

AWS re:Inforce

JUNE 13 - 14, 2023 | ANAHEIM, CA

I A M 3 3 2 - R

Practical identity and access management: The basics of IAM on AWS

Dario Goldfarb

Principal Security Solutions Architect
AWS

Arthur Mnev

Senior Security Solutions Architect
AWS



What you'll learn in this session

In this session you will learn how to build your IAM strategy, with opinionated prescriptive guidance

Agenda

- AWS identity strategy
 - How to prioritize
 - Building your IAM journey
- Practical IAM recommendations for each phase:
 - Quick Wins
 - Foundational
 - Efficient
 - Optimized
- Conclusions

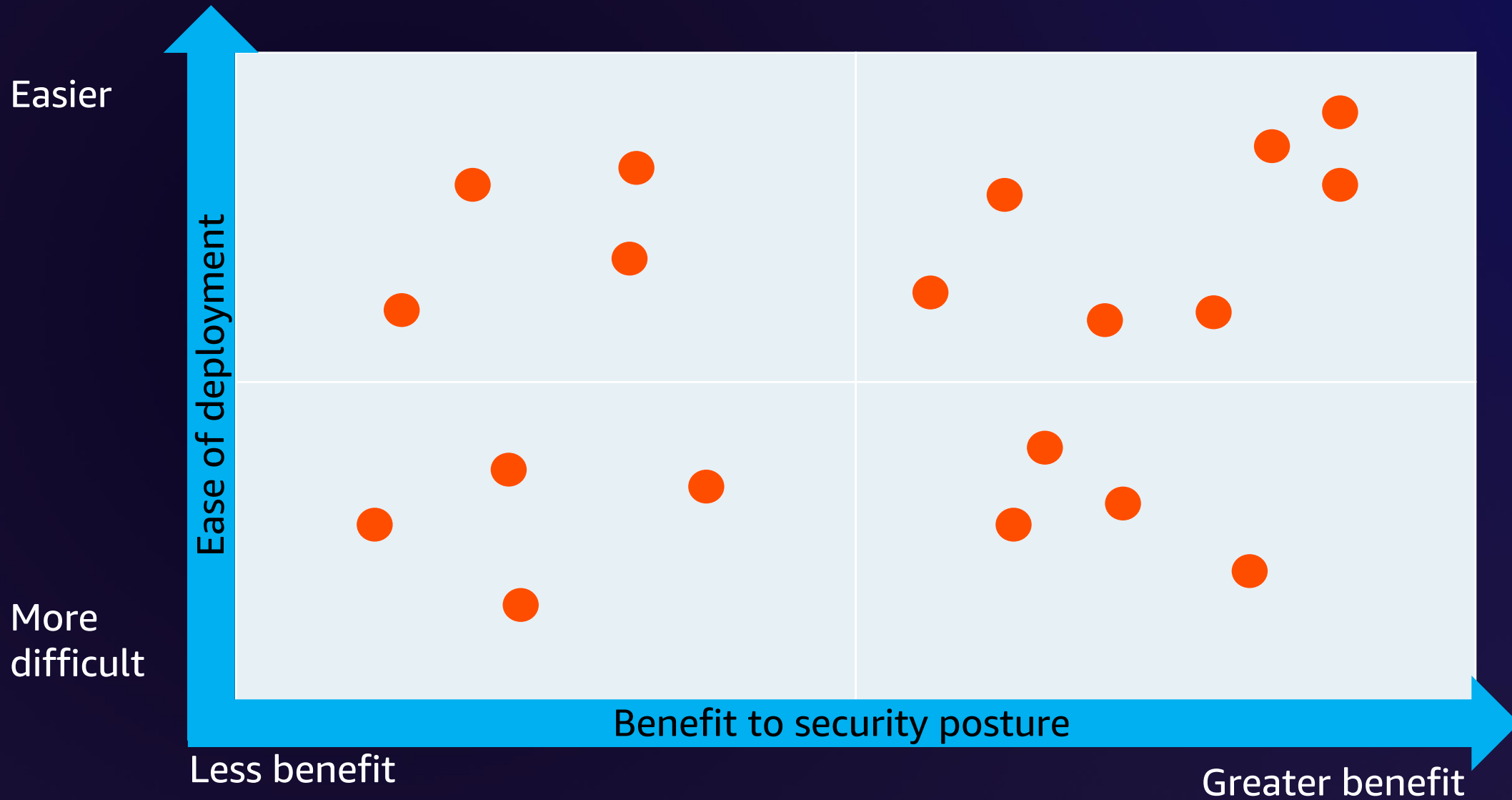
AWS identity strategy



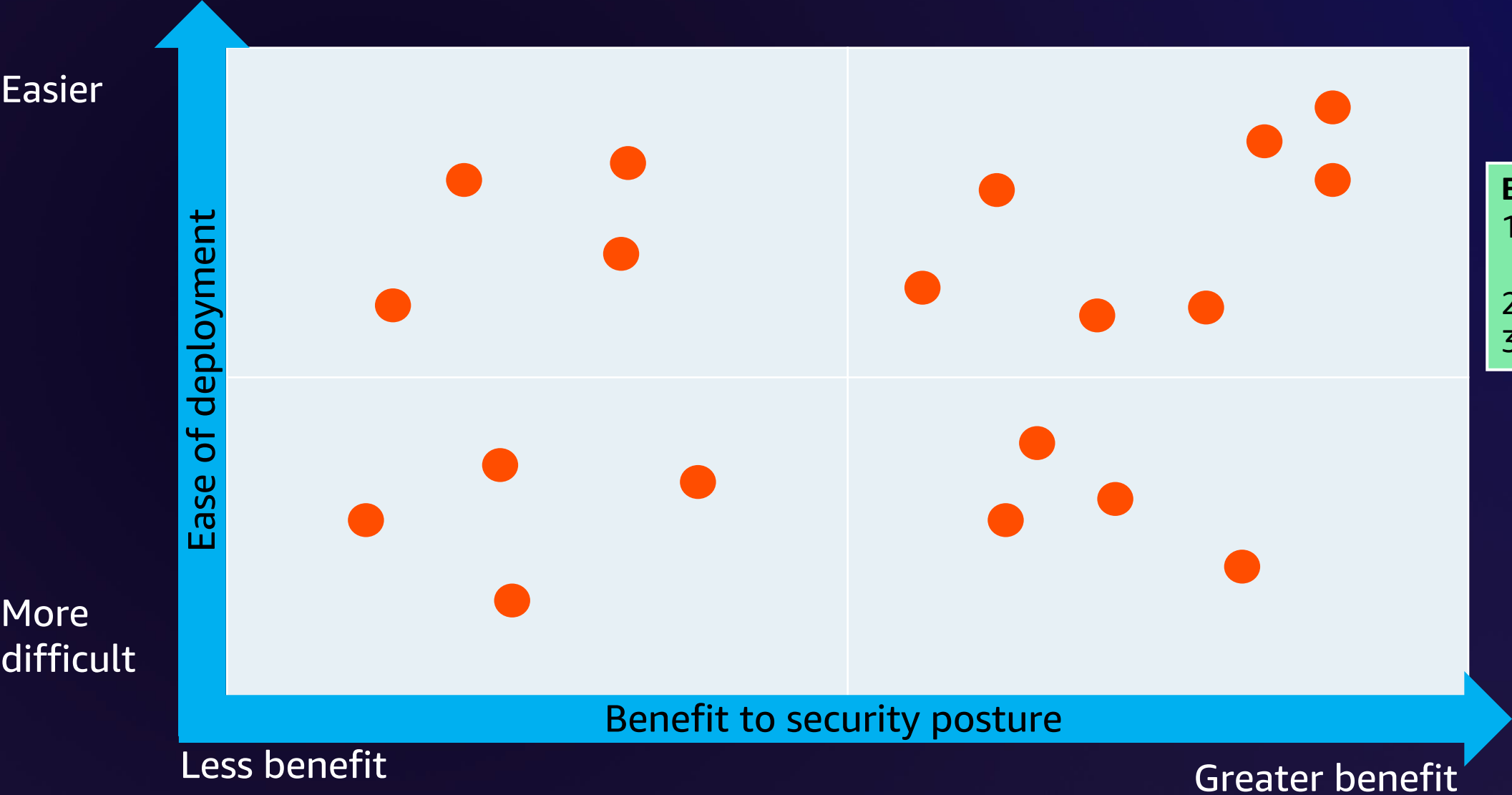
Improving your posture is a journey



AWS identity strategy: How to prioritize



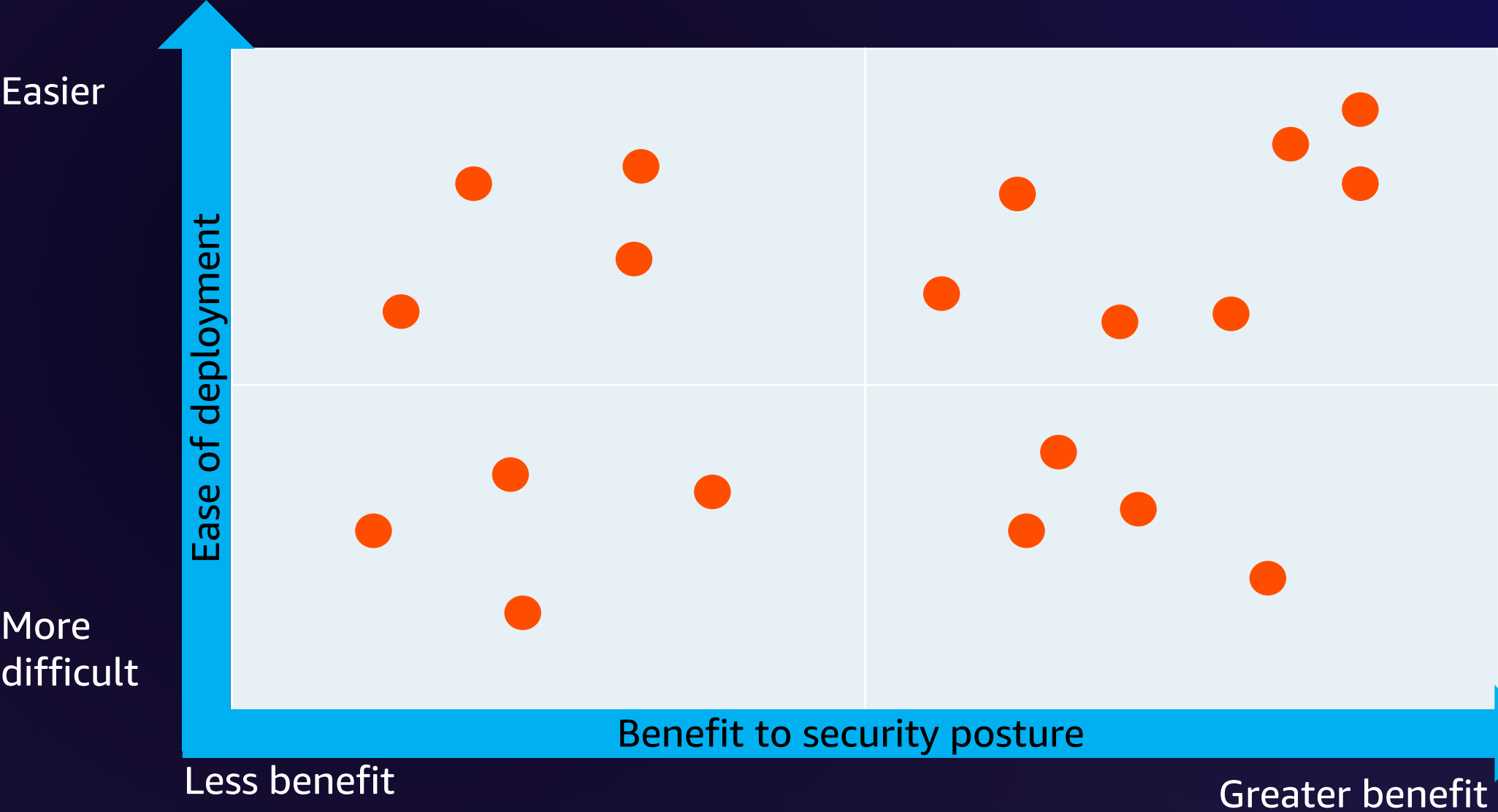
AWS identity strategy: How to prioritize



Easy
1. Quick/easy to implement
2. Low effort
3. Low cost



AWS identity strategy: How to prioritize

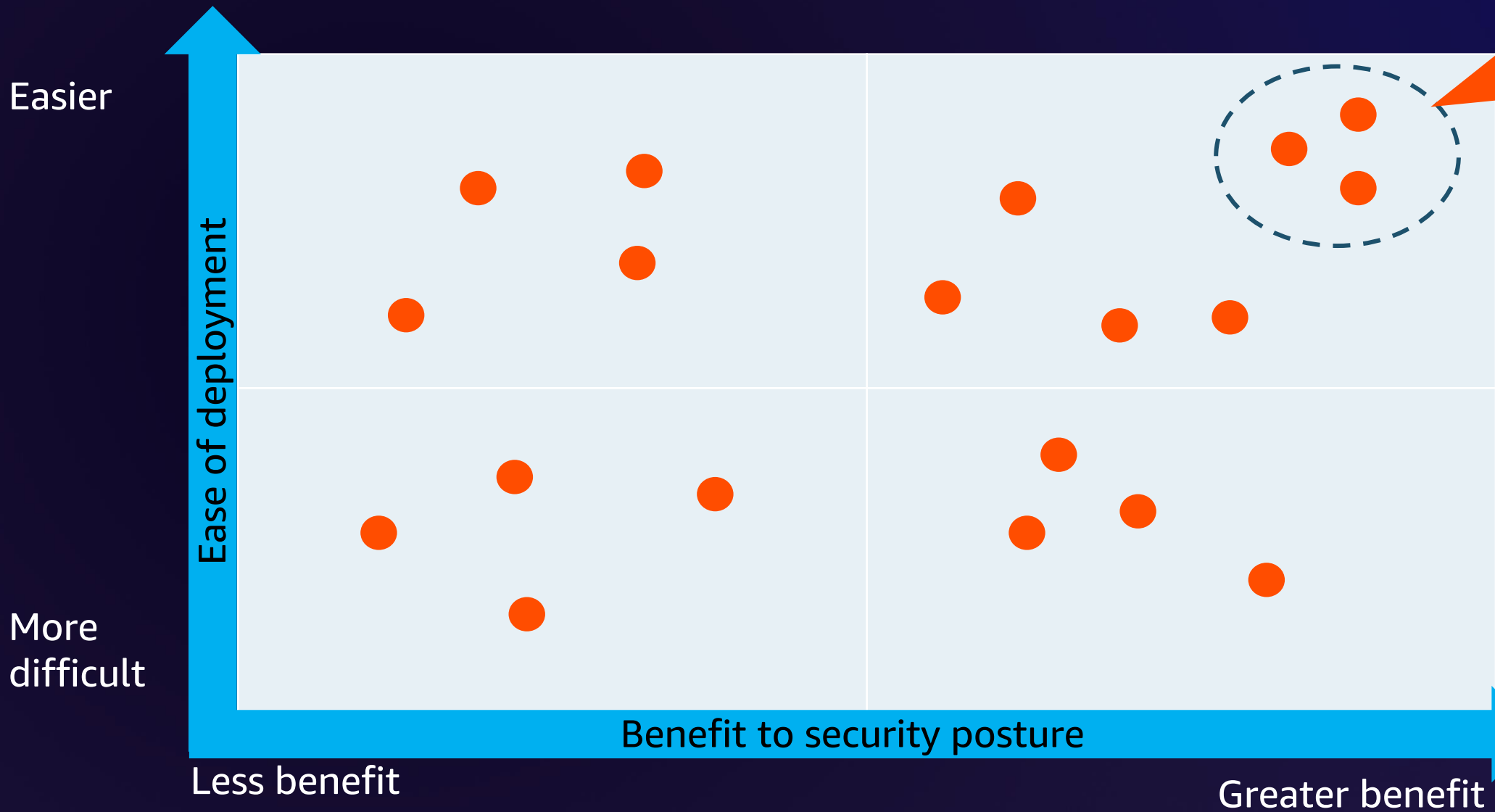


Easy
1. Quick/easy to implement
2. Low effort
3. Low cost

Benefit
Mitigation of critical risks or risks with high likelihood of occurrence



AWS identity strategy: How to prioritize



Quick wins

- All in 1 week
- Big benefit

Easy

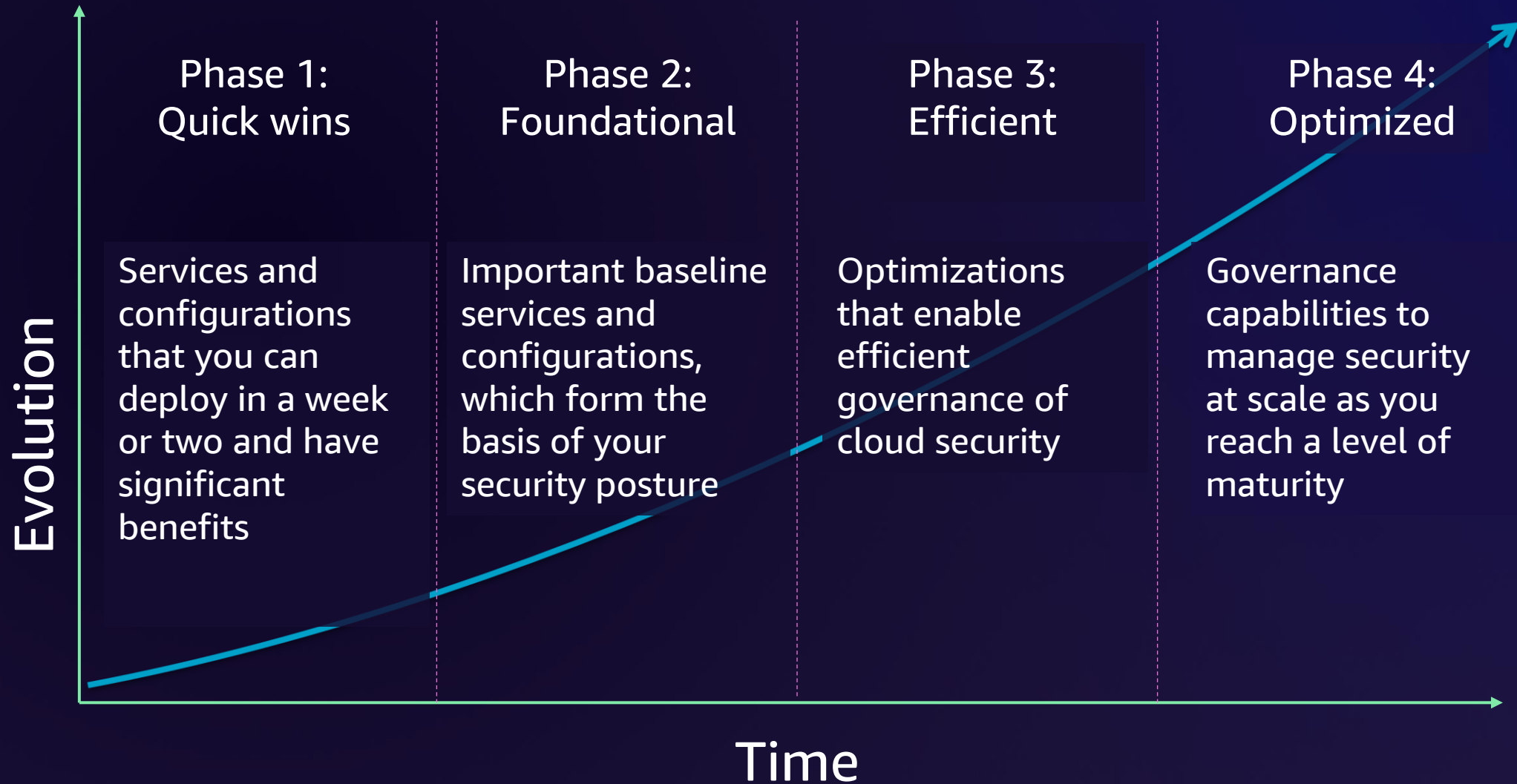
1. Quick/easy to implement
2. Low effort
3. Low cost

Benefit

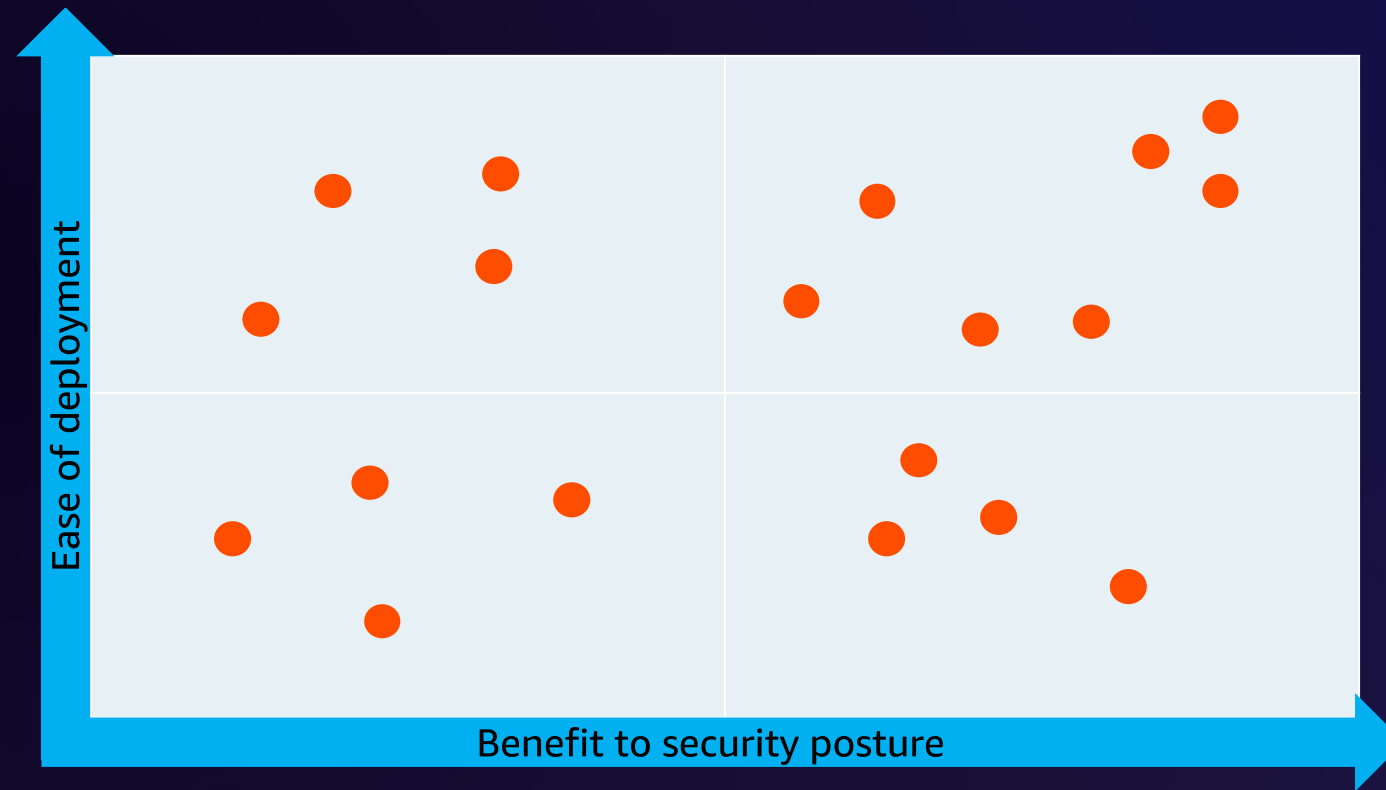
Mitigation of critical risks or risks with high likelihood of occurrence



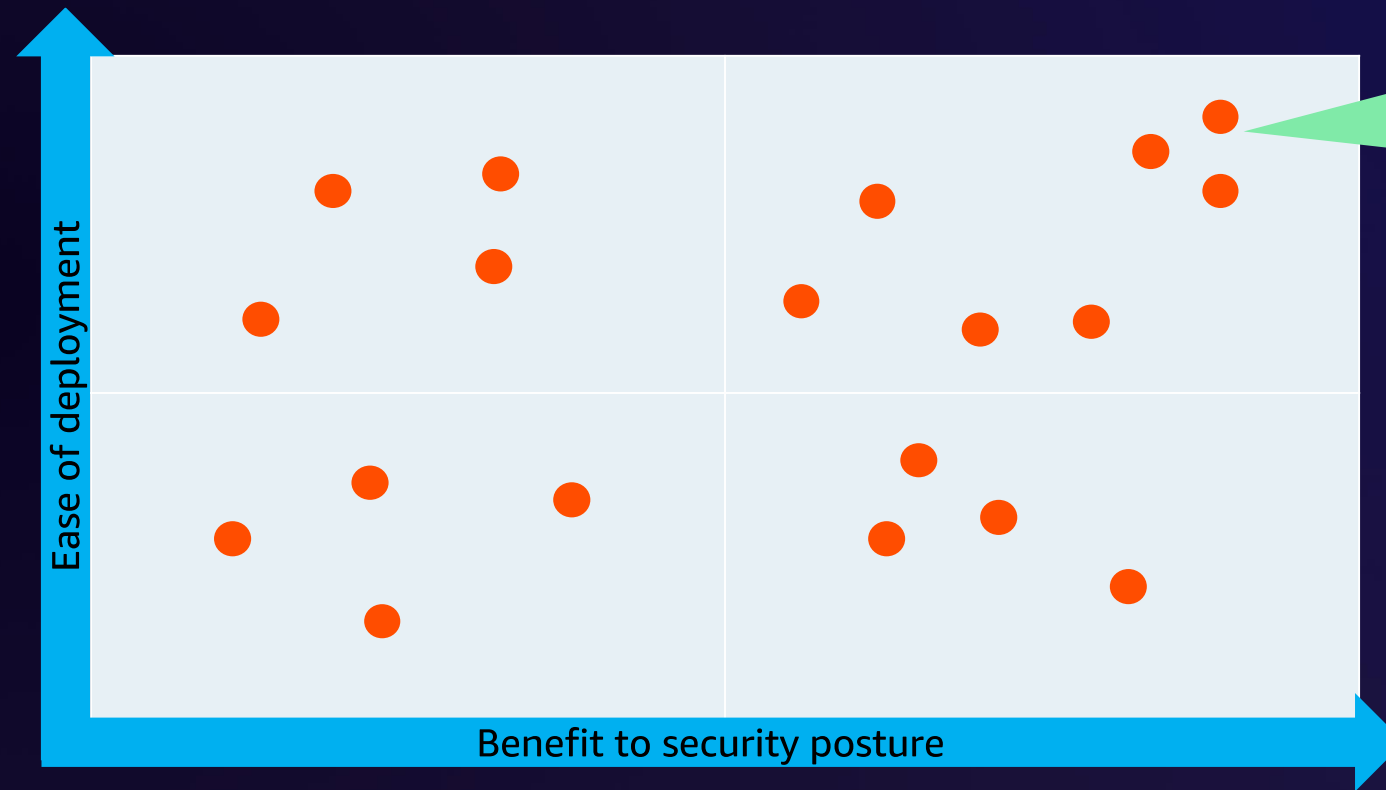
Building your IAM journey



AWS identity strategy: Examples



AWS identity strategy: Examples

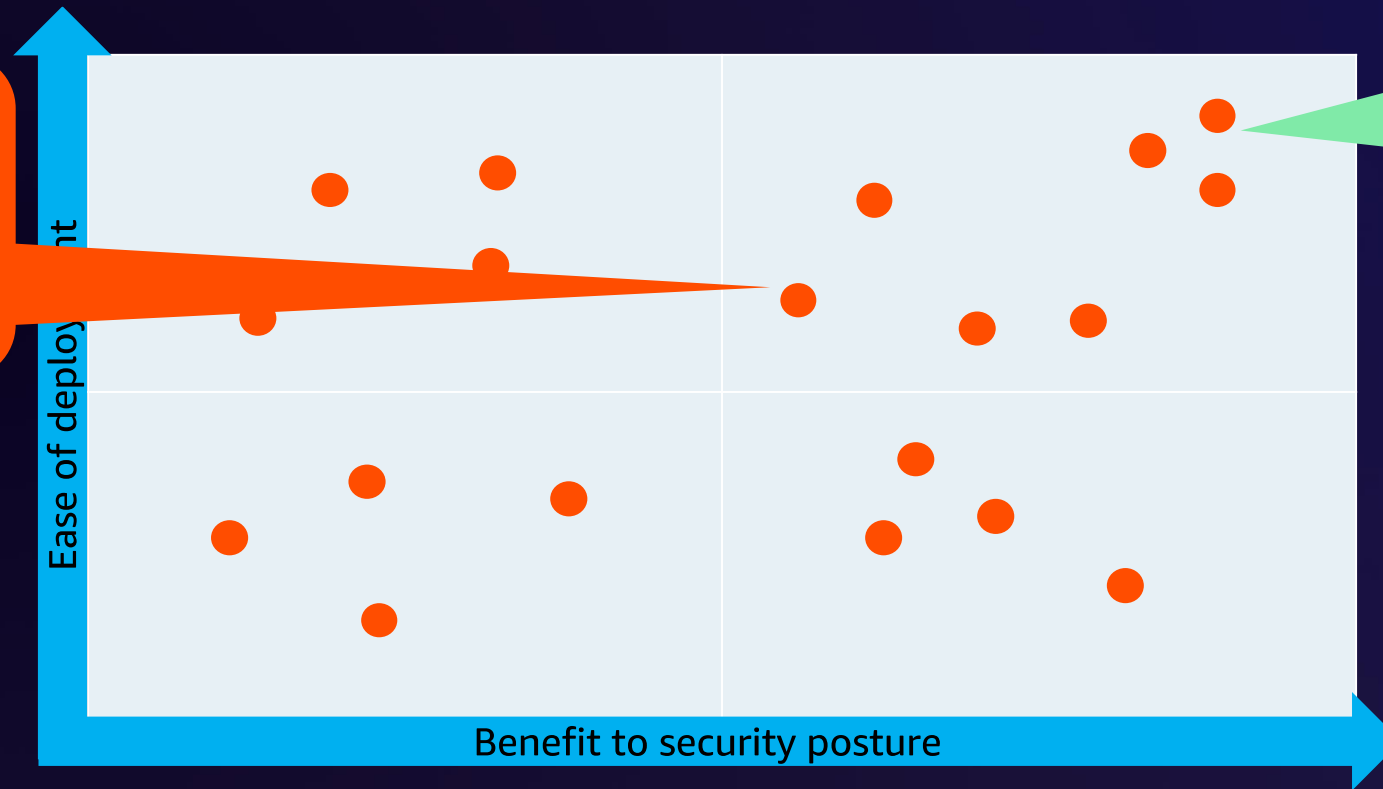


1. Quick wins
- MFA
- Identity federation

AWS identity strategy: Examples

2. Foundations

- Organizations with AWS Control Tower
- Reduce usage of Access Keys



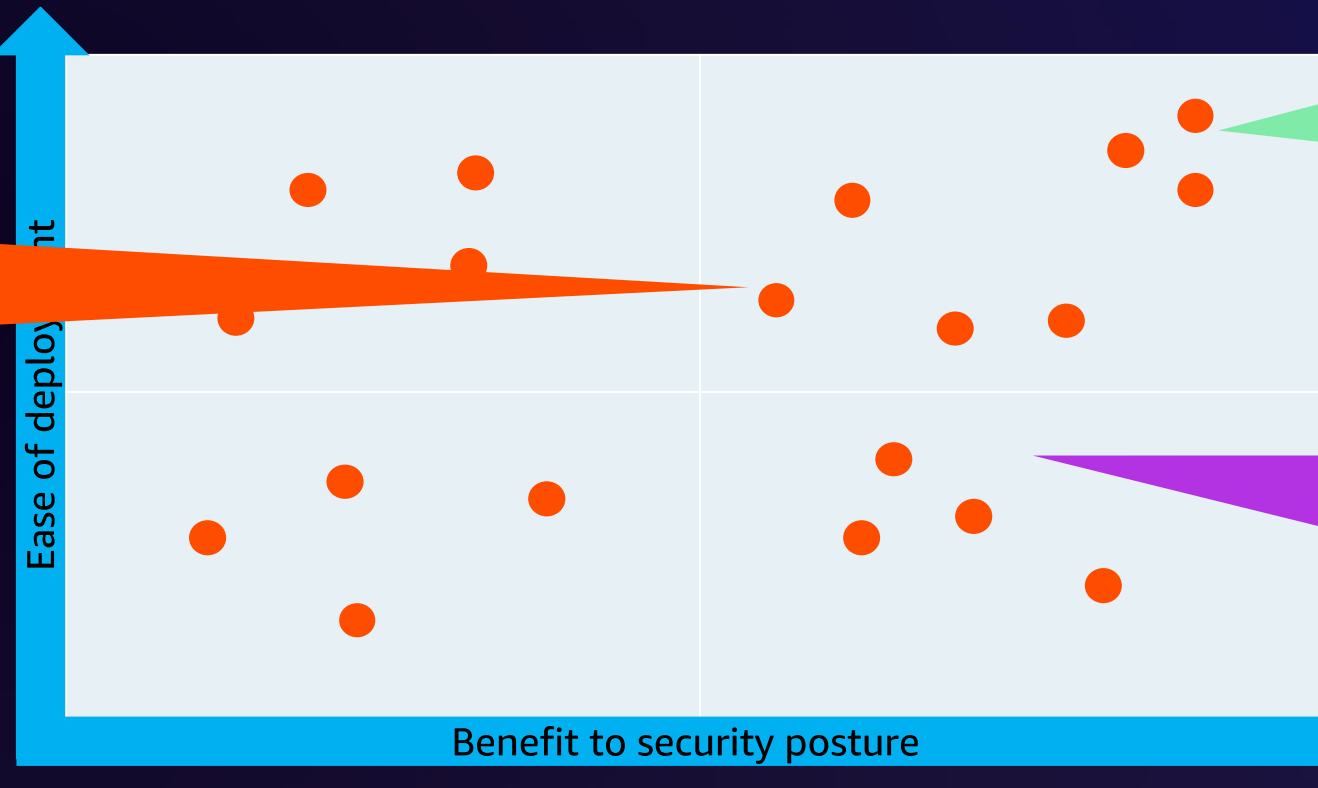
1. Quick wins

- MFA
- Identity federation

AWS identity strategy: Examples

2. Foundations

- Organizations with AWS Control Tower
- Reduce usage of Access Keys



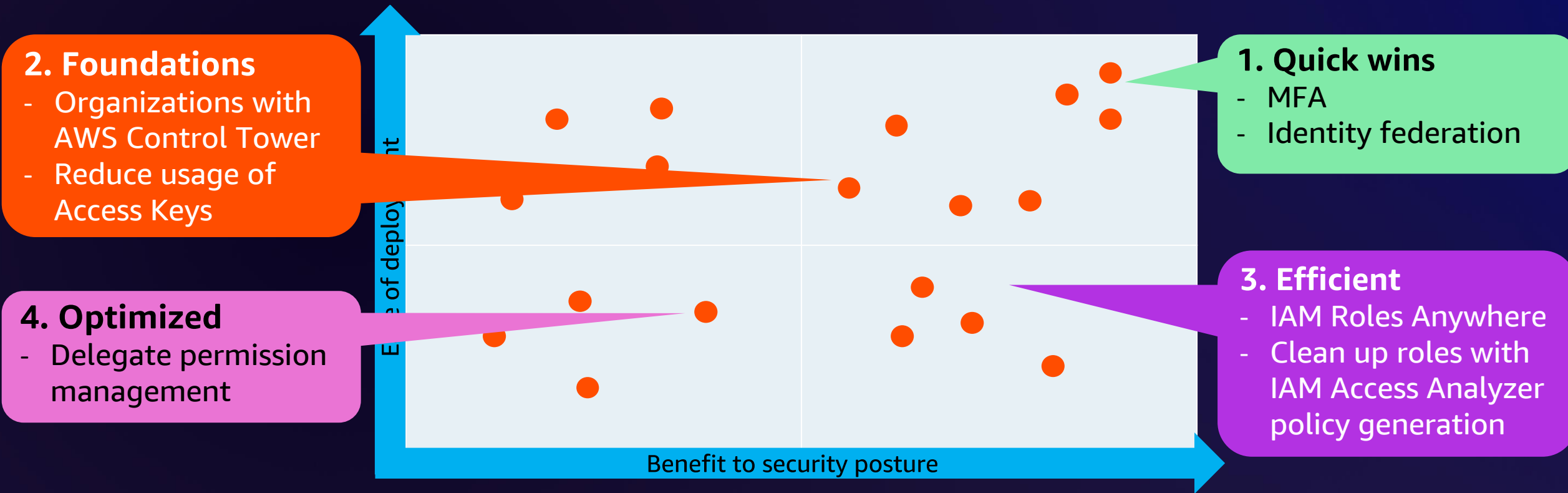
1. Quick wins

- MFA
- Identity federation

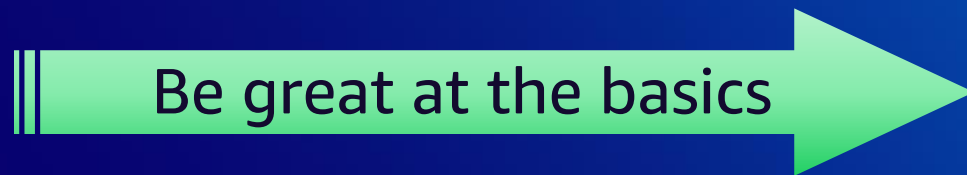
3. Efficient

- IAM Roles Anywhere
- Clean up roles with IAM Access Analyzer policy generation

AWS identity strategy: Examples



Phase 1: Quick Wins



Phase 1: IAM Quick Wins

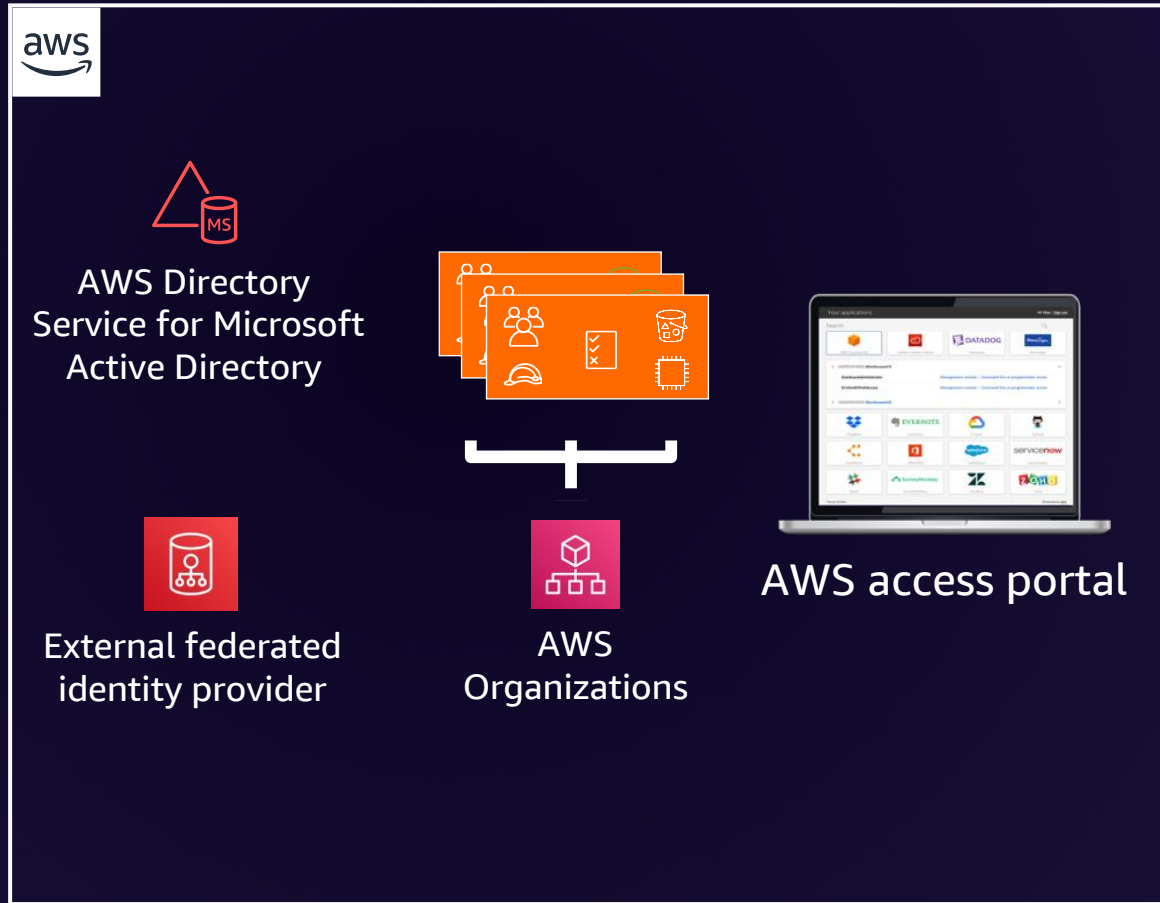
1. Implement AWS Control Tower with multiple accounts to segregate workloads
 - Federate your Identity Provider to IAM Identity Center
2. Enable MFA everywhere
 - Root, employees, contractors, customers (CIAM)
3. Avoid the use of root
 - Disable use of root on member accounts (with SCPs)

Phase 1: IAM Quick Wins

1. Implement AWS Control Tower with multiple accounts to segregate workloads
 - Federate your identity provider to IAM Identity Center

IAM Identity Center

NO ADDITIONAL COST



Benefits

- Access portal to **multiple accounts**
- Central permission assignment
- Integrated with AWS **CLI v2**
- You choose your identity provider

okta

Microsoft Azure
Active Directory

onelogin
by ONE IDENTITY

Ping
Identity

Microsoft
Active Directory

jumpcloud™

CYBERARK™

or use IAM Identity Center
directory if you don't have one

Phase 1: IAM Quick Wins

1. Implement AWS Control Tower with multiple accounts to segregate workloads
 - Federate your identity provider to IAM Identity Center
2. Activate MFA everywhere
 - Root, employees, contractors, customers (CIAM)

MFA

FREE MFA SECURITY KEY

IAM Identity Center × IAM Identity Center > Settings > Configure multi-factor authentication

Configure multi-factor authentication

Choose how often workforce users are prompted for multi-factor authentication (MFA) and which types of devices they can use to sign in to the AWS access portal. [Learn more](#)

MFA Settings

Prompt users for MFA

- Only when their sign-in context changes (context-aware)
Users with a registered MFA device are only prompted when their sign-in context changes (for example, they sign in from a new device or browser, or from an unknown IP address). Users can remember devices when this mode is selected.
- Every time they sign in (always-on)
Users with a registered MFA device are prompted every time they sign in.
- Never (disabled)
All users sign in with their standard user name and password only. Choosing this option disables MFA.

Users can authenticate with these MFA types

- Security keys and built-in authenticators
Users can verify their identity by using any FIDO2 or U2F capable device such as an external physical security key (for example, YubiKey or Feitian devices) or a built-in authenticator (for example, Apple TouchID or Windows Hello).
- Authenticator apps
Users can verify their identity by entering a code generated from a time-based one-time password authenticator app (for example, Authy, Google Authenticator, Microsoft Authenticator).

If a user does not yet have a registered MFA device




- Require them to register an MFA device at sign in
- Require them to provide a one-time password sent by email to sign in
- Block their sign-in
- Allow them to sign in

Who can manage MFA devices

- Users can add and manage their own MFA devices

Select MFA device [Info](#)

Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.

-  **Authenticator app**
Authenticate using a code generated by an app installed on your mobile device or computer.
-  **Security Key**
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.
-  **Hardware TOTP token**
Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.

Cancel **Save changes**

<https://aws.amazon.com/iam/features/mfa>

Phase 1: IAM Quick Wins

1. Implement AWS Control Tower with multiple accounts to segregate workloads
 - Federate your identity provider to IAM Identity Center
2. Activate MFA everywhere
 - Root, employees, contractors, customers (CIAM)
3. Avoid the use of root
 - Disable use of root on member accounts (with SCPs)

Avoid the use of root

- Eliminate access keys on root
- Limit use to admin tasks that require root
- Disable the use of root with SCPs or in AWS Control Tower:

```
"Action": "*",
"Resource": "*",
"Effect": "Deny",
"Condition": {
  "StringLike": { "aws:PrincipalArn": [ "arn:aws:iam::*:root" ]}}
```

	Service	Name	Control objective	Implementation	Resource	Behavior	Release date	Guidance	Severity
<input type="radio"/>	AWS Identity and Access Management (IAM)	[AWS-GR_RESTRICT_ROOT_USER] Disallow actions as a root user	Enforce least privilege	Service control policy (SCP)	AWS::::Account	Preventive	July 30, 2019	Strongly recommended	High

Phase 2: Foundations



Phase 2: IAM Foundations

1. Enforce Security Invariants using Service Control Policies (SCPs)
2. Limit the use of IAM Users and Access Keys to the absolute minimum
 - Use temporary credentials
 - Use IAM Roles for your compute resources (i.e., EC2 instance profile, Lambda execution roles)
3. Identify & delete unintended external permissions with IAM Access Analyzer

Phase 2: IAM Foundations

1. Enforce security invariants using service control policies (SCPs)

Enforce security invariants using SCPs

The screenshot shows the AWS Control Tower console interface. On the left sidebar, the 'All controls' link is highlighted with an orange box. The main content area displays a table of controls with the following columns: Service, Name, Control objective, Implementation, Resource, Behavior, Release date, Guidance, and Severity. The first control in the table is highlighted with an orange box around its name and implementation details.

Service	Name	Control objective	Implementation	Resource	Behavior	Release date	Guidance	Severity
AWS Identity and Access Management (IAM)	[AWS-GR_RESTRICT_ROOT_USER_ACCESS_KEYS] Disallow creation of access keys for the root user	Enforce least privilege	Service control policy (SCP)	AWS:::Account; AWS::IAM::AccessKey	Preventive	July 30, 2019	Strongly recommended	High

Enforce security invariants using SCPs

```
"Effect": "Deny",  
"Action": "ec2:RunInstances",  
"Resource": ["arn:aws:ec2:*:*:instance/*"],  
"Condition":  
{ "StringNotEquals": {"ec2:InstanceType": "t2.micro" } }
```

Allow only this
type of instances
in developer
sandbox account

```
"Effect": "Deny",  
"Action": [ "organizations:LeaveOrganization" ],  
"Resource": "*"
```

Accounts can't
leave the AWS
Organizations
organization

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples.html

Phase 2: IAM Foundations

1. Enforce security invariants using service control policies (SCPs)
2. Limit the use of IAM users and access keys to the absolute minimum
 - Use temporary credentials
 - Use IAM roles for your compute resources (i.e., Amazon EC2 instance profile, AWS Lambda execution roles)

Limit the use of IAM users and access keys

The amount of IAM users and access keys can become hard to manage; establish guardrails to prevent their use:

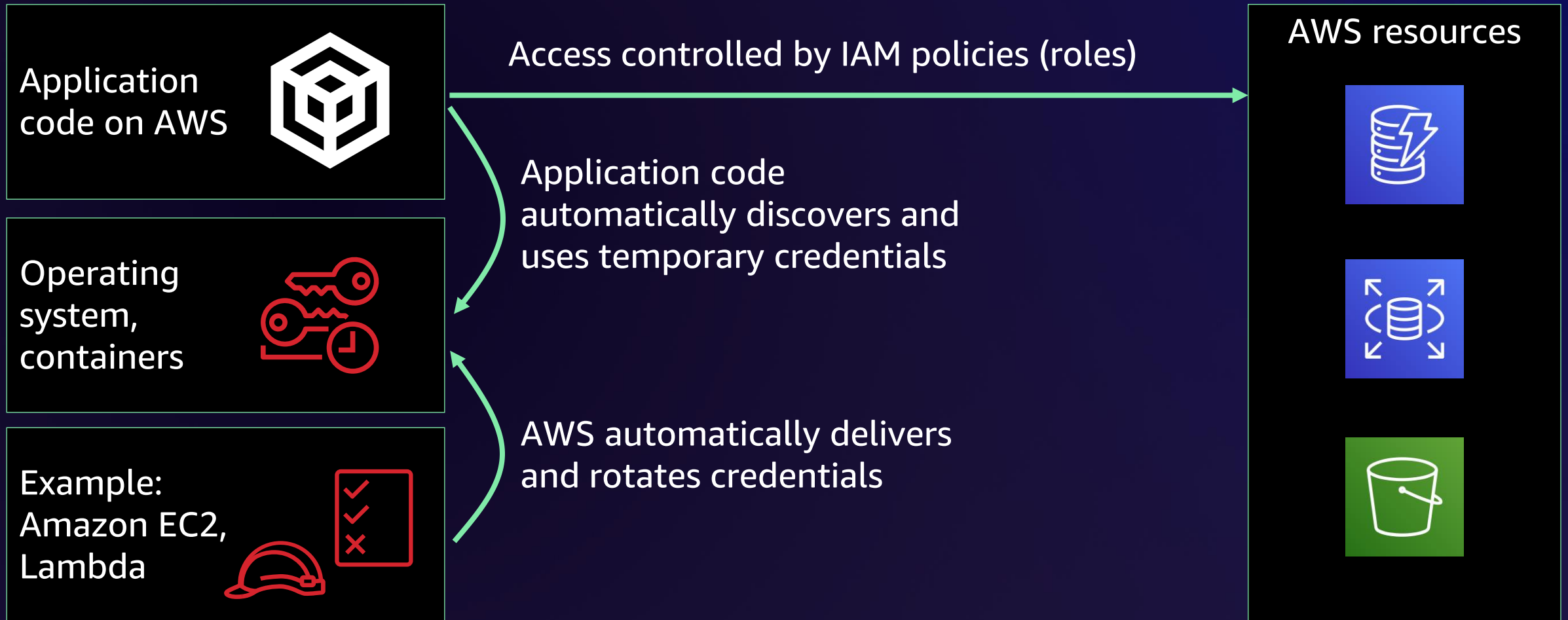
- Create SCP limiting who can create access keys

```
"Action": [ "iam:CreateUser", "iam:CreateAccessKey" ],  
"Resource": [ "*" ],  
"Effect": "Deny",  
"Condition":  
  { "StringNotEquals": { "aws:PrincipalARN": "arn:aws:iam::*:role/" } }
```

- Exceptions require tickets with justification and complete details – who the owner is, criticality, to which process it belongs, enforceable rotation
- Disable unused access keys; months later, if there are no complaints, eliminate

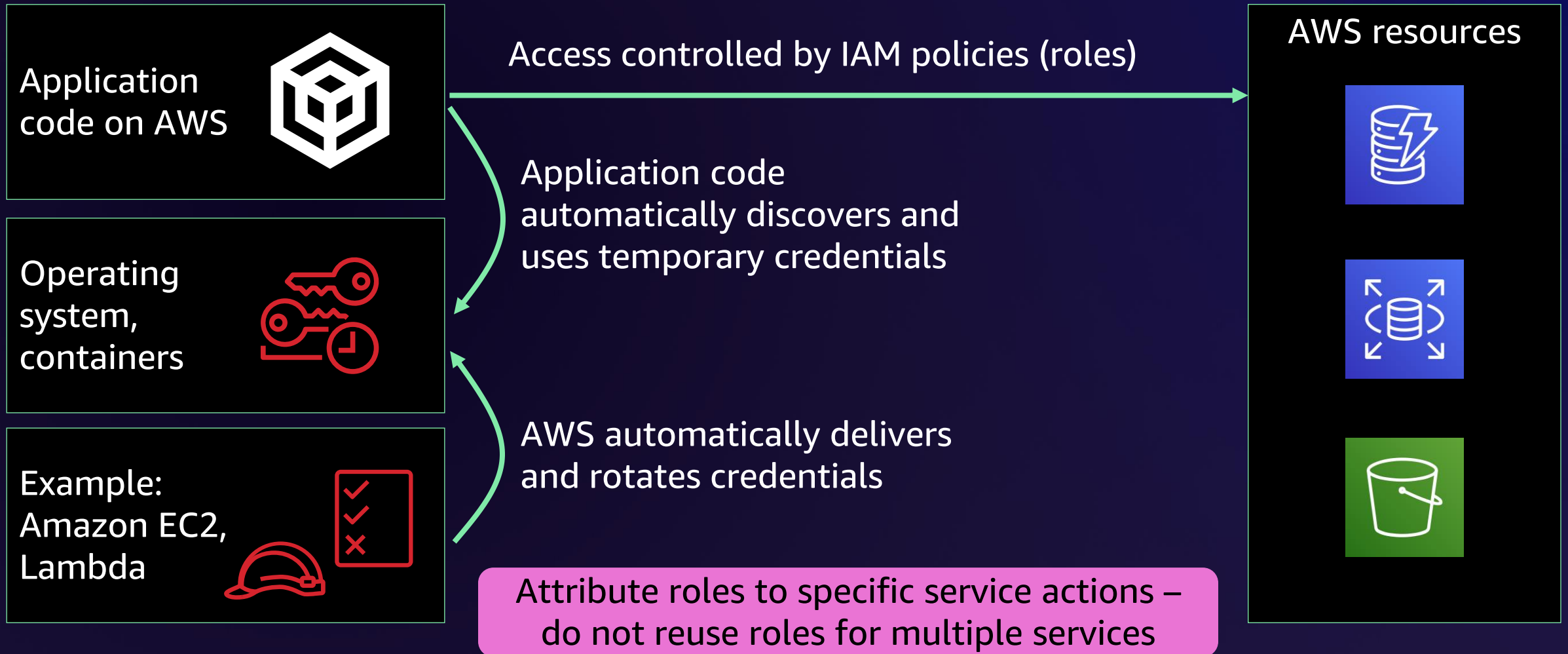
Temporary credentials for AWS-native use

USE OF AWS TEMPORARY CREDENTIALS WITH AWS SERVICES



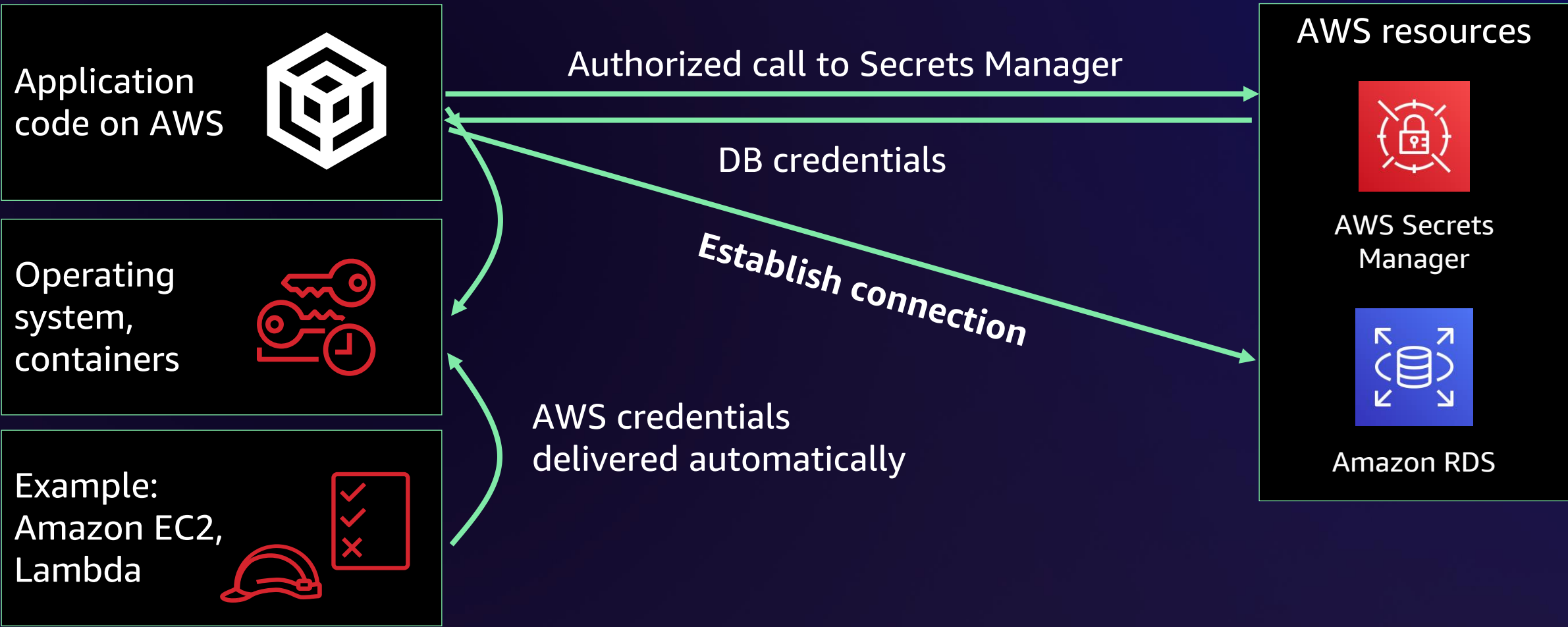
Temporary credentials for AWS-native use

USE OF AWS TEMPORARY CREDENTIALS WITH AWS SERVICES



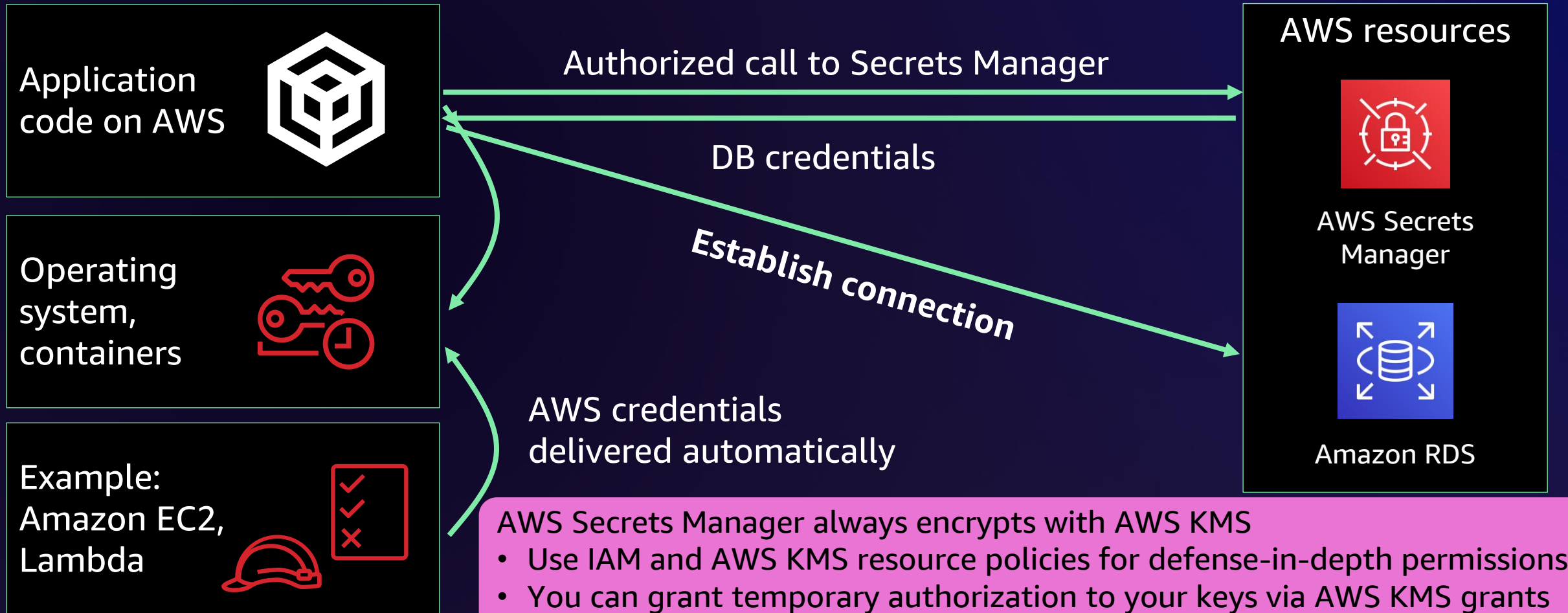
Credentials for non-AWS services

USING SHORT-TERM AWS CREDENTIALS FOR NON AWS SERVICES WITH AWS SECRETS MANAGER



Credentials for non-AWS services

USING SHORT-TERM AWS CREDENTIALS FOR NON AWS SERVICES WITH AWS SECRETS MANAGER



AWS Secrets Manager always encrypts with AWS KMS

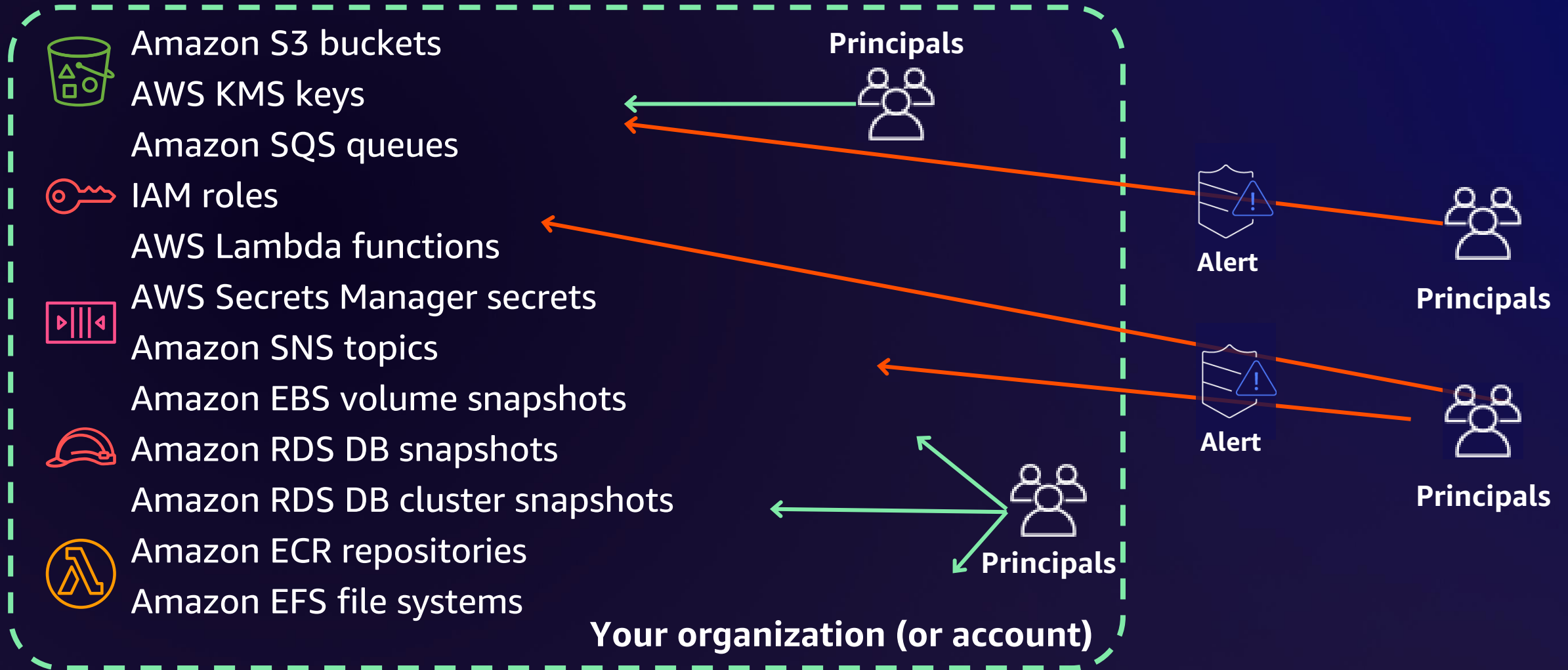
- Use IAM and AWS KMS resource policies for defense-in-depth permissions
- You can grant temporary authorization to your keys via AWS KMS grants without modifying IAM policies

Phase 2: IAM Foundations

1. Enforce security invariants using service control policies (SCPs)
2. Limit the use of IAM users and access keys to the absolute minimum
 - Use temporary credentials
 - Use IAM roles for your compute resources (i.e., Amazon EC2 instance profile, AWS Lambda execution roles)
3. Identify and delete unintended external permissions with IAM Access Analyzer

Identify & delete unintended external access

IAM ACCESS ANALYZER (NO ADDITIONAL COST)



Phase 3: Efficient



Phase 3: What are we talking about?

Phase 3: What are we talking about?

The screenshot shows the Gartner website page for 'Access Management Reviews and Ratings'. The page title is 'Products In Access Management Market'. It features a navigation bar with 'Overview', 'Products', and 'Gartner Research'. Below the title, there are filter options for 'Company Size', 'Industry', and 'Region'. The 'Company Size' filter is active, showing options: '<50M USD', '50M-1B USD', '1B-10B USD', '10B+ USD', and 'Gov't/PS/Ed'. The page displays 'Products 1 - 20 | View by Vendor' and 'Review weighting' options. The main content area features a product card for 'AWS Identity and Access Management (IAM) by Amazon Web Services (AWS)'. The card includes a 'Customers' Choice 2023' badge, a 4.5-star rating with 77 ratings, and a bar chart showing the distribution of ratings: 5 Star (61%), 4 Star (32%), 3 Star (5%), 2 Star (0%), and 1 Star (1%). The product description includes the quote: 'Improvise Security with comfort' and a highlighted sentence: 'AWS IAM is super easy to set up' and can be scaled up across multiple accounts with the help of SCPs under one organization and helps us easily manage our AWS Security. With the upcoming Security Lake ...

Star Rating	Percentage
5 Star	61%
4 Star	32%
3 Star	5%
2 Star	0%
1 Star	1%

Source: Gartner, 2023. Products in Access Management Market

Phase 3: What are we talking about?

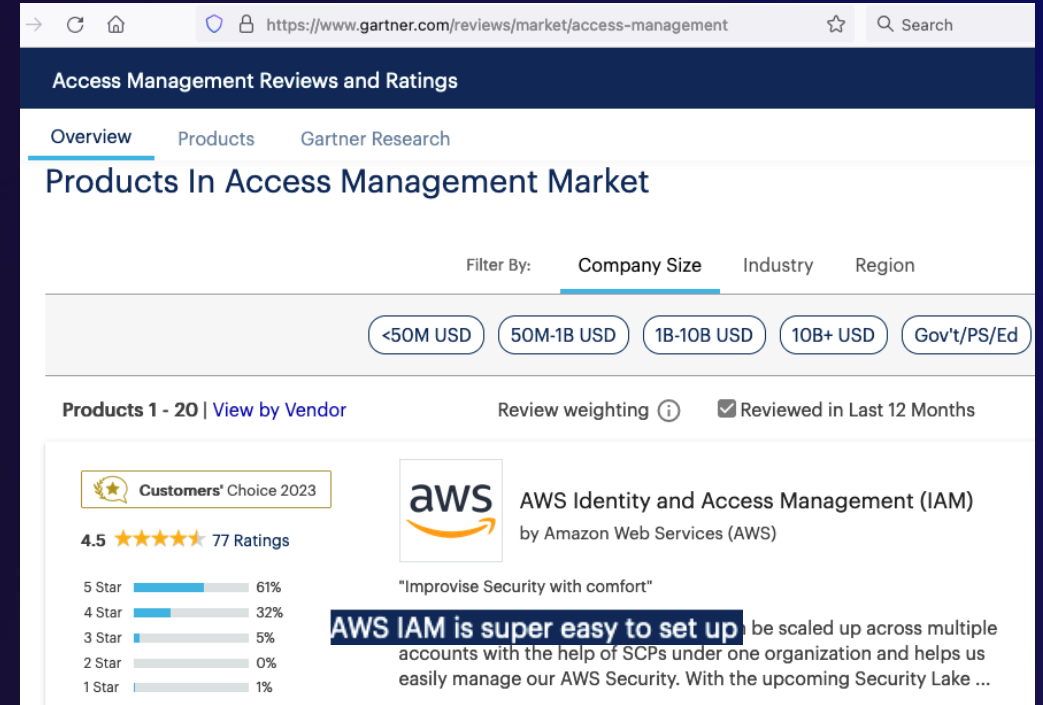
The screenshot shows the Gartner website page for 'Access Management Reviews and Ratings'. The page title is 'Products In Access Management Market'. The 'Filter By' section is set to 'Company Size', with options for '<50M USD', '50M-1B USD', '1B-10B USD', '10B+ USD', and 'Gov't/PS/Ed'. The 'Products 1 - 20 | View by Vendor' section shows 'AWS Identity and Access Management (IAM) by Amazon Web Services (AWS)'. The product has a 'Customers' Choice 2023' badge and a 4.5 star rating based on 77 ratings. A bar chart shows the distribution of ratings: 5 Star (61%), 4 Star (32%), 3 Star (5%), 2 Star (0%), and 1 Star (1%). A quote from a customer states: 'Improvise Security with comfort'. A highlighted text box says: 'AWS IAM is super easy to set up'. Below this, a snippet of text reads: 'be scaled up across multiple accounts with the help of SCPs under one organization and helps us easily manage our AWS Security. With the upcoming Security Lake ...'.

Star Rating	Percentage
5 Star	61%
4 Star	32%
3 Star	5%
2 Star	0%
1 Star	1%

Source: Gartner, 2023. Products in Access Management Market

Phase 3: What are we talking about?

Ease of use is directly proportionate to your knowledge and comfort with the tools you can use.



The screenshot shows the Gartner website page for "Access Management Reviews and Ratings". The page title is "Products In Access Management Market". The "Filter By" section is set to "Company Size" with options for "<50M USD", "50M-1B USD", "1B-10B USD", "10B+ USD", and "Gov't/PS/Ed". The "Products 1 - 20" section is displayed, with "View by Vendor" and "Reviewed in Last 12 Months" selected. The product shown is "AWS Identity and Access Management (IAM) by Amazon Web Services (AWS)". It has a "Customers' Choice 2023" badge and a 4.5-star rating based on 77 ratings. A bar chart shows the distribution of ratings: 5 Star (61%), 4 Star (32%), 3 Star (5%), 2 Star (0%), and 1 Star (1%). A quote from a customer states: "Improvise Security with comfort". A highlighted text box says: "AWS IAM is super easy to set up" followed by "be scaled up across multiple accounts with the help of SCPs under one organization and helps us easily manage our AWS Security. With the upcoming Security Lake ...".

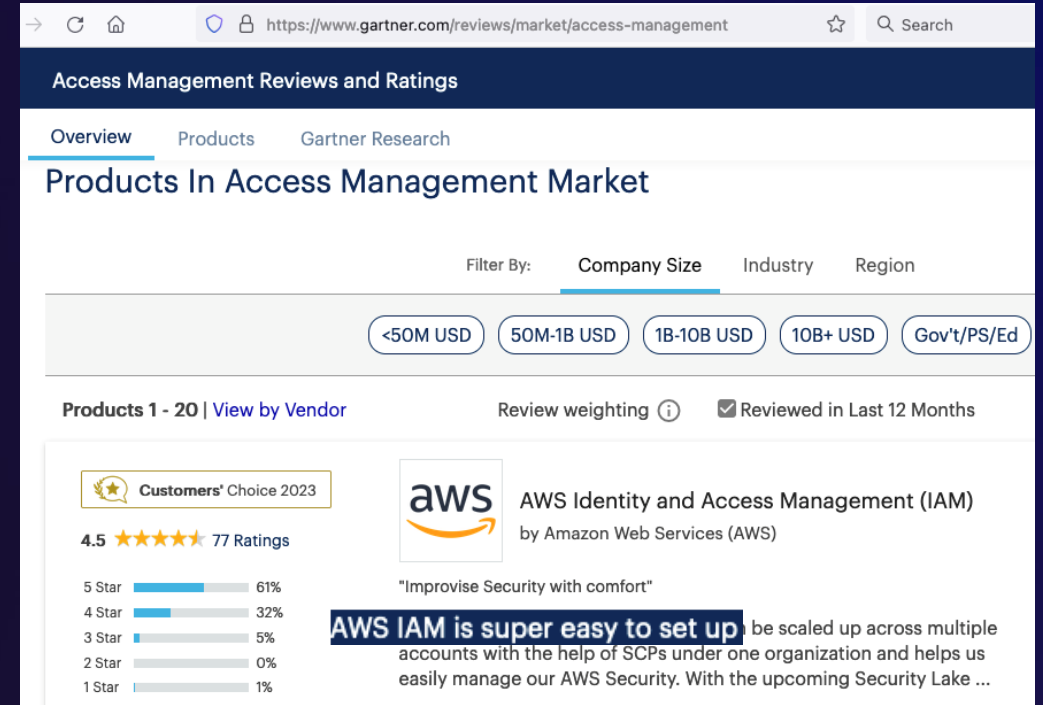
Star Rating	Percentage
5 Star	61%
4 Star	32%
3 Star	5%
2 Star	0%
1 Star	1%

Source: Gartner, 2023. Products in Access Management Market

Phase 3: What are we talking about?

Ease of use is directly proportionate to your knowledge and comfort with the tools you can use.

AWS security tools will help you with the undifferentiated heavy lift and work an "easy button" in your security efficiency journey.



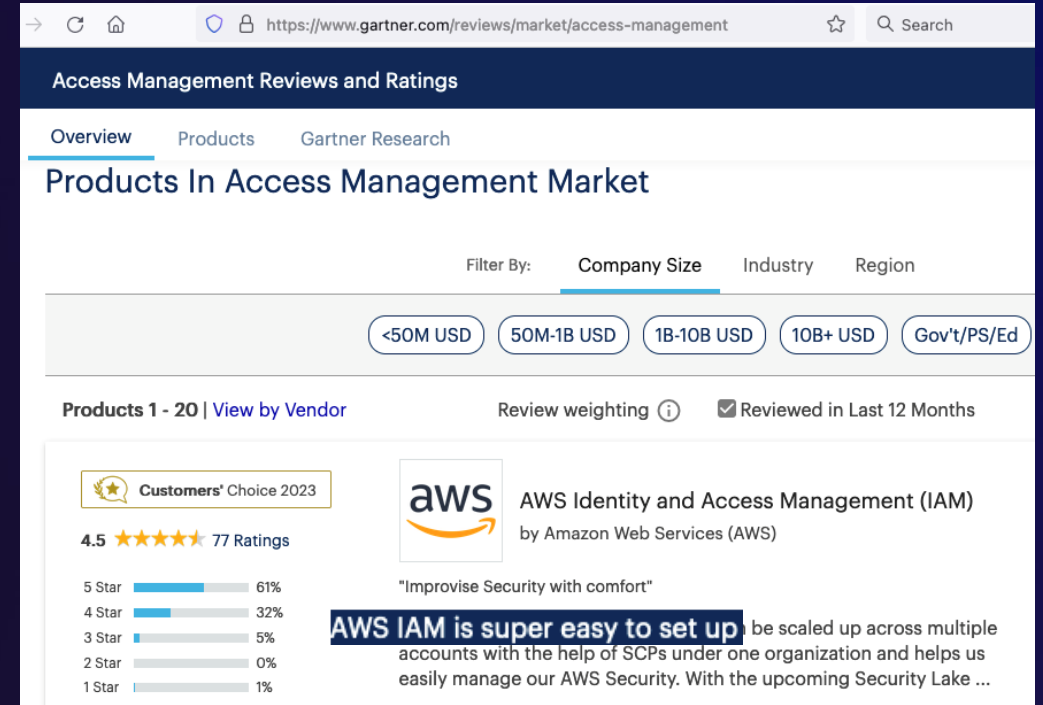
The screenshot shows the Gartner website page for "Access Management Reviews and Ratings". The page title is "Products In Access Management Market". The "Filter By" section is set to "Company Size" with options for "<50M USD", "50M-1B USD", "1B-10B USD", "10B+ USD", and "Gov't/PS/Ed". The "Products 1 - 20" section is displayed, showing "AWS Identity and Access Management (IAM) by Amazon Web Services (AWS)". The product has a "Customers' Choice 2023" badge and a 4.5 star rating based on 77 ratings. A star distribution chart shows: 5 Star (61%), 4 Star (32%), 3 Star (5%), 2 Star (0%), and 1 Star (1%). A quote from a customer states: "Improvise Security with comfort". A highlighted text box says: "AWS IAM is super easy to set up" followed by "be scaled up across multiple accounts with the help of SCPs under one organization and helps us easily manage our AWS Security. With the upcoming Security Lake ...".

Source: Gartner, 2023. Products in Access Management Market

Phase 3: What are we talking about?

Ease of use is directly proportionate to your knowledge and comfort with the tools you can use.

AWS security tools will help you with the undifferentiated heavy lift and work an "easy button" in your security efficiency journey.



Source: Gartner, 2023. Products in Access Management Market

Efficiency:

- Resources expended in relation to the accuracy and completeness with which users achieve their goals (NIST 800-55 R1)
- The ratio of useful work performed by a machine [...] (Oxford Dictionary)

Phase 3: IAM Efficient

1. Clean up what is not being used
 - Use IAM Access Advisor to remove unused access keys/permissions/roles
2. Clean up excessive permissions
 - Perform privilege reviews (work toward least privilege)
 - Leverage IAM Access Analyzer Policy Generation
3. Temporary credentials for external access
 - IAM Roles Anywhere
4. IAM as Code
 - Leverage versioning and infrastructure as code for IAM Policies

Phase 3: IAM Efficient

1. Clean up what is not being used

- Use IAM access advisor to remove unused access keys/permissions/roles

IAM access advisor: Delete unused permissions

Step 1: Identify unused access keys, roles and permissions

- Review the last activity date

Step 2: Disable/delete unused access keys, roles, and permissions

Access key ID	Created	Last used
AKIA[redacted]	2021-04-26 18:10 UTC-0300	2021-06-14 12:05

Identity and Access Management (IAM)

Summary

Creation date: December 02, 2021, 14:49 (UTC-03:00)

ARN: arn:aws:iam::[redacted]:role/amplify-login-lambda-[redacted]

Last activity: 7 months ago

Maximum session duration: 1 hour

Permissions | Trust relationships | Tags | **Access Advisor** | Revoke sessions

Access Advisor shows the services that this role can access and when those services were last accessed. Review this data to remove unused permissions. [Learn More](#)

Allowed services (1)

Access Advisor reports activity for services and EC2, IAM, Lambda, and S3 management actions. To view actions, choose the service name from the list. Recent service activity usually appears within 4 hours. Service activity is reported for the past 400 days. [Learn More](#)

Last accessed information is available for EC2, IAM, Lambda, and S3 management actions.

Service	Policies granting permissions	Last accessed
AWS Amplify	Amplify-backend	238 days ago

Identity and Access Management (IAM)

IAM > Roles

Roles (121) [Info](#) [Refresh](#) [Delete](#) [Create role](#)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search: amplify (8 matches)

<input type="checkbox"/>	Role name	Trusted entities	Last act...
<input type="checkbox"/>	amplify-amazonprimelearning-staging-[redacted]-authRole	None	-
<input type="checkbox"/>	amplify-amazonprimelearning-staging-[redacted]-unauthRole	None	-
<input type="checkbox"/>	amplify-login-lambda-11[redacted]	AWS Service: lambda	-
<input type="checkbox"/>	amplify-login-lambda-[redacted]-d9	AWS Service: lambda	237 days ago
<input type="checkbox"/>	amplify-primelearningamplify-staging-[redacted]-authRole	None	-
<input type="checkbox"/>	amplify-primelearningamplify-staging-131448-unauthRole	None	-
<input type="checkbox"/>	AmplifyDataStoreIAMRb752cd-ma2iqzcnibcalbyqkrptkb2le-staging	AWS Service: appsync	-



Phase 3: IAM efficient

1. Clean up what is not being used
 - Use IAM access advisor to remove unused access keys/permissions/roles
2. Clean up excessive permissions
 - Perform privilege reviews (work toward least privilege)
 - Use IAM Access Analyzer policy generation

Automatic activity-based policy generation

IAM ACCESS ANALYZER (NO ADDITIONAL COST)

Scenario: Development team doesn't create strong permissions

1. Configuration (e.g., 90 days)
2. Generate JSON policies from events in AWS CloudTrail
3. Review and customize the policy with minimum privilege
4. Create and associate the policy

Generated policy

Review and create managed policy

Review the permissions summary, add tags, and create the generated policy as a customer managed policy

Name*

Use alphanumeric and '+=, @-_' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Summary

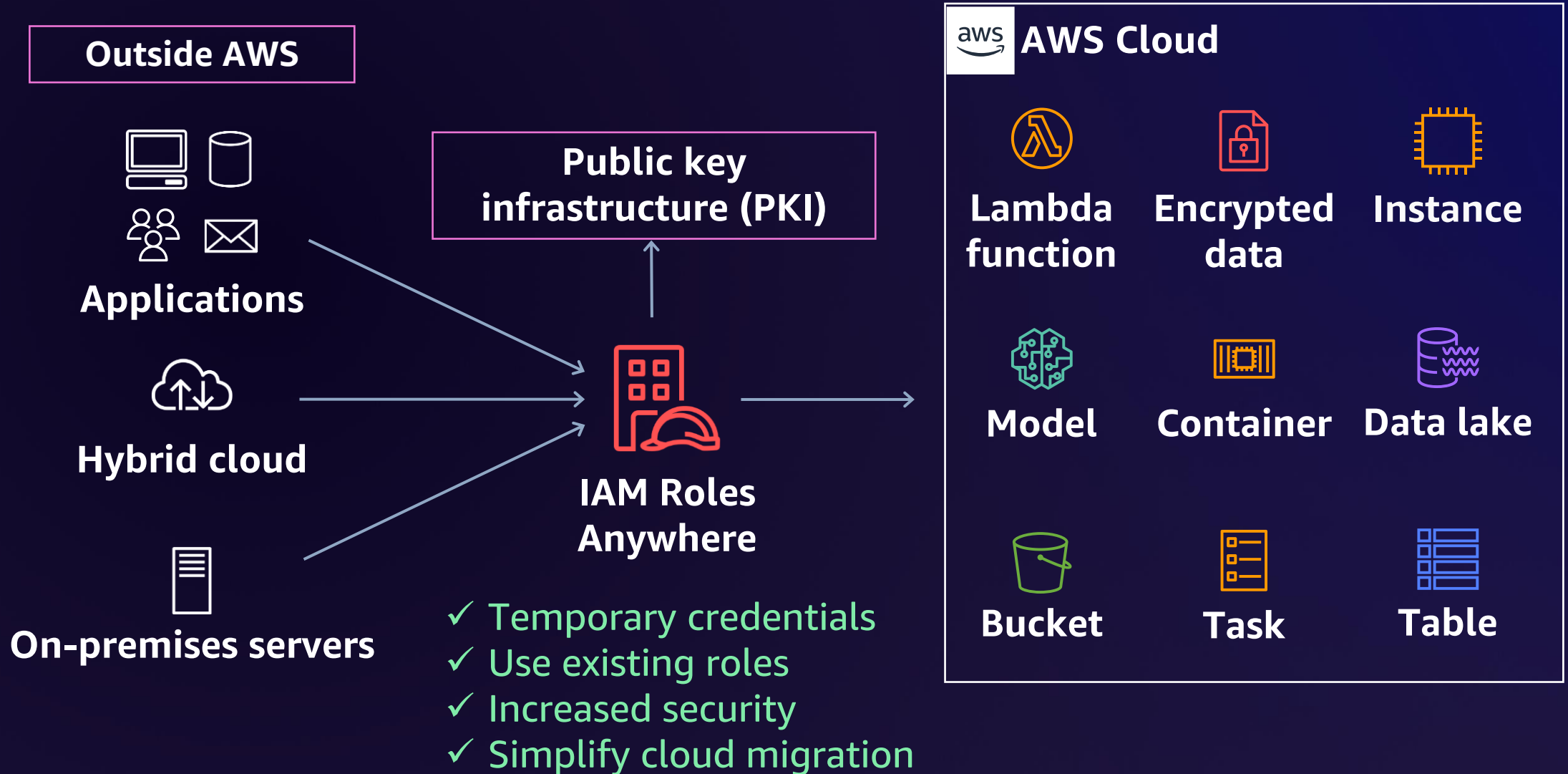
Service	Access level	Resource
Allow (7 of 299 services) Show remaining 292		
CloudFormation	Limited: List	StackName string like All
CloudWatch Logs	Limited: Write	LogGroupName string like All
EC2	Limited: List	All resources
Resource Group Tagging	Limited: Read	All resources
Resource Groups	Limited: List	arn:aws:resource-groups:us-west-2:██████████:group/Pickles-Pasture
S3	Limited: Read	BucketName string like All
Secrets Manager	Limited: Read	arn:aws:secretsmanager:us-west-2:██████████:secret:*

Phase 3: IAM efficient

1. Clean up what is not being used
 - Use IAM access advisor to remove unused access keys/permissions/roles
2. Clean up excessive permissions
 - Perform privilege reviews (work toward least privilege)
 - Use IAM Access Analyzer policy generation
3. Temporary credentials for external access
 - IAM Roles Anywhere
 - AWS IoT Core

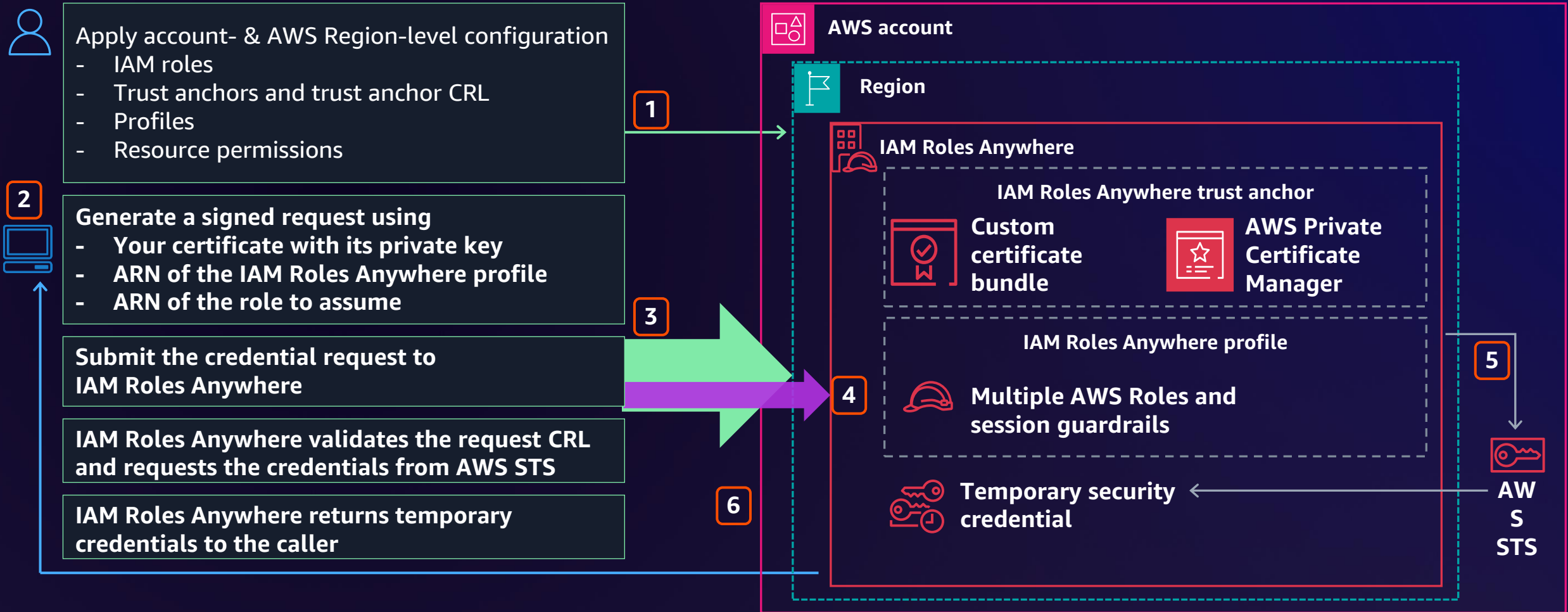
IAM Roles Anywhere

EXTEND THE USE OF IAM ROLES TO WORKLOADS OUTSIDE OF AWS



IAM Roles Anywhere

SIMPLIFIED FLOW DIAGRAM



IAM policies with IAM Roles Anywhere

USING UNIQUE FEATURES OF IAM ROLES ANYWHERE

IAM Roles Anywhere maps your certificate's X.509 subject and subject alternative name into principal tags

You can use principal tags within your trust policies, grant, or guardrails policies

IAM policies with IAM Roles Anywhere

USING UNIQUE FEATURES OF IAM ROLES ANYWHERE

IAM Roles Anywhere maps your certificate's X.509 subject and subject alternative name into principal tags

```
"Condition": {  
  "StringEquals": {  
    "aws:PrincipalTag/x509SAN/DNS": "example.com",  
    "aws:PrincipalTag/x509SAN/Name/CN": "Alice"  }  
  }  
}
```

You can use principal tags within your trust policies, grant, or guardrails policies

IAM policies with IAM Roles Anywhere

USING UNIQUE FEATURES OF IAM ROLES ANYWHERE

IAM Roles Anywhere maps your certificate's X.509 subject and subject alternative name into principal tags

You can use principal tags within your trust policies, grant, or guardrails policies

```
"Condition": {
  "StringEquals": {
    "aws:PrincipalTag/x509SAN/DNS": "example.com",
    "aws:PrincipalTag/x509SAN/Name/CN": "Alice" }
}
```

```
"Condition": {
  "StringEquals": {
    "aws:PrincipalTag/x509subject/CN": "Alice" }
}
```

Practical use notes

FOR USE OF AWS TEMPORARY CREDENTIAL

- Use PKI strengths
 - Attribute role assumptions to specific workloads – use certificate per workload
 - Expire your certificates per your business and security needs
 - Automate your CA's CRL publication to your IAM Roles Anywhere CRL store
- Limit the scope for role assumption
 - Use conditions in your IAM role trust policy to specify what entity can assume the role
 - Use conditions in your IAM Roles Anywhere session policy to set guardrails

Phase 3: IAM efficient

1. Clean up what is not being used
 - Use IAM Access Advisor to remove unused access keys/permissions/roles
2. Clean up excessive permissions
 - Perform privilege reviews (work toward least privilege)
 - Use IAM Access Analyzer policy generation
3. Temporary credentials for external access
 - IAM Roles Anywhere
4. IAM as code
 - Use versioning and infrastructure as code for IAM policies

Phase 4: Optimized



Phase 4: IAM Optimized

1. Delegate permission management

- Let developers safely create roles and get out of their way
- IAM Pipeline: Establishing a process to create roles

2. Analyze CloudTrail for proper access

- Denied actions are great signals of a misconfiguration or malicious activity

3. Establish a data perimeter

4. Restrict access using Zero Trust principles

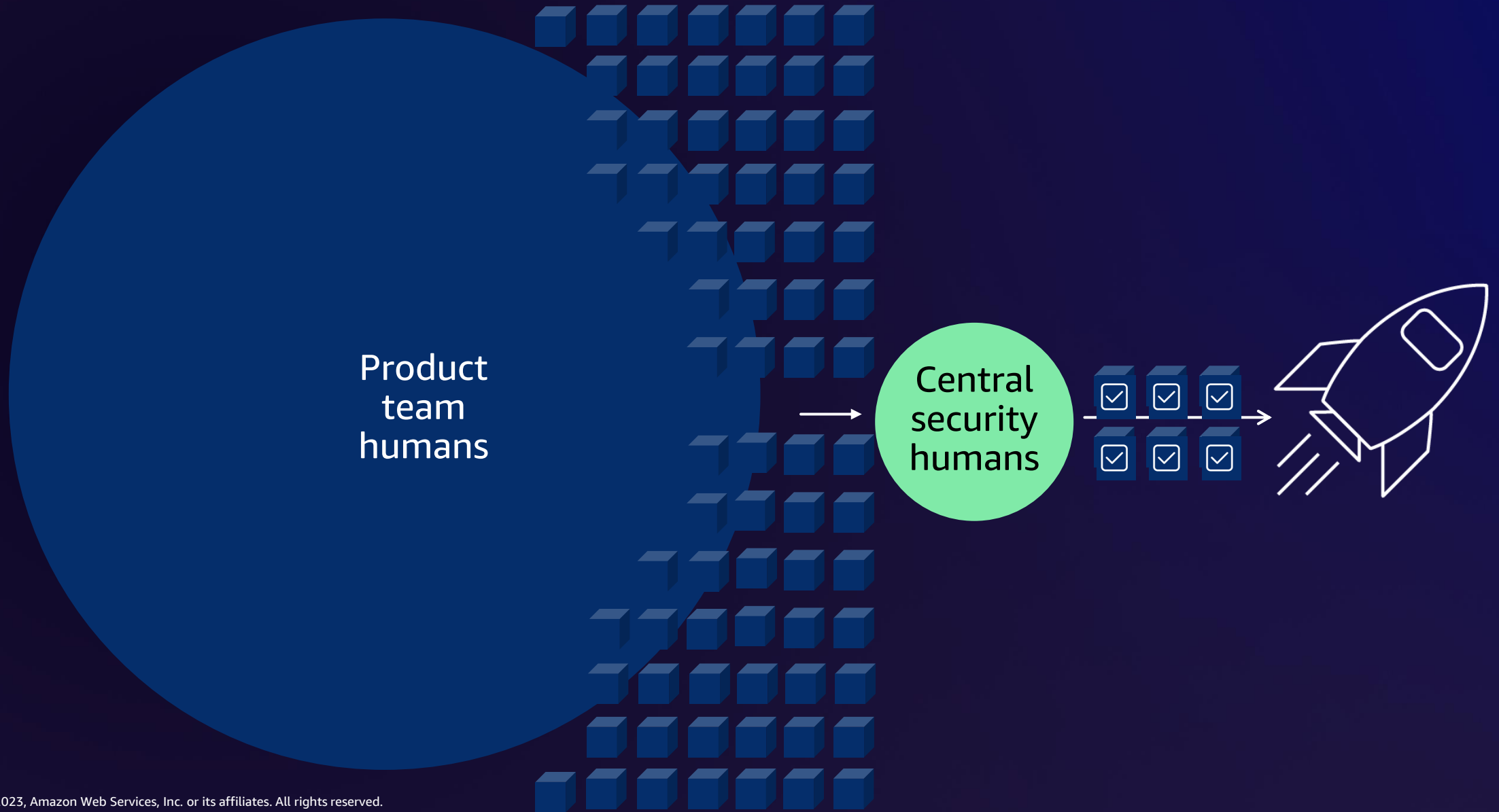
- Limited time authorization
Check out Temporary Elevated Access Management ([TEAM](https://aws-samples.github.io/iam-identity-center-team)) solution
<https://aws-samples.github.io/iam-identity-center-team>

Phase 4: IAM Optimized

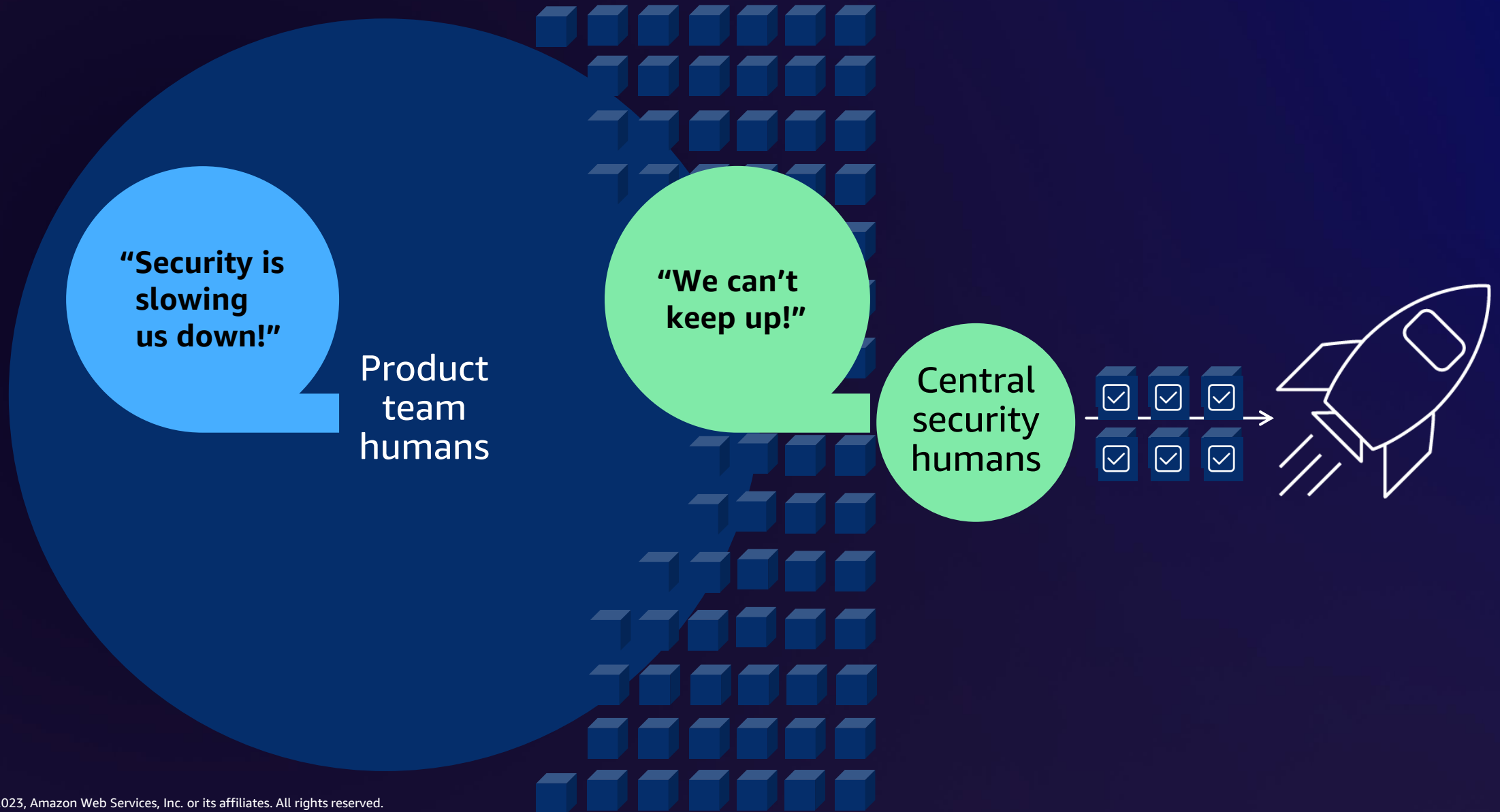
1. Delegate permission management

- Let developers safely create roles, and then get out of their way
- IAM pipeline – establishing a process to create roles

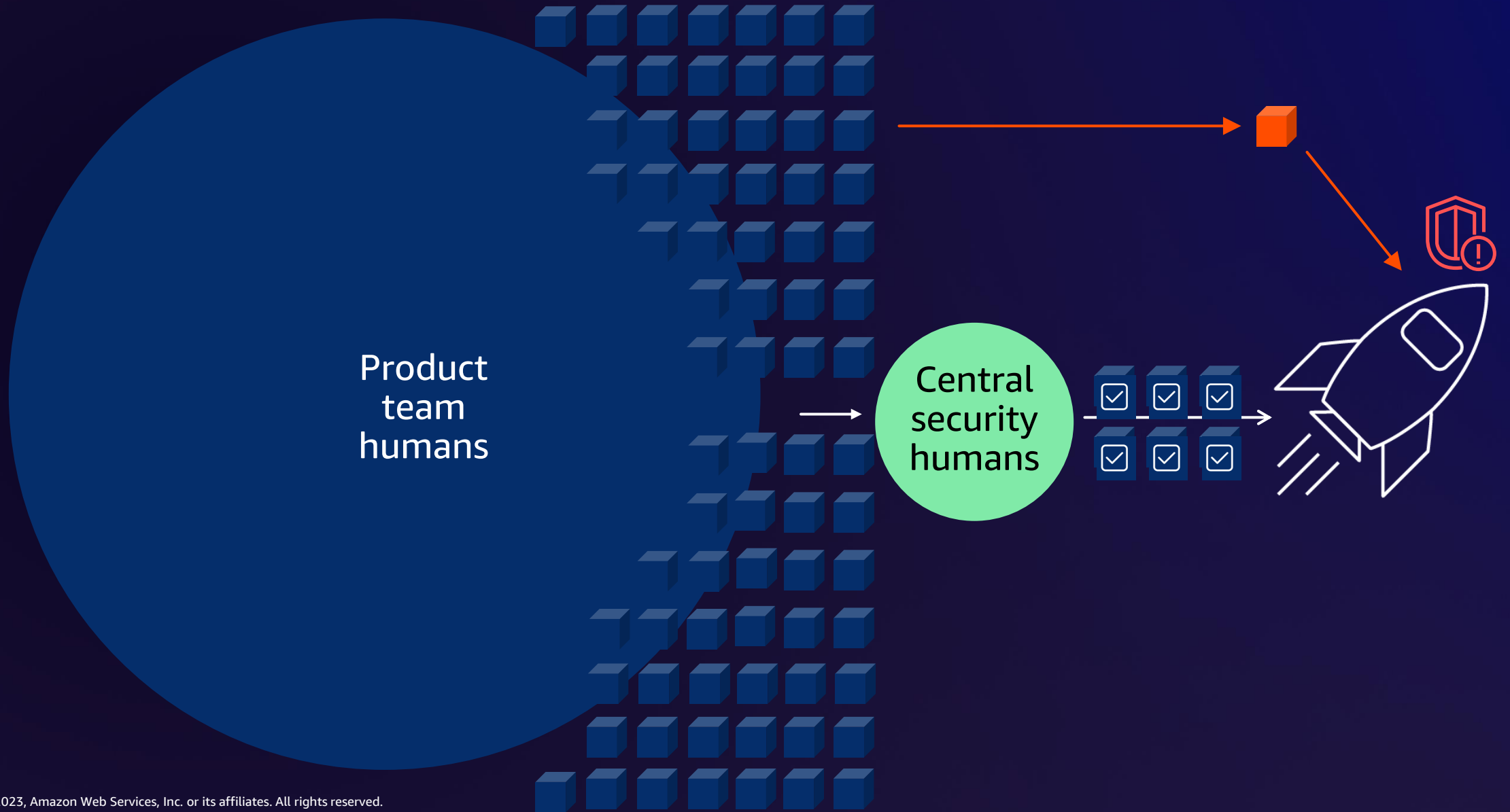
A challenge with scaling security: Humans



A challenge with scaling security: Humans



A challenge with scaling security: Humans



**Let developers safely create roles,
and then get out of their way**



Let developers safely create roles, and then get out of their way



**Dev creates
initial draft**

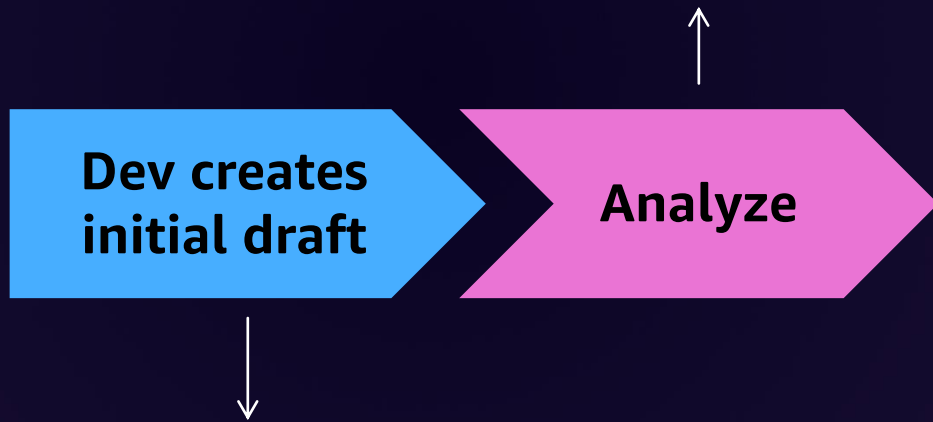


Developers create initial draft
of the policy

Leverage SCPs and permission
boundaries to limit maximum
permissions

Let developers safely create roles, and then get out of their way

Analyze the policy to ensure
that there are no risks
(IAM Access Analyzer)



Developers create initial draft
of the policy

Leverage SCPs and permission
boundaries to limit maximum
permissions

Let developers safely create roles, and then get out of their way

Analyze the policy to ensure that there are no risks (IAM Access Analyzer)



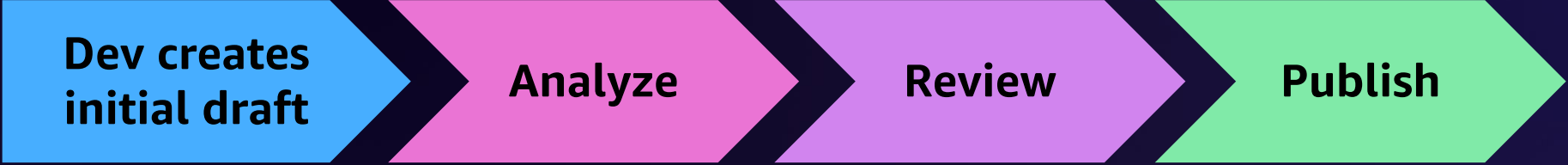
Developers create initial draft of the policy
Leverage SCPs and permission boundaries to limit maximum permissions

If risky/excessive permissions are requested, the security team reviews

Let developers safely create roles, and then get out of their way

Analyze the policy to ensure that there are no risks (IAM Access Analyzer)

Create the policy/roles



Developers create initial draft of the policy
Leverage SCPs and permission boundaries to limit maximum permissions

If risky/excessive permissions are requested, the security team reviews



Let developers safely create roles, and then get out of their way

Analyze the policy to ensure that there are no risks (IAM Access Analyzer)

Create the policy/roles



Developers create initial draft of the policy
Leverage SCPs and permission boundaries to limit maximum permissions

If risky/excessive permissions are requested, the security team reviews

Analyze 30-/90-day usage, and propose a reduction of unused permissions to developer

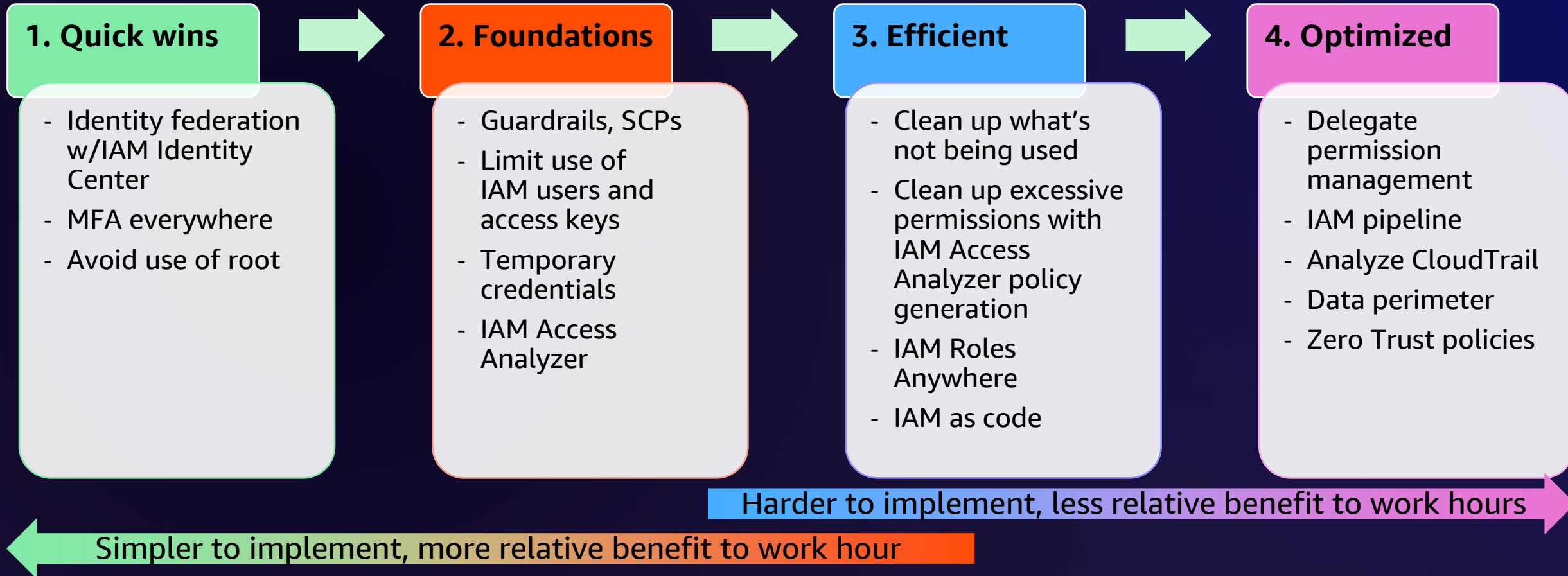
Phase 4: IAM Optimized

1. Delegate permission management
 - Let developers safely create roles and get out of their way
 - IAM pipeline – establishing a process to create roles
2. Analyze CloudTrail for proper access
 - Denied actions are great signals of a misconfiguration or malicious activity
3. Establish a data perimeter
4. Restrict access using Zero Trust principles
 - Limited time authorization
Check out Temporary Elevated Access Management ([TEAM](#)) solution
<https://aws-samples.github.io/iam-identity-center-team>

Conclusions



AWS identity strategy: How to prioritize



Note: This is different for each customer's situation; this is our general advice based on our experience

Related sessions

IDENTITY & ACCESS MANAGEMENT

IAM301: Establishing a data perimeter on AWS, featuring USAA

IAM302: Create enterprise-wide preventive guardrails, featuring Inter & Co

IAM305: Scaling access in IAM Identity Center, feat. Allegiant Airlines

IAM306: Managing hybrid workloads with IAM Roles Anywhere, featuring Hertz

IAM307: Steps towards a Zero Trust architecture on AWS

IAM331-R/-R1: Leaving static access keys behind: A modern path forward

Additional resources



[AWS Security Maturity Model](#): Security recommendations prioritized and categorized with concise explanations



[Blog post: IAM Access Analyzer makes it easier to implement least privilege permissions by generating IAM policies based on access activity](#)



[Blog post: Use IAM Access Analyzer to generate IAM policies based on access activity found in your organization trail](#)



[Blog post: Establishing a data perimeter on AWS](#)
Step-by-step instructions on how to establish a data perimeter using IAM conditions

Thank you!

Dario Goldfarb

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

Arthur Mnev

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



Please complete
the session survey
in the mobile app