

Module 4:

Secure your cloud applications

Sander Veenstra
Technical Trainer
AWS





Secure your infrastructure

Security is our top priority



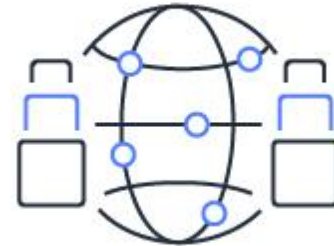
Designed for
security



Constantly
monitored



Highly
automated



Highly
available



Highly
accredited

Security of the cloud

- Hosts, network, software, facilities
- Protection of the AWS global infrastructure is top priority
- Availability of third-party audit reports

AWS

Foundation services

Compute

Storage

Database

Network

AWS global
infrastructure

Availability Zones

Regions

Edge Locations

Security in the cloud

Customer

Customer data

Platform, applications, identity & access management

Operating system, network & firewall configuration

Client-side data encryption &
Data integrity authentication

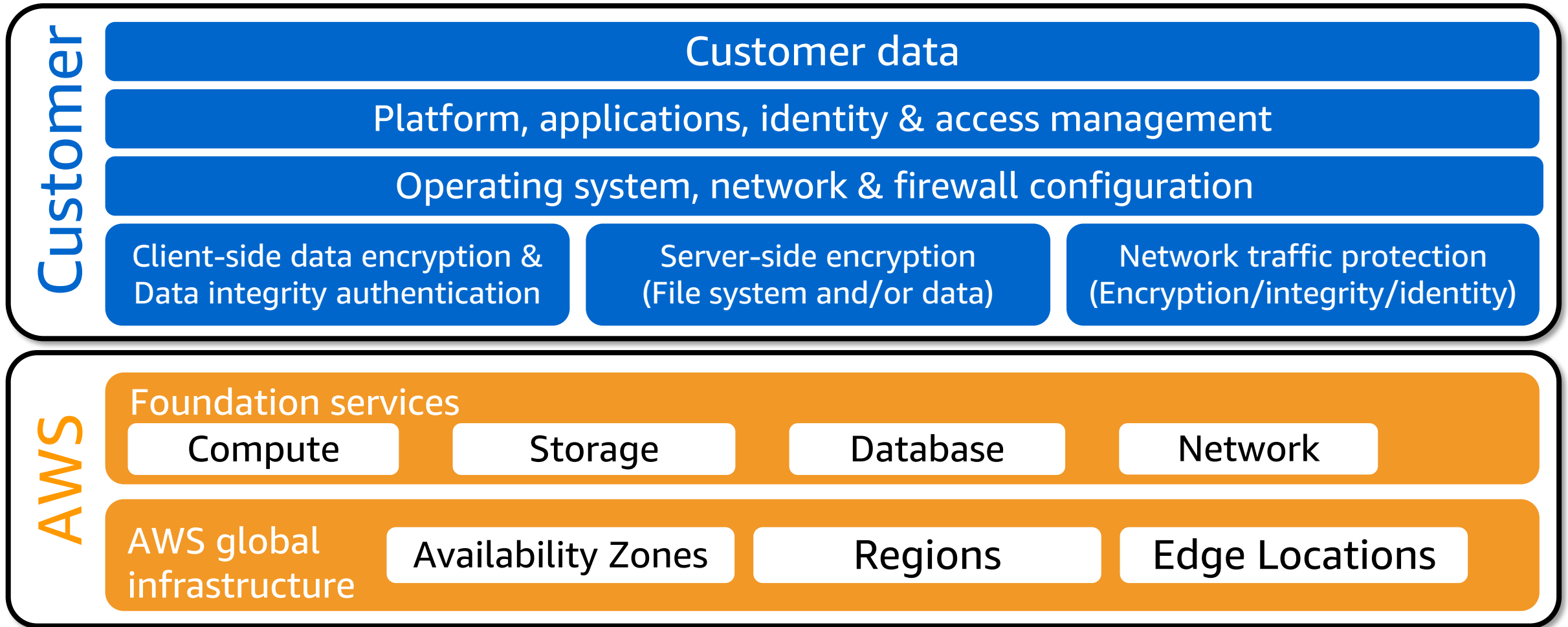
Server-side encryption
(File system and/or data)

Network traffic protection
(Encryption/integrity/identity)

Considerations

- What you should store
- Which AWS services you should use
- Which Region to store in
- In what content format and structure
- Who has access

AWS shared responsibility model



Security, identity, and compliance products

AWS Artifact

AWS Certificate Manager

Amazon Cloud Directory

AWS CloudHSM

Amazon Cognito

AWS Directory Service

AWS Firewall Manager

Amazon GuardDuty

**AWS Identity and Access
Management**

Amazon Inspector

AWS Key Management
Service

Amazon Macie

AWS Organizations

AWS Shield

AWS Secrets Manager

AWS Single Sign-On

AWS WAF



Manage authentication and authorization

AWS Identity and Access Management (IAM)

Securely control access to AWS resources



IAM user

A person or application that interacts with AWS



Group

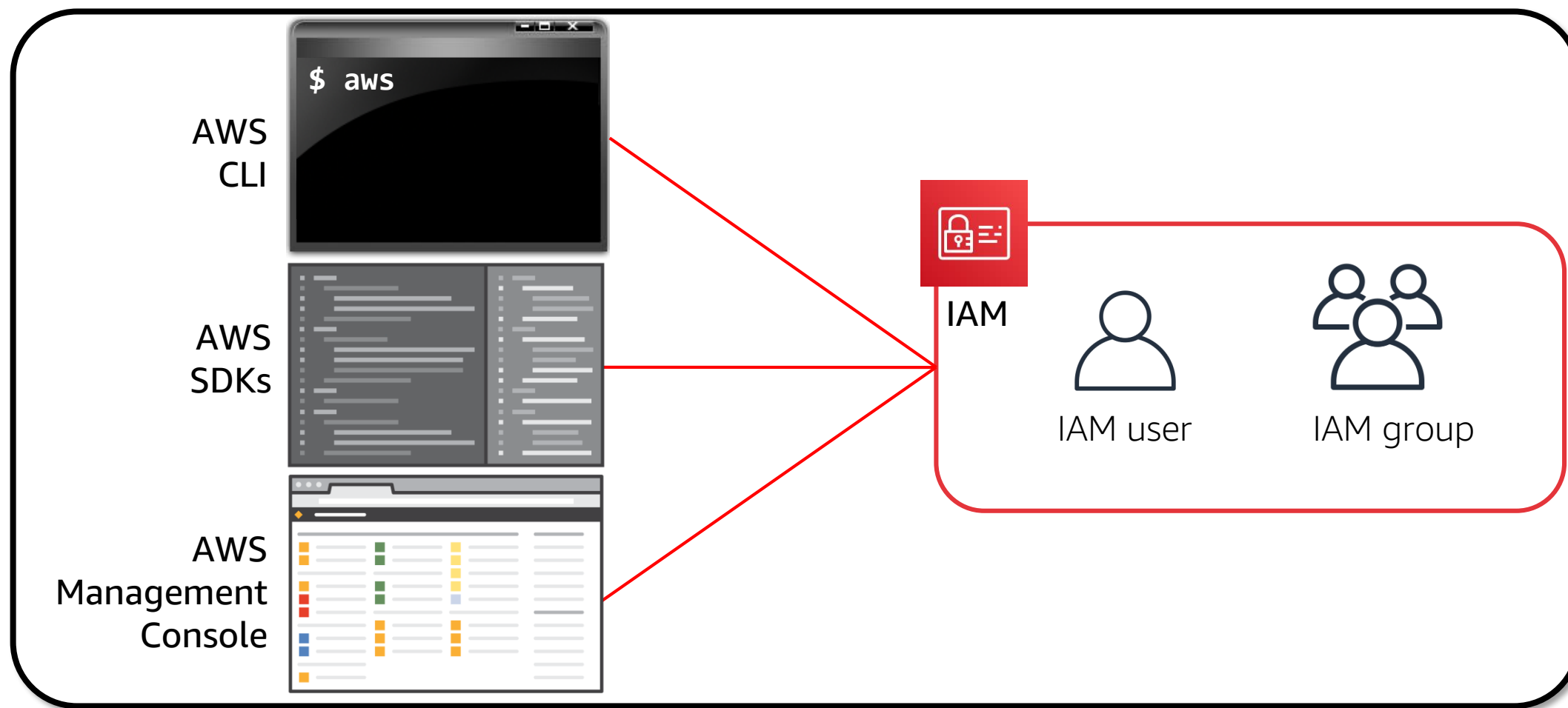
Collection of users with identical permissions



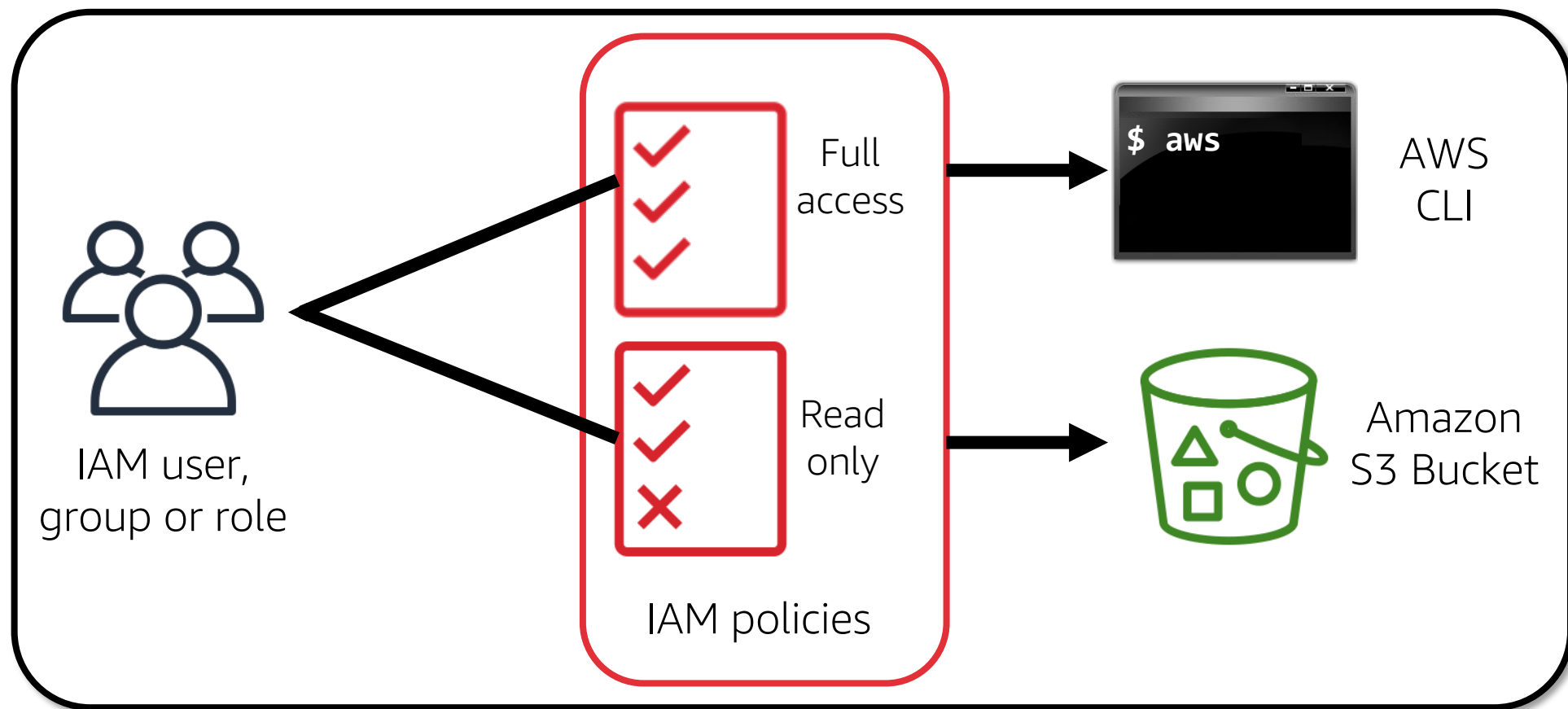
Role

Temporary privileges that an entity can assume

Authentication: Who are you?



Authorization: What can you do?



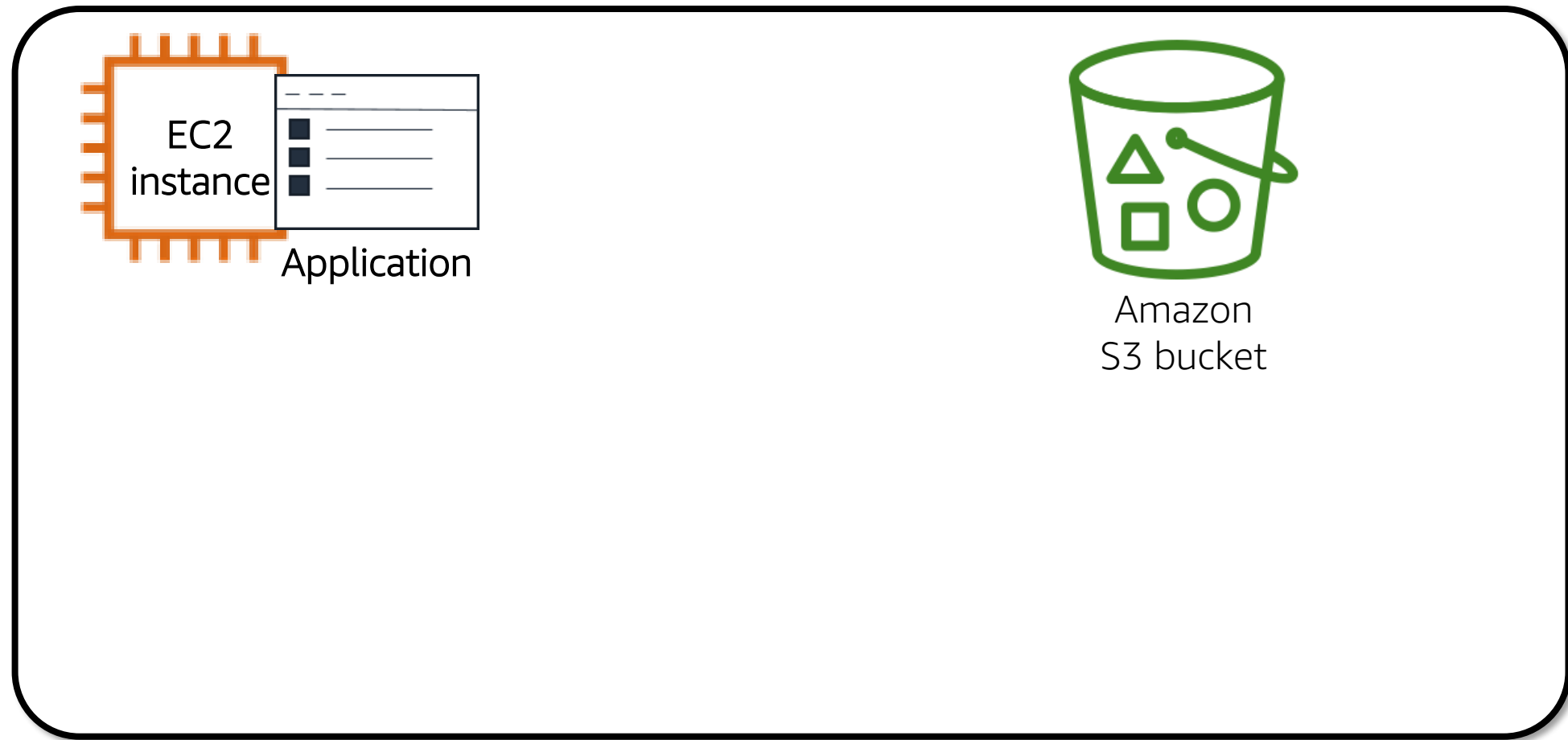
IAM roles



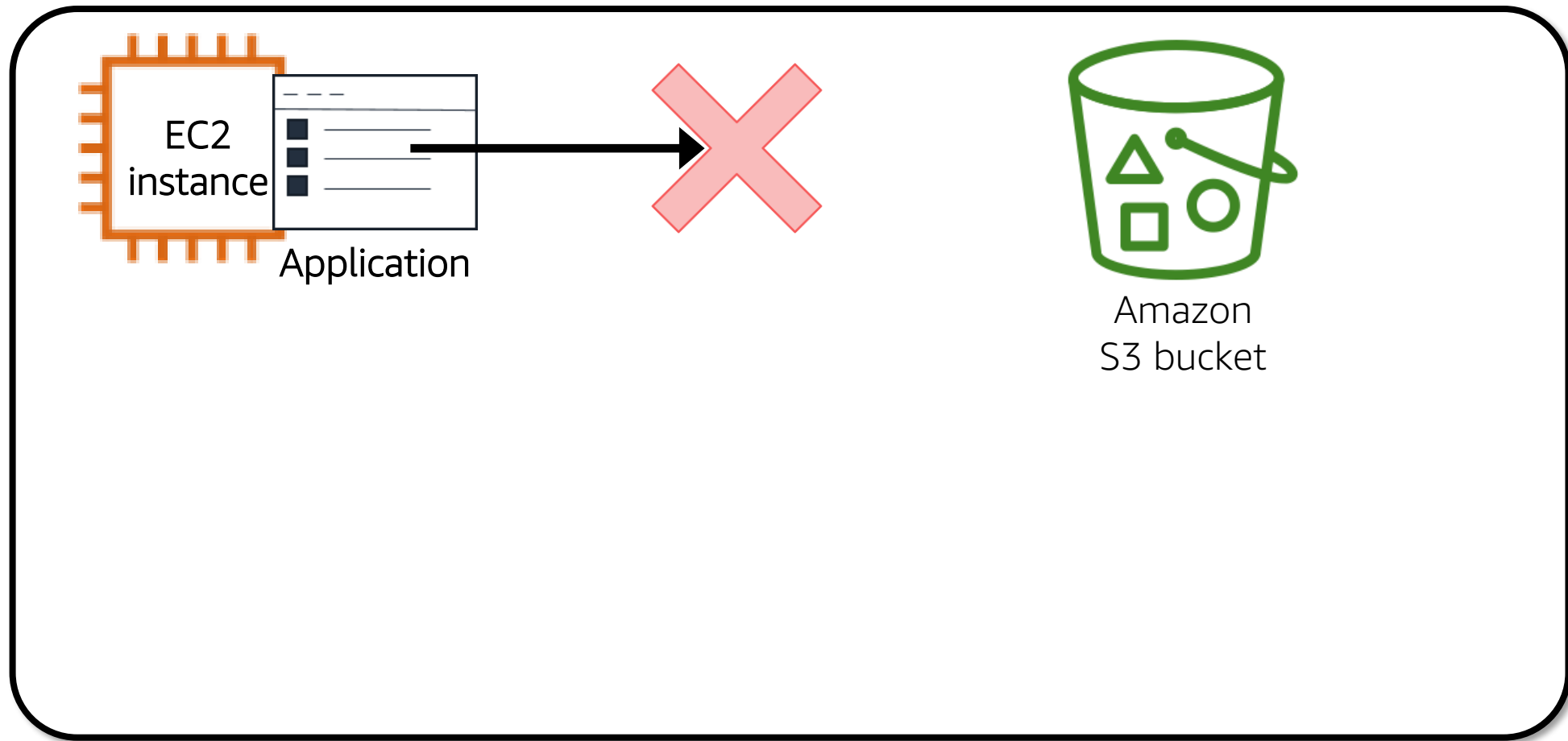
IAM role

- IAM users, applications, and services may assume IAM roles
- Roles use an IAM policy for permissions

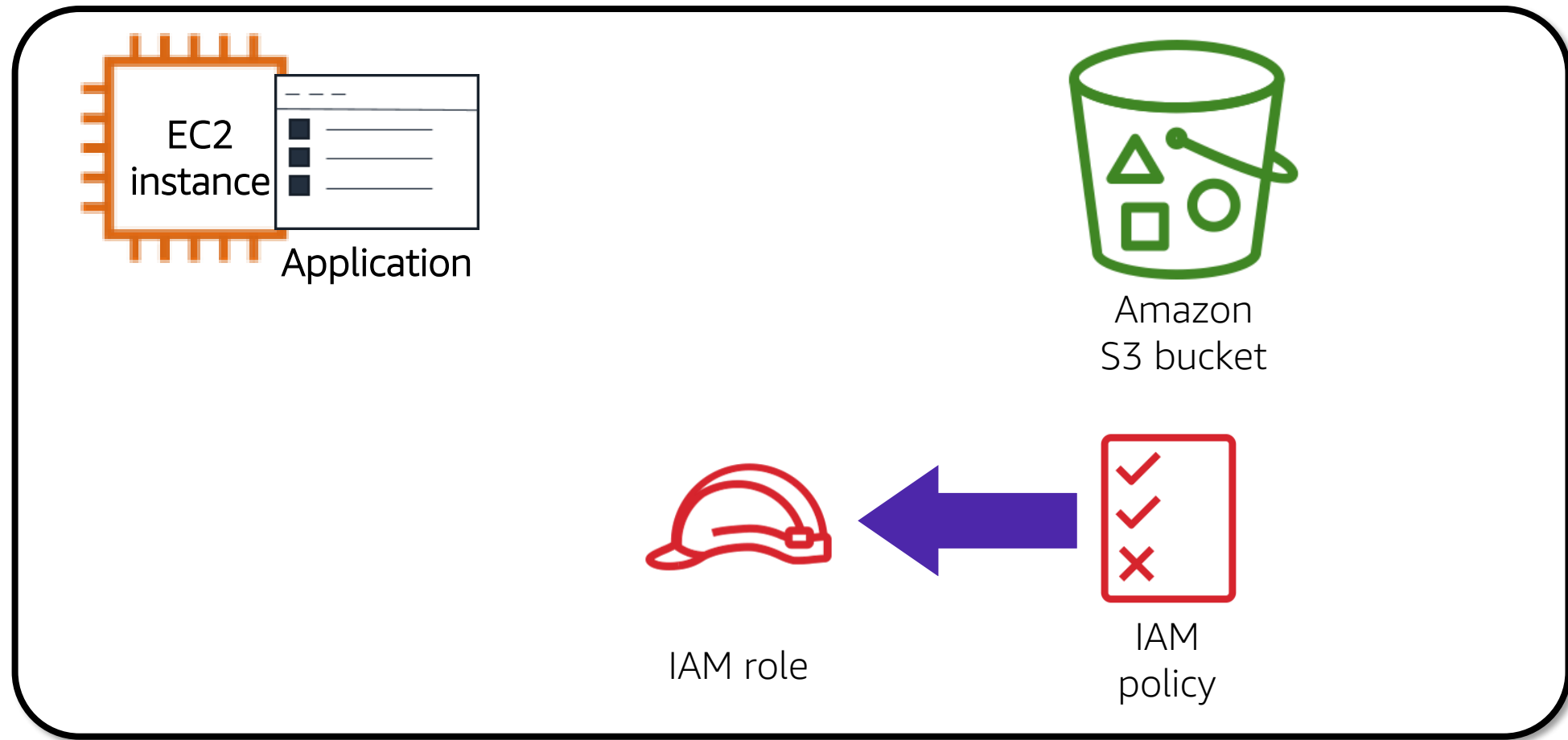
Using roles for temporary security credentials



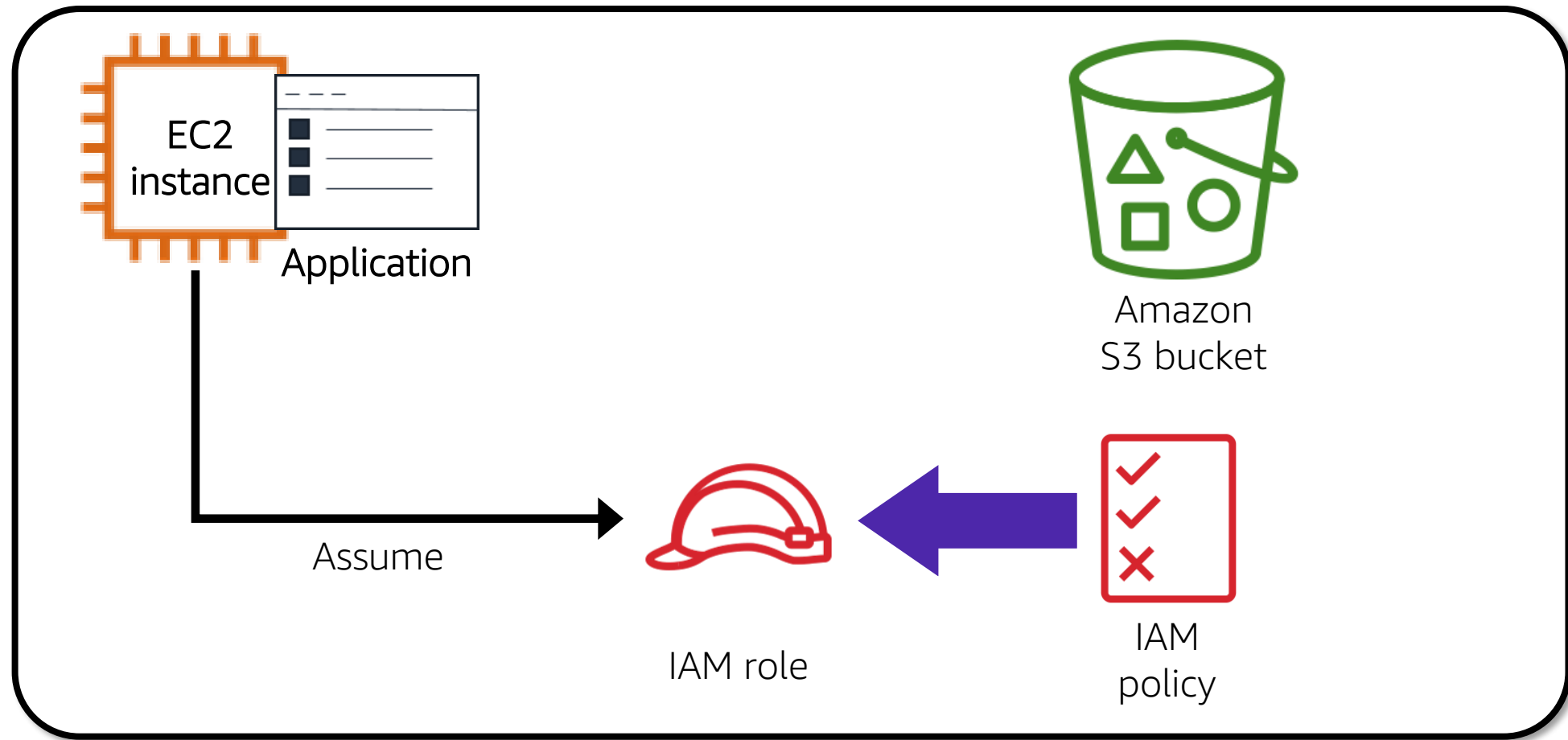
Using roles for temporary security credentials



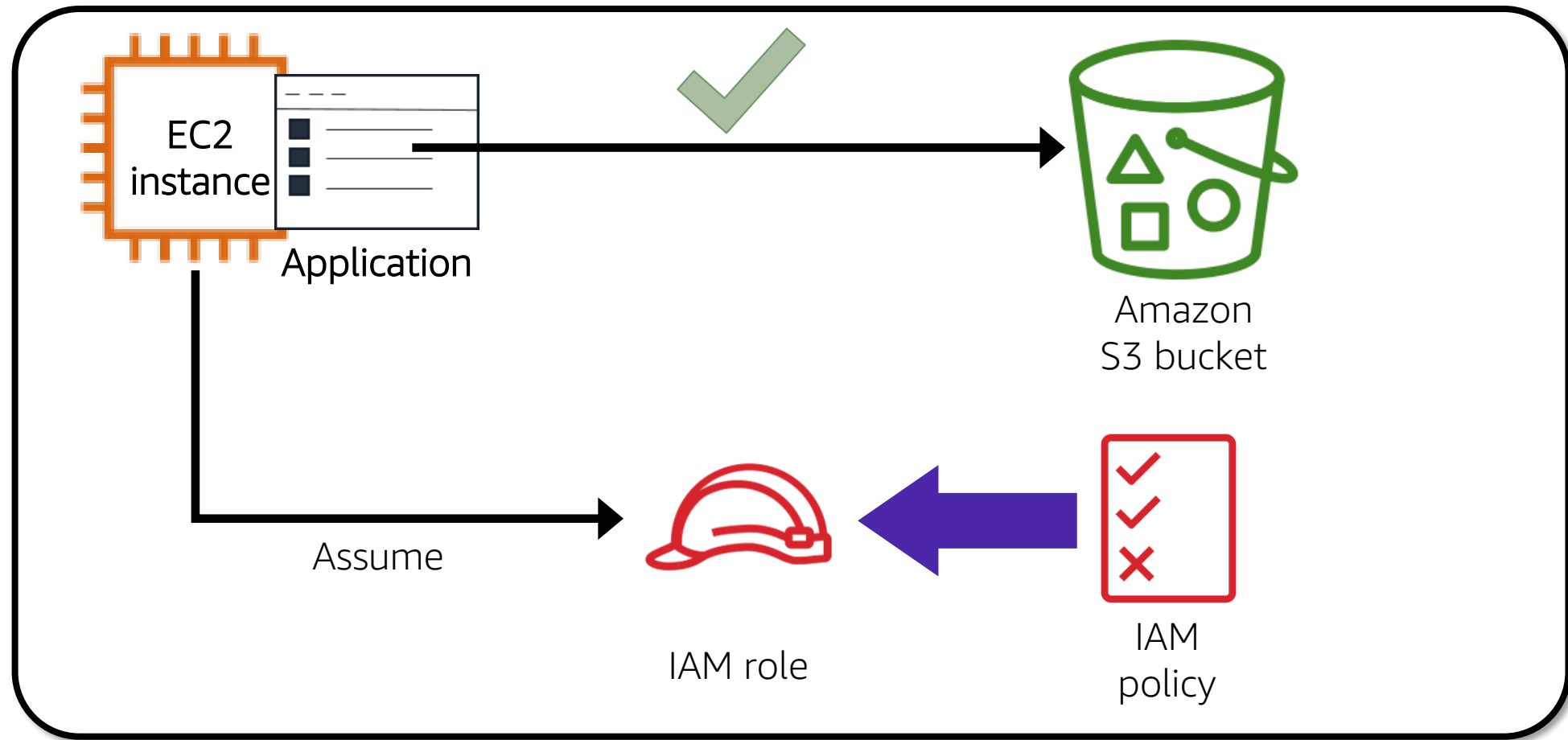
Using roles for temporary security credentials



Using roles for temporary security credentials



Using roles for temporary security credentials



Demo

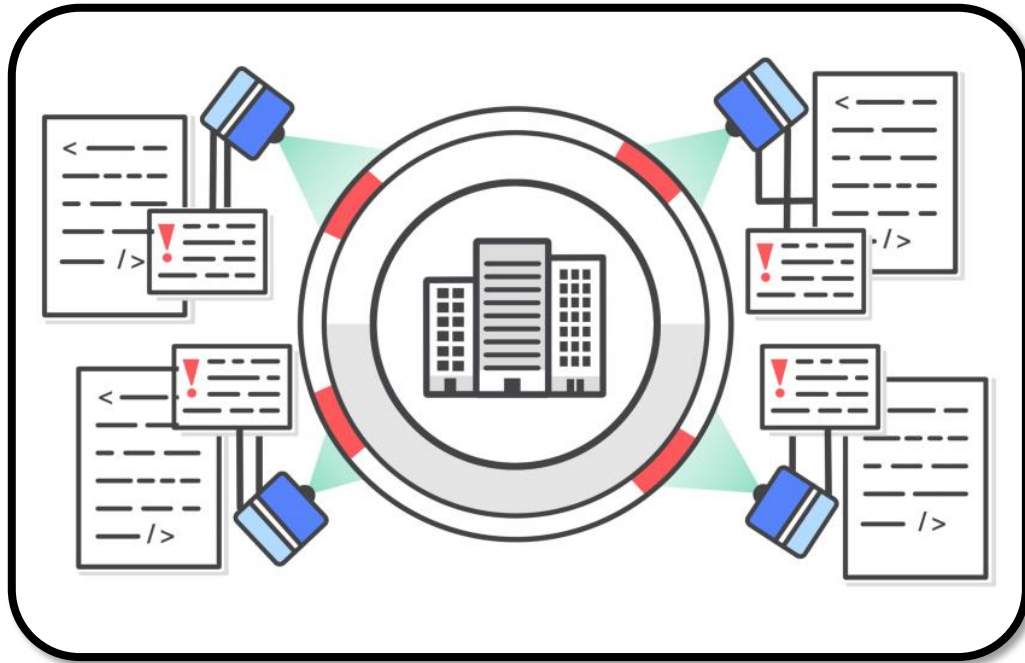
Best practices

- Delete access keys for the AWS account root user
- Activate multi-factor authentication (MFA)
- Only give IAM users permissions they need
- Use roles for applications
- Rotate credentials regularly
- Remove unnecessary users and credentials
- Monitor activity in your AWS account



Access your security and compliance

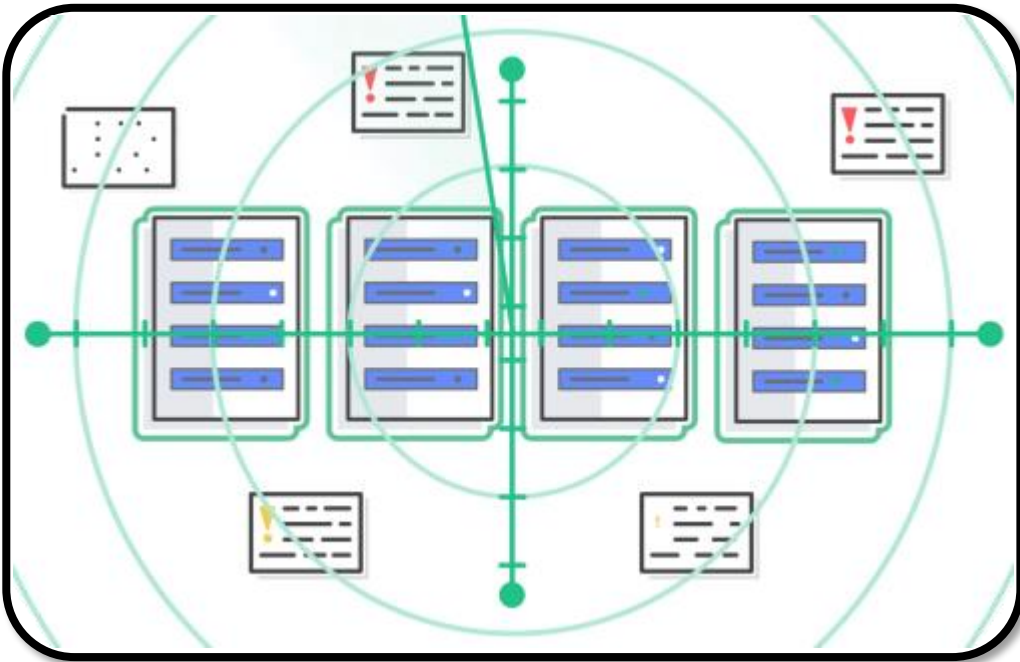
Challenges of threat assessment



- Expensive
- Complex
- Time-consuming
- Difficult to track IT changes

What is Amazon Inspector?

Automated security assessment as a service



- Assesses applications for vulnerabilities
- Produces a detailed list of security findings
- Leverages security best practices

Amazon Inspector findings

Amazon Inspector - Findings

Inspector findings are potential security issues discovered during Inspector's assessment of the specified application. [Learn more.](#)

Add/Edit attributes



Filter



Viewing 1-10 of 24

<input type="checkbox"/>	Severity	Application	Assessment	Rule package	Finding
<input type="checkbox"/>	▶ High ⓘ	Customer Processing	Comprehensive-Assessment	Authentication Best Practices	Instance i-aac4c46f is config
<input type="checkbox"/>	▶ High ⓘ	Customer Processing	Comprehensive-Assessment	Common Vulnerabilities and Ex...	Instance i-aac4c46f is vulne
<input type="checkbox"/>	▶ High ⓘ	Customer Processing	Comprehensive-Assessment	Authentication Best Practices	No password complexity me
<input type="checkbox"/>	▶ Informational ⓘ	Customer Processing	Comprehensive-Assessment	Operating System Security Best...	No potential security issues
<input type="checkbox"/>	▶ Informational ⓘ	Customer Processing	Comprehensive-Assessment	Network Security Best Practices	No potential security issues

Remediation recommendation

Finding for application - Customer Processing

Application name Customer Processing

Assessment name Comprehensive-Assessment

Rule package Authentication Best Practices

Finding Instance i-aac4c46f is configured to allow users to log in with root credentials over SSH. This increases the likelihood of a successful brute-force attack.

Severity High ⓘ

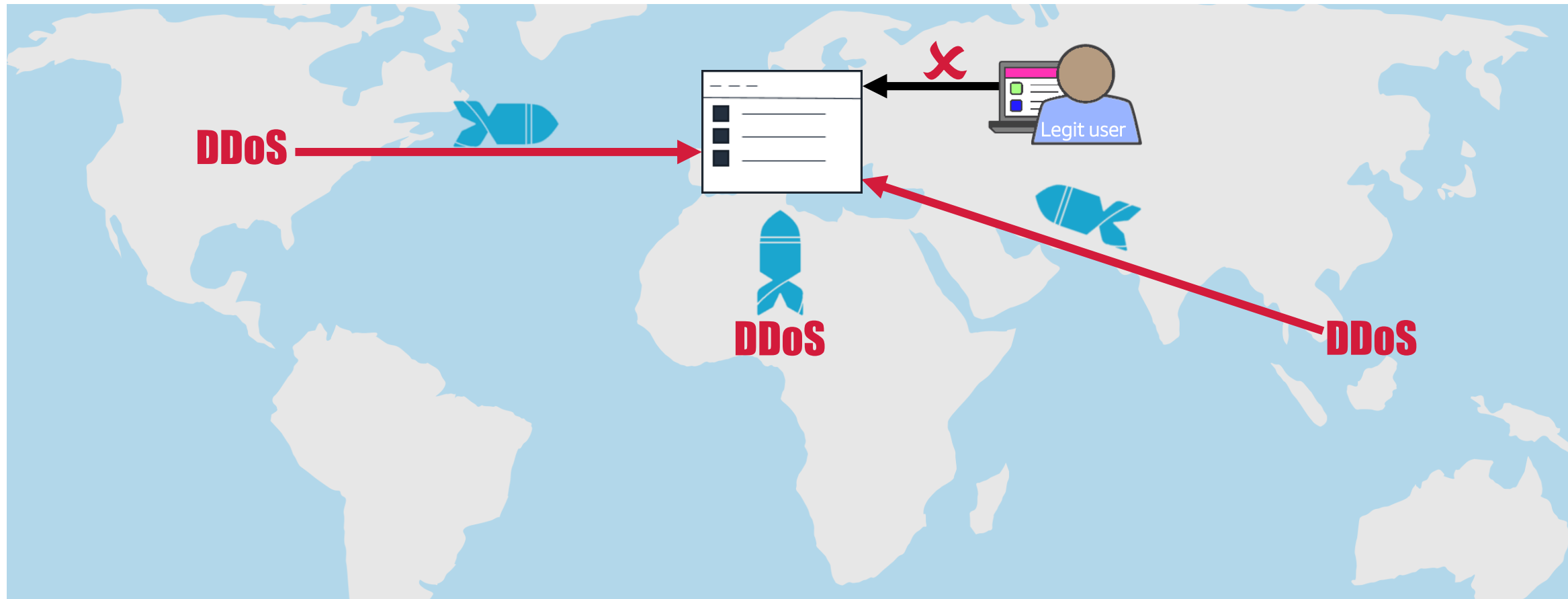
Description This rule helps determine whether the SSH daemon is configured to permit logging in to your EC2 instance as root.

Recommendation It is recommended that you configure your EC2 instance to prevent root logins over SSH. Instead, log in as a non-root user and use **sudo** to escalate.



Protect your infrastructure from Distributed Denial of Service (DDoS) attacks

What is DDoS?



DDoS mitigation challenges



Complex



Limited bandwidth



Involves rearchitecting



Manual



Degraded performance

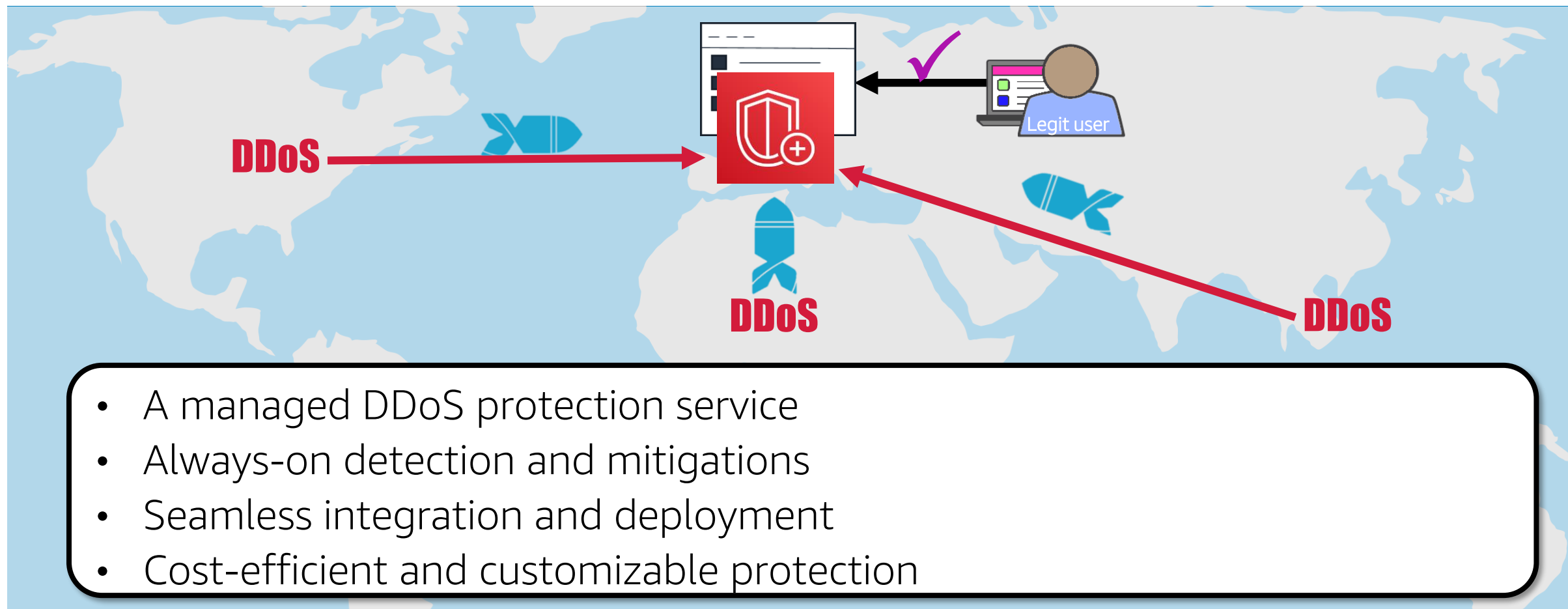


Time-consuming



Expensive

What is AWS Shield?



AWS Shield Standard and AWS Shield Advanced

AWS Shield Standard (included)

- Quick detection
- Inline attack mitigation

AWS Shield Advanced

- Enhanced detection
- Advanced attack mitigation
- Visibility and attack notification
- DDoS cost protection
- Specialized support



AWS security compliance

Assurance programs

Global



USA



Europe



Asia Pacific



How AWS helps customers achieve compliance

Sharing information

- Industry certifications
- Security and control practices
- Compliance reports directly under NDA

Assurance program

- Certifications/attestations
- Laws, regulations, and privacy
- Alignments/frameworks

Demo

Customer responsibility

You own your certification.

Review – **Design** – **Identify** – **Verify**

End of Module 4

Test Your Knowledge