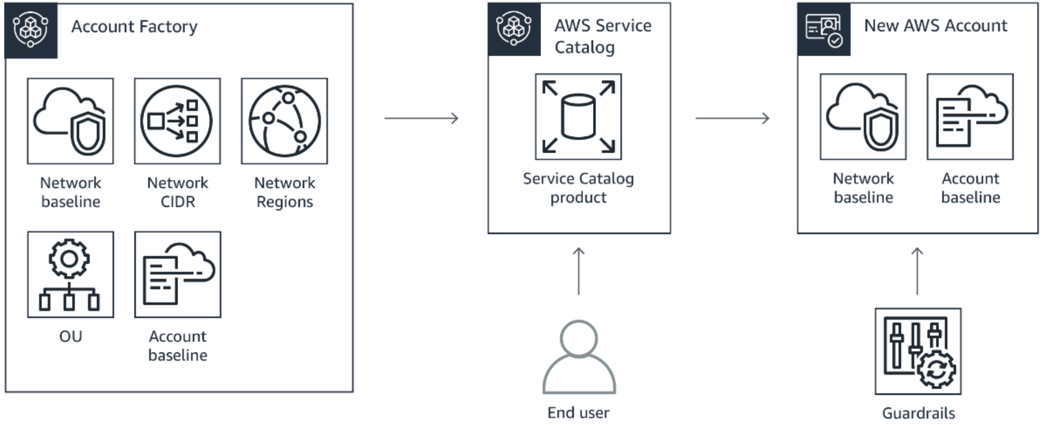
AWS Config

AWS Control Tower’s automated landing zone



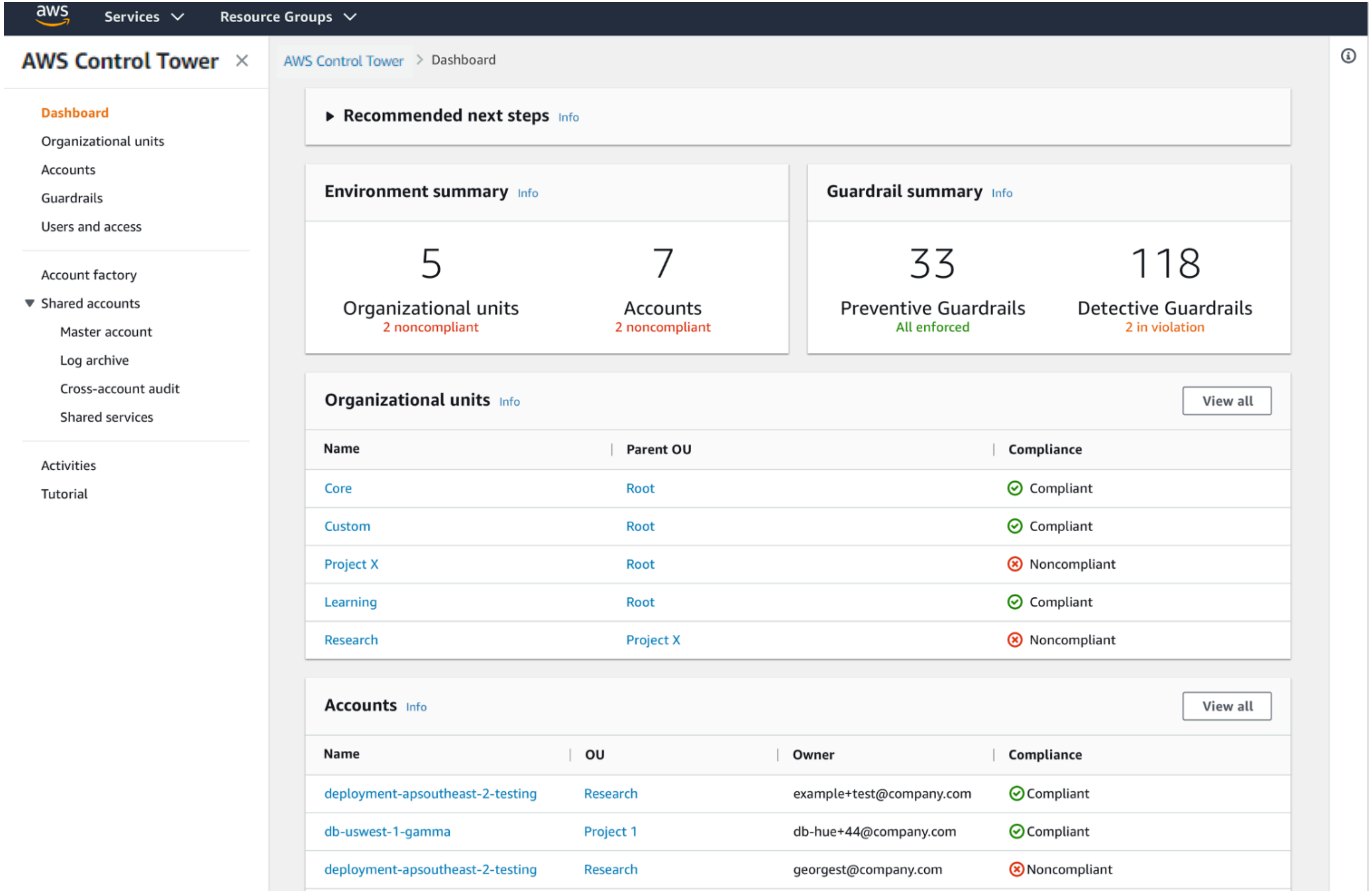
- ✓ AWS Organizations with a master and pre-created accounts for central log archive, cross-account audit, and shared services
- ✓ Pre-configured directory and single sign-on using AWS SSO (with Active Directory custom option)
- ✓ Centralized monitoring and alerts using AWS Config, AWS CloudTrail, and AWS CloudWatch

Account Factory



- Account factory for controls on account provisioning
  - Pre-approved account baselines with VPC options
  - Pre-approved configuration options
- End user configuration and provisioning through AWS Service Catalog
- Creates/updates AWS accounts under organizational units

Dashboard for Oversight



▶ **Recommended next steps** Info

Environment summary Info

5 Organizational units
2 noncompliant

7 Accounts
2 noncompliant

Guardrail summary Info

33 Preventive Guardrails
All enforced

118 Detective Guardrails
2 in violation

Organizational units Info

Name	Parent OU	Compliance
Core	Root	✓ Compliant
Custom	Root	✓ Compliant
Project X	Root	✗ Noncompliant
Learning	Root	✓ Compliant
Research	Project X	✗ Noncompliant

Accounts Info

Name	OU	Owner	Compliance
deployment-apsoutheast-2-testing	Research	example+test@company.com	✓ Compliant
db-uswest-1-gamma	Project 1	db-hue+44@company.com	✓ Compliant
deployment-apsoutheast-2-testing	Research	georgest@company.com	✗ Noncompliant

Control Tower ALZ Parity

ALZ – CT Feature Parity

	AWS Landing Zone V 2.x	AWS Control Tower @ GA
Region deployment / Reach	All regions except China and GovCloud	Four regions at launch: us-east-1, us-east-2, us-west-2, eu-west-1
Ability to add or configure custom blueprints and guardrails	Customer can create and configure custom blueprints and guardrails	Fixed blueprints and 30 guardrails at GA.
SSO Integration Options	High: Ability to integrate with existing SSO providers or user directories	Low: Only supports AWS SSO Directory with preconfigured permission sets and Service Catalog roles
Ability to integrate 3rd party products	High: Ability to integrate with ISV products through ALZ add-ons	Not Possible: No ability to customize blueprints or guardrails

ALZ – CT Feature Parity

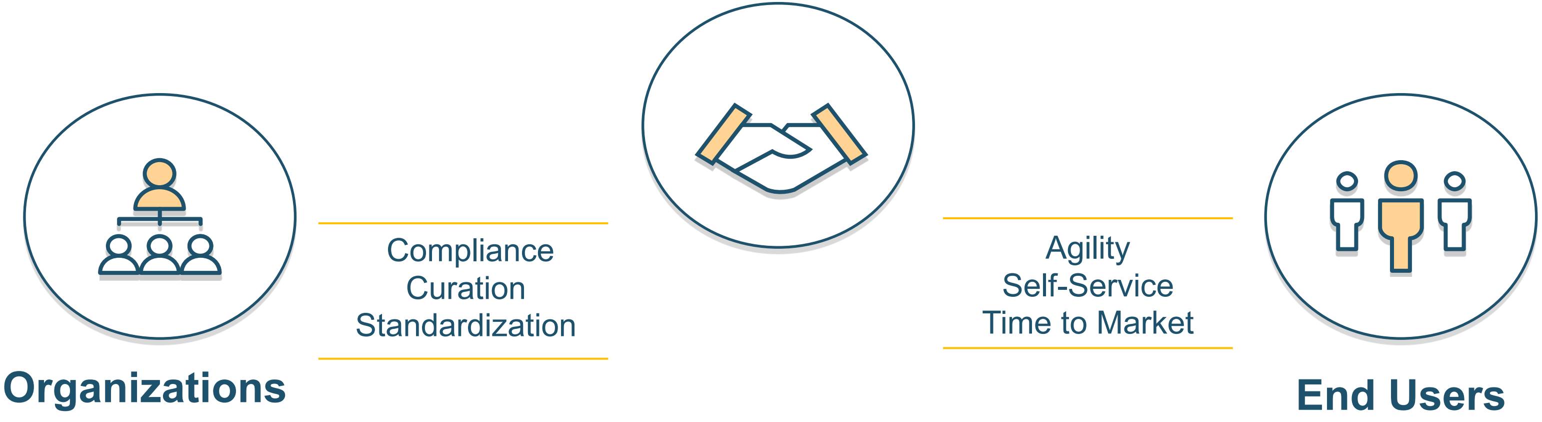
	AWS Landing Zone V 2.x	AWS Control Tower @ GA
Multi-account structure design	Complete flexibility to define and implement custom mullti-account structure. Out-of-the-box confiugration of three core accounts: Shared Services, Security and Logging with VPC in Shared Services account and optional network peering to VPC created via AVM	Two core accounts: Cross account audit and Log archive accounts.. Can create VPC with account factory
Ease of use	Low: Manual CFN deployment and requires expertise with Lambda, configuration files, etc. SA, Partner or ProServe involvement for initial deployment is highly recommended	High: Self-service: Guided deployment and guardrails can be activated in the AWS console
Migration of earlier solutions	N/A	CT will support new implementations only
Ability to deploy to an existing Organization	Yes, with care	Not possible
Nested OU support	Yes (starting in May)	NA

Thank you!

Control Tower Roadmap

- GA Q2 2019
  - Expanded set of guardrails
  - Support for Microsoft Active Directory and other SSO options
  - Integration with AWS Security Hub for security and compliance insights
- Q4 2019*
  - Upgrade from LZ 2.0 to CT
  - Deploy to a current running organization
  - Flexibility with core accounts
  - Custom blueprints will support integration with 3rd party SS0 providers.

Service Catalog: Simplifying Provisioning



Organizations

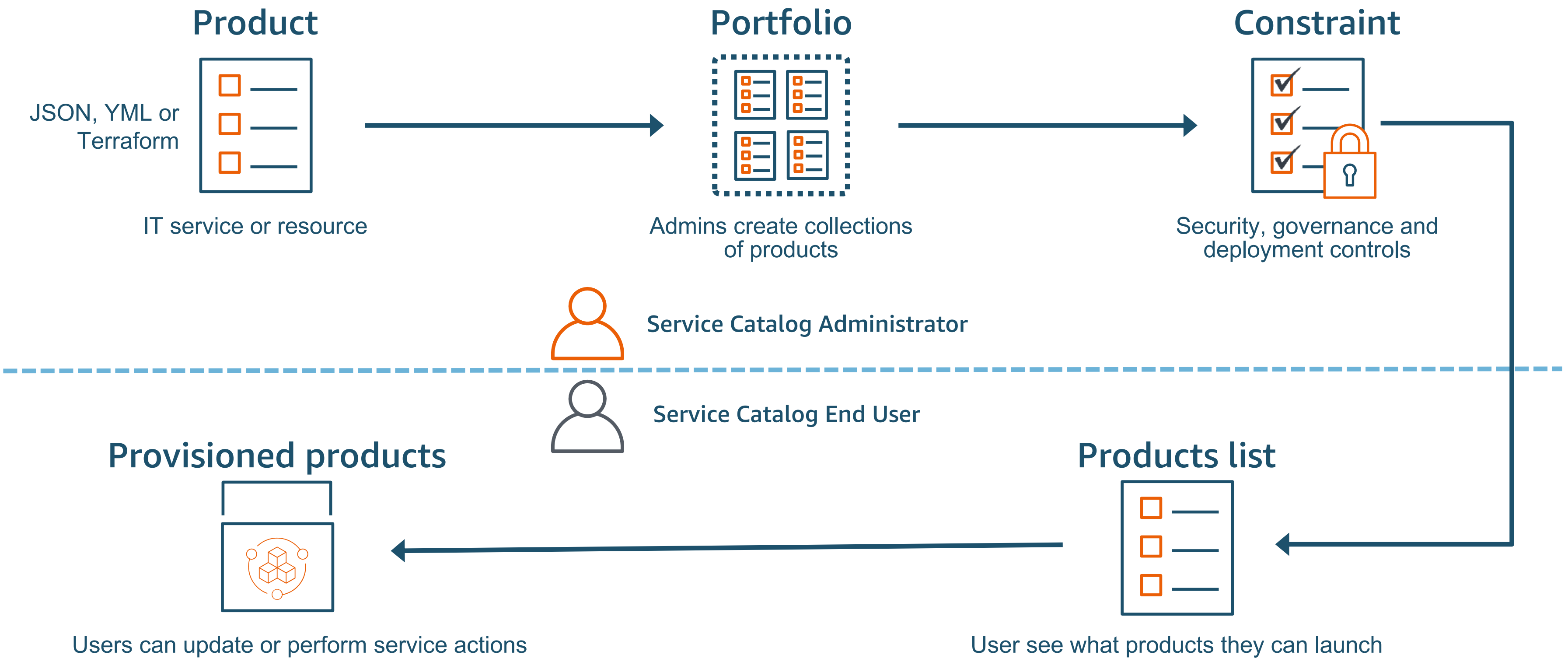
Compliance
Curation
Standardization

Agility
Self-Service
Time to Market

End Users

AWS Service Catalog allows organizations to create and manage catalogs of IT services and software on AWS. Users can quickly deploy approved IT services in a self-service manner.

Service Catalog: Simplifying Provisioning



Product

JSON, YML or
Terraform

IT service or resource

Portfolio

Admins create collections of products

Constraint

Security, governance and deployment controls

Service Catalog Administrator

Service Catalog End User

Provisioned products

Users can update or perform service actions

Products list

User see what products they can launch

Thank You!

Automated AWS Setup

- Automated “**landing zone”**, a pre-configured, secure, scalable, multi-account AWS environment based on best-practices blueprints
- Automated setup with a single click
- Multi-account management using AWS Organizations
- Built-in Account Factory to pre-configure network design, deployment regions, network configuration
- Identity and federated access management using AWS SSO and Microsoft AD (coming soon)
- End-user account provisioning through AWS Service Catalog
- Pre-configured architectures for centralized log archive, cross-account security audits, and configuration monitoring
- Options for customization