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

SEC311-R

Securing serverless workloads on AWS

Nikhil Enmudi

Sr. Solutions Architect
AWS

Reef D'Souza

Principal Solutions Architect
AWS

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

Agenda

Foundational security and a lens to create a threat model for your application

Overview of the shared responsibility model for serverless applications

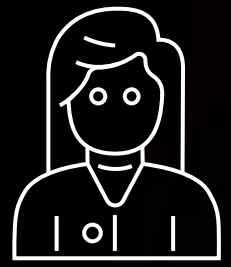
Layering in security for your serverless application

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

What are we trying to solve?

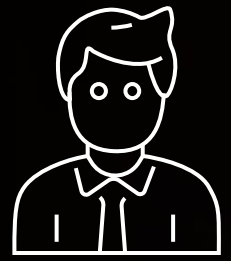
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What are we trying to solve?



DEVOPS

- Build secure applications
- Detect application vulnerabilities in code
- Monitor for security misconfigurations
- Instrument CI/CD pipelines to reduce risk early
- Map responsive controls to alerts
- Hardened environments to deploy a serverless app



SECURITY AND COMPLIANCE

- Understand the shared responsibility model
- Create a threat model for a serverless application

aws

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

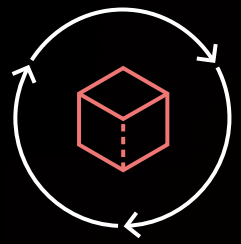
CIOs say that 80% of developers' time is spent on the operations and maintenance of applications and only 20% of the time is actually spent on innovation

Source: Deloitte 2019

aws

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

Why are customers building with a serverless-first strategy?









Agility Performance Cost Security

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

Foundational security framework

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

Foundational security



Identity and access management



Detective controls



Infrastructure protection



Data protection



Incident response

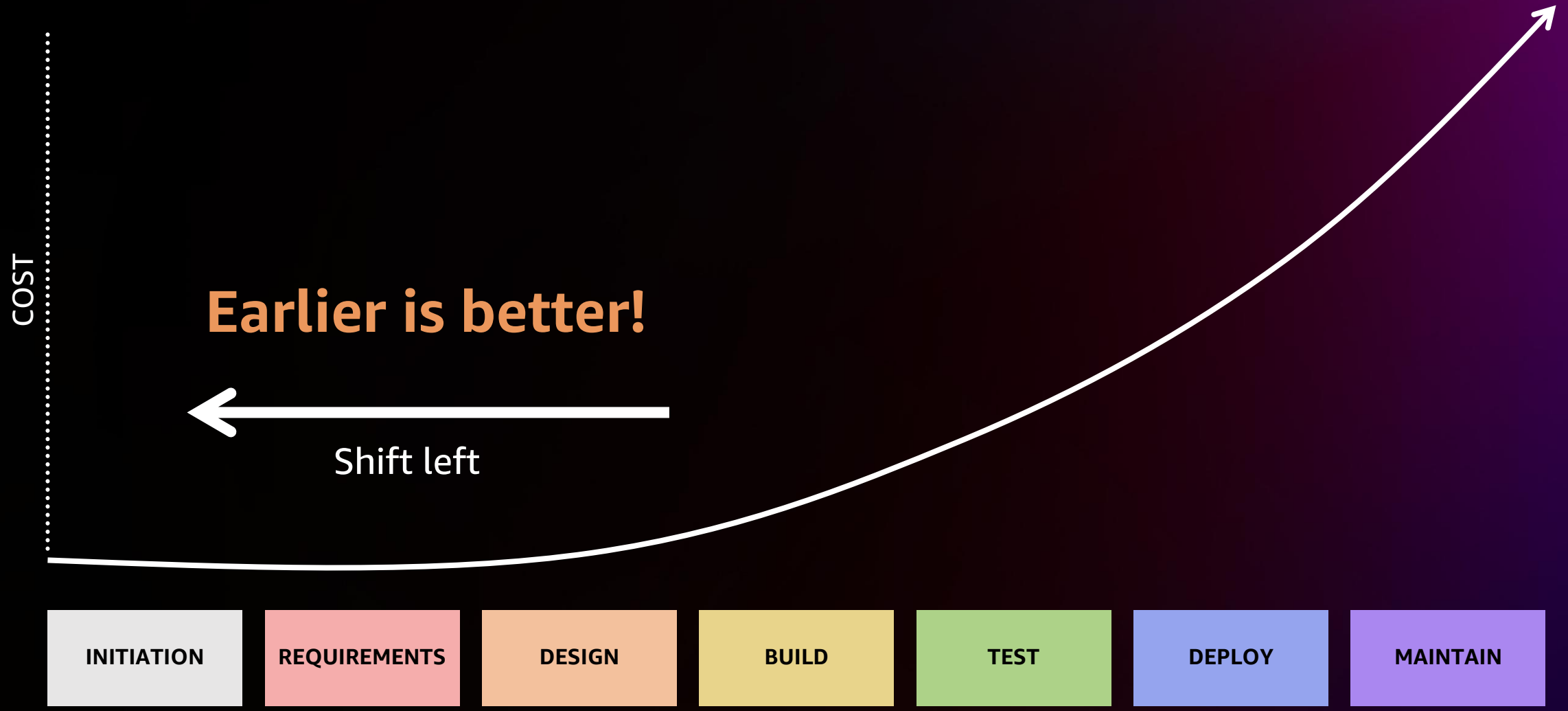
aws

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

Threat modeling

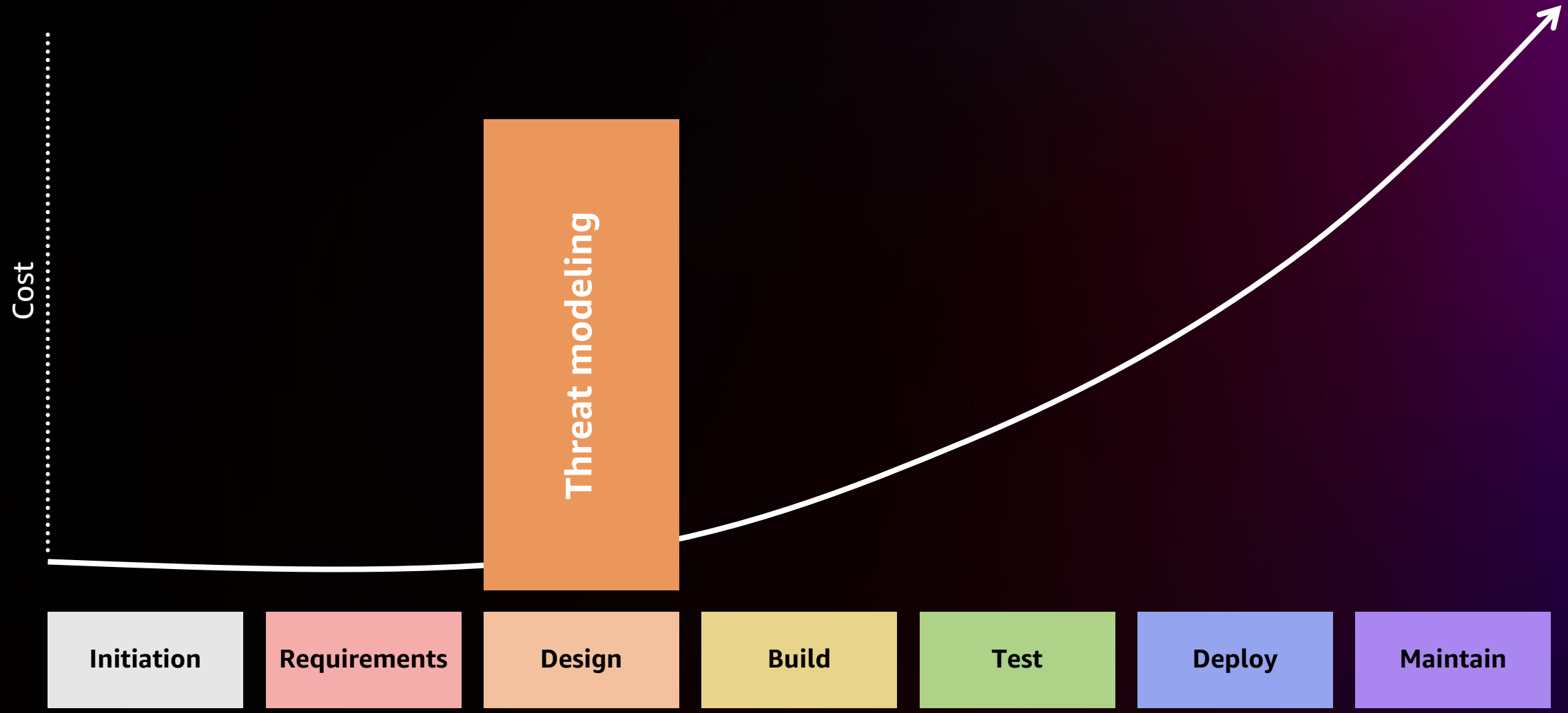
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cost of defect fixes



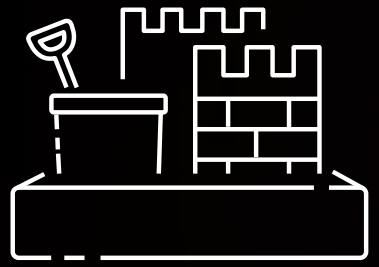
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cost of defect fixes

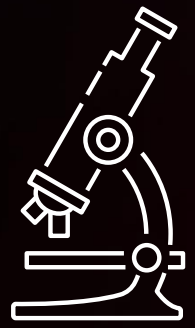


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Basic phases of threat modeling



What are we building?



What can go wrong?



What are we going to do about it?

aws

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

What can go wrong?

WHAT ARE WE BUILDING?

Design
Data flow
Entry points

ACTORS

Internal/external
Motivations/goals



STRIDE

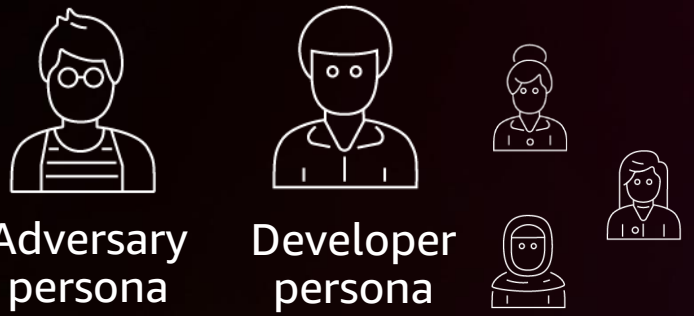
Spoofing
Tampering
Repudiation
Info. disclosure
Denial of service
Elevation of privilege

THREATS

OWASP Top 10
HITRUST Threat Catalogue
Your organization's threat catalog

BRAINSTORM

By following the data flows



Adversary persona

Developer persona

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

What are we going to do about it?

WHAT CAN GO WRONG



ANALYSIS AND PRIORITIZATION



Business persona

Defender persona

Developer persona

SOFTWARE CONTROLS

Input validation
Authentication
Session handling
Bounds handling

AWS SERVICE CONTROLS

Identity and access management
Data protection
Infrastructure security
Logging and monitoring

aws

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

Shared responsibility








Amazon EC2 | AWS Fargate | Amazon RDS | Amazon S3 | AWS KMS | Amazon DynamoDB

More customizable
+
More customer responsibility

Infrastructure services		Container Services		Abstracted Services	
CUSTOMER DATA	CUSTOMER IAM	CUSTOMER DATA	CUSTOMER IAM	CUSTOMER DATA	CUSTOMER IAM
PLATFORM & APPLICATION MANAGEMENT		NETWORK TRAFFIC PROTECTION		CLIENT-SIDE DATA ENCRYPTION	
OS, NETWORK, FIREWALL CONFIGURATION		CLIENT-SIDE DATA ENCRYPTION		SERVER-SIDE ENCRYPTION	AWS IAM
NETWORK TRAFFIC PROTECTION		FIREWALL CONFIGURATION		NETWORK TRAFFIC PROTECTION	
SERVER-SIDE ENCRYPTION		PLATFORM & APPLICATION MANAGEMENT	AWS IAM	PLATFORM & APPLICATION MANAGEMENT	
CLIENT-SIDE DATA ENCRYPTION / INTEGRITY		OS, NETWORK, FIREWALL CONFIGURATION		OS, NETWORK, FIREWALL CONFIGURATION	
COMPUTE / STORAGE / DATABASE / NETWORK	AWS IAM	COMPUTE / STORAGE / DATABASE / NETWORK		COMPUTE / STORAGE / DATABASE / NETWORK	
HARDWARE/AWS GLOBAL INFRASTRUCTURE		HARDWARE/AWS GLOBAL INFRASTRUCTURE		HARDWARE/AWS GLOBAL INFRASTRUCTURE	

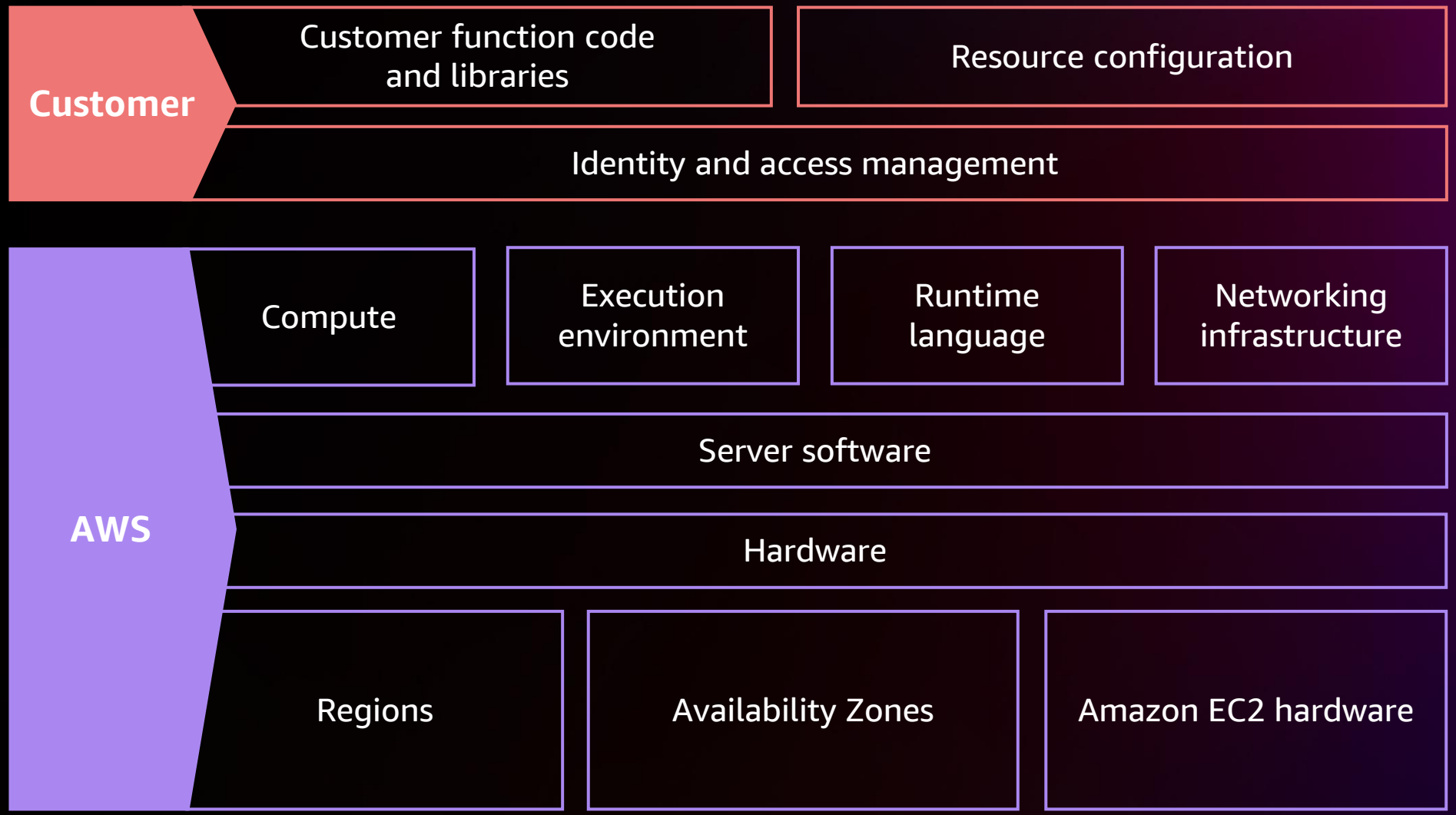
Less customizable
+
Less customer responsibility
+
More Best practices built-in

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

AWS Lambda customer security responsibility

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

Overview of customer responsibility



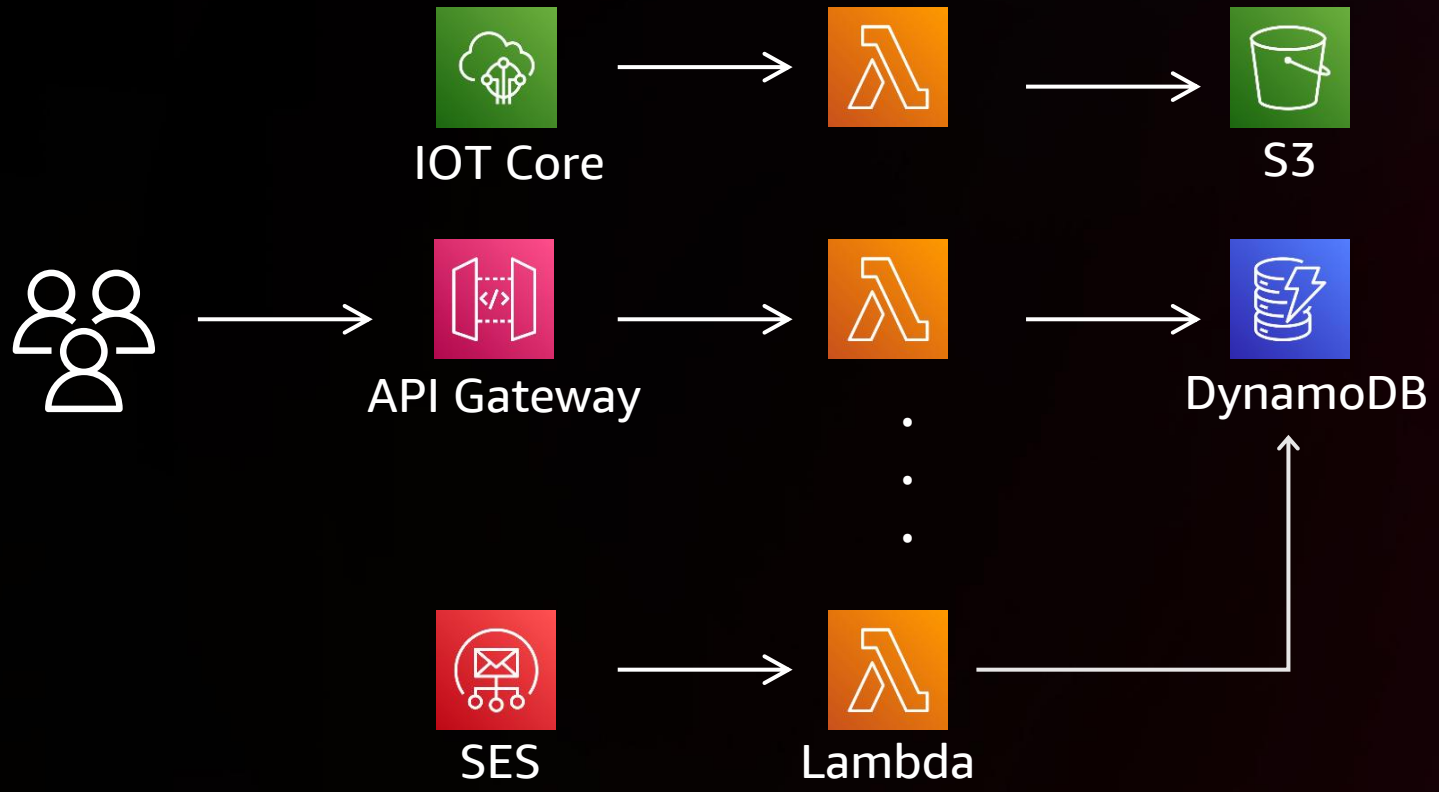
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Anatomy of serverless workloads

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

Anatomy of serverless workloads

A SIMPLE SERVERLESS APPLICATION

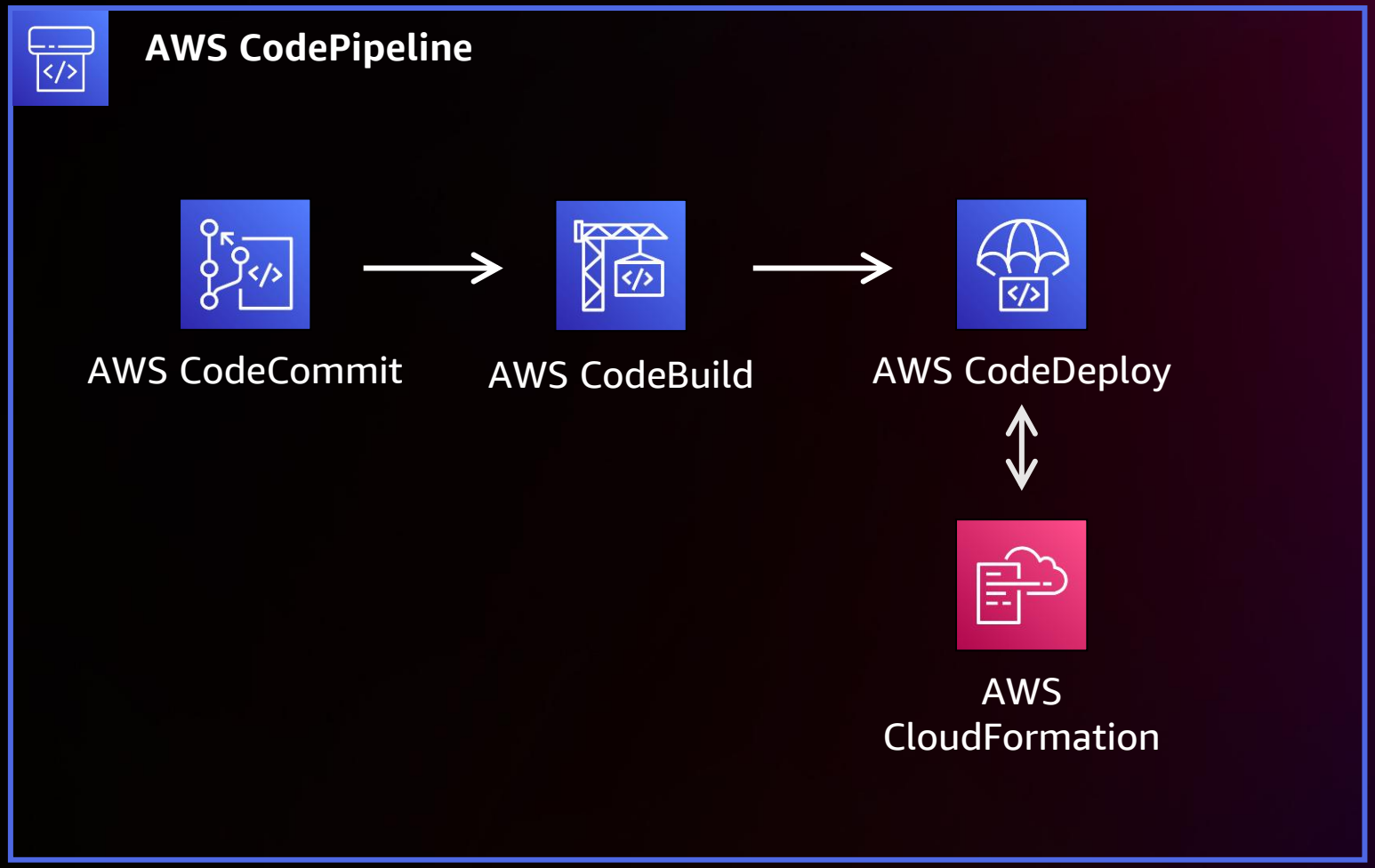


- Has multiple entry points
- Executes code
- Stores/Retrieves data

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

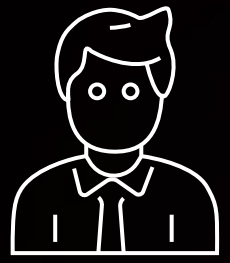
Anatomy of serverless workloads

DEPLOYMENT PIPELINE FOR SERVERLESS APPLICATION

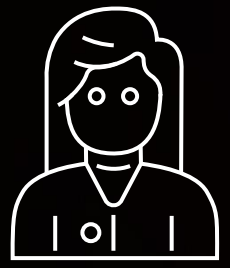


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Responsibility: Customer function code and libraries



SECURITY AND COMPLIANCE



DEVOPS

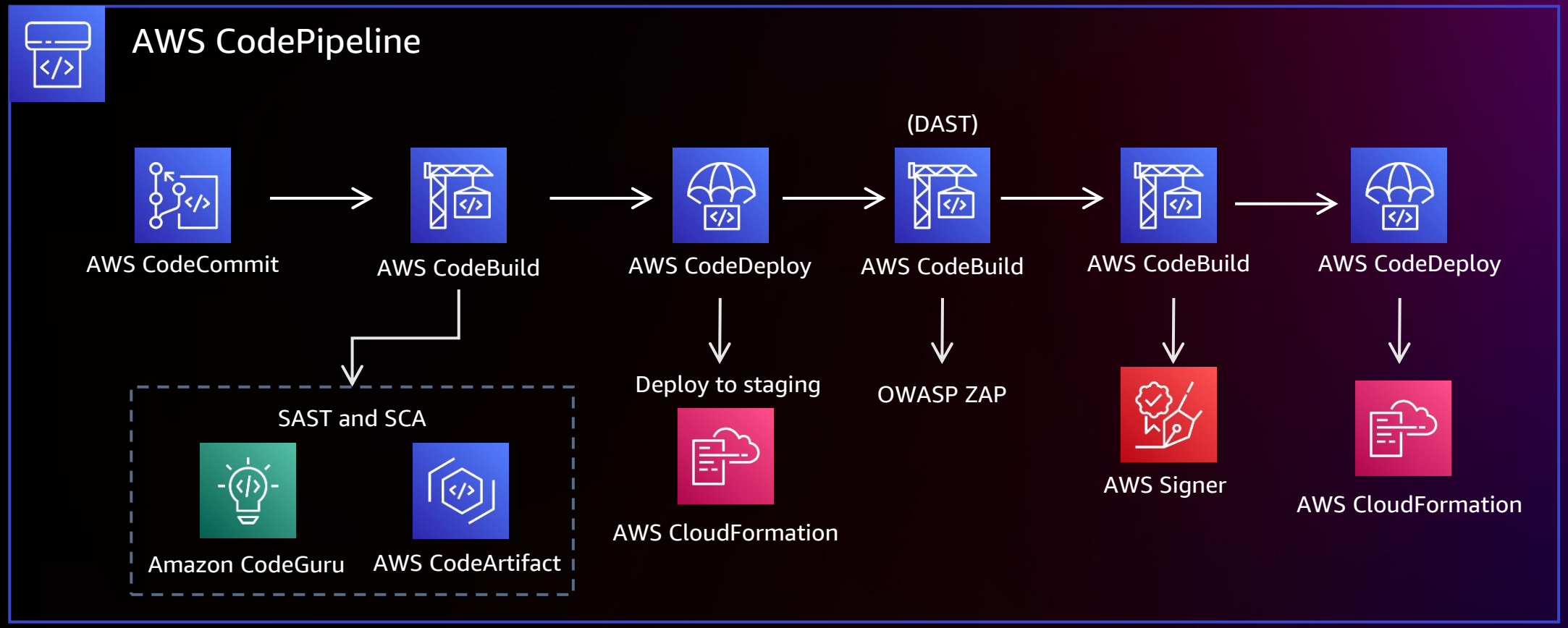
Concerns

- Are the applications using security-approved third-party libraries?
- Are there any security vulnerabilities in the application code?
- How can I ensure trust and integrity of code deployed to production?
- What tools/services can I use?
- How can it be integrated into the deployment pipeline?

aws

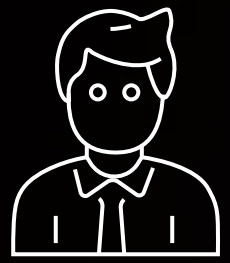
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Responsibility: Customer function code and libraries



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

Responsibility: Identity and access management



SECURITY AND COMPLIANCE

Concerns

- Do the applications have proper authentication and authorization mechanisms in place?
- Does any user or application resource have overly permissive policies?

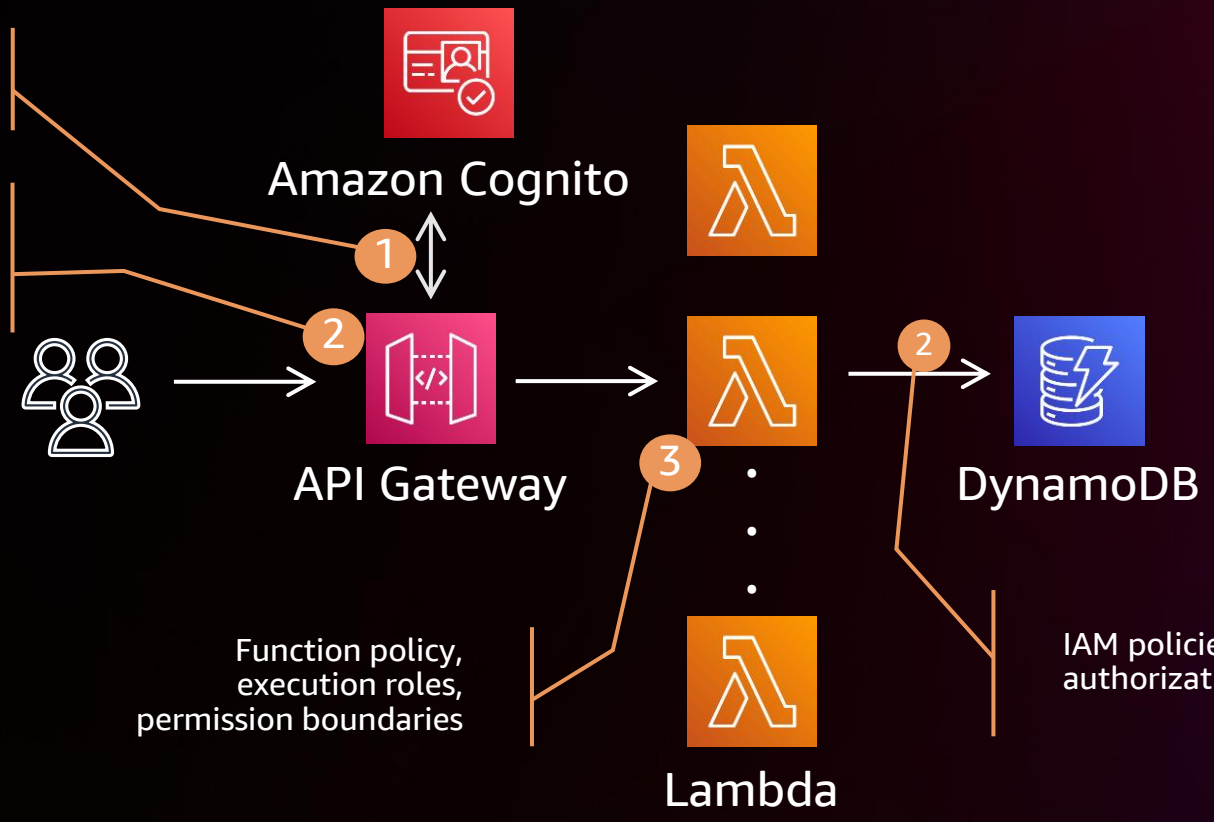
aws

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

Responsibility: Identity and access management

Authentication
- OIDC, SAML, OAUTH2
- Certificate-based

Authorization
- JWT & Cognito user pools
- Custom Lambda authorizer
- IAM authorization



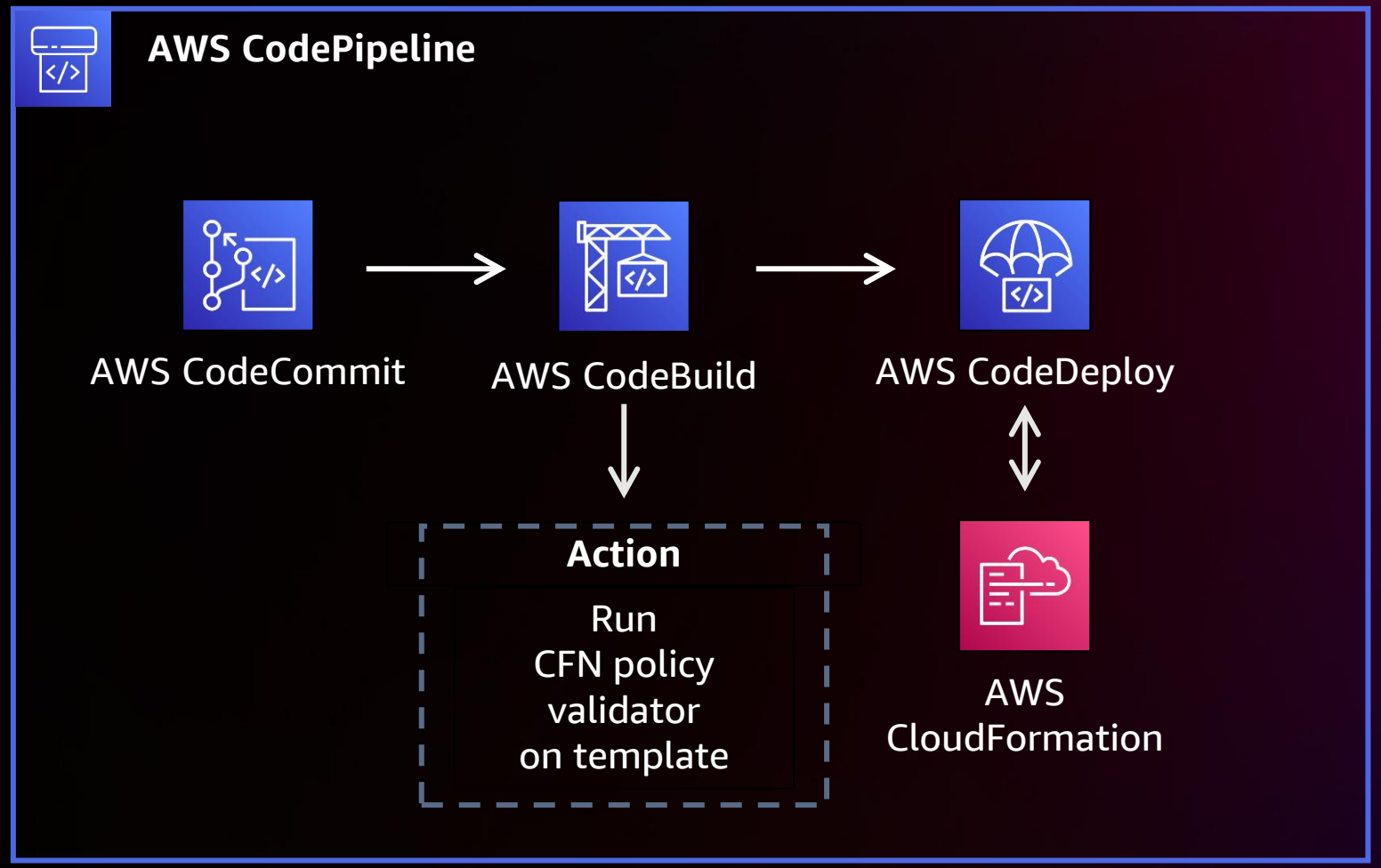
Tooling

IAM Access Analyzer

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

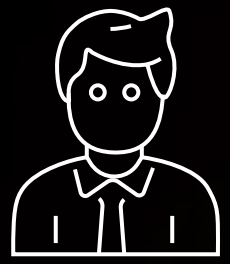
Responsibility: Identity and access management

AUTOMATING POLICY VALIDATION IN THE DEPLOYMENT PROCESS



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

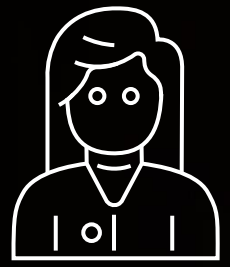
Responsibility: Resource configuration



SECURITY AND COMPLIANCE

Concerns

- Are sensitive credentials, keys, and data secured?
- Secure network configurations
- Ability to respond to security incidents



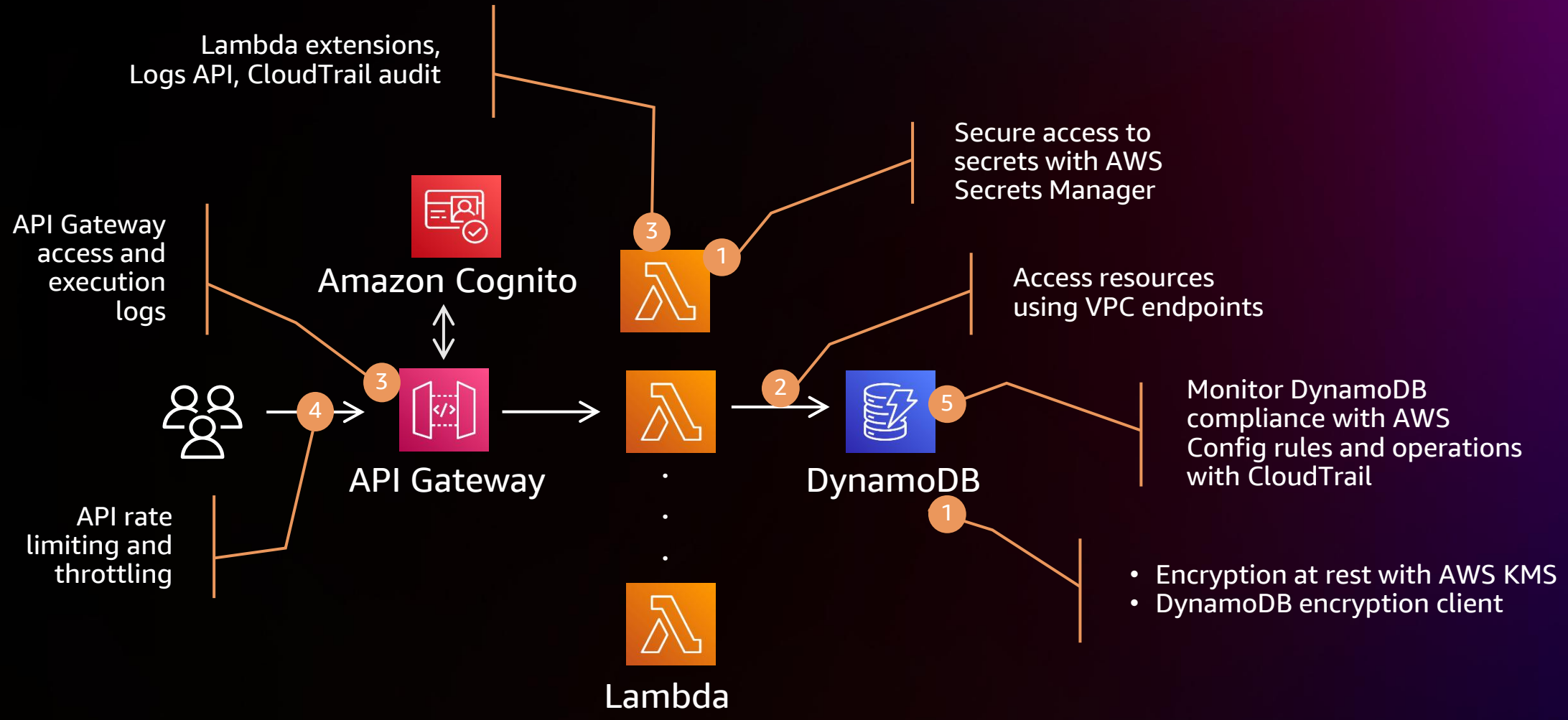
DEVOPS

- What tools/services can I use?
- How can it be integrated into the deployment pipeline?

aws

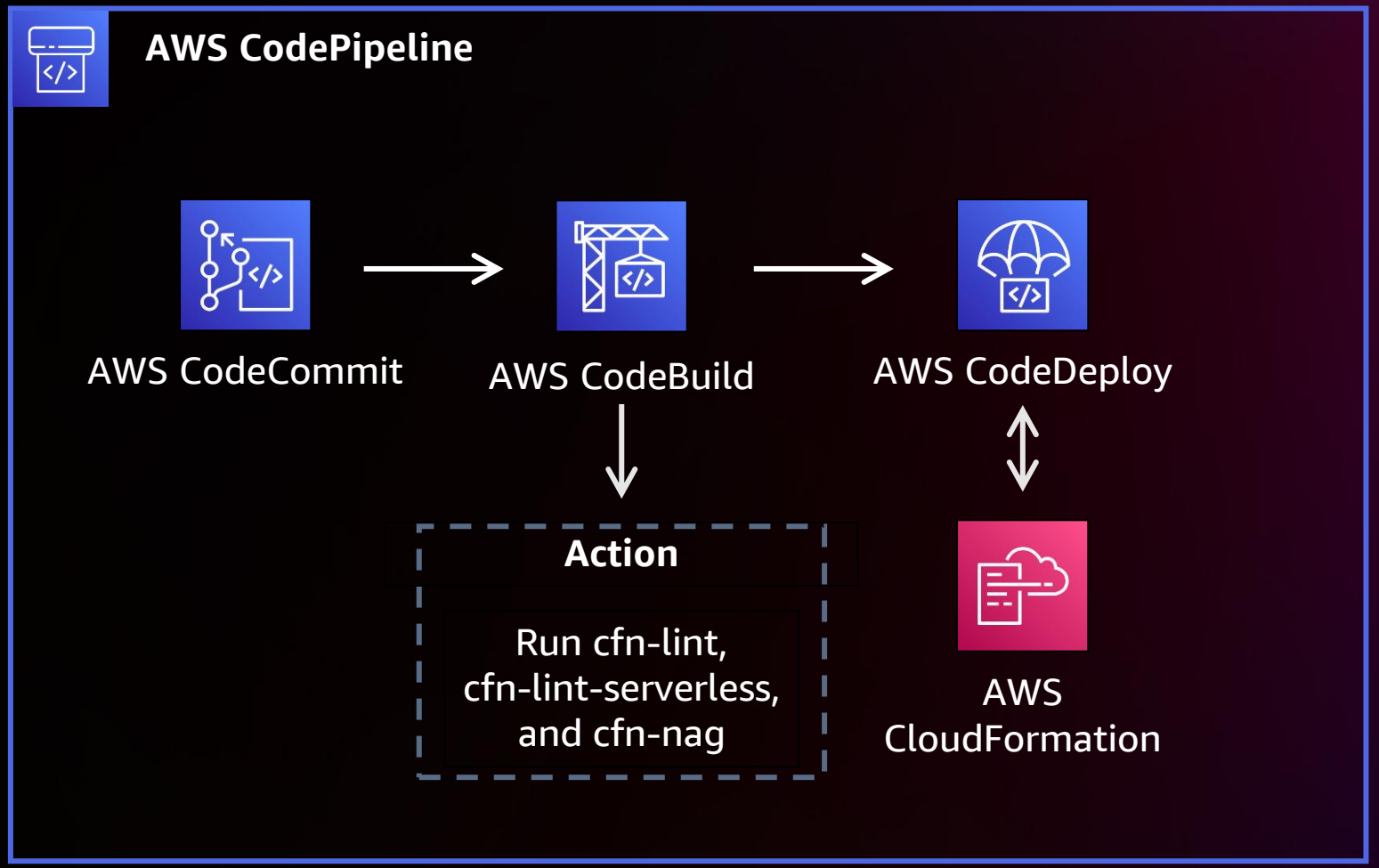
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Responsibility: Resource configuration



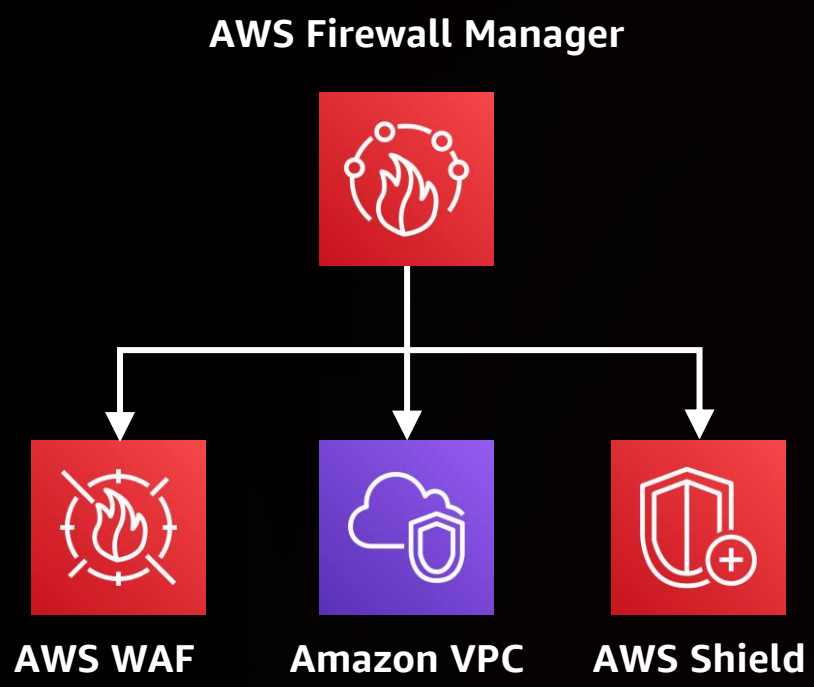
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Responsibility: Resource configuration



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

Perimeter security: Overall picture



- **Centrally enable baseline security** using **AWS WAF, AWS Shield, and Amazon VPC Security Groups** across your organization
- **Consistently enforce** the protections, even as new applications are created
- **View compliance posture** centrally across your AWS accounts

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

Additional serverless security resources

AWS Well-Architected Serverless Lens

https://go.aws/3yTQcyT

AWS Lambda security whitepaper

https://go.aws/3S9SzV6

Amazon API Gateway security whitepaper

https://bit.ly/3SfXxQa

aws

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

Thank you!



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

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