AWS re:Inforce

JUNE 10 – 12, 2024 | PHILADELPHIA, PA

IAM202

Refine unused access confidently with IAM Access Analyzer

Nini Ren

(He/Him)
Senior Product Manager – AWS Identity
AWS

Florian Holzhauer

(He/Him)
Senior Software Development Manager – AWS Identity
AWS

The next hour

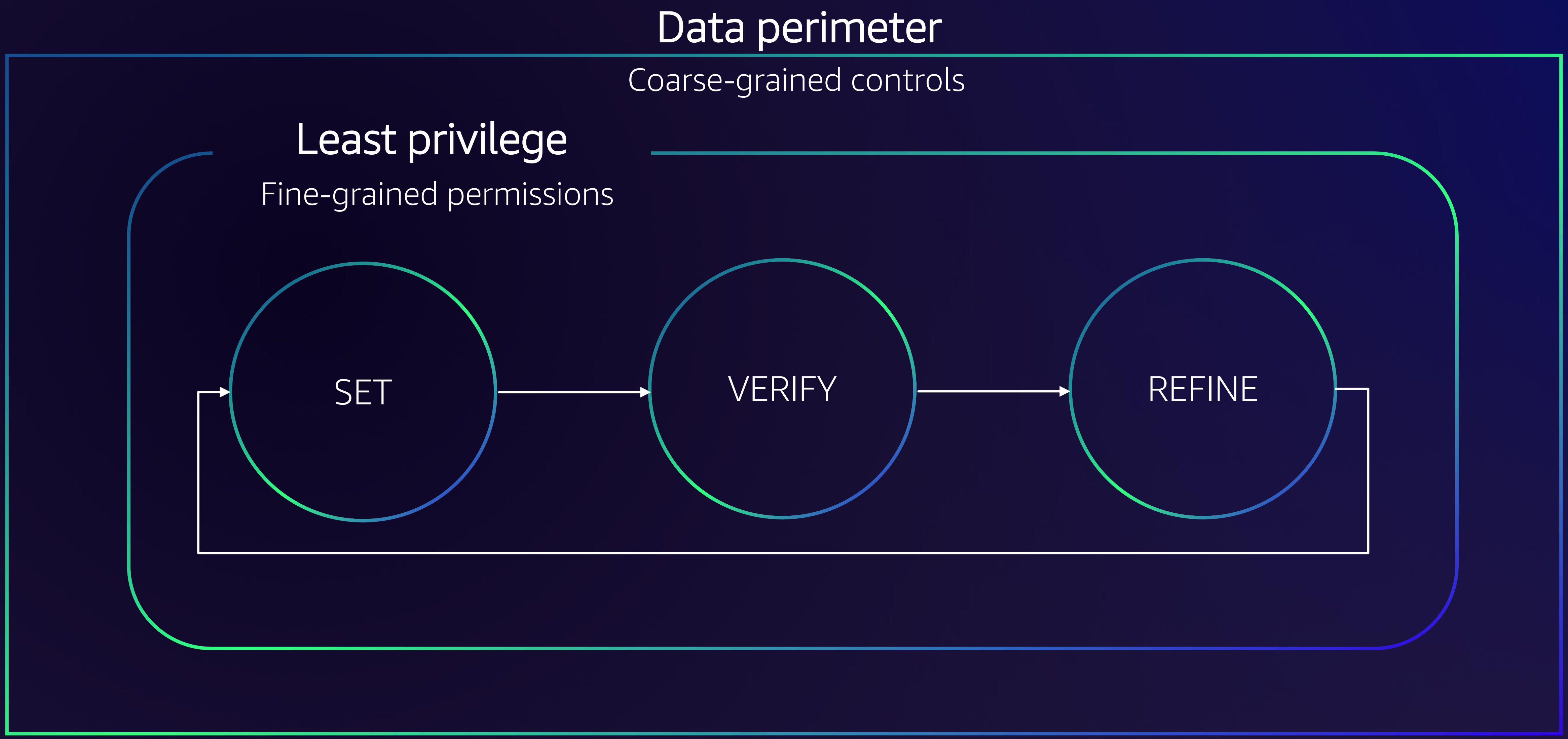
Least privilege – Who's responsible

IAM Access Analyzer – Least privilege simplified

New features for central security teams – live demo!

New features for developers – live demo!

Access controls for your AWS estate



Customer personas

Central security team

Set your security standards and set up your developers for success to build

Developer team

Provision and manage infrastructure for your applications with fine-grained permissions

Your role in central security

Your goal: Set up builders for success to build and adhere to your security standards

Security standards

Develop preventive guardrails to ensure that builders adhere to your organization's security standards

IAM configurations

Inspect permissions and notify teams to refine access

Central security team

Data perimeters

Establish controls to ensure only your trusted identities are accessing trusted resources from expected networks

Tools

Let teams access and use services, tools, and solutions to build on AWS

Your role in central security

Your goal: Set up builders for success to build and adhere to your security standards

Security standards

Develop preventive guardrails to ensure that builders adhere to your organization's security standards

IAM configurations

Inspect permissions and notify teams to refine access

Central security team

Data perimeters

Establish controls to ensure only your trusted identities are accessing trusted resources from expected networks

Tools

Let teams access and use services, tools, and solutions to build on AWS

Your role as a developer

Your goal: Provision and manage infrastructure for your applications with fine-grained permissions

Tools

Explore and determine services you need for your applications

Security best practices

Adhere to security standards early and often with IAM policies as code

Dev team

Resource access

Grant the right fine-grained access so that resources can talk to each other

Fine-grained permissions

Refine permissions as you determine application requirements

Your role as a developer

Your goal: Provision and manage infrastructure for your applications with fine-grained permissions

Tools

Explore and determine services you need for your applications

Resource access

Grant the right fine-grained access so that resources can talk to each other

Dev team

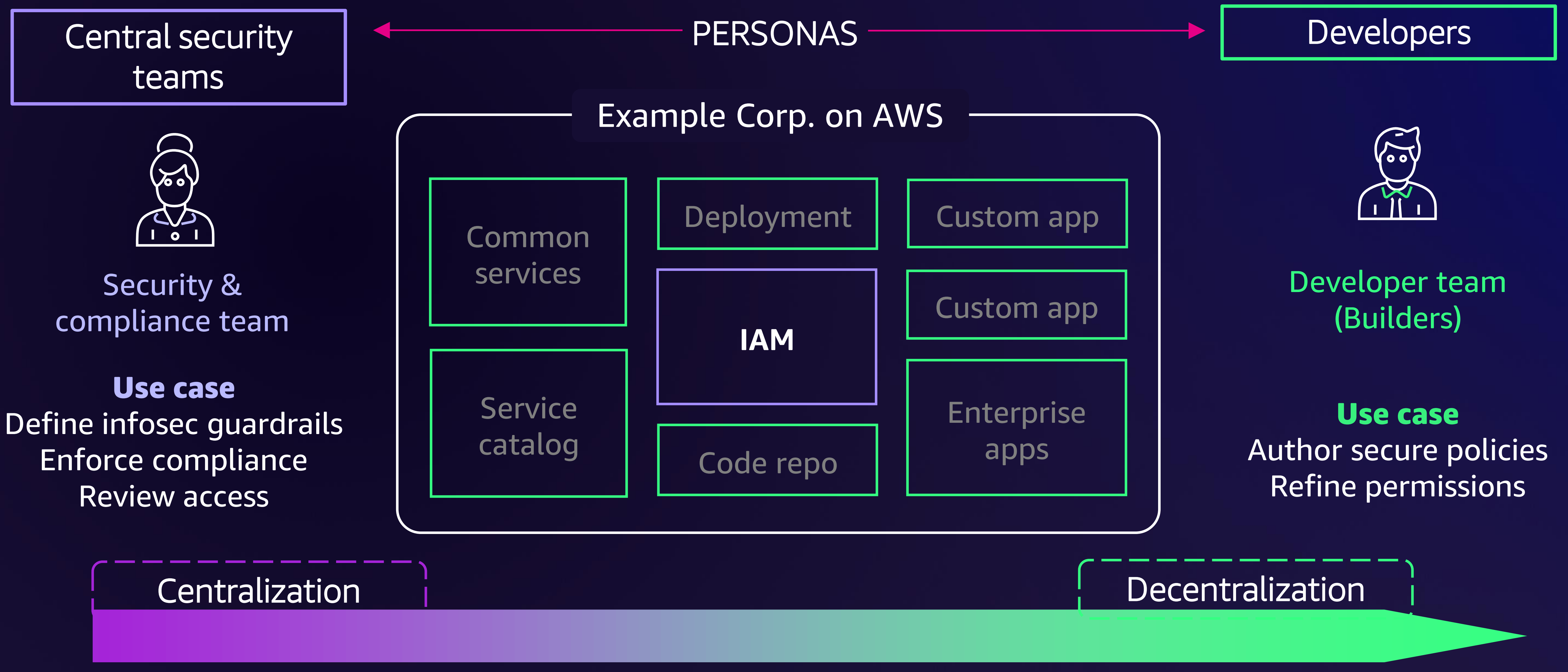
Security best practices

Adhere to security standards early and often with IAM policies as code

Fine-grained permissions

Refine permissions as you determine application requirements

Empowering developers to move fast



Security & compliance team

Use case
Define infosec guardrails
Enforce compliance
Review access

Developer team (Builders)

Use case
Author secure policies
Refine permissions

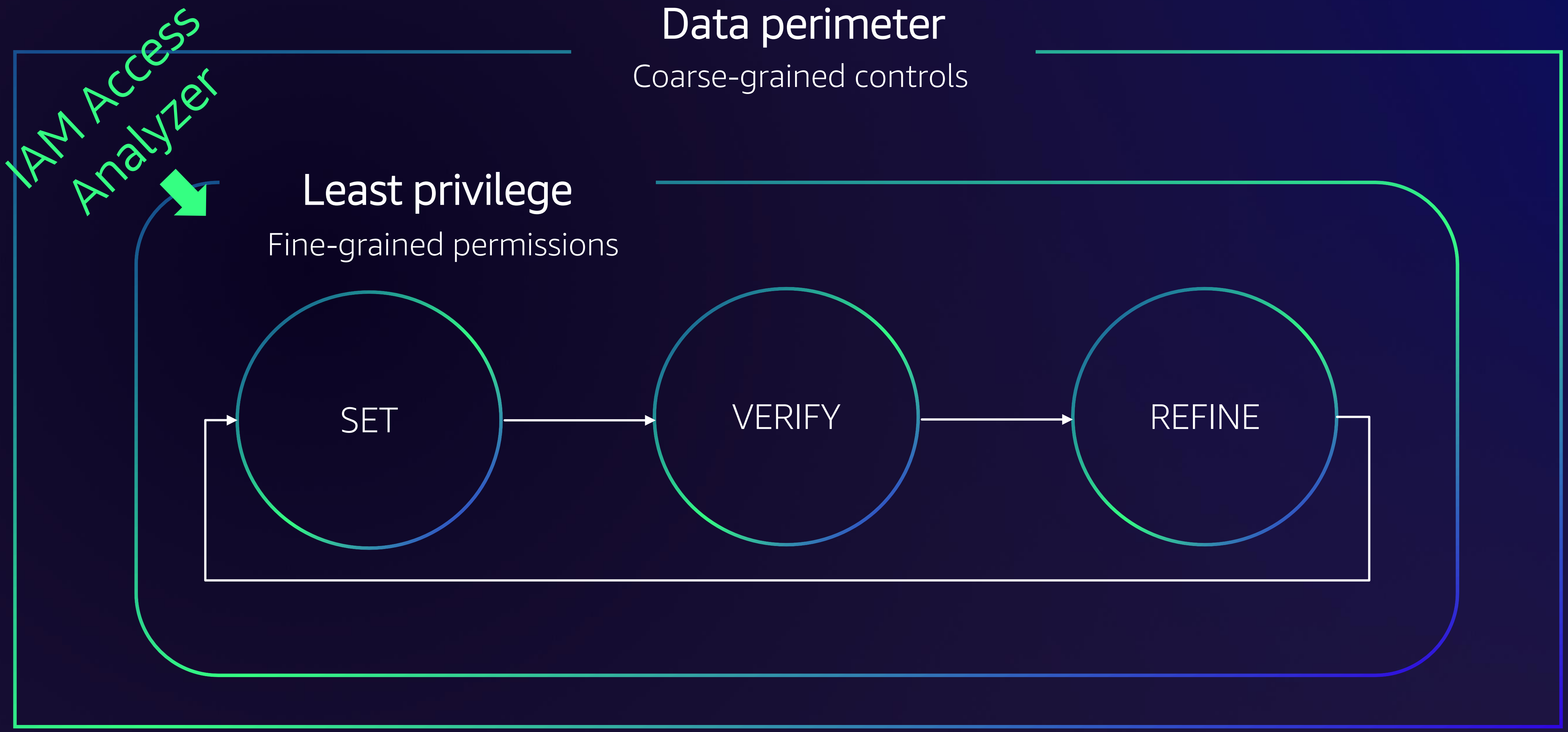
Where does AWS help?

AWS offers Cloud Infrastructure and Entitlement Management (CIEM) solutions

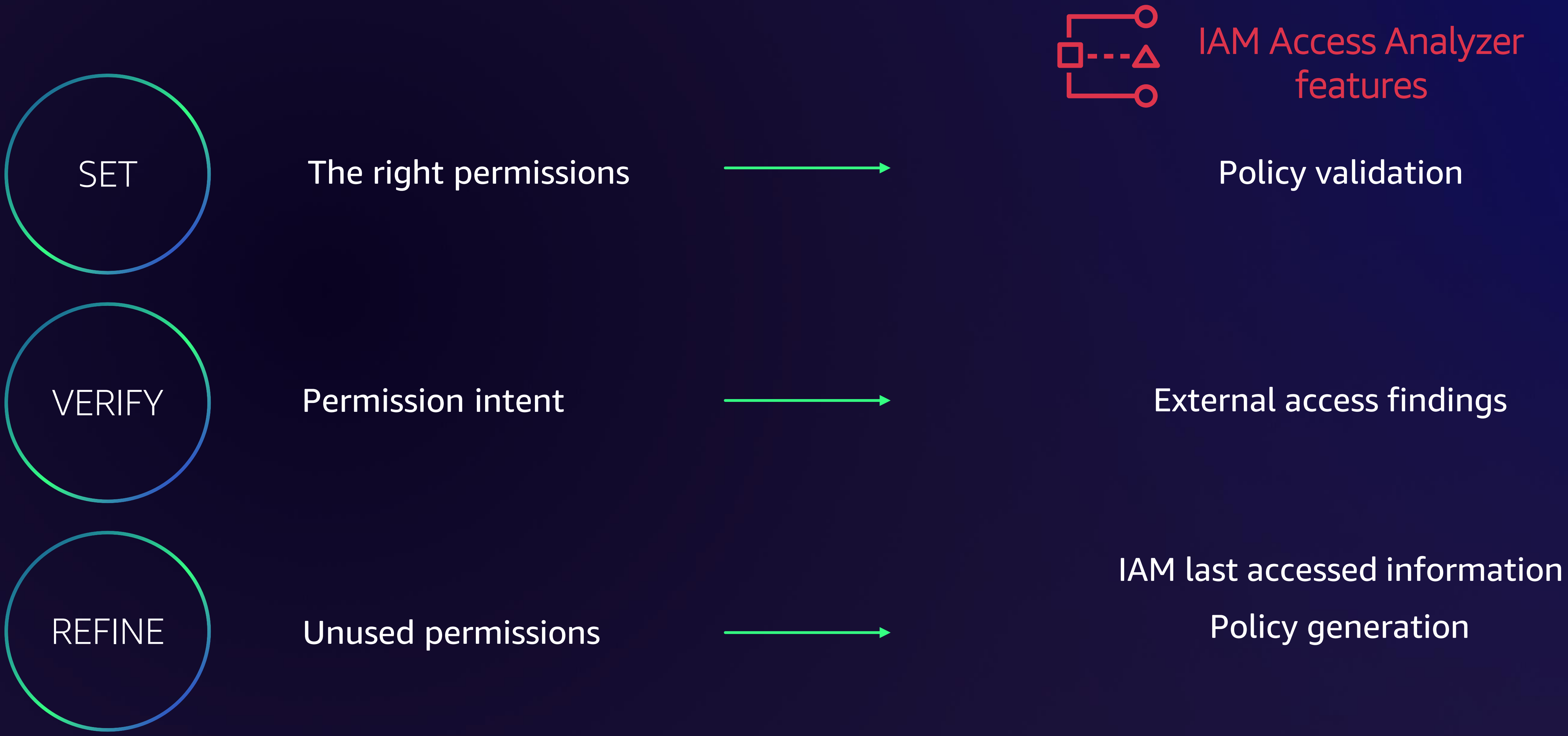
Right size	**Anomaly detection**	**Visualization**	**Compliance reporting**
IAM Access Analyzer	**Amazon GuardDuty**	**Amazon Detective**	**AWS Audit Manager**
Set, verify, and refine permissions confidently	Protect your identities with intelligent threat detection	Visualize data to identify potential security issues	Continually audit and simplify compliance assessment

IAM Access Analyzer – Least privilege simplified

Access controls for your AWS estate



IAM Access Analyzer features



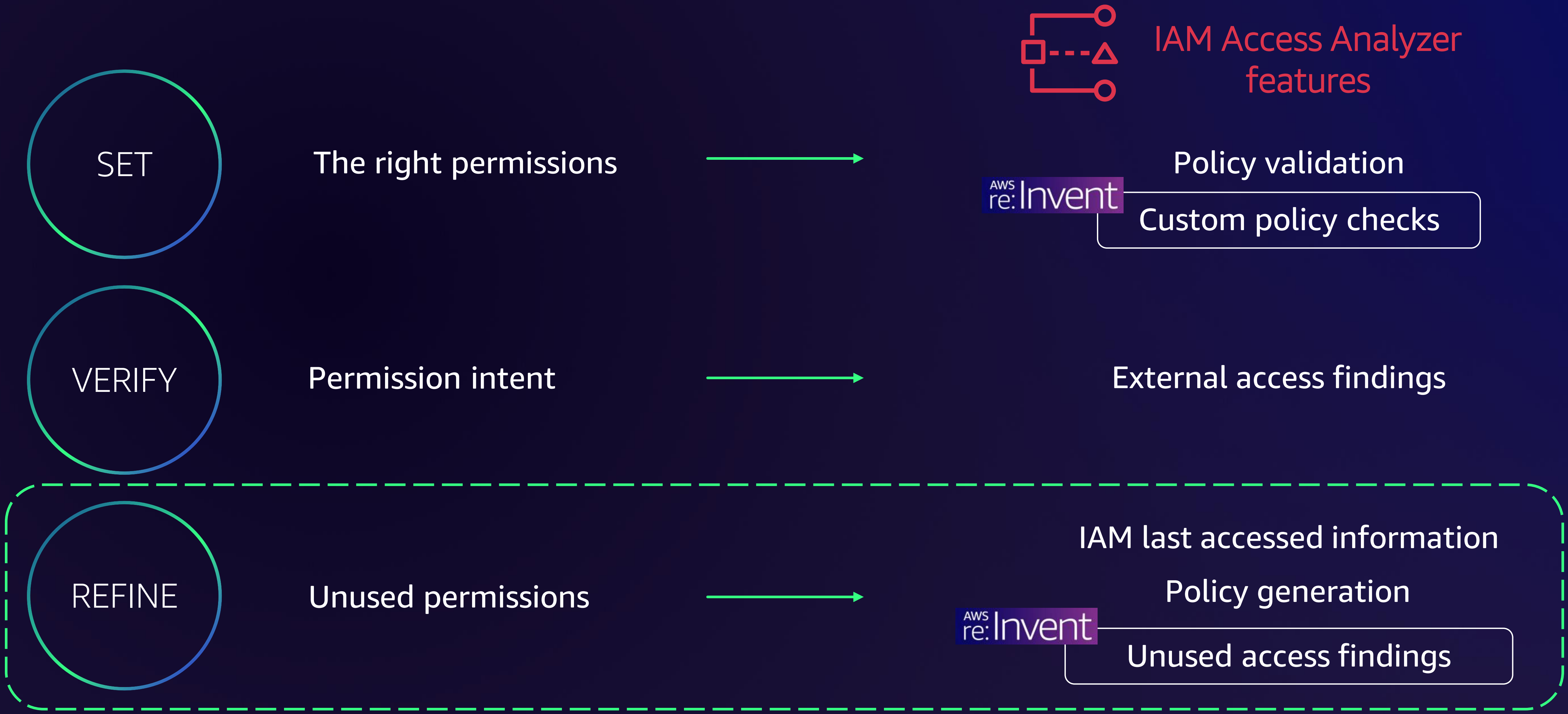
IAM Access Analyzer features

SET — The right permissions → Policy validation

VERIFY — Permission intent → External access findings

REFINE — Unused permissions → IAM last accessed information; Policy generation

IAM Access Analyzer features



IAM Access Analyzer features

SET — The right permissions → Policy validation

AWS re:Invent Custom policy checks

VERIFY — Permission intent → External access findings

REFINE — Unused permissions → IAM last accessed information

Policy generation

AWS re:Invent Unused access findings

Unused access findings

Visibility at scale

What we heard from our customers

Privilege creep is an increasing problem

- Access assigned to users, resources, and services accumulates over a period of time due to multiple factors:
  - Changes to cloud and hybrid environments
  - Changes to users' job role or functions
  - Evolving business, security, and compliance requirements
- Need frequently to monitor unused and overly permissive access
- Cost of least privilege journey is getting prohibitive

Refine permissions by gaining insights through unused access analysis

Enable IAM Access Analyzer unused access in:

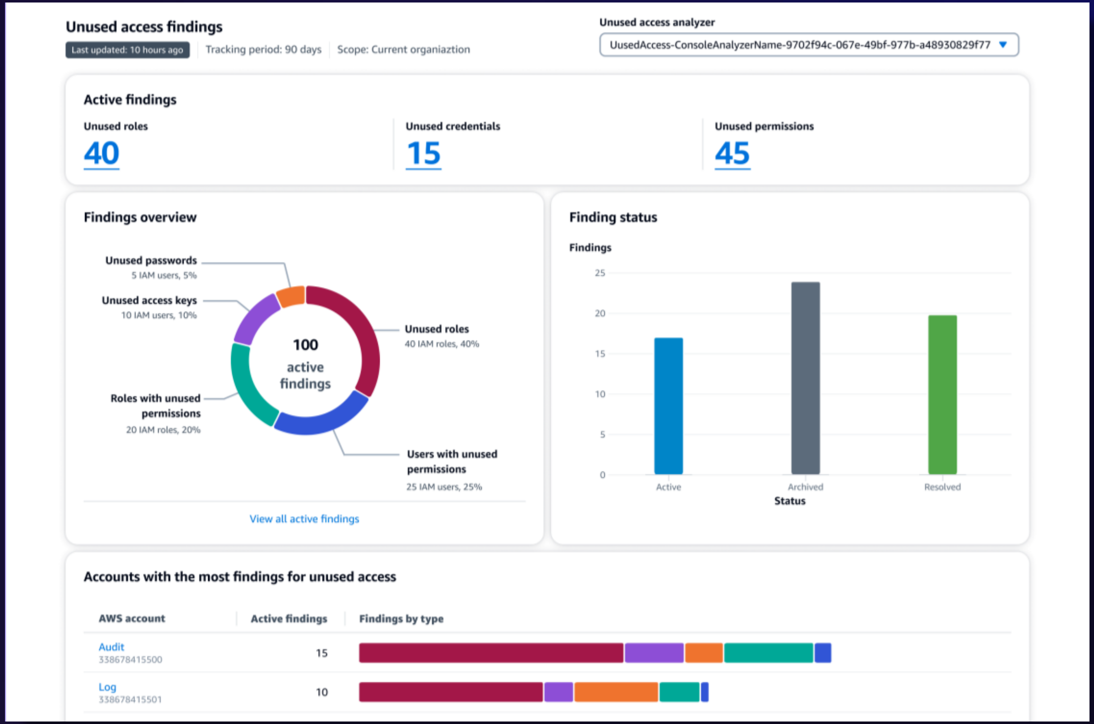
AWS Organizations

AWS account

Identify unused:

- IAM access keys
- IAM user passwords
- IAM roles
- AWS services and actions

Review and manage findings through the dashboard



Unused access findings

Last updated: 10 hours ago | Tracking period: 90 days | Scope: Current organiaztion

Unused access analyzer: UusedAccess-ConsoleAnalyzerName-9702f94c-067e-49bf-977b-a48930829f77

Active findings

Unused roles	Unused credentials	Unused permissions
40	15	45

Findings overview

View all active findings

Finding status

Accounts with the most findings for unused access

AWS account	Active findings	Findings by type
Audit 338678415500	15	
Log 338678415501	10	

Refine unused access

Centrally inspect all IAM users and roles with unused access to refine permissions

Continuously monitor and identify broad IAM access

Review and inspect findings through an easy-to-use dashboard

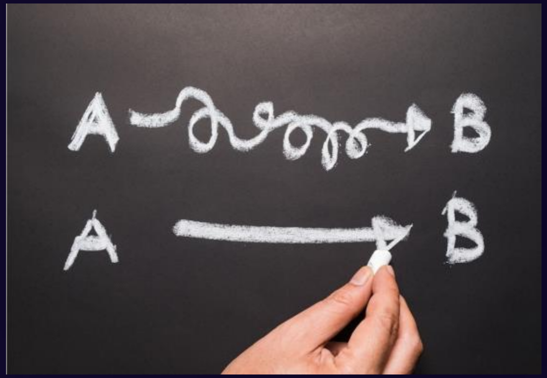
Aggregate findings by integrating with AWS Security Hub

Automate notifications by integrating with Amazon EventBridge

New: Unused access findings recommendations

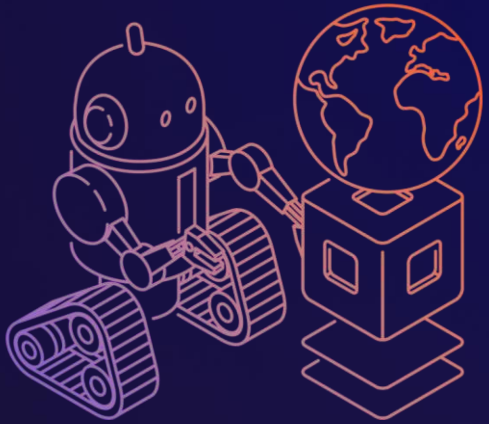
Refine permissions with policy recommendations

NEW



Simplify how you refine unused access

Update policies **effortlessly** with step-by-step recommendations



Let **automated reasoning** do the legwork to ensure IAM Access Analyzer recommends less permissive policies

Refine permissions with policy recommendations

Demo

Console dashboard and unused access findings remediation

Additional resources

What’s new on unused access recommendations

AWS IAM Access Analyzer now offers recommendations to refine unused access
https://aws.amazon.com/about-aws/whats-new/2024/06/aws-iam-access-analyzer-refine-unused-access/

IAM Access Analyzer unused access documentation

Findings for external and unused access
https://docs.aws.amazon.com/IAM/latest/UserGuide/access-analyzer-findings.html

AWS IAM Access Analyzer service page

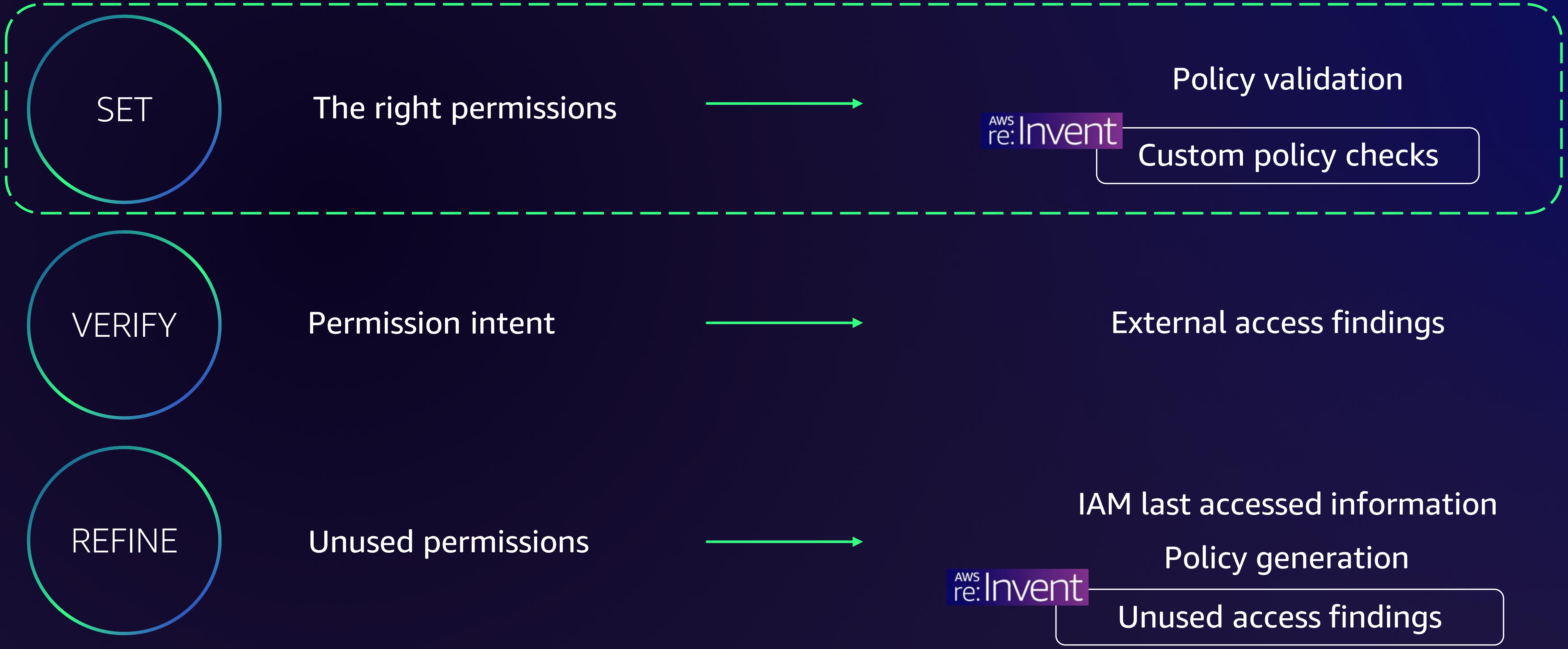
AWS IAM Access Analyzer
https://aws.amazon.com/iam/access-analyzer/

Custom policy checks

Automate policy reviews to help builders set the right permissions

IAM Access Analyzer features

IAM Access Analyzer features



SET

The right permissions → Policy validation

AWS re:Invent Custom policy checks

VERIFY

Permission intent → External access findings

REFINE

Unused permissions → IAM last accessed information

Policy generation

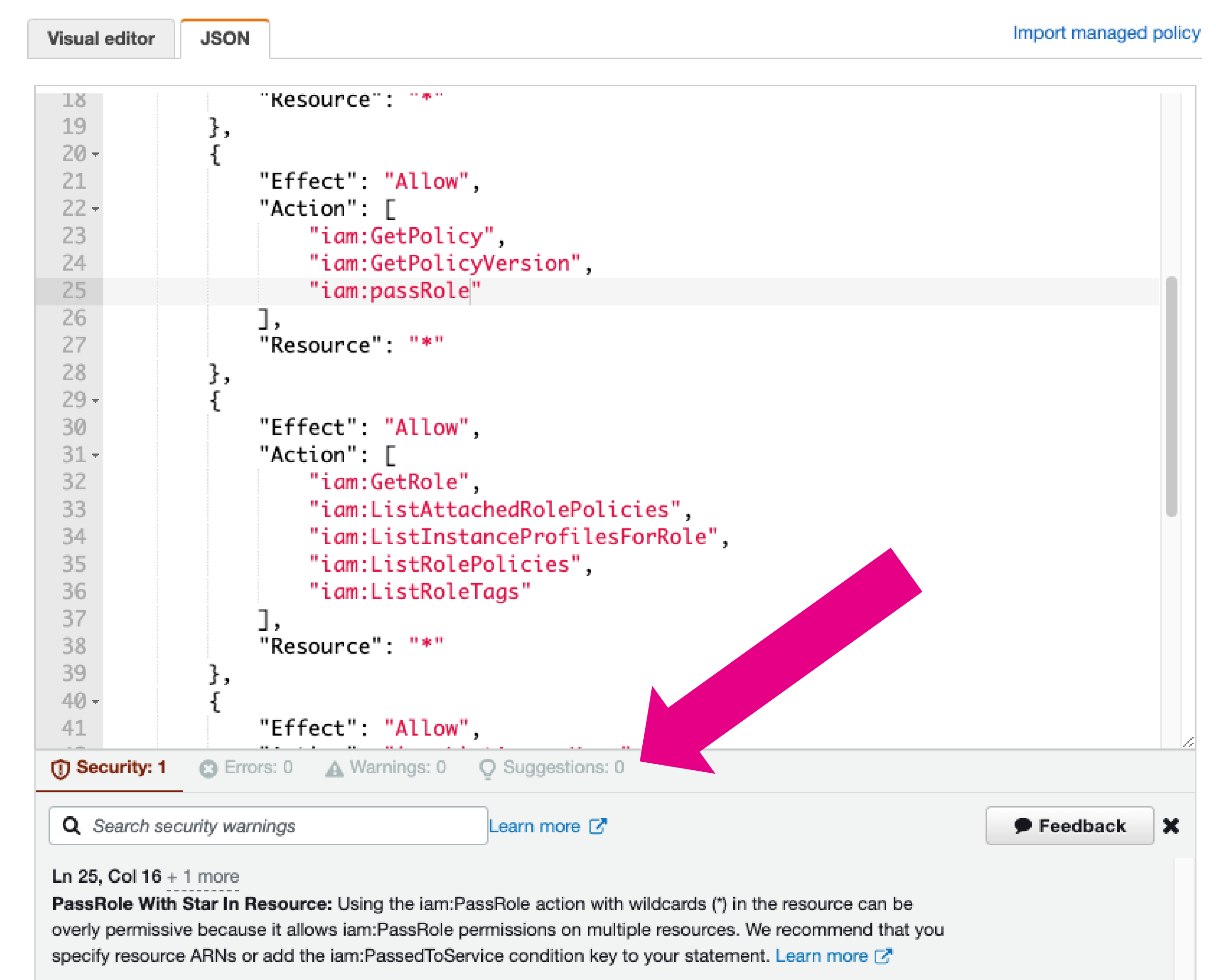
AWS re:Invent Unused access findings

IAM Access Analyzer policy validation

Default checks

Author functional policies that adhere to AWS best practices with IAM Access Analyzer policy validation

1. Security warnings
2. Errors
3. General warnings
4. Suggestions



```
18                "Resource": "*"
19            },
20            {
21                "Effect": "Allow",
22                "Action": [
23                    "iam:GetPolicy",
24                    "iam:GetPolicyVersion",
25                    "iam:passRole"
26                ],
27                "Resource": "*"
28            },
29            {
30                "Effect": "Allow",
31                "Action": [
32                    "iam:GetRole",
33                    "iam:ListAttachedRolePolicies",
34                    "iam:ListInstanceProfilesForRole",
35                    "iam:ListRolePolicies",
36                    "iam:ListRoleTags"
37                ],
38                "Resource": "*"
39            },
40            {
41                "Effect": "Allow",
```

Ln 25, Col 16 + 1 more

PassRole With Star In Resource: Using the iam:PassRole action with wildcards (*) in the resource can be overly permissive because it allows iam:PassRole permissions on multiple resources. We recommend that you specify resource ARNs or add the iam:PassedToService condition key to your statement. Learn more

Why automate policy reviews?

Developer team

Free developers to experiment and innovate quickly – and safely

Central security team

Free members of the security team to focus on high-value tasks that improve the business

Ensure permissions adhere to security standards

CheckNoNewAccess

Check that a policy change did not introduce any new access

Input
Previous and new policy

Output
Pass – No new access
Fail – New access with location

CheckAccessNotGranted

Check that a policy does not grant access to a list of critical actions

Input
Policy and list of actions

Output
Pass – Doesn’t grant actions in list
Fail – Grants access to action in list with location

Pro tip: Become besties with these IAM Access Analyzer APIs

New: Custom policy checks for public access

Ensure permissions adhere to security standards

NEW

CheckNoNewAccess

Check that a policy change did not introduce any new access

Input
Previous and new policy

Output
Pass – No new access
Fail – New access with location

NEW

CheckAccessNotGranted

Check that a policy does not grant access to a list of critical actions and **resources**

Input
Policy and list of actions and **resources**

Output
Pass – Doesn't grant actions or **resources** in list
Fail – Grants access to action or **resource** in list with location

NEW

CheckNoPublicAccess

Check that a resource policy does not grant public access to a resource

Input
Policy and resource type

Output
Pass – No public access
Fail – Public access with location

aws

Verify policies with custom policy checks

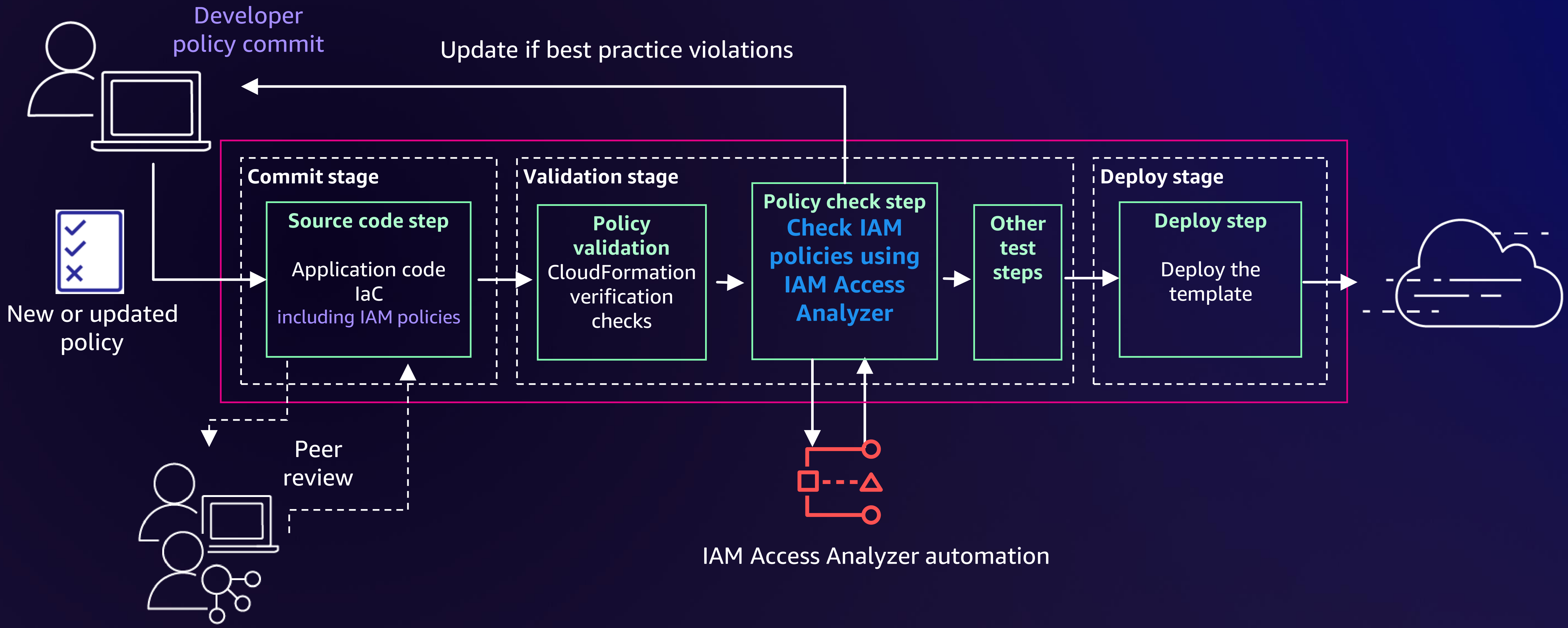
Simplify policy reviews by validating policies to match your corporate security standards

Automate policy reviews

Configurable checks

Accurate and scalable analysis

Automate policy reviews with IAM Access Analyzer



Developer policy commit

Update if best practice violations

New or updated policy

Commit stage

Source code step

Application code
IaC
including IAM policies

Validation stage

Policy validation
CloudFormation verification checks

Policy check step
Check IAM policies using IAM Access Analyzer

Other test steps

Deploy stage

Deploy step

Deploy the template

Peer review

IAM Access Analyzer automation

Pro tip: Shift left with policy review automation

Demo

New custom policy checks in action

Additional resources

Jeff Bar AWS News Blog

IAM Access Analyzer Update: Extending custom policy checks & guided revocation
https://aws.amazon.com/blogs/aws/iam-access-analyzer-update-extending-custom-policy-checks-guided-revocation/

Security Blog

Introducing IAM Access Analyzer custom policy checks
https://aws.amazon.com/blogs/security/introducing-iam-access-analyzer-custom-policy-checks/

Reference Policy Samples

IAM Access Analyzer custom policy check samples
https://github.com/aws-samples/iam-access-analyzer-custom-policy-check-samples

Takeaways

- Use IAM Access Analyzer on your journey to least privilege
- Use unused access findings to centrally inspect users and roles
- Remove unused access keys, passwords, users, roles, and permissions
- Use custom policy checks to automate policy reviews

Learn more about IAM Access Analyzer at re:Inforce

Check out the chalk talk after this

IAM334 | Refine unused access with IAM Access Analyzer
Jun. 12 | 4:00 PM – 5:00 PM (EDT)
PCC | 100 Level | 125