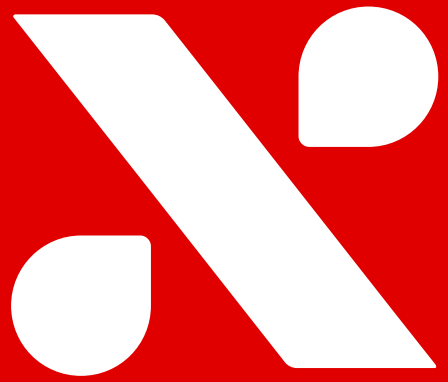


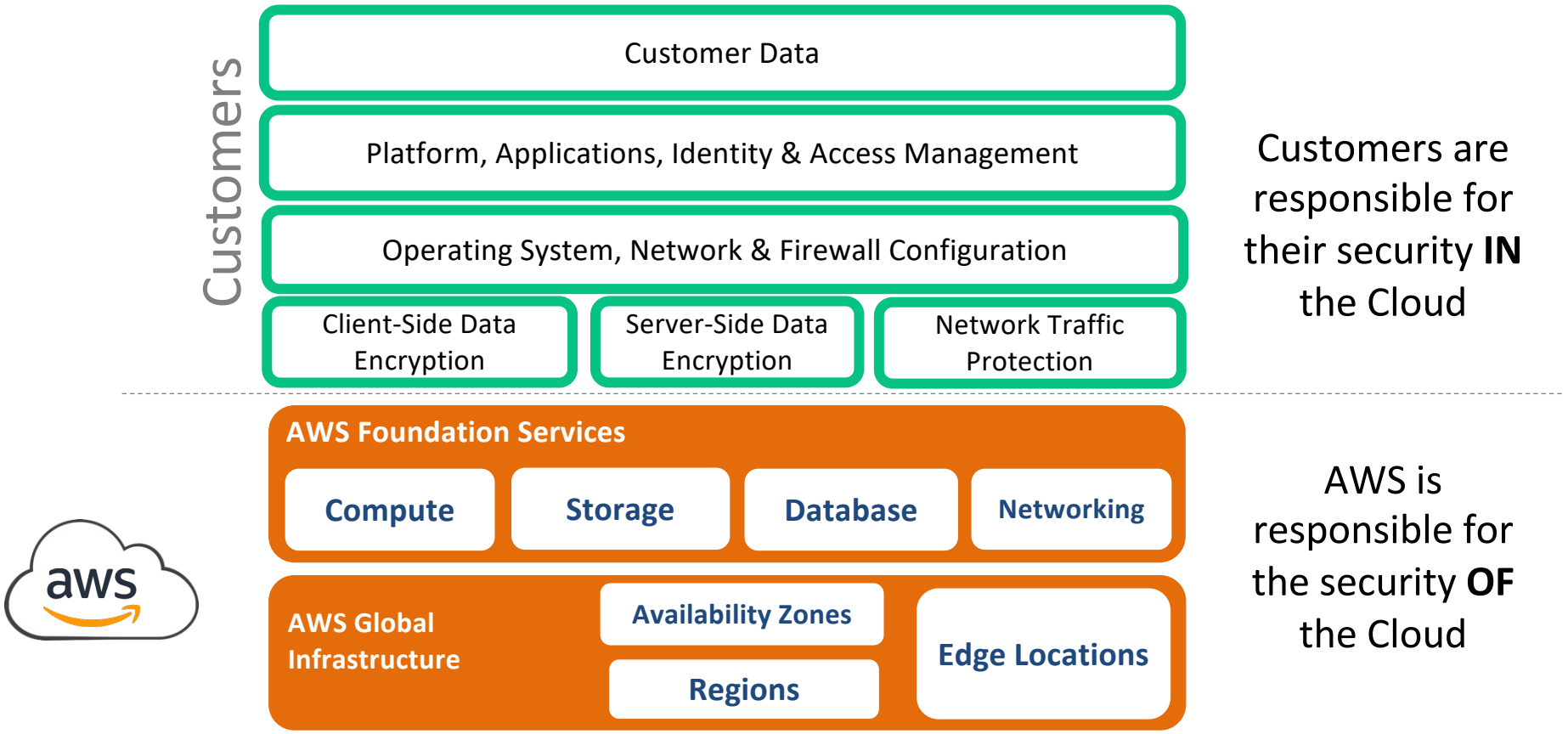
XPEPPERS

A Claranet Group Company

Introduction to Security Services

Paolo Latella – AWS Practice Manager

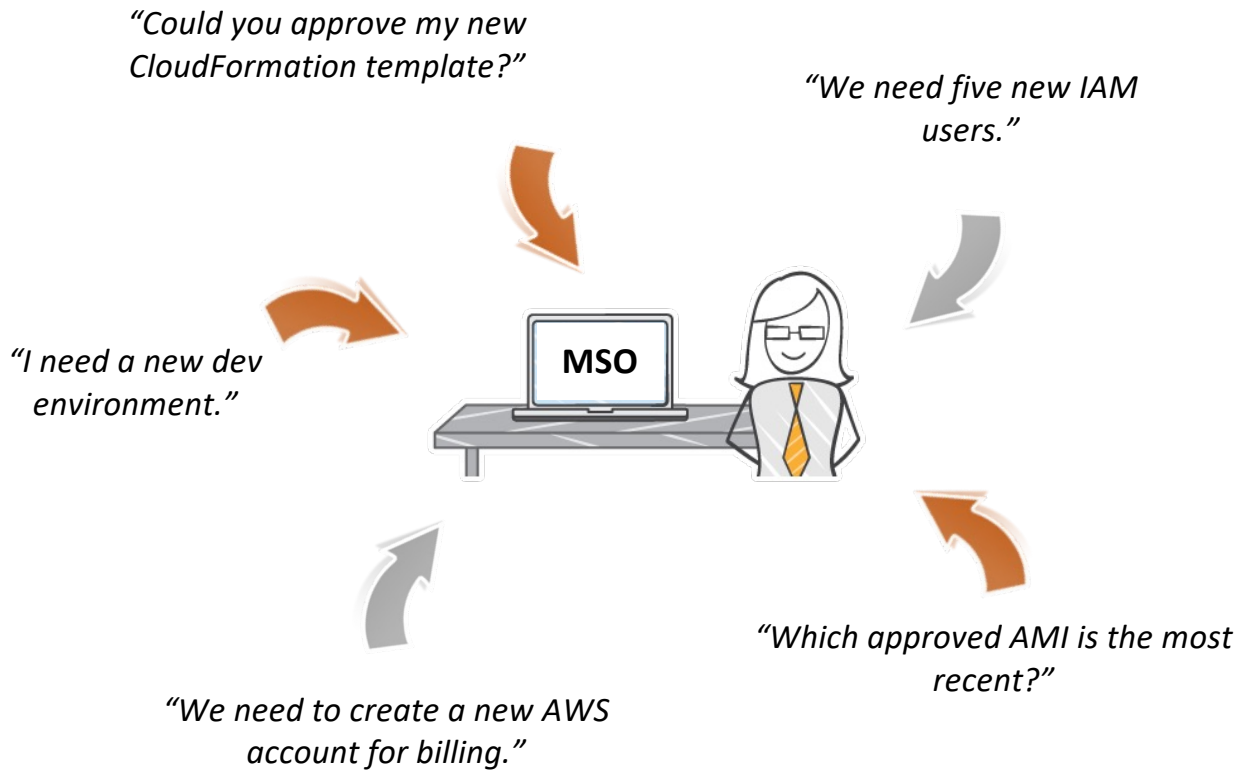
AWS Shared Responsibility Model



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

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

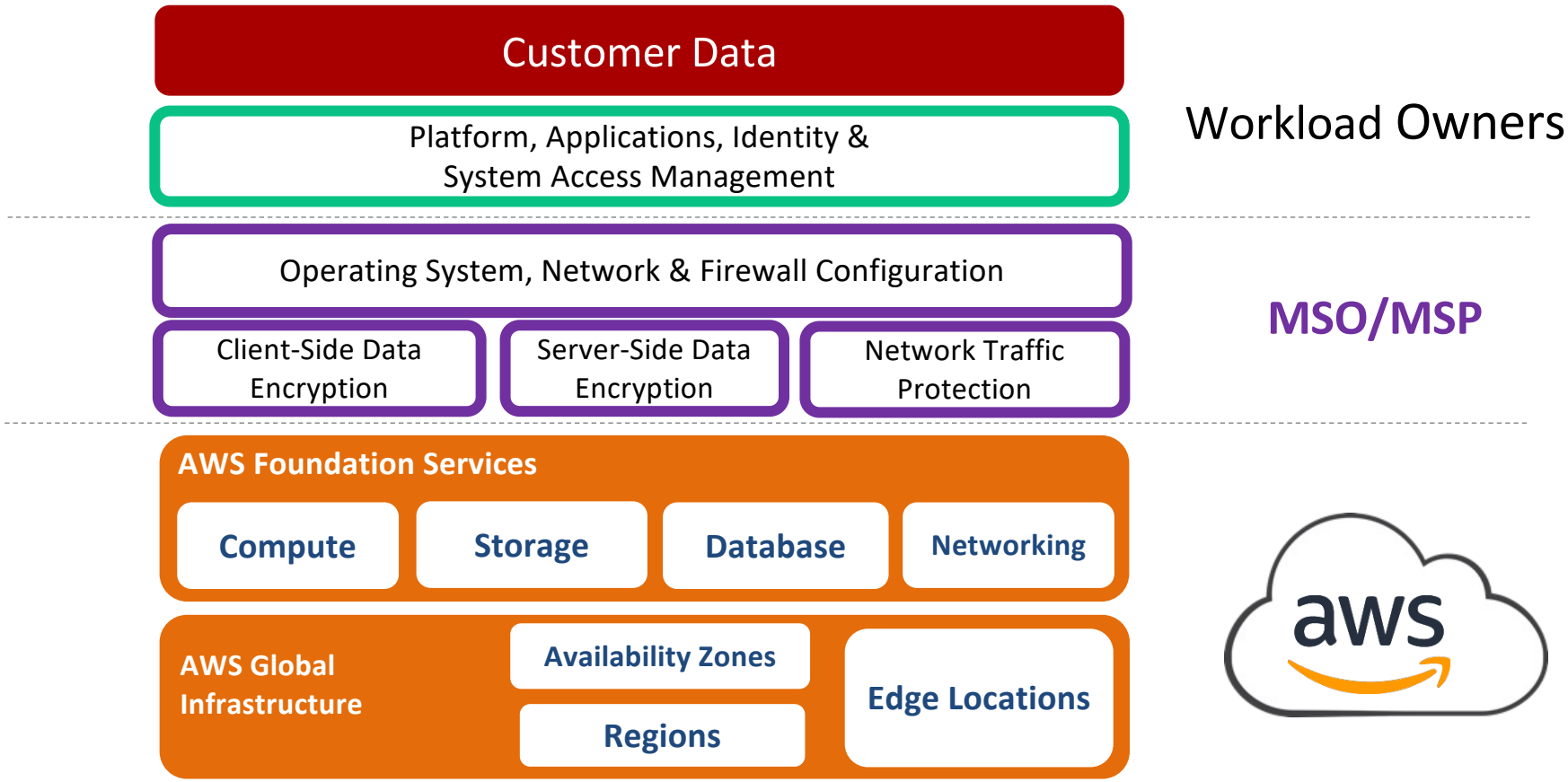
Managed Services Organization



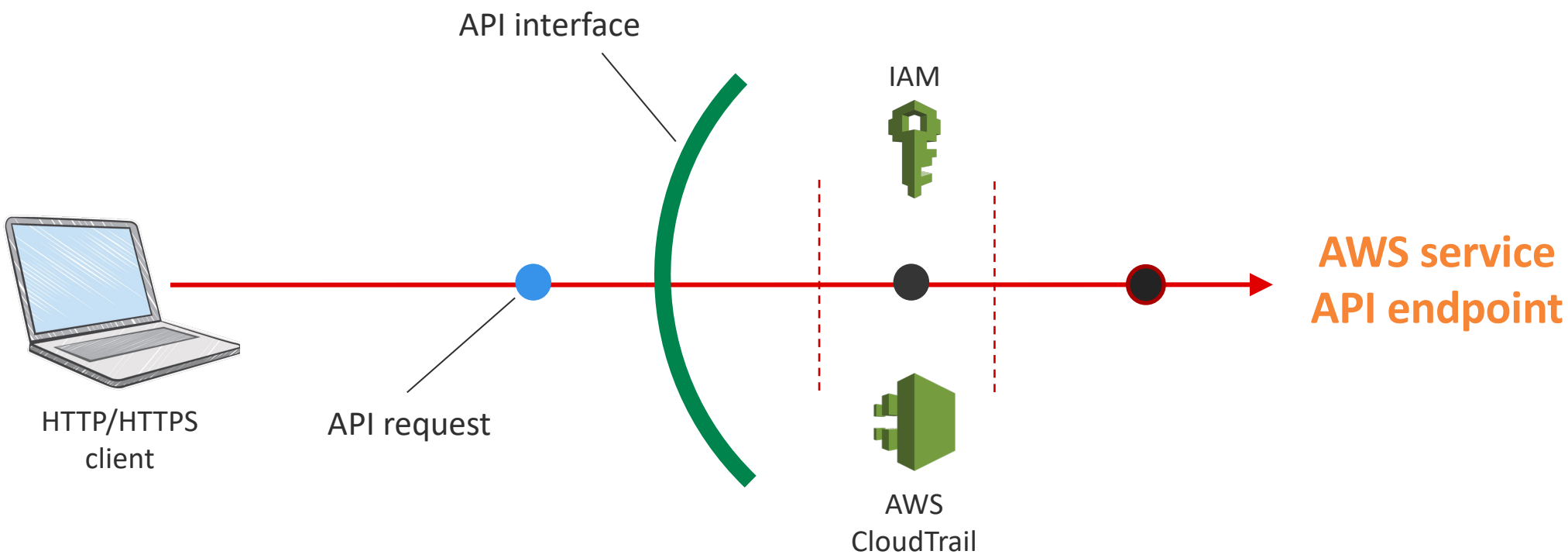
A **centralized** internal or external team responsible for:

- Establishing repeatable processes for deployment
- Defining guardrails for security and data protection
- Overseeing security and compliance auditing
- Hosting shared services

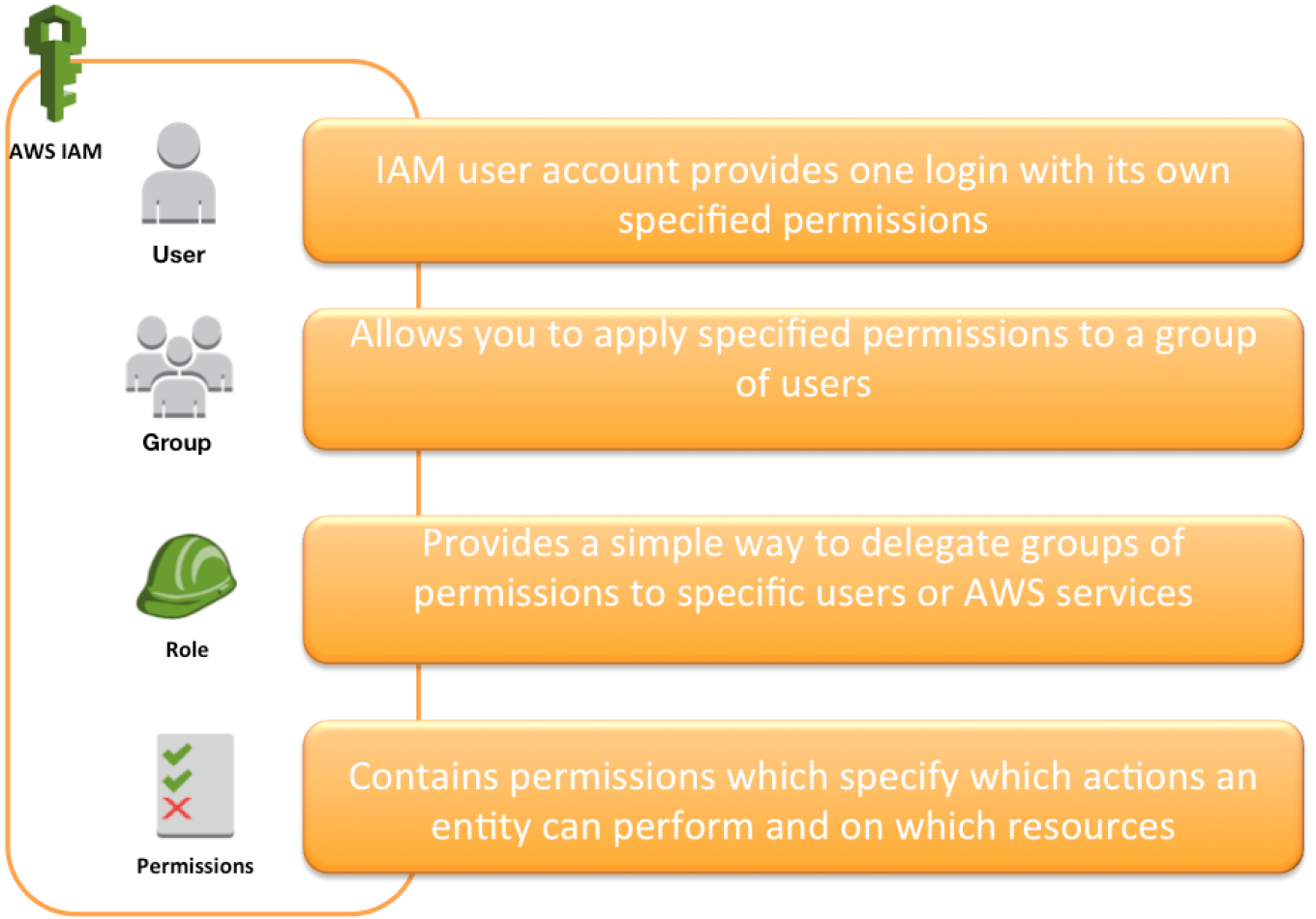
MSO Responsibility Model



API Request Flow



AWS IAM Overview



AWS Cloudtrail Overview

Who made the API call?

Who?

What?

What was the API call and what resources were affected?

Where was the API call made from?

Where?

When?

When was the API call made?

AWS Cloudtrail - Log Example

Who made the request?

```
{
    "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"
        },
```

When and from where?

```
"eventTime": "2018-03-06T21:01:59Z",
        "eventSource": "ec2.amazonaws.com",
        "eventName": "StopInstances",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "205.251.233.176",
        "userAgent": "ec2-api-tools 1.6.12.2",
```

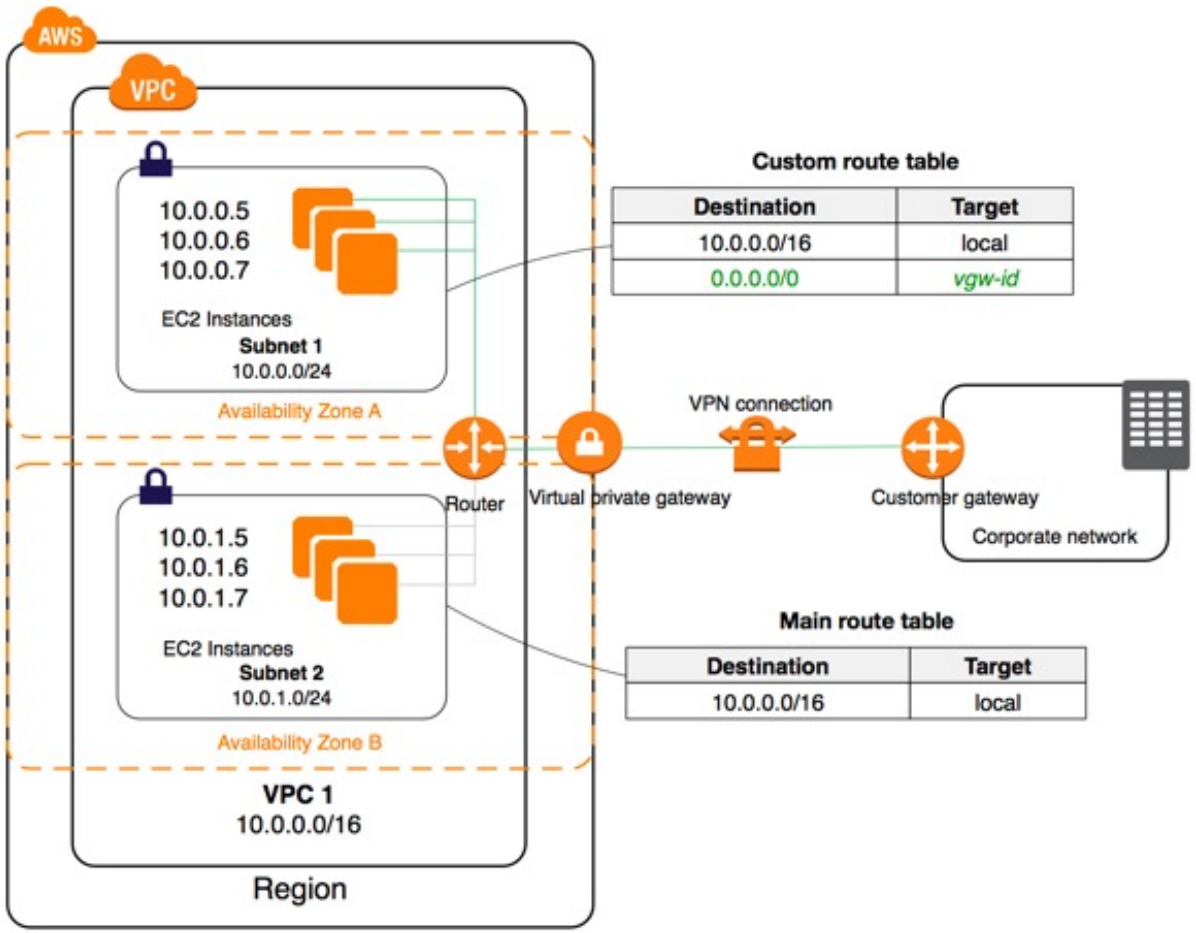
What was requested?

```
"requestParameters": {
      "instancesSet": {
          "items": [{
              "instanceId": "i-ebeaf9e2"
          }]
      },
      "force": false
  },
```

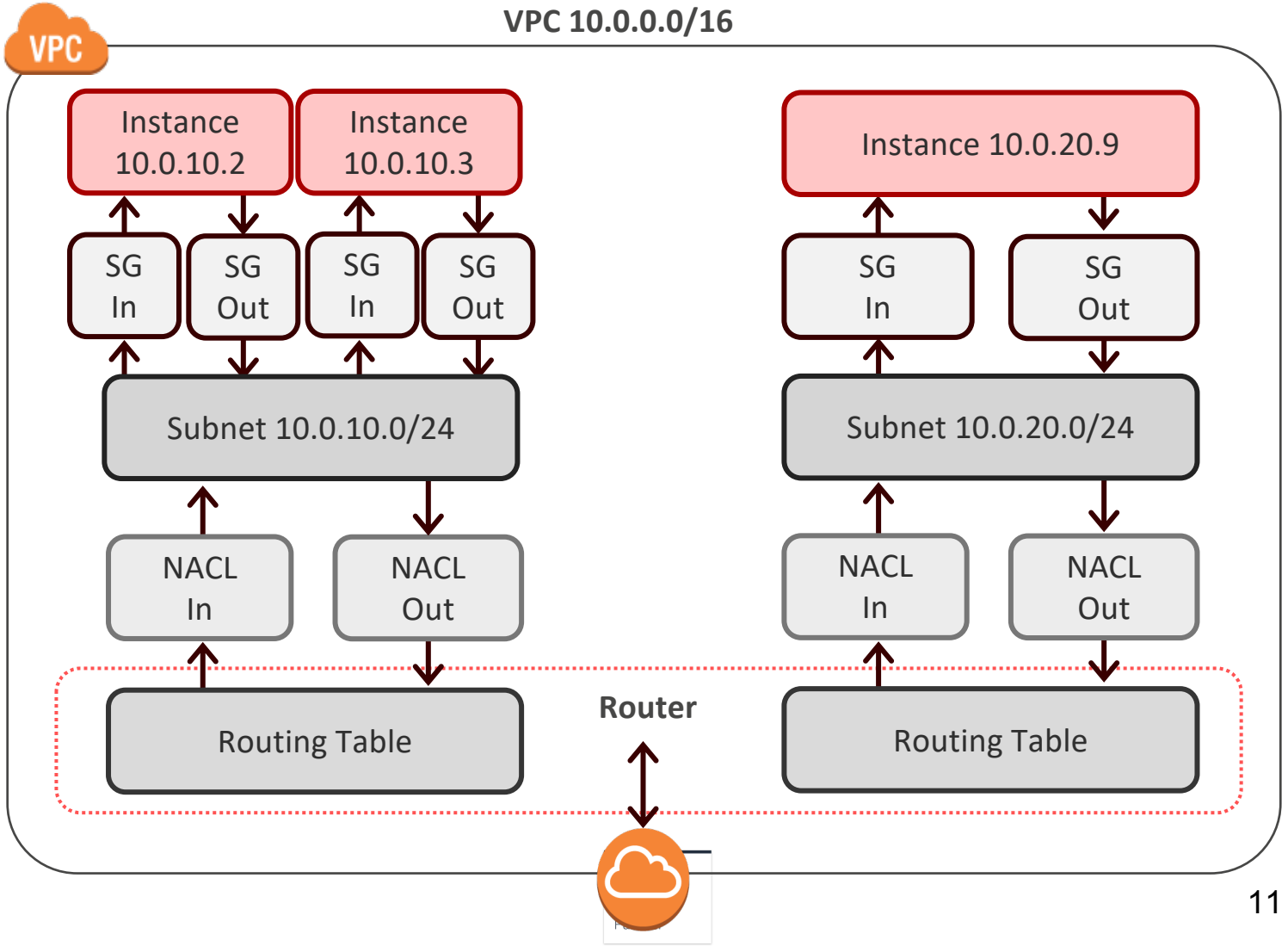
What was the response?

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

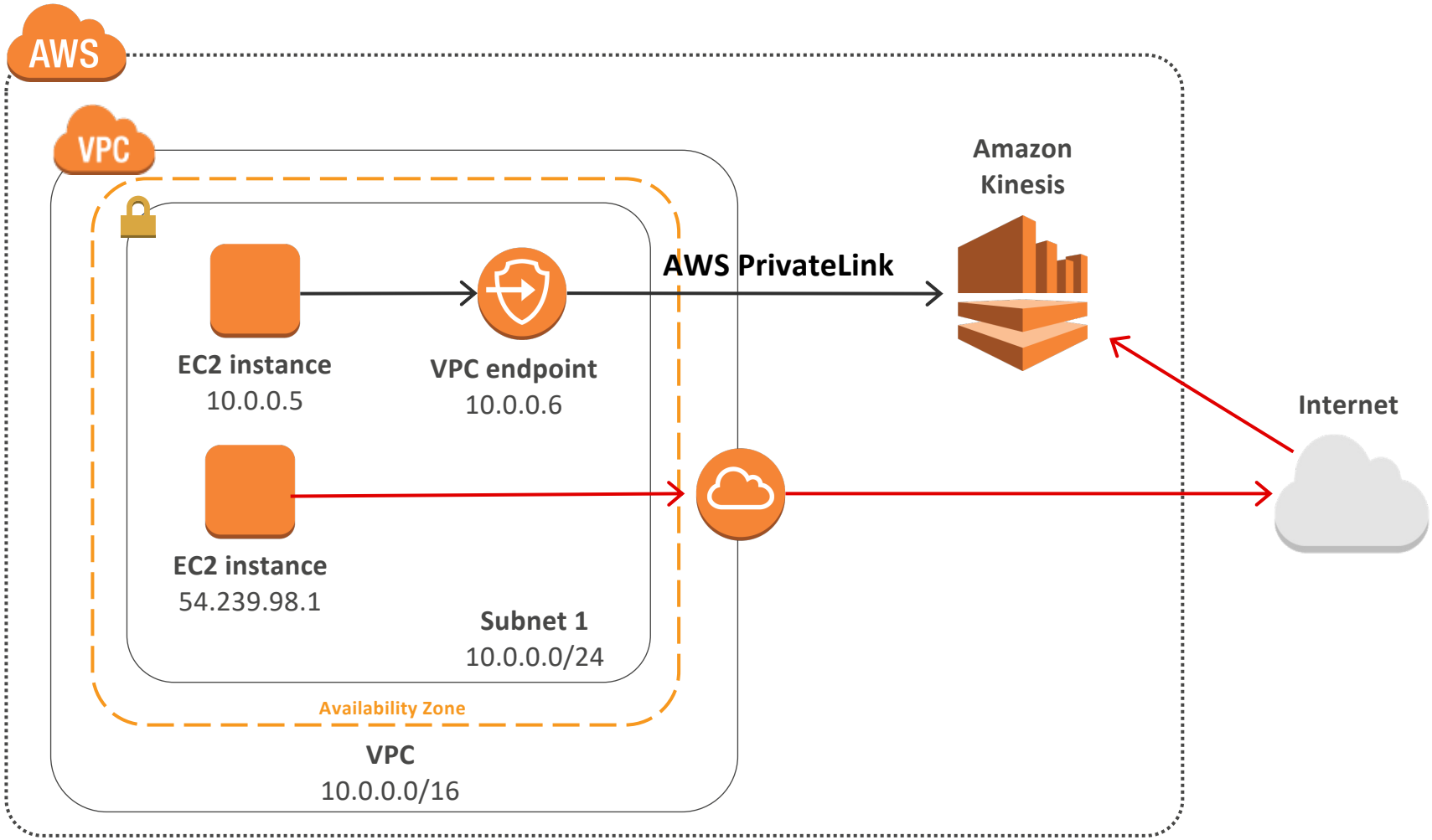
Amazon VPC


AWS
VPC
10.0.0.5
10.0.0.6
10.0.0.7
EC2 Instances
Subnet 1
10.0.0.0/24
Availability Zone A
10.0.1.5
10.0.1.6
10.0.1.7
EC2 Instances
Subnet 2
10.0.1.0/24
Availability Zone B
VPC 1
10.0.0.0/16
Region
Router
Virtual private gateway
VPN connection
Customer gateway
Corporate network
Custom route table
Destination
Target
10.0.0.0/16
local
0.0.0.0/0
vgw-id
Main route table
Destination
Target
10.0.0.0/16
local

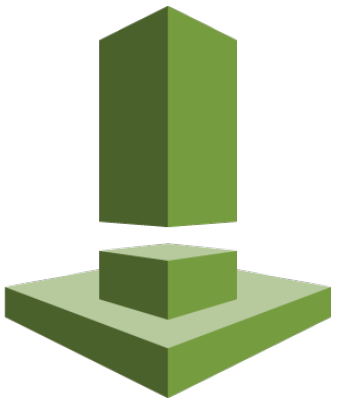
VPC - Defense in Depth



VPC - Private Link - Overview



Amazon Inspector Overview

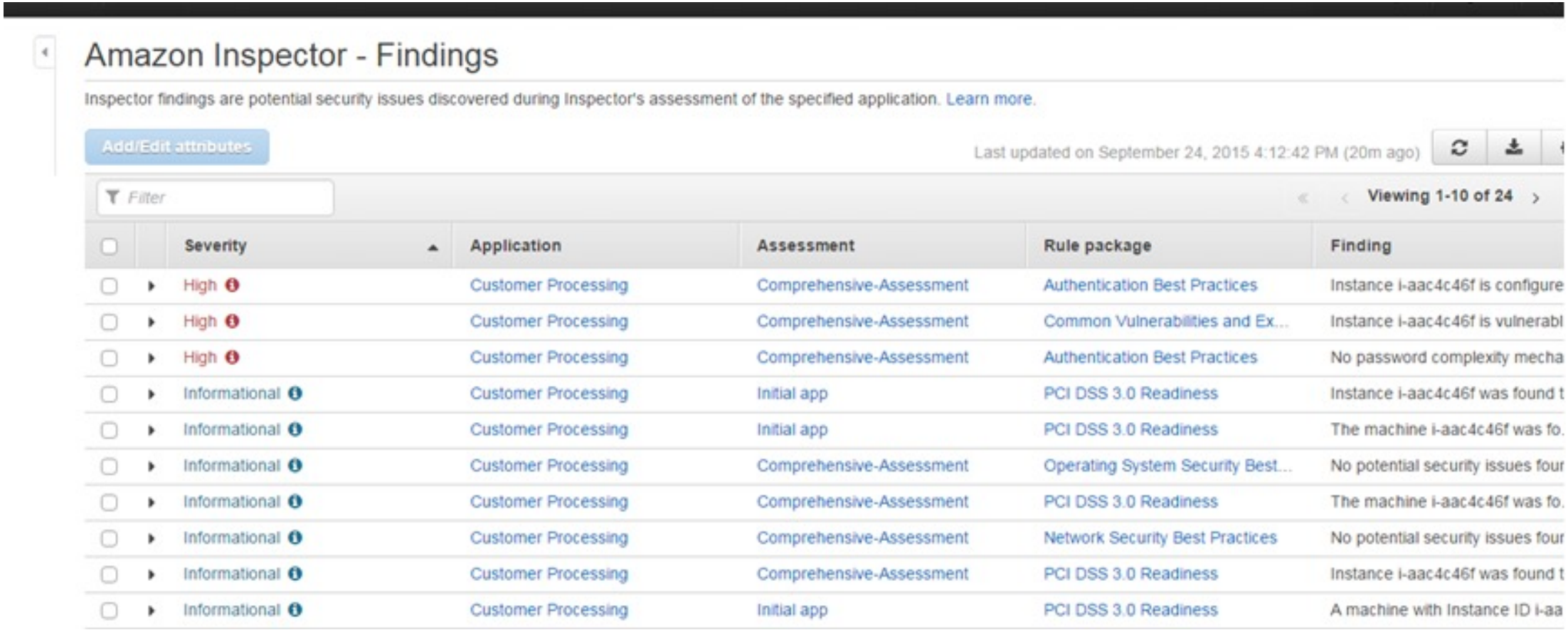


Amazon Inspector

Automated assessments that help improve security and compliance of applications

- Offers an agent-based solution
- Detects vulnerabilities
- Verifies security best practices
- Generates findings report
- Agent-less option available

Amazon Inspector - findings report



Amazon Inspector - Findings

Inspector findings are potential security issues discovered during Inspector's assessment of the specified application. Learn more.

Add/Edit attributes

Last updated on September 24, 2015 4:12:42 PM (20m ago)

Filter

Viewing 1-10 of 24

Severity	Application	Assessment	Rule package	Finding
High	Customer Processing	Comprehensive-Assessment	Authentication Best Practices	Instance i-aac4c46f is configure
High	Customer Processing	Comprehensive-Assessment	Common Vulnerabilities and Ex...	Instance i-aac4c46f is vulnerabl
High	Customer Processing	Comprehensive-Assessment	Authentication Best Practices	No password complexity mecha
Informational	Customer Processing	Initial app	PCI DSS 3.0 Readiness	Instance i-aac4c46f was found t
Informational	Customer Processing	Initial app	PCI DSS 3.0 Readiness	The machine i-aac4c46f was fo.
Informational	Customer Processing	Comprehensive-Assessment	Operating System Security Best...	No potential security issues four
Informational	Customer Processing	Comprehensive-Assessment	PCI DSS 3.0 Readiness	The machine i-aac4c46f was fo.
Informational	Customer Processing	Comprehensive-Assessment	Network Security Best Practices	No potential security issues four
Informational	Customer Processing	Comprehensive-Assessment	PCI DSS 3.0 Readiness	Instance i-aac4c46f was found t
Informational	Customer Processing	Initial app	PCI DSS 3.0 Readiness	A machine with Instance ID i-aa

AWS Shield - Overview

AWS Shield

Managed Distributed Denial of Service (DDoS) protection service

- Always-on detection
- Network and Transport layer protection
- Standard vs. Advanced
- Integration with Amazon Route 53, Amazon CloudFront, ELB

AWS Shield Standard vs Advanced

Features	Standard	Advanced
Always-on detection	✓	✓
Automatic inline mitigation	✓	✓
Layer 3 and 4 protection	✓	✓
Amazon CloudFront and Route 53 Protection	✓	✓
Amazon EC2 instance protection		✓
ELB protection		✓
24x7 DDoS Response Team		✓
Cost protection for DDoS spikes		✓
Access to real-time reports		✓

AWS Shield - Global Threat Dashboard

AWS WAF
Web ACLs
Rules

Conditions
Cross-site scripting
Geo match
IP addresses
Size constraints
SQL injection
String and regex matching

AWS Shield
Protected resources
Incidents
Global Threat Environment

Global Threat Environment

Following is a sample of the most significant attacks that AWS is monitoring and mitigating across its customers on Amazon CloudFront, Elastic Load Balancing, and Amazon Route 53.

Time period: Last Two Weeks

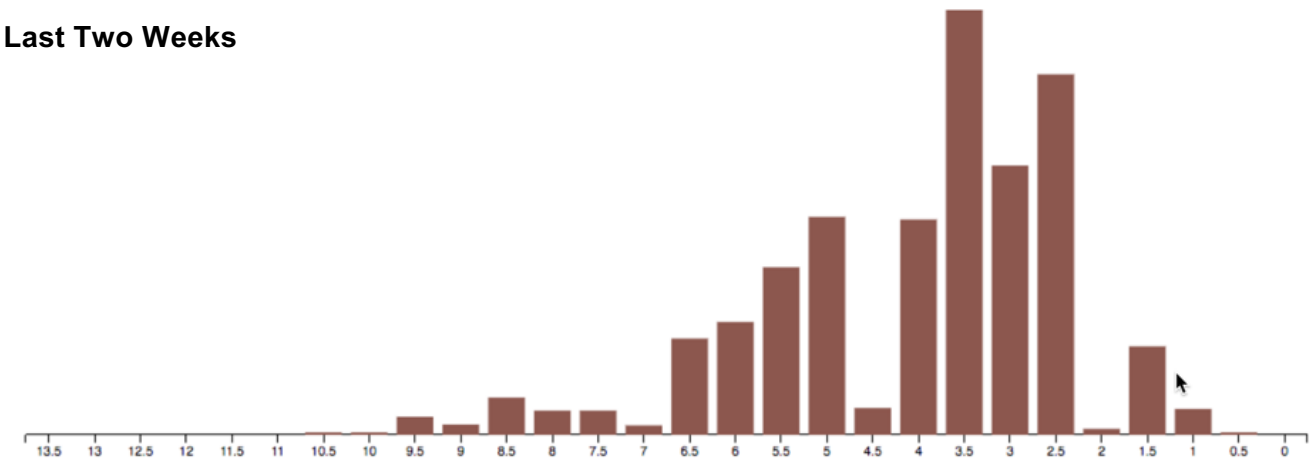
Last Two Weeks Summary

-- MBPS	**27** GBPS	**84** KRPS
Largest Packet Rate	Largest Bit Rate	Largest Request Rate

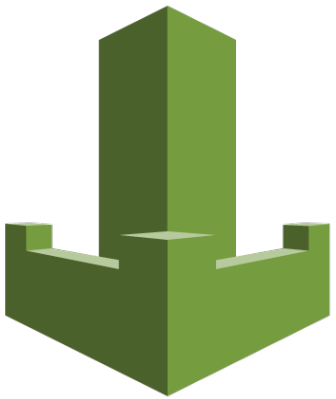
Most Common Vector: UDP_FRAGMENT

Threat Level: Normal

Attacks in Last Two Weeks



AWS WAF - Overview



AWS WAF

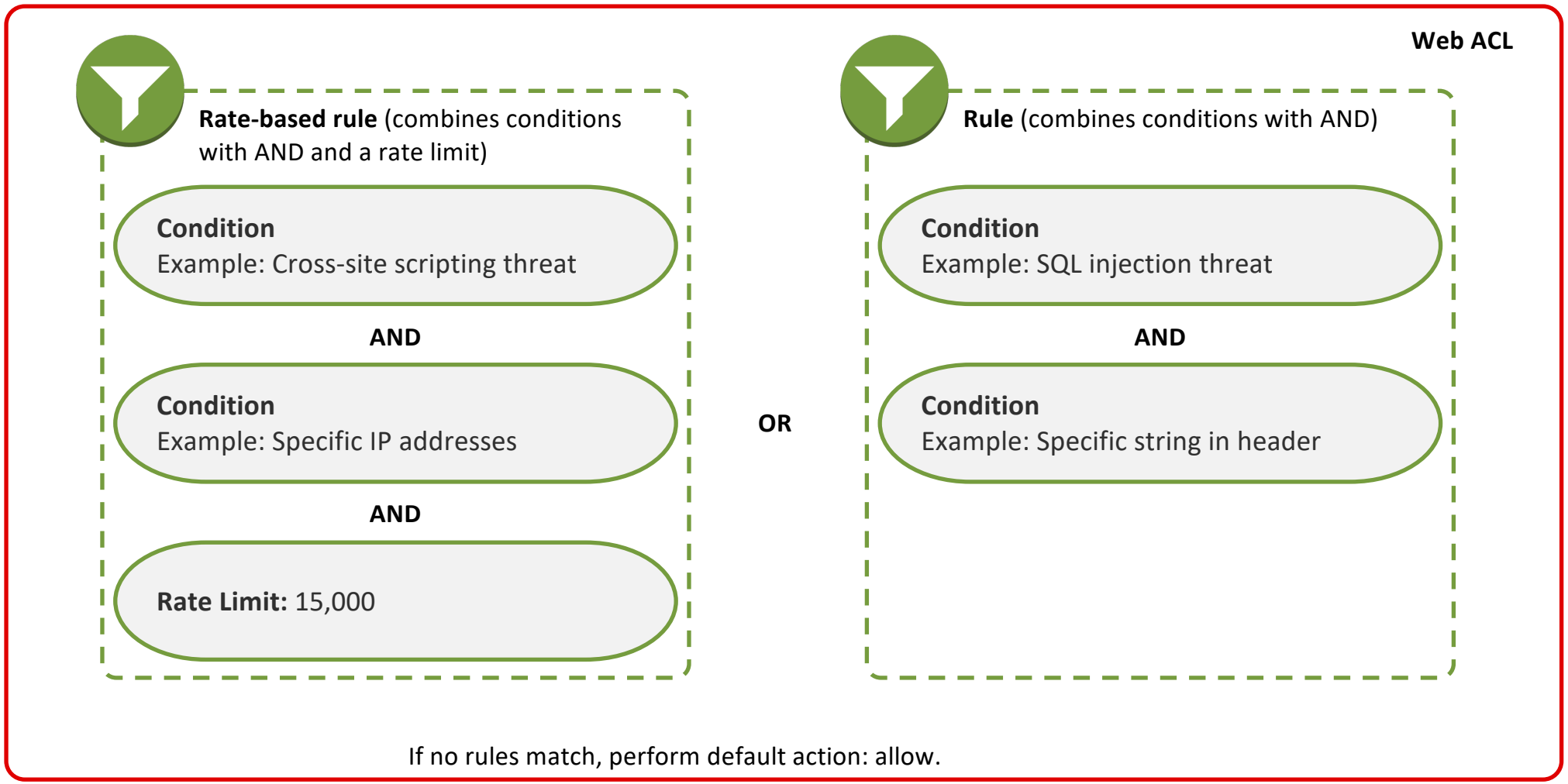
Helps detect and block malicious web requests targeted at your web applications

- Web traffic filtering
- Real-time metrics
- Application layer protection

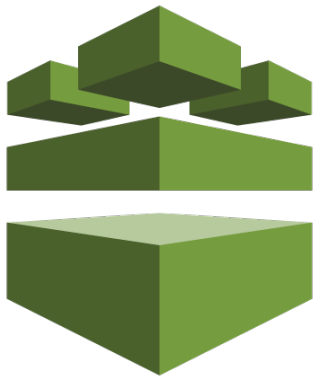
AWS WAF - Conditions

Condition	Allow or Block Requests Based On…
Cross-site scripting match	Whether the requests appear to contain malicious scripts
IP match	The IP addresses that they originate from
Geographic match	The country that they originate from
Size constraint	Whether the requests exceed a specified length
SQL injection match	Whether the requests appear to contain malicious SQL code
String match	Strings that appear in the requests
Regex match	A regex pattern that appears in the requests

Web ACLs and Rules



AWS Config - Overview



AWS Config

Managed service that provides resource inventory, configuration history, and change notifications

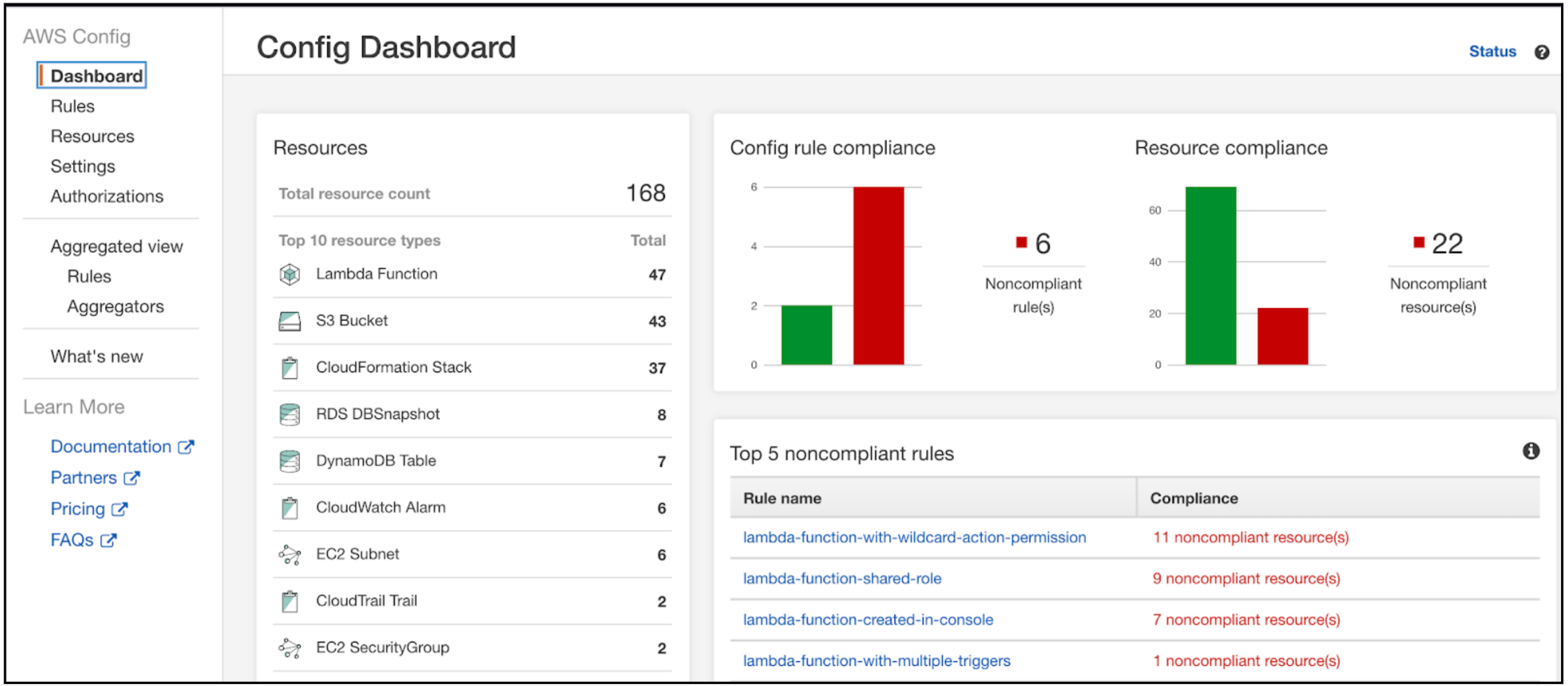
- Continuously captures details on all configuration changes associated with your resources
- Enables compliance monitoring and security analysis
- Sends notifications when changes occur

AWS Config Features

Allows you to answer the following questions regarding your resources:

- *Is everything safe?*
  - Retrieve the configuration of your AWS resources
- *What has changed?*
  - Retrieve historical configuration and receive resource change notifications
- *What will this change affect?*
  - View relationships between your resources
- *What resources exist?*
  - Get a snapshot of your current AWS configuration

AWS Config Rules Implementation

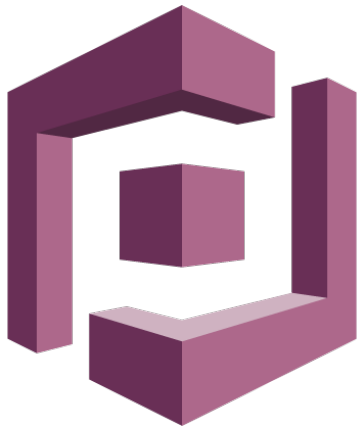


XPEPPERS
A Claranet Group Company

aws partner network
Training Partner

claranet

Amazon Cognito

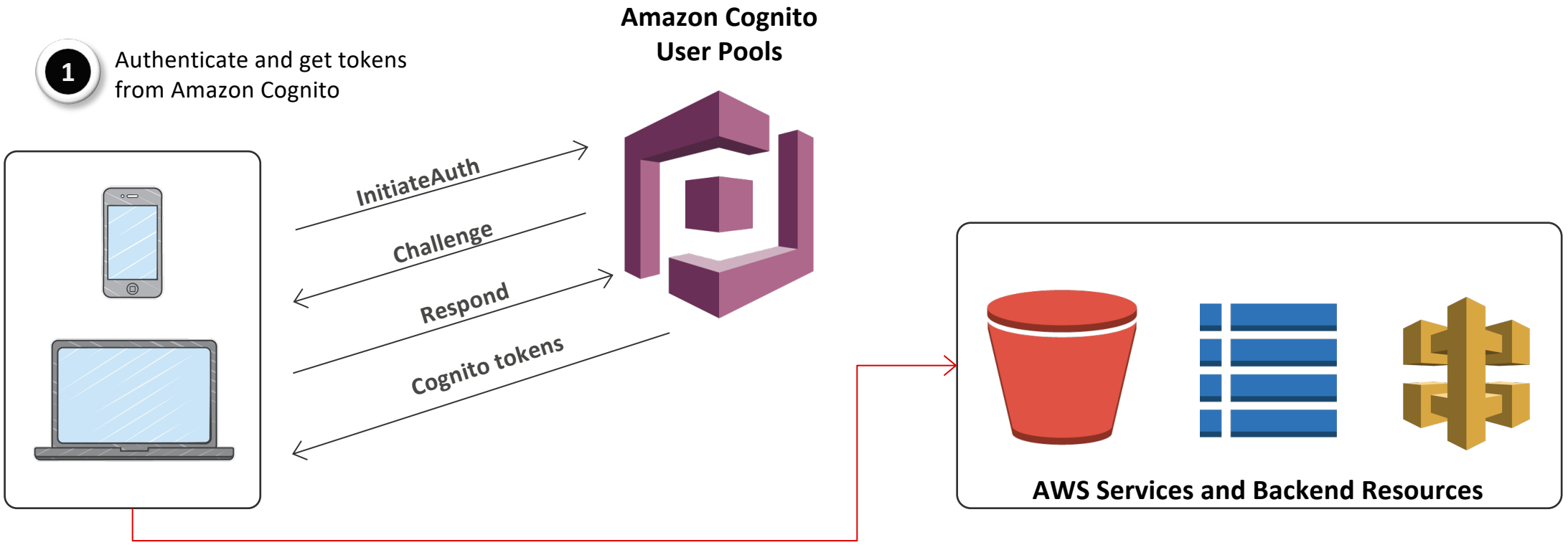


Amazon Cognito

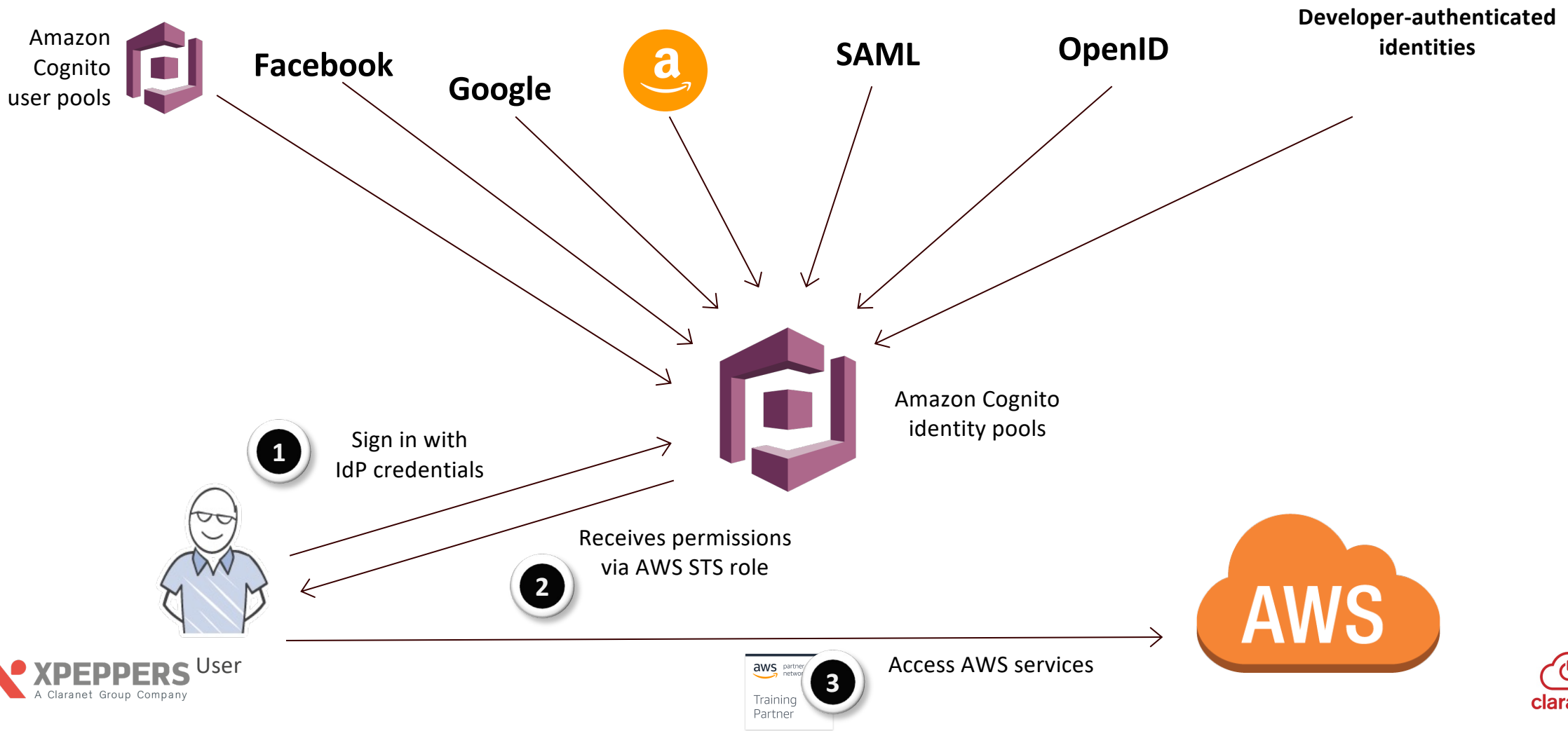
A fully managed solution providing access control and authentication for web/mobile apps

- Supports MFA
- Data at-rest and in-transit encryption
- Log in via social identity providers
- Support for SAML

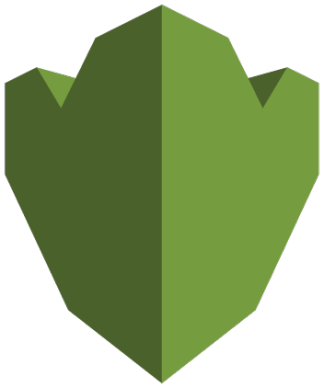
Amazon Cognito - User Pools



Amazon Cognito - Identity Pools



AWS KMS - Overview

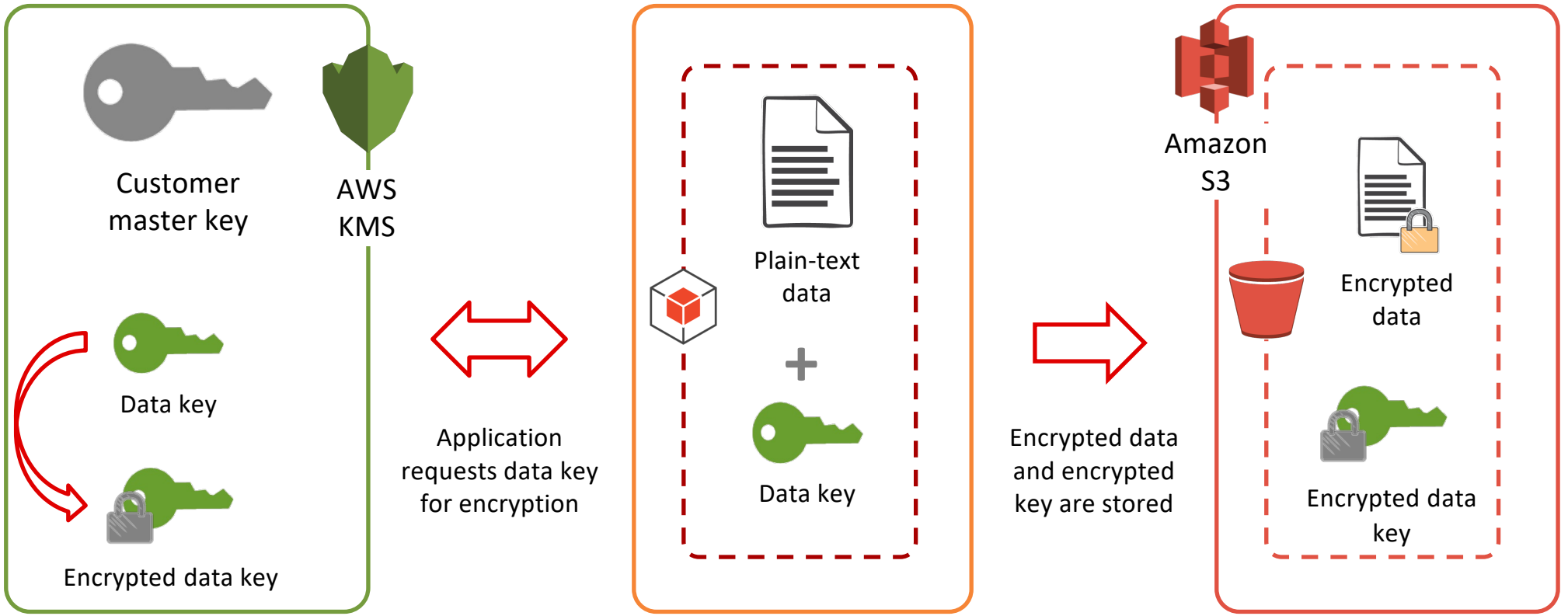


AWS Key Management Service

Managed encryption service that provides key storage and management, and data encryption

- Two-tiered key hierarchy using envelope encryption
- Centrally manage and secure keys
- Determine who can use keys with usage policies

AWS KMS - Envelope Encryption



Amazon Guarduty - Overview

Amazon GuardDuty

Intelligent threat detection and continuous monitoring to protect AWS accounts and workloads

- Identifies suspected attackers through integrated threat intelligence feeds
- Uses machine learning to detect anomalies in account and workload activity

Amazon Guarduty - Getting Started

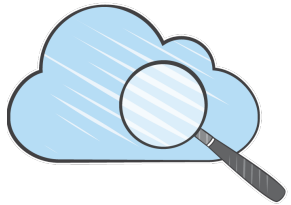
Enable Guarduty


CloudTrail Events

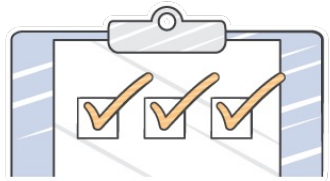

VPC Flow Logs


DNS Logs

Continuously Analyze

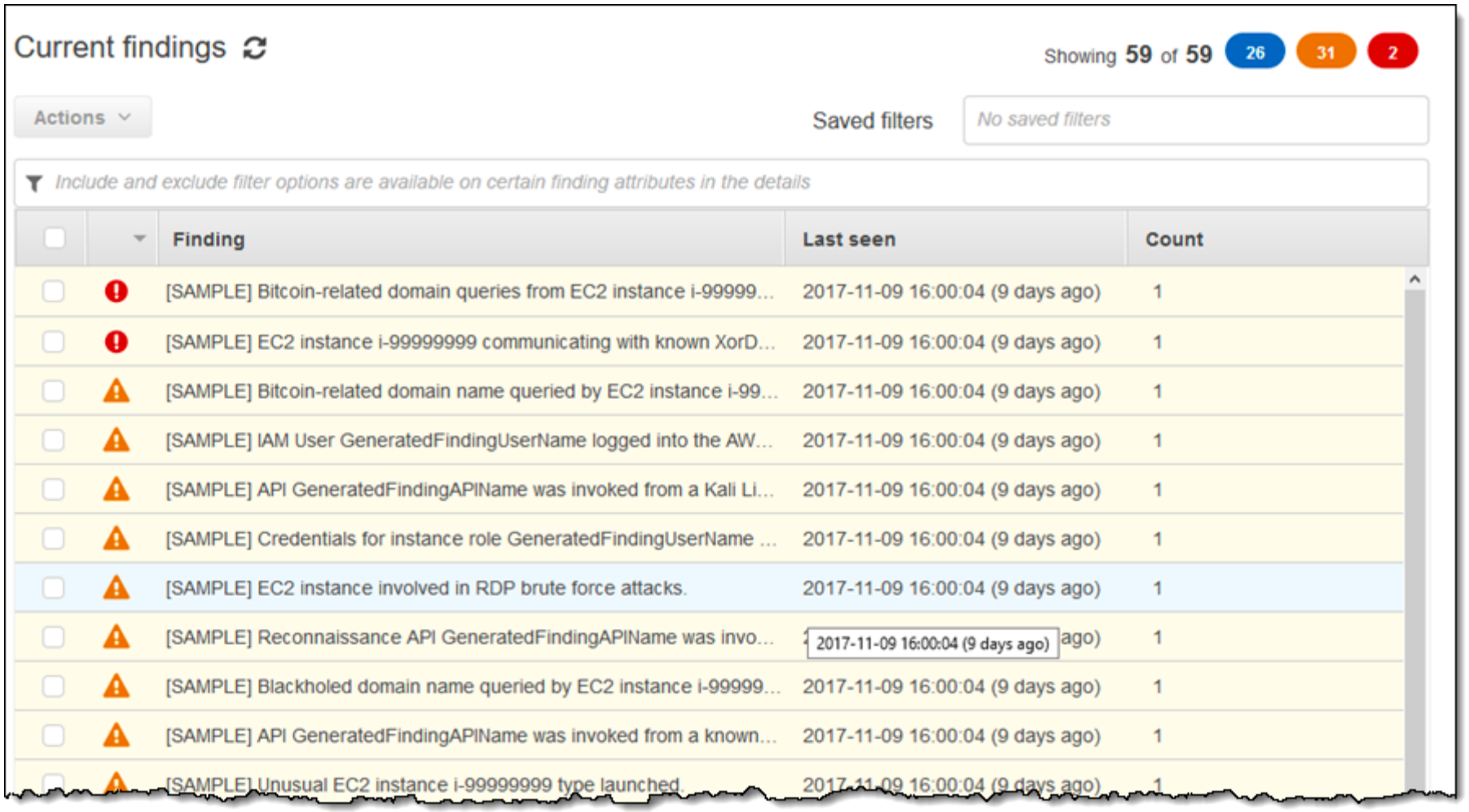


Intelligently Detect Threats

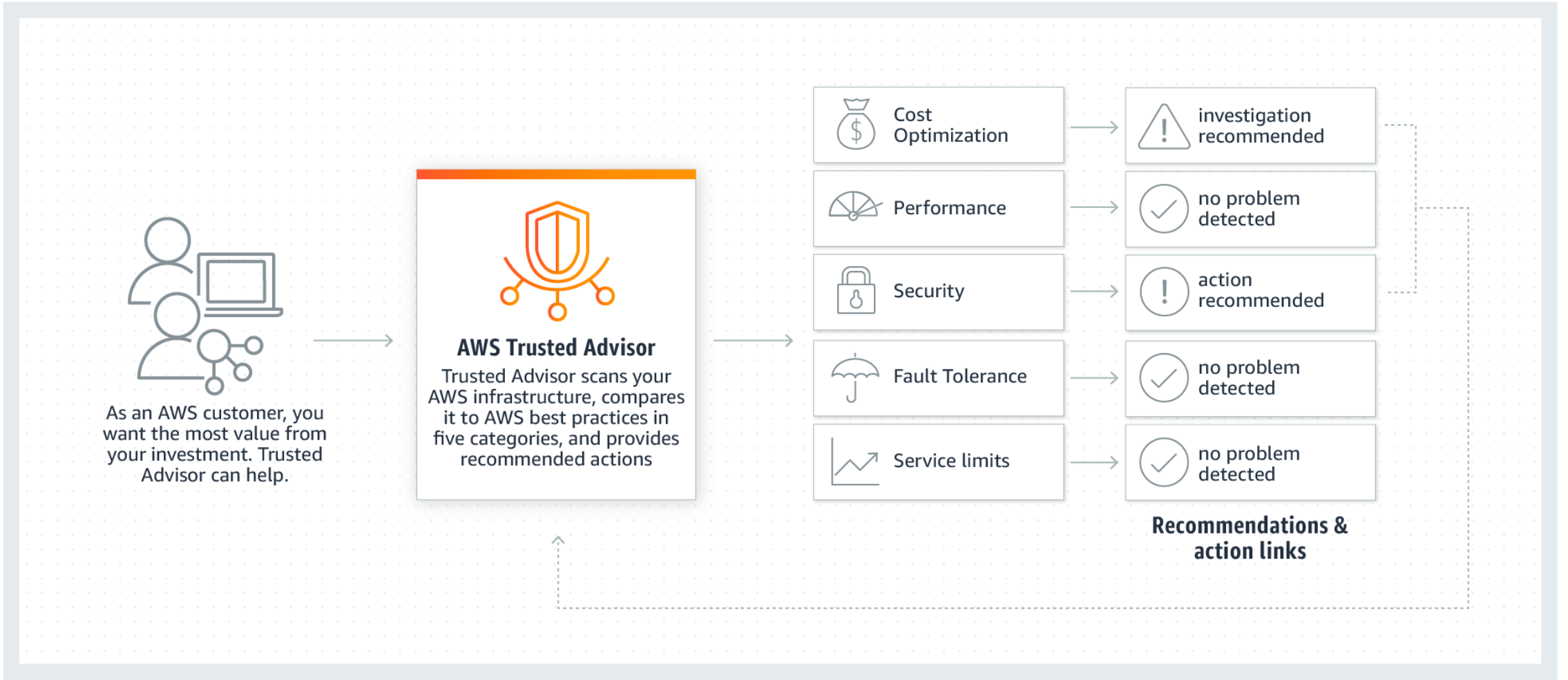


Take Action with Detailed Findings

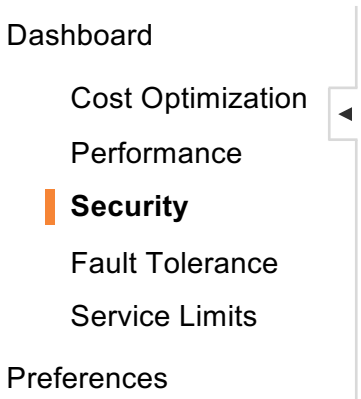
Amazon Guarduty - Findings



AWS Trusted Advisor - Overview



AWS Trusted Advisor - Dashboard



Security

1 1 1

Security Checks

Security Groups – Specific Ports Unrestricted *Updated 8/28/18 3:21 PM*

Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.

1 of 1 security group rules allows unrestricted access to a specific port.

MFA on Account Root *Updated 8/28/18 3:21 PM*

Checks the root account and warns if multi-factor authentication (MFA) is not enabled.

Yellow: MFA is not enabled on the root account.

Recommended Action

Log in to your root account and activate an MFA device. See **Checking MFA Status** and **Setting Up an MFA Device**.

IAM Use *Updated 8/28/18 3:21 PM*

Checks for your use of AWS Identity and Access Management (IAM).

At least one IAM user, group, or role has been created for this account.

Compliance

Global

CSA Cloud Security Alliance Controls

ISO 9001 Global Quality Standard

ISO 27001 Security Management Controls

ISO 27017 Cloud Specific Controls

ISO 27018 Personal Data Protection

PCI DSS Level 1 Payment Card Standards

SOC 1 Audit Controls Report

SOC 2 Security, Availability, & Confidentiality Report

SOC 3 General Controls Report

United States

CJIS Criminal Justice Information Services

DoD SRG DoD Data Processing

FedRAMP Government Data Standards

FERPA Educational Privacy Act

FFIEC Financial Institutions Regulation

FIPS Government Security Standards

FISMA Federal Information Security Management

GxP Quality Guidelines and Regulations

HIPAA Protected Health Information

ITAR International Arms Regulations

MPAA Protected Media Content

NIST National Institute of Standards and Technology

SEC Rule 17a-4(f) Financial Data Standards

VPAT / Section 508 Accessibility Standards

Asia Pacific

FISC [Japan] Financial Industry Information Systems

IRAP [Australia] Australian Security Standards

K-ISMS [Korea] Korean Information Security

MTCS Tier 3 [Singapore] Multi-Tier Cloud Security Standard

My Number Act [Japan] Personal Information Protection

Europe

C5 [Germany] Operational Security Attestation

Cyber Essentials Plus [UK] Cyber Threat Protection

ENS High [Spain] Spanish Government Standards

G-Cloud [UK] UK Government Standards

IT-Grundschutz [Germany] Baseline Protection Methodology

PCI Security Standards Council PARTICIPATING ORGANIZATION™

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations ™

ISO 27001 International Organization for Standardization

XPEPPERS A Claranet Group Company

aws partner network Training Partner

claranet

Guess What This Is!

Guess What This Is!

Quiz – Security on AWS

https://quizizz.com/join/

Code:

paolo.latella@it.clara.net
@LatellaPaolo