

The background features a dark navy blue field with abstract, overlapping shapes in vibrant magenta and deep red. Two thin, light blue lines intersect diagonally across the upper right portion of the image. The text is positioned on the left side.

AWS re:Invent

DECEMBER 2 – 6, 2024 | LAS VEGAS, NV

SEC337-R

Scaling IAM: Advanced administration and delegation patterns

Swara Gandhi

Sr. Identity Solutions Architect
AWS

Jeremy Ware

Sr. Security Solutions Architect
AWS



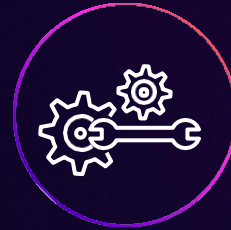
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda



Challenges

- Scaling challenges
- Managing access
- Securing identities



Solution

- Delegation strategies
- Centralizing and automating IAM management
- Implementing permissions guardrails
- Permissions management tools



Assessing your IAM posture

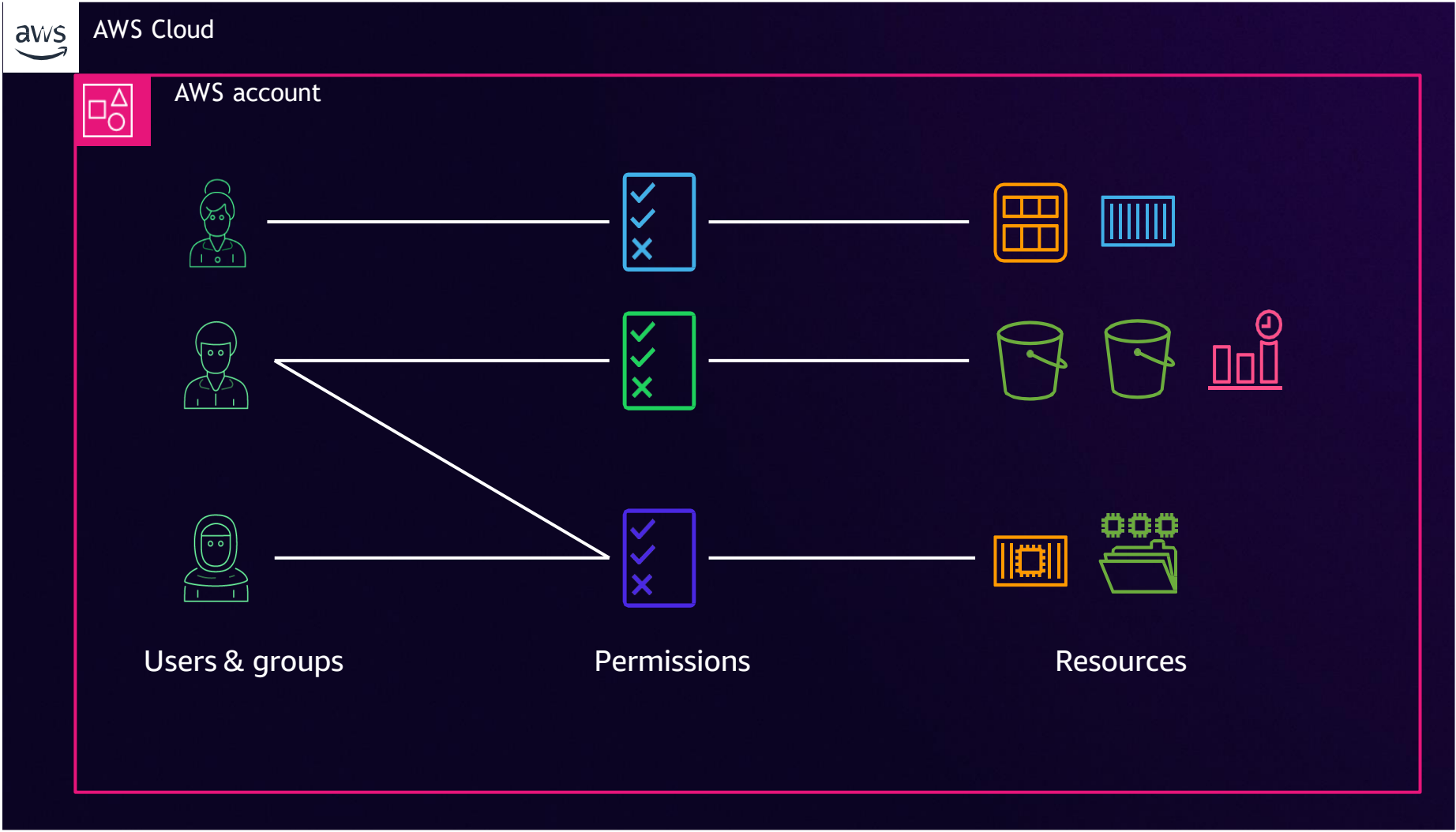
- Where are you starting from?
- Tying it all together



Wrap up

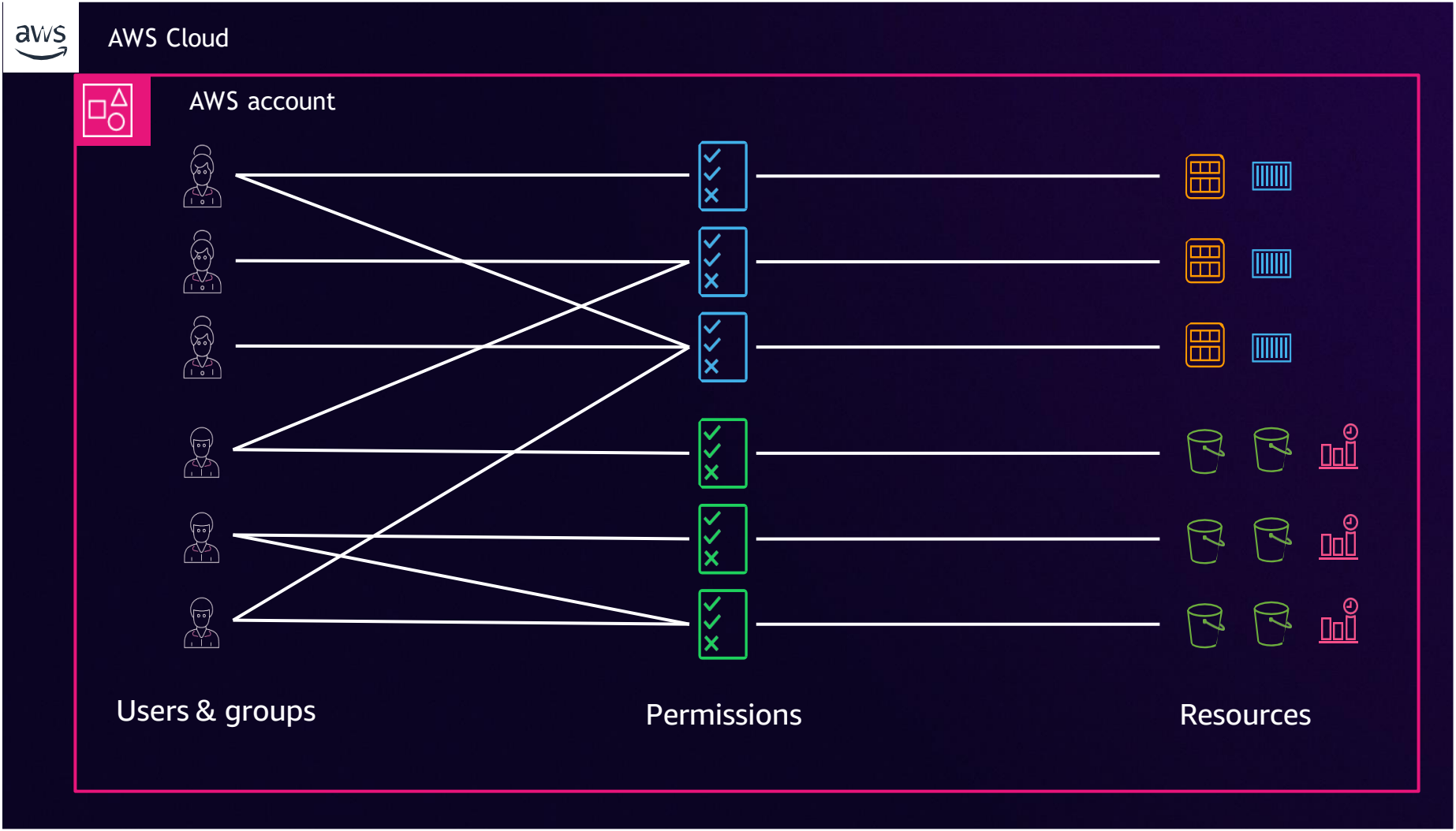
- Discussion
- Further reading material

Permissions to resources in one account



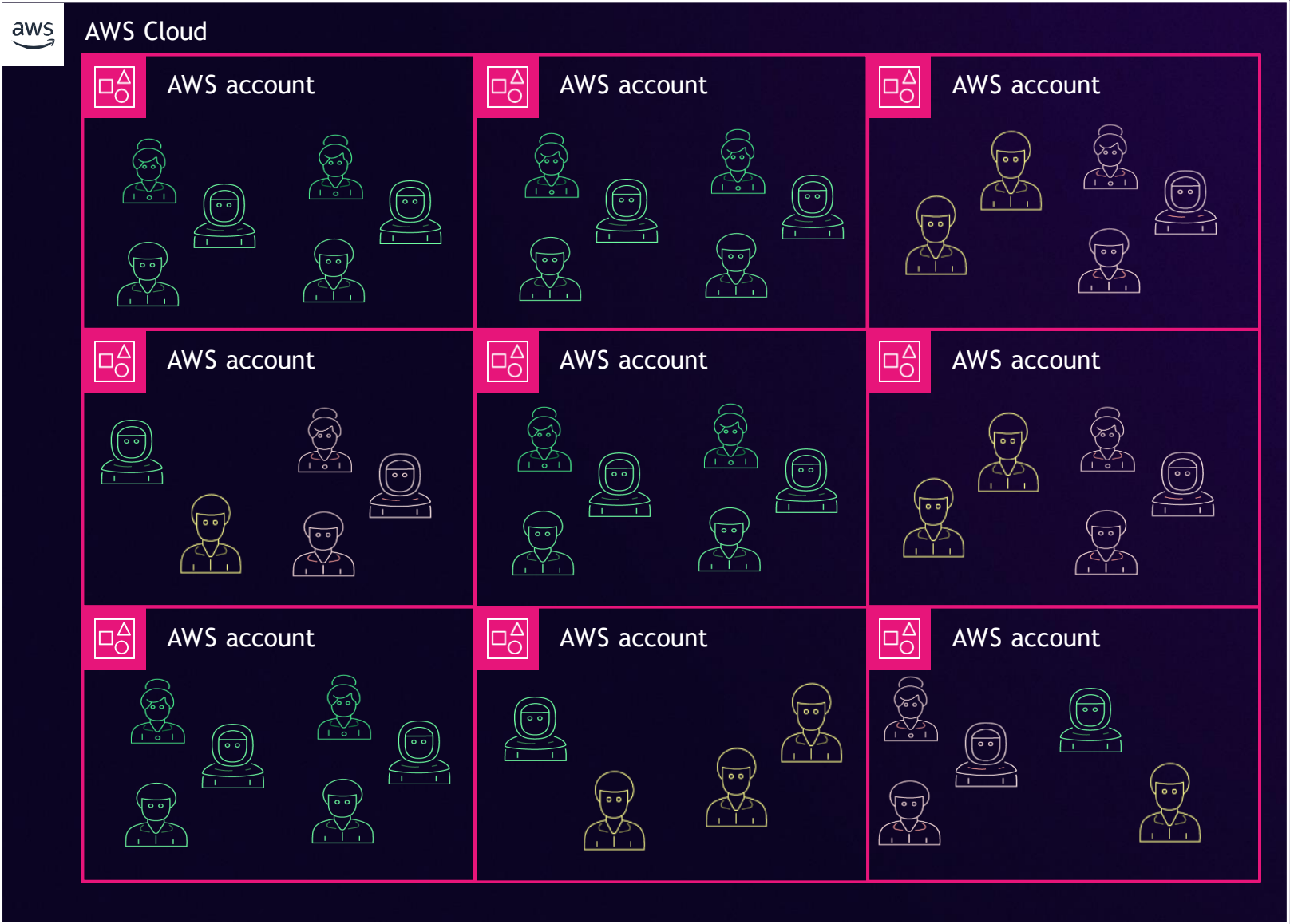
Central Security Team

More realistic scenario



Central Security Team

A common customer scenario



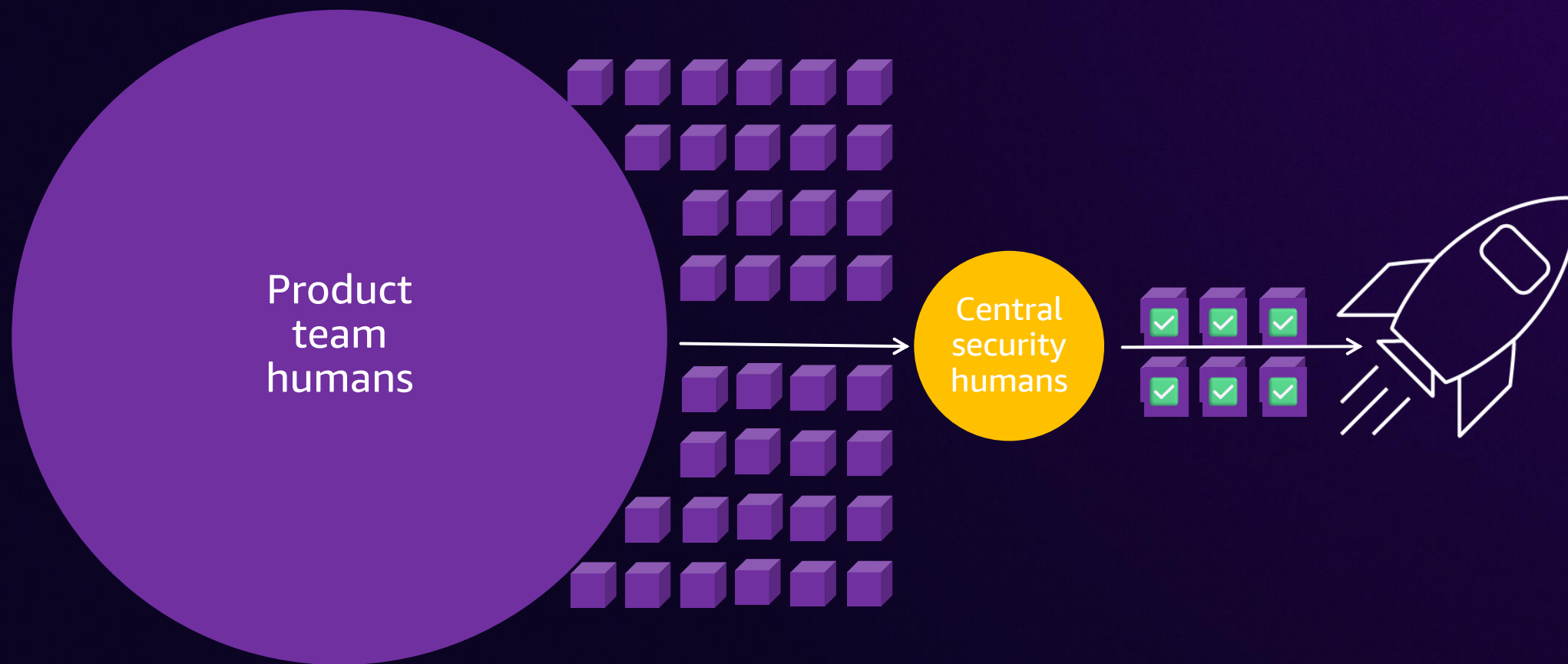
Central team managing access



Everyone needs to ask me for IAM permissions

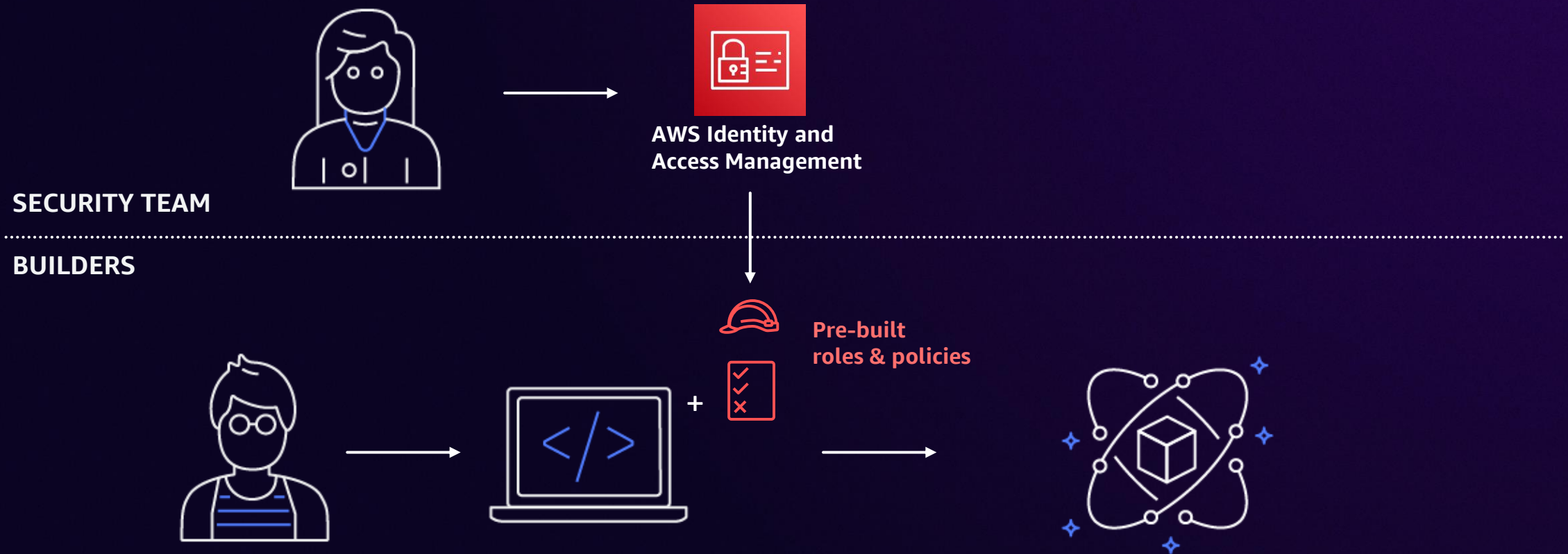


Central team becomes a bottleneck



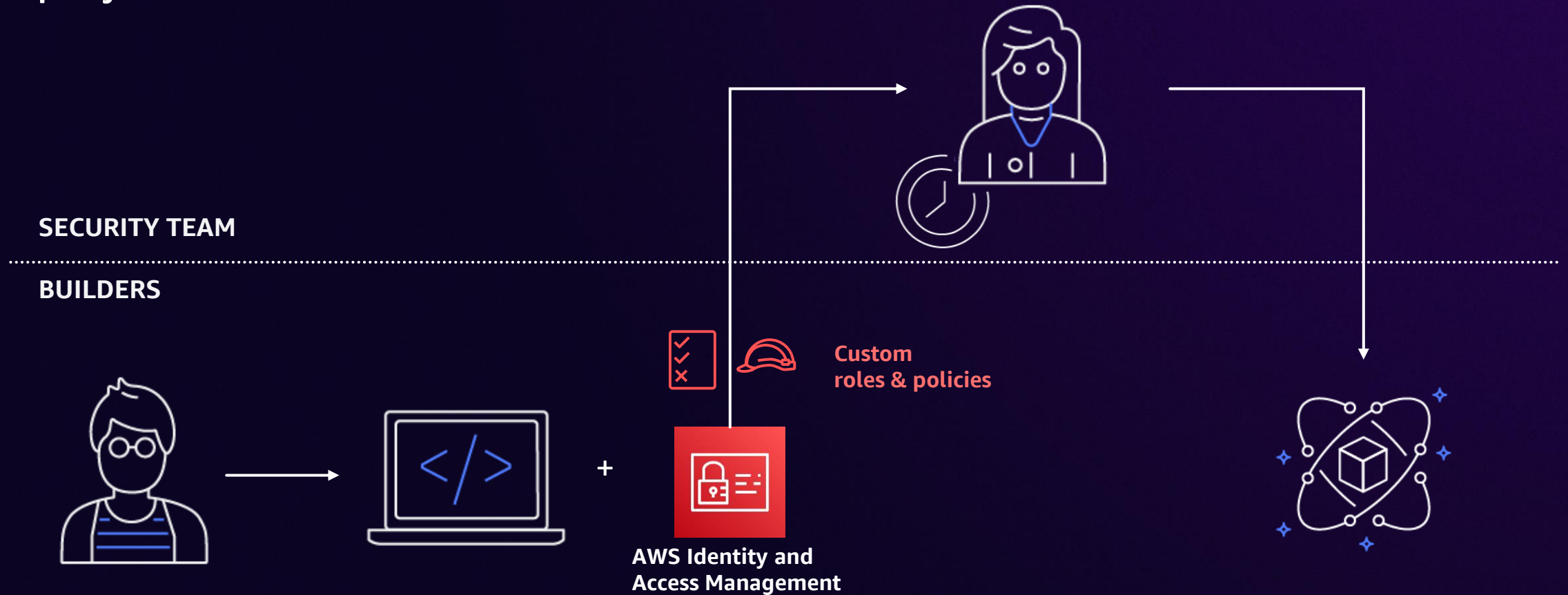
Centralized IAM Approach

Security team creates and deploys all IAM roles/policies; builders have no access to IAM

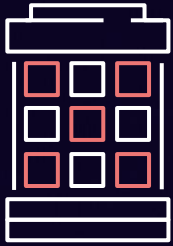


Gated IAM Approach

Builders codify the IAM roles and policies, but need Security to approve and deploy



Challenges



Lack of visibility

Who has access to what?

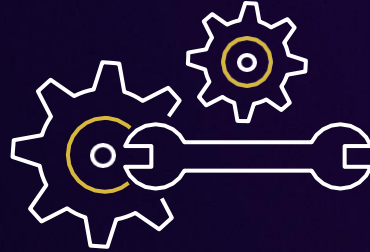
Identifying users with privileged actions



Scaling

Bottle-necked central team

Provisioning



Decentralized setup

Managing access

Operations



Security

Lack of governance and controls



User Experience

Agility to move quickly

Freedom for builders

Solution



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Path to self-service



Productized approach to IAM

Centralize IAM Management with IdC

- Centrally manage ~~users & groups~~
- Centrally manage permissions

Automate

- Machine identity management
- Resource creation
- Account delivery with defined feature set

Delegation

- Role vending
- Policy validation

Security controls

- Permissions guardrails
- Base set of policies

Delegation

What do we mean by delegation?

Builder Bob



I need a role to run
my application!

Security Susan

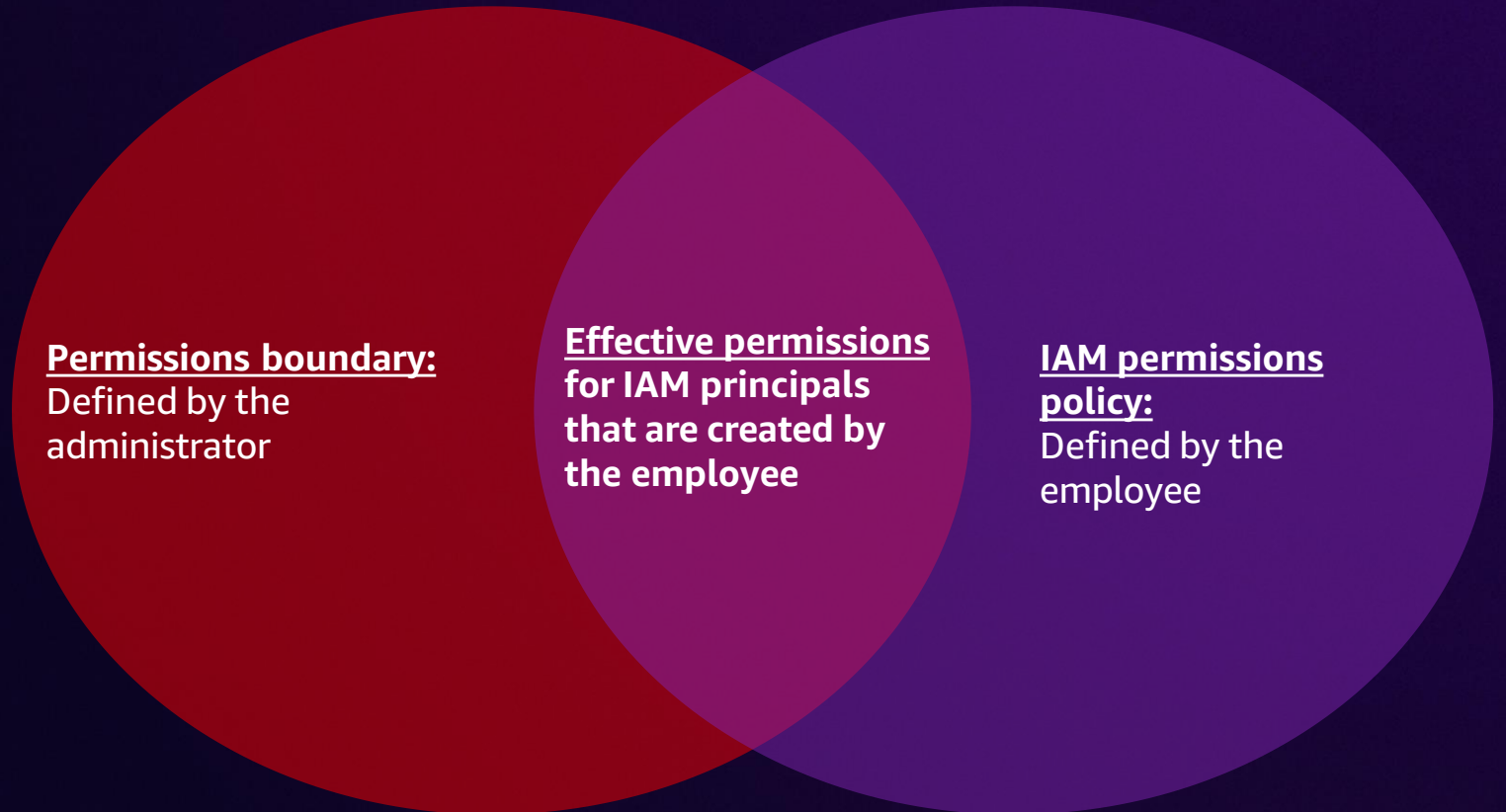


Create it yourself!

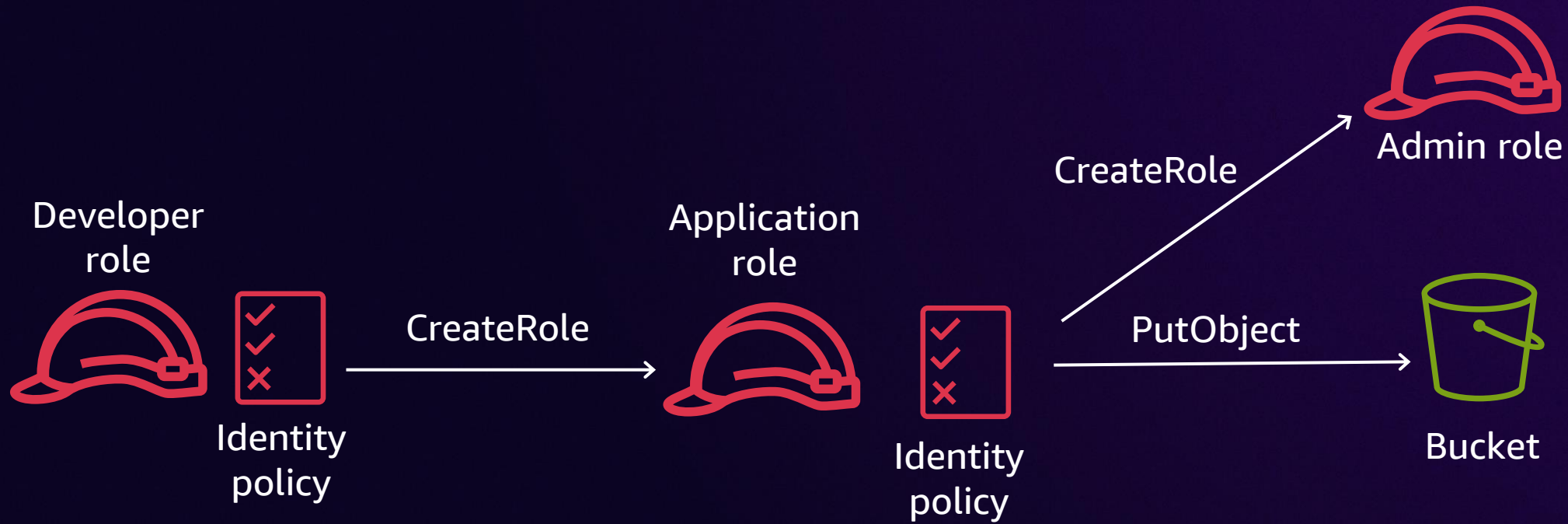
Permissions boundaries

Apply permissions boundaries to the **IAM roles created by developers**, rather than to the developers themselves

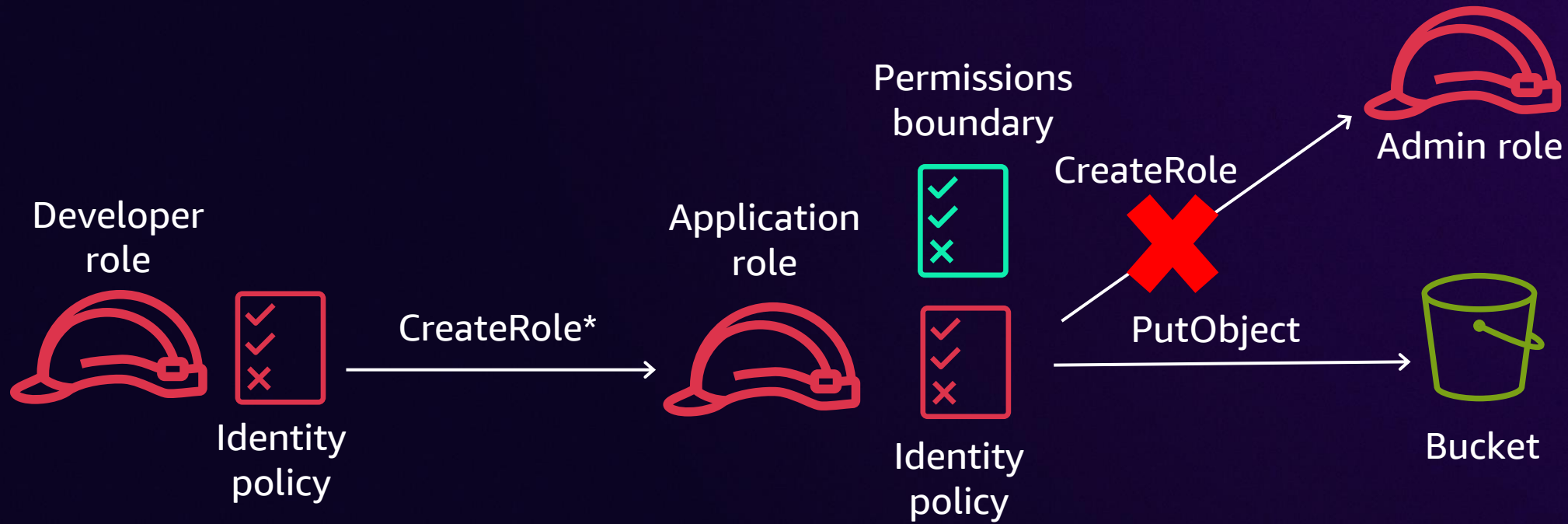
Group your **permissions boundaries into categories** that fit the scope of similar application functions (such as system automation and analytics)



Without permissions boundaries



With permissions boundaries



* But only if a permissions boundary is attached

Permissions boundary walkthrough

Account Admin Step 1: Create the permissions boundary only allowing certain AWS services (CompanyBoundary)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ServiceBoundaries",
      "Effect": "Allow",
      "Action": [
        "s3:*",
        "cloudwatch:*",
        "ec2:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Permissions boundary walkthrough

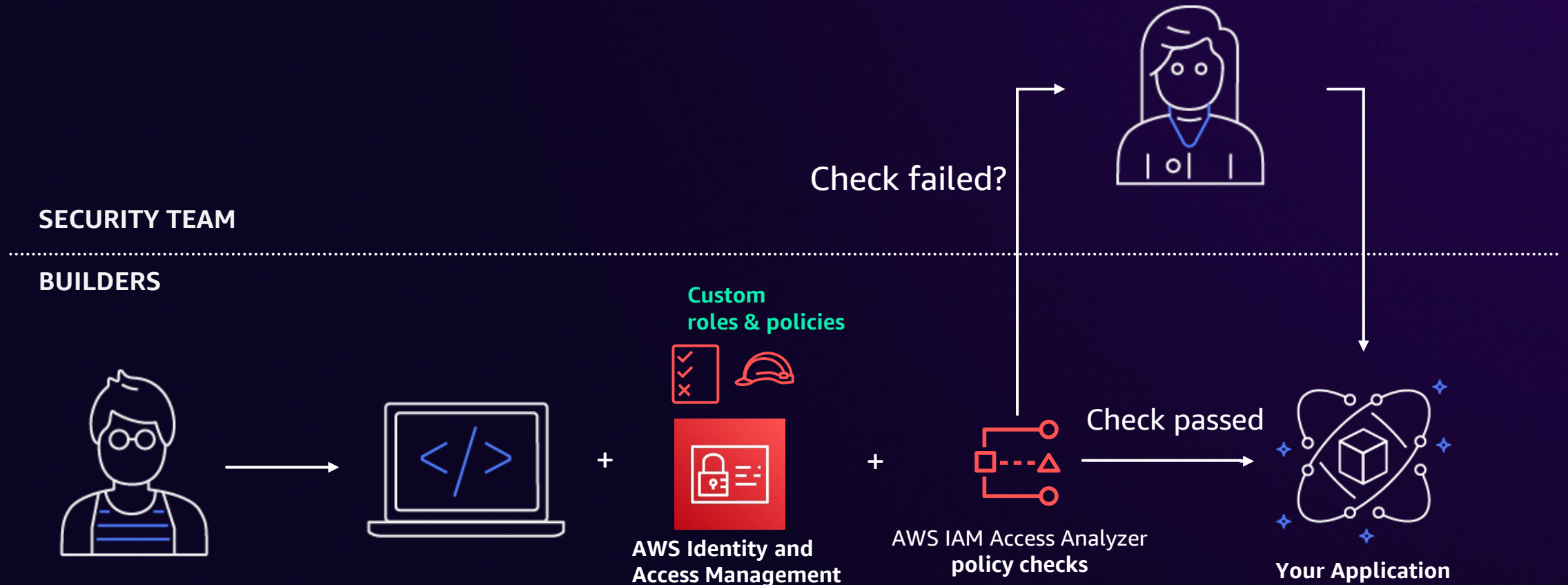
Account Admin Step 2: Allow role creation, but only if CompanyBoundary is specified. Attach permission policy to delegated IAM Admin principal

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SetPermissionsBoundary",
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PermissionsBoundary": "arn:aws:iam::123456789012:policy/CompanyBoundaries"
        }
      }
    },
    {
      "Sid": "CreateAndEditPermissionsPolicy",
      "Effect": "Deny",
      "Action": [
        "iam:CreatePolicy",
        "iam:CreatePolicyVersion",
        "iam>DeletePolicyVersion"
      ],
      "Resource": "arn:aws:iam::123456789012:policy/AppPolicies/*"
    }
  ]
}
```

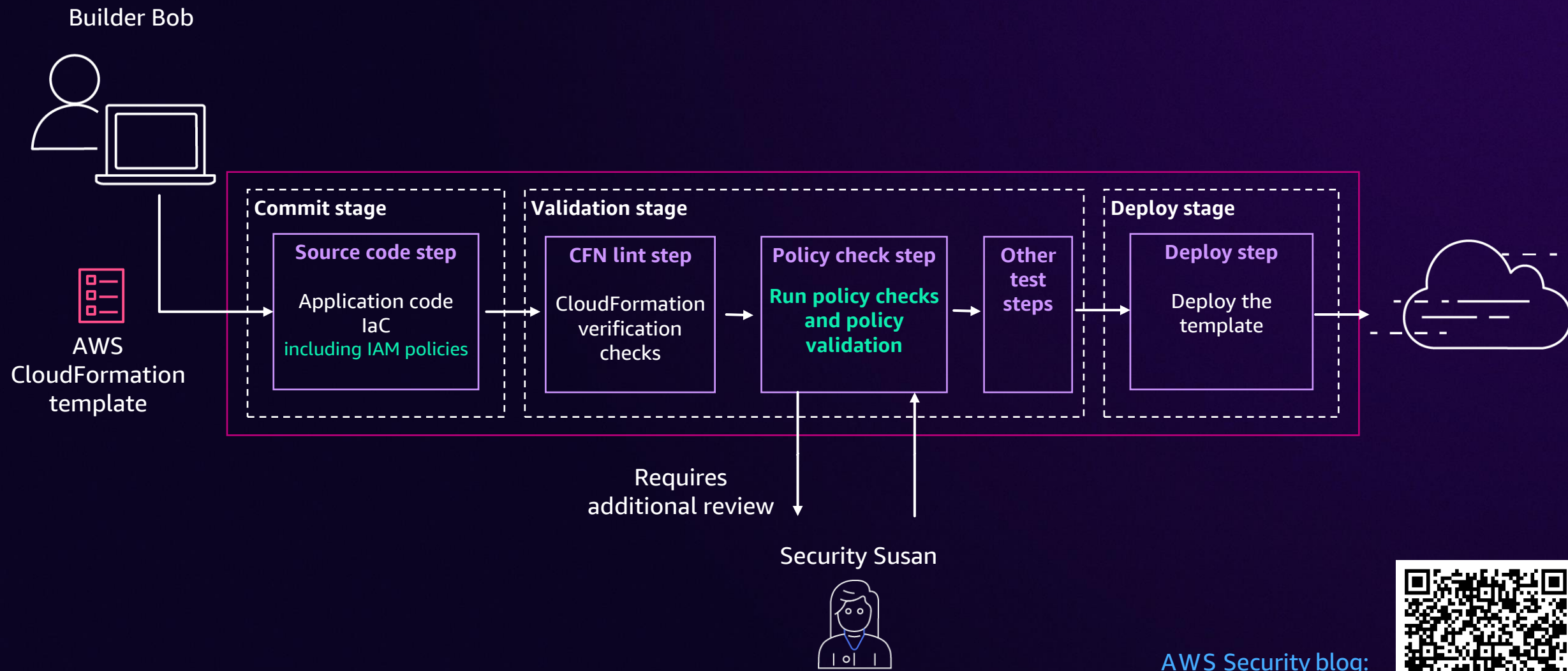


Delegated approach

Builders codify the IAM roles/policies. Security team uses automated policy validation to perform the security checks that were previously manual



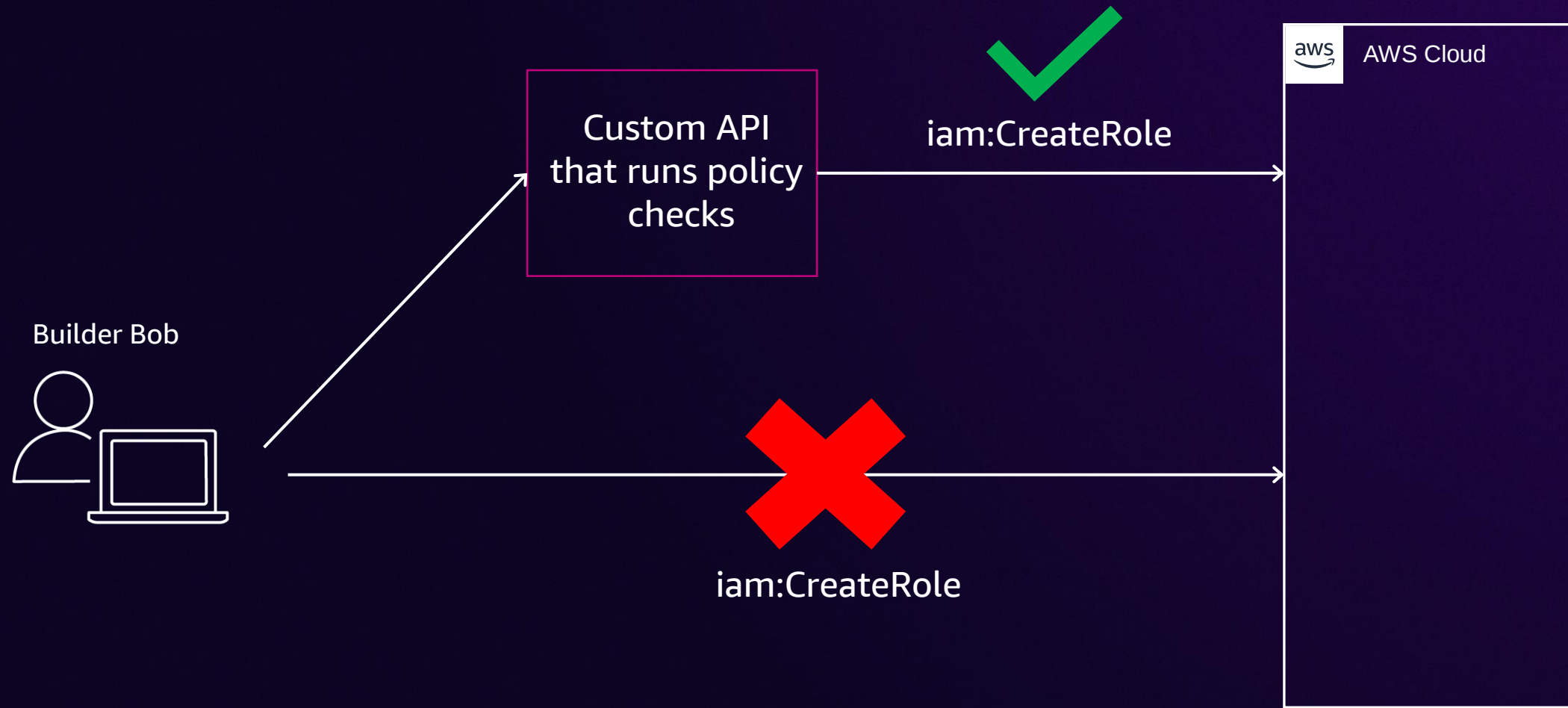
CI/CD pattern



[AWS Security blog:](#)
Validate IAM policies in CloudFormation
templates using IAM Access Analyzer



API to create roles pattern



CI/CD vs API

Controls in CI/CD Pipeline

Pros:

- AWS offered tooling
- Get started quickly
- Backwards compatible with existing tooling

Cons:

- Difficult to make consistent at scale
- Difficult to ensure all pipelines are covered

API to create roles

Pros:

- Limit scope for CreateRole* permission (API)
- Centralized evaluation
- Flexibility on responding to failed policy checks/validations via API response

Cons:

- Custom built

While maintaining security controls

AWS IAM policy types

Impact radius
Intent
Guardrail vs. Grant

Organization/OU/Account level

RCPs

Guardrail

SCPs

Guardrail

Declarative Policies

Guardrail

Resource level

Resource-based policies

VPC endpoint policies

Guardrail

IAM principal level

Identity-based policies

Permission boundaries

Guardrail

Session policies

AWS IAM policy types

Impact radius

Intent

Guardrail vs. Grant

Should be used by Central team



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Organization/OU/Account level

RCPs

For central control

SCPs

For central control

Declarative Policies

For central control

Resource level

Resource-based policies

VPC endpoint policies

IAM principal level

Identity-based policies

Permission boundaries

For delegation

Session policies

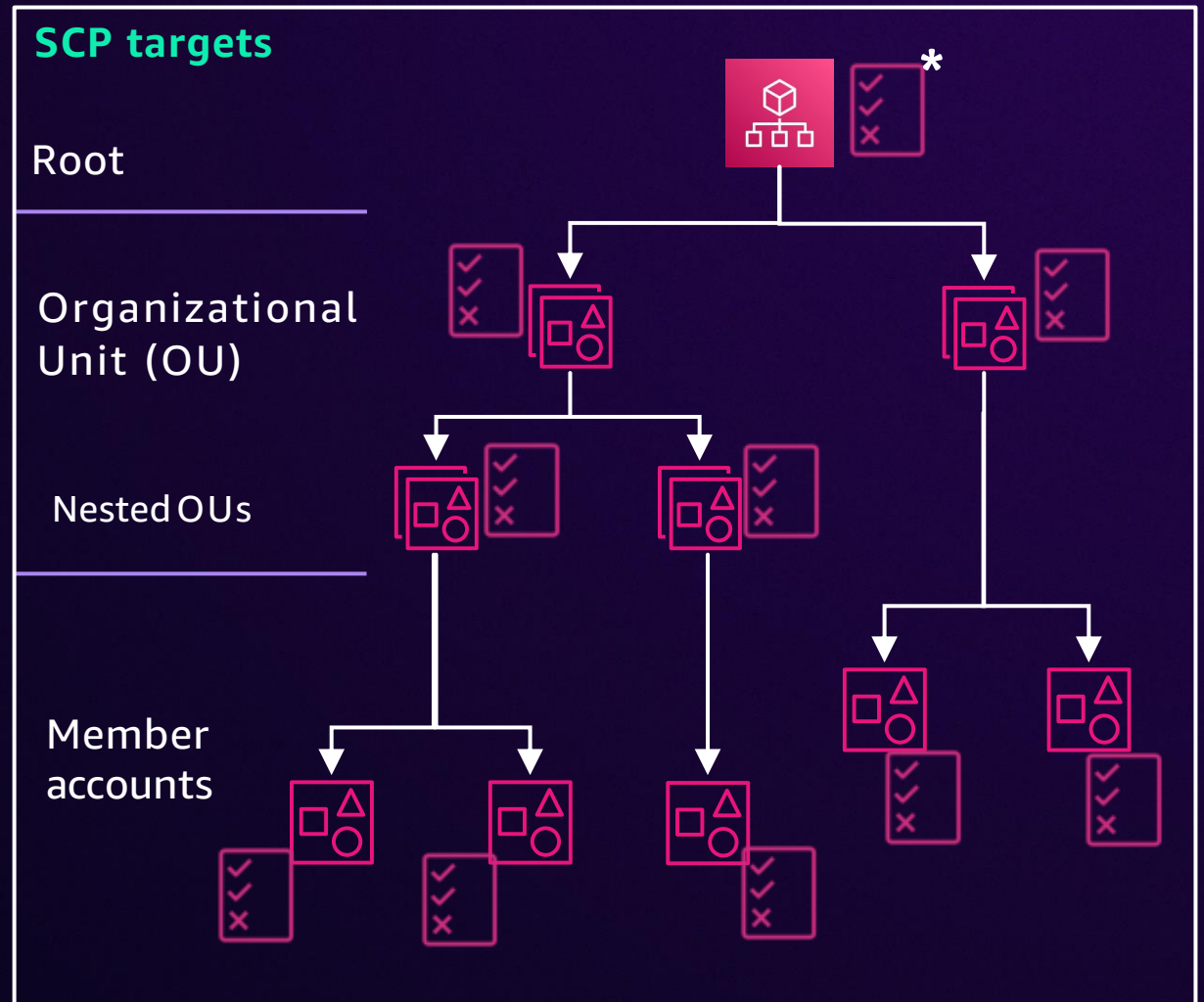
Service control policies (SCPs)

CENTRALLY CREATE AND APPLY PREVENTIVE GUARDRAILS FOR YOUR ORGANIZATION

Define maximum available permissions of the IAM principals for all accounts in your organization

Can be applied to organization root, OUs, or member accounts

Supports delegated administration



Resource control policies (RCPs)

CENTRALLY CREATE AND APPLY PREVENTIVE GUARDRAILS FOR YOUR ORGANIZATION

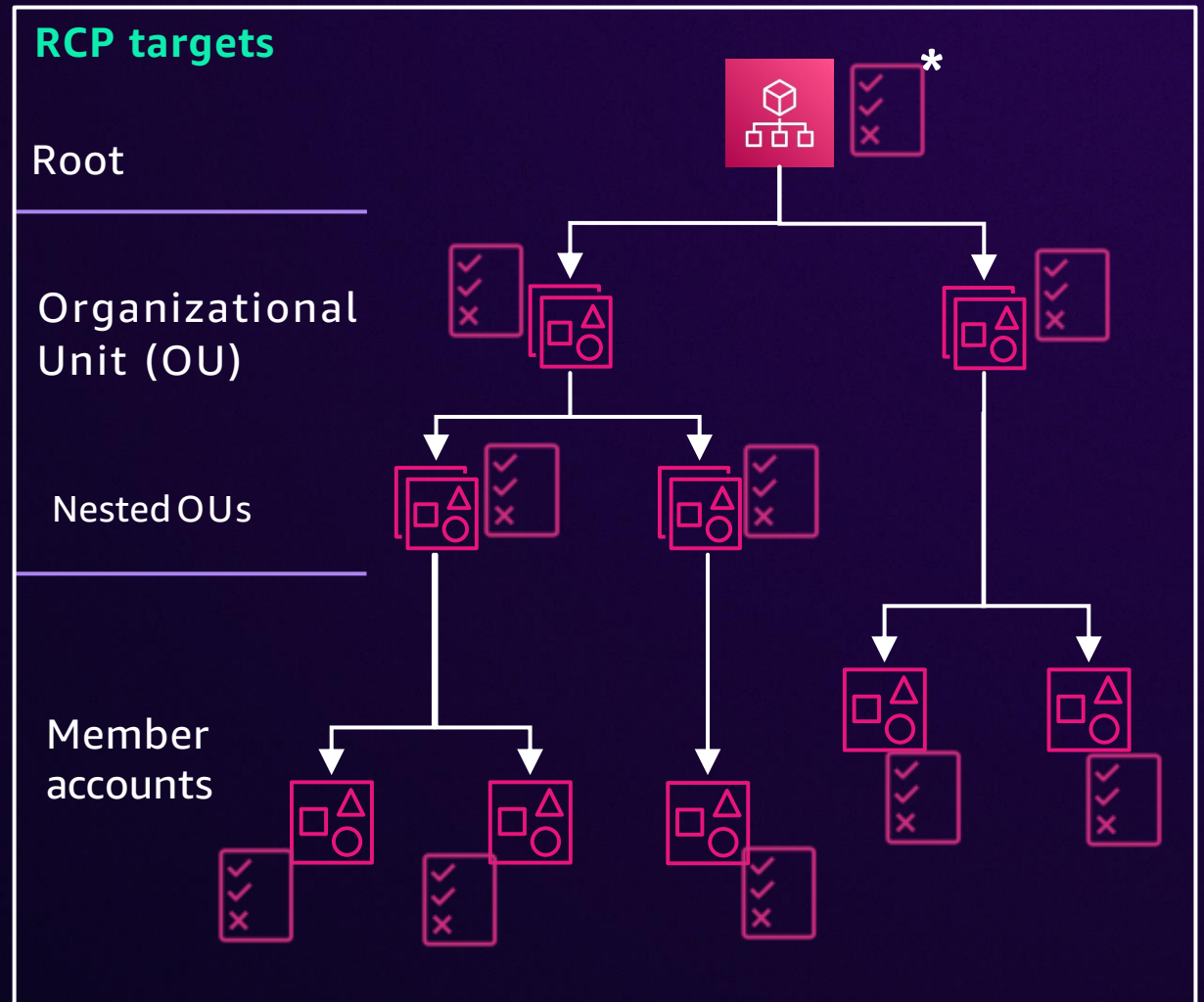
Define uniform access controls on resources across your AWS environment

Can be applied to organization root, OUs, or member accounts

Supports delegated administration



RCPs are only supported with few services today



Declarative policies for EC2

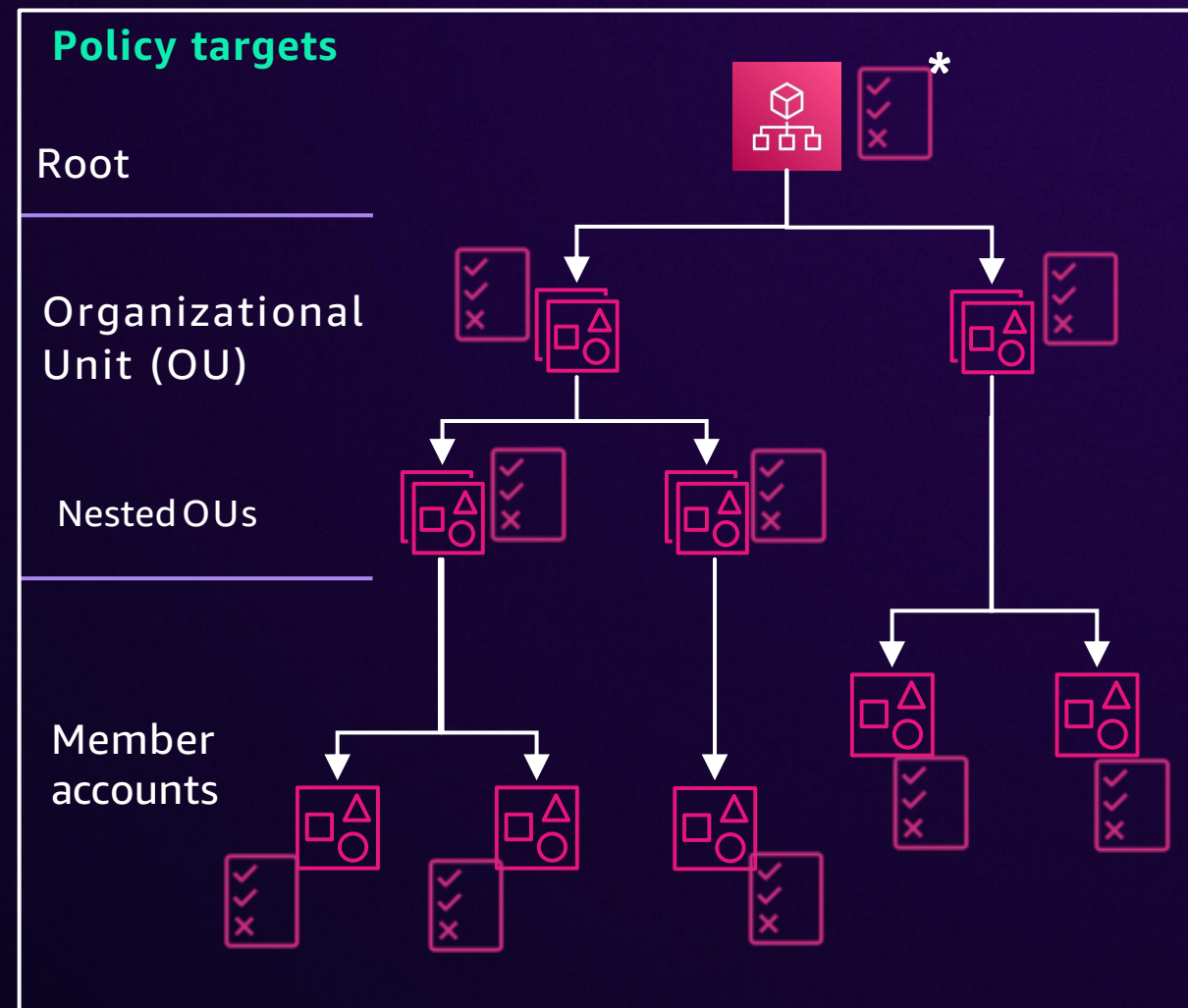
DECLARE AND ENFORCE DESIRED CONFIGURATION FOR A GIVEN AWS SERVICE

Once attached, the configuration is always maintained when EC2 adds new features or APIs

Can be applied to organization root, OUs, or member accounts

Examples:

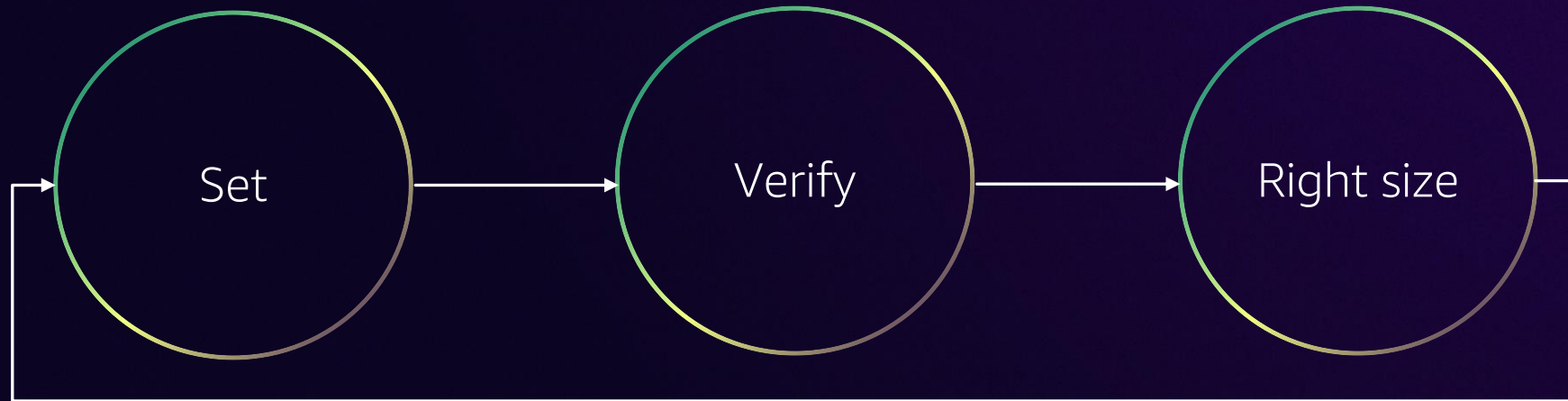
- EC2 image block public access
- Snapshot block public access
- VPC block public access



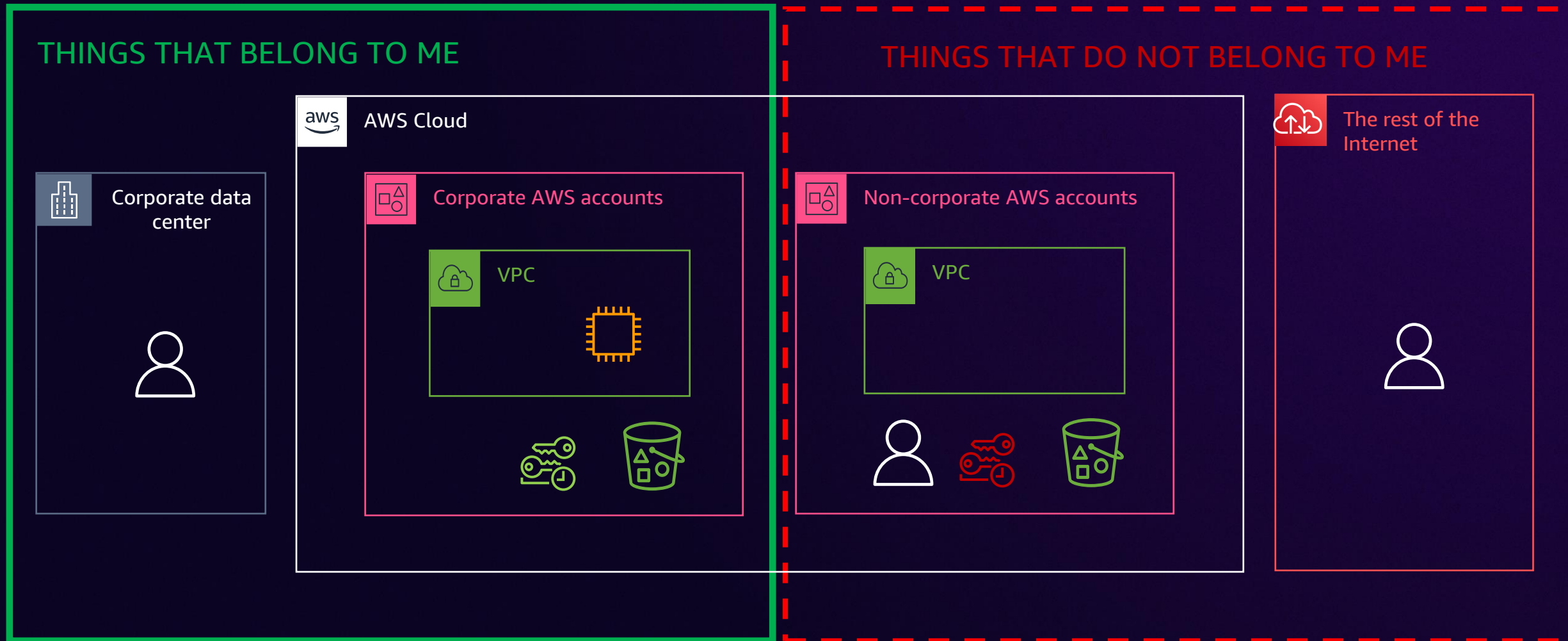
Access management strategy

Data perimeter
Coarse-grained controls

Least privilege
Fine-grained permissions



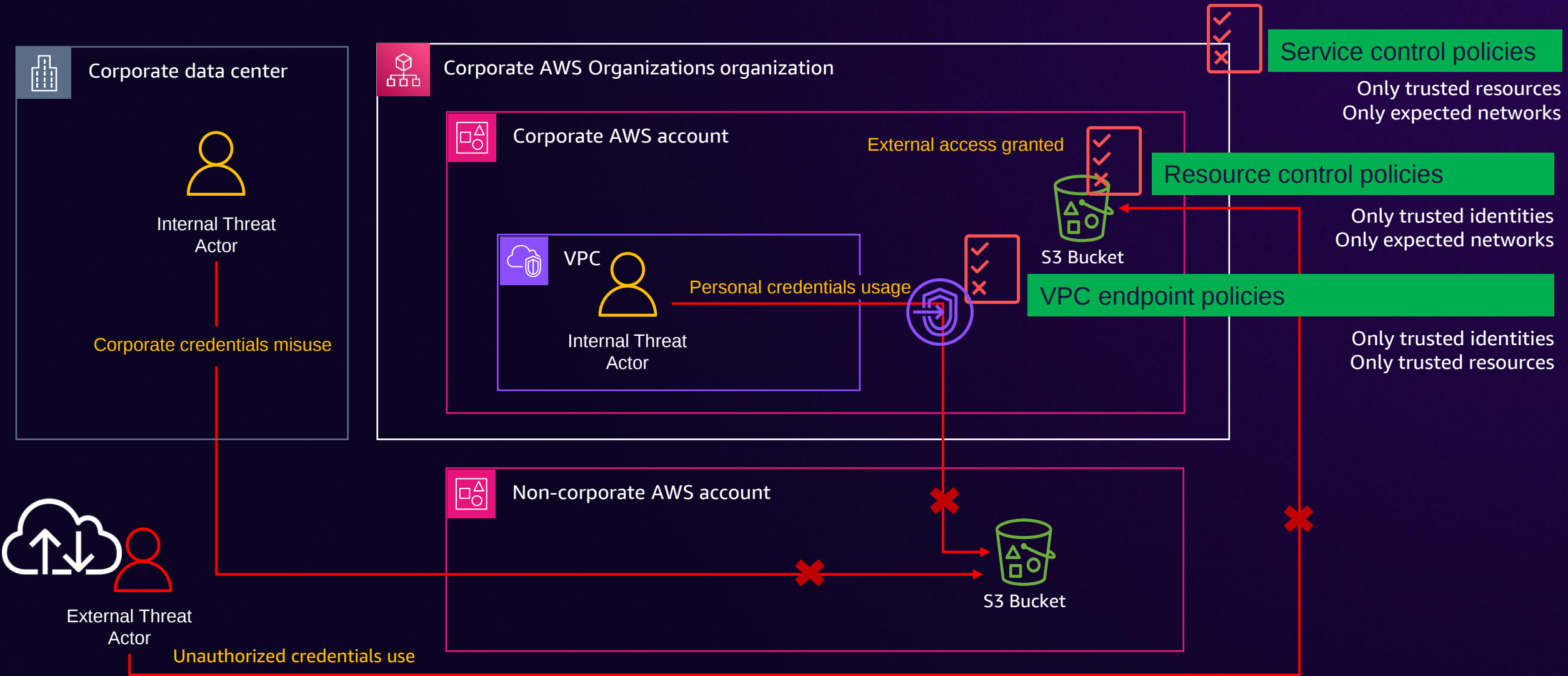
What is a data perimeter?



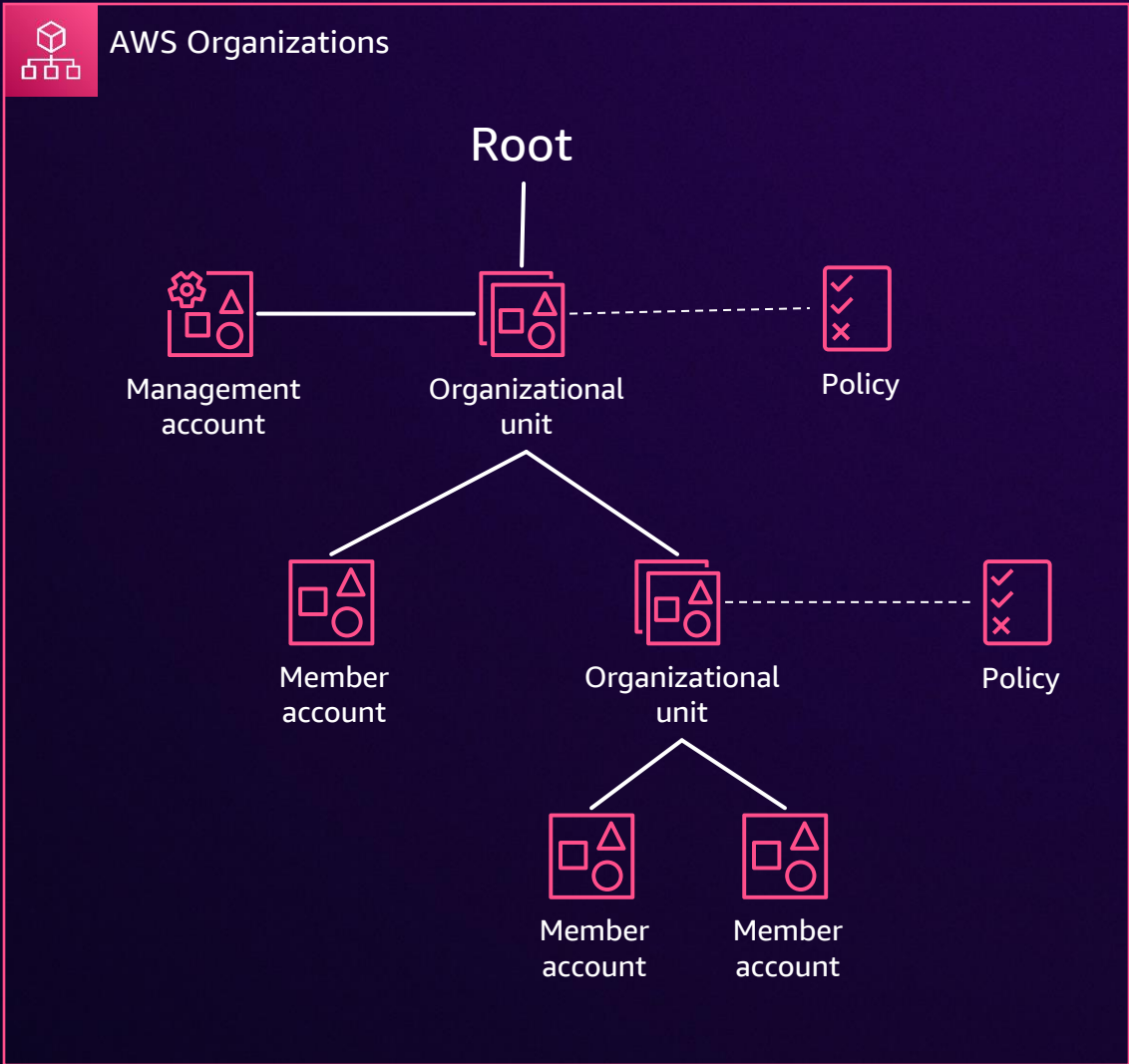
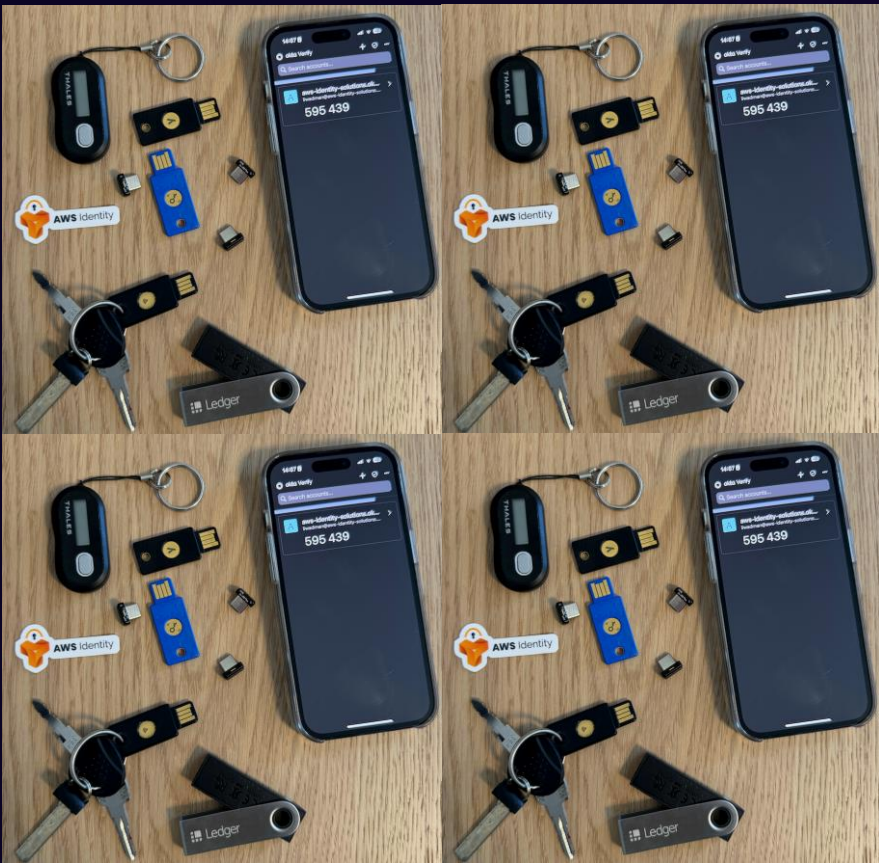
Data perimeter controls

Perimeter	Intent / Control Objective	Applied on	Using	Primary IAM feature
Identity	Only trusted identities can access my resources	Resources	RCP	aws:PrincipalOrgID aws:PrincipalIsAWSService
	Only trusted identities are allowed from my network	Network	VPC endpoint policy	aws:PrincipalOrgID aws:PrincipalIsAWSService
Resource	My identities can access only trusted resources	Identities	SCP	aws:ResourceOrgID
	Only trusted resources can be accessed from my network	Network	VPC endpoint policy	aws:ResourceOrgID
Network	My identities can access resources only from expected networks	Identities	SCP	aws:SourceIp aws:SourceVpc/aws:SourceVpce aws:ViaAWSService
	My resources can only be accessed from expected networks	Resources	RCP	aws:SourceIp aws:SourceVpc/aws:SourceVpce aws:ViaAWSService aws:PrincipalIsAWSService

Mitigating security risks with data perimeter controls



Managing root users in AWS Organizations



Central management for root access

PROVIDES CUSTOMERS WITH A SIMPLIFIED WAY TO MANAGE, SECURE, AND CONTROL HIGHLY PRIVILEGED ACCESS TO THEIR AWS MEMBER ACCOUNTS

Simplify audit and compliance

Easily manage root credentials

Tightly scoped privileged access

[IAM](#) > Root access management

Root access management [Info](#)

Centralize root access for your member accounts [Info](#)

You can delete root credentials for member accounts and perform privileged actions from the management or delegated account. [Learn more about centralizing root access](#)



Improved security

You can delete root user credentials for member accounts and eliminate the need for managing long term root user credentials and associated multi-factor authentication (MFA) devices.



Better compliance

You can prove root credential non existence for your audit and compliance needs, proving your root user is secured across your member accounts.



Total control

You will have the control to block or allow root password recovery for your password-less member accounts.

Enable

Access Analysis with IAM Access Analyzer

EXTERNAL AND UNUSED ACCESS ANALYSIS

The unused access analyzing tool can be **enabled** in your account or with Organizations

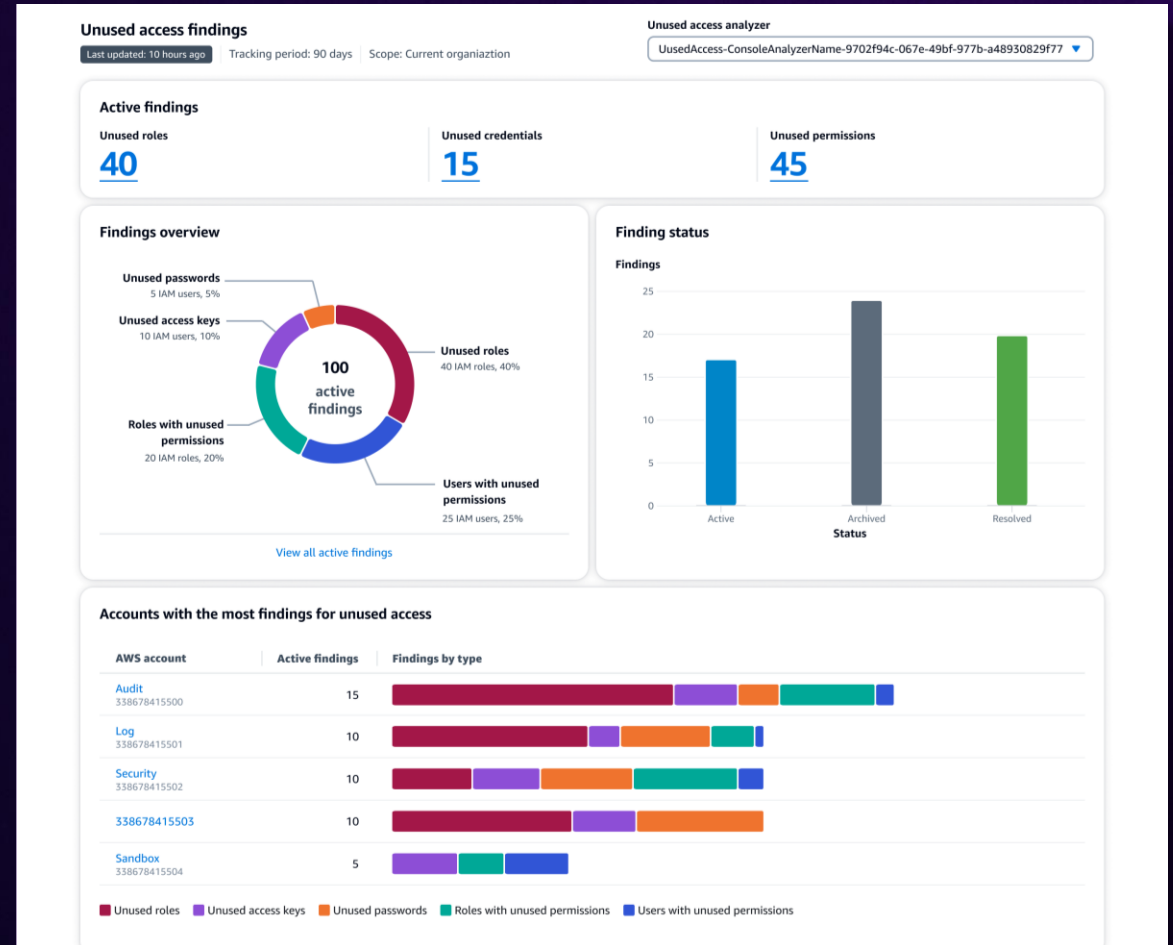
Continually **monitors and reviews** access activity across all IAM roles and users

Identifies unused **roles**, unused user **credentials**, and unused **permissions**

Generates findings for you to review over-permissive IAM roles and users

Review dashboard to identify accounts that need attention

Customers use action last accessed by individual roles for no additional charge; optionally, customers use this **paid offering** for continual monitoring and centralized review capabilities



Unused access analysis – Analyzer scoping



Specific accounts – using
account ID



Specific IAM principals – using
principal tags

How does it help?

- ☐ Focus unused access analysis on important AWS accounts and IAM principals
- ☐ “Prioritized” unused access findings based on specific accounts and principals
- ☐ Optimize the cost for unused access analysis

Assessing your IAM posture



Assess your AWS IAM posture

The screenshot shows the AWS IAM Dashboard. On the left is a navigation sidebar with sections: Identity and Access Management (IAM), Access management (containing User groups, Users, Roles, Policies, Identity providers, and Account settings), Access reports (containing Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity, Service control policies, and Resource control policies), and Related consoles (containing IAM Identity Center and AWS Organizations). The main content area is titled 'IAM Dashboard' and shows 'IAM resources' for the current AWS Account. A yellow warning banner states: 'You are approaching your quota of available IAM resources. Learn more'. Below this is a table of resources:

User groups	Users	Roles	Policies	Identity providers
1	4583	4898	70	1

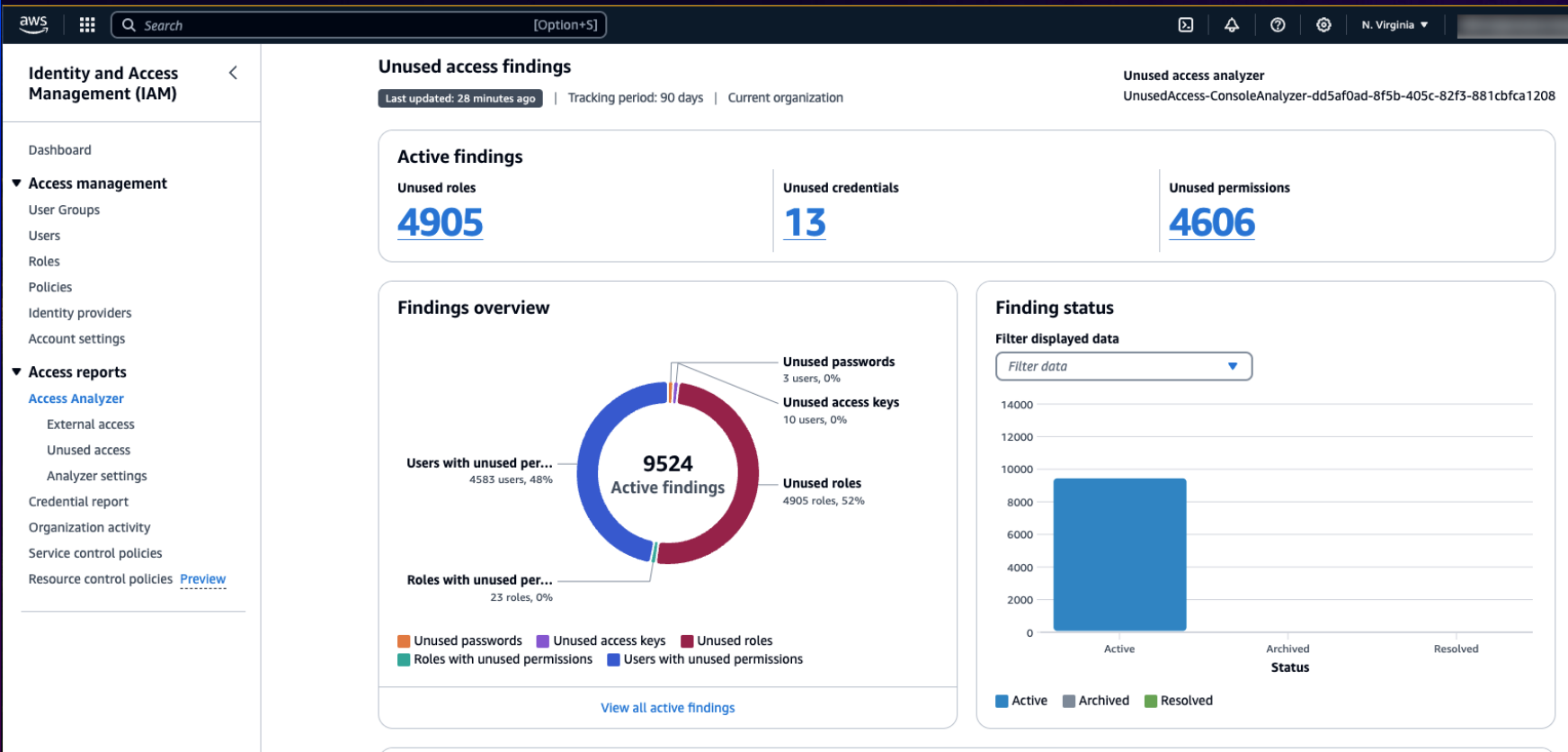
Below the table is a 'What's new' section with updates for features in IAM, including links to learn more about policy checks, unused access recommendations, bulk policy migration, and certificate attribute mapping.

Not good!

A lot of IAM users

Long-lived credentials
such as access keys

Assess your AWS IAM posture



Not good!

Overly-permissive permissions

Assess your AWS IAM posture

External access findings

Last updated: 10 hours ago

Zone of trust: Current organization

External access analyzer

ExternalAccess-ConsoleAnalyzerName-9702f94c-067e-49bf-977b-a48930829f77

Active findings ¹

Public access

10

Access outside of organization

90

Findings overview ²

Public access
10 findings, 10%



Access outside of organization
90 findings, 90%

Access outside of organization Public access

[View all active findings](#)

Primary resource types with active findings ³

Findings



Access outside of organization Public access

Not good!

External access on resources

Assess your AWS IAM posture

CloudTrail

Dashboard

Event history

Insights

Lake

- Dashboard
- Query
- Event data stores
- Integrations

Trails

Settings

Pricing

Documentation

Forums

FAQs

CloudTrail > Event history

Event history (1/5) Info

Event history shows you the last 90 days of management events.

Lookup attributes

User name

root

Filter by date and time

Event name

Event time

User name

Event source

Resource type

Resource name

☐

[ListRolePolicies](#)

September 09, 2024, 11:45:47 (UTC-04:...

root

iam.amazonaws.com

-

-

☐

[ListInstanceProfilesForRole](#)

September 09, 2024, 11:45:47 (UTC-04:...

root

iam.amazonaws.com

-

-

☐

[ListInstanceProfilesForRole](#)

September 09, 2024, 11:45:47 (UTC-04:...

root

iam.amazonaws.com

-

-

☐

[ListRolePolicies](#)

September 09, 2024, 11:45:46 (UTC-04:...

root

iam.amazonaws.com

-

-

☐

[ListAttachedRolePolicies](#)

September 09, 2024, 11:45:46 (UTC-04:...

root

iam.amazonaws.com

-

-

☐

[DeleteRole](#)

September 09, 2024, 11:45:46 (UTC-04:...

root

iam.amazonaws.com

AWS::IAM::Role

1130

☐

[ListRolePolicies](#)

September 09, 2024, 11:45:45 (UTC-04:...

root

iam.amazonaws.com

-

-

☐

[DeleteRolePolicy](#)

September 09, 2024, 11:45:45 (UTC-04:...

root

iam.amazonaws.com

AWS::IAM::Policy, AWS::...

ModivCareTest, 113

☐

[GetRole](#)

September 09, 2024, 11:45:32 (UTC-04:...

root

iam.amazonaws.com

-

-

☐

[GetRole](#)

September 09, 2024, 11:45:32 (UTC-04:...

root

iam.amazonaws.com

-

-

☐

[GetRole](#)

September 09, 2024, 11:45:32 (UTC-04:...

root

iam.amazonaws.com

-

-

☐

[GetRole](#)

September 09, 2024, 11:45:32 (UTC-04:...

root

iam.amazonaws.com

-

-

1 / 5 events selected

Not good!

Root user usage



Assess your AWS IAM posture

Not good!

Access keys are not rotated

No MFA

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

▼ Access reports

- Access Analyzer
 - External access
 - Unused access
 - Analyzer settings
- Credential report
- Organization activity
- Service control policies
- Resource control policies [New](#)

Related consoles

[IAM Identity Center](#)

[IAM](#) > [Users](#) > 1318

1318 [Info](#) [Delete](#)

Summary

ARN arn:aws:iam::[redacted]:user/1318	Console access Disabled	Access key 1 [redacted] - Active Used 108 days ago. 108 days old.
Created June 09, 2022, 00:27 (UTC-04:00)	Last console sign-in -	Access key 2 Create access key

Permissions | Groups | Tags | **Security credentials** | Access Advisor

Console sign-in [Enable console access](#)

Console sign-in link https://[redacted].signin.aws.amazon.com/console	Console password Not enabled
--	---------------------------------

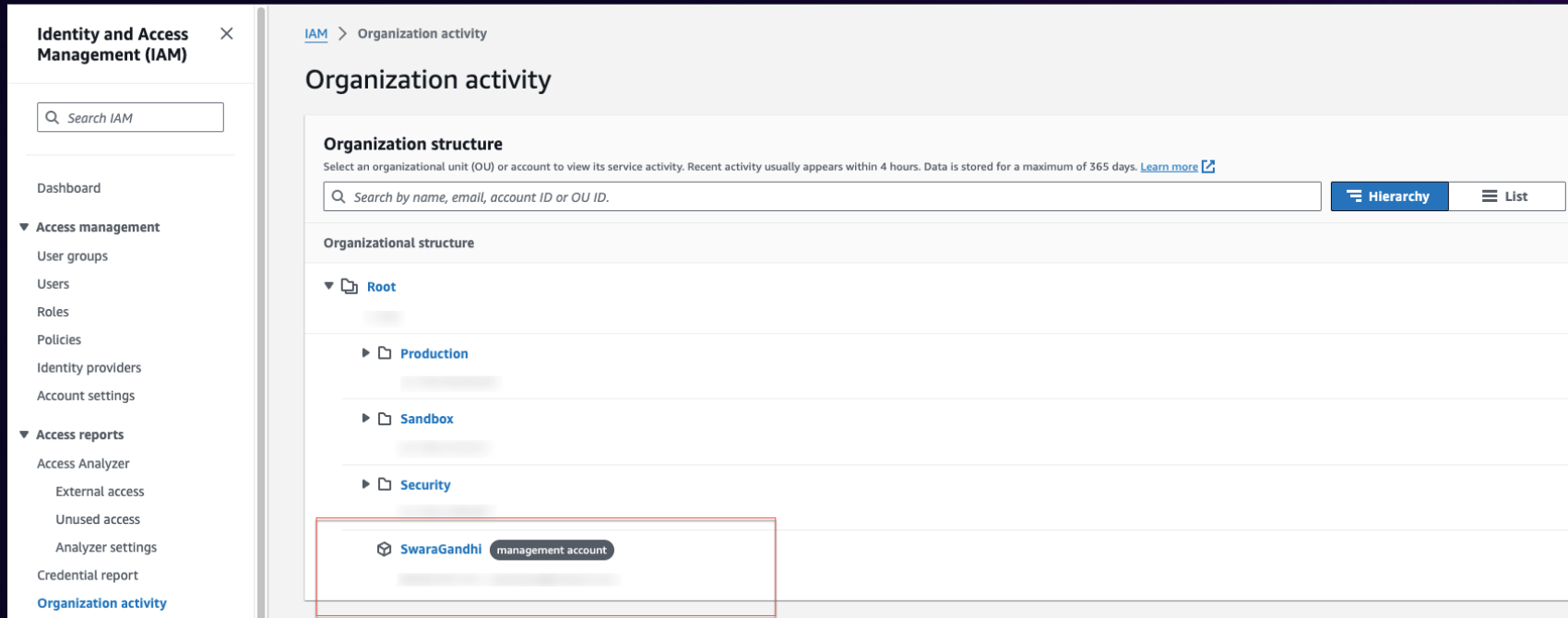
Multi-factor authentication (MFA) (0) [Remove](#) [Resync](#) [Assign MFA device](#)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

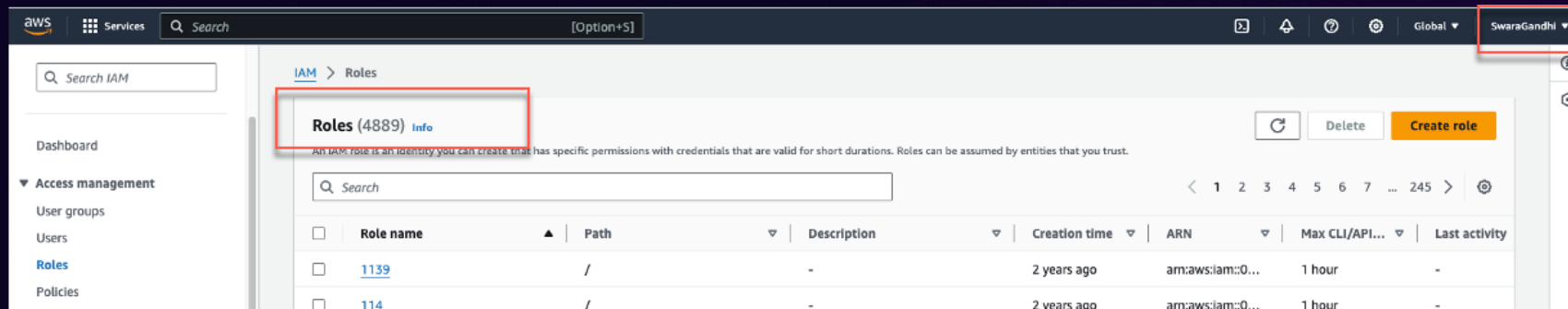
Type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment			

[Assign MFA device](#)

Assess your AWS IAM posture



The screenshot shows the AWS IAM console's 'Organization activity' page. The left sidebar contains navigation links for 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings), 'Access reports' (Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity), and 'Organization activity'. The main content area is titled 'Organization activity' and includes a search bar 'Search IAM'. Below this, the 'Organization structure' section is visible, showing a tree view of organizational units (OUs) and accounts. The tree includes 'Root', 'Production', 'Sandbox', and 'Security'. A red box highlights the 'SwaraGandhi' management account at the bottom of the tree.



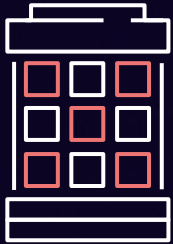
The screenshot shows the AWS IAM console's 'Roles' page. The left sidebar is the same as the previous screenshot. The main content area is titled 'Roles (4889)' and includes a search bar 'Search IAM'. Below this, a table lists roles. A red box highlights the 'Roles (4889)' header. Another red box highlights the 'SwaraGandhi' account name in the top right corner of the console. The table has columns: Role name, Path, Description, Creation time, ARN, Max CLI/API..., and Last activity. The first two rows are visible:

Role name	Path	Description	Creation time	ARN	Max CLI/API...	Last activity
1139	/	-	2 years ago	arn:aws:iam::0...	1 hour	-
114	/	-	2 years ago	arn:aws:iam::0...	1 hour	-

Not good!

Multiple IAM resources in
AWS Management
account

Elements of scaling



Visibility

IAM Access Analyzer

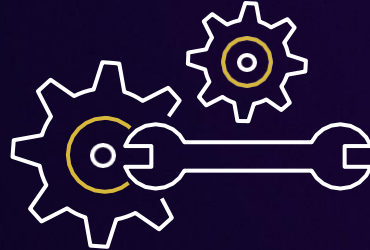
AWS Security Hub



Scaling

Automation

Delegate



Centralization

AWS IAM Identity
center

Policy deployment
pipeline



Security

Data perimeter
controls

Proactive controls
embedded in CI/CD



Defined Processes

Ownership

Feedback Loop

Just in time access

Resources

Validate IAM policies in
CloudFormation
templates using IAM
Access Analyzer



AWS CloudFormation
policy validator



AWS IAM Access
Analyzer custom policy
check samples



Data Perimeters
landing page



Thank you!

Swara Gandhi

 [linkedin.com/in/swaragandhi](https://www.linkedin.com/in/swaragandhi)

 ganswara@amazon.com

Jeremy Ware

 [linkedin.com/in/jeremyware104/](https://www.linkedin.com/in/jeremyware104/)

 jmware@amazon.com



Please complete the session survey in the mobile app