AWS re:Invent

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

SEC314-R2

The journey to least privilege on AWS

Cassia Martin
Security Solutions Architect
Amazon Web Services

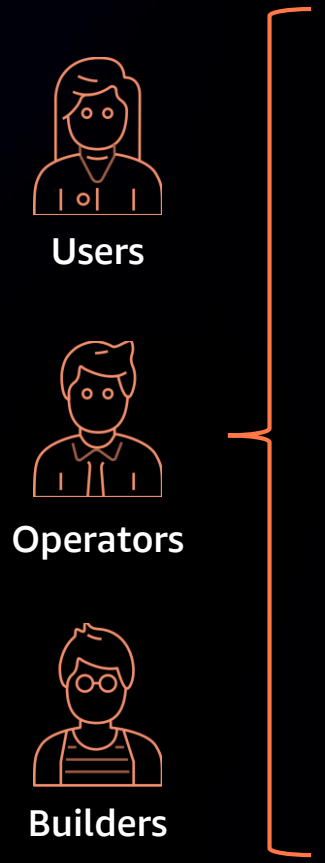
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What are we going to talk about?

- Establish security foundations with account isolation
- Set up preventive guardrails
- Continuously tune access permissions
- Wrap up

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

Scope for this discussion



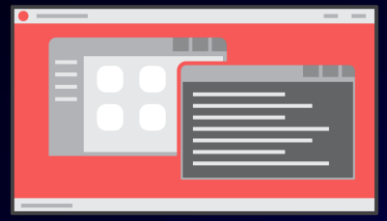
Application
Not in scope

Infrastructure
Not in scope

Cloud platform APIs
In scope



End user applications



Operating systems, relational databases, others



AWS Management Console, AWS Command Line Interface (AWS CLI), API

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

Your journey . . .

Build a secure environment

- Separate accounts
- Construct guardrails

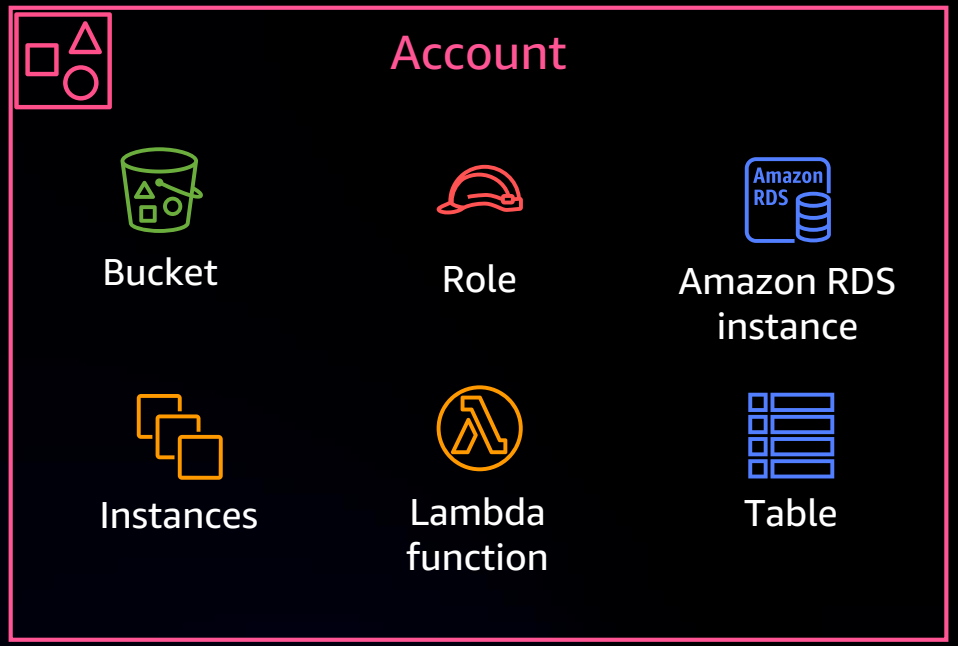
Set and iterate over time

- Allow experimentation
- Use tools to reduce unused access
- Build automation!



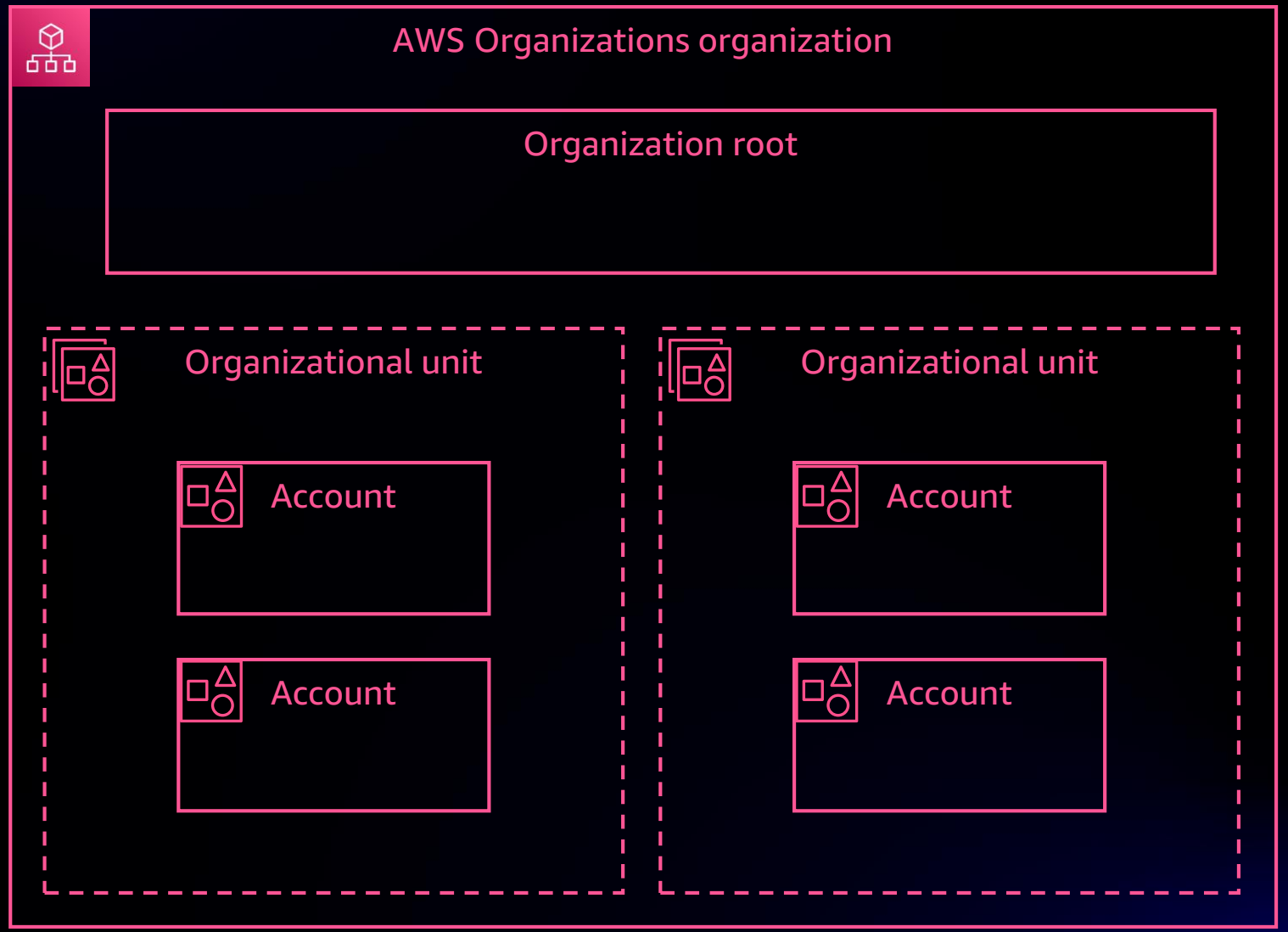
Isolate workloads using accounts

- Resource container for AWS cloud services
- Explicit security boundary
- Container for cost tracking and billing
- Mechanism to enforce limits and thresholds



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

Group accounts by security properties



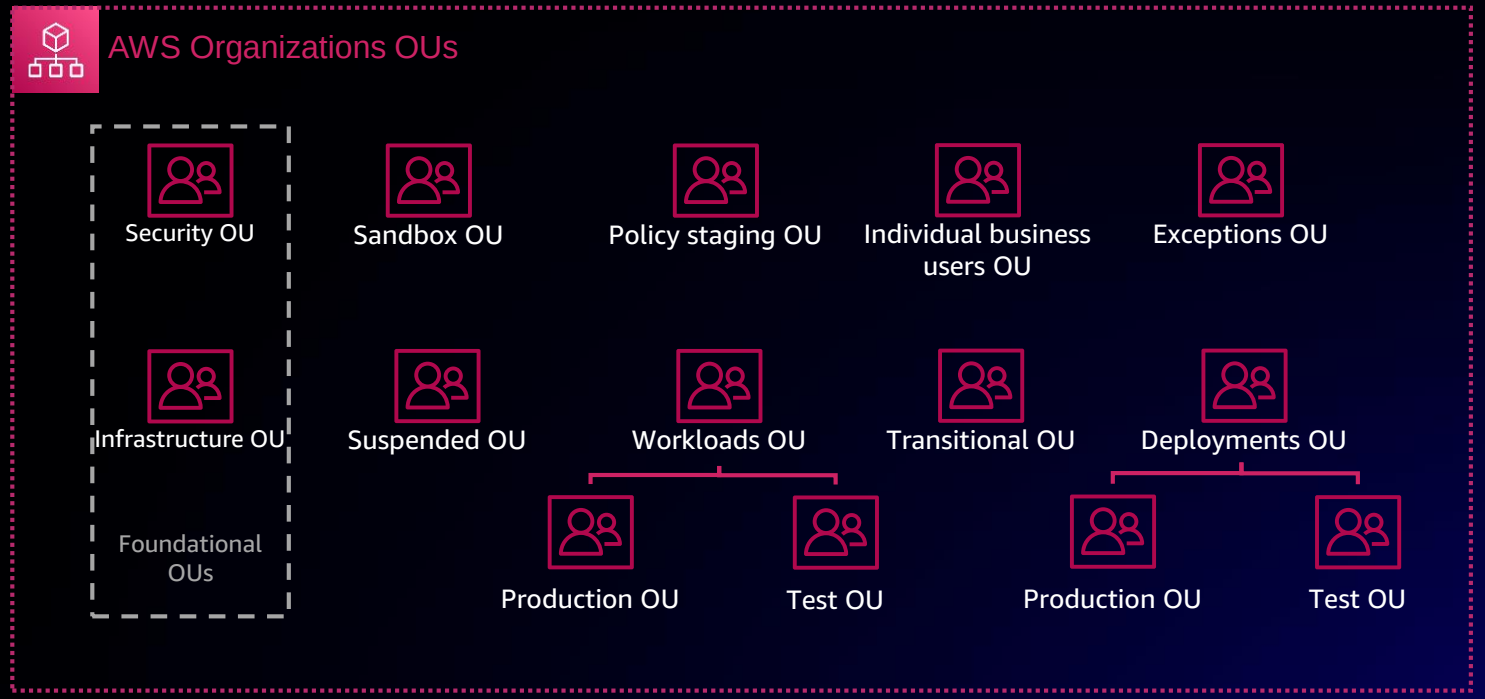
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Discussion

Q: How are you isolating your workloads using multiple accounts?

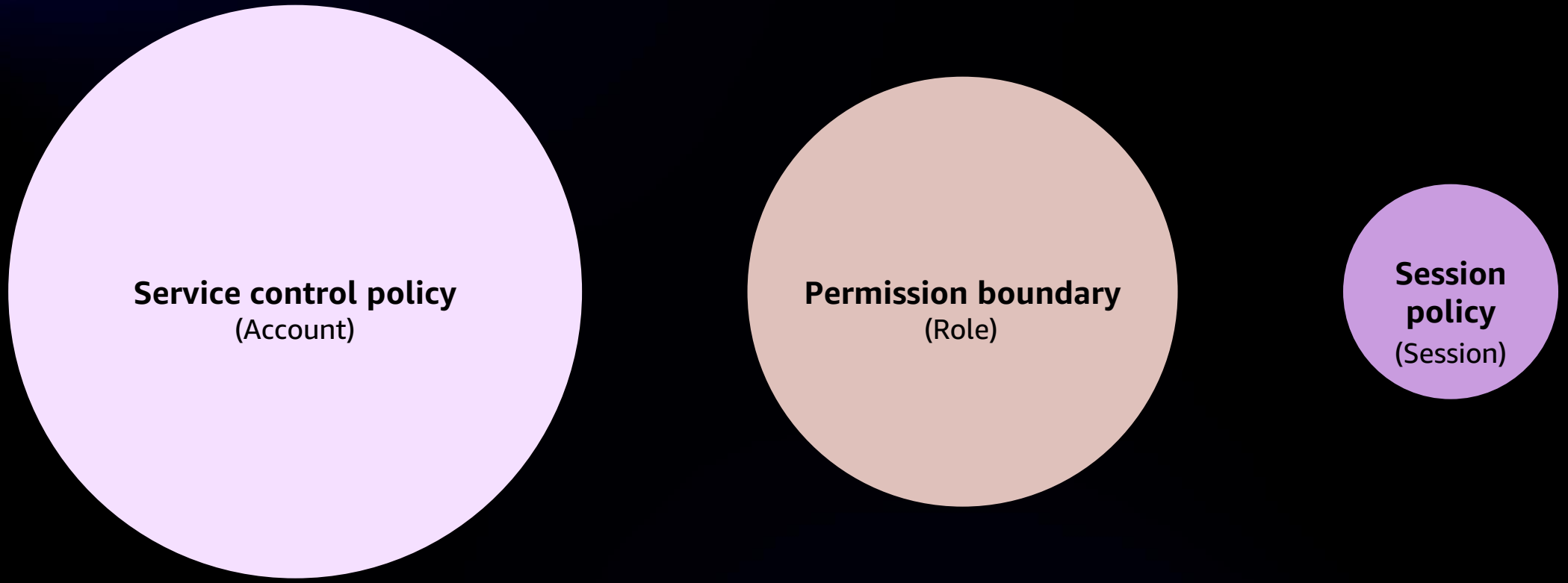
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Recommended OU structure



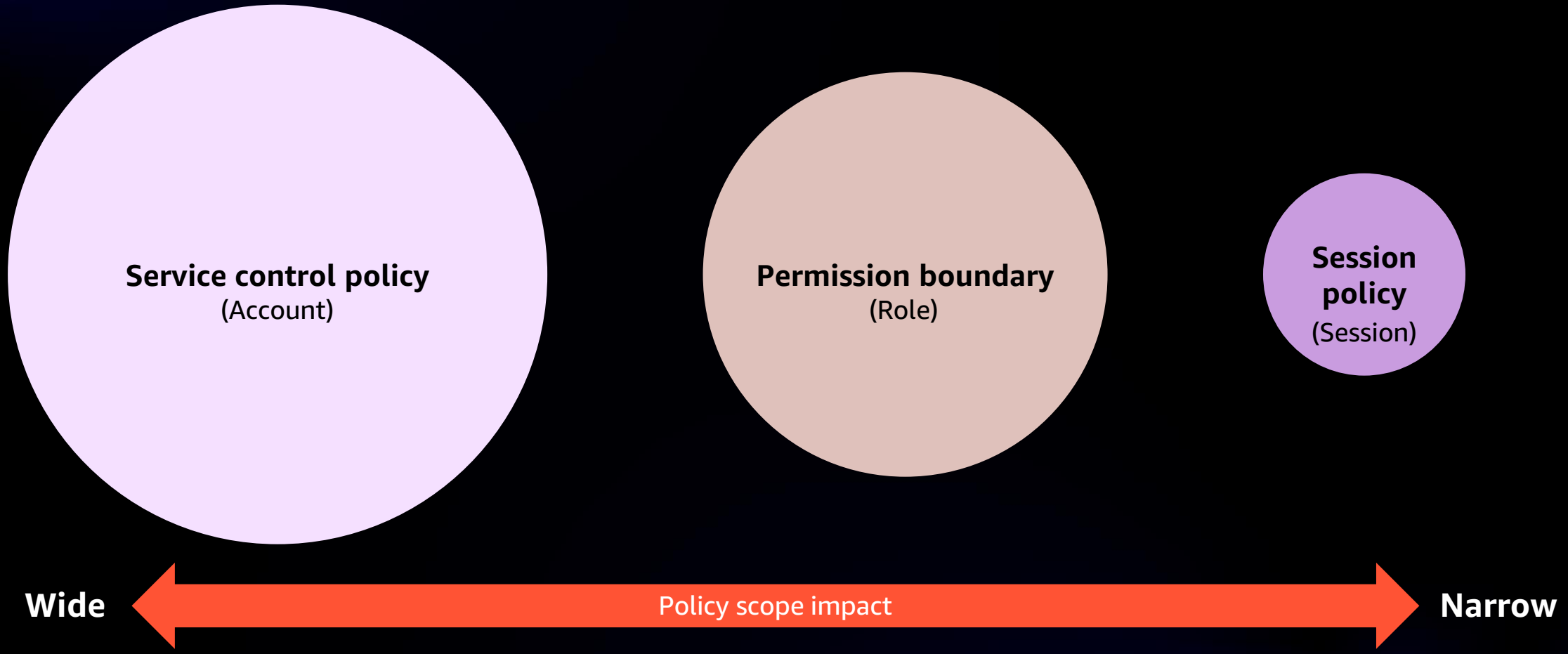
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Build guardrails to move quickly, safely



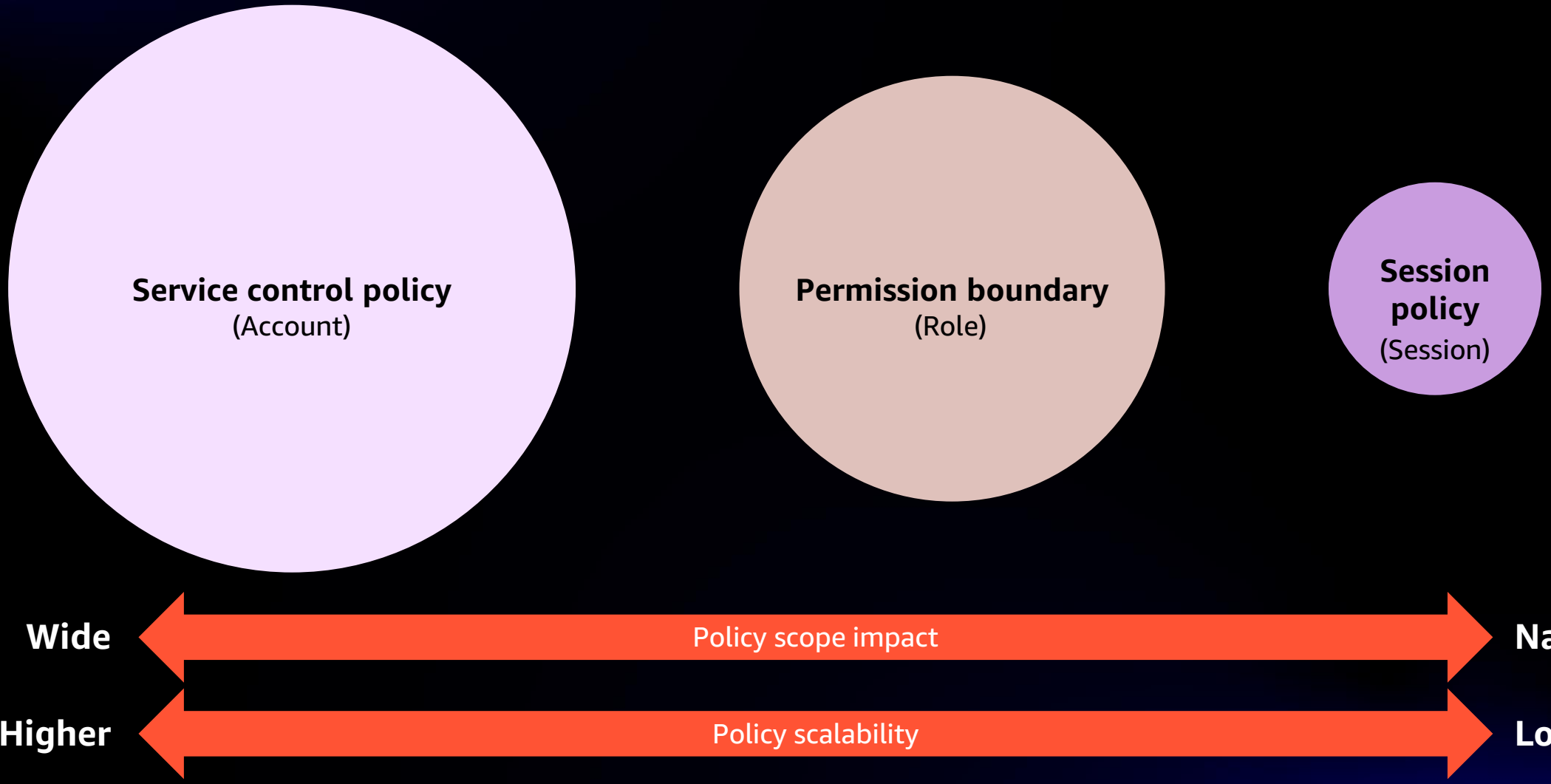
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Build guardrails to move quickly, safely



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

Build guardrails to move quickly, safely



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

Discussion

Q: How are you establishing initial sets of permissions and access for new roles/identities?

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

Discussion

Q: How are you using guardrails to enable innovation while staying within security boundaries?

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

Continuously review and right-size access

Use case	AWS service
Automate inventory and assessment of IAM roles and policies	AWS Config
Identify services/actions used to refine permissions	IAM last accessed information
Identify unused roles/users to remove	
Identify potential unintended access permissions	IAM Access Analyzer
Perform policy security checks and validations and previewing external access	
Generate IAM policies based on access activity	

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

Continuously review and right-size access

Use case	AWS service
Automate inventory and assessment of IAM roles and policies	**AWS Config**
Identify services/actions used to refine permissions	IAM last accessed information
Identify unused roles/users to remove	
Identify potential unintended access permissions	IAM Access Analyzer
Perform policy security checks and validations and previewing external access	
Generate IAM policies based on access activity	

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

Continuously review and right-size access

Use case	AWS service
Automate inventory and assessment of IAM roles and policies	AWS Config
Identify services/actions used to refine permissions	**IAM last accessed information**
Identify unused roles/users to remove	
Identify potential unintended access permissions	IAM Access Analyzer
Perform policy security checks and validations and previewing external access	
Generate IAM policies based on access activity	

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

Continuously review and right-size access

Use case	AWS service
Automate inventory and assessment of IAM roles and policies	AWS Config
Identify services/actions used to refine permissions	**IAM last accessed information**
Identify unused roles/users to remove	
Identify potential unintended access permissions	IAM Access Analyzer
Perform policy security checks and validations and previewing external access	
Generate IAM policies based on access activity	

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

Continuously review and right-size access

Use case	AWS service
Automate inventory and assessment of IAM roles and policies	AWS Config
Identify services/actions used to refine permissions	IAM last accessed information
Identify unused roles/users to remove	
Identify potential unintended access permissions	**IAM Access Analyzer**
Perform policy security checks and validations and previewing external access	
Generate IAM policies based on access activity	

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

Continuously review and right-size access

Use case	AWS service
Automate inventory and assessment of IAM roles and policies	AWS Config
Identify services/actions used to refine permissions	IAM last accessed information
Identify unused roles/users to remove	
Identify potential unintended access permissions	**IAM Access Analyzer**
Perform policy security checks and validations and previewing external access	
Generate IAM policies based on access activity	

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

Continuously review and right-size access

Use case	AWS service
Automate inventory and assessment of IAM roles and policies	AWS Config
Identify services/actions used to refine permissions	IAM last accessed information
Identify unused roles/users to remove	
Identify potential unintended access permissions	**IAM Access Analyzer**
Perform policy security checks and validations and previewing external access	
Generate IAM policies based on access activity	

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

Discussion

Q: How are you tuning your access permissions for existing roles/identities?

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

Wrapping up

- Mental model for thinking about your least privilege journey
- Establishing security foundations for isolation and guardrails
- Techniques for continuously tuning access permissions

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

Thank you!

Cassia Martin

ccsm@amazon.com



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