# AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

SEC203

# AWS Security Reference Architecture: Visualize your security

Neal J. Rothleder (he/him)
AWS Professional Services
Security & Infrastructure Global Specialty Practice
Amazon Web Services

Andy Wickersham (he/him)
AWS Professional Services
Security & Infrastructure Global Specialty Practice
Amazon Web Services

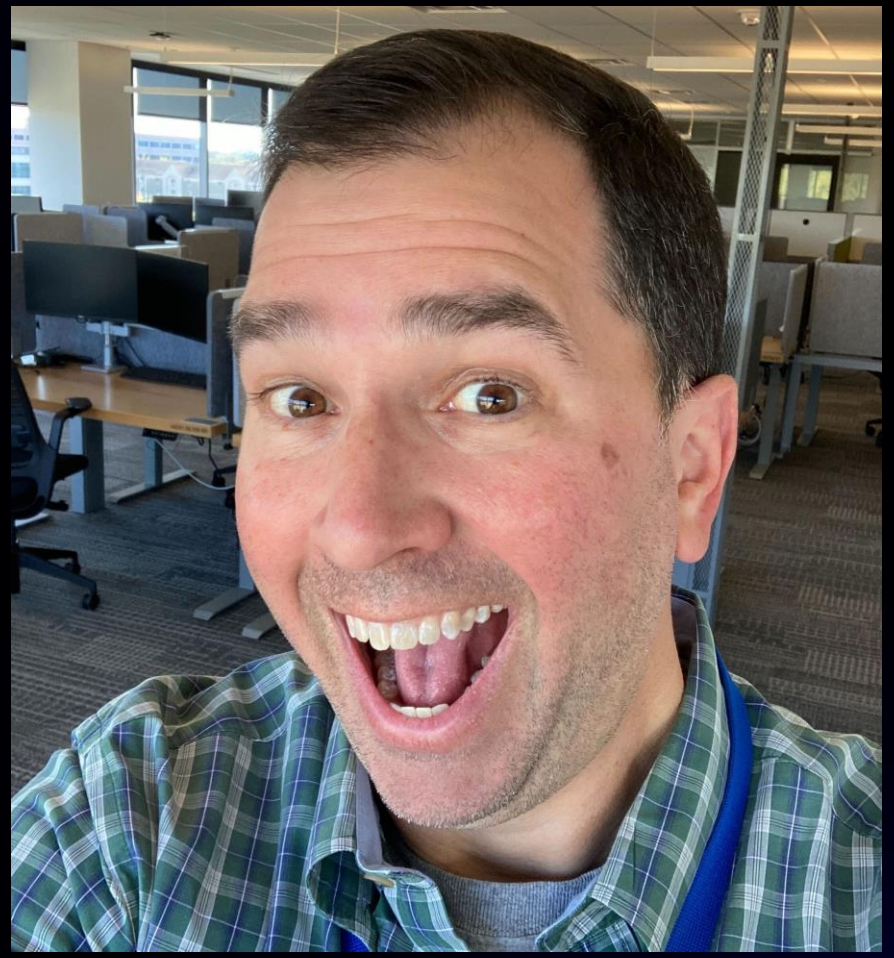
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# With a mask, people look so serious



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

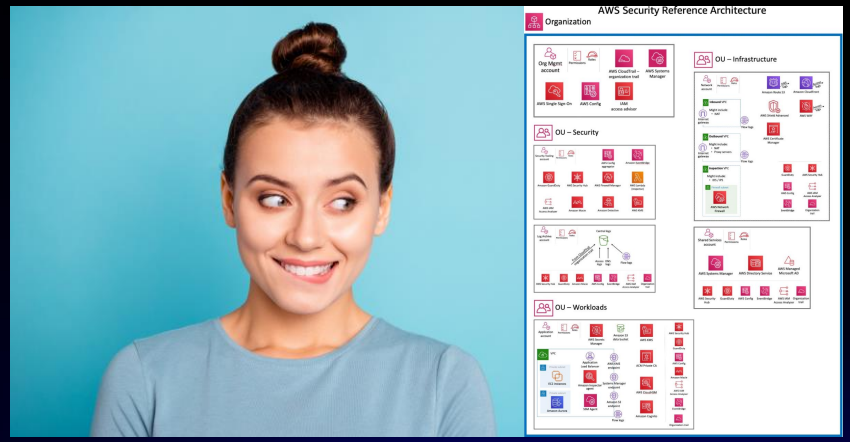
# Assume they look like this under the mask



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# What we will cover

- What the AWS Security Reference Architecture (AWS SRA) is and why it matters to you
- Share some highlights
- How to navigate the documents and code



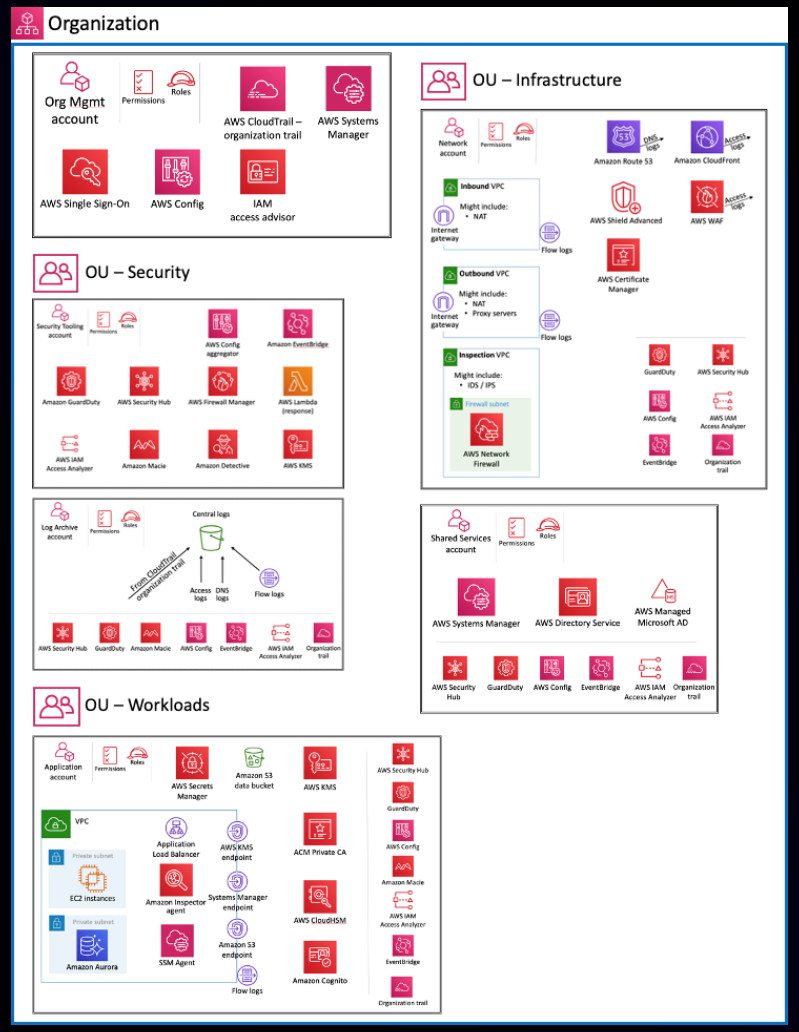

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

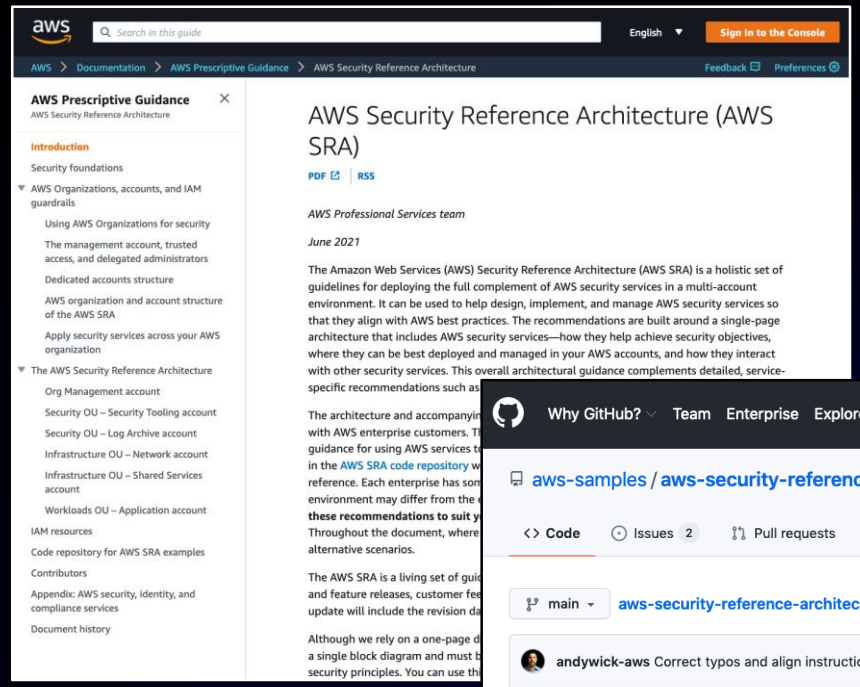
# Why build a security reference architecture?

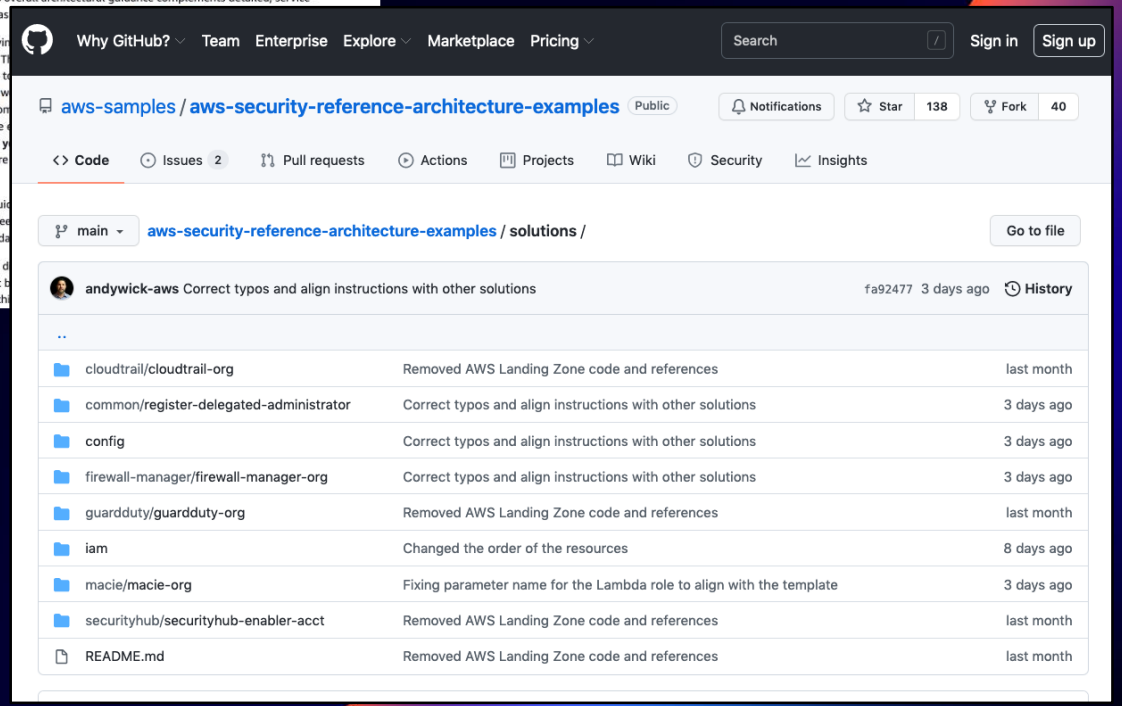



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS SRA




© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# How the AWS SRA can help you

1. Define target state for your own security architecture
2. Review (and revise) the designs and capabilities you have already implemented
3. Bootstrap the implementation of your own security architecture
4. Learn more about AWS security services and capabilities
5. Understand cloud security generally
6. Drive a discussion of organizational responsibilities for security

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# What can the AWS SRA help you do?

Ship more applications



faster

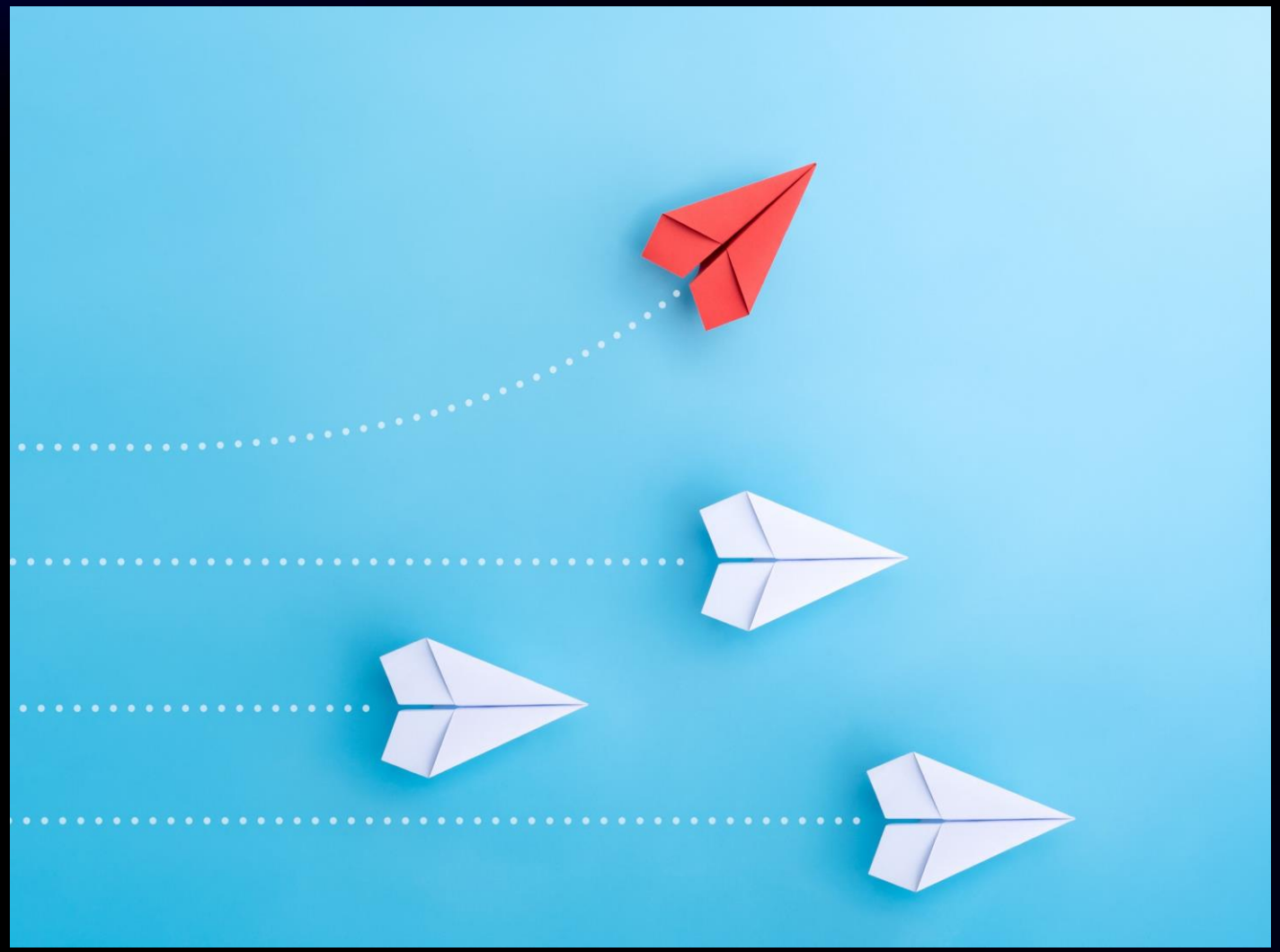


and more securely



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Want to do things differently?



That’s OK

Make informed, deliberate decisions

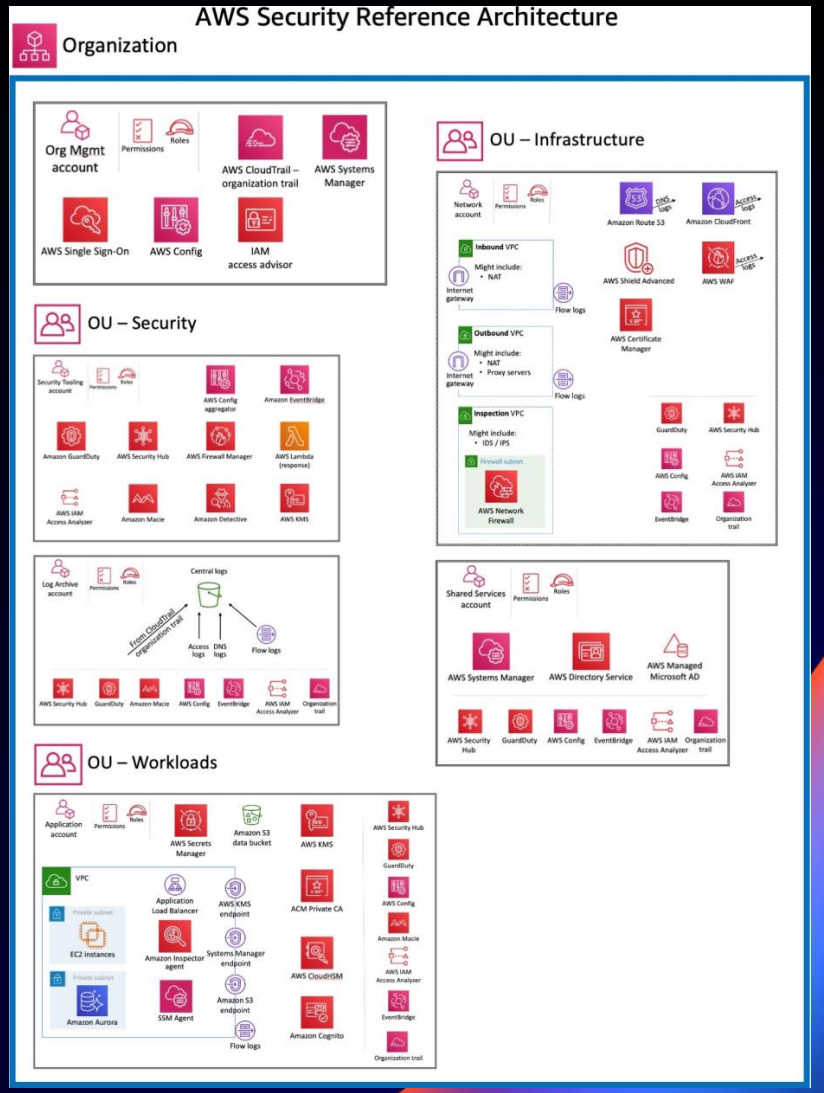
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Let’s look at the architecture

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Goal: Navigation and highlights



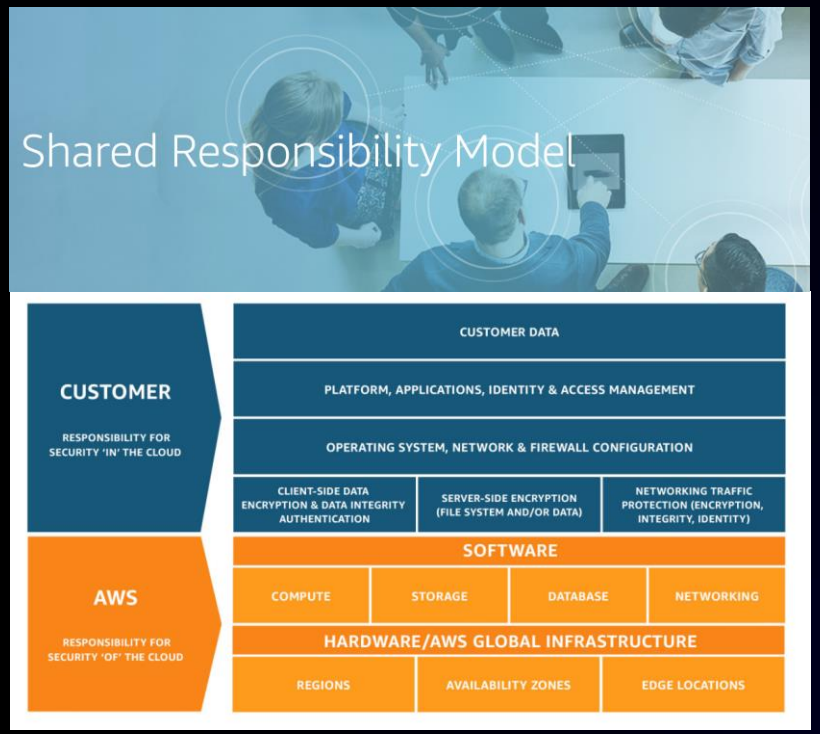



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Security foundations

## AWS Cloud Adoption Framework

Accelerating your organization's path to successful cloud adoption




## AWS Well-Architected

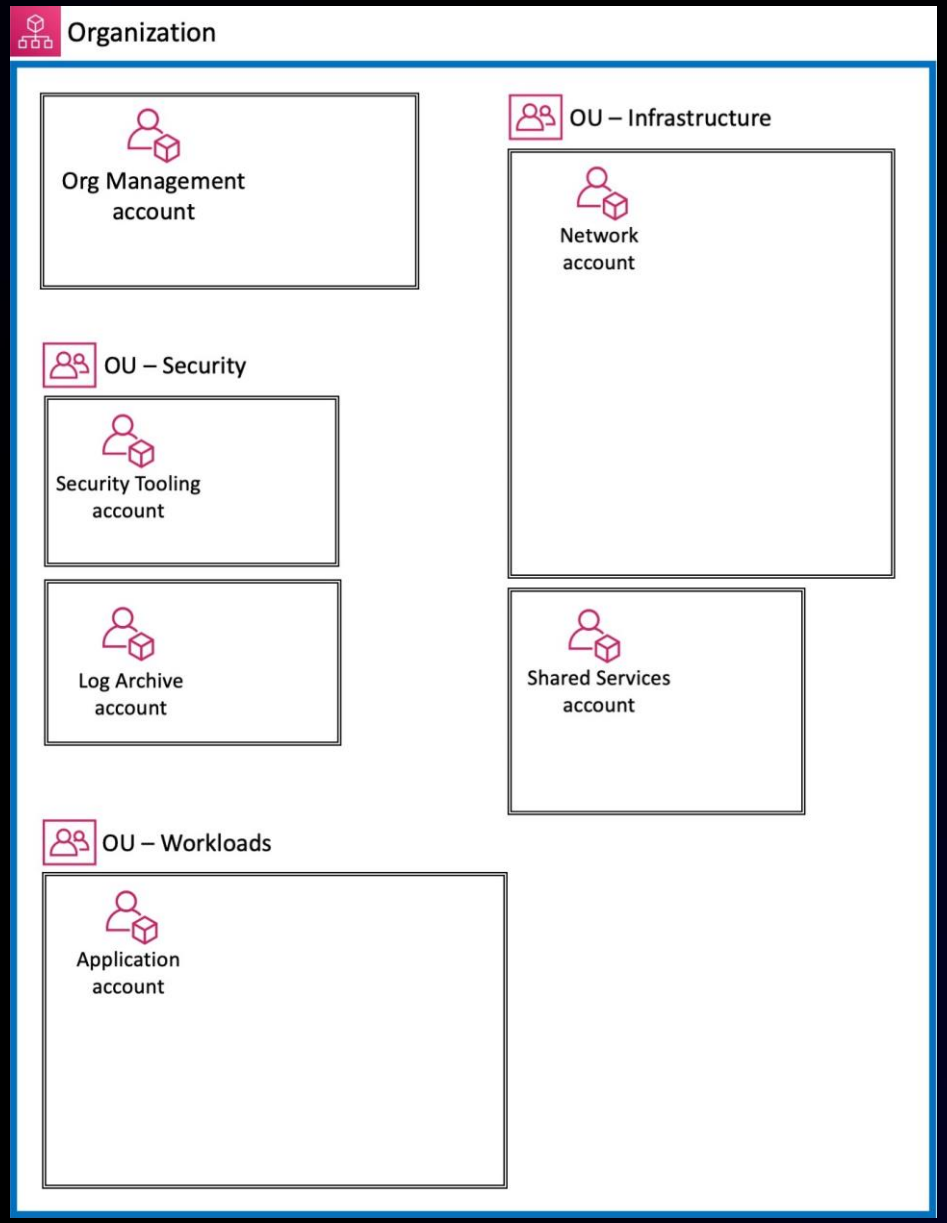
Learn, measure, and build using architectural best practices

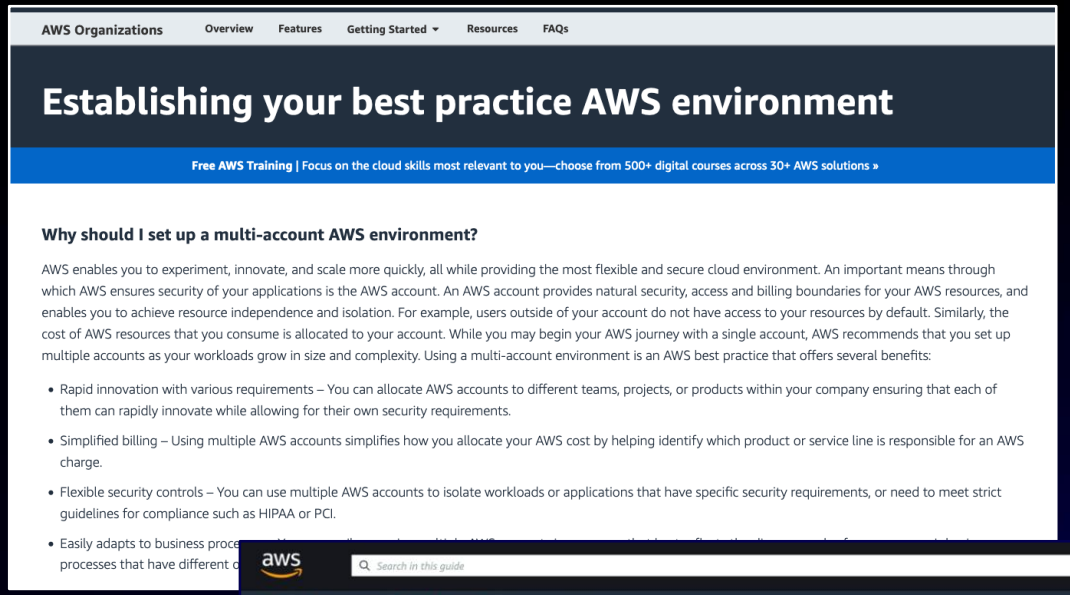
Get started with the AWS Well-Architected Tool

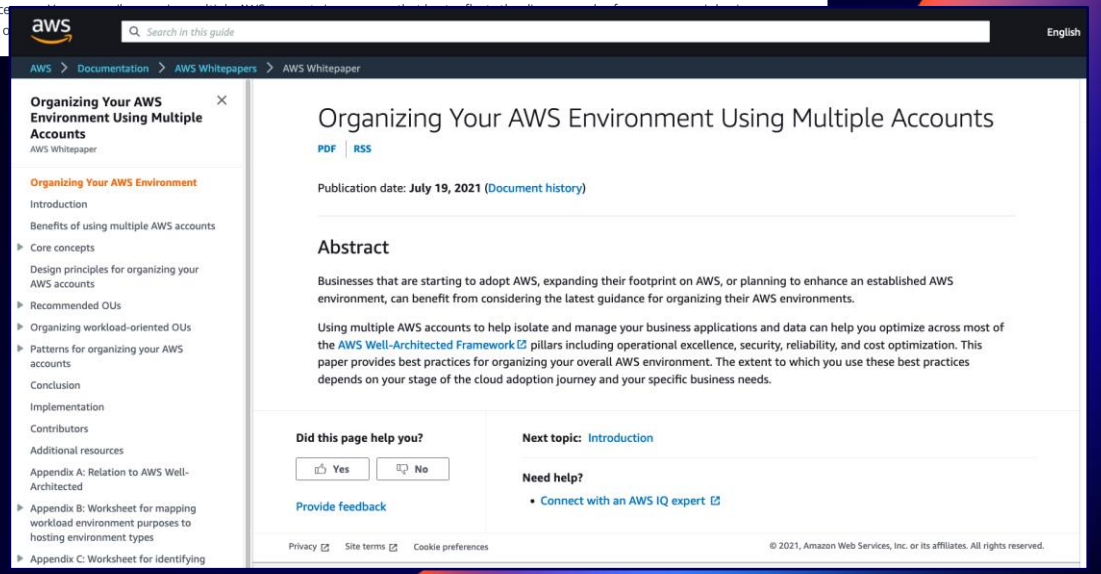
| AWS Well-Architected Tool | AWS Well-Architected Guidance | AWS Well-Architected Lenses | AWS Architecture Center |
|---|---|---|---|

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS SRA: High-level account structure

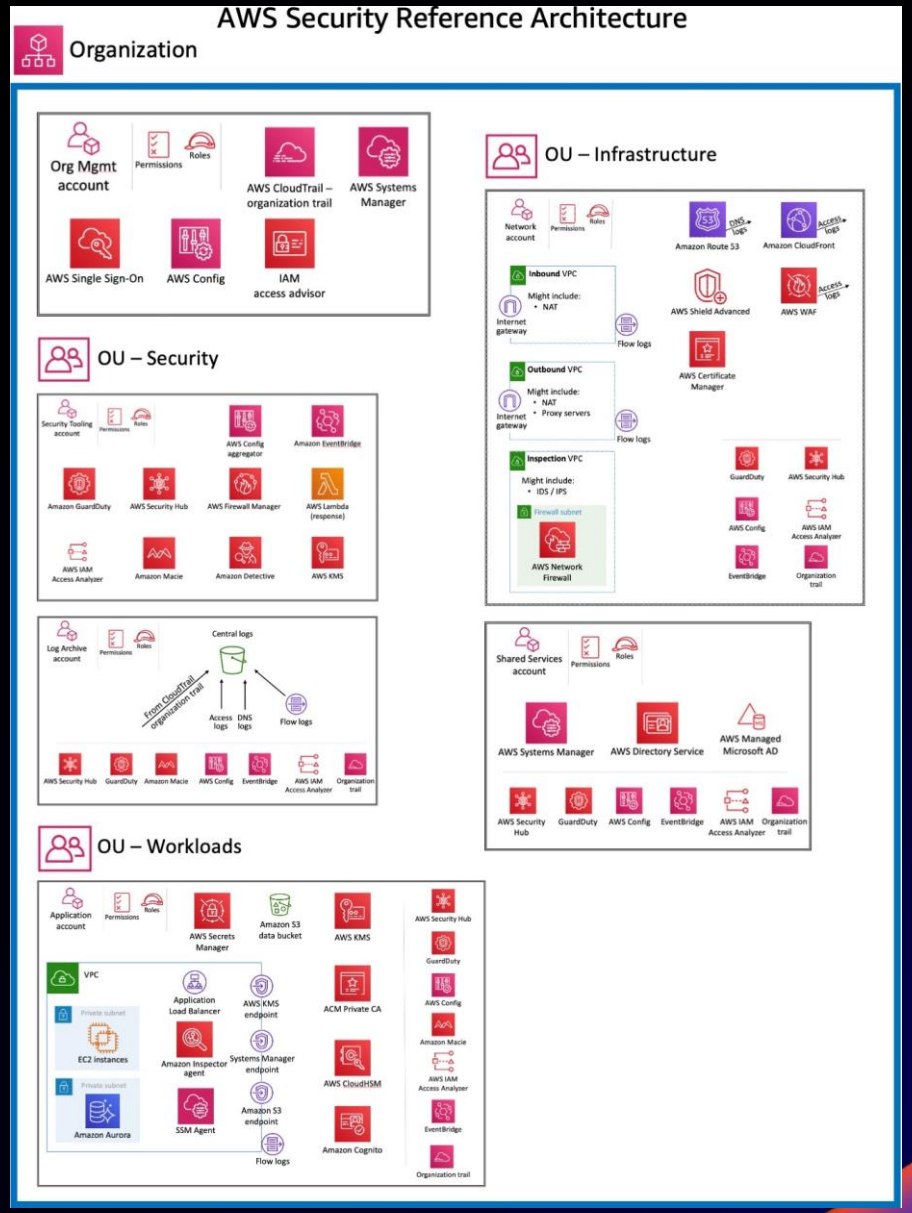


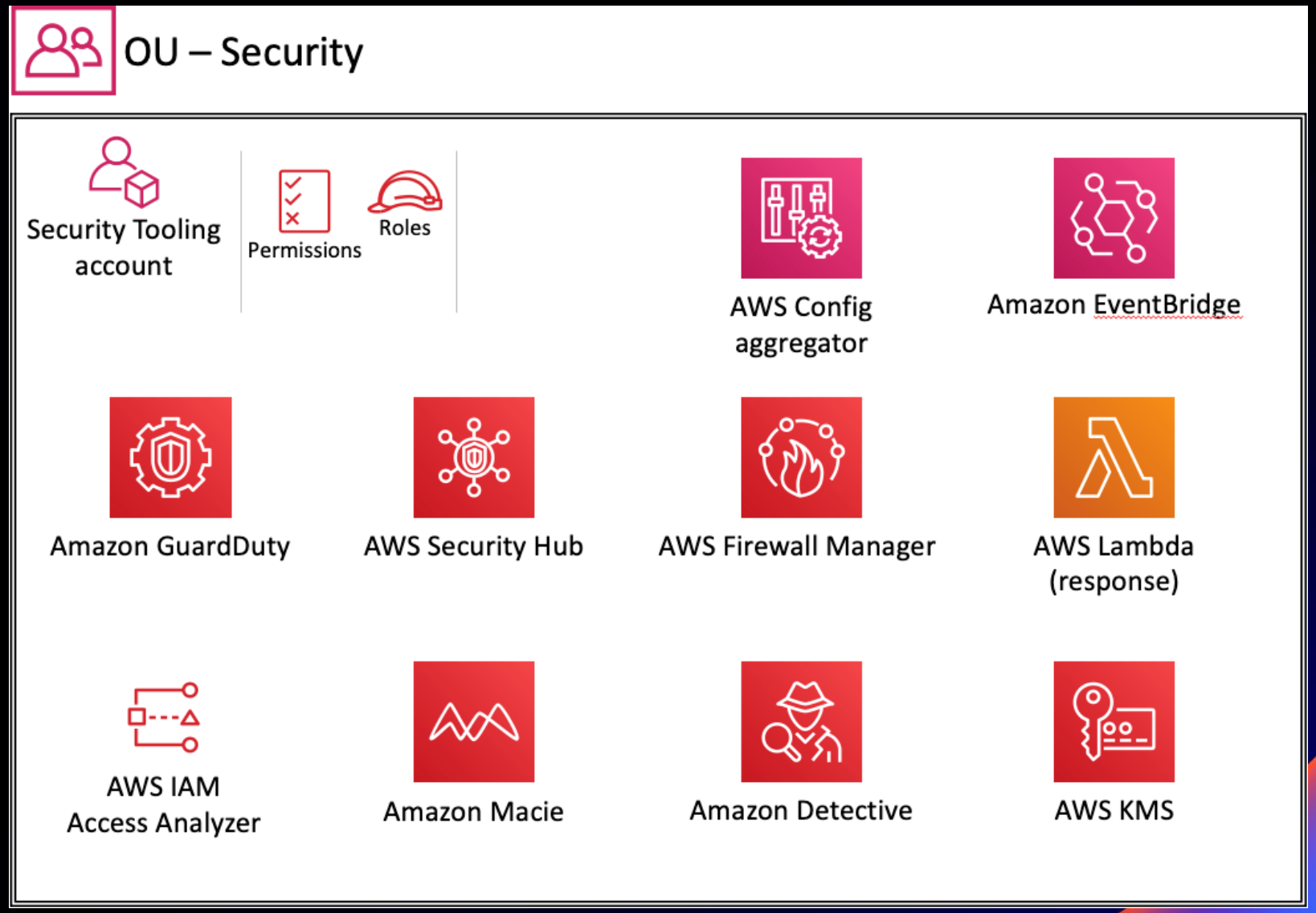

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS SRA: Show all the security services



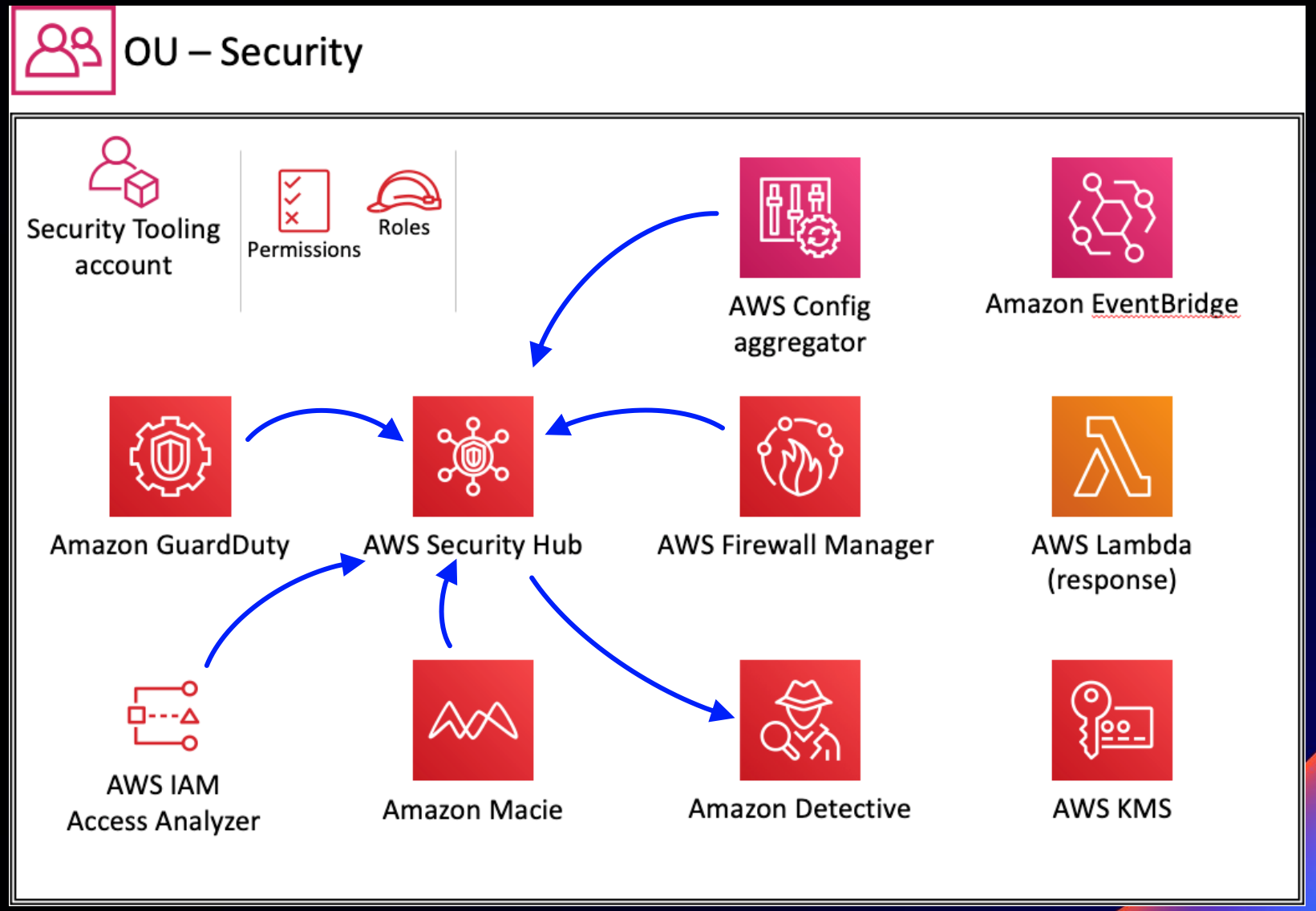

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS SRA: Security Tooling account



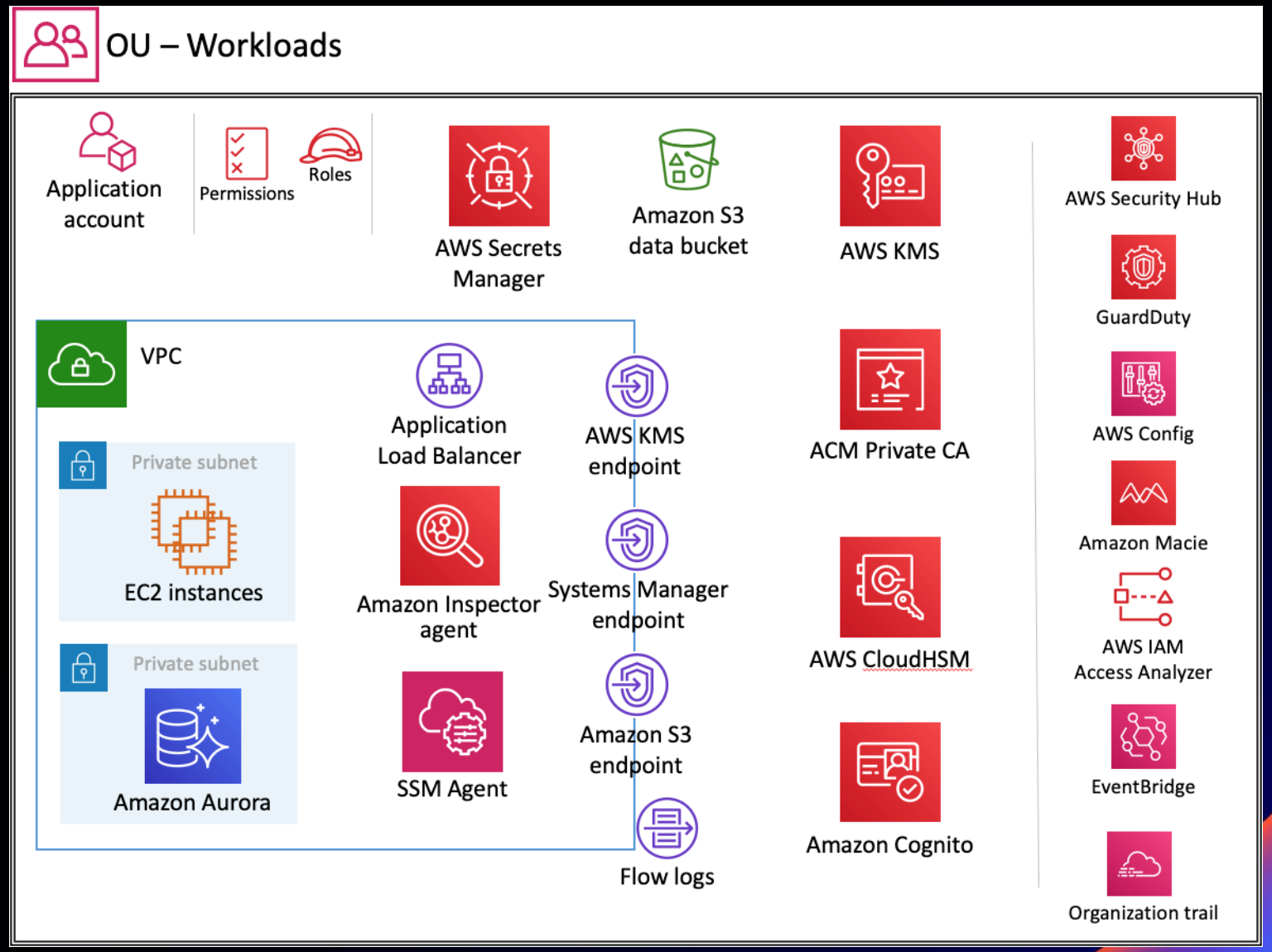

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS SRA: Security Tooling account




© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

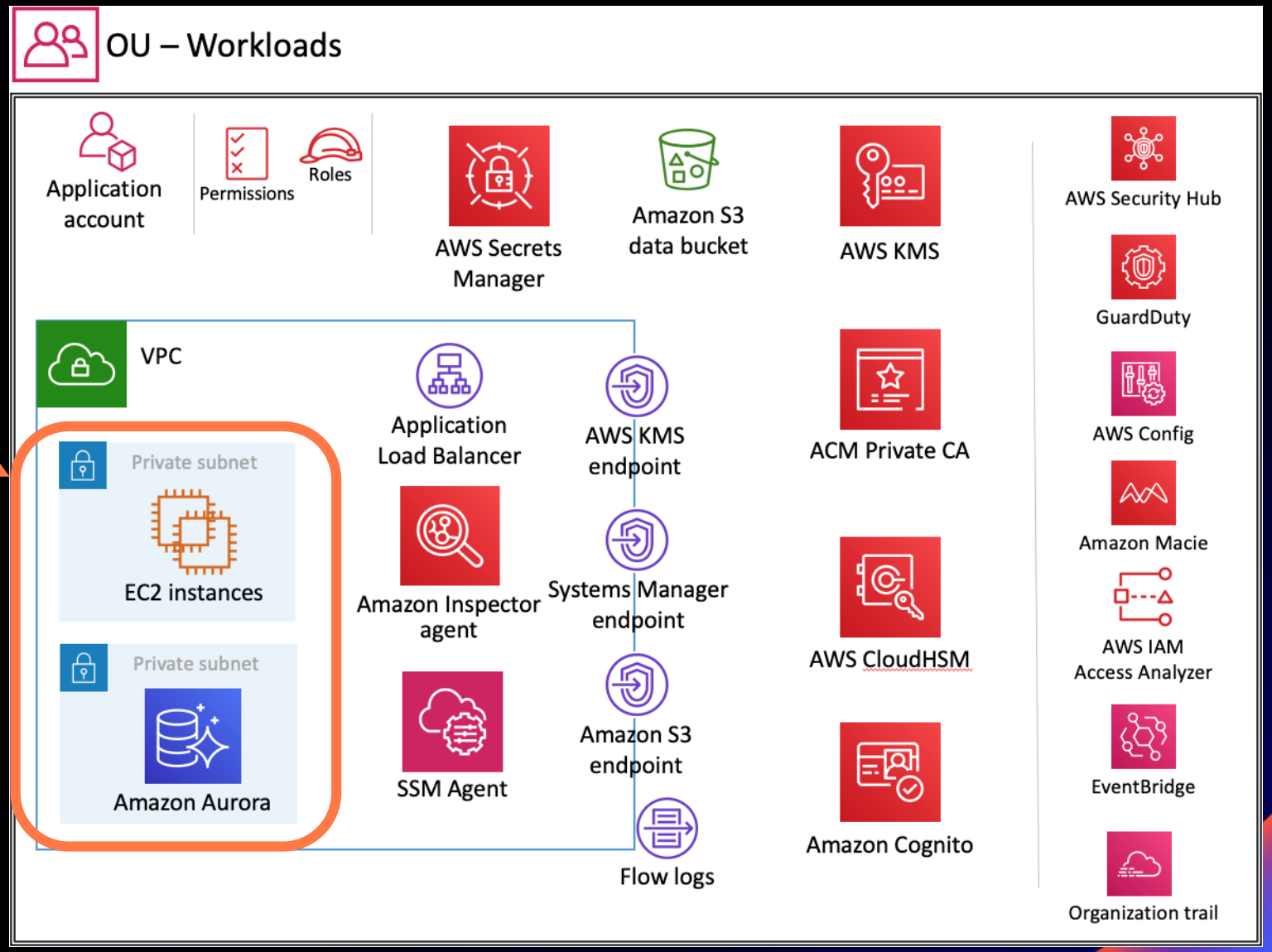
# AWS SRA: Application account




© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

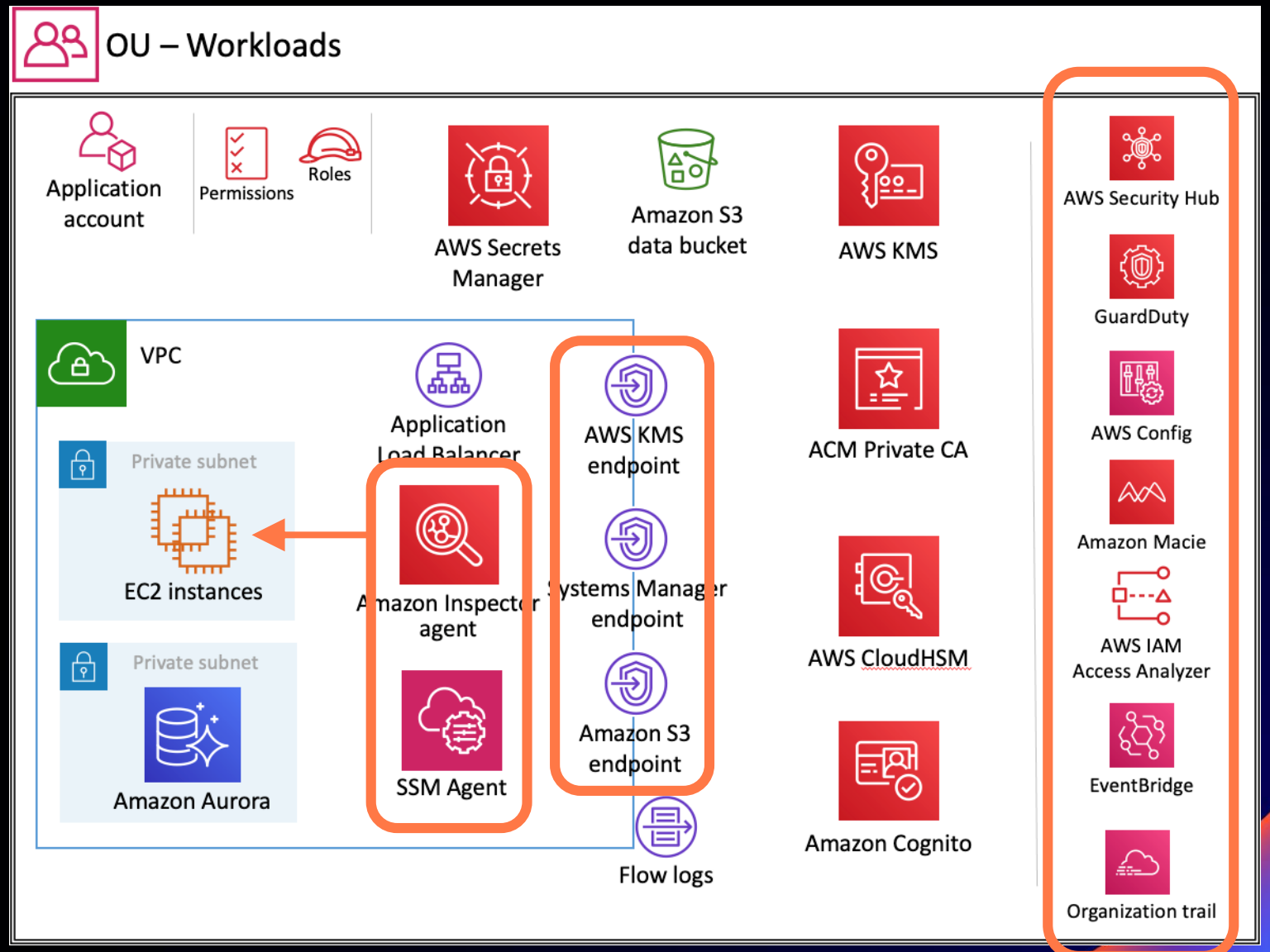
# AWS SRA: Application account

Application




© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS SRA: Application account



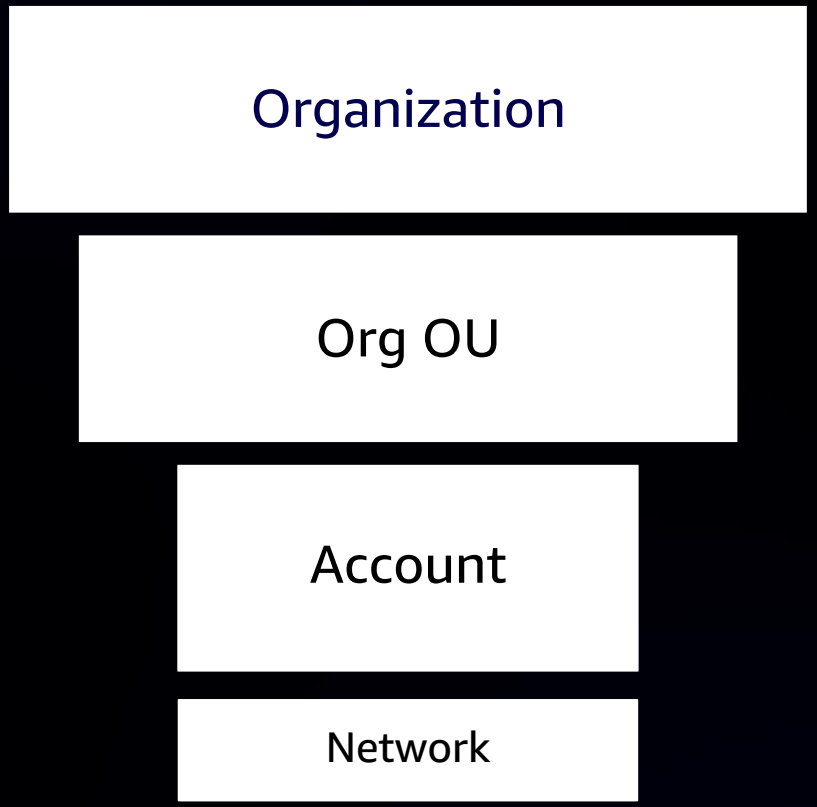

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Security at all layers

## AWS Well-Architected

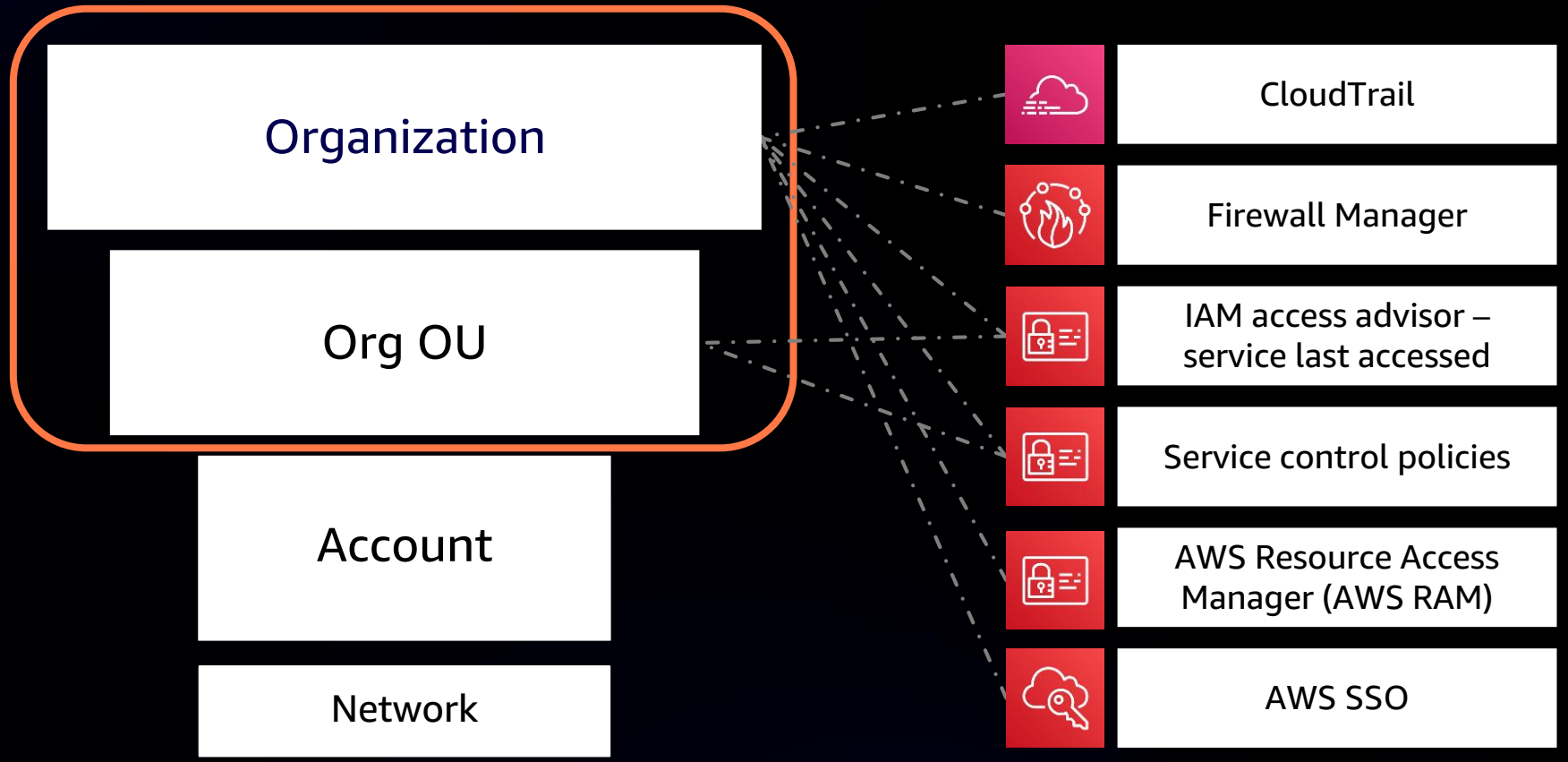
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Your AWS environment in layers



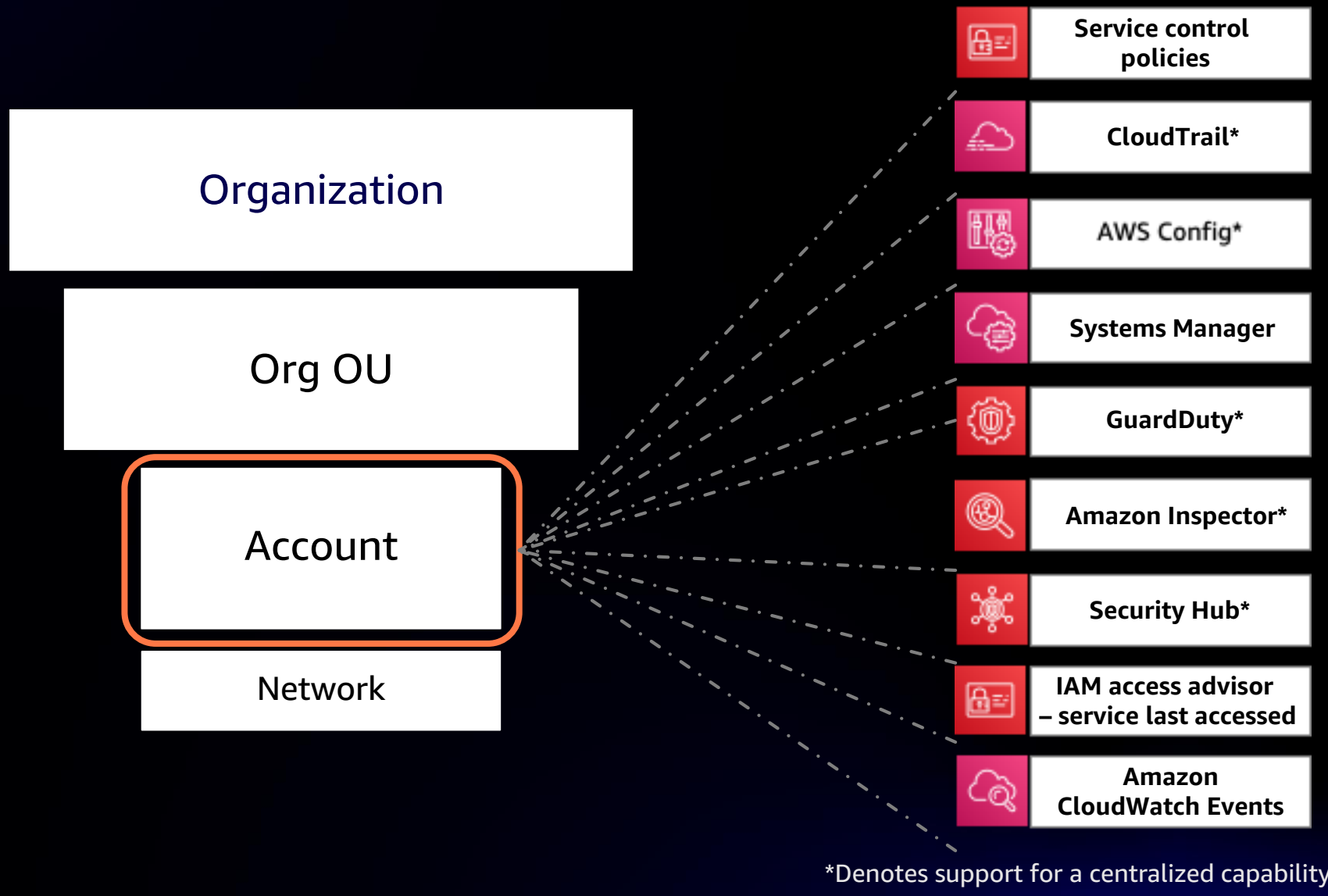

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Protecting the AWS organization and OUs




© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

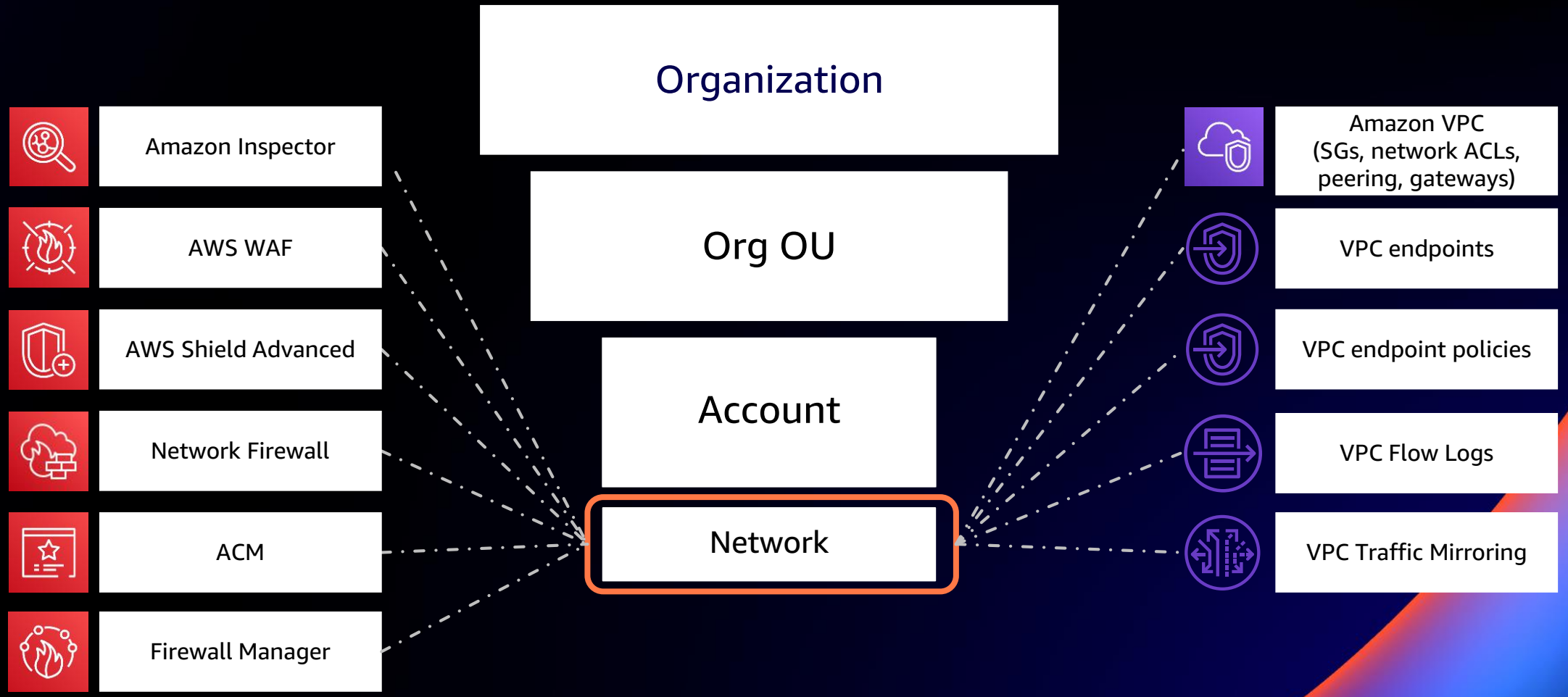
# Protecting accounts




*Denotes support for a centralized capability

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Protecting networks

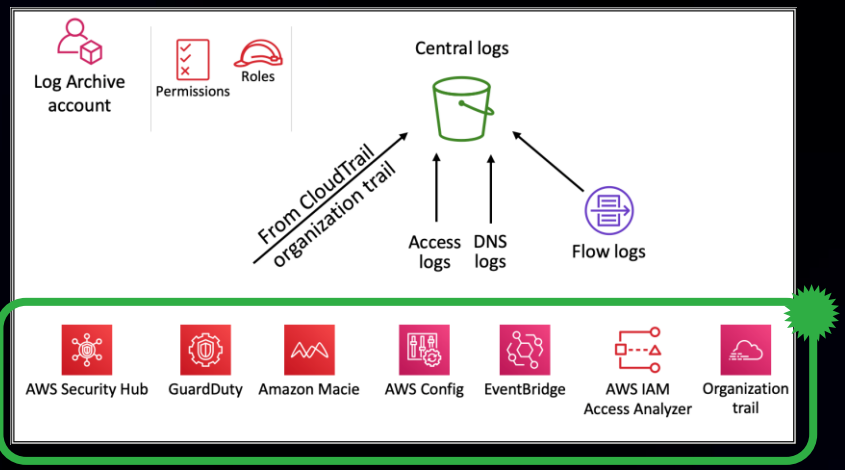


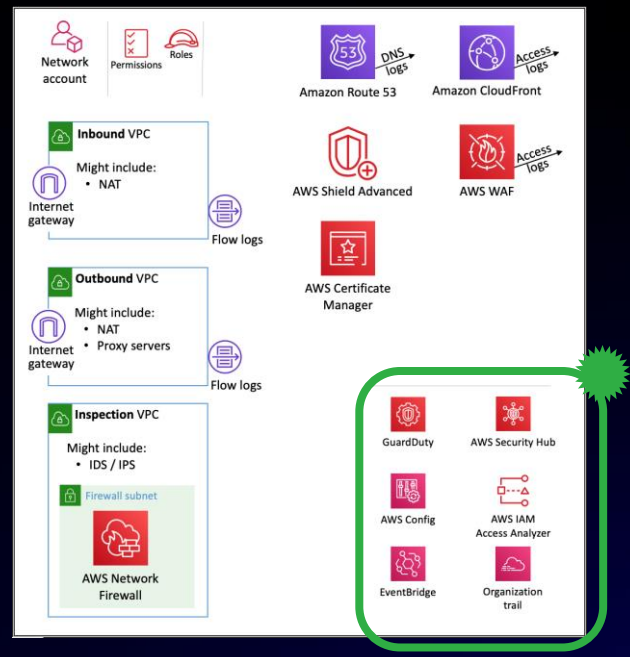

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

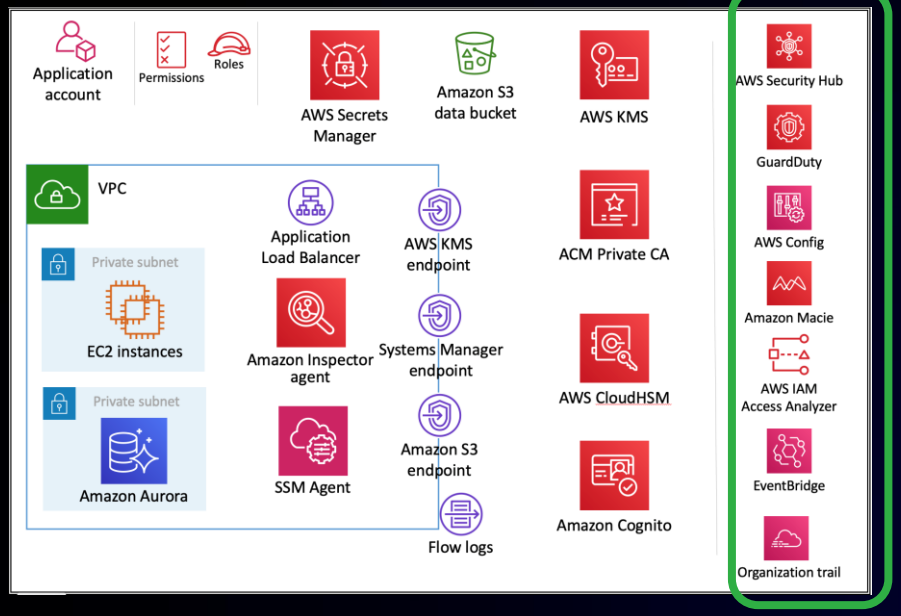
# Recurring guardrails and centralized management

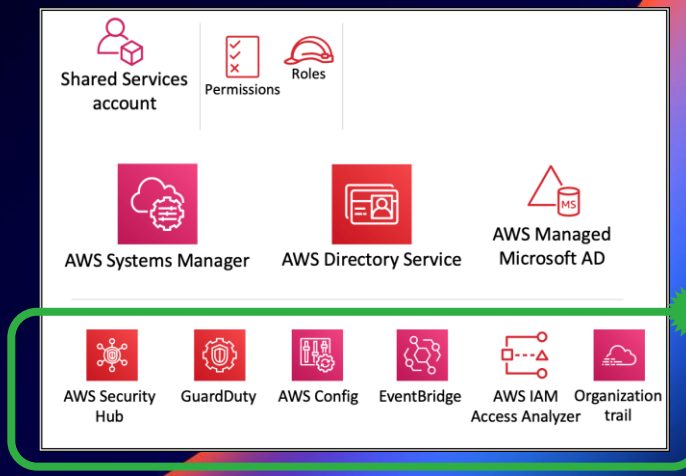
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Recurring, distributed, . . .



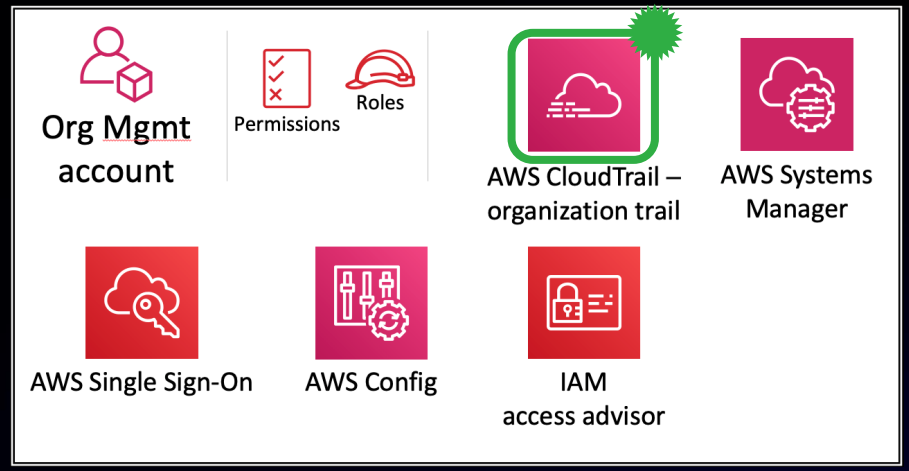



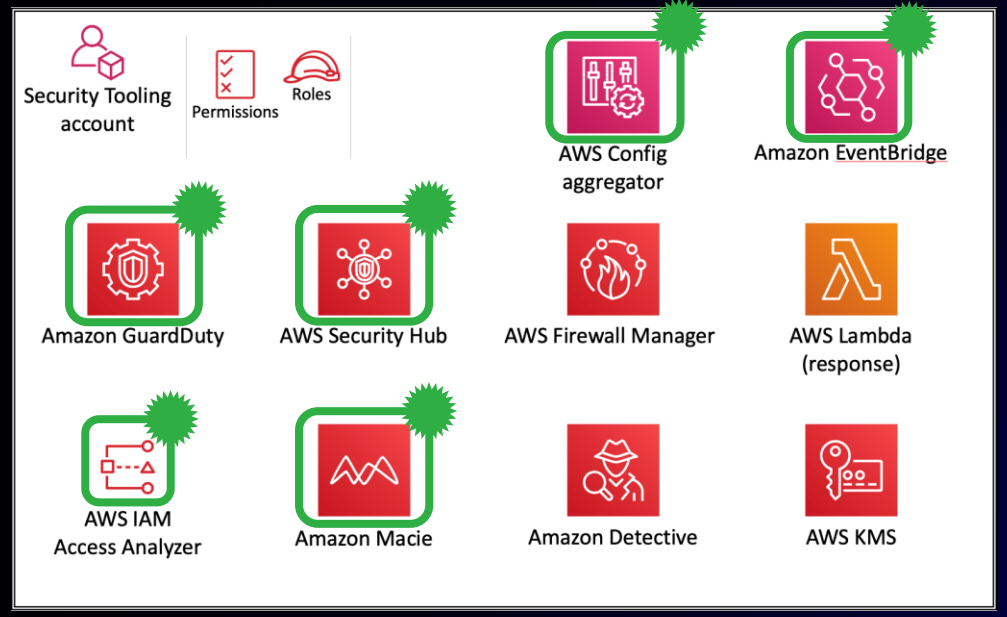




© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# . . . and centralized



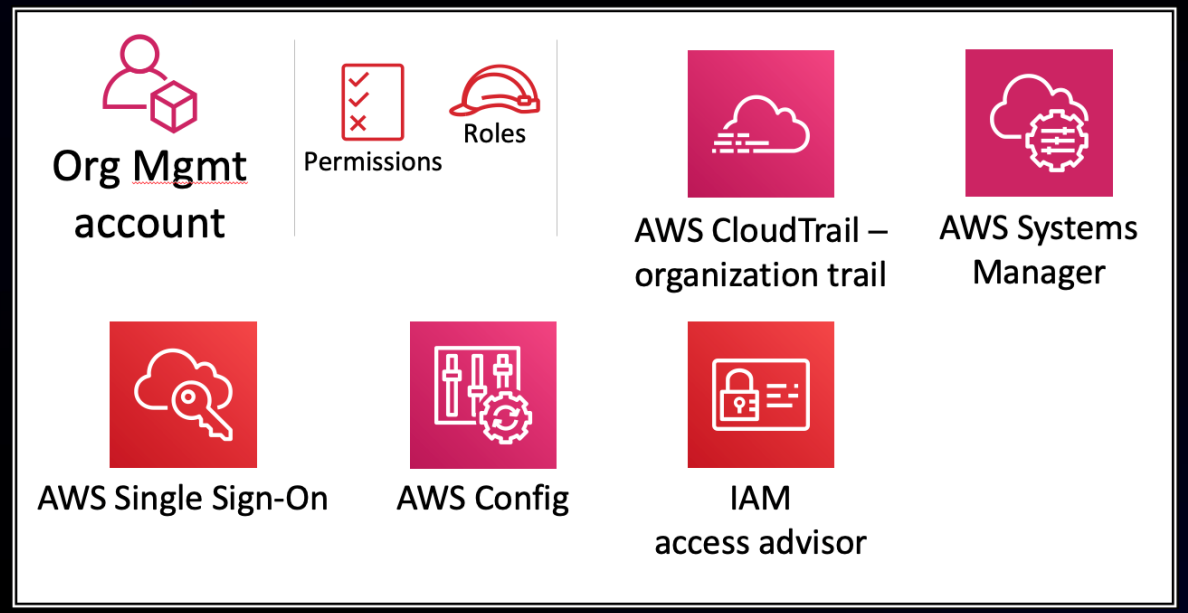



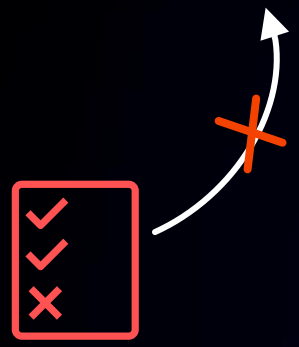

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

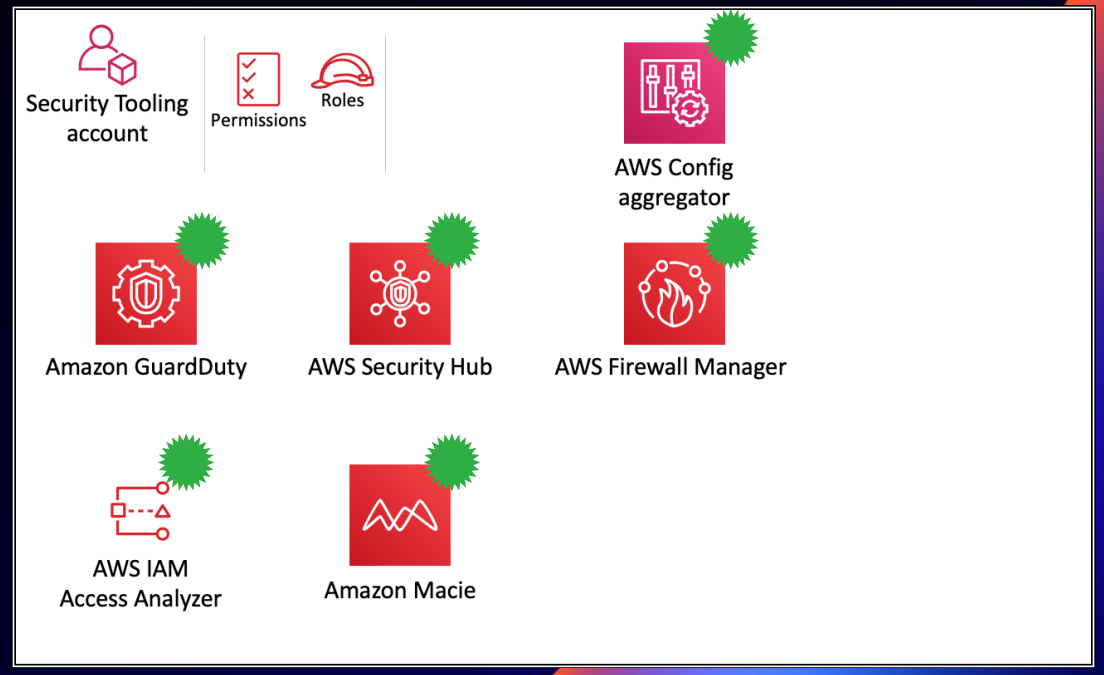
# Delegated admin: Protecting the organization management account

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Protection with delegated administrator




= Delegated administrator

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS SRA code repository

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# What we will cover

Current available code examples

Additional items included with each example

How to deploy the solutions within AWS Control Tower

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS SRA code

CURRENT MODULES

## AWS Organizations



CloudTrail

## AWS Organizations with delegated admin



AWS Config aggregator



AWS Config conformance packs



Firewall Manager



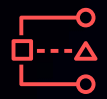
Security Hub



GuardDuty



Macie



IAM Access Analyzer

## Default account configurations



IAM password policy



Amazon EBS default encryption



Amazon S3 public access block

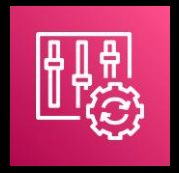
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS security service benefits



## Organization AWS CloudTrail

Benefits: Central configuration, member accounts cannot disable



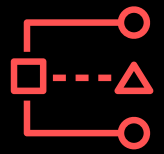
## AWS Config Conformance Packs

Benefits: Deploy a collection of related AWS Config rules



## AWS Firewall Manager Security Group Policies

Benefits: Monitor and remediate security groups

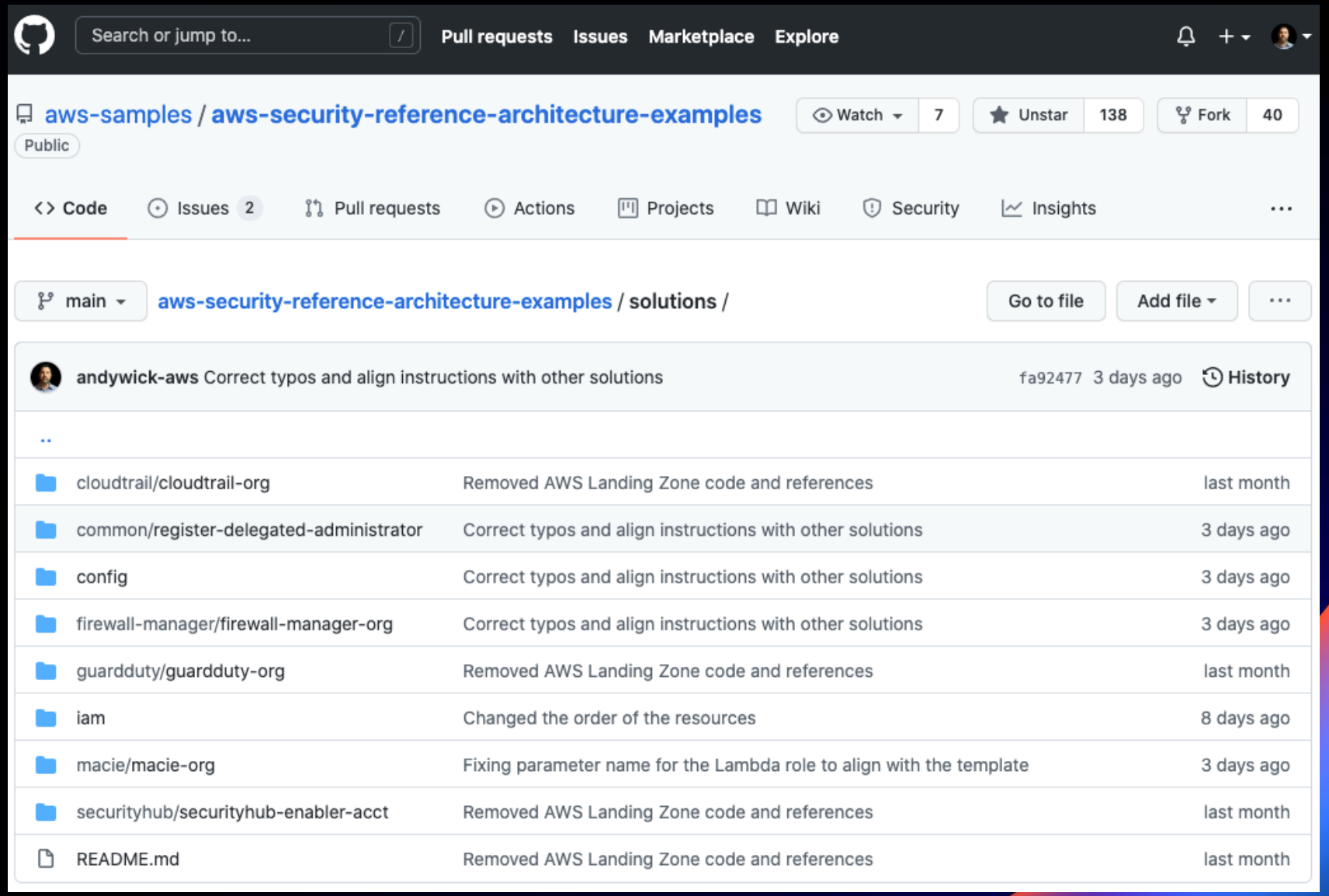


## AWS IAM Access Analyzer

Benefits: Identify resources shared with an external entity

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Public GitHub repository

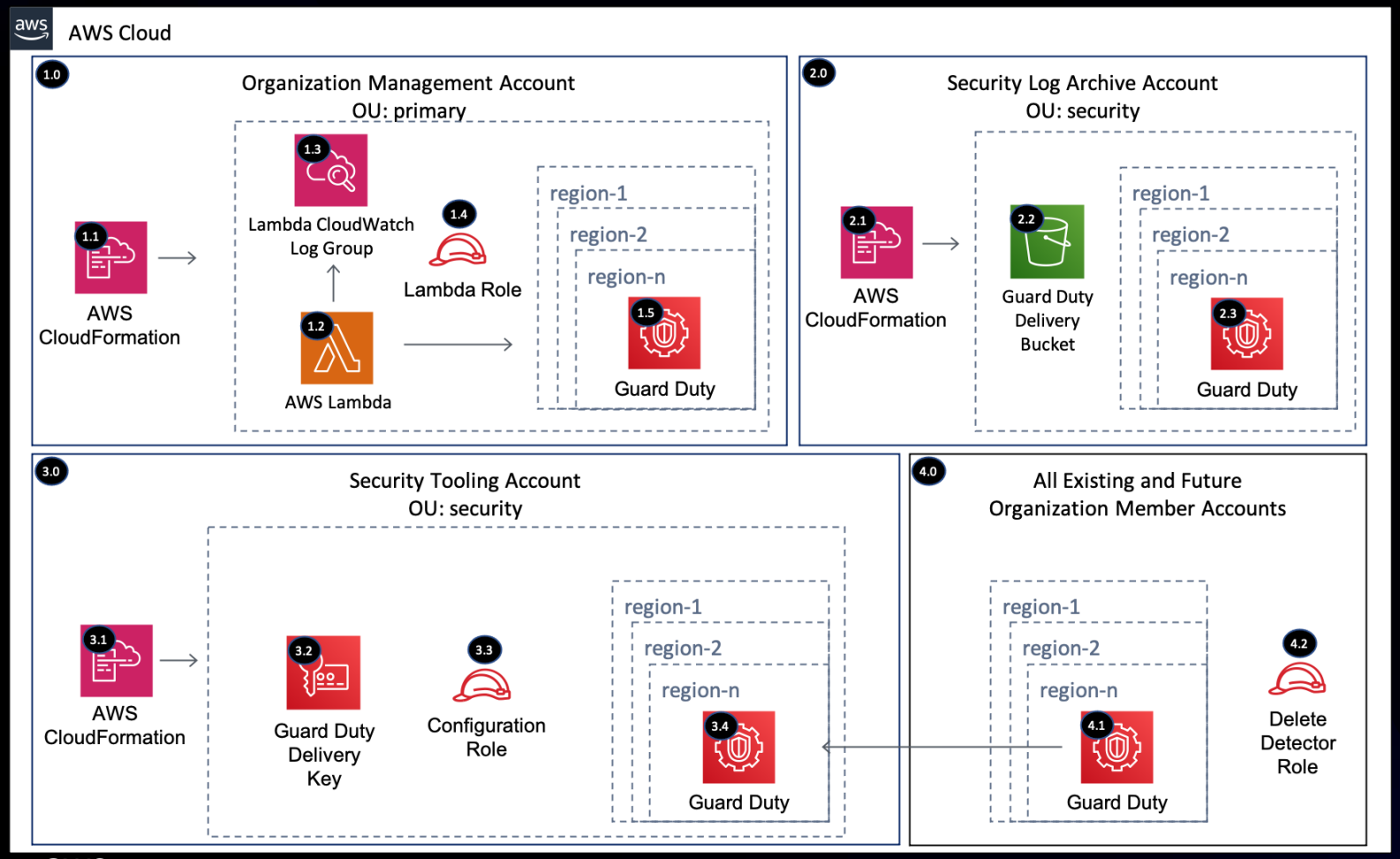



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS SRA code

WHAT ELSE IS INCLUDED?

## GuardDuty solution




- Architecture diagram
- Resource descriptions
- Implementation guides
- Least privilege permissions
- Configuration logic
- AWS KMS setup
- Cleanup scripts

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS SRA code

IMPLEMENT WITH AWS CONTROL TOWER

## 1 Set up environment



AWS Control Tower



Customizations pipeline

## 2 Download SRA code



Clone GitHub repository

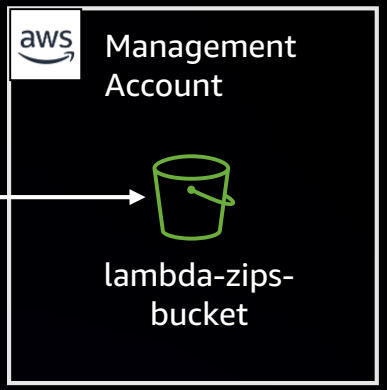
## 3 Package and stage code



Lambda function



Required libraries




## 4 Update and stage configuration files

**CFCT configuration**



Parameter files



Manifest file



Template files

## 5 Trigger the pipeline



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Where to find it

- AWS Prescriptive Guidance

  https://go.aws/3ljbsYv

  Search “AWS security reference architecture”

- Code repository

  https://bit.ly/3iHhyjF

  Search “AWS security reference architecture github”

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.