Organization Integration and Best Practices

Brian Eiler
CLOUD ARCHITECT

www.thecoursewaregroup.com

Overview

Trusted Access

Monitoring an Organization

Landing Zone

Security Hub

AWS Organizations: Best Practices

GLOBOMANTICS

“I understand that AWS Organizations allows centralized account management and control accounts’ access through policies. Are there any centralized services?”

Trusted Access

Trusted Access Overview

AWS Organizations integrates certain AWS services across its accounts

For this functionality, these services require permissions to perform tasks in the organization and its accounts

These permissions are allowed by enabling trusted access in AWS Organizations

Trusted access can be enabled or disabled

Trusted Access and Service-linked Roles

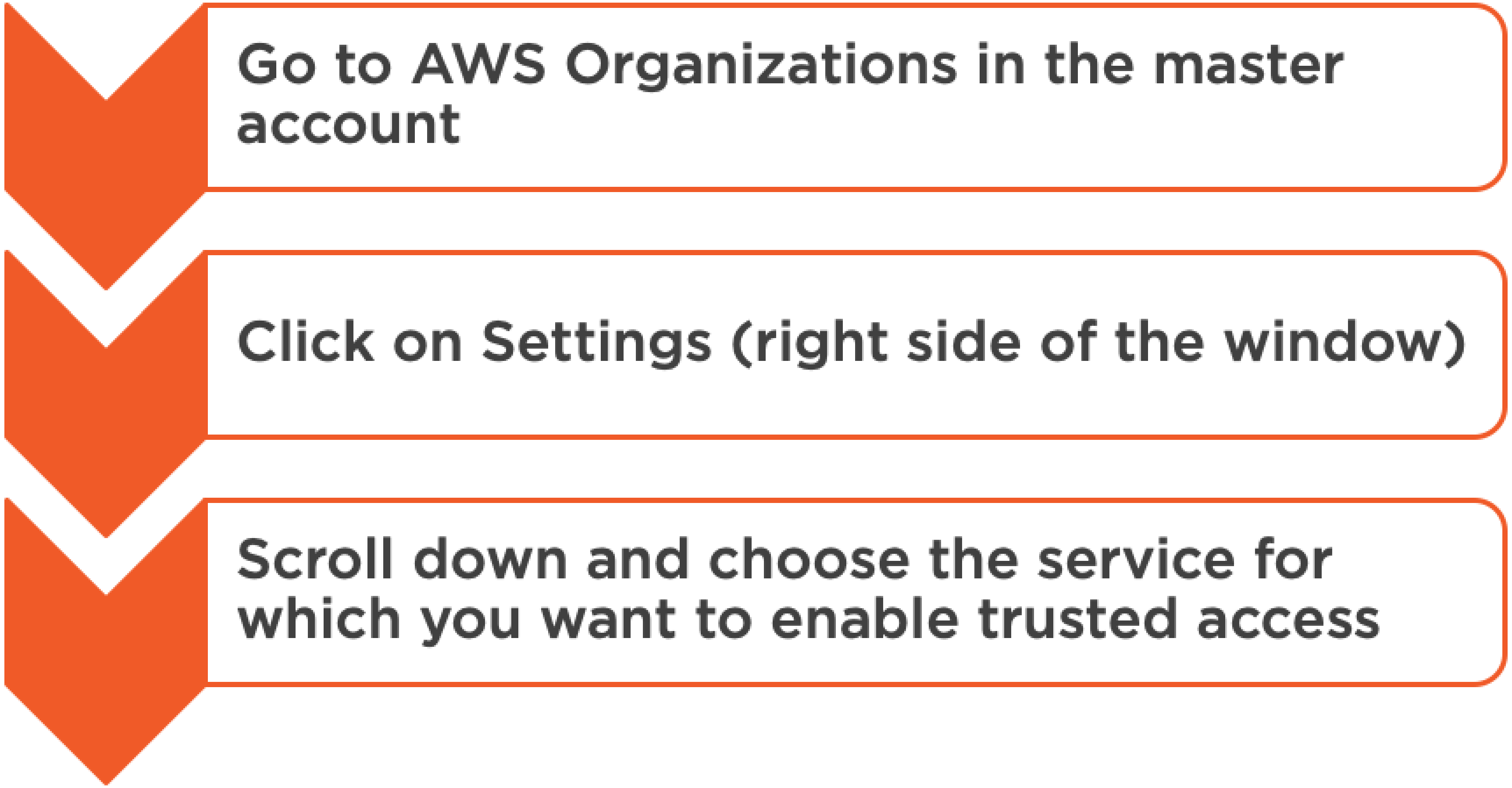
When trusted access is enabled for a service, an IAM service-linked role is automatically created in a member account

These roles are created asynchronously as needed

AWS manages all service-linked roles; therefore, it cannot be attached, detached, modified or deleted

Services use these roles to perform tasks in accounts

Enabling Trusted Access



1. Go to AWS Organizations in the master account
2. Click on Settings (right side of the window)
3. Scroll down and choose the service for which you want to enable trusted access

Trusted Access: Supported Services - Security

AWS Directory Service

AWS Single Sign-On (SSO)

AWS Firewall Manager

AWS Resource Access Manager (RAM)

Trusted Access: Supported Services - Compliance

- AWS Artifact
- AWS Config
- AWS CloudTrail
- AWS License Manager
- AWS Service Catalog

Trusted Access: AWS Directory Service

AWS Directory Service

AWS Managed Microsoft AD is a service that hosts and manages Microsoft Active Directory (AD) in the AWS Cloud

An account can share its directory with other accounts and VPCs within a region

Trusted Access: AWS Single Sign-on

AWS Single Sign-On

A service that centrally manages single sign-on (SSO) access to multiple AWS accounts and business applications

It can connect with AWS Managed Microsoft AD and allow existing Active Directory users to connect to the member accounts or use its own directory

Permissions to these users can be configured from the master account

Trusted Access: AWS Firewall Manager

AWS Firewall Manager

A service that centrally configures and manages firewall rules for Application Load Balancers and Amazon CloudFront distributions across accounts and applications

These firewall rules are configured in the master account once and automatically applied in the member accounts

Trusted Access: AWS Resource Access Manager

AWS Resource Access Manager

A service that allows you to share resources such as Transit Gateways, Subnets, Route 53 Resolver rules, and License Manager configurations

Can be shared with any account(s) or entire AWS Organizations

Create once and access like native resources in each shared account

Subject to the standard IAM permissions on the resources in each shared account

Trusted Access: AWS Artifact

AWS Artifact

Provides on-demand access to AWS’ security and compliance reports and certain online agreements

Master account can accept all agreements on behalf of the member accounts

Members accounts can still view and download agreements

Trusted Access: AWS Config

AWS Config

A service that continuously monitors, assesses, and records AWS resource configurations

All this configuration data can be aggregated from all member accounts into the master account

An administrator deploys a multi-account aggregator to gather data across regions and accounts.

This allows centralized compliance monitoring of all accounts in an enterprise

Trusted Access: AWS CloudTrail

AWS CloudTrail

A service that continuously monitors and records AWS API calls from the Management Console, CLI, SDKs, or direct API calls

Auditing data from all accounts in an organization is stored in a centralized S3 bucket

By default, member accounts can see the trails, but can’t change or delete them or access the S3 bucket with the logged data

Allows centralized compliance, risk, and governance monitoring of all accounts in an enterprise

Trusted Access: AWS License Manager

AWS License Manager

A tool to manage software licenses in AWS, on-premises, and even in other non-AWS clouds

Works with rules to define soft and hard limits for license utilization

Works with per vCPU, per physical core, or per machine licensing

This allows centralized license management throughout an enterprise

Trusted Access: AWS Service Catalog

AWS Service Catalog

A list of approved IT services that end users can self-deploy

Administrators can define the services, constraints (such as region or instance type) when deploying, and the users allowed to access each service

Services can be versioned

This allows centralized control and self-service of IT resources

GLOBOMANTICS

“At Globomantics, we currently use Active Directory. We can certainly implement AD on AWS and manage all existing users centrally via the AWS Single Sign-On service. This will achieve one of our compliance requirements.”

Monitoring an Organization

Monitoring the Master Account

AWS Config

AWS CloudTrail

AWS CloudWatch Events

AWS CloudWatch

Amazon CloudWatch

A monitoring and management service that:

- Monitors AWS resources and applications
- Collects monitoring data through metrics, logs and events
- Uses alarms to notify or automate actions

AWS CloudWatch Events

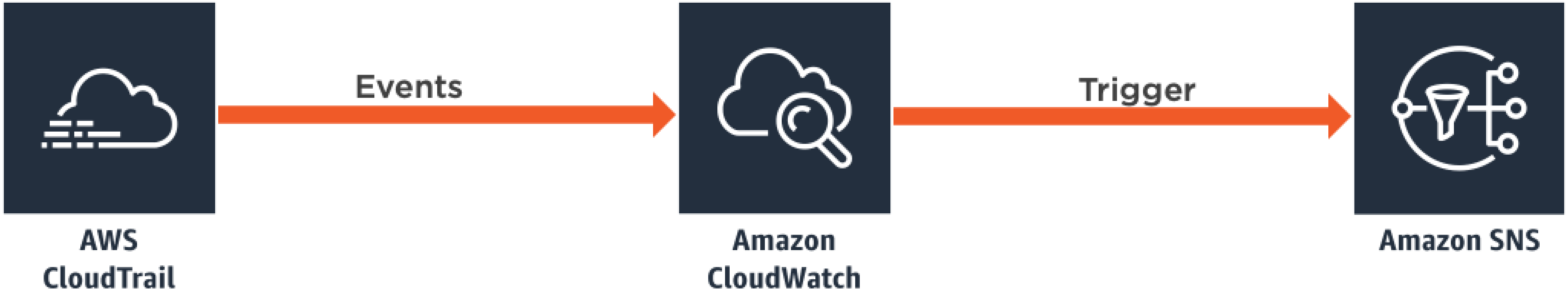
A stream of system events describing changes in AWS Resources

Events recorded by AWS CloudTrail can be monitored by AWS CloudWatch Events

Rules can be created to match certain events in CloudTrail

These rules can trigger actions on other AWS resources

AWS CloudWatch Events: Event Flow Example



```
[…]
"eventTime": "2018-08-30T21:42:18Z",
"eventSource":
"organizations.amazonaws.com",
"eventName": "CreateAccountResult",
[…]
```

GLOBOMANTICS

"At Globomantics, using multiple accounts will be necessary. AWS Organizations will help, but how do we get started? There seems to be so much to do before we do anything, and doing it according to best practices sounds very challenging."

Landing Zone

Saving Time with Landing Zone

Multi-account structure

Account Vending Machine

User access

Security baseline

Notifications

Multiple Account Structure

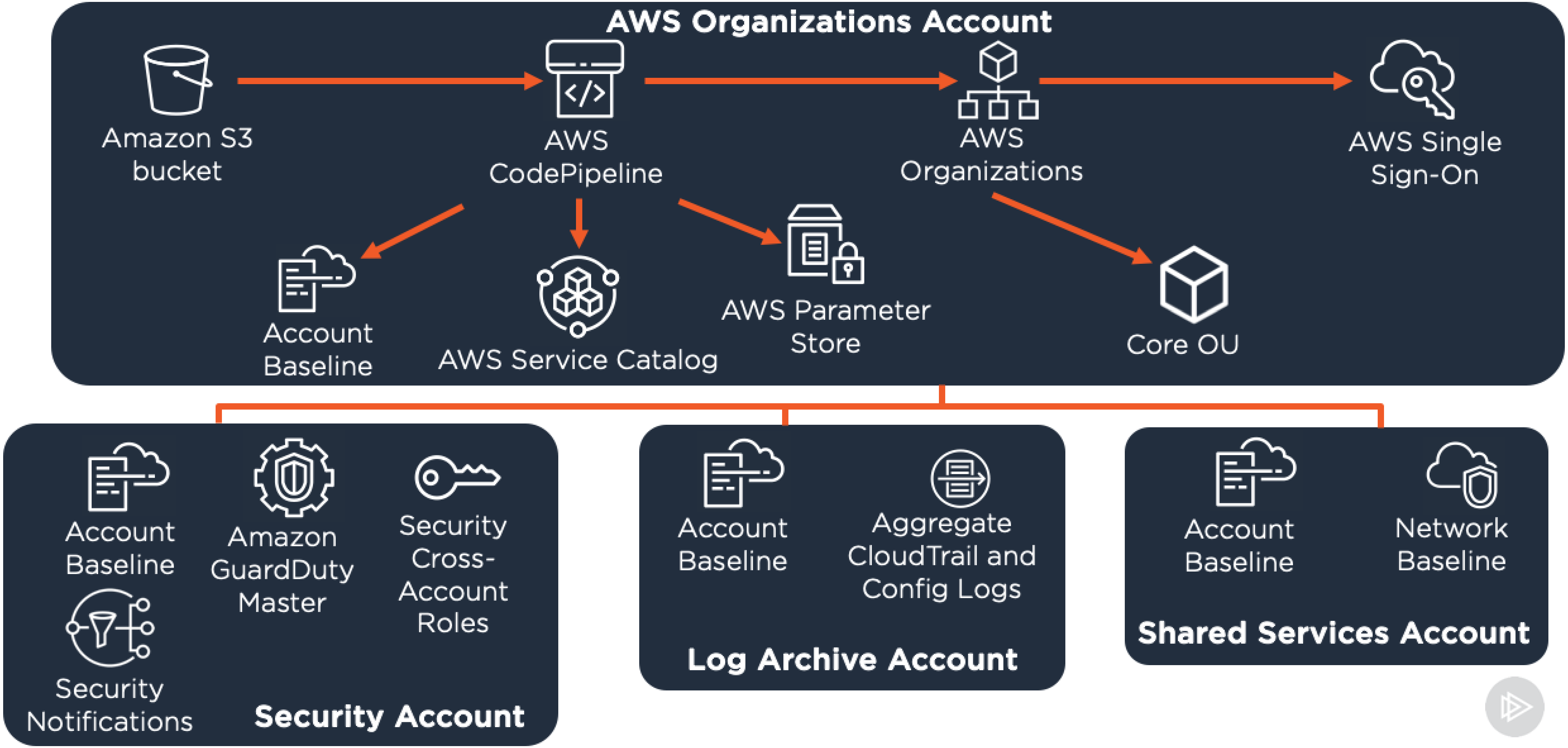
AWS Service Catalog

Includes four accounts:

- AWS Organizations account
- Shared services account
- Log archive account
- Security account

Deployed using AWS Service Catalog

Multi-account Diagram



Account Vending Machine (AVM)

Permissions

AWS Service Catalog

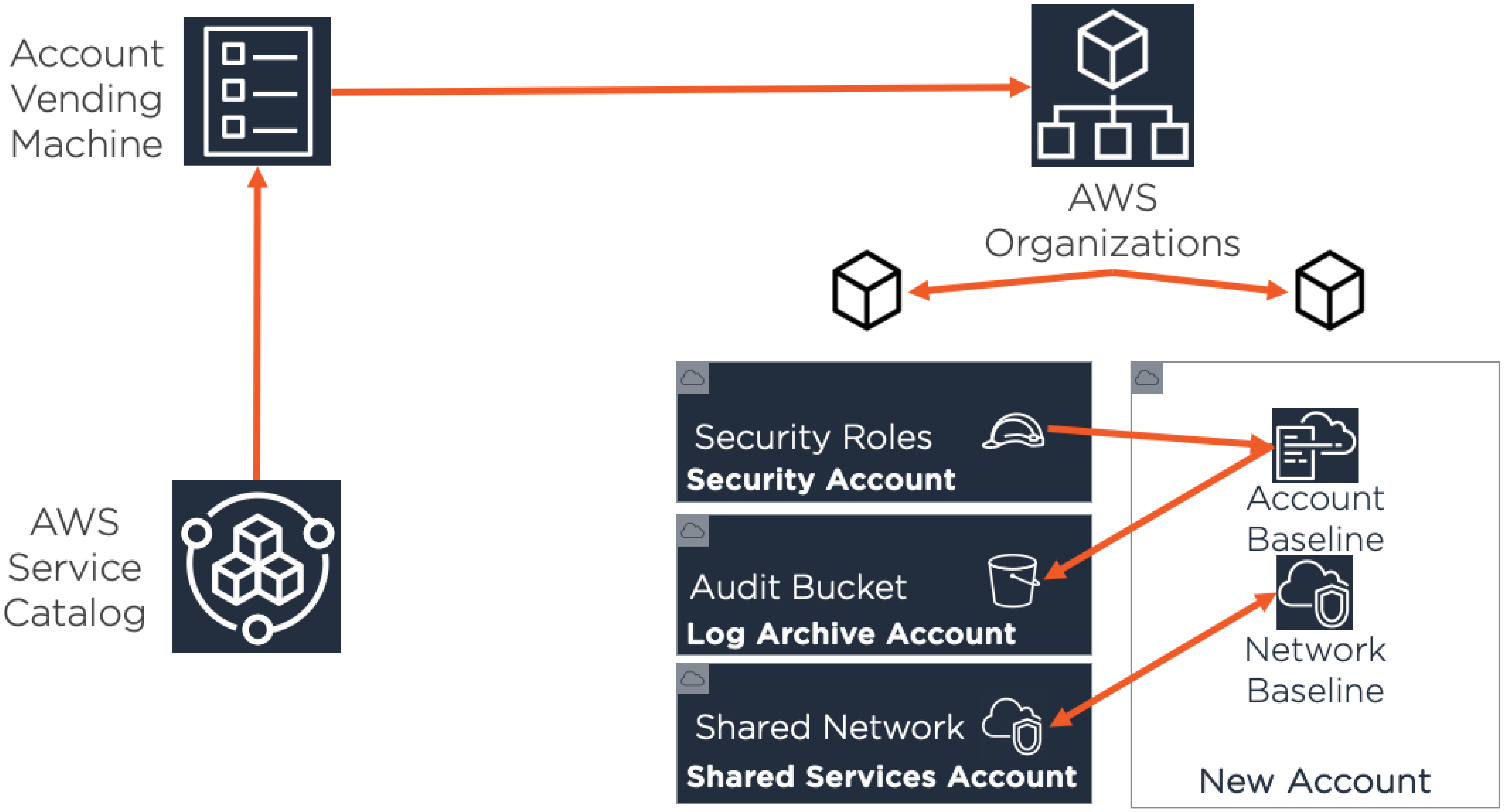
Allows users to create new accounts in Organizational Units

Uses AWS Service catalog to give administrators permissions in Landing Zone

Leverages launch constraints

Deploys account and network baselines in each new account

AVM Diagram


Account
Vending
Machine
AWS
Organizations
AWS
Service
Catalog
Security Roles
Security Account
Audit Bucket
Log Archive Account
Shared Network
Shared Services Account
Account
Baseline
Network
Baseline
New Account

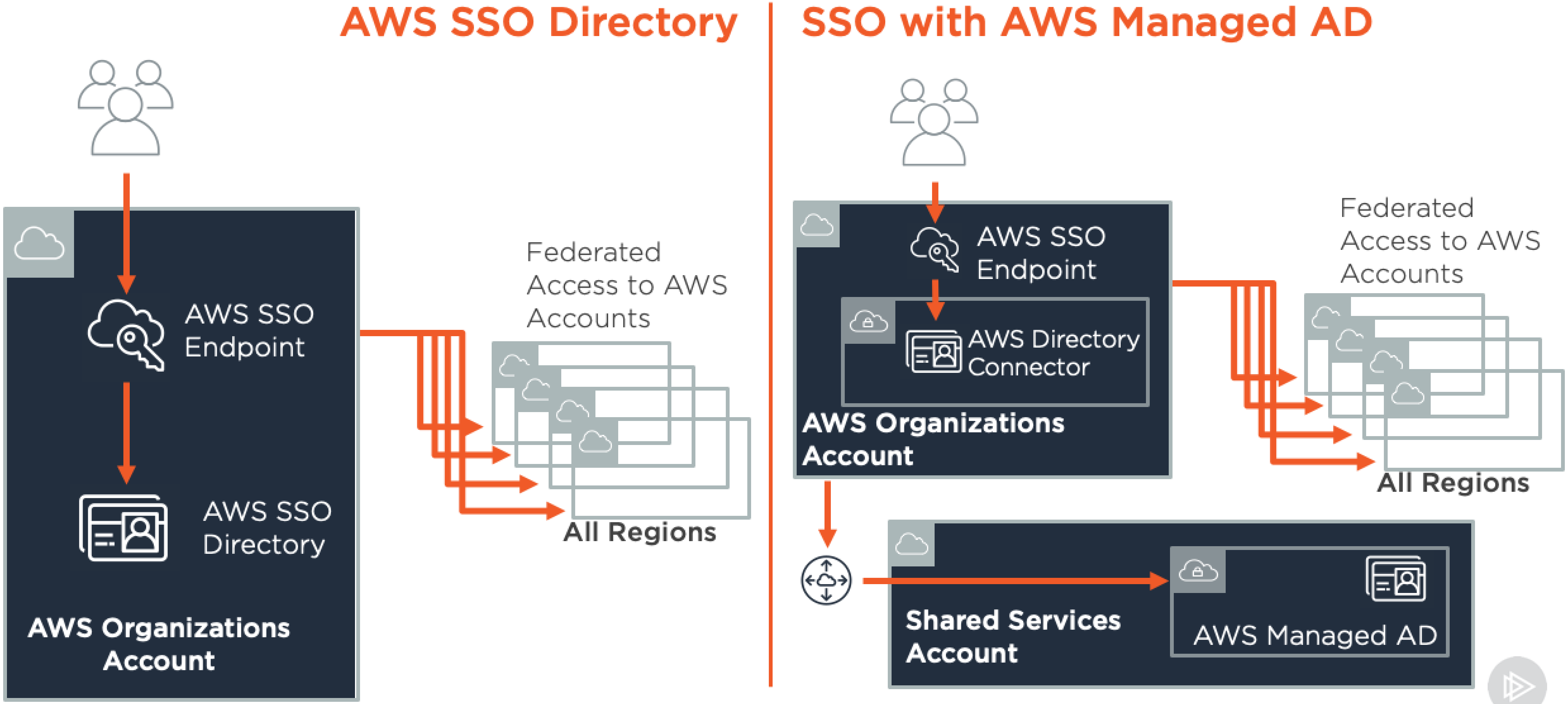
User Accounts

AWS Single Sign-On

Two options to store users and groups

- SSO with AWS SSO Directory
- SSO with AWS Managed Microsoft Active Directory

User Access Diagram



Security Baseline

Initial baseline comes with Landing Zone and can be customized

Settings include:

- CloudTrail
- AWS Config and Config rules
- AWS IAM password policies
- VPC setup and peering
- GuardDuty

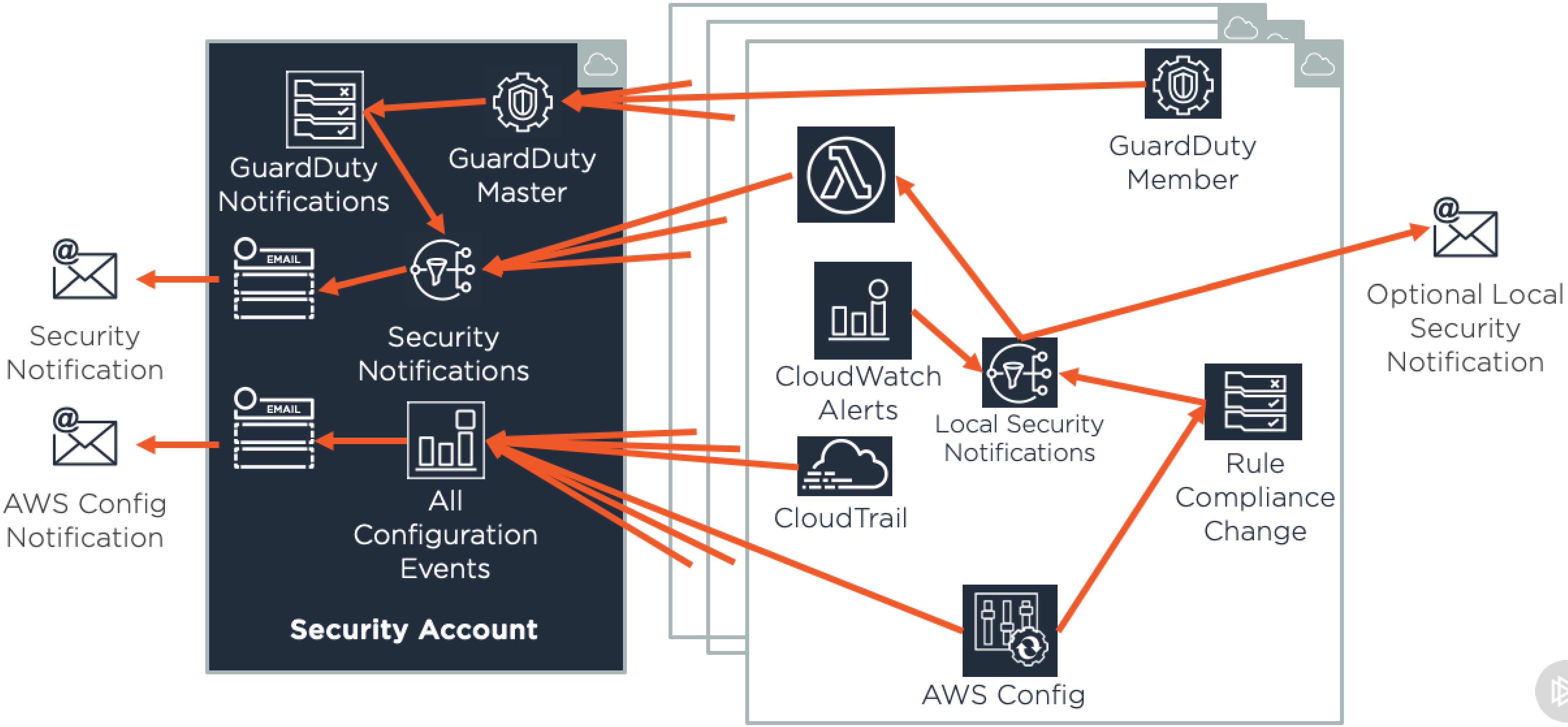
Notifications

Notifications to operations and security personnel are automated

Landing Zone uses CloudWatch and GuardDuty notifications via SNS to send notifications like:

- Sign-in failures
- API authentication failures
- Changes to account
- Changes to resources

Notification Diagram



GLOBOMANTICS

"Landing Zone appears to get us going quickly and according to best practices. Our concern, though, is drowning in notifications and monitoring our compliance status."

Security Hub

Security Simplified

Simple dashboard view of security alerts and compliance status

Aggregates, organizes and prioritizes security alerts and findings across AWS services

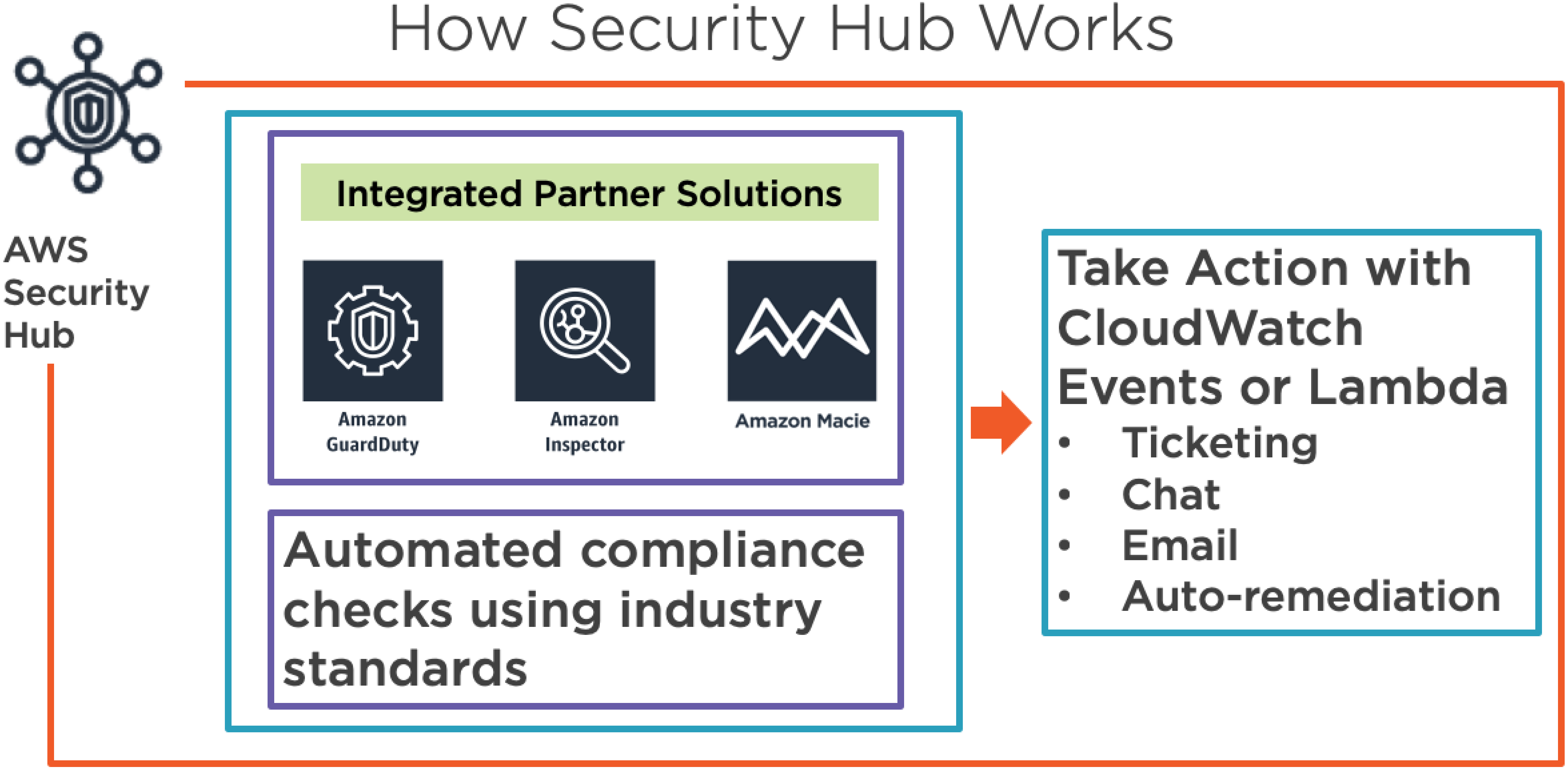
Benefits of Security Hub

Save time

Improved compliance

Quick action

How Security Hub Works



AWS Security Hub

Integrated Partner Solutions

Amazon GuardDuty

Amazon Inspector

Amazon Macie

Automated compliance checks using industry standards

Take Action with CloudWatch Events or Lambda

- Ticketing
- Chat
- Email
- Auto-remediation

Partners Include

ALERT LOGIC®

IBM Security

f5®

Check Point®
SOFTWARE TECHNOLOGIES LTD.

McAfee™
Together is power.

Barracuda®

splunk>®

Symantec.™

TREND MICRO™

AWS Organizations: Best Practices

Create a Strategy for Multiple Accounts

Define Multi-account Strategy

Match account grouping to corporate structure

Understand the purpose of the account

Use organizational units (OUs)

Plan out nested hierarchies in advance

Secure the Master Account

Secure Master Account

Apply MFA on root of the master account

Apply strict least privilege principal

Apply MFA for all users on the master account

Turn on AWS CloudTrail

Don’t use the master account to create or manage resources

Manage SCP Rollouts

Manage Rollouts

Create a testing OU with an account

Test changes on this testing OU and account before applying changes to the other accounts

Do a gradual rollout starting from lowest level of the hierarchy

Consider the Lifecycle of Accounts

Think about Account Lifecycle

Create a 'Deny-All' OU

Move an account with security issues to this OU

To remove an account

- Log in from master account using IAM role
- Delete all resources
- Close the account

Automate

Minimize Human Interaction

Recognize automatable tasks

Develop scripts to automate processes such as account creation and movement of accounts to the appropriate OU

Monitoring and Auditing

Monitor and Audit

Create a separate dedicated account (instead of using master account)

Write and secure all audit logs to a dedicated logging account

Use AWS Config, AWS CloudTrail, Amazon CloudWatch Events, and more

Separate security and audit roles in all accounts

Utilize SCPs

Leverage SCPs

Use either whitelist or blacklist (stick with one approach for the organization)

Test and review policy results using IAM policy simulator

Attach SCPs to OUs instead of individual accounts whenever possible

Federate

Leverage Federation

Configure federated access to all accounts

Utilize trusted access for AWS Directory Service and AWS Single Sign-On

Summary

Trusted Access

Monitoring an Organization

Landing Zone

Security Hub

AWS Organizations: Best Practices