



ondia



# **AWS Security**

# AGENDA

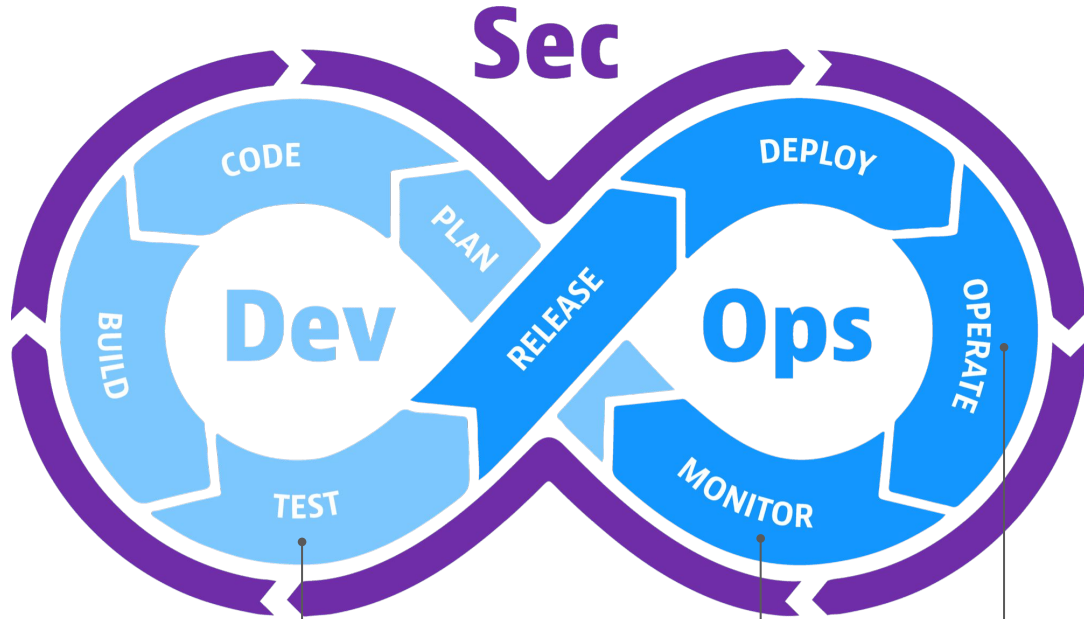


- ▶ **General Cyber Security Concepts**
- ▶ **Cyber Security Tools & Technology**
- ▶ **AWS Security Tools & Technology**



# General Cyber Security Concepts

# DevSecOps



- “DevOps” has extended to “**DevSecOps**”
- **Security is integrated** with development and operations
- It's important to understand **security concepts and tooling**

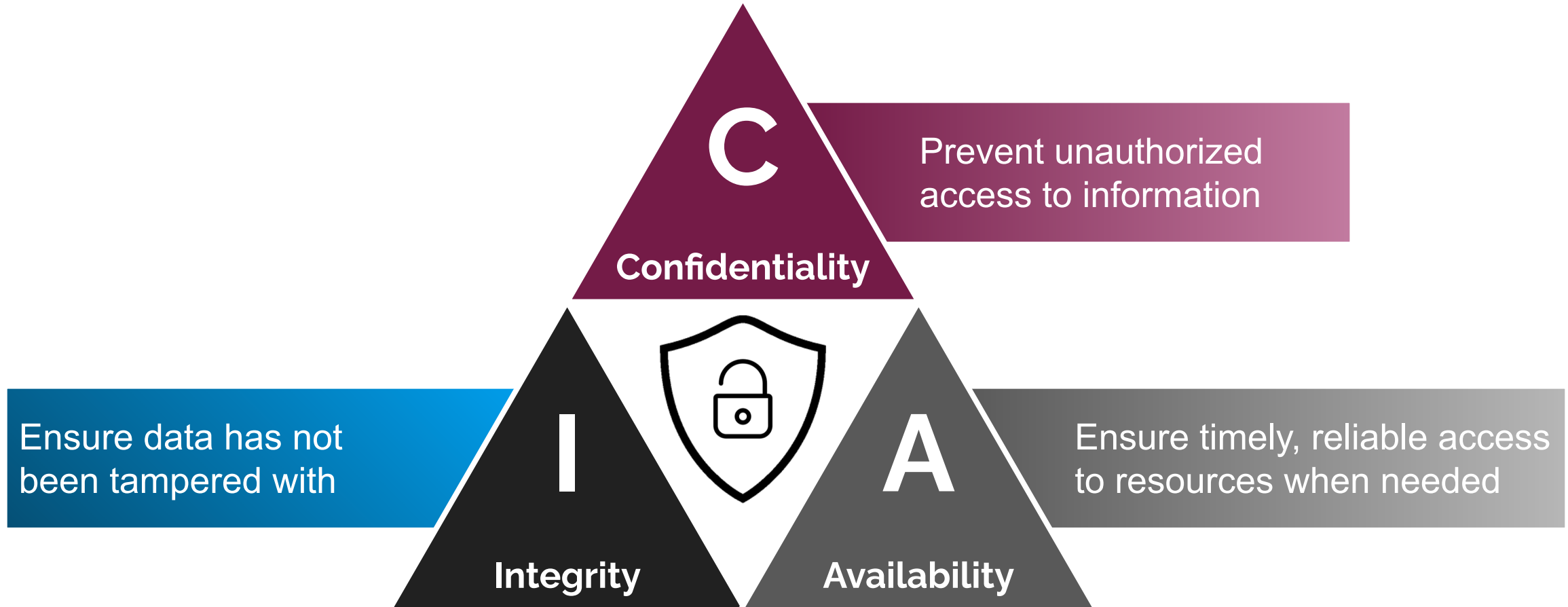
- Enforce configuration
- e.g. Firewall rules

- Monitor for security incidents
- e.g. Botnets

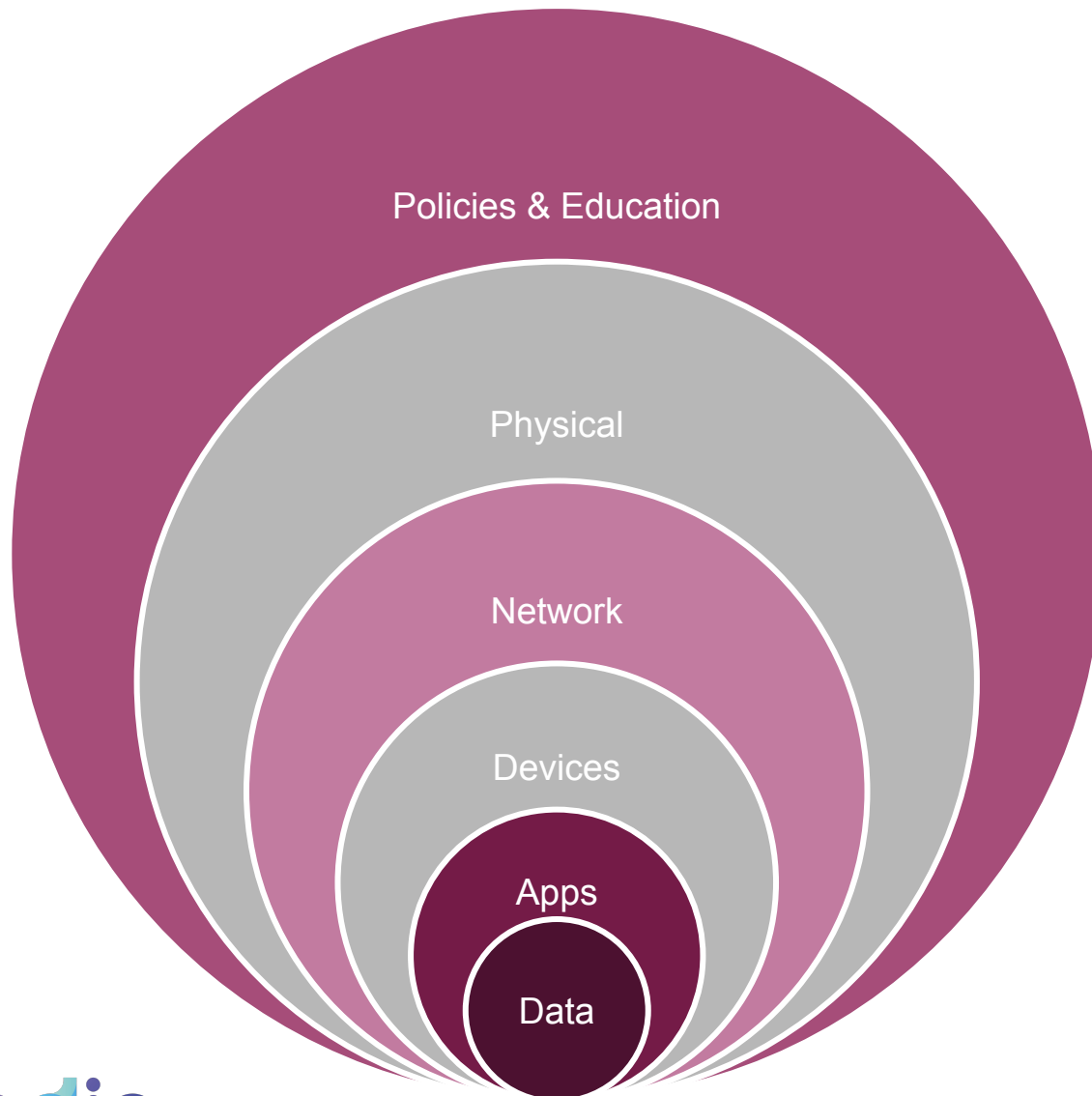
- Add security testing to code tests
- e.g. SQL Injection

} examples of security integrated with development and operations

# CIA Principles of Cyber Security

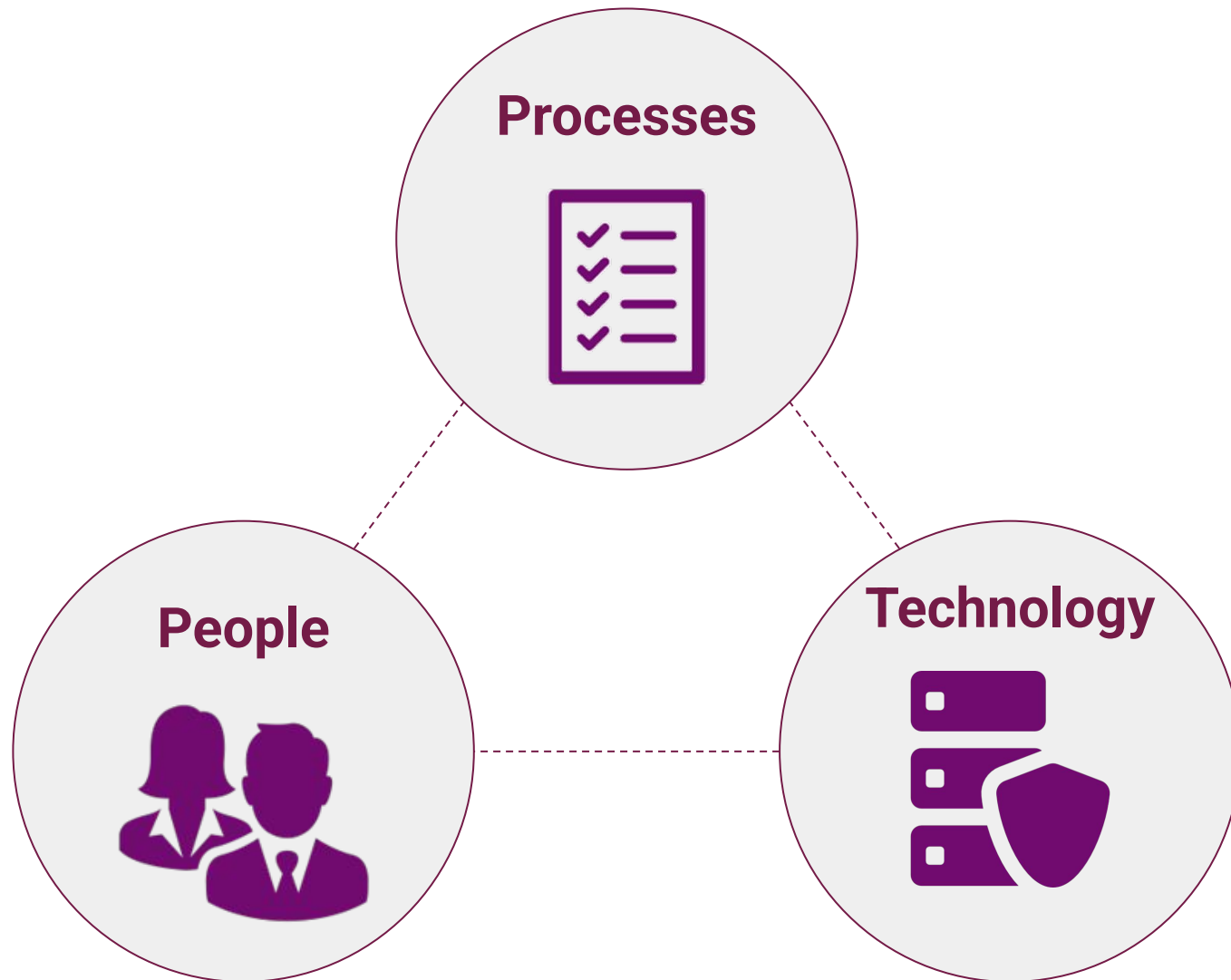


# Defense-in-Depth



- Best practice for information security
- Layered approach
- No silver bullet at any layer

# Cyber Security: More Than Technology



- **Technology** plays a **part** in cyber security
- Must be **complemented with policies and procedures**
- **Educating** people is also key



# Preventative vs. Detective Controls



A security control is a **safeguard** for an information system designed to **protect the confidentiality, integrity, and availability** of its information and to meet a set of defined **security requirements**



## Detective

- **Identifies** threats, **logs** events and sends **alerts**
- Requires **manual or automated remediation**



## Preventative

- Automatically **disallows** actions
- Can lead to **stopping legitimate** behavior

# Compliance Regulations



HIPAA



FedRAMP

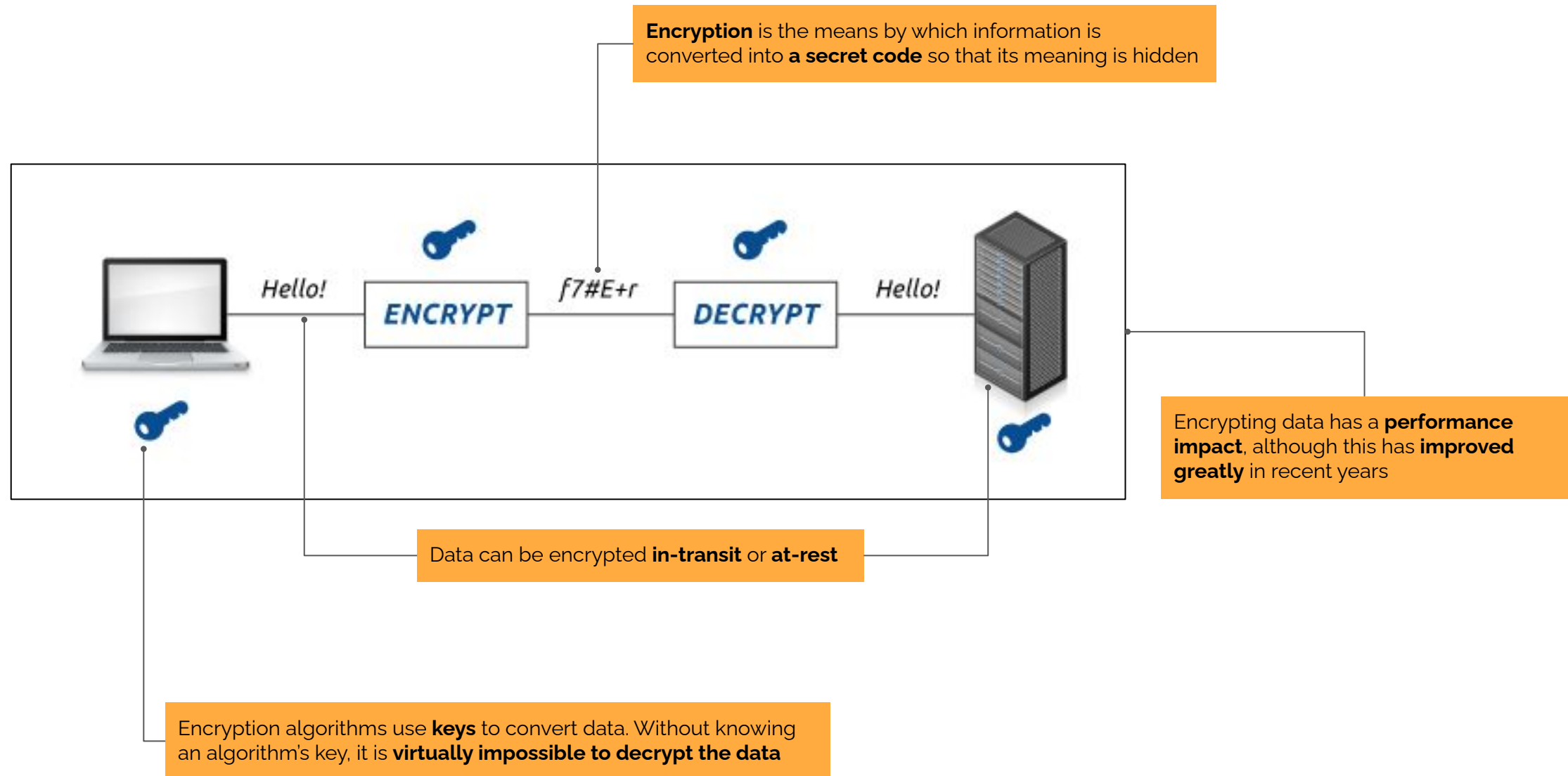


- Cyber security and data protection regulations are defined sets of **policies, procedures and controls**
- They can be **industry specific** or more **generic**
- Organizations must undergo **audits** to prove compliance

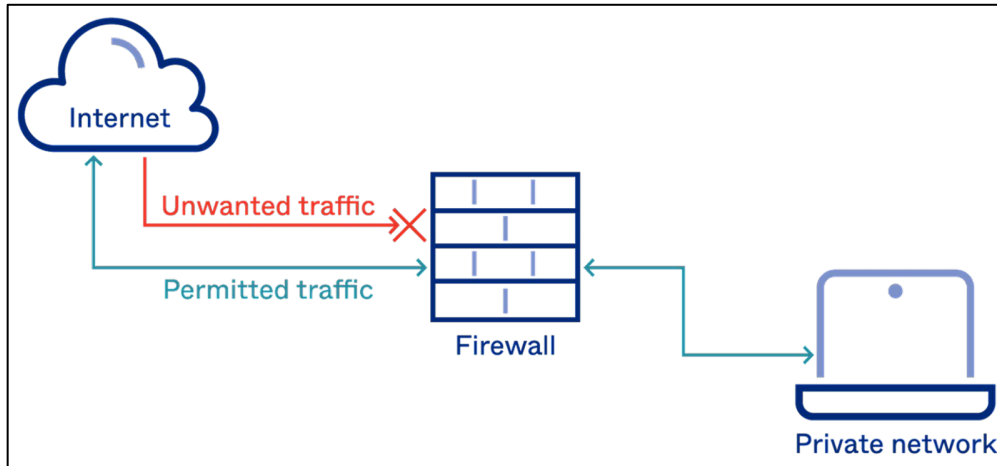


# Security Solutions

# Encryption

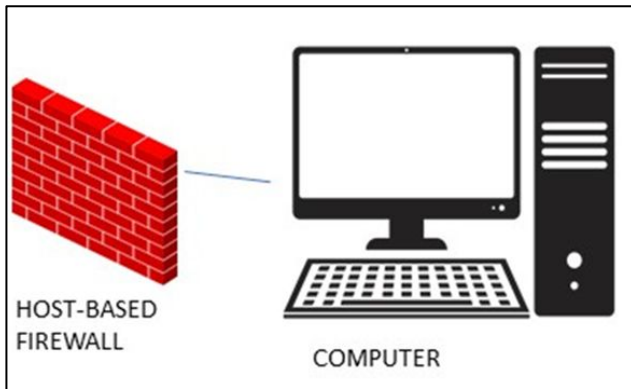


# Firewall



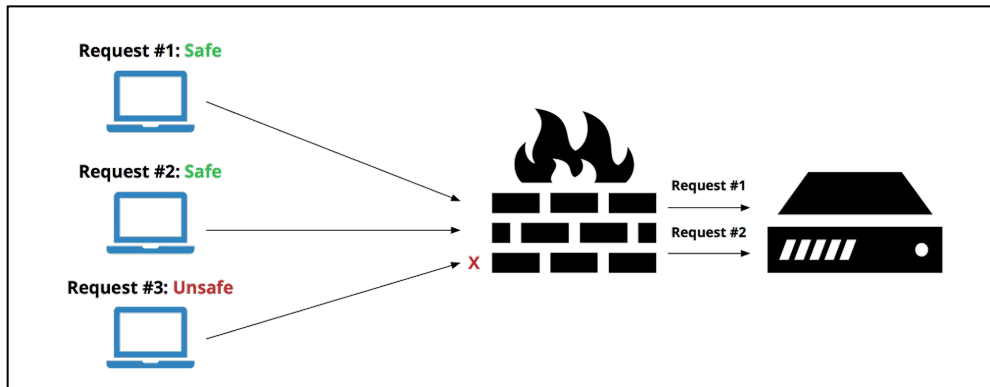
- **Network device** that controls inbound and outbound network traffic based on a set of security rules
- Typically control which traffic can ingress to or egress from an **internal network to an external network** (e.g. Internet)
- Can be an **appliance** (HW+SW) or just SW
- Today's firewalls are quite sophisticated and control traffic based on many factors:
  - **IP, port and protocol**
  - **Packet inspection**
  - **Anti-virus modules**
  - **Known bad IPs and domains**

# Host-Based Firewall



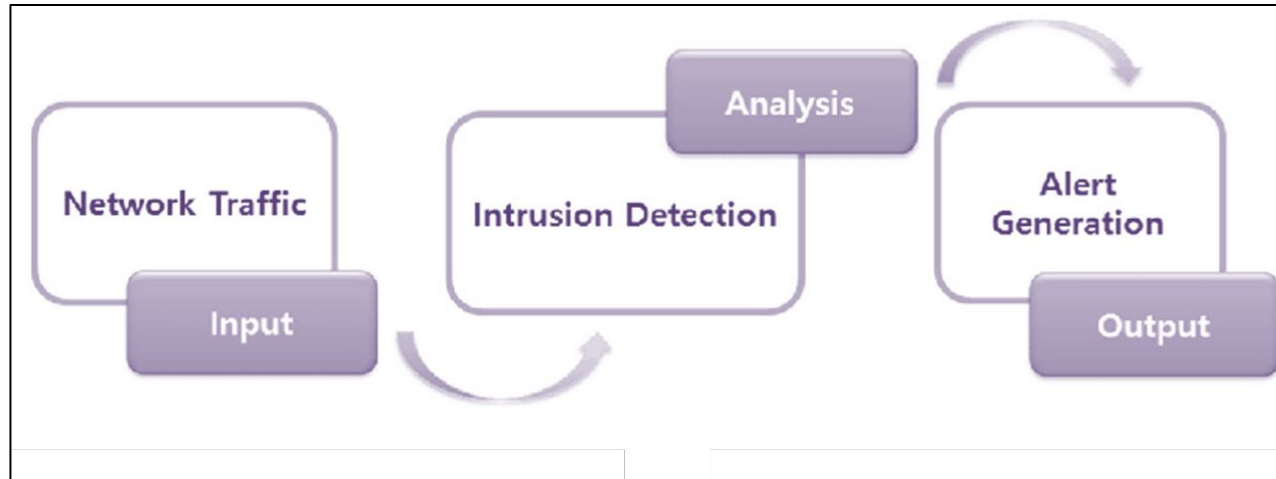
- A **software-based** firewall **installed on a host** to monitor and control incoming and outgoing network traffic
- Operates at layers 3 & 4 of the OSI model
  - i.e. **IP, port and protocol**
- Examples:
  - **Windows Defender**
  - **IPTables**

# Web Application Firewall (WAF)



- Network device that operates specifically at protocol **layer 7** and monitors **HTTP traffic**
- Typically protects web applications against specific attacks:
  - **cross-site forgery**
  - **cross-site-scripting (XSS)**
  - **SQL injection**
  - **distributed-denial-of-service (DDOS)**
- Operates via a **set of rules** (policies)

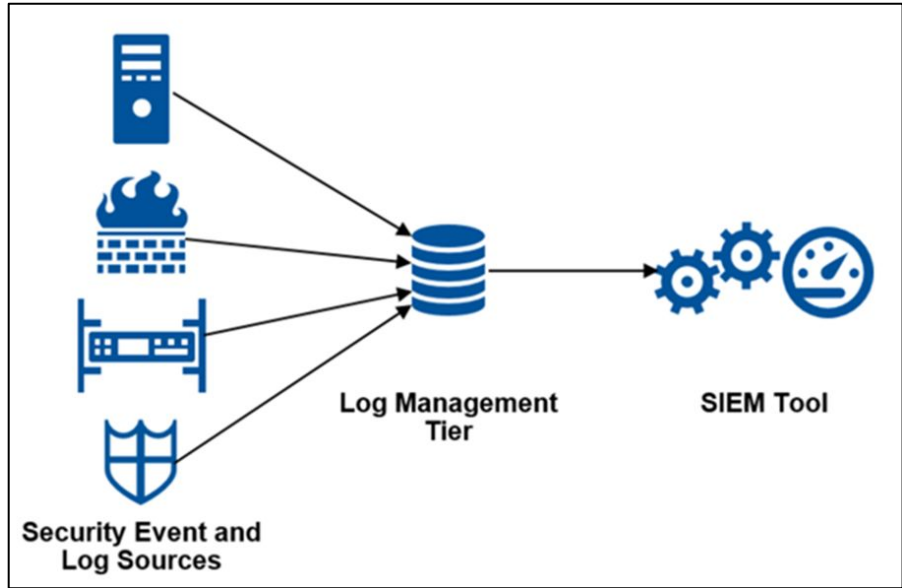
# Intrusion Detection and Prevention



- Intrusion detection systems (**IDS**) **monitor and analyze** network traffic for for signs of imminent threats
- Intrusion prevention systems (**IPS**) go one step further and **block traffic** that pose such threats
- Together, IDS/IPS solutions are typically a module in a "**Next Generation Firewall**" (**NGFW**)
- Typically use 4 types of algorithms:
  - **signature-based** detection
  - **anomaly-based** detection
  - **stateful protocol** analysis
  - **reputation** analysis
- These are **dynamic rules** applied to network packets



# Security Information and Event Management (SIEM)



- A **SIEM** is a device that **ingests and aggregates logs**, including network log information
- Can perform analysis by cross-referencing various log information to **identify network-related threats**
- Unlike IDS/IPS, this type of **analysis is based on logs**, rather than traffic packets

# Vulnerability Scanners

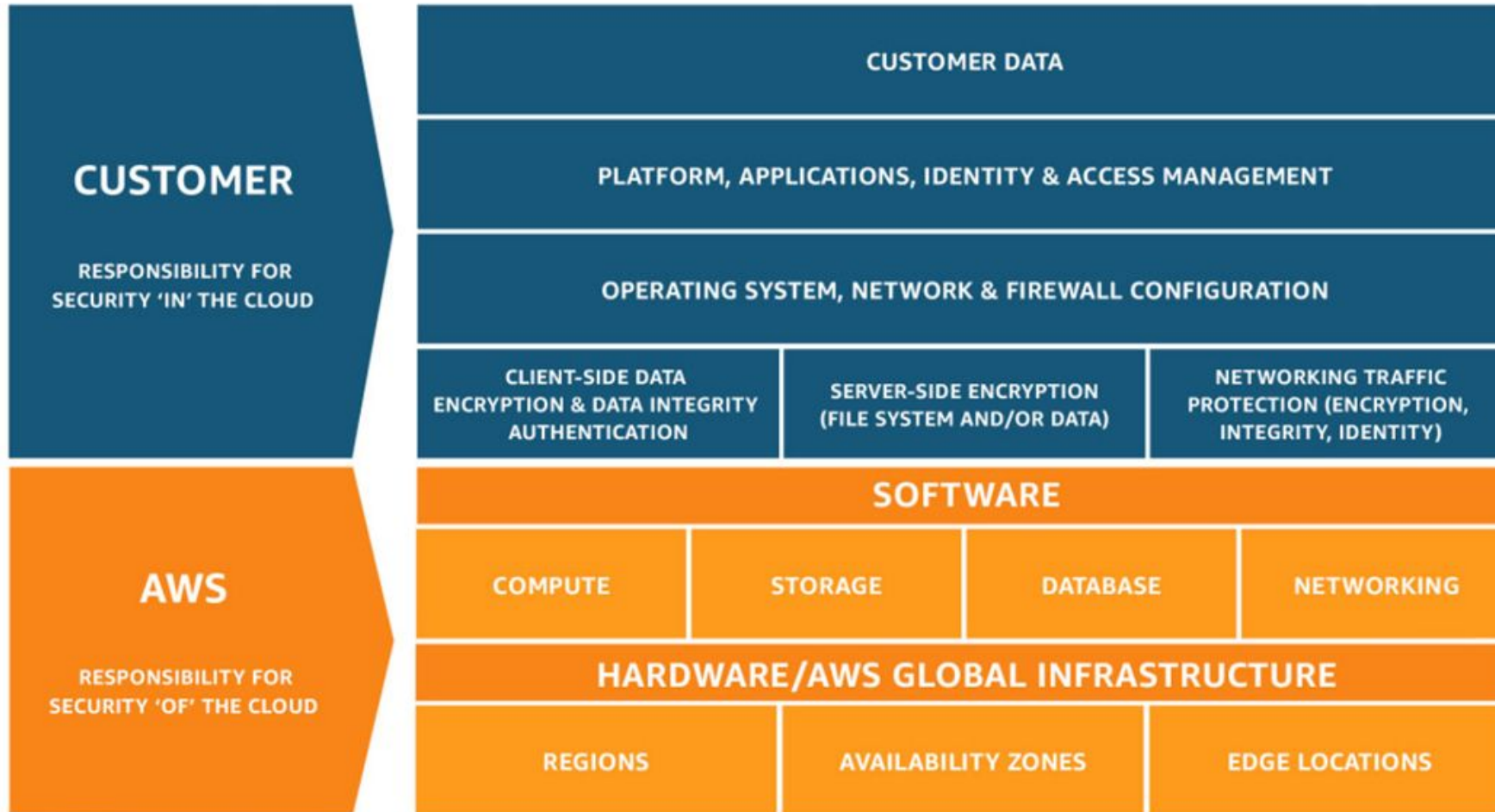


- After operating systems and software is released into the market, quite often **security vulnerabilities** are identified
- These vulnerabilities can be **exploited by hackers** in order to gain access to systems
- A publicly available **CVE (“common vulnerabilities and exposures”) database** lists the vulnerabilities and remedies
- A vulnerability scanner **identifies unremediated exposures in hosts** within your environment

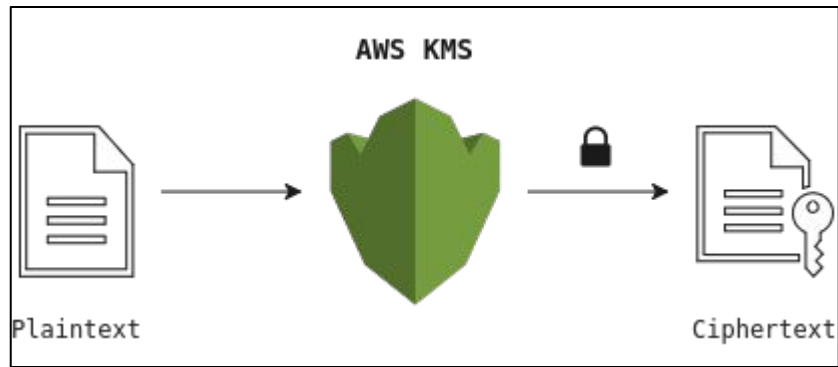
A large purple triangle pointing to the right, located on the left side of the slide.

# AWS Security Services

# Shared responsibility model



# AWS Key Management Service (KMS)



- Encrypts **data at rest**
  - EBS, S3, EFS, RDS, DynamoDB, more
- **Centralized management**
  - create, delete, view, set policies
  - Automatic **key rotation**
- Performance impact is **negligible**
- Permissions governed by **IAM and Key Policies**
- Must be cautious about **permissions and protecting keys from deletion**

# KMS Key Types

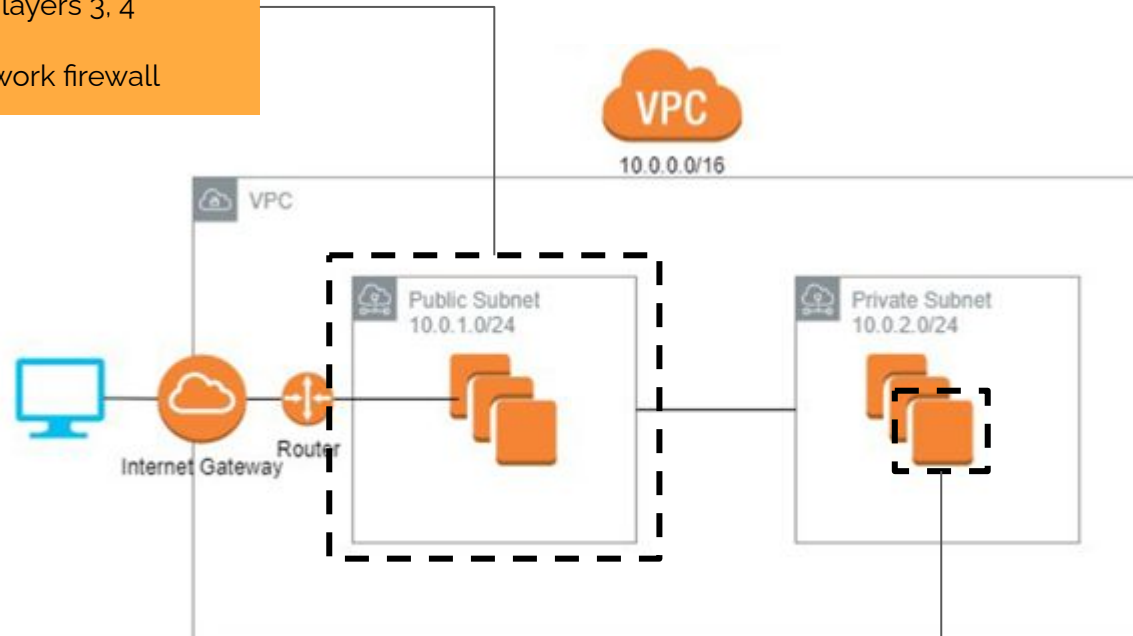


Type of KMS Key	Specific to Account?	Customer Manages?	Automatic Rotation	Key Policy Possible?
<u>Customer Managed</u> Key	Yes	Yes	Optional	Yes
<u>AWS Managed</u> Key	Yes	No	Every 3 yrs.	No
<u>AWS Owned</u> Key	No	No	AWS Dependent	No

# Security Groups and NACLs



- NACLs are firewall rules applied at the subnet level
- IP, Port & Protocol (i.e. layers 3, 4 protection)
- **Similar** to a basic network firewall



- Security Groups are firewall rules applied at the instance level
- IP, Port & Protocol (i.e. layers 3, 4 protection)
- **Similar** to a host-based firewall
- However, they do not belong to or run on the host

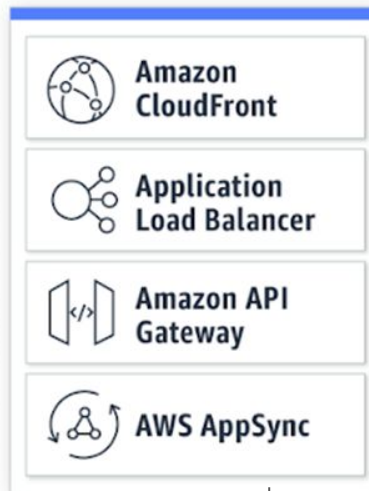
# AWS WAF



- Functionality is same as a standard web application firewall
  - protect against web exploits
  - SQL injection, cross-site scripting, etc...

- Has available "rule packages"
  - AWS Managed
  - 3rd Party Vendors

- Can run in detective or preventative mode



**Create a policy**  
Build your own rules using the visual rule builder, code in JSON, or deploy managed rules maintained by AWS and/or sellers from AWS Marketplace



**Block & Filter**  
Protect against exploits and vulnerabilities such as SQLi/XSS attacks; filter out unwanted traffic by defining specific patterns or by IP address



**Monitor**  
Use Amazon CloudWatch for incoming traffic metrics & Amazon Kinesis Firehose for request details, then tune rules based on metrics & log data

- Can manage rules centrally and apply to all endpoints in an organization

- Works with AWS endpoints



# AWS Network Firewall



*Going beyond  
IP/Port/Protocol filtering*



## Intrusion Prevention (IPS)

*Preventative*

*Signature based IPS, centralized threat intelligence*



## FQDN & IP Blacklisting

*Preventative*

*Guard against botnets, misuse*



## Stateful Packet Inspection

*Preventative*

*Improved security through dynamic/deeper packet inspection*

# AWS Inspector



Install Inspector Agent  
on EC2 Instances



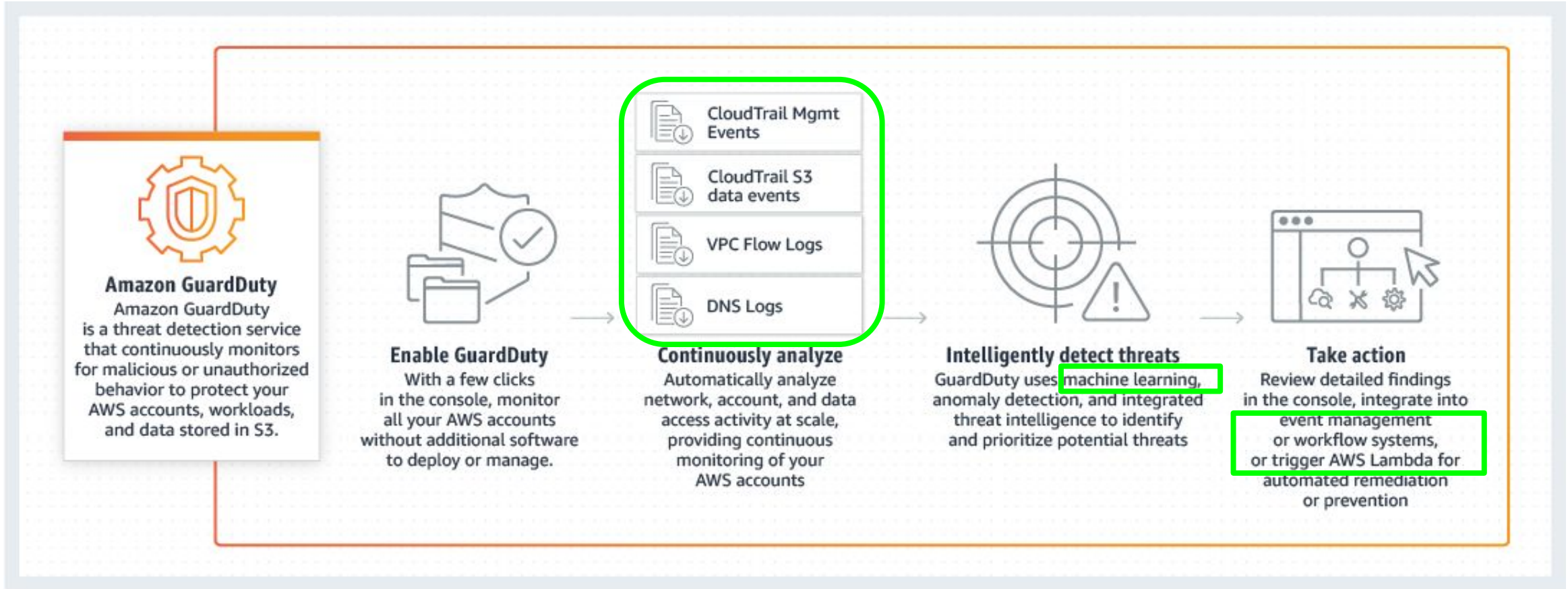
AWS Inspector  
Create Assessment Targets  
and Run the template



Review findings and  
resolve issues

- **Vulnerability management** service that can continuously scans AWS workloads for software vulnerabilities and unintended network exposure.
  - EC2, ECR and Lambda
- Creates **findings** AND provides **remediation recommendations**
- Customer responsibility to remediate any issues

# AWS GuardDuty

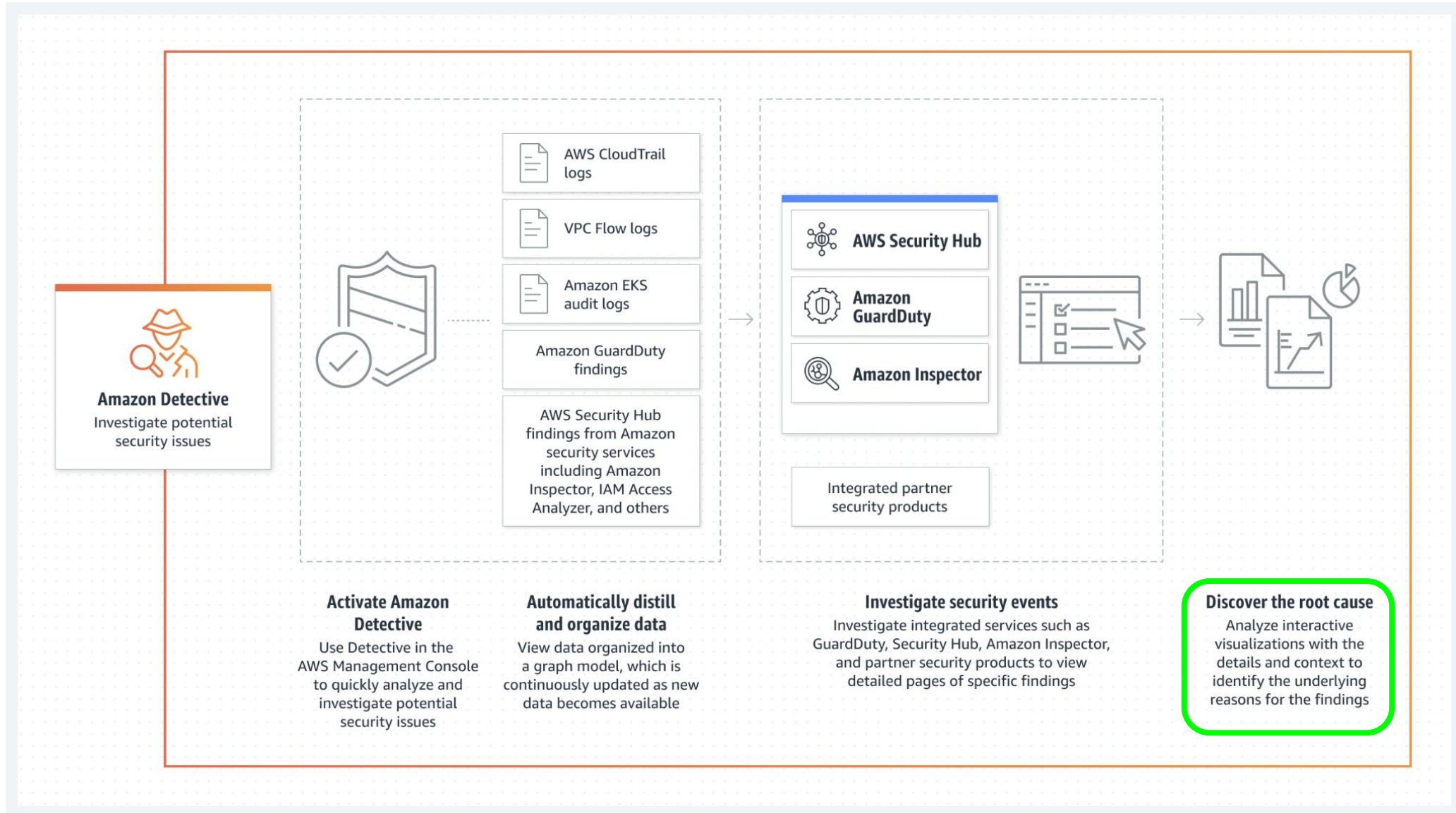




## AWS Security Hub

- **Integrates** with other AWS & 3rd party security services
  - Guard Duty
  - Inspector
  - Firewall manager
  - and more ...
- Provides a comprehensive view of security state
  - “**single pane of glass**”
- Also **creates alerts** based on security best practices

# Amazon Detective





# AWS Shield

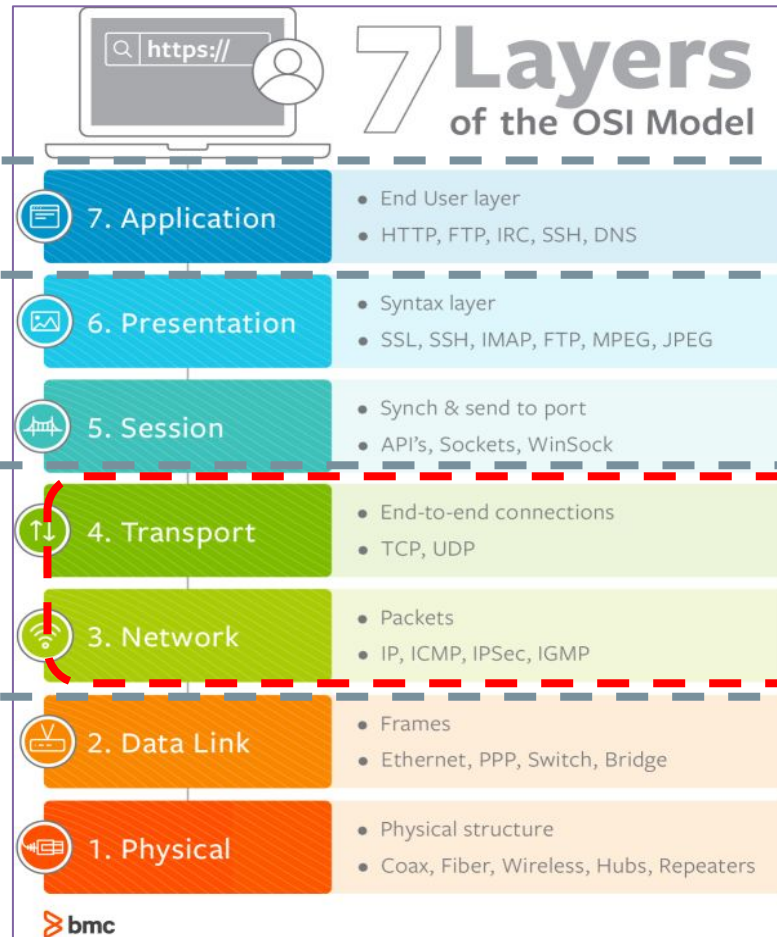


Layer 7

Layer 3, 4



Layer 3, 4



# Summary of AWS Security Services



## AWS Shield Advanced/ DDos Attack

### AWS WAF /Web App. Firewall

*Preventative*

L7 protection on AWS APIGW, AWS ALBs, and AWS CloudFront

### Security Groups /Host-Based Firewall

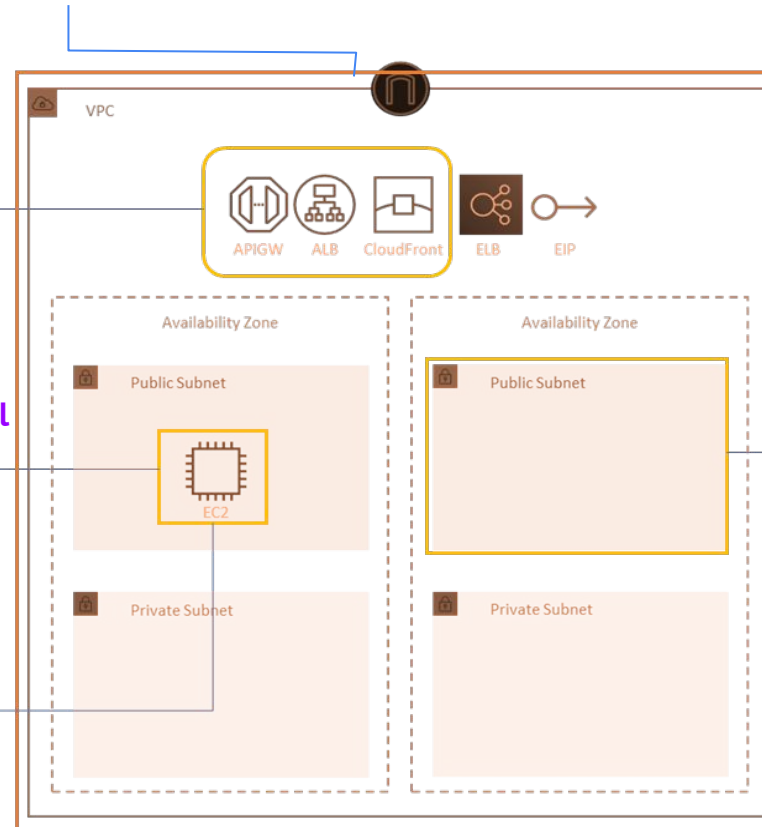
*Preventative*

IP/Port/Protocol filtering protection on instances

### AWS Inspector /Vulnerability Scanners

*Detective*

Rule-based vulnerability detection



### AWS Network Firewall

*Preventative*

IP/Port/Protocol filtering at VPC

/Intrusion Prevention/Detection System

### Network Access Control List (NACL) / Network Firewall

*Preventative*

IP/Port/Protocol filtering at subnet level

### GuardDuty / Security Information and Event Management (SIEM)

*Detective*

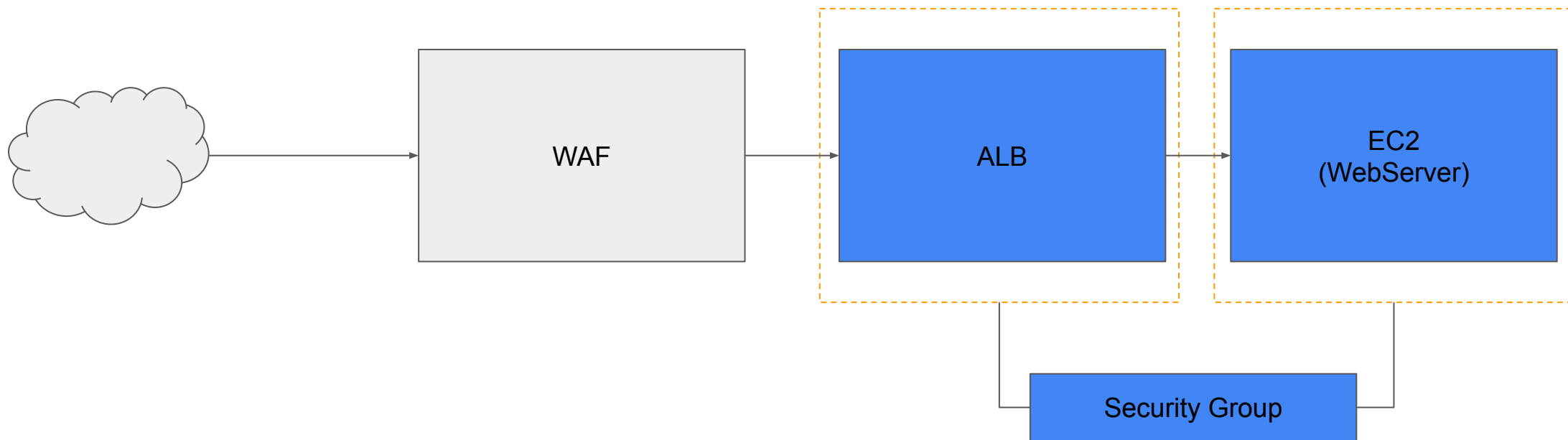
Log monitoring and alerting

# Summary of AWS Security Services



AWS Security Service	Protects Against	Applies To	Similar To
Security Groups	Unauthorized access to VPC resources	Instance @ Layer 3, 4 (IP, Port, Protocol)	Host-based Firewall
Network Access Control List (NACL)	Unauthorized access to VPC resources	Subnet @ Layer 3, 4 (IP, Port, Protocol)	Network Firewall
AWS WAF	Web attacks e.g. SQL Injection, cross-site scripting	Layer 7 (HTTP)	WAF
AWS Network Firewall	Malicious network intrusion	Layer 3, 4, 7	IPS / IDS
Guard Duty	Malicious network traffic	Log analysis	SIEM
AWS Inspector	Exploitable vulnerabilities	EC2, ECR	Vulnerability scanner
SecurityHub	Provides single pane of glass view	Network, accounts	SIEM
AWS Shield	DDos Attack	Layer 3, 4 (Shield Standard) Layer 7 (Shield Advanced)	WAF







# THANKS!

**Any questions?**

