



Los Angeles Learning Days

Security is top priority

Kain Leo

Solutions Architect – SLG / EDU

Introduction

Security at AWS is
“**Job Zero**” by which we
mean it’s even more
important than any
number one priority.



Why is Security so difficult?



**Lack of
visibility**



**Low degree
of automation**

Before...

Move fast  OR Stay secure

Now...

Move fast  Stay secure

AWS Layered Security Services



AWS security, identity, and compliance solutions



Identity and access management

AWS Identity and Access Management (IAM)

AWS IAM Identity Center (successor to AWS SSO)

AWS Organizations

AWS Directory Service

Amazon Cognito

AWS Resource Access Manager



Detective controls

AWS Security Hub

Amazon GuardDuty

Amazon Inspector

Amazon CloudWatch

AWS Config

AWS CloudTrail

VPC Flow Logs

AWS IoT Device Defender



Infrastructure protection

AWS Firewall Manager

AWS Network Firewall

AWS Shield

AWS WAF

Amazon VPC

AWS PrivateLink

AWS Systems Manager



Data protection

Amazon Macie

AWS Key Management Service (KMS)

AWS CloudHSM

AWS Certificate Manager

AWS Secrets Manager

AWS VPN

Server-Side Encryption



Incident response

Amazon Detective

Amazon EventBridge

AWS Backup

AWS Security Hub

AWS Elastic Disaster Recovery



Compliance

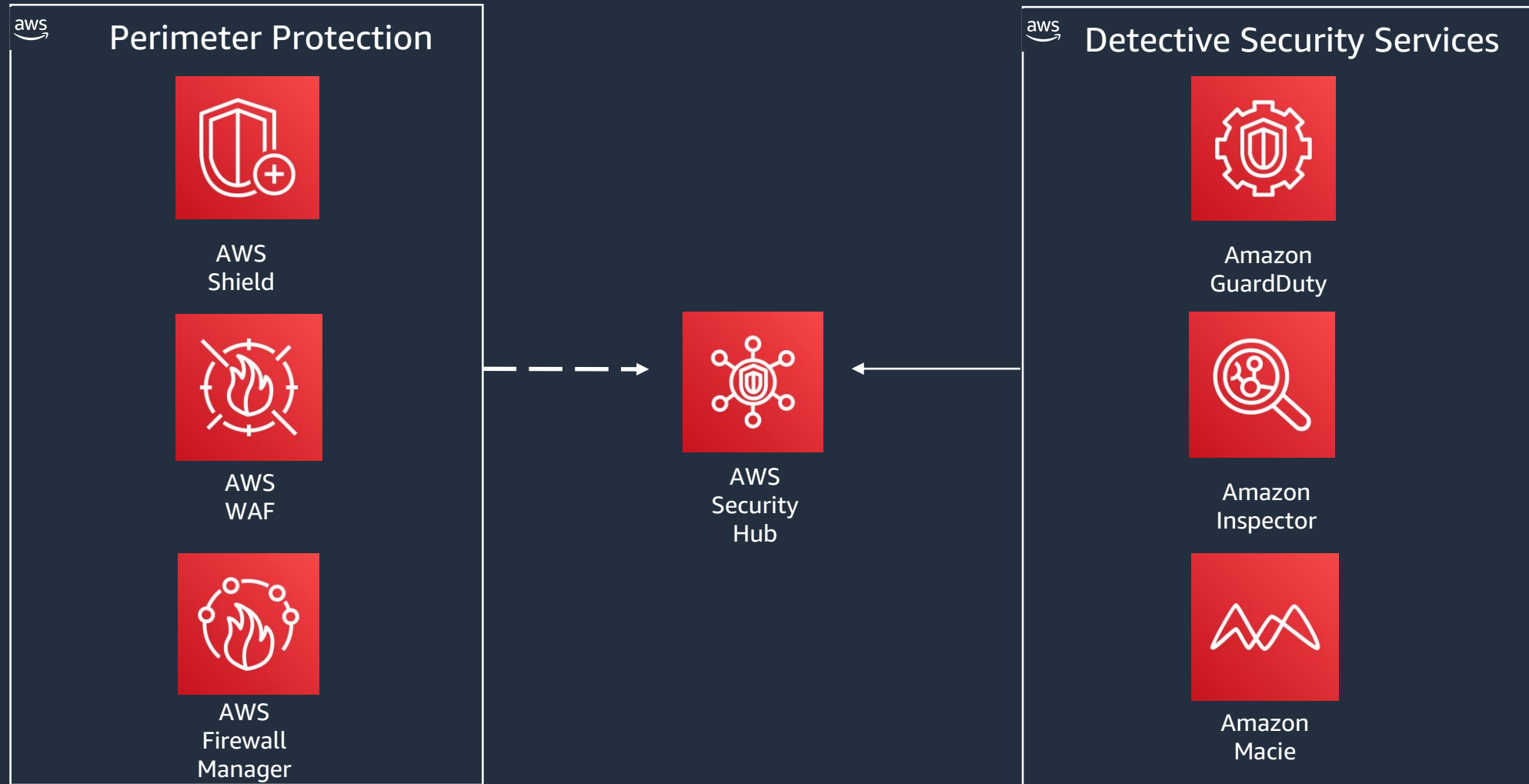
AWS Artifact

AWS Audit Manager

AWS foundational and layered security services



Layered Security Services



Amazon GuardDuty

Detective Security Services

How does Amazon GuardDuty work?

Easy One-Click Activation without
Architectural or Performance Impact



How does Amazon GuardDuty work?

No Agents, No Sensors, No Network Appliances



How does Amazon GuardDuty work?



Amazon GuardDuty

Threat Detection Types

Bitcoin Mining



Instance Compromise



Account Compromise



Total of 47 detections



Data Sources



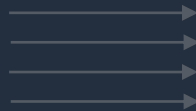
VPC flow logs



DNS Logs



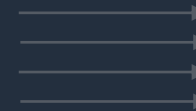
CloudTrail Events



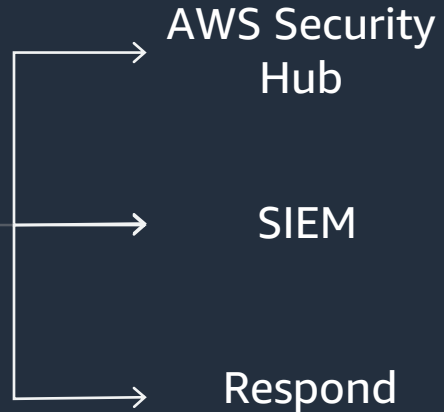
Threat intelligence



Anomaly Detection (ML)



Findings



Automate with integrated services

Automated threat remediation

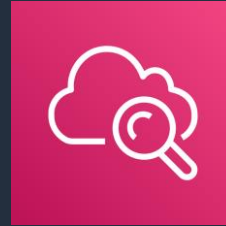
GuardDuty
Finding



Amazon
GuardDuty



CloudWatch
Event



Amazon
CloudWatch



Lambda



AWS Lambda

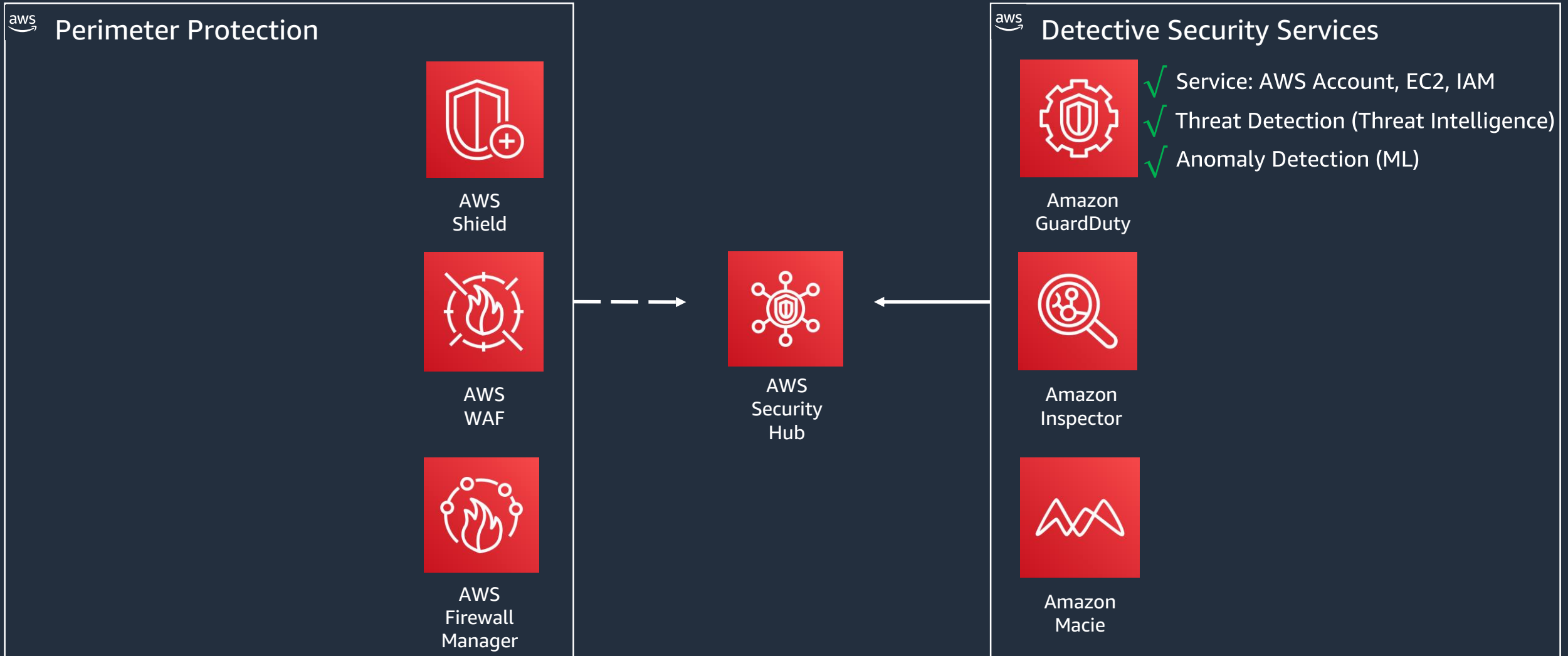


Event (time-base)



Lambda
function

Layered Security Services



Amazon Inspector

Detective Security Services

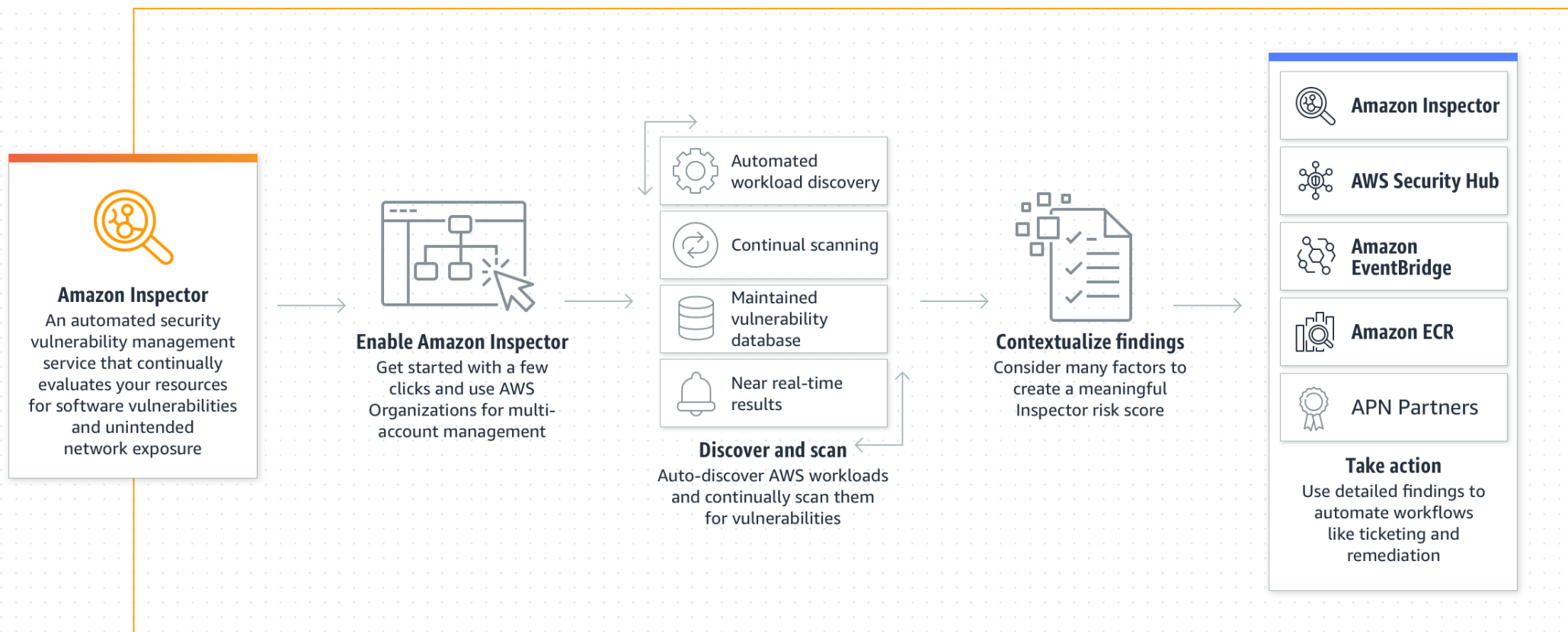


Amazon Inspector

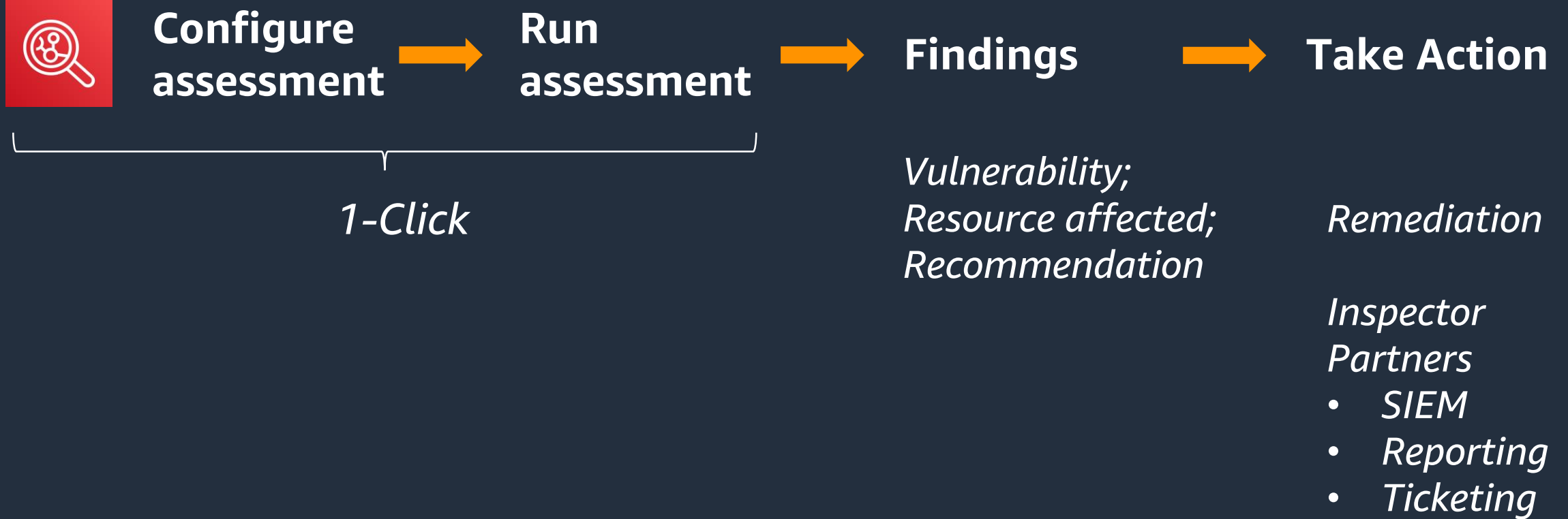
Automated security assessment service to help improve the security and compliance of applications deployed on AWS



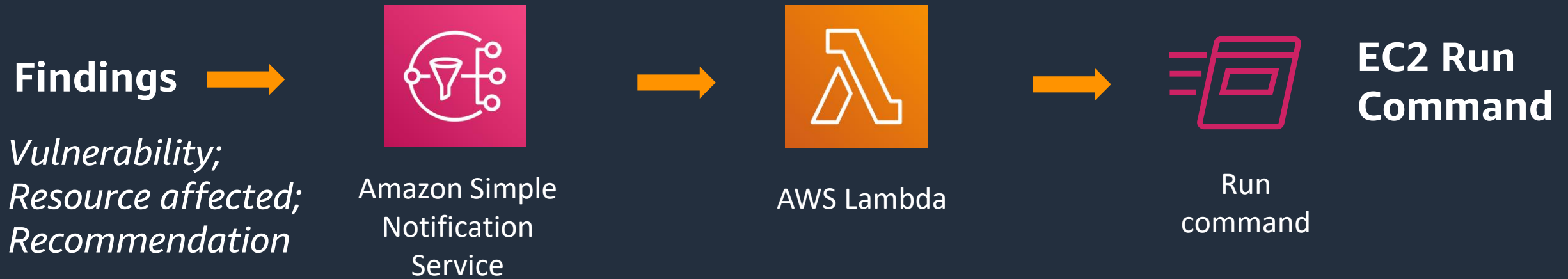
Amazon Inspector – How it works



How to use Amazon Inspector?



Automate use of findings



Network Reachability – key features

- Validate and fix your AWS Networking configuration



Avoid complexity
and impact of
scanners



Shows all open paths
(Internet, VPN, etc.)



Actionable
insights

How does it work?

Amazon Inspector analyzes AWS network configuration to find what is reachable?

List of resources analyzed:

- Security Groups
- VPCs
- Network interfaces
- Subnets
- Network ACLs
- Route tables
- Elastic load balancers
- Application load balancers
- Internet gateways
- Virtual private gateways
- Direct Connect
- VPC peering connections

Amazon Inspector

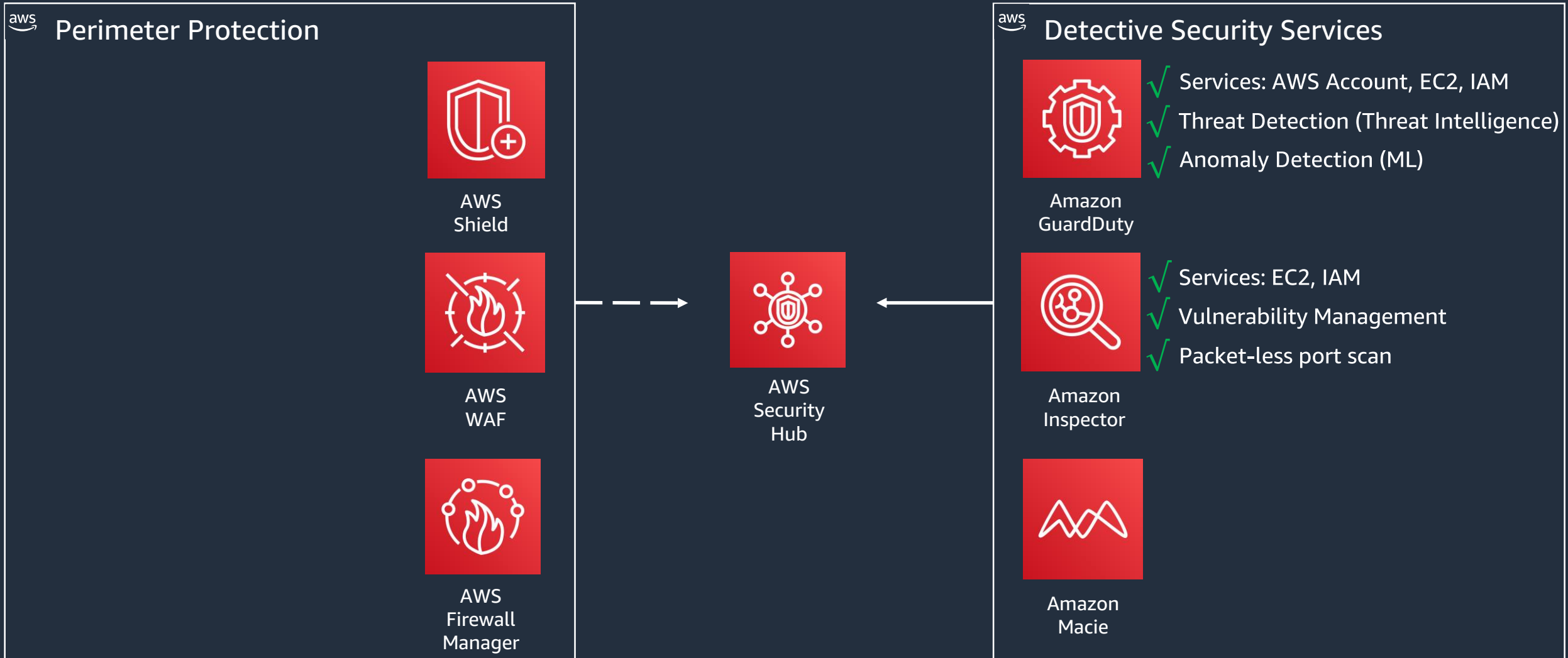
EC2 Host assessment

Amazon Inspector can assess:

- Vulnerabilities in software (CVE)
- Host hardening guidelines (CIS Benchmark)
- AWS Security best practices.



Layered Security Services



Amazon Macie

Detective Security Services

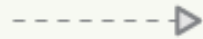


How does Amazon Macie work?

HOW MACIE WORKS



Enroll your AWS Account
with Amazon Macie



Select the Buckets for
Content Discovery and
Classification

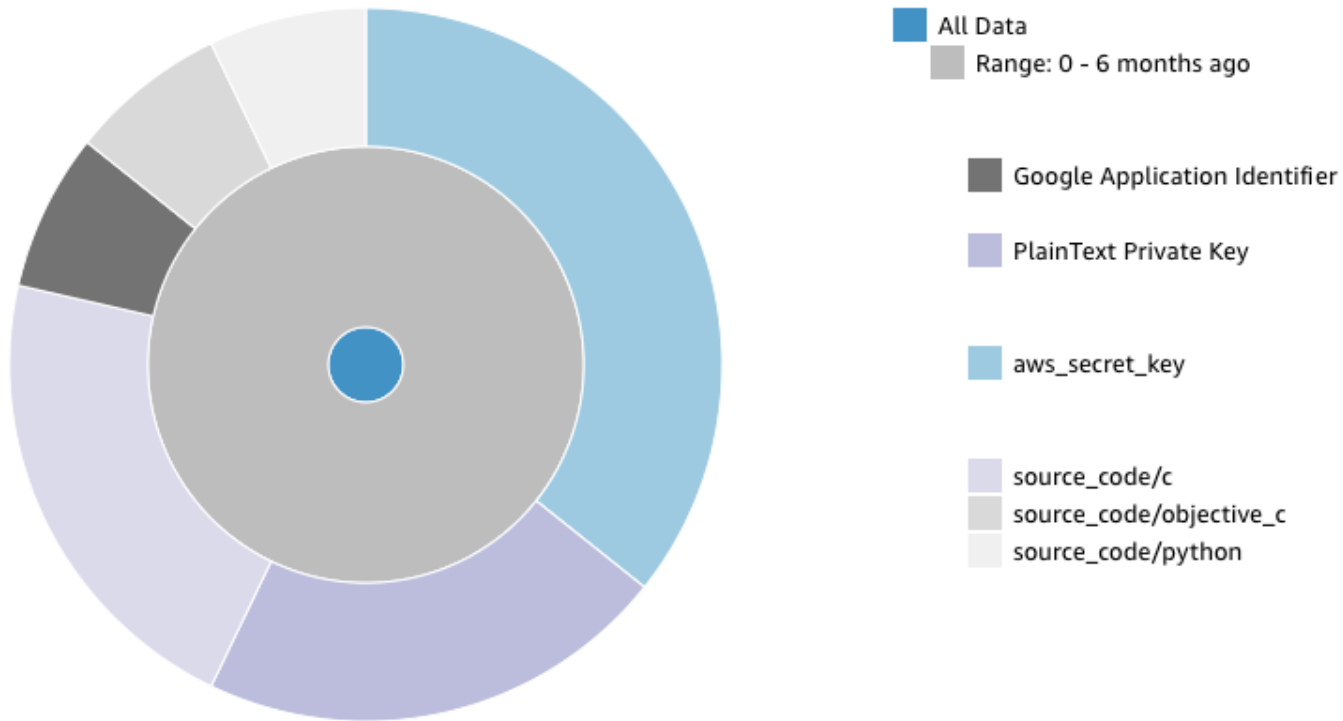


Review your Alerts in the
Amazon Macie
Dashboard

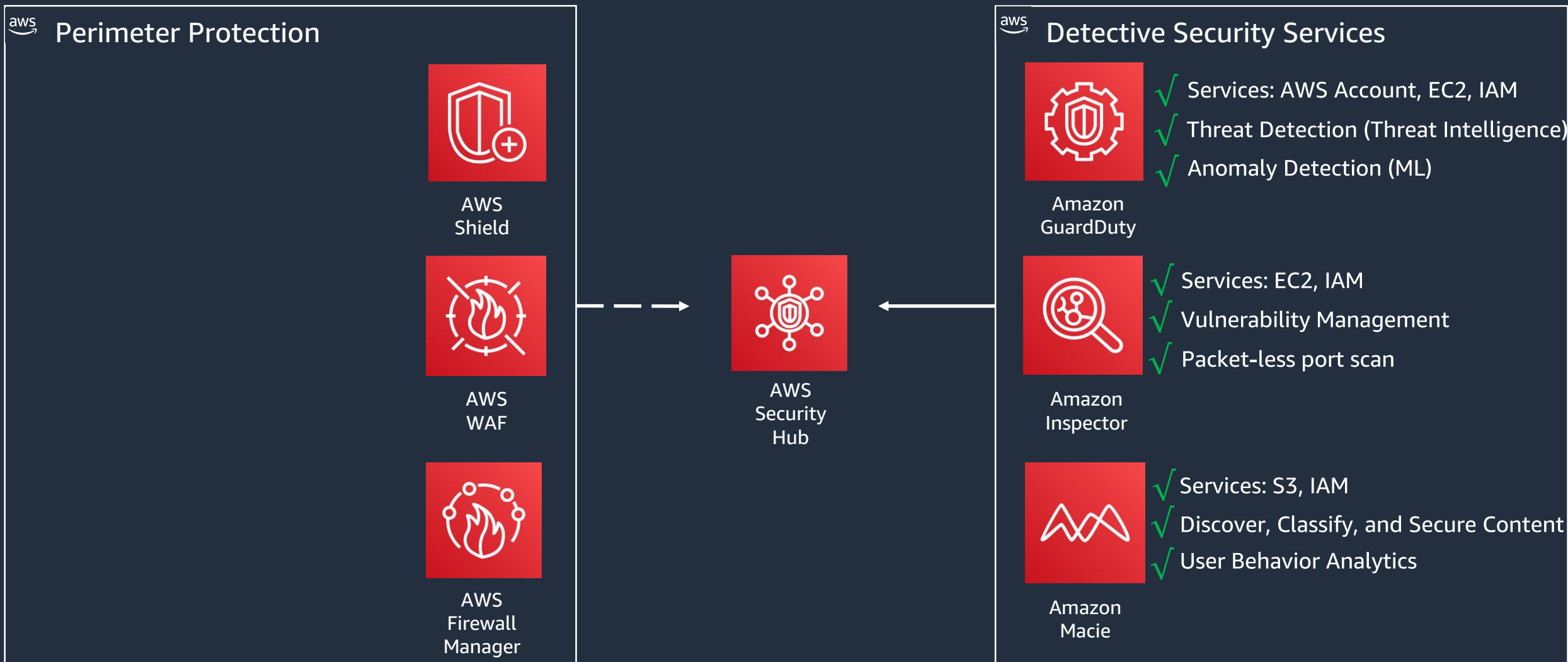
How does Macie work?

S3 objects for selected time range - minRisk: (10)

The following graph shows S3 objects grouped into top 20 matching themes for the selected time range. To further investigate your S3 objects, double-click sections of the graph or color chart. [Learn more](#)



Layered Security Services

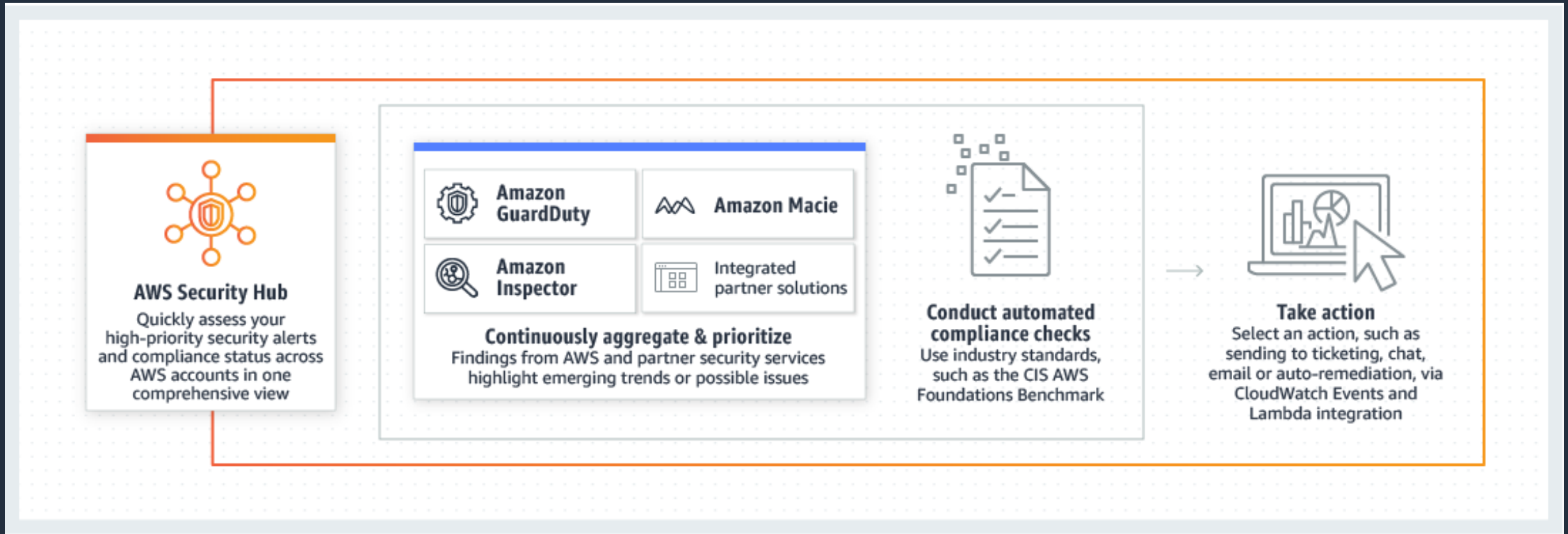


AWS Security Hub

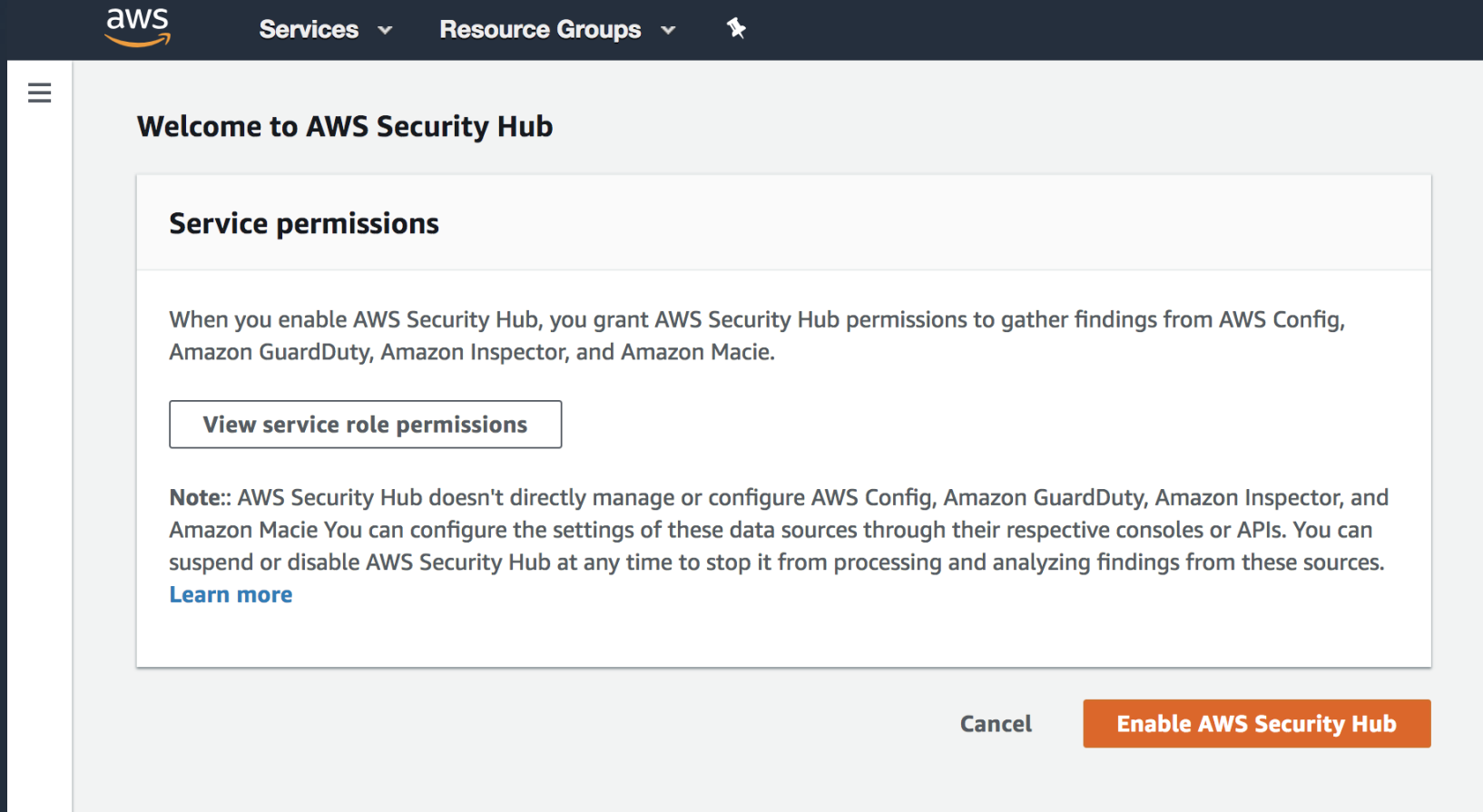
Cloud Security Posture Management




How does AWS Security Hub work?



Getting Started - AWS Security Hub work?



AWS Security Hub – Partner Integrations



Services

Resource Groups

SecurityHubDemo/shillomie-Ise...

Oregon

Support

AWS Security Hub × (preview)


Summary

Standards

Insights

Findings

Settings



awsmarketplace

Amazon: GuardDuty


A threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads.

Default Insights

0

Links

[Purchase](#) [Configure](#)



Your account is subscribed

Amazon: Inspector


An automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

Default Insights

0

Links

[Purchase](#) [Configure](#)



Your account is subscribed

Amazon: Macie


A security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS.

Default Insights

0

Links

[Purchase](#) [Configure](#)



Your account is subscribed

ARMOR: Armor Anywhere


Armor Anywhere delivers managed security and compliance for AWS.

Default Insights

0

Links

[Purchase](#) [Configure](#)



Your account is subscribed

Alert Logic: SIEMless ThreatManagement


Get the right level of coverage: Vulnerability and asset visibility, threat detection and incident management, WAF, and assigned SOC analyst options.

Default Insights

0

Links

[Purchase](#) [Configure](#)



Your account is subscribed

Barracuda Networks: Cloud Security Guardian


Barracuda Cloud Security Sentry helps organizations stay secure while building applications in, and moving workloads to, the public cloud.

Default Insights

0

Links


[Configure](#)



Your account is subscribed


Check Point: CloudGuard IaaS

Check Point CloudGuard easily extends comprehensive threat prevention security to AWS while protecting assets in the cloud.




Check Point: Dome9 Arc


A SaaS Platform that delivers verifiable cloud network security, advanced IAM protection and comprehensive compliance and governance.



CrowdStrike: CrowdStrike Falcon


CrowdStrike Falcon's single lightweight sensor unifies next-gen antivirus, endpoint detection and response, and 24/7 managed hunting, via the cloud.





© 2019

AWS Security Hub – Insights

 Services ▾ Resource Groups ▾ ⌵

SecurityHubDemo/shllomie-Ise... ▾ Oregon ▾ Support ▾

AWS Security Hub ×
(preview)

Summary

Standards

Insights

Findings

Settings


Security Hub > Insights

Insights (54)
An insight is a collection of related security findings defined by an aggregation statement and optional filters.

[Create insight](#)


< 1 2 3 >

0. What products are sending findings? (custom insight)




24 current result

1. AWS resources with the most findings




100+ current result

2. S3 buckets with public write or read permissions




1 current result

3. AMIs that are generating the most findings




21 current result

4. EC2 instances involved in known Tactics, Techniques, and Procedures (TTPs)




0 current result

5. AWS users with the most suspicious activity




23 current result

6. AWS resources instances that don't meet security standards / best practices




21 current result

7. AWS resources associated with potential data exfiltration




0 current result

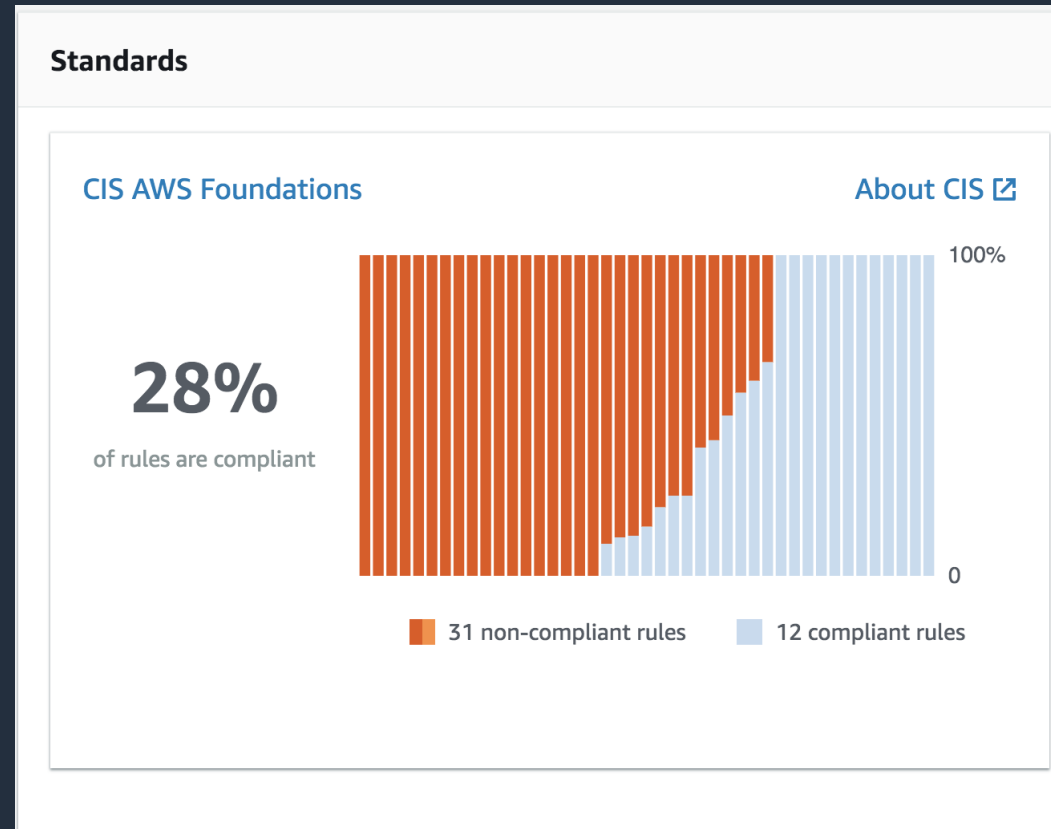
8. AWS resources associated with unauthorized resource consumption



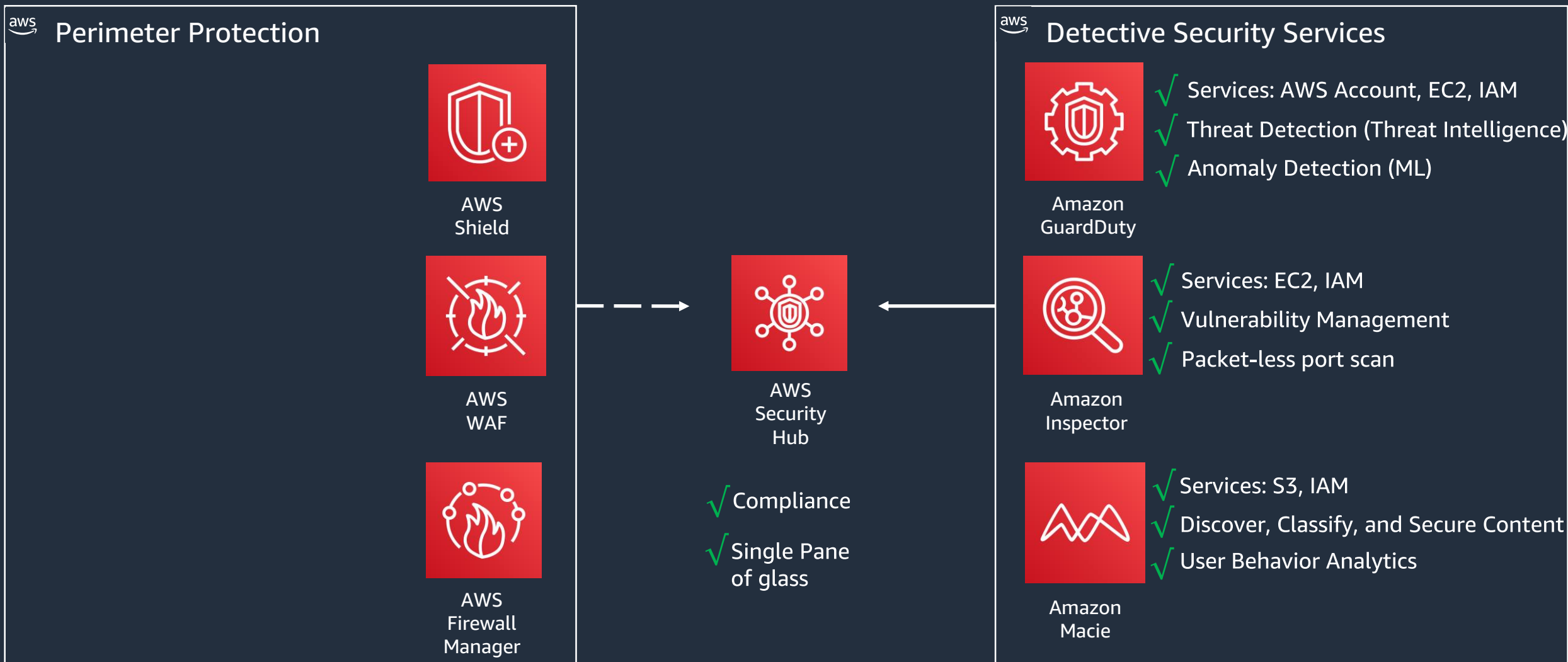
23 current result

 © 2024, Amazon Web Services, Inc. or its affiliates.

AWS Security Hub – Compliance Checks (CIS)



Layered Security Services



Perimeter Protection



AWS Shield Advanced Perimeter Protection

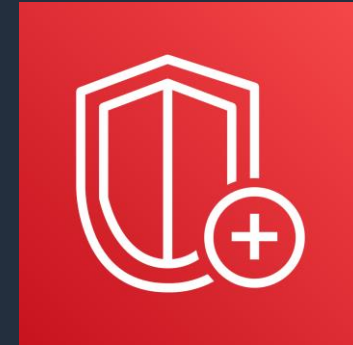


AWS Shield

A Managed DDoS Protection Service

There are two tiers of AWS Shield:

- AWS Shield Standard
- AWS Shield **Advanced**

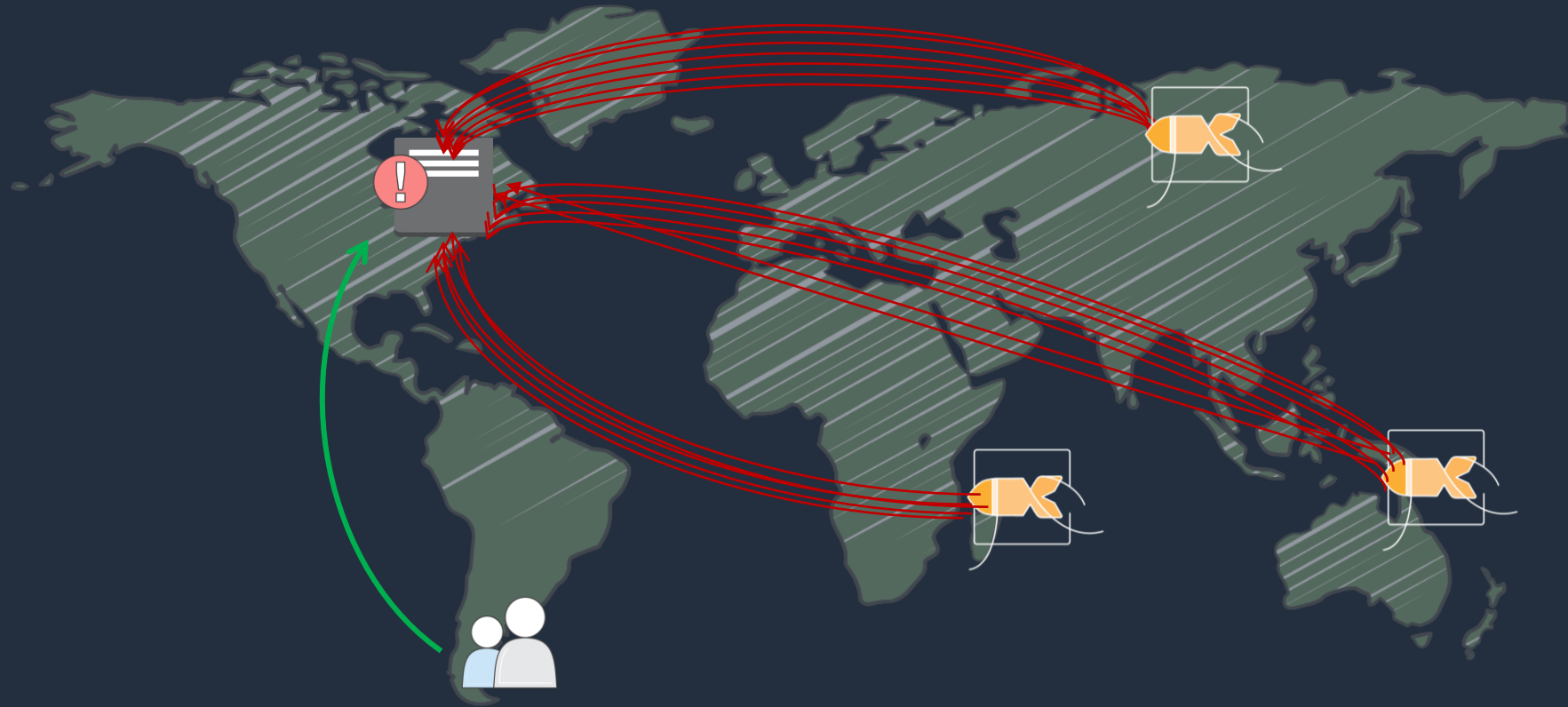


AWS Shield



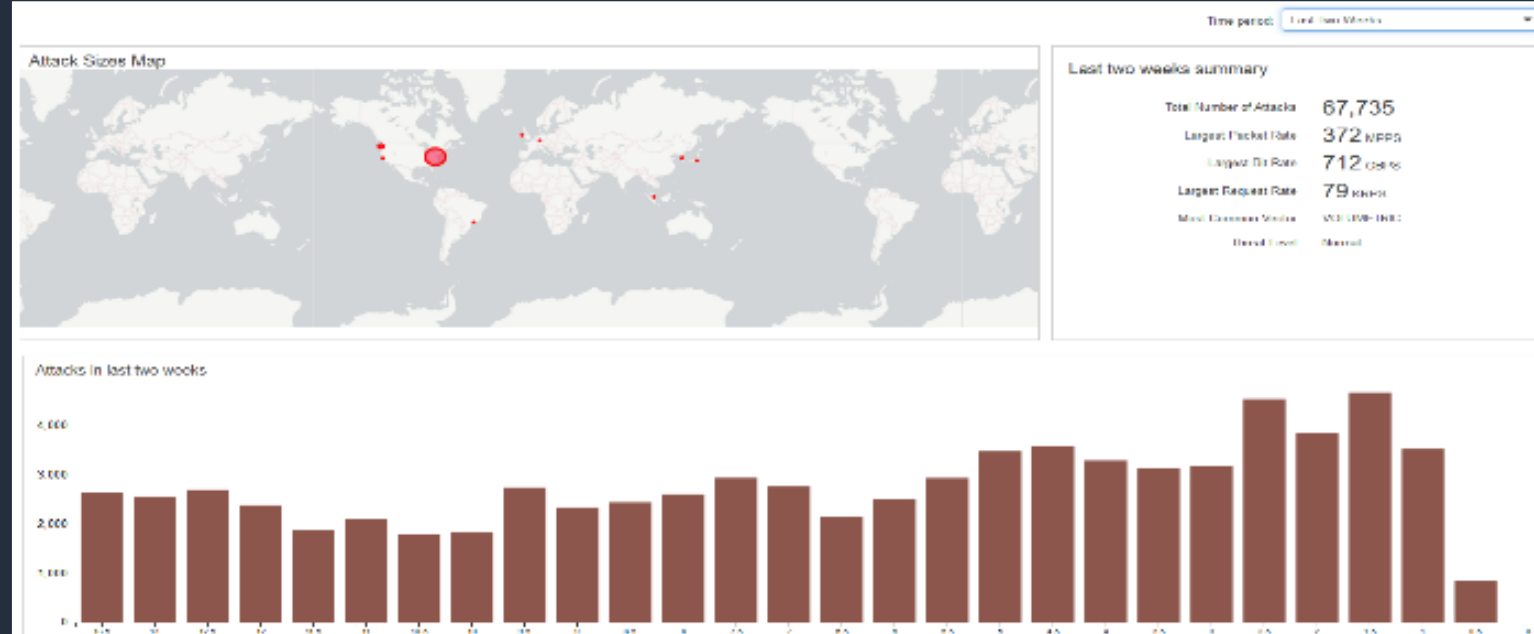
AWS Shield Advanced - DDoS Attack threats and Trends:

Network / Transport Layer DDoS



DDoS Threats and Trends

AWS Shield detects and mitigates **1,000's of DDoS Attacks Daily**



Source: AWS Global Threat Dashboard (Available for **AWS Shield Advanced** customers)

AWS Shield Standard

DDoS
Expertise

Built-in DDoS
Protection for
Everyone

AWS Shield Standard & Advanced

DDoS Expertise

Built-in DDoS
Protection for
Everyone

Enhanced
Protection

24x7 access to
DDoS Response
Team (DRT)

Visibility & Compliance

CloudWatch Metrics

Attack
Diagnostics

Global threat
environment
dashboard

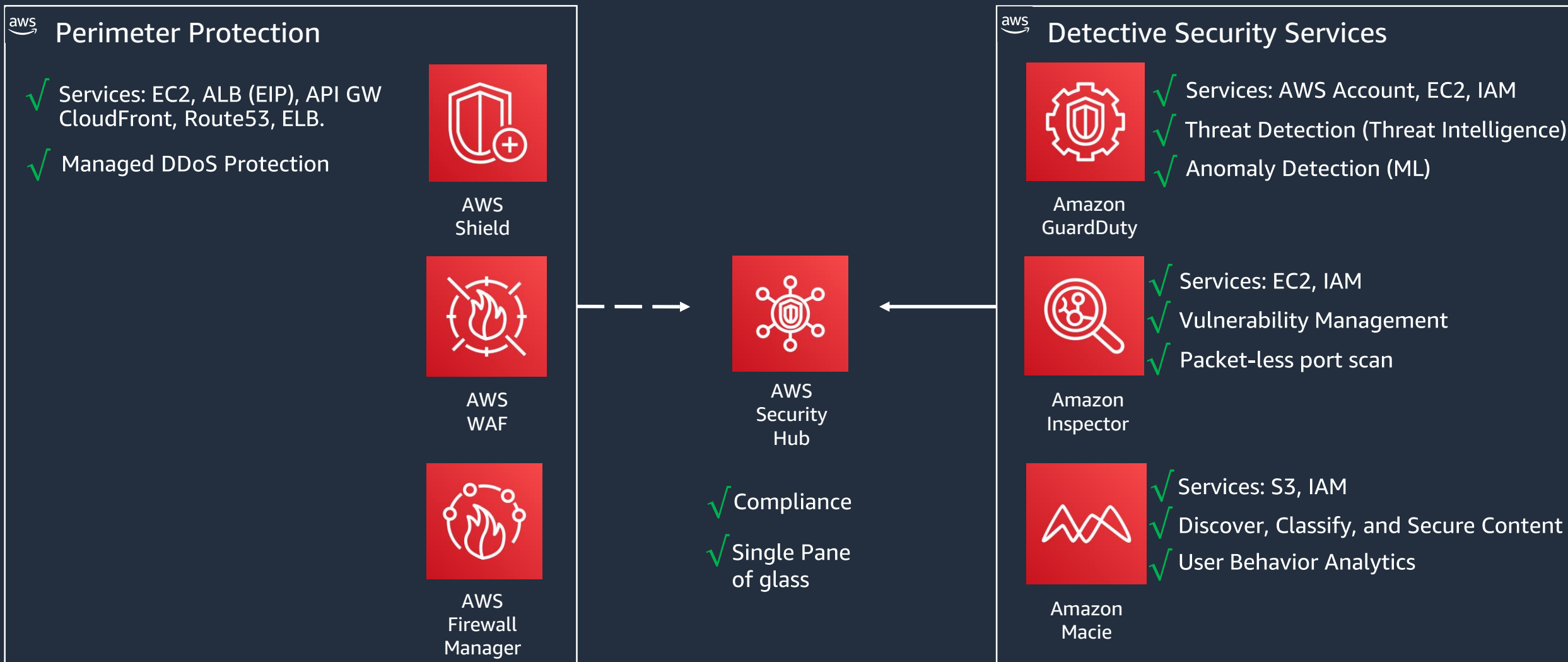
Economic Benefits

AWS WAF at no
additional cost
for protected resources

AWS Firewall
Manager
at no additional cost

Cost Protection for
scaling

Layered Security Services



AWS WAF

Perimeter Protection



Protecting Your Applications Using AWS WAF



Application Vulnerabilities



HTTP Flood



Bots & Scrapers

AWS Web Application Firewall (WAF): Popular deployment modes



1. Custom
Rules



2. Managed Rules



3. Security
Automation

*Or use any combination of the
above ...*



Managed Rules for AWS WAF - Web Application Firewall

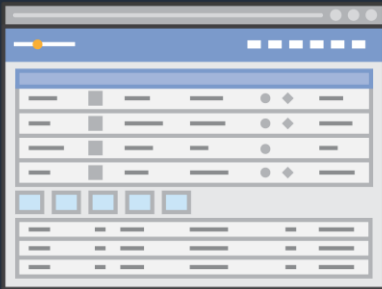
Protect Your Web Application with Pre-configured Rules on AWS WAF

Managed Rules for AWS Web Application Firewall (WAF) are a set of rules written, curated and managed by AWS Marketplace Sellers that can be easily deployed in front of your web applications running on AWS Application Load Balancers or Amazon CloudFront. With these managed rules, you can quickly get started and protect your web application or APIs against common threats like the [OWASP Top 10 security](#) risks, threats specific to Content Management Systems (CMS) like WordPress or Joomla, or even emerging Common Vulnerabilities and Exposures (CVE) without having to manage infrastructure. AWS security sellers will automatically update the managed rules for you as new vulnerabilities and bad actors emerge. Managed Rules for AWS WAF are designed to help you spend less time writing firewall rules and more time building applications.

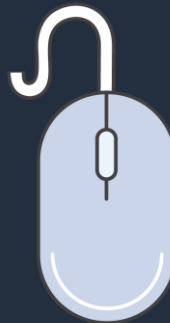


Get Started With AWS WAF

AWS Web Application Firewall (WAF): Deploy in 3 easy steps



Find rules on
AWS WAF console or
AWS marketplace

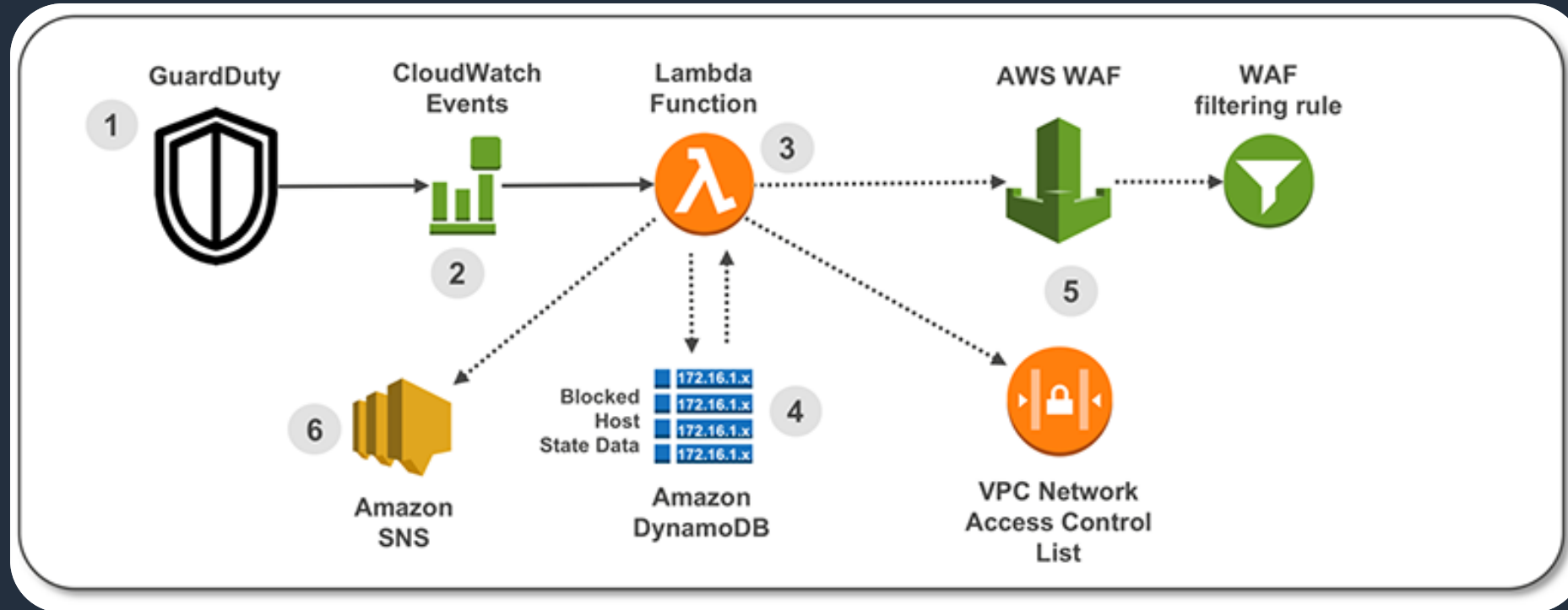


Click and
subscribe

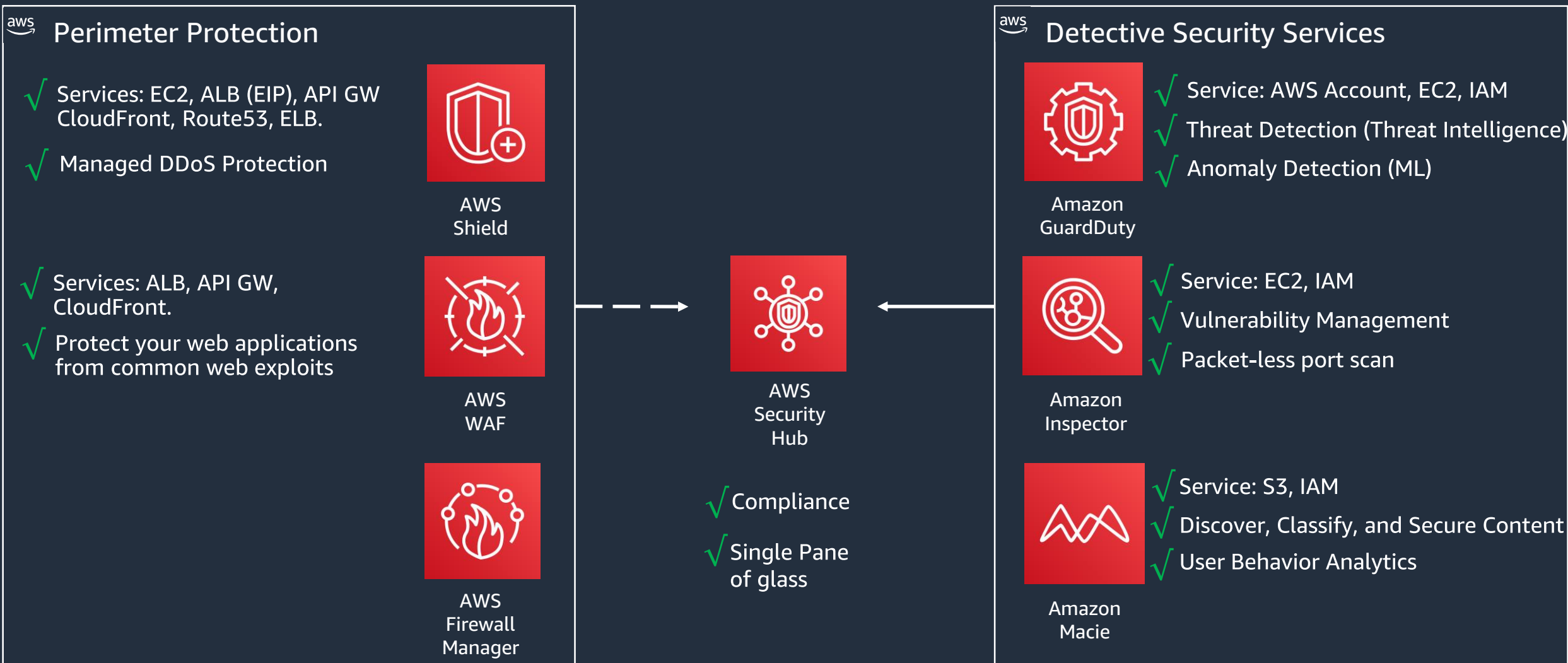


Associate rules in
AWS WAF

Automatic block of suspicious hosts using Amazon GuardDuty and AWS WAF.



Layered Security Services



AWS Firewall Manager

Perimeter Protection

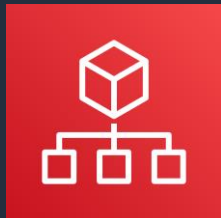


AWS Firewall Manager Key Benefits

Simplified Management of WAF Rules

Integrated with AWS Organizations

Centrally managed global rules, and Account-specific rules



Ensure Compliance to WAF Rules

Ensure entire Organization adheres to mandatory set of rules

Apply protection even when new Accounts or resources are created

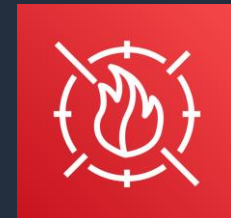


Central Visibility Across Organization

Central visibility of WAF threats across Organization

Compliance Dashboard for audit **firewall** status

An organization's InfoSec team learns and operates WAF instead of each Account owner



AWS Firewall Manager Key Benefits

Enable Rapid Response to Internet Attacks at scale

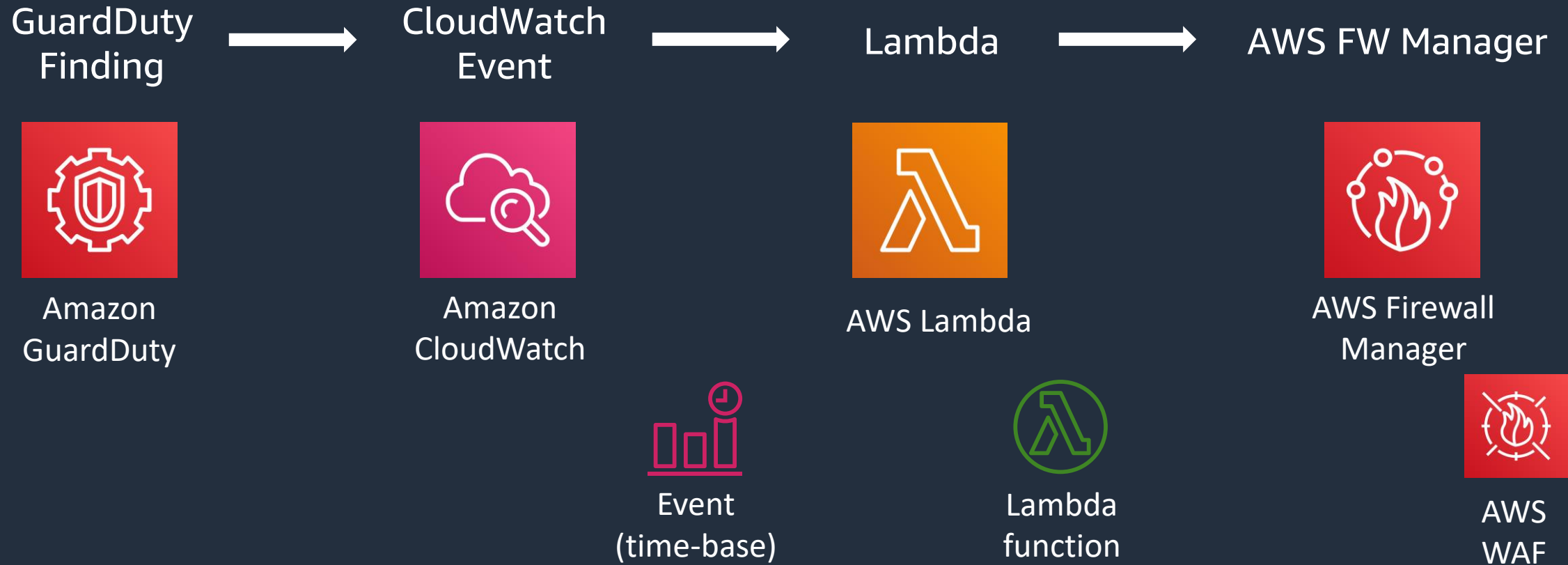
Security administrators have a single console to receive real-time threats, and respond within minutes

Quickly apply *CVE Patches* across all applications in your Organization, or ***block malicious IP addresses detected by GuardDuty*** across entire Organization



Automate with integrated services

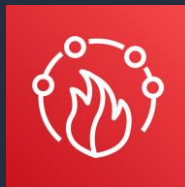
Automated threat remediation



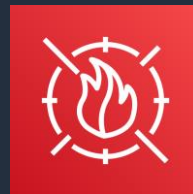
Typical Use Cases

Deploy OWASP rules for PCI compliance

- PCI DSS 3.0 Requirement 6 suggests customers deploy a WAF, with rules like OWASP top 10
- Subscribe to [Managed Rules from AWS Marketplace](#)
- Ensure the OWASP rule is [applied across all PCI-tagged resources](#)

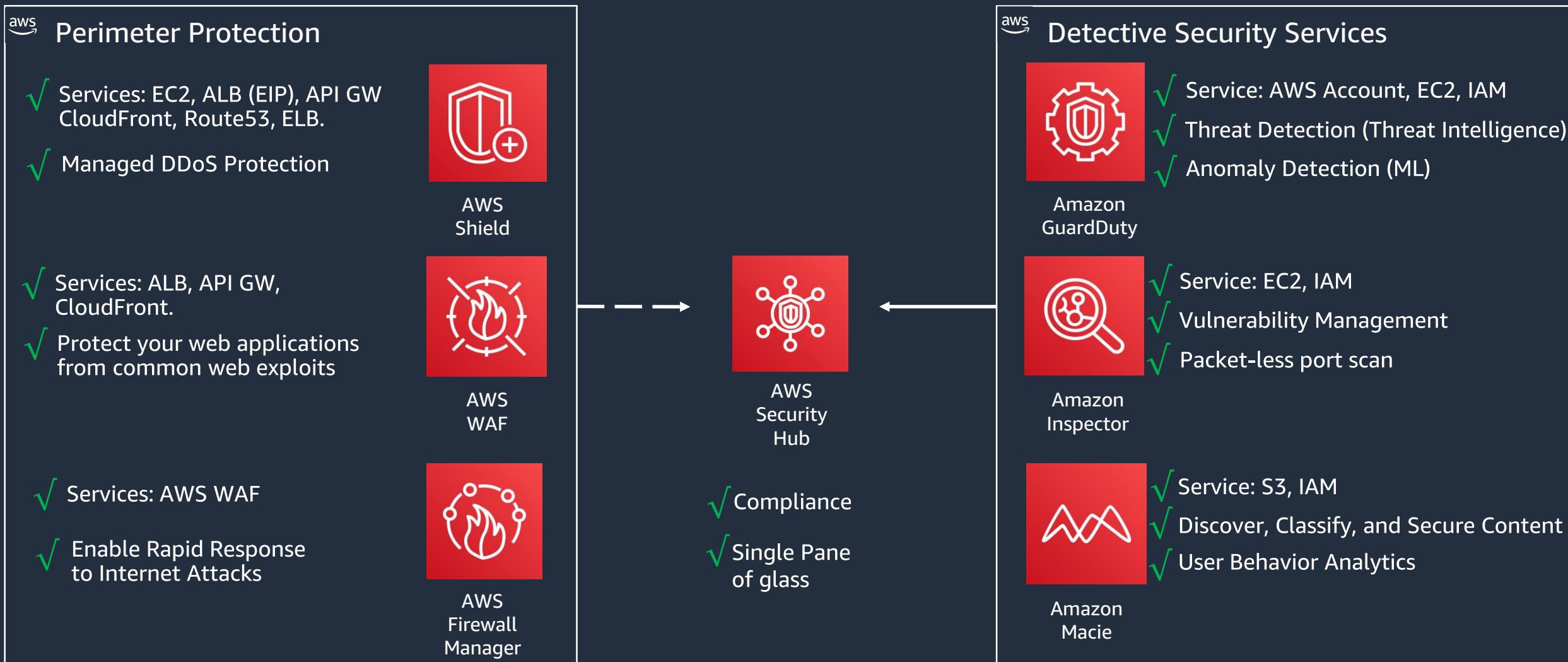


AWS
Firewall
Manager

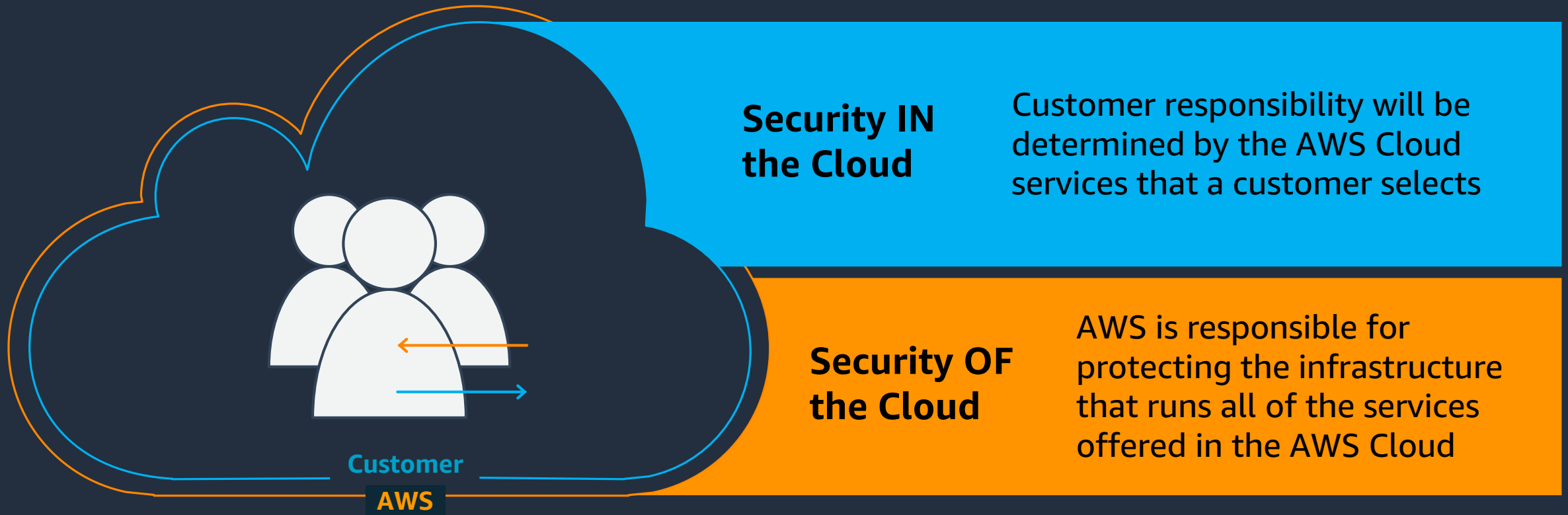


AWS
WAF

Layered Security Services



Shared responsibility model





Thank you!

Kain Leo

leokai@amazon.com

Survey

