
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

COP318

Setting up controls at scale in your AWS environment

Jamie St. Onge (she/her)
Sr. Manager Product and UX
AWS Control Tower
AWS

Kuntal Shah (he/him)
Product Manager, Cloud Platform Engineering
PIMCO

Jens Jacobsen (he/him)
Sr. User Experience Researcher
AWS Control Tower
AWS

Tom Wolstencroft (he/him)
Director, Cloud Solutions Engineering
The Depository Trust & Clearing Corporation

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- AWS Cloud Ops
- AWS Control tower overview
- Customer journeys
- Governance challenges
- Demo

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why AWS Cloud Ops?



Return on Investment (ROI)

241% ROI over 3 years*



Staff productivity

62% more efficient IT infrastructure staff



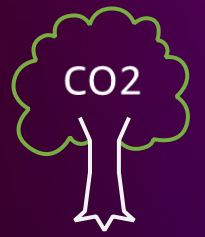
Operational resilience

57% decrease in downtime



Business agility

37% decrease in time to market



Carbon savings

88% reduction in carbon footprint of IT operations

Based on independent research of 1,500 AWS enterprise customers

*Source: "The Total Economic Impact of AWS Cloud Operations: Cost Savings And Business Benefits Enabled By Operation on AWS, May 2022, A commissioned study conducted by Forrester Consulting on behalf of Amazon Web Services."

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Your journey to operating at cloud scale

Get started with AWS Cloud Operations

1) Setup



Establish a secure foundation for governance and compliance

2) Build & Migrate



Migrate applications to the cloud, or build new applications

3) Operate

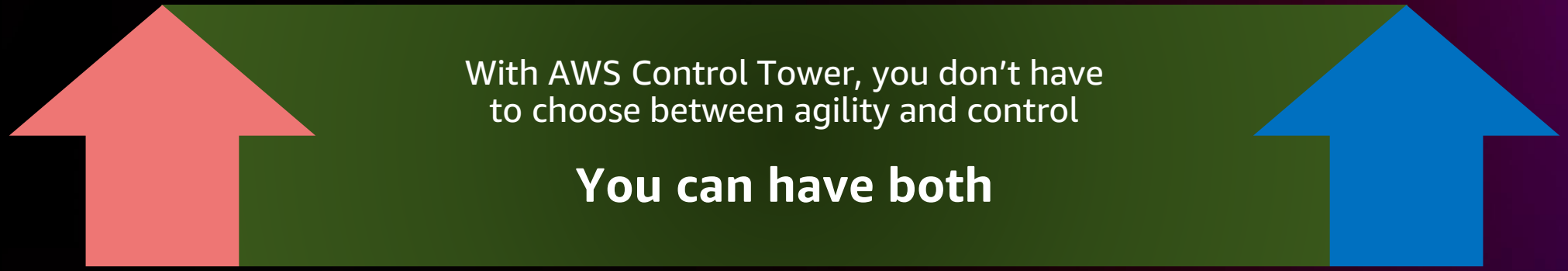


Monitor application performance, detect and remediate noncompliance or operational risks quickly

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Business agility and governance control



Governance

Security

Compliance

Operations

Spend management

Agility

Self-service access

Experiment fast

Respond quickly to change

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Control Tower: A 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 controls



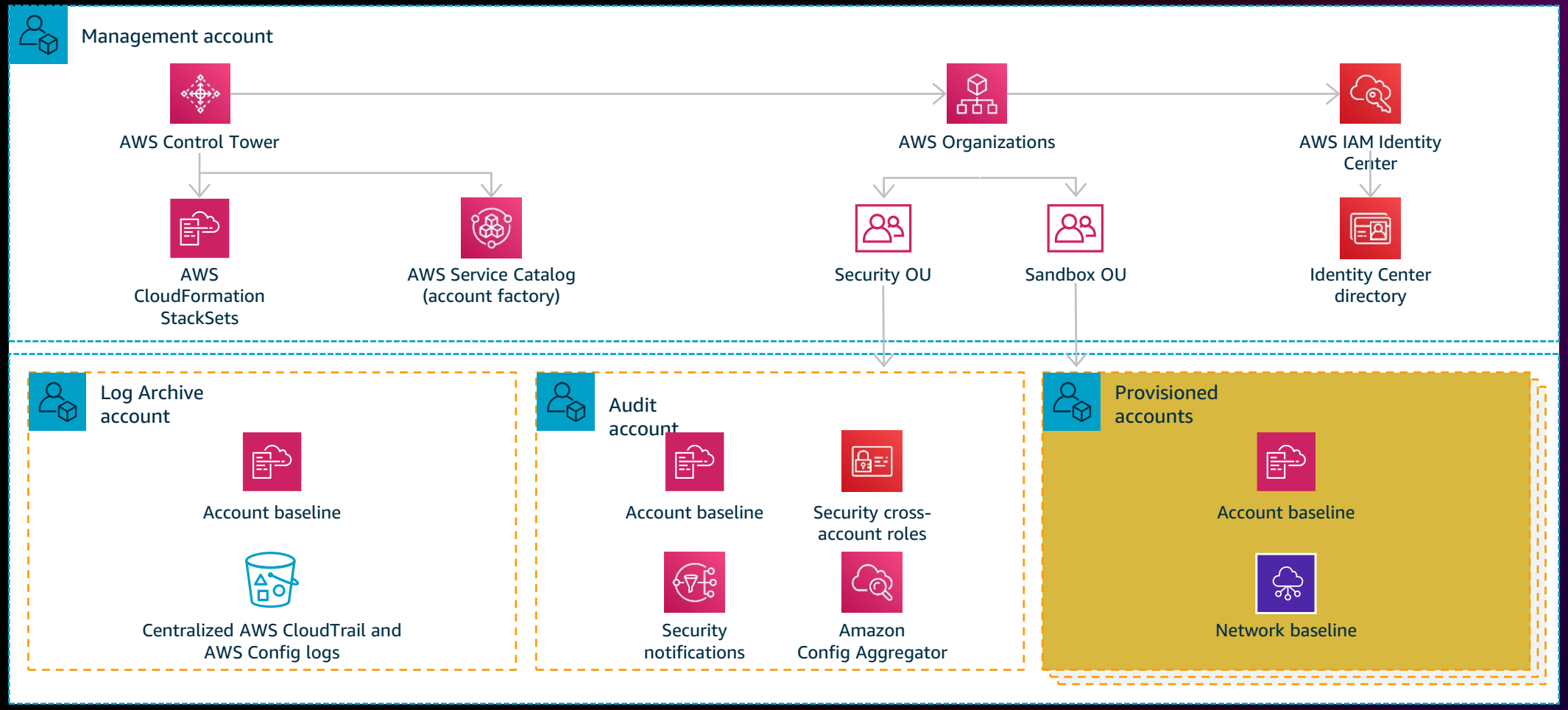
Automated account creation based on AWS best practices



Dashboard for monitoring compliance status

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Landing zone foundation



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Custom account provisioning



AWS Control Tower
Account Factory Customization



Accelerate development of custom accounts during account provisioning



Fully service-managed solution

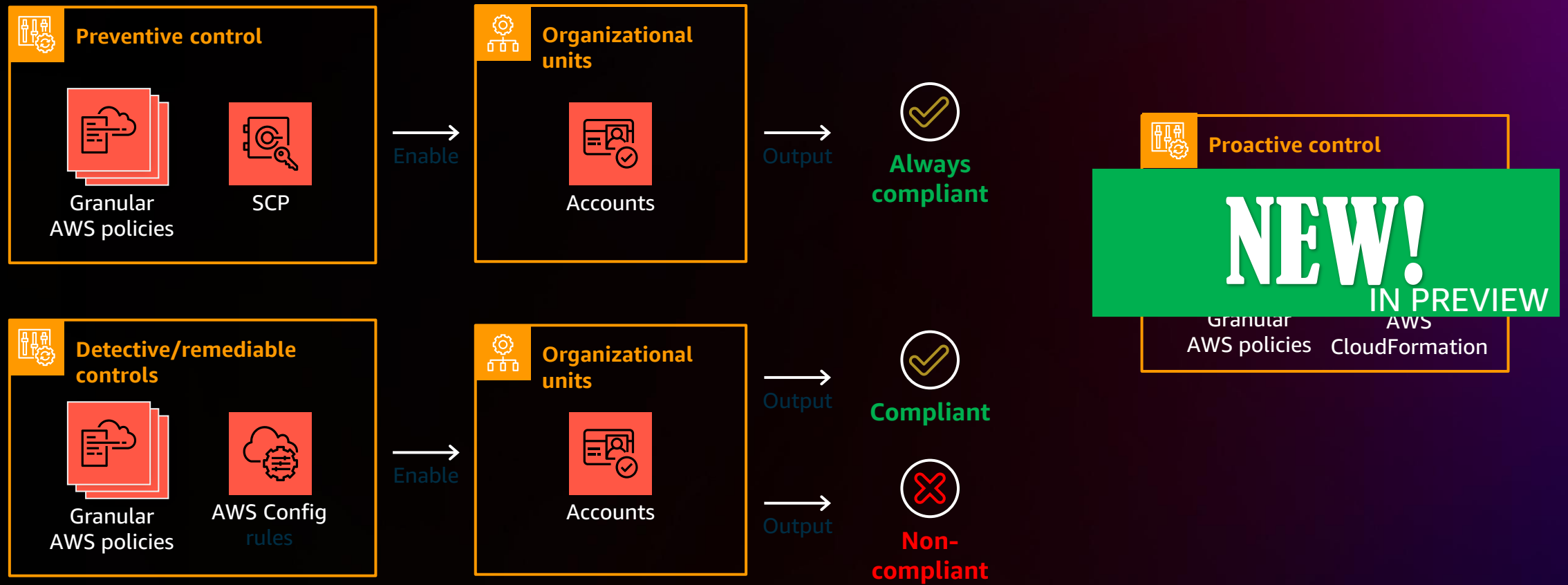


Supports existing AWS Control Tower and non-Control Tower accounts

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

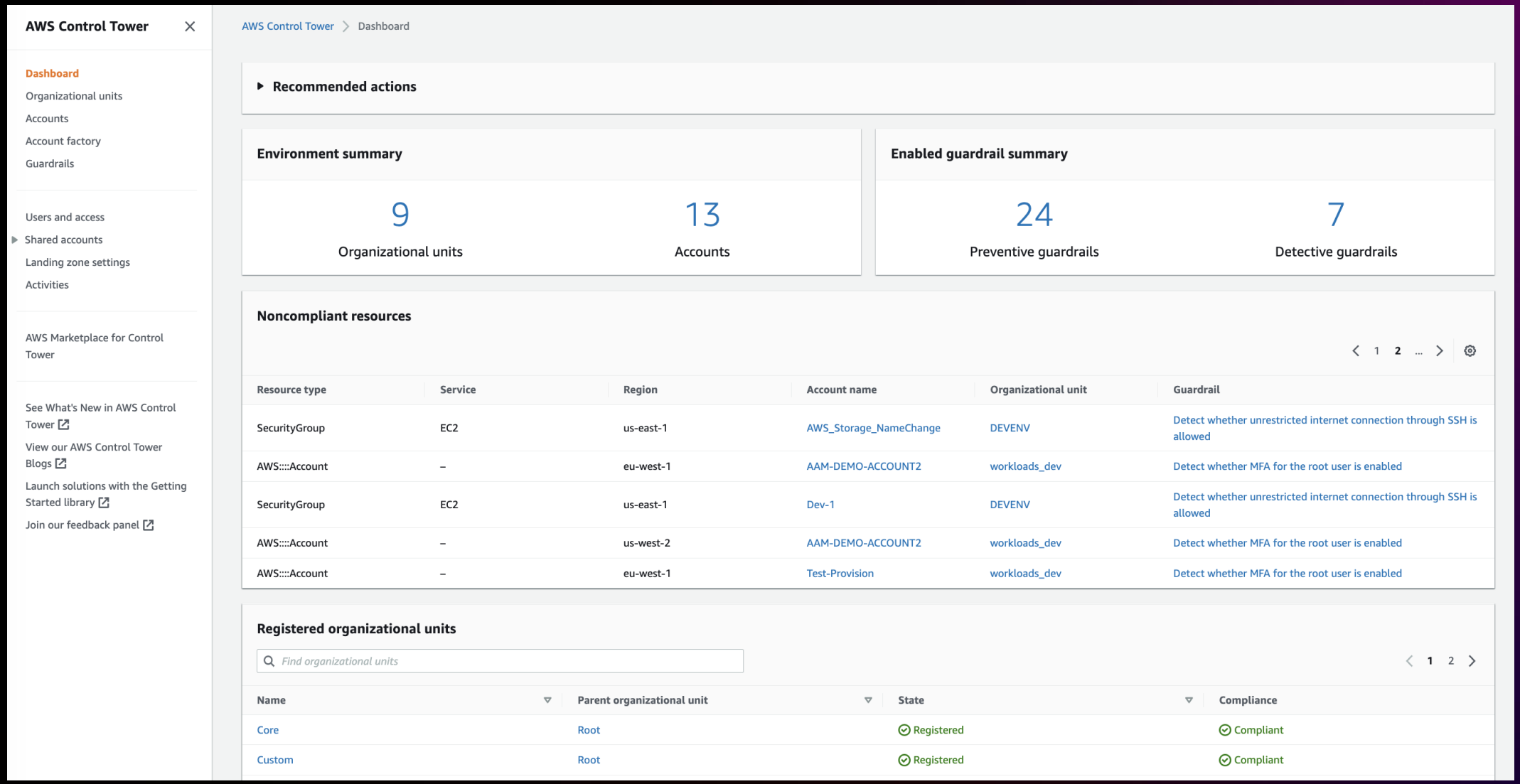
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Apply governance policies with AWS managed controls



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Dashboard for oversight



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

If you haven’t looked at AWS Control Tower in a while…

- 44 releases since General availability in 2019
- Support for using AWS Control Tower with an existing Organization (2020)
- Support for nested OUs (2021)
- Region deny, and data residency controls (2021)
- Support for 16 AWS Regions, and GovCloud (US) region (2022)
- Customization of logging, bring your own core accounts (2022)
- Controls APIs (2022)
- Account factory customization built into AWS Control Tower (this week)
- More to come (today!)

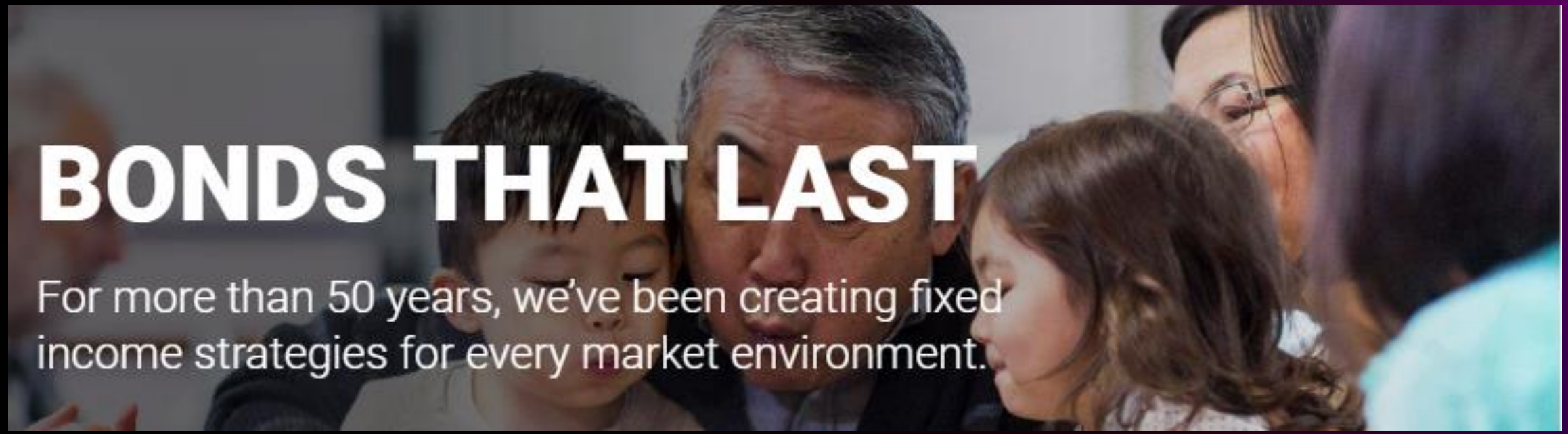
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Voice of the customer - PIMCO

Kuntal Shah (he/him)
Product Manager, Cloud Platform Engineering

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

PIMCO at a Glance



- PIMCO is a global leader in active fixed income.
- For more than 50 years, we have worked relentlessly to help millions of investors pursue their objectives – regardless of shifting market conditions.

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

PIMCO journey to cloud and the next steps

Leverage cloud to generate competitive advantage

1) PaaS -> Cloud Native

2) Iterate Faster

3) Customizations



Governance in parallel to agility and innovation.



Secure best practice environments with preventive and detective controls



Flexibility to apply custom policies for different workloads

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lessons learned from migration to AWS Control Tower

- Planning is key before launching a new AWS Control Tower deployment
- Design an Organization structure that is flexible for future requirements
- Leverage ‘Customization framework’ for custom controls tied to lifecycle events
- Operational readiness and security service integrations to support continuous compliance
- Use the new 'Data residency' and 'Region deny’ controls for regulated environments

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use Case: Region control and data residency



Allow access only to Regions that you have controls in place

Enable application teams to meet data residency requirements

Allow use of the Home Region and certain global services

Manage cross-Region network security and costs by controlling Regions

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data residency controls with AWS Control Tower

Without AWS Control Tower, **need custom SCPs** to implement the controls:

1. SCPs need to be enabled at the Organization/Account level.
2. Need to maintain SCPs as new services and regions are added.
3. Need to carefully exempt services and operations that need to be allowed.

Data residency controls are **purpose-built** in AWS Control Tower:

1. Applies to Landing Zone as a whole.
2. Content cannot be created or transferred outside of allowed Regions
3. Controls can be **setup in hours**.
4. Includes most common preventive controls for internet access, VPN and cross-region traffic.

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What’s on our wish list?

Ecosystem Integration	Custom Controls	Shared Responsibility	Custom Dashboards	What If Analysis
Seamless integration with AWS Security Hub, AWS Config and other services	Show compliance issues detected by custom controls in AWS Control Tower	Visibility to control status for application teams	Ability to build views for Control Objectives with filters and sharing	Preview compliance issues from controls before enabling

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Voice of the customer - The Depository Trust & Clearing Corporation

Tom Wolstencroft (he/him)
Director, Cloud Solutions Engineering

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

About DTCC

ADVANCING FINANCIAL MARKETS. TOGETHER.™

With over **45 years of experience**, DTCC is the **premier post-trade market infrastructure** for the global financial services industry.

From operating facilities and data centers around the world DTCC, through its subsidiaries, **automates**, **centralizes**, and **standardizes** the processing of financial transactions across the trade lifecycle and **mitigates risk** for **thousands of institutions** worldwide.

OUR PROMISE: We deliver resiliency, value and expertise for our clients. We were built in partnership with the industry to provide stability and efficiency in the global capital markets. With a focus on exceptional service, we promise to advance solutions and next-level innovation.

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

WE BRING ECONOMIES OF SCALE

$2.37 QUADRILLION
SECURITIES PROCESSED IN 2021

FIXED INCOME CLEARING

Processes **$4.5 trillion** per day in U.S. Government Securities and a monthly average of **8.35 trillion** Mortgage-Backed Securities transactions

SETTLEMENT & ASSET SERVICES

World's largest depository holds **1.39 Million** active U.S issues worth **$87 Trillion**

Settles **643 Million** U.S. Transactions per year

EQUITIES CLEARING

Clears **202 Million** Broker-to-Broker Transactions Per Day

Worth **$2.02 Trillion** for **50+** Exchanges and Trading Venues

DERIVATIVES REPORTING

Covers all asset classes and processes **16.5 billion** messages annually for **8,500+ firms globally**

60+ regulators across the globe have access to our data from across **35** countries

INSTITUTIONAL TRADE PROCESSING

Processes an average of **3.3 Million** institutional trades daily.

Our unique capabilities and decades of experience deliver a network no other market infrastructure can match –

5,850 CLIENT FIRMS IN 93 COUNTRIES.

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

DTCC's Cloud Journey

2012 – 2017: DTCC began its cloud journey with a public data reporting application. This was followed by adoption in the Solutions business and a focus on commodity services. Invested in education and training across IT disciplines.

2017 – 2021: Implemented foundational capabilities to further enable the cloud platform.

- Developed strong partnership with AWS
- Contractual addendums to meet Regulatory and Compliance requirements
- Co-developed new services with AWS to meet resilient, Tier 1 requirements
- Education of regulatory bodies and compliance groups
- Cost management and optimization – flattening spend while increasing usage

2022: Refreshing approach to AWS as a Platform focusing on automation of scaled, secure consumption and supporting all DTCC workload types. Improving proactive management capabilities and updating our cloud operating model to support cloud delivery at scale.



2017
Cloud program initiating AWS 2.0 with additional security & compliance oversight

2018
Core financial capabilities (costing and allocation); Cloud Governance Insights (CGI) Developed

2019
Advanced optimization and consumption transparency; Reactive Compliance Remediation

2020
Expansion into new data warehouse (Snowflake)

2021
Cloud CoE Established; Focused effort on optimization, shutdowns, and clean up

2022
Refresh of cloud approach and strategy focused on ability to scale (AWS as a platform)

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Business Benefits of DTCC's Cloud Investment



Accelerating Time to Market for New Product or Features

- Secure and compliant platform by design
- Reusable patterns that are pre-approved by Security and Compliance to accelerate time to market for product development



Risk Mitigation and Improved Incident Response Capability

- Greater visibility and automated response to security posture, threat vectors, and data access
- Improved availability and resilient architectures to minimize downtime



Improved Used Experience

- Better application performance
- Ability to consolidate data and build multi-platform user apps quickly



IT Cost Optimization

- Increase Staff Productivity
- Decrease IT Infrastructure Cost
- Better alignment of cost to value



Increased Business Agility and More Rapid Response to Market Fluctuations

- Automated scale up and down of business systems based on market demand
- Ability to burst capacity for internal or external event-driven analytics

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IN PREVIEW

Comprehensive Controls Management with AWS Control Tower

Jamie St. Onge (her/she)
Sr. Manager Product and UX
AWS Control Tower

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Governance challenges

IN PREVIEW

Customers are challenged with balancing compliance requirements with the desire to allow engineers to make their own design choices.

Time and effort to assess each AWS service to identify risks, threats, and ability to meet compliance requirements.

Definition of controls required to meet common control objectives **requires a special skill set** with advanced knowledge of AWS services, relationships, and dependencies.

Automation of control implementation at scale drives **custom built solutions**.

New features and **changes** to existing features demand services to be reassessed.

Required to **navigate multiple AWS services** to view controls enabled and their status.

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The AWS Control Tower solution

IN PREVIEW

1. Opinionated **purpose built controls** required to meet the most common control objectives

2. **Automated control management** across your multi-account environment.

3. **Comprehensive guidance** for control definition, dependencies, relationships, and manual steps

4. Shift compliance left with **new proactive controls** block CloudFormation deployment of non-compliant resources

5. Consolidated view of controls applied to accounts and OUs

6. AWS managed service

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

>300 Purpose built controls for AWS services

IN PREVIEW

- Mapped to common control objectives & frameworks
- Severity identifies importance of control
- Guidance on control relationships and dependencies
- Access to the control policy for proactive and preventive controls
- Compliant and noncompliant resource templates for proactive controls

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multiple control implementation options

IN PREVIEW

Preventive Controls (service control policies)

- ensures that your accounts maintain compliance, because it disallows actions that lead to policy violations

NEW! Proactive controls (CloudFormation hooks and Guard rules)

- Proactively blocks noncompliant resources before they are provisioned by CloudFormation
- Policies are automatically enforced on all CloudFormation deployments



Detective controls (now powered by AWS Security Hub)

- Detect noncompliance and security risks in existing resources in line with AWS Foundational Security Best Practices
- Findings generated at the resource level

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NEW! Detective Controls powered by AWS Security Hub

IN PREVIEW

- 160 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



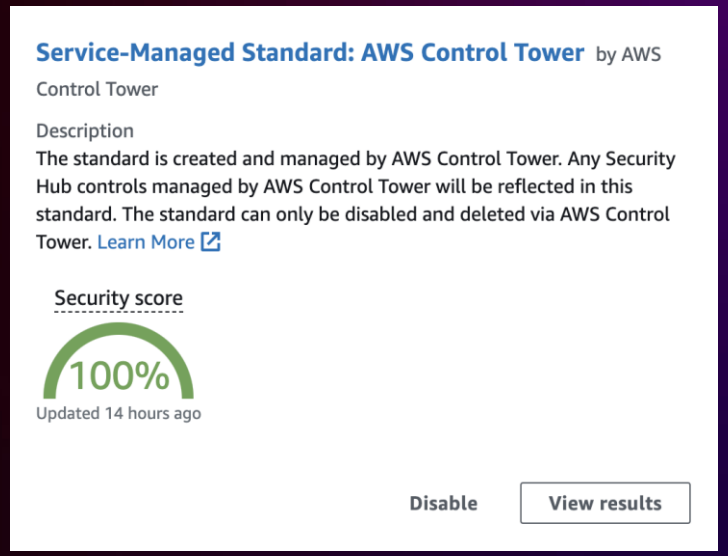
AWS Control Tower

Manages & deploys



AWS Security Hub

Checks

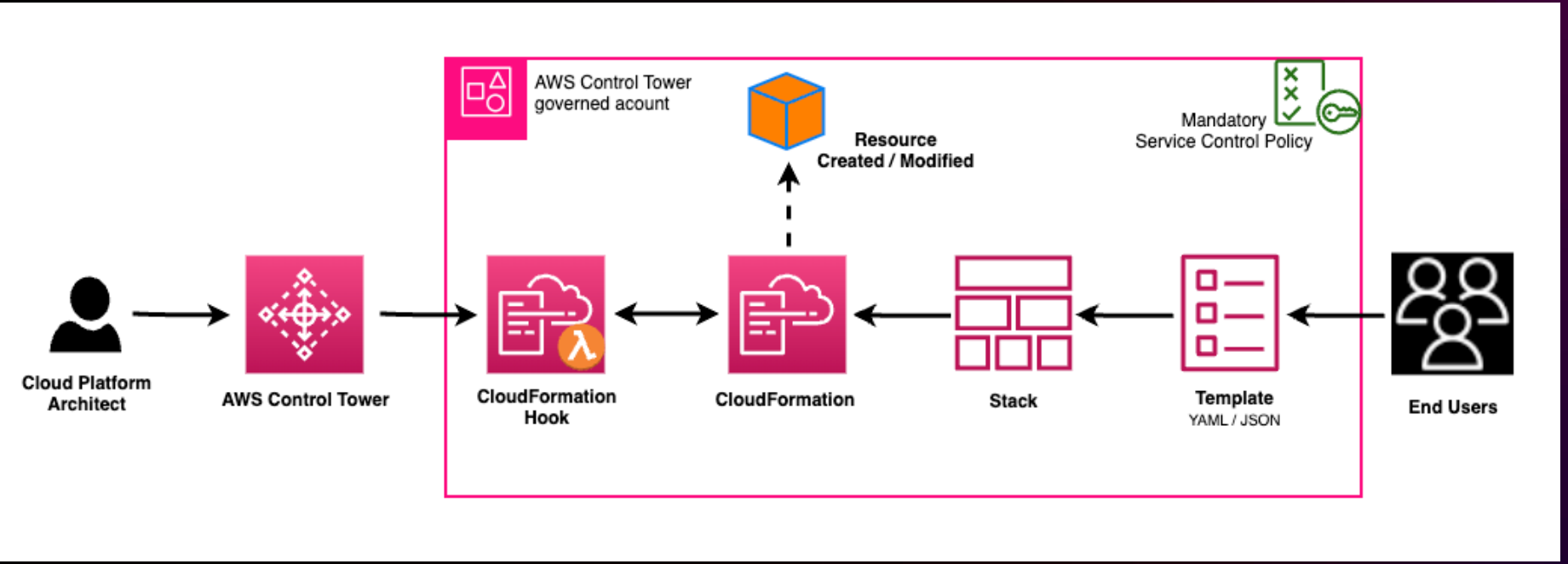


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NEW! Proactive controls

IN PREVIEW

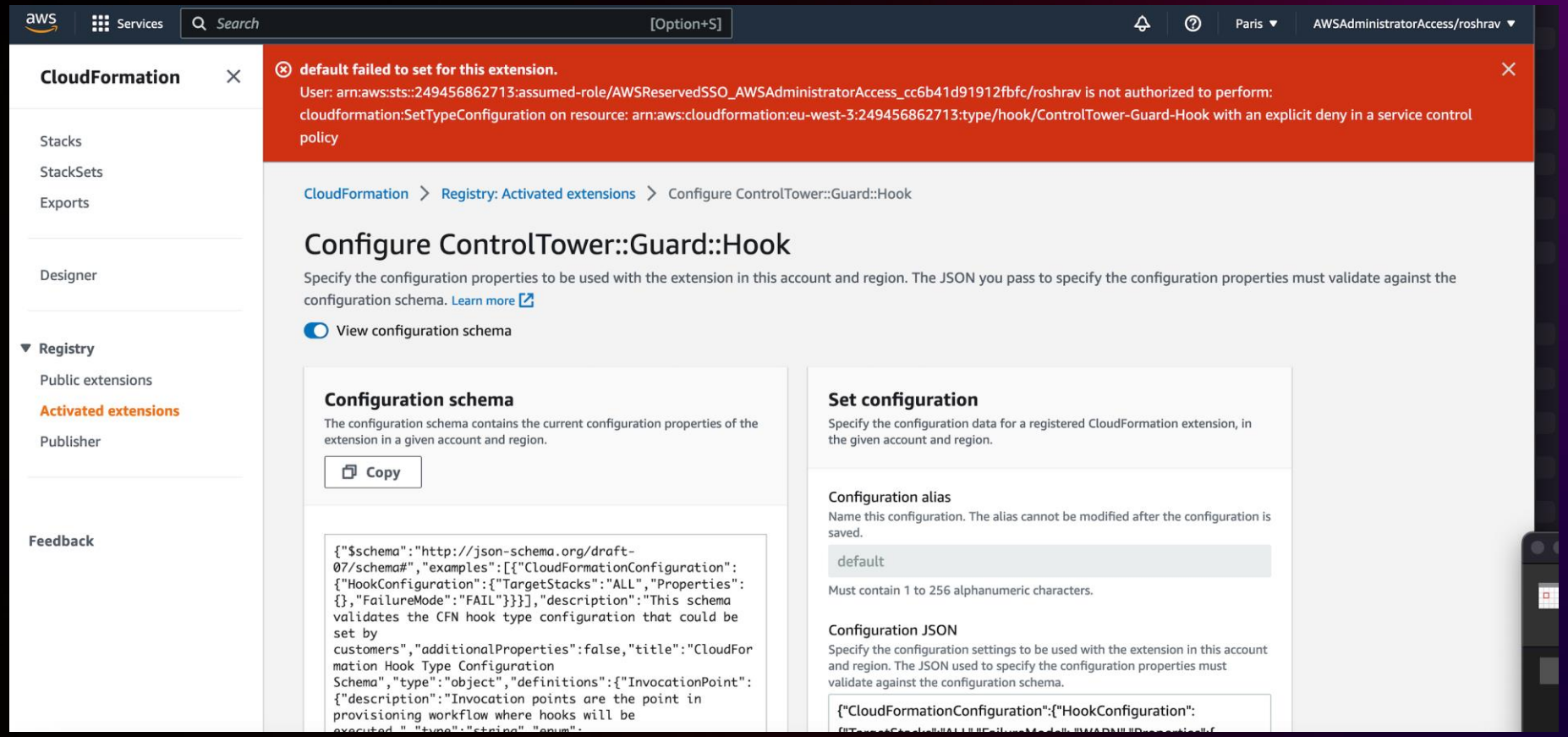
- Proactively block noncompliant resources before they are provisioned by CloudFormation
- Policies are automatically enforced on all CloudFormation deployments



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

End-user experience

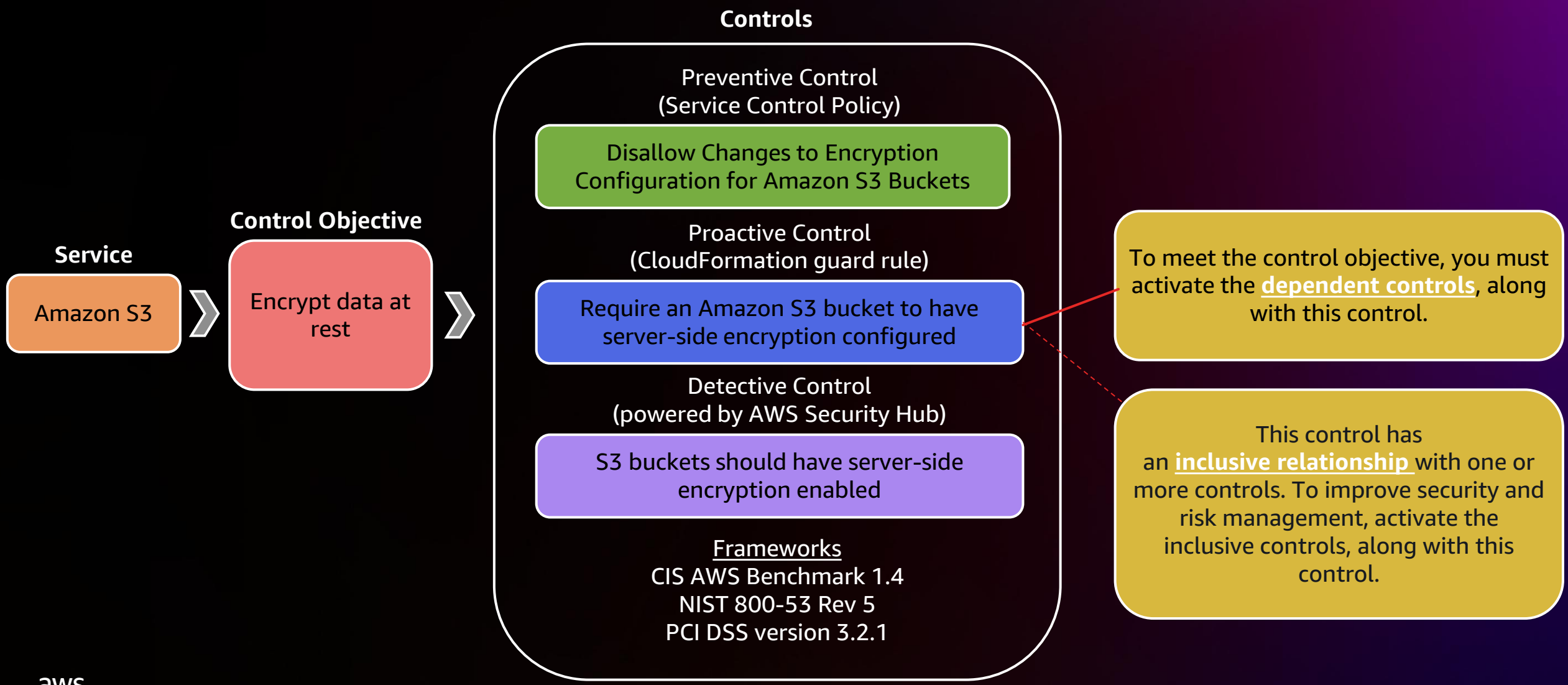
- The Hook logic executes prior to CloudFormation proceeding with the deployment resource creation/update; a pre-deployment validation.
- If the proposed create/update stack operation is in violation of any enabled proactive control, the stack operation will fail.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Example: S3 Encrypt data at rest

IN PREVIEW



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Control Tower

Dashboard
Getting started
Organization
Account factory

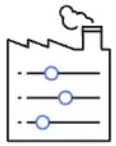
Controls library
Categories Preview
All controls Preview

Users and access
Shared accounts
Landing zone settings
Activities

AWS Marketplace for Control Tower

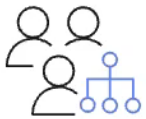
See What's New in AWS Control Tower
View our AWS Control Tower Blogs
Launch solutions with the Getting Started library
Join our feedback panel

Recommended actions



Programmatically manage controls with APIs

AWS Control Tower customers can manage controls programmatically across their organization, at scale.



Add or register organizational units

Add or register organizational units (OUs) to organize accounts and projects.



Enable more controls

Enable additional controls to meet your security, operational, and compliance requirements.



Review users and access

Review your user identity store and single sign-on access for your users across accounts.



Review shared accounts

Review the settings of the shared accounts that AWS Control Tower has set up for you.

Environment summary

4	5
Organizational units	Accounts

Enabled control summary

22	165
Preventive controls	Detective controls

2
Proactive controls

Noncompliant resources

1

Resource ID	Resource type	Service	Region	Account name	Organizational unit	Control

No noncompliant resources found

No noncompliant resources detected on controls with a Clear status.

aws © 2022, A

Want to see more AWS Cloud Operations?

Please complete the session survey in the mobile app



Ask us anything at our kiosks in the AWS Village Expo



Find related sessions in our re:Invent blog

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How do I get started?

- Getting started
- AWS Control Tower workshops
- Attend an AWS Control Tower activation day held regionally/time-zone based: Contact your account team
- AWS Well-Architected Management and Governance Lens
- AWS Management and Governance blog
- AWS Management and Governance YouTube channel



AWS Control Tower getting started



AWS Management and Governance blog



AWS Well-Architected Management and Governance Lens

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Insert image here

Controls Engineering







Please complete the session survey in the **mobile app**

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.