

AWS
re:Invent



MGT307

How to onboard existing AWS accounts onto AWS Control Tower

Justin Fox

Director, Software Engineering
Mastercard

Vishal Sharma

Senior Specialist
AWS

Agenda

Simplifying management and governance in AWS

Best practices using AWS Control Tower

Using AWS Control Tower to simplify SecOps

Extending AWS Control Tower to enhance operational guardrails

Deep dive on governance capabilities

Simplifying management and governance in AWS



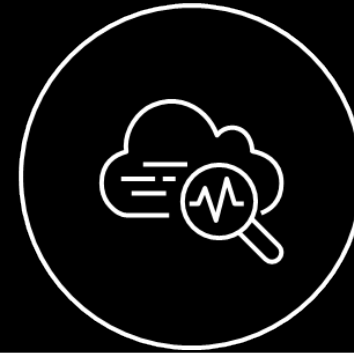
Simplifying management in AWS



Enable



Provision



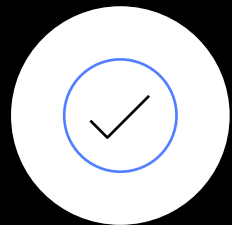
Operate

Business agility + governance control

AWS Control Tower and AWS Service Catalog

AWS Control Tower

The self-service solution to automate the setup and management of **multi-account AWS environments**



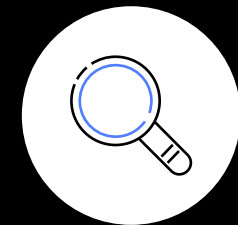
An AWS service offering account creation based on AWS best practices



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

Out of the box in 1 hour...0 lines of code written



Automated landing zone



Guardrails



Account Factory



Dashboard for visibility



Built-in identity and access



Preconfigured log archive and
audit access to accounts

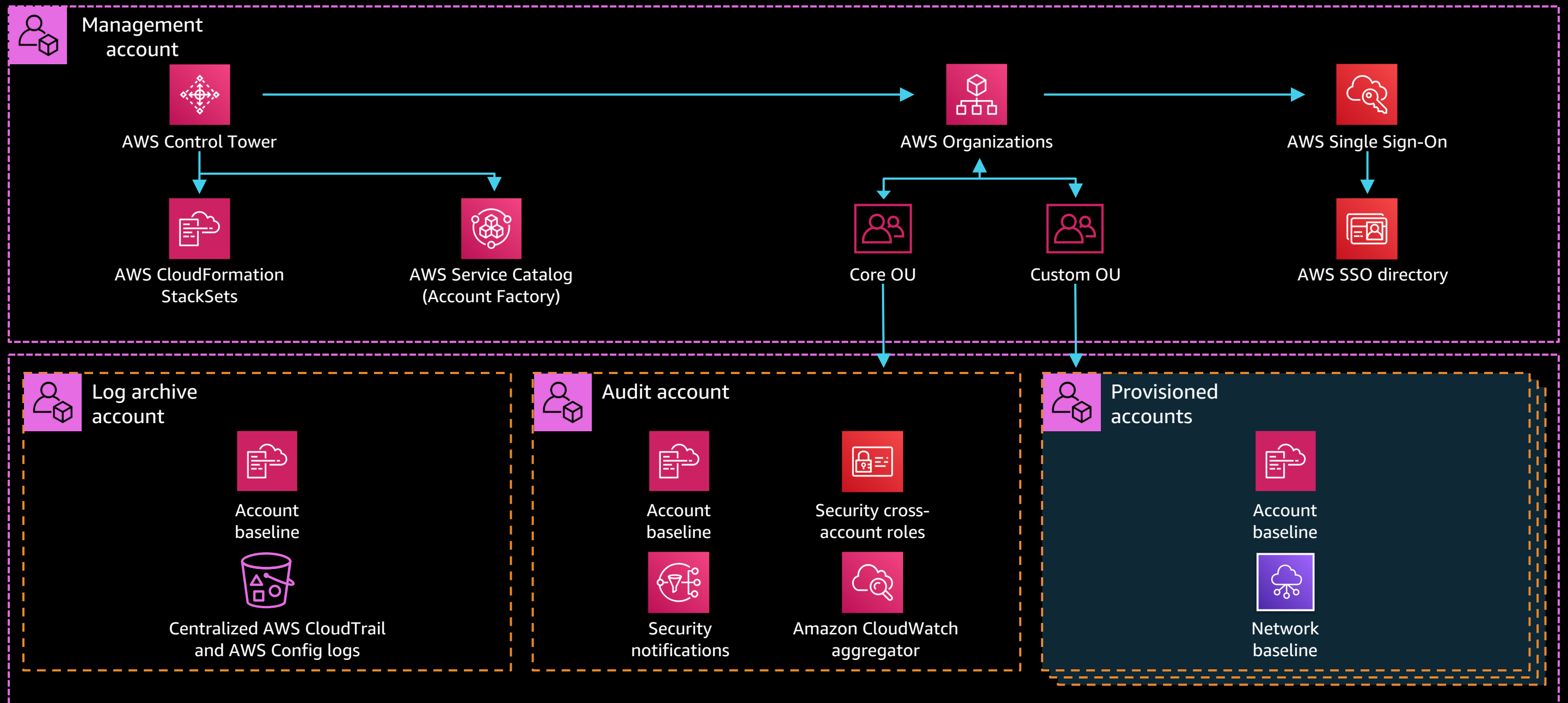


Built-in monitoring
and notifications

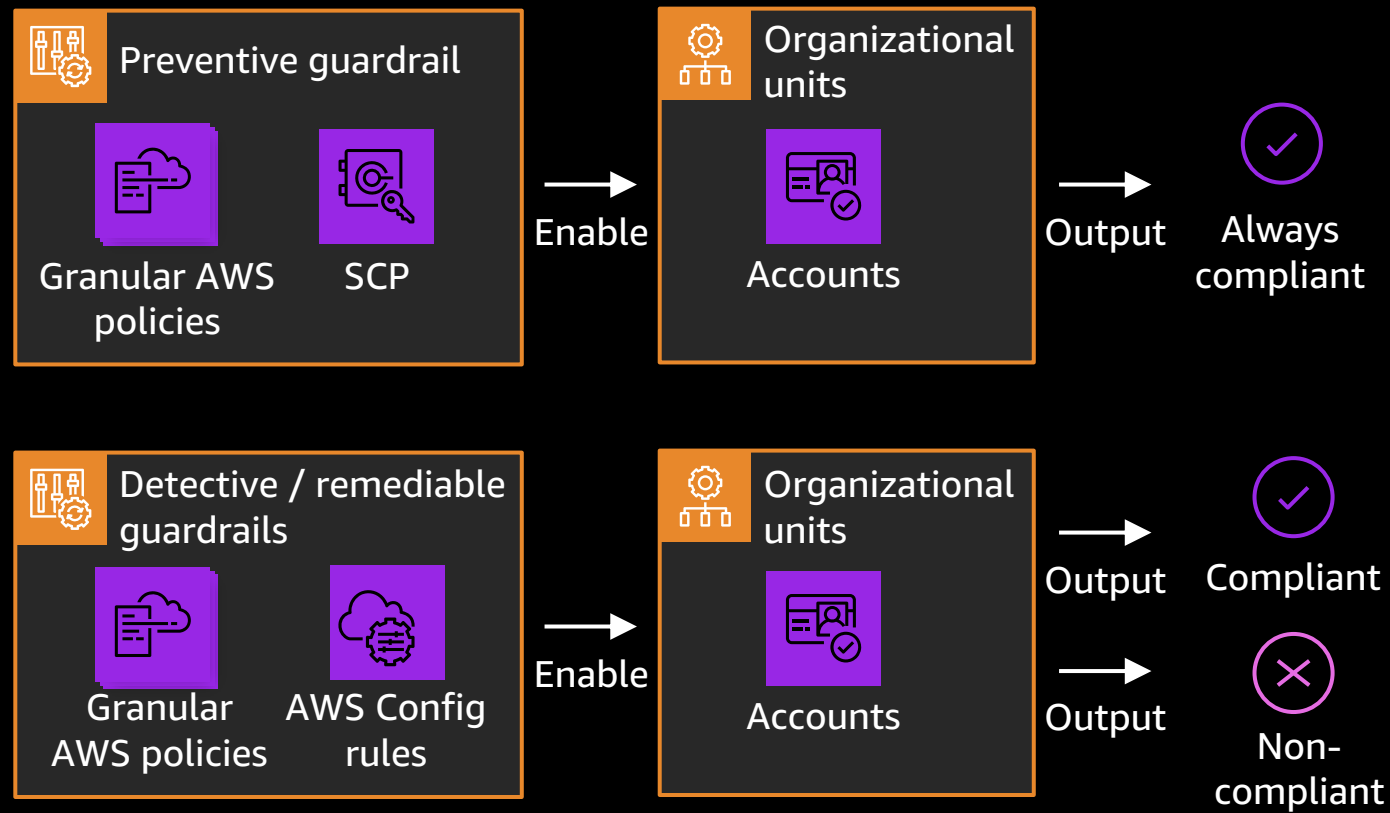


Automatic updates

AWS Control Tower setup



Establish guardrails



Automated provisioning through the AWS Control Tower

- Guardrails are preconfigured governance rules for security, compliance, change management, and operations
- AWS Control Tower applies the mandatory guardrails by default
- Applied guardrails become part of the account baseline

Preventive guardrails

- Prevents policy violations through enforcement
- Enhance preventative posture by adding SCPs, tag policies, IAM policies, Firewall Manager, and AWS CloudFormation StackSets and ChangeSets

Detective guardrails

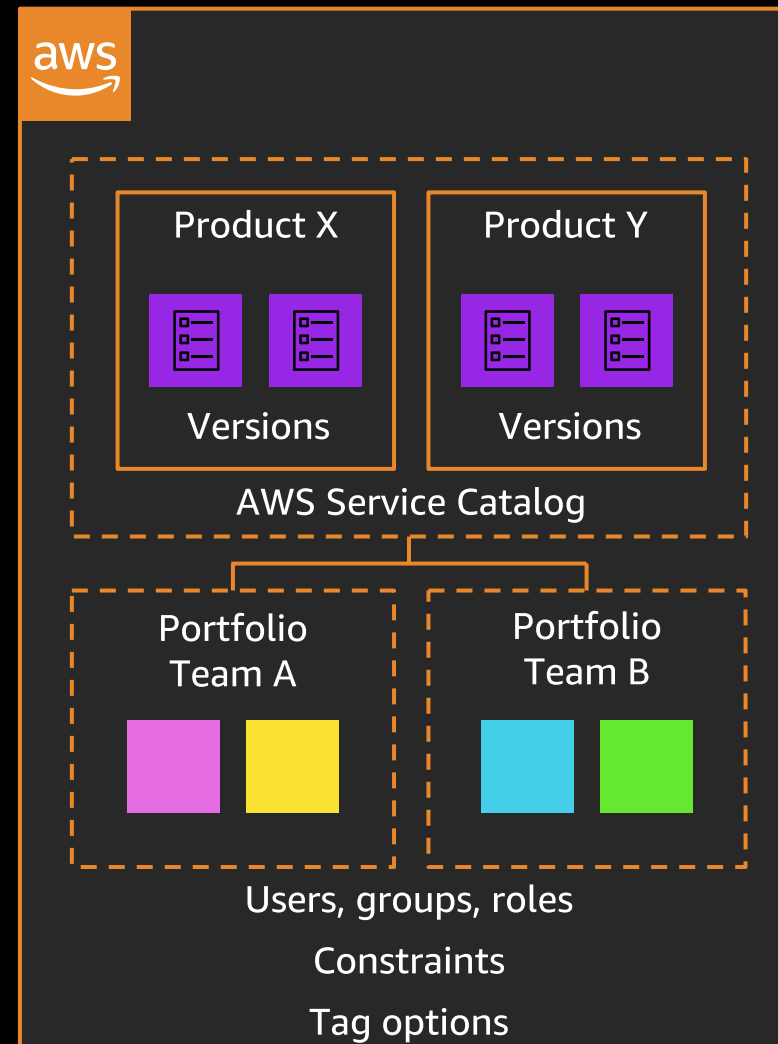
- Detects policy violations and alerts in the AWS Control Tower dashboards
- Add more controls using AWS Config rules, Macie, IAM Access Analyzer, and AWS Budgets

AWS Service Catalog: Simplifying provisioning



AWS Service Catalog end users
Users only see products they are entitled to and can launch, update, and terminate

2
Self-service provisioning



1
Organize and entitle



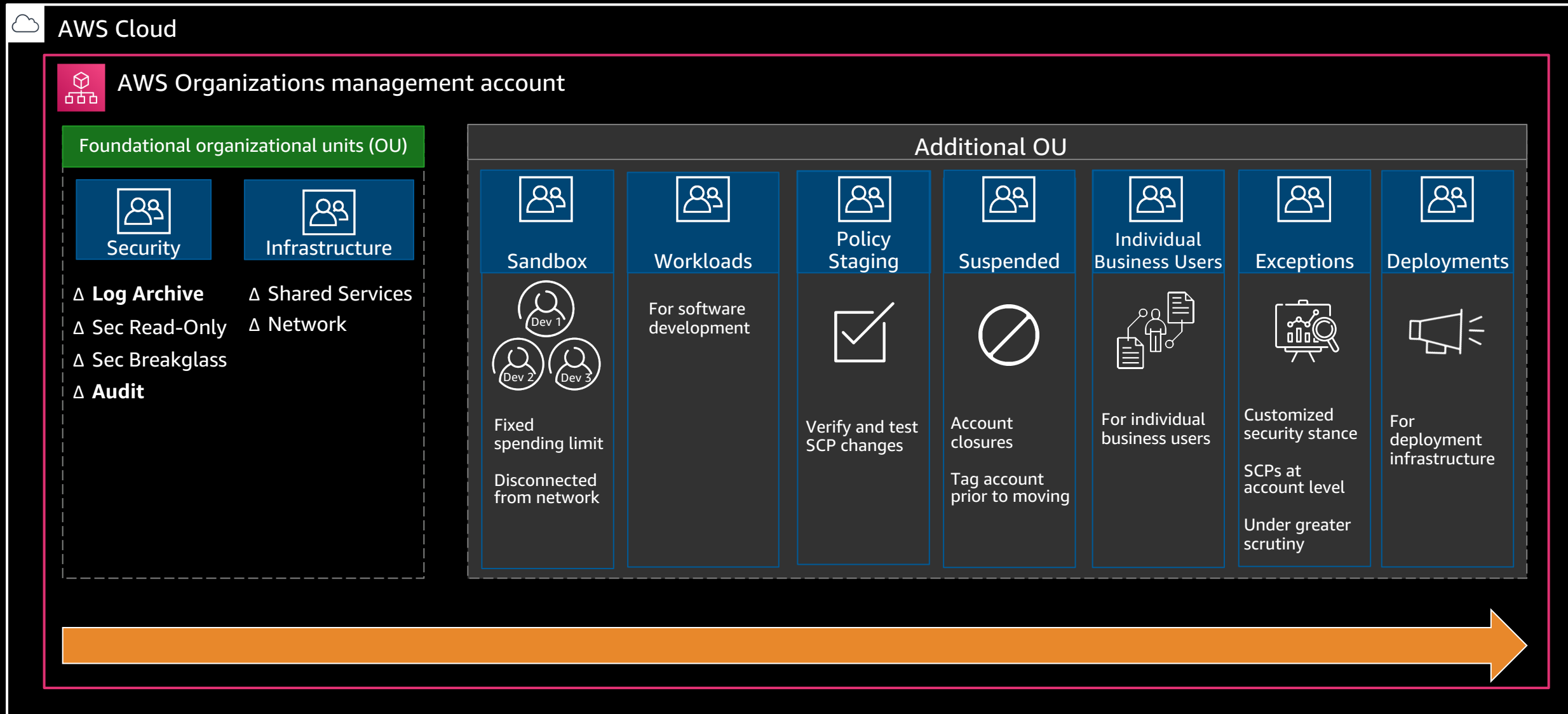
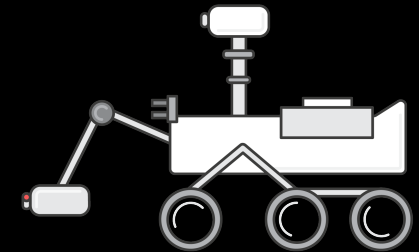
AWS Service Catalog administrator
Administrators organize, govern, and entitle users to portfolios of products

Service catalogs enable organizations to deploy and manage infrastructure and applications that reflect the organization's security and operational policies

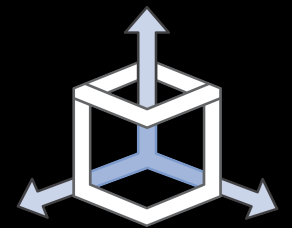
Best practices using AWS Control Tower



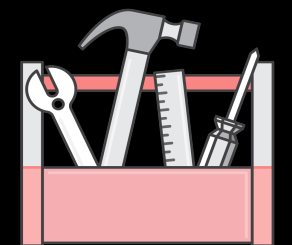
Extend AWS Control Tower to align to multi-account framework



Automated



Scalable



Self-service

Enrolling existing environment under AWS Control Tower governance

THREE PATTERNS TO ENROLL EXISTING ENVIRONMENT

- Deploy AWS Control Tower in new management account
- Create new accounts using Account Factory
- Migrate workloads in those accounts

- Deploy AWS Control Tower in existing management account
- Enroll existing AWS Organization units / accounts in the landing zone created by AWS Control Tower

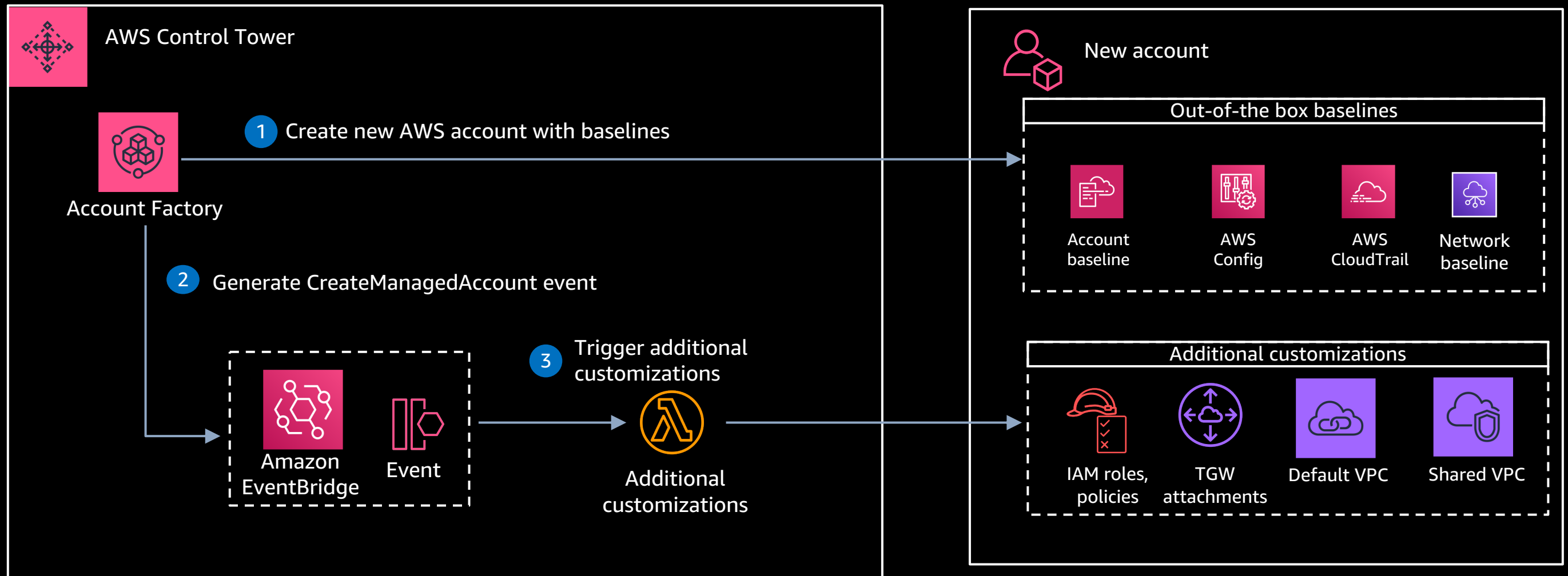
- Deploy AWS Control Tower in new management account
- Enroll existing AWS accounts in the newly created landing zone setup

AWS Control Tower life cycle events to add further customization and automation

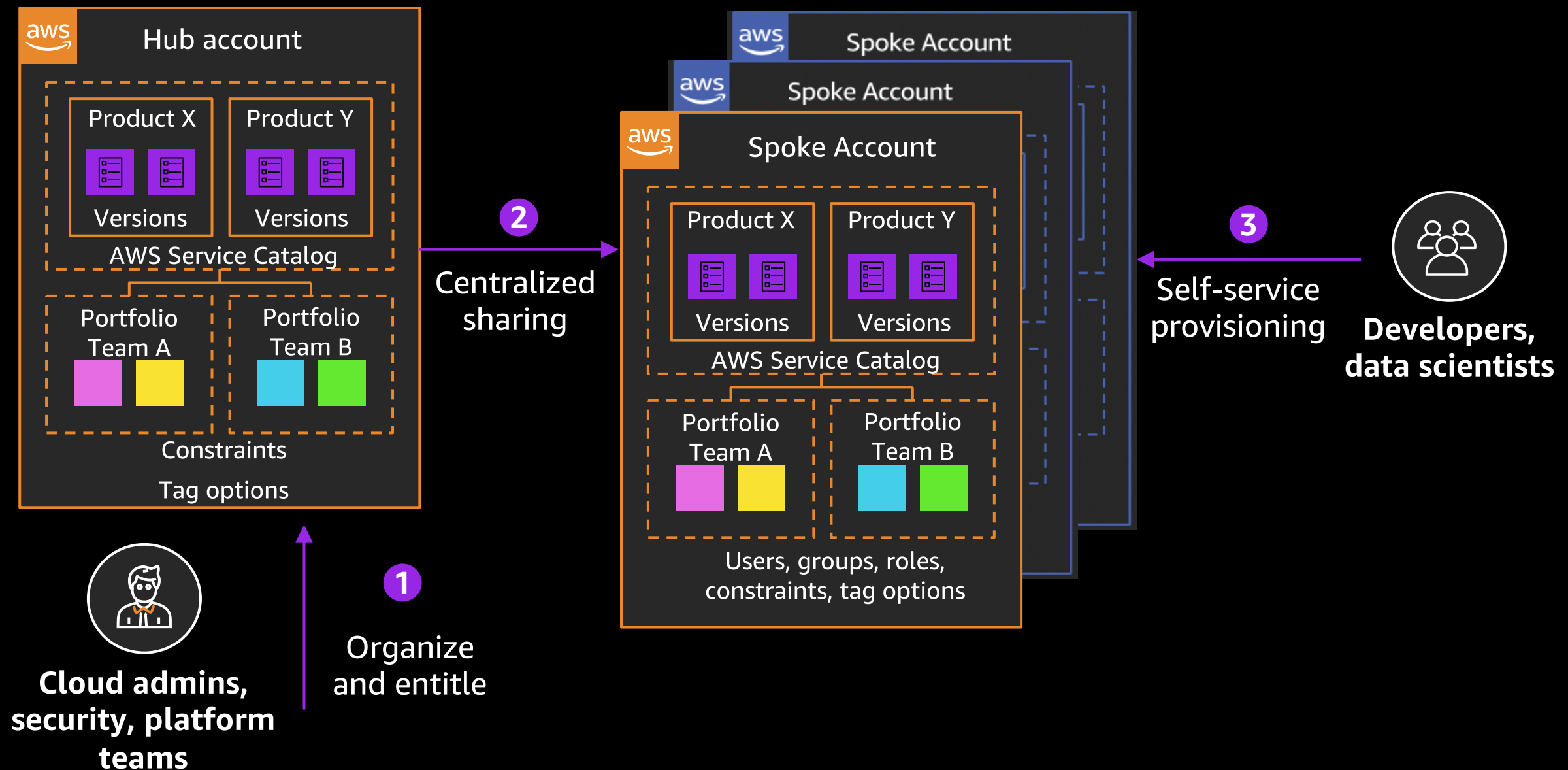
1. Add customization on top of base foundation – networking, identity management, logging strategies
2. Extend AWS Control Tower governance using AWS Config Conformance Packs
3. Centralized management of security tooling services (AWS Security Hub, Amazon GuardDuty) in audit account
4. Automate service limit increase and enterprise support
5. Integration with operational processes – ITSM, Asset Management, CMDB

Customization on top of the baseline

CreateManagedAccount – the log records whether AWS Control Tower successfully completed every action to create and provision a new account using Account Factory



Automate governance at scale in multi-account setup using AWS Service Catalog

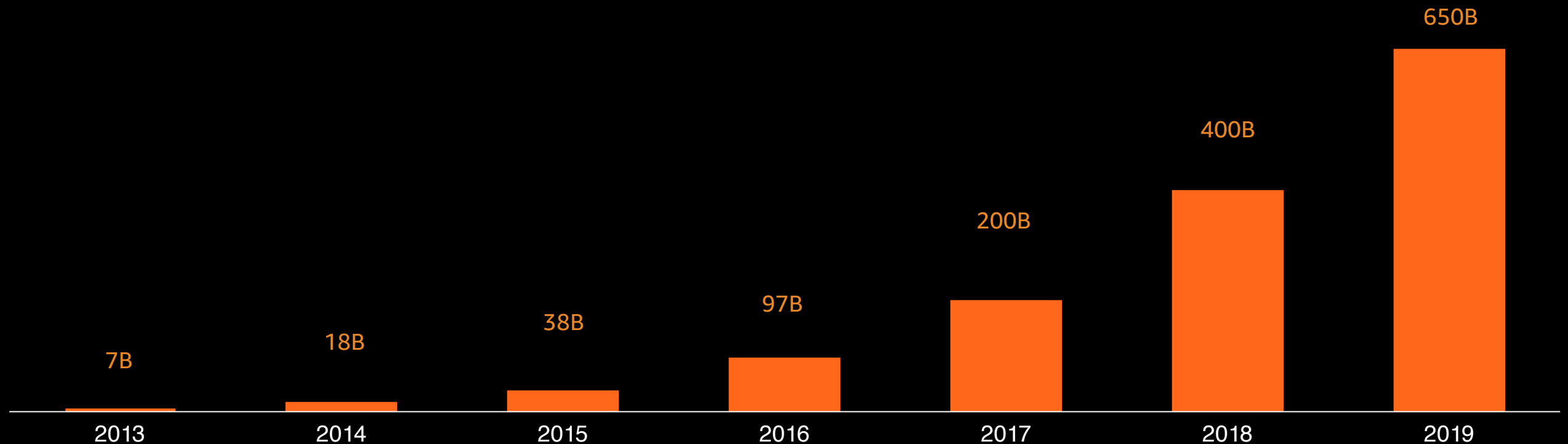


About NuData and the journey



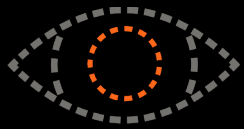
About NuData Security

Access to the world's largest behavioral network with billions of events monitored every year*

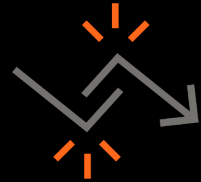


*This number is the combination of data points in our trust consortium, hashed and made unidentifiable as it crosses our network. Only the data from the clients connected to the consortium is included in the calculation.

About NuData Security



Recognize consumer patterns using behavioral biometrics



Block unauthorized access while removing unnecessary friction in real time



Leverage machine learning to detect evolving security risks

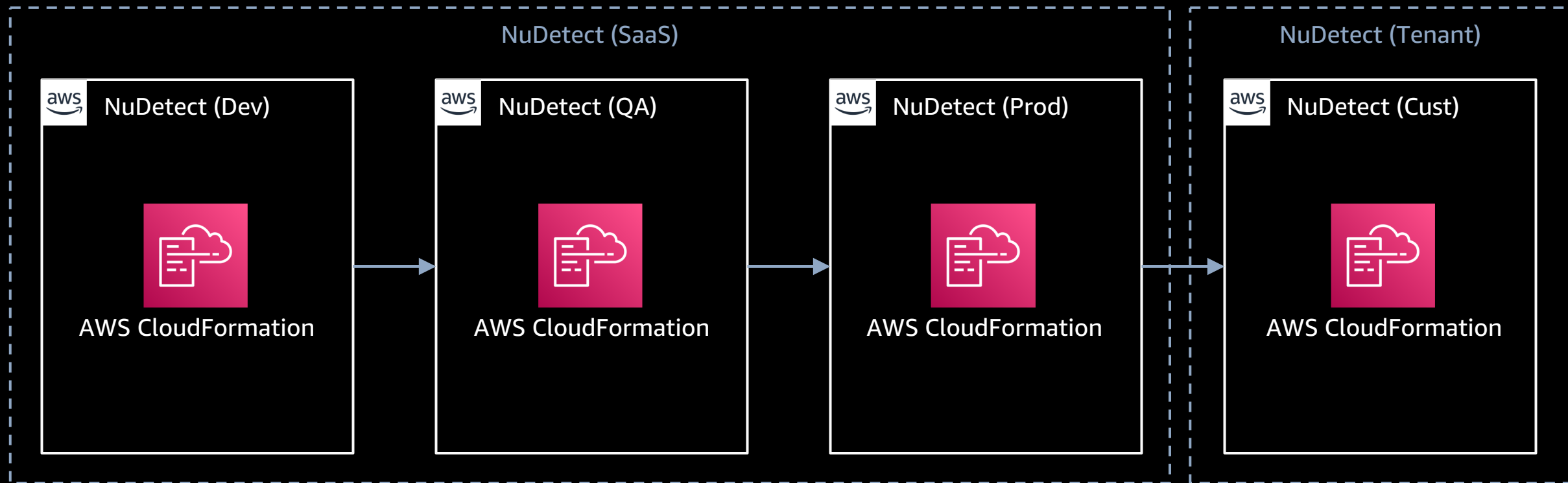


Using AWS Control Tower to simplify SecOps



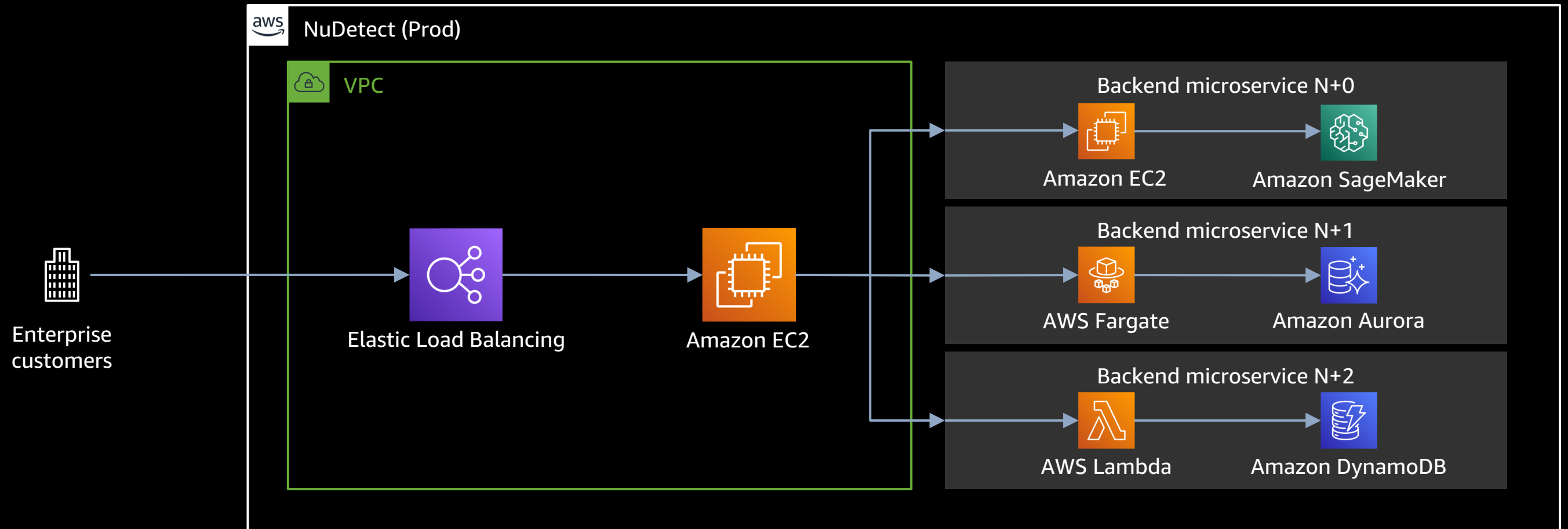
In the early days of NuData Security...

We had 3+ AWS environments, ranging from “dev” to “prod” to “cust”



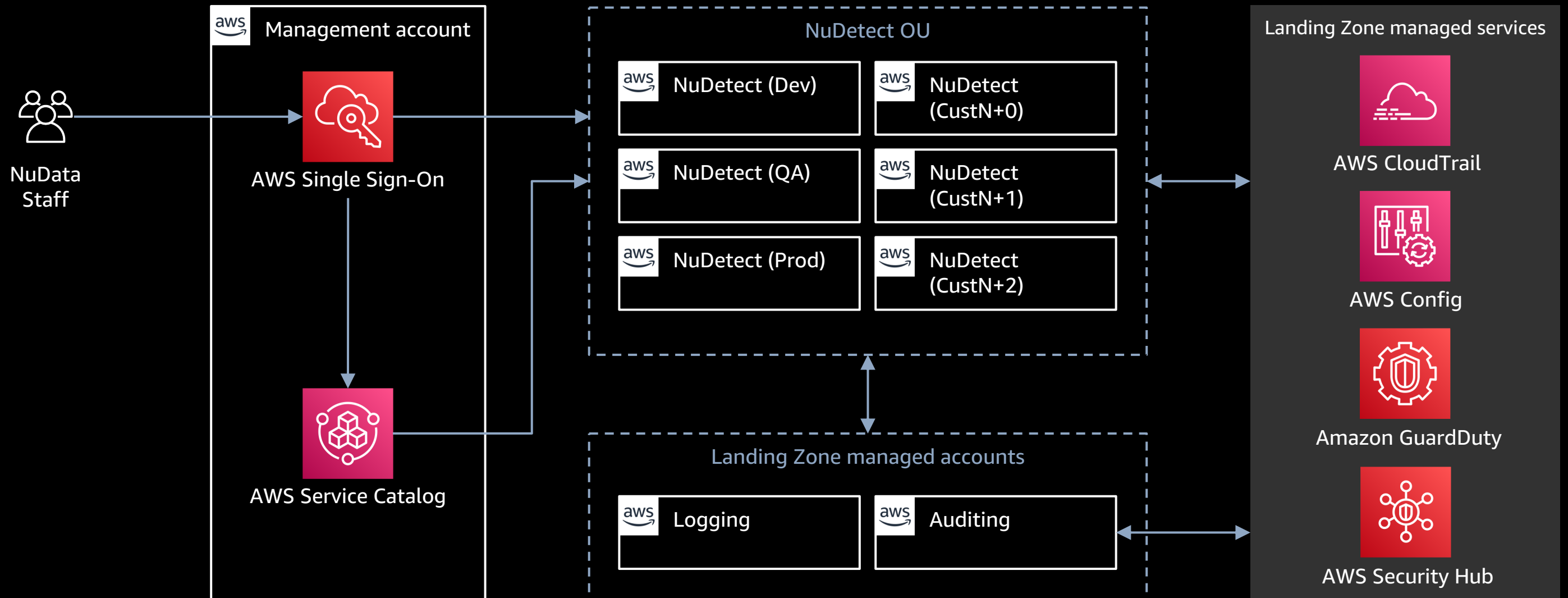
In the middle days of NuData Security...

CloudFormation stacks spawning more stacks were out of control



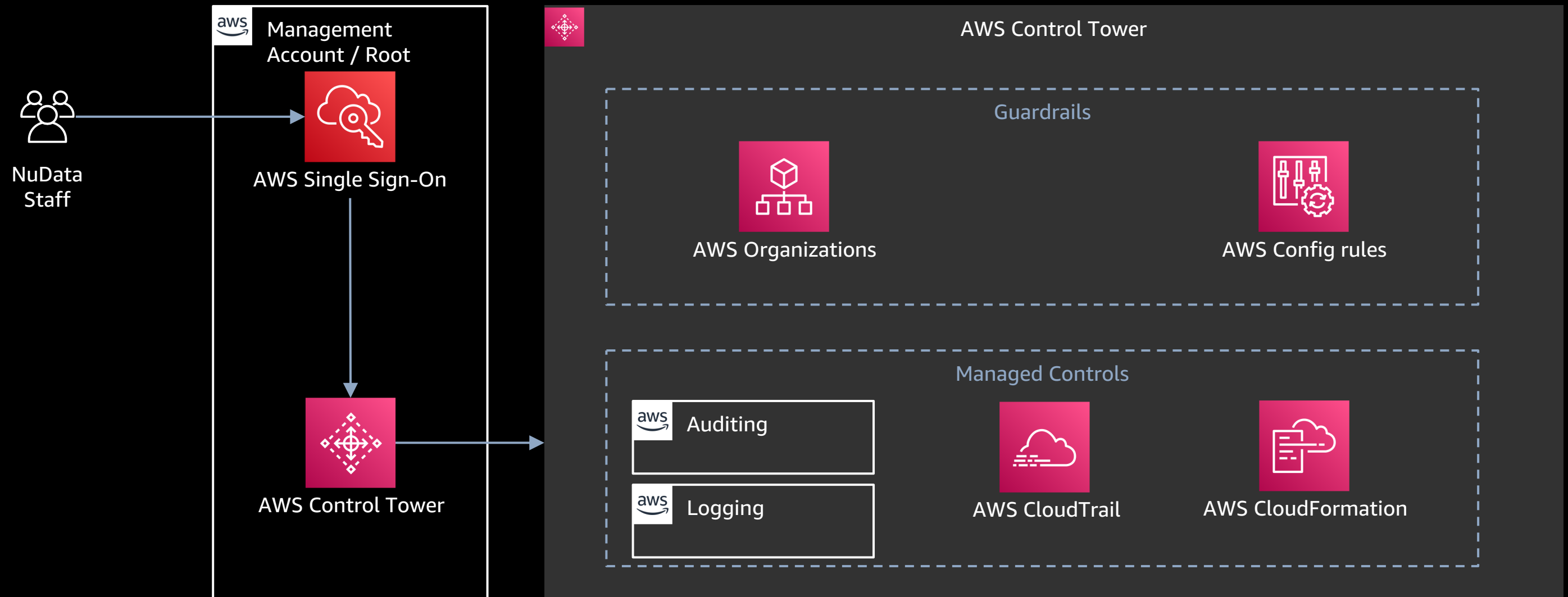
In the grown days of NuData Security...

AWS SSO and the AWS Landing Zone solution enabled rapid growth



Now, for the evolution of NuData Security...

AWS Control Tower simplifies multi-account and enhances security



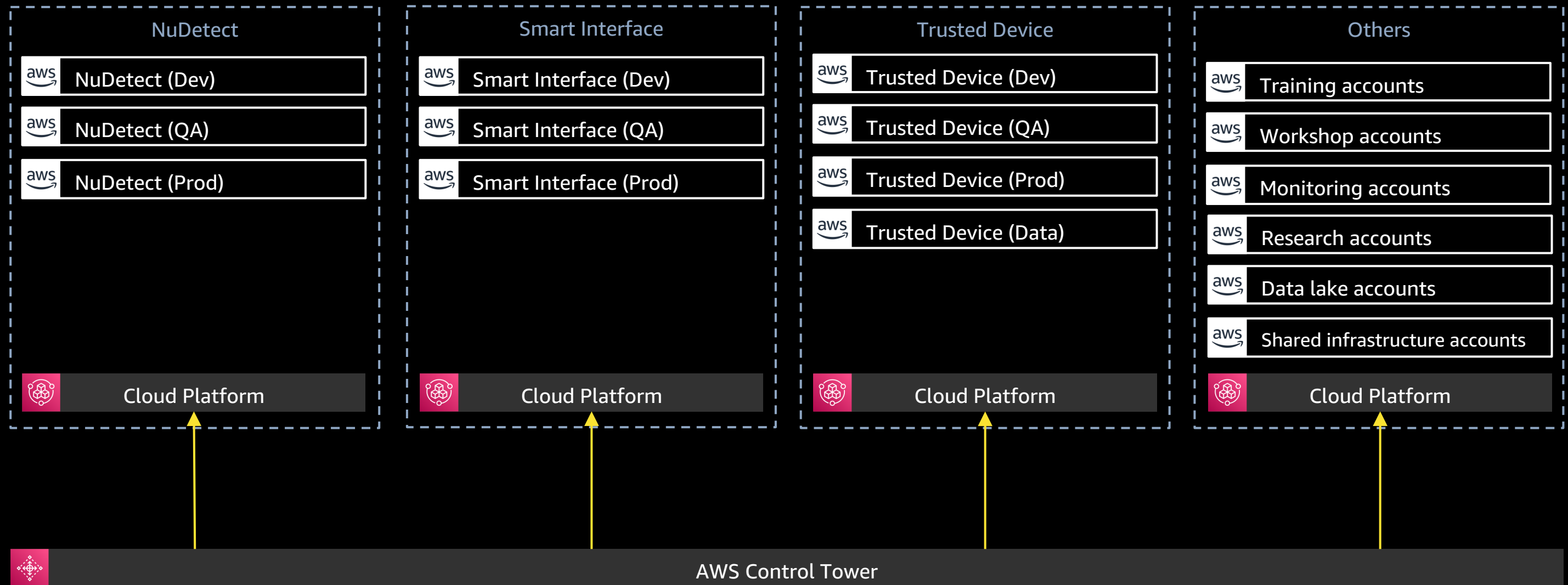
**“Our teams reduced
account provisioning
errors by 30% using
AWS Control Tower.”**

Kate O’Loughlin

Manager, Information
Security Operations
Mastercard

True multi-account support on AWS

AWS Control Tower enables the multi-account pattern



Extending AWS Control Tower to enhance operational guardrails



Language matters... and so do names!

The names of organizational units and accounts have a big impact

Organizational unit		Product name	Environment label
	(NuData)	Trusted Device	- Dev
	(NuData)	Trusted Device	- QA
	(NuData)	Trusted Device	- Prod

Affected services


AWS Organizations


AWS Control Tower

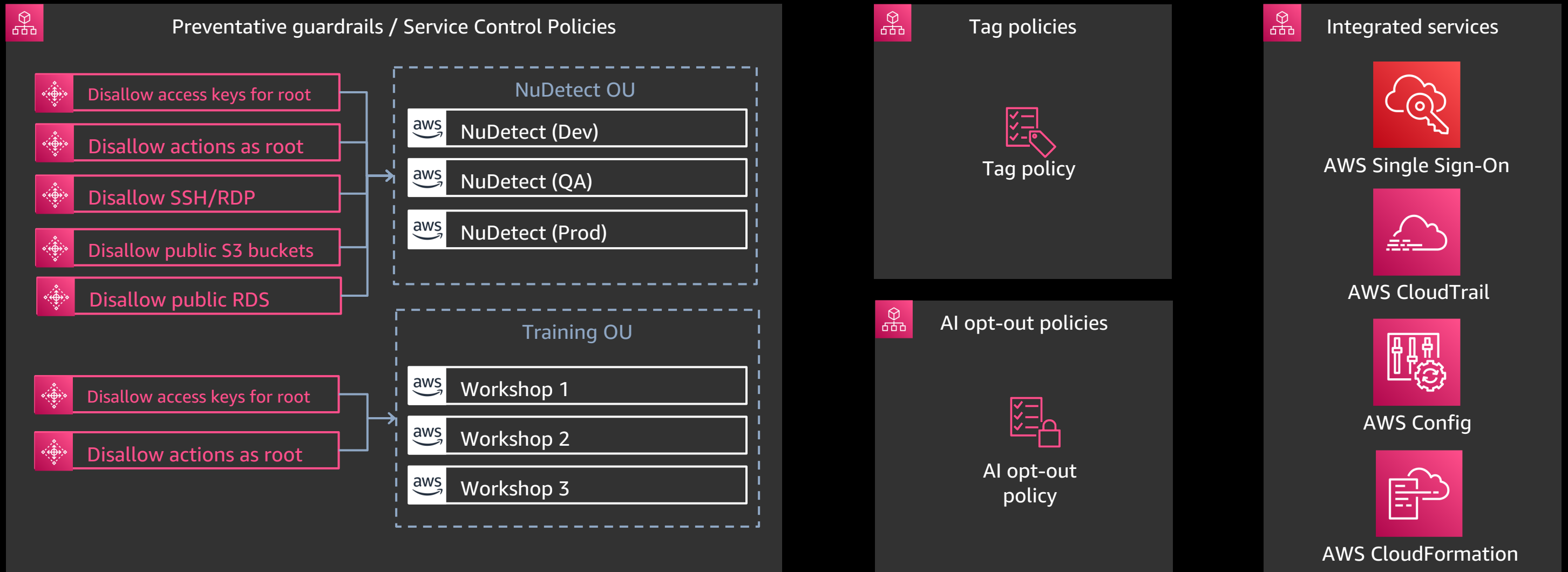

AWS Single Sign-On


Amazon GuardDuty


AWS Security Hub

Applying policy controls to AWS accounts

Integration of AWS Organizations is key to guardrail deployment



“The guardrails provided by AWS Control Tower added insights into our account compliance dashboards.”

Ian Cheng

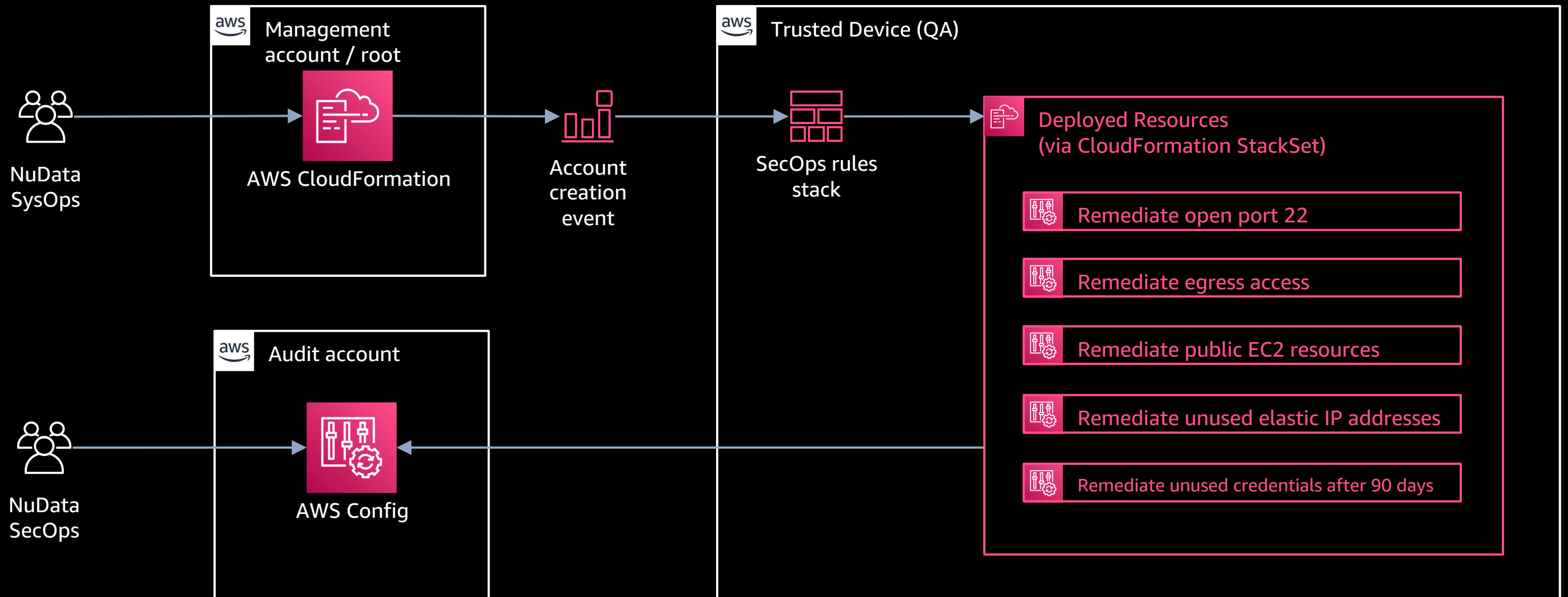
Director, DevOps Engineering
Mastercard

Deep dive into governance capabilities



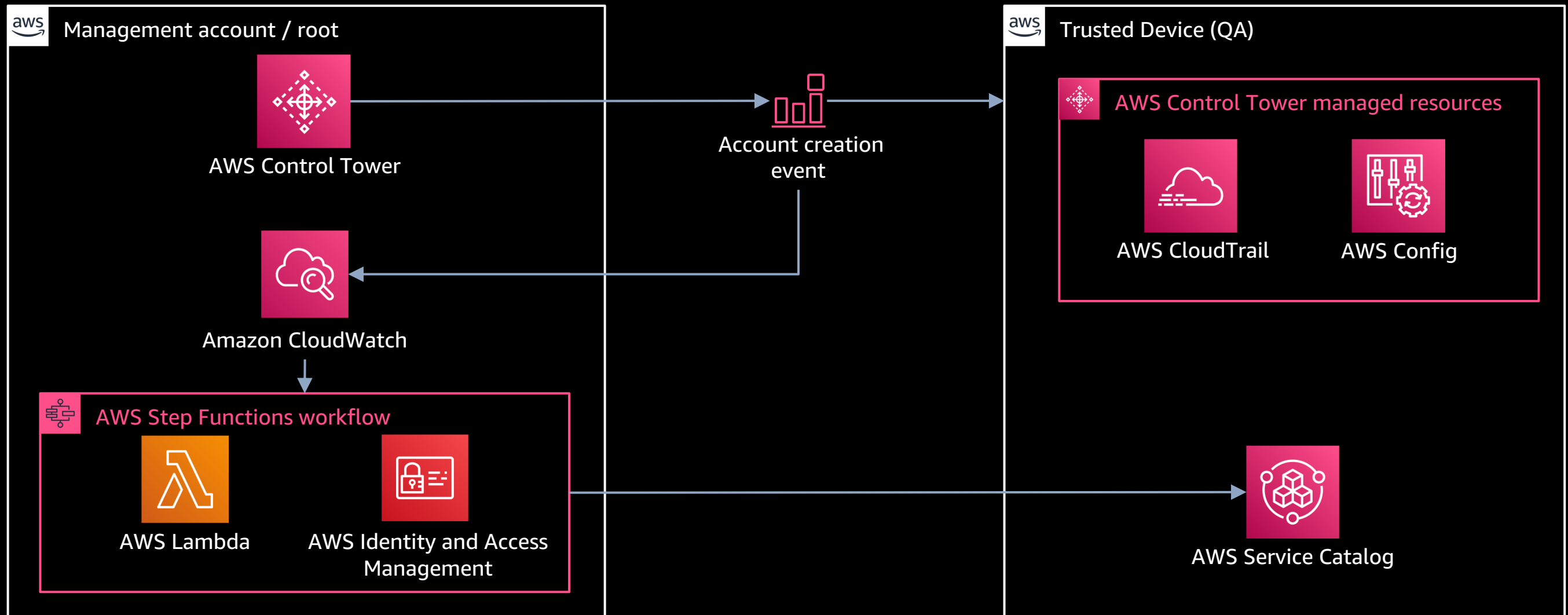
Identify and remediate issues with resources

AWS Config rules is a powerful auto-remediation tool



React to events and trigger custom workflows

Use account creation events to share product portfolios and more



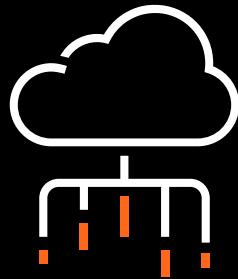
Next steps



Improve cloud governance through training



Double down
on training

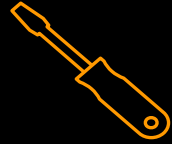


Power decisions
with data



Offload
undifferentiated
heavy lifting

How can you get started?



Activate AWS Control Tower

- Set up AWS Control Tower
- Whiteboard multi-account architecture
- Set up account onboarding integration



Set up for scale and operations

- Enroll existing accounts pilot
- Set up account enrollment automation
- Set up AWS Control Tower configuration / customization framework



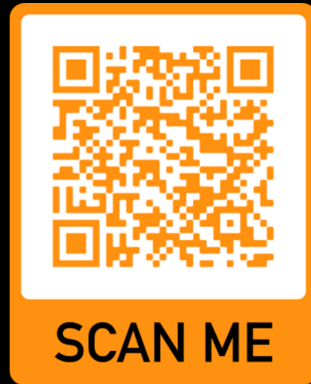
Accelerate adoption

- Enroll existing AWS accounts and organizational units
- Integrate partner / third-party solutions

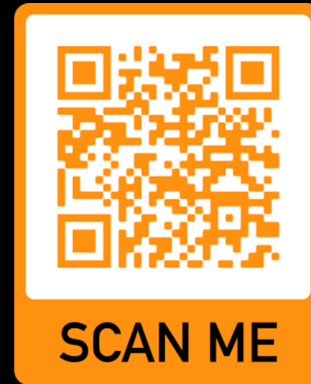
Learning resources



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/>

AWS Control Tower blogs:

- Guardrail mitigation: <https://tinyurl.com/y56dsalz>
- Self-service provisioning: <https://tinyurl.com/y3fk3fpk>
- Using AWS Config Conformance Packs for AWS Control Tower guardrail modeling: <https://tinyurl.com/CTModeler>
- 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 and governance): <https://tinyurl.com/y3yeohkm>

Thank you!





Please complete
the session survey