Part 2

AWS Workshop Series

Day 2: Security on AWS

Taking Enterprise Beyond the Cloud by TrueIDC

Mr. Athiwat Itthiwatana

Cloud & Solution Consultant

Presented by

- Athiwat Itthiwatana (HAM)
- Cloud & Solution Consultant, TrueIDC
- AWS Specialist
- SAP Basis Specialist
- athiwat.itt@ascendcorp.com

aws certified
Solutions Architect
PROFESSIONAL

aws certified
SAP on AWS
SPECIALTY

aws certified
Security
SPECIALTY

Agenda

- Encryption in AWS
- Amazon GuardDuty
- AWS WAF & Shield
- Lab: AWS WAF Workshop

Source: AWS Immersion day

Encryption in AWS

Basic definitions

Plaintext

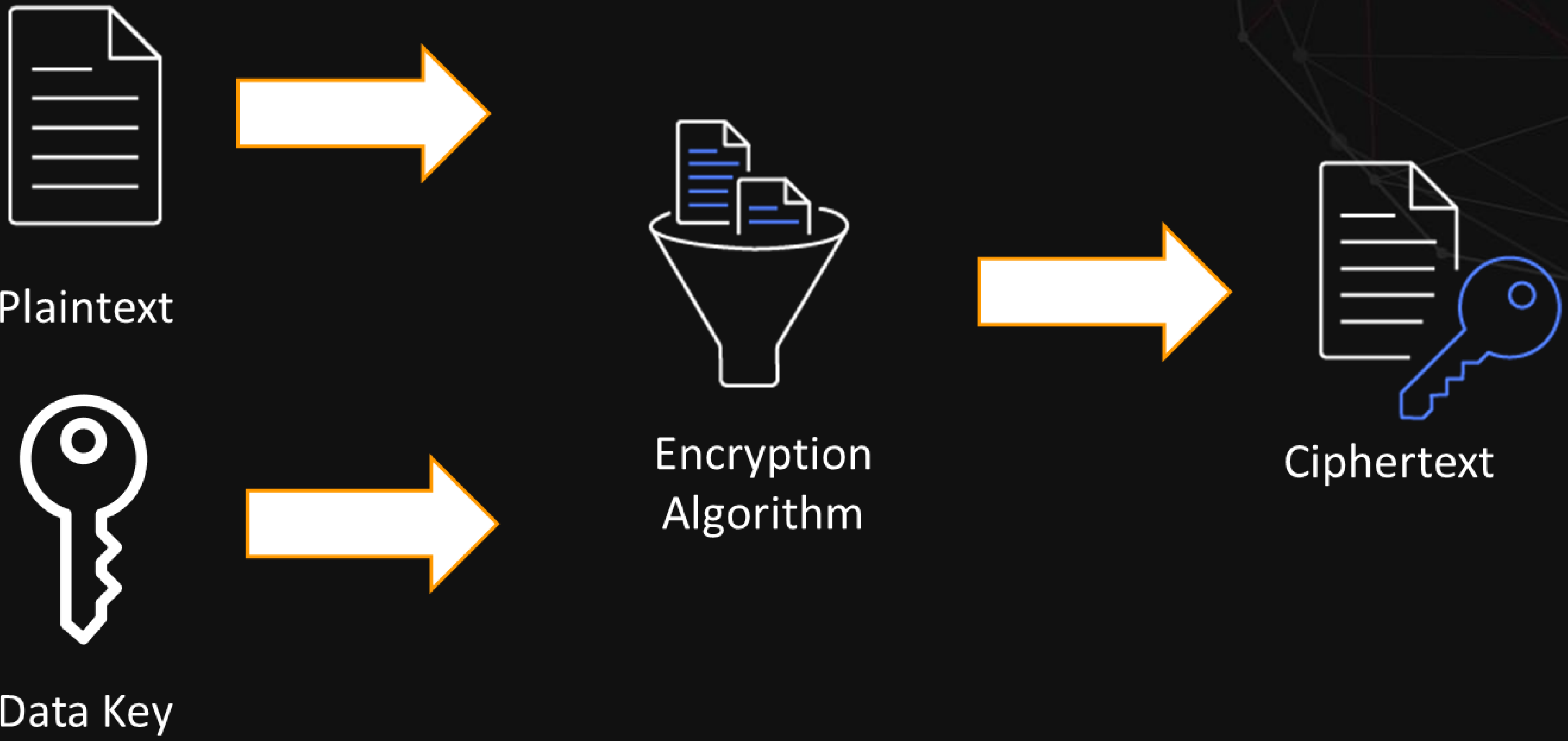
Data Key

Encryption Algorithm

Ciphertext

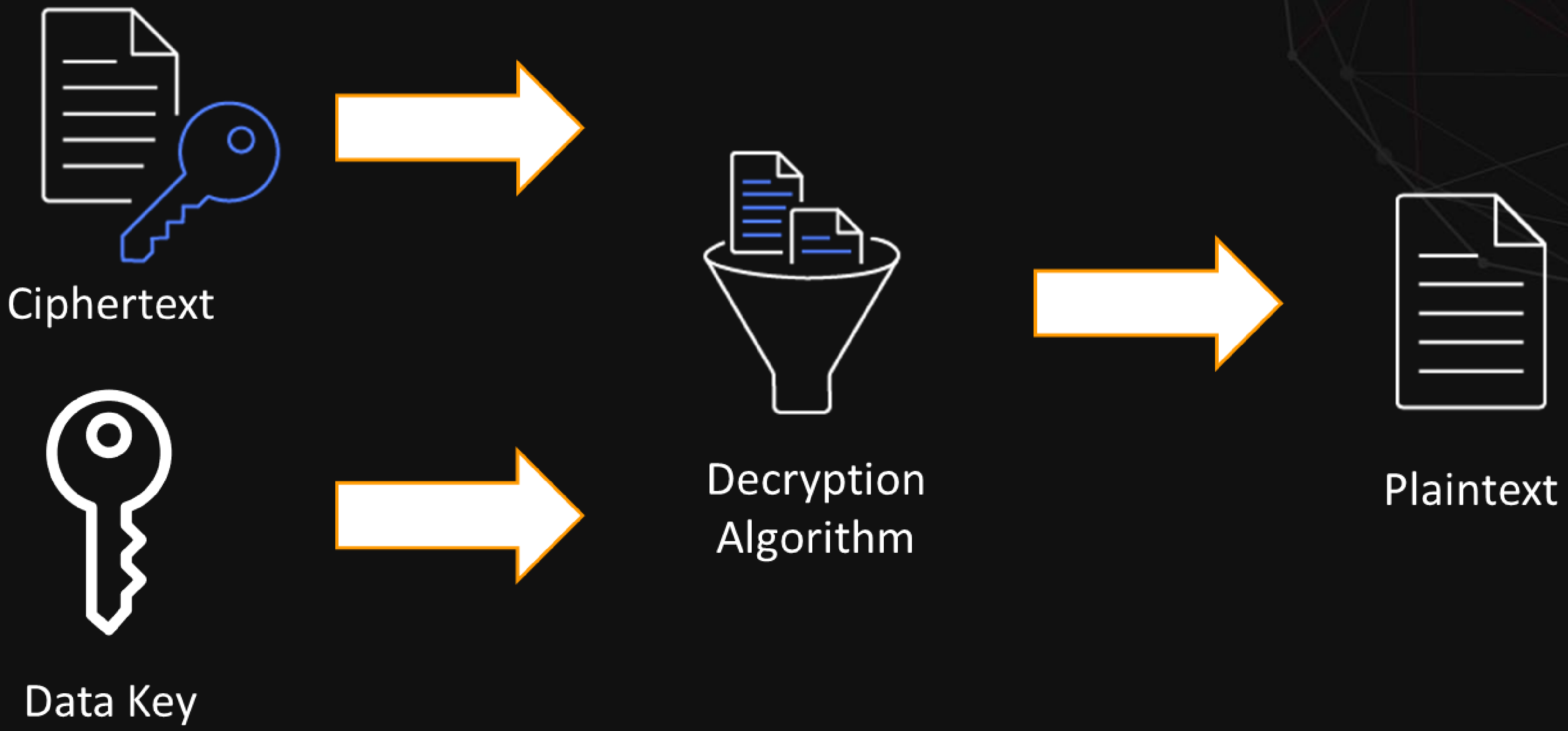
Source: AWS Immersion day

Encryption



Source: AWS Immersion day

Encryption

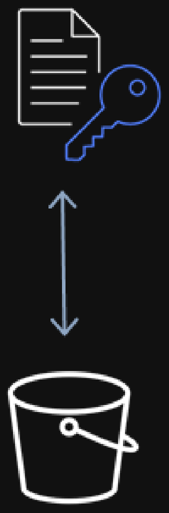


Source: AWS Immersion day

Encrypt, where? Encrypt everywhere!

Data at rest

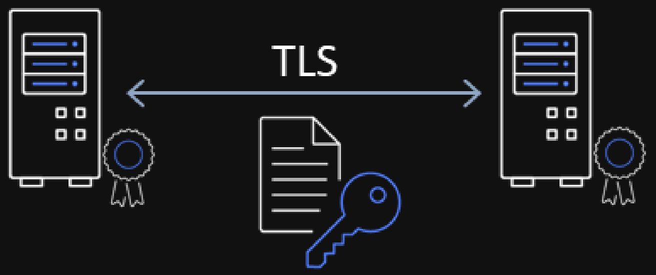
Storage encryption



S3 Bucket

Data in motion

Network encryption



TLS

Application Data

Application level encryption

Application Code

Source: AWS Immersion day

AWS Key Management Service

AWS Key Management Service (KMS) makes it easy to create, manage, and securely store cryptographic keys

KMS is incorporated in over 90 AWS services to encrypt sensitive data and create digital signatures.

AWS Key Management Service

Source: AWS Immersion day

AWS KMS Benefits

Fully Managed Key Service

Secure, Centralized Key Management

Native Integrations with AWS Services

Encrypt Data in Your Applications

Audit and Monitor Encryption Keys

Pay as You Go Pricing

Source: AWS Immersion day

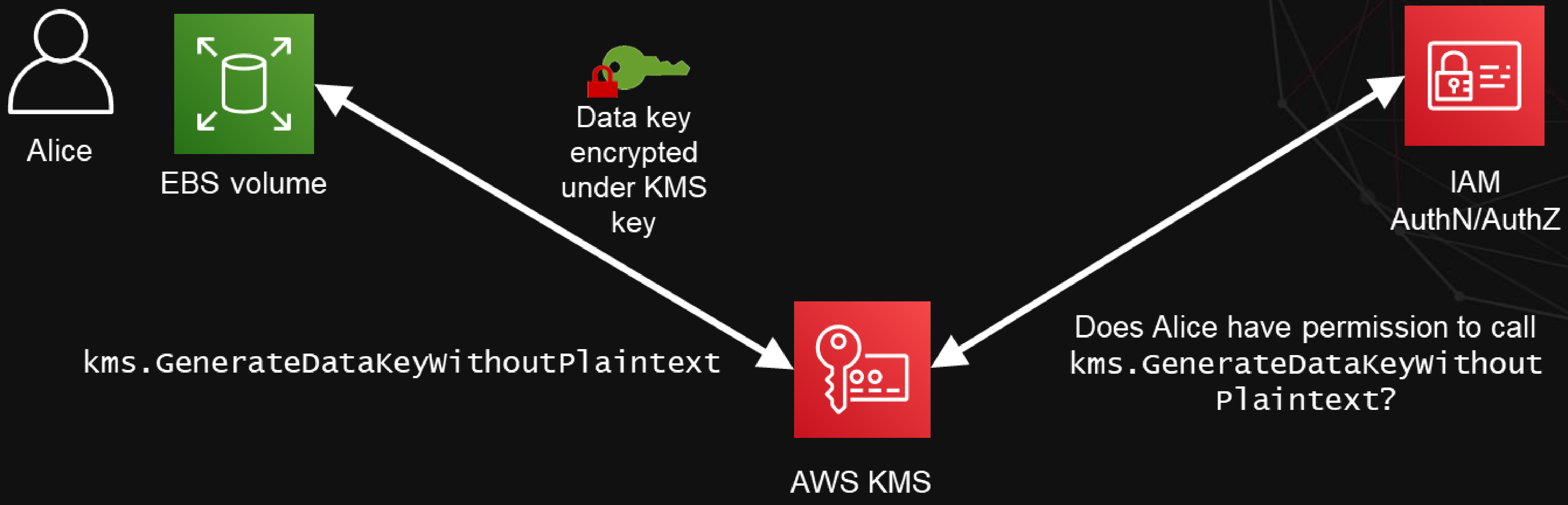
Data at rest: KMS

- Encryption is available in every AWS service where you can store data
- AWS services, such as S3 and EBS, utilize KMS to generate, retrieve, and protect data keys that are used to encrypt your sensitive data
- Many services support data key caching or features like S3 Bucket Keys to help reduce your KMS costs

S3 Bucket Key: A bucket-level key that is used for a time-limited period within Amazon S3. This reduces the need for S3 to make requests to KMS, allowing you to access AWS KMS-encrypted objects in S3 at a fraction of the previous cost.

Source: AWS Immersion day

EBS encryption: Create volume

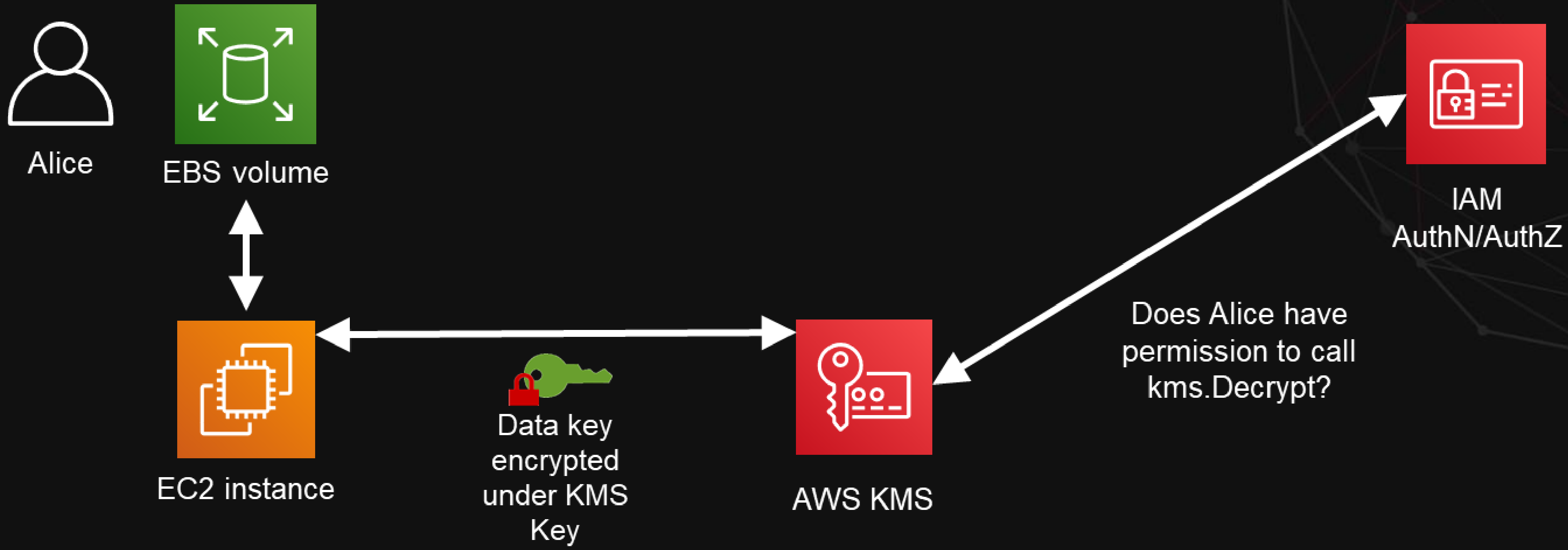

Alice
EBS volume
Data key encrypted under KMS key
kms.GenerateDataKeyWithoutPlaintext
AWS KMS
IAM AuthN/AuthZ
Does Alice have permission to call kms.GenerateDataKeyWithout Plaintext?

Example: EBS service creates encrypted volume

- EBS service requests a new data key to protect the volume
- KMS checks the KMS key policy and IAM policy to ensure the appropriate permissions are granted
- KMS creates the data key and provides it to EBS service to encrypt the volume

Source: AWS Immersion day

EBS encryption: Attach volume


Alice
EBS volume
EC2 instance
Data key encrypted under KMS Key
AWS KMS
IAM AuthN/AuthZ
Does Alice have permission to call kms.Decrypt?

Example: EC2 service attempts to attach an encrypted EBS volume

- **KMS checks the KMS key policy and IAM policy to ensure the appropriate permissions are granted for decryption**
- **KMS decrypts the data key and provides it to EC2 service in order to decrypt and attach the EBS volume**

Source: AWS Immersion day

Data in motion: AWS Certificate services

AWS Certificate Manager (ACM)

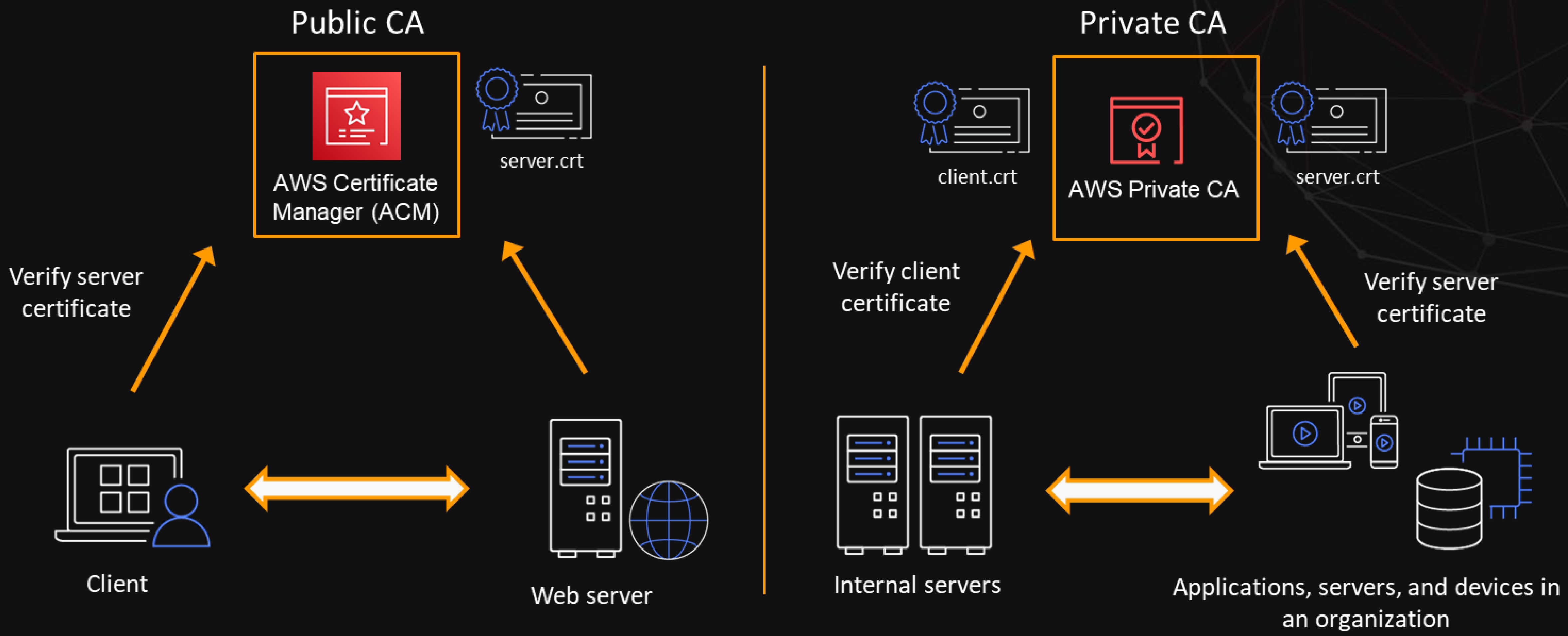
Easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources

AWS Private Certificate Authority (CA)

Highly-available private certificate authority service without the upfront investment and ongoing maintenance costs of operating your own private CA

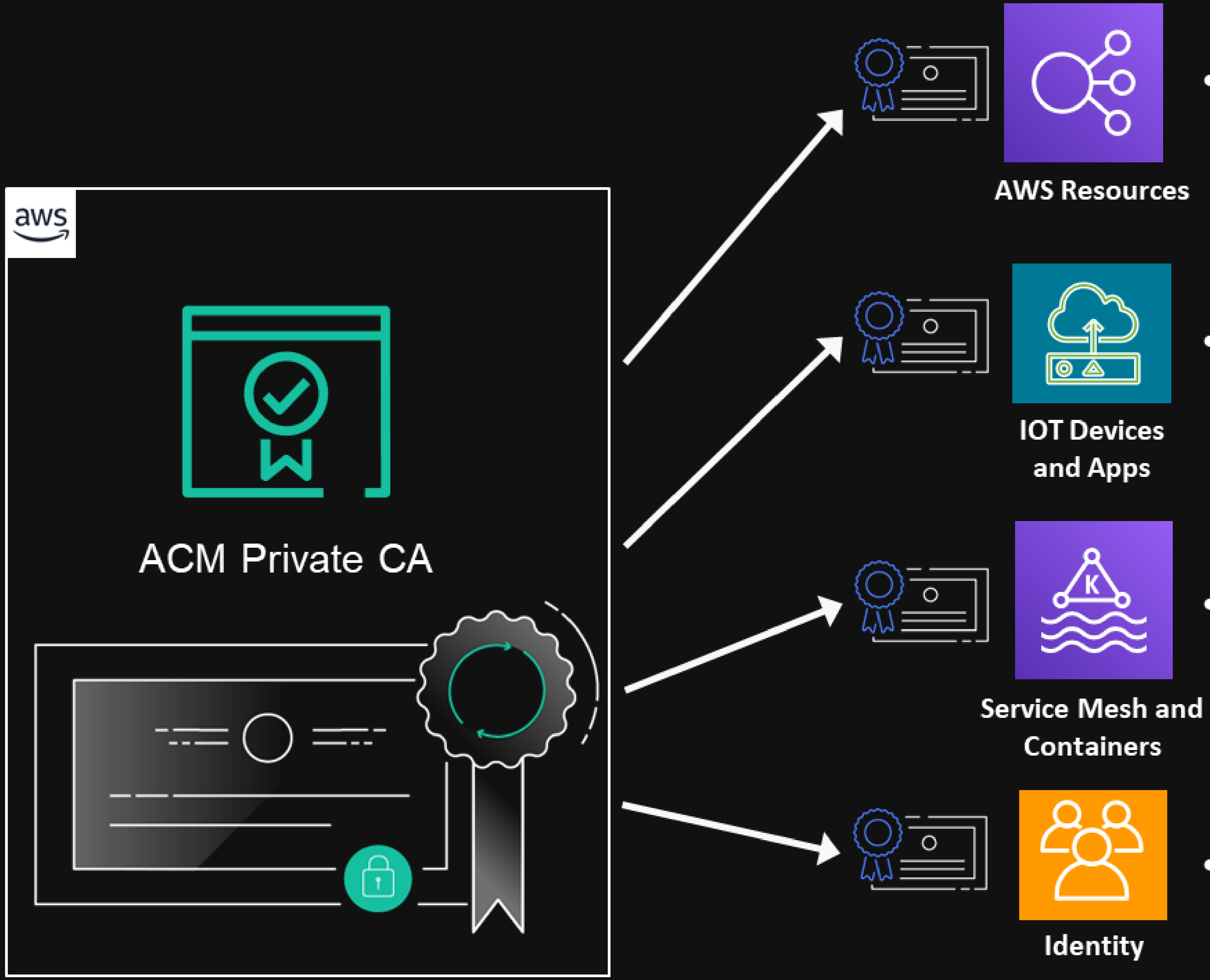
Source: AWS Immersion day

Public vs. Private Certificate Authority


Public CA
AWS Certificate Manager (ACM)
server.crt
Verify server certificate
Client
Web server
Private CA
client.crt
AWS Private CA
server.crt
Verify client certificate
Verify server certificate
Internal servers
Applications, servers, and devices in an organization

Source: AWS Immersion day

When to use Private CA?



- Implement end-to-end encryption to AWS resources or on-prem servers
- Issue certificates for IoT or manufactured devices
- Provide real time certificates for service meshes and container workloads
- Issue identity certificates for devices, machines, and users

Source: AWS Immersion day

Application Data: AWS Encryption SDK

Outside of AWS service integrations, you can use the AWS Encryption SDK to encrypt data within custom-built applications in AWS or hosted in your on-premises data center

In order to encrypt, developers have to keep track of only two things

- The message/file/stream they want to encrypt
- An identifier that points to the source of their keys (i.e., key provider)

Advanced users can customize the SDK in multiple ways

- Encrypt under different keys in different regions
- Cache data keys for re-use to minimize call rate to AWS KMS for better performance

Source: AWS Immersion day

Amazon GuardDuty

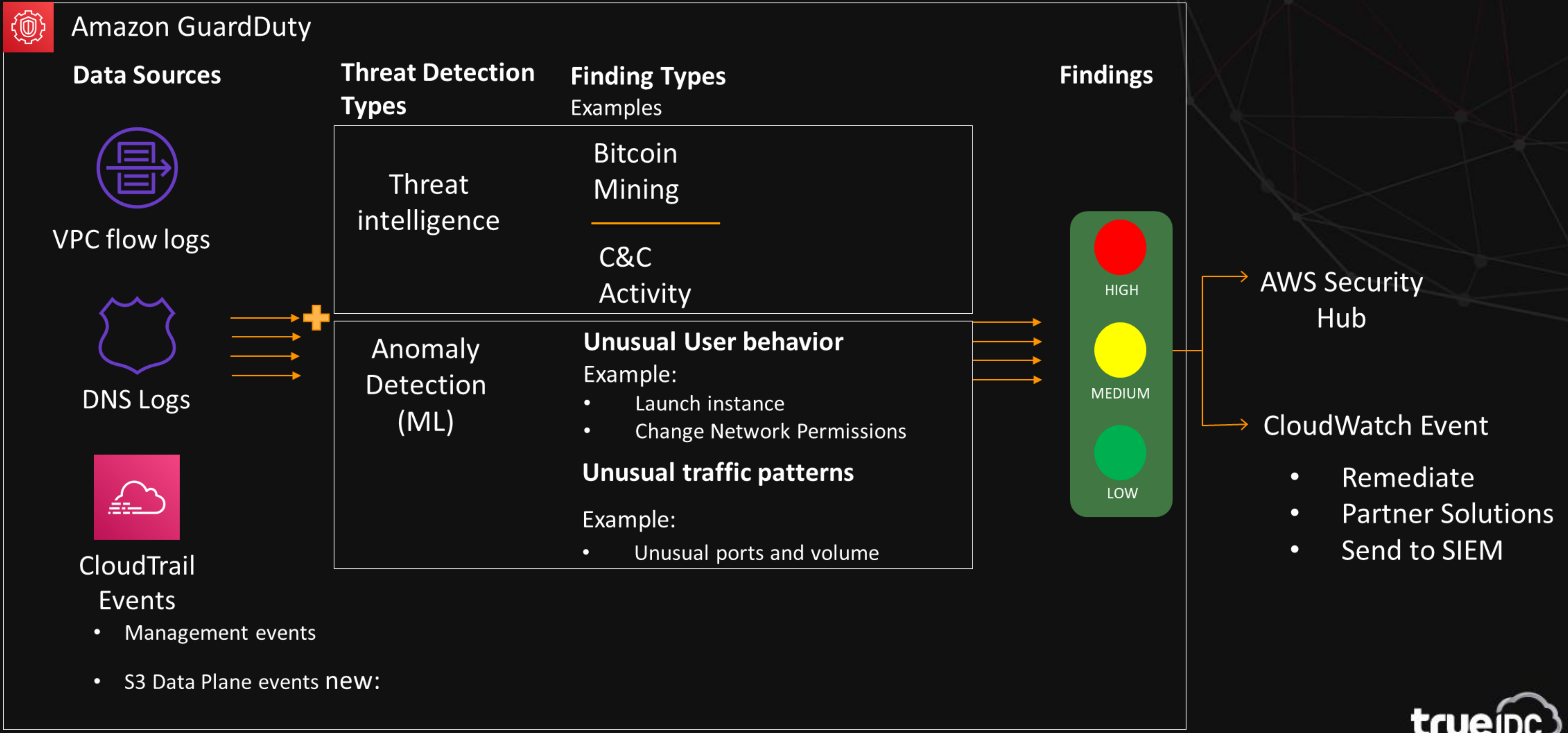
AWS GuardDuty

!! *Foundational security monitoring and detection* !!

- Provides continuous monitoring of the following data sources (without needing to manually configure any of them!):
  - CloudTrail Logs (Management Events)
  - DNS Logs
  - S3 Logs (Data Events)
  - VPC Flow Logs
- Threat intel and machine learning based threat detection

Source: AWS Immersion day

How Amazon GuardDuty works?



Amazon GuardDuty

Data Sources

VPC flow logs

DNS Logs

CloudTrail Events

- Management events
- S3 Data Plane events new:

Threat Detection Types

Finding Types
Examples

Threat intelligence

Bitcoin Mining

C&C Activity

Anomaly Detection (ML)

Unusual User behavior

Example:

- Launch instance
- Change Network Permissions

Unusual traffic patterns

Example:

- Unusual ports and volume

Findings

AWS Security Hub

CloudWatch Event

- Remediate
- Partner Solutions
- Send to SIEM

Source: AWS Immersion day

AWS WAF & Shield

Common External Threats

Denial of Service

SYN Floods

Reflection Attacks

Web Request Floods

App Vulnerabilities

SQL Injection

Cross-site Scripting (XSS)

OWASP Top 10

Common Vulnerabilities and Exposures (CVE)

Bad Bots

Crawlers

Content Scrapers

Scanners & Probes

Source: AWS Immersion day

AWS WAF – Web Application Firewall

- **Protect web applications and APIs against common web attacks and bots**

- **Provides ability to create security rules that control bot traffic and block common attack patterns.**

Seamless Integration

Amazon CloudFront

AWS Application Load Balancer

Amazon API Gateway

AWS AppSync

Source: AWS Immersion day

AWS WAF: Application-Level Security

Virtual Patching

IP reputation lists

SQL injection

Cross-site scripting

HTTP floods (DDoS attack)

Bots and scrapers

Bots: Scanners & probes

Machine Learning based

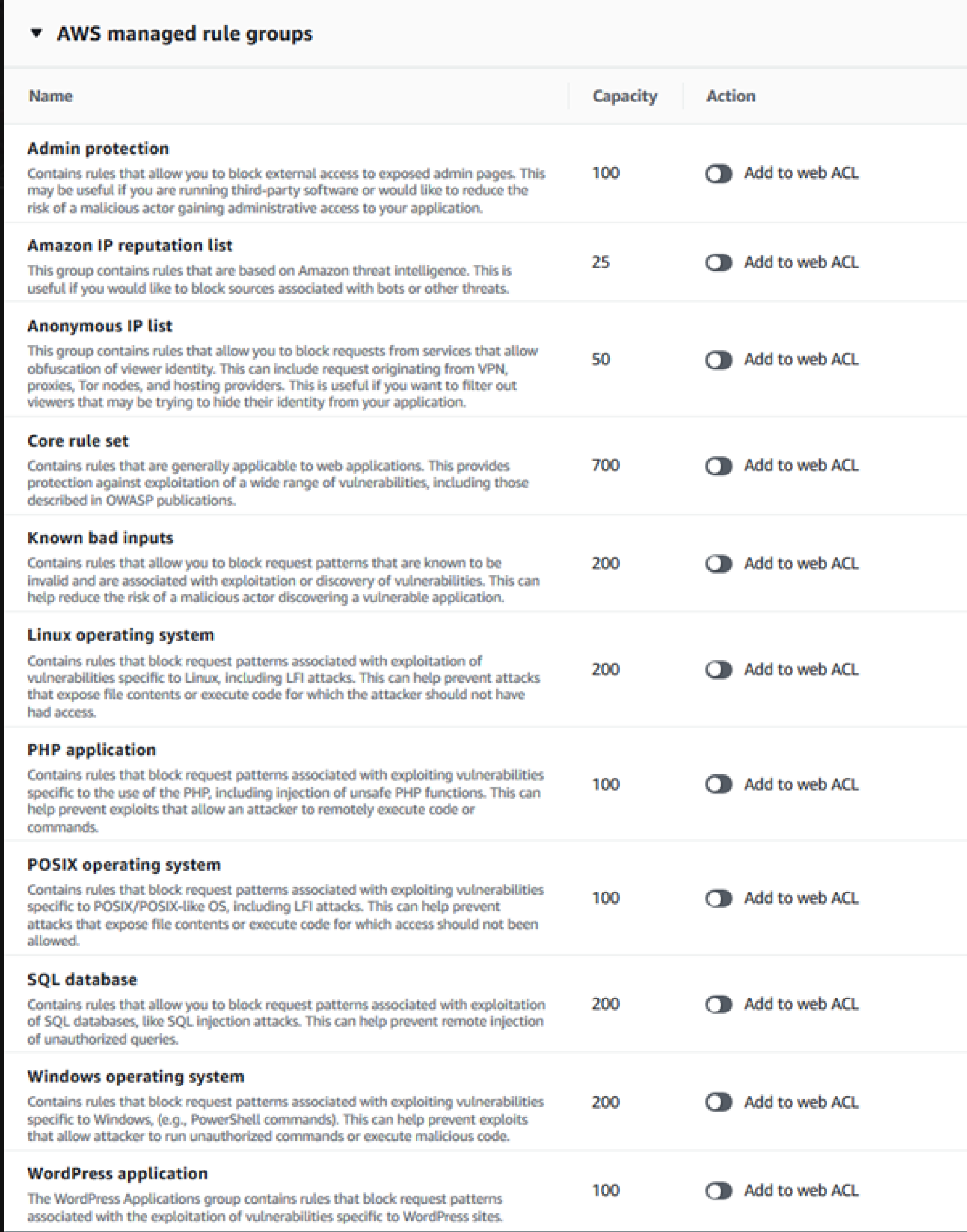
Source: AWS Immersion day

AWS WAF:
AWS Managed Rules

Pre-configured rules

- Covers common attack vectors and threats
- Curated and maintained by SRT
- Influenced by OWASP Top 10

Source: AWS Immersion day



▼ AWS managed rule groups

Name	Capacity	Action
Admin protection Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application.	100	Add to web ACL
Amazon IP reputation list This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats.	25	Add to web ACL
Anonymous IP list This group contains rules that allow you to block requests from services that allow obfuscation of viewer identity. This can include request originating from VPN, proxies, Tor nodes, and hosting providers. This is useful if you want to filter out viewers that may be trying to hide their identity from your application.	50	Add to web ACL
Core rule set Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications.	700	Add to web ACL
Known bad inputs Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application.	200	Add to web ACL
Linux operating system Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access.	200	Add to web ACL
PHP application Contains rules that block request patterns associated with exploiting vulnerabilities specific to the use of the PHP, including injection of unsafe PHP functions. This can help prevent exploits that allow an attacker to remotely execute code or commands.	100	Add to web ACL
POSIX operating system Contains rules that block request patterns associated with exploiting vulnerabilities specific to POSIX/POSIX-like OS, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which access should not been allowed.	100	Add to web ACL
SQL database Contains rules that allow you to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. This can help prevent remote injection of unauthorized queries.	200	Add to web ACL
Windows operating system Contains rules that block request patterns associated with exploiting vulnerabilities specific to Windows, (e.g., PowerShell commands). This can help prevent exploits that allow attacker to run unauthorized commands or execute malicious code.	200	Add to web ACL
WordPress application The WordPress Applications group contains rules that block request patterns associated with the exploitation of vulnerabilities specific to WordPress sites.	100	Add to web ACL

AWS WAF: Partner Managed Rules

- Select Partner Rule Sets to Implement on the AWS WAF
  - AlertLogic
  - Fortinet
  - F5
  - Imperva
  - TrendMicro
  - TrustWave

- Subscribe to Partner Rules and Leave Management to Them
  - Simple Monthly Fees, Global Availability, Instant Rule Deployment

Source: AWS Immersion day

AWS Shield – DDoS

- Managed Distributed Denial of Service (DDoS) protection service.
- Protects transport layer, mitigates large DDoS attacks.
- Provides Cost protection against DDoS related traffic spikes

Seamless Integration

Amazon CloudFront

Elastic Load Balancing

AWS Global Accelerator

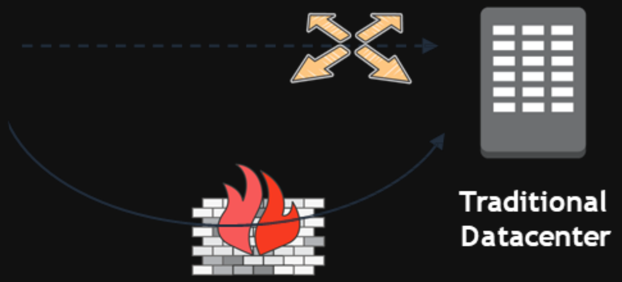
Elastic IP Address

Source: AWS Immersion day

AWS Shield Advanced: Managed DDoS Protection

Solve Traditional Service Issues

Operator involvement to initiate mitigation



Re-route traffic via distant scrubbing location

Increased time to mitigate

Source: AWS Immersion day

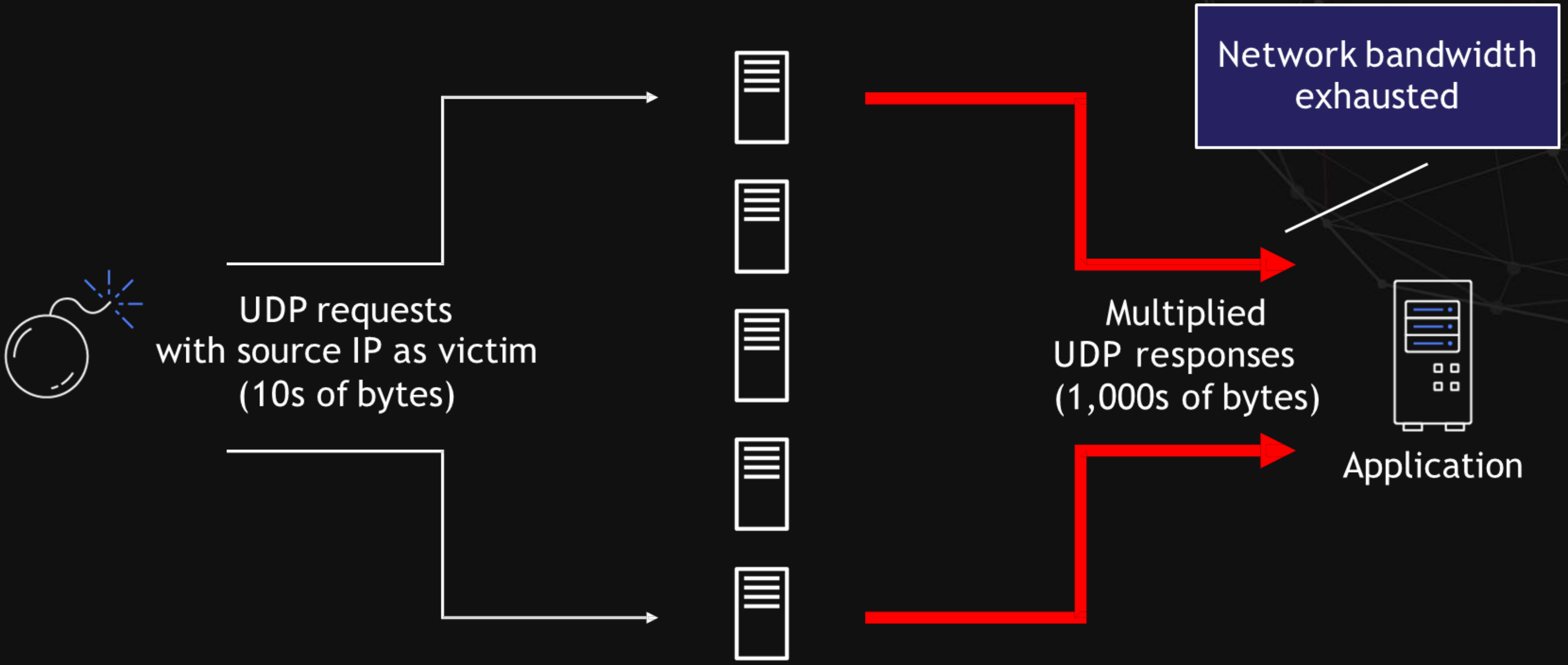
AWS Shield Advanced: Managed DDoS Protection

- In Line Protections on the Edge and within the AWS Region
- No Architectural Changes Required

- Additional Detection & Monitoring
- Protection Against Large DDoS Attacks
- Visibility into Attack Detection & Mitigation
- AWS WAF at No Additional Cost
- 24x7 DDoS Response Team-SRT
- Cost Protection (Absorb DDoS Scaling Cost)

Source: AWS Immersion day

DDoS Attack



Network bandwidth exhausted

UDP requests
with source IP as victim
(10s of bytes)

Multiplied
UDP responses
(1,000s of bytes)

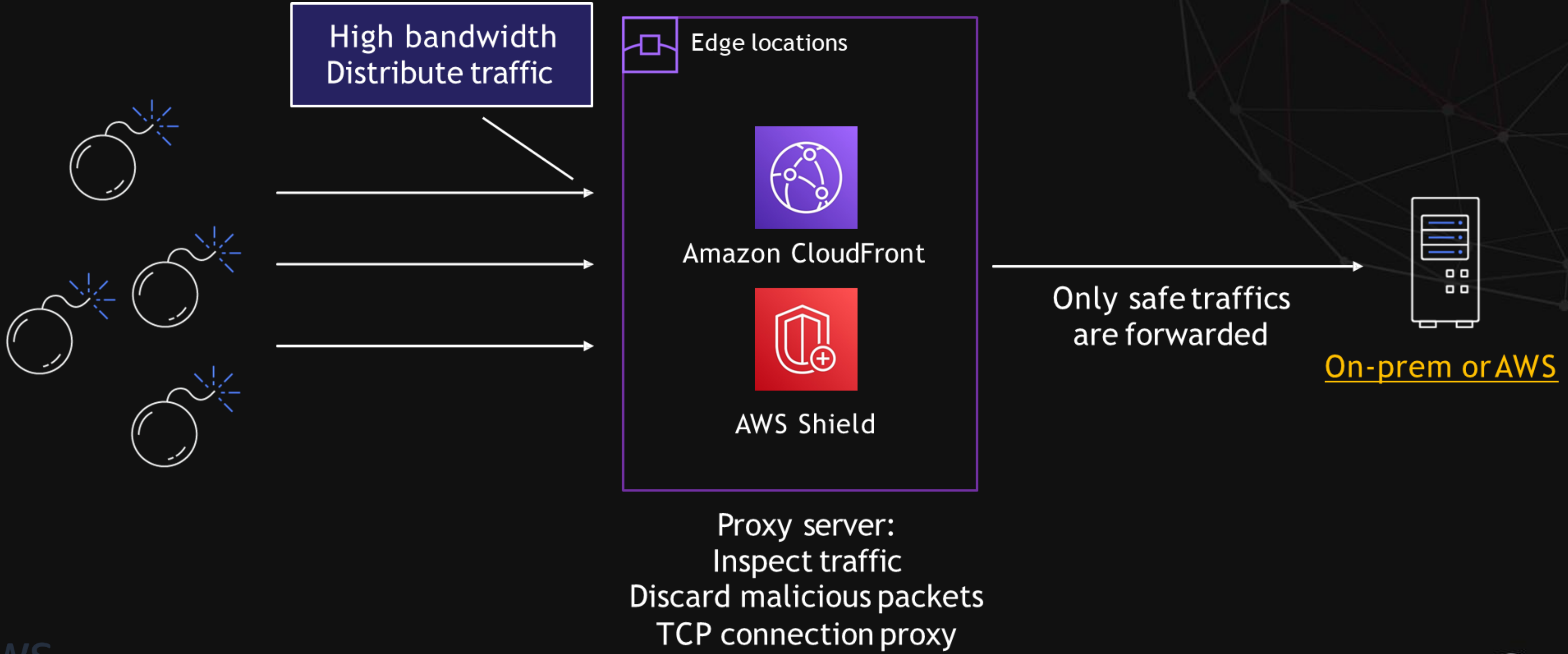
Application

aws

Source: AWS Immersion day

trueIDC

DDoS Attack Mitigation



High bandwidth
Distribute traffic

Edge locations

Amazon CloudFront

AWS Shield

Only safe traffics
are forwarded

On-prem or AWS

Proxy server:
Inspect traffic
Discard malicious packets
TCP connection proxy

Source: AWS Immersion day

Shield Advanced Engagement Case Study

Gaming customer

Request and error counts spike
Healthy resources dropping to zero
Gaming sites failing to load

Engaged SRT

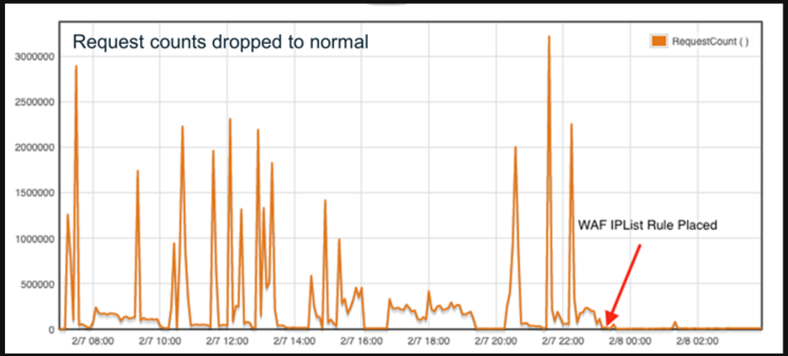
Created SIM Ticket
Customer learned correct SRT engagement channels

SRT Action

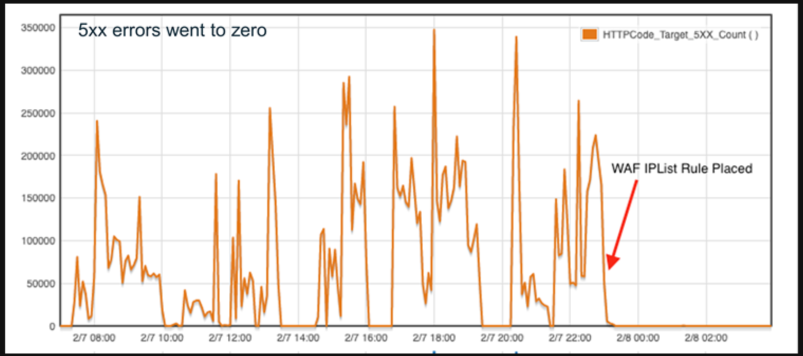
Enabled AWS WAF logging
Ran AWS WAF logs through attack analysis
Built IP block list for 4K+ suspicious IPs
Created additional AWS WAF Rules

Back to normal

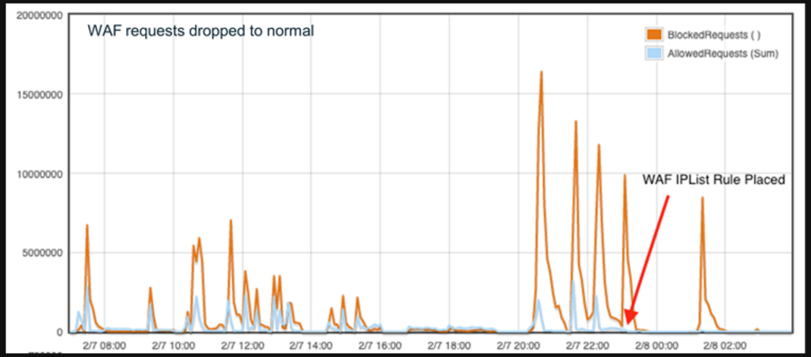
Request counts back to normal
5xx errors went to zero
AWS WAF requests dropped to normal


Request counts dropped to normal

WAF IPList Rule Placed


5xx errors went to zero

WAF IPList Rule Placed


WAF requests dropped to normal

WAF IPList Rule Placed

Source: AWS Immersion day

AWS Shield Standard vs Advanced

AWS Shield Standard

- Protect Against 96% of Infrastructure Layer Attacks
- Network flow monitoring for Layer 3 / 4 Attack
- Self-service & pay-as-you-go WAF for web attacks

AWS Shield Advanced

- Protection Against Largest & Sophisticated attacks
- Additional Detection & Monitoring
- Attack Notification & Details via CloudWatch
- 24x7 Access to DDoS Response Team
- Include AWS WAF at No Additional cost

Source: AWS Immersion day

Lab: AWS WAF Workshop

https://github.com/TIDC-PS-Inter/AWS-Workshop trueIDC

REGIONAL
DATA CENTER &
CLOUD SERVICE
PROVIDER