
AWS
re:Invent

ARC211

Build governance at scale with AWS Control Tower

Matheus Arrais
Partner Solutions Architect
AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Governance and agility

Overview AWS Control Tower

Landing zone

Multi-account strategy

Lifecycle events and customization

Customer journey



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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 and compliant

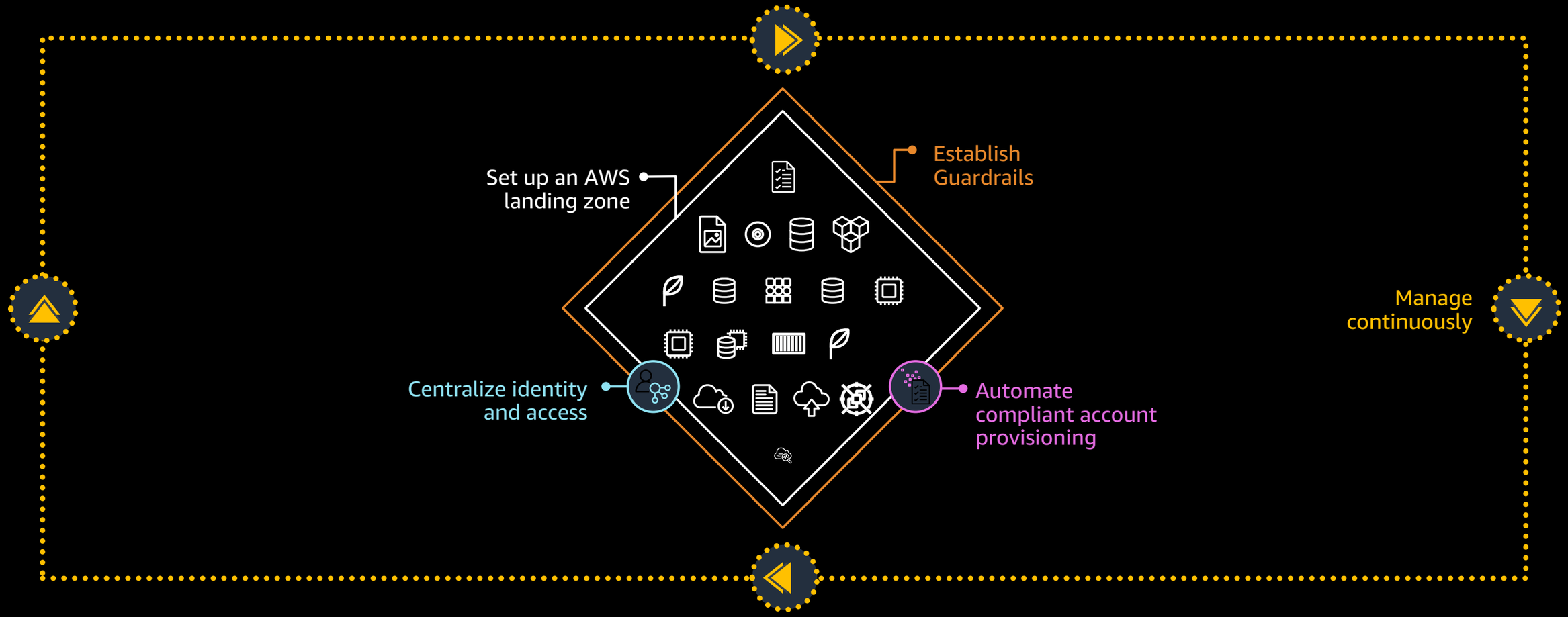
Operations and spend management

Why use AWS Control Tower?

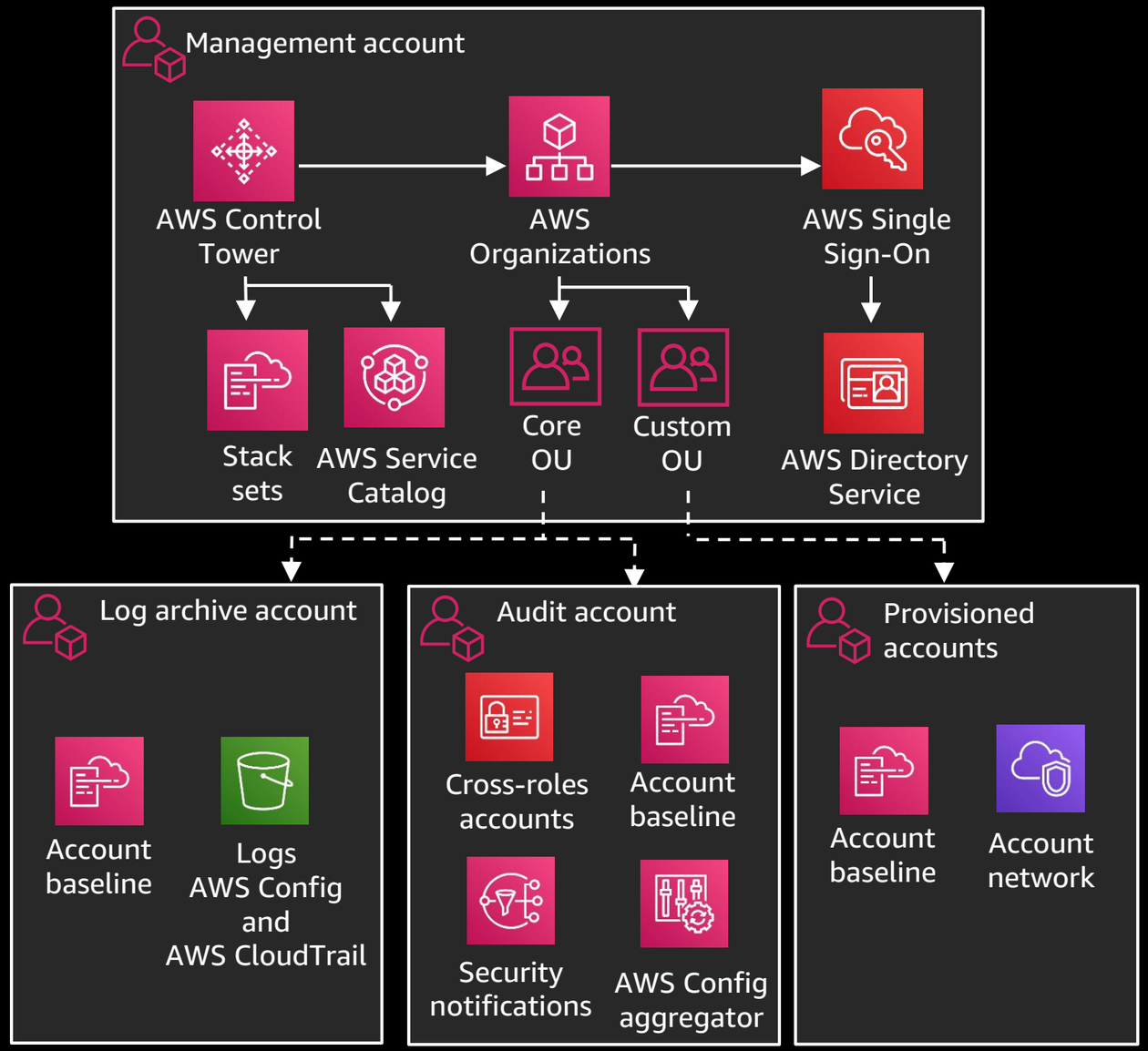


- Set up a best-practices AWS environment in a few clicks
- Standardize account provisioning
- Centralize policy management
- Enforce governance and compliance proactively
- Enable end user self-service
- Get continuous visibility into your AWS environment
- Gain peace of mind

Enable governance at scale

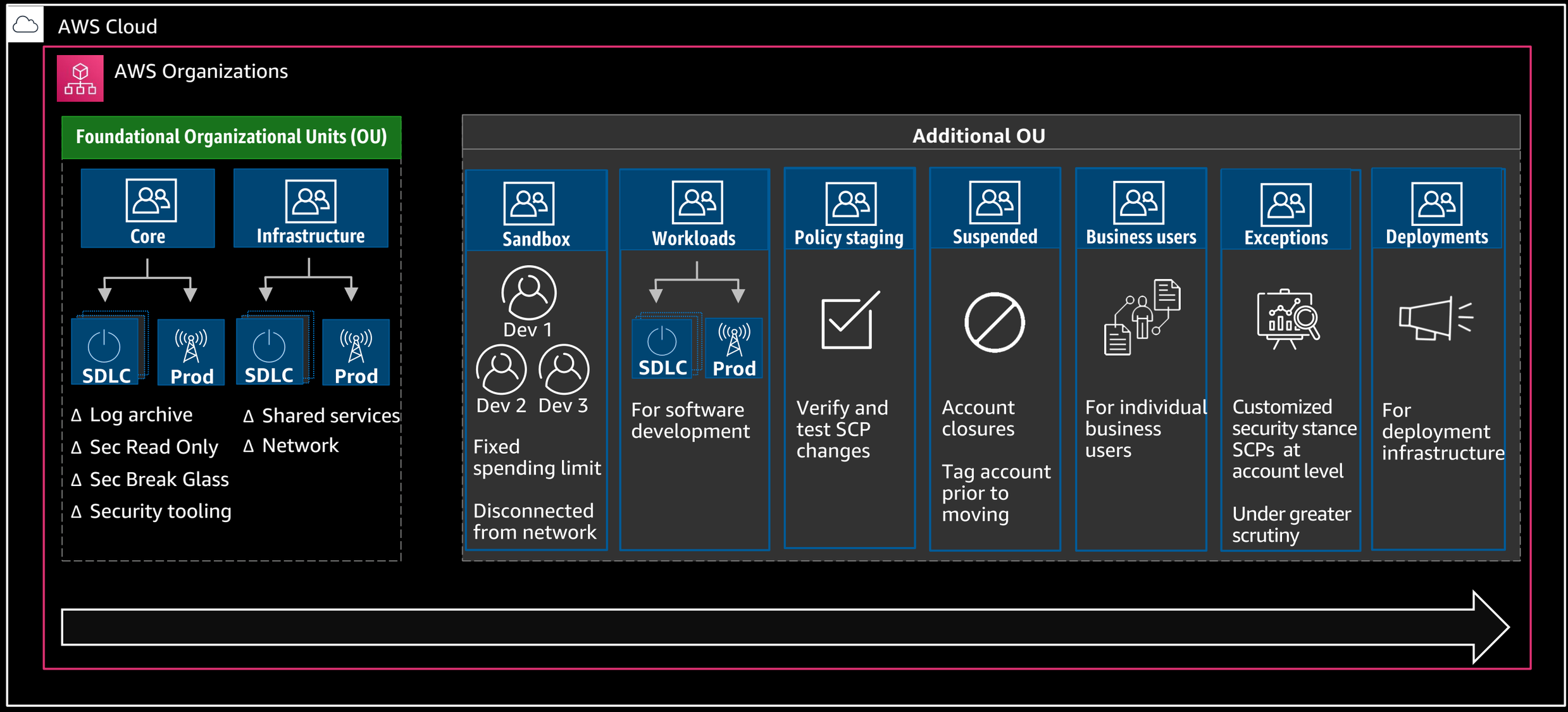


Set up an AWS landing zone

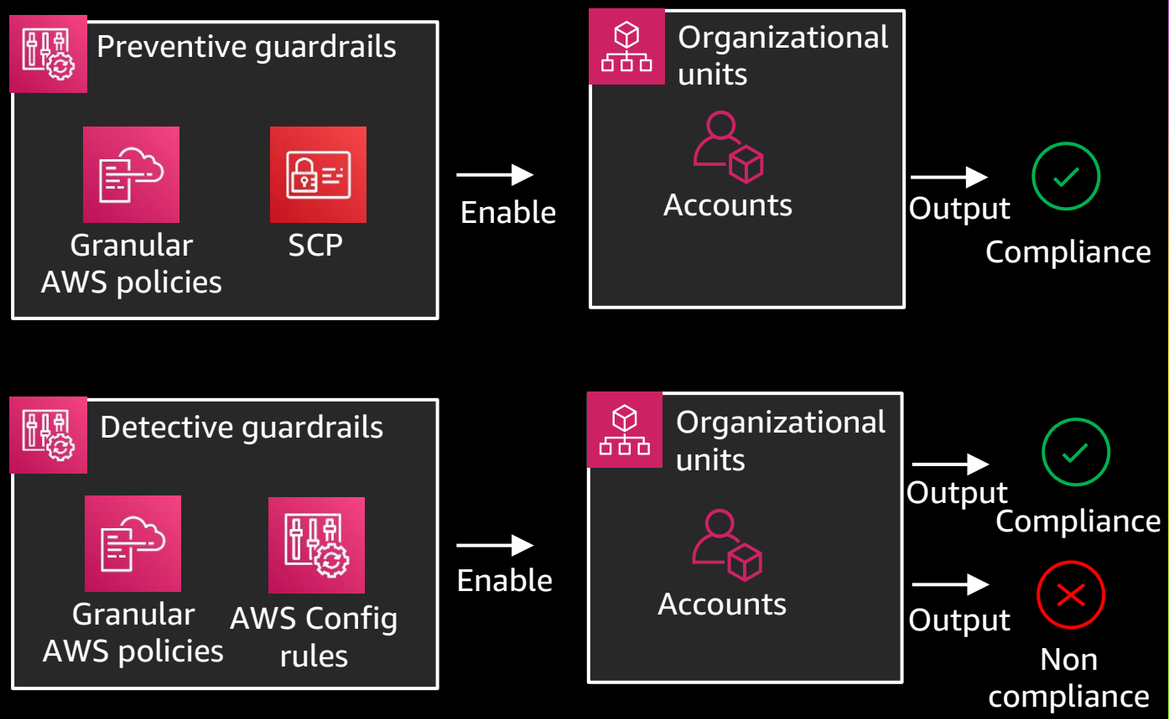


- Landing zone – A preconfigured, secure, scalable, multi-account AWS environment based on best-practice blueprints
- Multi-account management using AWS Organizations
- Identity and federated access management using AWS SSO
- Centralized log archive using AWS CloudTrail and AWS Config
- Cross-account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

Extend AWS Control Tower to align to multi-account framework

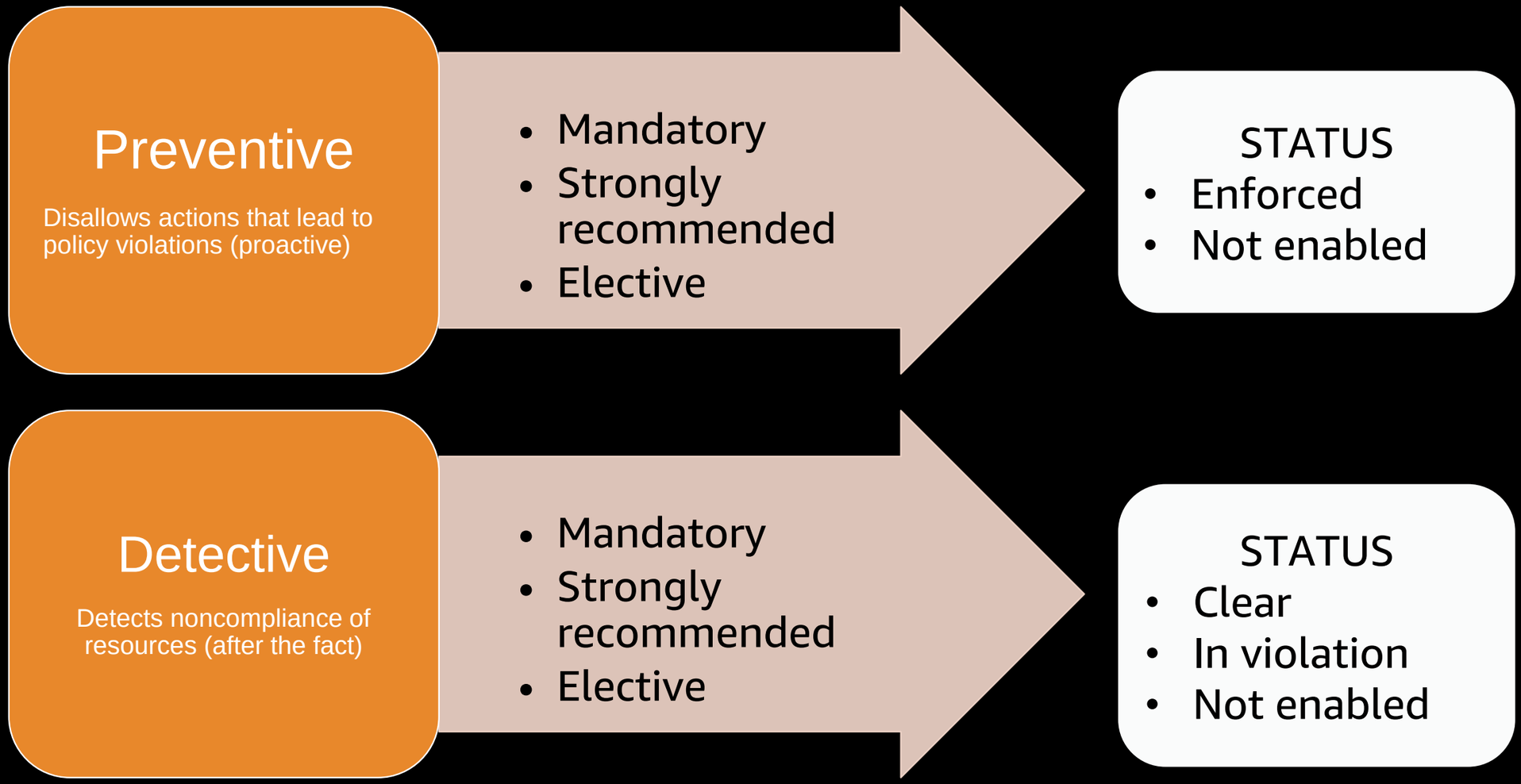


Establish guardrails



- 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

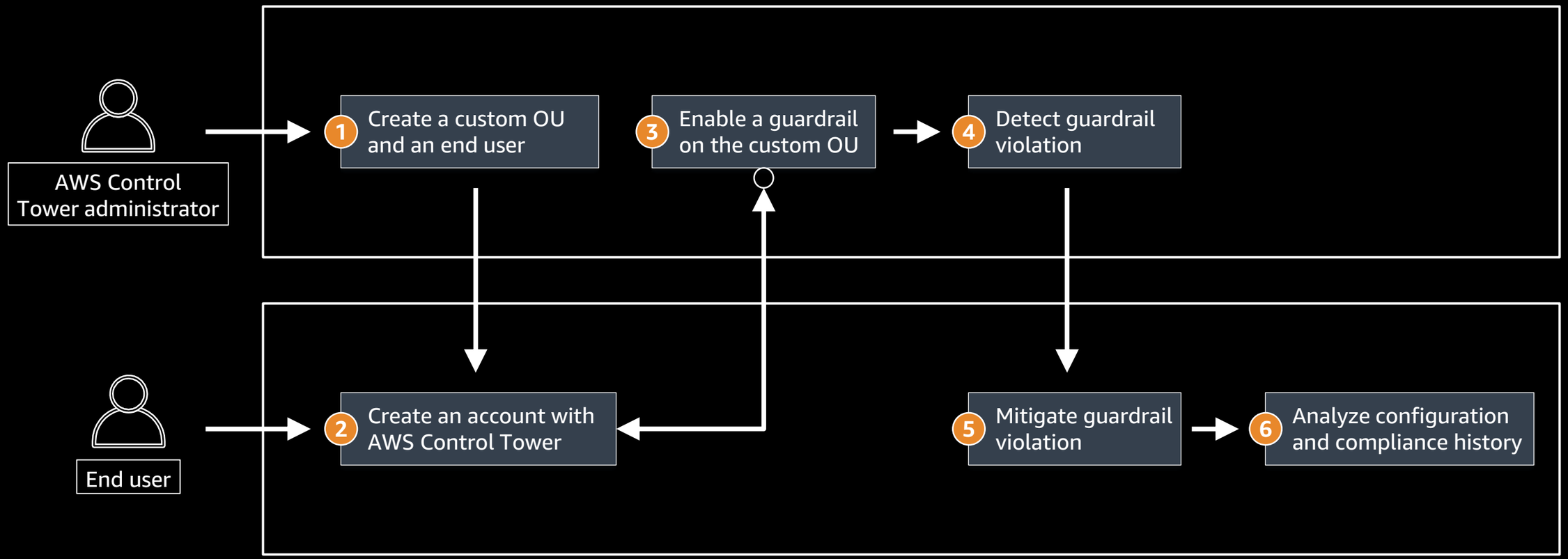
AWS Control Tower guardrails



Guardrail examples

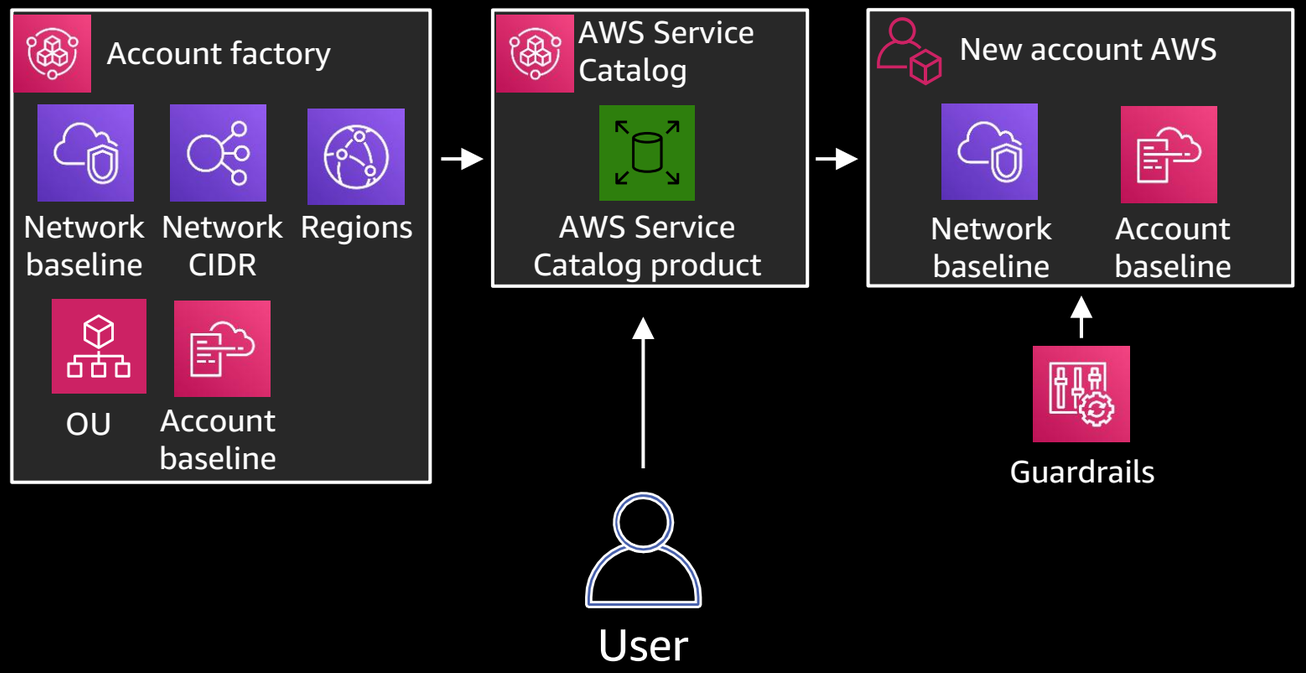
Goal/category	Example
IAM security	Require MFA for root user
Data security	Disallow public read access to Amazon S3 buckets
Network security	Disallow internet connection via Remote Desktop Protocol (RDP)
Audit logs	Enable AWS CloudTrail and AWS Config
Monitoring	Enable AWS CloudTrail integration with 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

Detect and mitigate guardrail violations



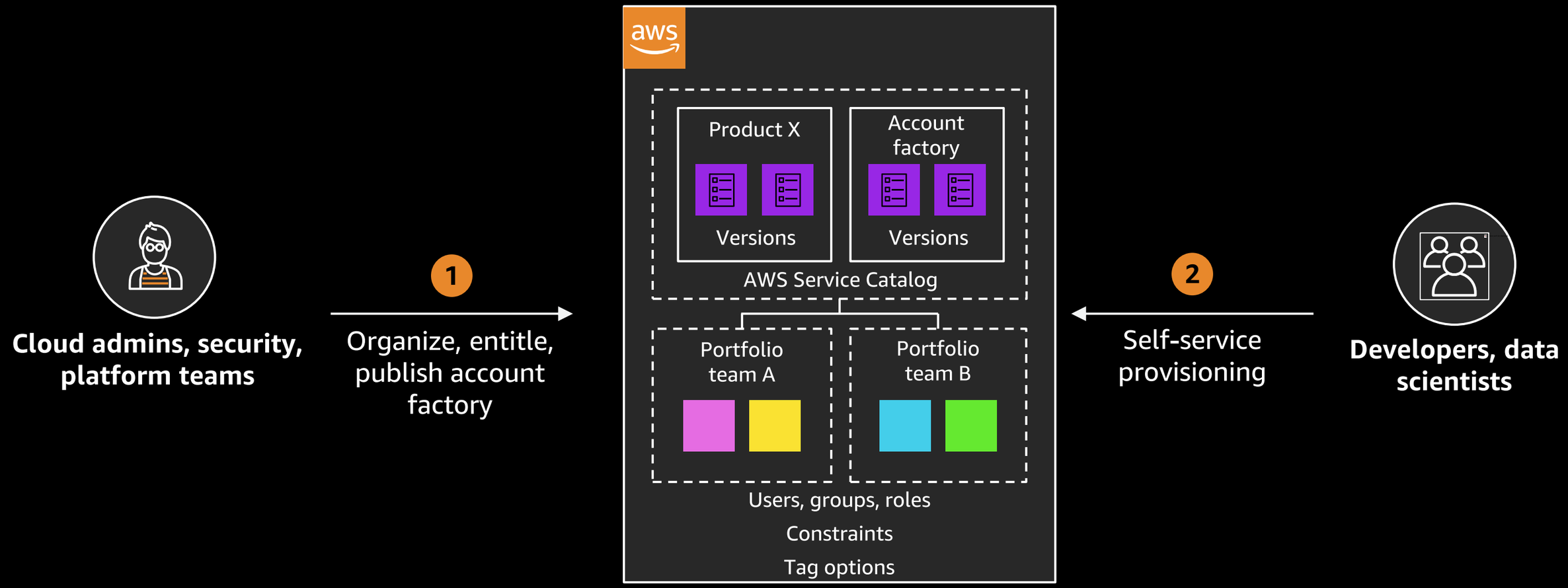
Reference: **https://tinyurl.com/y56dsalz**

Automate compliant account provisioning

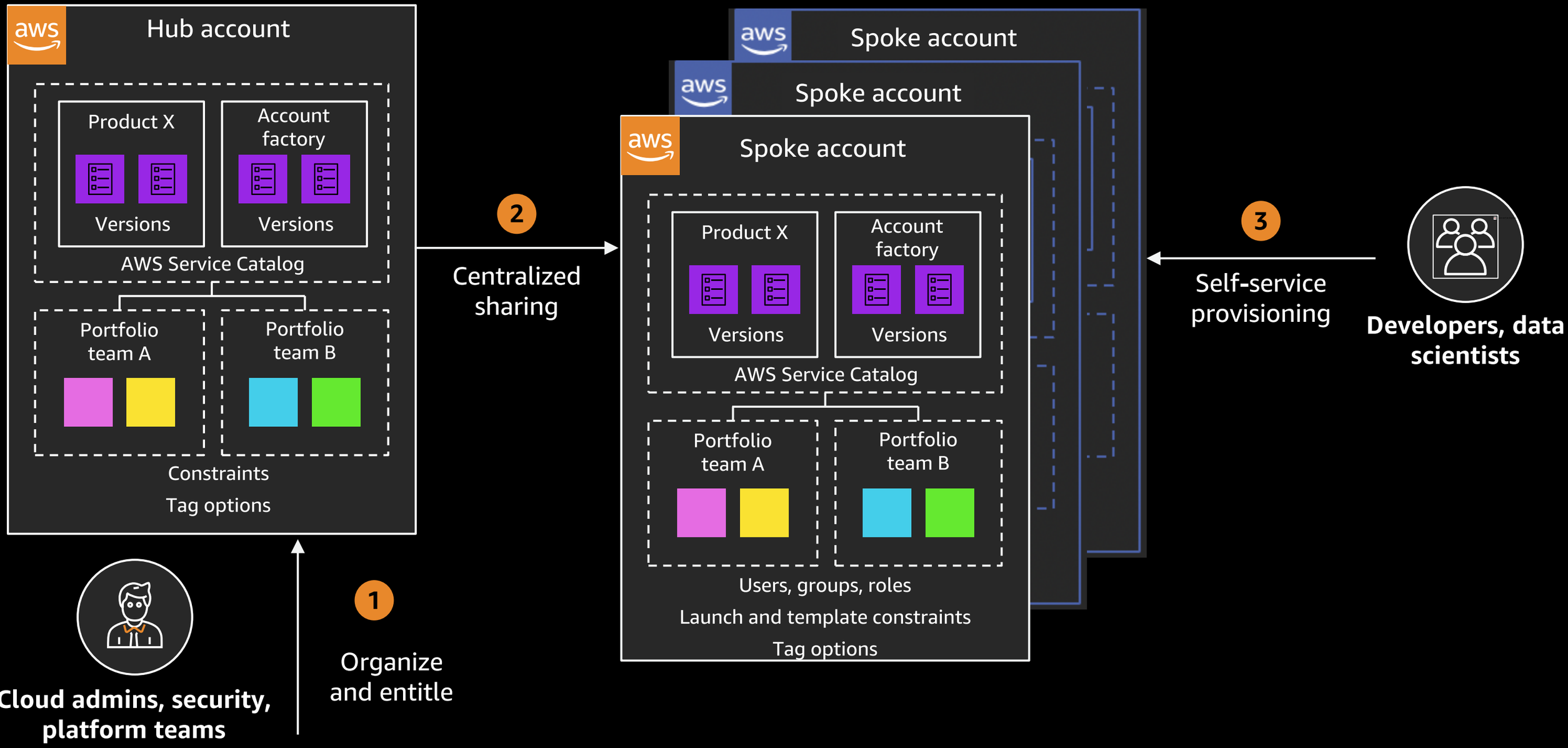


- Built-in account factory provides a template to standardize account provisioning
- Configurable network settings (e.g., subnets, IP addresses)
- Automatic enforcement of account baselines and guardrails
- Published to AWS Service Catalog

Enable self-service with AWS Service Catalog



Automate governance at scale



Benefits of governance at scale



Security

Curation
Compliance
Standardization

Speed

Agility
Self-service
Time to market



Organizations

AWS Service Catalog enables organizations to deploy and manage infrastructure and applications that reflect the organization's security and operational policies



End users

Operate with agility and control

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

Operate with agility and control



Monitor resources and applications
Amazon CloudWatch

Audit user activity and resource configurations
Amazon CloudTrail
AWS Config

Manage resources and take operational action
AWS Systems Manager

Optimize to reduce cost and improve security posture
AWS Trusted Advisor
AWS Cost and Usage Report
AWS Cost Explorer
AWS Budgets

Lifecycle events

Benefits

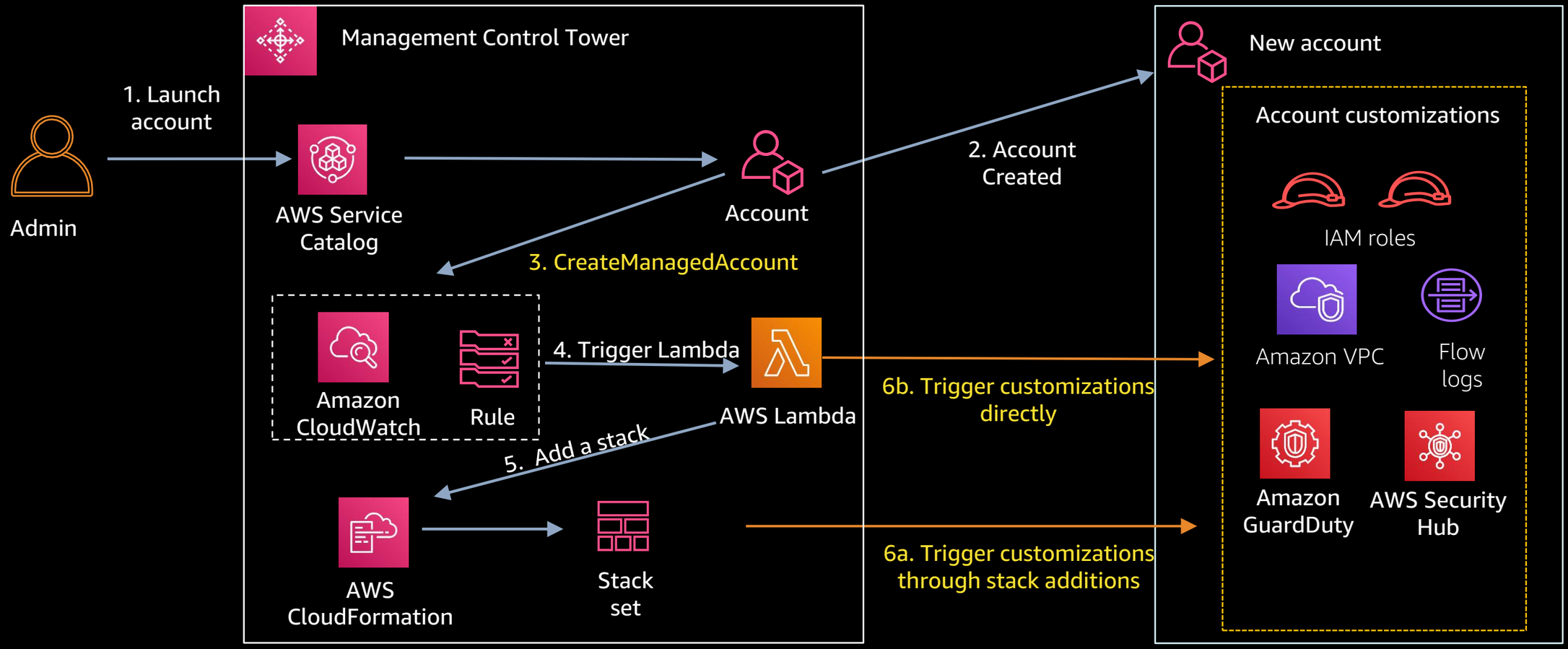
- Amazon EventBridge integration
- Operation status

Events supported

- CreateManagedAccount
- UpdateManagedAccount
- EnableGuardrail
- DisableGuardrail
- SetupLandingZone
- UpdateLandingZone
- RegisterOrganizationalUnit
- DeregisterOrganizationalUnit

Configure with AWS Control Tower lifecycle events

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



Customer journey to the cloud

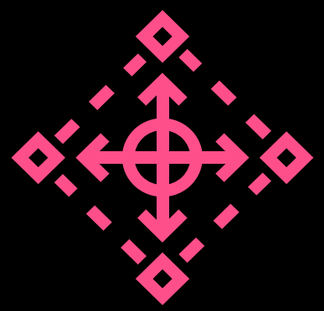
Implementation

Identity and network

Security

Monitoring and insights

Innovation



onelogin

aviatrix

ALERT LOGIC

CROWDSTRIKE

tenable

TREND MICRO

CHECK POINT CloudGuard

logz.io

New Relic

splunk>

sumo logic

Reference: https://tinyurl.com/CTMarketplace

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

How do I get started?



Management & Governance AWS Blog



AWS Control Tower Getting Started



AWS Organizations Getting Started

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

AWS Control Tower blogs:

- Guardrail mitigation: **https://tinyurl.com/y56dsalz**
- Enroll existing accounts: **https://tinyurl.com/y3stlxvo**
- Using AWS Config conformance packs for Control Tower guardrail modeling: **https://tinyurl.com/CTModeler**
- Enabling Amazon GuardDuty in AWS Control Tower: **https://tinyurl.com/CTGuardDuty**

How-to videos (management and governance):
https://tinyurl.com/y3yeohkm

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.