Hochschule für Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Advanced Security (Information Security Management) – Cloud Security

Prof. Dr.-Ing. Sebastian Schlesinger

Professor of Business Computer Science (Security and Embedded Systems Engineering)

Goals

- Obtain an fundamental understanding on AWS security
  - Best practices for building cloud applications
  - Cloud-native security services

While we focus on AWS, the insights are not closely tied to AWS and transferrable to other cloud providers

Cloud Security

Recap and Introduction

Security in the AWS Cloud

Introduction to Security on AWS

Benefits of the cloud

Trade fixed expense for variable expense.

Benefit from massive economies of scale.

Stop guessing on your capacity needs.

Increase speed and agility.

Stop spending money to run and maintain data centers.

Go global in minutes.

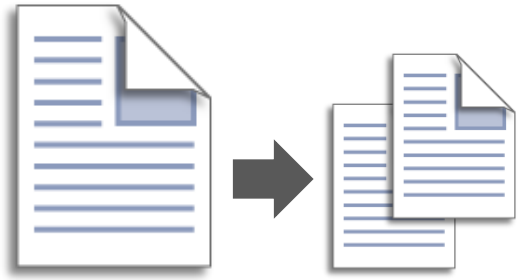
Security is familiar

Confidentiality

- Limit access and disclosure to authorized users
- Prevent access by unauthorized people

Integrity

- Maintain data consistency during its lifecycle
- Preserve data at rest and data in transit



Availability

- Have access to information resources when needed

AWS Cloud security: Objectives

- Controllability
- Auditability
- Visibility
- Agility
- Automation

AWS Cloud security: Controllability

- Can I effectively manage users?
- How can I provide temporary credentials?
- Can I use my own keys?

AWS Identity and Access Management (IAM)

AWS Cloud security: Auditability

- Who has access to this resource?
- Who performed what action?
- When was the action performed and from where?
- Where is the evidence?

AWS CloudTrail

AWS Cloud security: Visibility

- What is in my environment?
- What impact did a particular action have?
- What has changed?
- Where is the evidence?

AWS Config

AWS Cloud security: Agility and automation

- How do I ensure high availability?
- Can I automatically deploy applications with security and compliance-related settings?
- How can I apply security checks in a reproducible manner?

AWS CloudFormation

Security design principles

Introduction to Security on AWS

1. Apply the principle of least privilege

- Grant access as needed
- Enforce separation of duties
- Avoid long-term credentials

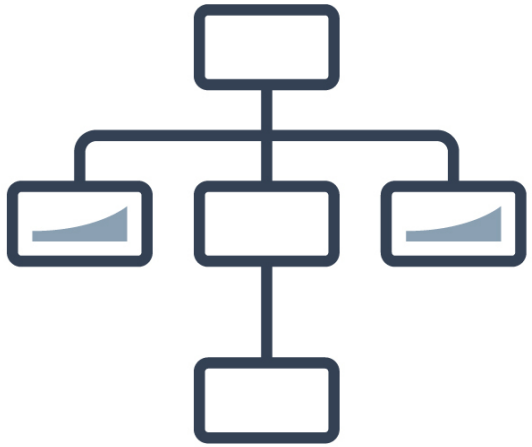
1 2 3 4 5 6 7

2. Enable traceability

- Monitor actions and changes
- Use logs and metrics
- Audit your cloud resources

1 2 3 4 5 6 7

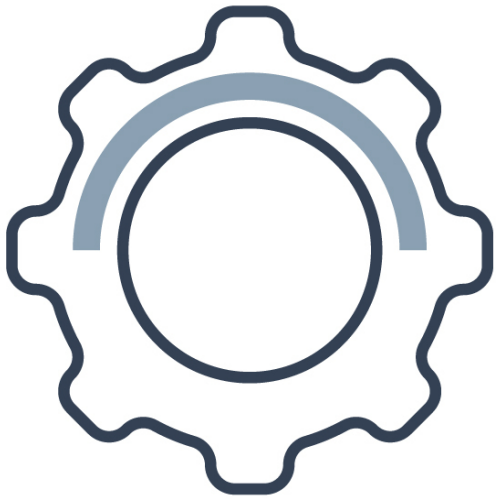
3. Secure all layers



- Use a defense in depth approach
- Use different AWS services

1 2 3 4 5 6 7

4. Automate security



- Automate routine security tasks with APIs
- Implement infrastructure as code

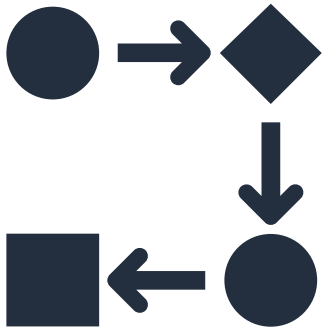
1 2 3 **4** 5 6 7

5. Protect data in transit and data at rest

- Use encryption and access controls
- Classify your data with tags
- Use VPN and TLS connections

1 2 3 4 **5** 6 7

6. Prepare for security events



- Mitigate the impact of security incidents
- Create processes to isolate incidents and restore operations

1 2 3 4 5 **6** 7

7. Minimize the attack surface

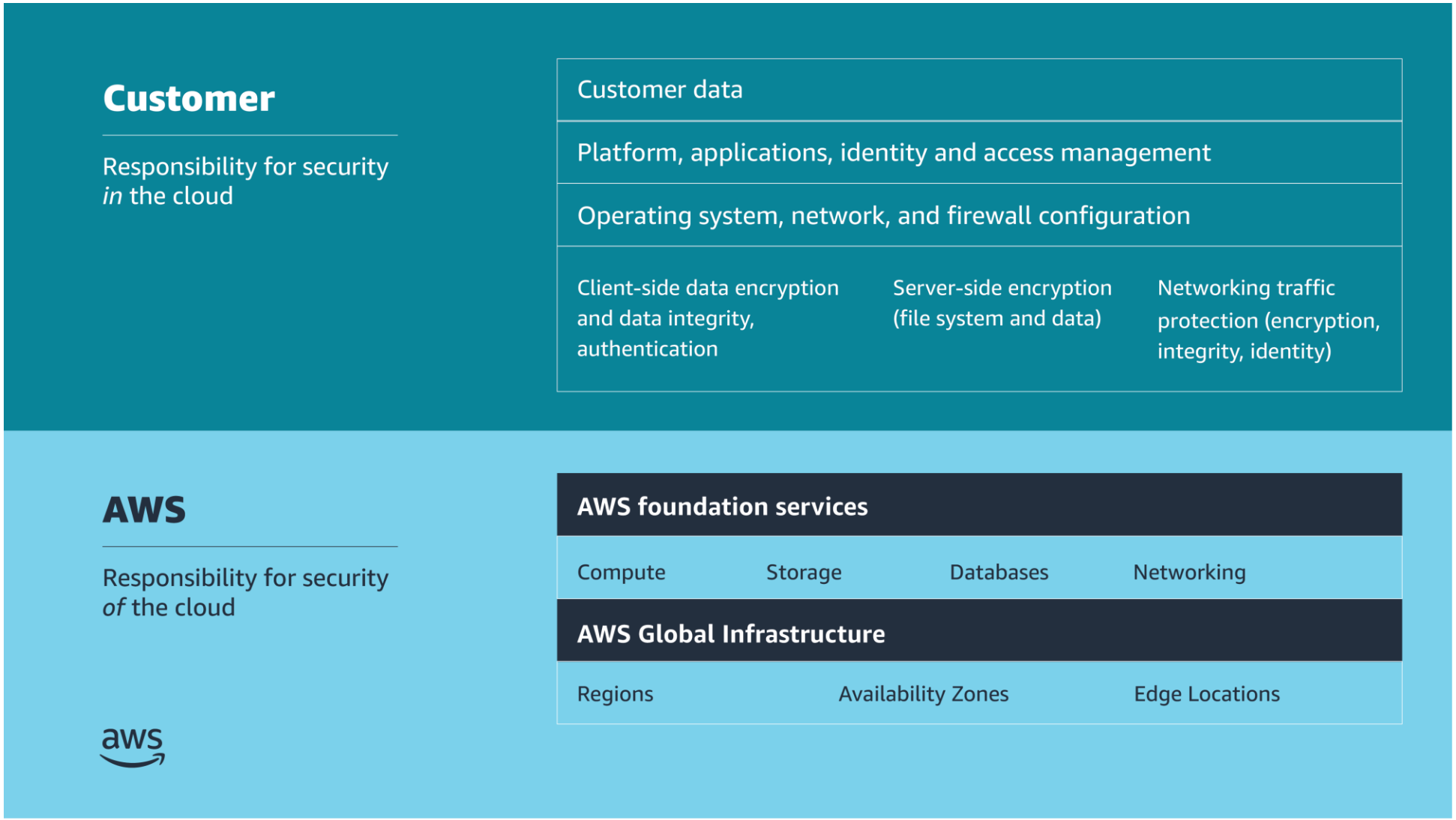
- Be ready to scale and absorb the attack
- Safeguard exposed resources

1 2 3 4 5 6 **7**

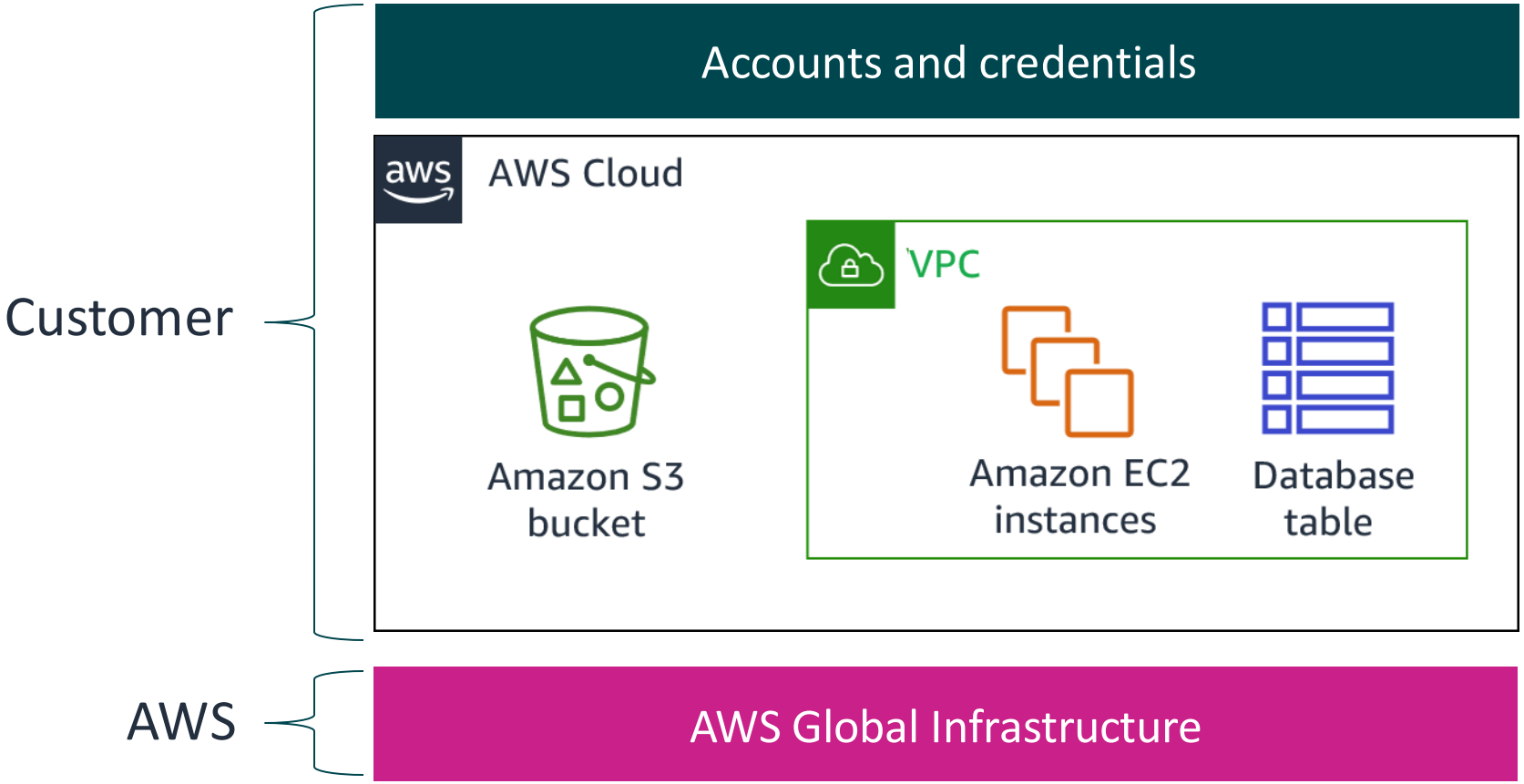
Shared responsibility model

Introduction to Security on AWS

AWS shared responsibility model



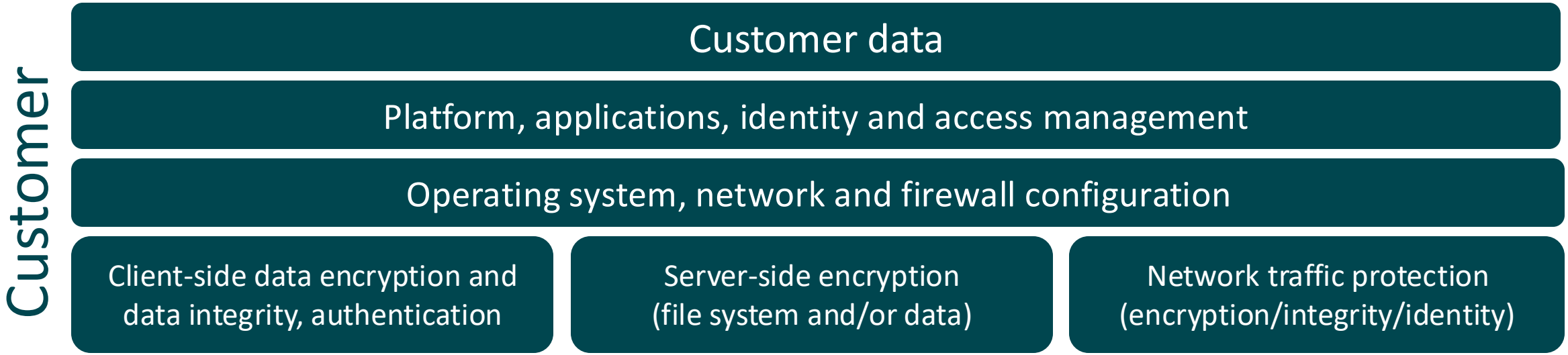
Shared responsibility example



Customer responsibility examples:

- Guest OS configuration
- Application-level security
- Security group configuration

Security *in* the cloud

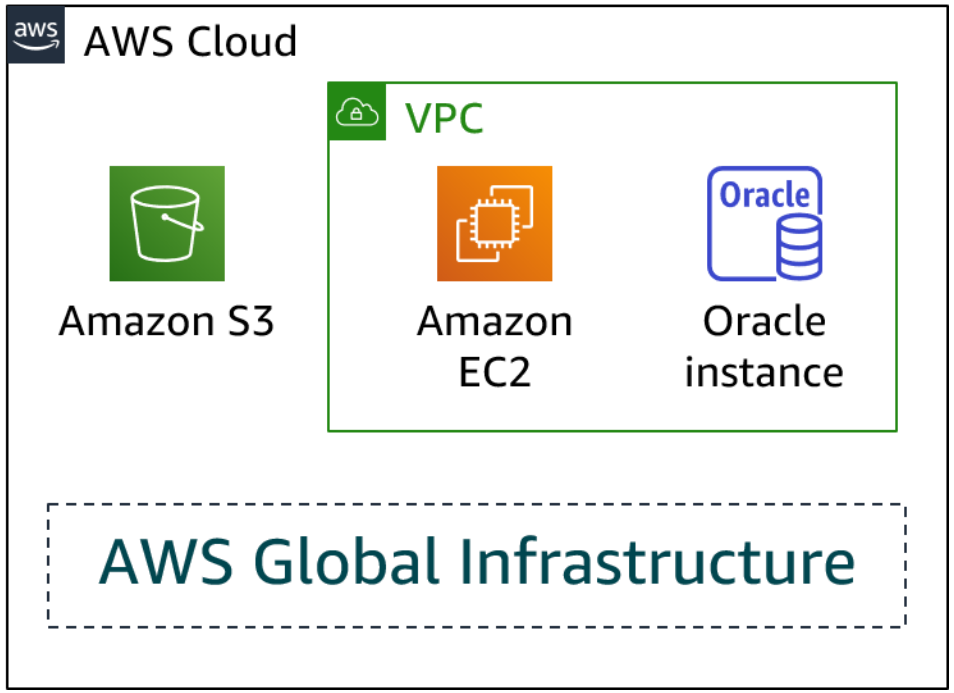


Considerations

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

Activity: Scenario 1 of 2

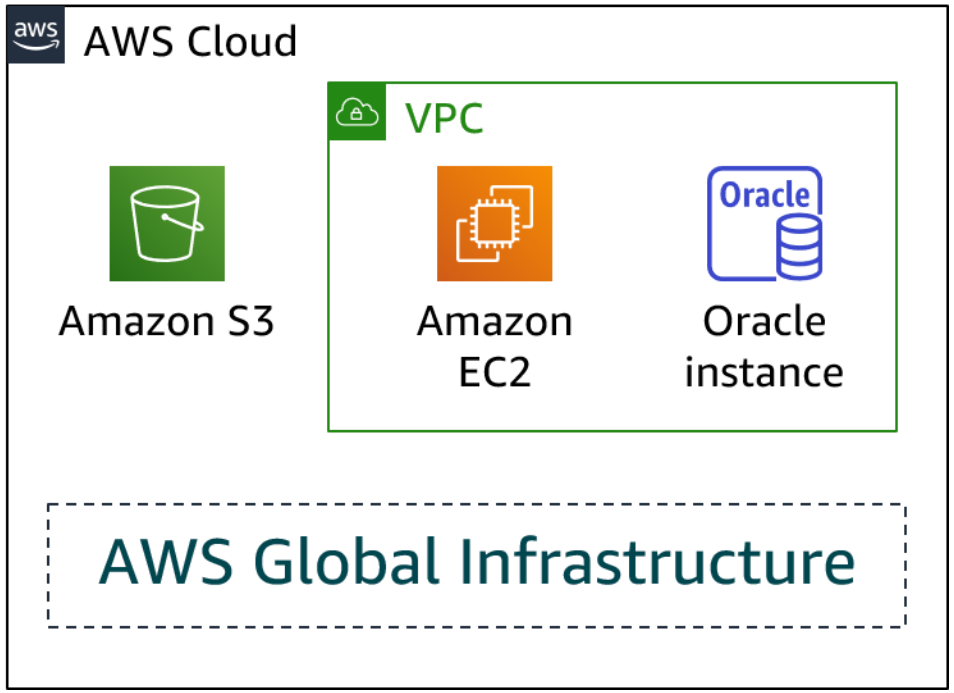
Consider this deployment. Who is responsible: AWS or the customer?



1. Upgrades and patches to the operating system on the EC2 instance?
2. Physical security of the data center?
3. Virtualization infrastructure?
4. EC2 security group settings?
5. Configuration of applications that run on the EC2 instance?
6. Oracle upgrades or patches if the Oracle instance runs as an Amazon RDS instance?
7. Oracle upgrades or patches if Oracle runs on an EC2 instance?
8. S3 bucket access configuration?

Activity: Scenario 1 of 2 answers

Consider this deployment. Who is responsible: AWS or the customer?



1. Upgrades and patches to the operating system on the EC2 instance?

   Answer: The customer

2. Physical security of the data center?

   Answer: AWS

3. Virtualization infrastructure?

   Answer: AWS

4. EC2 security group settings?

   Answer: The customer

5. Configuration of applications that run on the EC2 instance?

   Answer: The customer

6. Oracle upgrades or patches if the Oracle instance runs as an Amazon RDS instance?

   Answer: AWS

7. Oracle upgrades or patches if Oracle runs on an EC2 instance?

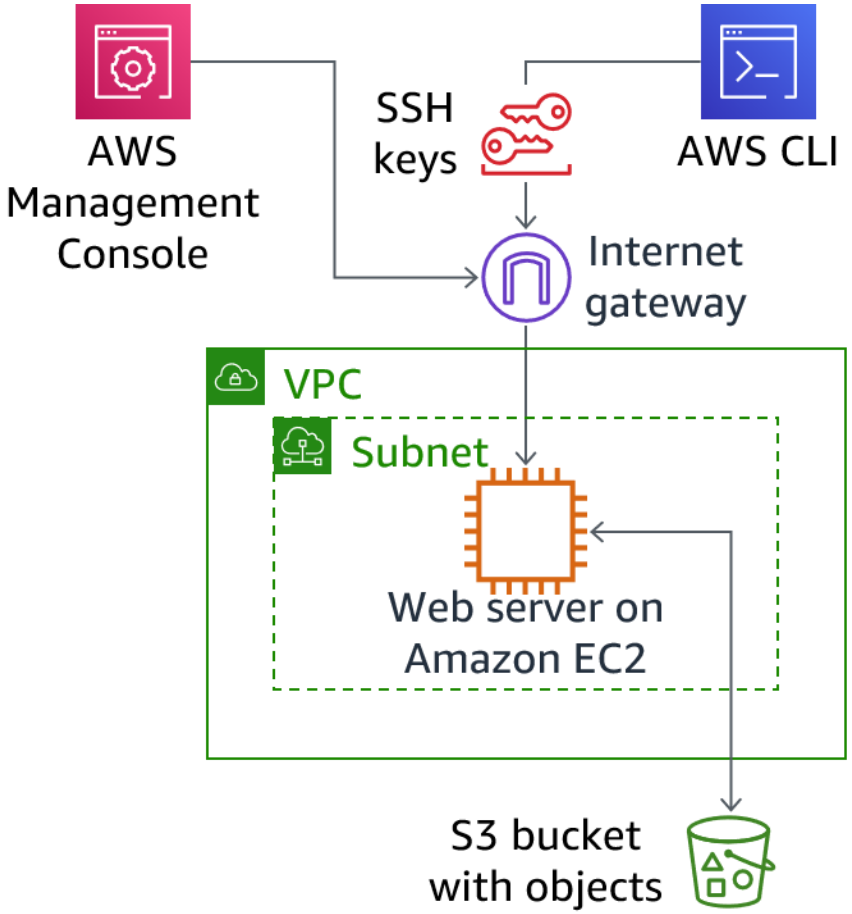
   Answer: The customer

8. S3 bucket access configuration?

   Answer: The customer

Activity: Scenario 2 of 2

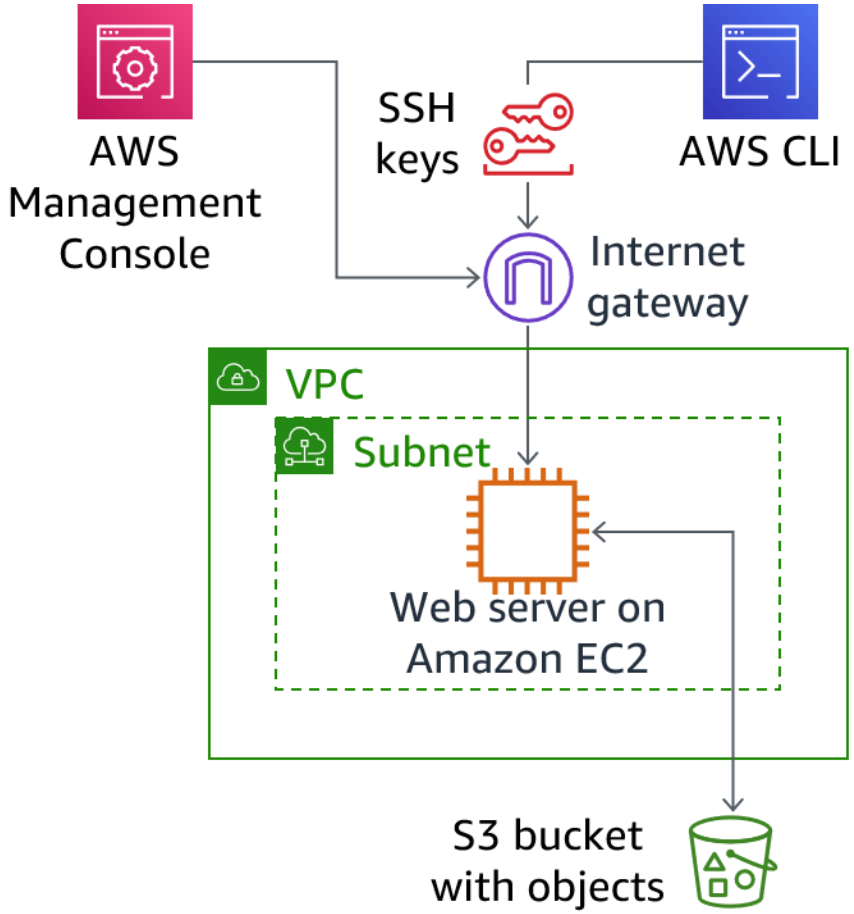
Consider this deployment. Who is responsible: AWS or the customer?



1. Ensuring that the AWS Management Console is not hacked?
2. Configuring the subnet?
3. Configuring the VPC?
4. Protecting against network outages in AWS Regions?
5. Securing the SSH keys?
6. Ensuring network isolation between AWS customers' data?
7. Ensuring low-latency network connection between the web server and the S3 bucket?
8. Enforcing multi-factor authentication for all user logins?

Activity: Scenario 2 of 2 answers

Consider this deployment. Who is responsible: AWS or the customer?



1. Ensuring that the AWS Management Console is not hacked?

   Answer: AWS

2. Configuring the subnet?

   Answer: The customer

3. Configuring the VPC?

   Answer: The customer

4. Protecting against network outages in AWS Regions?

   Answer: AWS

5. Securing the SSH keys?

   Answer: The customer

6. Ensuring network isolation between AWS customers' data?

   Answer: AWS

7. Ensuring low-latency network connection between the web server and the S3 bucket?

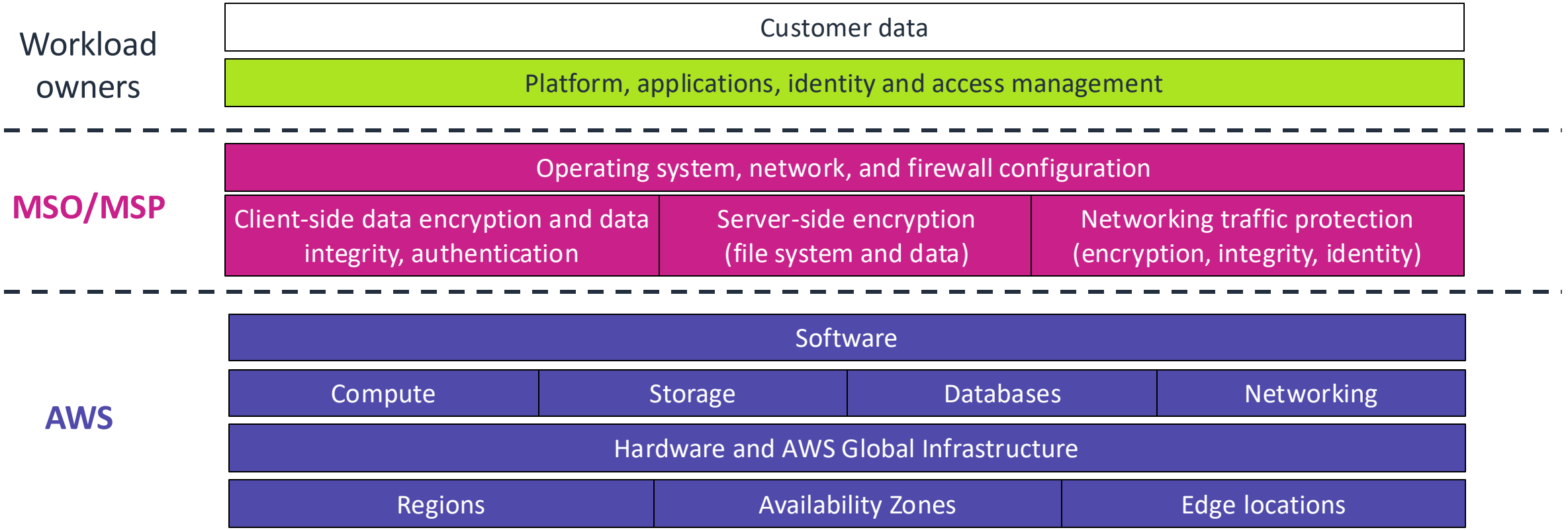
   Answer: AWS

8. Enforcing multi-factor authentication for all user logins?

   Answer: The customer

Managed services organization

MSO responsibility model



Sample exam question

According to the shared responsibility model, who is responsible for configuring security group rules to determine which ports are open to an EC2 Linux instance?

Choice	Response
A	AWS is responsible for configuring security group rules.
B	The customer is responsible for configuring security group rules.
C	Security group rules are not needed.
D	AWS is responsible for configuring security group rules, and the customer must open ports to the instance.

Sample exam question answer

Copy and paste the same question here.

The correct answer is B.

The keywords in the question are **configuring security group rules**.

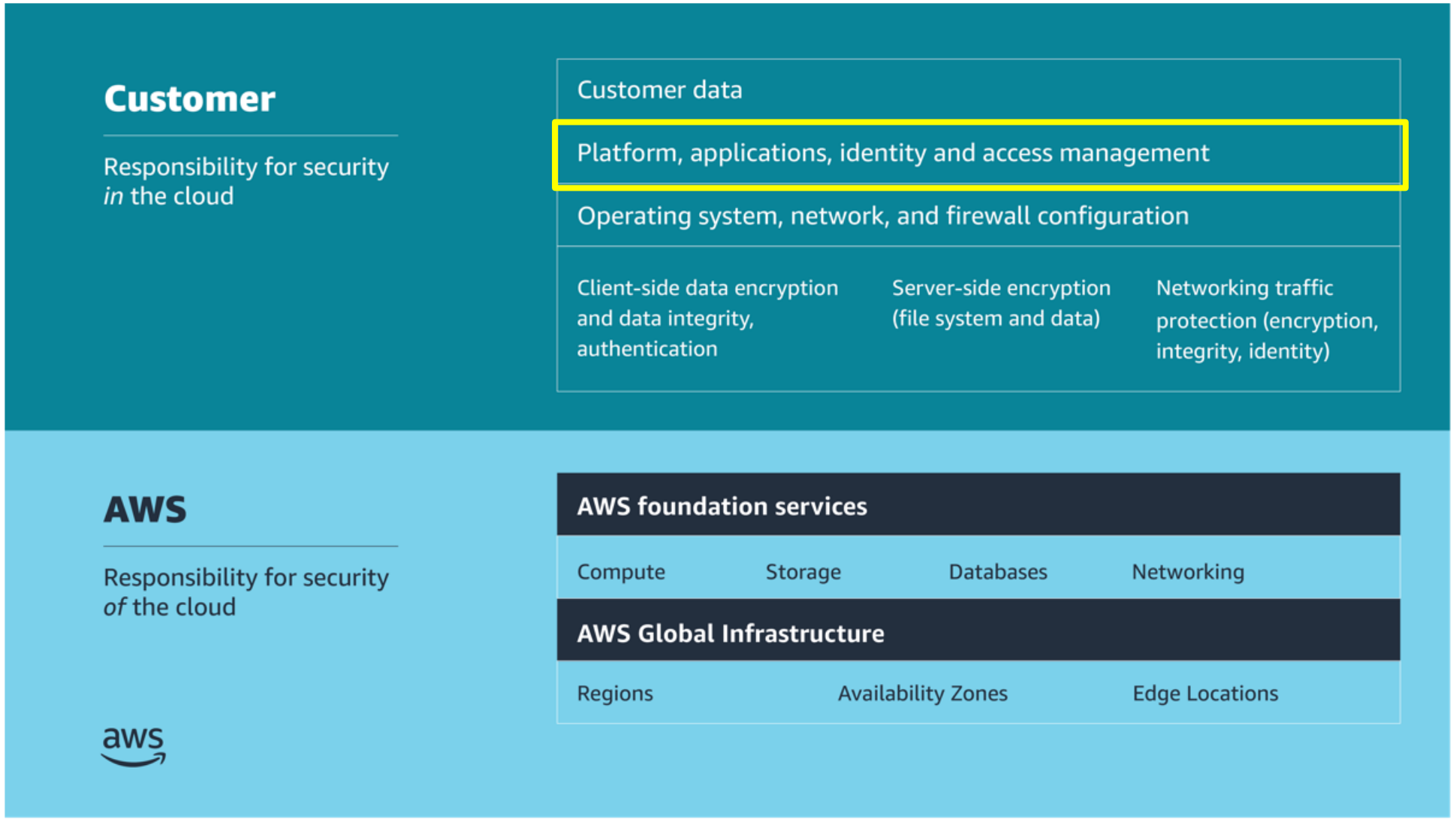
Securing Access to Cloud Resources

AWS Academy Cloud Security Foundations

Introduction

Securing Access to Cloud Resources

Shared responsibility model



IAM fundamentals

Securing Access to Cloud Resources

AWS Identity and Access Management (IAM)

- Securely shares and controls individual and group access to your AWS resources
- Integrates with many other AWS services
- Supports federated identity management
- Supports granular permissions
- Supports multi-factor authentication (MFA)
- Provides identity information for assurance

AWS Identity and Access Management (IAM)

What IAM provides

- Authentication
  - **Who** is requesting access to the AWS account and the resources in it?
  - It's important to establish the identity of the requester through credentials.
  - The requester could be a *person* or an *application*; IAM calls them *principals*.
- Authorization
  - After the requester has been authenticated, **what** should they be allowed to do?
  - IAM checks for policies that are relevant to the request to determine whether to allow or deny the request.

IAM overview

User

A person or application that can authenticate with an AWS account

Group

A collection of IAM users who are granted identical authorization

Role

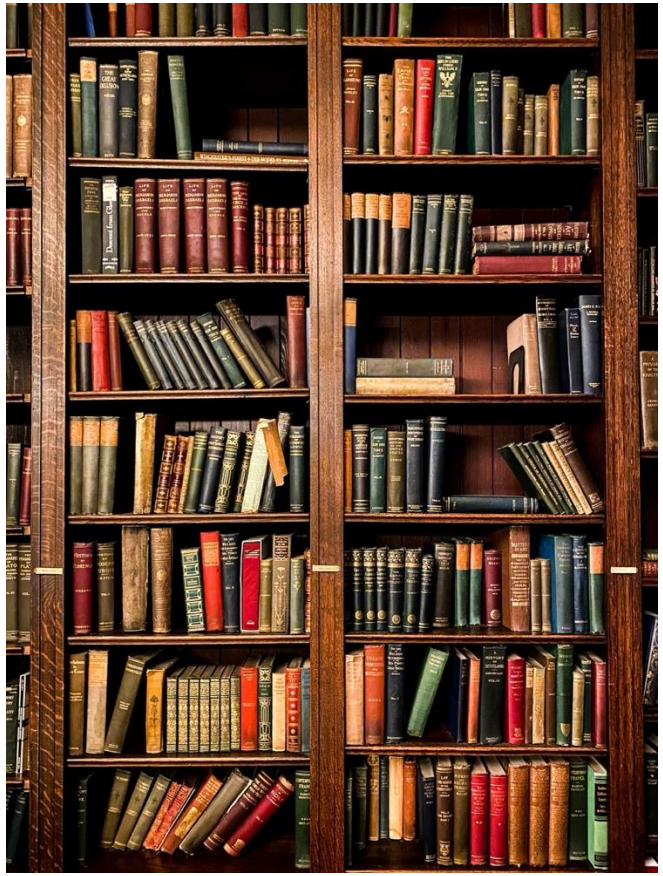
An identity used to grant a temporary set of permissions to make AWS service requests

IAM policy

The document that defines which resources can be accessed and the level of access to each resource

IAM terminology

- *IAM entity:* Used by AWS for authentication (users and roles)
- *IAM identity:* Used to identify and group
  - You can attach a policy to an IAM identity (user, group, or role).
- *IAM resource:* The user, group, role, policy, and identity provider objects that are stored in IAM
  - You can add, edit, and remove resources from IAM.
- *Principal:* A person or application that uses the AWS account root user, IAM user, or IAM role to sign in and make requests to AWS



Requests in IAM

A *request* is made any time a principal attempts to use the AWS Management Console, application programming interface (API), or AWS Command Line Interface (AWS CLI).

The request contains the following information:

- *Actions or operations:* What the principal wants to perform
- *Resources:* The object upon which the actions or operations are performed
- *Principal:* The person or application that sends a request by using a user or role
- *Environment data:* The IP address, user agent, Secure Sockets Layer (SSL) enabled status, or time of day
- *Resource data:* Data related to the resource being requested

Service endpoints

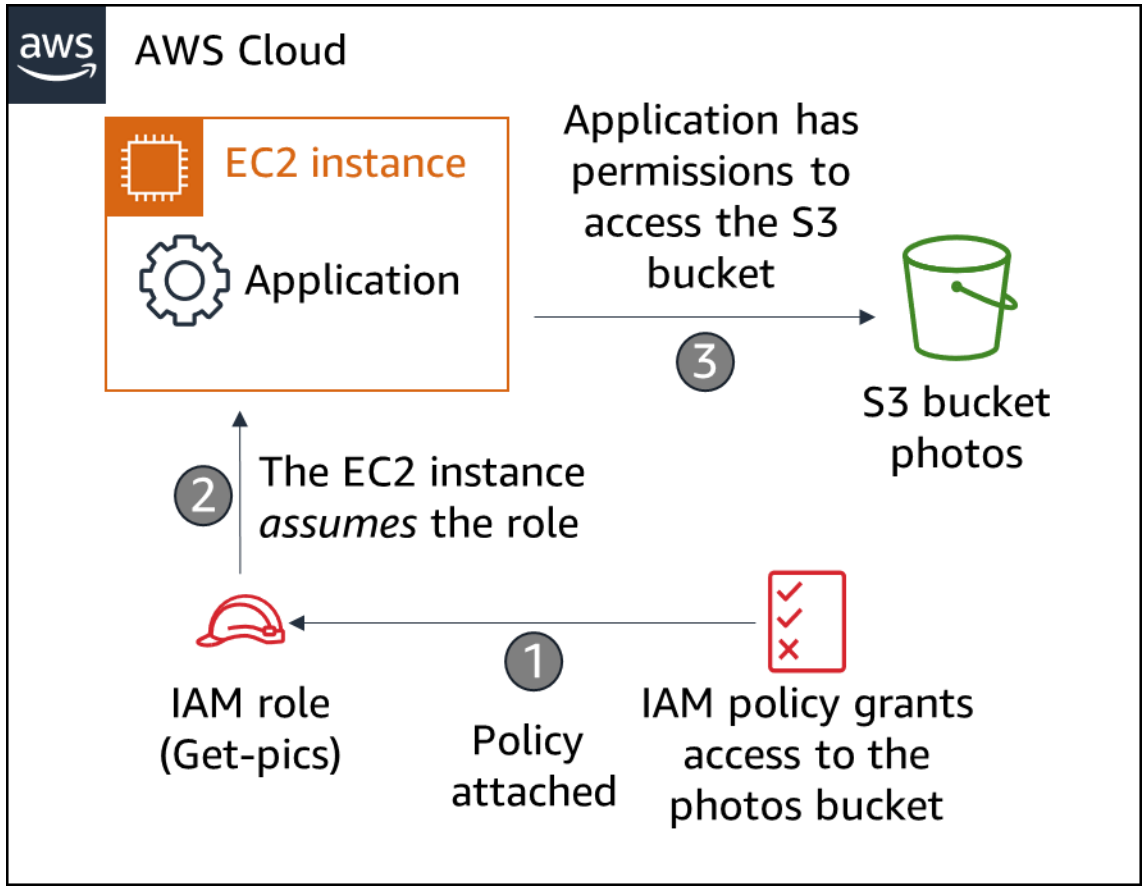
- To connect to an AWS service, you must use the URL of the entry point for that service, known as an *endpoint*.
- The AWS software development kits (SDKs) and AWS CLI use the default endpoint for each service in an AWS Region.
- You can specify alternate endpoints for API requests based on configuration requirements.

Authenticating with IAM

Securing Access to Cloud Resources

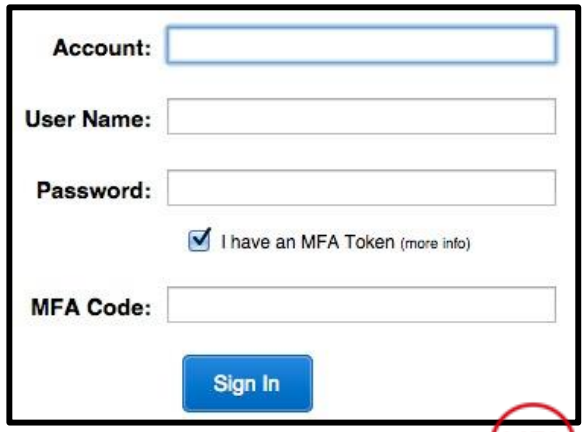
IAM roles

- IAM role characteristics
  - It provides *temporary* security credentials.
  - A role is **not** uniquely associated with one person.
  - A *person*, *application*, or *AWS service* can assume a role.
  - A role is often used to delegate access.
  - The AWS Security Token Service (AWS STS) issues temporary security credentials.
- Common use cases
  - Applications that run on Amazon Elastic Compute Cloud (Amazon EC2)
  - Cross-account access for an IAM user
  - Mobile applications



IAM credentials for authentication

User name and password
(console access)



AWS Management Console

MFA Option

Access key ID and secret access key
(programmatic access)

```
[redacted]:~ [redacted]$ aws configure
AWS Access Key ID [****************O22A]:
AWS Secret Access Key [****************4m8i]:
Default region name [ap-southeast-1]:
Default output format [json]:
```

AWS CLI

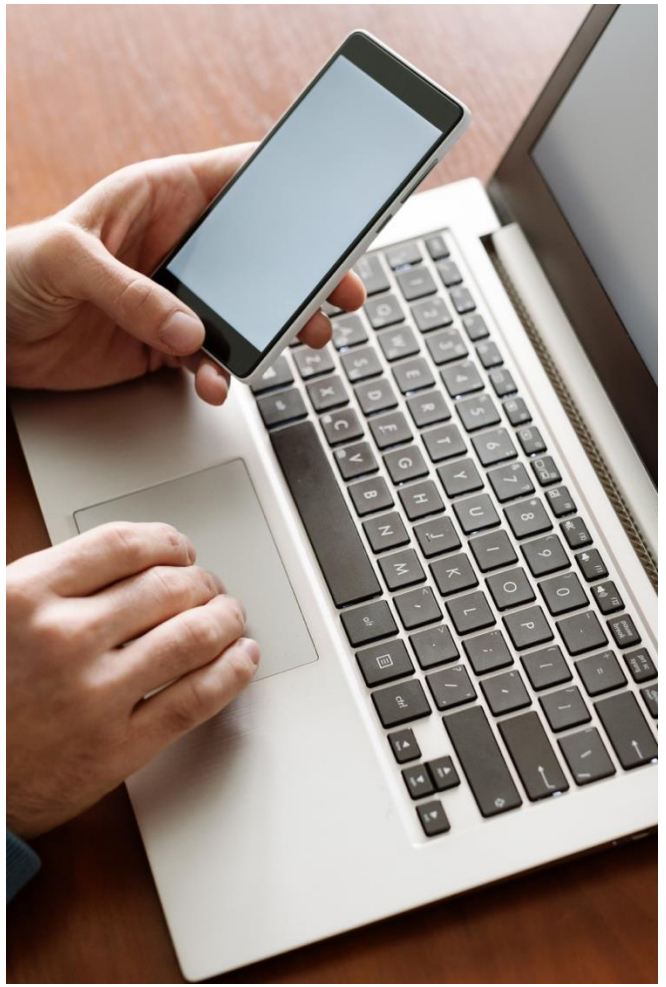
ACCESS KEY ID
AKIAIOSFODNN7EXAMPLE
SECRET KEY
wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

API access

MFA Option

Multi-factor authentication (MFA)

- Adds an extra layer of protection on top of your user name and password
  - Users prompted for an authentication code
  - Can be hardware based or a virtual device
- Activate MFA for:
  - AWS Management Console users
  - AWS API users (requires temporary security credentials)
- Examples of MFA devices:
  - Security keys (YubiKey, Gemalto)
  - Applications (Google Authenticator, Authy)
  - Hardware devices



Authentication scenario

Production account

1. The admin creates a role that grants the development account read/write access to the productionapp bucket.

Role: UpdateApp

S3 bucket: productionapp

3. A user requests access to the role.

4. AWS STS returns the role credentials.

5. The user updates the bucket by using the role credentials.

Development account

Group: Testers

Group: Developers

2. The admin grants permissions to the members of the Developers group to assume the UpdateApp role.

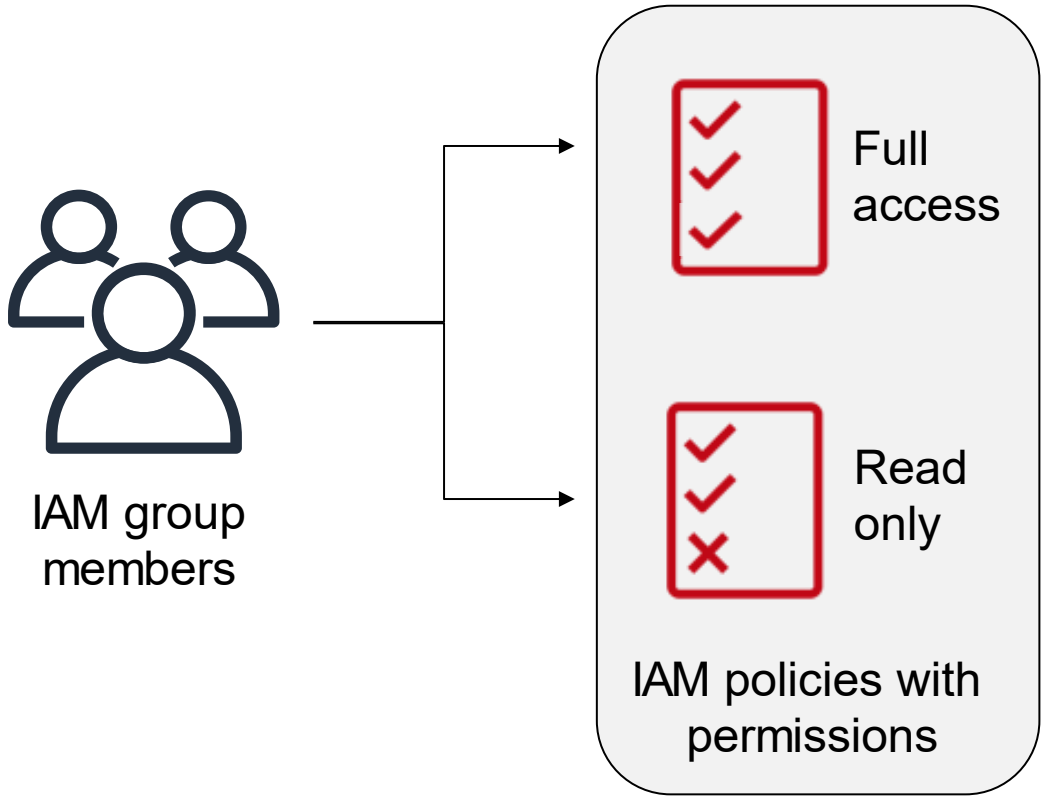
Key takeaways: Authenticating with IAM

- A best practice is to attach IAM policies to IAM groups, and then assign IAM users to these IAM groups.
- IAM roles use temporary security credentials.
- AWS STS provides temporary credentials for roles.
- MFA adds an extra layer of protection on top of your user name and password.

Authorizing with IAM

Securing Access to Cloud Resources

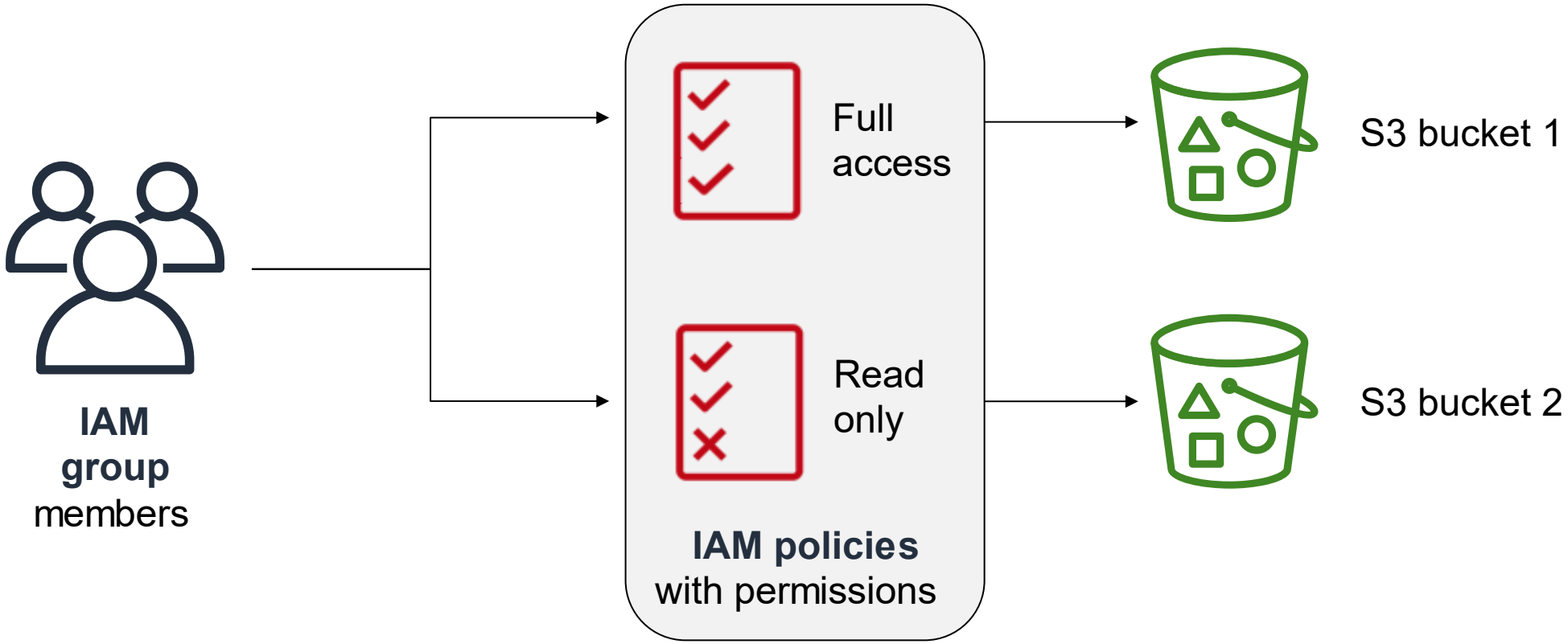
Principle of least privilege



Best practices:

- Start by granting the minimum AWS account permissions that are needed for the job role.
- Grant additional access as needed.

Policies and permissions



Identity-based and resource-based policies

Identity-based policies

What does a particular identity have access to?

Carlos

Resource	Read	Write	List
Resource X	Allow	Allow	Allow

Richard

Resource	Read	Write	List
Resource Y	Allow	N/A	N/A
Resource Z	Allow	N/A	N/A

Managers

Resource	Read	Write	List
Resource X	N/A	N/A	Allow
Resource Y	N/A	N/A	Allow
Resource Z	N/A	N/A	Allow

Resource-based policies

Who has access to a particular resource?

Resource X

User	Read	Write	List
Ana	Allow	Allow	Allow
Akua	Allow	Allow	Allow
Mary	Allow	N/A	Allow
Mateo	N/A	N/A	Allow

Resource Y

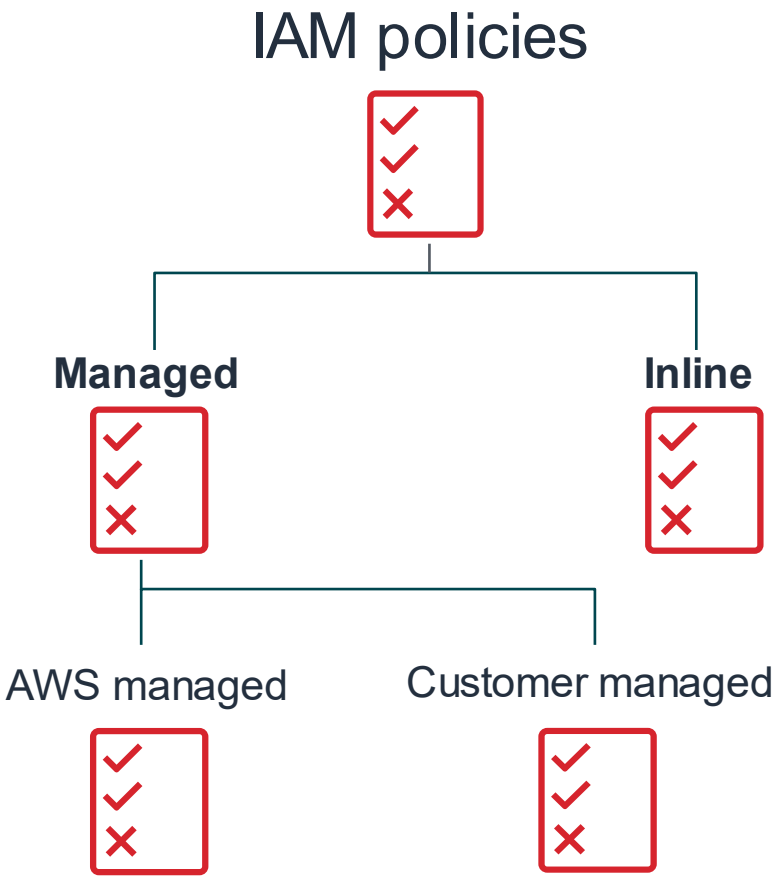
User	Read	Write	List
Paulo	Allow	Allow	Allow
Nikki	Allow	N/A	N/A
Mateo	N/A	Allow	Allow

Managed and inline IAM policies

Managed policies

- Are standalone, *identity-based* policies
- Can be attached to multiple users, groups, and roles

Features:
- Reusability
- Central change management
- Versioning and rollback
- Permissions management that can be delegated to others
- Provides the use of *permissions boundaries*

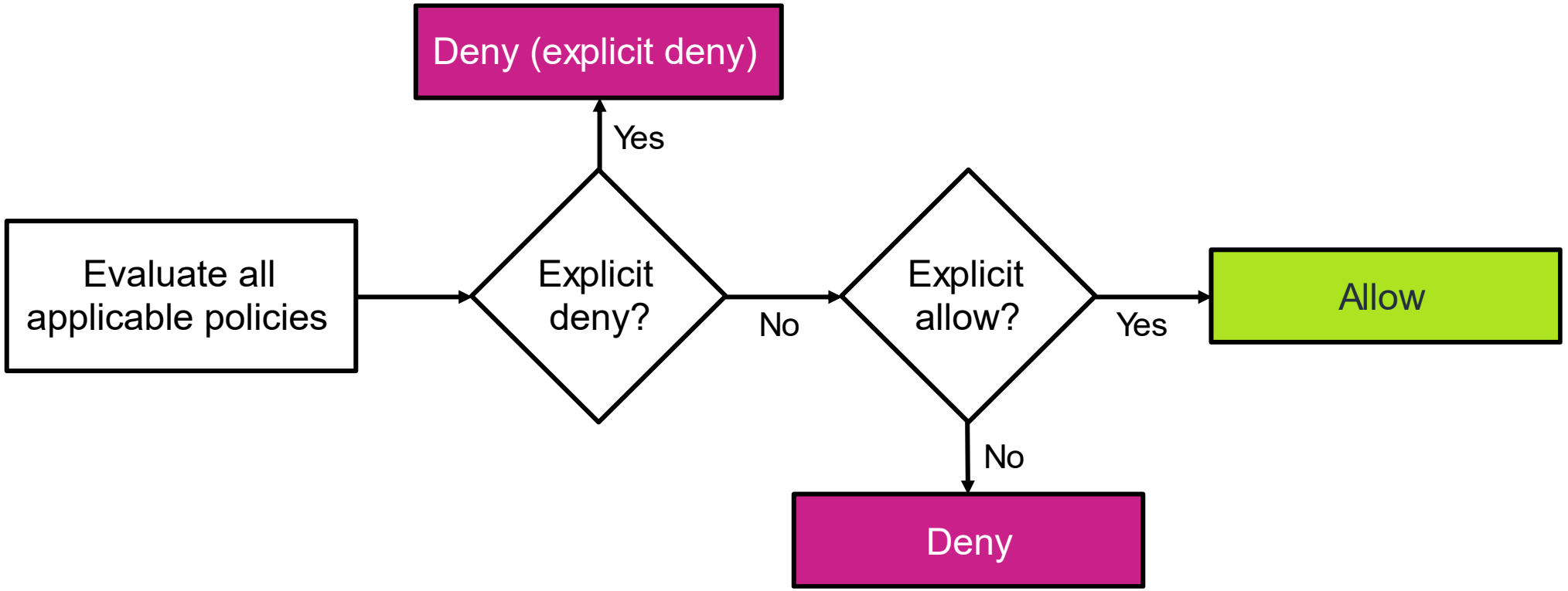


Inline policies

- Are embedded in a principal entity (for example, user, group, or role)

- Are useful for a strict 1:1 relationship between a policy and the entity

Evaluation logic for IAM policies



Key takeaways: Authorizing with IAM

- Permissions to access AWS account services and resources are defined in IAM policy documents.
- Attach IAM policies to IAM users, IAM groups, or IAM roles.
- Follow the principle of least privilege when you grant account access.
- When IAM determines permissions, an explicit deny will always override any allow statement.

Examples of authorizing with IAM

Securing Access to Cloud Resources

Example: Identity-based policy

```
{
  "Version": "2018-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "iam:*LoginProfile",
          "iam:*AccessKey*",
          "iam:*SSHPublicKey*"
    ],
    "Resource": "arn:aws:iam::account-id-without-
hyphens:user/${aws:username}"
  }
}
```

These are the actions allowed by the policy

These are the AWS resources that the allowed actions can be performed on

Example: Cross-account, resource-based policy

```
{
  "Version": "2018-10-17",
  "Statement": {
    "Sid": "AccountBAccess1",
      "Principal": {"AWS": "111122223333"},
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": [
          "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
      ]
  }
}
```

Account B principal allowed by Account A to make the request

Actions allowed by Account A

Resources shared by Account A

Example IAM policy: Allow statement

```
{
  "Version": "2012-10-17",
    "Statement":[{
    "Effect":"Allow",
    "Action":["dynamodb:*","s3:*"],
    "Resource":["arn:aws:dynamodb:region:account-number-without-hyphens:table/coursenotes",
      "arn:aws:s3:::course-notes-web",
      "arn:aws:s3:::course-notes-mp3/*"]
    },
    {
    "Effect":"Deny",
    "Action":["dynamodb:*","s3:*"],
    "NotResource":["arn:aws:dynamodb:region:account-number-without-
hyphens:table/coursenotes",
      "arn:aws:s3:::course-notes-web",
      "arn:aws:s3:::course-notes-mp3/*"]
    }
  ]
}
```

Allows the entity to perform any DynamoDB or S3 action on this DynamoDB table and these S3 buckets

Example IAM policy: Deny statement

```
{
  "Version": "2012-10-17",
    "Statement":[{
    "Effect":"Allow",
    "Action":["dynamodb:*","s3:*"],
    "Resource":["arn:aws:dynamodb:region:account-number-without-hyphens:table/coursenotes",
      "arn:aws:s3:::course-notes-web",
      "arn:aws:s3:::course-notes-mp3/*"]
    },
    {
    "Effect":"Deny",
    "Action":["dynamodb:*","s3:*"],
    "NotResource":["arn:aws:dynamodb:region:account-number-without-
hyphens:table/coursenotes",
      "arn:aws:s3:::course-notes-web",
      "arn:aws:s3:::course-notes-mp3/*"]
    }
  ]
}
```

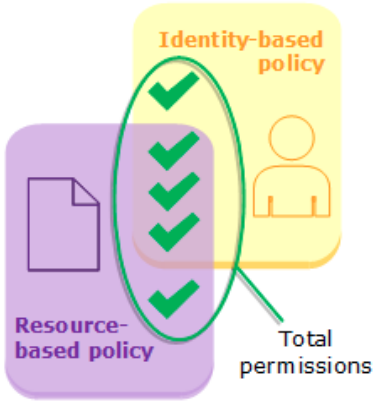
Ensures that the entity can't perform any action on any DynamoDB table or S3 bucket except the tables and buckets that the policy specifies

An explicit deny statement takes precedence over an allow statement.

Example IAM policy: Permissions boundary

1

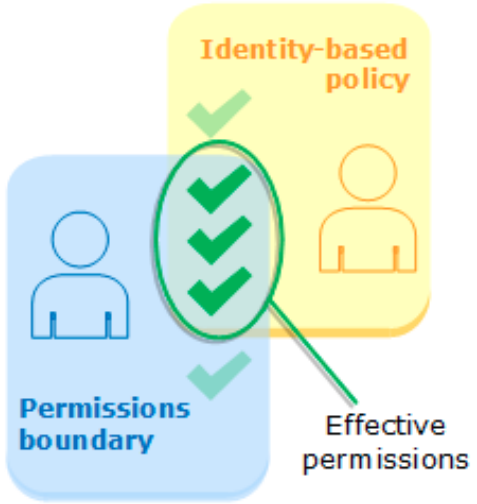
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:*",
        "cloudwatch:*",
        "ec2:*"
      ],
      "Resource": "*"
    }
  ]
}
```



If policy 1 is attached to a user…

2

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "iam:CreateUser".
    "Resource": "*"
  }
}
```



…followed by policy 2, then any attempt to create a user in IAM will fail because of the boundary restrictions placed by policy 1.

Additional authentication and access management services

Securing Access to Cloud Resources

Identity federation

- Identity federation is a system of trust between two parties to authenticate users and convey information that is needed to authorize resource access.
  - *Identity providers* are responsible for user authentication.
  - *Service providers* are responsible for resource access.
- Two AWS services are available to provide federation to AWS accounts and applications:
  - AWS Single Sign-On (AWS SSO)
  - AWS Identity and Access Management (IAM)

AWS Single Sign-On (AWS SSO)

- Create or connect identities once and manage access centrally across your AWS accounts.
- AWS SSO provides a unified administration experience to define, customize, and assign fine-grained access.
- Users are provided a user portal to access all their assigned AWS accounts or cloud applications.
- You can flexibly configure access to run parallel to or replace AWS account access management by using IAM.

AWS Single Sign-On (AWS SSO)

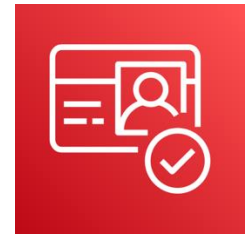
AWS Directory Service

- AWS Directory Service for Microsoft Active Directory, also called AWS Managed Microsoft AD
- Facilitates directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud
- Provides the ability to extend your existing Active Directory to AWS by using your existing on-premises user credentials to access cloud resources
- Supports Active Directory SSO to AWS applications by using a single set of credentials

AWS Directory Service

Amazon Cognito

- Integrates user sign-up, sign-in, and access control with web and mobile applications
- Provides a secure identity store that can scale to millions of users with Amazon Cognito user pools
- Offers user sign-in through enterprise identity providers and social identity providers such as Apple, Google, Facebook, and Amazon
- Provides the ability to create unique identities for your users and federate them with identity providers through Amazon Cognito identity pools



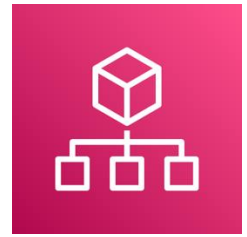
Amazon Cognito

Using AWS Organizations

Securing Access to Cloud Resources

AWS Organizations

- Account management service that you can use to consolidate multiple AWS accounts into a centrally managed organization
- Includes account creation and management as well as consolidated billing capabilities
- Provides for hierarchical grouping of accounts
- Supports centralized policy control over AWS services and API actions using service control policies (SCPs)
- Integrates with IAM and other services



AWS Organizations

Example: SCP

Prevent member accounts from leaving the organization:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [ "organizations:LeaveOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

Sample exam question

How would a system administrator add an additional layer of login security to protect a user's access to the AWS Management Console?

Choice	Response
A	Use Amazon Cloud Directory.
B	Audit AWS Identity and Access Management (IAM) roles.
C	Activate multi-factor authentication (MFA).
D	Enable AWS CloudTrail.

Sample exam question answer

How would a system administrator add an additional layer of login security to protect a user's access to the AWS Management Console?

The correct answer is C.

The keywords in the question are **additional layer of login security**.

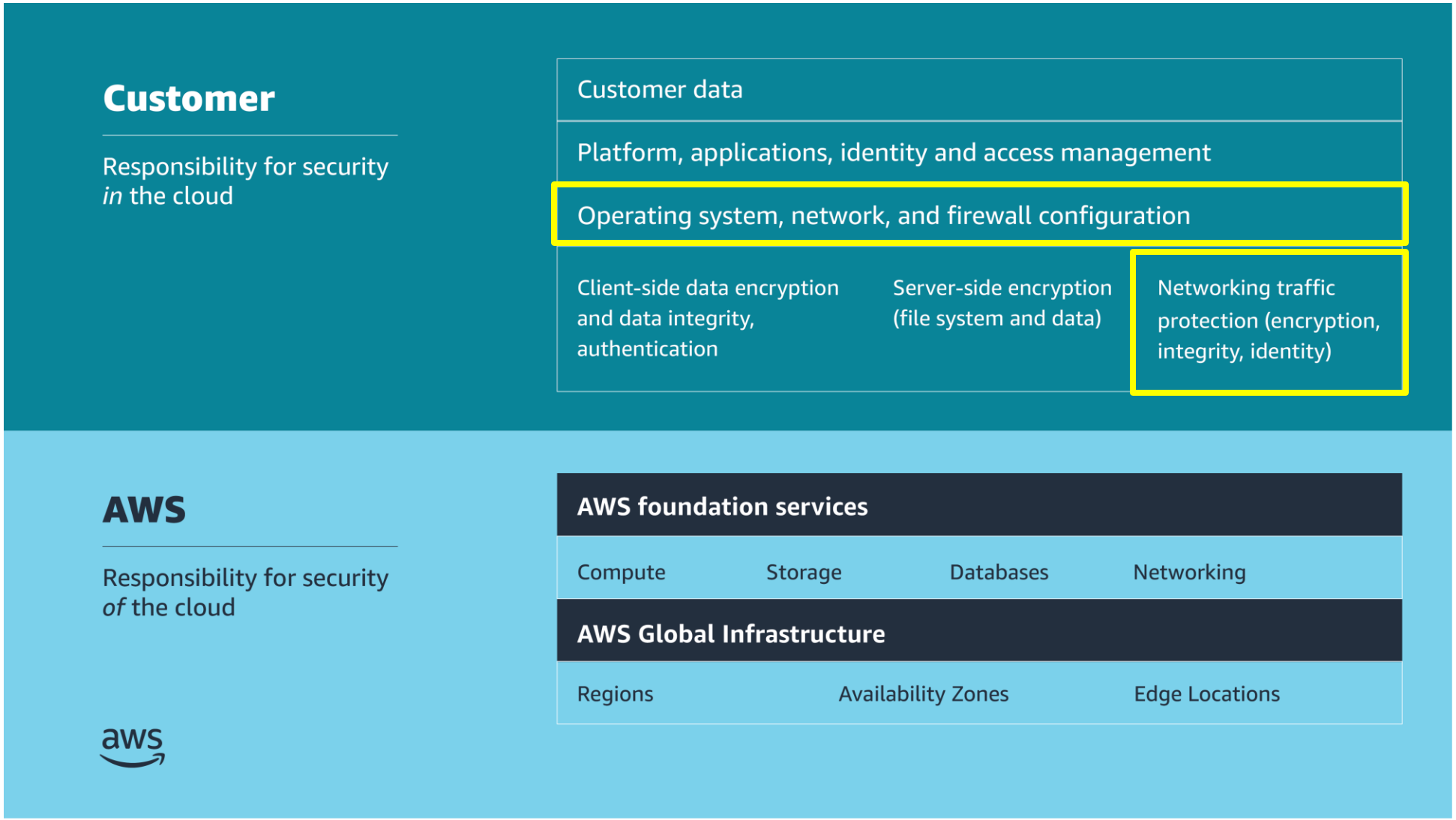
Securing Your Infrastructure

AWS Academy Cloud Security Foundations

Introduction

Securing Your Infrastructure

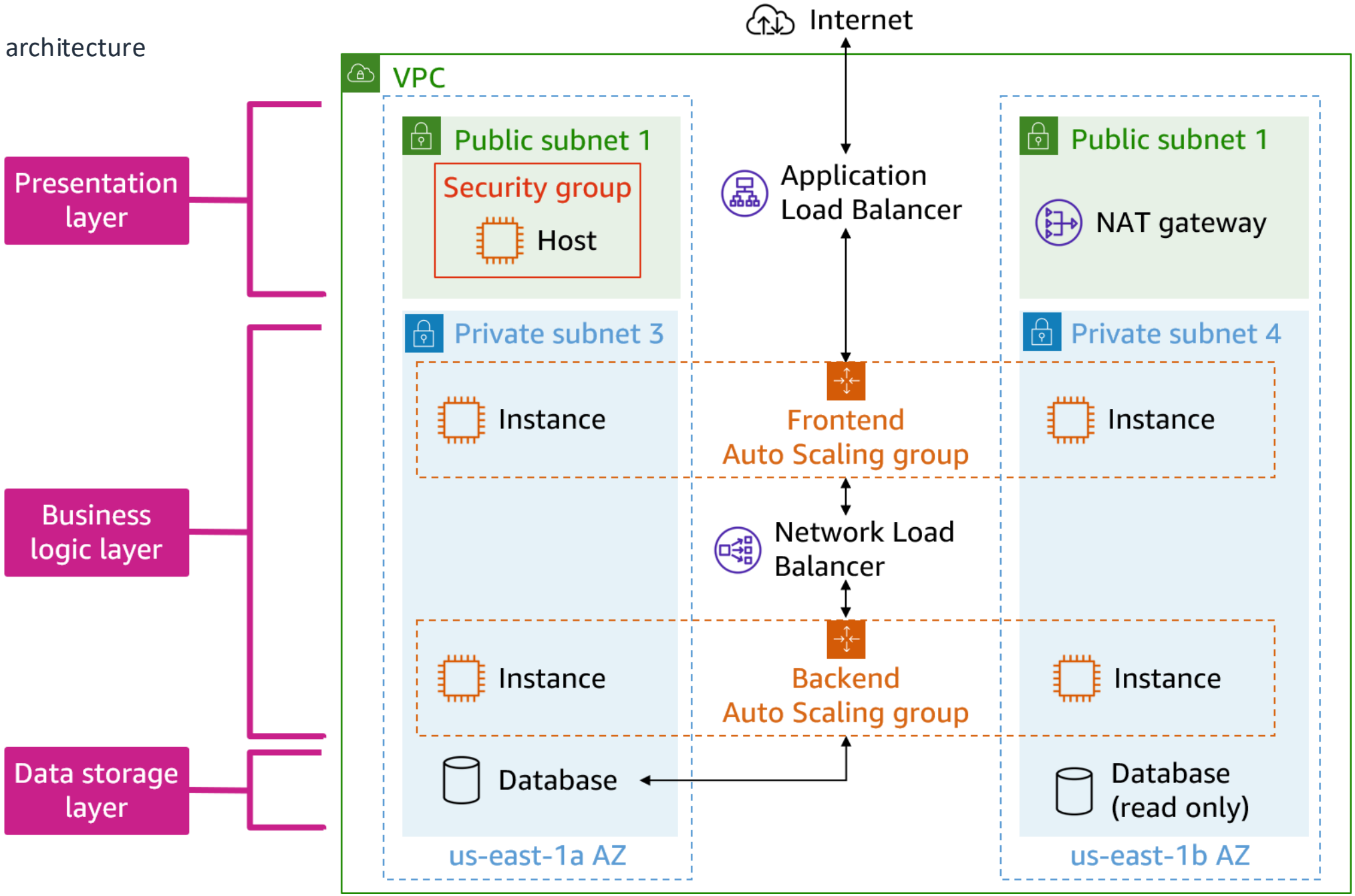
Shared responsibility model



Structure of a three-tier web application

Securing Your Infrastructure

Three-tier architecture



Using a VPC

Securing Your Infrastructure

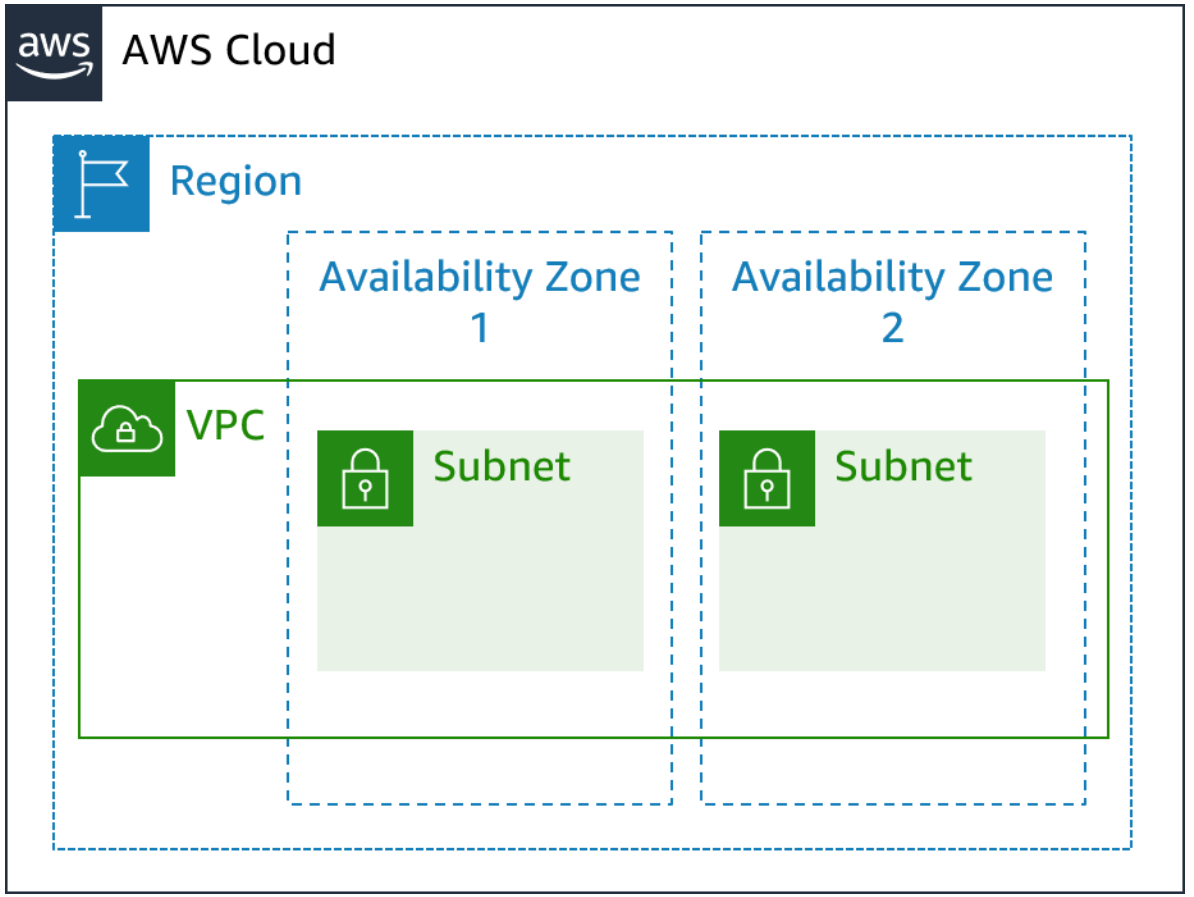
Amazon Virtual Private Cloud (Amazon VPC)

- Provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define.
- Control your virtual networking resources, including the following:
  - Select the IP address range.
  - Create subnets.
  - Configure route tables and network gateways.
- Customize the network configuration for your VPC.
- Use multiple layers of security.

Amazon Virtual Private Cloud (Amazon VPC)

VPCs and subnets

- VPC
  - Is logically isolated from other VPCs
  - Is dedicated to your AWS account
  - Belongs to a single AWS Region and can span multiple Availability Zones
- Subnet
  - Is a range of IP addresses that divide a VPC
  - Belongs to a single Availability Zone
  - Is classified as public or private



Setting up public and private subnets and internet protocols

Securing Your Infrastructure

Internet gateway

- Provides a target in your VPC route tables for internet-routable traffic
- Performs network address translation (NAT) for instances that have been assigned public IPv4 addresses
- Supports IPv4 and IPv6 traffic
- Doesn't incur an additional charge in your account

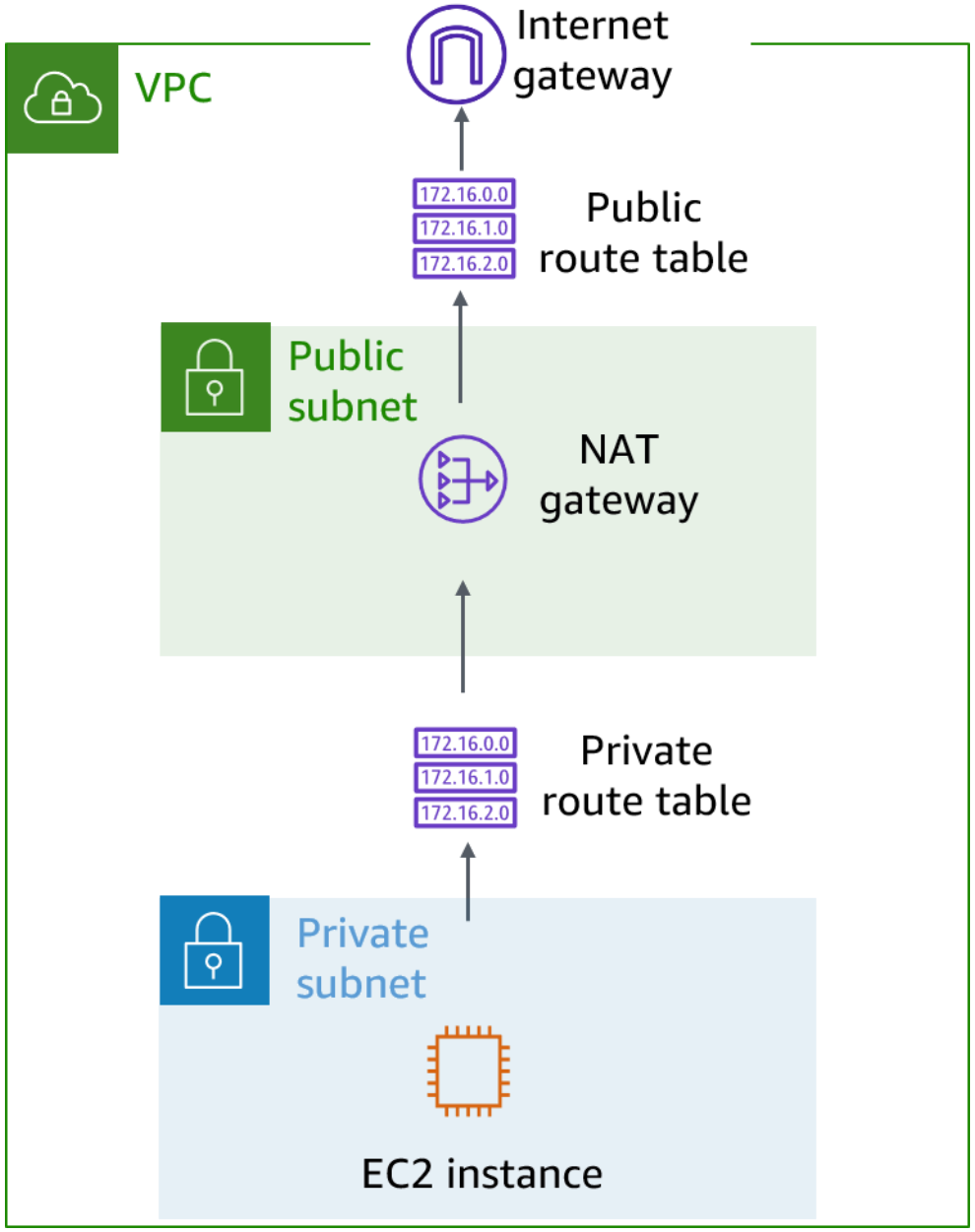
NAT gateway

- Supports instances in a private subnet to connect to the internet or other AWS services
- Prevents the internet from initiating a connection to those instances
- Requires that you specify the following at creation:
  - Public subnet in which the NAT gateway should reside
  - An Elastic IP address to associate with the NAT gateway
- After creation, requires that you update the route table for one or more of your private subnets to direct internet-bound traffic to the NAT gateway

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html

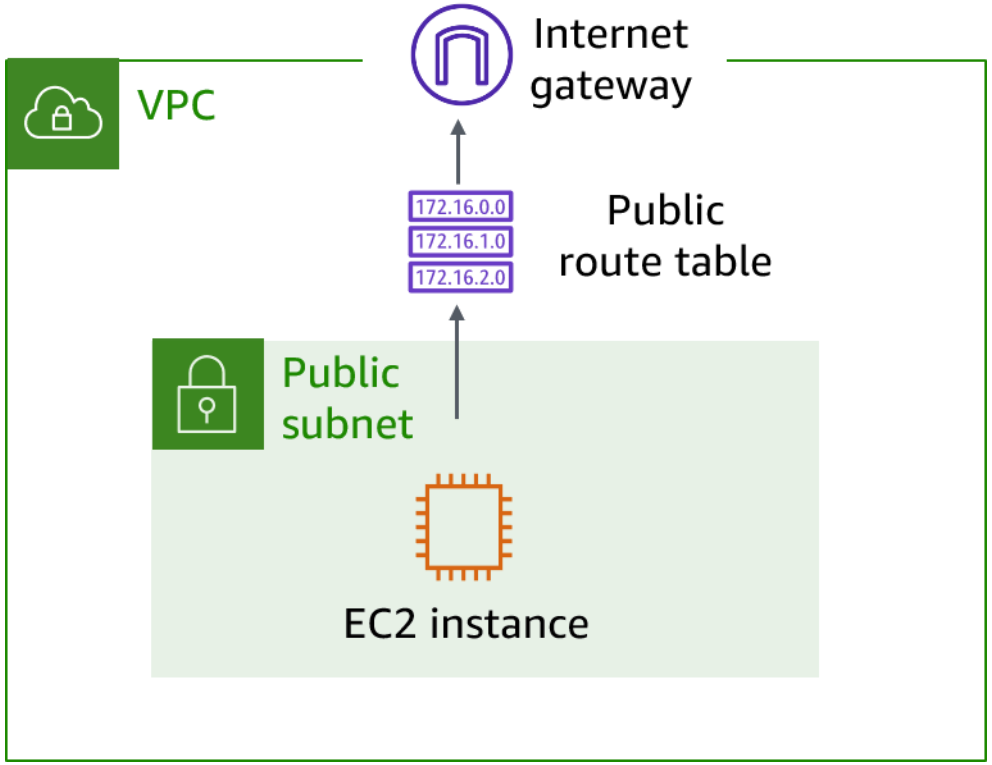
Private subnet

- All subnets consist of a contiguous range of IP addresses.
- Interfaces that are attached to instances in private subnets cannot be reached from outside the parent VPC.
- Private subnets are often used to host database instances that don't need to be accessed through the public internet.



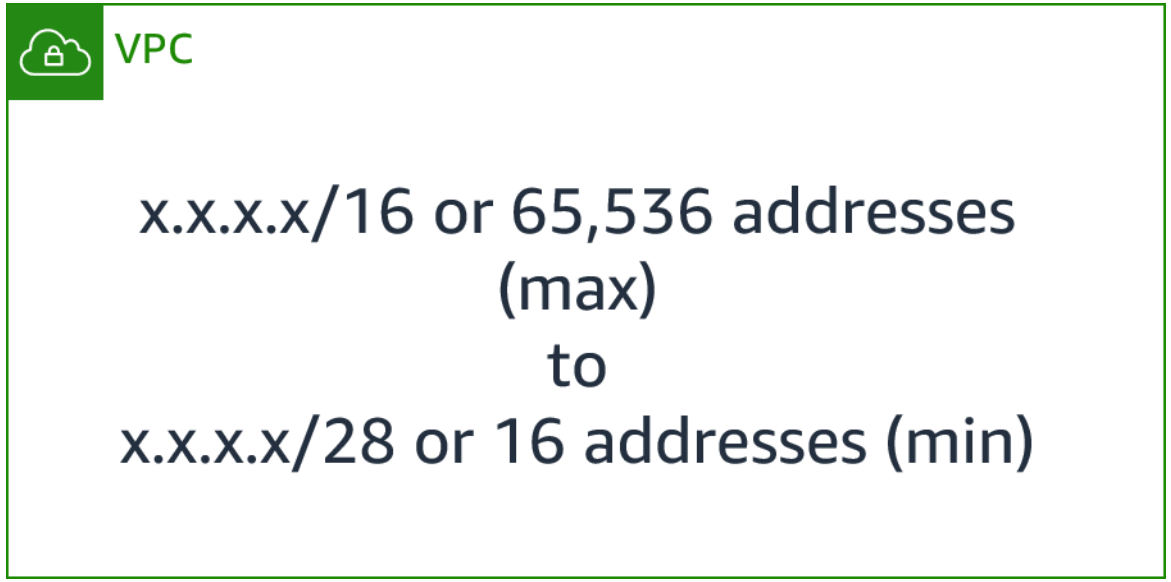
Public subnet

- When external traffic needs to reach an interface, such as an Amazon Elastic Compute Cloud (Amazon EC2) instance, the interface requires the following:
  - A public IP address must be assigned to an EC2 instance.
  - The subnet's route table must include an entry to the interface.
- With these two factors in place, the subnet is considered to be a public subnet.



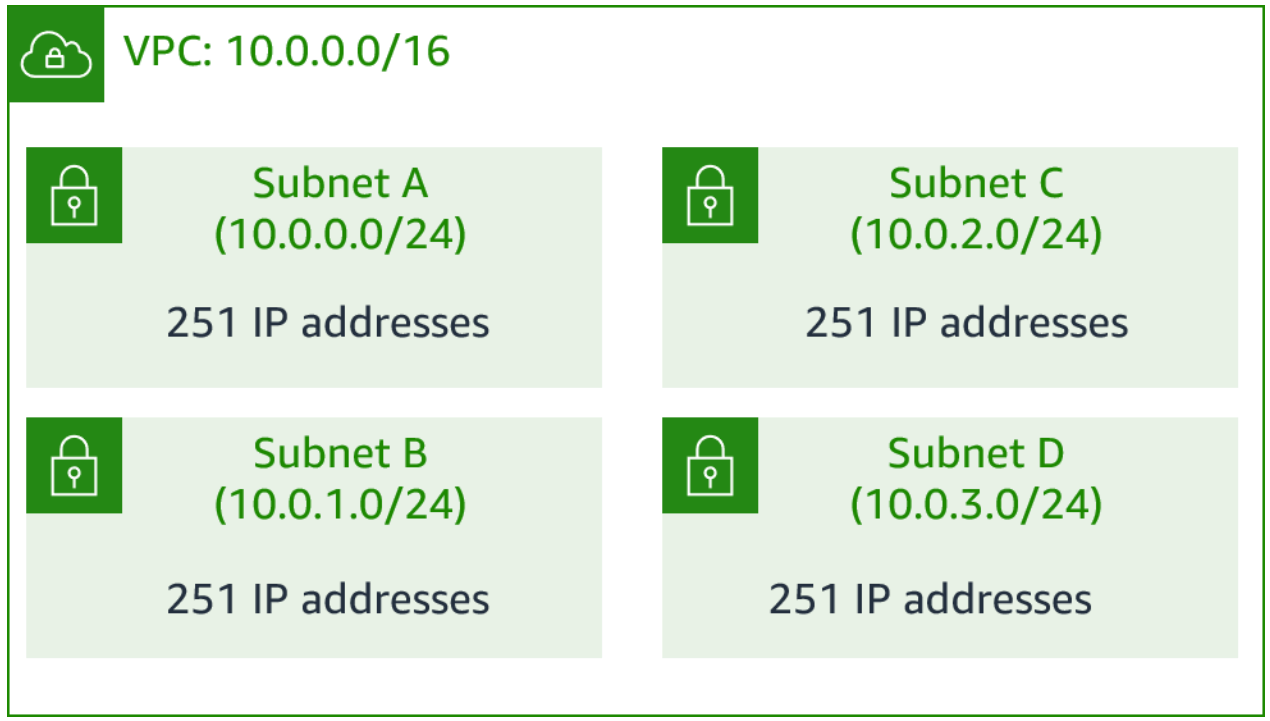
IP addressing

- When you create a VPC, you assign a CIDR range (a range of private addresses).
- You cannot change the range in a VPC or subnet, but you can add more CIDR ranges to your VPC.
- The largest CIDR block size is /16, and the smallest is /28.
- The CIDR ranges of subnets shouldn't overlap.



Reserved IP addresses

Example: A VPC with an IPv4 CIDR block of 10.0.0.0/16 has 65,536 total IP addresses. The VPC has four subnets, all with /24 CIDR blocks. Although each subnet has 256 IP addresses, only 251 IP addresses are available for use in each.



IP Addresses for CIDR Block 10.0.0.0/24	Reserved for
10.0.0.0	Network address
10.0.0.1	Internal communication
10.0.0.2	Domain Name System (DNS) resolution
10.0.0.3	Future use
10.0.0.255	Network broadcast address

Public IP address

- A public IP address is an IP address that is used to access the internet.
- A public IP address can be automatically assigned if you modify the subnet's auto-assign public IP address properties.
- Public IP addresses are dynamic. If you stop or start your instance, a new public IP is assigned. For production projects, use an Elastic IP address rather than an assigned public IP, which will be dissociated if you stop the instance.

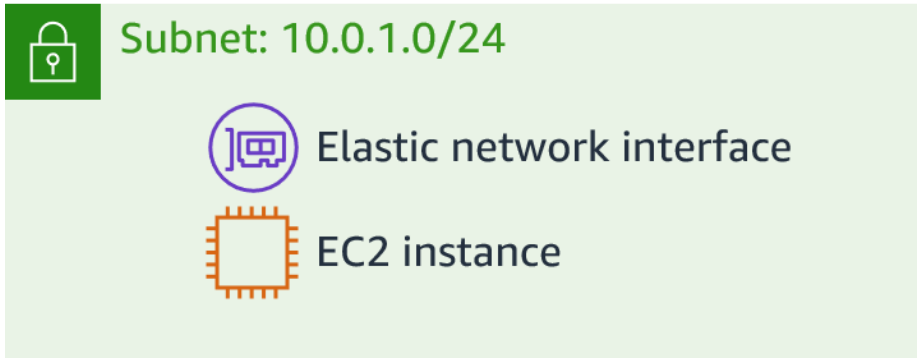
Elastic IP address

- Is associated with an AWS account
- Is static and doesn't change over time
- Comes from Amazon's pool of IPv4 addresses
  - If you unassign an Elastic IP address, you are charged until you remove it completely.

Elastic IP addresses get allocated to your account and stay the same. Use an Elastic IP address when you work on a long-term project and configuring IP addresses can be time-consuming.

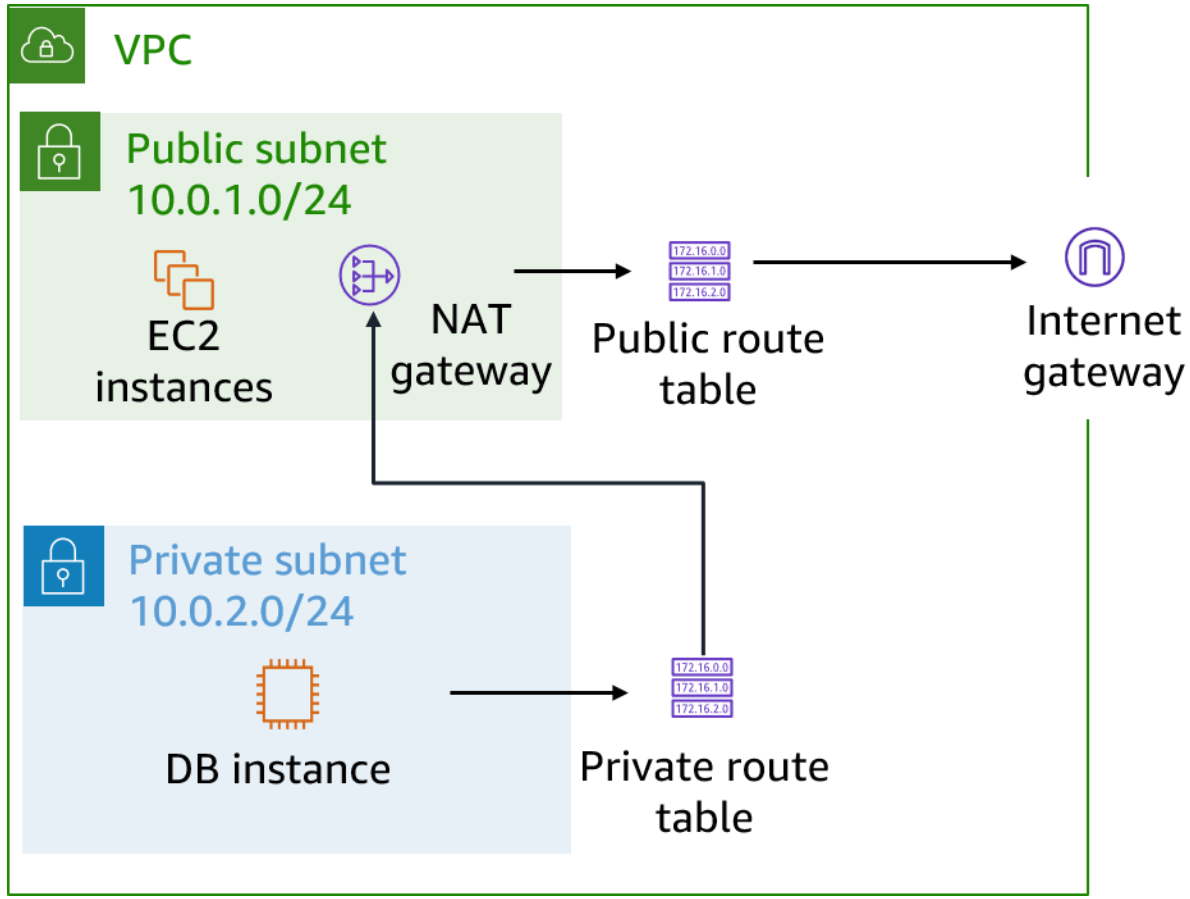
Elastic network interface

- An elastic network interface is a virtual network interface. You can do the following:
  - Attach it to an instance.
  - Detach it from the instance, and attach it to another instance to redirect network traffic.
- Its attributes follow when it is reattached to a new instance.
- Each instance in your VPC has a default network interface, which can be assigned a private IPv4 address from your VPC's range.



Route tables and routes

- A route table contains a set of rules (or routes), which you can configure to direct network traffic from your subnet.
- Each route specifies a destination and a target.
- By default, every route table contains a local route for communication within the VPC.
- Each subnet should have its own route table.



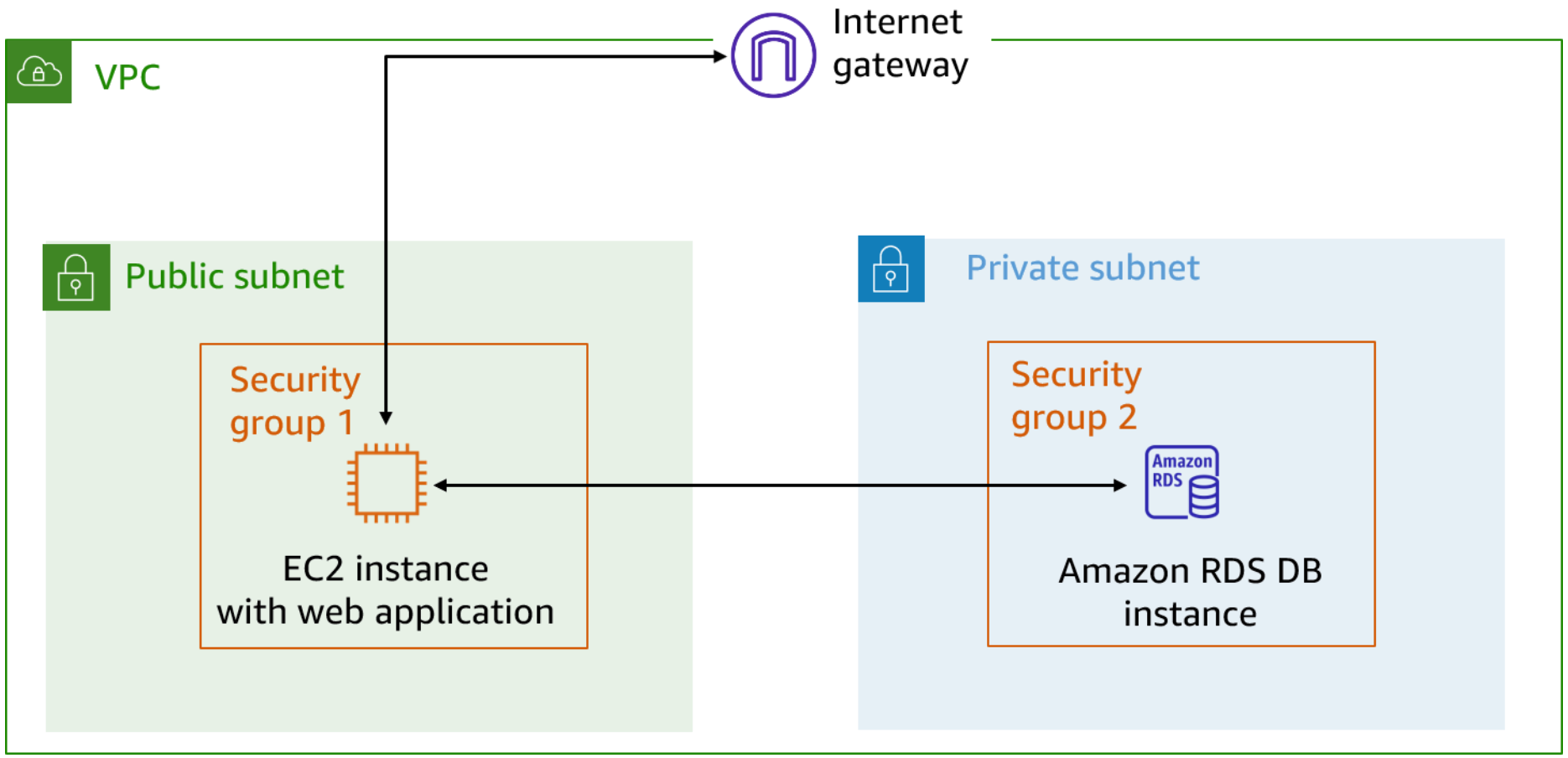
Key takeaways: Setting up public and private subnets and internet protocols

- Public subnets are used when external traffic needs to reach an interface, such as an EC2 instance.
- Private subnets are often used to host database instances that don't need to be accessed through the public internet.
- Route tables determine where traffic is routed in your VPC.

Using AWS security groups

Securing Your Infrastructure

Security groups (1 of 2)



Security groups (2 of 2)

- Security groups have rules that control inbound and outbound instance traffic.
- Default security groups deny all inbound traffic and allow all outbound traffic. This is considered *stateful*.

Inbound

Source	Protocol	Port Range	Description
sg-xxxxxxxx	All	All	Allow inbound traffic from network interfaces that are assigned to the same security group.

Outbound

Destination	Protocol	Port Range	Description
0.0.0.0/0	All	All	Allow all outbound IPv4 traffic.
::/0	All	All	Allow all outbound IPv6 traffic.

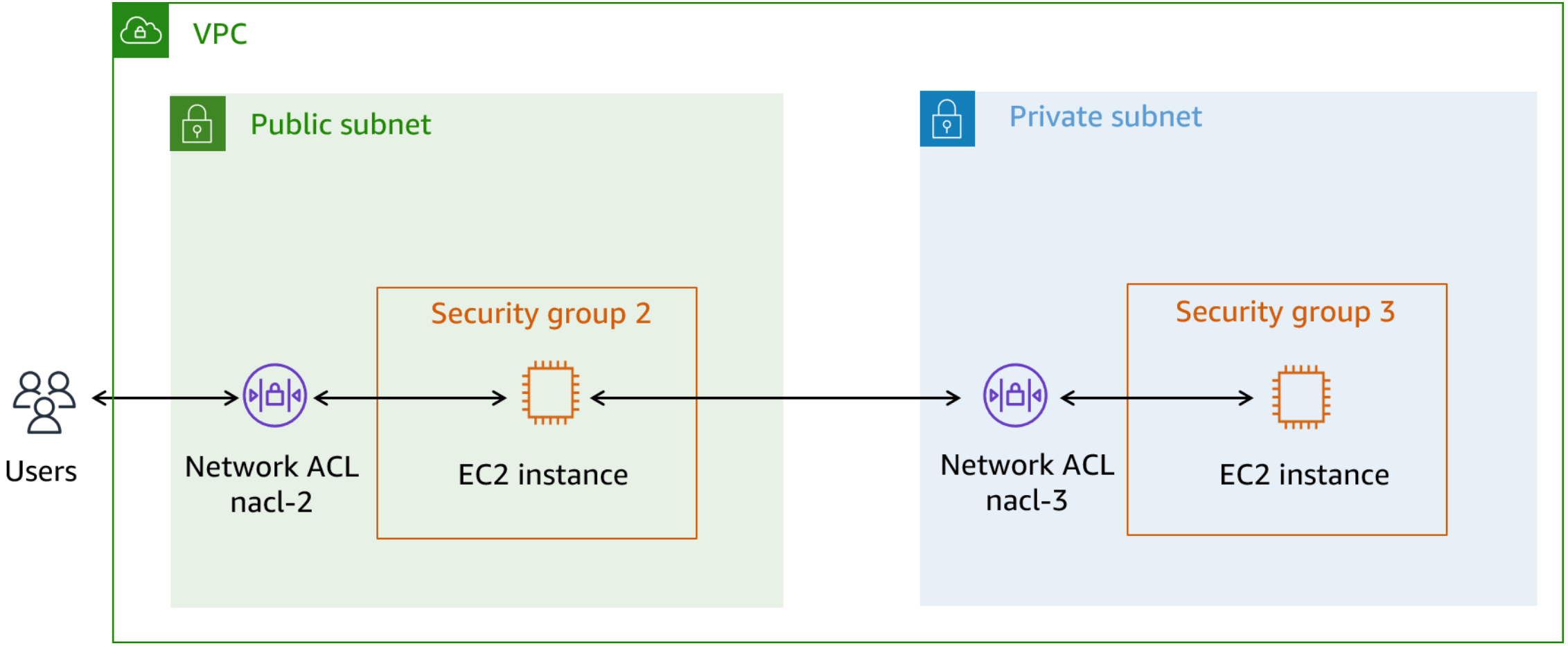
Key takeaways: Using AWS security groups

- A security group acts as a virtual firewall for an instance to control inbound and outbound traffic.
- Security groups are stateful, which means that state information is kept even after a request is processed.
- All rules are evaluated before a decision is made to allow traffic.

Using AWS network ACLs

Securing Your Infrastructure

Network ACLs (1 of 2)



Network ACLs (2 of 2)

- A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic. Network ACLs are stateless.
- Each VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic.
- You can create a custom network ACL and associate it with a subnet. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.

Default inbound and outbound rules

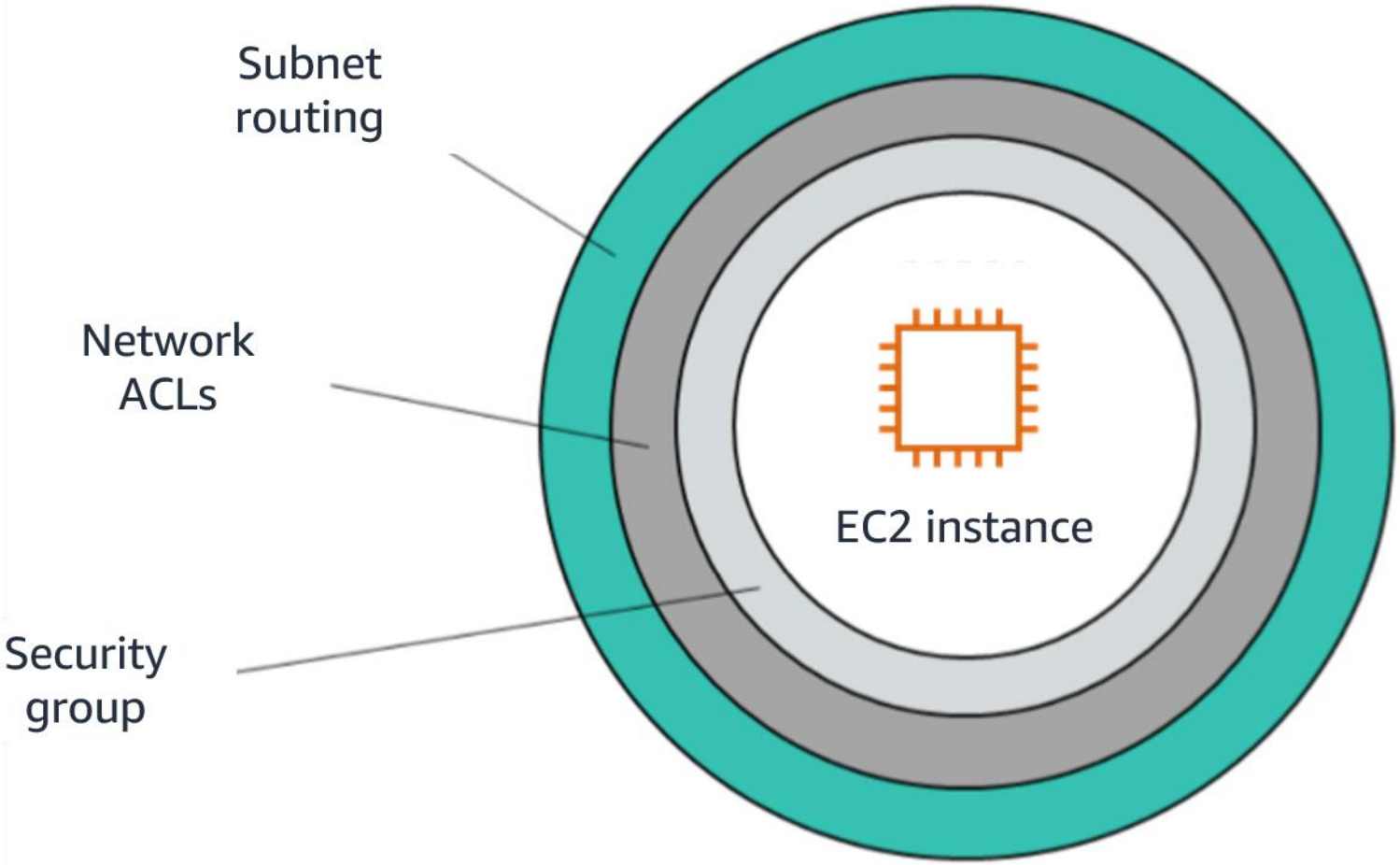
Rule	Type	Protocol	Port Range	Source	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Comparing security groups and network ACLs

Attribute	Security Groups	Network ACLs
Scope	Instance or interface level	Subnet level
Supported Rules	Allow rules only	Allow and deny rules
State	Stateful (return traffic is automatically allowed, regardless of rules)	Stateless (return traffic must be explicitly allowed by rules)
Order of Rules	All rules are evaluated before a decision is made to allow traffic	Rules are evaluated in number order before a decision is made to allow traffic

VPC security features

- Security groups
- Network ACLs
- Subnets
- Route tables



Note: VPC Flow Logs can log activity down to the interface level.

Key takeaways: Using AWS network ACLs

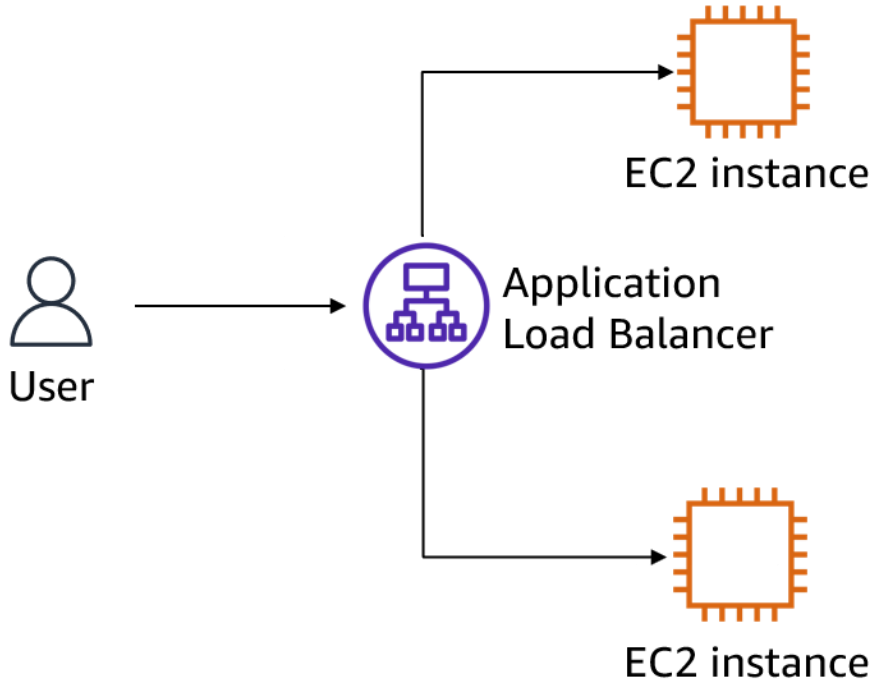
- A network ACL is an optional layer of security for your VPC and acts as a firewall to control traffic at the subnet level.
- Each subnet in your VPC must be associated with a network ACL.
- Network ACLs are stateless, which means that responses to inbound traffic are subject to the rules for outbound traffic (and vice versa).
- Rules are evaluated in number order before a decision is made to allow traffic.

Using AWS load balancers

Securing Your Infrastructure

Elastic Load Balancing (ELB)

- Distributes incoming application traffic
- Supports high availability
- Performs health checks on instances
- Provides the following:
  - Application Load Balancer
  - Network Load Balancer
  - Classic Load Balancer



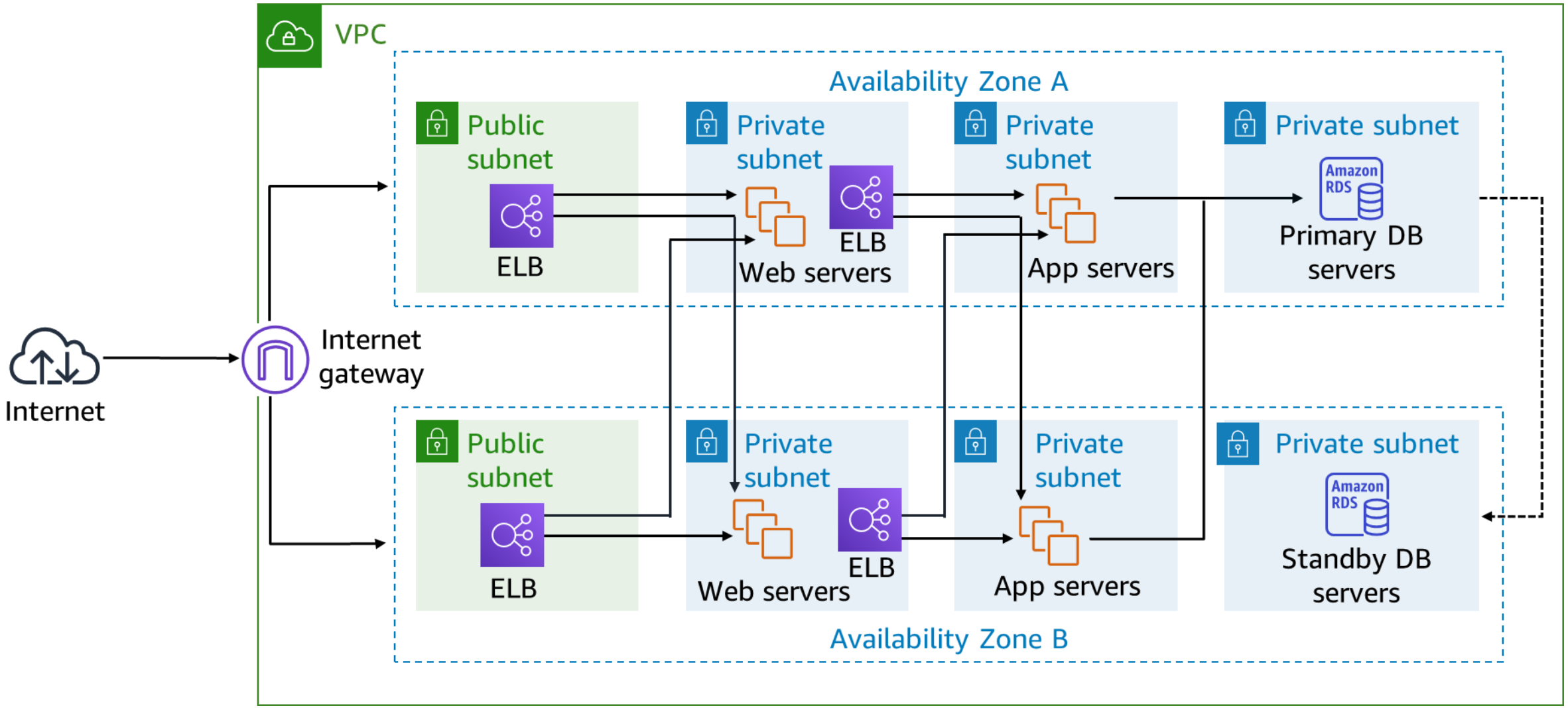
Data protection in ELB

Single point of contact

Encryption at rest

Encryption in transit

Load balancers in action



Key takeaways: Using AWS load balancers

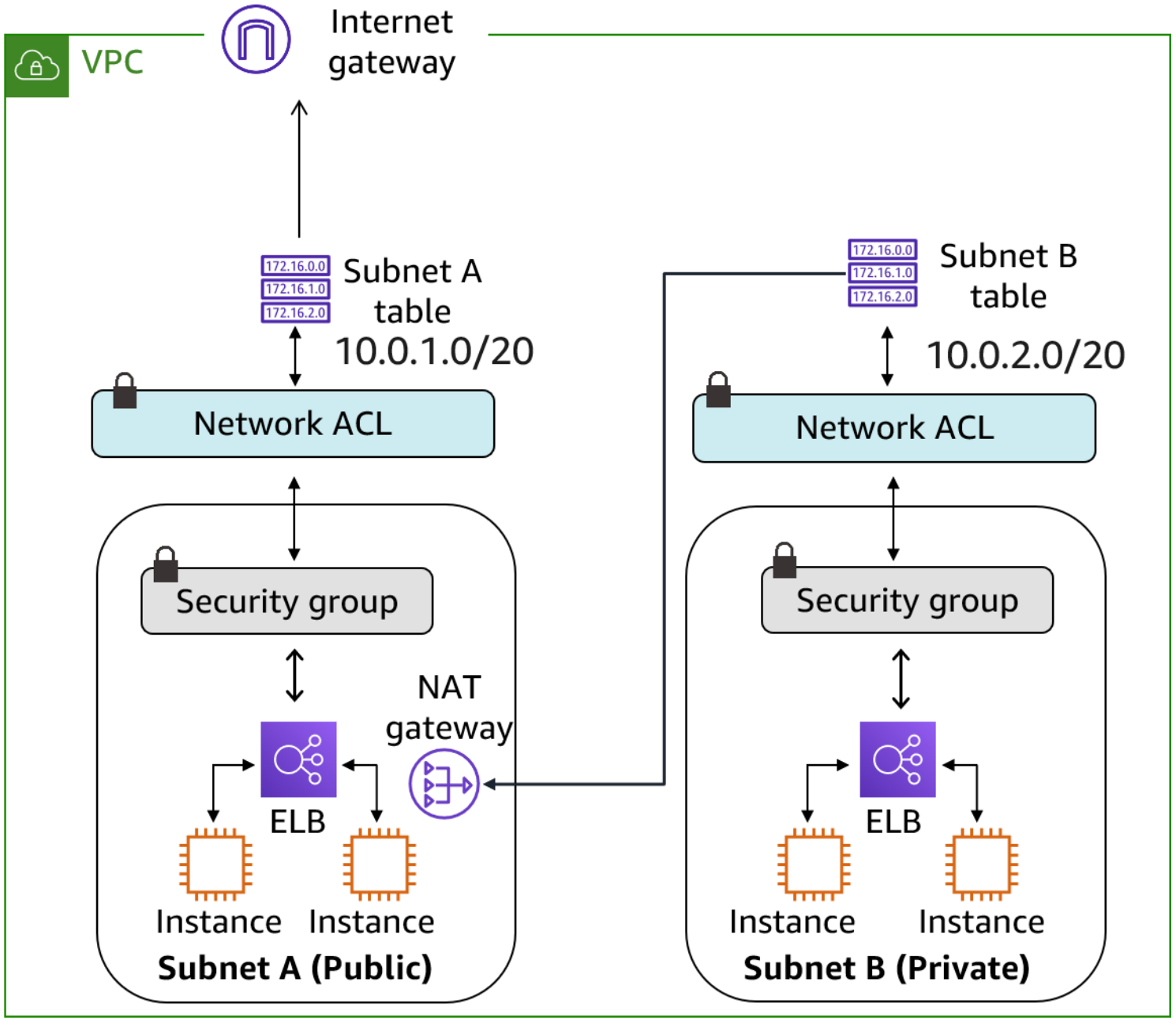
- ELB automatically distributes incoming application traffic across multiple targets, such as EC2 instances, containers, IP addresses, and Lambda functions.
- ELB can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones.
- You can add and remove instances from your load balancer as your needs change, without disrupting the overall flow of requests to your application.

Pulling it all together

Securing Your Infrastructure

Workflow

VPC
10.0.0.0/16 (IPv4)
2001:db8:1234:1a00::/56 (IPv6)



Best practices to protect your network

- Control traffic at all layers.
- Inspect and filter your traffic at the application level.
- Automate network protection.
- Limit exposure.

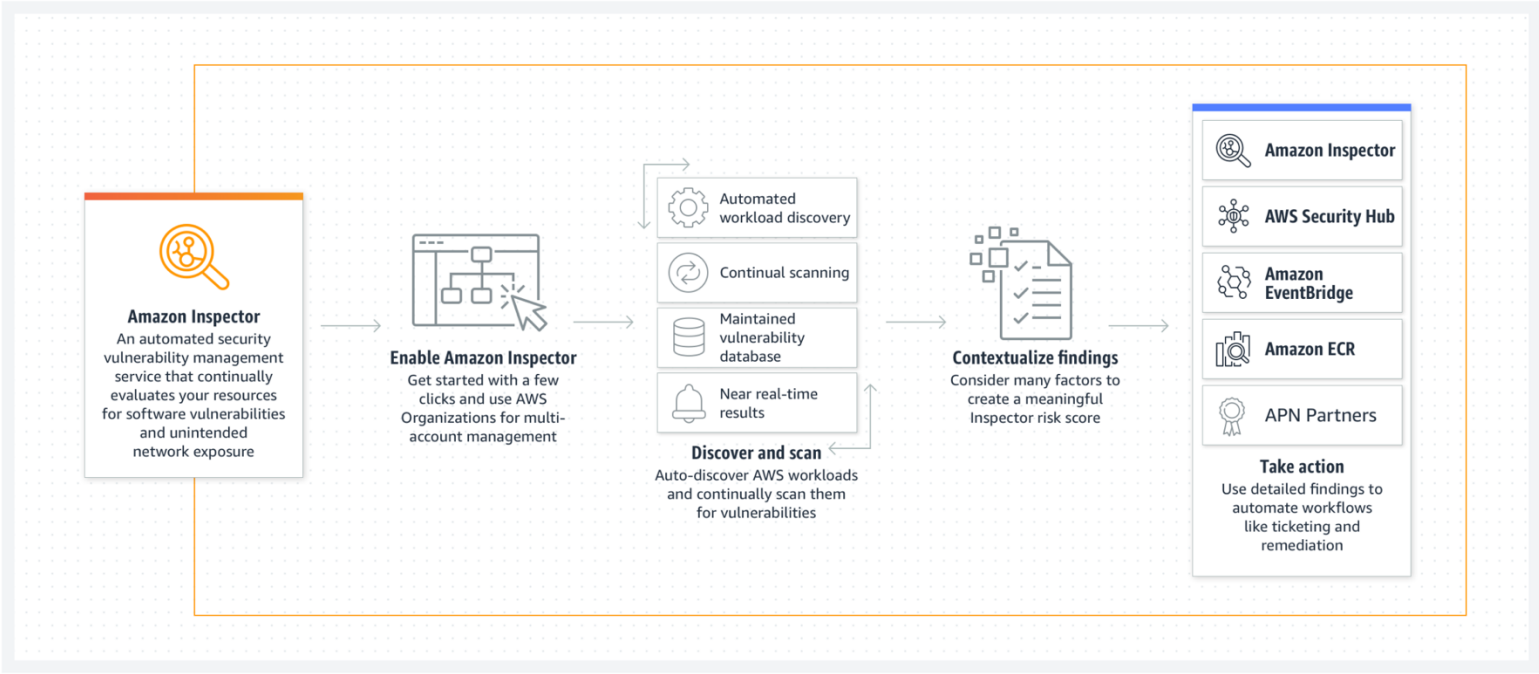
Protecting your compute resources

Securing Your Infrastructure

Amazon Inspector

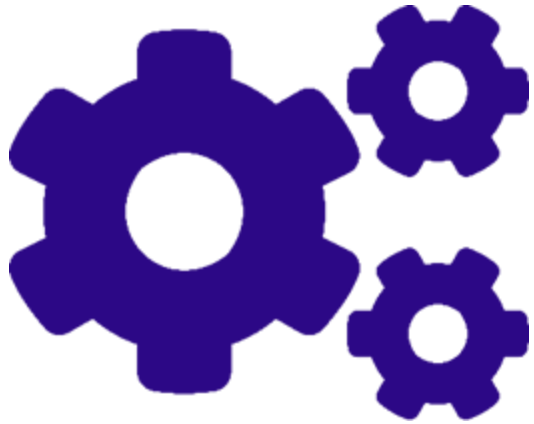
- Run automated security assessments on EC2 instances and applications.
- Identify application security issues.
- Enforce security standards and best practices.
- Generate assessment reports.

Amazon Inspector



Security benefits of Amazon Inspector

- Automate tasks to help you respond to security issues
- Regularly monitor your resources
- Benefit from AWS security expertise
- Integrate security into DevOps



AWS Systems Manager

- Amazon Inspector uses the widely deployed AWS Systems Manager Agent (SSM Agent) to collect the software inventory and configurations from your EC2 instances.

- The collected application inventory and configurations are used to assess workloads for vulnerabilities.

AWS Systems Manager

Sample exam question

A system administrator created a single EC2 instance, and set up network ACLs and the appropriate subnet routing. However, they want to provide an extra layer of security by applying a firewall to control access to and from the EC2 instance. Which action should the system administrator take?

Choice	Response
A	Create a network ACL.
B	Configure a security group.
C	Update the subnet route tables.
D	Set up a load balancer.

Sample exam question answer

A system administrator created a single EC2 instance, and set up network ACLs and the appropriate subnet routing. However, they want to provide an extra layer of security by applying a firewall to control access to and from the EC2 instance. Which action should the system administrator take?

The correct answer is B.

The keywords in the question are **applying a firewall** and **control access to and from the EC2 instance**.

Protecting Data in Your Application

AWS Academy Cloud Security Foundations

Introduction

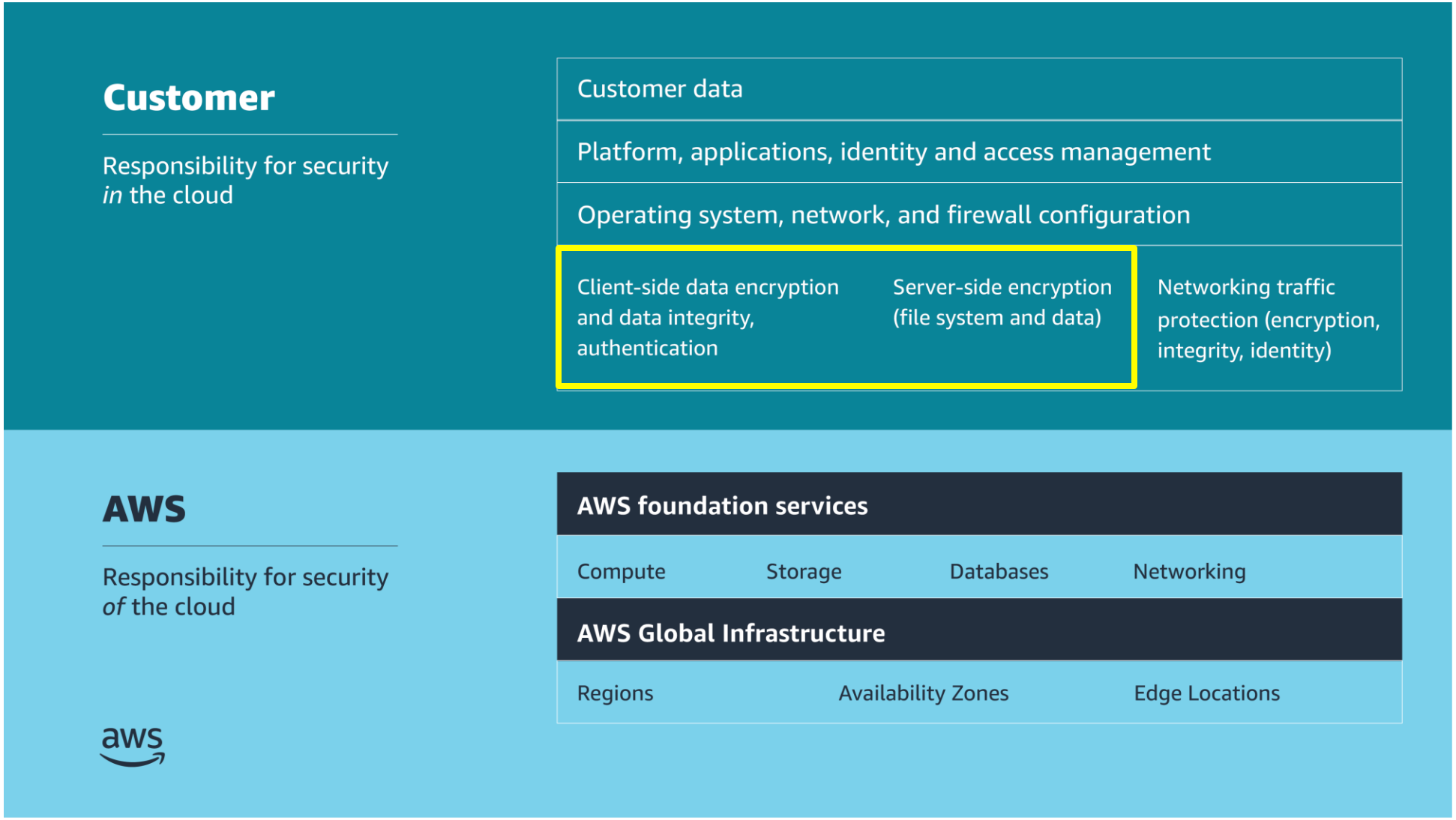
Protecting Data in Your Application

Module overview

Sections

- Protect data at rest
- Amazon S3 protection features
- Protection through encryption
- Protect data in transit
- Best practices to protect data in Amazon S3
- Additional data protection services

Shared responsibility model



Protect data at rest

Protecting Data in Your Application

Why protect data at rest?

- Common scenarios
  - Information disclosure
  - Data integrity compromise
  - Accidental or malicious deletion
  - System, hardware, and software availability
- Extra layer of protection if your system is compromised

Data at rest in Amazon S3

Data stored in Amazon S3 is private by default and requires AWS credentials for access.

- Use bucket policies for granular access to objects.
- Consider encrypting data at rest.

Granting permissions

Identity based
(Attached to an *IAM principal*)

Bob

Resource	Get	Put	List
Bucket X	ALLOW	ALLOW	ALLOW
Bucket Y	N/A	N/A	ALLOW

Resource based
(Attached to an *AWS resource*)

Bucket X

User	Get	Put	List
Bob	ALLOW	DENY	ALLOW

Bucket Y

User	Get	Put	List
Bob	ALLOW	N/A	ALLOW

Can Bob GET, PUT, or LIST for bucket X?

Can Bob GET or LIST for bucket Y?

Amazon S3 protection features

Protecting Data in Your Application

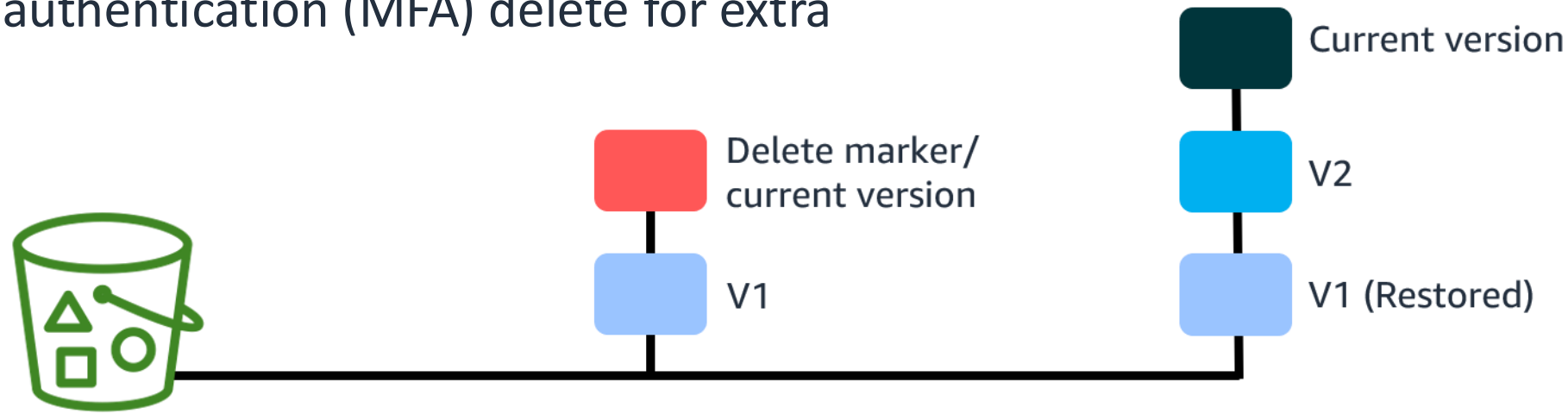
Amazon S3 Block Public Access

- Helps you manage public access to Amazon S3 resources
- Has four settings:
  - **BlockPublicAcls:** Block public access granted by new ACLs.
  - **IgnorePublicAcls:** Block public access granted by any ACLs.
  - **BlockPublicPolicy:** Block public access granted by new public bucket policies.
  - **RestrictPublicBuckets:** Block public and cross-account access by any public bucket policies.

Bucket with block public access settings

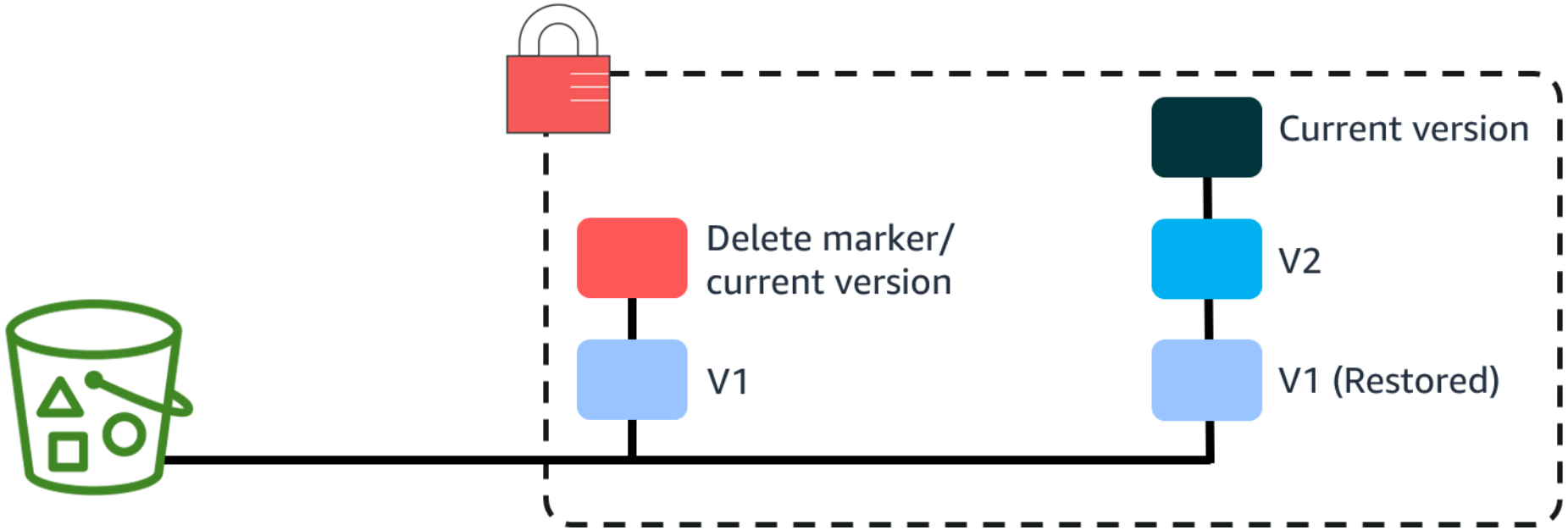
Amazon S3 Versioning

- Creates a new version with every upload
- Protects from unintended deletion
- Provides retrieval of deleted objects
- Can be used with lifecycle policies for cost savings
- Can’t be turned off once enabled (only suspended)
- Offers multi-factor authentication (MFA) delete for extra security



Amazon S3 Object Lock

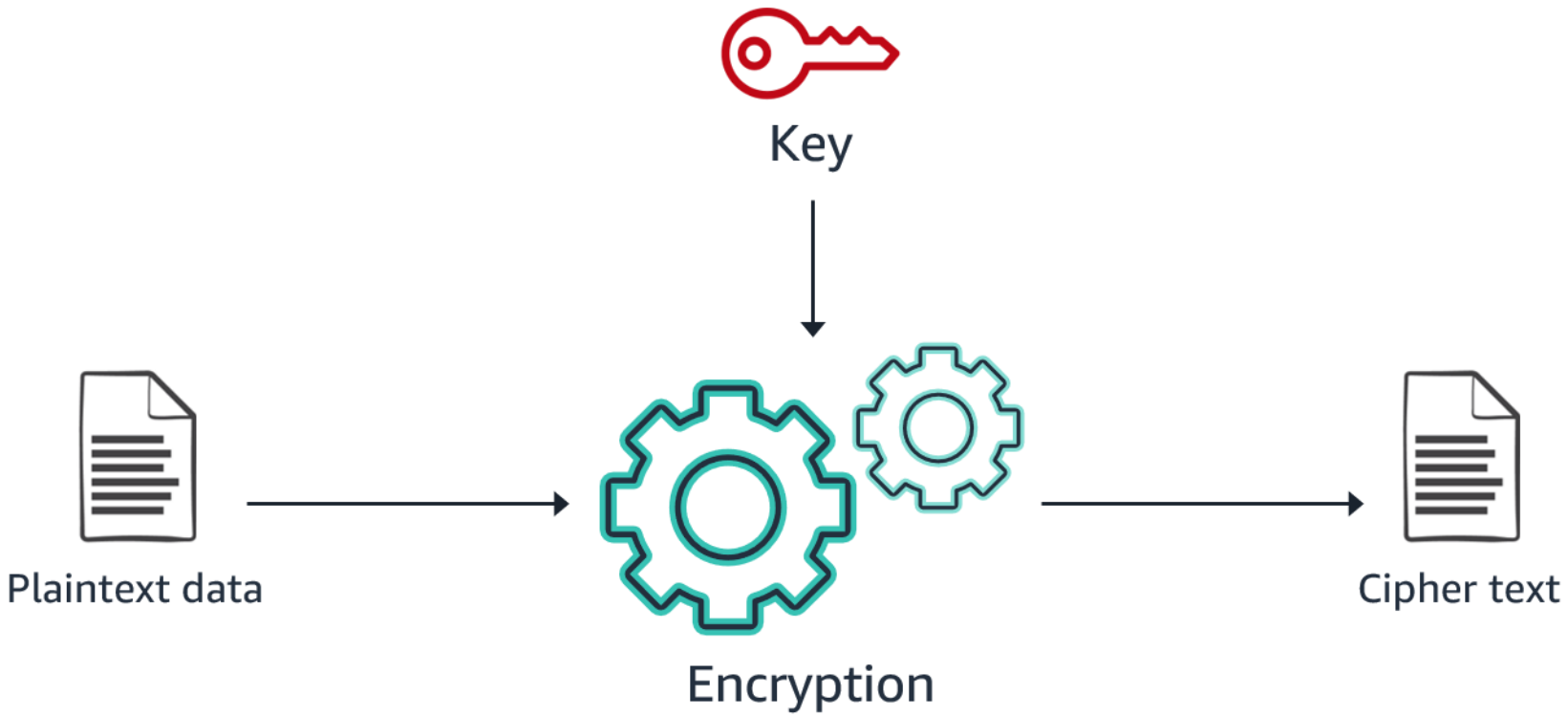
- Stores objects by using the write-once-read-many (WORM) model
- Works only in versioned buckets
- Provides the ability to manage object retention
- Provides two retention modes:
  - Governance
  - Compliance



Protection through encryption

Protecting Data in Your Application

Encryption: What, how, and why



Comparing client-side and server-side encryption

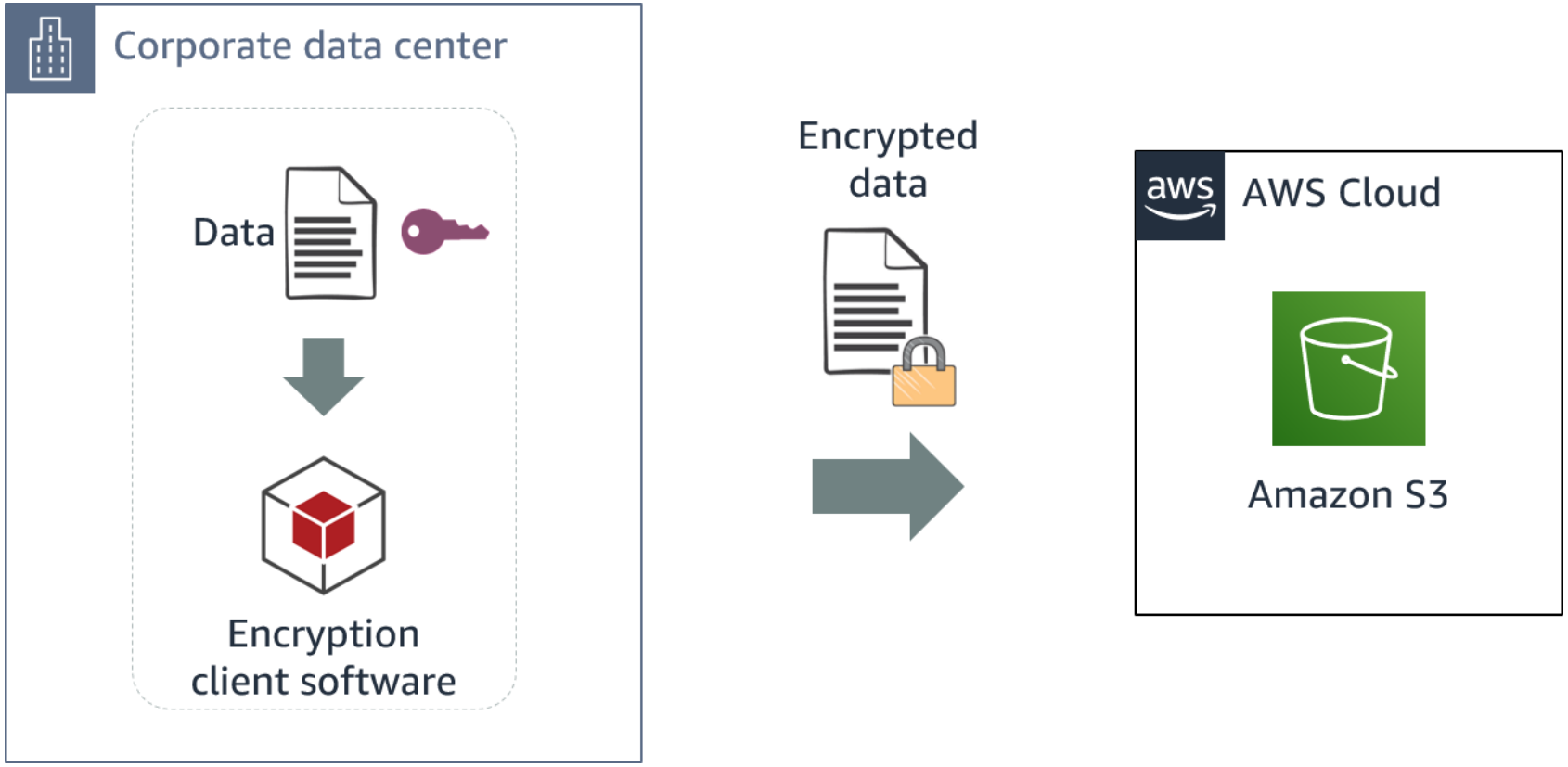
Client-side encryption (CSE)

- Your application encrypts data before sending it to AWS.
- Data is stored in its encrypted state.
- The keys and algorithms are known only to you.

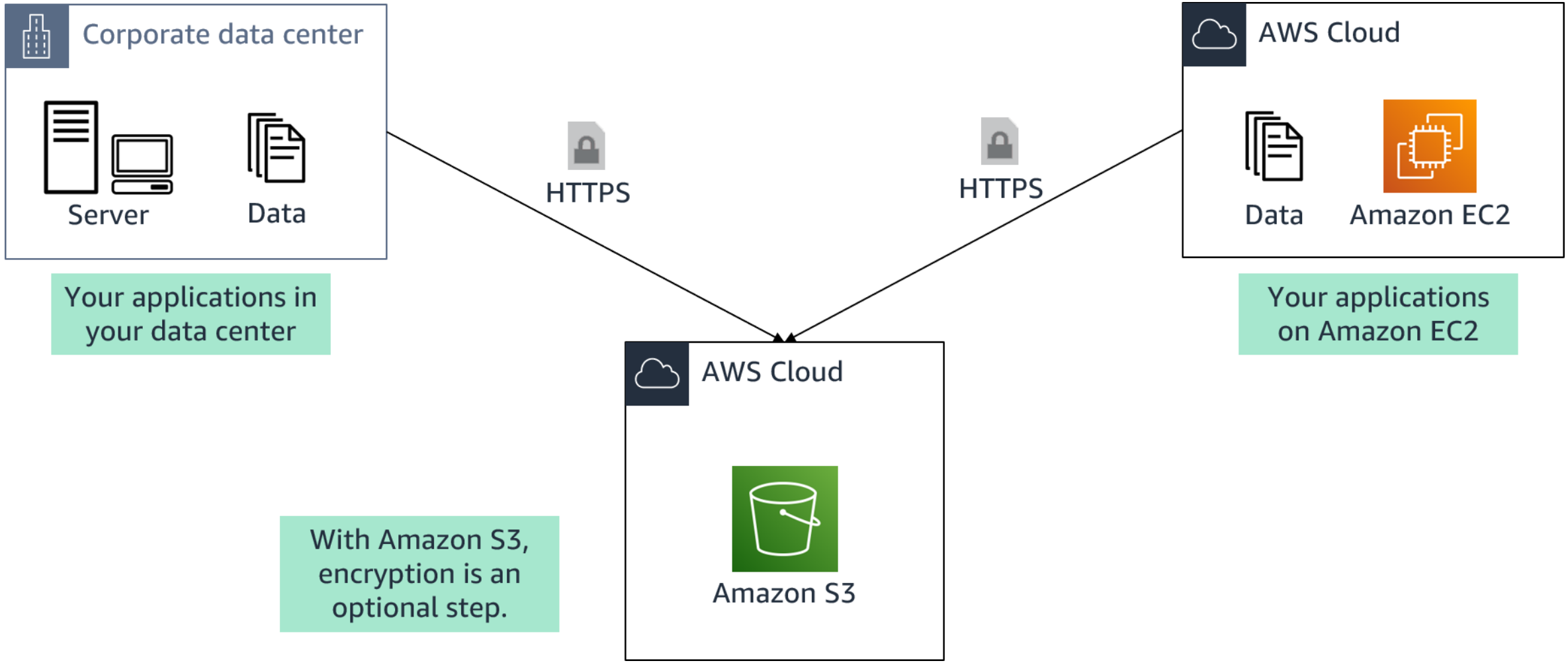
Server-side encryption (SSE)

- AWS encrypts data on your behalf after receiving it.
- The process is transparent to the user.

Client-side encryption



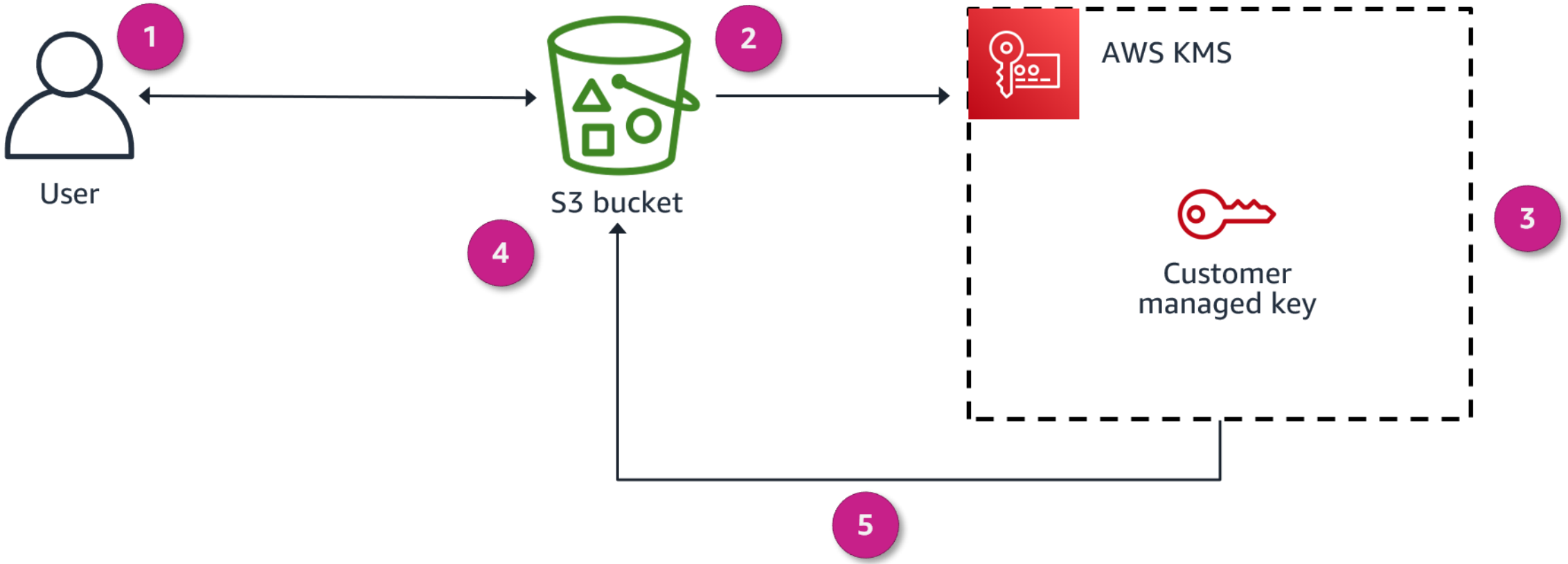
AWS server-side encryption



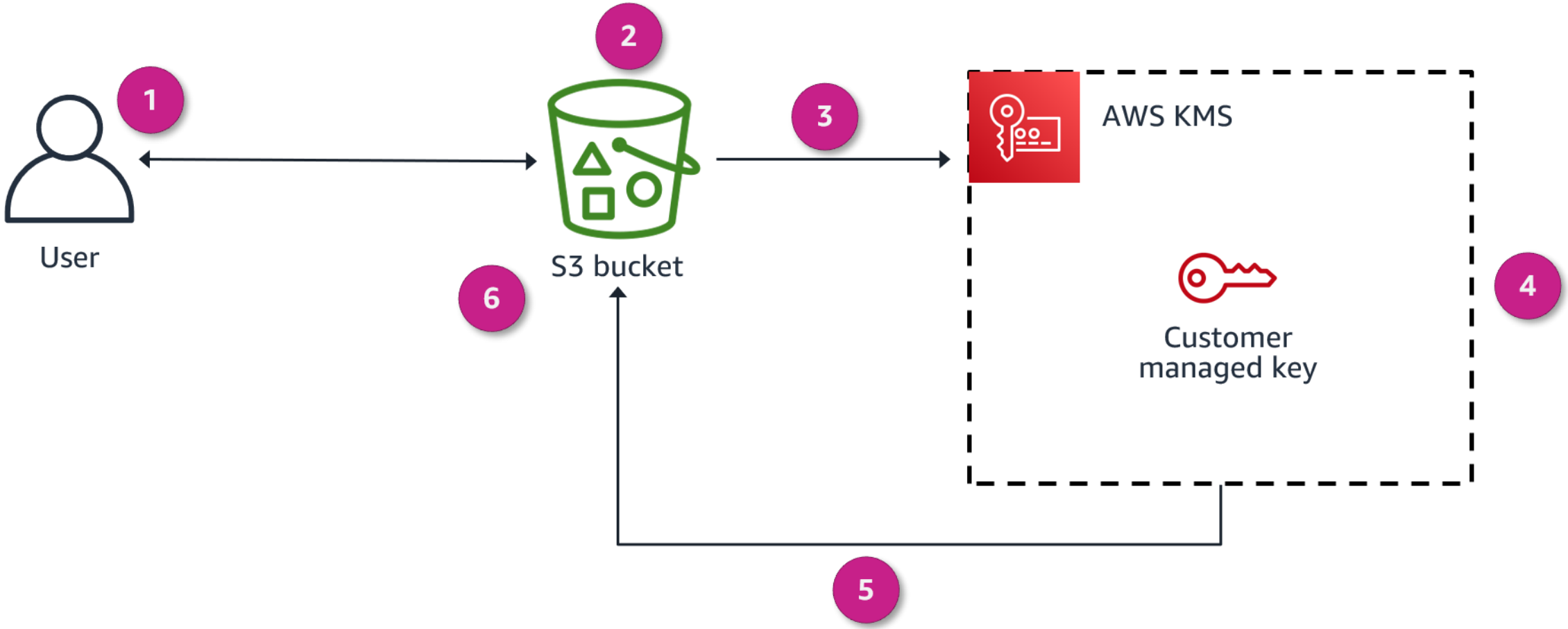
Types of Amazon S3 server-side encryption

SSE-C	SSE-S3	SSE-KMS
• You retain control of the keys. • Amazon S3 doesn't store the encryption keys that you provide.	• AWS manages the keys. • The encrypted data and keys are stored in separate hosts.	• AWS manages the keys. • An envelope key is used for added protection.

Encryption overview



Decryption overview

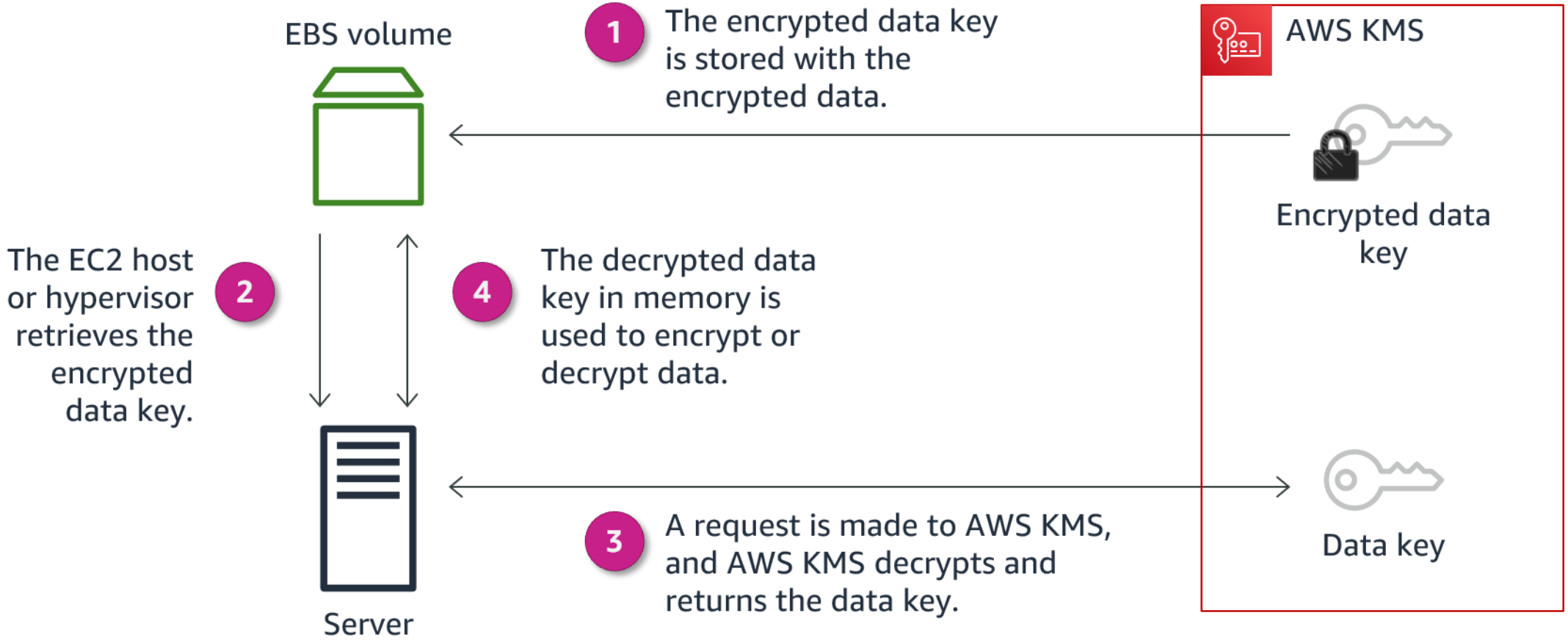


AWS Key Management Service (AWS KMS)

- Provides the ability to create and manage cryptographic keys
- Uses hardware security modules (HSMs) to protect your keys
- Is integrated with other AWS services
- Provides the ability to set usage policies to determine which users can use keys

AWS Key Management Service (AWS KMS)

AWS KMS example with Amazon EBS



Key takeaways: Protection through encryption

- AWS supports both client-side and server-side encryption.
  - CSE: You encrypt your data before sending it to AWS.
  - SSE: AWS encrypts data on your behalf after receiving it.
- AWS provides three types of SSE:
  - SSE with customer-provided keys (SSE-C)
  - SSE with Amazon S3 managed keys (SSE-S3)
  - SSE with AWS KMS keys (SSE-KMS)
- AWS KMS can create and control the keys used to encrypt your data.

Protect data in transit

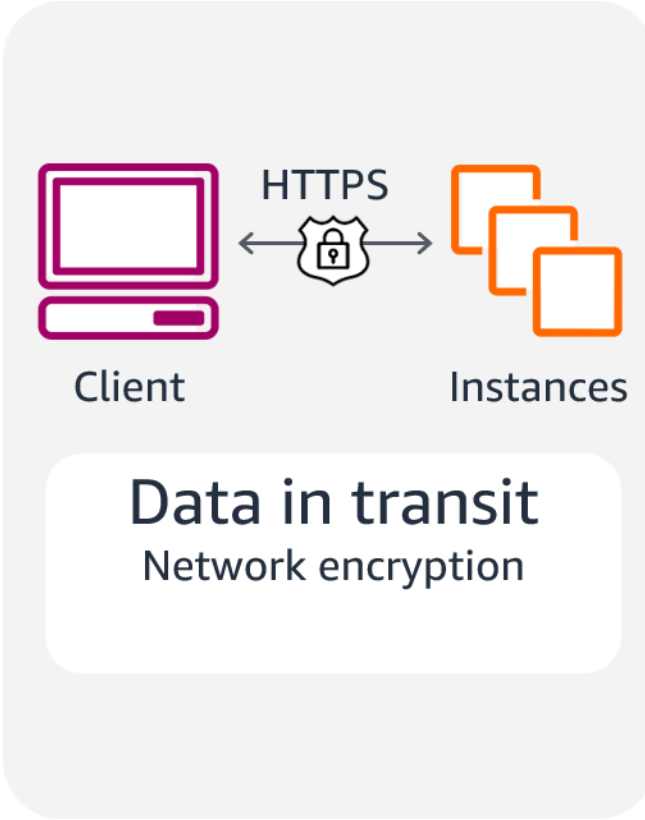
Protecting Data in Your Application

Why protect data in transit?

- Your communications might go through the public internet.
- What are the risks that data in transit is exposed to?
  - Accidental information disclosures
  - Data integrity compromises
  - Identity compromises
    - Man-in-the-middle (MITM) attacks
    - Identity spoofing

Protecting data in transit

- Use Secure Sockets Layer (SSL) endpoints over Transport Layer Security (TLS) (HTTPS).
- Use encryption.
- Use Amazon Virtual Private Cloud (Amazon VPC) endpoints to limit access to your bucket.



Protecting remote connections to servers

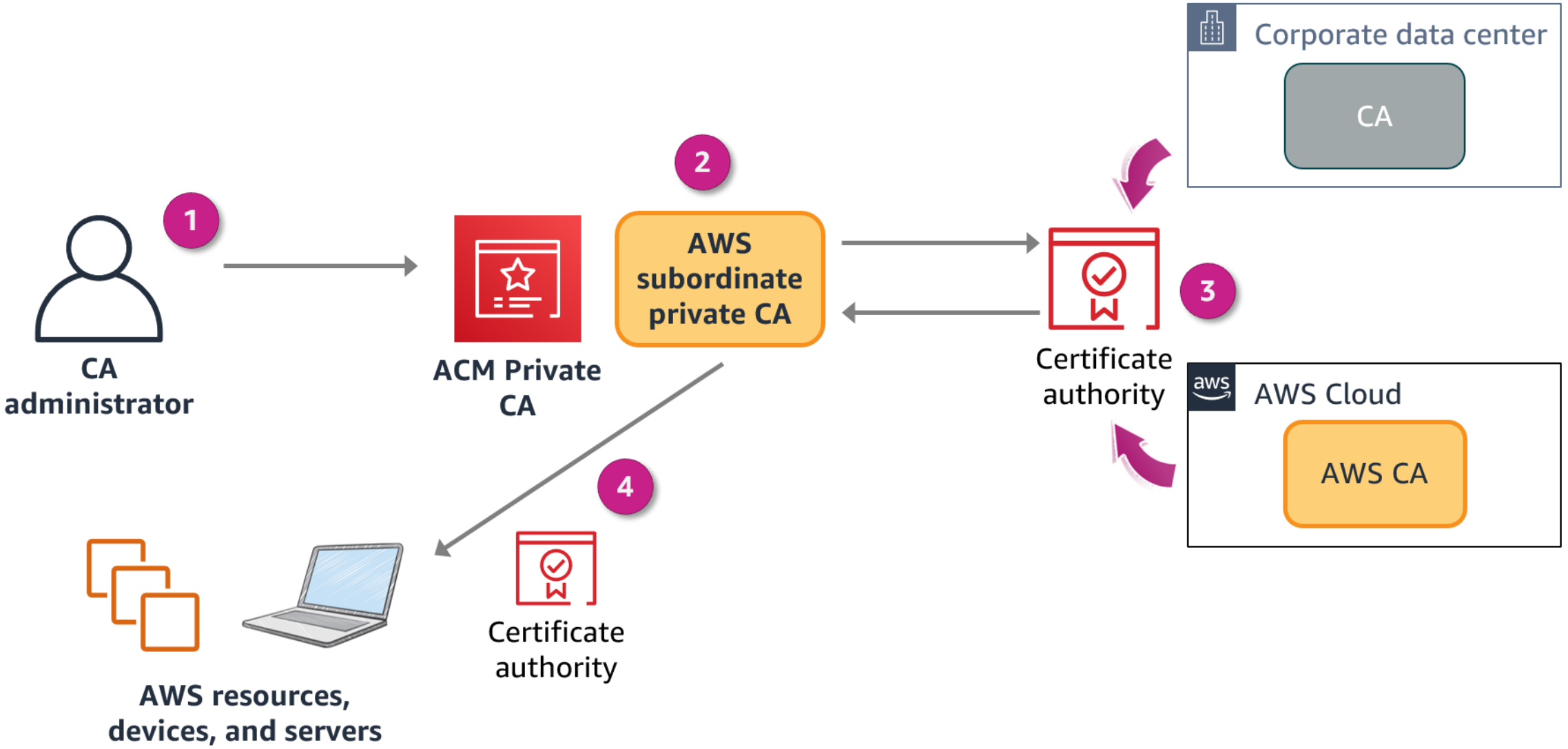
- Remote Desktop Protocol (RDP) is typically used for Windows servers.
  - RDP establishes an underlying SSL/TLS connection.
  - For better security, issue a trusted X.509 certificate.
  - Don't use the default self-signed certificates.
- Secure Shell (SSH) is typically used for Linux servers.
  - SSH establishes a secure communication channel.
  - Use tunneling to protect the application session in transit.
  - Don't allow the root user to use an SSH terminal.
  - Be sure that all users log in with an SSH key pair, and then deactivate password authentication.

AWS Certificate Manager (ACM)

- Provides a single interface to manage both public and private certificates
- Makes it easy to deploy certificates
- Protects and stores private certificates
- Minimizes downtime and outages with automatic renewals

AWS Certificate Manager (ACM)

AWS Certificate Manager Private Certificate Authority



Key takeaways: Protect data in transit

- Protect data in transit by using SSL or client-side encryption when you run applications in the cloud.
- Use VPC endpoints to limit access to S3 buckets.
- The ACM service handles the complexity of creating and managing public SSL/TLS certificates for your AWS based websites and applications.
- ACM Private CA can manage the lifecycle of your private certificates centrally and in a highly available way.

Best practices to protect data in Amazon S3

Protecting Data in Your Application

Presigned URLs

- Generate an S3 Presigned URL, and use it to upload files (objects).

- A presigned URL uses three parameters to limit user access:
  - Bucket: Bucket that the object is in (or will be in)
  - Key: Name of the object
  - Expires: Amount of time that the URL is valid

Security considerations and best practices (1 of 2)

- Consider encryption of data at rest, and enforce encryption of data in transit.
- Ensure that your S3 buckets use the correct policies and are not publicly accessible.
- Use the principle of least privilege.
- Enable MFA delete for buckets.
- Enforce encryption for each PUT request.
- Use presigned URLs for applications that refer to Amazon S3 objects.

Security considerations and best practices (2 of 2)

- To encrypt all objects, set default encryption on a bucket.
- If using S3 Object Lock, use the appropriate retention mode.
- Use S3 Block Public Access.
- Upload data to Amazon S3 over SSH File Transfer Protocol (SFTP) through AWS Transfer for SFTP.
- Enable S3 Versioning.

Additional data protection services

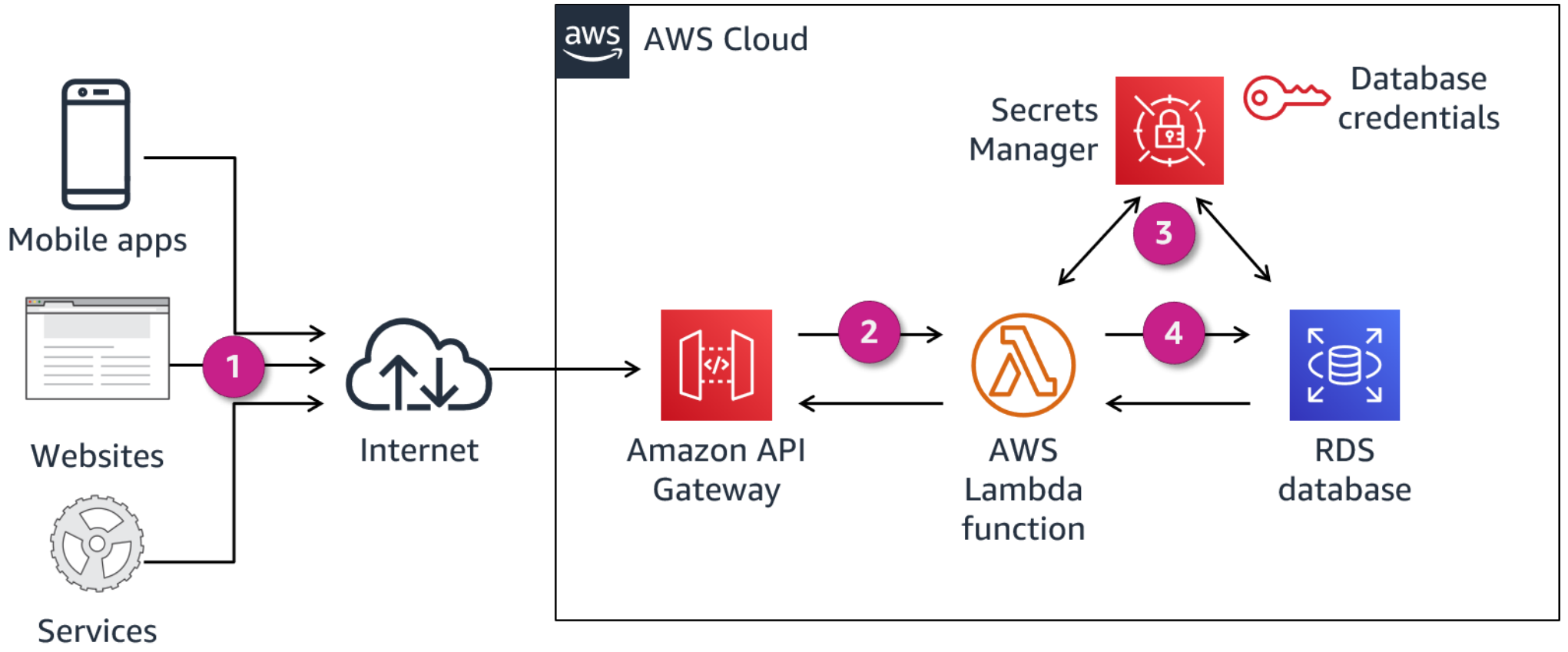
Protecting Data in Your Application

AWS Secrets Manager

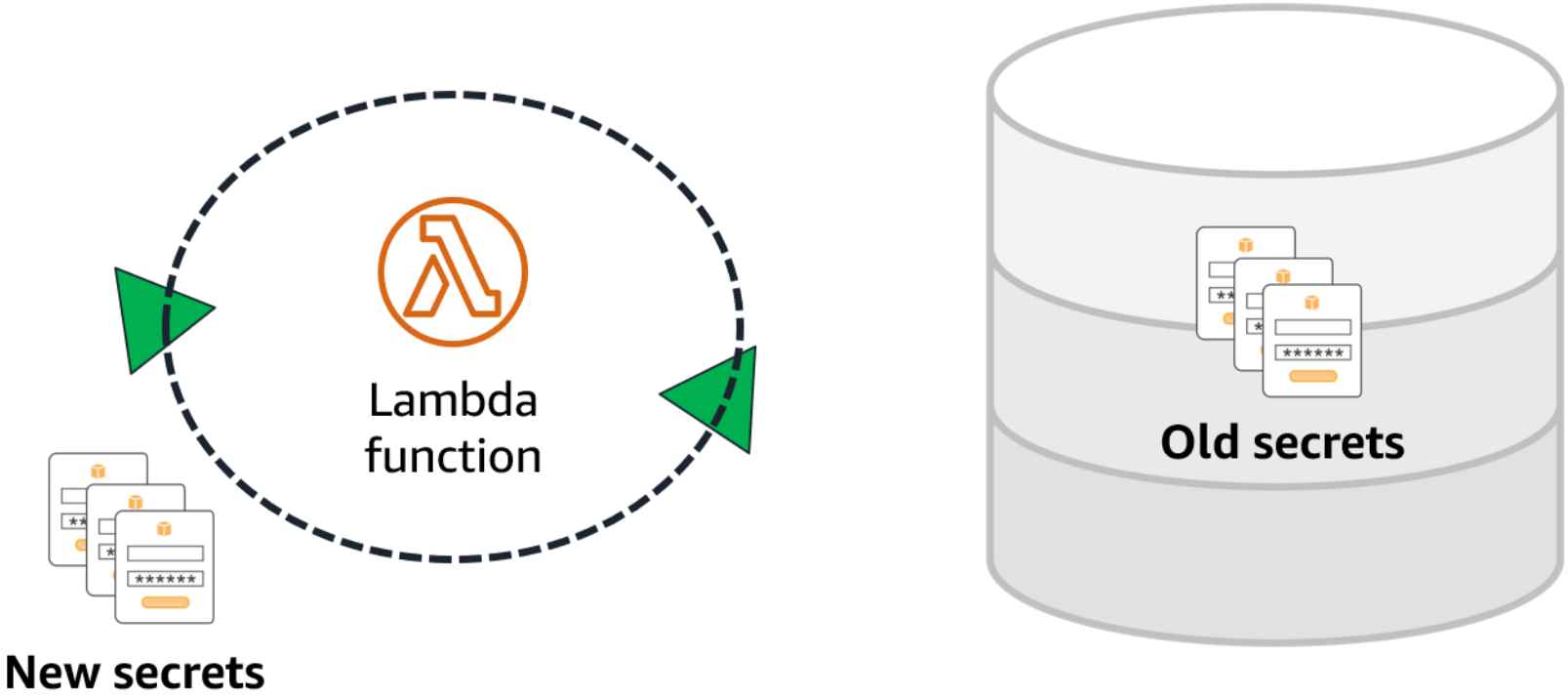
- Is a secure and scalable method for managing access to secrets
- Is a way to meet regulatory and compliance requirements
- Rotates secrets safely without breaking applications
- Audits and monitors the lifecycle of secrets
- Helps you to avoid putting secrets in code or config files

AWS Secrets Manager

Using Secrets Manager



Rotating secrets



Built-in Lambda function for Amazon RDS DB engine credentials
Custom Lambda function for other credentials

Amazon Macie

- Recognizes sensitive data such as personally identifiable information (PII), financial information, encryption keys, and credentials
- Allows for custom-defined data types
- Protects data stored in Amazon S3 by monitoring resource policies and ACLs
- Provides full API coverage for management
- Integrates with AWS Organizations

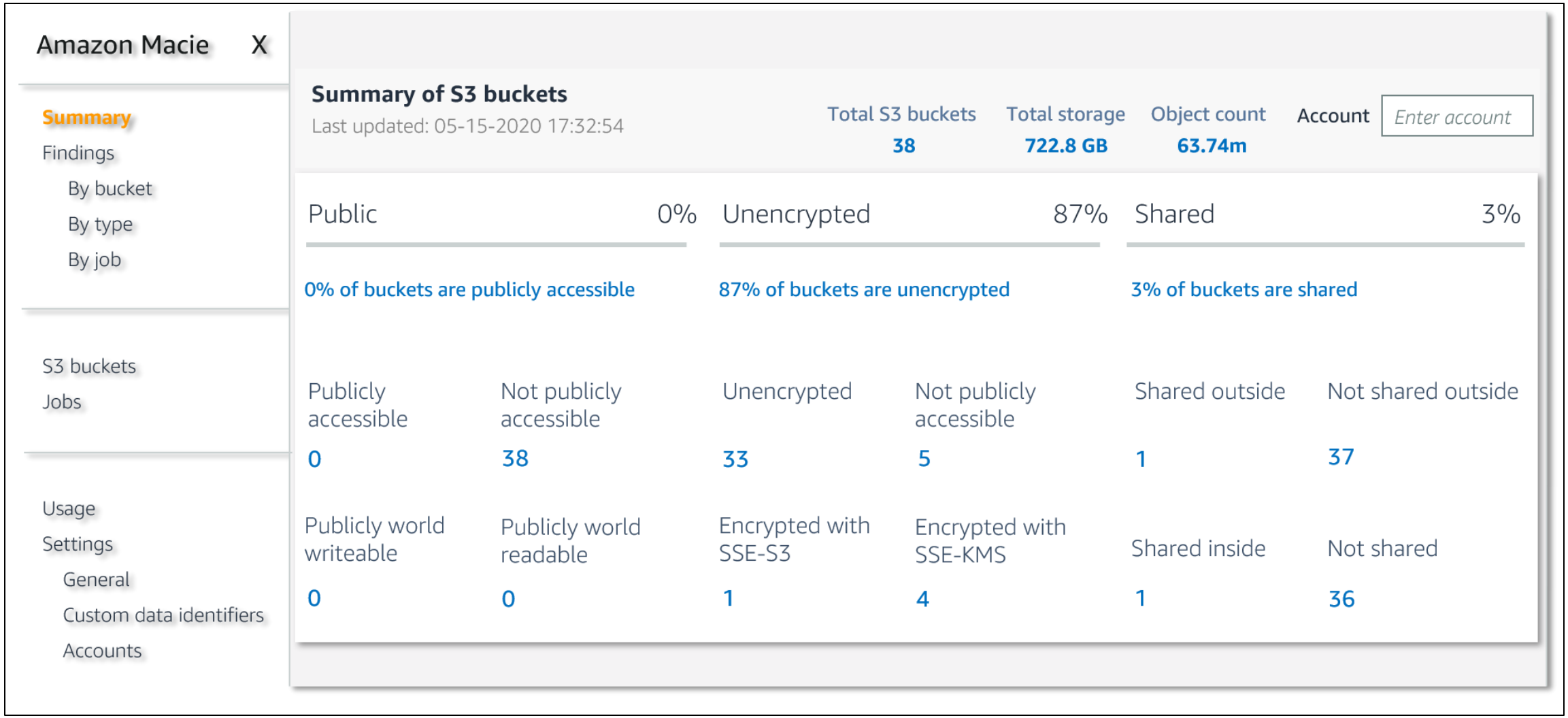
Amazon Macie

Classify data and monitor its access permissions

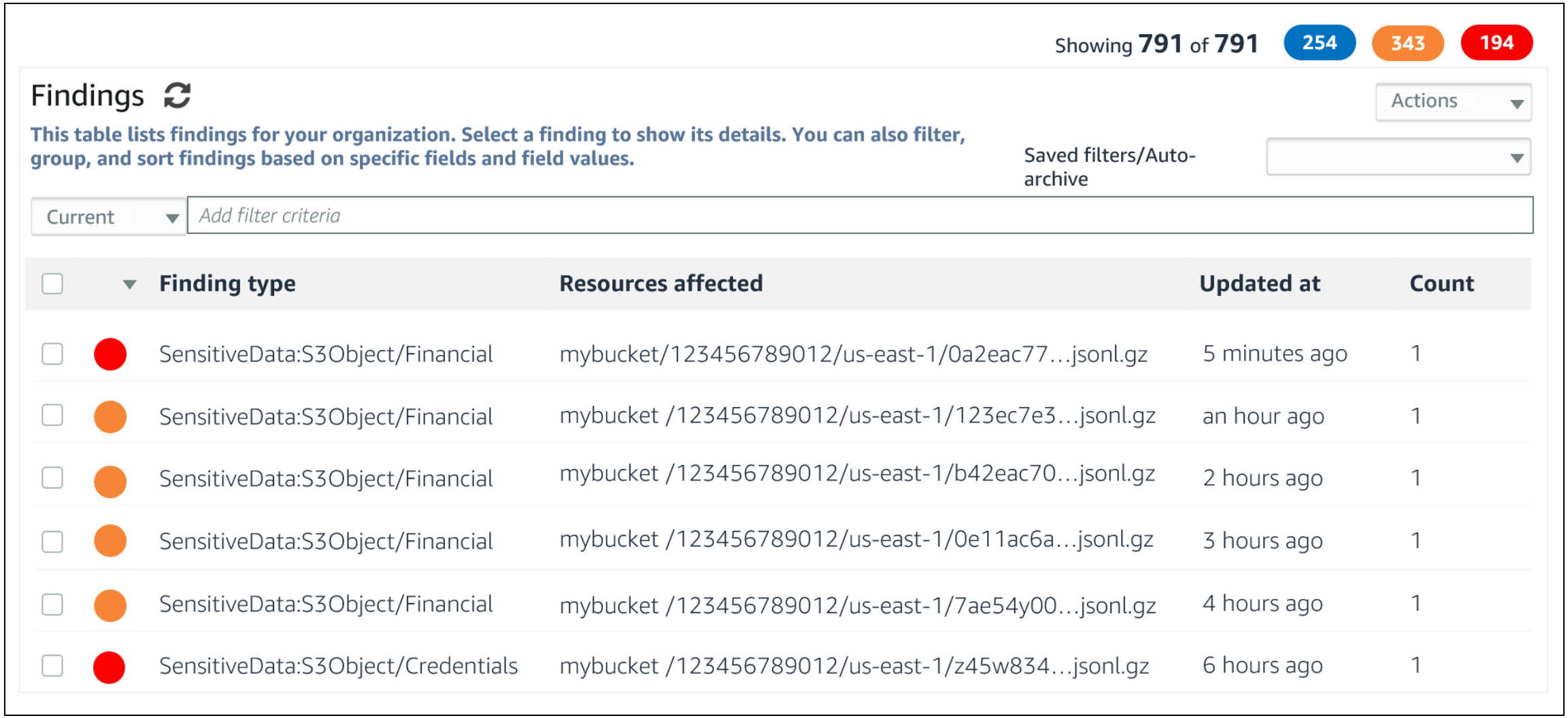
- Macie scans and evaluates bucket objects for policy violations and sensitive data.

- Macie generates findings in real-time for the following:
  - Buckets that are public
  - Buckets that are not encrypted
  - Buckets that are shared or replicated

Macie summary



Macie findings



Sample exam question

A company requires that data stored in AWS be encrypted at rest. Which approach would meet this requirement?

Choice	Response
A	When storing data in Amazon EBS, use only EBS-optimized EC2 instances.
B	When storing data in Amazon S3, use S3 Versioning and MFA delete.
C	When storing data in an EC2 instance store, encrypt the volume by using AWS KMS.
D	When storing data in Amazon S3, enable server-side encryption.

Sample exam question answer

A company requires that data stored in AWS be encrypted at rest. Which approach would meet this requirement?

The correct answer is D.

The keywords in the question are **data stored in AWS** and **encryption at rest**.

Logging and Monitoring

AWS Academy Cloud Security Foundations

Introduction

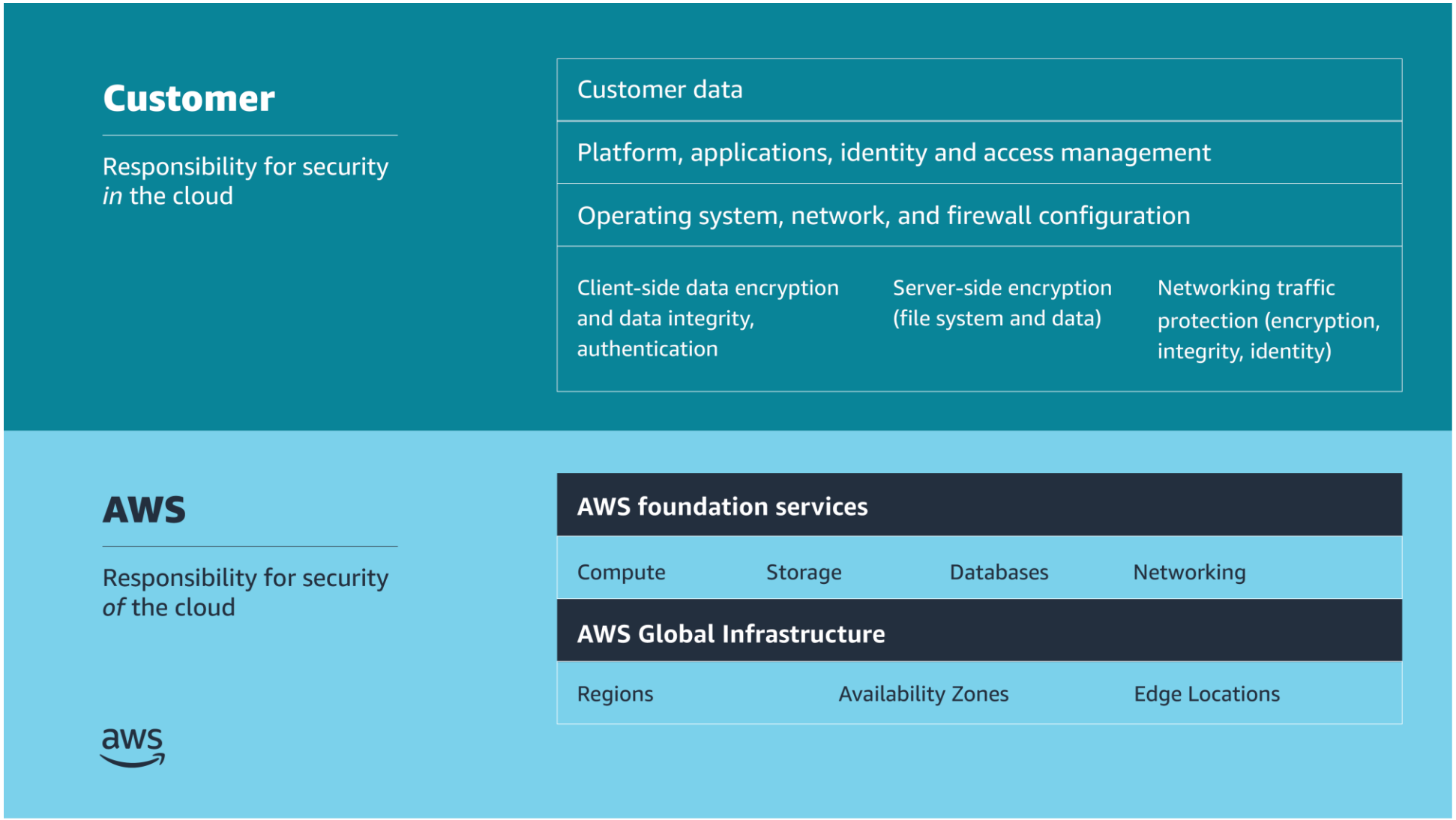
Logging and Monitoring

Module overview

Sections

- Importance of logging and monitoring
- Capture and collect
- AWS services with built-in logs
- Monitor and report
- Best practices for logging and monitoring
- Additional AWS services for logging and monitoring

Shared responsibility model

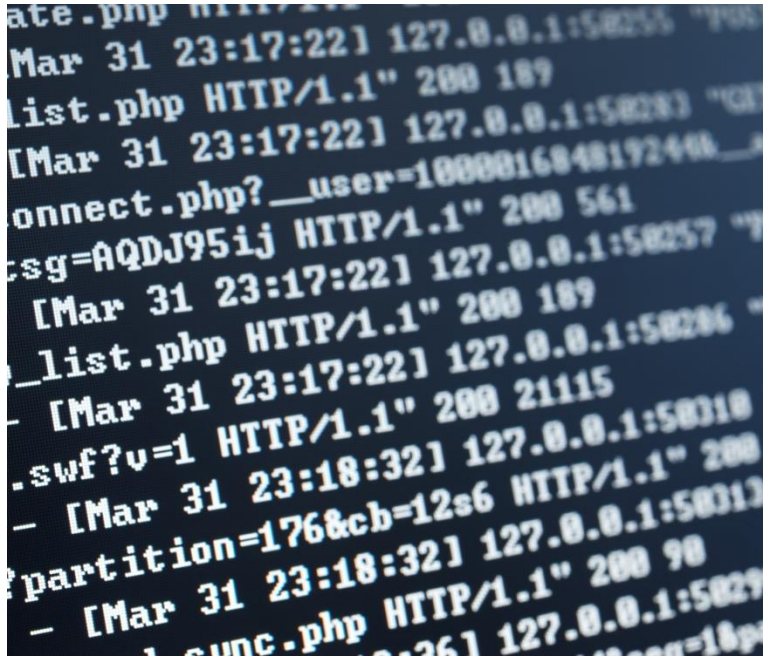


Importance of logging and monitoring

Logging and Monitoring

What is logging?

- Logging is the collection and recording of activity and event data.
  - Provided by the service itself
  - Provided by a secondary service
- Information logged will vary based on the service conducting the logging.
- Common log elements:
  - Date and time of event
  - Origin of event
  - Identity of resources accessed



Why is logging important?

- Logging provides a record of events, which is useful for the following:
  - Troubleshooting
  - Auditing
  - Recordkeeping
  - Incident response and remediation
- Logs are a requirement for demonstrating compliance with regulations, such as the following:
  - HIPAA
  - GDPR
  - LGPD

What is monitoring?

- Monitoring is the continuous verification of the security and performance of your resources, applications, and data.
- AWS provides several services that give you the visibility to spot issues before they impact operations:
  - AWS CloudTrail
  - Amazon CloudWatch
  - Amazon EventBridge
  - AWS X-Ray

Capture and collect

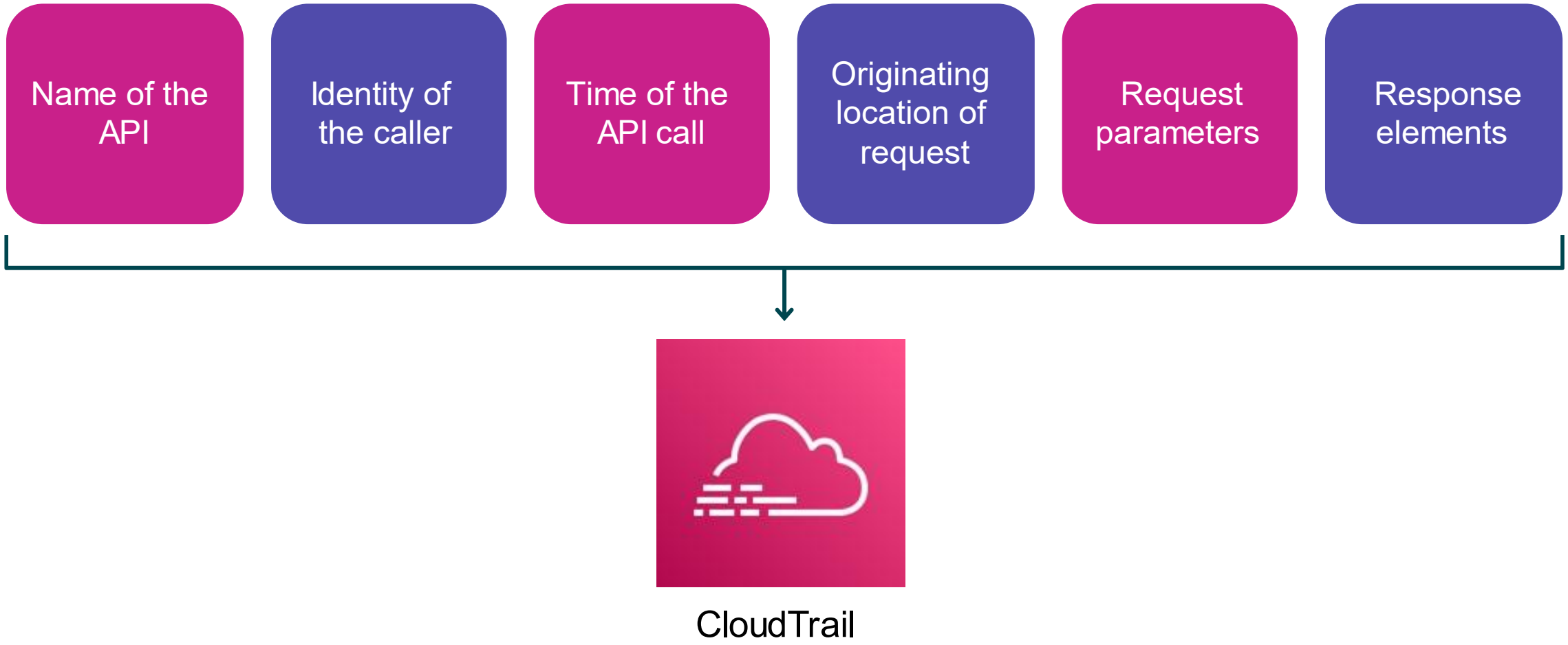
Logging and Monitoring

AWS CloudTrail

- Assists you to enable governance and compliance, as well as operational and risk auditing of your AWS account
- Records actions taken by a user, role, or AWS service as events
- Provides visibility of events in the CloudTrail console
- Can be used to view, search, download, archive, analyze, and respond to account activity across your AWS infrastructure

AWS CloudTrail

API security-relevant information



Reading a log: Identity of the caller


```
{
  "Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:iam::111122223333:user/Jane",
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "Jane"
    },
```

Reading a log: Time and origin of the request


```
"eventTime": "2021-07-06T21:01:59Z",
"eventSource": "ec2.amazonaws.com",
"eventName": "StopInstances",
"awsRegion": "us-east-2",
"sourceIPAddress": "203.0.113.176",
"userAgent": "ec2-api-tools 1.6.12.2",
```

Reading a log: Request parameters and response elements


```
"requestParameters": {
  "instancesSet": {
    "items": [{
      "instanceId": "i-ebeaf9e2" } ] },
  "force": false },
"responseElements": {
  "instancesSet": {
    "items": [{
      "instanceId": "i-ebeaf9e2",
      "currentState": {
        "code": 64,
        "name": "stopping" },
      "previousState": {
        "code": 16,
        "name": "running" } } ] },
```

AWS services with built-in logs

Logging and Monitoring

Services with built-in logs: Amazon S3

- Amazon S3 provides detailed access request records through Amazon S3 server access logging.
- Server access logs provide useful information for security and access audits.
- Server access logs can provide insight into your customer base and assist you to understand your Amazon S3 bill.

Amazon Simple Storage Service (Amazon S3)

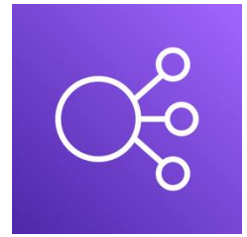
Services with built-in logs: Amazon VPC

- With VPC Flow Logs, you can capture information about inbound and outbound IP traffic from the following:
  - VPC
  - Subnets
  - Individual network interfaces
- Publish flow log data to CloudWatch or Amazon S3.
- Flow log data is collected outside of the path of your network traffic, with no impact on throughput or latency.

Amazon Virtual Private Cloud (Amazon VPC)

Services with built-in logs: ELB

- ELB access logs capture detailed information about requests sent to your load balancer.
- Use access logs to analyze traffic patterns and for troubleshooting.
- ELB captures, compresses, and stores logs in a specified S3 bucket.



Elastic Load Balancing (ELB)

Monitor and report

Logging and Monitoring

Amazon CloudWatch

- Is a monitoring and observability service
- Provides a unified view of the operational health of your AWS resources, applications, and services
- Collects metrics in the AWS Cloud and on premises
- Can be used for infrastructure monitoring and troubleshooting
- Provides the ability to customize logs and events

Amazon CloudWatch

Comparing CloudTrail and CloudWatch

AWS CloudTrail	Amazon CloudWatch
Continuously monitors and logs user activities	Continuously monitors resource and application performance
Useful for compliance auditing, security analysis, and troubleshooting	Useful for detecting anomalous service behavior, setting alarms, and discovering insights
Helps you determine WHO performed WHAT unauthorized action and WHEN they did it	Alerts you that an issue has occurred due to an unauthorized action

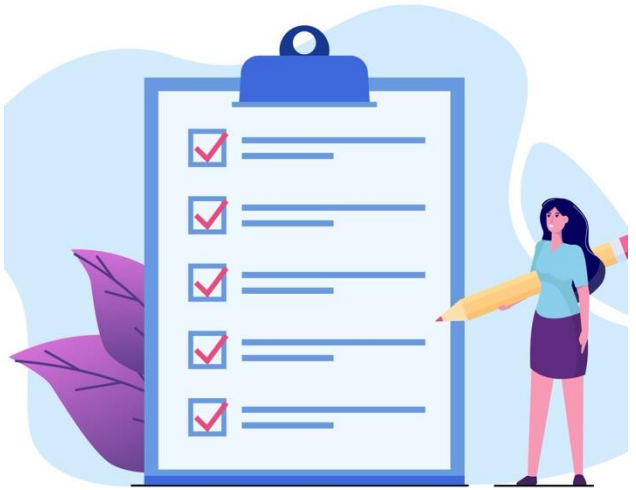
When used together, you can create custom CloudWatch dashboards, alarms, and notifications for key metrics and specific CloudTrail events.

Best practices for logging and monitoring

Logging and Monitoring

Best practices for logging and monitoring

- Define your organizational requirements for logs, alerts, and metrics.
- Configure service and application logging throughout your workload.
- Analyze your logs centrally.



Additional AWS services for logging and monitoring

Logging and Monitoring

AWS Trusted Advisor

- Provides recommendations based on five categories of AWS best practices: cost optimization, security, fault tolerance, service limits, and performance improvement
- Evaluates your account to suggest improvements and optimizations for your resources
- Is accessible through the AWS Management Console and available to all support tiers

AWS Trusted Advisor

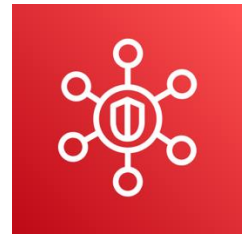
Amazon EventBridge

- Is a serverless event bus service that is used to connect your applications with data from a variety of sources
- Provides a stream of real-time data from applications and services to targets, such as AWS Lambda or event buses
- Was formerly called Amazon CloudWatch Events

Amazon EventBridge

AWS Security Hub

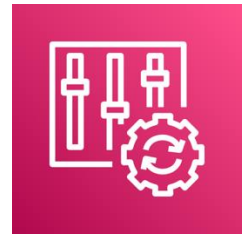
- Aggregates security alerts from various AWS services and partner products in a standardized format
- Collects data across accounts and checks cloud security posture against AWS security best practices
- Helps you to understand your overall security posture by using a consolidated security score across all of your AWS accounts



AWS Security Hub

AWS Config

- Helps to assess, audit, and evaluate the configurations of your AWS resources
- Continuously monitors and records AWS resource configurations
- Provides automated evaluation of recorded configurations against desired configurations



AWS Config

Sample exam question

A system administrator discovers that a user has deleted an Amazon S3 bucket without authorization, which triggered an incident response.

Which AWS service can they use to determine the identity of the user that committed the incident?

Choice	Response
A	Amazon CloudWatch
B	AWS Config
C	AWS CloudTrail
D	AWS Trusted Advisor

Sample exam question answer

A system administrator discovers that a user has deleted an Amazon S3 bucket without authorization, which triggered an incident response.

Which AWS service can they use to determine the identity of the user that committed the incident?

The correct answer is C.

The keywords in the question are **identity** and **user**.

Responding to and Managing an Incident

AWS Academy Cloud Security Foundations

Introduction

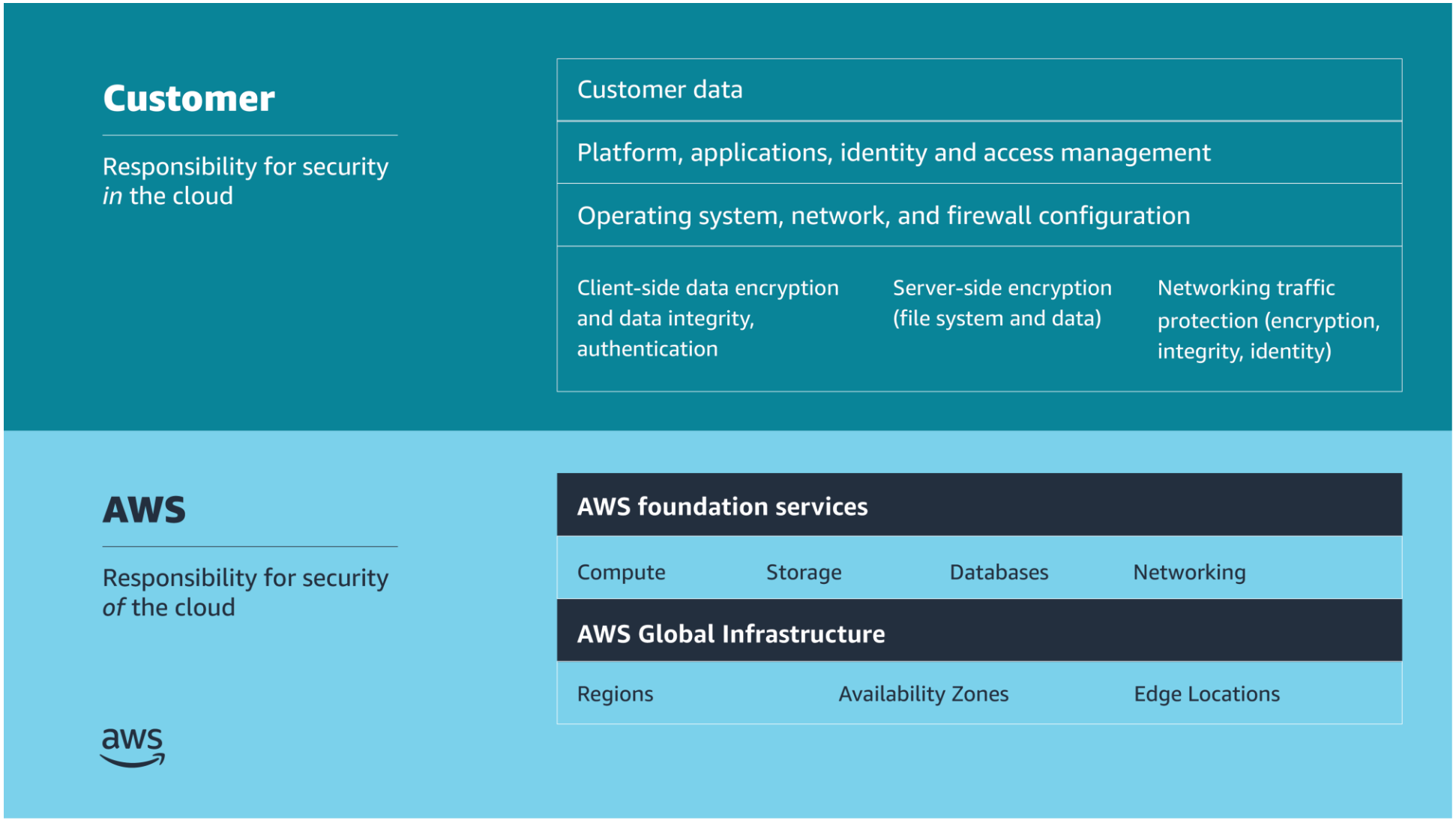
Responding to and Managing an Incident

Module overview

Sections

- Identifying an incident
- AWS services that support the discovery and recognition phase
- AWS services that support the resolution and recovery phase
- Best practices for handling an incident

Shared responsibility model



Identifying an incident

Responding to and Managing an Incident

Incident recognition and response

- Is a set of information security policies and procedures that you can use to identify, contain, and eliminate cyberattacks
- Enables an organization to quickly detect and halt attacks
- Helps you to minimize damage and prevent future attacks

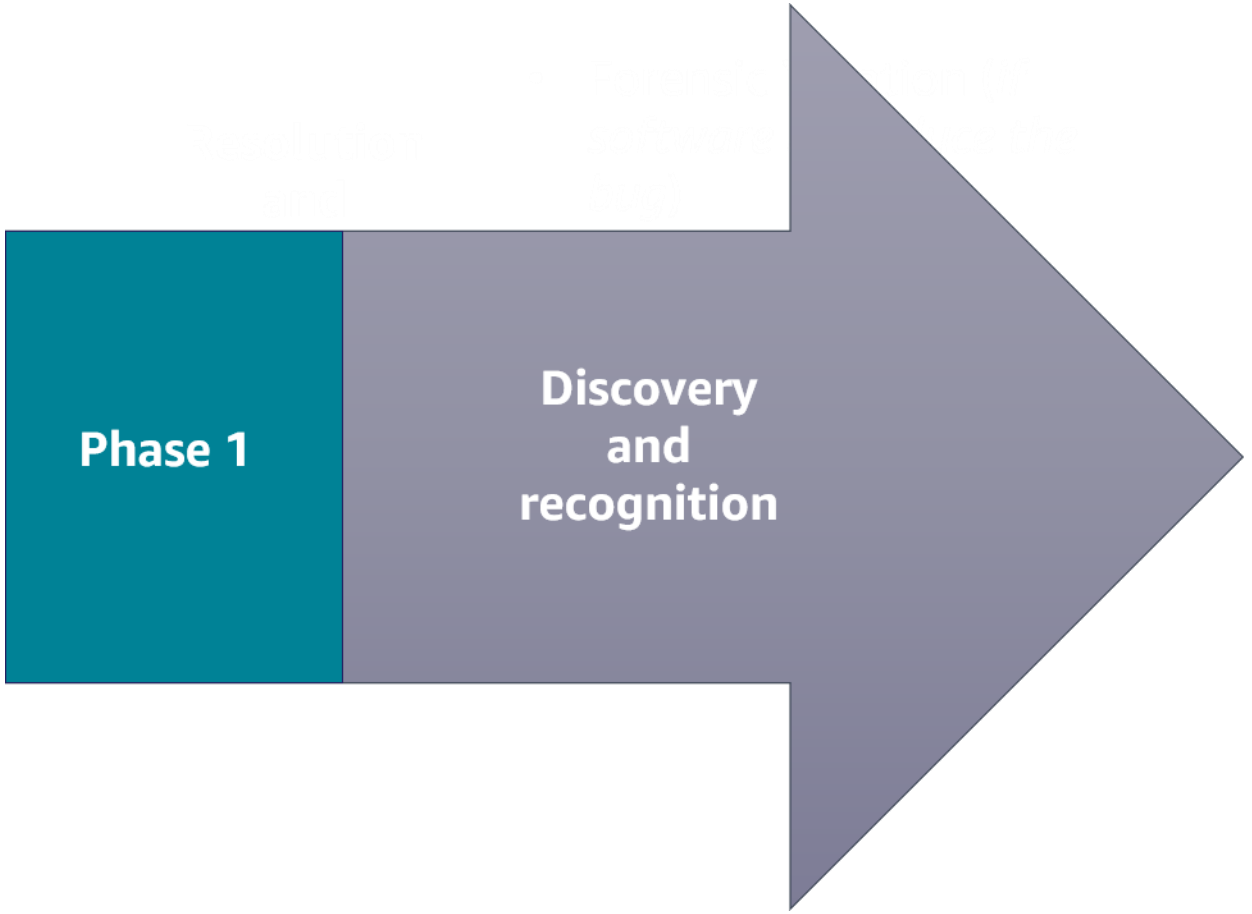
Recognizing incidents

Not all events are incidents in need of immediate remedy.

- Logging in from a remote location
- Failing hard drive that is still fully operational
- Employee trying to access resources that they shouldn't access

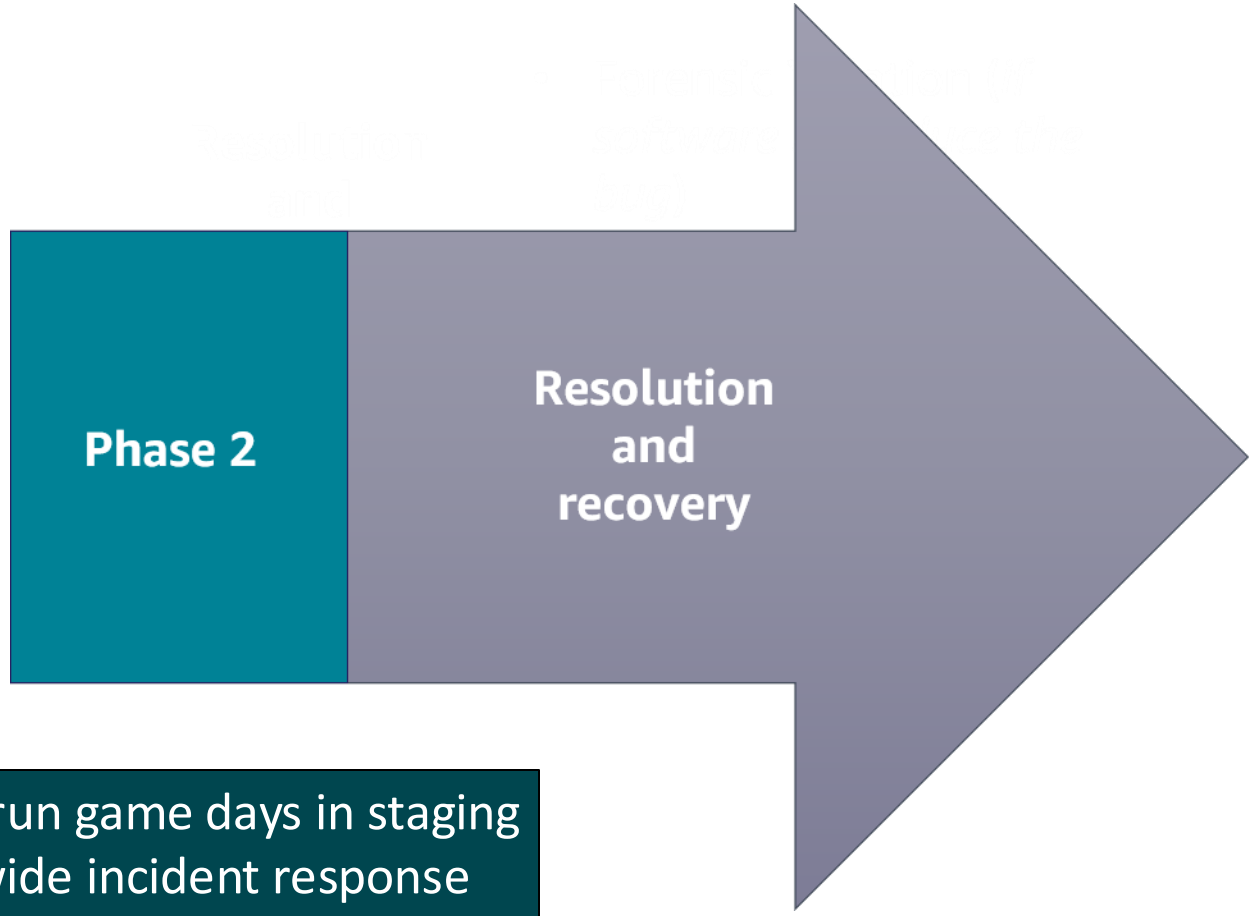
Phase 1: Discovery and recognition

- Incident identification, logging, and categorization
- Incident notification and escalation
- Investigation and diagnosis



Phase 2: Resolution and recovery

- Forensic isolation (if software, reproduce the bug)
- Stage a fix
- Deploy the fix
- Incident closure



Automate theses processes wherever possible, and run game days in staging (safe) environments to fine-tune your corporate-wide incident response process.

AWS services that support the discovery and recognition phase

Responding to and Managing an Incident

Discovery and recognition phase

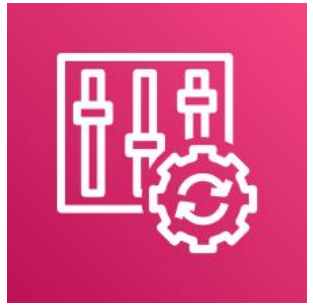
AWS Trusted Advisor

Amazon CloudWatch

Amazon Inspector

Amazon GuardDuty

AWS Shield



AWS Config

AWS Trusted Advisor

- Draws upon best practices learned from serving hundreds of thousands of AWS customers
- Inspects your AWS environment, and then makes recommendations when opportunities exist to improve performance and help close security gaps

AWS Trusted Advisor

Amazon CloudWatch

- Provides a reliable, scalable, and flexible monitoring solution that you can start using within minutes
- Automatically displays metrics about every AWS service that you use
- Provides the ability to create alarms that watch metrics and send notifications

Amazon CloudWatch

Amazon Inspector

- Is a vulnerability management service that continuously scans your AWS workloads for vulnerabilities
- Automatically discovers and scans Amazon Elastic Compute Cloud (Amazon EC2) instances and container images that reside in Amazon Elastic Container Registry (Amazon ECR)
- Creates a finding when it discovers a vulnerability or network issue

Amazon Inspector

Amazon GuardDuty

- Is a continuous security monitoring service
- Identifies unexpected and potentially unauthorized or malicious activity
- Uses threat intelligence feeds

Amazon GuardDuty

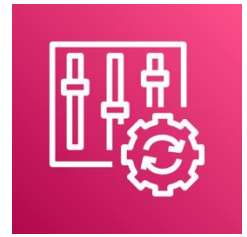
AWS Shield

- Automatically protects an enterprise network from a distributed denial of service (DDoS) attack
- Offers the AWS Shield Advanced managed threat protection service to improve your security posture with additional DDoS detection, mitigation, and response capabilities

AWS Shield

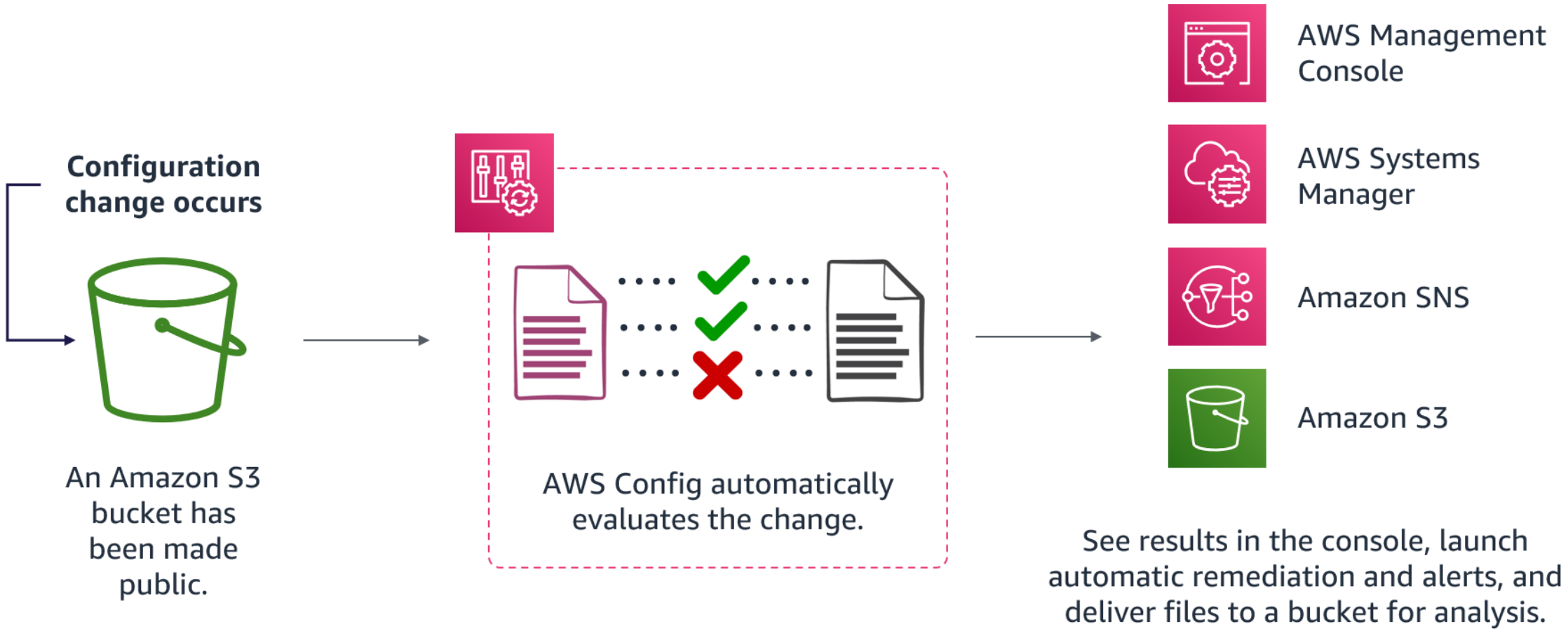
AWS Config

- Is a continuous monitoring and assessment service
- Provides the ability to view current and historic configurations of a resource and use this information to troubleshoot outages
- Sends notifications when changes occur
- Integrates with other AWS services to remediate issues



AWS Config

Evaluating rules



AWS services that support the resolution and recovery phase

Responding to and Managing an Incident

Resolution and recovery

AWS Systems Manager

AWS CloudFormation

Event-driven responses

Amazon Simple Notification Service (Amazon SNS)

AWS Step Functions

AWS Lambda

AWS Systems Manager

- Gives you visibility and control of your infrastructure on AWS
- Provides a unified user interface so that you can view operational data from multiple AWS services
- Provides the ability to group resources by application and view operational data for monitoring and troubleshooting
- Helps you to keep your instances in their defined state and perform on-demand changes, such as updating applications or running shell scripts

AWS Systems Manager

AWS CloudFormation

- Helps you model and set up your AWS resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS
- Provides the ability to create a template that describes all the AWS resources that you want
- Can be used to re-create a staging environment inside an isolated, or forensic, virtual private cloud (VPC)

AWS CloudFormation

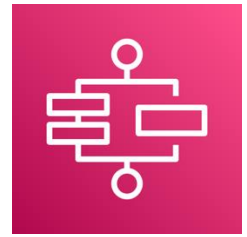
Amazon Simple Notification Service (Amazon SNS)

- Is an event-driven web service that provides the ability for applications, end users, and devices to instantly send and receive notifications from the cloud

Amazon Simple Notification Service (Amazon SNS)

AWS Step Functions

- Is a visual workflow service that developers use to build distributed applications, and automate IT and business processes
- Provides the ability to create event-driven workflows to manage failures, retries, parallelization, service integrations, and observability so that developers can focus on higher value business logic



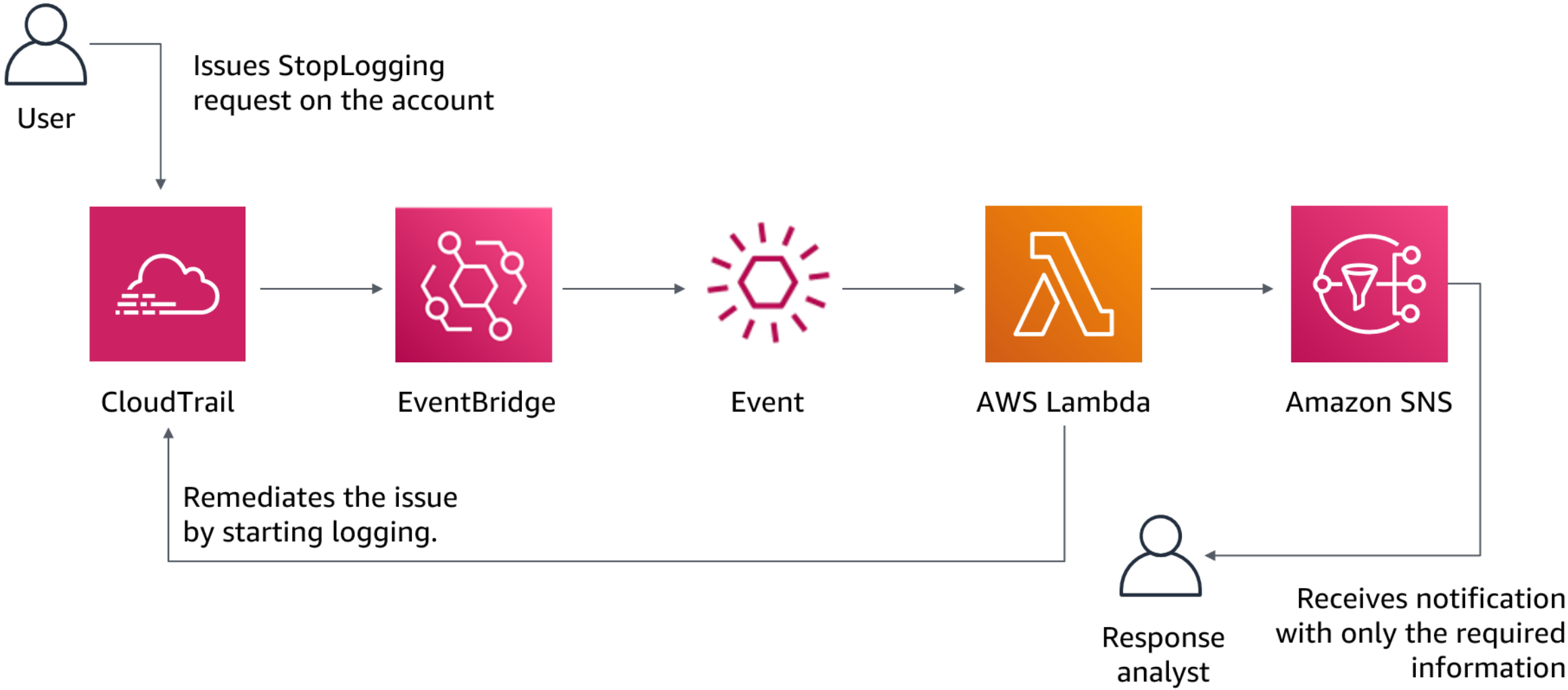
AWS Step Functions

AWS Lambda

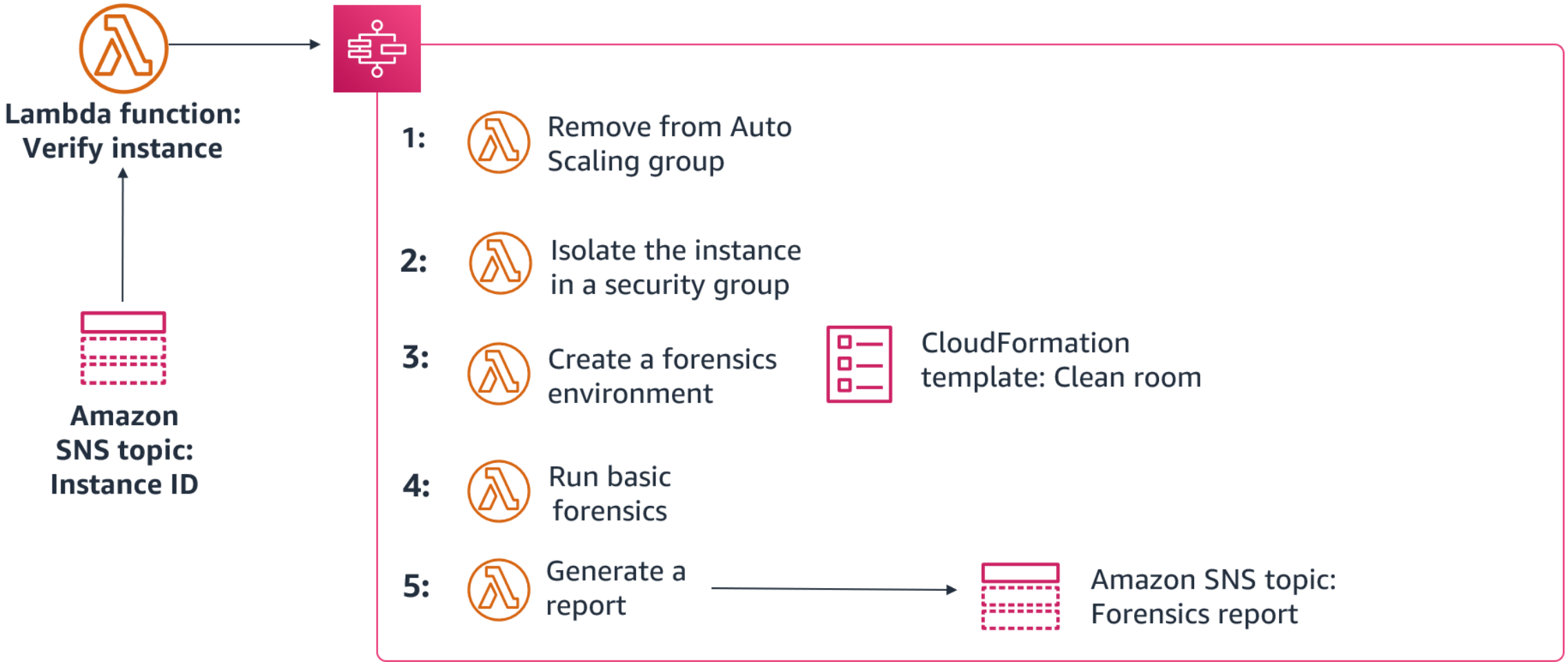
- Is a serverless, event-driven compute service that provides the ability to run code on demand without provisioning or managing servers
- Lambda functions are stateless

AWS Lambda

Lambda for incident response



Working together for incident response



Best practices for handling an incident

Responding to and Managing an Incident

Industry best practices for handling incidents

- Identify key personnel, external resources, and tooling.
- Automate containment capabilities.
- Develop incident response plans.
- Pre-provision access and tools.
- Run incident response game days.

Sample exam question

An administrator would like to use a continuous monitoring and assessment service that provides an inventory of AWS resources. Which AWS service would meet their need?

Choice	Response
A	AWS Lambda
B	AWS CloudTrail
C	AWS Config
D	AWS Fargate

Sample exam question answer

An administrator would like to use a continuous monitoring and assessment service that provides an inventory of AWS resources. Which AWS service would meet their need?

The correct answer is C.

The keywords in the question are **continuous monitoring**, **assessment service**, and **inventory**.