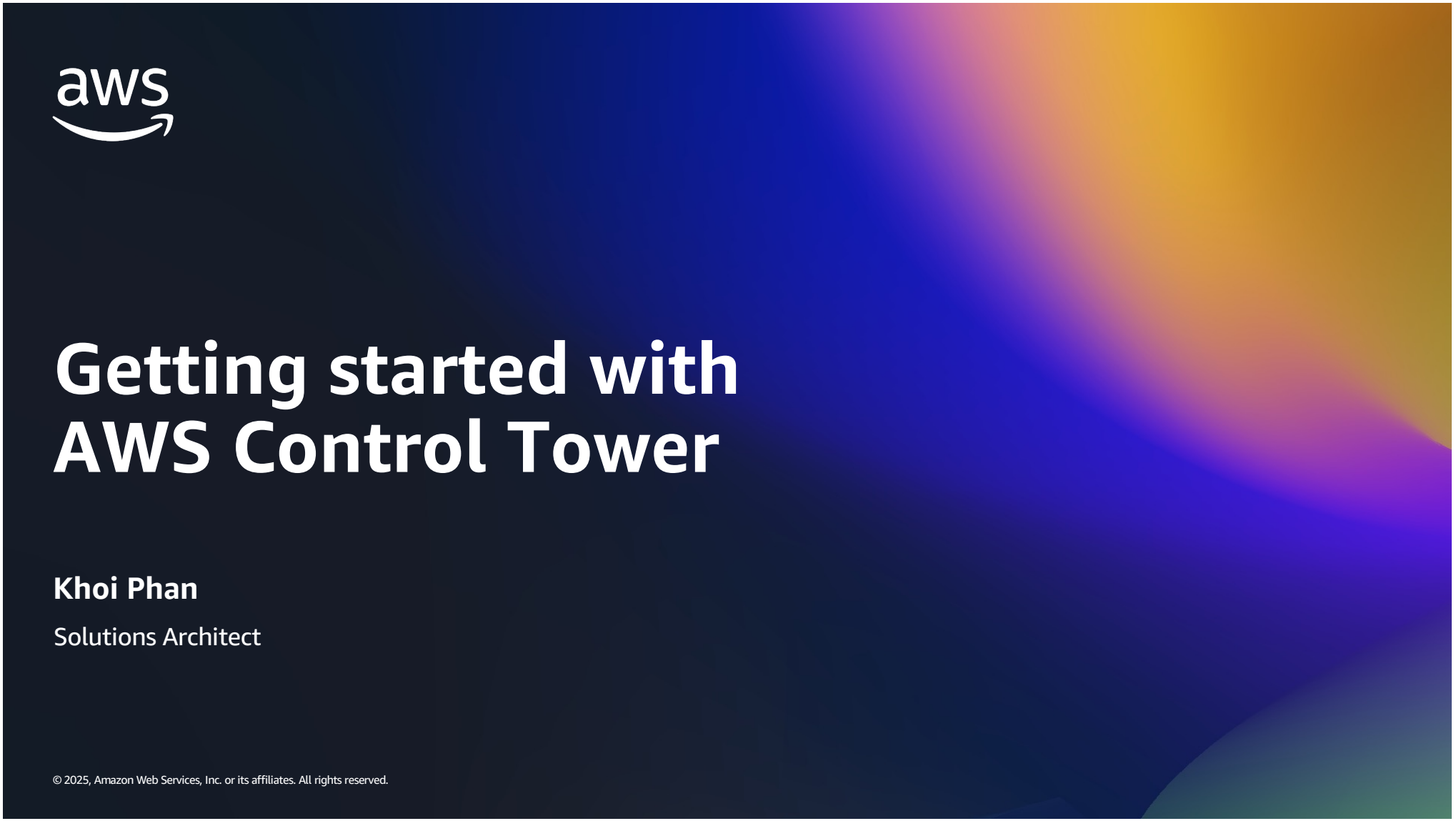


Getting started with AWS Control Tower

Khoi Phan

Solutions Architect

Business agility and governance control

Governance

Security

Compliance

Operations

Spend management

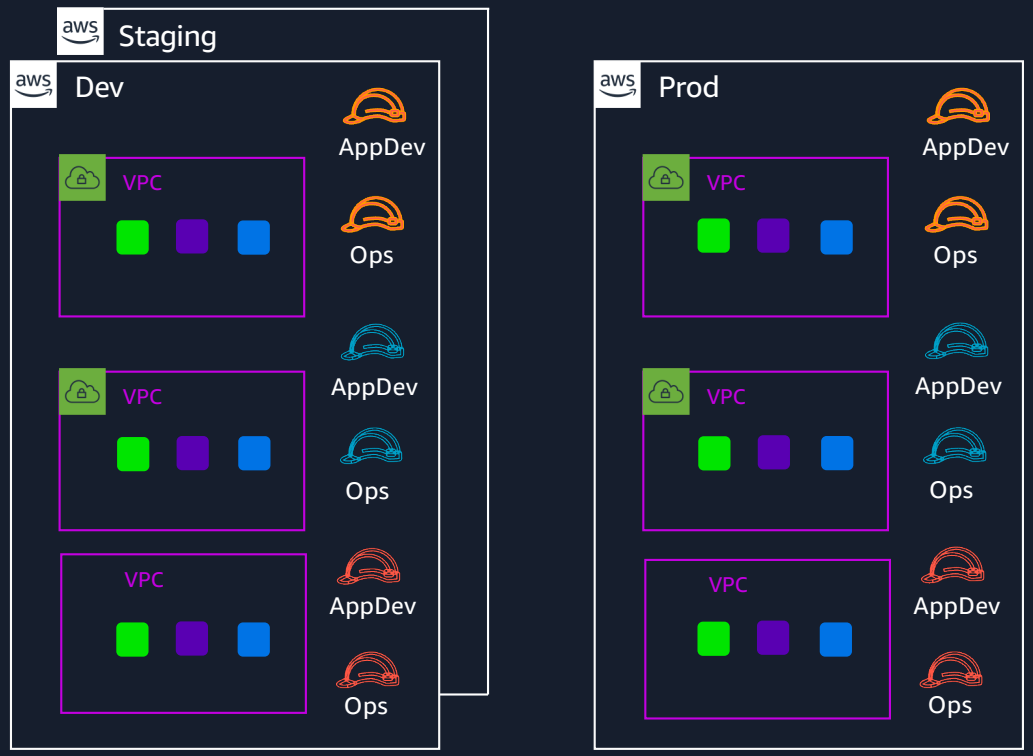
Agility

Self-service access

Experiment fast

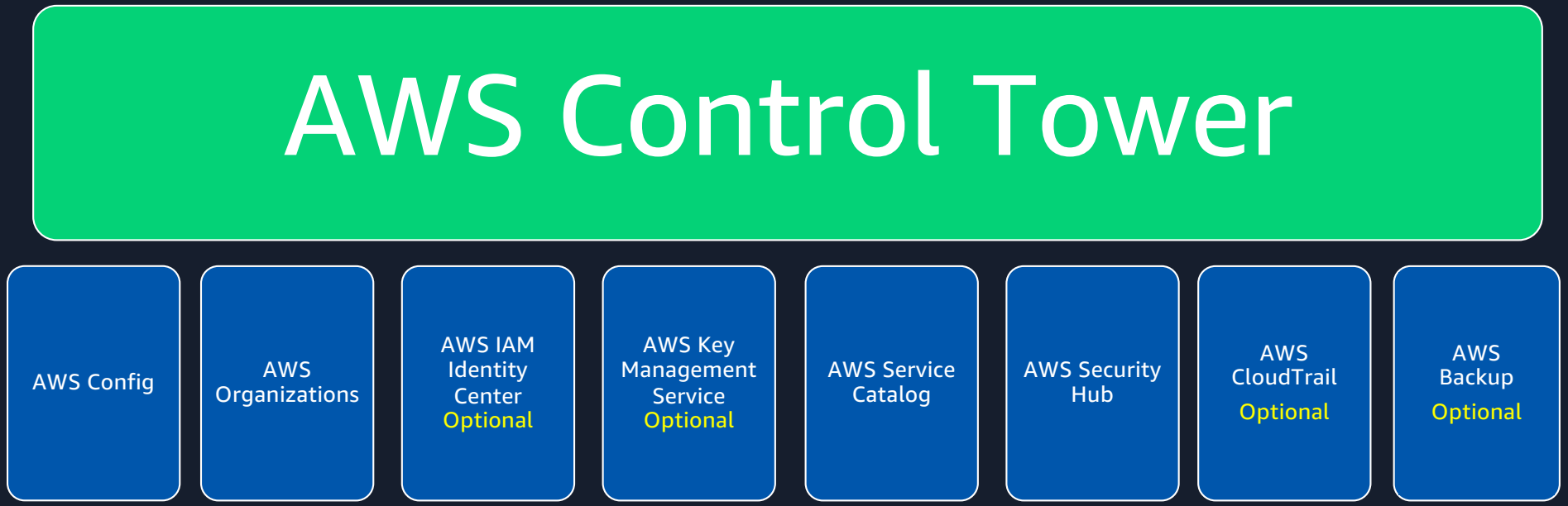
Respond quickly
to change

A common starting point



- Complicated and messy over time
- “Grey” boundaries
- Difficult to track resources
- Step on each other’s toes

What is AWS Control Tower?



Why use AWS Control Tower

Automatically create a landing zone via the console or with APIs

Establish a foundational environment on AWS

Automate account provisioning

Programmatically manage 500+ controls out of the box with APIs

AWS Control Tower - Benefits

Automated landing zone with best practice configurations

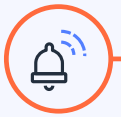
AWS best practice controls for policy management

Account factory for account provisioning

Dashboard for visibility and actions

Built-in identity and access management (IAM)

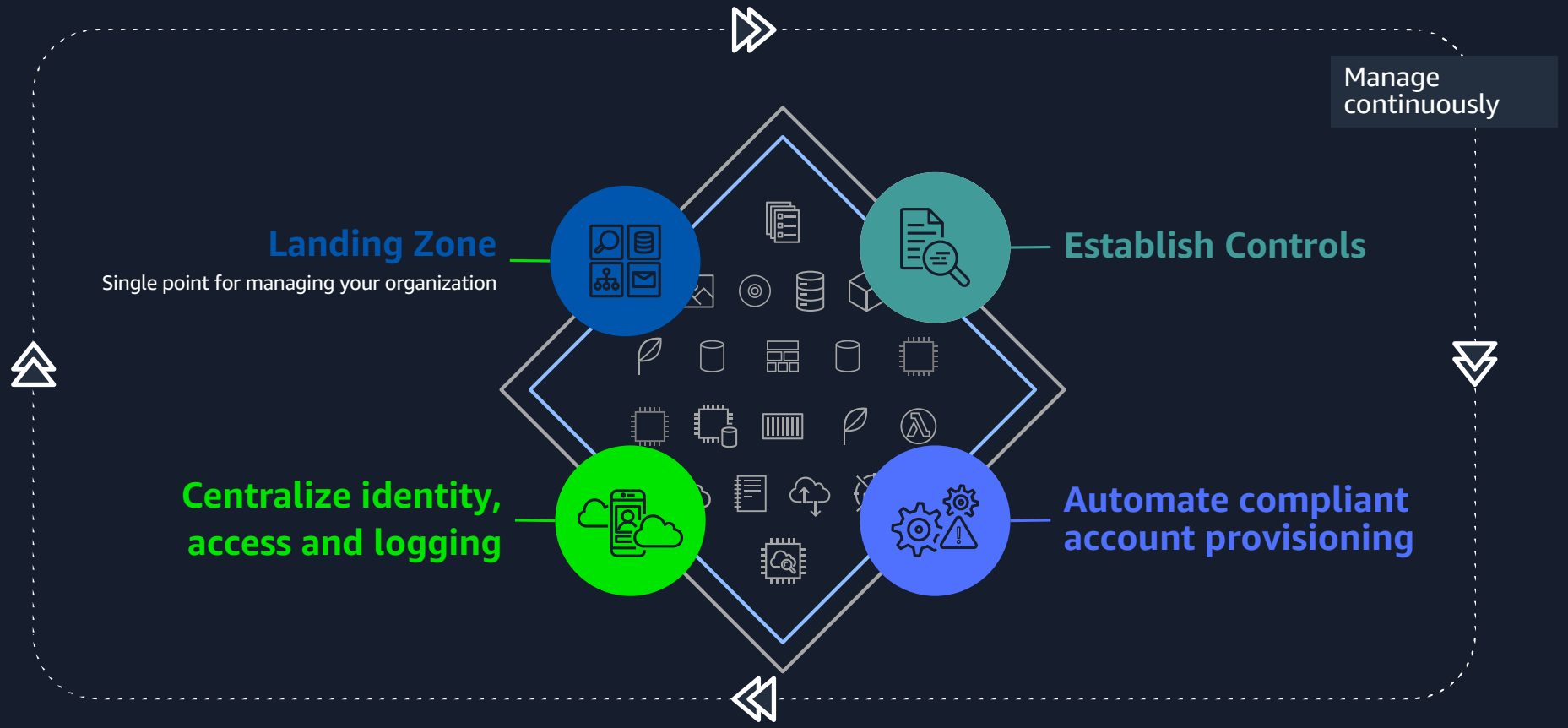
Preconfigured log archive and audit access to accounts



Built-in monitoring and notifications

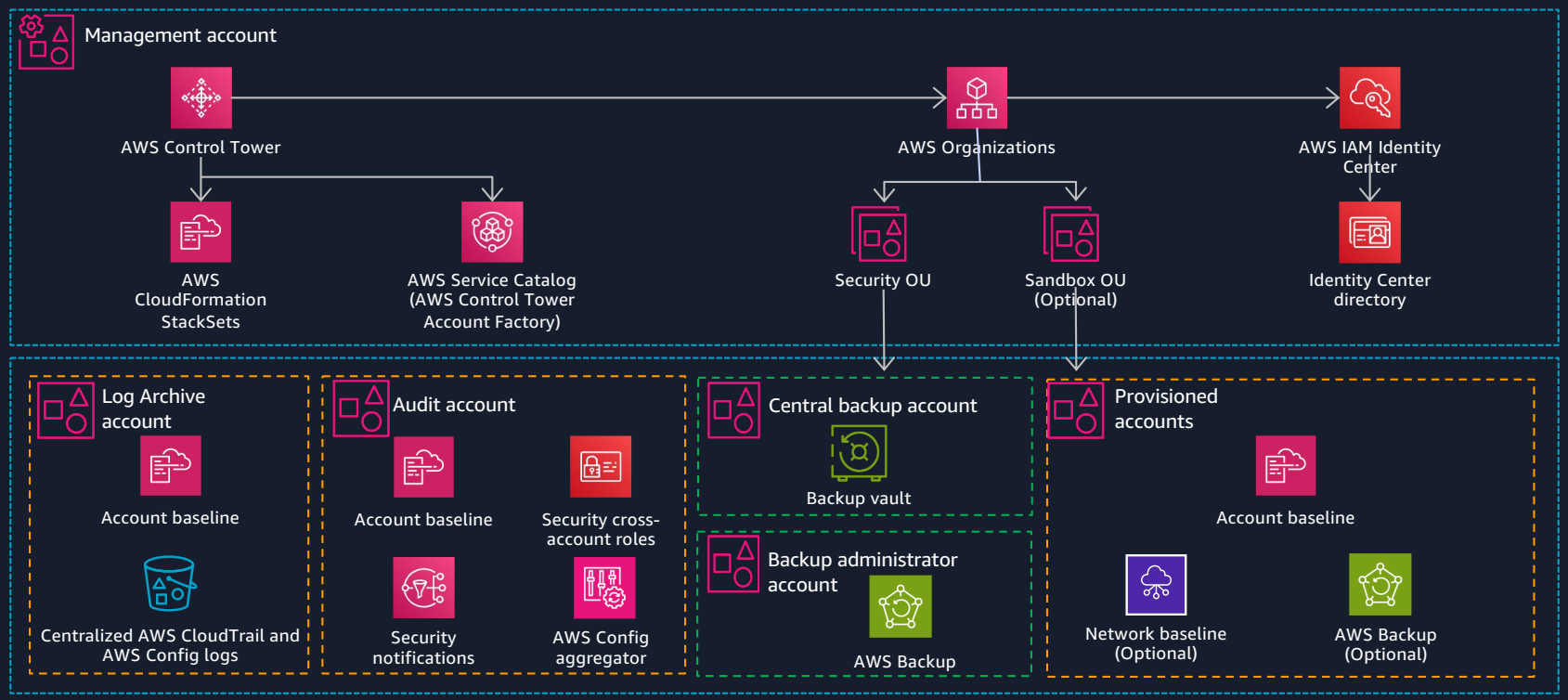
Extensible with third-party ISV solutions available via AWS Marketplace

AWS Control Tower: Enabling agility and governance



AWS Control Tower Architecture

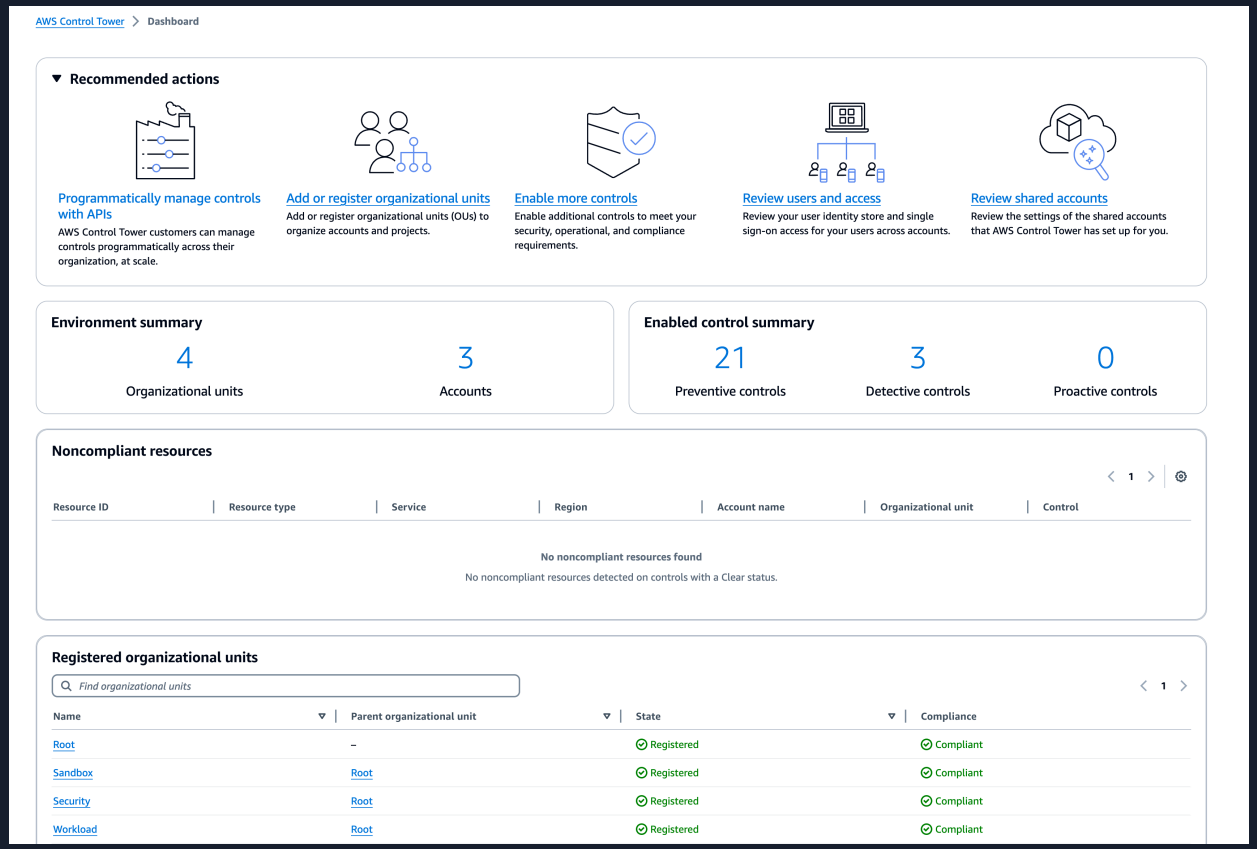
Architecture Overview



Available Landing Zone APIs

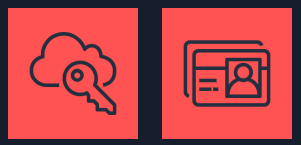
- CreateLandingZone
- GetLandingZoneOperation
- GetLandingZone
- UpdateLandingZone
- ListLandingZones
- ResetLandingZone
- DeleteLandingZone
- ListLandingZoneOperations

Dashboard for oversight



Centralized Identity and Access, Logging & Monitoring, and Data Protection

Automatically set-up Identity Center

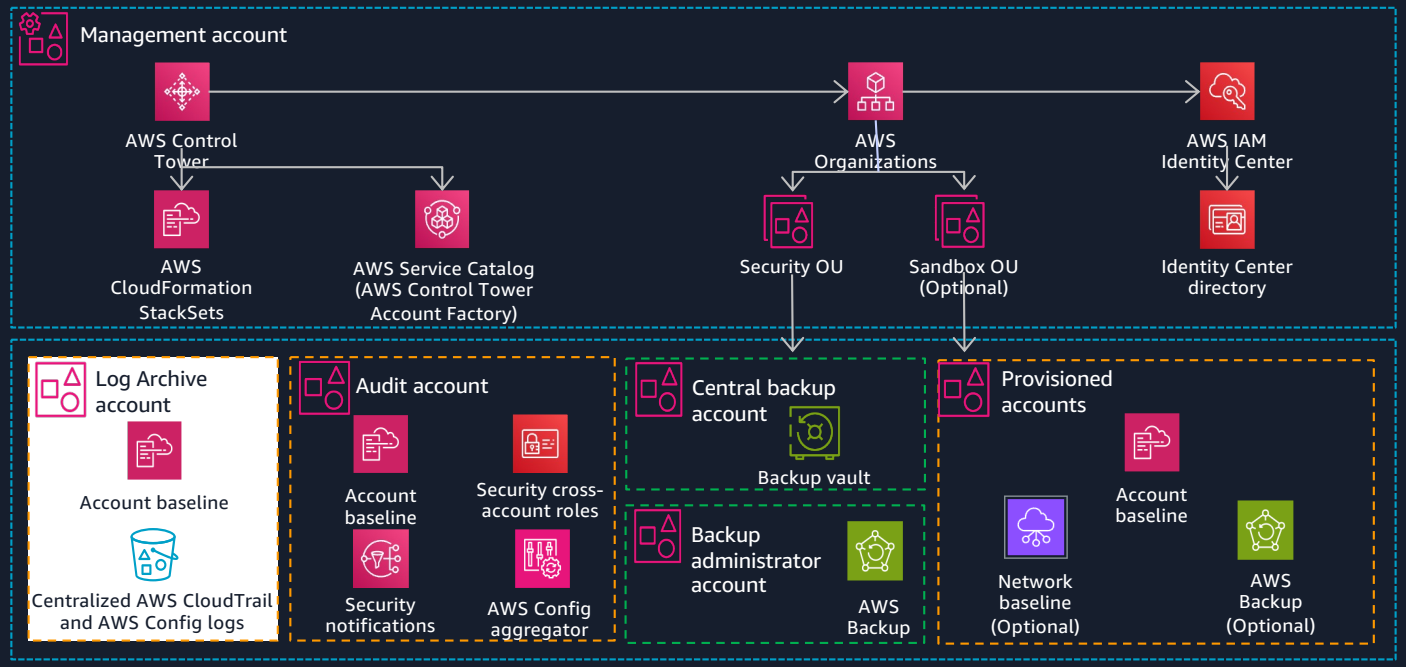


- AWS IAM Identity Center provides default directory for identity
- AWS IAM Identity Center also allows federated access management across all accounts in your organization
- Preconfigured groups (such as AWS Control Tower administrators, auditors and AWS Service Catalog end users)
- Preconfigured permission sets (e.g., admin, read-only, write)
- AWS IAM Identity Center integrates with third-party IDP (Microsoft Azure AD, Ping, Okta)

Log Archive Account

A DEDICATED ACCOUNT FOR SECURELY STORING LOGS FOR ARCHIVING AND FORENSIC ACTIVITIES.

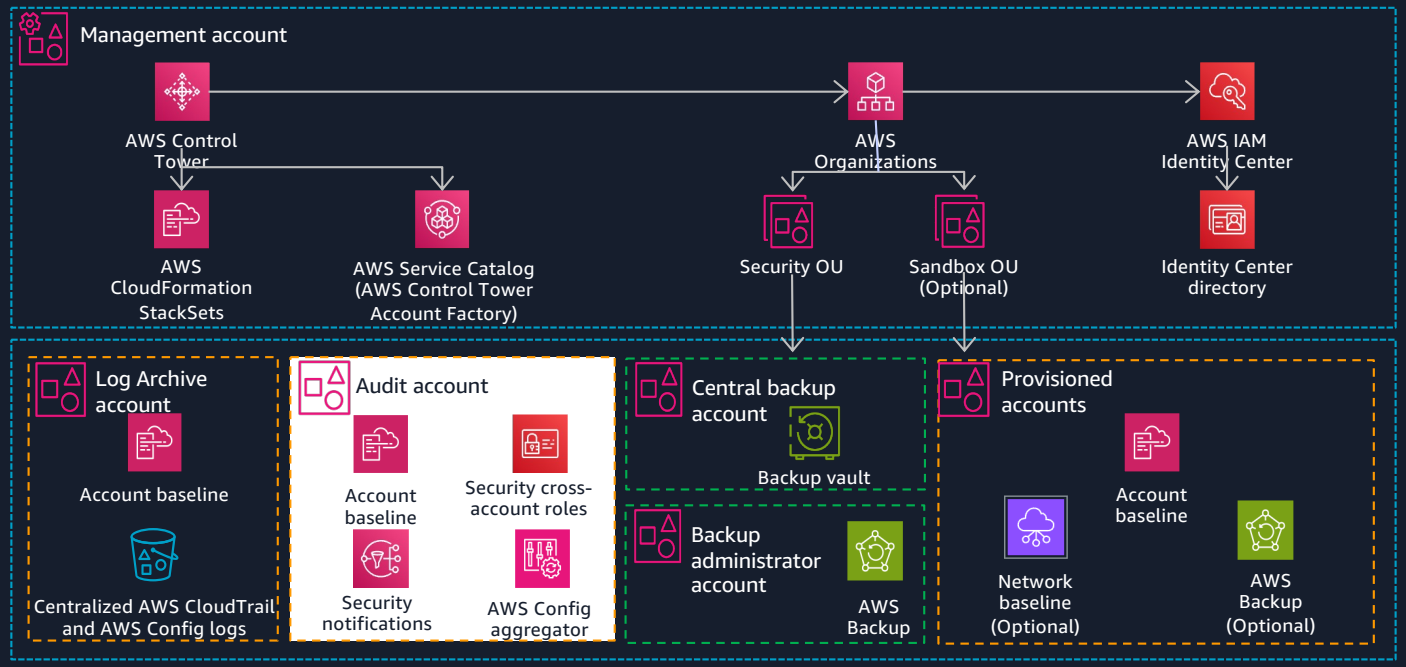
- Account baseline – provides customers with a centralized location for log storage
- Aggregate CloudTrail and Config Logs – account configuration log files are stored in a centrally managed Amazon S3 bucket in the logging account



Audit Account

A CORE SECURITY ACCOUNT IS CREATED TO FACILITATE

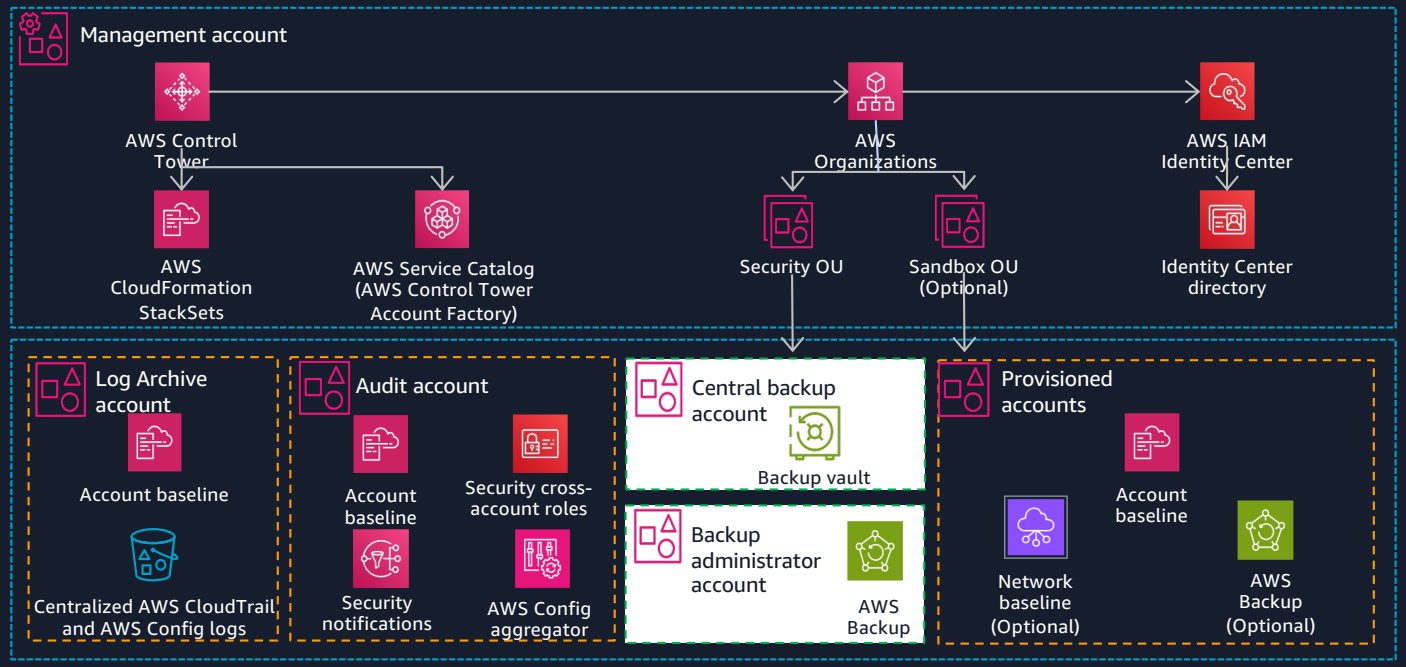
- **Security notifications** - configures alarms to monitor and send notifications on changes within an account
- **Security Cross-Account roles –** break-glass access to managed accounts



Data protection accounts

BRING YOUR DATA PROTECTION ACCOUNTS

- **Central backup account –** stores your AWS Control Tower backup vault and your backups. This vault is created in all AWS Regions governed by Control Tower
- **Backup administrator account –** delegated administrator account for AWS Backup. Stores Backup Audit Manager report plans



Controls Management

Available Control APIs

- DisableControl
- EnableControl
- GetControlOperation
- GetEnabledControl
- ListEnabledControls
- ListTagsForResource
- UntagResource
- TagResource
- UpdateEnabledControl
- ListControlOperations
- *All managed controls have their own unique API ‘Control Identifier’

Available Control Catalog APIs

- GetControl
- ListCommonControls
- ListControls
- ListDomains
- ListObjectives

Control types

Detective

Detect resources that violate your defined security policies

COMPLIANT

NONCOMPLIANT

Preventive

Disallow actions that would lead to violations of your security policies

ALWAYS COMPLIANT

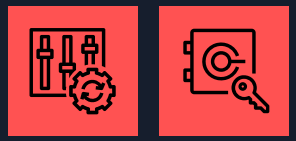
Proactive

Scans resources before they are provisioned, blocking provisioning if resources aren't compliant

APPROVED RESOURCES ONLY

ALWAYS COMPLIANT

Digital Sovereignty and Region Deny controls

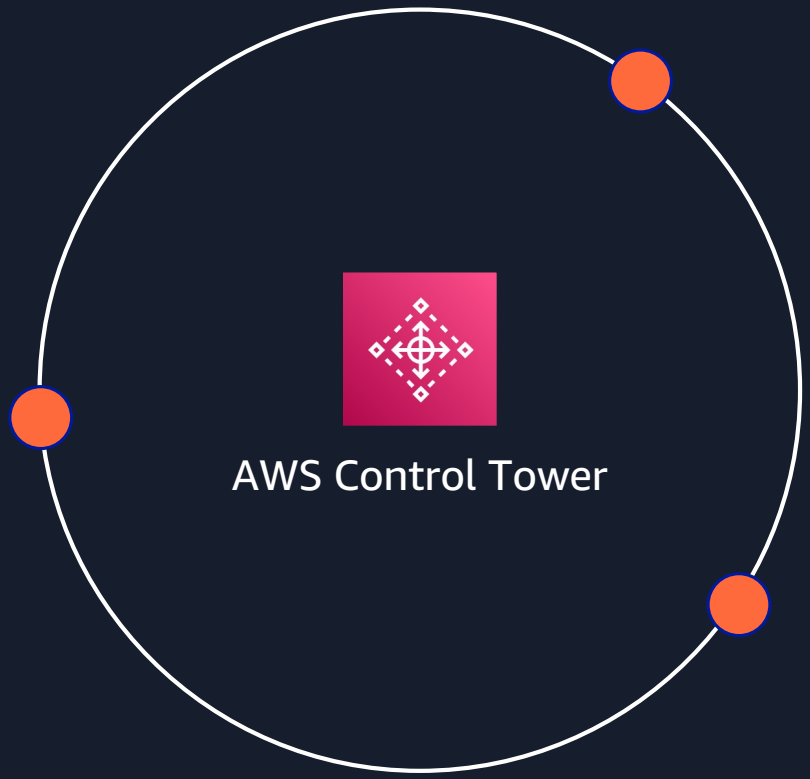


- Prevent actions and detect resource changes regarding data residency, granular access restriction, encryption, and resiliency capabilities

- Parameterized Region deny control at the OU level, for increased granularity of governance, while maintaining additional Region governance at the landing zone level

Control Behaviors

Detective controls
- Powered by AWS Security Hub and Config rules
- Detects non-compliance and security risks in existing resources in line with AWS Foundational Security best practices



Preventive controls
- Service control policies, resource control policies and declarative policies
- Ensures that your accounts maintain compliance because it disallows actions that lead to policy violations

Proactive controls
- Policies are automatically enforced on all AWS CloudFormation deployments

Control Objectives

Categories Info

Categories are groups of AWS-managed controls that help you achieve compliance for your environment. **Enable**, or **disable**, multiple categories across your organizational units (OUs). Up to 100 operations can run at the same time. To learn more about exceptions with multi-selecting controls, view the *help panel*. To run control operations, go to *Recent Operations*.

Control objectives | Services | Frameworks | Groups

Control objectives (15) Info

Control actions

Find control objectives

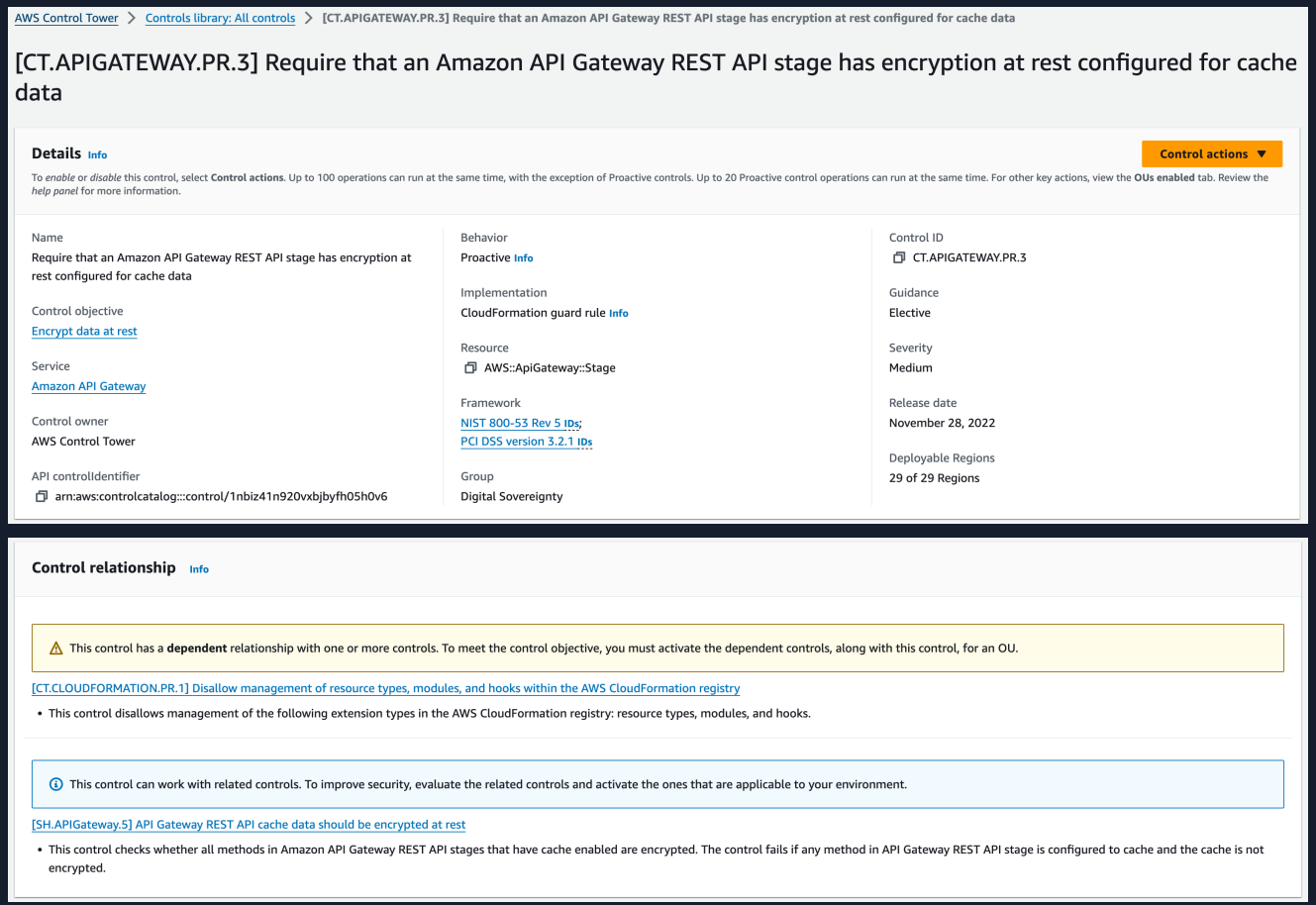
1

Control objective	Controls
Encrypt data at rest	64
Establish logging and monitoring	58
Use strong authentication	16
Encrypt data in transit	48
Protect configurations	63
Manage vulnerabilities	26
Enforce least privilege	96
Improve availability	48
Improve resiliency	25
Limit network access	104
Optimize costs	7
Protect data integrity	21
Prepare for disaster recovery	5
Prepare for incident response	10
Manage secrets	4

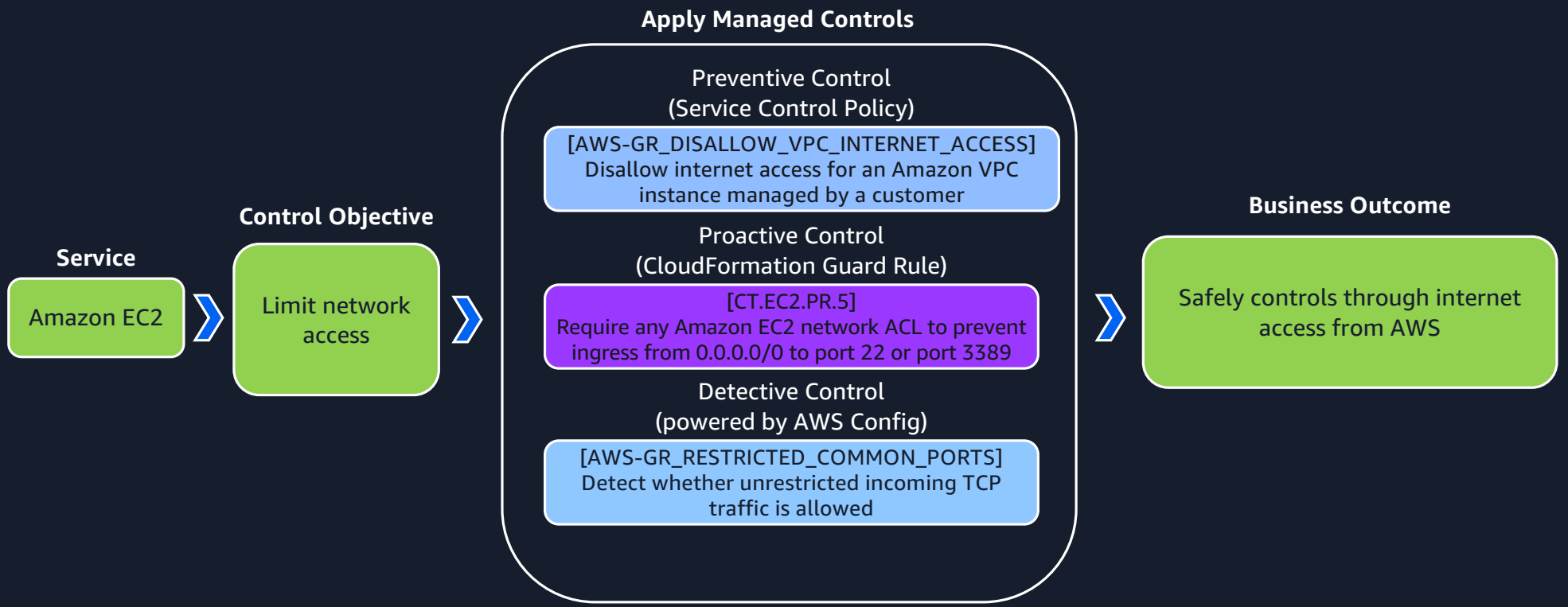
Control Details

Bulk options:

- Enable multiple controls in a single OU
- Enable one control across multiple OUs
- Enable multiple controls across multiple OUs



Enforce limit network access

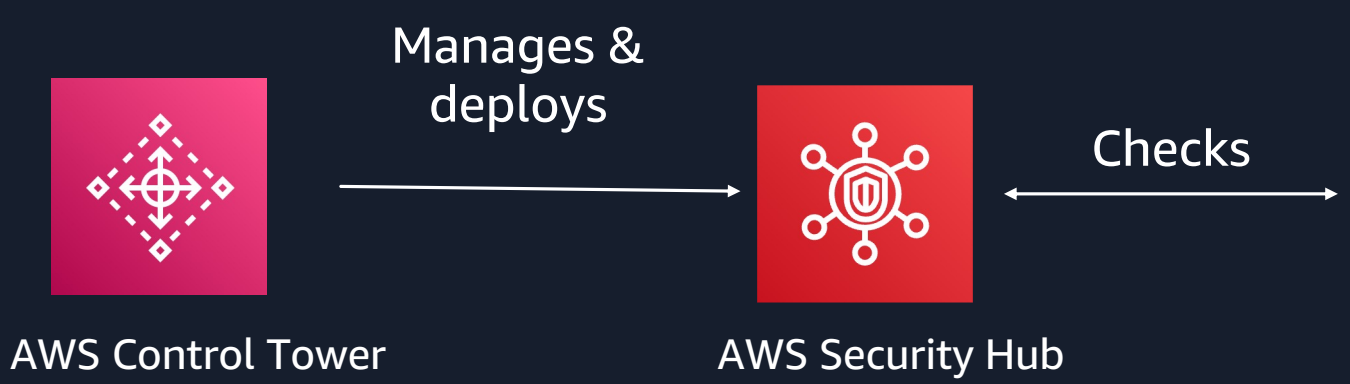


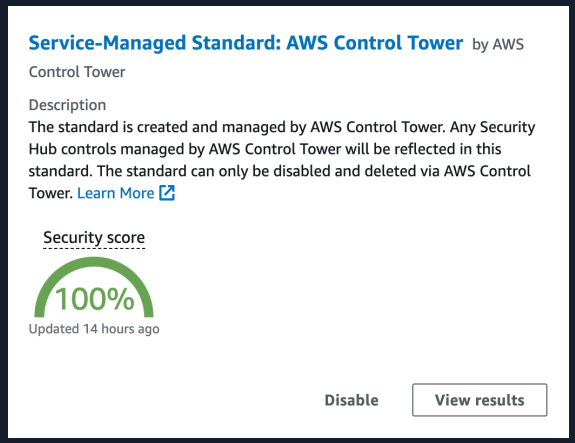
Control Examples

Control Name	Behavior	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 changes to bucket policy for AWS Control Tower created Amazon S3 buckets in log archive	Preventive	Mandatory
Integrate CloudTrail events with CloudWatch Logs	Preventive	Mandatory
Detect whether versioning for Amazon S3 buckets is enabled	Detective	Elective
Disallow delete actions on S3 buckets without MFA	Detective	Elective
Require an Amazon S3 bucket to have server-side encryption configured with KMS key	Proactive	Elective

Security Hub Integration

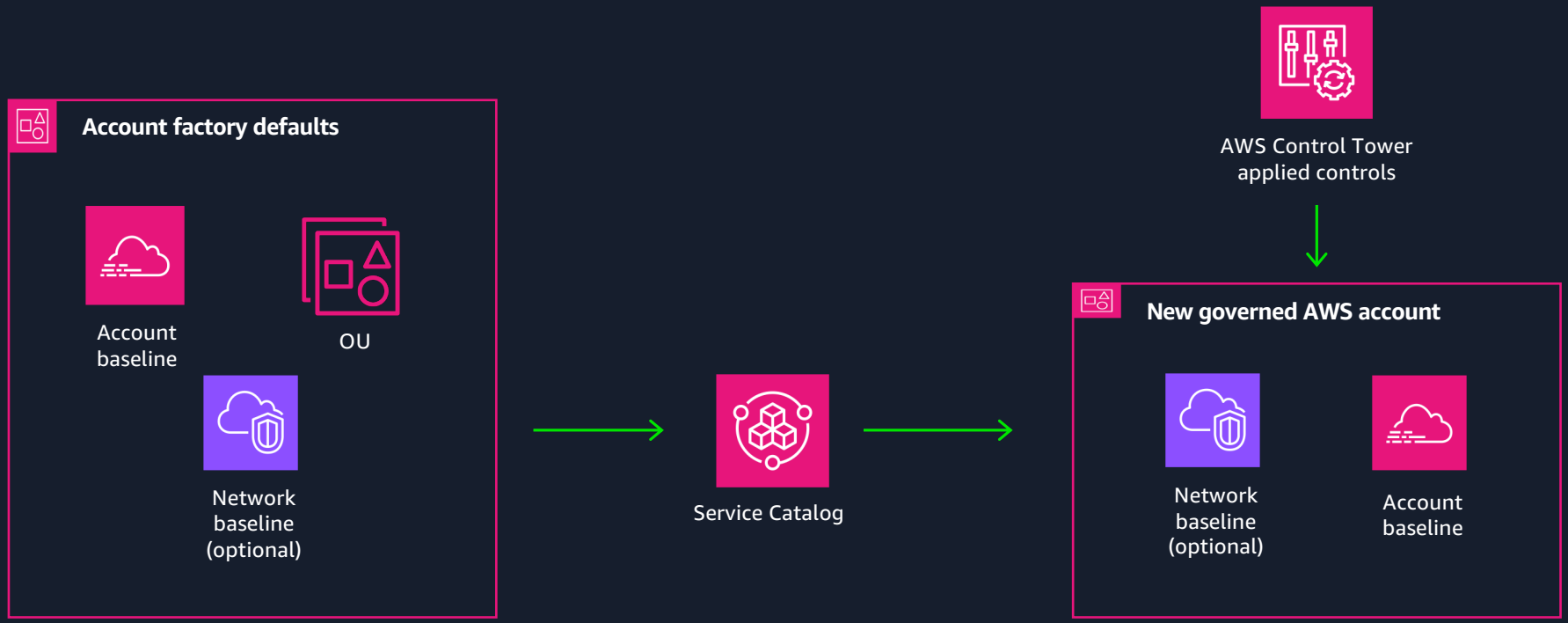
- 180+ AWS foundational security best practice controls
- Enable individual controls within the new standard across an entire OU for all of the regions governed by AWS Control Tower





Automate Account Provisioning

Provision Accounts with Account Factory



Customizing your AWS Control Tower accounts

Native capability

AWS CloudFormation

Stacks and StackSets

Feature of AWS Organizations

Native
Out of the box

AFC

Account Factory Customization

Feature of AWS Control Tower

Based on AWS Service Catalog

Easy to Implement

AWS Control Tower solutions

CfCT

Customizations for AWS Control Tower

AWS-provided solution

AWS CloudFormation based

Automate many Accounts

AFT

Account Factory for Terraform

AWS-provided Terraform module

Terraform Adopters

Account Factory Customization (AFC)

Accelerate development of custom accounts during account provisioning

Native capability

Supports existing AWS Control Tower and non-Control Tower accounts

- Integrated into existing account workflow
- Build fully customized account blueprints
- Access 12+ partner blueprints

Customizations for AWS Control Tower (CfCT)

- Find in the AWS Solutions Library
- CI/CD pipeline to extend Account Factory
- Keeps resources in sync via CloudFormation StackSets
- Account customization of existing accounts
- Customization to meet your procedures

Account Factory for Terraform (AFT)

Terraform pipeline to provision and customize your accounts in Control Tower

Control Tower governance benefits

Create and customize accounts

Supports
Terraform Cloud
Terraform Enterprise
Terraform Open Source

AWS Control Tower with existing environments

Design principles for multiple AWS accounts

- Organize by security and operational needs
- Avoid deep complex OU structures
- Start small and expand
- No workloads in Management accounts
- Separate production from non production
- Single / small set of related workload per account

Your multi-account journey

One account to rule them all

Prod Account

Test Account

AWS Organizations

OU Prod

Prod Account A

OU Test

Test Account B

Business Group A

OU Prod

Prod Account A

OU Test

Test Account A

Business Group B

OU Prod

Prod Account B

High level Steps

Complete AWS Control Tower pre-requisites

temporary mitigation may be required

Setup AWS Control Tower in existing AWS Organizations

no impact to existing accounts

protect AWS Control Tower infrastructure

Enroll existing account to AWS Control Tower

non invasive baseline control

assess impact of optional control

AWS partners with an AWS Control Tower competency

Functions & ISV Partners

AWS Control Tower

Controls

BigID
Cloud Checkr
Lacework
sumo logic
snyk
sysdig
Spot by NetApp

Networking

cisco
aviatrix
BLUECAT
ExtraHop

Identity Management

okta
onelogin
sonrai SECURITY
Ping Identity
CYBERARK

Centralized security

paloalto NETWORKS
CROWDSTRIKE
TREND MICRO
ALERT
TIGERA
snyk
ermetic
aqua
Lacework

Observability

CHECK POINT CloudGuard Dome9
New Relic.
tenable
DATADOG
splunk
logz.io
dynatrace

Pricing Scenarios

Cost Scenario #1

Basic Setup

Minimum Setup Costs

- 3 mandatory detective controls – AWS Config
- 1 region in governance
- 2 default accounts created
- Single organization CloudTrail - management events only
- Remain in free tier Service Catalog/CloudWatch/SNS
- No configuration changes per month

Approximate Cost: $0.011

Cost Scenario #2

Small Use Setup

10 Extra Accounts Created

- 5 detective controls in 10 accounts – AWS Config
- 1 region in governance
- 10 accounts created including 2 default accounts
- Single organization CloudTrail - data events recorded
- 100 Service Catalog API calls ?
- 10 configuration changes per month

Approximate Cost: $5.06

Cost Scenario #3

Large Use Setup

25 Extra Accounts Created

- 5 detective controls in 25 accounts – AWS Config
- 3 regions in governance
- 25 accounts created including 2 default accounts
- Single organization CloudTrail - data events recorded
- 250 Service Catalog API calls
- 15 configuration AWS Config changes per month

Approximate Cost: $86.92

Items that create cost variability

- Number of regions in governance
- Number of accounts
- Number of detective controls
- Number of CloudTrail's
- Disable default network config
- Number of configuration changes – ephemeral workloads

What are customers saying?

“Data residency in AWS Control Tower adds to our toolbox of programmatically setting up guardrails and data controls. As data regulations evolve, this capability will assist compliance and help us enable innovation to serve patients around the world.”

— William Taggart, Executive Director, Cloud Computing and DevOps, Bristol Myers Squibb

"By using AWS Control Tower, Growens has now standardized its account creation procedure, which prevents duplicate accounts from being created. As a result, we have decreased time to create accounts by 95 percent, and thanks to AWS Single Sign-On, login times have decreased by 90 percent."

— Michele Cappellini, Chief Information Officer (CIO) - Growens

“Getting started on AWS Control Tower was incredibly easy. Within five minutes, Control Tower had begun creating a best-practice accounts structure, enabling security guardrails, and establishing governance controls for us. What previously took us weeks of effort was completed in about an hour.”

— Ryan Matteson, Director of Systemwide Cloud Acceleration – California State University

How do I get started?

- Getting Started
- AWS Control Tower Workshops
- Contact your account team about attending on of our Cloud Governance events
- AWS Cloud Governance Page
- AWS Cloud Operations Blog
- AWS Cloud Operations YouTube Channel
- AWS Marketplace Control Tower Solutions

AWS Control Tower getting started

AWS Cloud Operations blog

Thank you!