AWS State, Local, and Education Learning Days

Security is top priority

Anuraj Pahuja(He/Him)

Sr. Solutions Architect

Agenda

- Introduction
- AWS Layered Security Services

Introduction

Why is security traditionally so difficult?

Lack of visibility

Low degree of automation

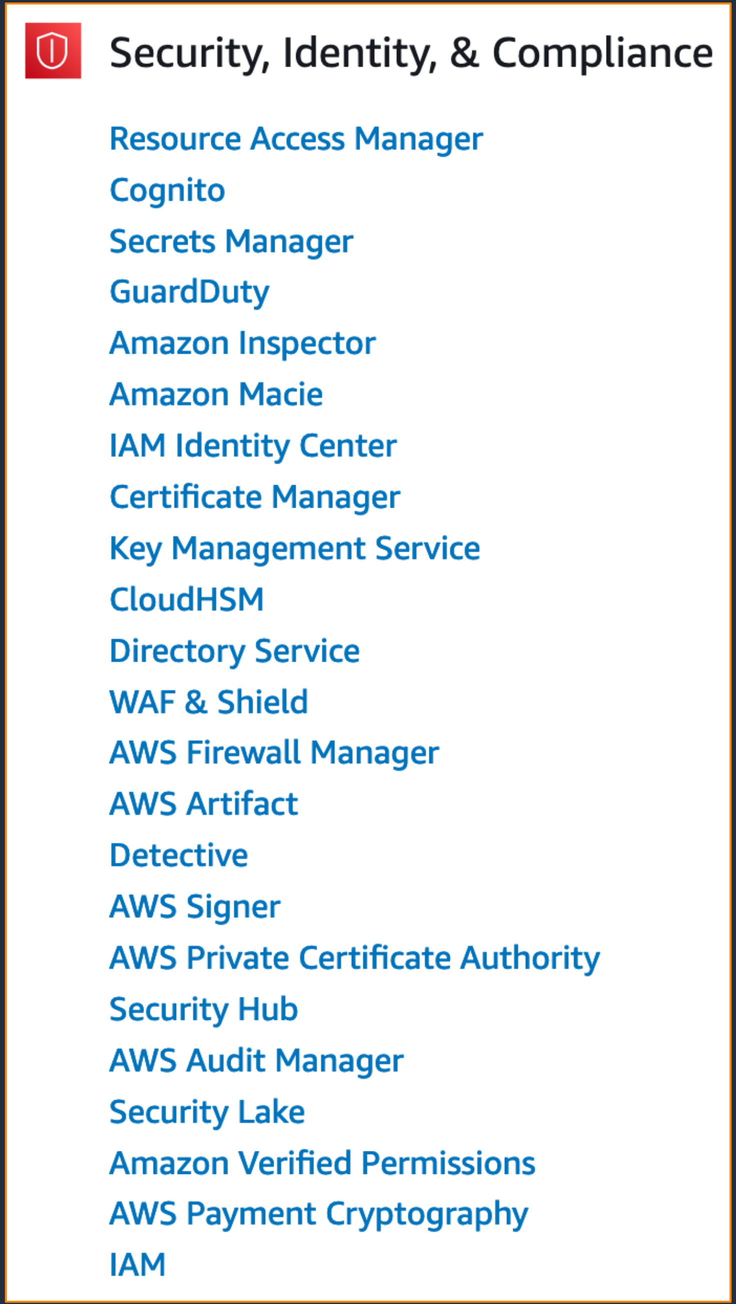
Before…

Move fast **OR** Stay secure

Now…

Move fast **AND** Stay secure

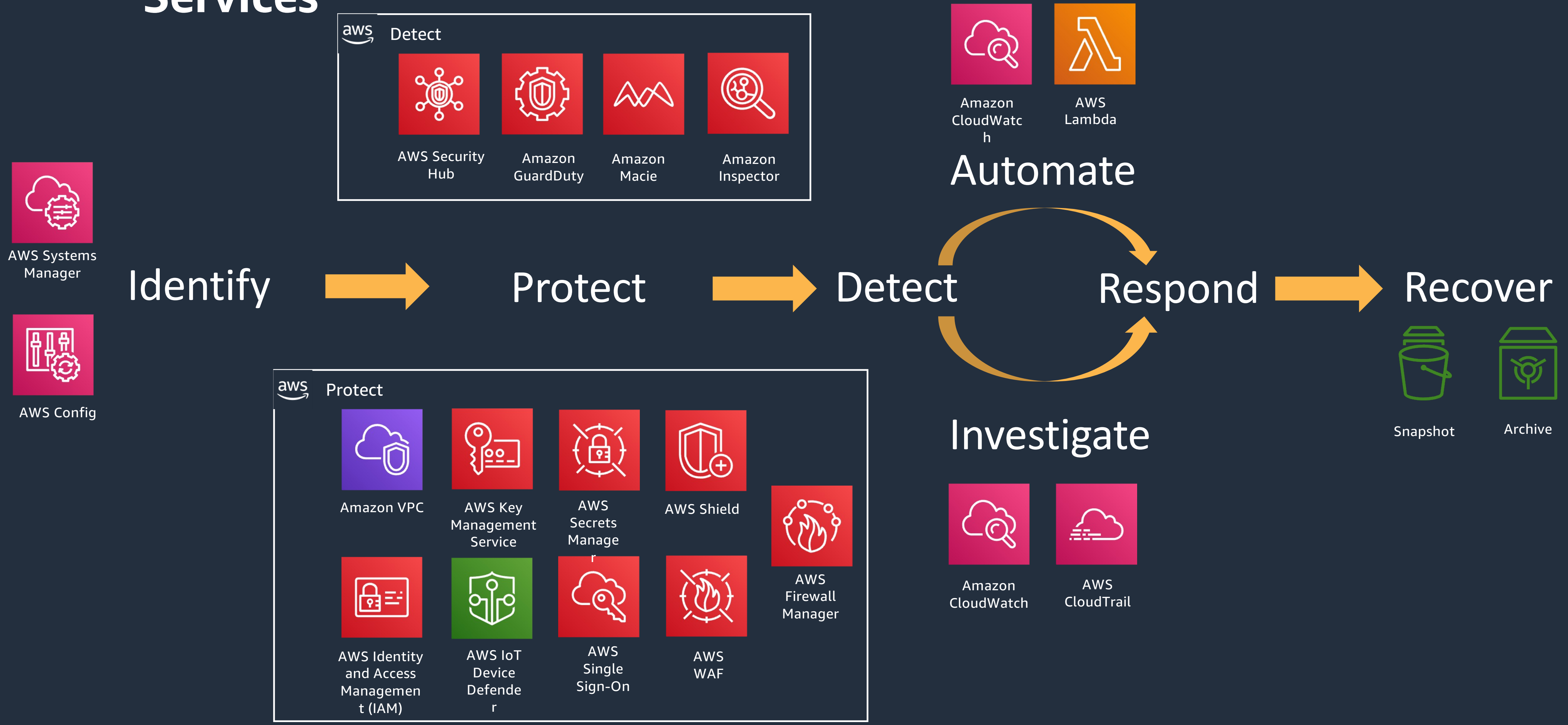
AWS Layered Security Services



Security, Identity, & Compliance

- Resource Access Manager
- Cognito
- Secrets Manager
- GuardDuty
- Amazon Inspector
- Amazon Macie
- IAM Identity Center
- Certificate Manager
- Key Management Service
- CloudHSM
- Directory Service
- WAF & Shield
- AWS Firewall Manager
- AWS Artifact
- Detective
- AWS Signer
- AWS Private Certificate Authority
- Security Hub
- AWS Audit Manager
- Security Lake
- Amazon Verified Permissions
- AWS Payment Cryptography
- IAM

Layered Security Services



Identify

AWS Systems Manager

AWS Config

Protect

Detect

Respond

Recover

Automate

Investigate

Detect

AWS Security Hub

Amazon GuardDuty

Amazon Macie

Amazon Inspector

Amazon CloudWatc h

AWS Lambda

Protect

Amazon VPC

AWS Key Management Service

AWS Secrets Manage r

AWS Shield

AWS Firewall Manager

AWS Identity and Access Managemen t (IAM)

AWS IoT Device Defende r

AWS Single Sign-On

AWS WAF

Amazon CloudWatch

AWS CloudTrail

Snapshot

Archive

Our mental model for security services: Two types

AWS Key Management Service

AWS Identity and Access Management (IAM)

AWS Single Sign-On

AWS Secrets Manager

Amazon VPC

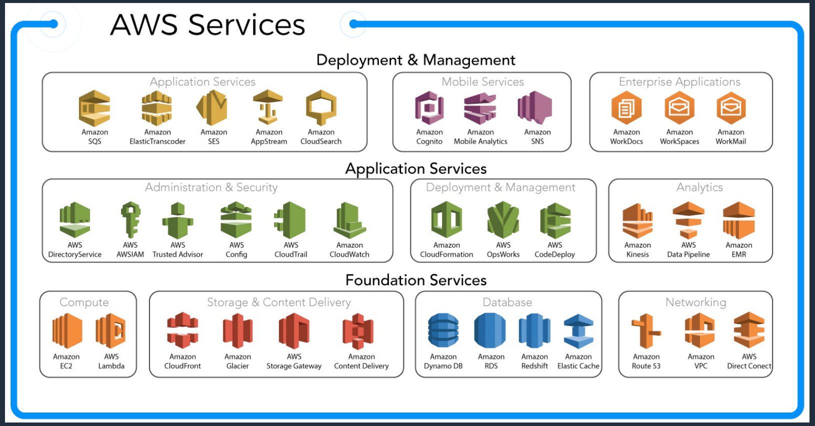
AWS CloudTrail

AWS Systems Manager

AWS Config

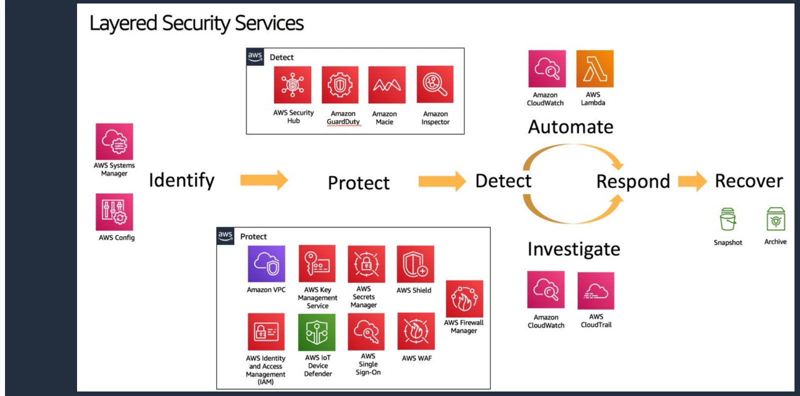
Amazon CloudWatch

Foundational Security Services



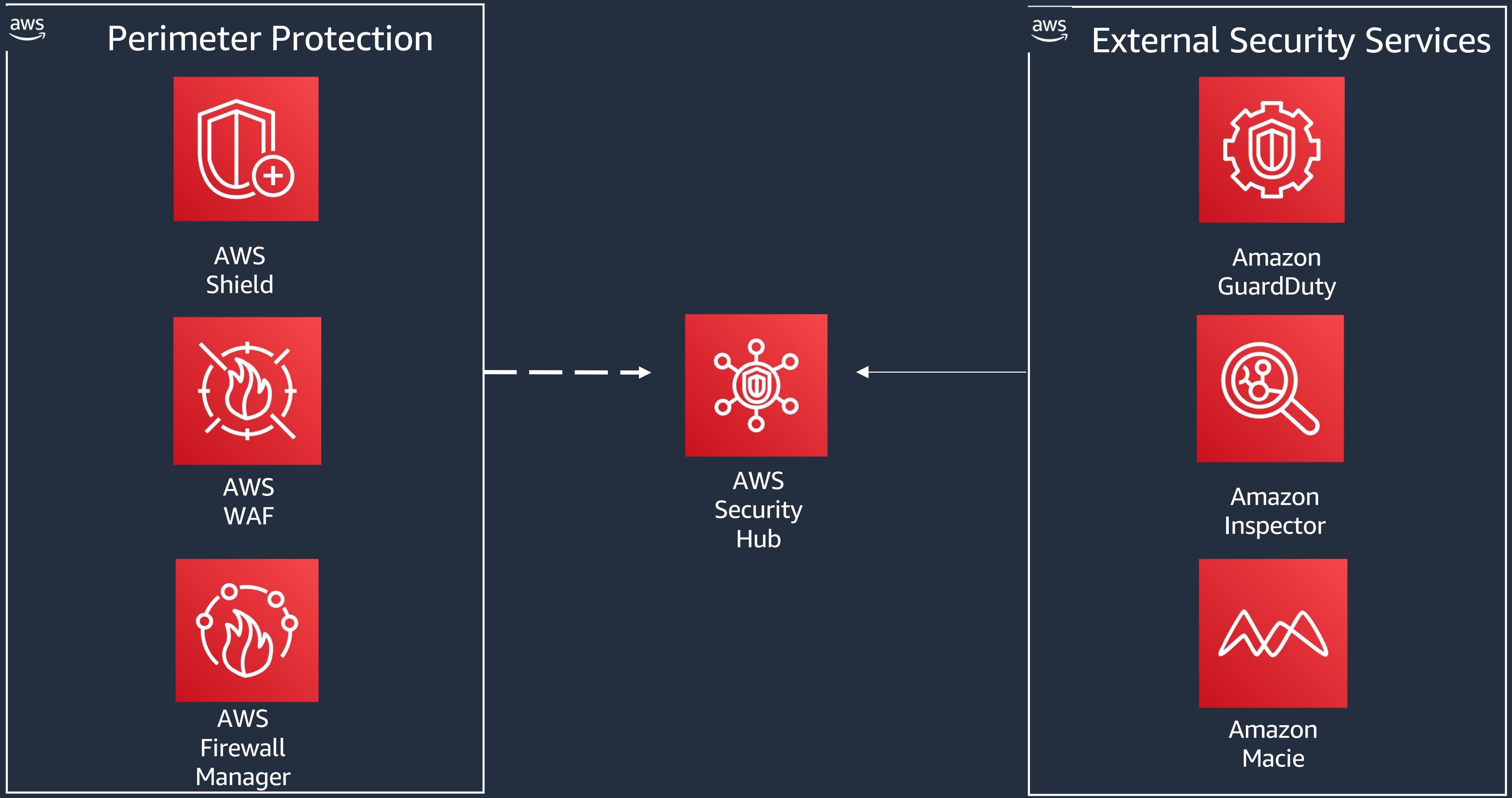
Consumed & integrated workload by workload

Layered Security Services



“Once” applies to **all workloads.**

Layered Security Services



Perimeter Protection

AWS Shield

AWS WAF

AWS Firewall Manager

AWS Security Hub

External Security Services

Amazon GuardDuty

Amazon Inspector

Amazon Macie

Amazon GuardDuty

External Security Services

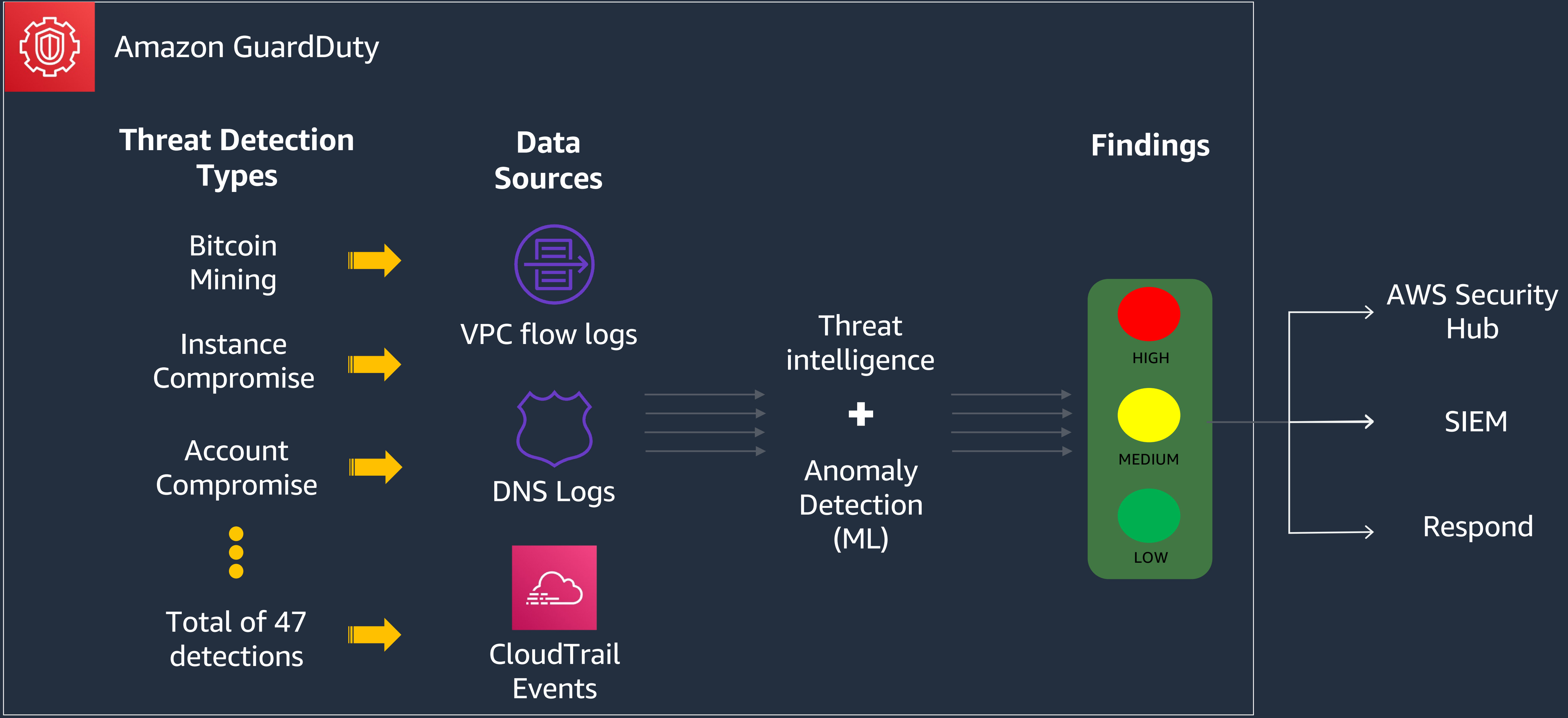
How does Amazon GuardDuty work?

Easy One-Click Activation without Architectural or Performance Impact

How does Amazon GuardDuty work?

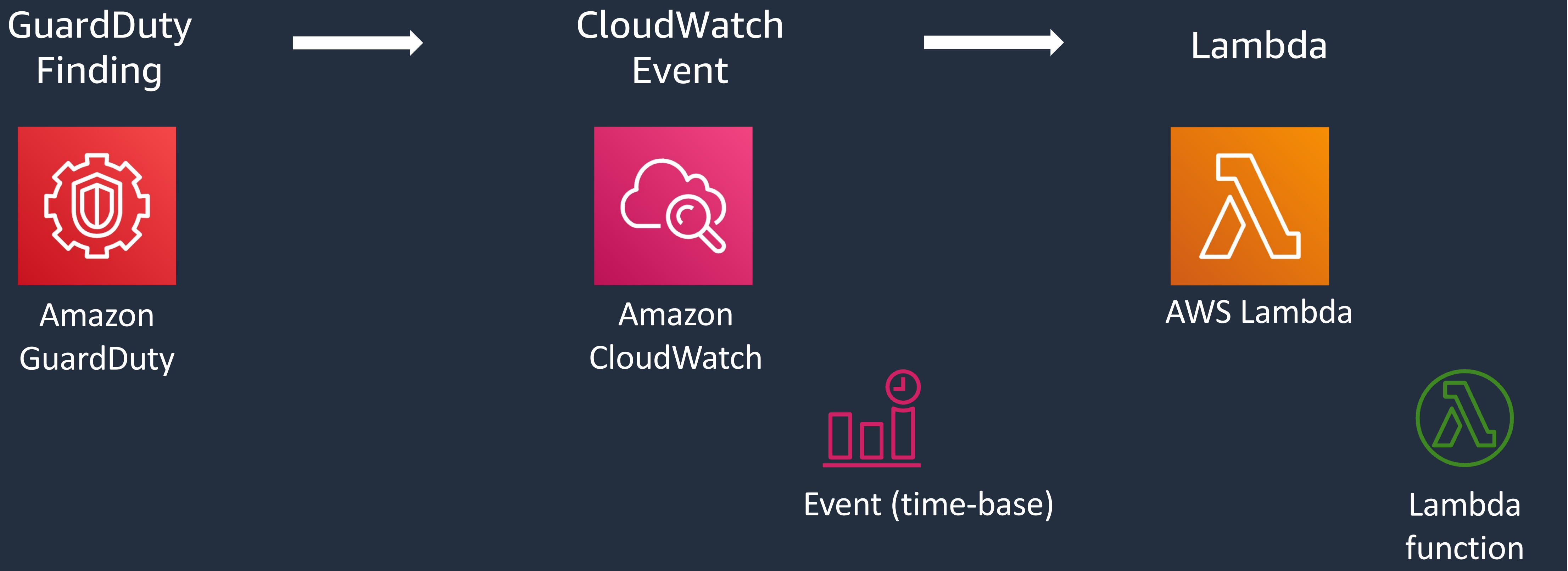
No Agents, No Sensors, No Network Appliances

How does Amazon GuardDuty work?



Automate with integrated services

Automated threat remediation



GuardDuty Finding

CloudWatch Event

Lambda

Amazon GuardDuty

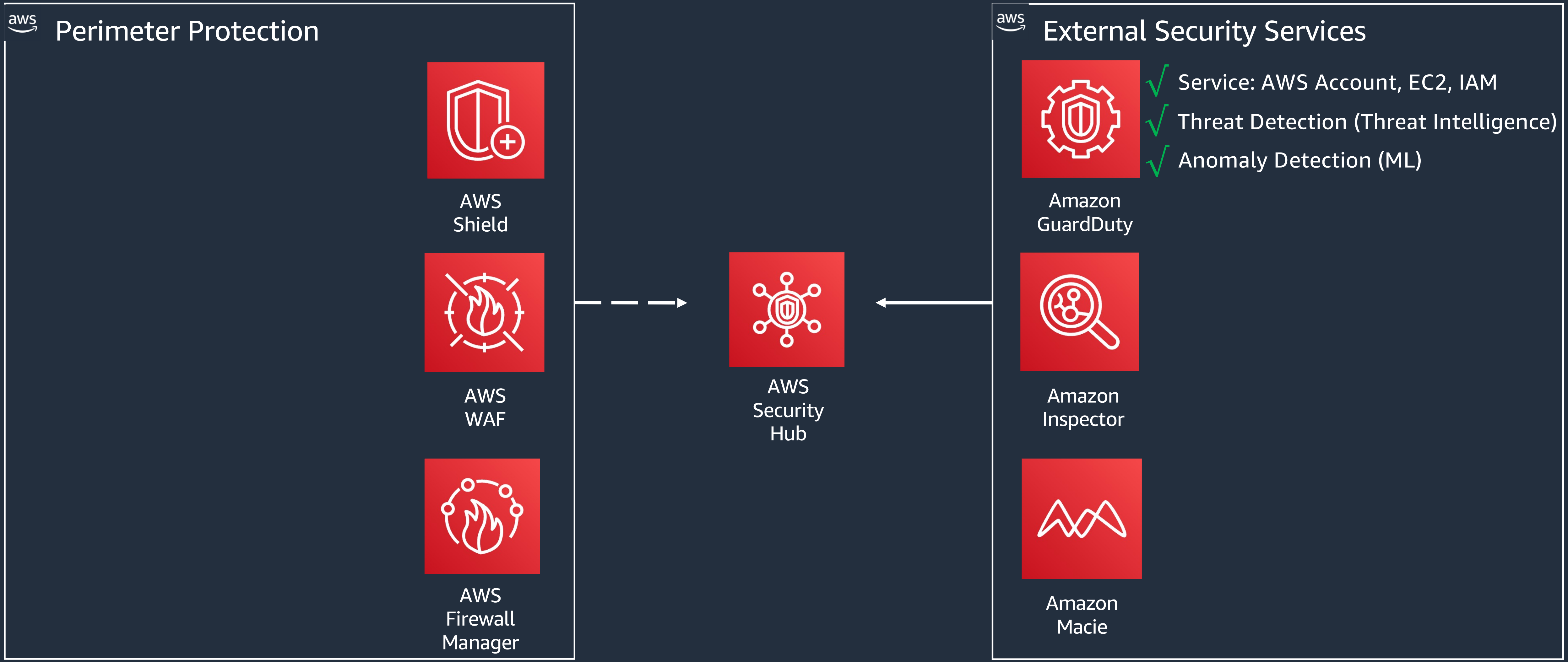
Amazon CloudWatch

AWS Lambda

Event (time-base)

Lambda function

Layered Security Services



Perimeter Protection

- AWS Shield
- AWS WAF
- AWS Firewall Manager

AWS Security Hub

External Security Services

- Amazon GuardDuty
  - √ Service: AWS Account, EC2, IAM
  - √ Threat Detection (Threat Intelligence)
  - √ Anomaly Detection (ML)
- Amazon Inspector
- Amazon Macie

Amazon Inspector

External Security Services

Amazon Inspector

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

Amazon Inspector

Network Reachability Assessments

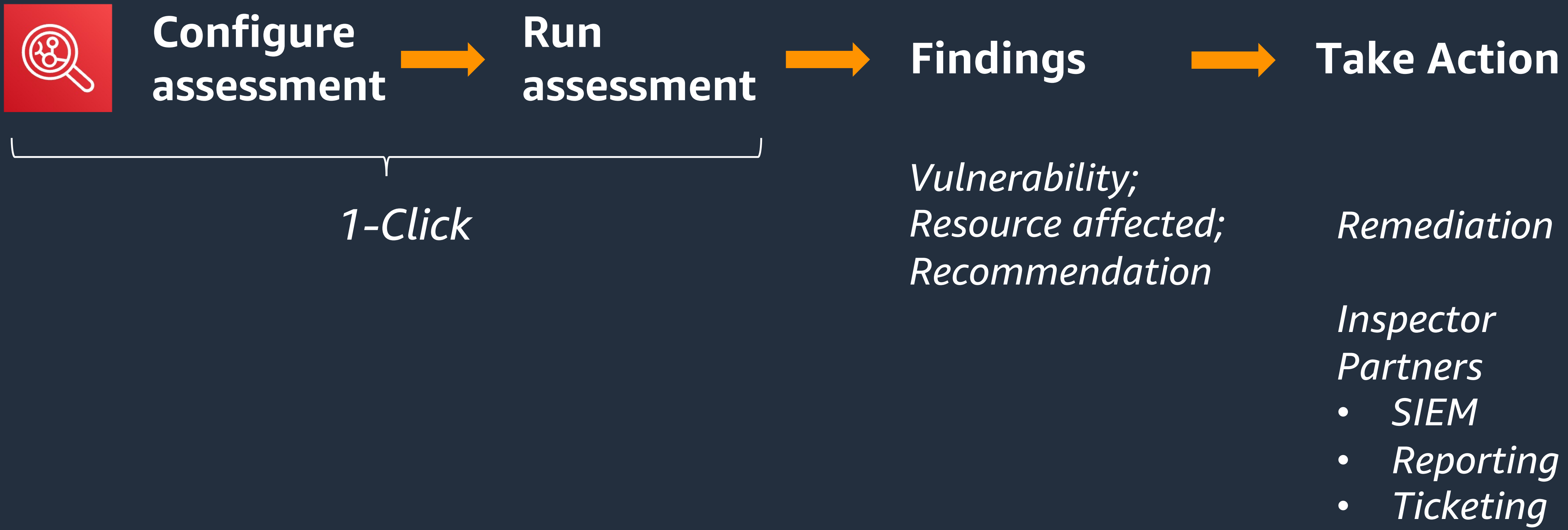
Agentless network assessments

Find externally accessible EC2 instances (internet, VPN, peering). (ex. SSH open to internet)

Enhanced - with agent (optional)

Using Agent, customer will get information about software listening on the ports.

How to use Amazon Inspector?



Configure assessment → **Run assessment** → **Findings** → **Take Action**

1-Click

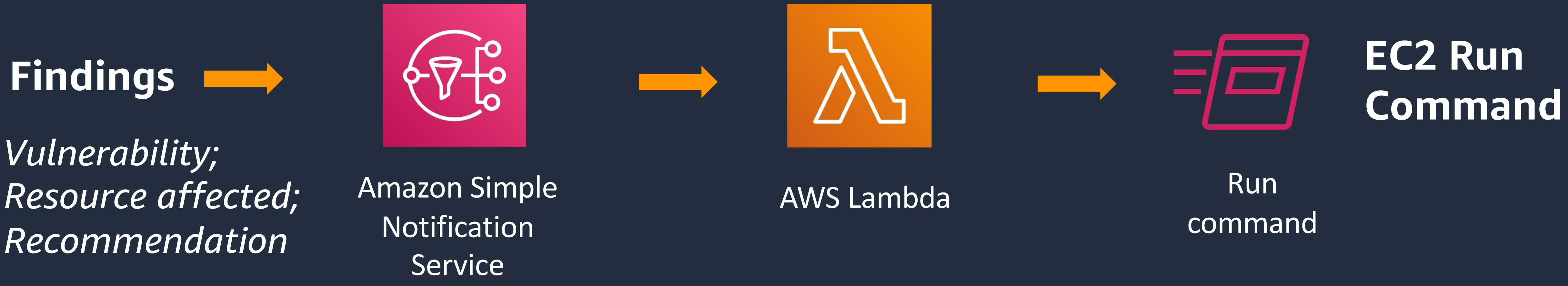
Vulnerability;
Resource affected;
Recommendation

Remediation

Inspector Partners

- *SIEM*
- *Reporting*
- *Ticketing*

Automate use of findings



Findings

Vulnerability; Resource affected; Recommendation

Amazon Simple Notification Service

AWS Lambda

Run command

EC2 Run Command

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

Amazon Inspector
Network Reachability Findings

Amazon Inspector findings show:

WHERE is a port is reachable from?

- Internet via IGW (including instances behind ELB/ALB)
- VPN or DX via VGW
- Peered VPC

HOW is this allowed?

- Security Group
- VPC: Subnet, NACL, IGW, etc.

Which process is listening on port [With optional agent]

- Process name & process id
- Binary / executable

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

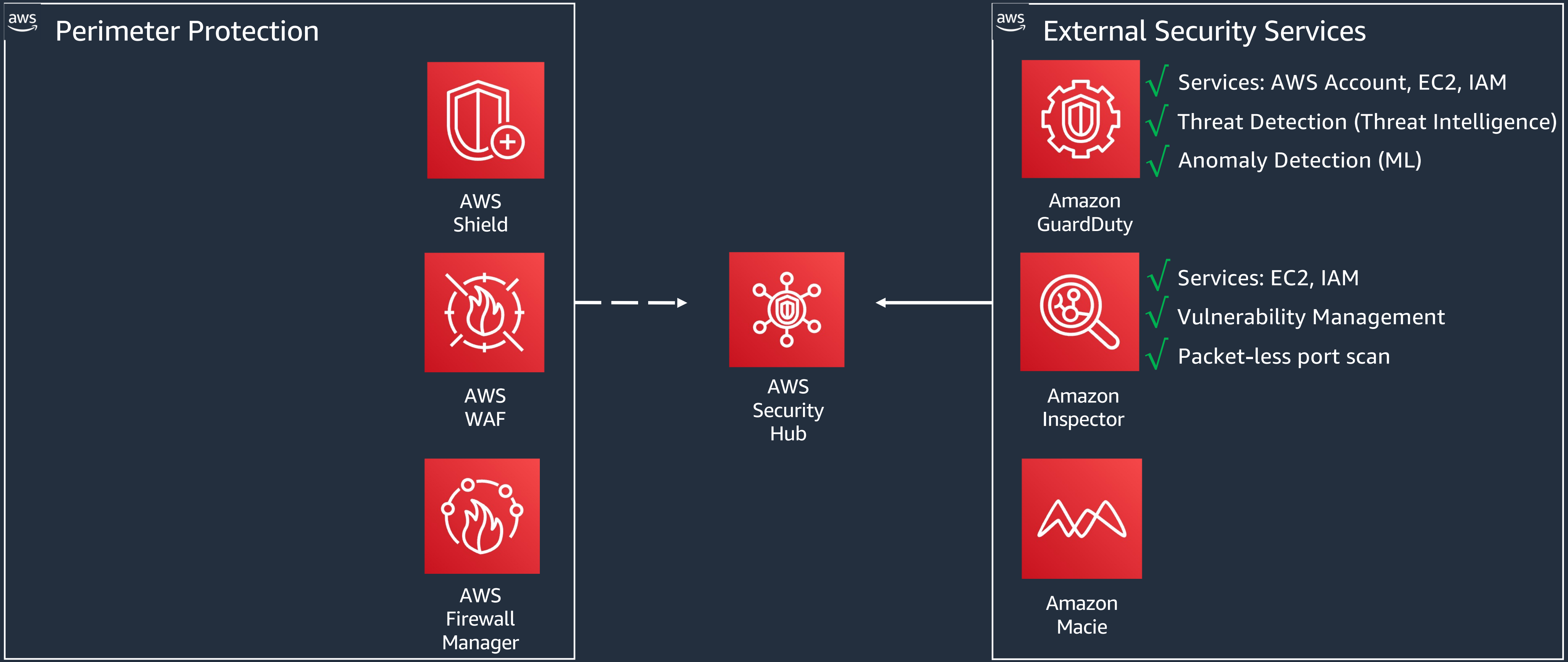
Amazon Inspector

EC2 Host assessment

Using an Agent installed on EC2, Amazon Inspector can assess:

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

Layered Security Services



Perimeter Protection

AWS Shield

AWS WAF

AWS Firewall Manager

AWS Security Hub

External Security Services

Amazon GuardDuty

- √ Services: AWS Account, EC2, IAM
- √ Threat Detection (Threat Intelligence)
- √ Anomaly Detection (ML)

Amazon Inspector

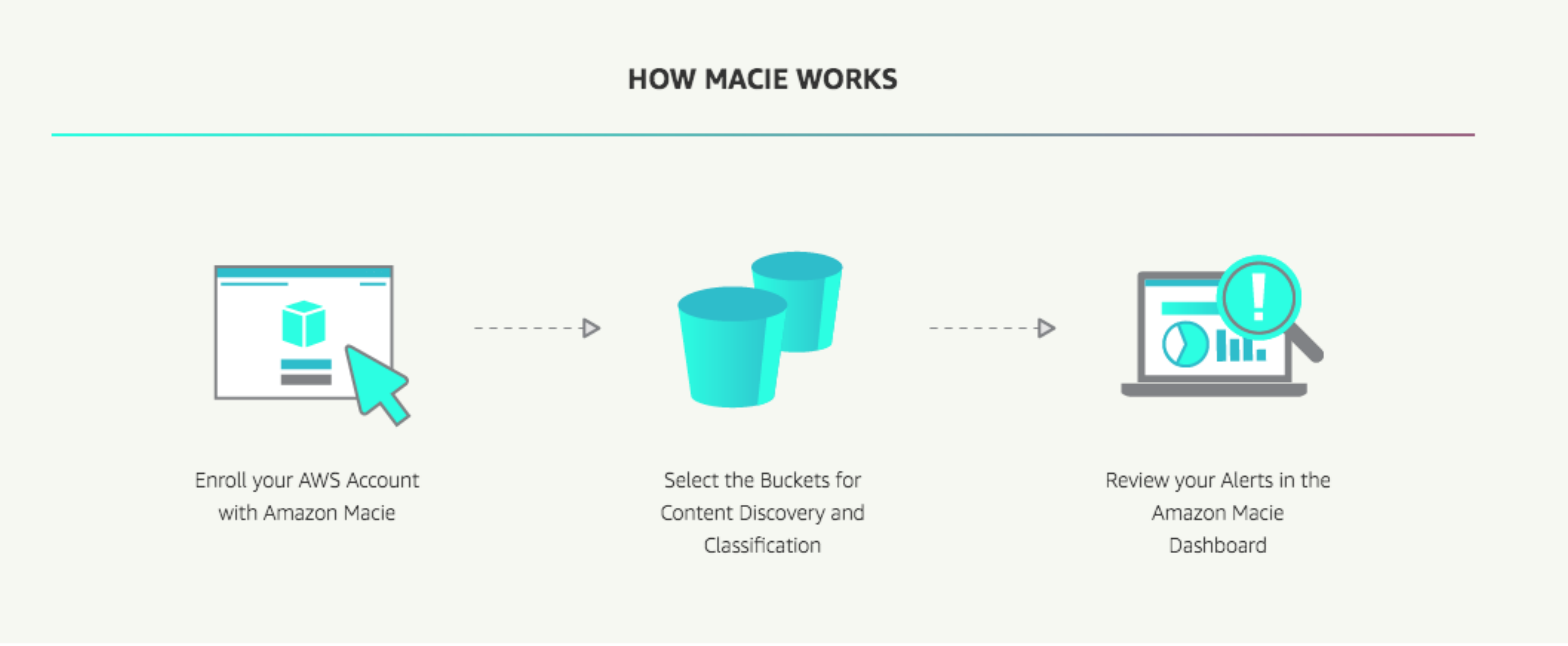
- √ Services: EC2, IAM
- √ Vulnerability Management
- √ Packet-less port scan

Amazon Macie

Amazon Macie

External Security Services

How does Amazon Macie work?



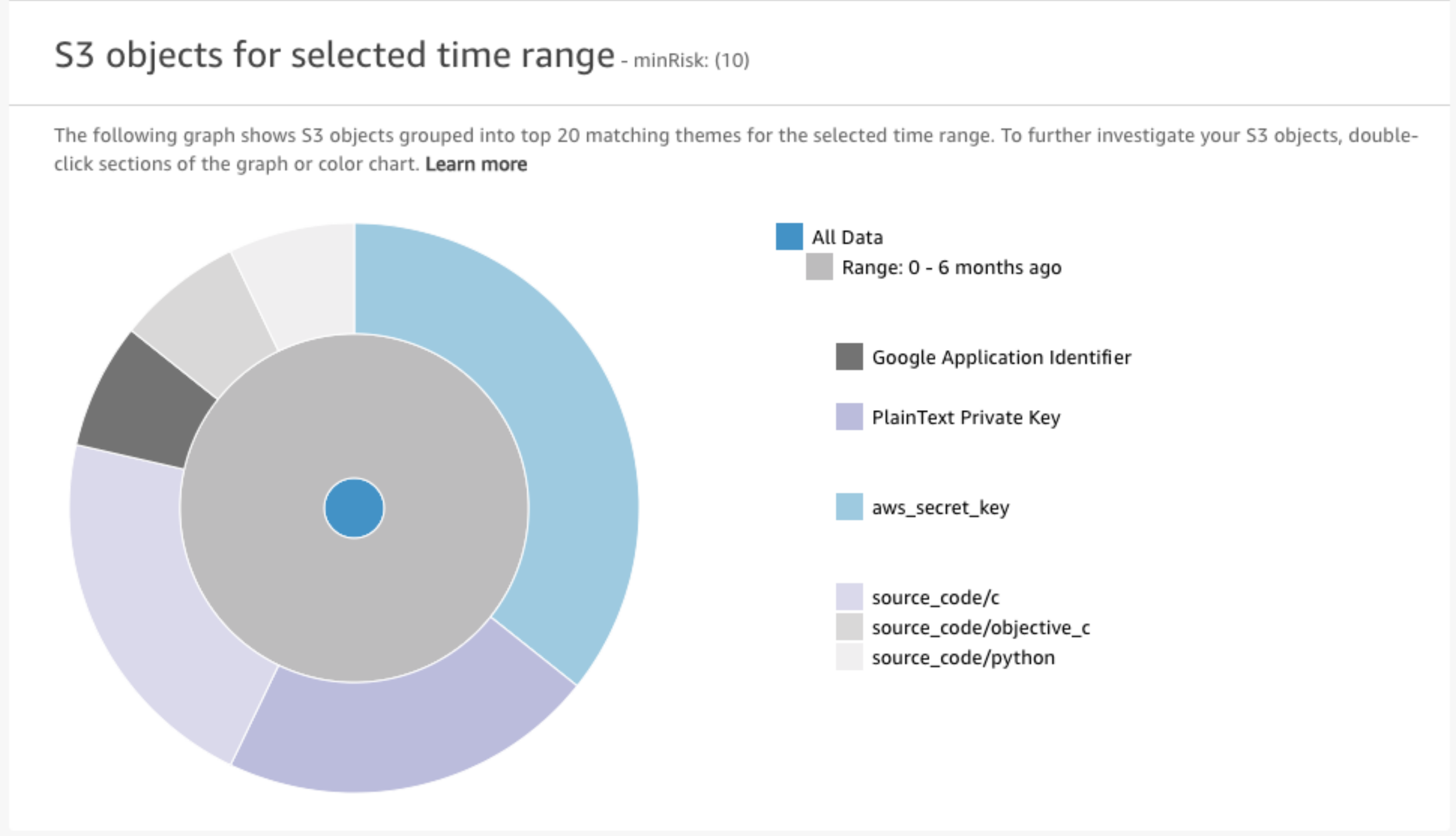
HOW MACIE WORKS

Enroll your AWS Account with Amazon Macie

Select the Buckets for Content Discovery and Classification

Review your Alerts in the Amazon Macie Dashboard

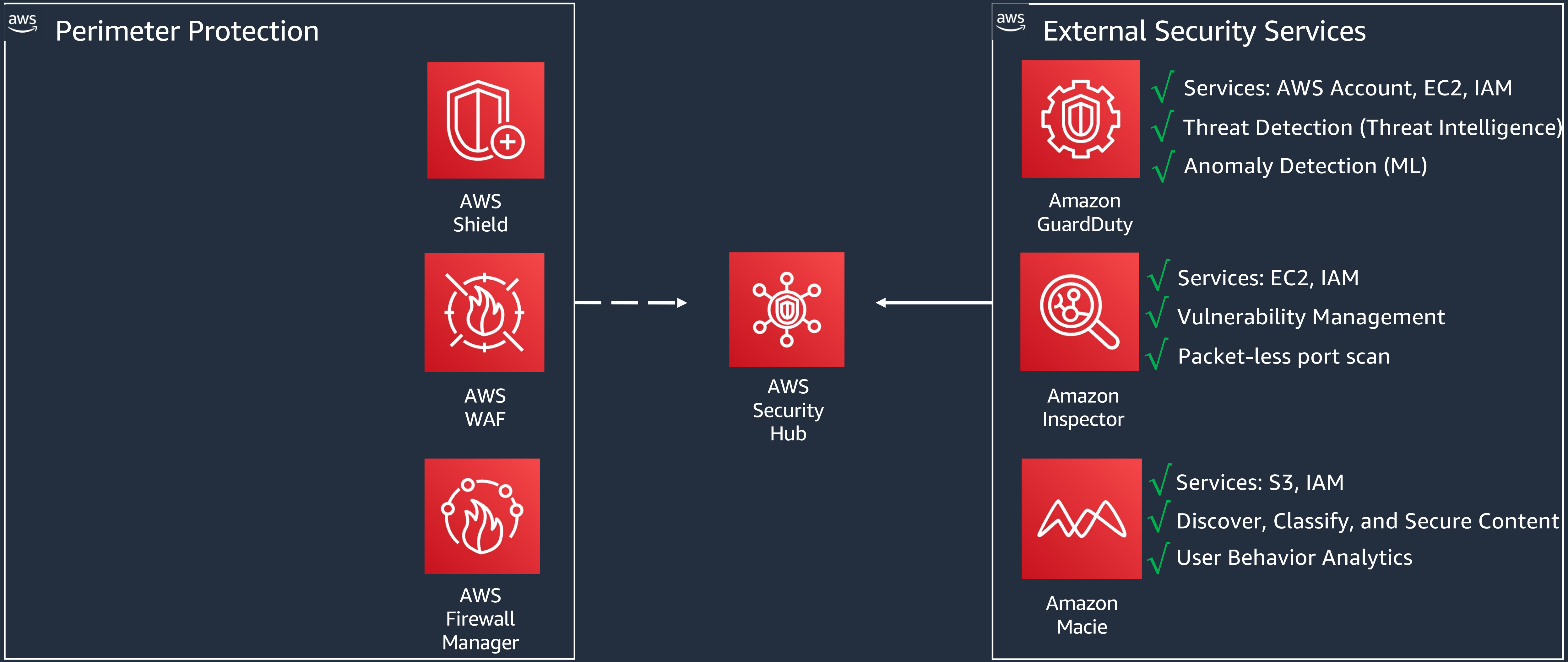
How does Macie work?



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



Perimeter Protection

AWS Shield

AWS WAF

AWS Firewall Manager

AWS Security Hub

External Security Services

Amazon GuardDuty

- √ Services: AWS Account, EC2, IAM
- √ Threat Detection (Threat Intelligence)
- √ Anomaly Detection (ML)

Amazon Inspector

- √ Services: EC2, IAM
- √ Vulnerability Management
- √ Packet-less port scan

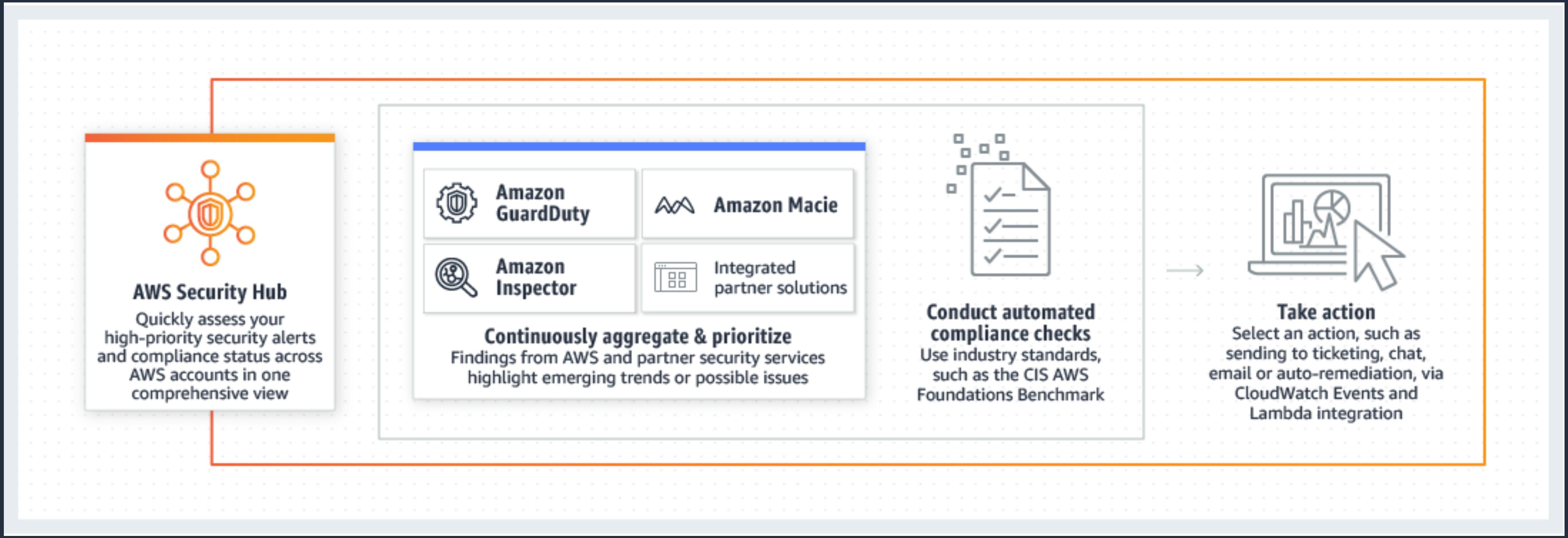
Amazon Macie

- √ Services: S3, IAM
- √ Discover, Classify, and Secure Content
- √ User Behavior Analytics

AWS Security Hub

External Security Services

How does AWS Security Hub work?



AWS Security Hub

Quickly assess your high-priority security alerts and compliance status across AWS accounts in one comprehensive view

Amazon GuardDuty

Amazon Macie

Amazon Inspector

Integrated partner solutions

Continuously aggregate & prioritize

Findings from AWS and partner security services highlight emerging trends or possible issues

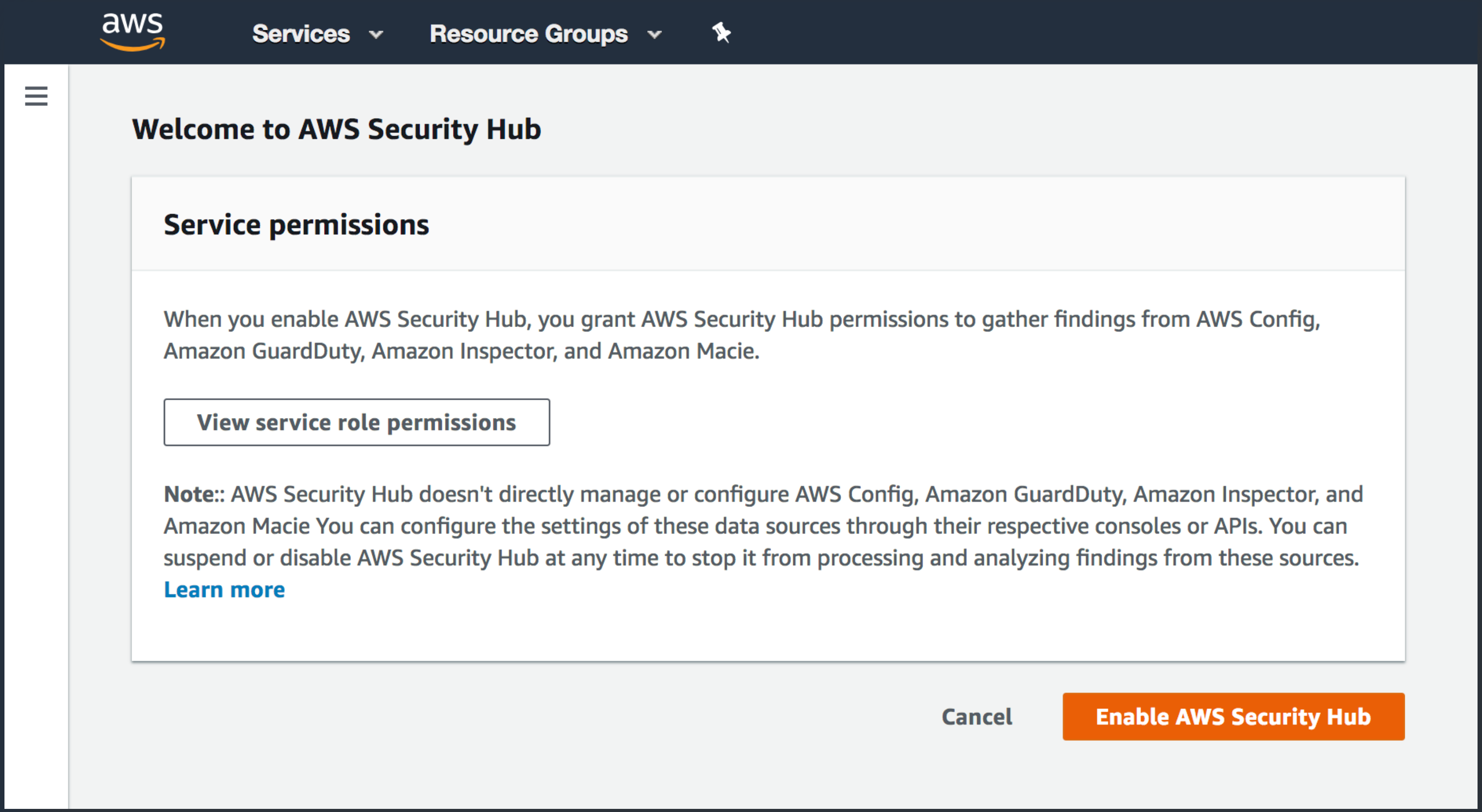
Conduct automated compliance checks

Use industry standards, such as the CIS AWS Foundations Benchmark

Take action

Select an action, such as sending to ticketing, chat, email or auto-remediation, via CloudWatch Events and Lambda integration

Getting Started - AWS Security Hub work?



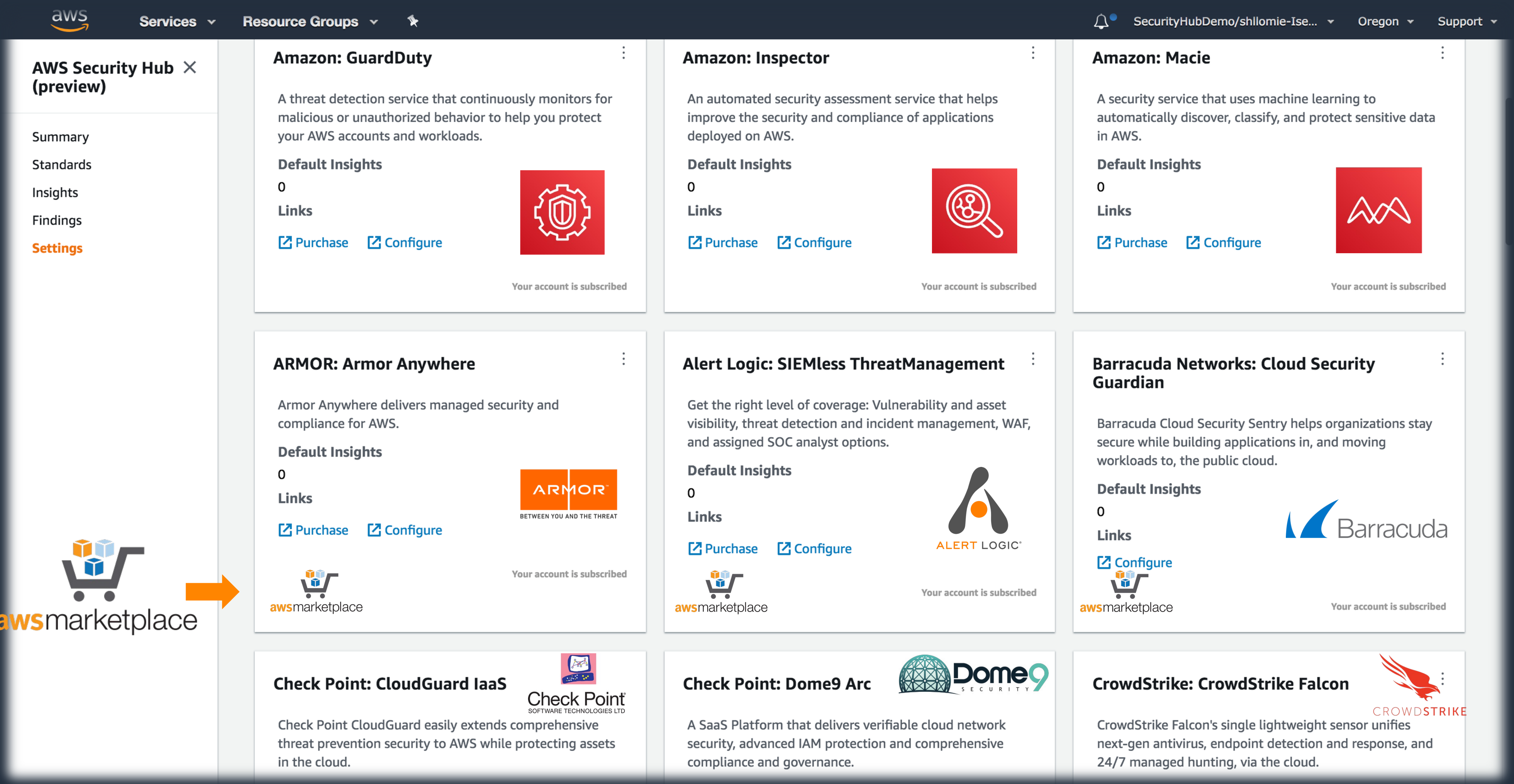
Welcome to AWS Security Hub

Service permissions

When you enable AWS Security Hub, you grant AWS Security Hub permissions to gather findings from AWS Config, Amazon GuardDuty, Amazon Inspector, and Amazon Macie.

Note:: AWS Security Hub doesn't directly manage or configure AWS Config, Amazon GuardDuty, Amazon Inspector, and Amazon Macie You can configure the settings of these data sources through their respective consoles or APIs. You can suspend or disable AWS Security Hub at any time to stop it from processing and analyzing findings from these sources. **Learn more**

AWS Security Hub – Partner Integrations



AWS Security Hub (preview)

- Summary
- Standards
- Insights
- Findings
- Settings

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.

awsmarketplace
ARMOR BETWEEN YOU AND THE THREAT
ALERT LOGIC
Barracuda
Check Point SOFTWARE TECHNOLOGIES LTD
Dome9 SECURITY
CROWDSTRIKE

AWS Security Hub – Partner Integrations

Firewalls

f5

paloalto NETWORKS

Check Point SOFTWARE TECHNOLOGIES LTD.

Barracuda

FORTINET

Endpoint

CROWDSTRIKE

TREND MICRO

Symantec.

SOPHOS Security made simple.

Vulnerability

tenable

Qualys. Continuous Security

RAPID7

Compliance

Check Point SOFTWARE TECHNOLOGIES LTD.

paloalto NETWORKS

Qualys. Continuous Security

Cloud Custodian

SOAR

turbot

DEMISTO

splunk>

MSSP

ARMOR CLOUD SECURITY, UNCOMPROMISED.™

ALERT LOGIC

AWS Managed Services

SIEM

IBM Security

sumologic

splunk>

Other

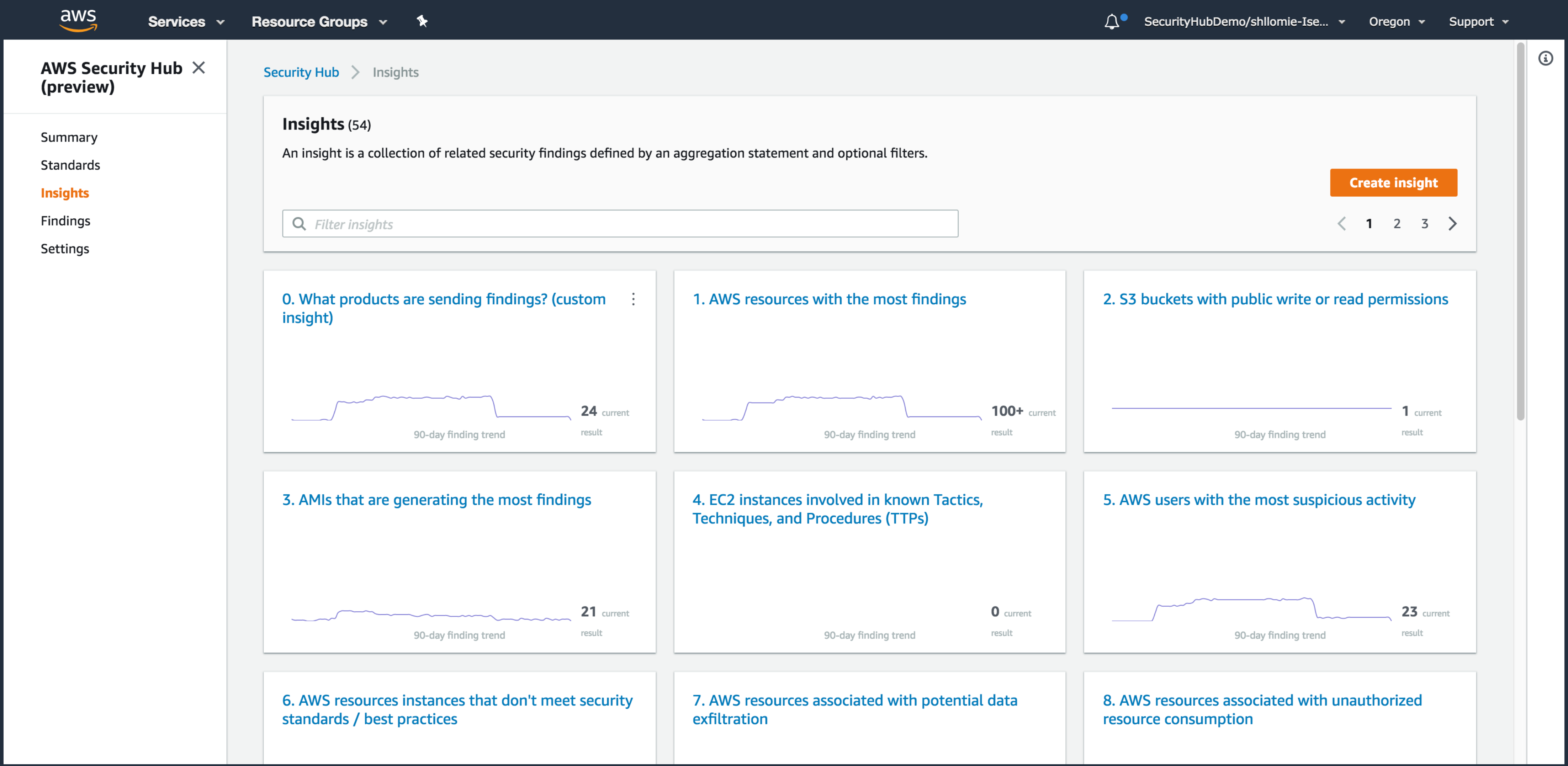
McAfee Together is power.

CYBERARK

Twistlock

aws

AWS Security Hub – Insights



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

Filter insights

< 1 2 3 >

0. What products are sending findings? (custom insight) — 90-day finding trend — 24 current result

1. AWS resources with the most findings — 90-day finding trend — 100+ current result

2. S3 buckets with public write or read permissions — 90-day finding trend — 1 current result

3. AMIs that are generating the most findings — 90-day finding trend — 21 current result

4. EC2 instances involved in known Tactics, Techniques, and Procedures (TTPs) — 90-day finding trend — 0 current result

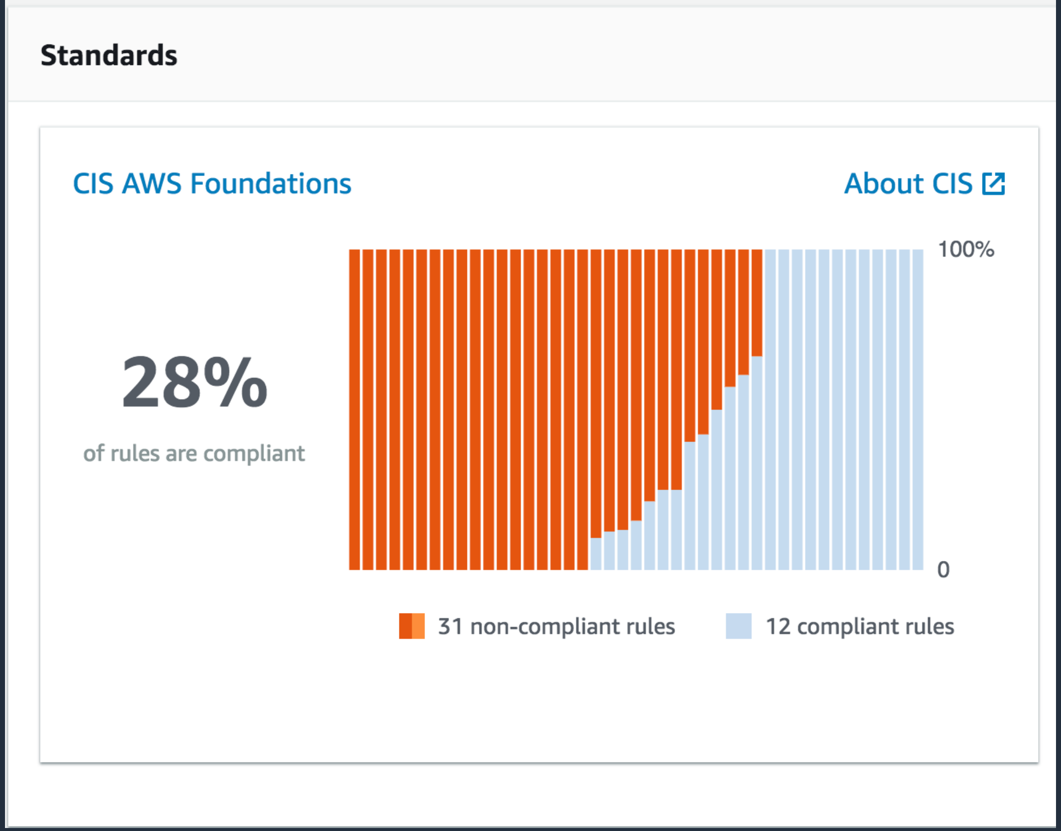
5. AWS users with the most suspicious activity — 90-day finding trend — 23 current result

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

7. AWS resources associated with potential data exfiltration

8. AWS resources associated with unauthorized resource consumption

AWS Security Hub – Compliance Checks (CIS)



Standards

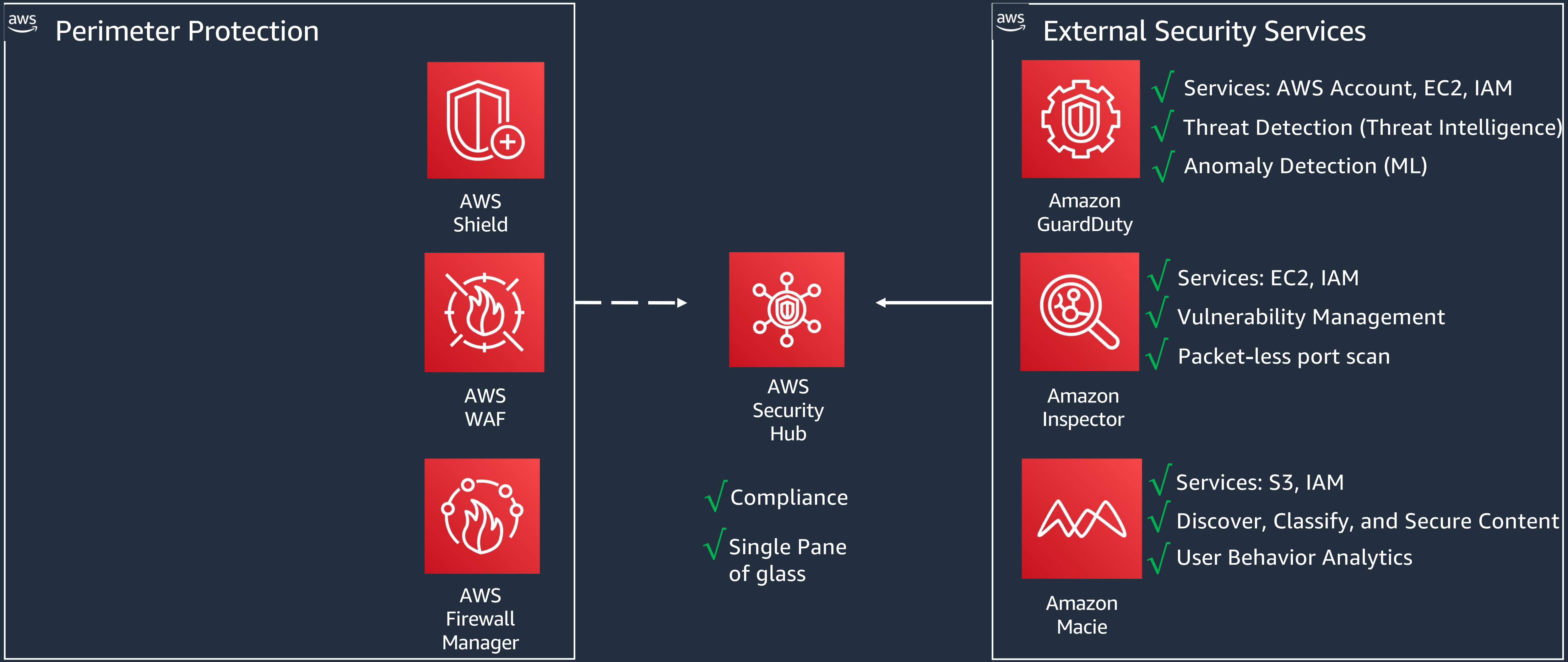
CIS AWS Foundations

About CIS

28%

of rules are compliant

Layered Security Services



Perimeter Protection

AWS Shield

AWS WAF

AWS Firewall Manager

AWS Security Hub

√ Compliance

√ Single Pane of glass

External Security Services

Amazon GuardDuty

√ Services: AWS Account, EC2, IAM

√ Threat Detection (Threat Intelligence)

√ Anomaly Detection (ML)

Amazon Inspector

√ Services: EC2, IAM

√ Vulnerability Management

√ Packet-less port scan

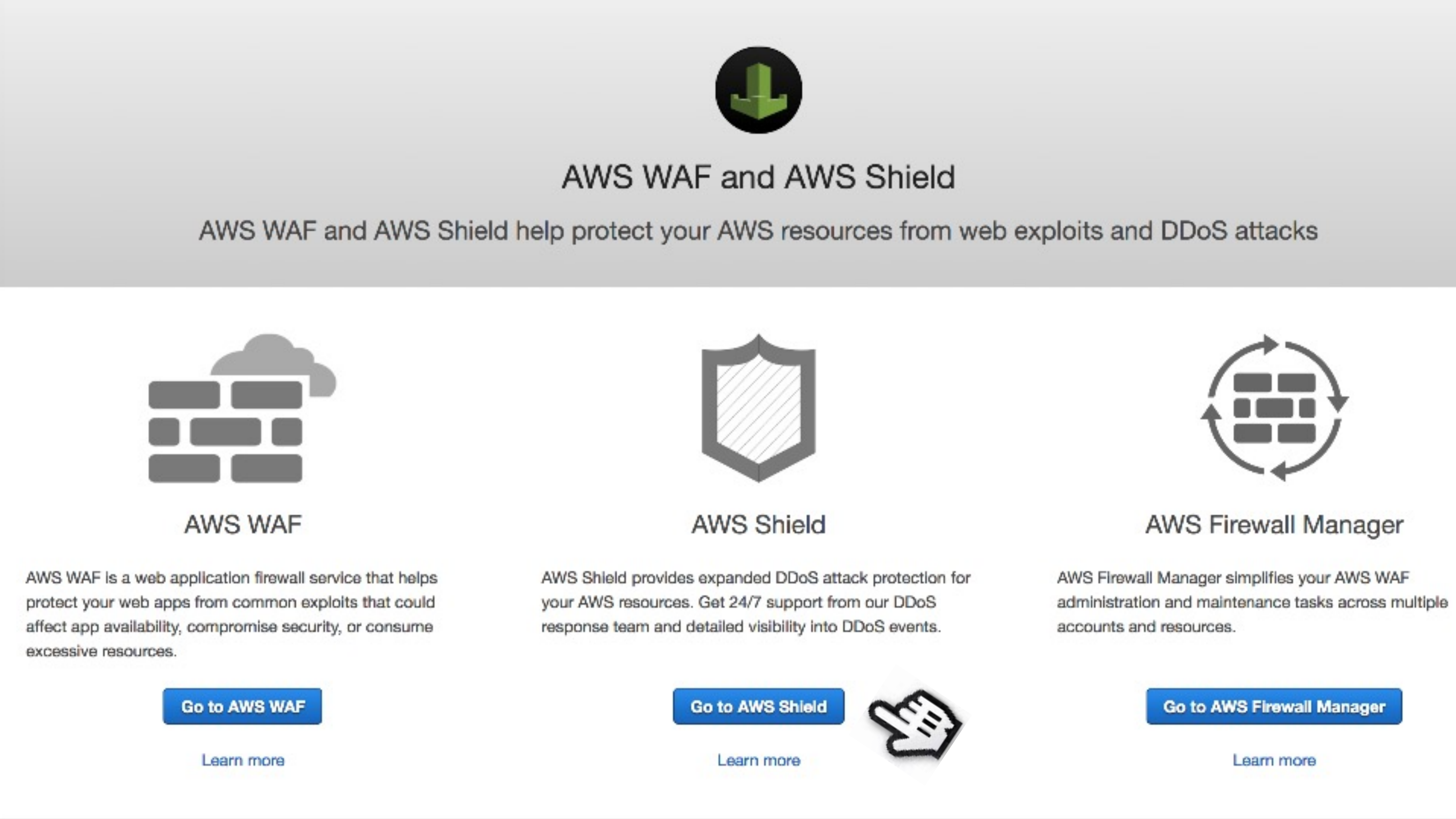
Amazon Macie

√ Services: S3, IAM

√ Discover, Classify, and Secure Content

√ User Behavior Analytics

Perimeter Protection



AWS WAF and AWS Shield

AWS WAF and AWS Shield help protect your AWS resources from web exploits and DDoS attacks

AWS WAF

AWS WAF is a web application firewall service that helps protect your web apps from common exploits that could affect app availability, compromise security, or consume excessive resources.

AWS Shield

AWS Shield provides expanded DDoS attack protection for your AWS resources. Get 24/7 support from our DDoS response team and detailed visibility into DDoS events.

AWS Firewall Manager

AWS Firewall Manager simplifies your AWS WAF administration and maintenance tasks across multiple accounts and resources.

AWS Shield Advanced

Perimeter Protection

AWS Shield

A Managed DDoS Protection Service

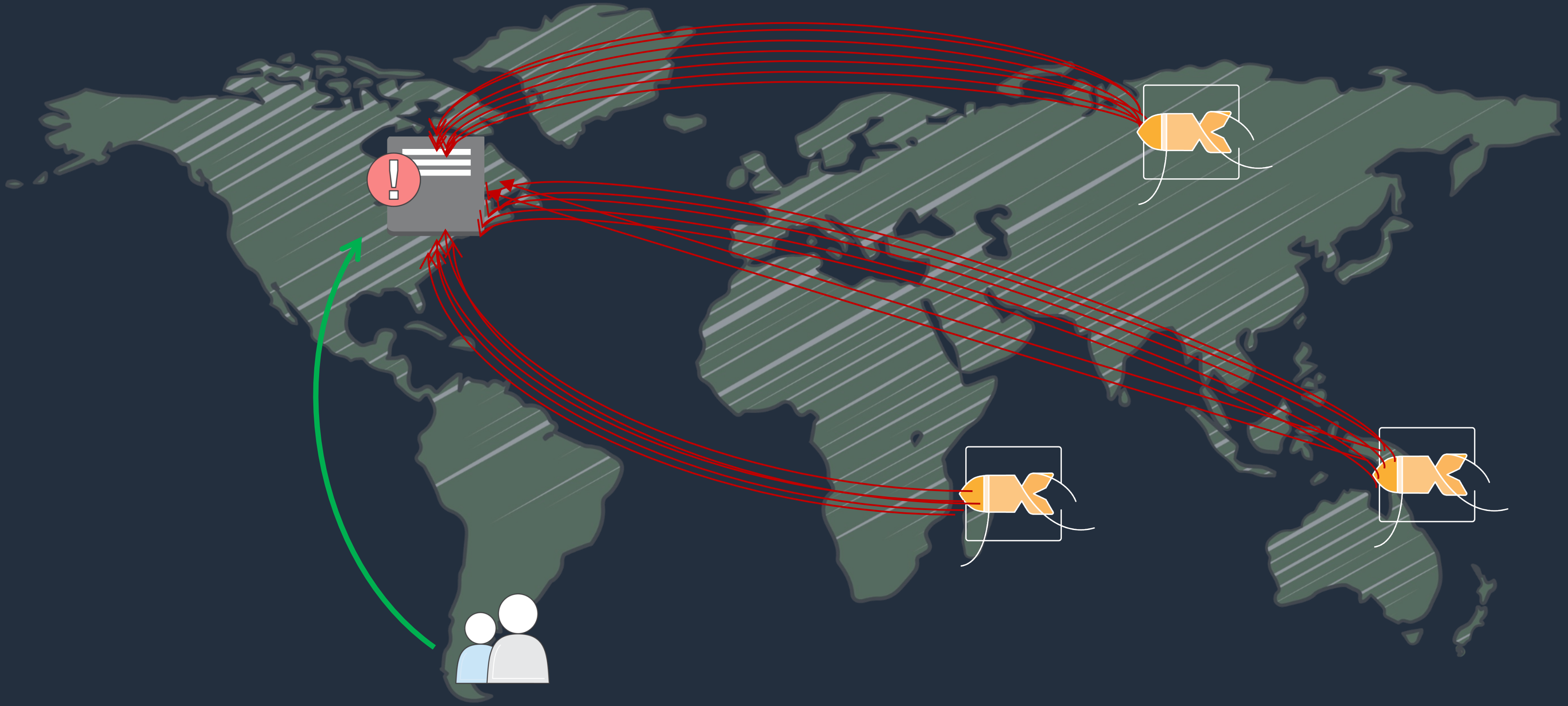
There are two tiers of AWS Shield:

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

AWS Shield

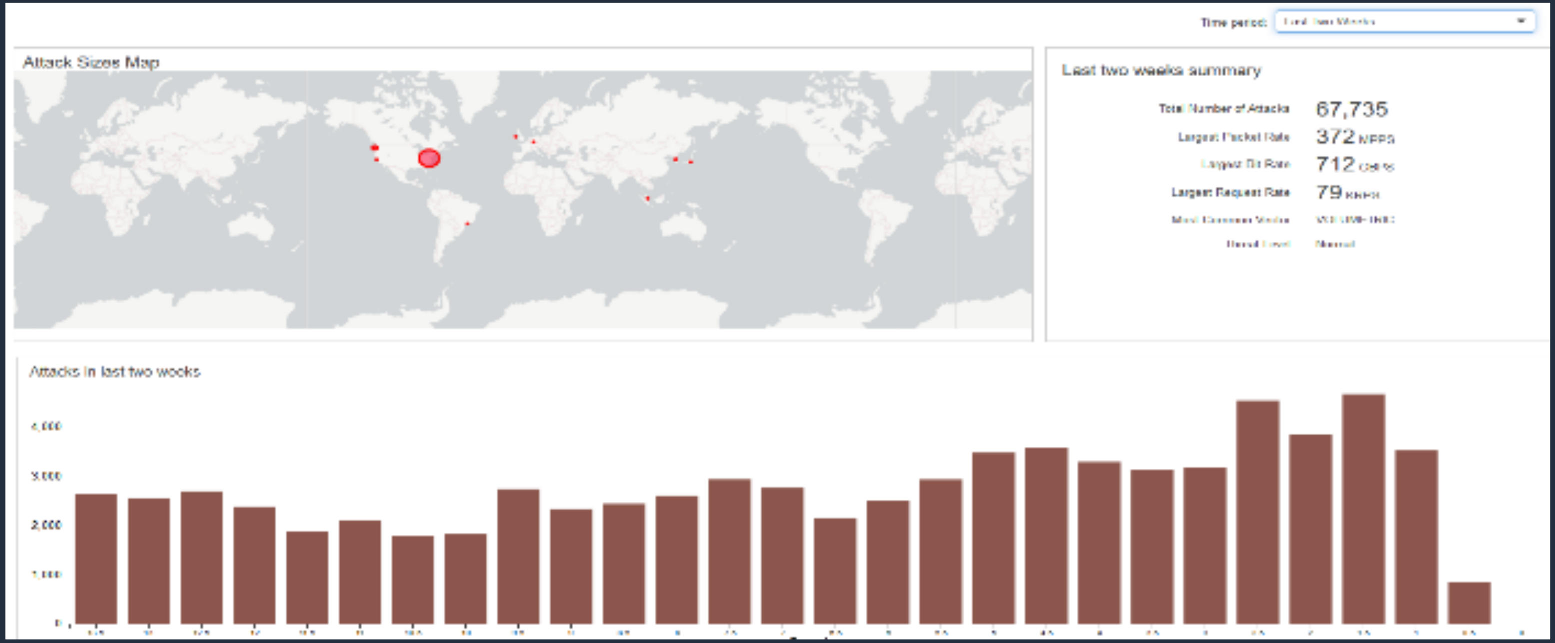
AWS Shield Advanced - DDoS Attack threats and Trends:

Network / Transport Layer DDoS



DDoS Threats and Trends

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



Time period: Last Two Weeks

Attack Sizes Map

Last two weeks summary

Total Number of Attacks	67,735
Largest Packet Rate	372 MPPS
Largest Bit Rate	712 Gbps
Largest Request Rate	79 KRPS
Most Common Vector	[illegible]
Threat Level	Normal

Attacks in last two weeks

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

AWS Shield **Standard**

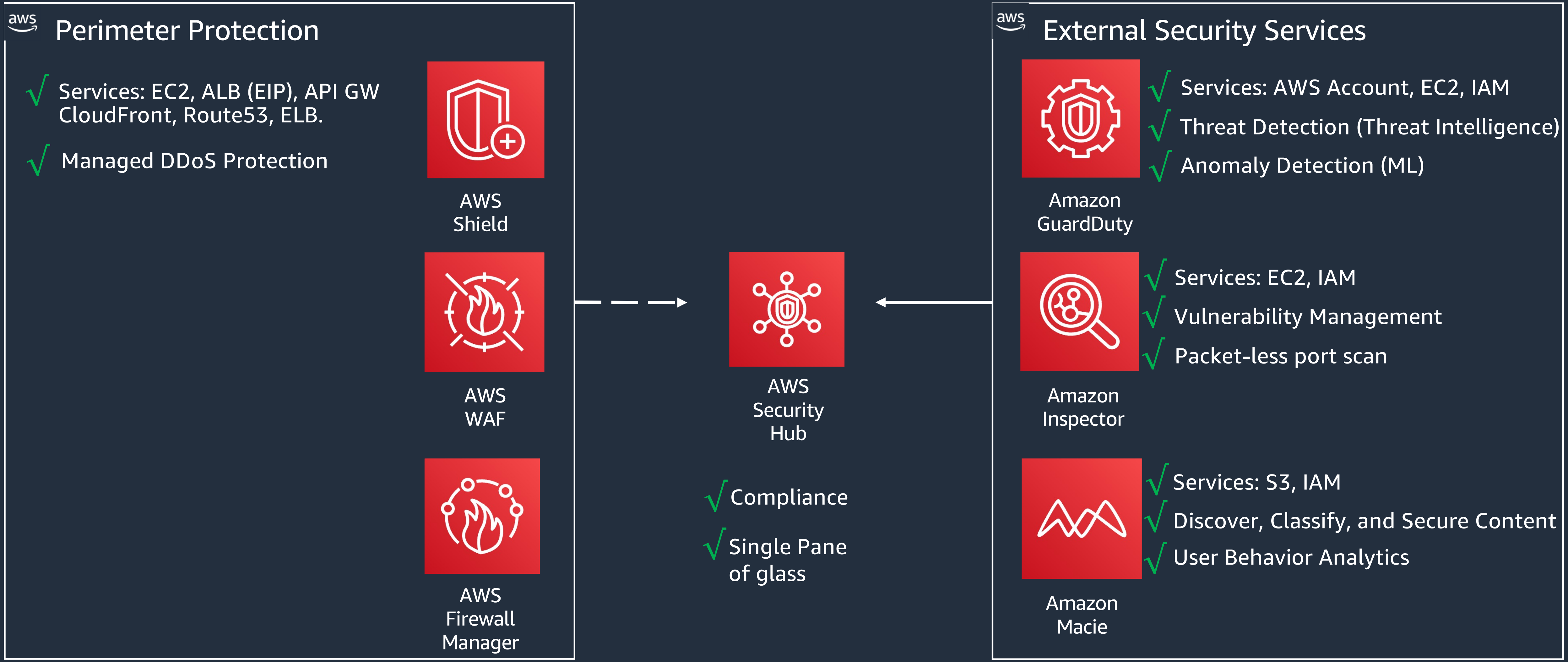
DDoS Expertise

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



Perimeter Protection

- √ Services: EC2, ALB (EIP), API GW CloudFront, Route53, ELB.
- √ Managed DDoS Protection

- √ Compliance
- √ Single Pane of glass

External Security Services

- √ Services: AWS Account, EC2, IAM
- √ Threat Detection (Threat Intelligence)
- √ Anomaly Detection (ML)

- √ Services: EC2, IAM
- √ Vulnerability Management
- √ Packet-less port scan

- √ Services: S3, IAM
- √ Discover, Classify, and Secure Content
- √ User Behavior Analytics

AWS WAF

Perimeter Protection

Protecting Your Applications Using AWS WAF

Application Vulnerabilities

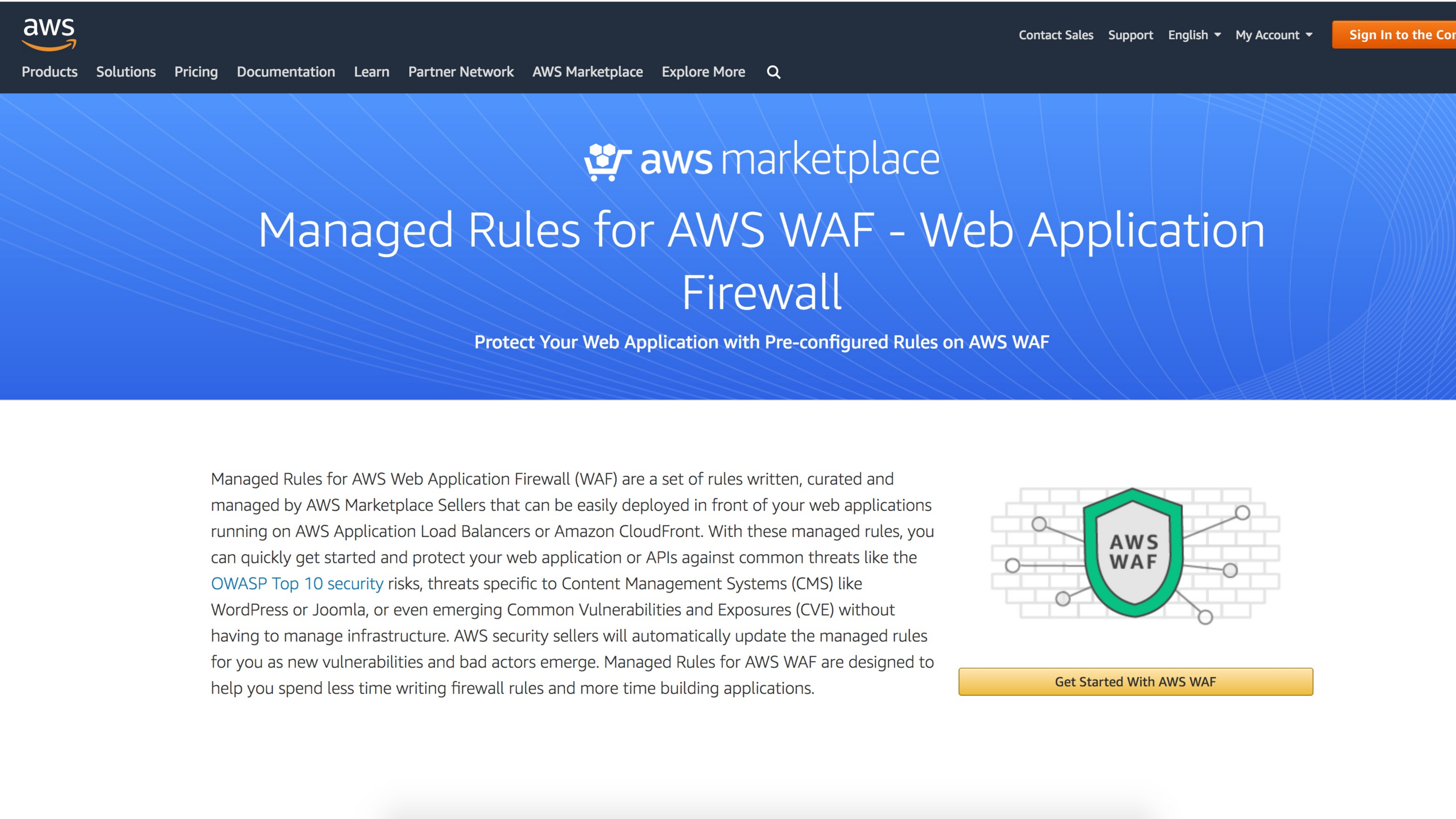
HTTP Flood

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.

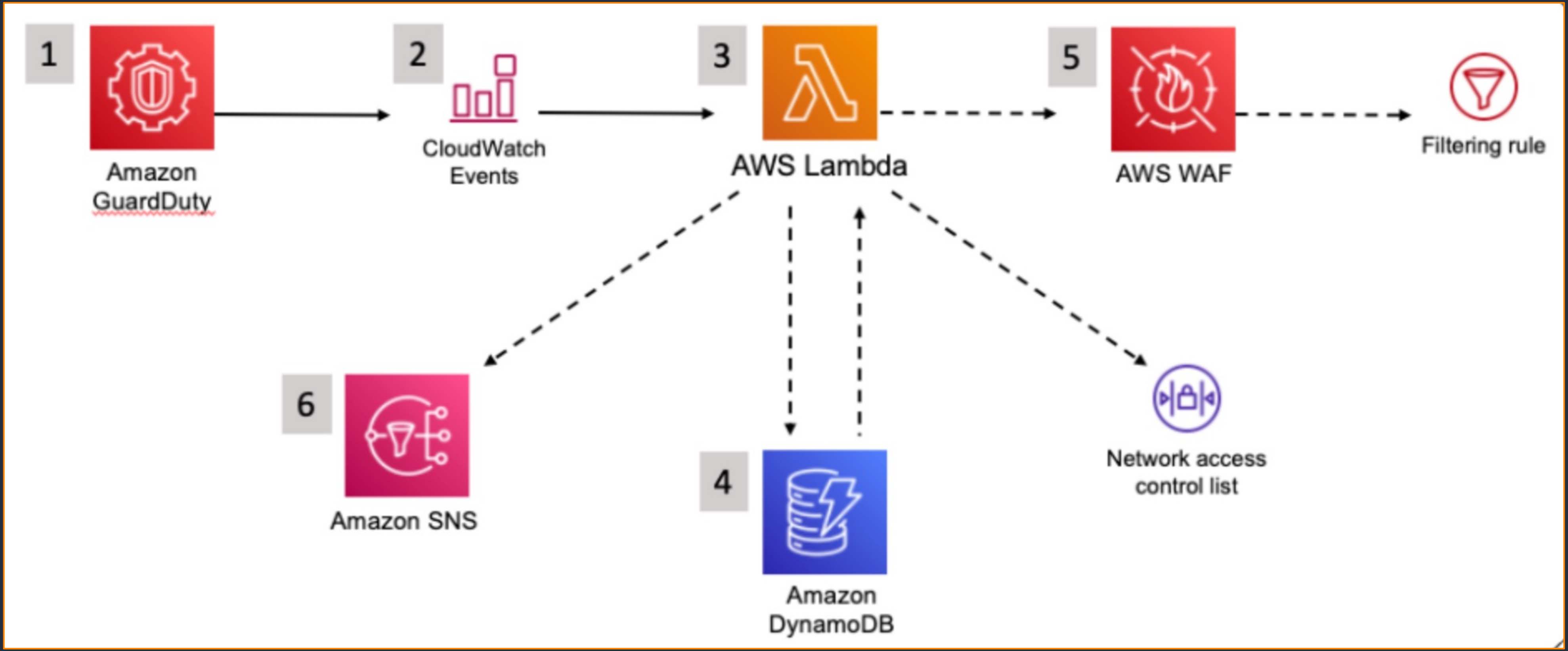
AWS Web Application Firewall (WAF):
Deploy in 3 easy steps

Find rules on
AWS WAF console or
AWS marketplace

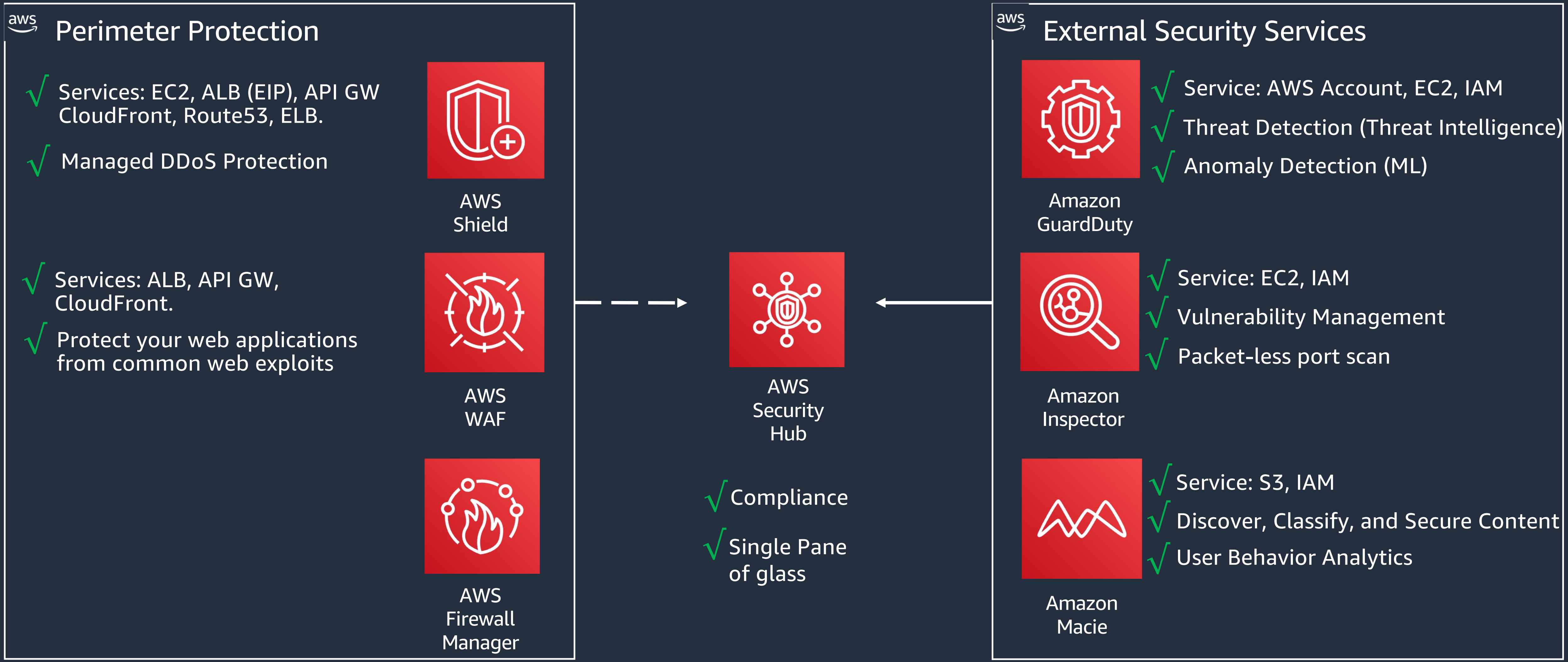
Click and
subscribe

Associate rules in
AWS WAF

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



Layered Security Services



Perimeter Protection

- √ Services: EC2, ALB (EIP), API GW CloudFront, Route53, ELB.
- √ Managed DDoS Protection

AWS Shield

- √ Services: ALB, API GW, CloudFront.
- √ Protect your web applications from common web exploits

AWS WAF

AWS Firewall Manager

AWS Security Hub

- √ Compliance
- √ Single Pane of glass

External Security Services

Amazon GuardDuty

- √ Service: AWS Account, EC2, IAM
- √ Threat Detection (Threat Intelligence)
- √ Anomaly Detection (ML)

Amazon Inspector

- √ Service: EC2, IAM
- √ Vulnerability Management
- √ Packet-less port scan

Amazon Macie

- √ Service: S3, IAM
- √ Discover, Classify, and Secure Content
- √ User Behavior Analytics

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

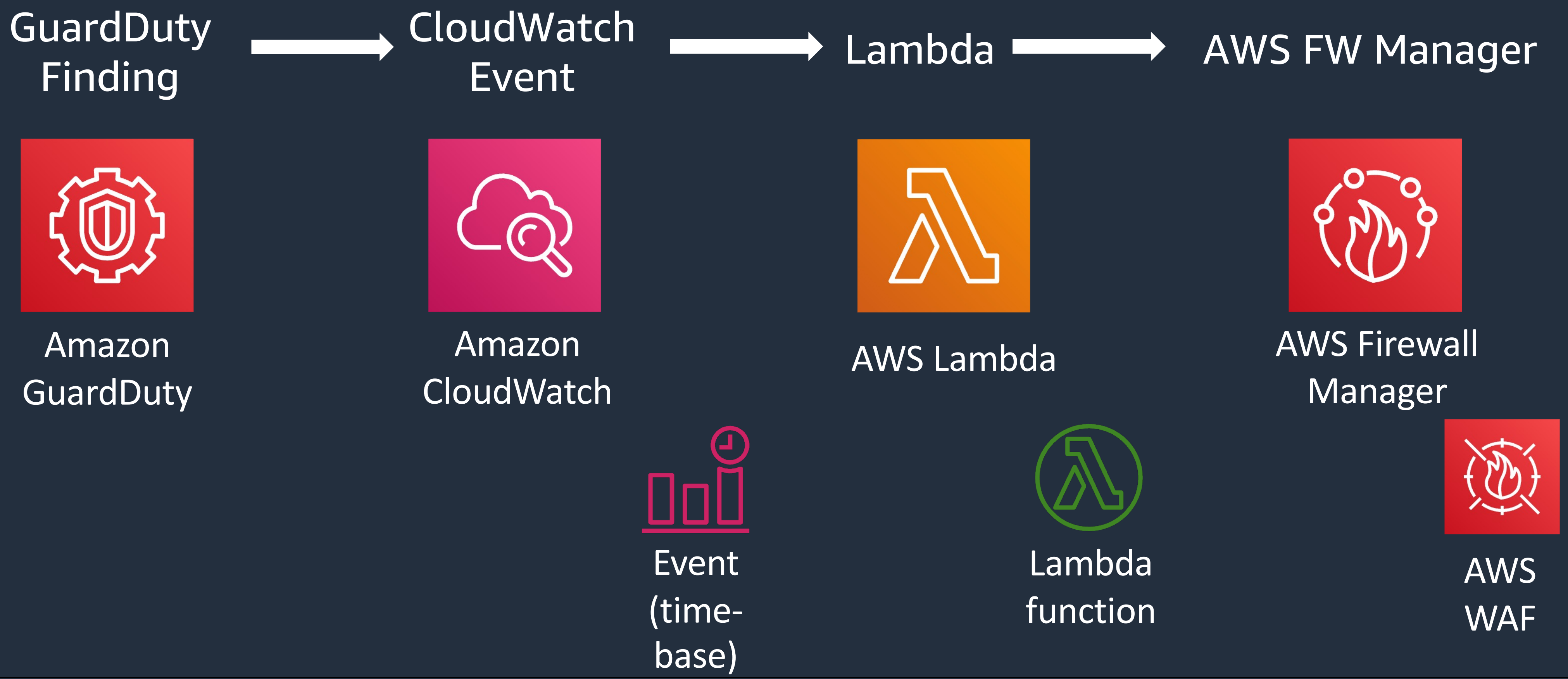
Enable Rapid Response to Internet Attacks at scale

Security administrator 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



GuardDuty Finding → CloudWatch Event → Lambda → AWS FW Manager

Amazon GuardDuty

Amazon CloudWatch

AWS Lambda

AWS Firewall Manager

Event (time-base)

Lambda function

AWS WAF

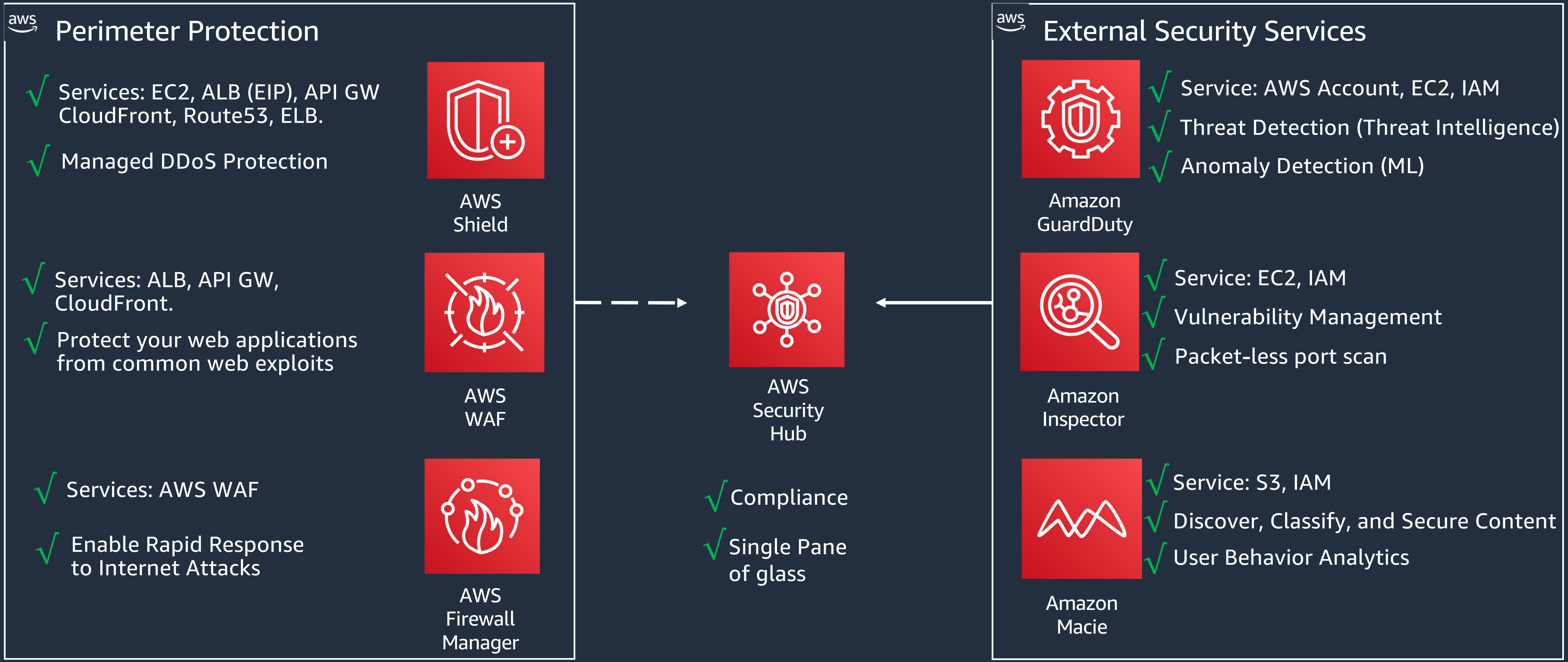
Typical Use Cases
Deploy OWASP rules for PCI compliance

- 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



Perimeter Protection

√ Services: EC2, ALB (EIP), API GW CloudFront, Route53, ELB.

√ Managed DDoS Protection

AWS Shield

√ Services: ALB, API GW, CloudFront.

√ Protect your web applications from common web exploits

AWS WAF

√ Services: AWS WAF

√ Enable Rapid Response to Internet Attacks

AWS Firewall Manager

AWS Security Hub

√ Compliance

√ Single Pane of glass

External Security Services

Amazon GuardDuty

√ Service: AWS Account, EC2, IAM

√ Threat Detection (Threat Intelligence)

√ Anomaly Detection (ML)

Amazon Inspector

√ Service: EC2, IAM

√ Vulnerability Management

√ Packet-less port scan

Amazon Macie

√ Service: S3, IAM

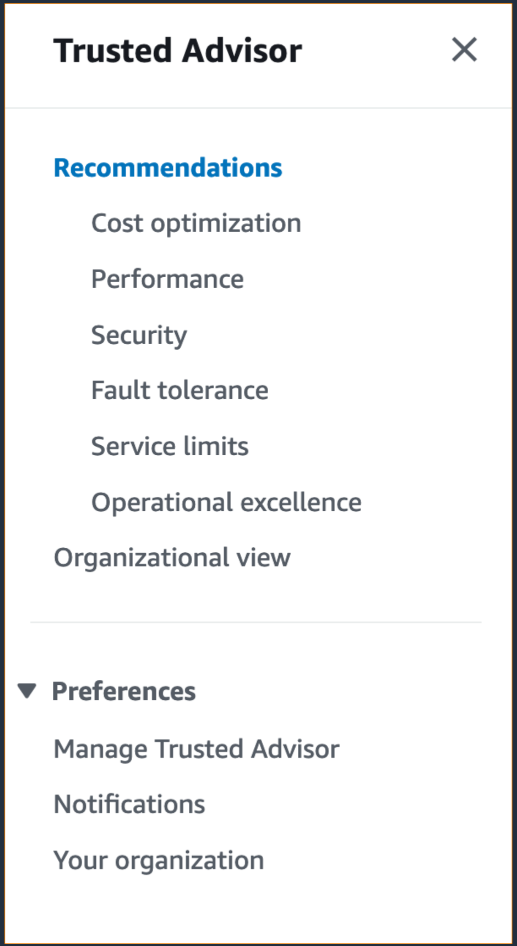
√ Discover, Classify, and Secure Content

√ User Behavior Analytics

AWS Trusted Advisor

AWS Trusted Advisor

LEVERAGE TRUSTED ADVISOR TO ANALYZE YOUR AWS RESOURCES FOR BEST PRACTICES FOR AVAILABILITY, COST, PERFORMANCE, AND SECURITY.



Trusted Advisor ✕

Recommendations

- Cost optimization
- Performance
- Security
- Fault tolerance
- Service limits
- Operational excellence

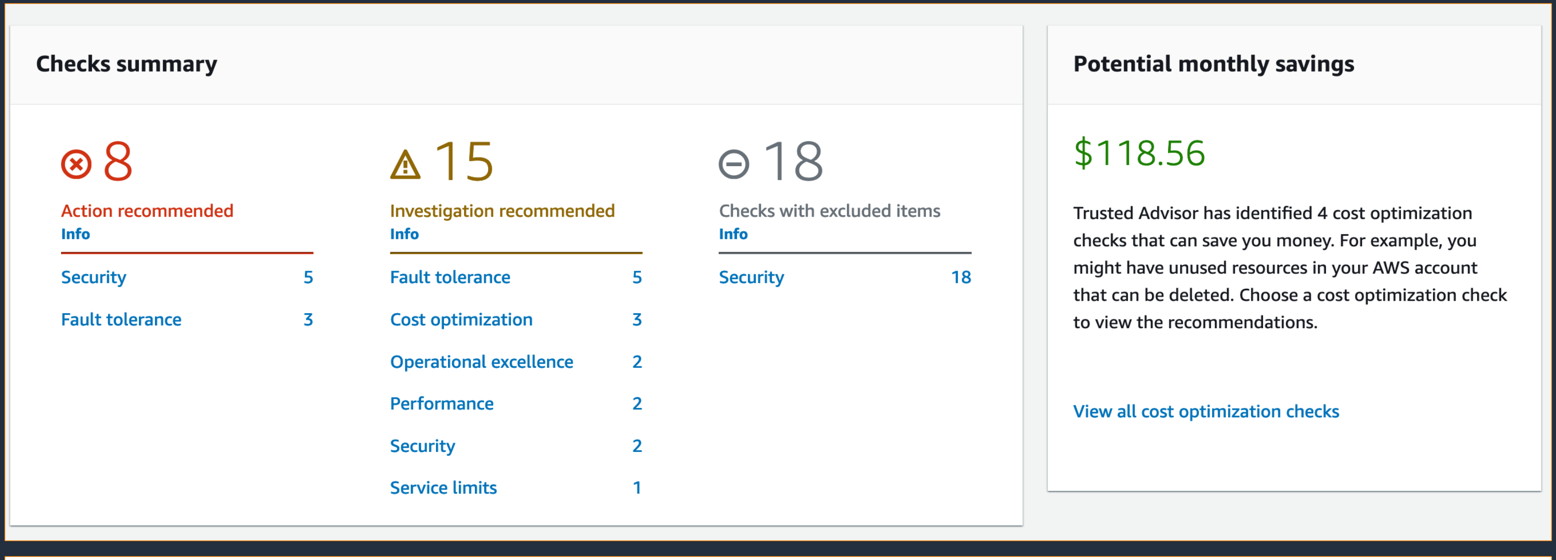
Organizational view

▼ **Preferences**

Manage Trusted Advisor

Notifications

Your organization



Checks summary

⊗ 8

Action recommended

Info

Security	5
Fault tolerance	3

⚠ 15

Investigation recommended

Info

Fault tolerance	5
Cost optimization	3
Operational excellence	2
Performance	2
Security	2
Service limits	1

⊖ 18

Checks with excluded items

Info

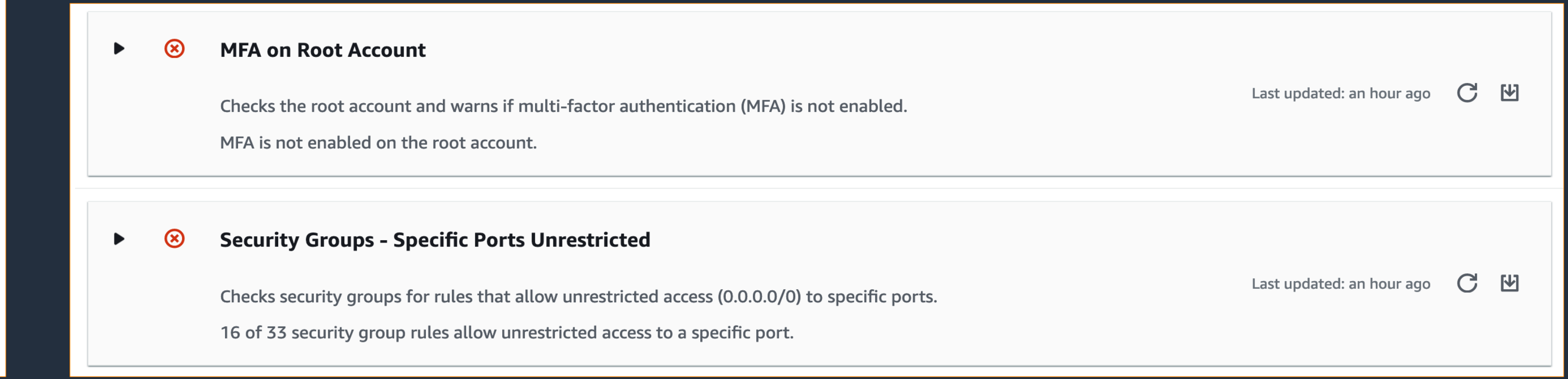
Security	18

Potential monthly savings

$118.56

Trusted Advisor has identified 4 cost optimization checks that can save you money. For example, you might have unused resources in your AWS account that can be deleted. Choose a cost optimization check to view the recommendations.

View all cost optimization checks



▶ ⊗ **MFA on Root Account**

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

MFA is not enabled on the root account.

Last updated: an hour ago

▶ ⊗ **Security Groups - Specific Ports Unrestricted**

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

16 of 33 security group rules allow unrestricted access to a specific port.

Last updated: an hour ago

Security Health Improvement Program (SHIP)

Security Health Improvement Program (SHIP)

Improving Security Health on AWS

Which AWS security services should be prioritized?

Does my company adhere to AWS security best practices?

How can we continuously improve security?

Thank you!

Anuraj Pahuja
anurajpa@amazon.com

Rohan Roberts
rohrober@amazon.com

Please take the survey:

Security is top priority