
AWS
re:Invent
DECEMBER 2 – 6, 2024 | LAS VEGAS, NV

CDN307-R

AWS WAF: What a BOT it?

Julian Ju
(he/him)
Sr Solutions Architect – Edge Services
AWS

Joanna Knox
(she/her)
Sr Cloud Support Engineer
AWS

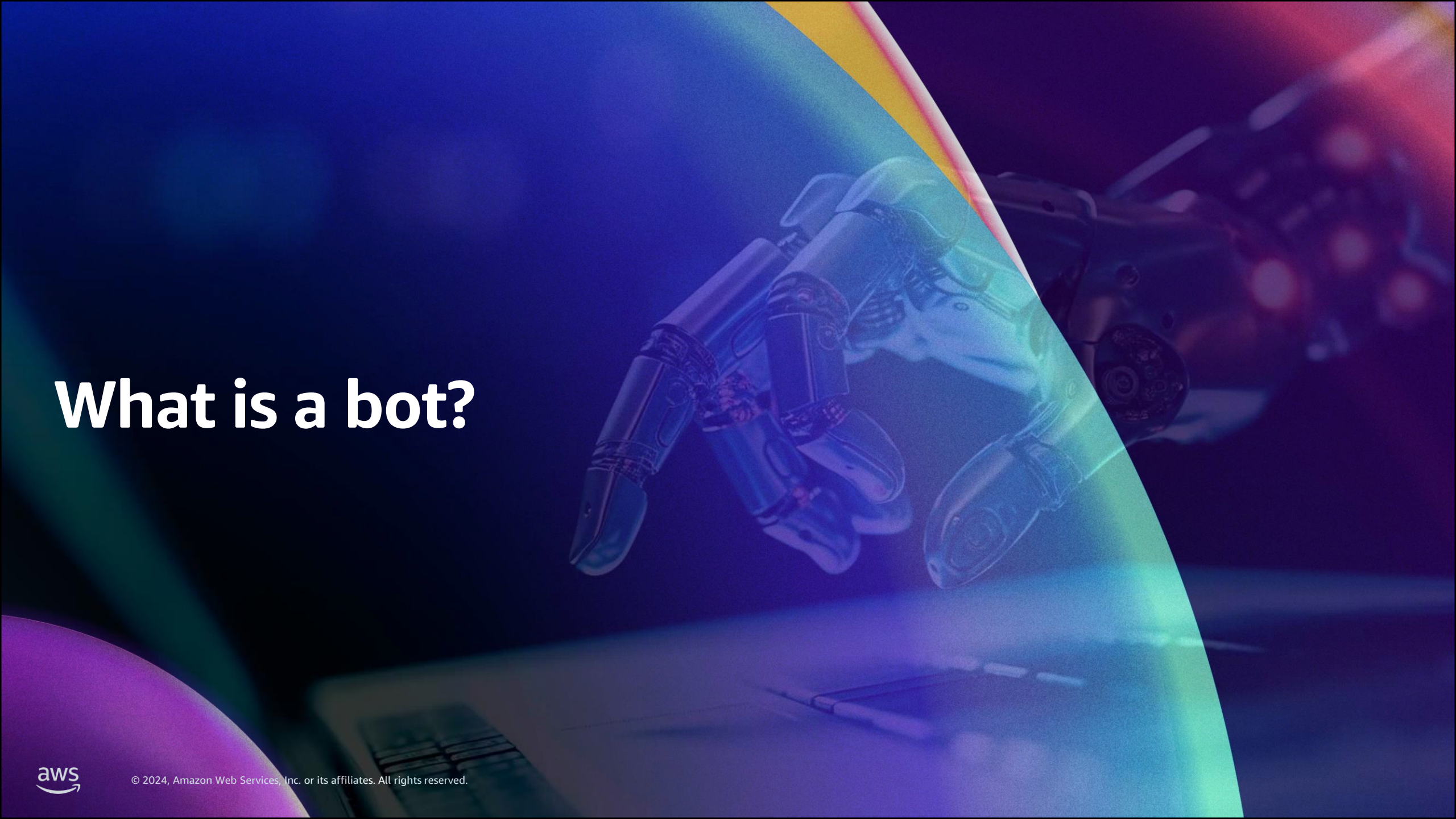
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- What is a bot?
- AWS WAF overview
- Foundational rules
- AWS WAF Bot Control and Fraud Control
- Customer examples

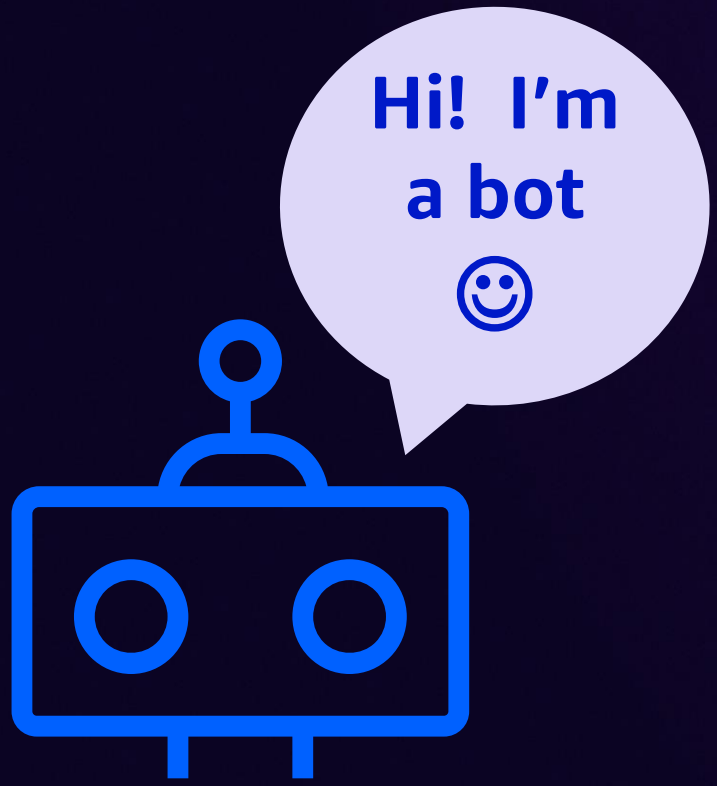
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

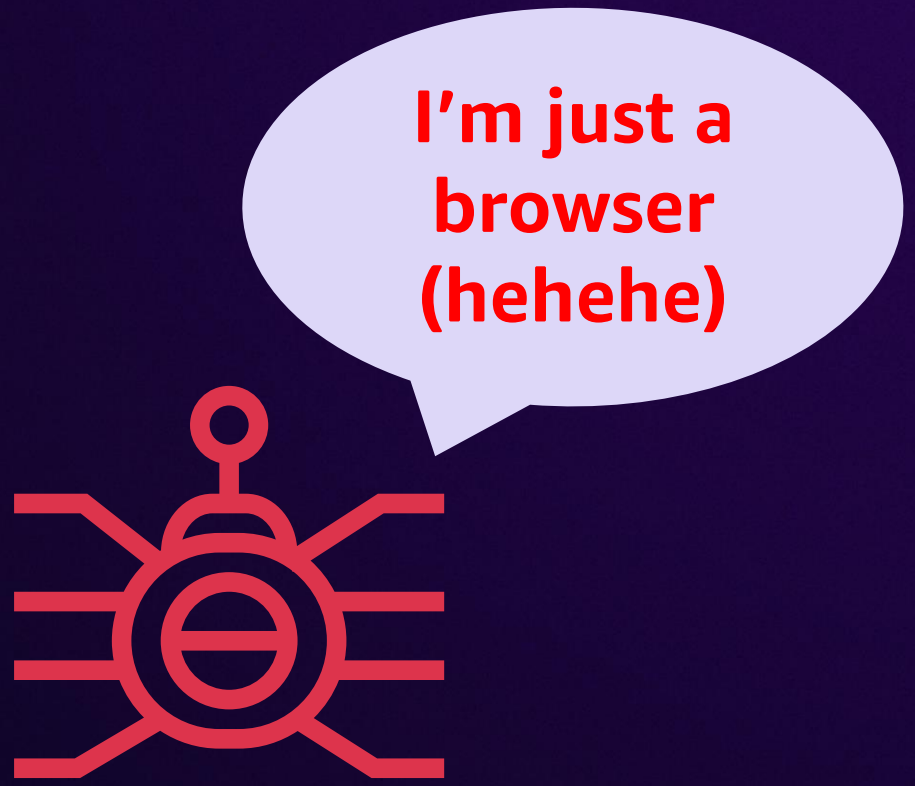
What is a bot?



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is a bot?





© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bot use cases

Good bots	Bad bots	Grey area
• Search engine • Site monitoring • Authorized vulnerability scans	• DDoS • Account/credit card fraud • Scraping/data theft • SMS pumping • “Click” bots	• Social media • AI bots • Accidental bots

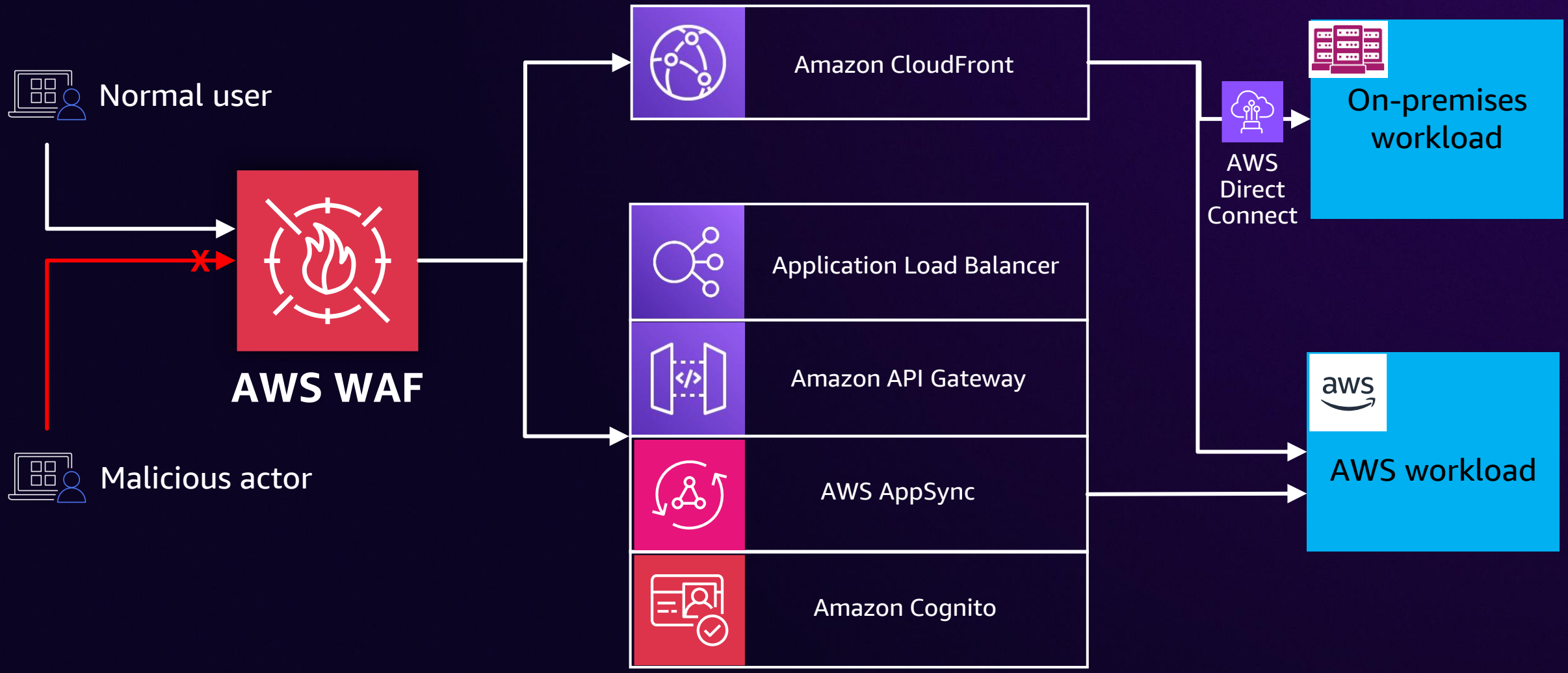
aws

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS WAF overview

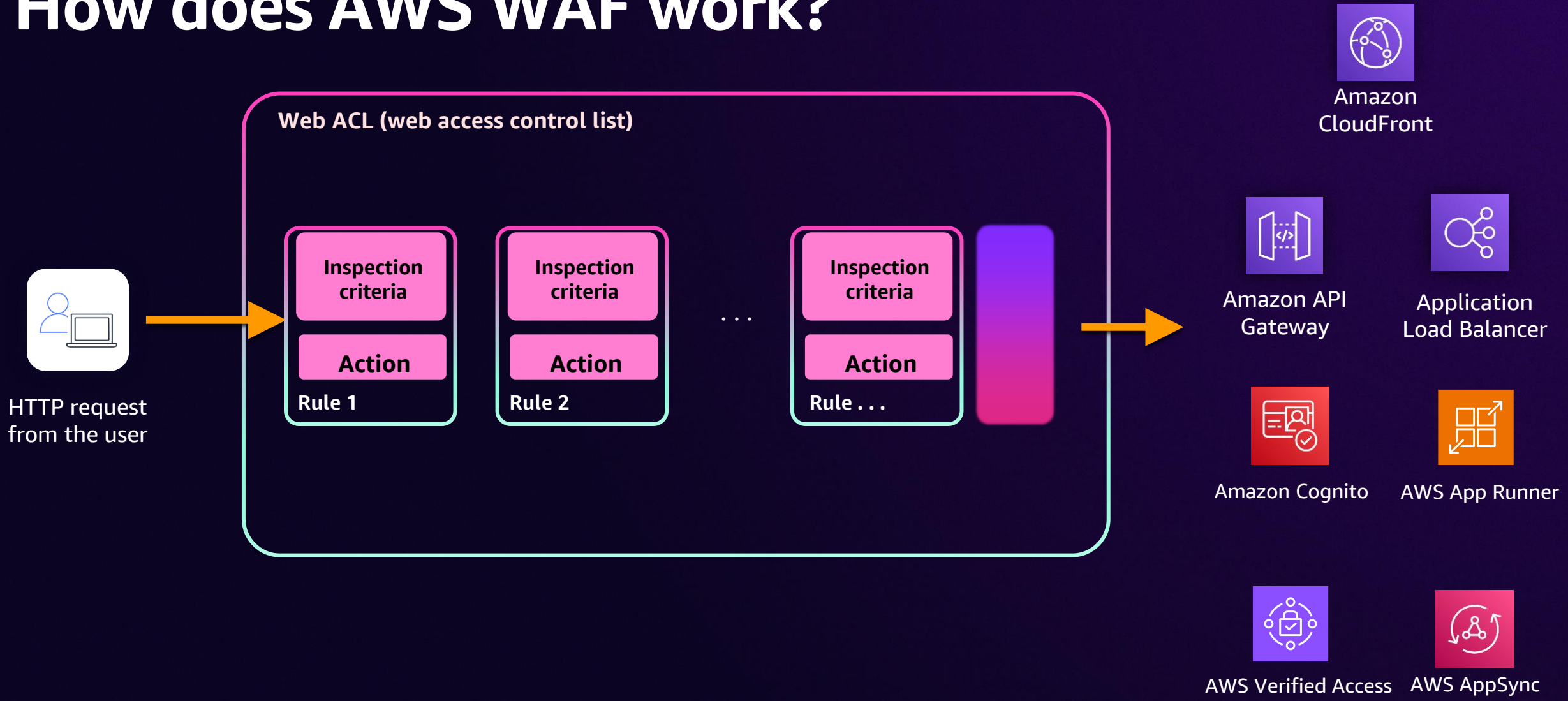
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Protect AWS and on-premises applications



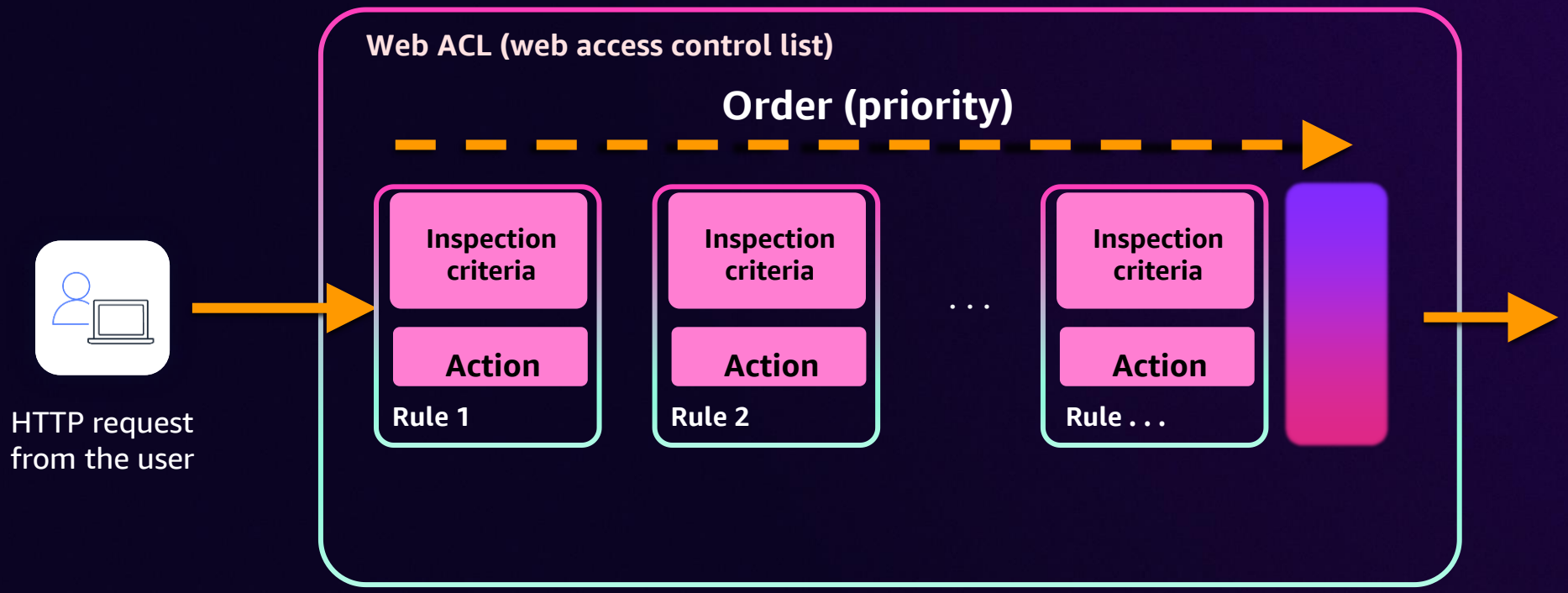
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How does AWS WAF work?



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How does AWS WAF work?



Amazon CloudFront

Amazon API Gateway

Application Load Balancer

Amazon Cognito

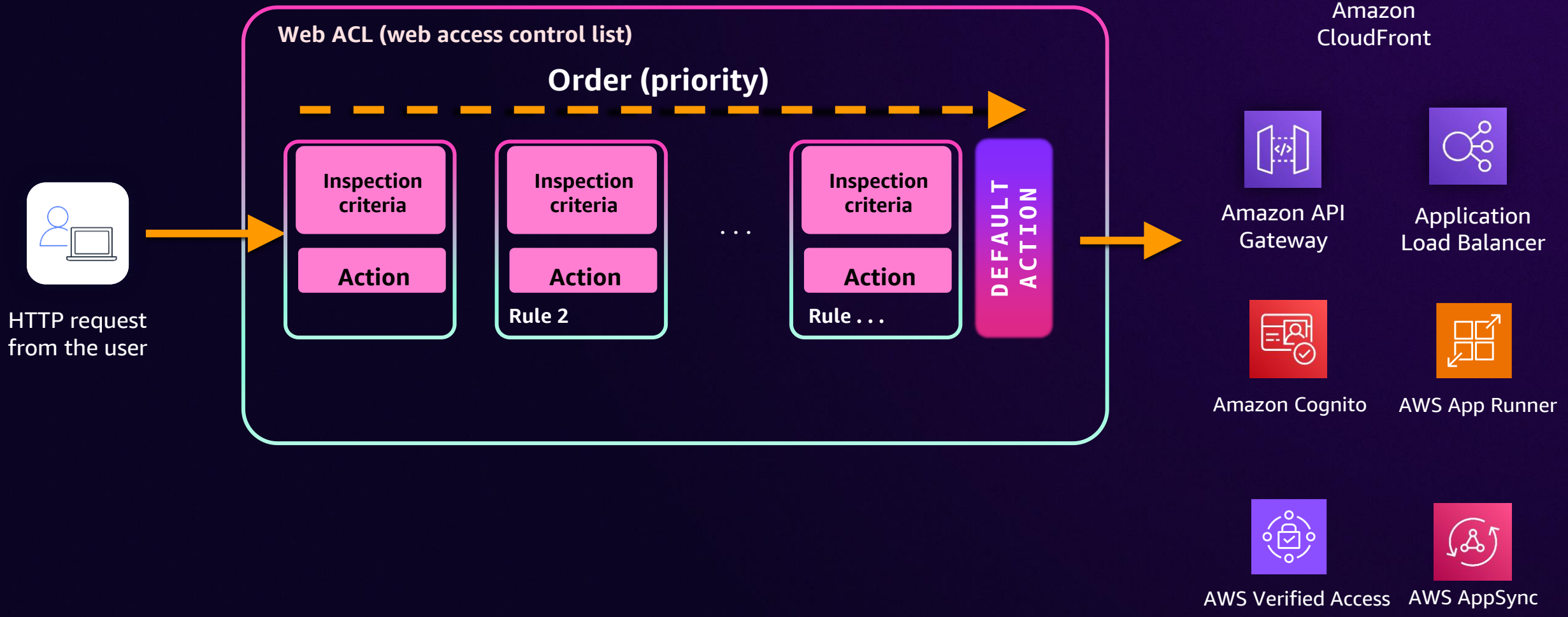
AWS App Runner

AWS Verified Access

AWS AppSync

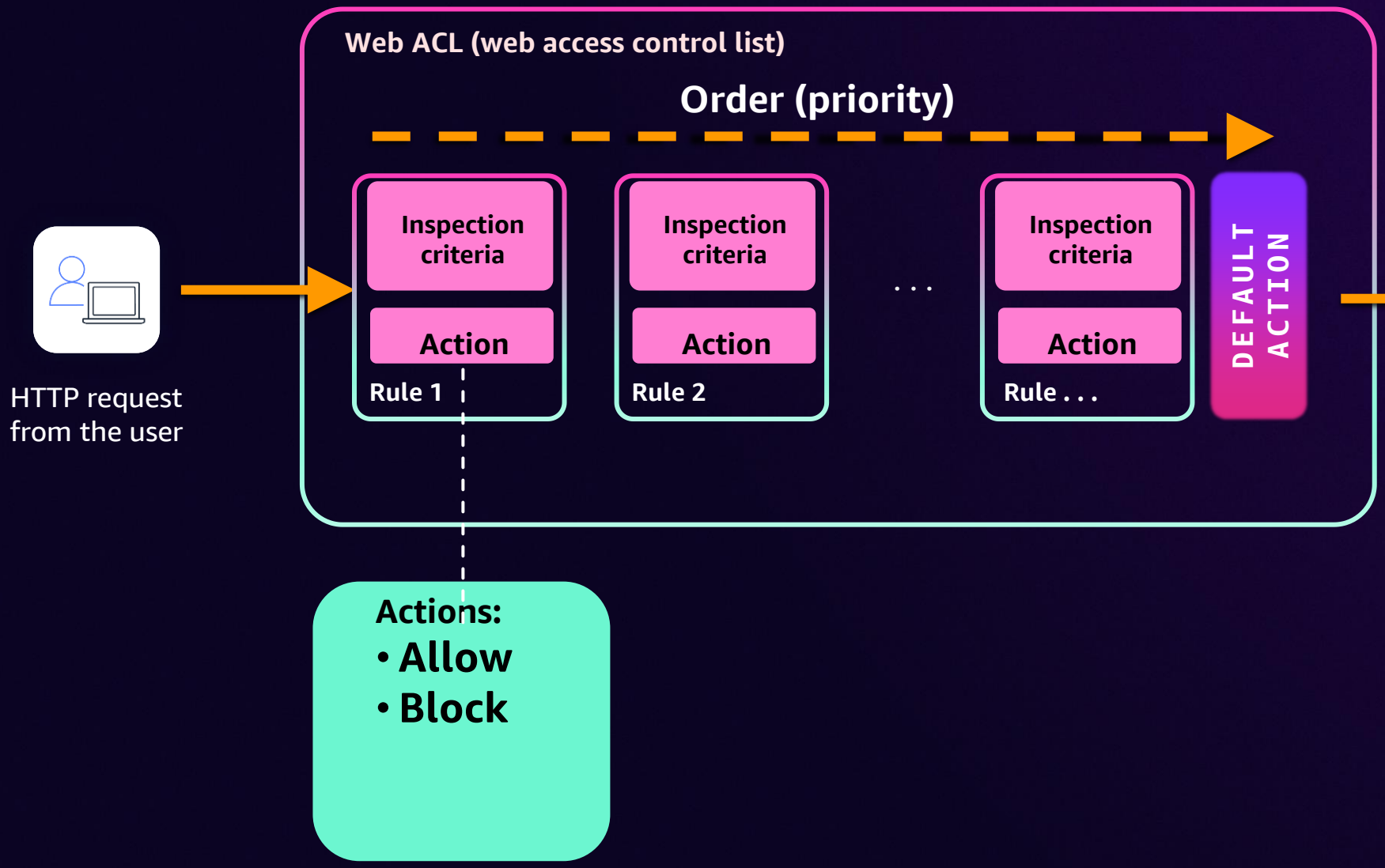
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

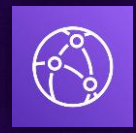
How does AWS WAF work?



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How does AWS WAF work?





Amazon CloudFront

Amazon API Gateway

Application Load Balancer

Amazon Cognito

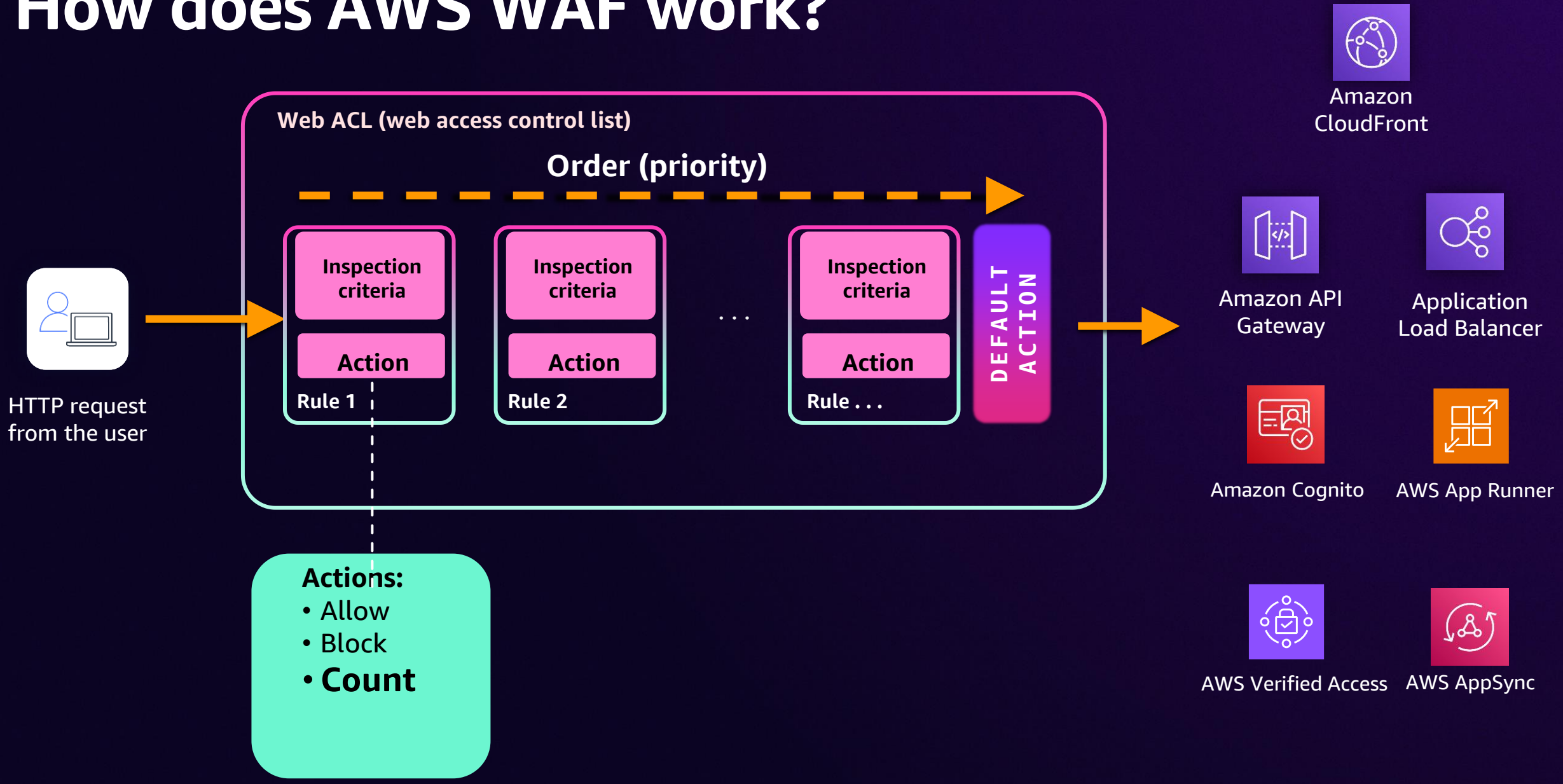
AWS App Runner

AWS Verified Access

AWS AppSync

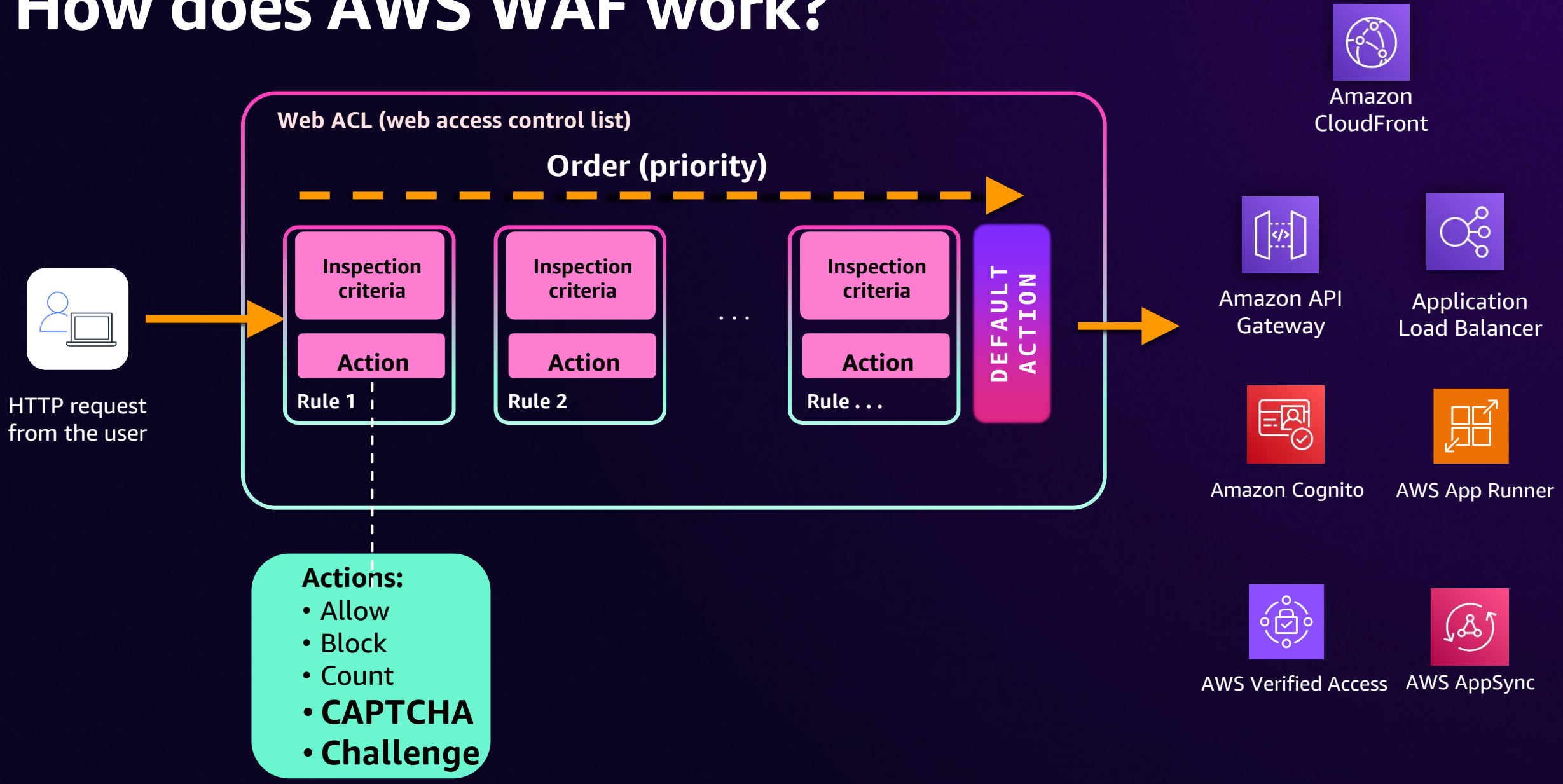
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How does AWS WAF work?



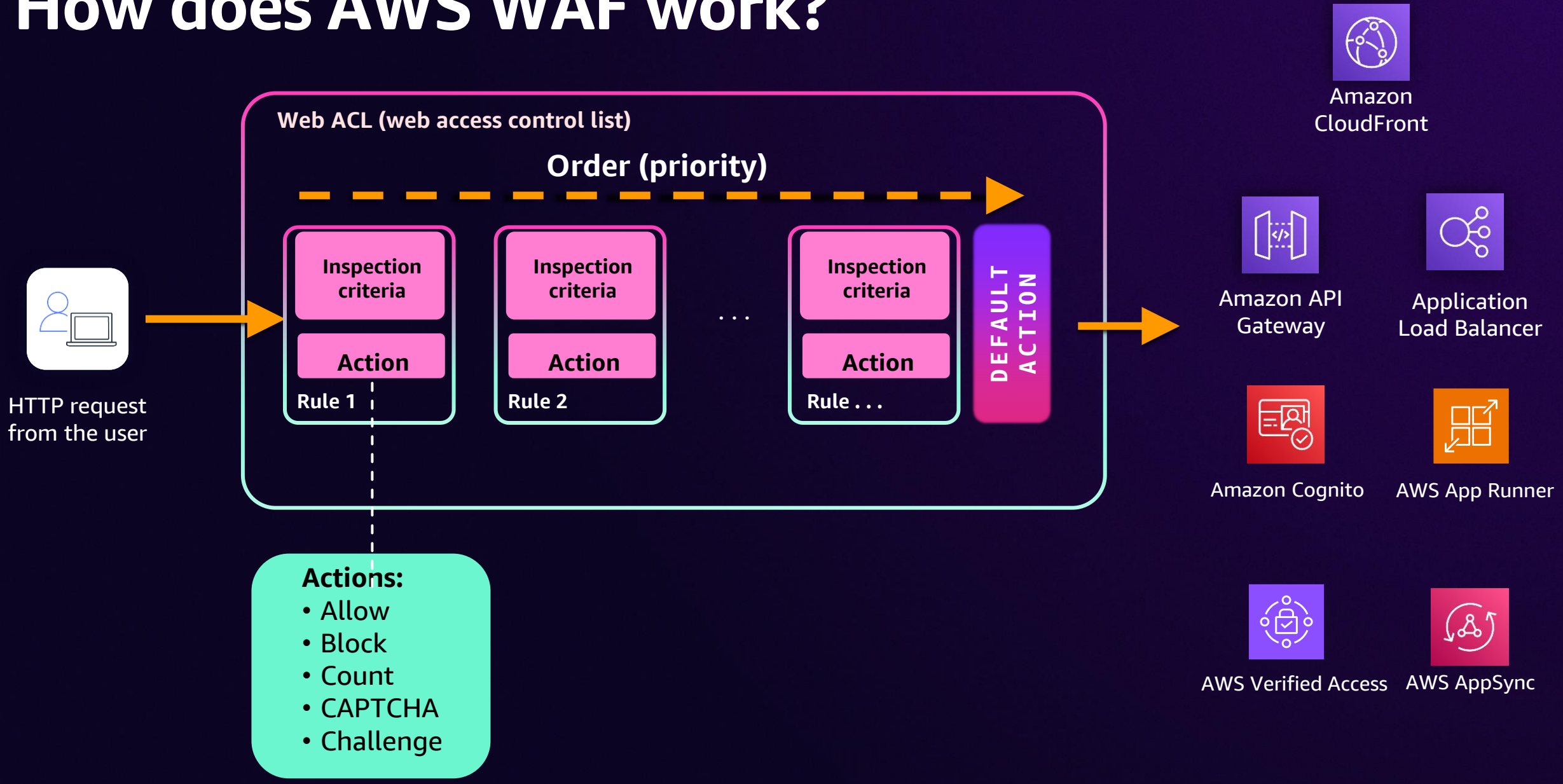
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How does AWS WAF work?



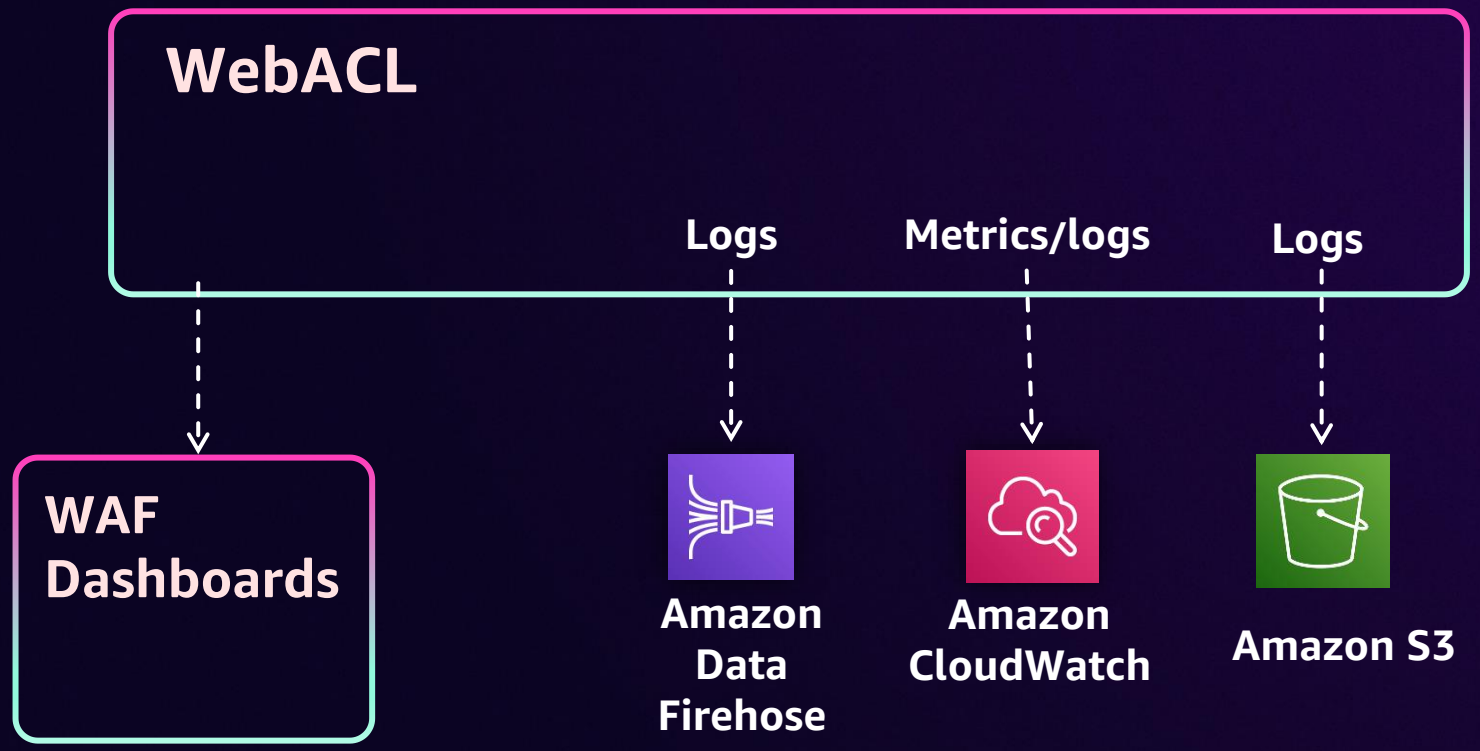
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How does AWS WAF work?



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Visibility is power



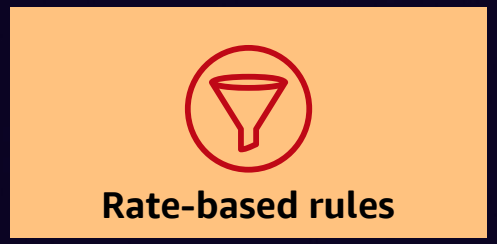
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Foundational rules

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Rate-based rules

Detect the HTTP flood attack and suppress the requests

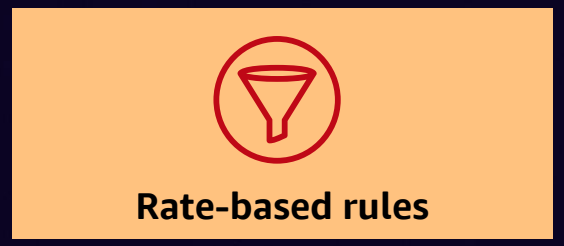


Block L7 DDoS attacks once a rate threshold is reached

aws

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Layering rate-based rules



Catch-all rule

Rule type: Rate-based

Rule name: rbr_global

Scope-down: None (matches all)

Aggregation key: IP (default)

Evaluation window: 300 (default)

Limit: **500**

Action: Block

API rule

Rule type: Rate-based

Rule name: rbr_api

Scope-down: If uri starts_with ‘/api/’

Aggregation key: IP (default)

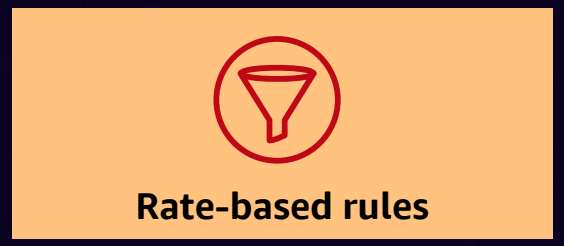
Evaluation window: 300

Limit: **50**

Action: Block

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Layering rate-based rules – Anti-DDoS



Anti-DDoS rule

Rule type: Rate-based

Rule name: rbr_ddos

Scope-down: None

Aggregation key: Header (Host) + URI + IP

Evaluation window: 60

Limit: **10**

Action: Block

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IP-based controls

Protection against attacks from known malicious IP addresses

Block or allow **requests from specific IPs** or IP sets

Amazon IP reputation list managed rule group

AWSManagedIPReputationList
Rule action: **Block**
Choose rule action override

AWSManagedReconnaissanceList
Rule action: **Block**
Choose rule action override

AWSManagedIPDDoSList
Rule action: **Count**
Choose rule action override

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“Challenge” rule action

JavaScript challenge

AWS WAF token

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS WAF Bot Control and Fraud Control

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS WAF Bot and Fraud Control overview

Bot Control

- Identifies, labels, and manages both friendly and malicious bots
- 2 levels of protection
  - Common – for self-identifying bots
  - Targeted – for evasive bots

Fraud prevention

- Detects and prevents fraud attempts
- Account takeover prevention (ATP)
- Account creation fraud prevention (ACFP)

aws

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Detecting common bots

What are the common bots?

- Self-identifying
- Search engines/social media/HTTP library

```
GET /
Host: www.example.com
Accept: */*
Accept-Encoding: deflate, gzip
User-Agent: facebookexternalhit/1.1
(+http://www.facebook.com/externalhit_uatext.php)
Range: bytes=0-524287
X-FB-CrawlerBot: AaknqfYgnBhDfF.....
```

What does common bot control do?

- Looks for request, IP, TLS fingerprint
- Verifies the bot
- Provides labels

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Challenges of evasive bots

Challenges

- Use existing browser headers and values
- Not using well-known bot IP addresses
- Mimic the real browser activities such as JavaScript execution

Responses

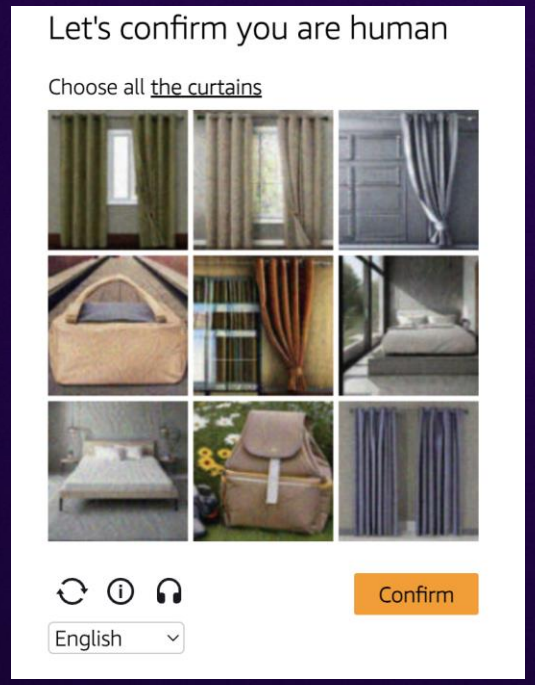
- Client interrogation
- Uniquely identify the client session
- Monitor the client session behavior

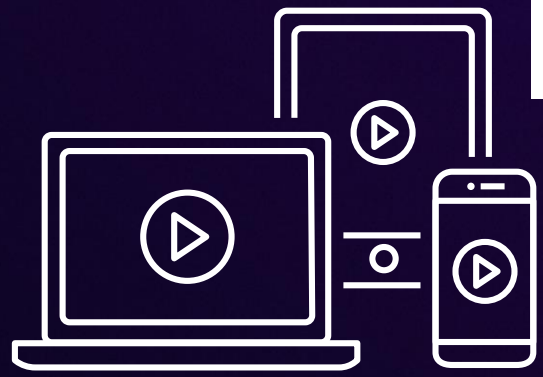
aws

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

A bit more on client interrogation

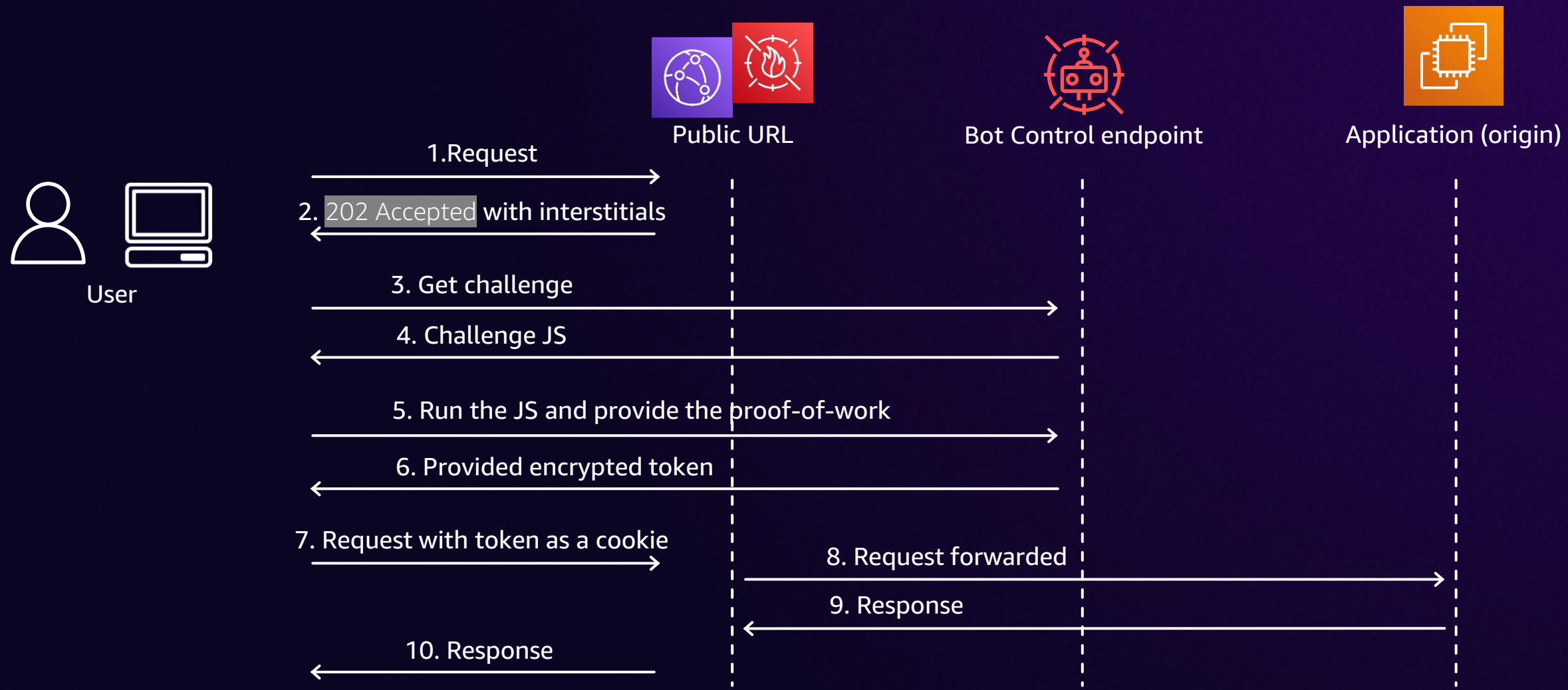
- JavaScript execution or CAPTCHA puzzle
- Collect client information
  - Canvas info/installed fonts/installed plugins/other
- Look for browser automation
  - Selenium/Puppeteer
- Collect client telemetries
  - Mouse movement/key press





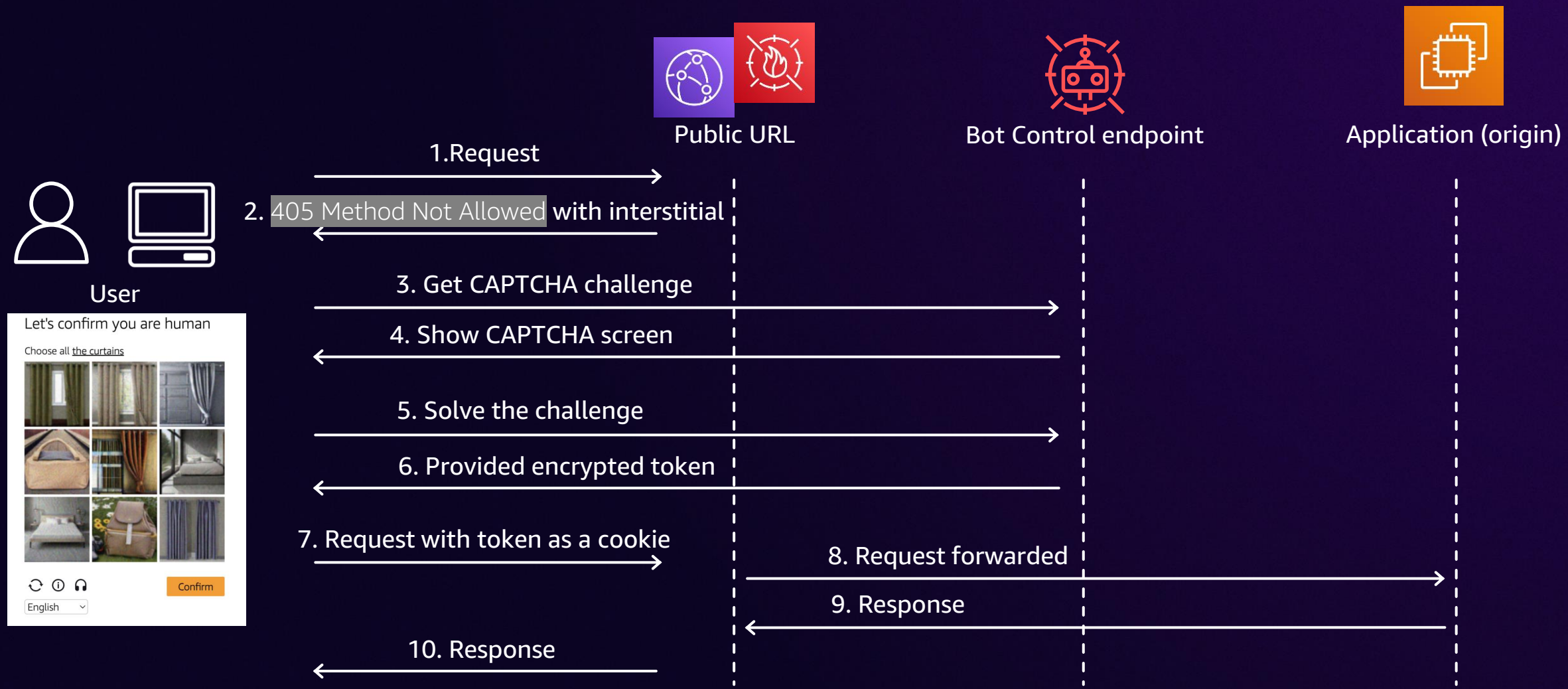
aws
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Silently challenging the browser



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Challenging with the CAPTCHA



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

SDK integration

Without SDK integration

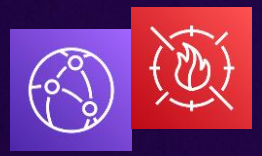
Static frontend

Mobile app

1. API call such as `fetch()`

2. Challenge or CAPTCHA

3. ???



API endpoint

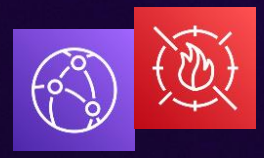
- Client interrogation and token creation
- Can programmatically throw CAPTCHA
- Lower latency

With SDK integration

Static frontend

Mobile app

`AwsWafIntegration.fetch()`



API endpoint

2. Detect and respond

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Token for tracking

Detects	Details	Default action
Too many requests without token	More than 5 requests from 1 IP	Challenge
Too many requests from a session	Baseline determined with historic patterns Confidence level: Low/medium/high/maximum	Block for maximum CAPTCHA for high
Suspected automated browser	Indicators of browser automation found during the client challenge	CAPTCHA
Browser inconsistency	Indicators of browser inconsistency found during the client challenge	CAPTCHA
Single token among multiple IP, multiple ASN, multiple countries	Multiple level: Low/medium/high	Count for low CAPTCHA for medium Block for high

aws

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Fraud prevention

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Account takeover prevention (ATP)

Protects from credential stuffing and brute force

- Analyzes POST request to the login URL
- Detects compromised credentials
- Login and password traversal
- Tracks response too (when used with CloudFront)

Stolen credentials	
Login A	Password A
Login B	Password B
Login C	Password C

Brute force	
Login X	password
Login X	p@ssw0rd
Login X	pa$$word

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Account creation fraud prevention (ACFP)

Prevents fraud account creation

- Analyzes human interaction in the registration page and POST request
  - SDK integration is mandatory for human interaction detection
- Detects phone number and address abuse

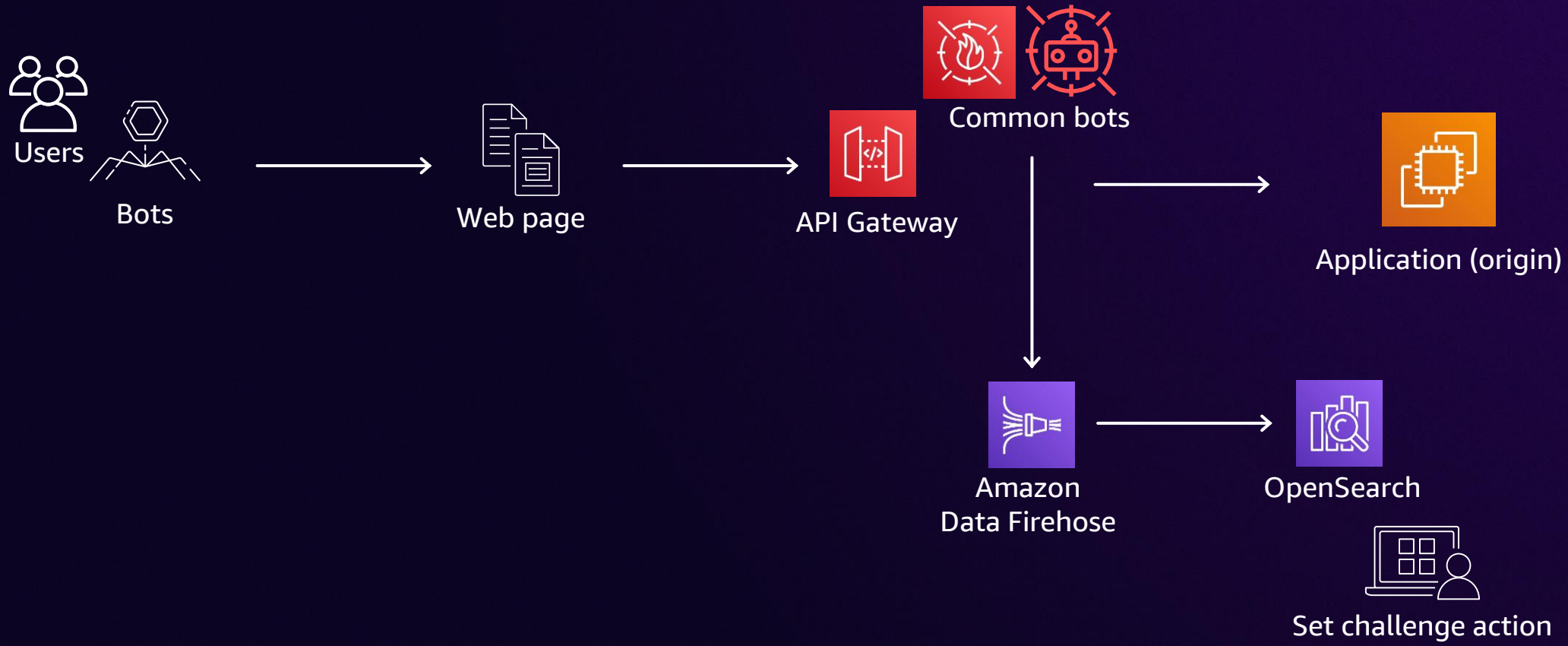
Detections include:
Compromised credentials
Human interactivity is absent
Same phone number or address is used multiple times
High volume of successful account creation

aws
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Customer examples

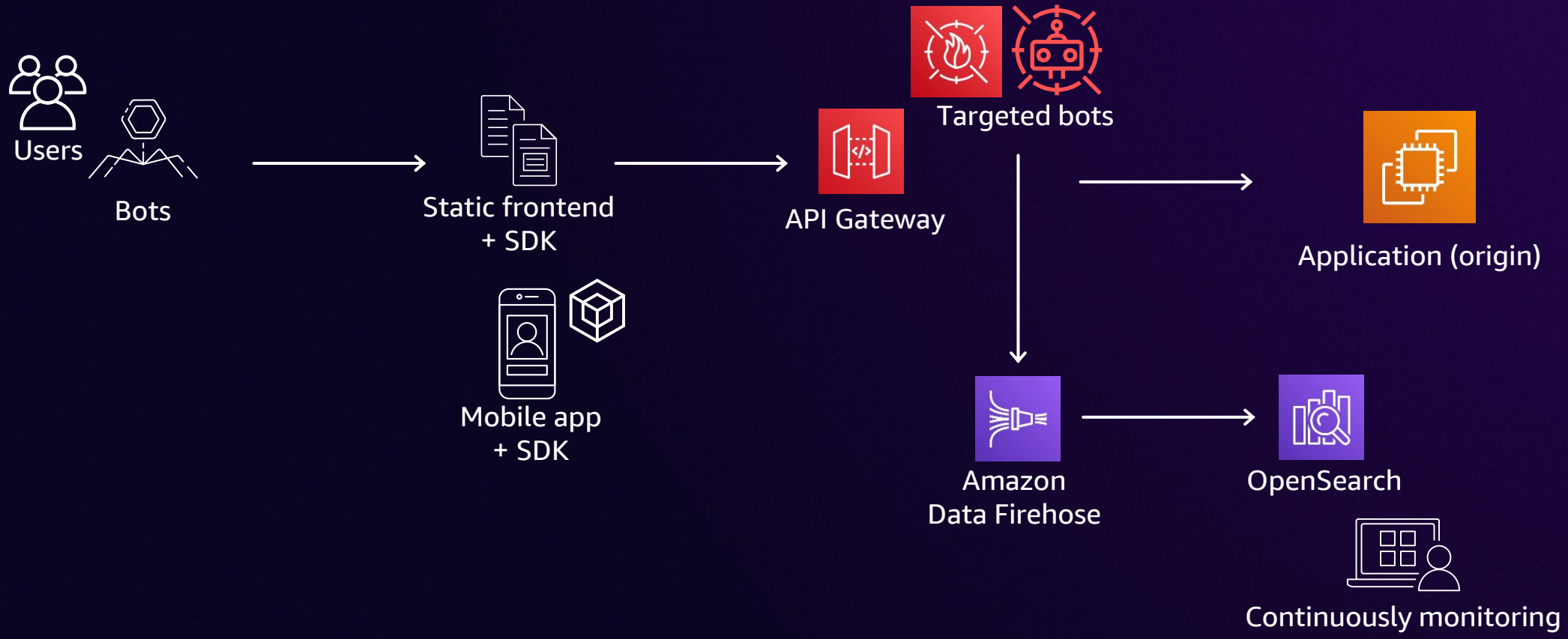
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bot Control building up example



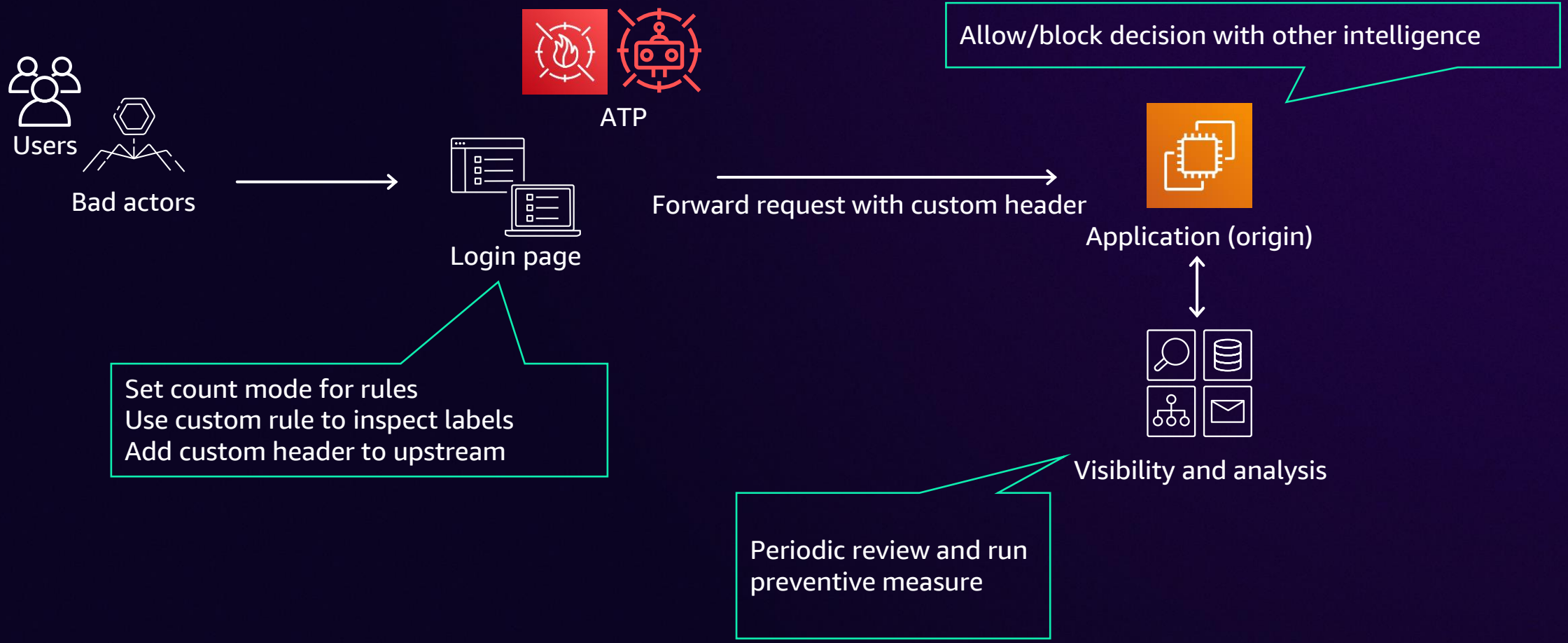
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bot Control building up example



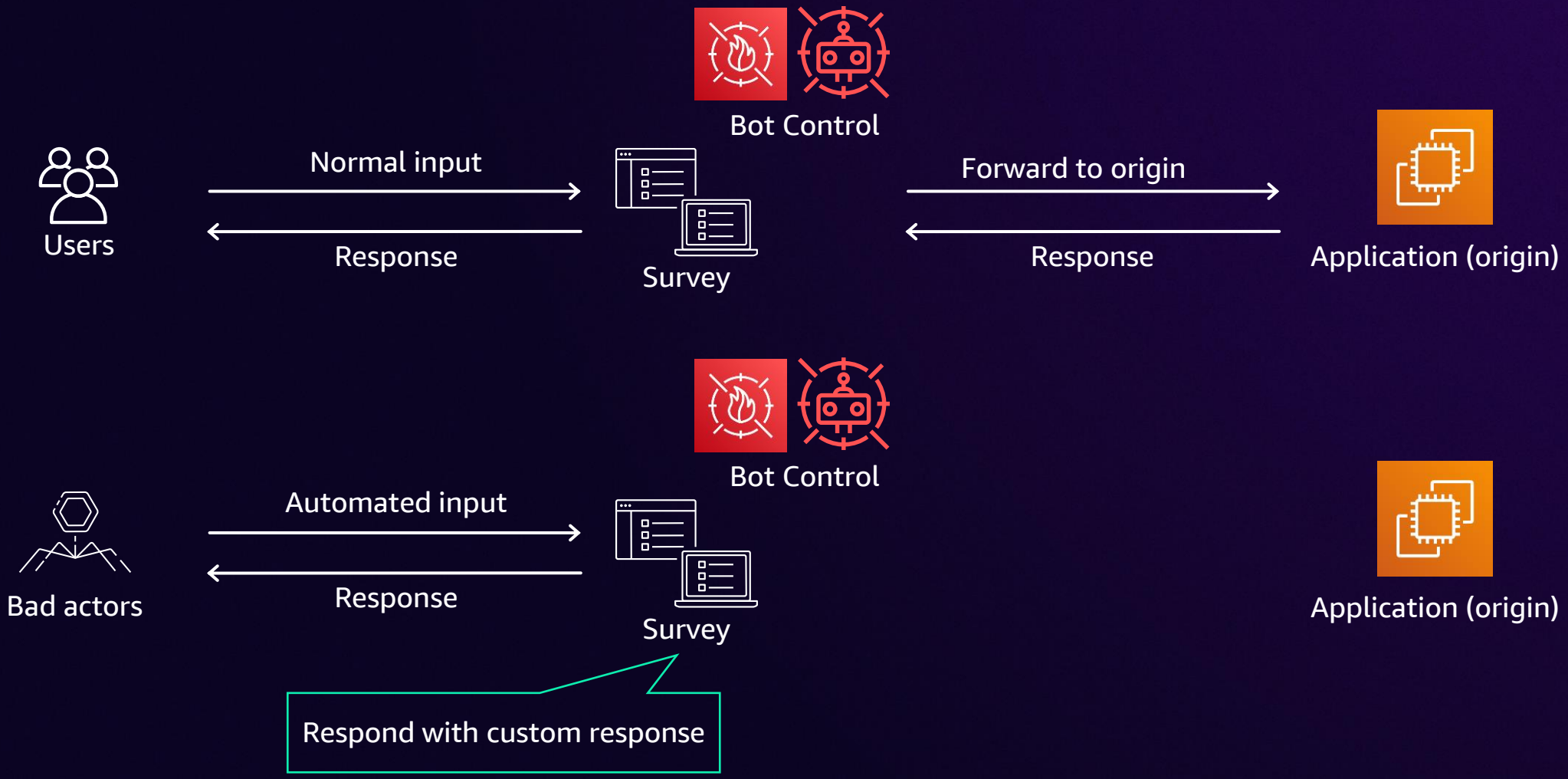
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ATP example – Collecting intelligence



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Don’t let them know we know



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Please complete the session survey in the mobile app

Julian Ju
linkedin.com/in/julianju/

Joanna Knox
linkedin.com/in/joanna-knox-3161a34/

aws
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.