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

SEC203

# Revitalize your security with the AWS Security Reference Architecture


Sarah Currey

Security Practice Manager,
Professional Services
AWS

Johnny Ray

Senior Security Engineer,
Amazon Managed Services
AWS


What's your goal?

# Agenda

- Common challenges
- Overview of AWS SRA
- Customer story
- High-level architecture
- Code repository
- Actionable next steps

# Common challenges

How do we define our target state for security architecture?

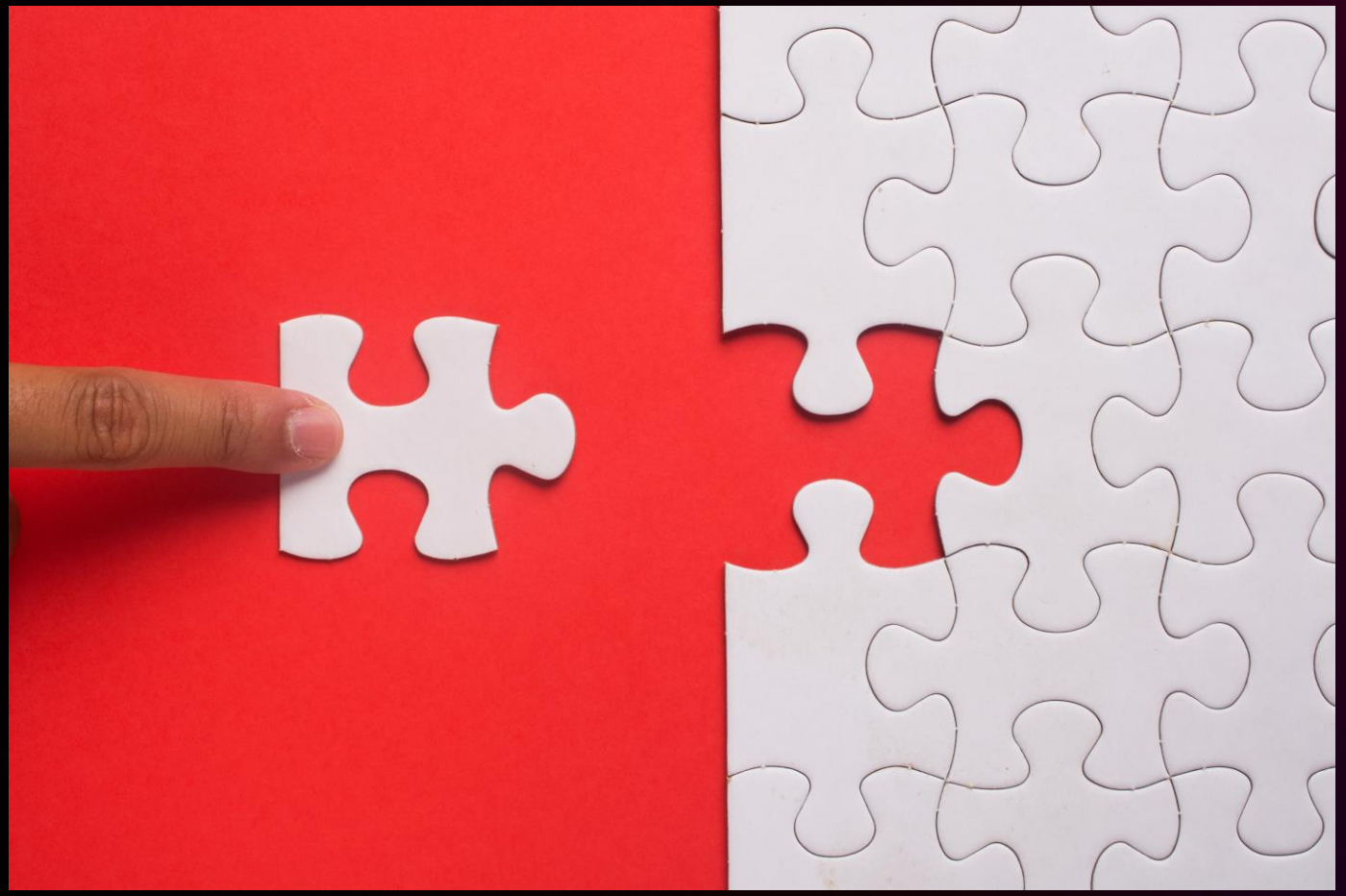
What is the best way to keep up with the latest AWS security services and capabilities?

How can we implement our own security architecture?

How do we drive discussions of organizational governance and responsibilities for security?

# Common challenges

How do the AWS security services and capabilities work together?



# Secure your castle = Secure your AWS environment

The vault

AWS Secrets Manager

Castle guards

AWS Identity and Access Management (IAM)

A watcher on the wall

Amazon GuardDuty

AWS CloudTrail

Stone wall

AWS Network Firewall

“Too much light often blinds [people] . . . They cannot see the forest for the trees.”

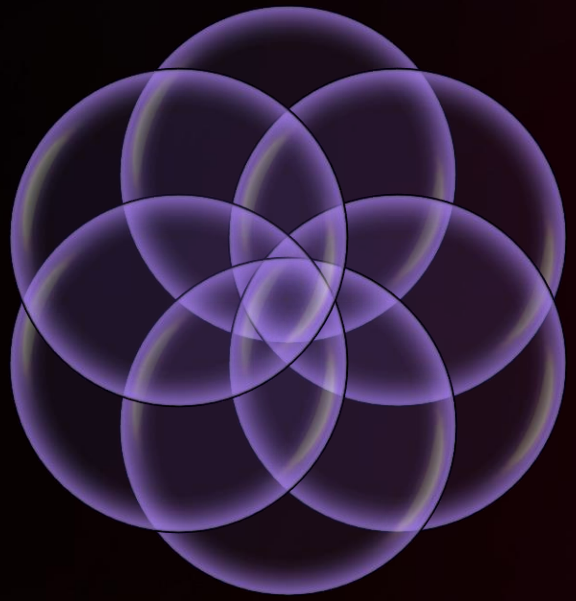
Christoph Martin Wieland (1733-1813)

# The AWS Security Reference Architecture (AWS SRA)

# How to use the AWS SRA

Define

Drive discussions



Review & revise

Understand

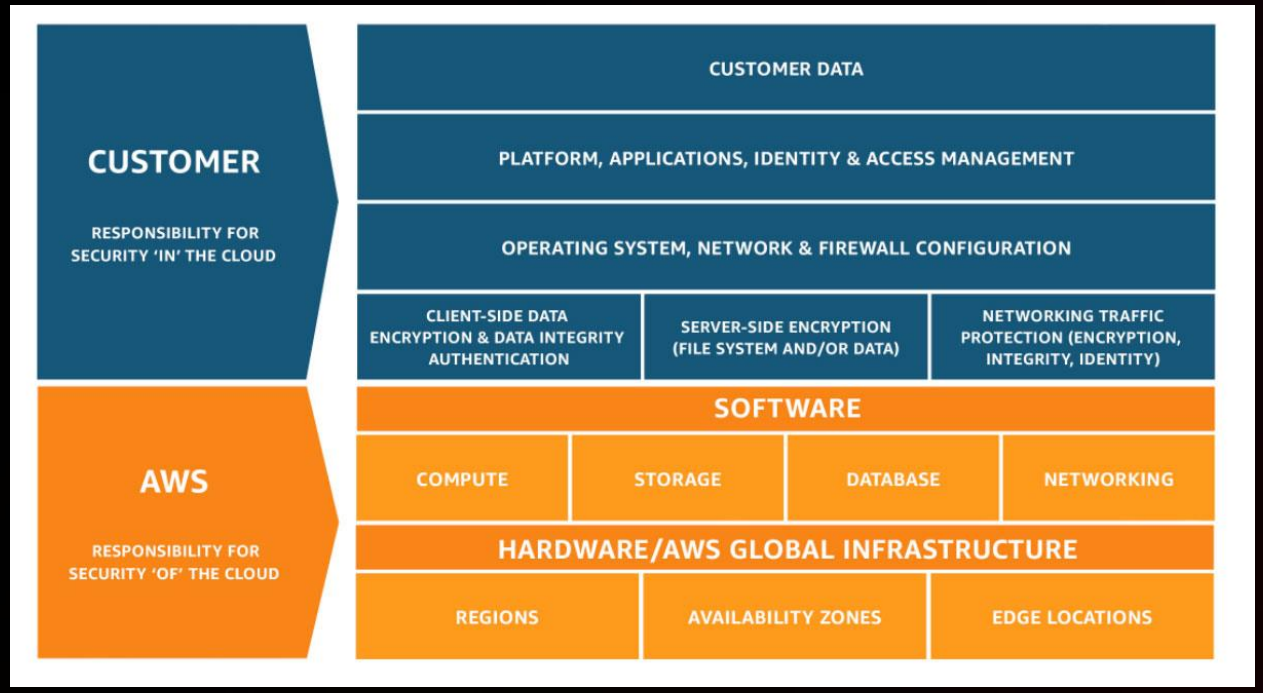
Execute

Learn

# Customer story

# AWS Security Foundations

## AWS Shared Responsibility Model




## AWS Well-Architected Framework

## AWS Cloud Adoption Framework

# Comparison of the AWS SRA

## AWS Well-Architected Framework

- Aims to help cloud architects build a secure, high-performing, resilient, and efficient infrastructure for their applications and workloads
- The security pillar describes how to take advantage of cloud technologies to help protect data, systems, and assets in a way that can improve your security posture
- A set of seven design principles that turn specific security areas into practical guidance that can help you strengthen your workload security

## AWS Cloud Adoption Framework

- Aims to help customers design and follow an accelerated path to successful cloud adoption
- The security perspective helps to structure the selection and implementation of controls across your business
- Outlines nine capabilities that help you achieve the confidentiality, integrity, and availability of your data and cloud workloads

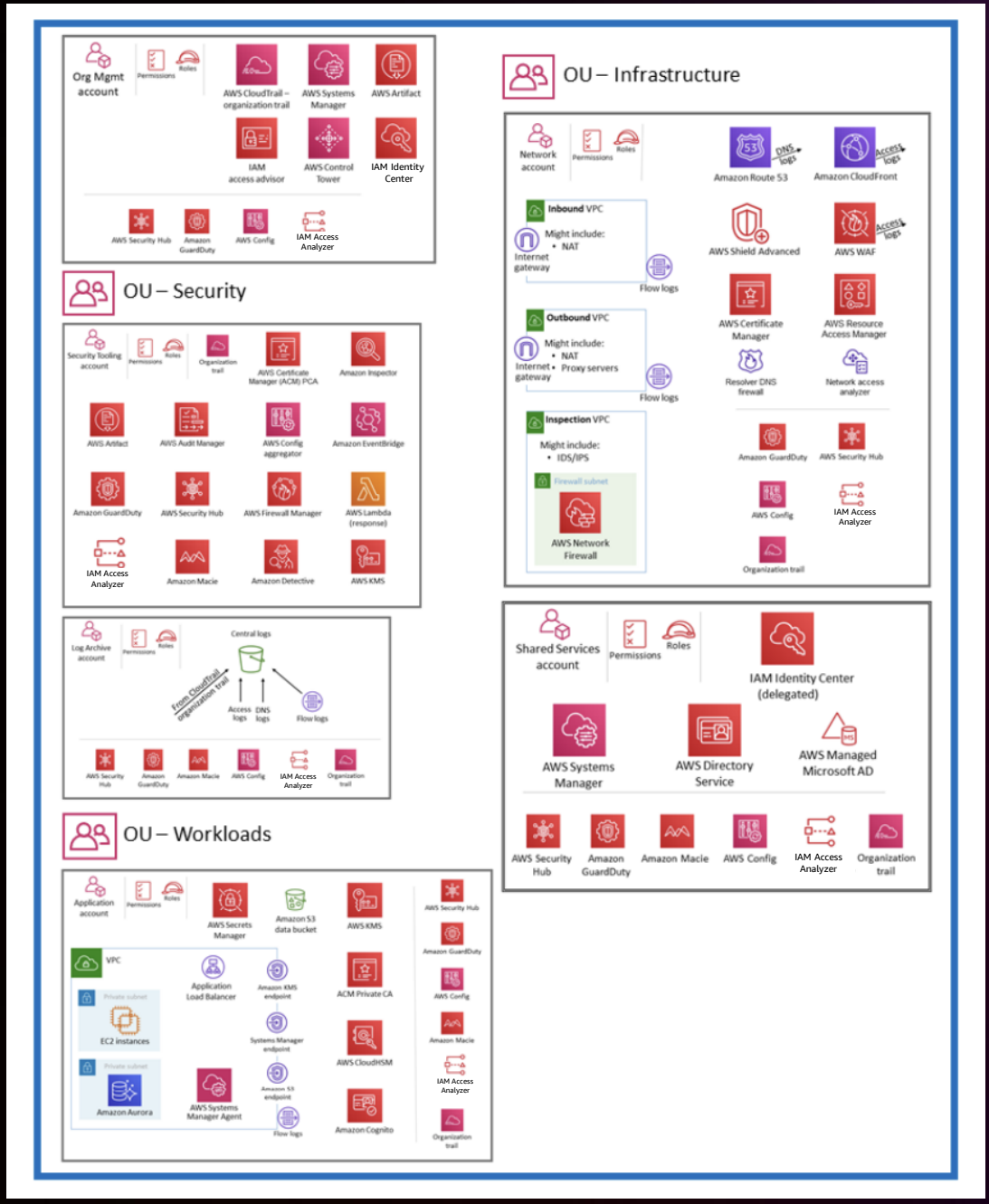
# Want to do things differently?

That’s ok.

Make informed, deliberate decisions.

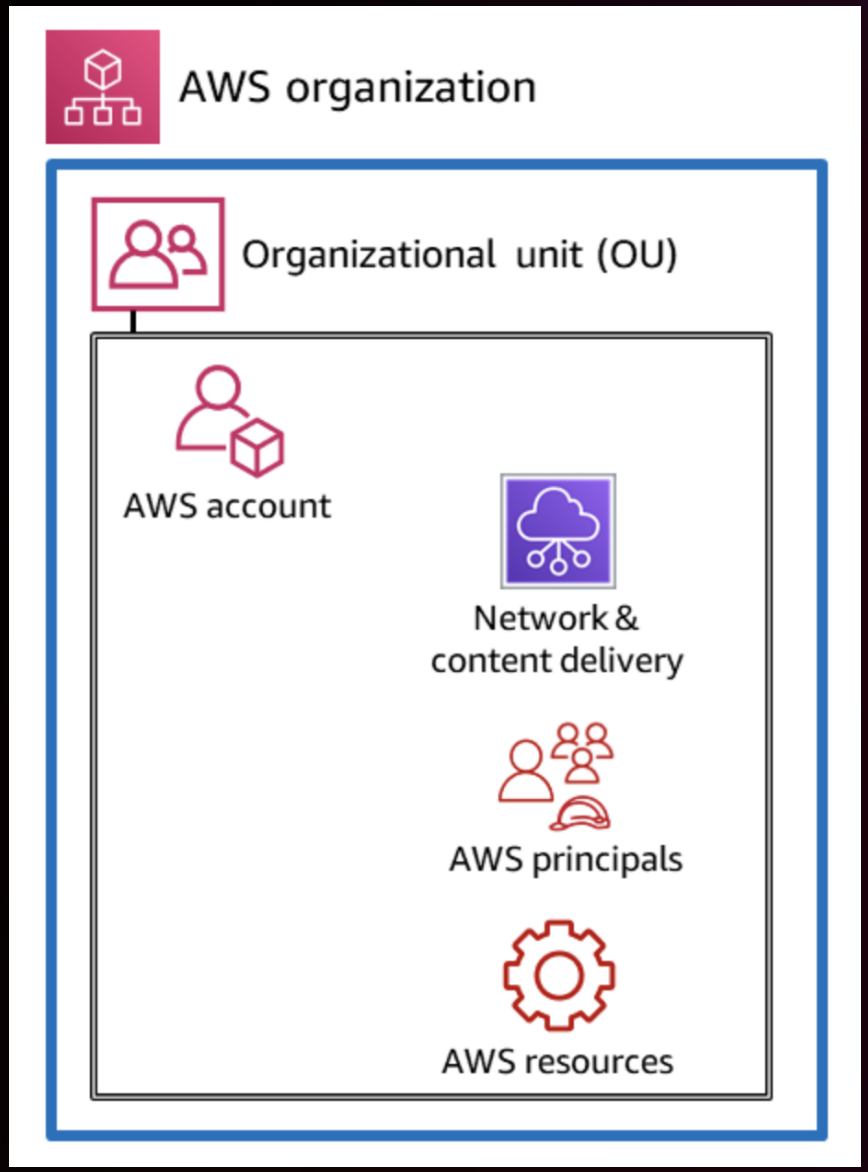
# AWS SRA Building Blocks

# AWS SRA

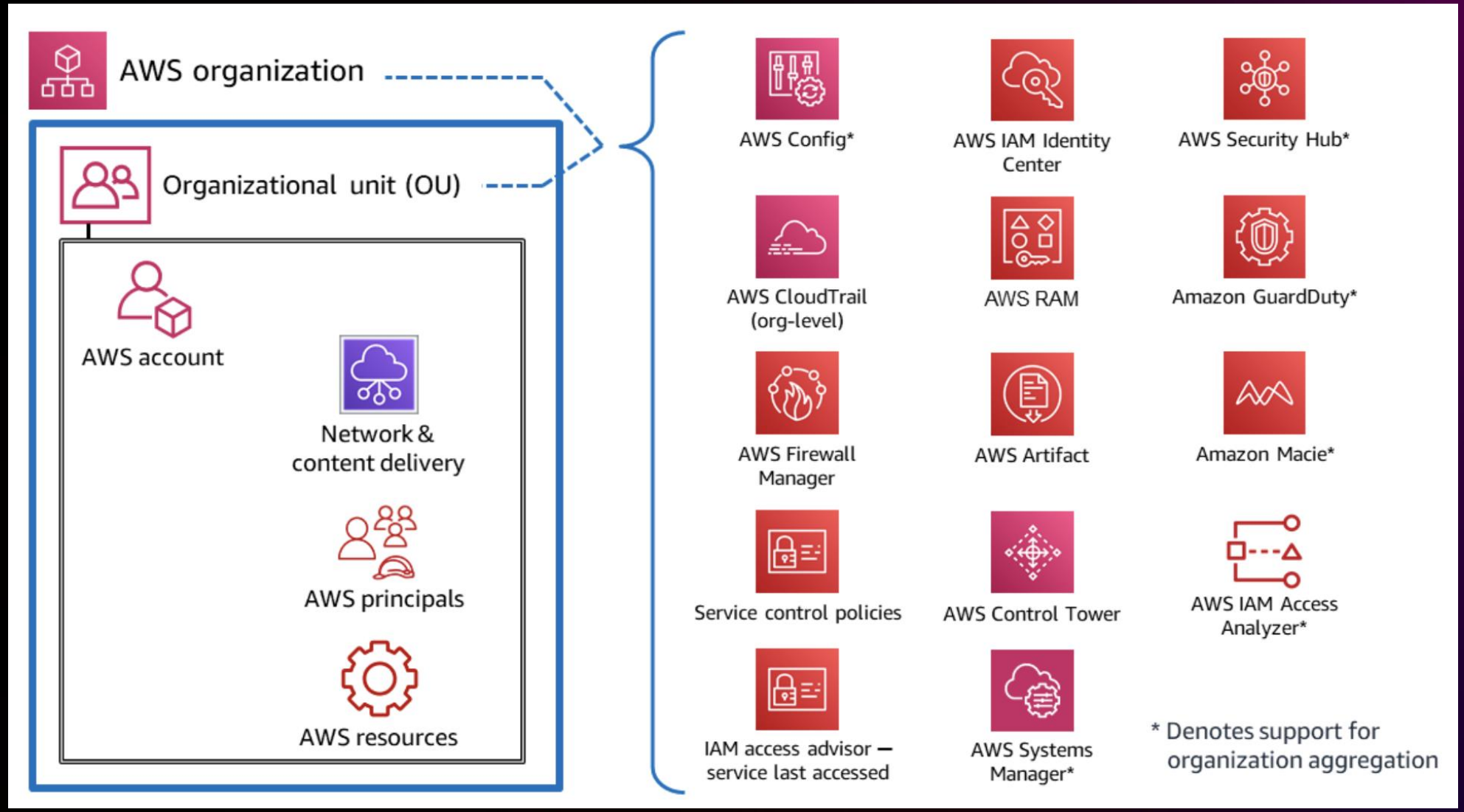


# Security at all layers

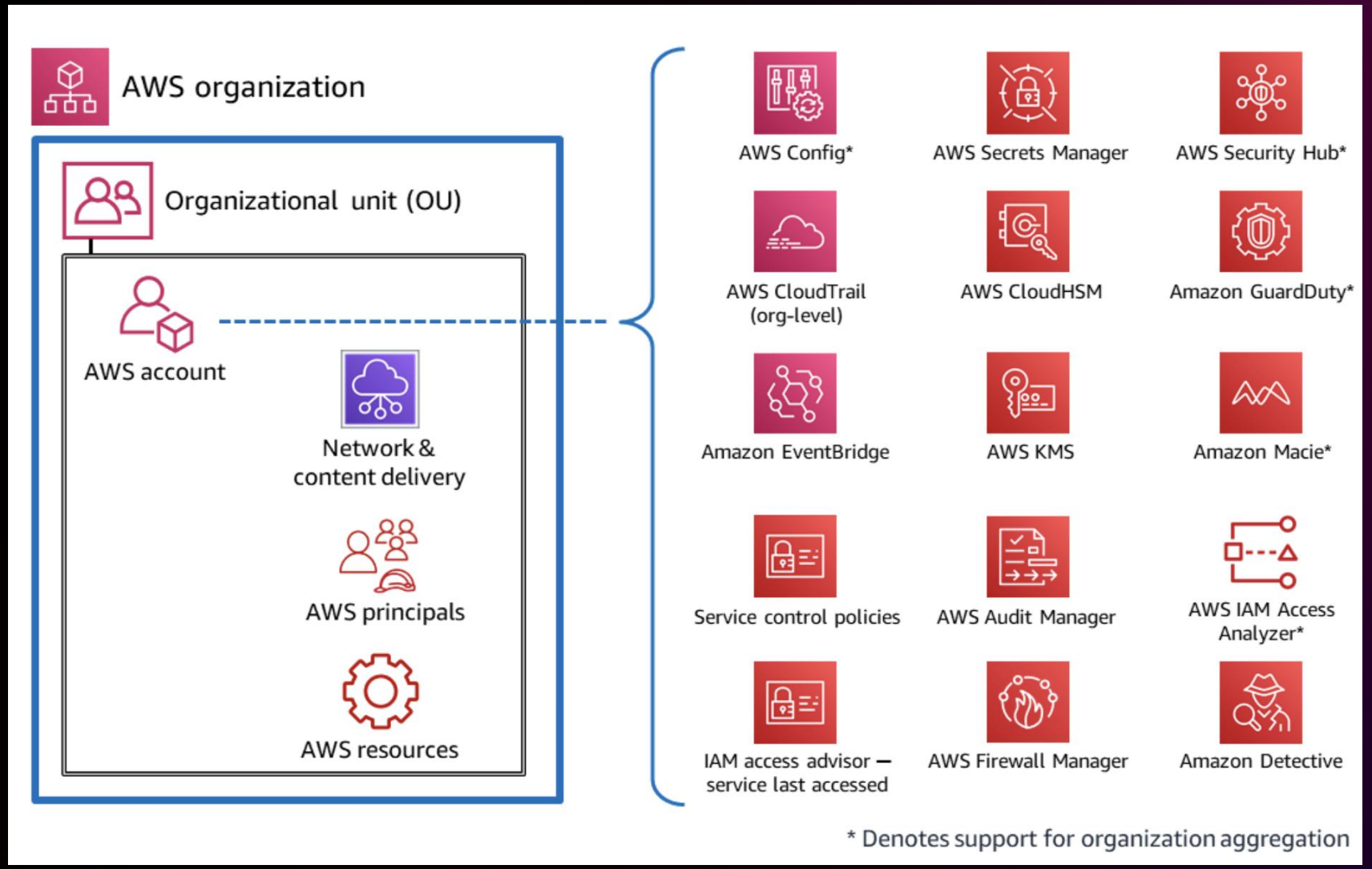
# Your AWS environment in layers



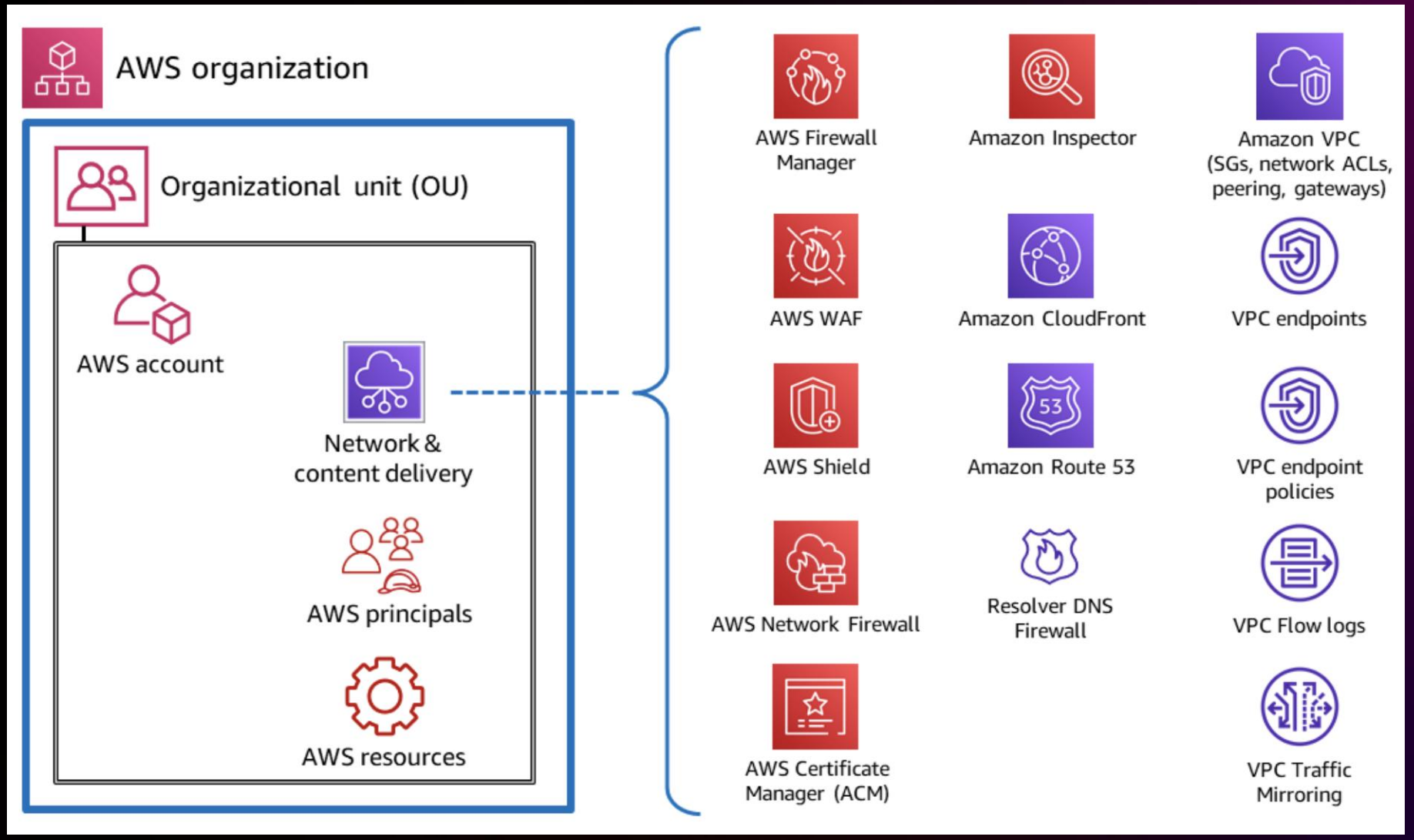
# Protecting the AWS organization and OUs



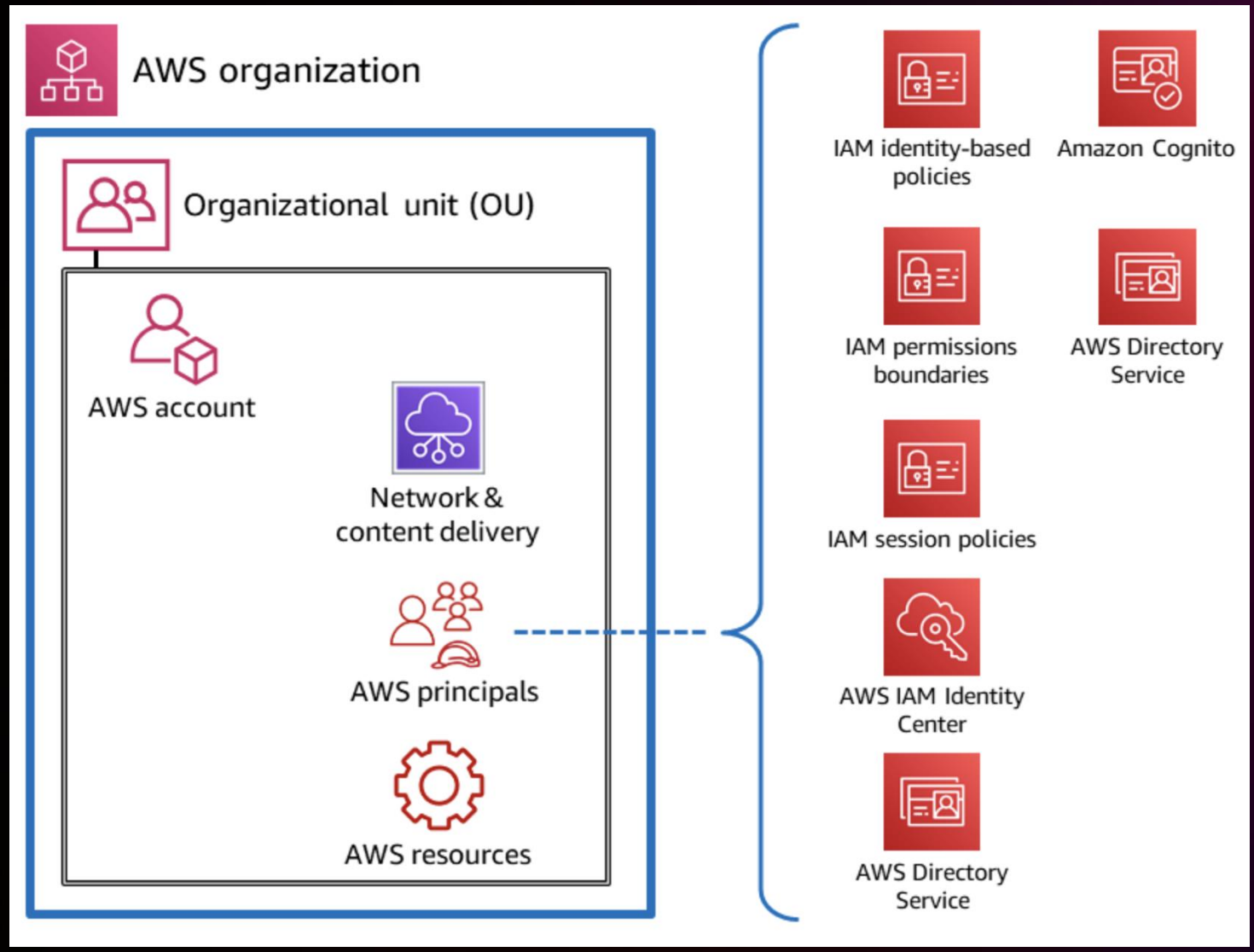
# Protecting accounts



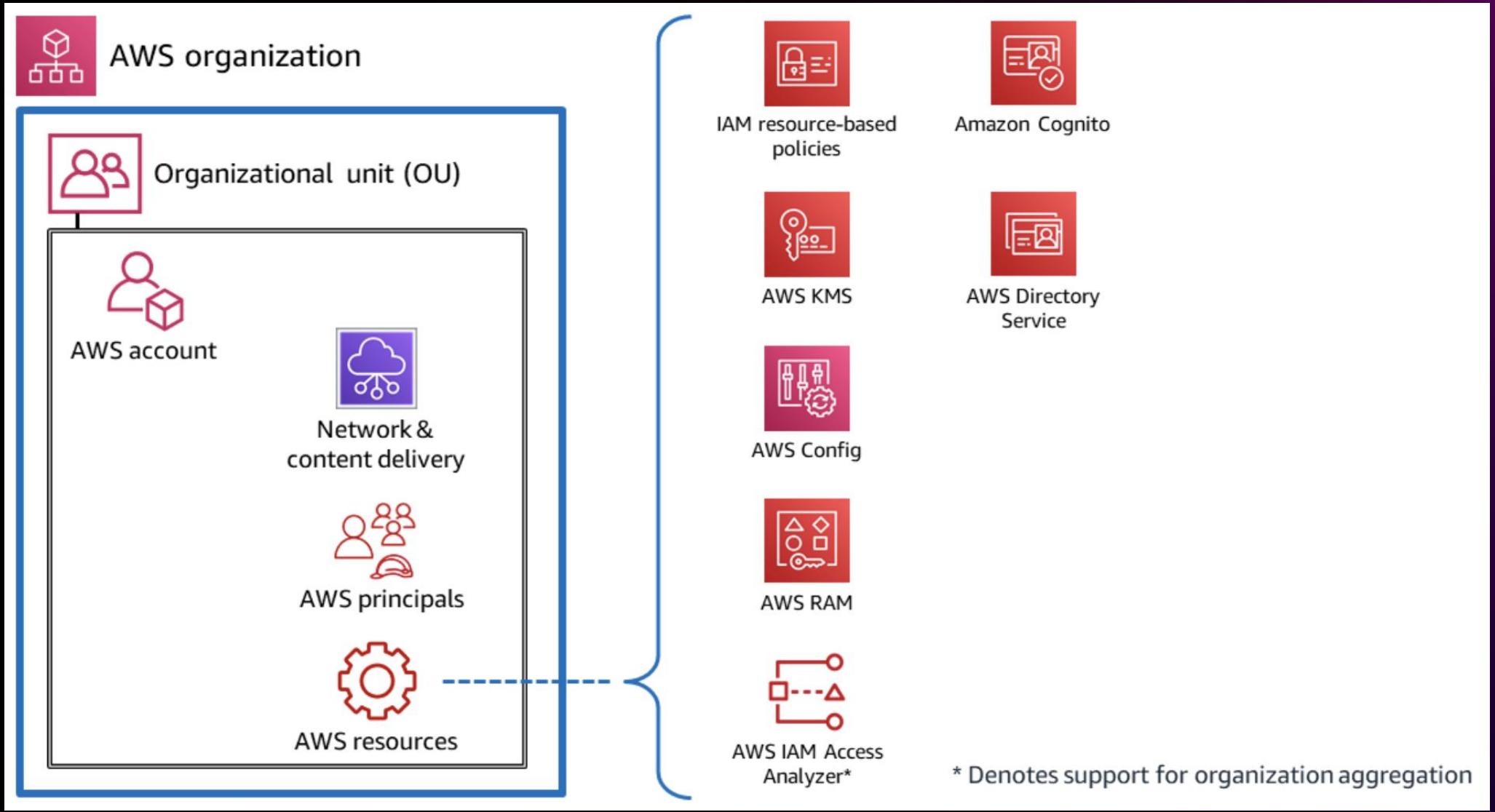
# Protecting the network



# Protecting AWS principals

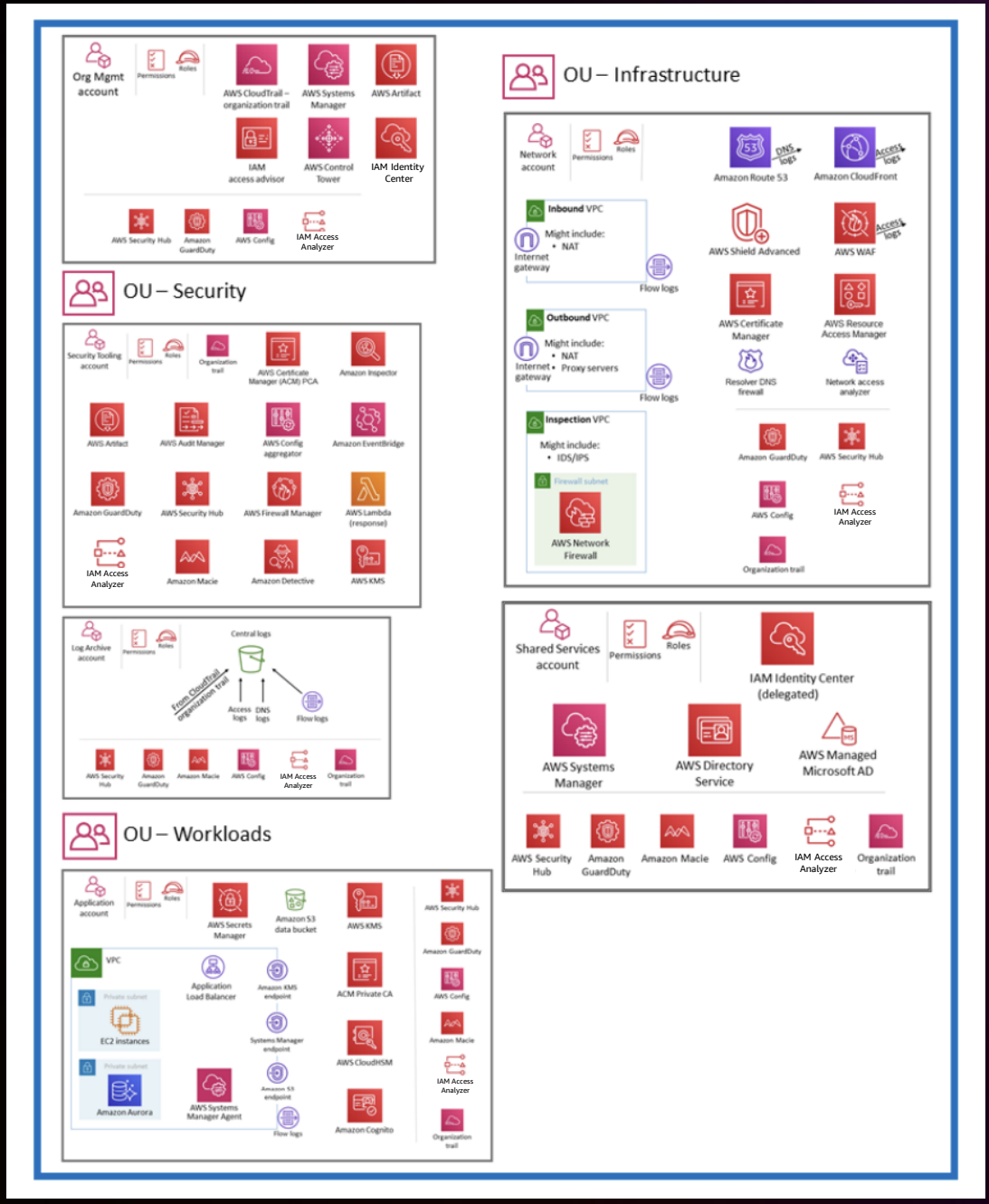


# Protecting AWS resources



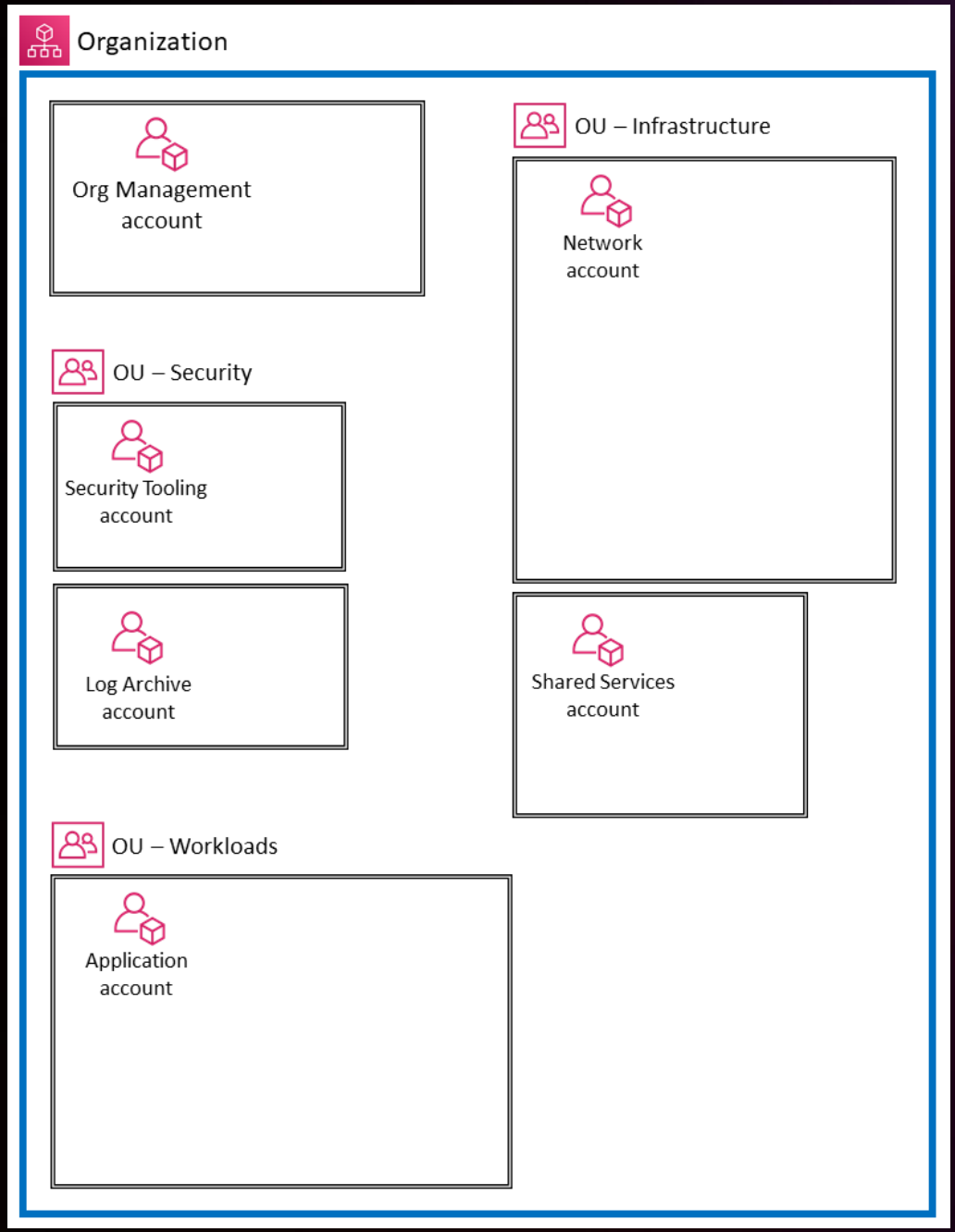
# Let’s dive into the architecture

# AWS SRA



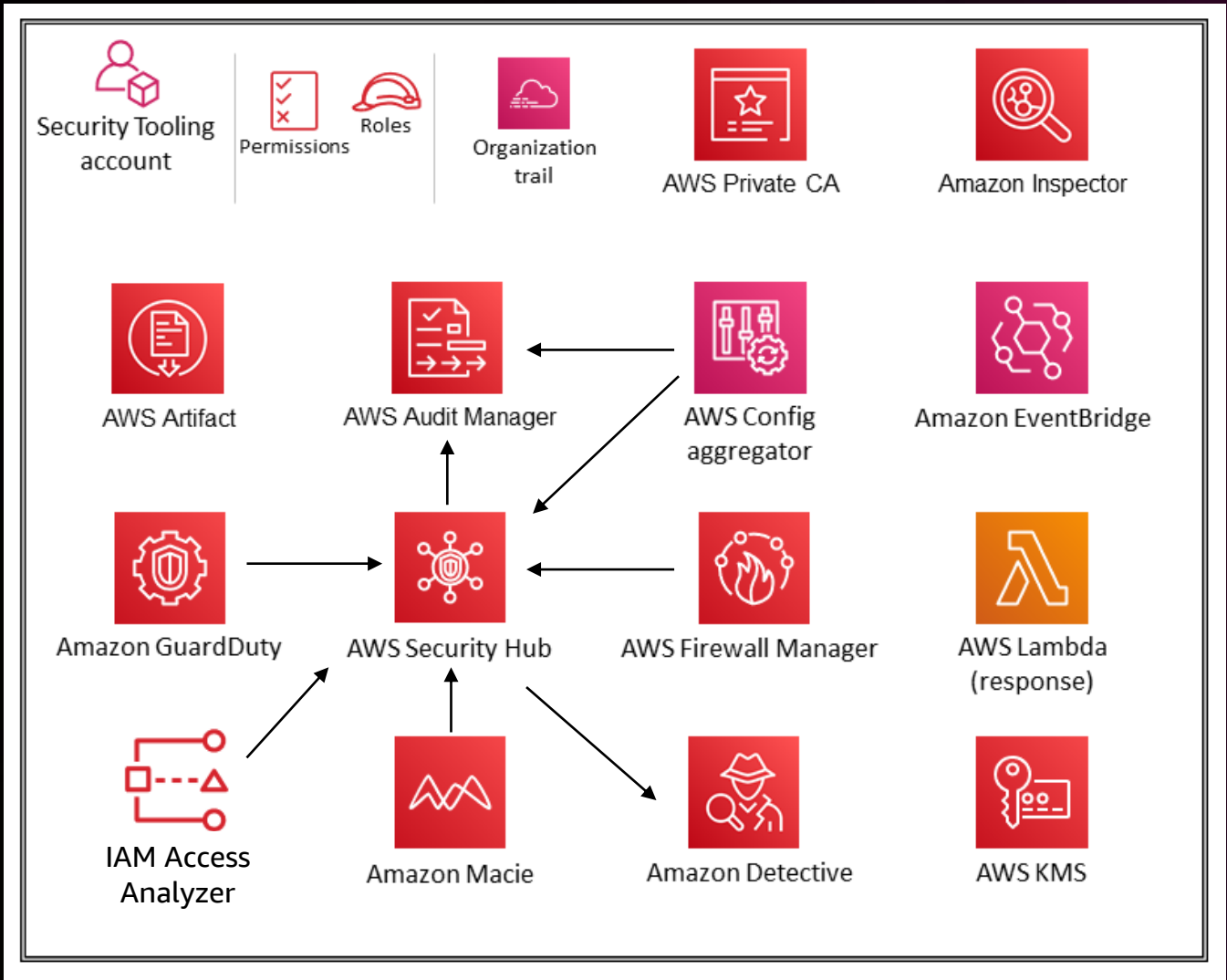
# AWS SRA

Organizational Unit (OU) →

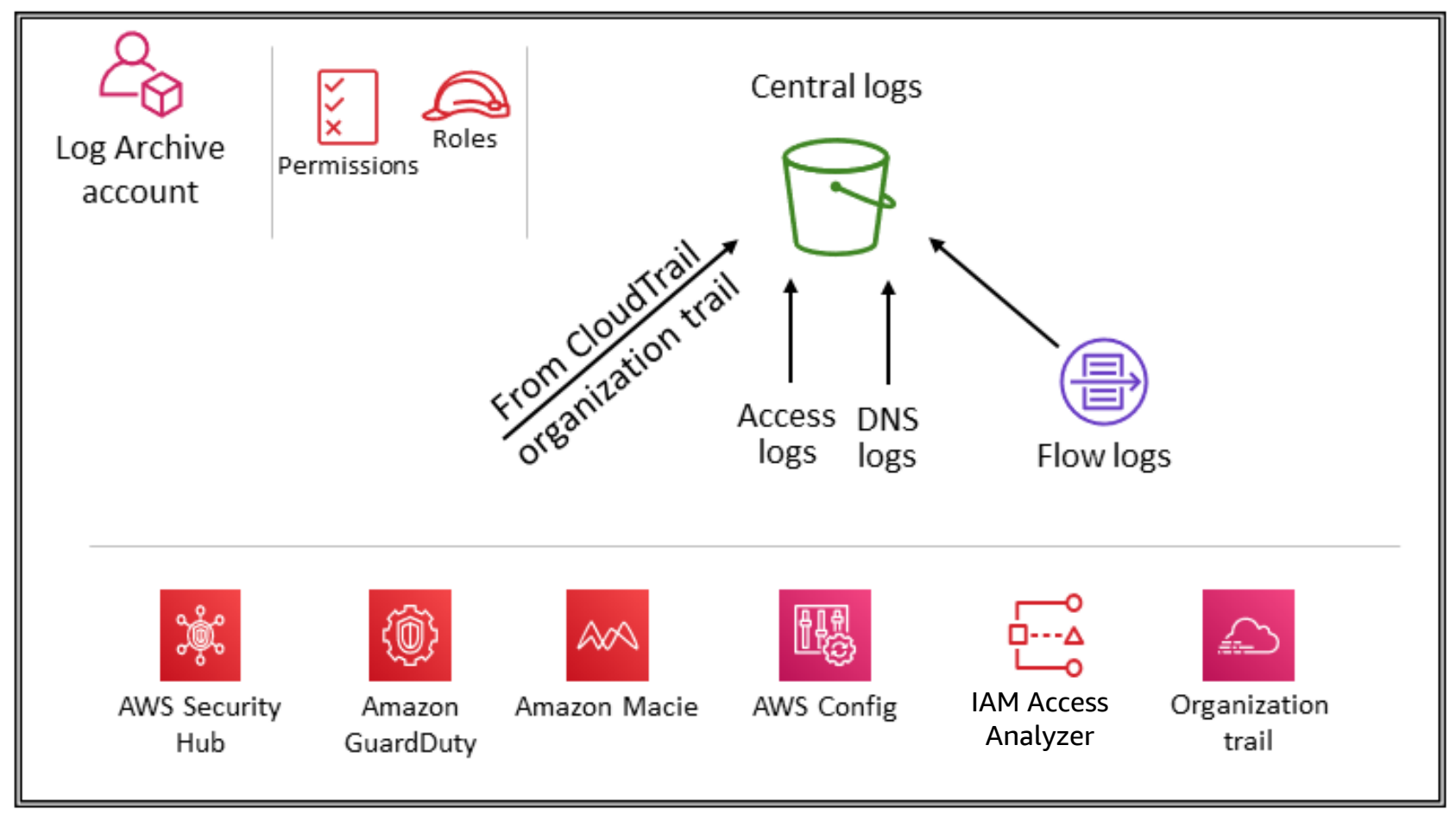



← A Single AWS Organization

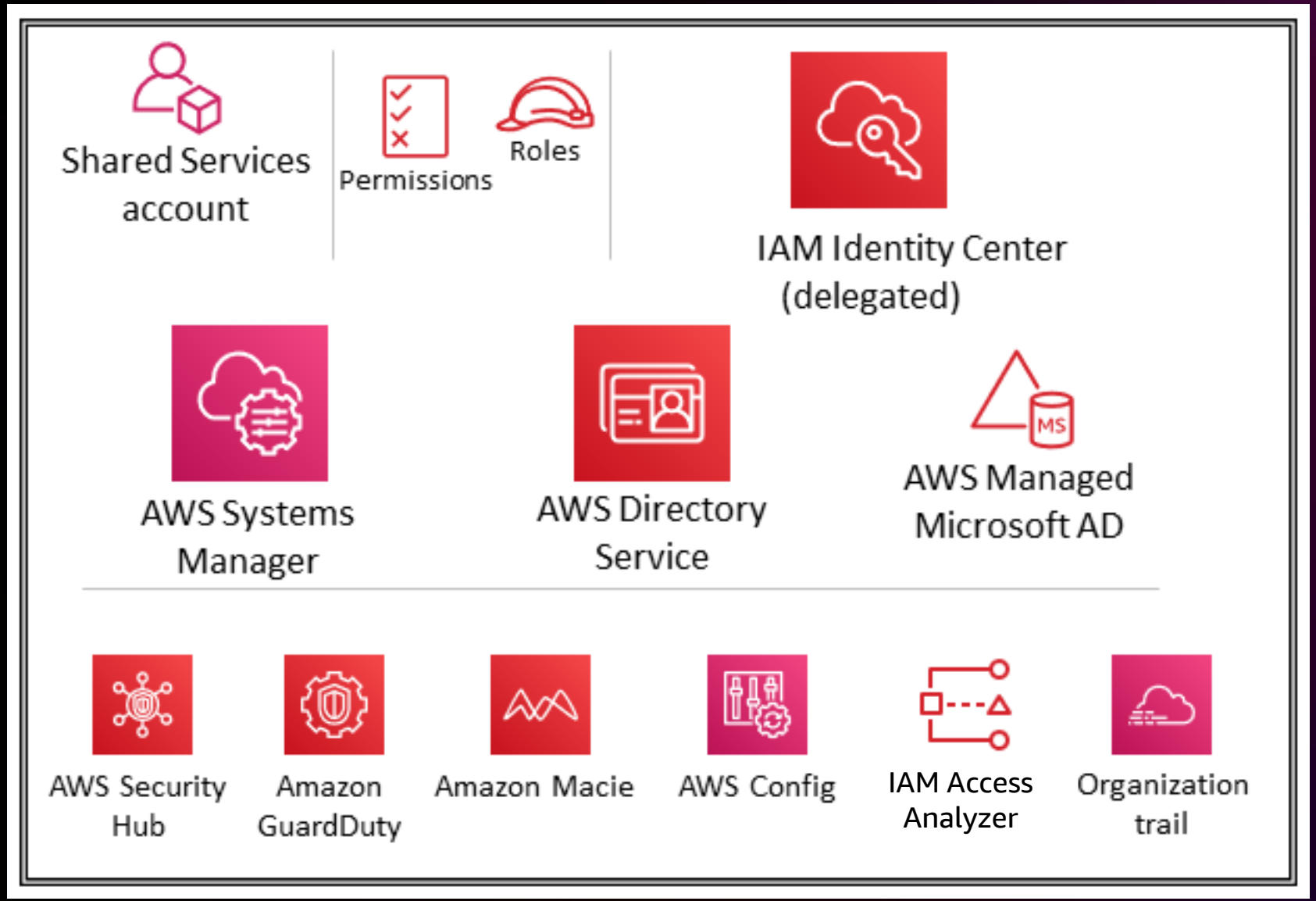
# Security OU: Tooling account



# Security OU: Log Archive account

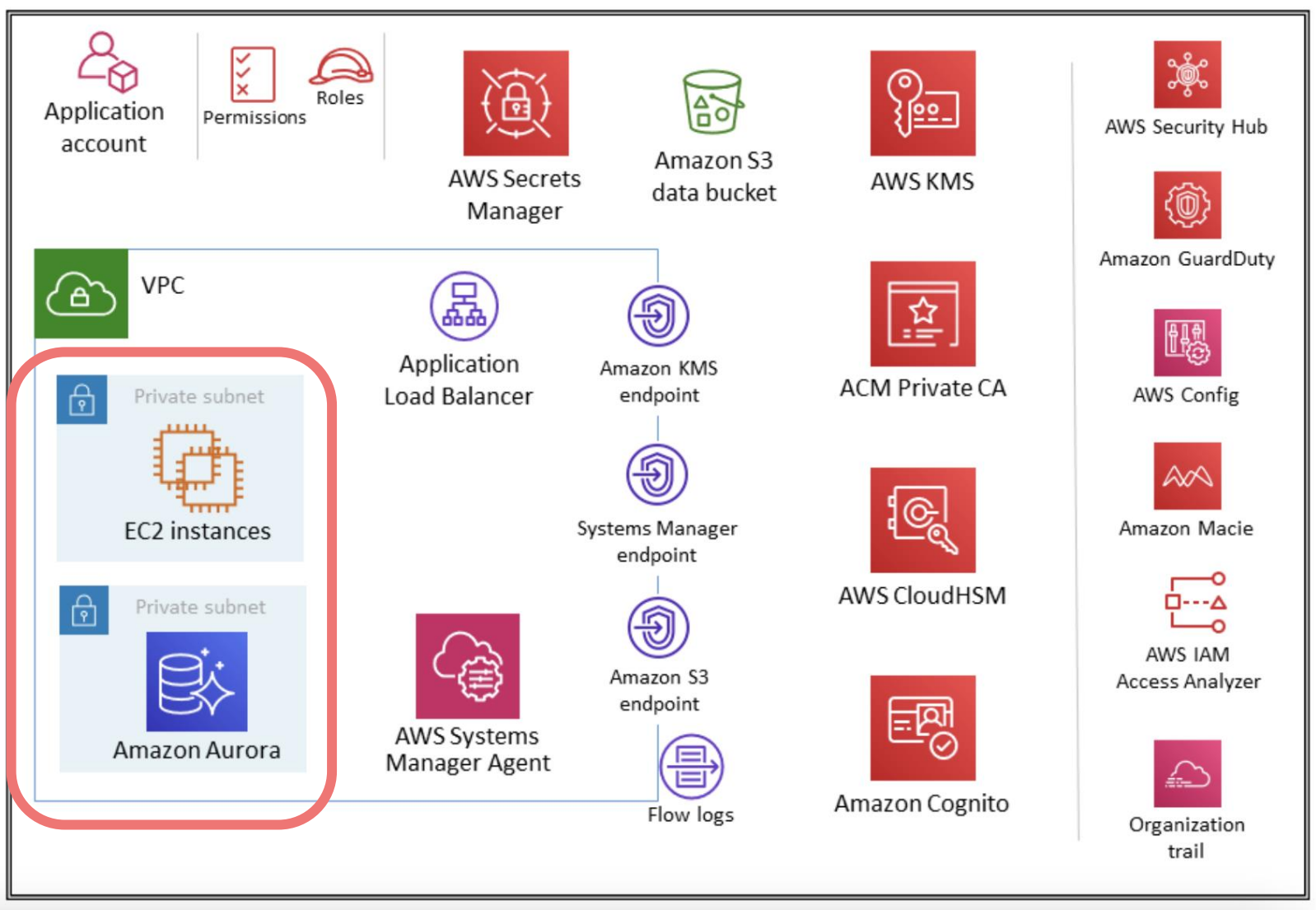


# Infrastructure OU: Shared Services account

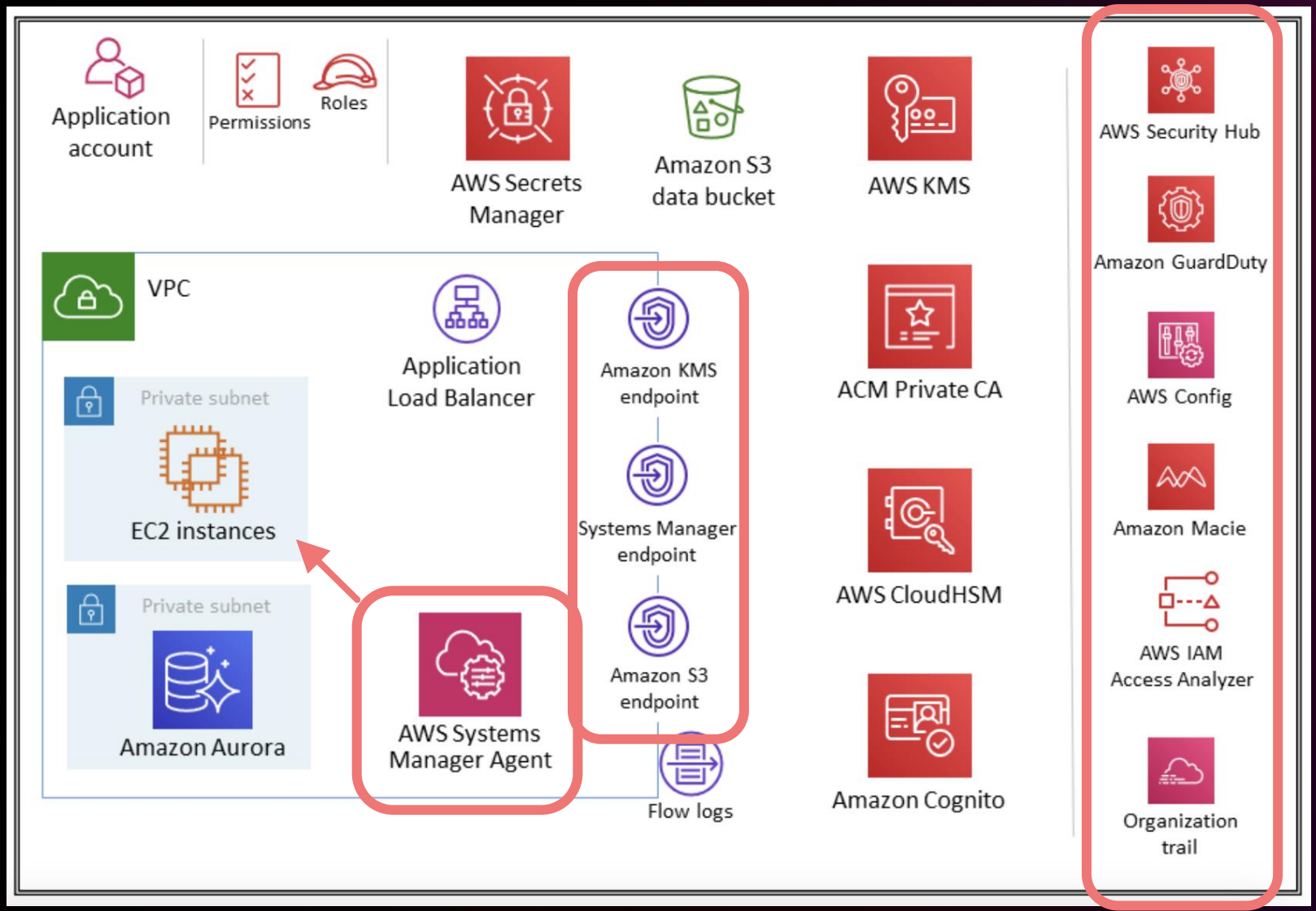


# Workloads OU: Application account

Application



# Workloads OU: Application account



# AWS SRA code repository

# AWS SRA Code

WHAT ELSE IS INCLUDED?

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

# AWS SRA code: Example solutions

CURRENT MODULES

## AWS Organizations

AWS CloudTrail

## AWS Organizations with delegated admin

AWS Config aggregator

AWS Config conformance packs

AWS Firewall Manager

AWS Security Hub

Amazon GuardDuty

Amazon Macie

IAM Access Analyzer

## Default account configurations

IAM password policy

Amazon EBS default encryption

Amazon S3 public access block

# AWS SRA code prerequisites

- **Prerequisites**
  - Download and stage the SRA solutions: https://bit.ly/3yWP25O

    **Note:** This only needs to be done once for all the solutions
  - Verify that the SRA prerequisites solution has been deployed: https://bit.ly/3CG3AYr
- **Solution deployment**
  - Choose a deployment method

    AWS CloudFormation: https://bit.ly/3T8XZB1

    Customizations for AWS Control Tower: https://bit.ly/3MBGPtj

# AWS SRA Code

IMPLEMENT WITH AWS CONTROL TOWER

1 Setup environment

AWS Control Tower

Customizations pipeline

2 Download SRA code

Clone GitHub repository

3 Package and stage code

Lambda function

Required libraries

aws Management account

lambda-zips-bucket

4 Update and stage configuration files

CFCT configuration

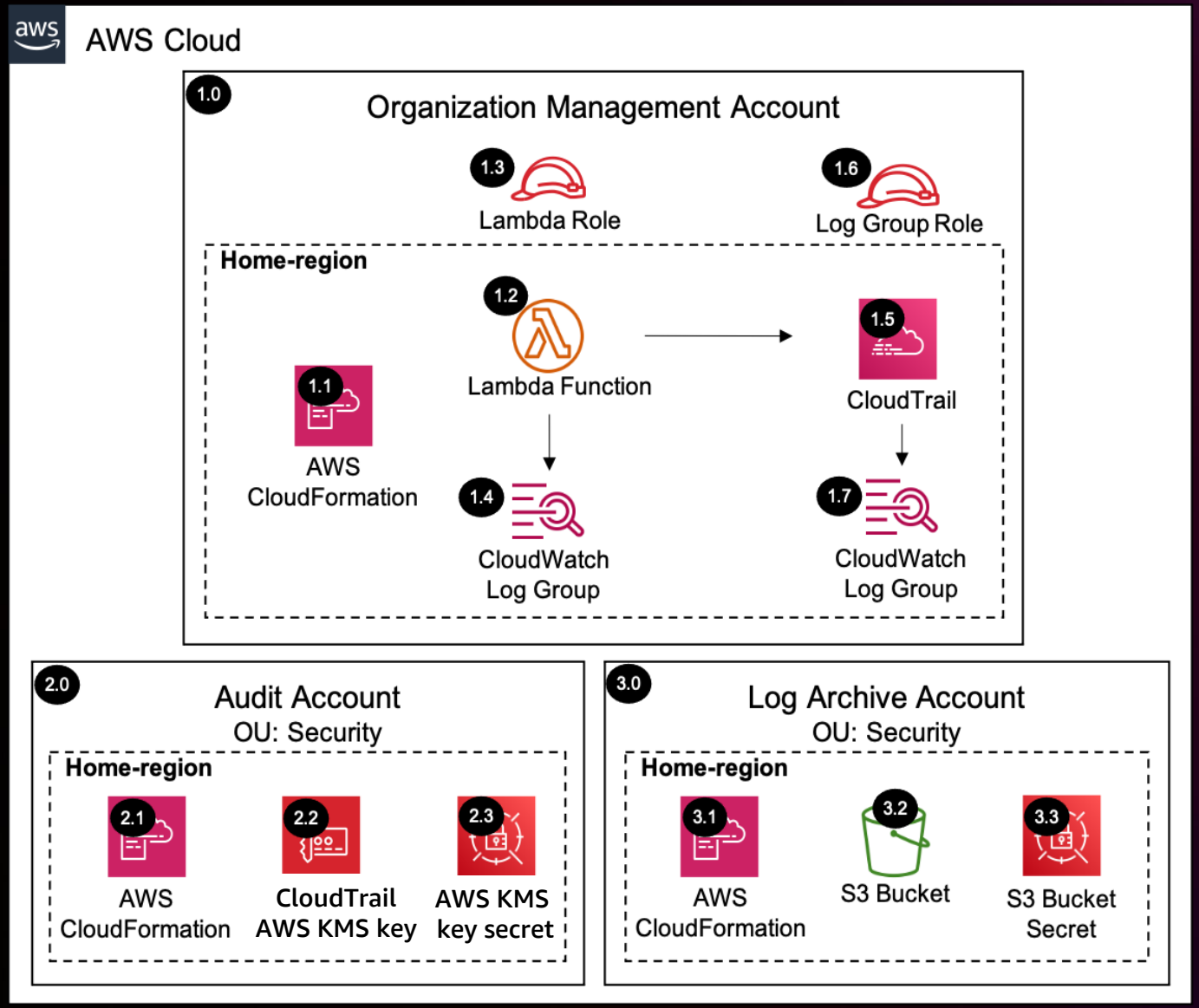
Parameter files

Manifest file

Template files

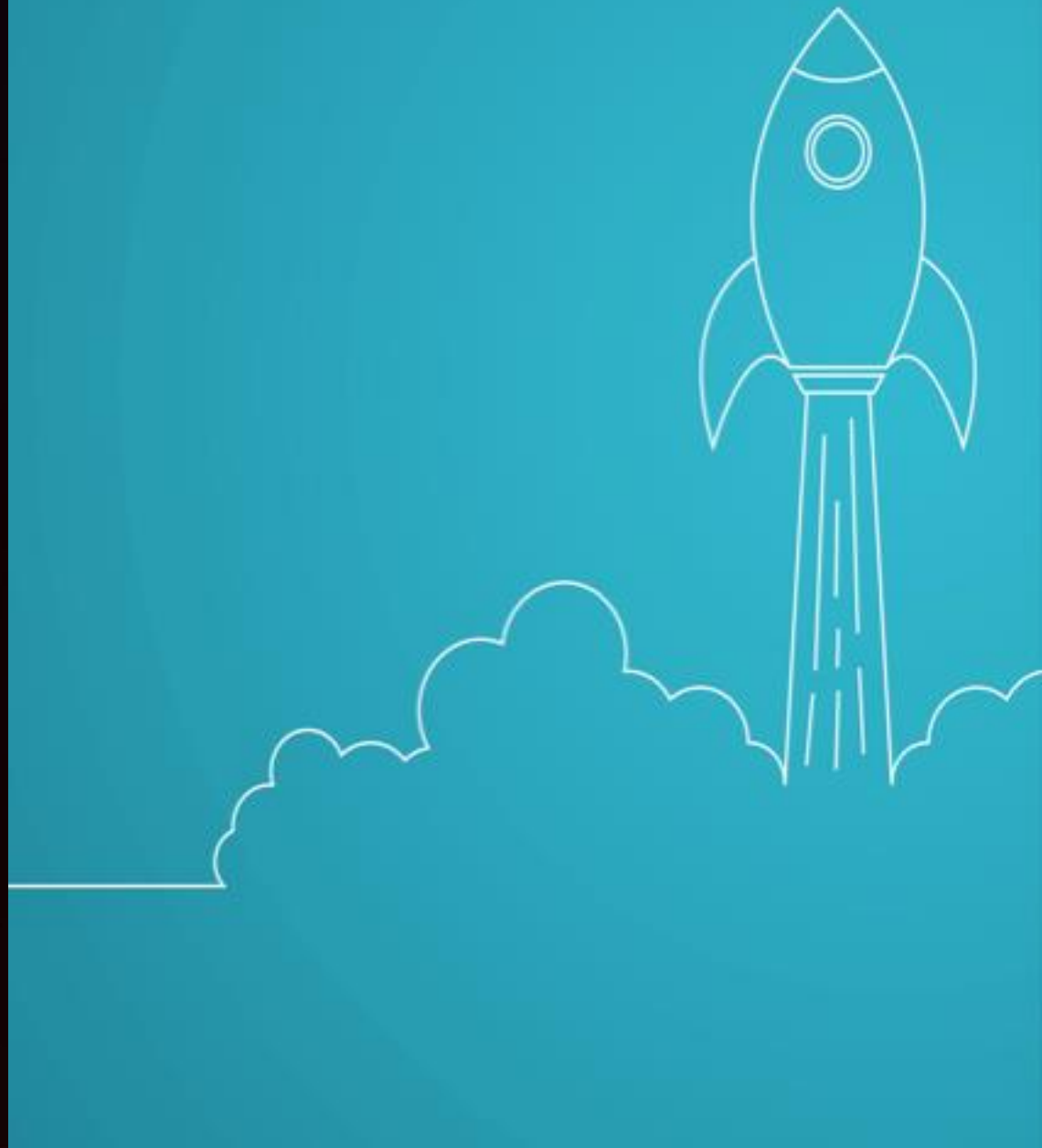
5 Trigger the pipeline

# AWS SRA module: AWS CloudTrail



# Key takeaways

- Define target state for your own security architecture
- Review (and revise) the designs and capabilities you have already implemented
- Use IaC to implement your security architecture
- Learn more about AWS security services and capabilities
- Understand cloud security generally
- Drive a discussion of organizational responsibilities for security



# Apply what you have learned today

## Within the next week:

- Assess your organization's current security architecture
- Learn about the latest AWS security services and features

## Within the next three months:

- Identify 1–2 security improvements in your org's architecture
- Host a Lunch & Learn to help peers understand how security improvements can accelerate business outcomes

## Within the next six months:

- Work with stakeholders to earn trust and help them understand the importance of cloud security
- Establish a mechanism to validate your security architecture as major changes happen within your AWS environment

# Link to AWS SRA resources

AWS SRA
Prescriptive Guidance

AWS SRA
Code Repository

# Secure your castle

# Be a guardian for your AWS environment

# Thank you!

Sarah Currey
sccurrey@amazon.com

Johnny Ray
ryjohnn@amazon.com

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