AWS re:Invent

SEC332-R

Bot mitigation at the edge

Tyler Paxton
Principal Product Manager
Amazon Web Services

Paul Bodmer
Engineering Manager, Shield Advanced
Amazon Web Services

Paul Campbell
Head of Delivery
Daemon Solutions

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Expectations

Key observations on the evolving bot landscape

Introduction to recently released AWS WAF updates

Learn more about AWS WAF Security Automations

Insight into how Daemon Solutions built a customized security solution

Related breakouts

SEC407-R: A defense-in-depth approach to building web applications

- Monday, Dec 2, 2:30 PM - 3:30 PM – Mirage, Events Center B1 Blue
- Wednesday, Dec 4, 5:30 PM - 6:30 PM – MGM, Level 3, Chairman's Ballroom 366

SEC334-R: Architecture best practices for DDoS resiliency

- Tuesday, Dec 3, 11:30 AM - 12:30 PM – Aria, Level 1 East, Josh
- Wednesday, Dec 4, 1:00 PM - 2:00 PM – Mirage, Antigua A

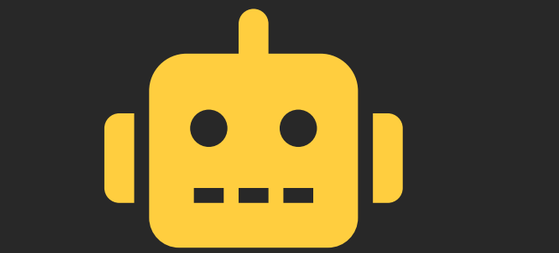
SEC333-R: Protect distributed web apps: AWS WAF & AWS Firewall Manager

- Thursday, Dec 5, 1:45 PM - 2:45 PM – MGM, Level 3, South Concourse 302
- Friday, Dec 6, 10:00 AM - 11:00 AM – Mirage, Antigua A

Bot landscape overview

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Internet traffic

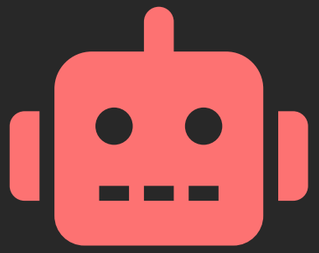


Good Bot





Human

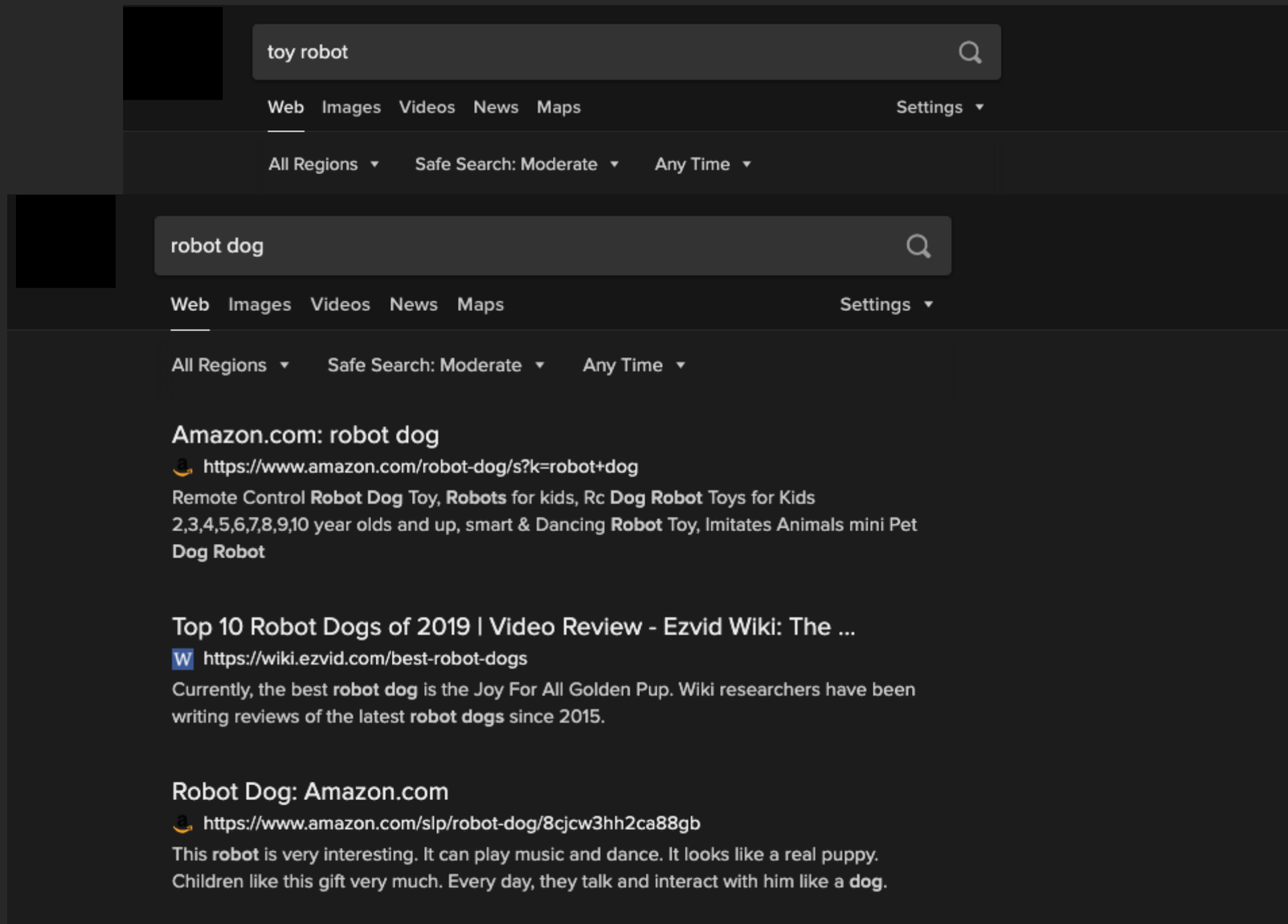


Bad Bot

Benefits of good bots

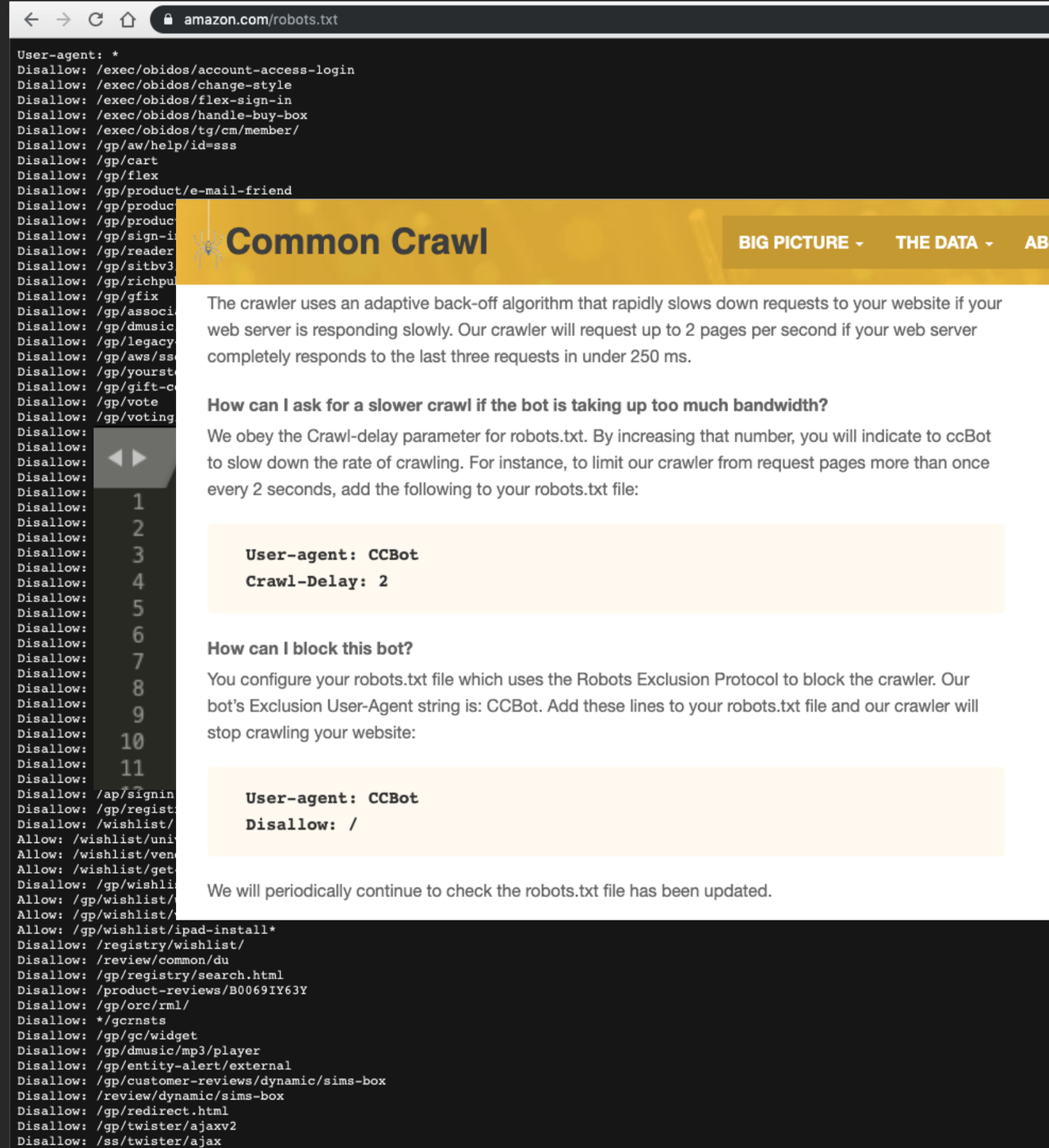
Examples of Good Bots:

- Crawlers
- Scrapers
- Automation
- Testing/Quality Assurance
- Monitors



Good bot etiquette

- ✓ Use the API when available
- ✓ Self-Identify
- ✓ Follow robots.txt
- ✓ Respect meta tags like `nofollow`, `noindex`
- ✓ Meter requests
- ✓ Cache data between requests



Bot attacks

Infrastructure Attacks

- Distributed Denial of Service (DDoS)
  - SYN Flood
  - UDP reflection
  - HTTP Flood

https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

Introduction: Denial of Service Attacks

A Denial of Service (DoS) attack is a deliberate attempt to make your website or application unavailable to users, such as by flooding it with network traffic. To achieve this, attackers use a variety of techniques that consume large amounts of network bandwidth or tie up other system resources, disrupting access for legitimate users. In its simplest form, a lone attacker uses a single source to execute a DoS attack against a target, as shown in Figure 1.



Figure 1: Diagram of DoS Attack

But in a Distributed Denial of Service (DDoS) attack, an attacker uses multiple sources – which may be distributed groups of malware infected computers, routers, IoT devices, and other endpoints– to orchestrate an attack against a target. As illustrated in the following DDoS attack diagram (Figure 2), a network of compromised hosts participates in the attack, generating a flood of packets or requests to overwhelm the target.

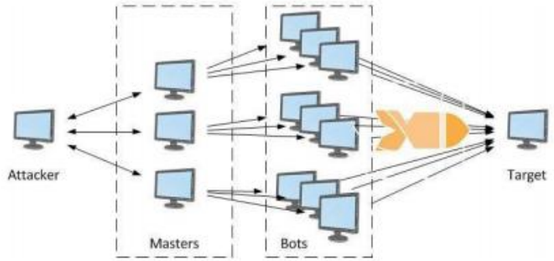


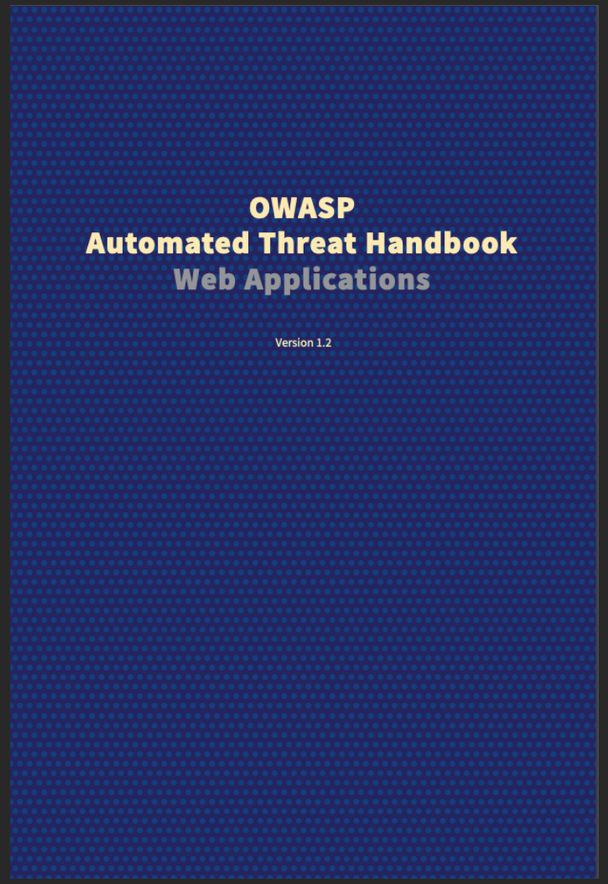
Figure 2: Diagram of DDoS Attack

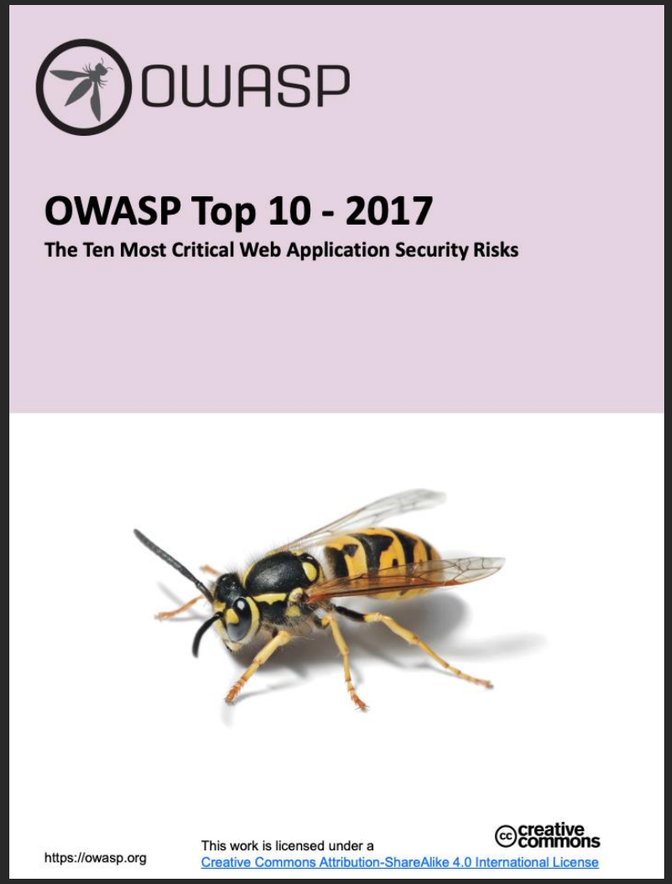
DDoS attacks are most common at layers 3, 4, 6, and 7 of the Open Systems Interconnection (OSI) model, which is described in Table 1. Layer 3 and 4 attacks correspond to the Network and Transport layers of the OSI model. We'll refer to these collectively as *infrastructure layer attacks*. Layer 6 and 7 attacks correspond to the Presentation and Application layers of the OSI model. We'll address these together as *application layer attacks*. We describe examples of these attack types in the next sections.

AWS DDoS metrics

1,399,370	Total number of attacks
942	Largest bit rate (Gbps)
364	Largest packet rate (Mpps)
1,585,615	Largest request rate (rps)

Bot attacks





Application Attacks

OWASP Top 10

- SQL Injection
- Cross Site Scripting (XSS)

OWASP Automated Threats

- Vulnerability Scanning
- Scraping
- Account Takeover (ATO)

Bot attack impact



Infrastructure Attacks

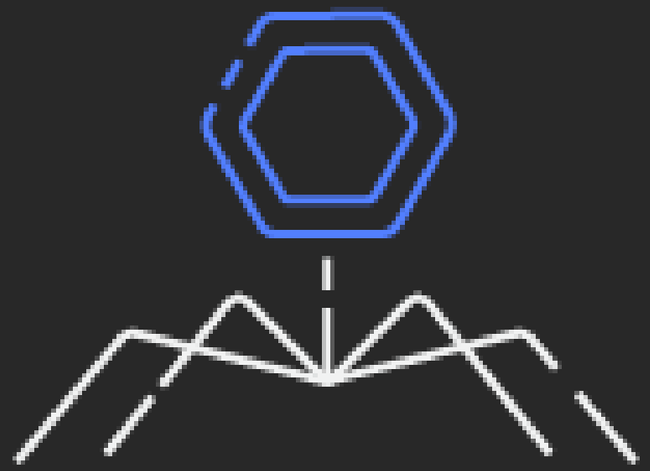
- Increased infrastructure costs
- Downtime and instability
- Manual intervention
- Lost income



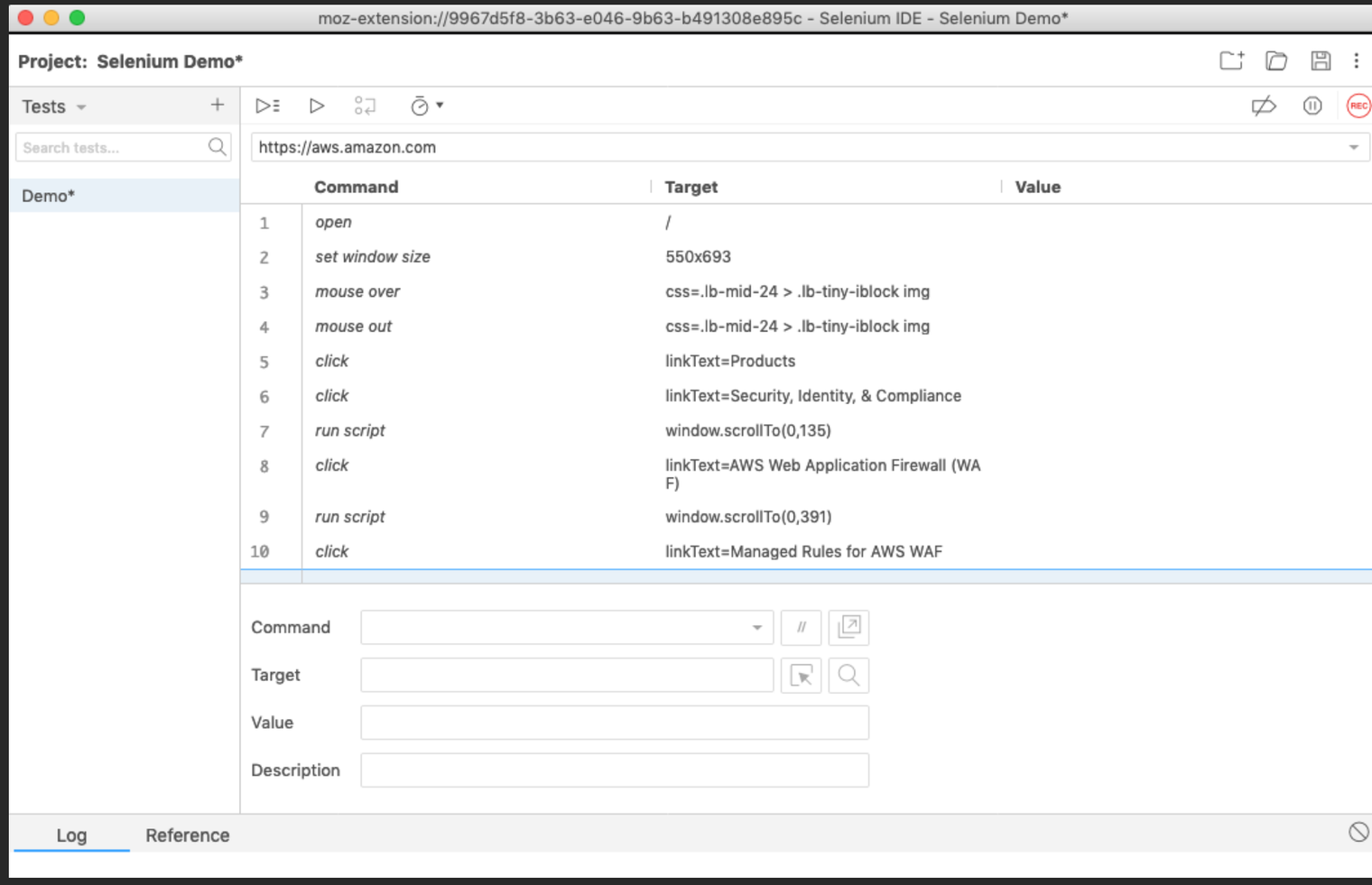
Application Attacks

- Stolen Data
- Compromised Credentials
- Spam / Fake Reviews
- Loss of goodwill
- Financial repercussions

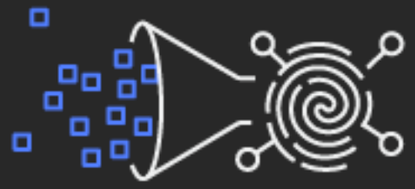
Simple bots



- Known Automation Tools
- Single Device/IP
- Missing or malformed request data



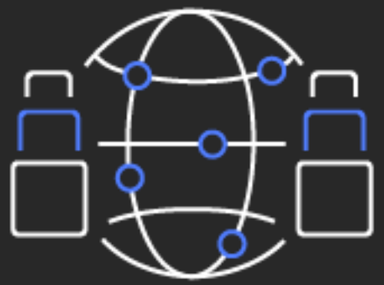
Advanced bot characteristics



- Executes JavaScript
- Generates valid fingerprints



- Mimics human interaction
- Emulates workflows



- Distributed widely
- Masks origin

Bot attack mitigation



Architecture

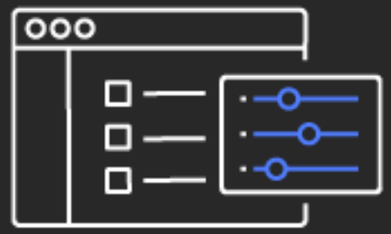


Application



DDoS Service

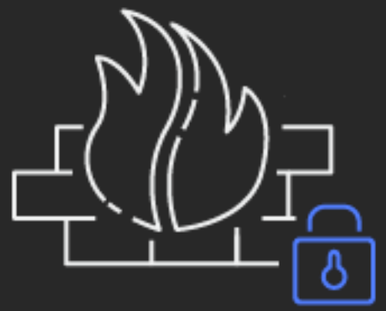
+



Configuration



Alerting



Web Application Firewall

AWS offerings

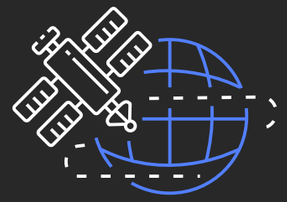
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Our mission



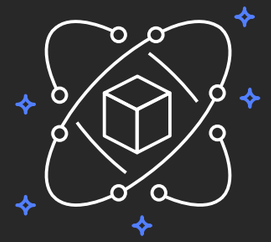
Protect Customers

Protect against the evolving internet threat landscape



Protect AWS

Protect all service infrastructure and availability



Integrate with AWS

Make it easy for customers to implement security measures

Our services



AWS
Shield



AWS WAF

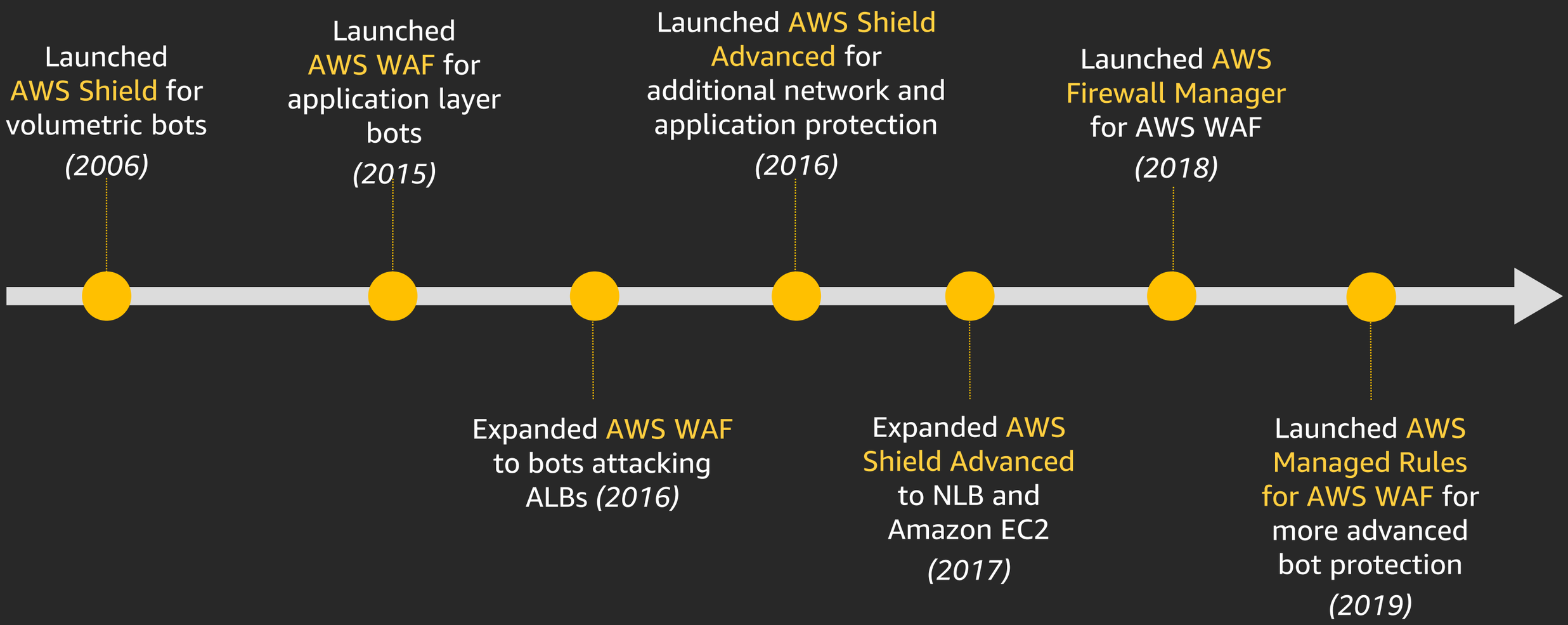


AWS
Firewall
Manager



AWS
Shield
Advanced

Our journey


Launched AWS Shield for volumetric bots (2006)
Launched AWS WAF for application layer bots (2015)
Expanded AWS WAF to bots attacking ALBs (2016)
Launched AWS Shield Advanced for additional network and application protection (2016)
Expanded AWS Shield Advanced to NLB and Amazon EC2 (2017)
Launched AWS Firewall Manager for AWS WAF (2018)
Launched AWS Managed Rules for AWS WAF for more advanced bot protection (2019)

What's new in AWS WAF?



Write hundreds of rules



Document-based rule writing in JSON



Streamlined console and API workflow



New detection capabilities

AWS Managed Rules for AWS WAF

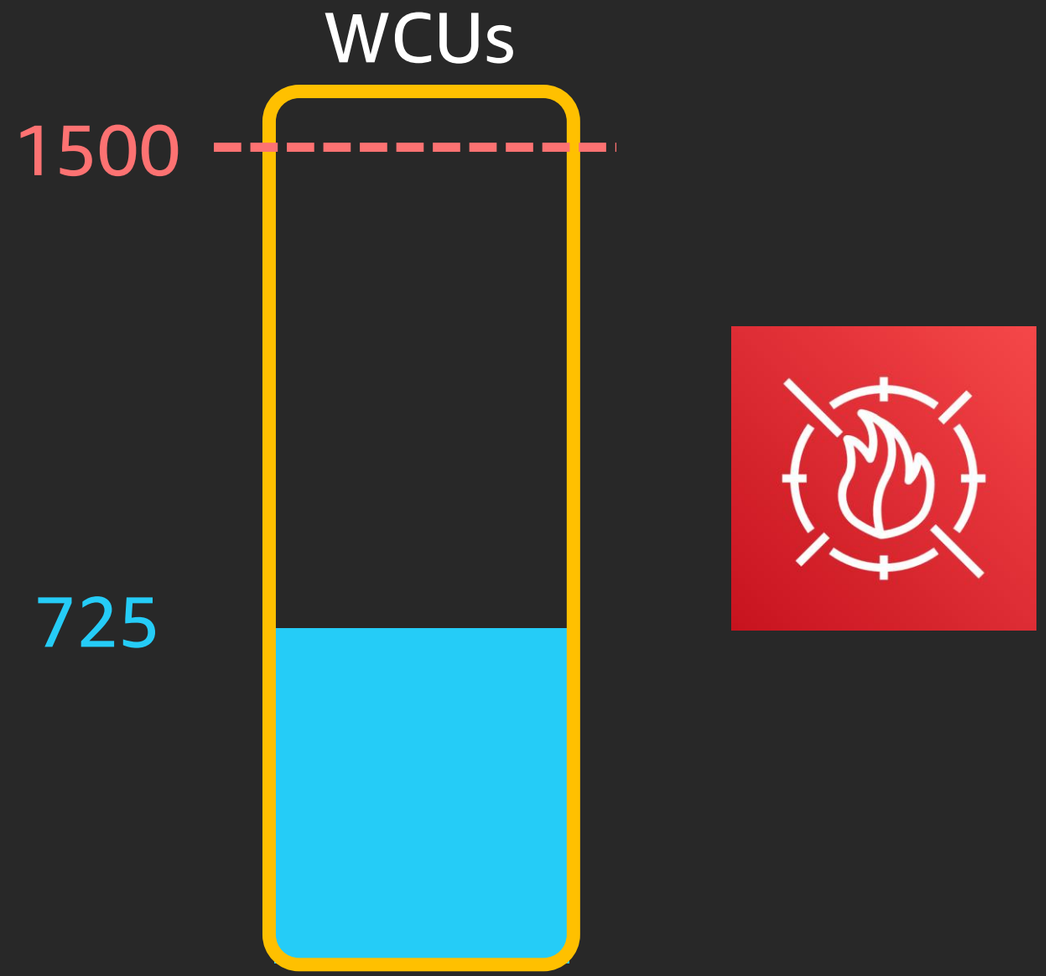
Set of rules built directly into AWS WAF

- Curated and maintained by the AWS Threat Research Team (TRT)
- Leverages security knowledge and threat intelligence gained within Amazon.com
- Primarily influenced by OWASP Top 10

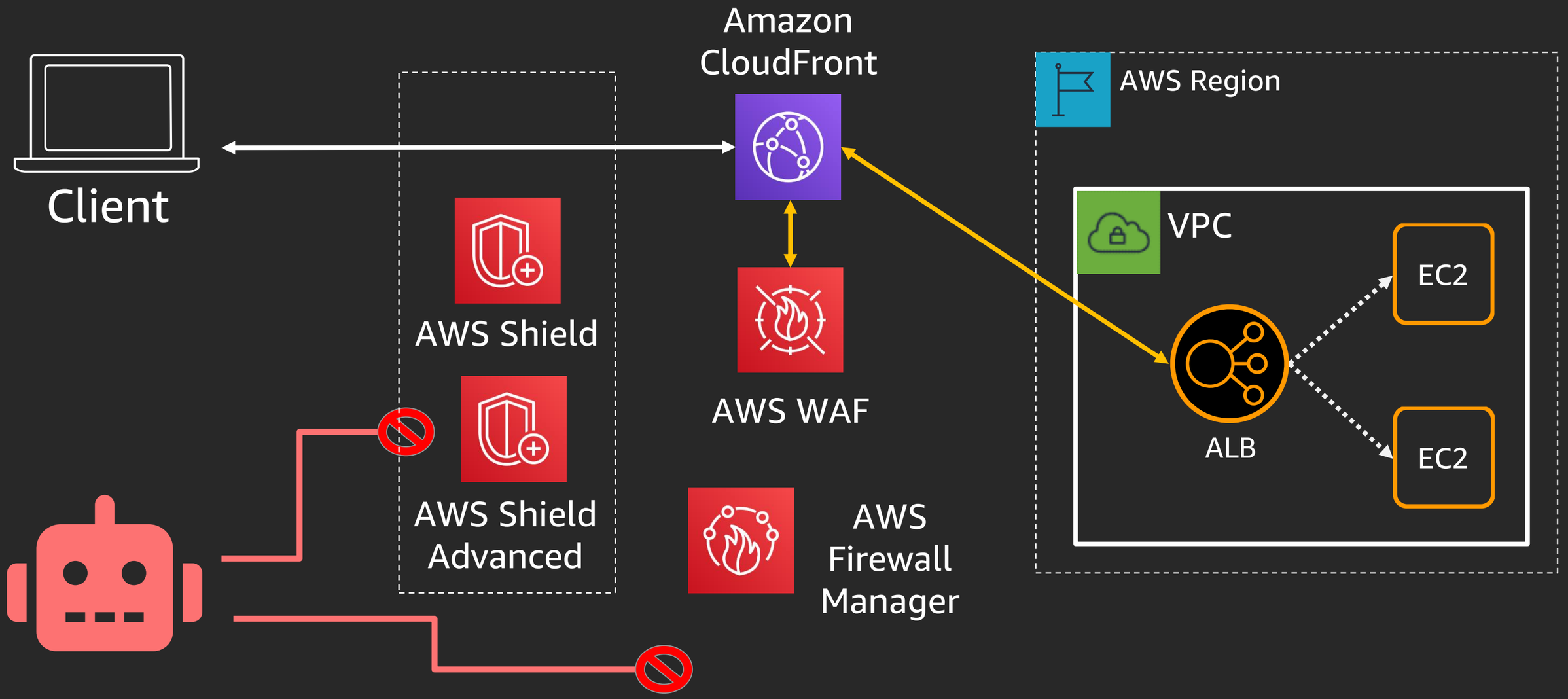
Category	Ruleset	Description	WCU
CRS	Core Ruleset	Based on OWASP Top 10	700
EXR	Admin Protection	Blocks common administrative access attempts	100
EXR	SQL DB	Predefined SQL injection rules on certain headers	200
EXR	Linux	Blocks path traversal attempts on Linux-based OS	200
EXR	Known Bad Inputs	Blocks well-known bad request indicators	200
EXR	PHP	Blocks PHP specific exploits	100
EXR	WordPress	Blocks WordPress specific exploits	100
EXR	POSIX	Blocks path traversal attempts on Unix-based OS	100
EXR	Windows	Blocks path traversal attempts on Windows-based OS	200
IP List	Amazon IP Reputation List	Blocks IP that is known to have bot activities	25

AWS Managed Rules for AWS WAF

- Core Ruleset
- Amazon IP List
- WordPress
- SQL Database
- Windows
- Known Bad Inputs
- Linux
- Unix
- PHP Application
- Admin Protection



Layered approach to protection



Mitigating bot impact
Protect Your Network Infrastructure

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Protecting your network infrastructure



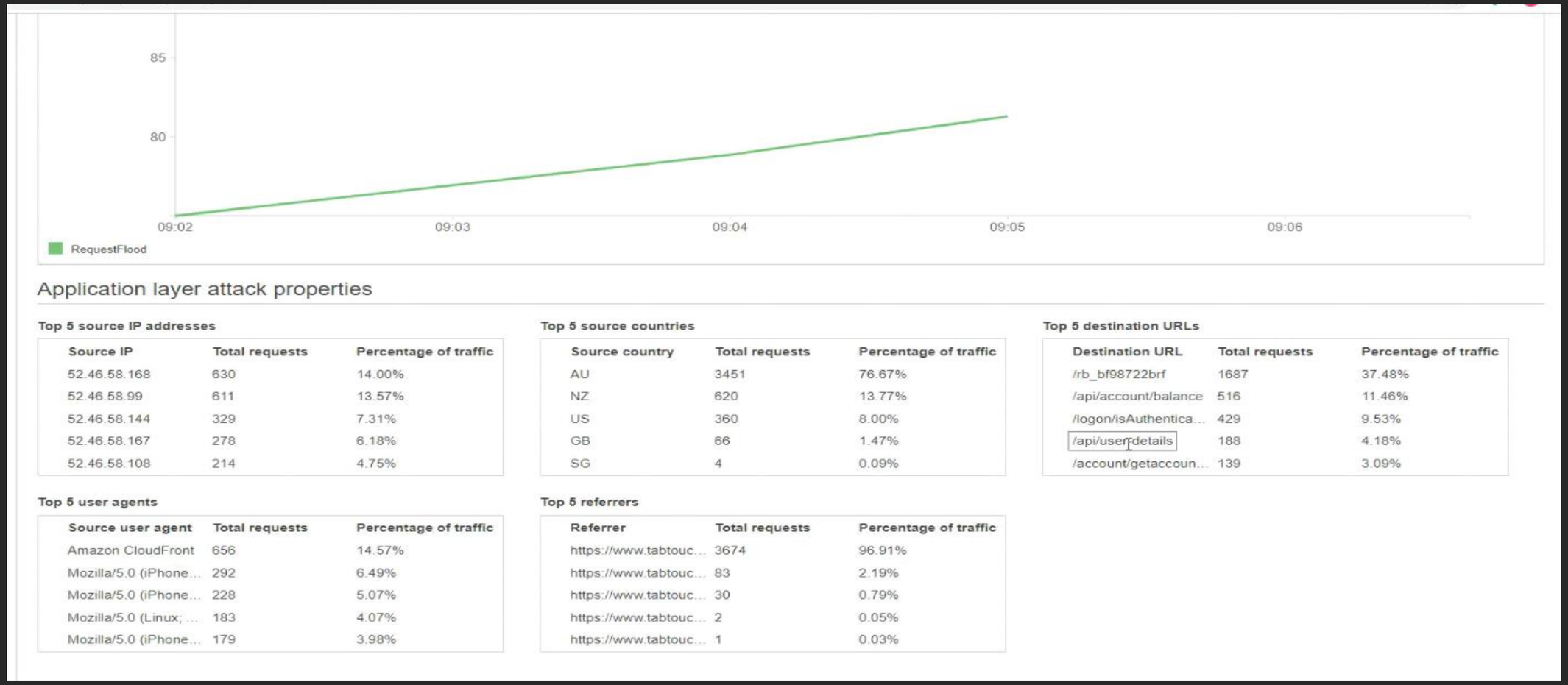
AWS Shield Standard

- Protects resources against DDoS attacks
- Automatic mitigation for network attacks

Protecting your network infrastructure



AWS Shield Advanced



Application layer attack properties

Top 5 source IP addresses

Source IP	Total requests	Percentage of traffic
52.46.58.168	630	14.00%
52.46.58.99	611	13.57%
52.46.58.144	329	7.31%
52.46.58.167	278	6.18%
52.46.58.108	214	4.75%

Top 5 source countries

Source country	Total requests	Percentage of traffic
AU	3451	76.67%
NZ	620	13.77%
US	360	8.00%
GB	66	1.47%
SG	4	0.09%

Top 5 destination URLs

Destination URL	Total requests	Percentage of traffic
/rb_bf98722brf	1687	37.48%
/api/account/balance	516	11.46%
/logon/isAuthentica...	429	9.53%
/api/userdetails	188	4.18%
/account/getaccoun...	139	3.09%

Top 5 user agents

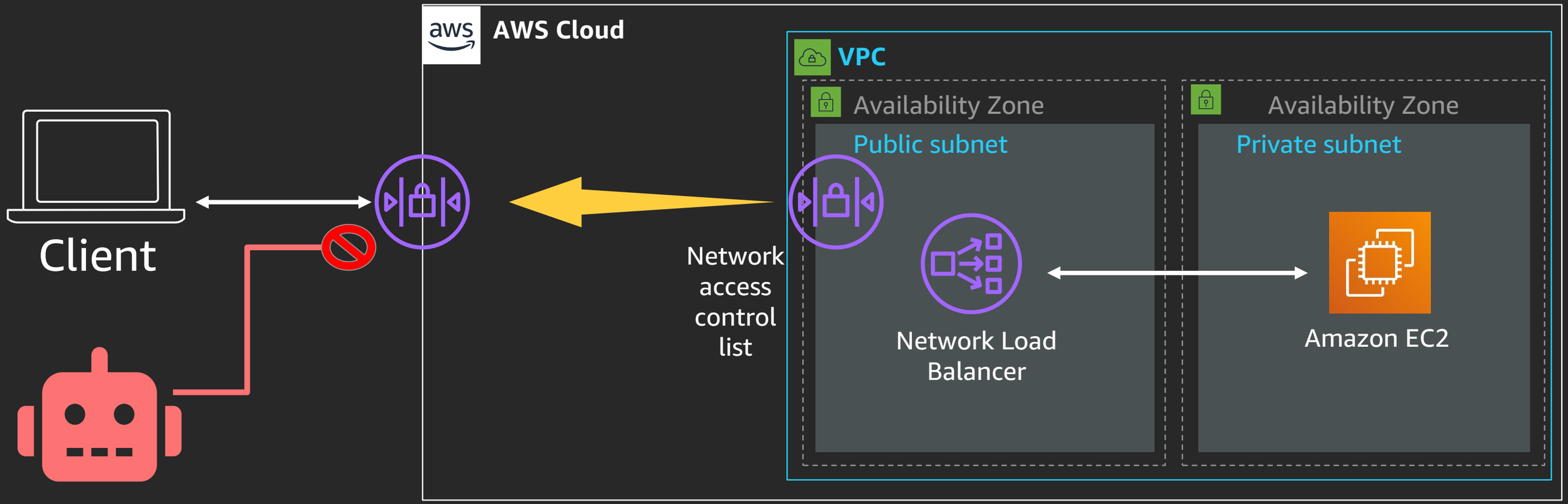
Source user agent	Total requests	Percentage of traffic
Amazon CloudFront	656	14.57%
Mozilla/5.0 (iPhone...	292	6.49%
Mozilla/5.0 (iPhone...	228	5.07%
Mozilla/5.0 (Linux; ...	183	4.07%
Mozilla/5.0 (iPhone...	179	3.98%

Top 5 referrers

Referrer	Total requests	Percentage of traffic
https://www.tabtouc...	3674	96.91%
https://www.tabtouc...	83	2.19%
https://www.tabtouc...	30	0.79%
https://www.tabtouc...	2	0.05%
https://www.tabtouc...	1	0.03%

Protecting your network infrastructure

AWS Shield Advanced



Mitigating bot impact

Managing Simple Bots

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

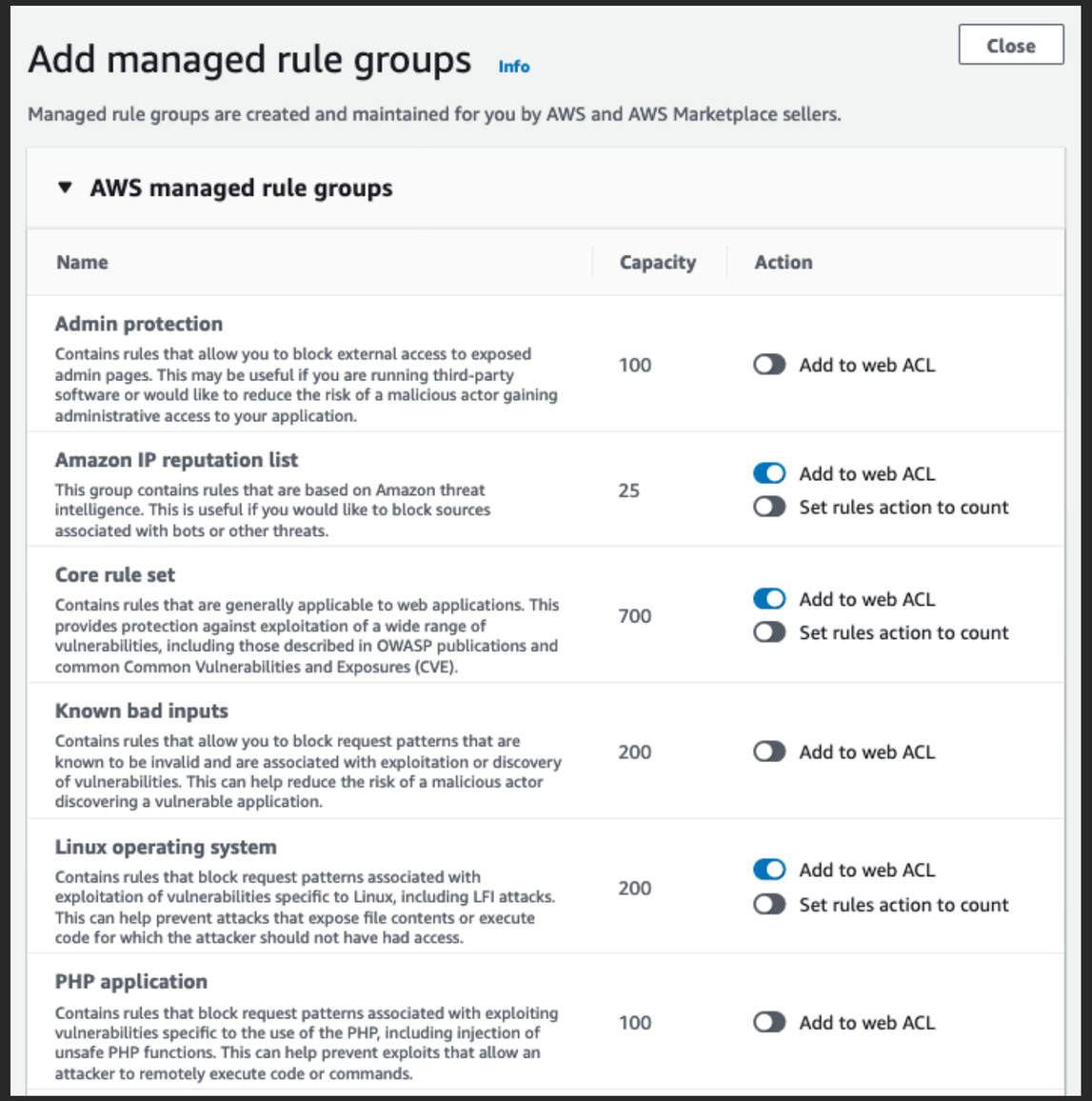
aws

Use Amazon.com threat intelligence

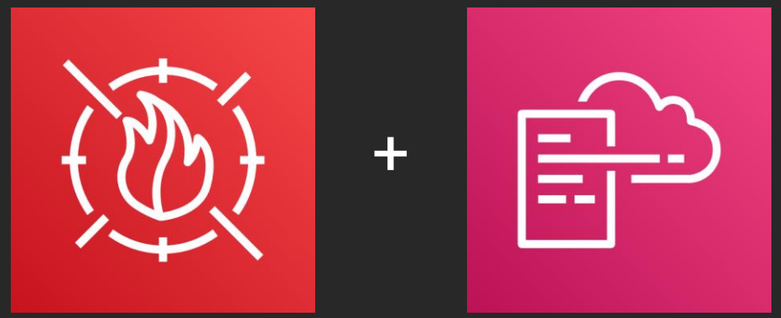


AWS Managed Rules for AWS WAF

Amazon IP reputation list



Leverage external threat feeds



AWS WAF Security Automations

Known IP reputation list

AWS WAF Security Automations introduction



AWS CloudFormation



AWS WAF



Lambda



Amazon Kinesis



Amazon S3



API Gateway



Amazon CloudWatch

- Whitelist
- Blacklist
- SQL Injection
- XSS
- HTTP Flood
- Scanners & Probes
- IP Reputation Lists
- Bad Bots

WAF Security Automations: Simple to deploy

AWS WAF Security Automations

Version 2.3.0
Last updated: 04/2019
Author: AWS

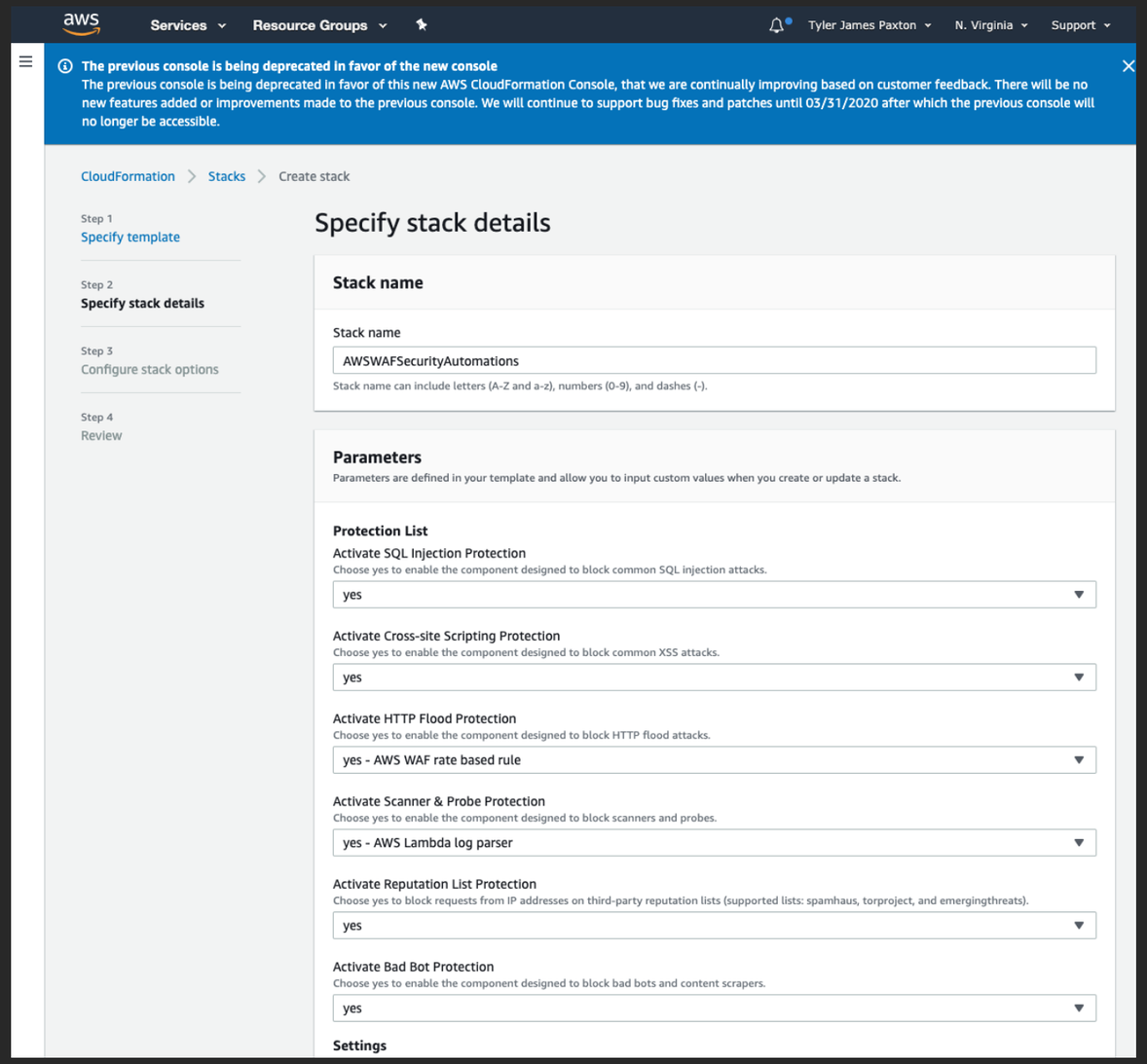
Estimated deployment time: 15 min

Source code
CloudFormation template

View deployment guide

Launch solution in the AWS Console





https://aws.amazon.com/solutions/aws-waf-security-automations/

AWS WAF Security Automations: Customizable templates

aws-waf-security-automations (1).template — UNREGISTERED

aws-waf-security-automations (1).template

```
AWSTemplateFormatVersion: 2010-09-09
Description: >-
  (SO0006) - AWS WAF Security Automations v2.3.0: This AWS CloudFormation template helps
  you provision the AWS WAF Security Automations stack without worrying about creating and
  configuring the underlying AWS infrastructure.

  **WARNING** This template creates an AWS Lambda function, an AWS WAF Web ACL, an Amazon S3 bucket,
  and an Amazon CloudWatch custom metric. You will be billed for the AWS resources used if you
  create a stack from this template.

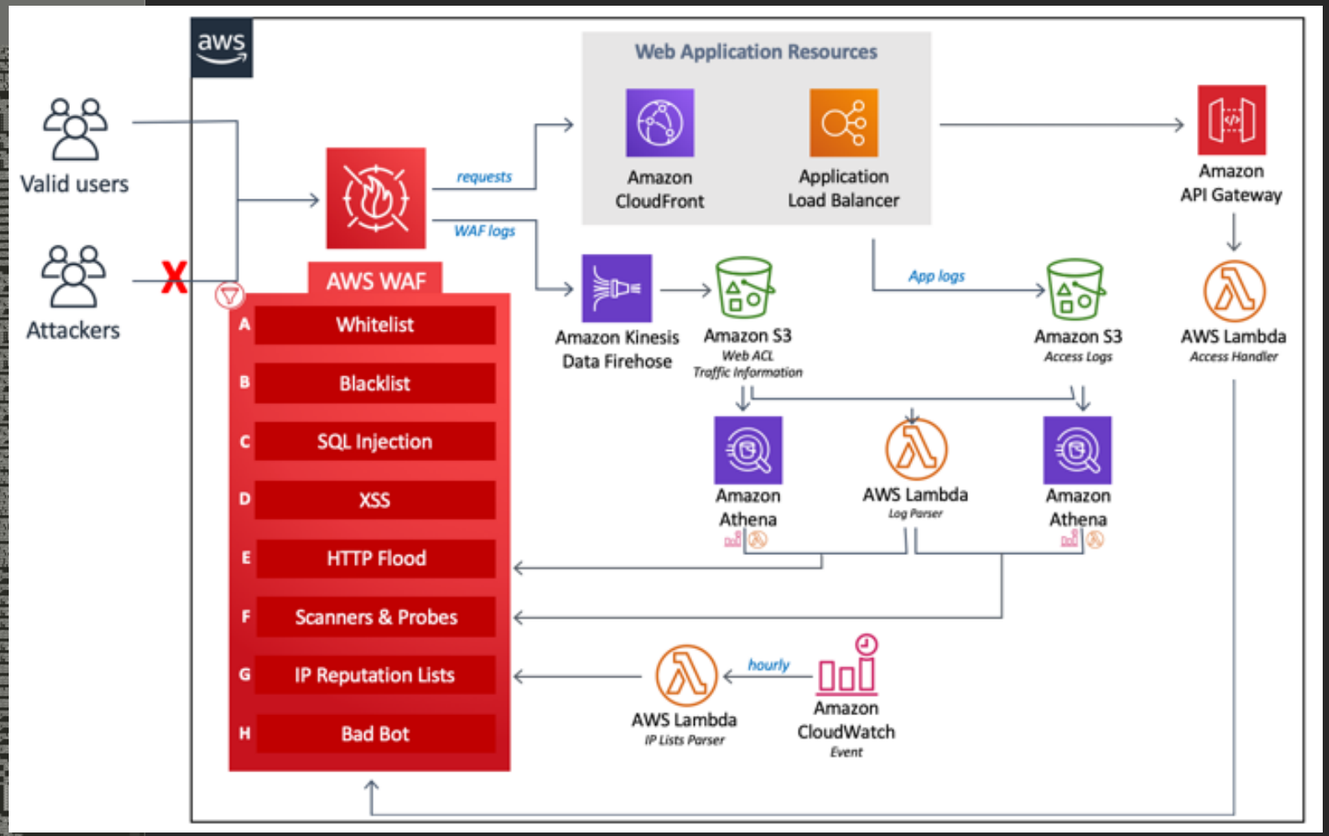
  **NOTICE** Copyright 2019 Amazon.com, Inc. or its affiliates. All Rights Reserved. Licensed under
  the Amazon Software License (the License). You may not use this file except in compliance with the
  License. A copy of the License is located at http://aws.amazon.com/asl/ or in the license file
  accompanying this file. This file is distributed on an AS IS BASIS, WITHOUT WARRANTIES OR
  CONDITIONS OF ANY KIND, express or implied. See the License for the specific language governing
  permissions and limitations under the License.


Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
          default: Protection List
        Parameters:
          - ActivateSqlInjectionProtectionParam
          - ActivateCrossSiteScriptingProtectionParam
          - ActivateHttpFloodProtectionParam
          - ActivateScannersProbesProtectionParam
          - ActivateReputationListsProtectionParam
          - ActivateBadBotProtectionParam

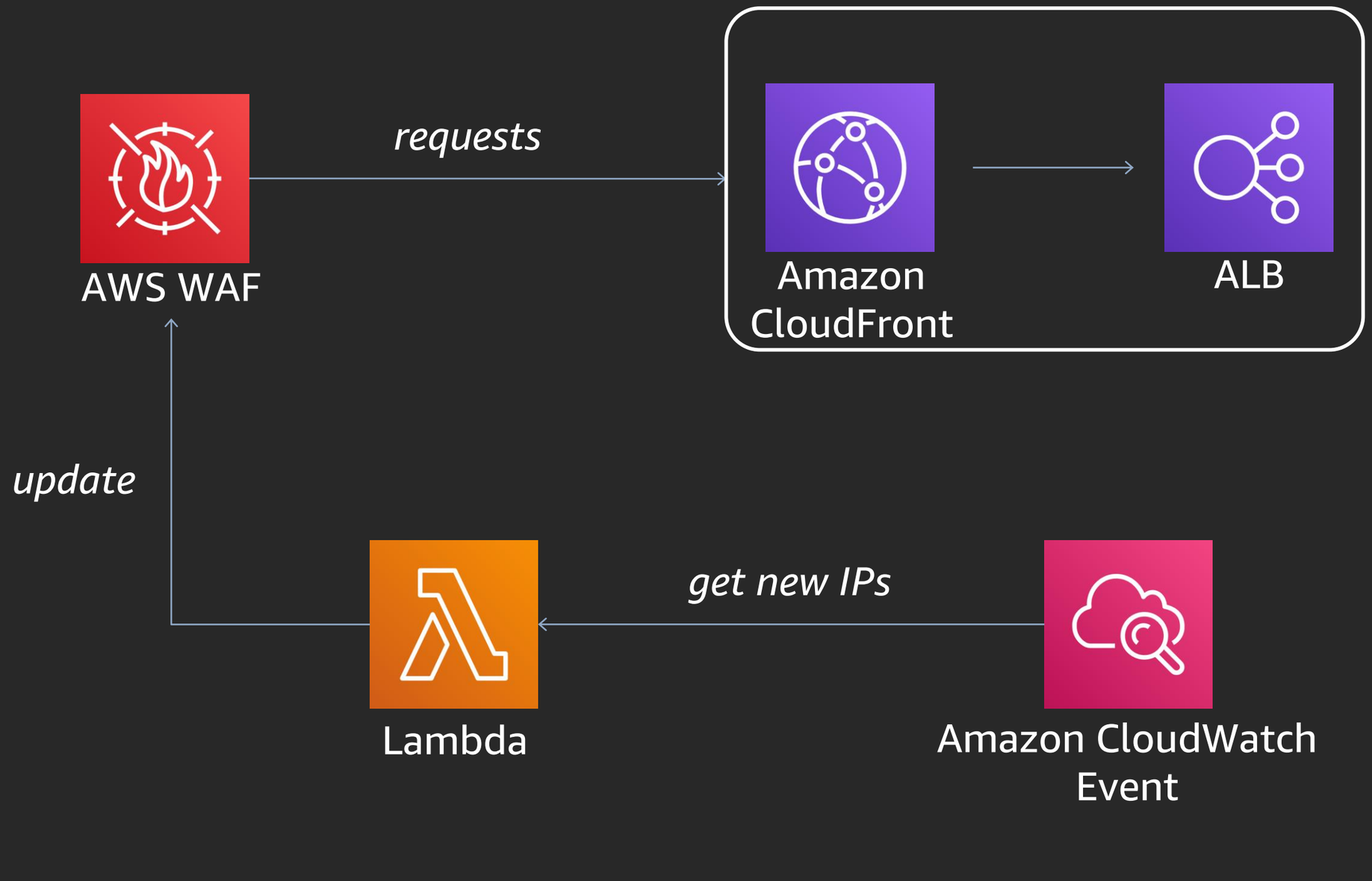
      - Label:
          default: Settings
        Parameters:
          - EndpointType
          - AppAccessLogBucket

```

Line 4, Column 91 — Tab Size: 4 — Plain Text



AWS WAF Security Automations IP Reputation lists



AWS WAF Security Automations IP reputation lists



Amazon CloudWatch

```
{
  "lists": [
    {"url":"https://www.spamhaus.org/drop/drop.txt"},
    {"url":"https://www.spamhaus.org/drop/edrop.txt"},
    {"url":"https://check.torproject.org/exit-addresses", "prefix":"ExitAddress"},
    {"url":"https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt"}
  ],
  "apiType": "waf",
  "region": "us-east-1",
  "ipSetIds": ["30b15e8a-f085-4555-a1c3-7abb156b9dac"]
}
```



Lambda

Function name ▲	Description	Runtime ▽	Code size ▽
AWSWAFSecurityAutomations-LambdaWAFReputationLists-1983EXD3977MD	This lambda function checks third-party IP reputation lists hourly for new IP ranges to block. These lists include the Spamhaus Dont Route Or Peer (DROP) and Extended Drop (EDROP) lists, the Proofpoint Emerging Threats IP list, and the Tor exit node list.	Node.js 8.10	976.6 kB

AWS WAF Security Automations IP reputation lists

```
526                 ipSetDescriptors.forEach(function (ipSetDescriptor) {
527                     var cidr = ipSetDescriptor.Value;
528                     var found;
529                     // try to find the IPSet descriptor on the ranges slice
530                     for (var i = 0; i < rangeSlice.length; i++) {
531                         if (rangeSlice[i].cidr === cidr) {
532                             rangeSlice.splice(i, 1);
533                             found = true;
534                             break;
535                         }
536                     }
537                     // if this descriptor is not found in the ranges slice, it is deleted
538                     if (!found) updates.push({ Action: 'DELETE', IPSetDescriptor: ipSetDescriptor });
539                 });
```

1 →

2 →

```
551                     Array.prototype.push.apply(tasks, batches.map(function(updateBatch) {
552                         return function (callback) {
553                             async.waterfall([
554                                 function (callback) {
555                                     waf.getChangeToken({}, callback);
556                                 },
557                                 function (response, callback) {
558                                     console.log('[handler] Updating IP set ' + ipSetName + ' with ' + updateBatch.length + ' updates');
559                                     waf.updateIPSet({
560                                         ChangeToken: response.ChangeToken,
561                                         IPSetId: ipSet.IPSetId,
562                                         Updates: updateBatch
563                                     }, callback);
564                                 }
```

3 →

4 →

AWS WAF Security Automations IP reputation lists



AWS WAF

When a request originates from an IP address in AWSWAFSecurityAutomations - IP Reputation Lists Set
IP Addresses in AWSWAFSecurityAutomations - IP Reputation Lists Set
167.114.113.127/32
102.13.240.0/20
213.160.32.233/32
190.53.135.159/32
185.220.101.3/32
185.35.136.0/22
91.83.93.105/32
104.153.244.0/22
185.180.192.0/22
185.113.128.30/32
..... (See all IP addresses and ranges here.)

Mitigating bot impact

Protect Your Application Against Advanced Attacks

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Prevent volumetric application attacks

If incoming traffic



Block/**Allow**

Matches:

- ✓ URI: /login.html
- ✓ Method: POST
- ✓ From: Country X

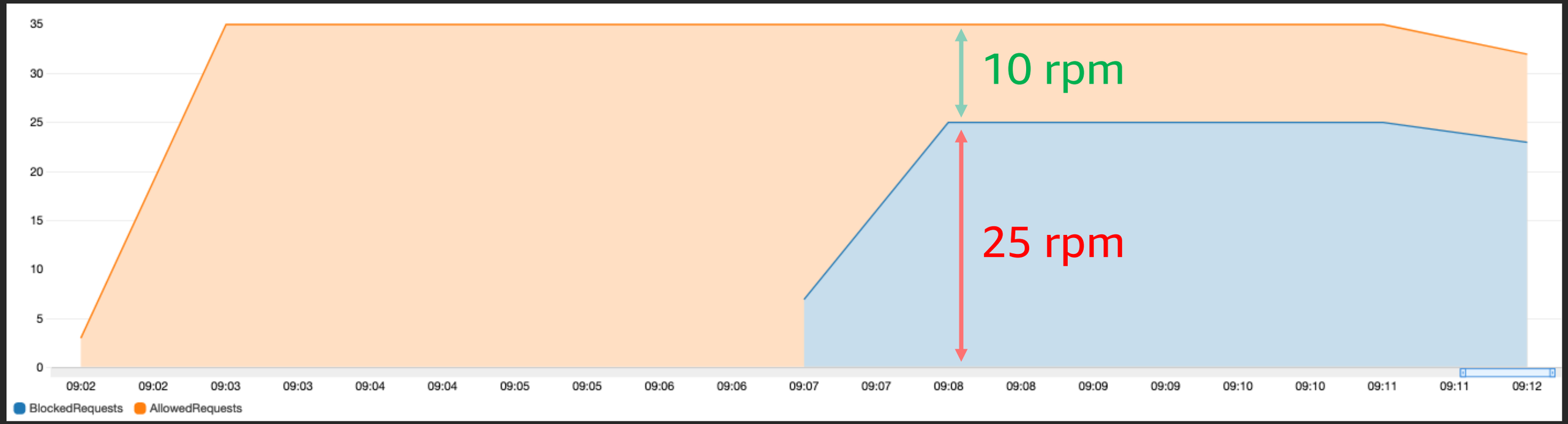
Rate exceeds:

100 requests per 5 minutes

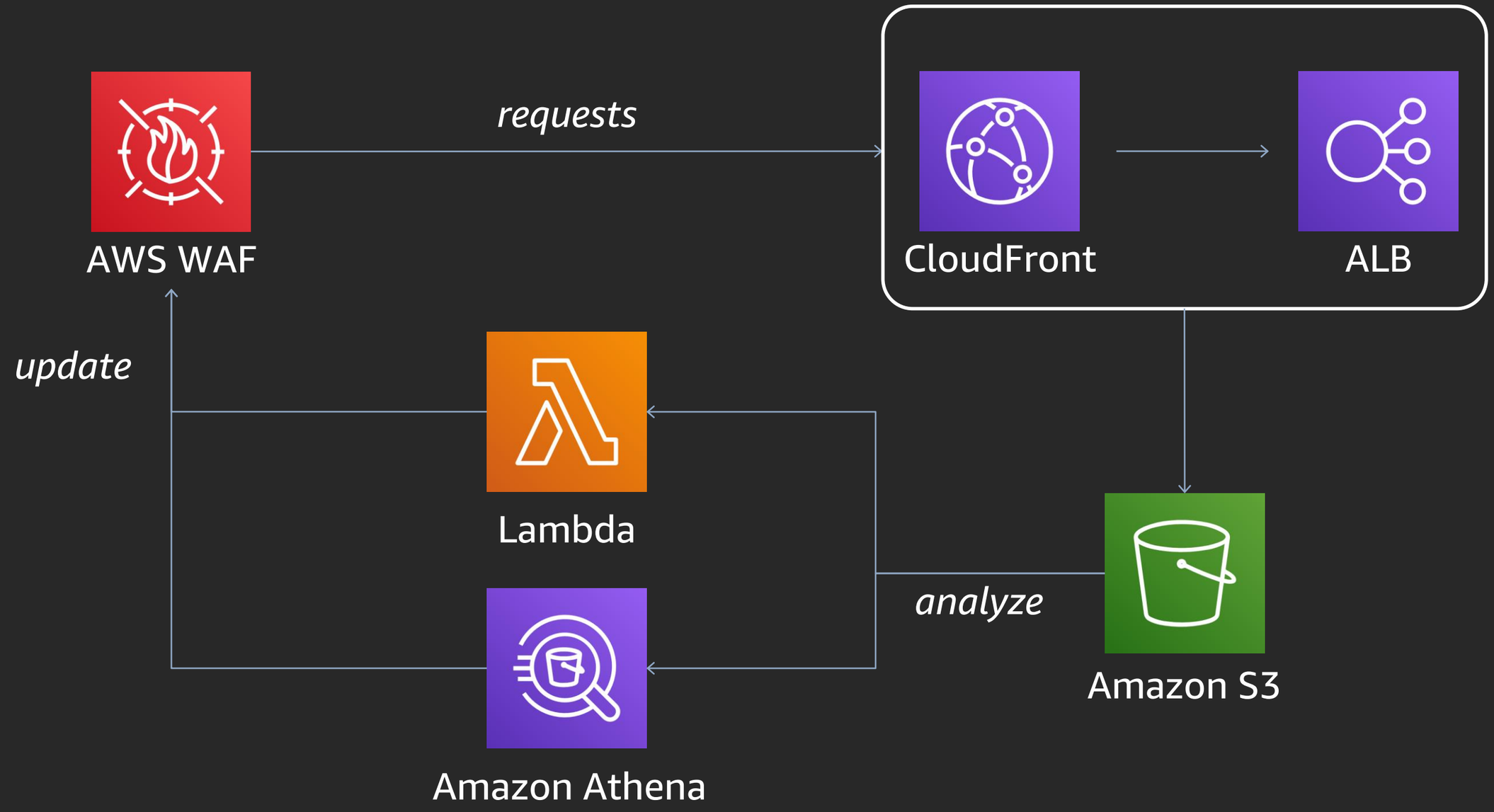
AWS WAF rate-based rules

Two source IPs sending requests:

- IP1: 10 requests per minute = 50 requests per 5 minutes
- IP2: 25 requests per minute = 125 requests per 5 minutes
- Rate is exceeded after 4 minutes and blocking starts



AWS WAF Security Automations: Account takeover



Mitigate account takeover attacks

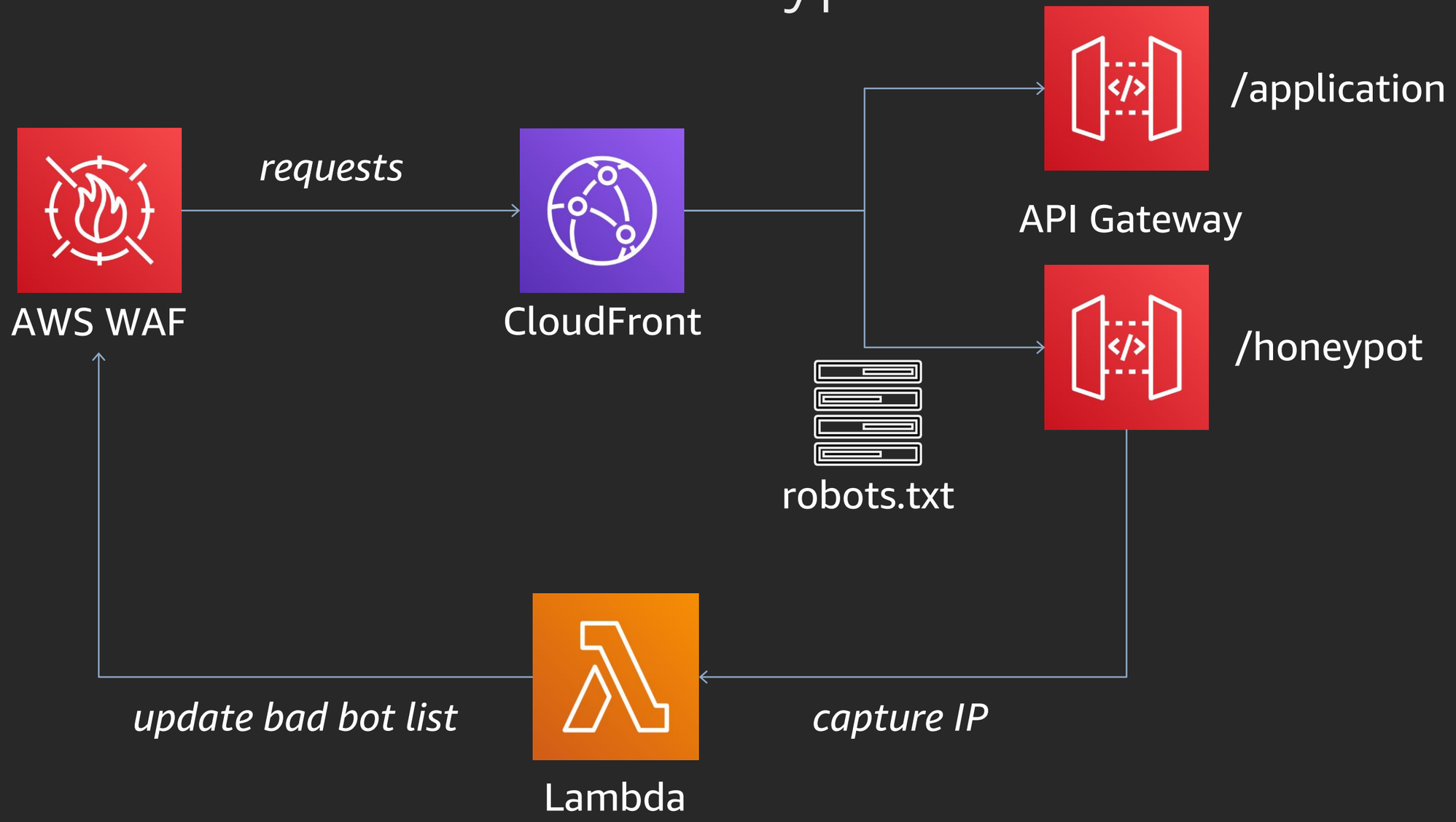
Complete control over:

- Error thresholds
- Block periods in minutes
- Error code matching
- URI list

AWSWAFSecurityAutomations-app_log_conf.json

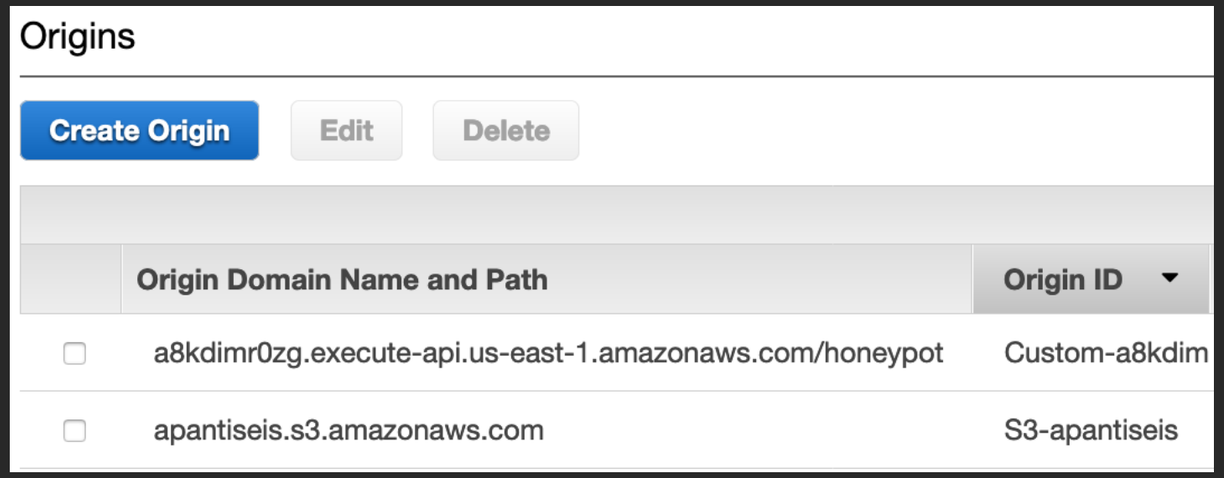
```
{
    "general":
    {
        "errorThreshold": 50,
        "blockPeriod": 240,
        "errorCodes":
        [
            "400",
            "401",
            "403",
            "404",
            "405"
        ]
    },
    "uriList": {"/login.html"}
}
```

Detect bad bot behavior: Honeypot



Detect bad bot behavior: Honeypot

Step 1: Set up your distribution



Step 2: robots.txt file

*User-agent: **
Disallow: /honeypot/

Step 3: Add hidden link

```
32    <div class="container" ng-controller="list">
33      <a href="/honeypot" rel="nofollow" style="display: none" aria-hidden="true">honeypot link</a>
34      <br>
```

Detect bad bot behavior: Honeypot

APIs (1)

Find APIs

Name	Description
Security Automations - WAF Bad Bot API	API created by AWS WAF Security Automations CloudFormation template. This endpoint will be used to capture bad bots.

```
209 #---------------------------------------------------------
210 # Read inputs parameters
211 #---------------------------------------------------------
212 logging.getLogger().info(event)
213 source_ip = event['headers']['X-Forwarded-For'].split(',')[
214
215 global waf
216 if environ['LOG_TYPE'] == 'alb':
217     session = boto3.session.Session(region_name=environ['RE
218     waf = session.client('waf-regional', config=Config(retr
219 else:
220     waf = boto3.client('waf', config=Config(retries={'max_a
221
222 waf_update_ip_set(environ['IP_SET_ID_BAD_BOT'], source_ip)
223
224 message = {}
225 message['message'] = "[%s] Thanks for the visit."%source_ip
226 response['body'] = json.dumps(message)
227
228 send_anonymous_usage_data()
```

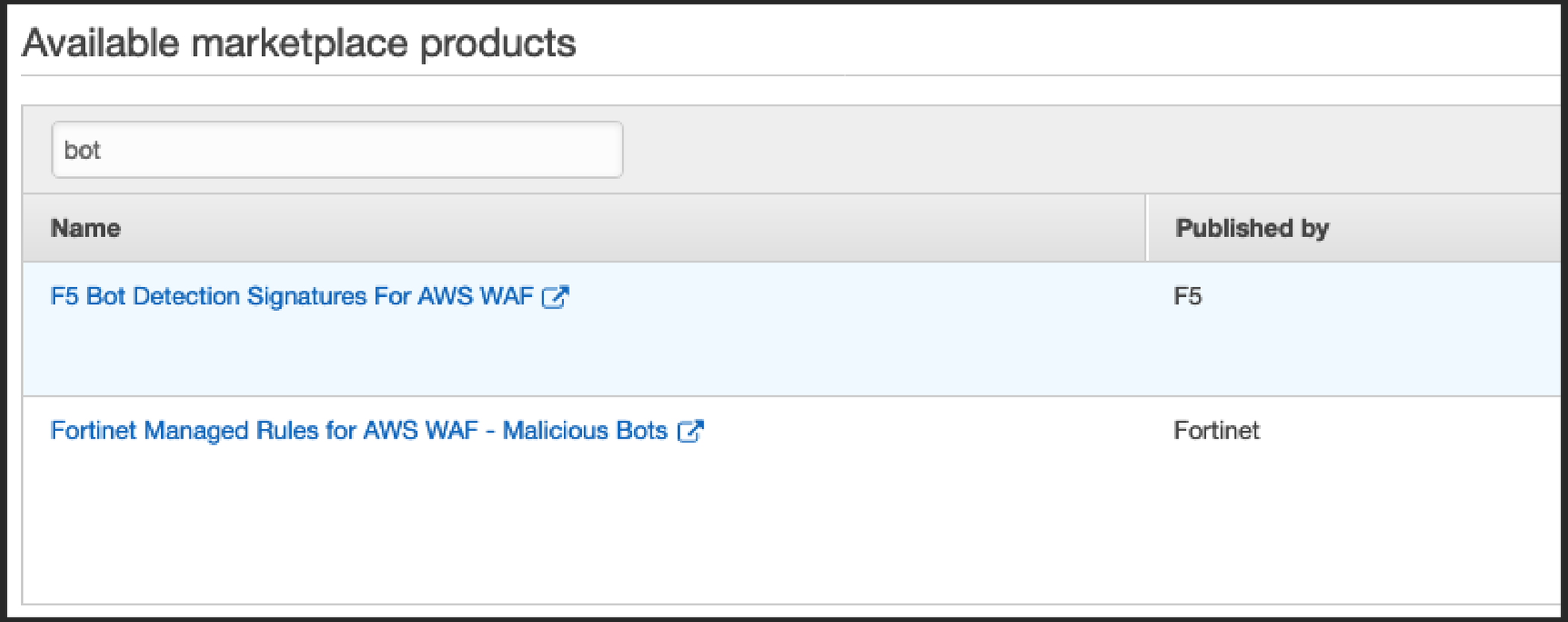
When a request originates from an IP address in AWSWAFSecurityAutomations - IP Bad Bot Set

IP Addresses in AWSWAFSecurityAutomations - IP Bad Bot Set
54.240.197.238/32
54.240.197.234/32

Managed Rules for AWS WAF



Use a Managed Ruleset from the AWS Marketplace



Bot mitigation vendors





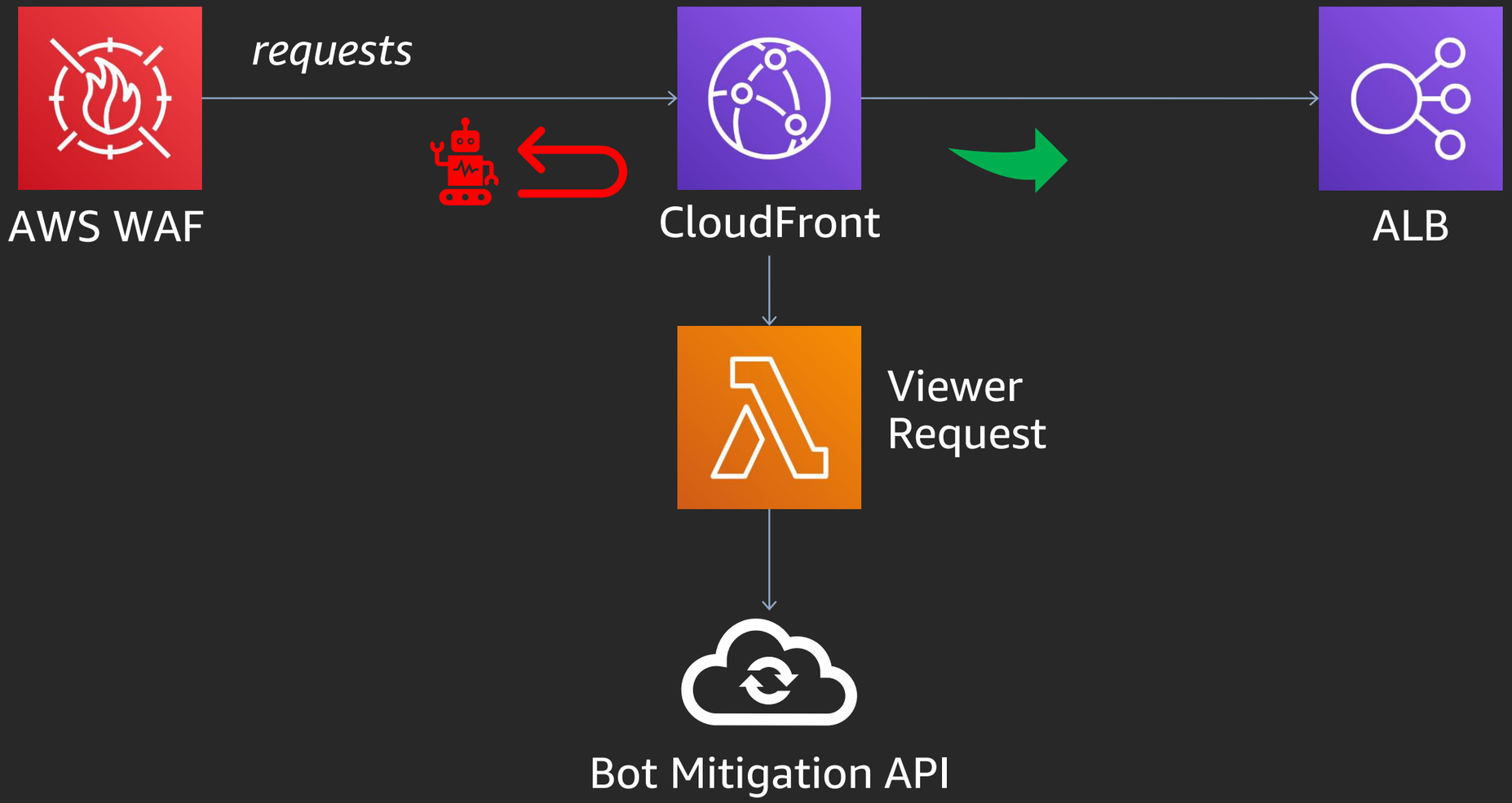




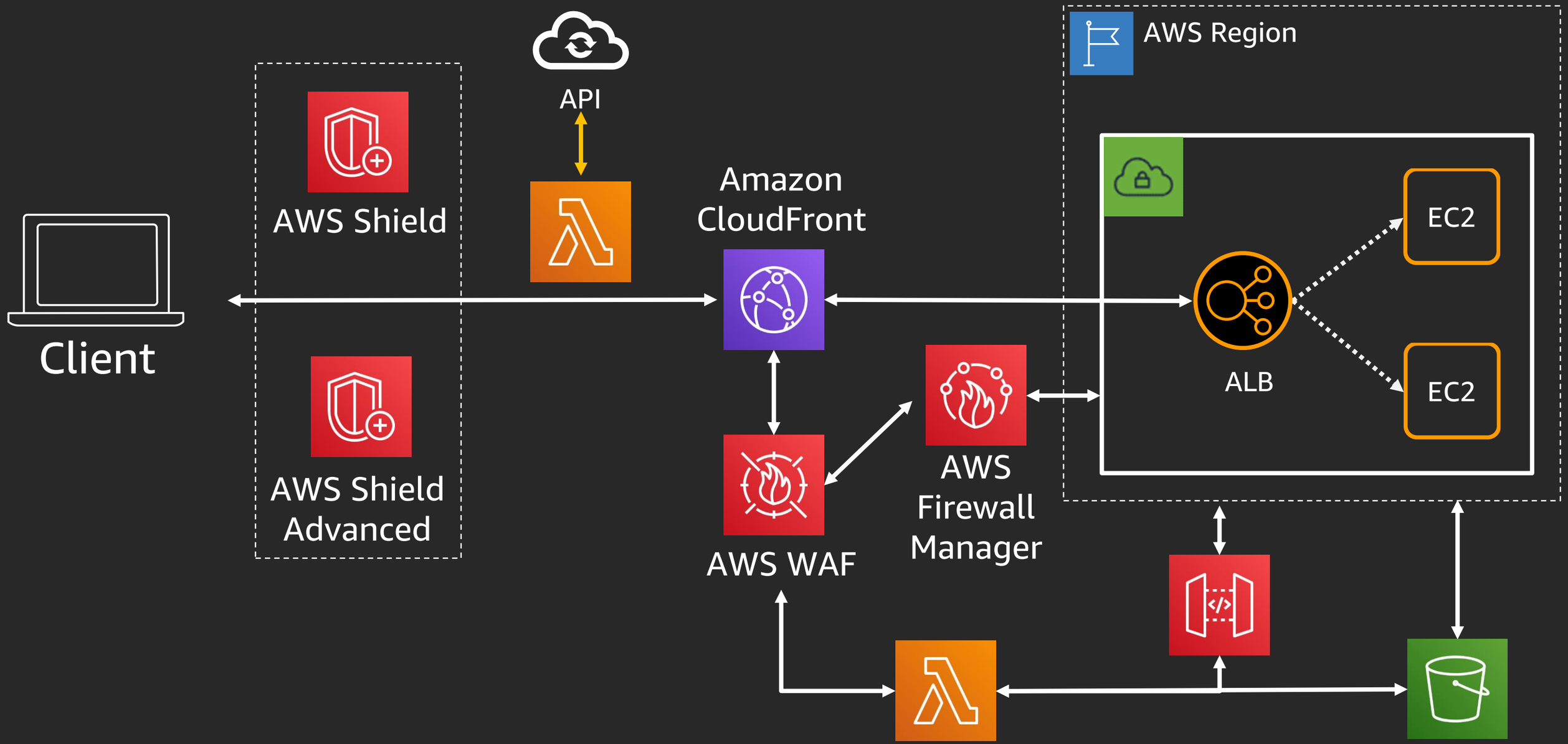




Integrations for additional bot mitigation



Layered approach to protection



Bot mitigation and WAF
Augmentation for Enterprise Retail

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Daemon Solutions



Paul Campbell

Head of Delivery *at* Daemon Solutions

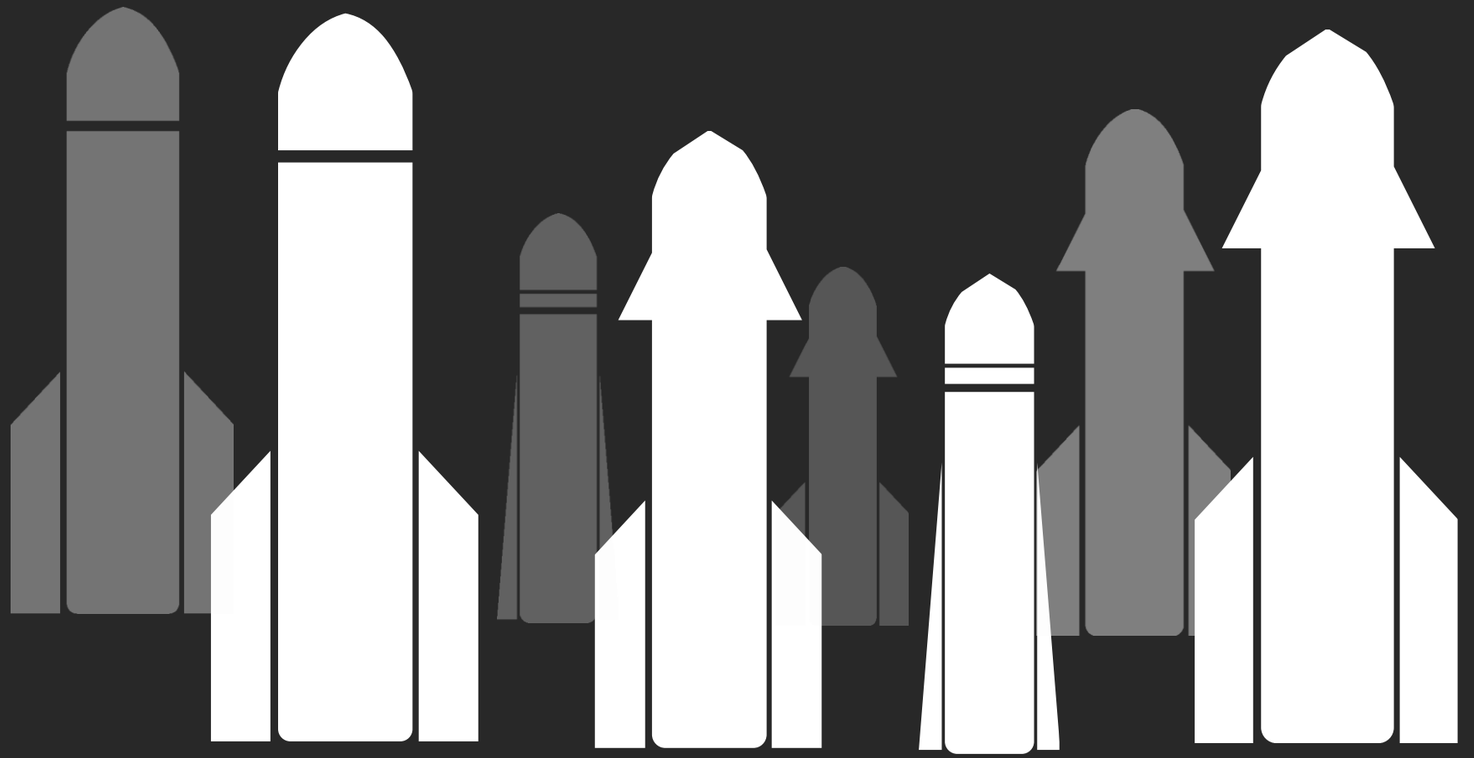
Retail

The Customer experience is paramount
But security is never a trade-off



Daemon Solutions

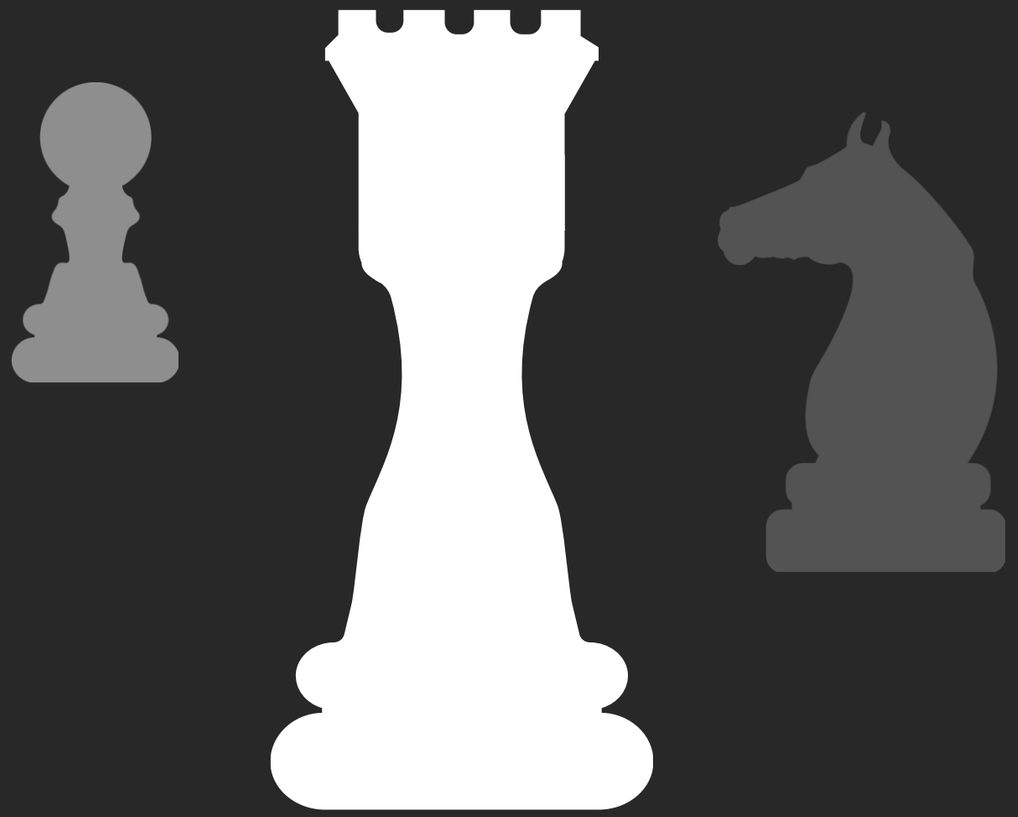
Security is like an arms race



Daemon Solutions

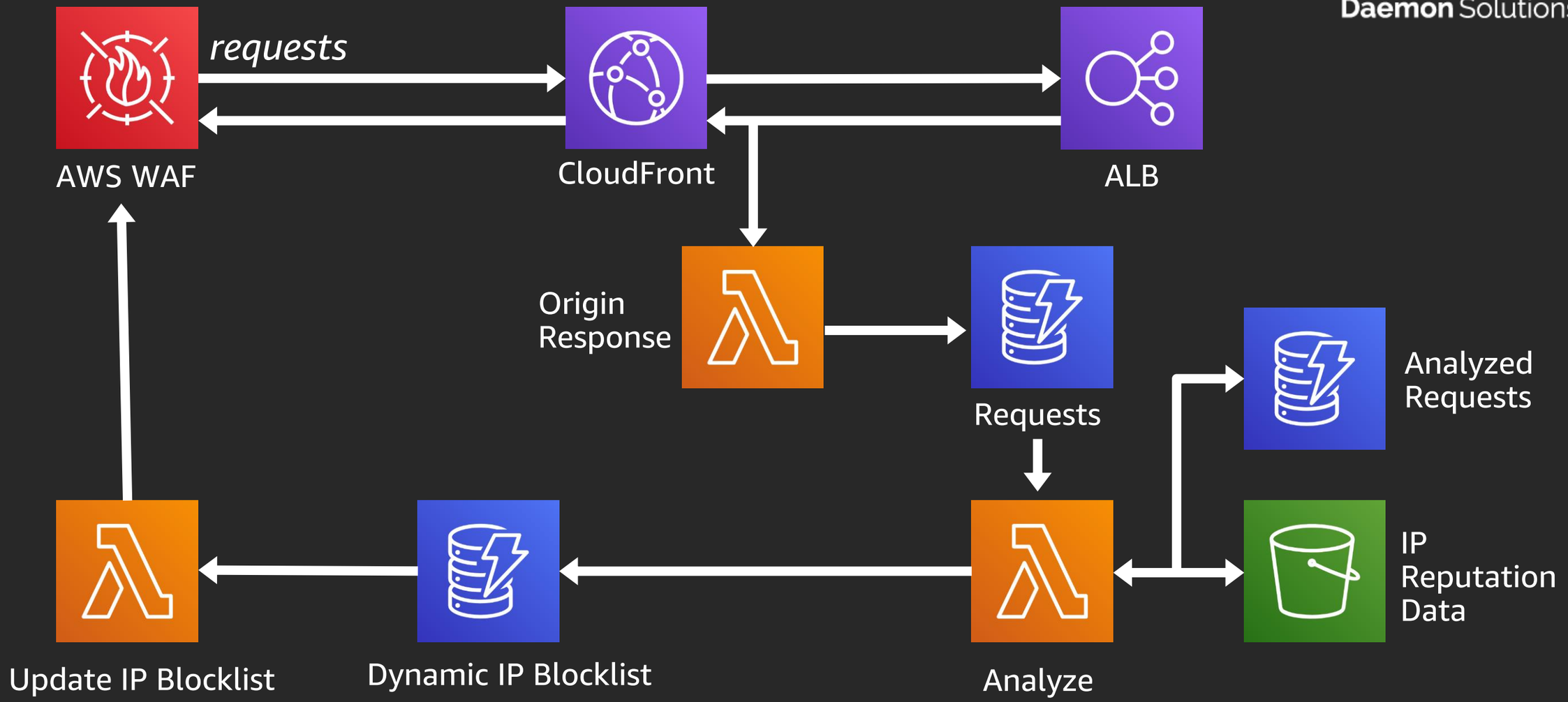
We need to be thinking two moves ahead

Daemon Solutions



Building on AWS

Daemon Solutions



Key metrics 

Daemon Solutions



4,000

Over 5 minutes



10ms

Added to interested URIs only



1 min

Max time to block malicious IPs



$1-$5/day*

Normal day - price of a cup of coffee!

Things to consider

Cost, monitoring, speed of execution



Daemon Solutions

Recap



Blocking Simple Bots

- Common bot signatures (AWS WAF Security automation, managed rules from AWS Marketplace)

Blocking Advanced Bots

- AWS managed rules, honeypot solutions, rate-based rules, bot mitigation software integrations

Learn security with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate cloud security skills



30+ free digital courses cover topics related to cloud security, including Introduction to Amazon GuardDuty and Deep Dive on Container Security



Classroom offerings, like AWS Security Engineering on AWS, feature AWS expert instructors and hands-on activities



Validate expertise with the **AWS Certified Security - Specialty** exam

Visit aws.amazon.com/training/paths-specialty/

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws training and certification

Thank you!

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws



Please complete the session survey in the mobile app.

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.