



SF LEARNING DAY

Security is Top Priority

Lana Lee, CISSP (she/her)

AWS Solutions Architect, WWPS

lanaaa@amazon.com

Agenda

- Introduction
- AWS Layered Security Services
- Best Practices for Ransomware Protection

Introduction

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

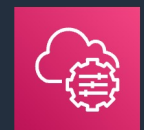


Compliance

AWS Artifact

AWS Audit Manager

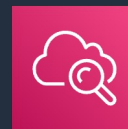
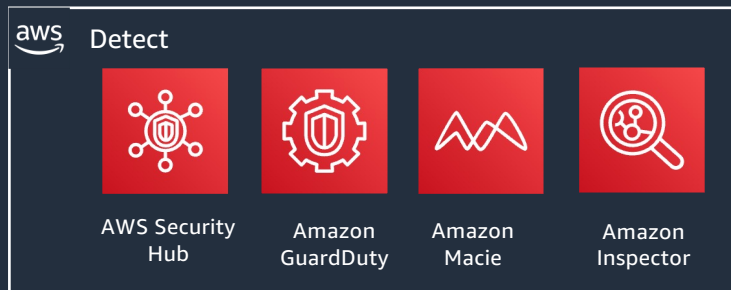
Layered Security Services



AWS Systems Manager



AWS Config



Amazon CloudWatch



AWS Lambda

Automate

Identify



Protect



Detect



Respond



Recover



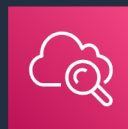
Snapshot



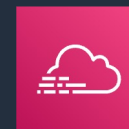
Archive



Investigate



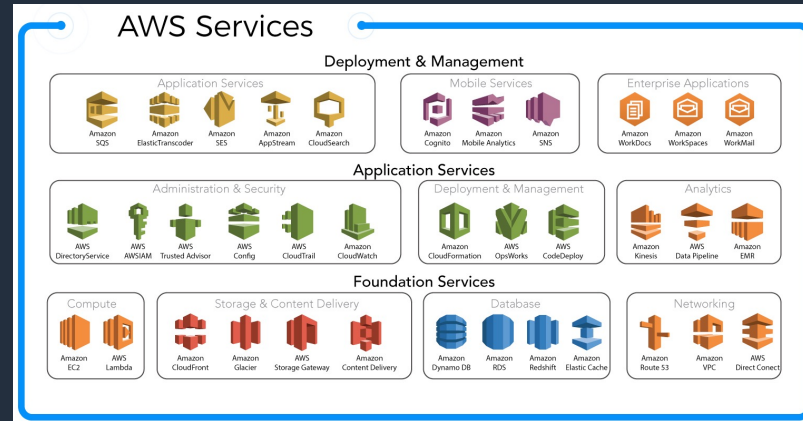
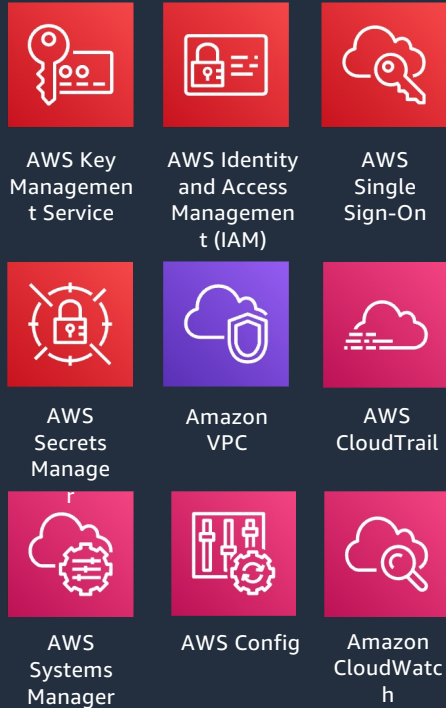
Amazon CloudWatch



AWS CloudTrail

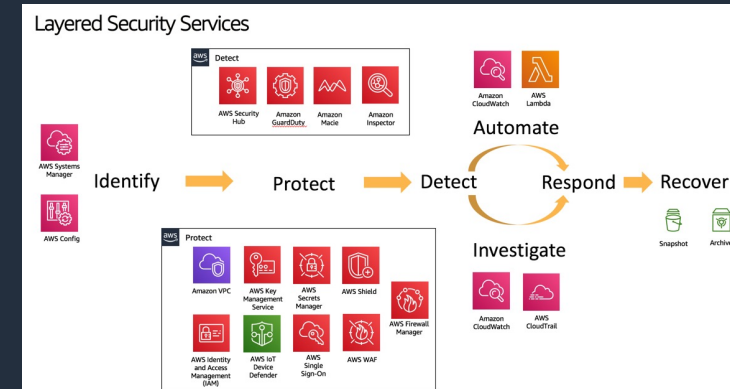
Our mental model for security services: Two types

Foundational Security Services



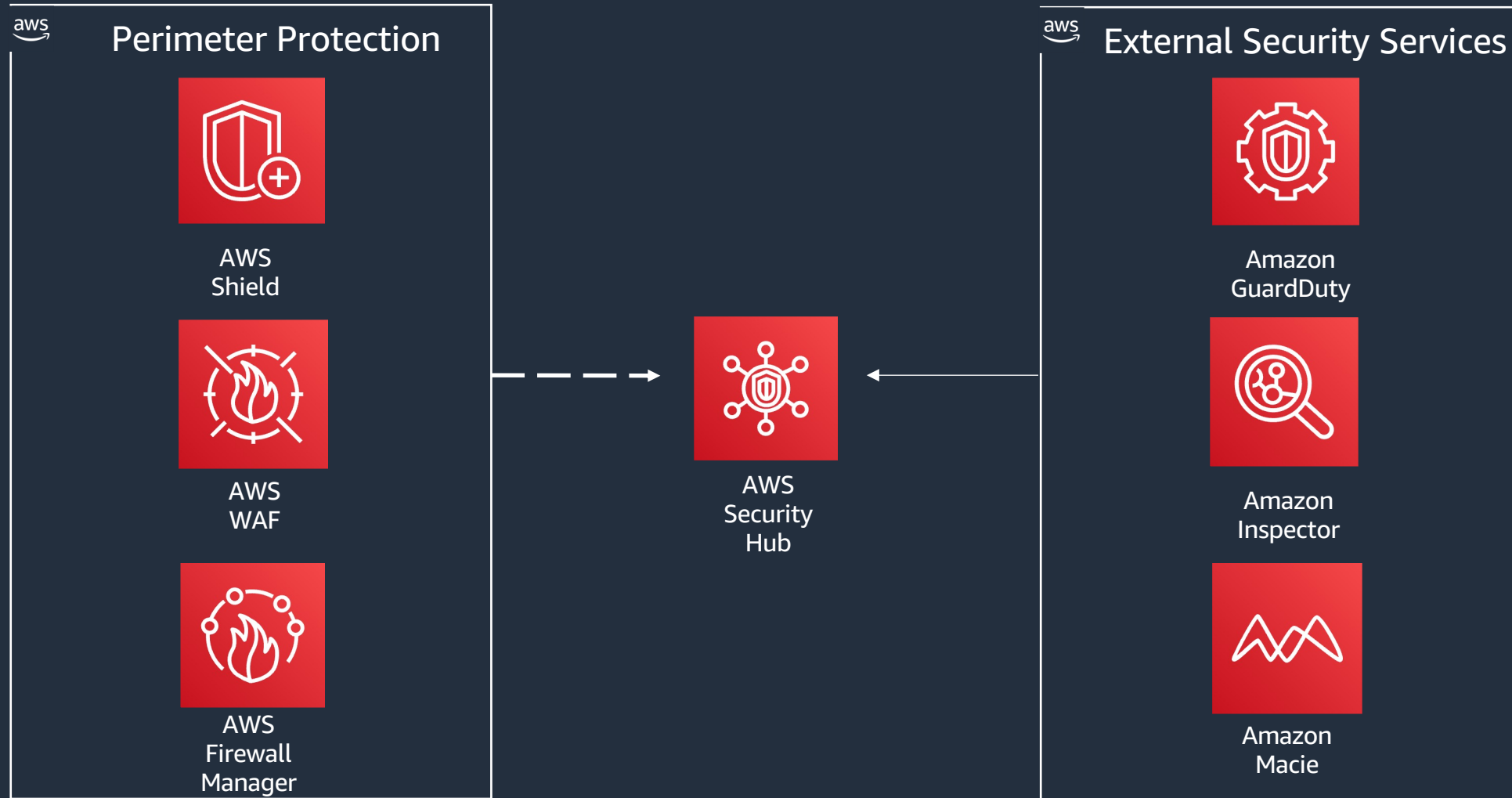
Consumed & integrated workload by workload

Layered Security Services



"Once" applies to all workloads.

Layered Security Services



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?



Amazon GuardDuty

Threat Detection Types

Bitcoin Mining



Instance Compromise



Account Compromise



Total of 47 detections



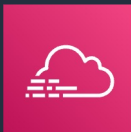
Data Sources



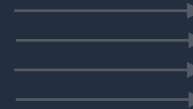
VPC flow logs



DNS Logs



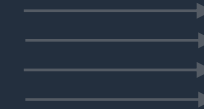
CloudTrail Events



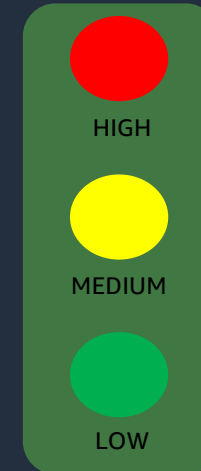
Threat intelligence



Anomaly Detection (ML)



Findings



AWS Security Hub



SIEM



Respond

Automate with integrated services

Automated threat remediation

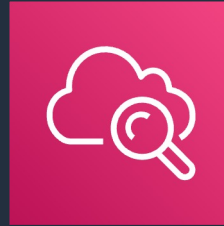
GuardDuty
Finding



Amazon
GuardDuty



CloudWatch
Event



Amazon
CloudWatch



Lambda



AWS Lambda

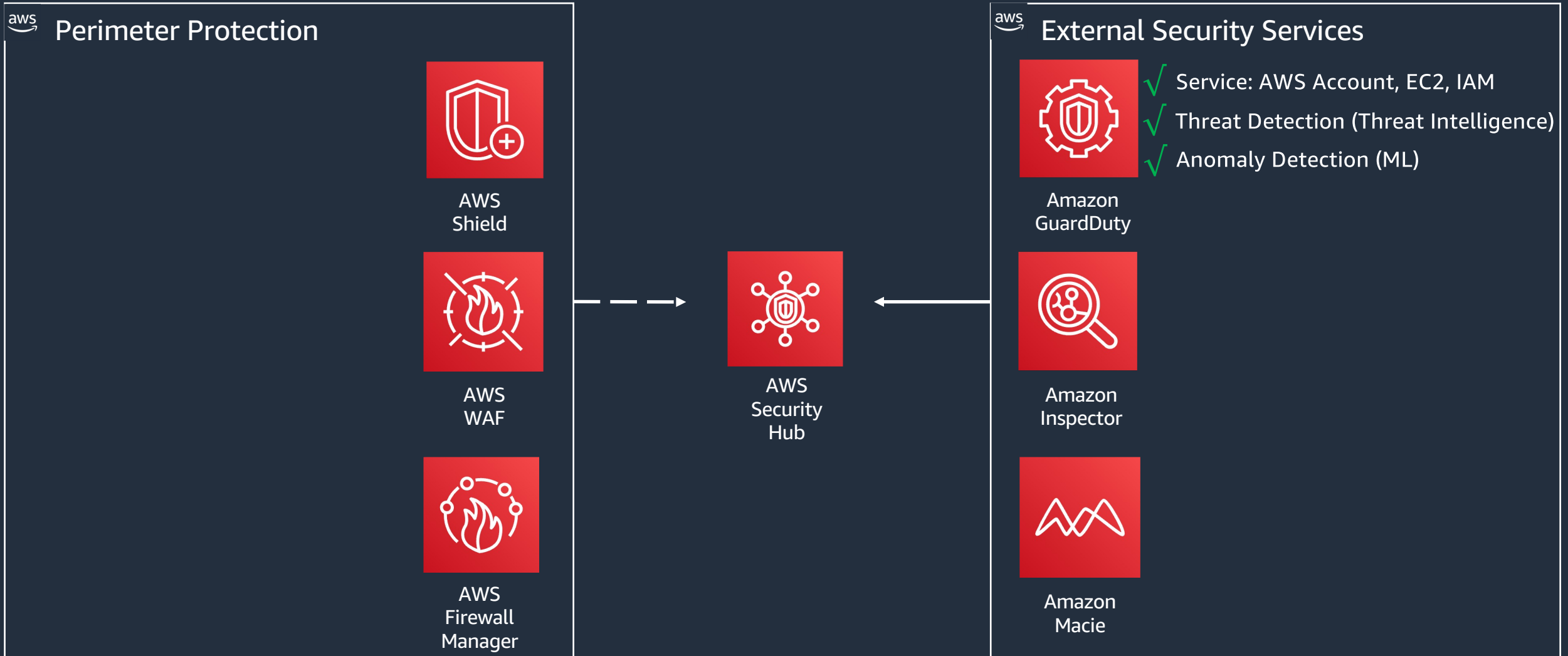


Event (time-base)



Lambda
function

Layered Security Services



Amazon Inspector

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

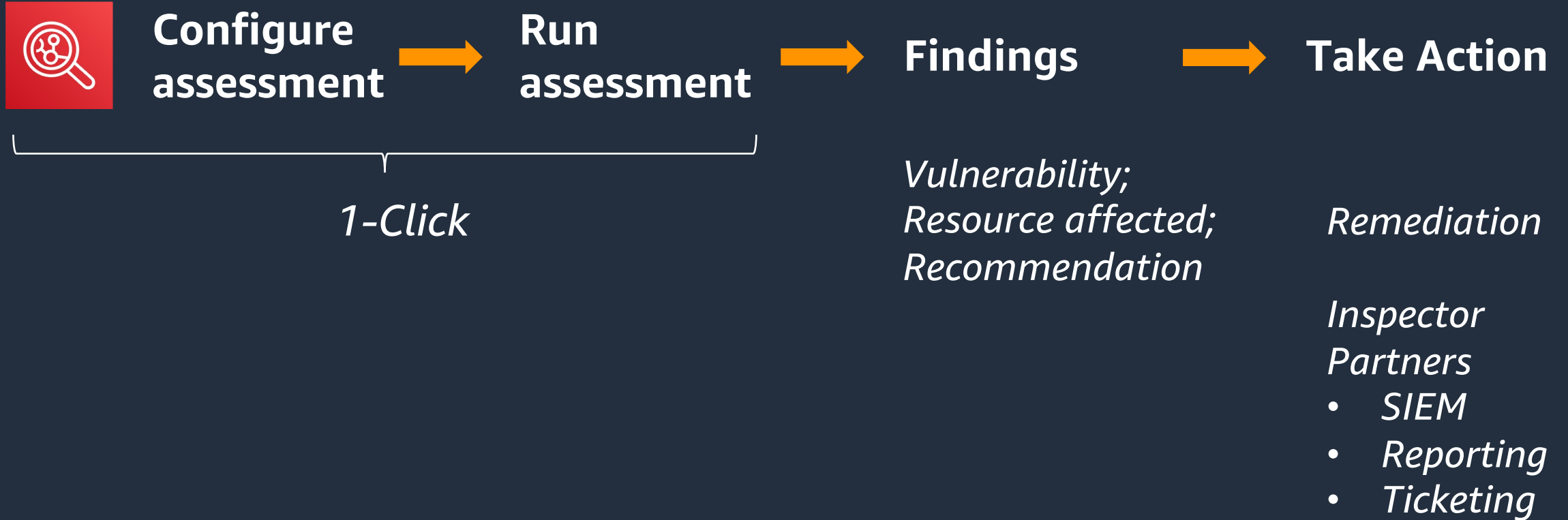
Agentless network assessments

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?



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

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

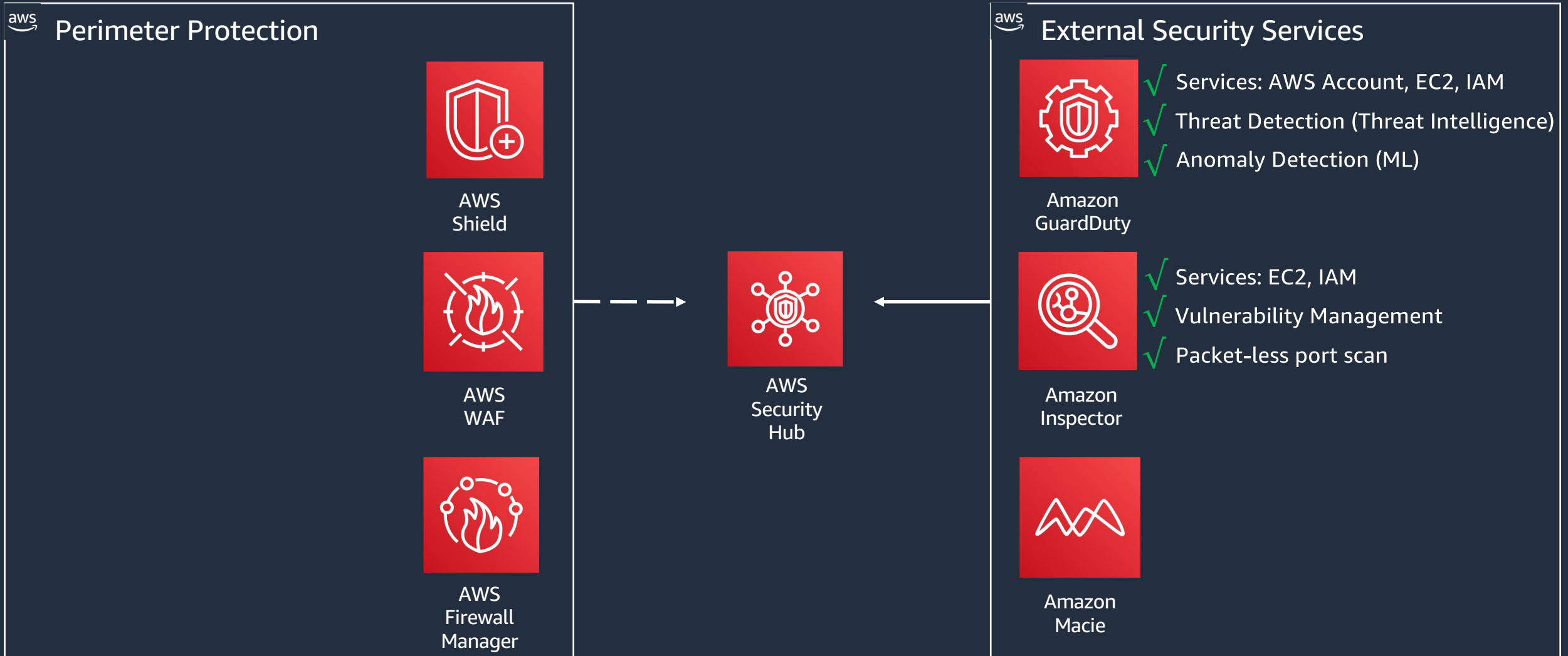
Amazon Inspector

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



Amazon Macie

External Security Services

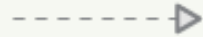


How does Amazon Macie work?

HOW MACIE WORKS



Enroll your AWS Account
with Amazon Macie



Select the Buckets for
Content Discovery and
Classification

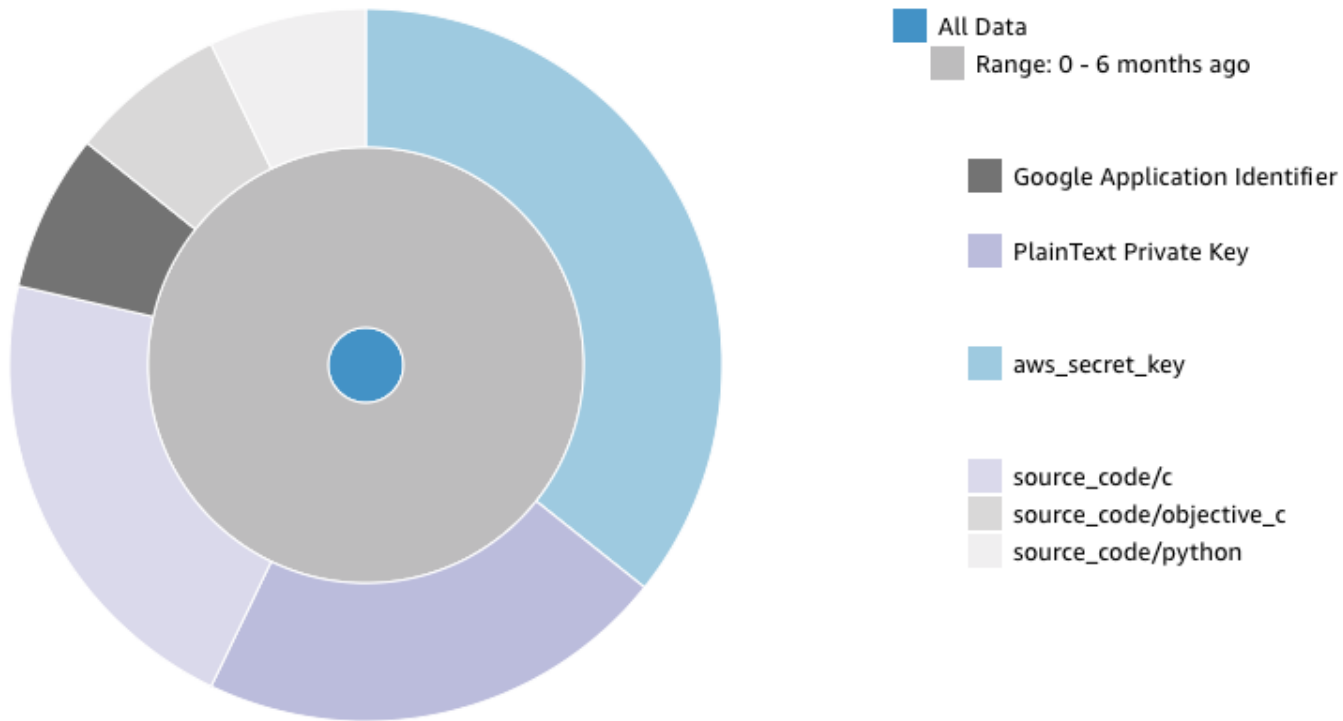


Review your Alerts in the
Amazon Macie
Dashboard

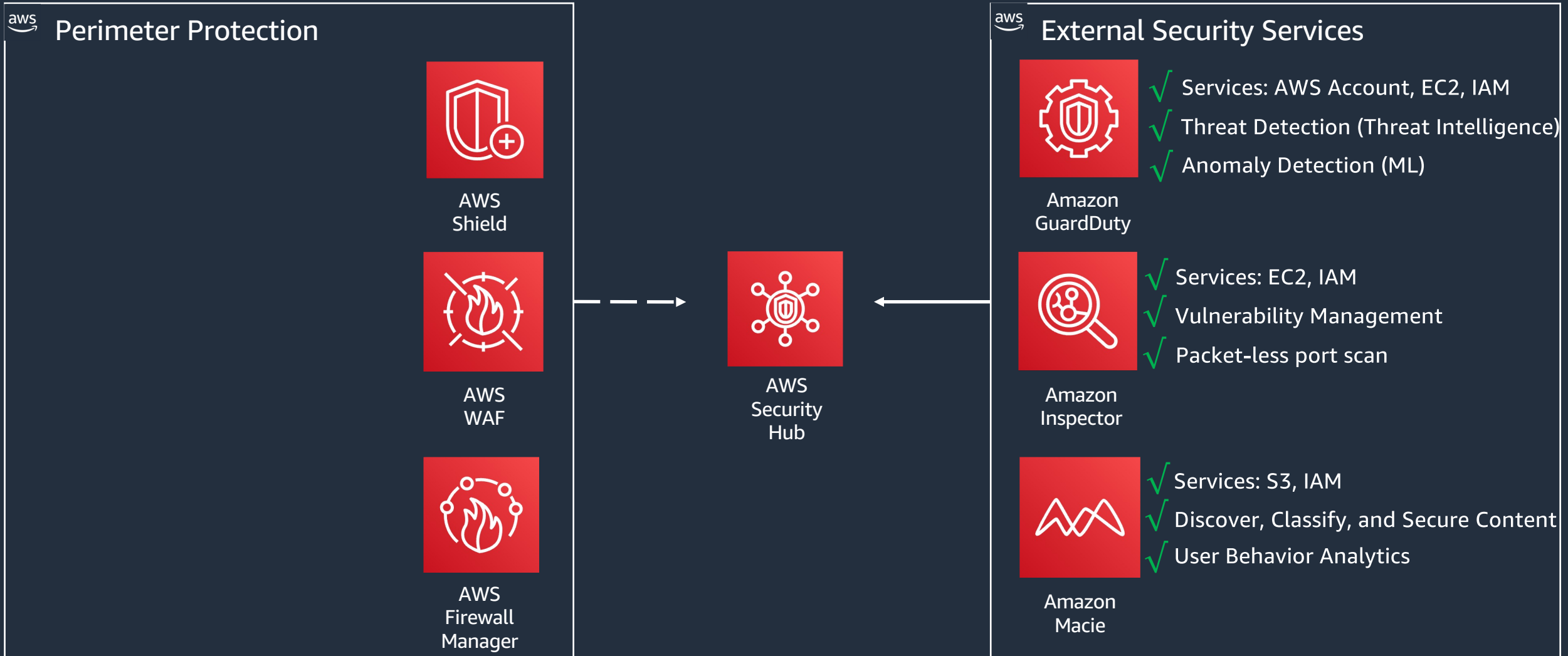
How does Macie work?

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

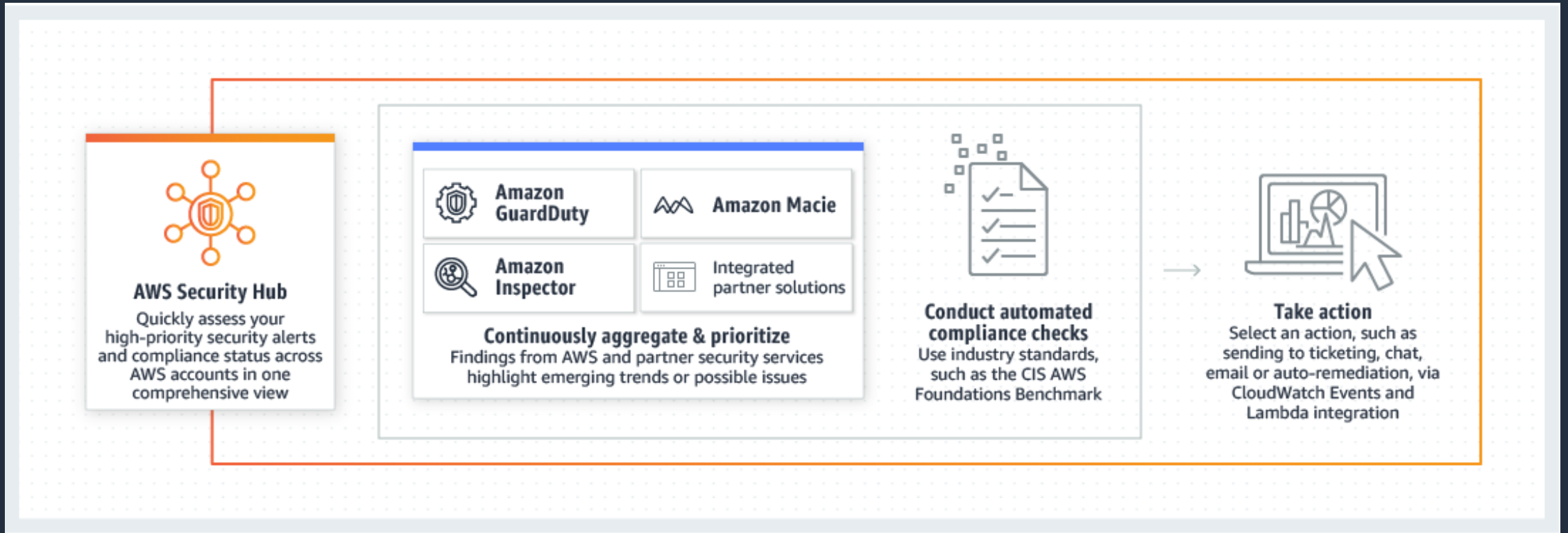


AWS Security Hub

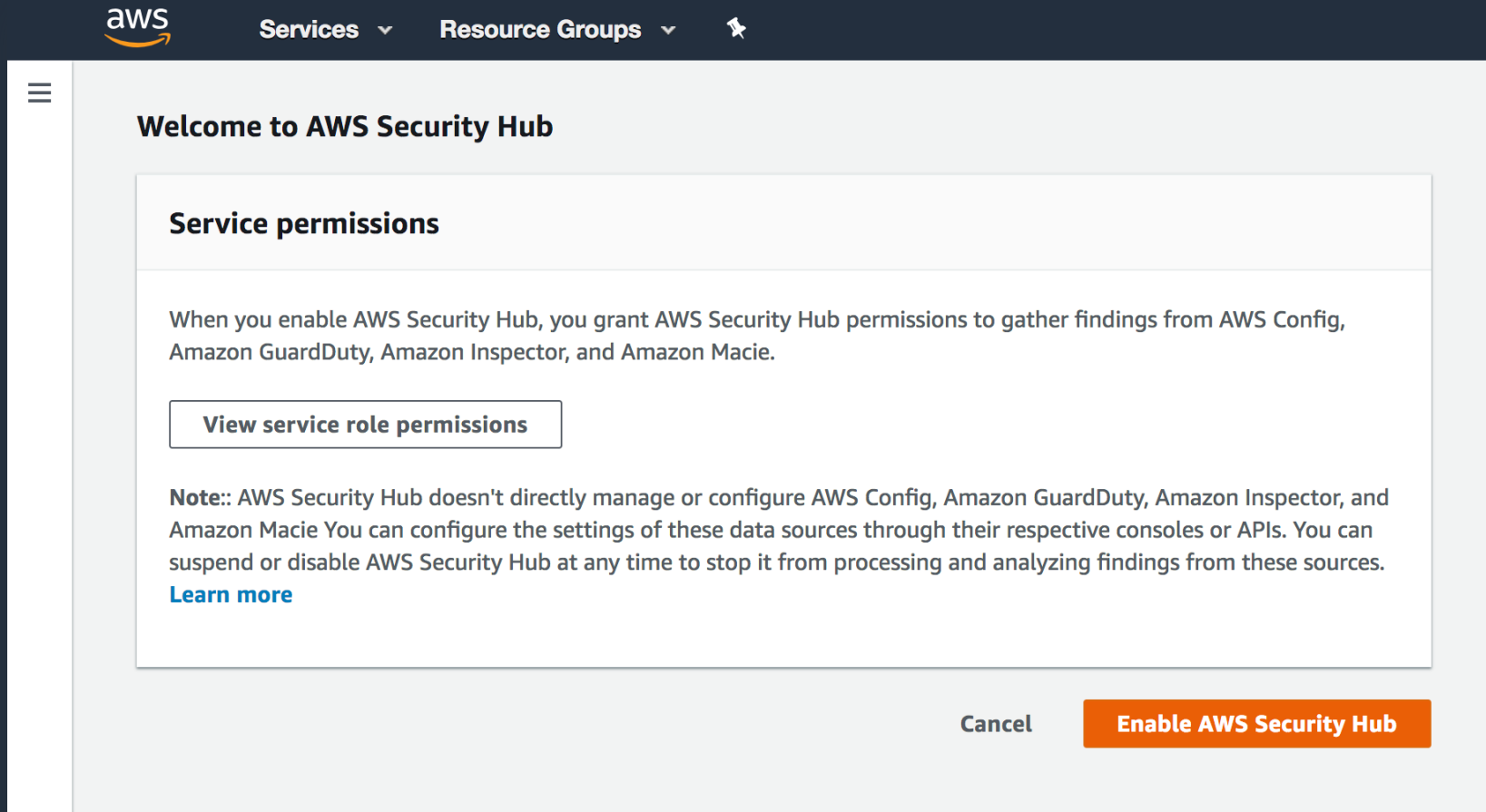
External Security Services




How does AWS Security Hub work?



Getting Started - AWS Security Hub work?



AWS Security Hub – Partner Integrations



Services ▾

Resource Groups ▾

✦

SecurityHubDemo/shllomie-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](#)




awsmarketplace

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](#)




awsmarketplace

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](#)





awsmarketplace

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.






AWS Security Hub – Partner Integrations

Firewalls	    	Endpoint	   
Vulnerability	  	Compliance	   
SOAR	  	MSSP	  
SIEM	  	Other	  


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.



<


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



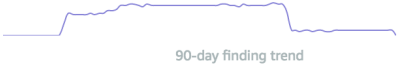
21 current result

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



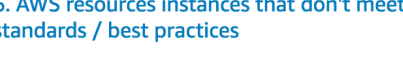
0 current result

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

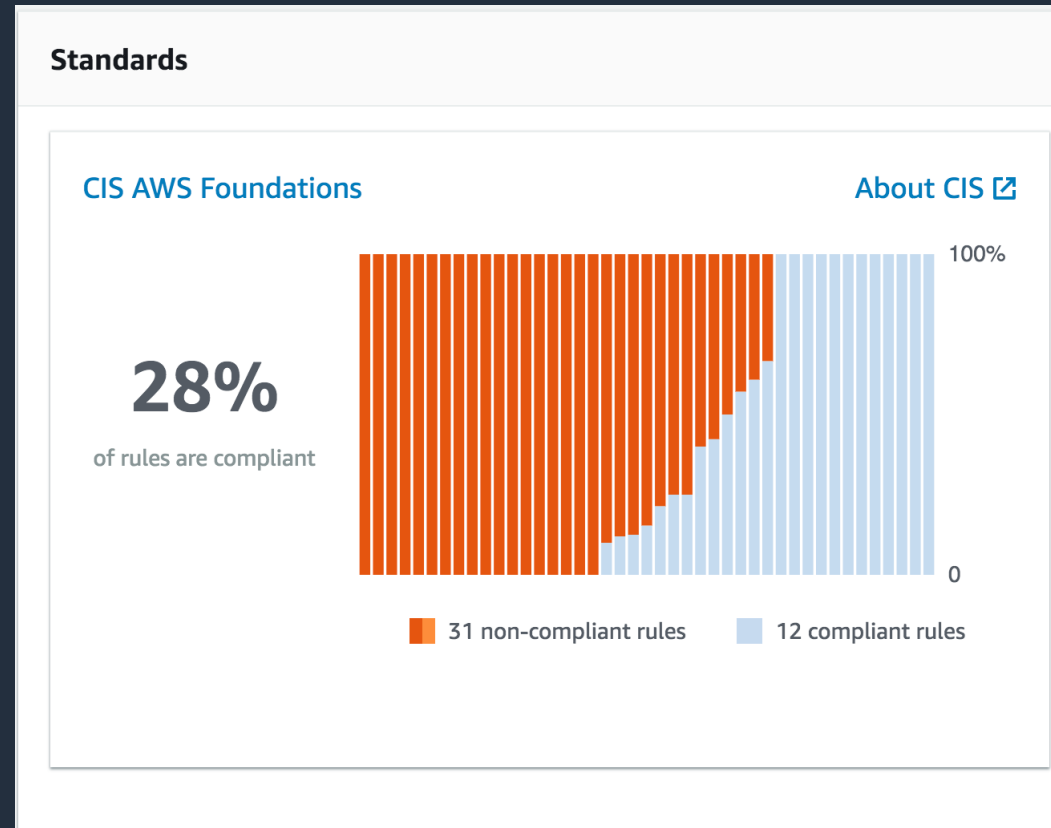


23 current result

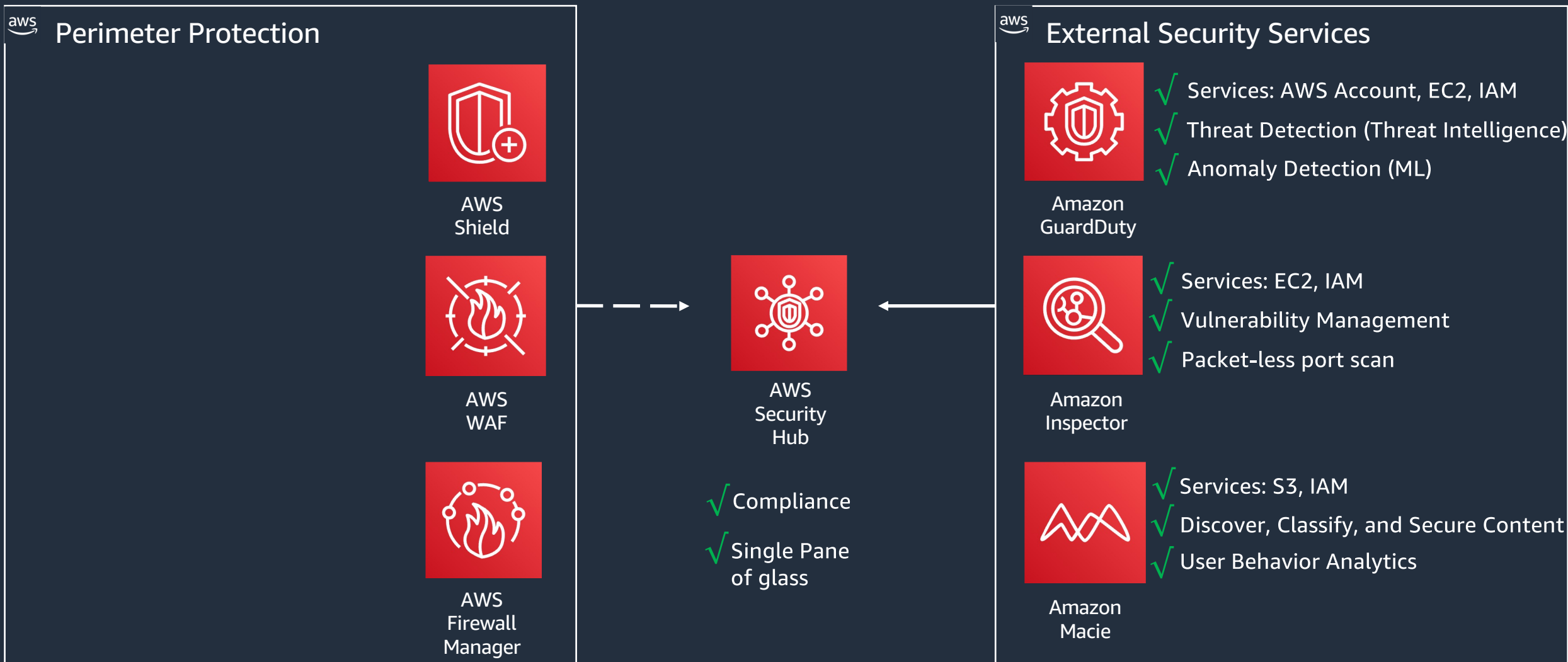


© 2024, Amazon Web Services, Inc. or its affiliates.

AWS Security Hub – Compliance Checks (CIS)



Layered Security Services



Perimeter Protection





AWS 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.

[Go to AWS WAF](#)

[Learn more](#)



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.

[Go to AWS Shield](#)

[Learn more](#)



AWS Firewall Manager

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

[Go to AWS Firewall Manager](#)

[Learn more](#)



AWS Shield Advanced Perimeter Protection



AWS Shield

A Managed DDoS Protection Service

There are two tiers of AWS Shield:

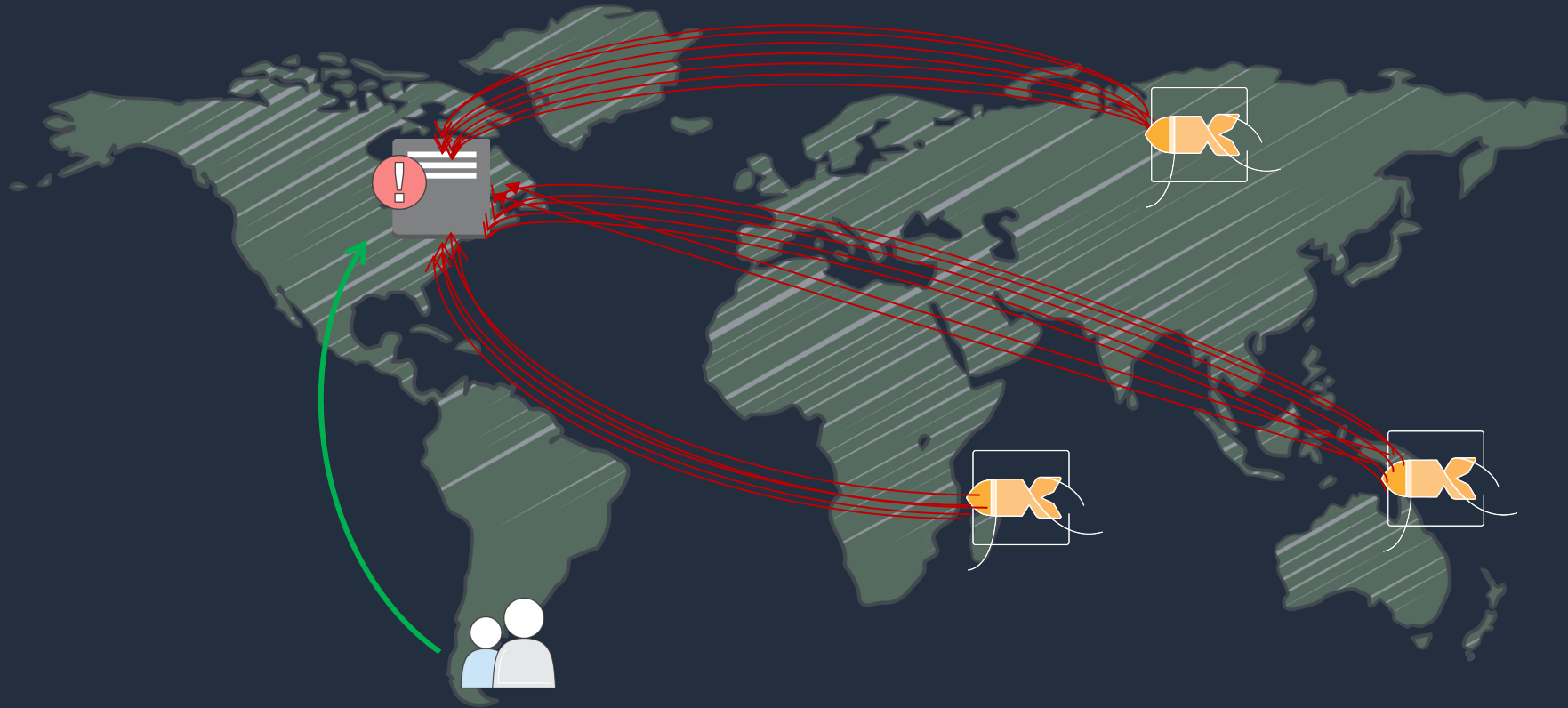
- AWS Shield Standard
- AWS Shield **Advanced**



AWS Shield

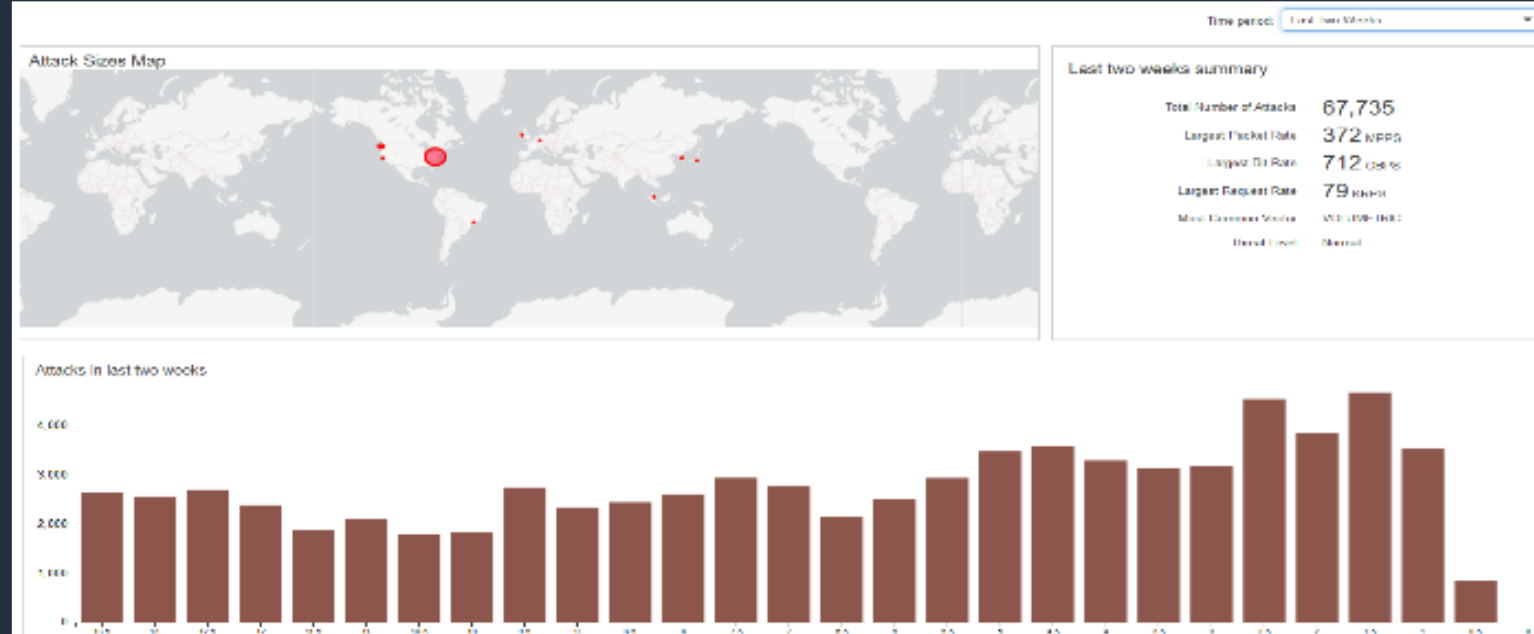
AWS Shield Advanced - DDoS Attack threats and Trends:

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

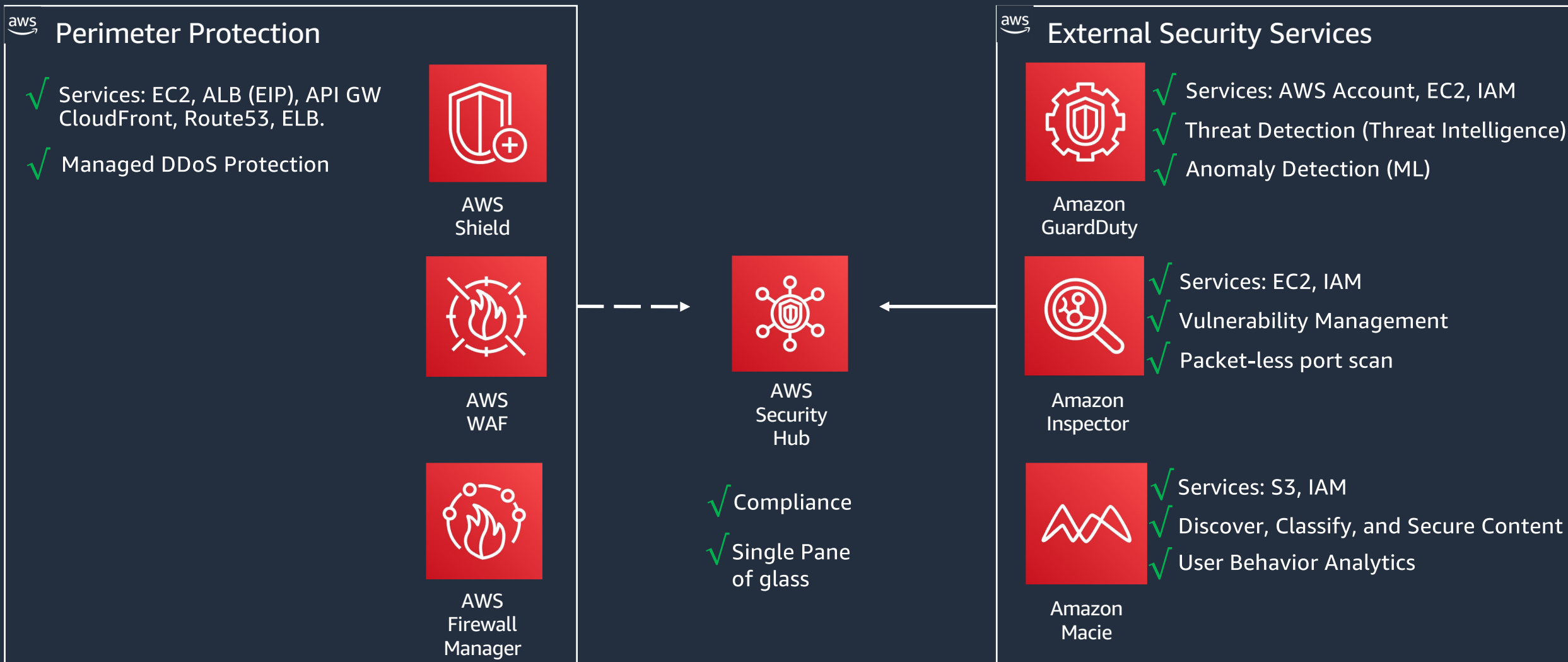
Economic Benefits

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

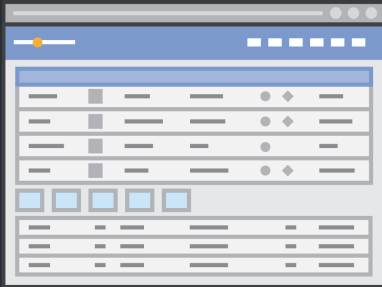
Protect Your Web Application with Pre-configured Rules on AWS WAF

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.

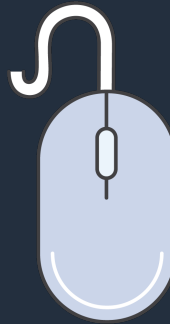


Get Started With AWS WAF

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



Find rules on
AWS WAF console or
AWS marketplace

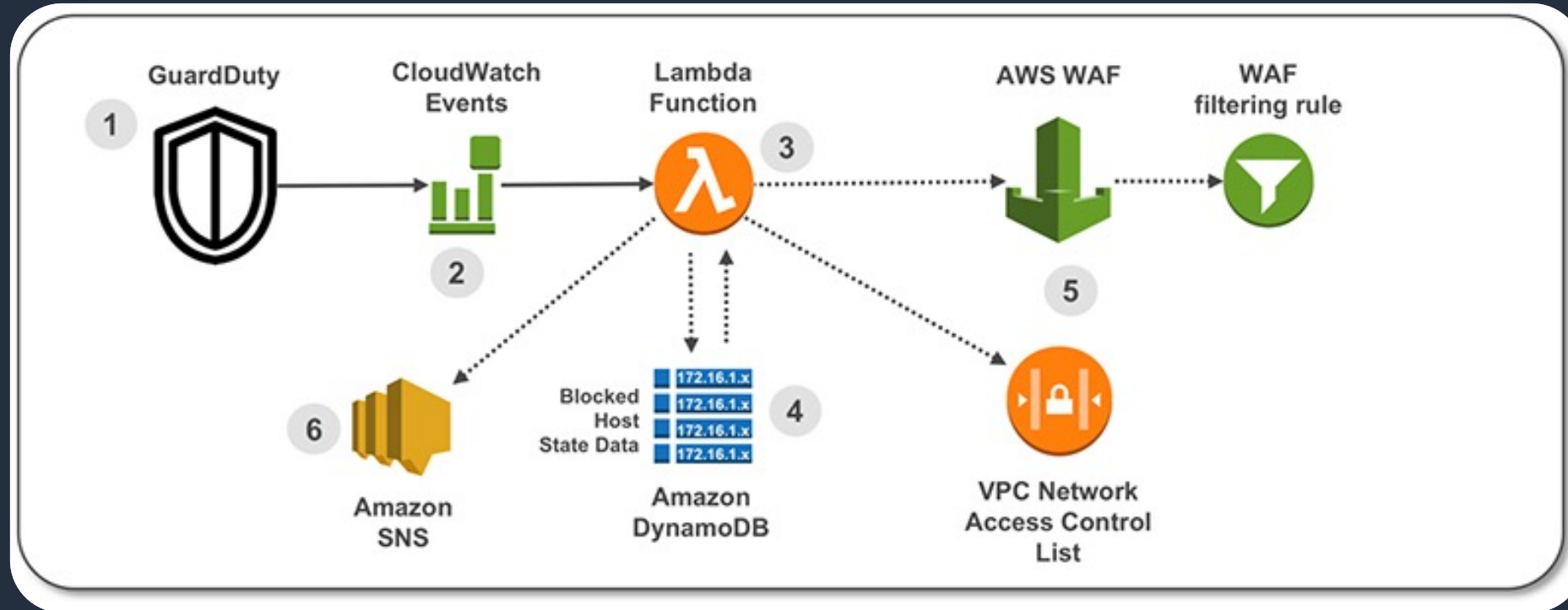


Click and
subscribe

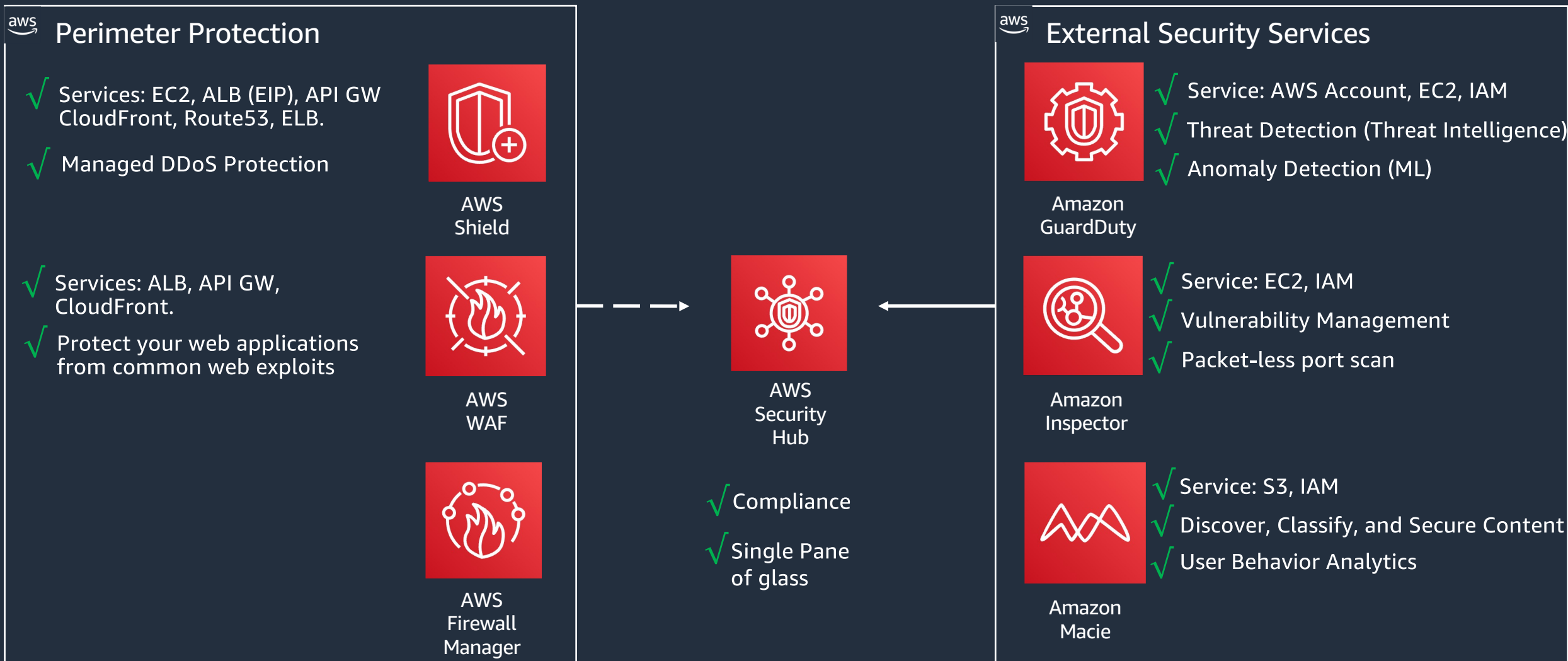


Associate rules in
AWS WAF

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

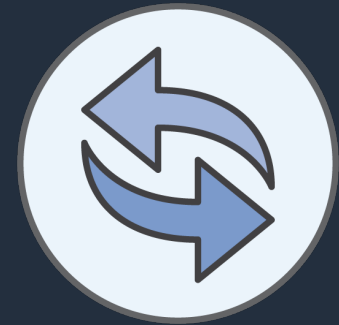


AWS Firewall Manager Key Benefits

Enable Rapid Response to Internet Attacks at scale

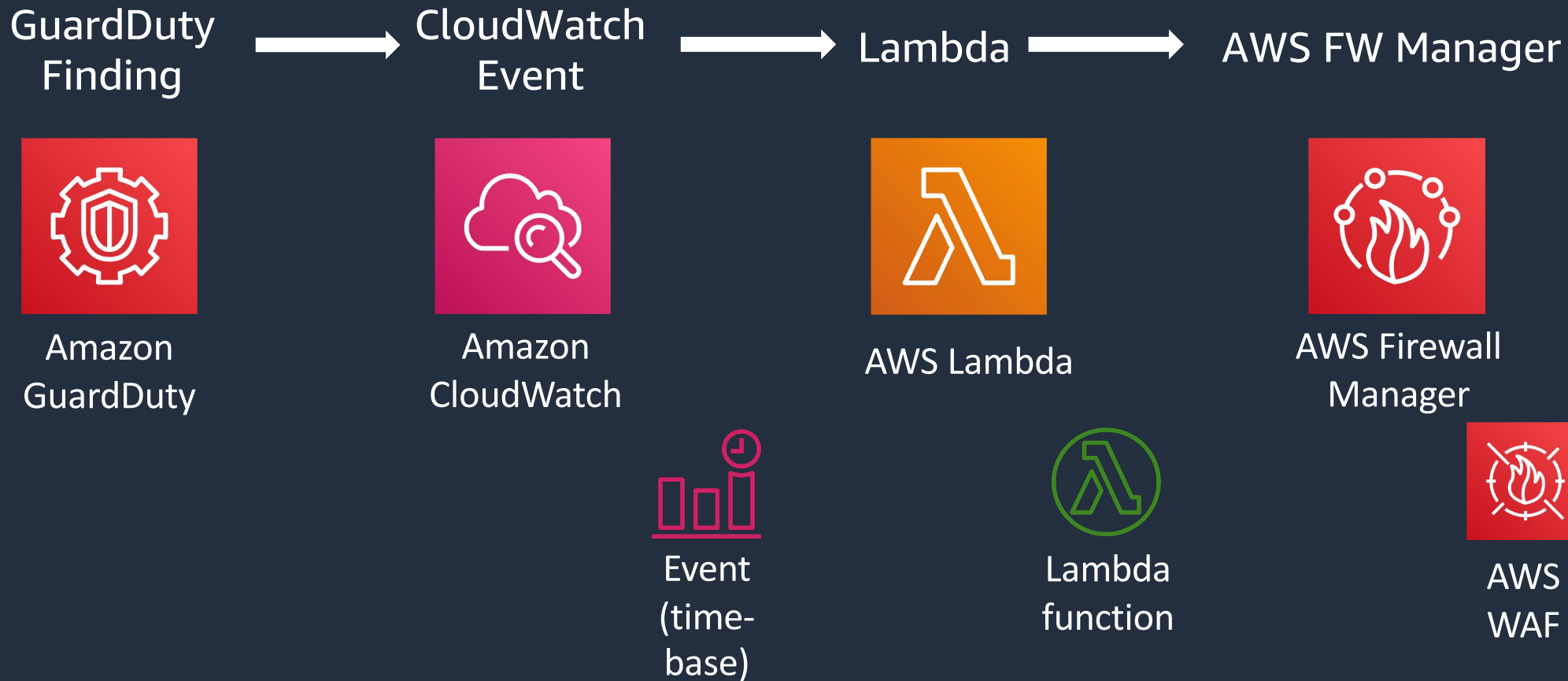
Security administrators have a single console to receive real-time threats, and respond within minutes

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

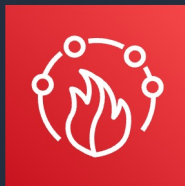
Automated threat remediation



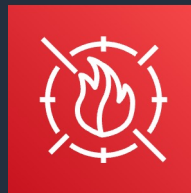
Typical Use Cases

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](#)

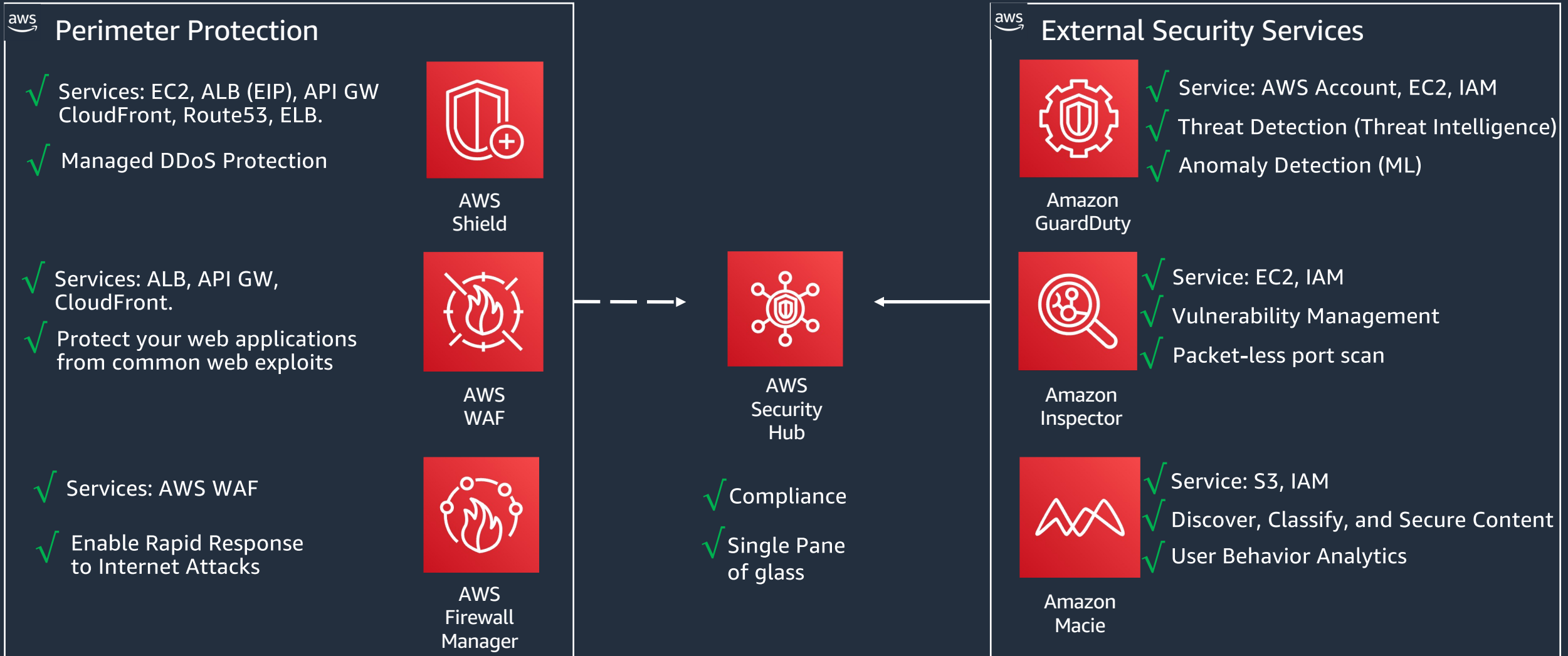


AWS
Firewall
Manager



AWS
WAF

Layered Security Services



Best Practices for Ransomware Protection

Ransomware threats

75% of IT organizations will face one or more **ransomware threats** by 2025

Gartner, "[Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware](#)"

Ransomware attacks grow, crippling cities and businesses

"Hackers are locking people out of their networks and demanding big payments to get back in. New data shows just how common and damaging the attacks have become."

[The New York Times](#)

Scripps enters fourth week of ransomware attack

"... the region's second-largest medical provider enters the fourth-straight week of an attack that snarled the organization's digital resources from scheduling to patient care"

[The San Diego Union-Tribune](#)

'Cybersecurity issue' forces systems shutdown at MGM hotels and casinos

"... multiple gambling machines at hotels had gone offline and that several guests were unable to charge anything to their rooms, make reservations or use their digital room keys."

[The New York Times](#)

Ransomware attack on Bose exposes employee SSNs and financial information

"The company was forced to notify New Hampshire officials after employees in the state had their information accessed"

[ZDNet](#)

NIST Cybersecurity Framework

is an industry standard . . .



IDENTIFY

Identify an organization's critical functions, assets, and processes, and how cybersecurity risks could disrupt them



PROTECT

Define safeguards necessary to protect critical infrastructure services



DETECT

Implement the right measures to identify threats and cyber risks promptly



RESPOND

Define the measures necessary to react to an identified threat



RECOVER

Strategic plans to restore and recover any capabilities damaged during a cybersecurity incident

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

NIST Cybersecurity Framework

is an industry standard . . .
but most companies lack a
reliable data protection and
recovery strategy



IDENTIFY

Identify an organization's critical functions, assets, and processes, and how cybersecurity risks could disrupt them



PROTECT

Define safeguards necessary to protect critical infrastructure services



DETECT

Implement the right measures to identify threats and cyber risks promptly



RESPOND

Define the measures necessary to react to an identified threat



RECOVER

Strategic plans to restore and recover any capabilities damaged during a cybersecurity incident

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

Strategy Formation

What is the most important data that we want to protect?

Should the recovery of some data be prioritized over others?

What is an acceptable recovery time?

NIST Cybersecurity Framework

- Industry standard to manage risks
- Most organizations struggle with a reliable data protection and resiliency strategy
- Industries are now prioritizing the 'Recover' function



Identify



Protect



Detect



Respond



Recover



AWS Systems Manager



AWS Config



Amazon VPC



AWS Key Management Service



AWS Secrets Manager



AWS Firewall Manager



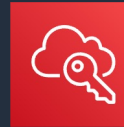
AWS Identity and Access Management (IAM)



AWS Shield



AWS IoT Device Defender



AWS Single Sign-On



AWS WAF



AWS Security Hub



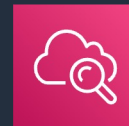
Amazon GuardDuty



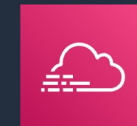
Amazon Macie



Amazon Inspector



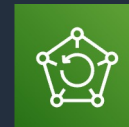
Amazon CloudWatch



AWS CloudTrail



Amazon Detective



AWS Backup



AWS Elastic Disaster Recovery

Data protection practices to meet resiliency objectives



Identify

Start with a strategy



Protect

Manage and control access to data

Implement data encryption

Automate continuous data protection



Detect

Manage data governance and compliance

Implement monitoring and alerting



Respond

Incorporate backup and recovery in incident response, DR, and BCP plans



Recover

Build a ransomware recovery strategy

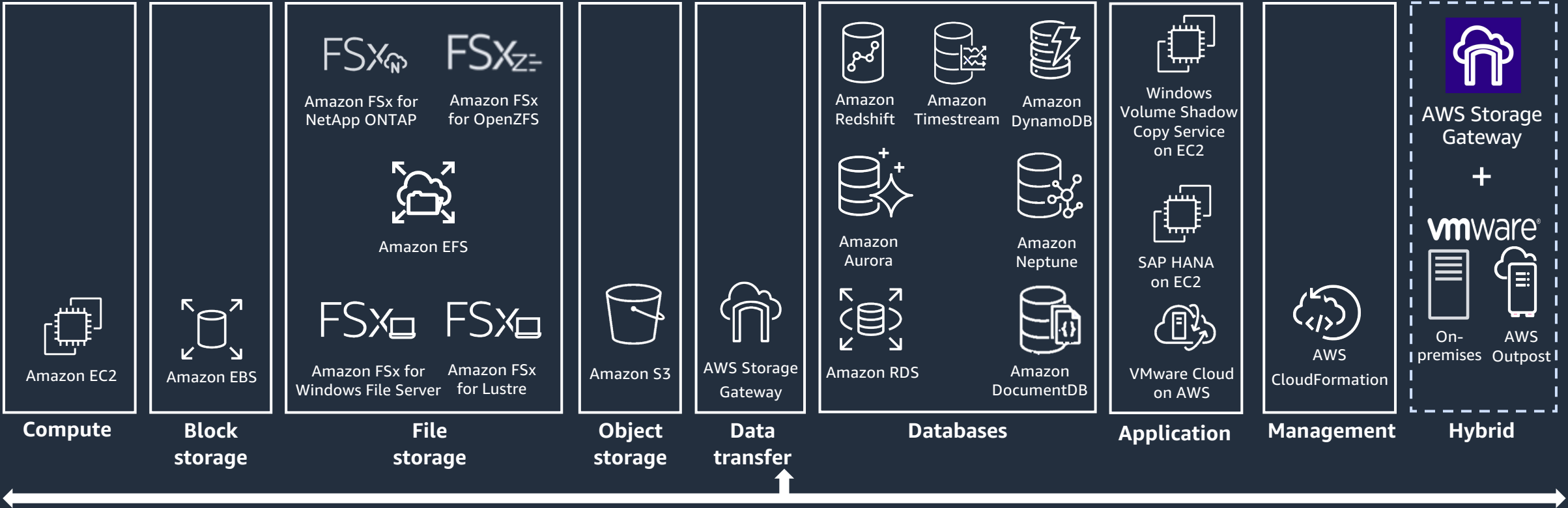
Test recovery capabilities

Overview of AWS Backup



AWS Backup

A fully **managed, policy-based** service that **centralizes and automates** data protection across multiple **AWS services** and **hybrid workloads** with data protection **compliance analytics and insights**



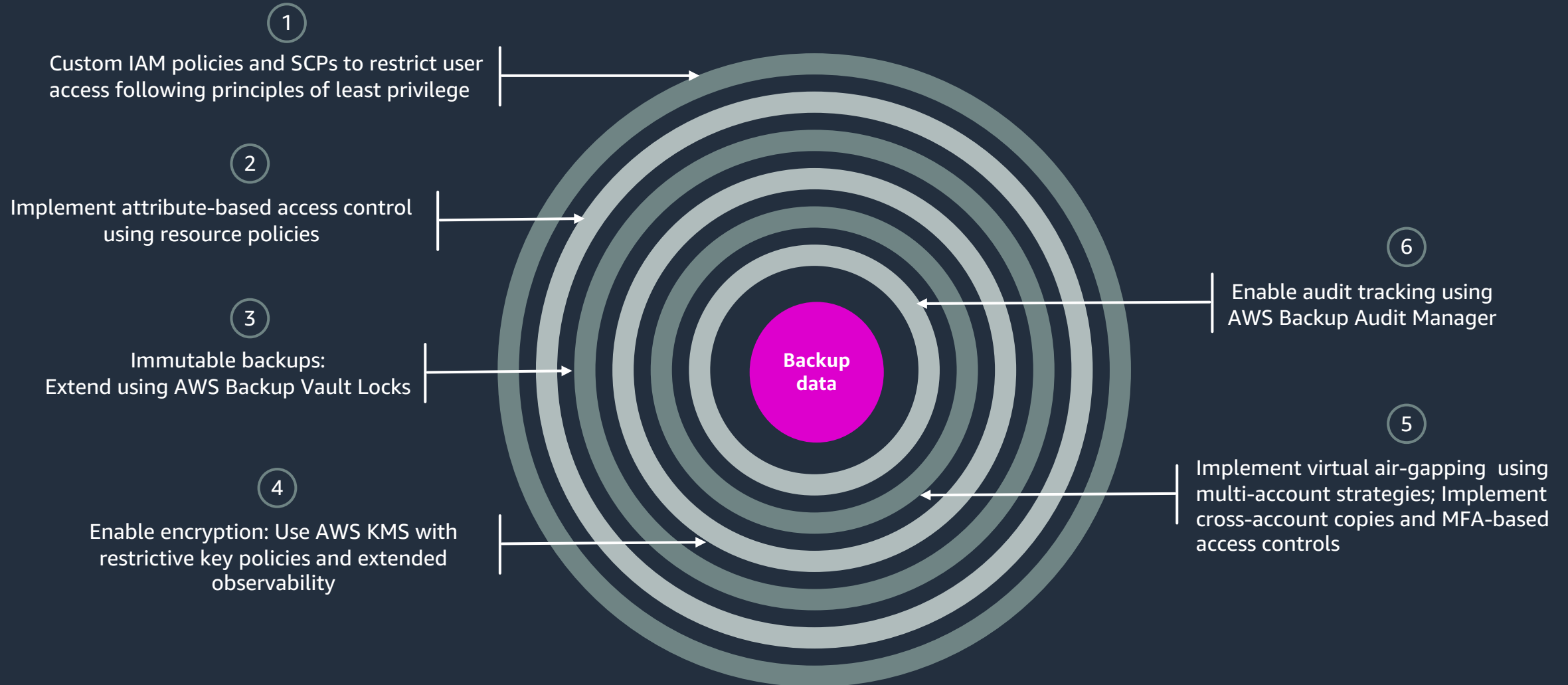
Monitoring, auditing, reporting
© 2024, Amazon Web Services, Inc. or its affiliates.



AWS Backup Audit Manager

Implement defense in depth using AWS controls

PROTECT DATA WITH MULTIPLE LAYERS OF SECURITY



Ransomware Protection – Best Practices

Implementing ransomware protection strategies with AWS backup best practices involves a combination of preventative measures and reactive measures. Here are some steps you can take to protect your data from ransomware attacks:

1. **Enable versioning on S3 buckets:** This enables you to maintain multiple versions of a file, allowing you to restore a previous version if the current one is encrypted by ransomware.
2. **Implement a data lifecycle policy:** This automatically moves data to lower-cost storage tiers or deletes it based on predefined rules. This can help prevent ransomware from infecting older versions of your data.
3. **Use AWS Backup:** This is a fully managed backup service that centralizes and automates the backup of your AWS resources. It provides an additional layer of protection against ransomware by creating immutable backups that cannot be altered or deleted by ransomware.

Ransomware Protection – Best Practices

4. **Implement IAM best practices:** Ensure that your AWS Identity and Access Management (IAM) policies are properly configured to limit access to your AWS resources only to authorized personnel.
5. **Implement network security best practices:** Use AWS security services such as AWS Shield and AWS WAF to protect against DDoS attacks and other network-based threats.
6. **Use AWS Key Management Service (KMS):** AWS KMS is a fully managed service that makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services. You can encrypt your backups and ensure that they can only be accessed by authorized personnel.
7. **Implement AWS CloudTrail:** AWS CloudTrail is a service that enables you to log, continuously monitor, and retain events related to API calls across your AWS infrastructure. You can track changes made to your infrastructure and detect suspicious activity that may be indicative of a ransomware attack.

Ransomware Protection – Best Practices

8. **Test and Monitor your backups:** Regularly test and monitor your backups to ensure that they are being created and stored as expected. This can help you identify any issues that may arise and address them before they become a problem.
9. **Implement AWS Config:** AWS Config is a fully managed service that provides you with an inventory of your AWS resources and their current configurations, enabling you to audit your AWS infrastructure for compliance and security purposes.
10. **Implement AWS Security Hub:** AWS Security Hub provides you with a comprehensive view of your security posture across your AWS accounts and regions. By integrating with other AWS security services, Security Hub enables you to quickly identify security findings and prioritize remediation efforts.

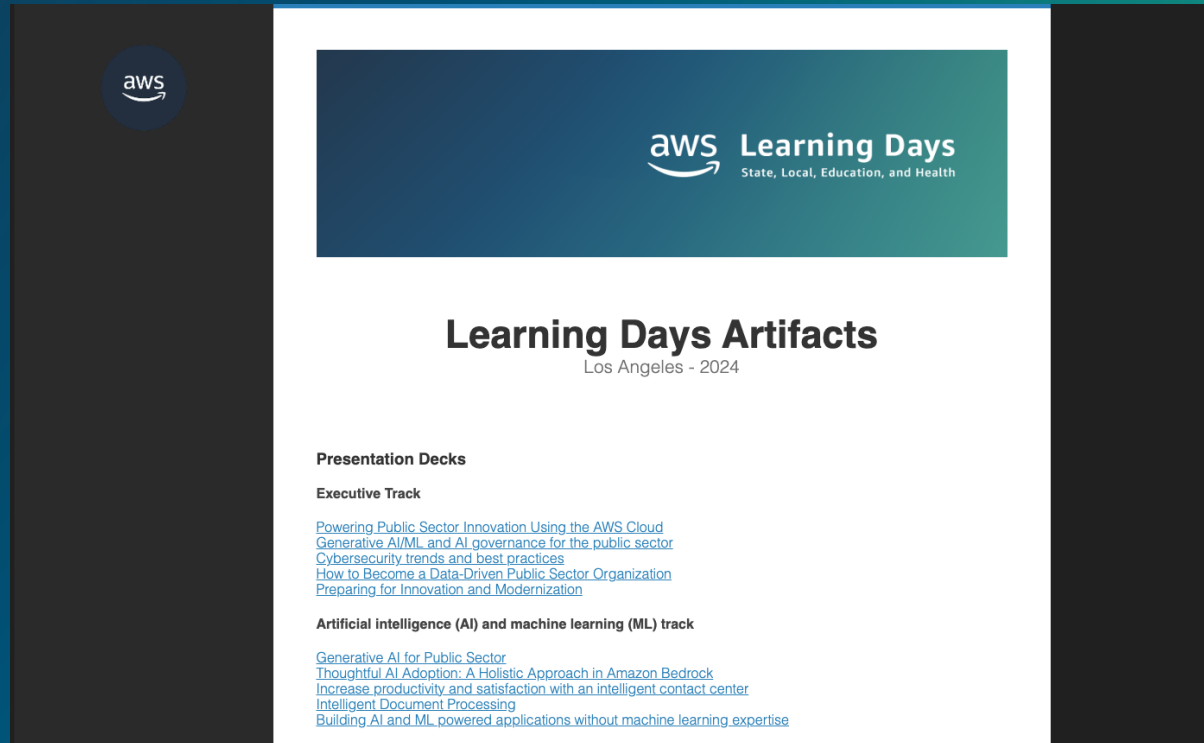
Please Provide Your Feedback



Step 1: Select **Security and application modernization track**
Step 2: Select **Security is top priority**

Learning Day Content

<https://sanfrancisco2024.awslearningday.com/>





Thank you!

Lana Lee

lanaaa@amazon.com