Security Essentials

Yasser Quraishi, AWS Solutions Architect – yquraish@amazon.com

Jeff Hosley, AWS Account Manager – jhosley@amazon.com

Overview

Overview of the AWS cloud security concepts such as the AWS Security Center, Shared Responsibility Model, and Identity and Access Management.

AWS Security

At AWS, cloud security is our highest priority.

Gain access to a world-class security team

Where would some of the world's top security people like to work? At scale on huge challenges with huge rewards

So AWS has world-class security and compliance teams watching your back!

Every customer benefits from the tough scrutiny of other AWS customers

aws

Broad Accreditations & Certifications

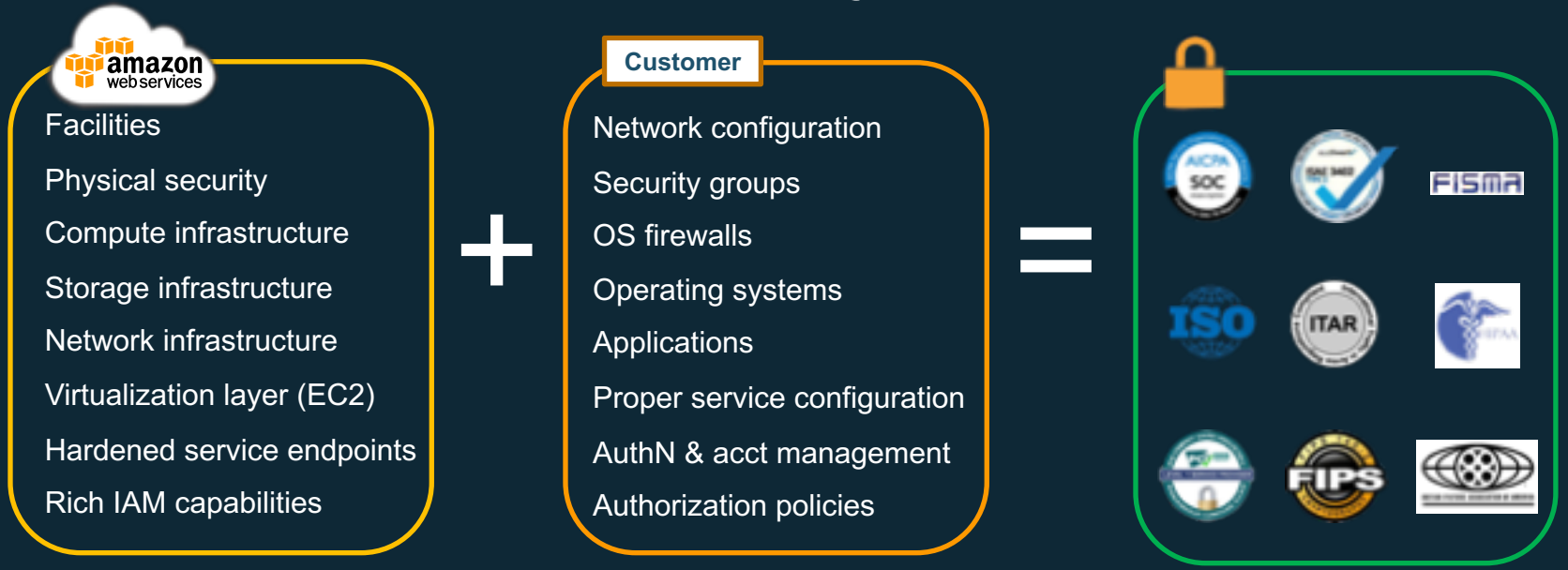
Glacier Vault Lock
& SEC Rule 17a-4(f)

See https://aws.amazon.com/compliance/programs/ for full list

aws

Shared Responsibility Model

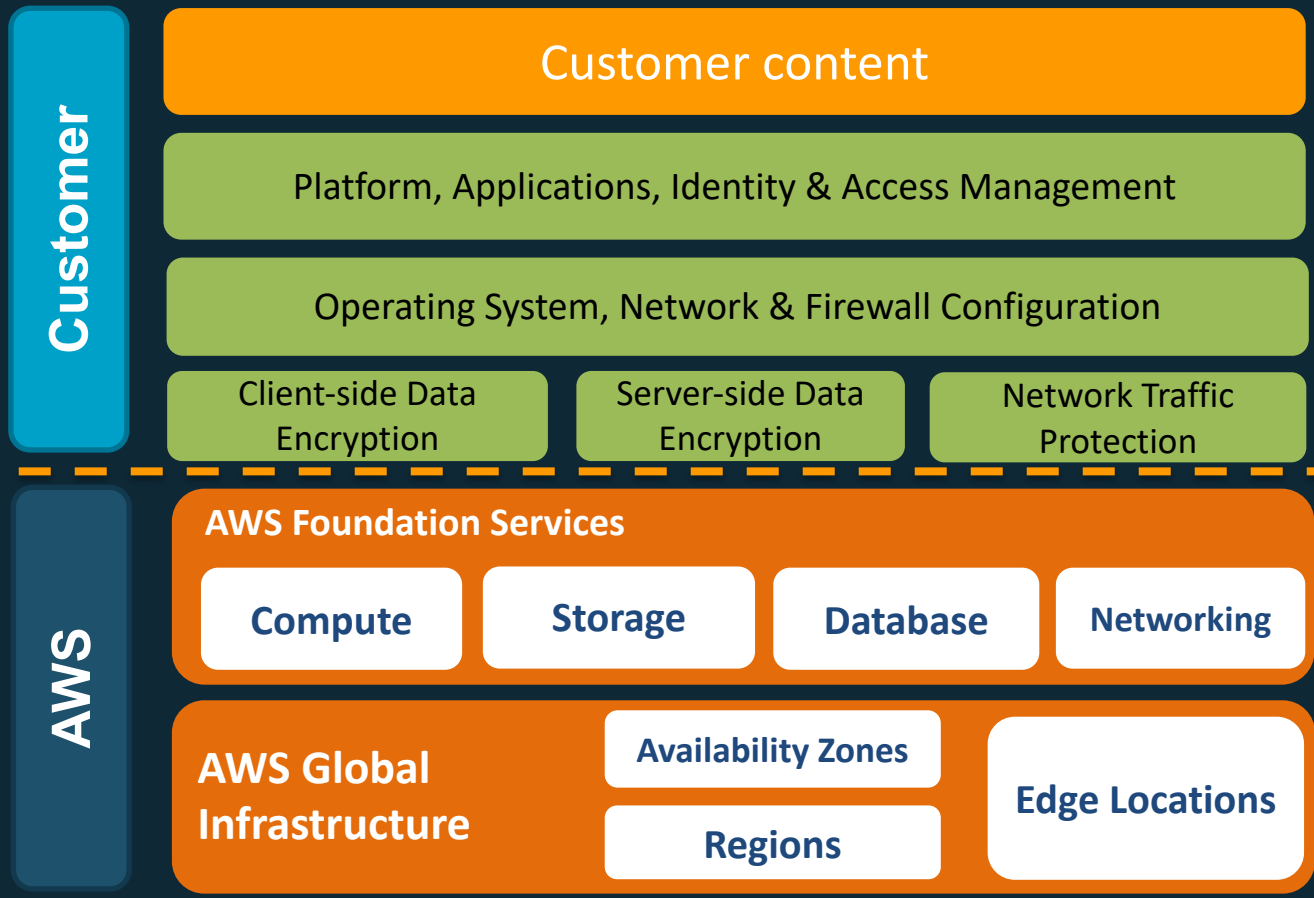
AWS Shared Responsibility Model



- Scope of responsibility depends on the type of service offered by AWS: **Infrastructure, Container, Abstracted Services**
- Understanding who is responsible for what is critical to ensuring your AWS data and systems are secure!

aws

Shared Responsibility Model



Customers are responsible for their security and compliance **IN** the Cloud

AWS is responsible for the security **OF** the Cloud

Meet your own security objectives

Customer

Your own accreditation

Your own certifications

Your own external audits

Customer scope and effort is reduced

Better results through focused efforts

AWS

AWS Foundation Services

Compute | Storage | Database | Networking

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

Built on AWS consistent baseline controls

aws

AWS Responsibilities

Physical Security of Data Center

- **Amazon has been building large-scale data centers for many years.**
- **Important attributes:**
  - Non-descript facilities
  - Robust perimeter controls
  - Strictly controlled physical access
  - Two or more levels of two-factor authentication
- **Controlled, need-based access.**
- **All access is logged and reviewed.**
- **Separation of Duties**
  - Employees with physical access don't have logical privileges.

AWS Responsibilities

EC2 Security

- **Host (hypervisor) operating system**
  - Individual SSH keyed logins via bastion host for AWS admins
  - All accesses logged and audited
- **Guest (EC2 Instance) operating system**
  - Customer controlled (customer owns root/admin)
  - AWS admins cannot log in
  - Customer-generated key-pairs
- **Stateful firewall**
  - Mandatory inbound firewall, default deny mode
  - Customer controls configuration via Security Groups

Network Security

- IP Spoofing prohibited at host OS level.
- Unauthorized Port Scanning a violation of TOS and is detected/blocked.
- Inbound ports blocked by default.

AWS Responsibilities

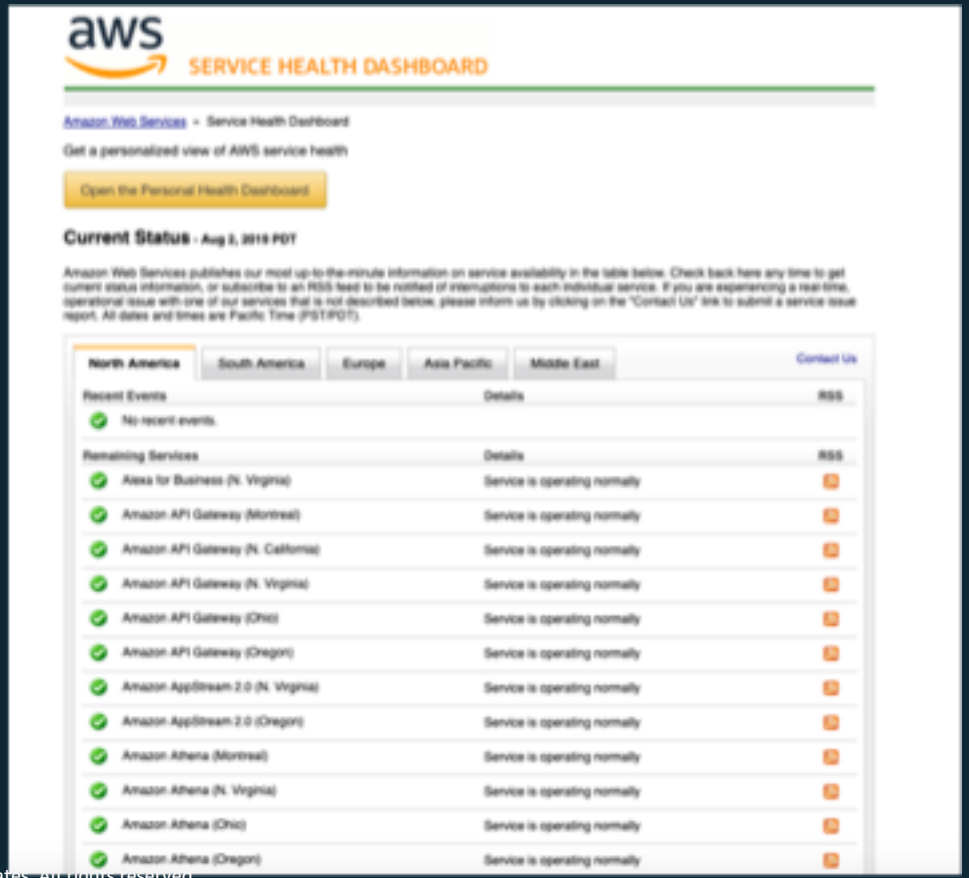
Configuration Management

- Most updates are done in such a manner that they will not impact the customer.
- Changes are authorized, logged, tested, approved, and documented.
- AWS will communicate with customers, either via email, the AWS Service Health Dashboard (http://status.aws.amazon.com/), or the AWS Personal Health Dashboard (https://phd.aws.amazon.com/) when there is a potential for service being affected.

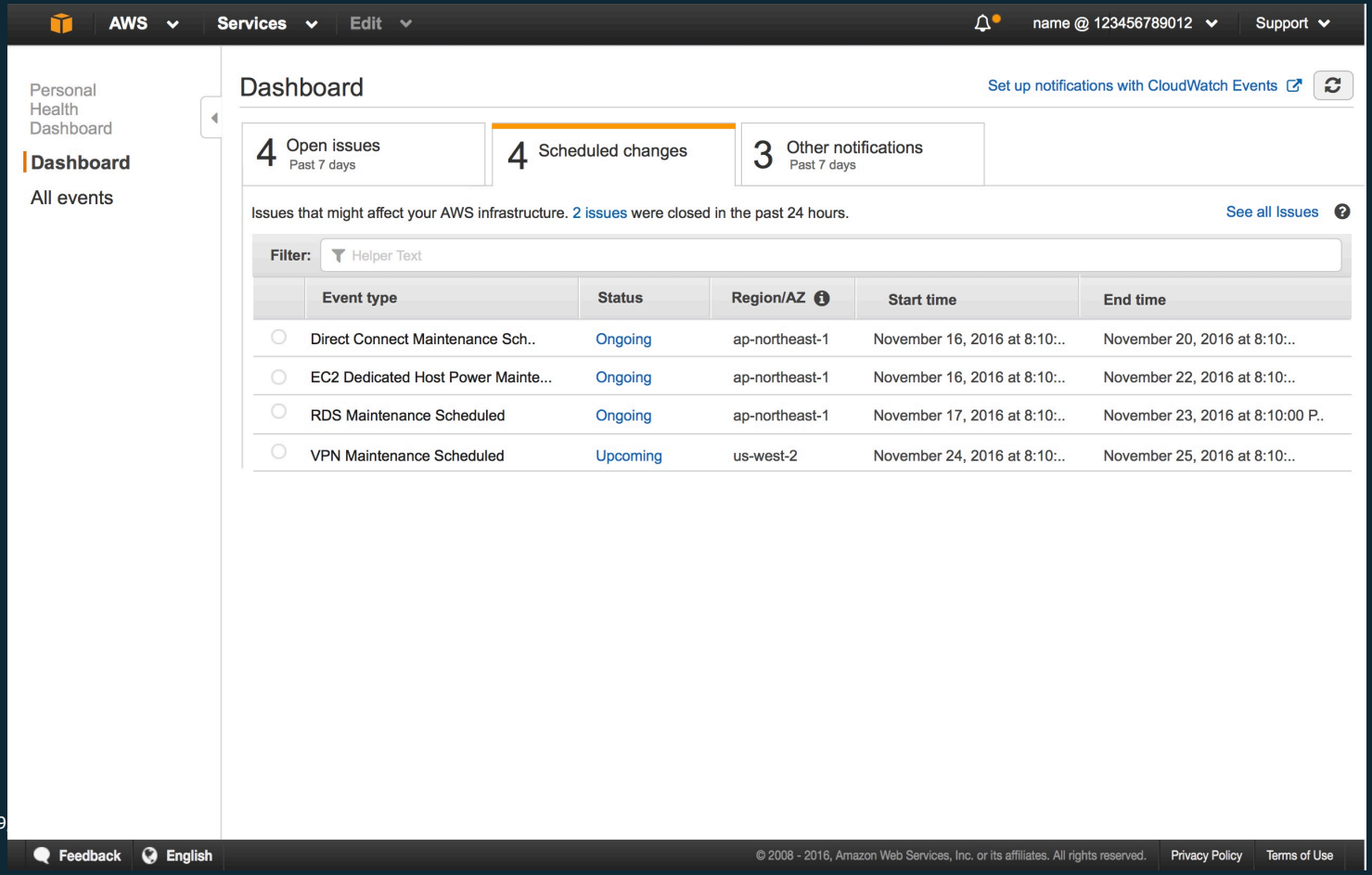
Built for "Continuous Availability"

- **Scalable, fault tolerant services.**
- **All availability zones (AZs) are always on.**
  - There is no "Disaster Recovery Datacenter"
  - All managed to the same standards
- **Robust Internet connectivity**
  - Each AZ has redundant, Tier 1 ISP Service Providers
  - Resilient network infrastructure

Service Health Dashboard



Personal Health Dashboard



AWS Responsibilities

Disk Management

- Proprietary disk management prevents customers from accessing each other's data.
- Disks wiped prior to use.
- Disks can also be encrypted by the customer for additional security.

Storage Device Decommissioning

- All storage devices go through process using techniques from:
  - DoD 5220.22-M ("National Industrial Security Program Operating Manual ").
  - NIST 800-88 ("Guidelines for Media Sanitization").
- Ultimately devices are:
  - Degaussed.
  - Physically destroyed.

Under the AWS Shared Responsibility Model

AWS Responsibility? or Customer Responsibility?

Configuring the Security Group rules that determine which ports are open on the EC2 Linux instance

Patching the operating system with the latest security patches

Installing camera systems to monitor the physical datacenters

Shredding disk drives before they leave a datacenter

Toggling on the Server-side encryption feature for S3 buckets

Preventing packet sniffing at the hypervisor level

Securing the internal network inside the AWS datacenters

aws

Under the AWS Shared Responsibility Model

AWS Responsibility? or Customer Responsibility?

Configuring the Security Group rules that determine which ports are open on the EC2 Linux instance

Patching the operating system with the latest security patches

Installing camera systems to monitor the physical datacenters

Shredding disk drives before they leave a datacenter

Toggling on the Server-side encryption feature for S3 buckets

Preventing packet sniffing at the hypervisor level

Securing the internal network inside the AWS datacenters

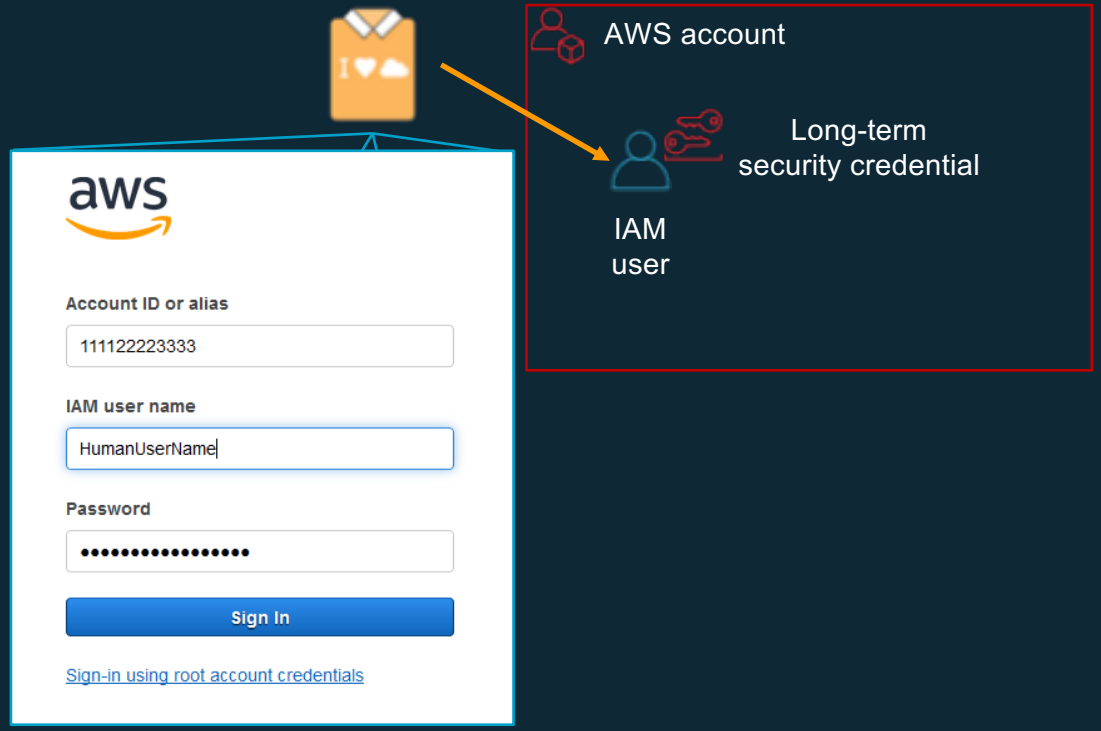
aws

Identity and Access Management

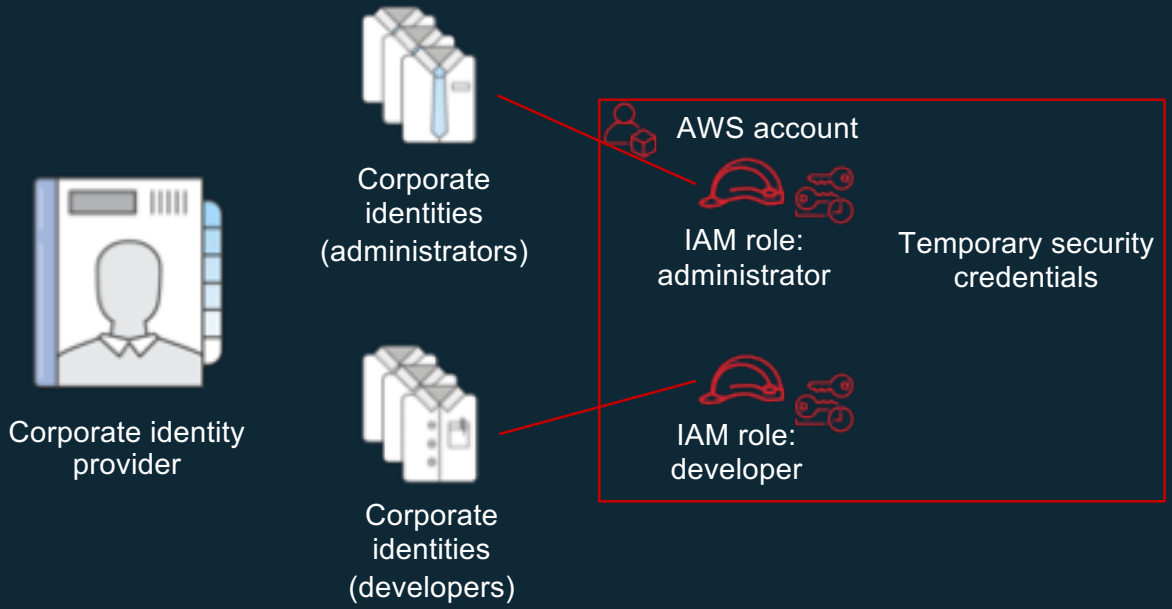
AWS IAM

- **What it is**
  - I – Authentication: Support for human and application caller identities
  - AM – Authorization: Powerful, flexible permissions language for controlling access to cloud resources
- **Why it matters to you**: Every AWS service uses IAM to authenticate and authorize API calls
- **What builders need to know**
  - How to make authenticated API calls to AWS from IAM identities
  - Basic fluency in IAM policy language
  - Where to find and how to understand service-specific authorization

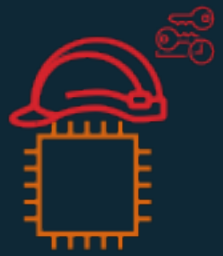
AWS identities for human callers: IAM users



AWS identities for human callers: Federated identities



AWS identities for non-human callers



Amazon EC2 instance

AWS Lambda function

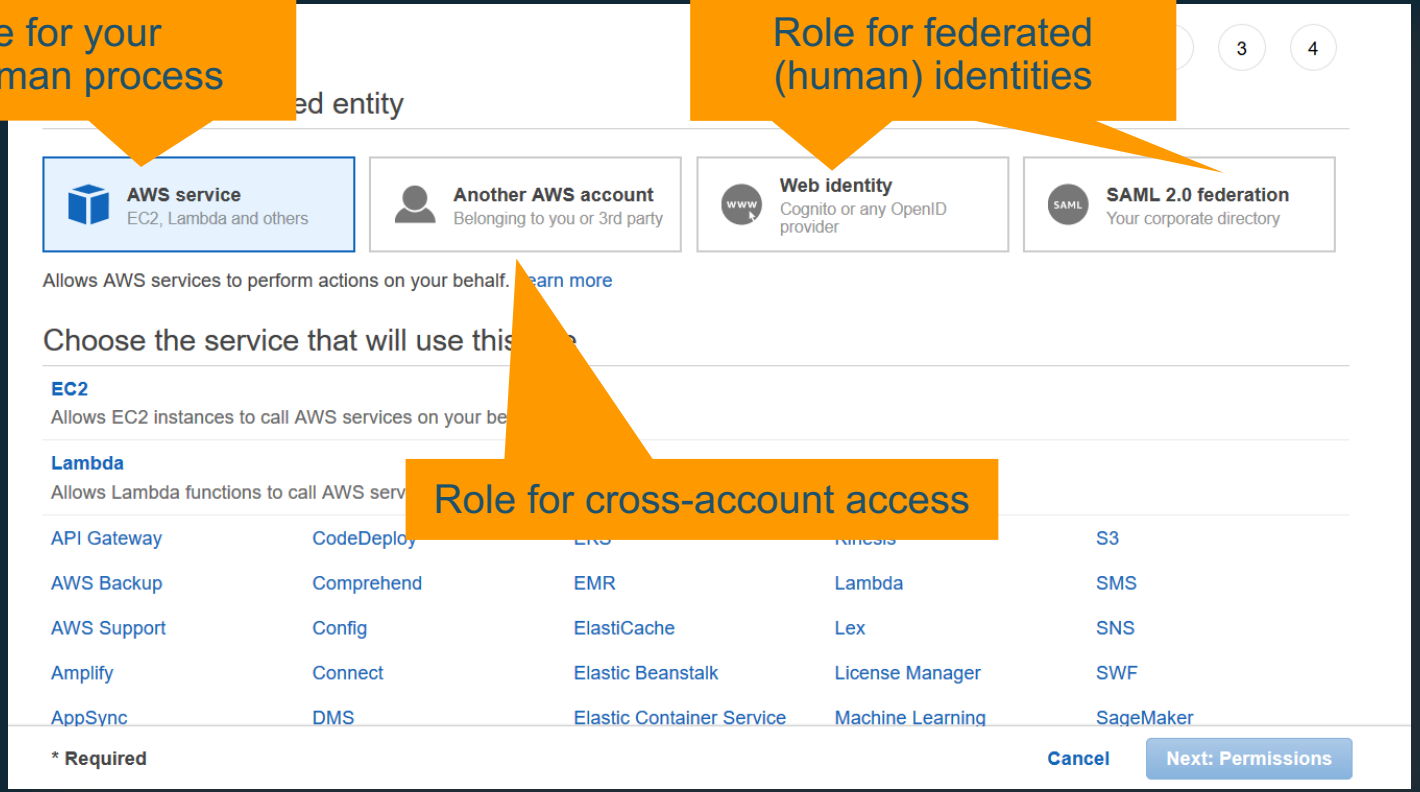
Amazon SageMaker notebook

AWS Glue crawler

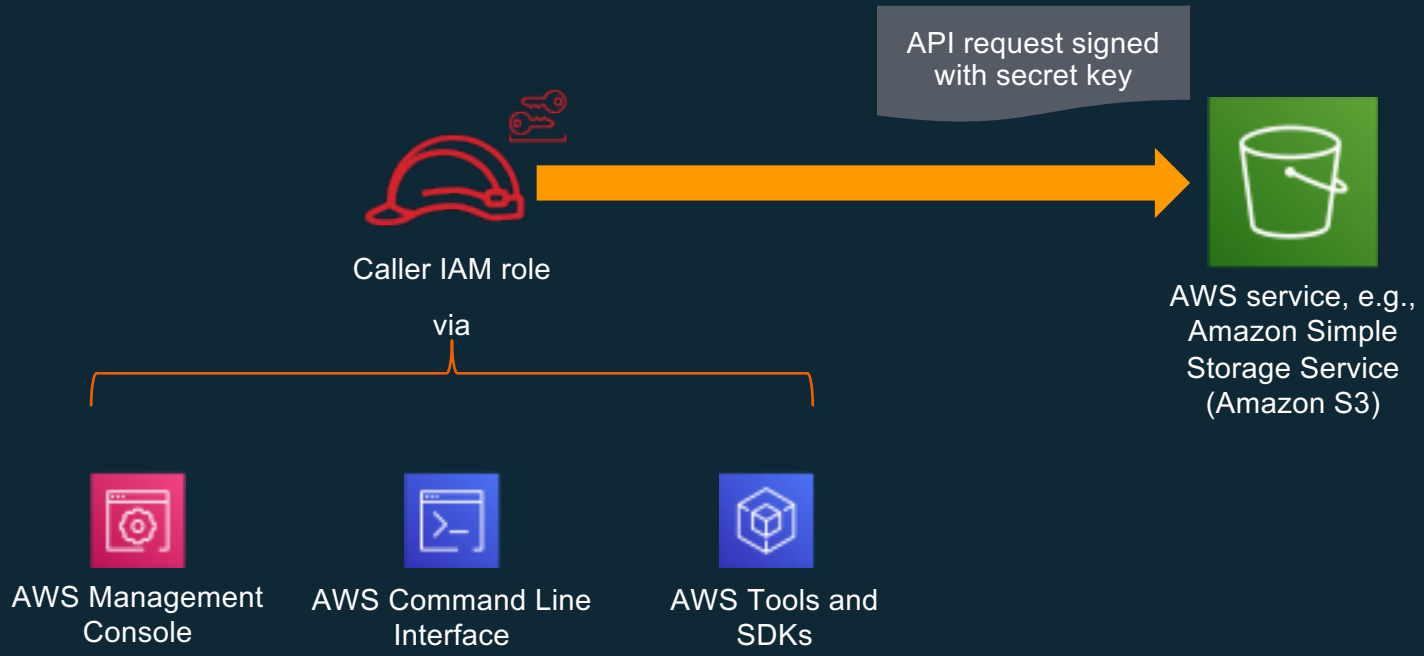
Amazon ECS task

…and many others

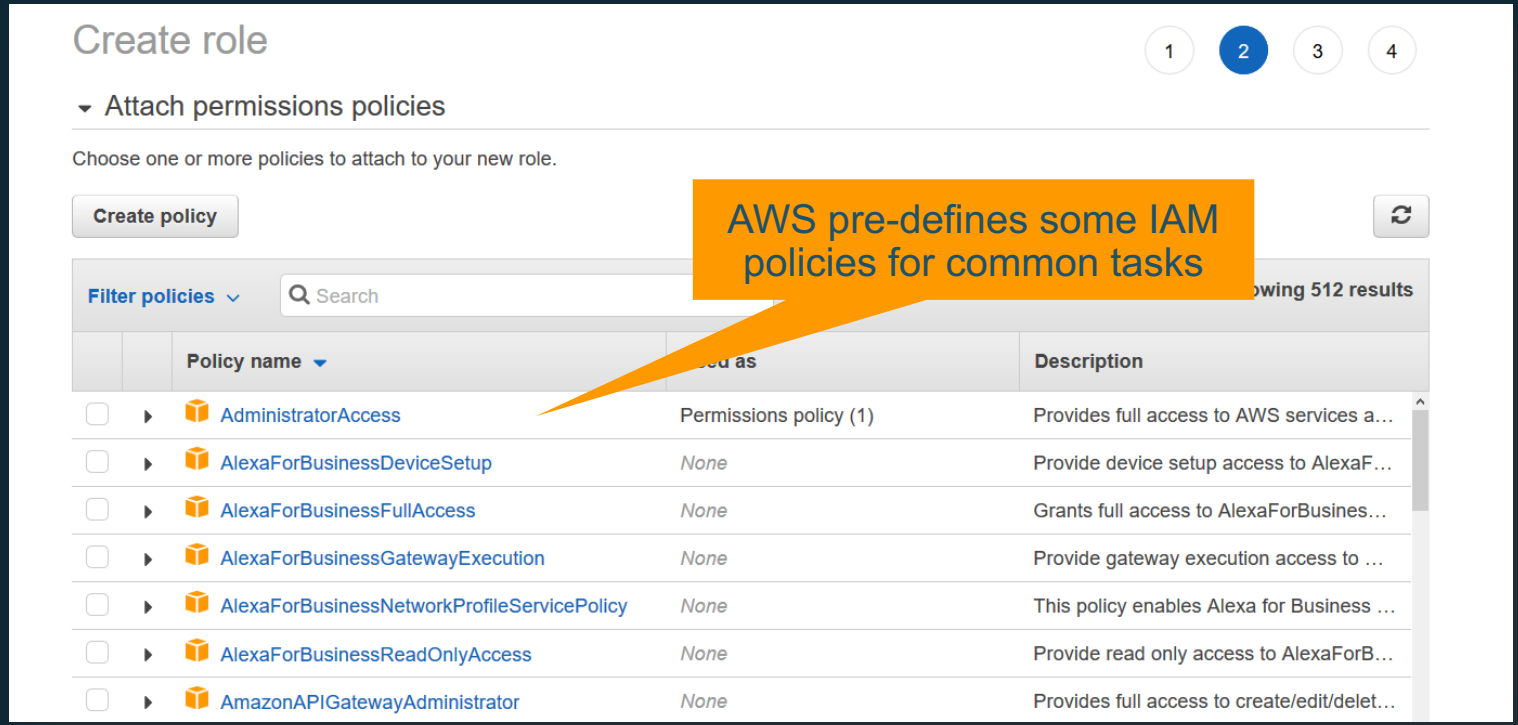
Creating a role in the AWS Management Console



How an authentication works in AWS



AWS-managed policies for common sets of permissions



Reading and writing IAM policy

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

Allow or deny?

What can (or can't) you do?

What can (or can't) you do it to?

In English: Allowed to take all Amazon DynamoDB actions

Reading and writing IAM policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:BatchGetItem",
        "dynamodb:GetItem",
        "dynamodb:Query"
      ],
      "Resource": "*"
    }
  ]
}
```

In English: Allowed to take only a few specific Amazon DynamoDB actions

aws

Reading and writing IAM policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:BatchGetItem",
        "dynamodb:GetItem",
        "dynamodb:Query",
      ],
      "Resource": [
        "arn:aws:dynamodb:us-east-2:111122223333:table/MyTableName",
        "arn:aws:dynamodb:us-east-2:111122223333:table/MyTableName/index/*"
      ]
    }
  ]
}
```

In English: Allowed to take specific Amazon DynamoDB actions on a specific table and its indexes

This is an Amazon Resource Name (ARN);
All AWS services use them, and they follow this format

aws

Reading and writing IAM policy

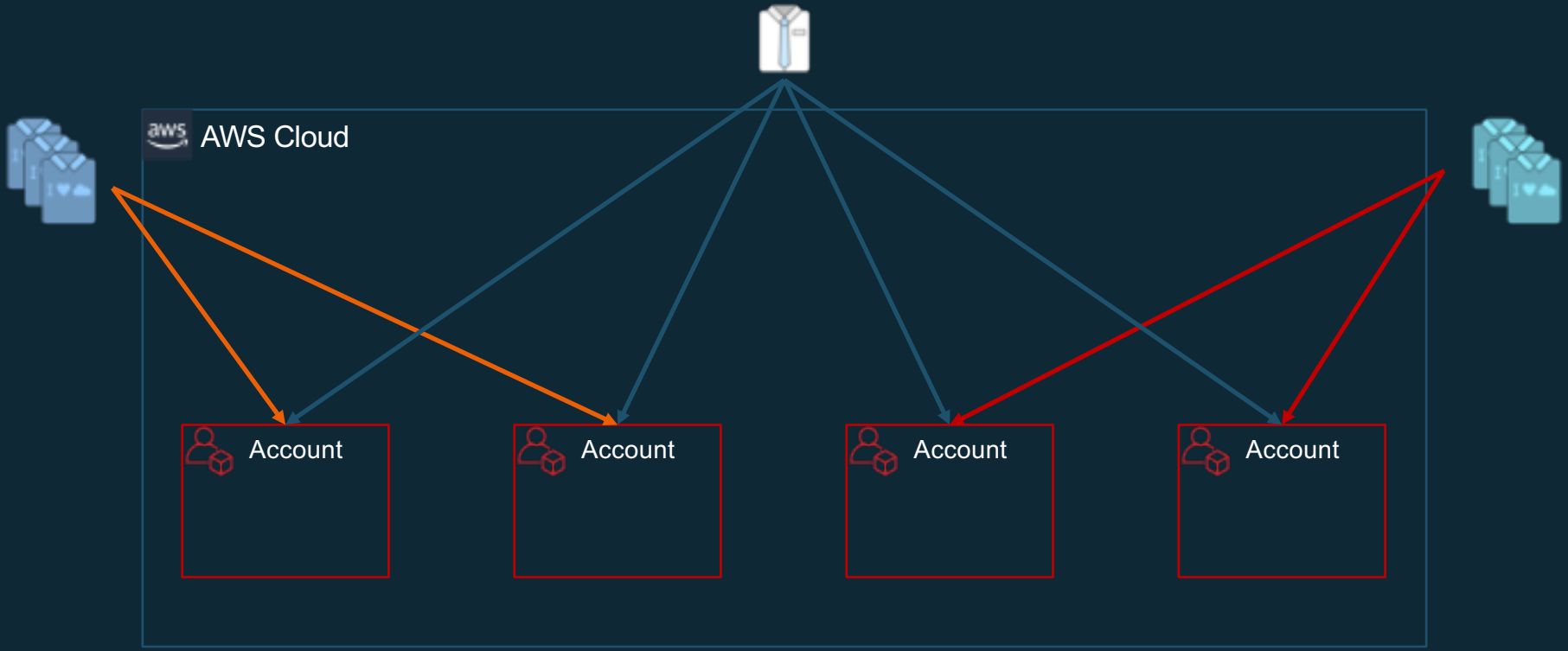
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "secretsmanager:ResourceTag/Project": "${aws:PrincipalTag/Project}"
        }
      }
    }
  ]
}
```

In English: You can read secrets whose project tag matches your own

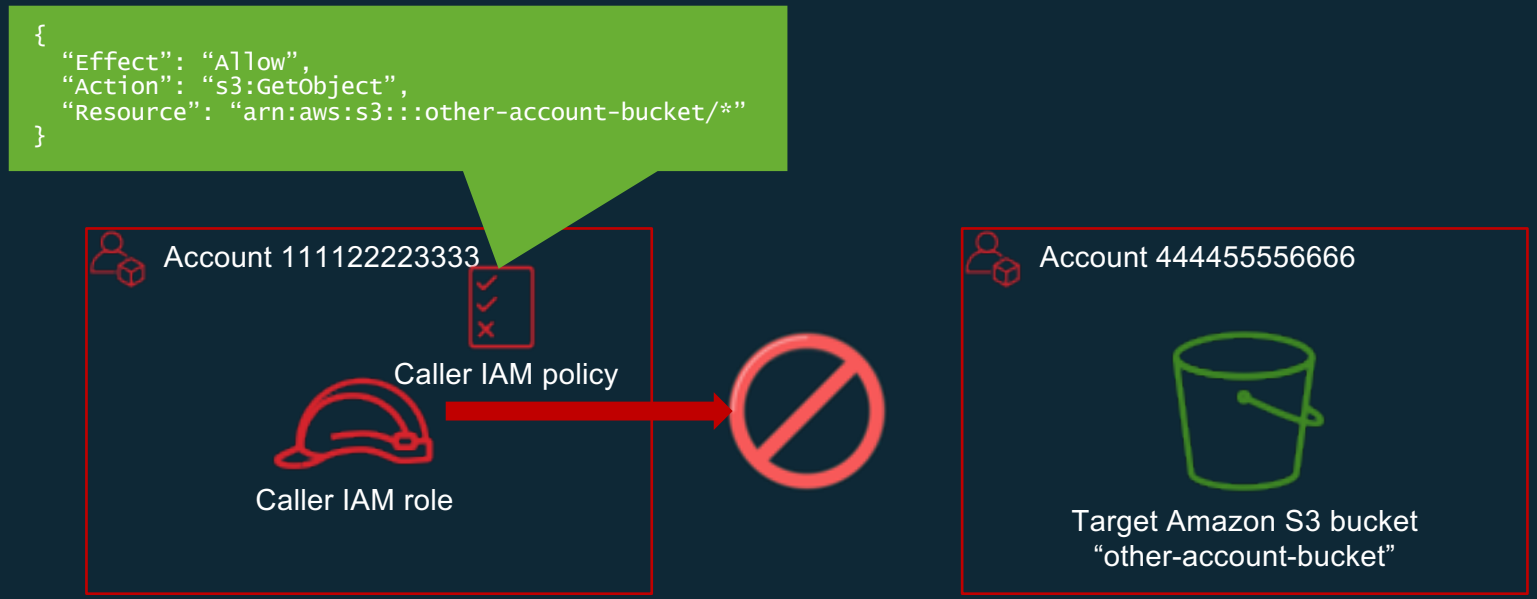
Attribute-based access control (ABAC)

aws

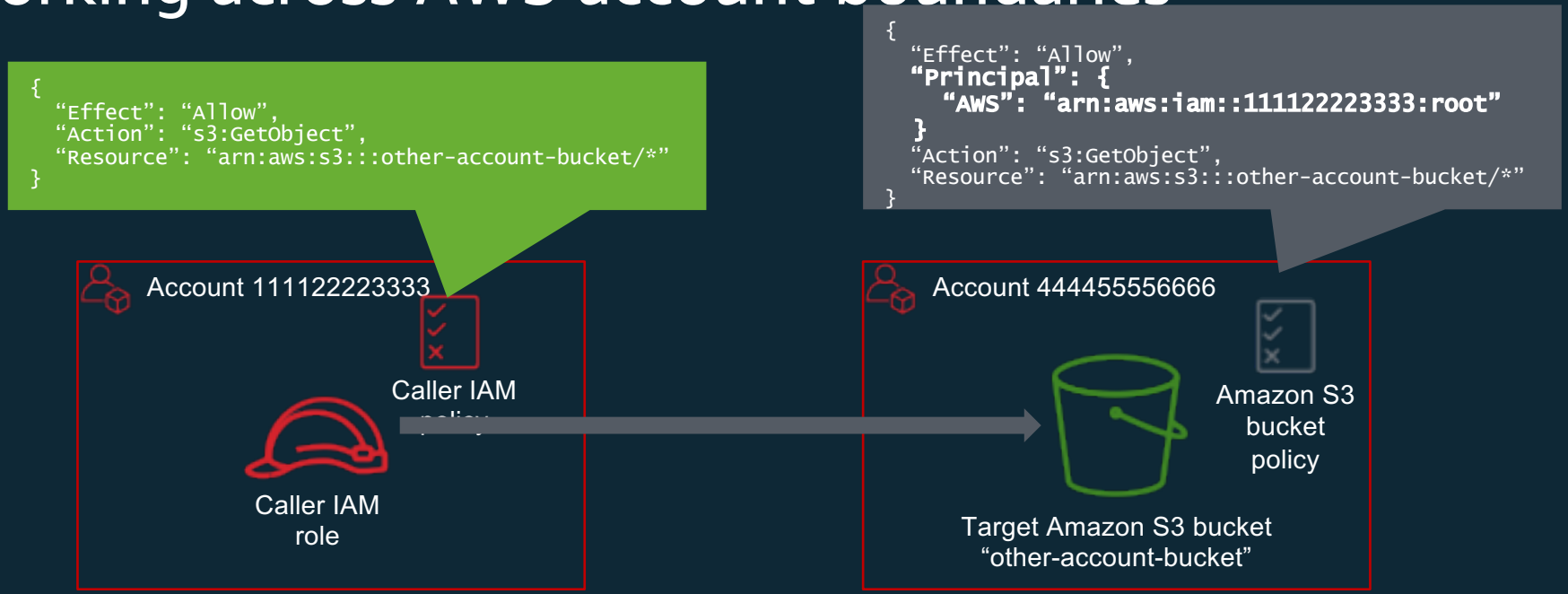
IAM in an AWS enterprise environment



Working across AWS account boundaries



Working across AWS account boundaries



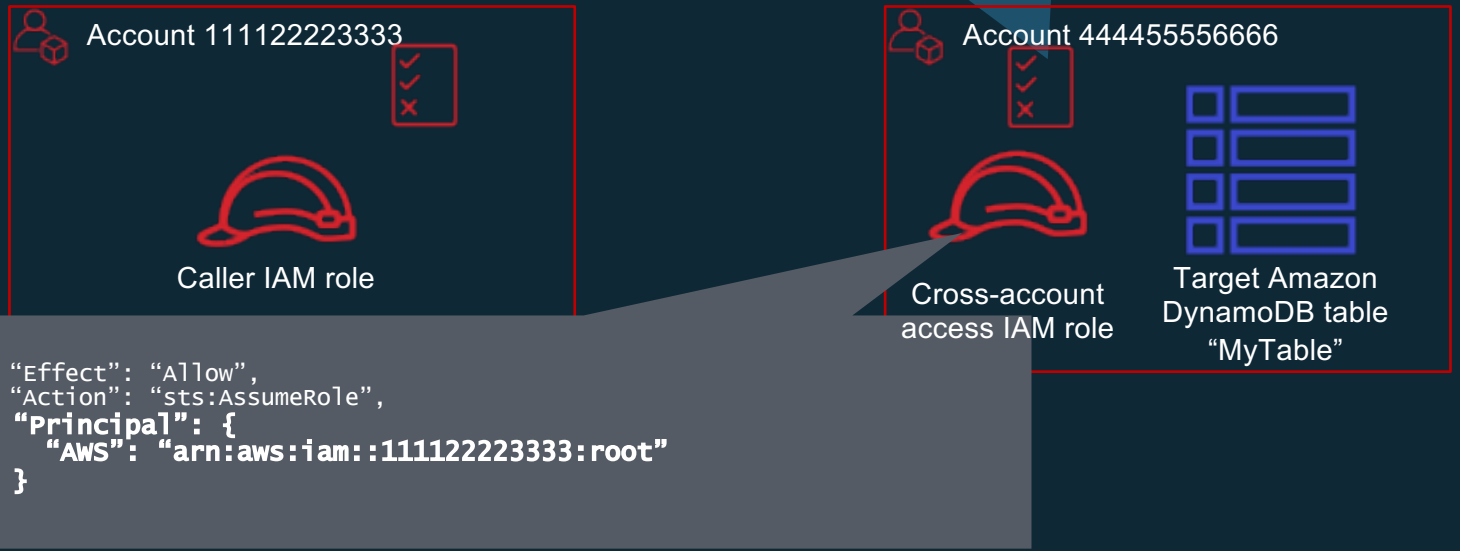
Working across AWS account boundaries

Working across AWS account boundaries

```
{
  “Effect”: “Allow”,
  “Action”: “dynamodb:GetItem”,
  “Resource”: “arn:aws:dynamodb:us-west-
2:444455556666:table/MyTable”
}
```

Working across AWS account boundaries

```
{
  “Effect”: “Allow”,
  “Action”: “dynamodb:GetItem”,
  “Resource”: “arn:aws:dynamodb:us-west-
2:444455556666:table/MyTable”
}
```

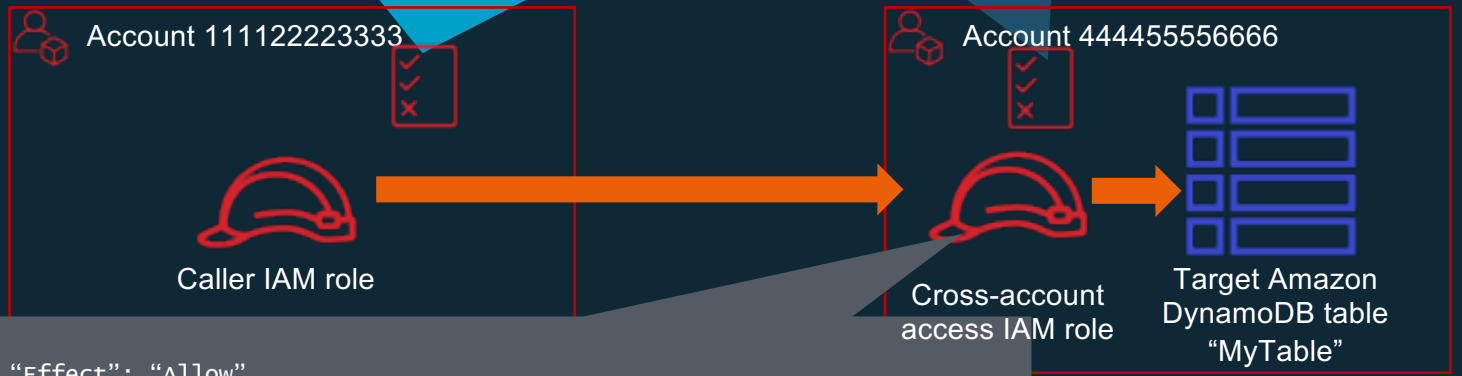



```
{
  “Effect”: “Allow”,
  “Action”: “sts:AssumeRole”,
  “Principal”: {
    “AWS”: “arn:aws:iam::111122223333:root”
  }
}
```

Working across AWS account boundaries

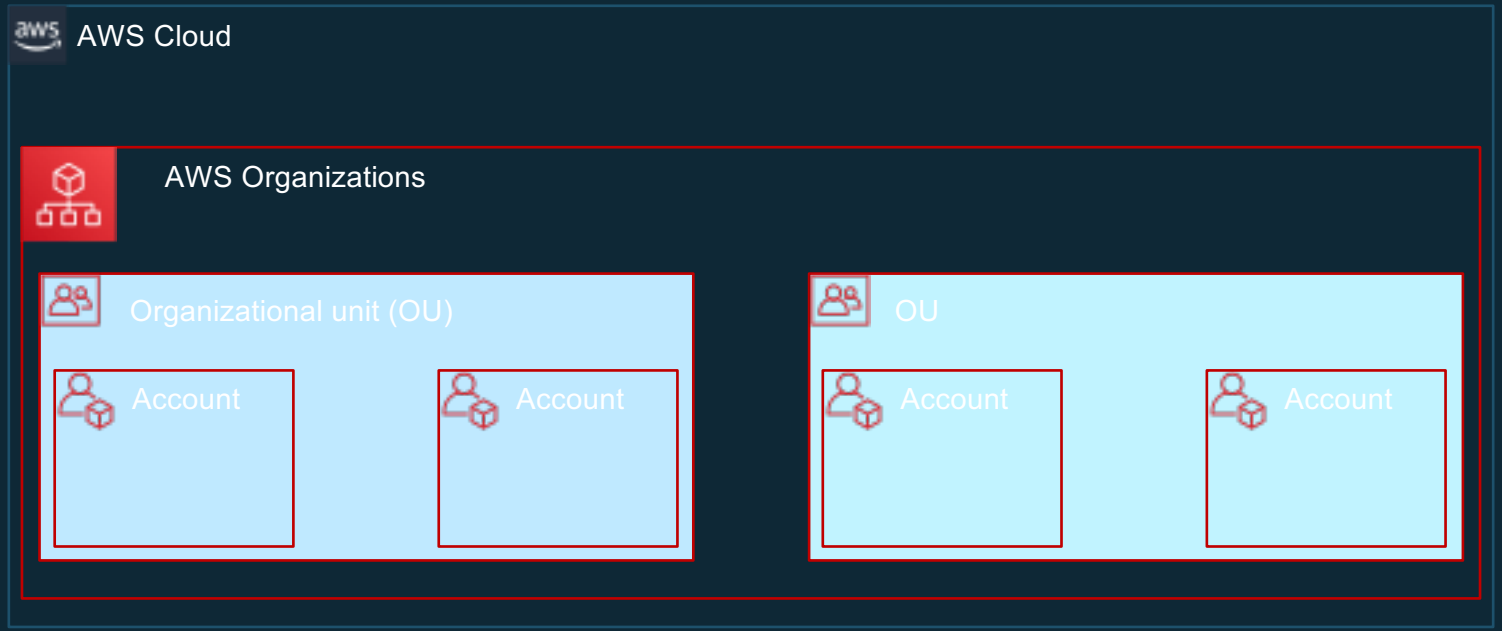
```
{
  "Effect": "Allow",
  "Action": "sts:AssumeRole",
  "Resource": "arn:aws:iam::444455556666:role/CrossAccountAccess"
}
```

```
{
  "Effect": "Allow",
  "Action": "dynamodb:GetItem",
  "Resource": "arn:aws:dynamodb:us-west-2:444455556666:table/MyTable"
}
```

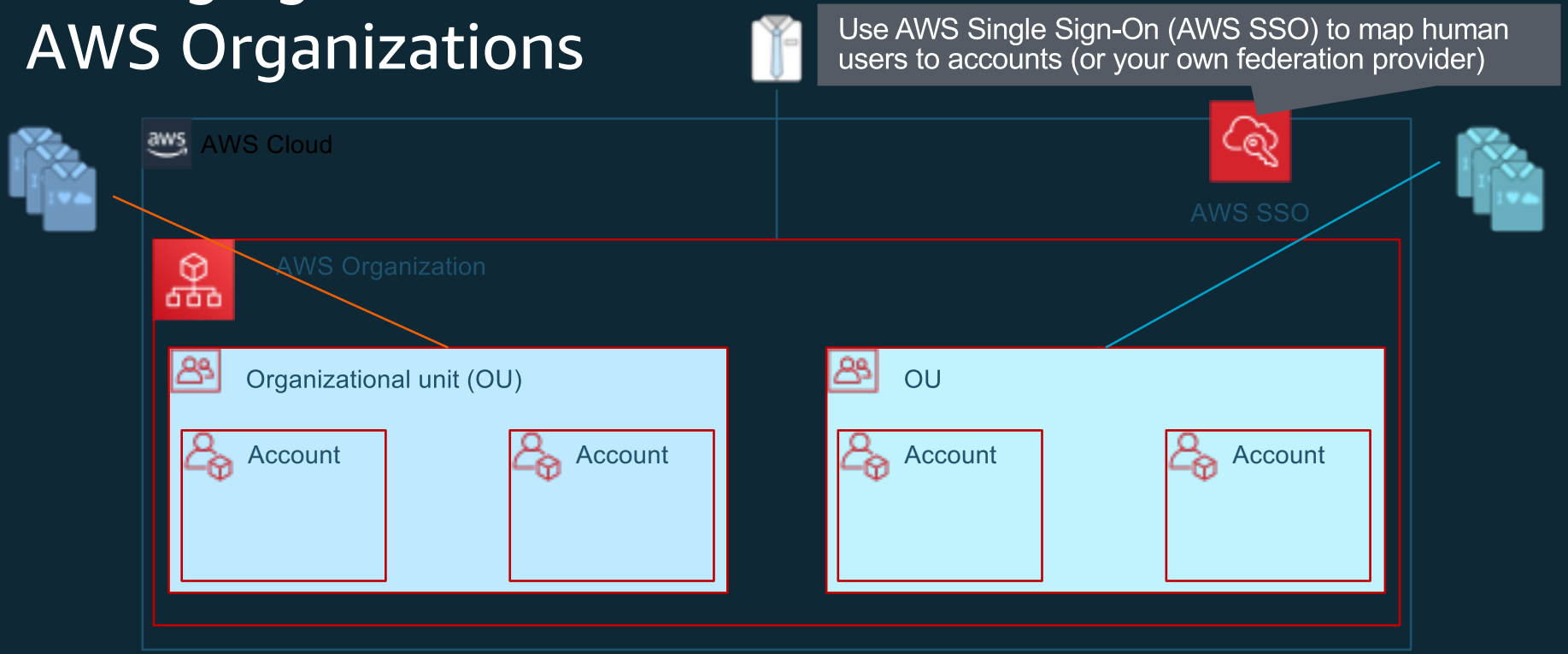



```
{
  "Effect": "Allow",
  "Action": "sts:AssumeRole",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
  }
}
```

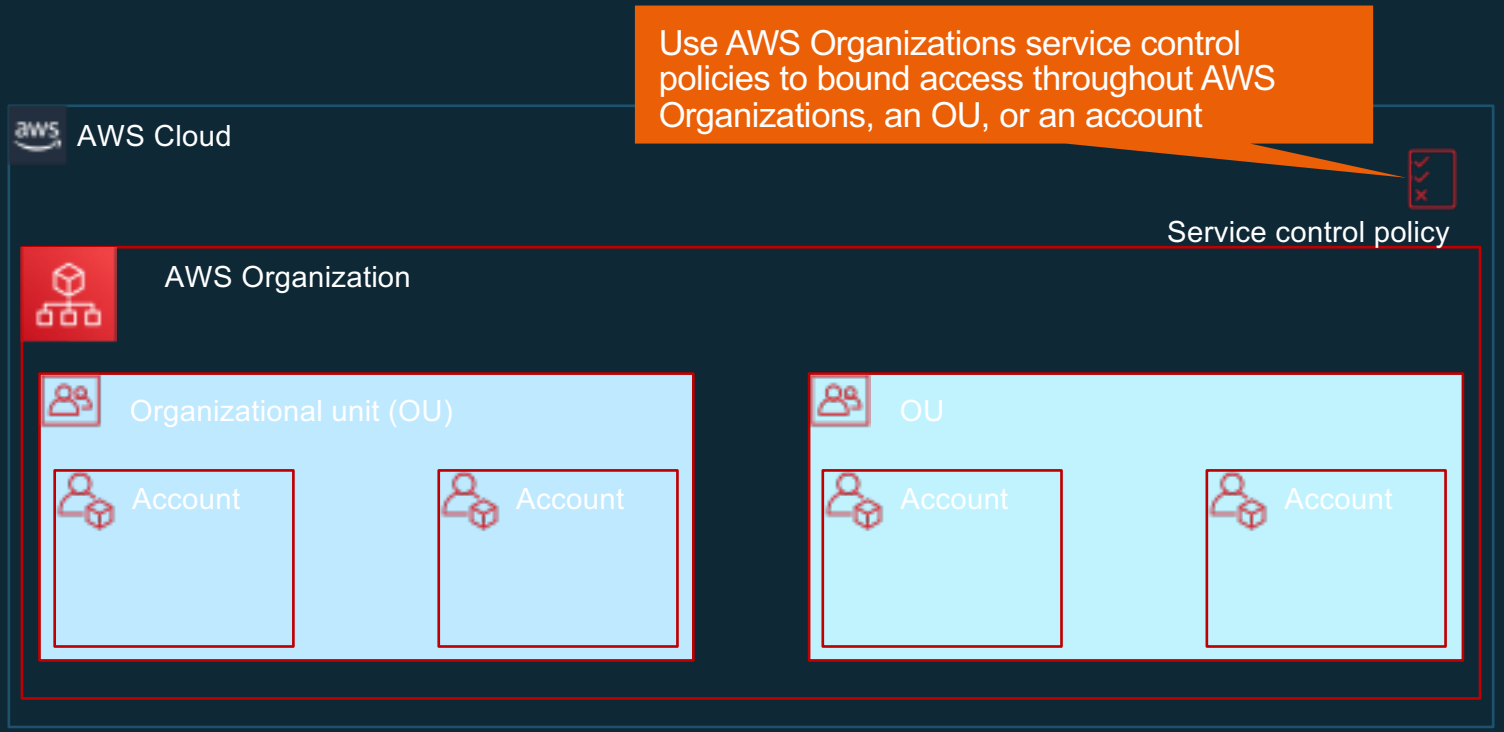
Managing multi-account environments with AWS Organizations



Managing multi-account environments with AWS Organizations



AWS Organizations provides guardrails for IAM



Encryption

How are you currently encrypting your data?

The mechanics of an AWS KMS key

For encrypting individual pieces of data (<=4KB)

- KMS.Encrypt("hello world") ➔ AQICAHiwKPHZcwiIv….
- KMS.Decrypt("AQICAHiwKPHZcwiIv….") ➔ "hello world"

For encrypting application data, use envelope encryption

- KMS.GenerateDataKey ➔ symmetric dat
  and encrypted)
- Use plaintext data key to encrypt your d
- Store encrypted data key alongside your data
- To decrypt

EncryptedDataKey:
AQIDAHiwKPHZcwiIv+V4760rokzKMlVWo0M9O2D5yV
e3tqrBtwGBaaY6AwTrEcsjY0gTN8J8AAAAfjB8Bgk…

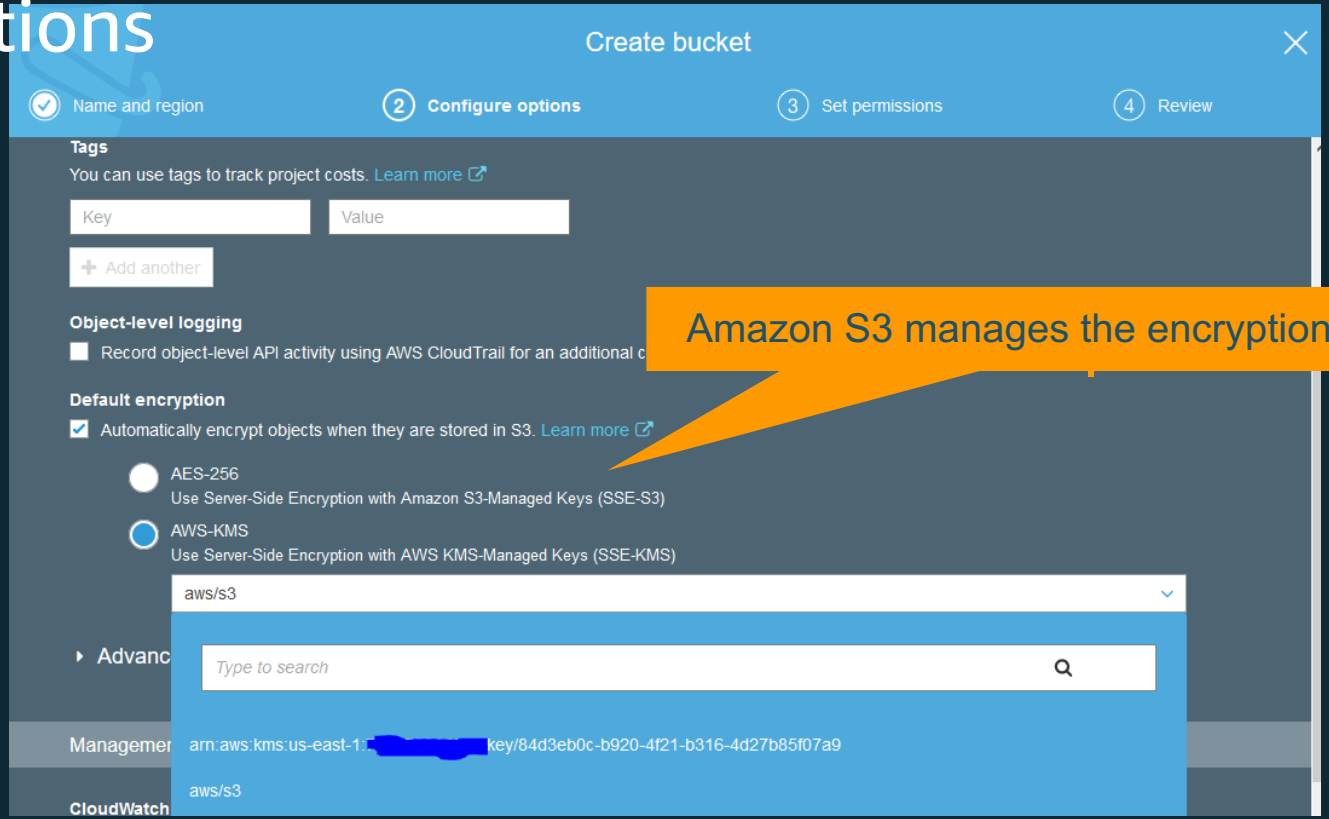
EncryptedPayload:
AQICAHiwKPHZcwiIv+V4760rokzKMlVWo0M9O2D5yV
e3tqrBtwGEZdK9s3SxlUE11PSPSadGAAAAaTBnBgk…

aws

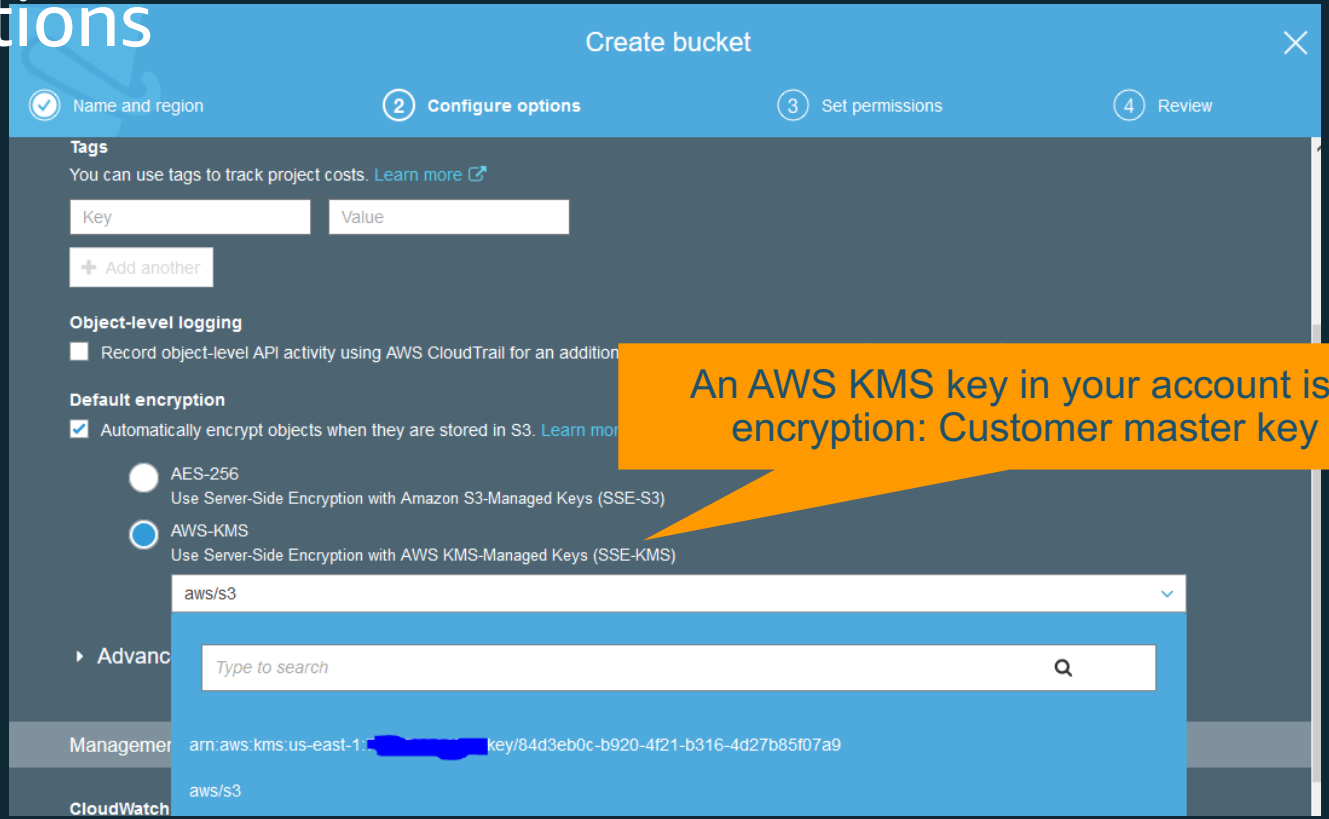
Why you didn’t need to understand that:

AWS services manage the AWS KMS mechanics for you

Encrypting the easy way with AWS service integrations

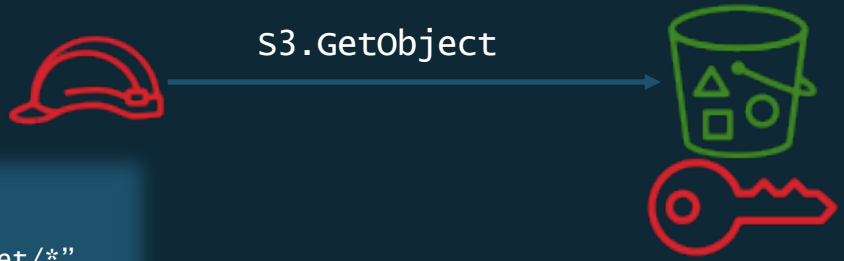


Encrypting the easy way with AWS service integrations



IAM permissions for AWS KMS keys

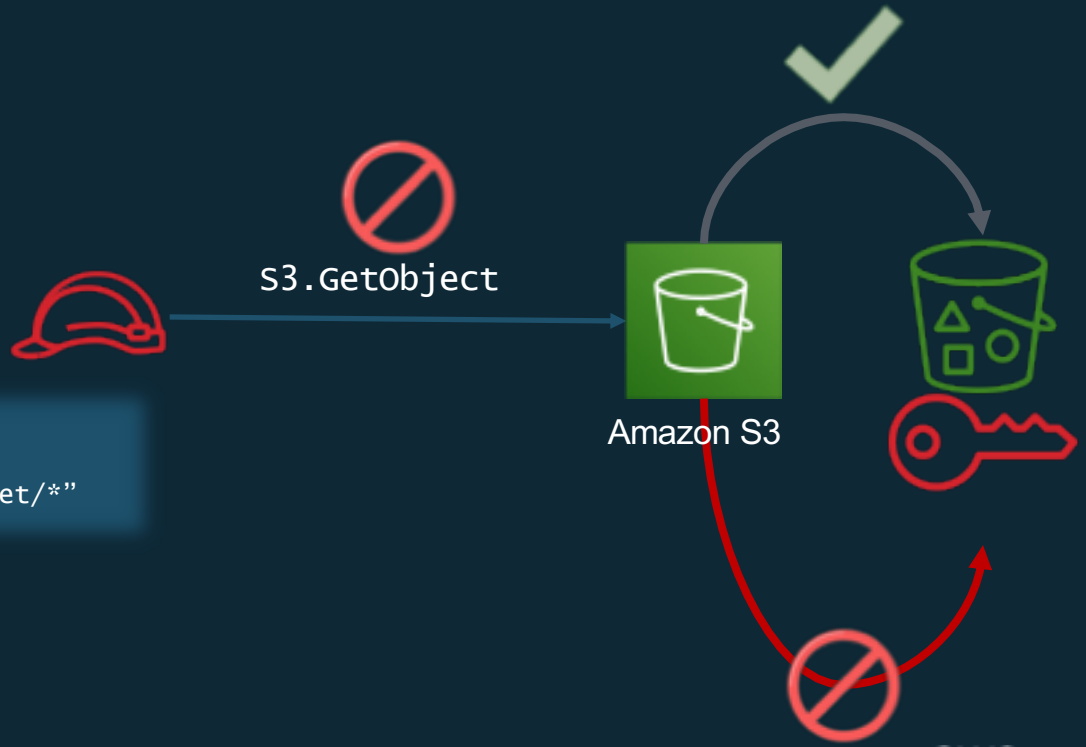
Question: What happens here?




```
{
  “Effect”: “Allow”,
  “Action”: “s3:GetObject”,
  “Resource”: “arn:aws:s3:::my-bucket/*”
}
```

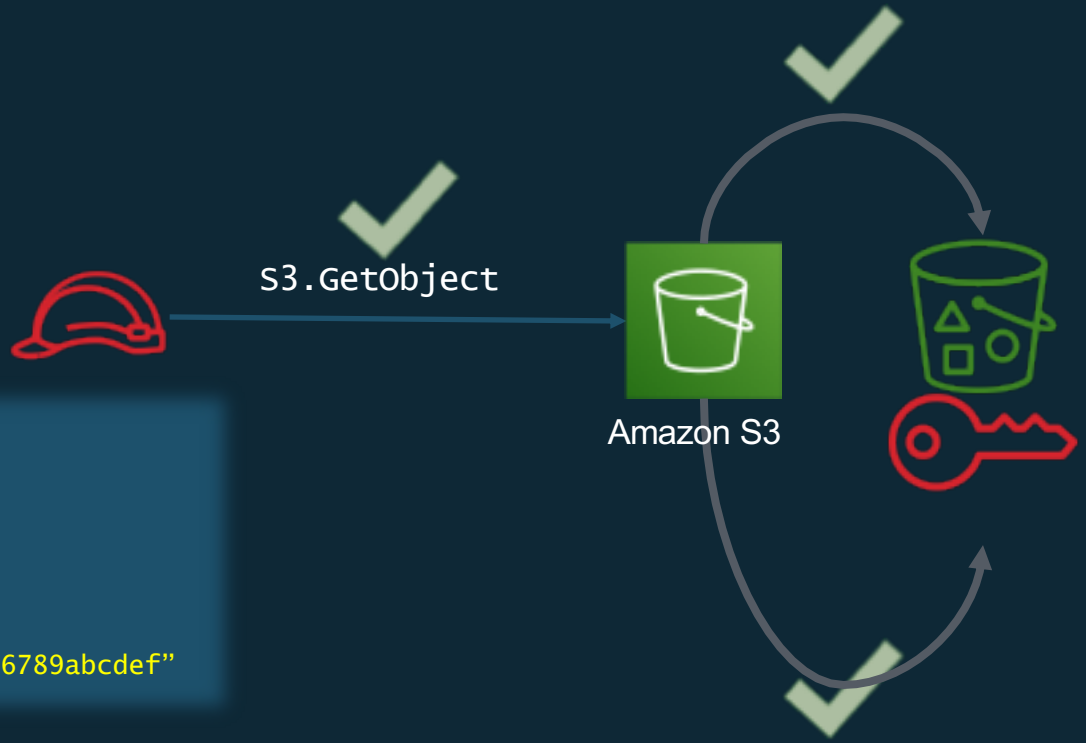

aws

IAM permissions for AWS KMS keys




```
{
  “Effect”: “Allow”,
  “Action”: “s3:GetObject”,
  “Resource”: “arn:aws:s3:::my-bucket/*”
}
```

IAM permissions for AWS KMS keys




```
{
  “Effect”: “Allow”,
  “Action”: “s3:GetObject”,
  “Resource”: “arn:aws:s3:::my-bucket/*”
},
{
  “Effect”: “Allow”,
  “Action”: “kms:Decrypt”,
  “Resource”: “arn:aws:kms:us-east-
2:111122223333:key/01234567-89ab-cdef-0123-456789abcdef”
}
```

Configuration Management

Amazon Inspector

- Vulnerability Assessment Service
  - Built from the ground up to support DevSecOps
  - Automatable via APIs
  - Integrates with CI/CD tools
  - On-Demand Pricing model
  - Static & Dynamic Rules Packages
  - Generates Findings

AWS WAF

Web Traffic Filtering with Custom Rules

Create custom rules that can block, allow or monitor requests based on IP address, HTTP headers, or a combination of both.

Malicious Request Blocking

AWS WAF can recognize and block common web application security risks like SQL injection (SQLi) and cross-site scripting (XSS).

Active monitoring & tuning

Monitor and configure the requests that are being blocked and allowed by the Web ACL rules.

AWS CloudTrail

Web service that records AWS API calls for your account and delivers logs.

Who?	When?	What?	Where to?	Where from?
Bill	3:27pm	Launch Instance	us-west-2	72.21.198.64
Alice	8:19am	Added Bob to admin group	us-east-1	127.0.0.1
Steve	2:22pm	Deleted DynamoDB table	eu-west-1	205.251.233.176


```
{
"Records": [
        {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-03-25T18:45:11Z"
                }
            }
        },
        "eventTime": "2014-03-25T21:08:14Z",
        "eventSource": "iam.amazonaws.com",
        "eventName": "AddUserToGroup",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "AWSConsole",
        "requestParameters": {
            "userName": "Bob",
            "groupName": "admin"
        },
        "responseElements": null
    },
    ...additional entries
  ]
}
```

AWS CloudWatch

Monitoring services for AWS Resources and AWS-based Applications.

What does it do?

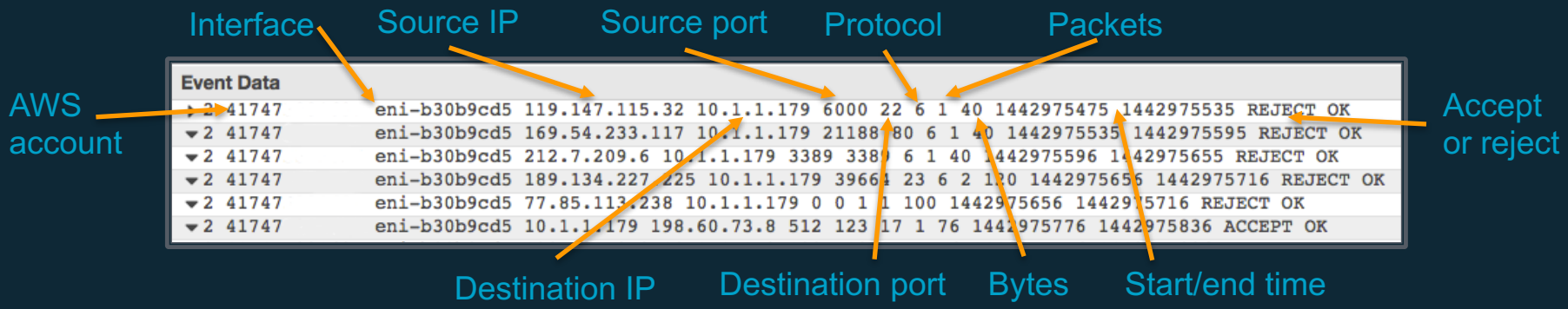
- Collect and Track Metrics
- Monitor and Store Logs
- Set Alarms (react to changes)
- View Graphs and Statistics

How can you use it?

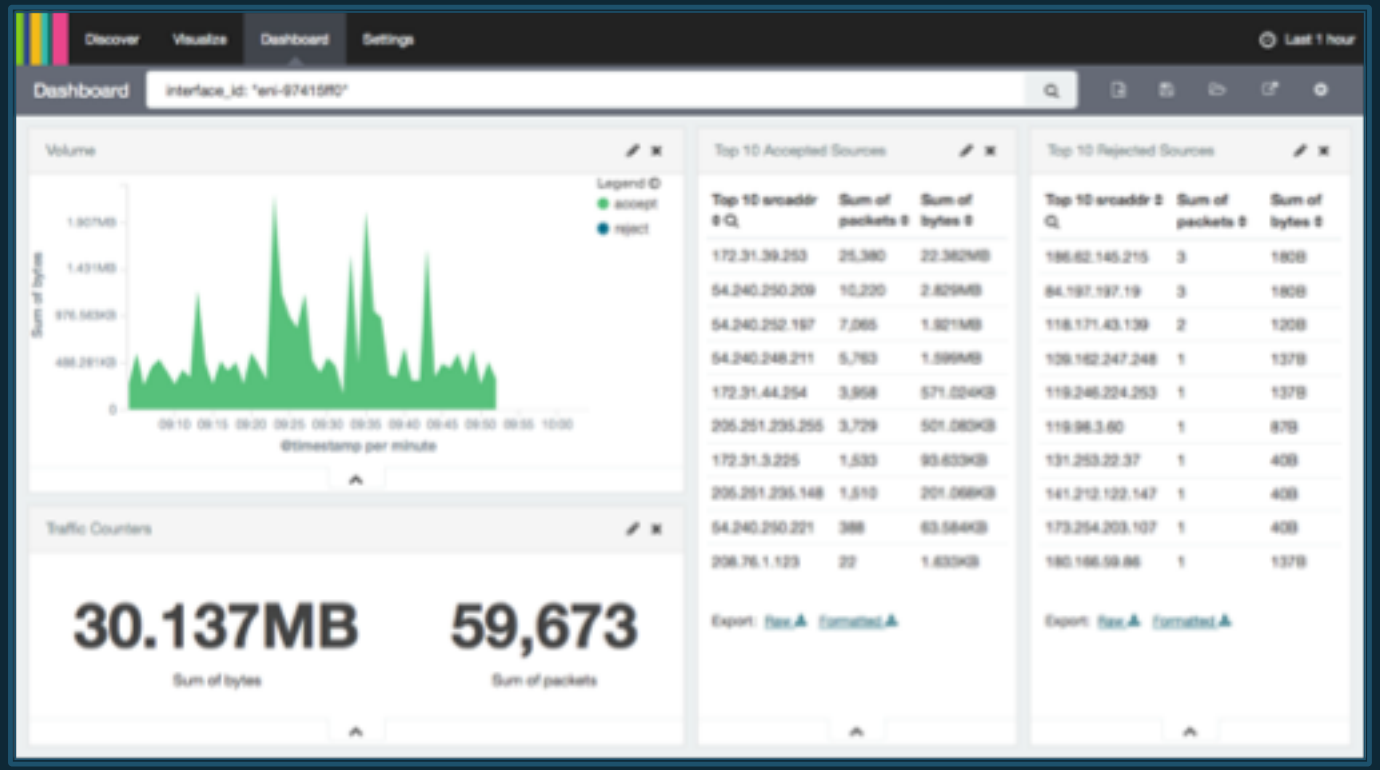
Monitor CPU, Memory, Disk I/O, Network, etc.	← CloudWatch Metrics
React to application log events and availability	← CloudWatch Logs / CloudWatch Events
Automatically scale EC2 instance fleet	← CloudWatch Alarms
View Operational Status and Identify Issues	← CloudWatch Dashboards

VPC Flow Logs

- Agentless
- Enable per ENI, per subnet, or per VPC
- Logged to AWS CloudWatch Logs
- Create CloudWatch metrics from log data
- Alarm on those metrics



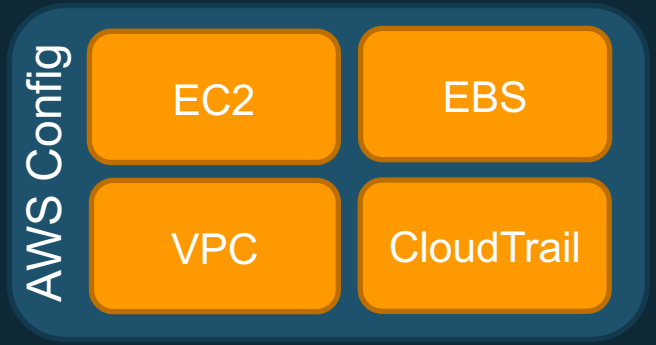
VPC Flow Logs



- Amazon Elasticsearch Service
- Amazon CloudWatch Logs subscriptions

AWS Config

Managed service for tracking AWS inventory and configuration, and configuration change notification.



Security Analysis

Audit Compliance

Change Management

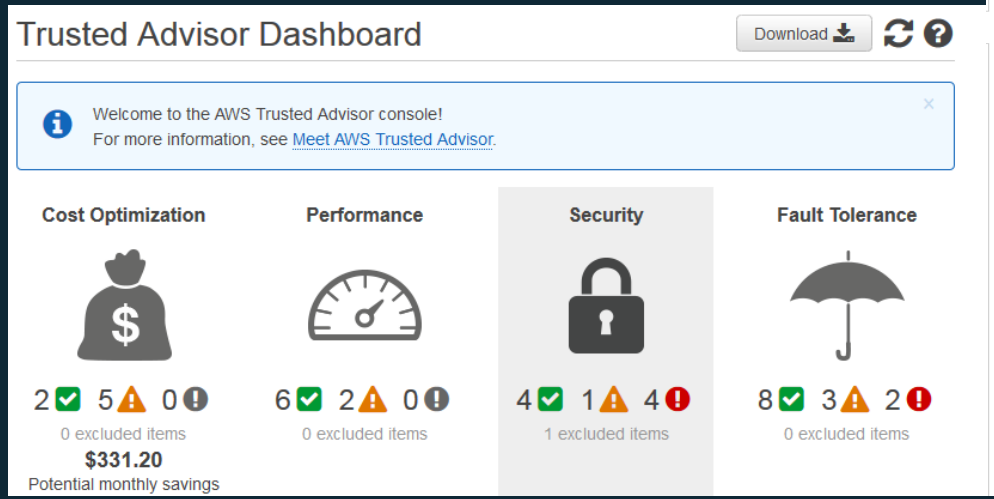
Troubleshooting

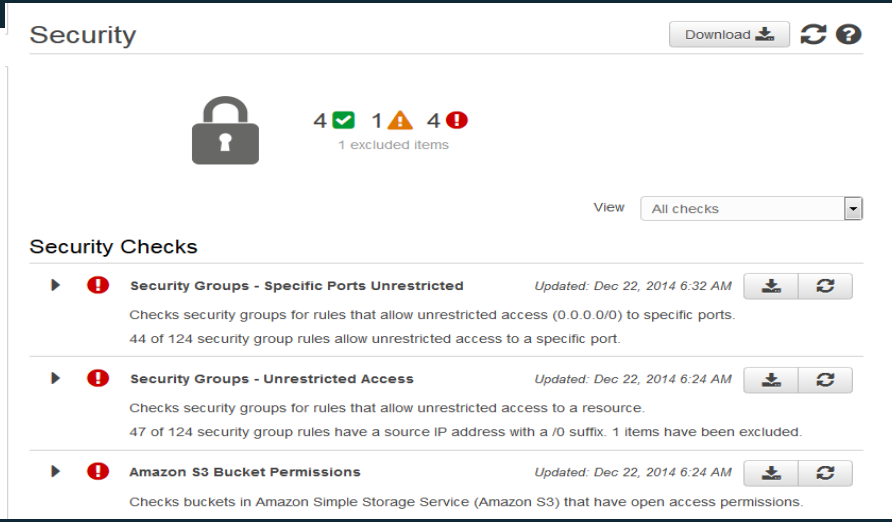
Discovery

Additional Best Practices

AWS Trusted Advisor

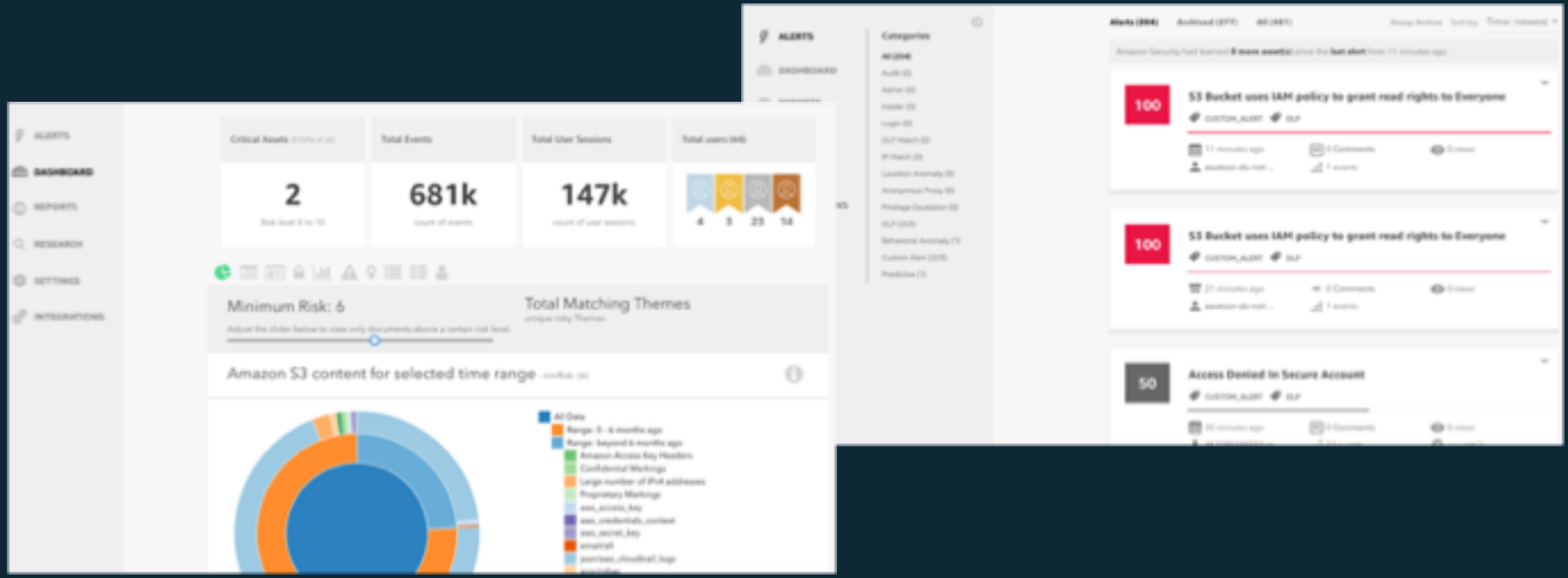
Leverage Trusted Advisor to analyze your AWS resources for best practices for availability, cost, performance and security.





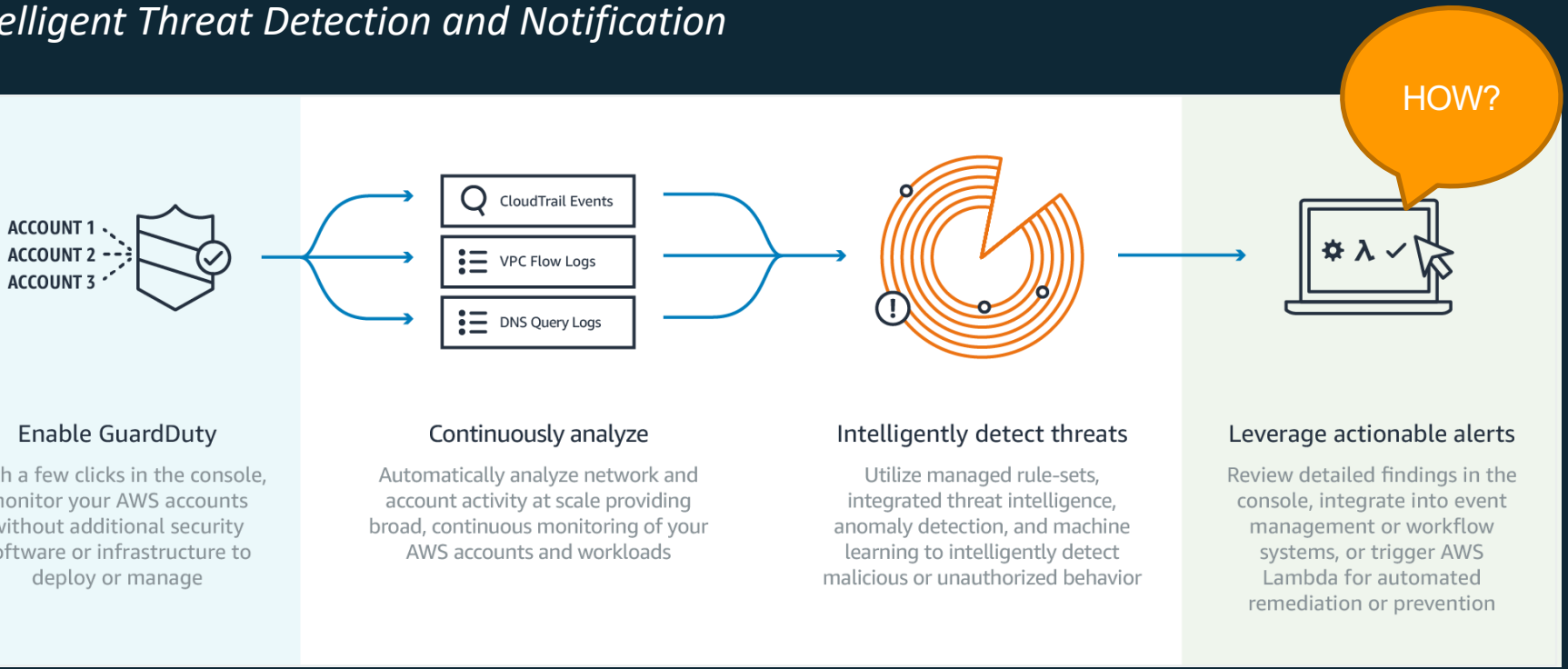
Amazon Macie

Leverage Amazon Macie to help prevent data loss in AWS.



Amazon GuardDuty

Intelligent Threat Detection and Notification



Enable GuardDuty

With a few clicks in the console, monitor your AWS accounts without additional security software or infrastructure to deploy or manage

Continuously analyze

Automatically analyze network and account activity at scale providing broad, continuous monitoring of your AWS accounts and workloads

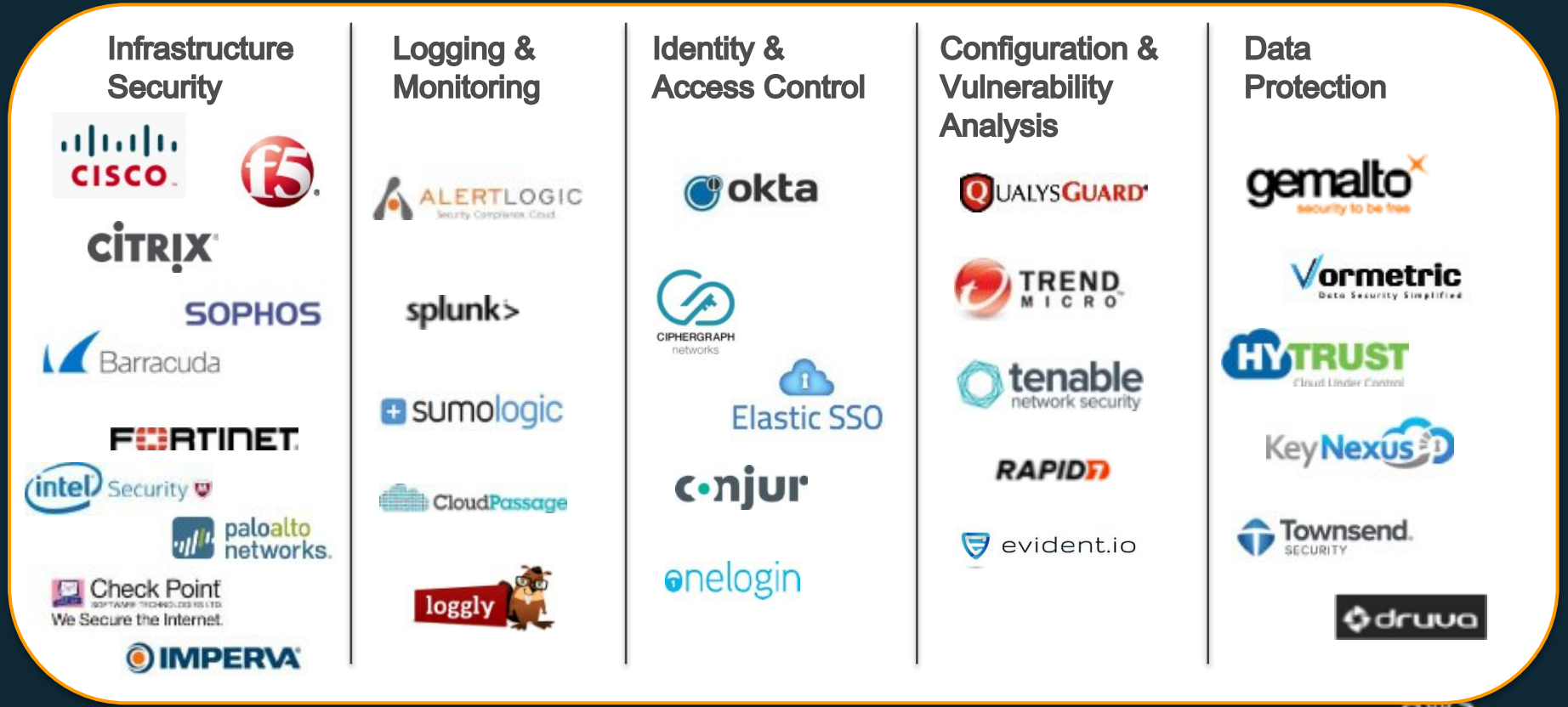
Intelligently detect threats

Utilize managed rule-sets, integrated threat intelligence, anomaly detection, and machine learning to intelligently detect malicious or unauthorized behavior

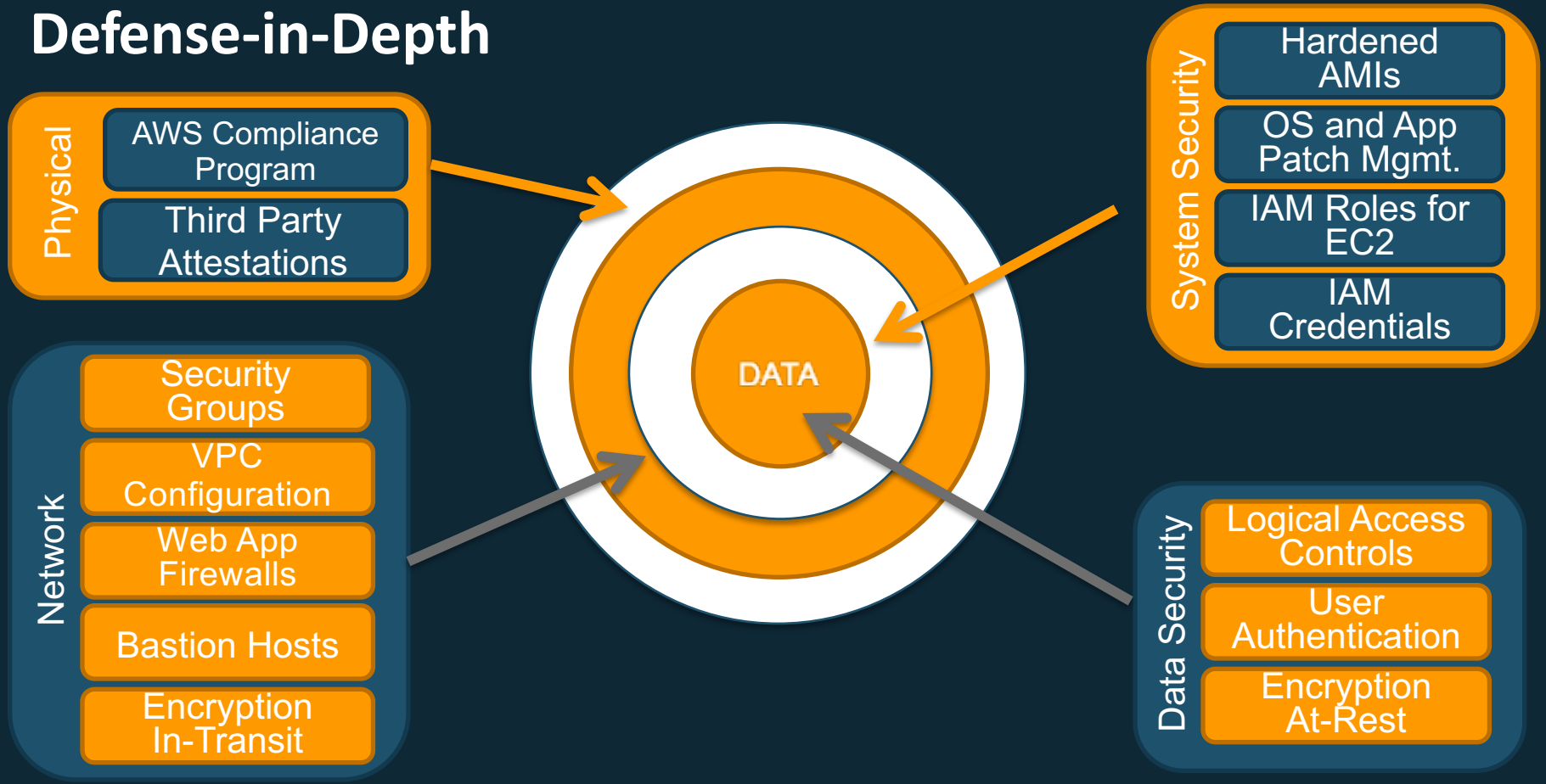
Leverage actionable alerts

Review detailed findings in the console, integrate into event management or workflow systems, or trigger AWS Lambda for automated remediation or prevention

AWS Marketplace Security Partners



Defense-in-Depth



AWS Security Center

AWS Security Center

Comprehensive security portal to provide a variety of security notifications, information and documentation.

http://aws.amazon.com/security

Security Whitepapers
- Overview of Security Process
- AWS Risk and Compliance
- AWS Security Best Practices

Security Bulletin

Security Resources

Vulnerability Reporting

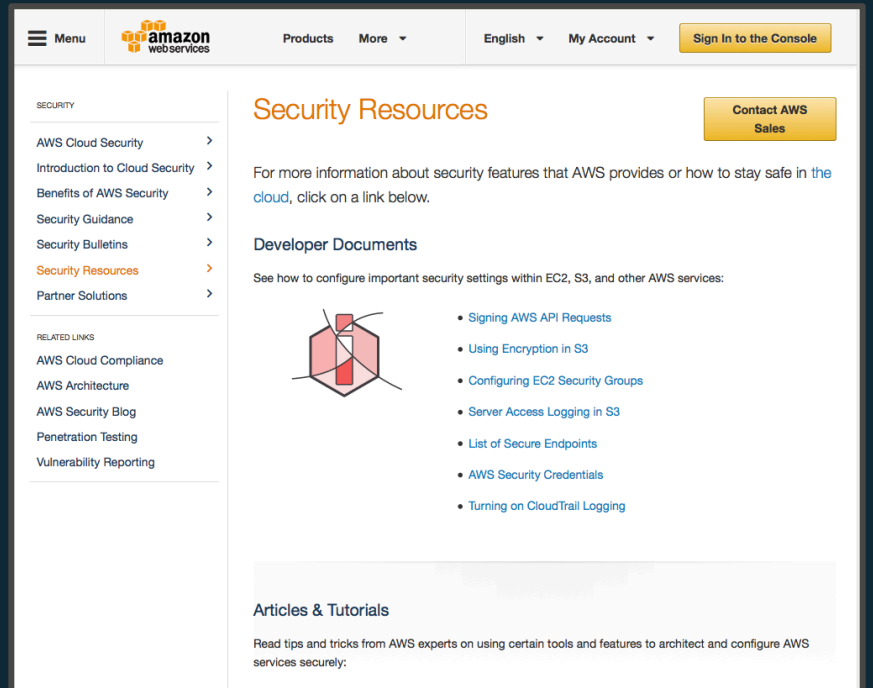
Penetration Testing Requests

Report Suspicious Emails

Security Resources

http://aws.amazon.com/security/security-resources/

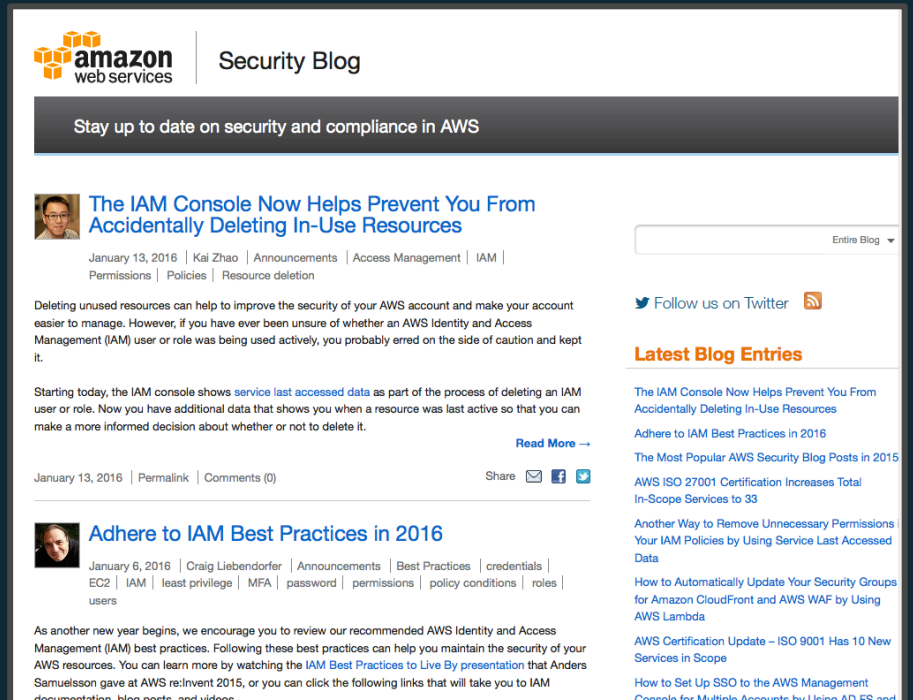
Developer Information, Articles and Tutorials, Security Products, and Whitepapers



AWS Security Blog

http://blogs.aws.amazon.com/security/

Subscribe to the blog – it's a great way to stay up-to-date on AWS security and compliance.



Questions