

AWS re:Invent 2024 reCap

Edge security

Achraf Souk

Principal Solutions Architect



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

Scale of edge security on AWS

700+ points of presence in 100+ cities across 50 countries

100+ billion AWS managed rules requests processed per day

Exabytes of data are analyzed every 60 sec



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

How AWS uses active defense to protect you

MadPot

Globally-distributed **network of honeypot** threat sensors with automated response capabilities

Observe and react to threat actors' evolving tactics, techniques, and procedures (TTPS)

Sonaris

An **active defense tool** that analyzes potentially harmful network traffic

Deny attempts to find unintentionally public S3 buckets and vulnerable services

Mithra

An internal **neural network graph model** that uses algorithms for threat intelligence

Ranks domain trustworthiness to help protect customers from threats



Honeypots of Madpot



100M

Volume of potential threat interactions observed daily,
WW



500K

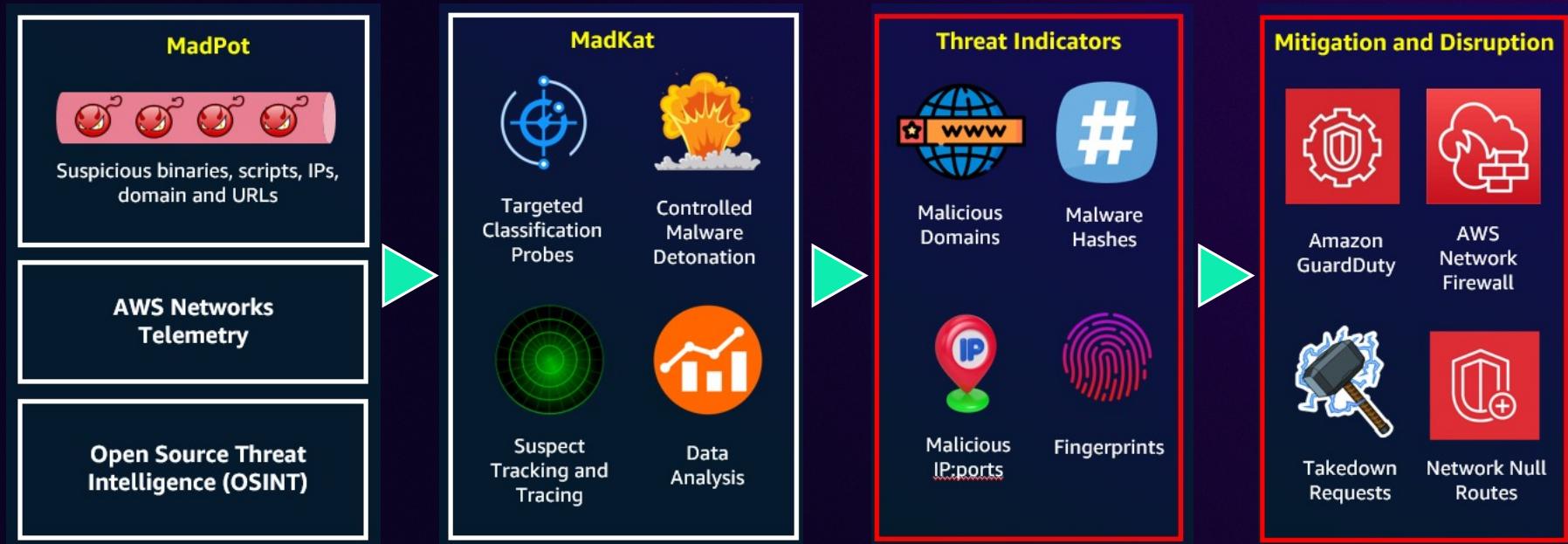
of observed activities
that are classified as
malicious



90secs

Time taken for workload
to be discovered by
probes

From threat data to **actionable** intelligence



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

Case Study - Anonymous Sudan

 United States
Attorney's Office
Central District of California

About | Meet the U.S. Attorney | News | Divisions | Programs | Community Engagement | Employment | Contact Us

Justice.gov > U.S. Attorneys > Central District of California > Press Releases > Two Sudanese Nationals Indicted For Alleged Role In Anonymous Sudan Cyberattacks On Hospitals, Government Facilities, and Other Critical Infrastructure In Los Angeles and Around The World

PRESS RELEASE

Two Sudanese Nationals Indicted for Alleged Role in Anonymous Sudan Cyberattacks on Hospitals, Government Facilities, and Other Critical Infrastructure in Los Angeles and Around the World

Wednesday, October 10, 2024

For Immediate Release
U.S. Attorney's Office, Central District of California

LOS ANGELES—A federal grand jury indictment unsealed today charges two Sudanese nationals with operating and controlling Anonymous Sudan, an online cybercriminal group responsible for tens of thousands of Distributed Denial of Service (DDoS) attacks against critical infrastructure, corporate networks, and government agencies in the United States and around the world. In March 2024, pursuant to court-authorized seizure warrants, the U.S. Attorney's Office and FBI seized and disabled Anonymous Sudan's powerful DDoS tool, which the group allegedly used to perform DDoS attacks, and sold as a service to other criminal actors.

Ahmed Salah Youssf Omer, 22, and Alaa Salah Yusuf Omer, 27, were both charged with one count of conspiracy to damage protected computers. Ahmed Salah was also charged with three counts of damaging protected computers.

"Anonymous Sudan sought to maximize havoc and destruction against governments and businesses around the world by perpetrating tens of thousands of cyberattacks," said United States Attorney Martin Estrada. "This group's attacks were callous and brazen—the defendants went so far as to attack hospitals providing emergency and urgent care to patients. My office is committed to safeguarding our nation's infrastructure and the people who use it, and we will hold cyber criminals accountable for the grave harm they cause."

"The FBI's seizure of this powerful DDoS tool successfully disabled the attack platform that caused widespread damage and disruptions to critical infrastructure and networks around the world," said Special Agent in Charge Rebecca Day of the FBI Anchorage Field Office. "With the FBI's mix of unique authorities, capabilities, and partnerships, there is no limit to our reach when it comes to combating all forms of cybercrime and defending global cybersecurity."

"These charges and the results of this investigation, made possible through law enforcement and private sector partnerships, have an immeasurable impact on the security of networks in the U.S. and of its allies, and demonstrate the resolve of the Defense Criminal Investigative Service (DCIS) to safeguard the Department of Defense from evolving cyber threats," said Kenneth A. DeCellis, DCIS Cyber Field Office, Special Agent in Charge. "Cybercriminals need to understand that if they target America's warfighters, they will face consequences."

amazon | Search

Who We Are | What We Do | Our Workplace | Our Impact | Our Planet | Follow Us | Subscribe | EN

News / AWS

5 min

October 16, 2024

f t m p

Amazon helps the US Department of Justice thwart international cybercriminal group Anonymous Sudan

Written by Amazon Staff



5 min

Reading:

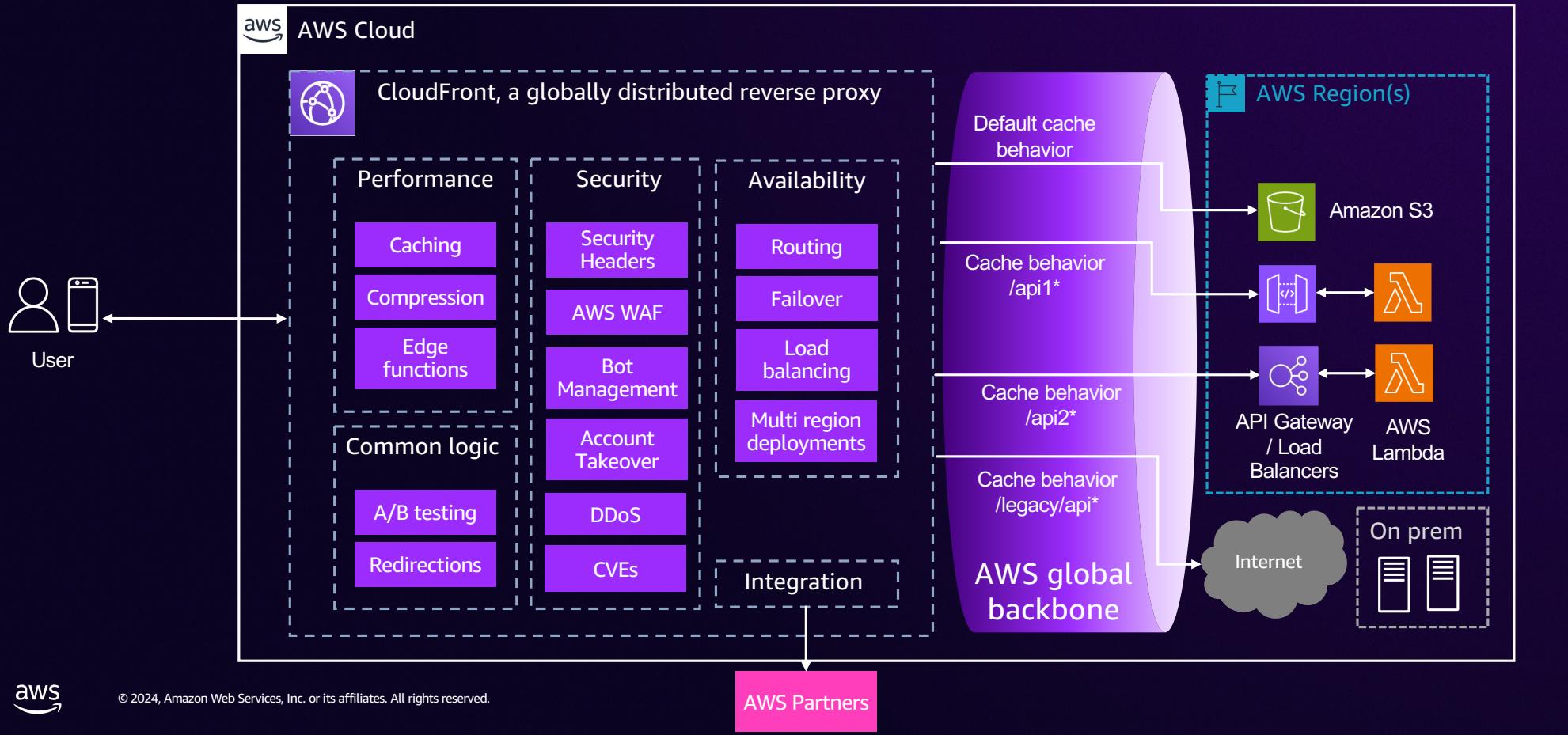
Amazon helps the US Department of Justice thwart international cybercriminal group Anonymous Sudan

Two individuals behind the Anonymous Sudan cybercriminal group were indicted by the U.S. Department of Justice, which acknowledged AWS for its contributions.

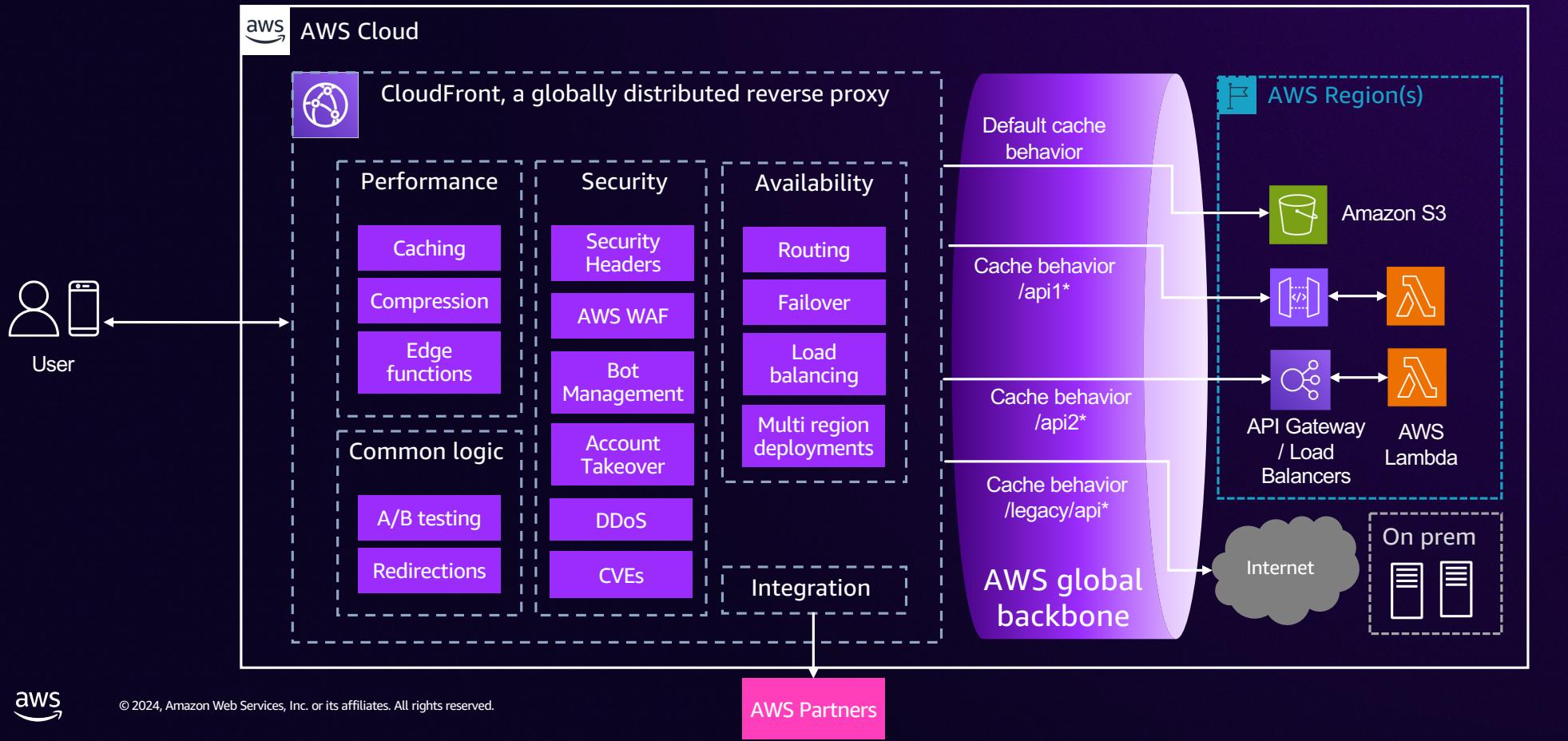


© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudFront – Mental model



What's new on the user side?



Amazon CloudFront Expanding in KSA



Edge Location

© Vemaps.com



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

PCI DSS v4.0 embraced Client Side Protection

The screenshot shows a section of the PCI DSS Requirements and Testing Procedures page. At the top, there's a header with the PCI Security Standards Council logo. Below it, a teal bar contains the title "Requirements and Testing Procedures". Underneath, requirement 11.6 is listed: "11.6 Unauthorized changes on payment pages are detected and responded to." This requirement is divided into two columns: "Defined Approach Requirements" and "Defined Approach Testing Procedures".

Defined Approach Requirements	Defined Approach Testing Procedures
<p>11.6.1 A change- and tamper-detection mechanism is deployed as follows:</p> <ul style="list-style-type: none">To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser.The mechanism is configured to evaluate the received HTTP header and payment page.The mechanism functions are performed as follows:<ul style="list-style-type: none">At least once every seven days	<p>11.6.1.a Examine system settings, monitored payment pages, and results from monitoring activities to verify the use of a change- and tamper-detection mechanism.</p> <p>11.6.1.b Examine configuration settings to verify the mechanism is configured in accordance with all elements specified in this requirement.</p> <p>11.6.1.c If the mechanism functions are performed at an entity-defined frequency, examine the entity's targeted risk analysis for determining the frequency to verify the risk analysis was performed in accordance with all elements specified at Requirement 12.3.1.</p>

Below the table, the word "OR" is centered. The AWS logo is visible in the bottom left corner of the screenshot area.

This screenshot shows the AWS Marketplace listing for "PCI DSS 4 Compliance powered by HUMAN Client-side Defense". The listing includes the HUMAN logo, a brief description, and purchase options. It also shows a 0-star rating and a "View purchase options" button.

This screenshot shows the AWS Marketplace listing for "DataDome Page Protect". It includes the DataDome logo, a brief description, and purchase options. It also shows a 0-star rating and a "View purchase options" button.

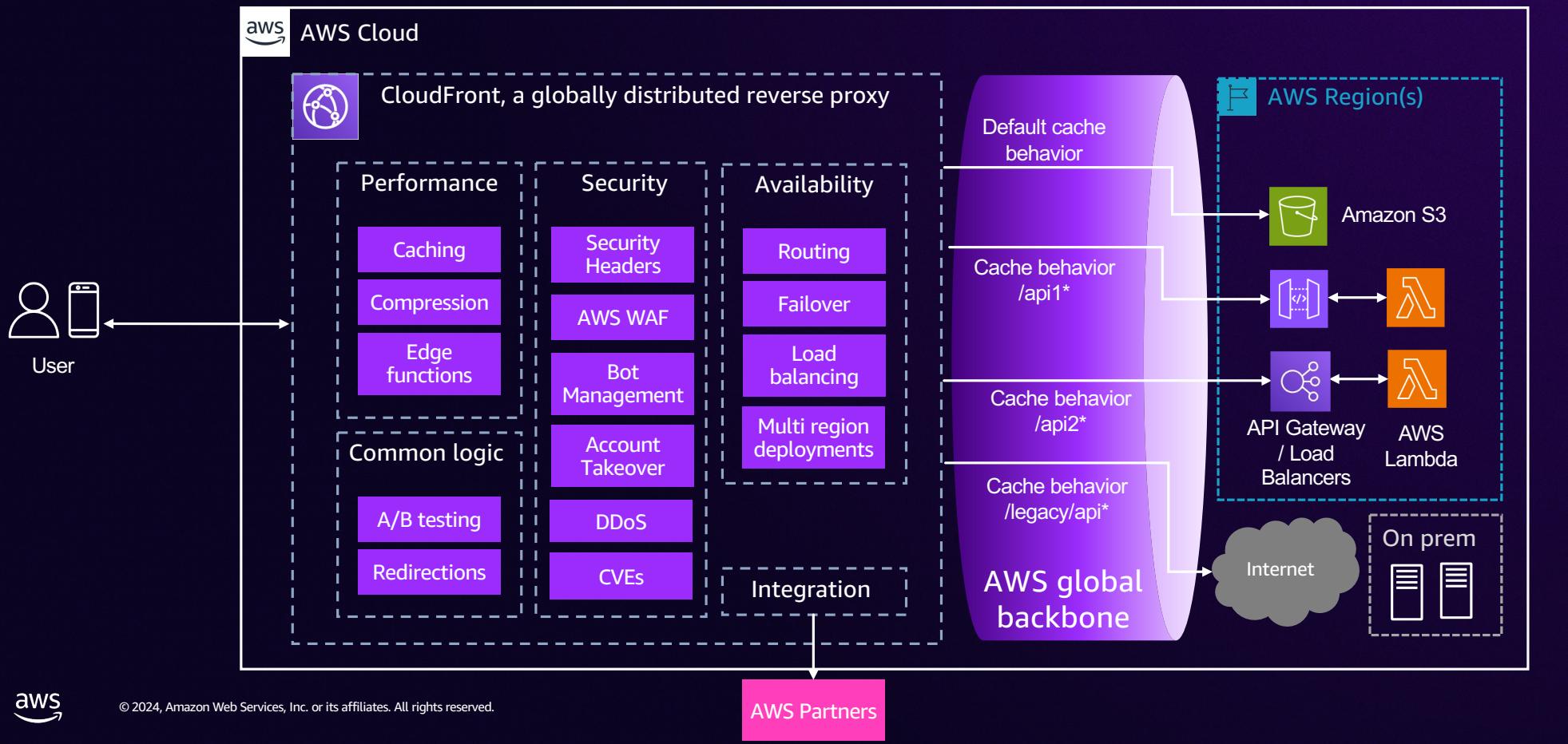
Allow-list your endpoint IPs in customer firewalls

- B2B Business, e.g. SaaS or Connected devices
- How to prevent the firewall of your customers to block traffic to your CloudFront based endpoint?
- **Anycast Static IPs** provides a fixed, dedicated set of IPs that do not change



Enterprise Applications
Allow-Listing

What's new on AWS WAF?



🚀 Announcing Shield Advanced Anti-DDoS Managed rule in preview 🚀

AntiDDoS Protection for Layer 7 attacks

Provides protection against DDoS attacks targeting the application layer, also known as Layer 7 attacks.

Rule group configuration

Block sensitivity level
Blocks requests that are labeled high suspicion DDoS requests by the detection system

Low

Action totals for the specified time range - Anti-DDoS

Counts of all terminating actions applied to requests that were evaluated by the anti-DDoS managed rule group. This area shows counts for the last 24 hours.

Total	Blocked	Allowed
956.38K	571.99K	0

100% 100%

- Mitigation in seconds
- High accuracy
- Granular control
- Native dashboards

in preview



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



**CloudFront no
longer charges for
requests blocked
by AWS WAF**

LLMs are hungry
... for your **public** data



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

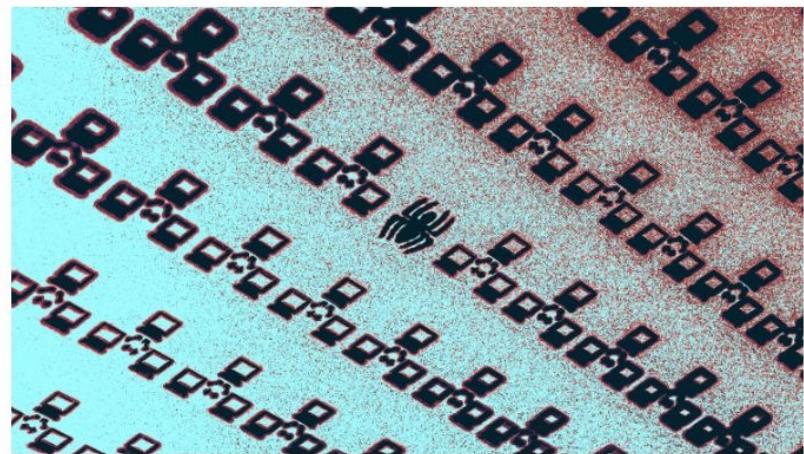


AI crawlers can bring your website down

09-26-2024 | TECH

AI crawlers are hammering sites and nearly taking them offline

Websites claim they're collateral damage for the AI revolution's voracious appetite for information—but companies like Anthropic and OpenAI say their bots aren't to blame.



[Source Photo: Getty Images]

AI

Like digital locusts, OpenAI and Anthropic AI bots cause havoc and raise costs for websites

Darius Rafieyan Sep 19, 2024, 1:00 PM GMT+4

[Share](#) | [Save](#) | [Read in app](#)



CSO

Getty Images; Alyx

ChatGPT API flaws could allow DDoS, prompt injection attacks

News

21 Jan 2025 • 3 mins

[APIs](#) [DDoS](#) [Vulnerabilities](#)



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

Opting out of AI crawling

- Robots.txt
- No standard for disallowing all AI crawlers (e.g. User-Agent: AI-Ingest)
 - Disallowing specific AI bots:
User-Agent: GPTBot
Disallow: /
 - Or Disallowing all bots, but allowing specific desired ones (e.g. Google Bot)



New signals for AI bots in AWS WAF Bot Control

awswaf:managed:aws:bot-control:CategoryAI

awswaf:managed:aws:bot-control:bot:name:**anthropic**
awswaf:managed:aws:bot-control:bot:name:**chatgpt**
awswaf:managed:aws:bot-control:bot:name:**chatgpt_user**
awswaf:managed:aws:bot-control:bot:name:**gptbot**
awswaf:managed:aws:bot-control:bot:name:**bytespider**
awswaf:managed:aws:bot-control:bot:name:**claudebot**
awswaf:managed:aws:bot-control:bot:name:**cohere**
awswaf:managed:aws:bot-control:bot:name:**bedrockbot**

Rate-limiting criteria [Learn more](#)

Rate limit
The maximum number of requests to allow during the specified time window that satisfy your criteria. You can narrow requests using a scope-down statement. You can group requests by component types for count aggregation. You can also use an aggregation component or a scope-down statement.

1000

Rate limit must be between 10 and 2,000,000,000.

Evaluation window
The amount of time to use for request counts.

10 minutes (600 seconds)

The default time span is 5 minutes. Valid values are 1, 2, 5, and 10 minutes.

Count all
Count and rate limit all requests that match the rule's scope-down statement.

Count only the requests that match the following statement

If a request matches the statement

Statement

Inspect

Has a label

Labels
Labels are strings that rules add to the web request. You can evaluate labels that are added by rules that run before this one in the same web ACL.

Match scope

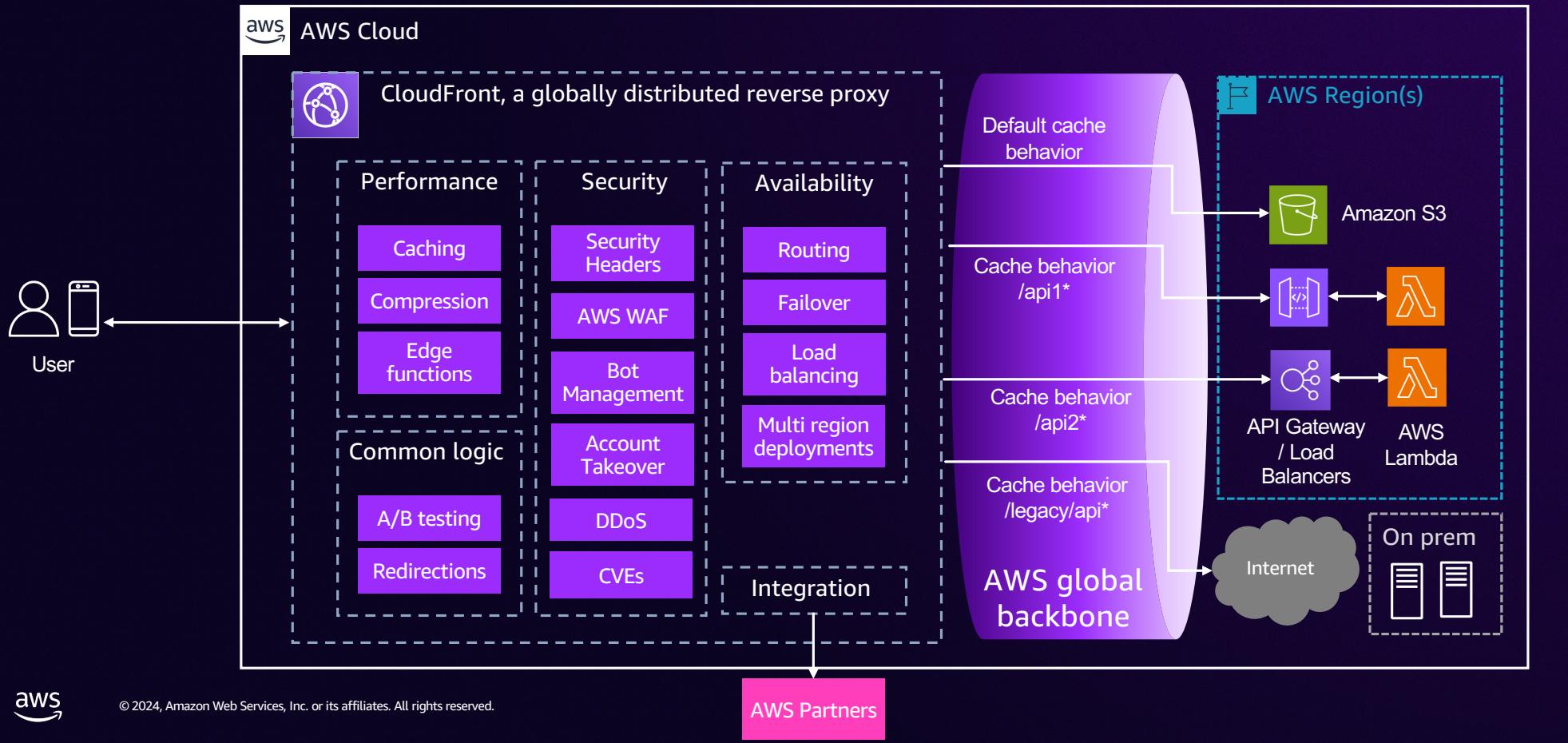
Label
 Namespace

Match key
Enter the string containing the label name and optional prefix and namespaces. For example, namespace1:name or awswaf:managed:aws:managed-rule-set:namespace1:name.

awswaf:managed:aws:bot-control:CategoryAI



What's new in origin integration?



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

AWS Partners



A close-up photograph of a knight in full armor. The knight is wearing a silver-colored helmet with a visor partially open, showing a dark interior. A chainmail coif is visible at the base of the helmet. The knight is holding a lance with a brown shaft and a silver tip. The background is blurred, showing trees with autumn-colored leaves.

Attack the origin

Origin cloaking

Origin Cloaking stops malicious actors from by-passing CloudFront and its security controls to attack the origin directly.



PAGE CONTENT

[Overview](#)

[At network layer](#)

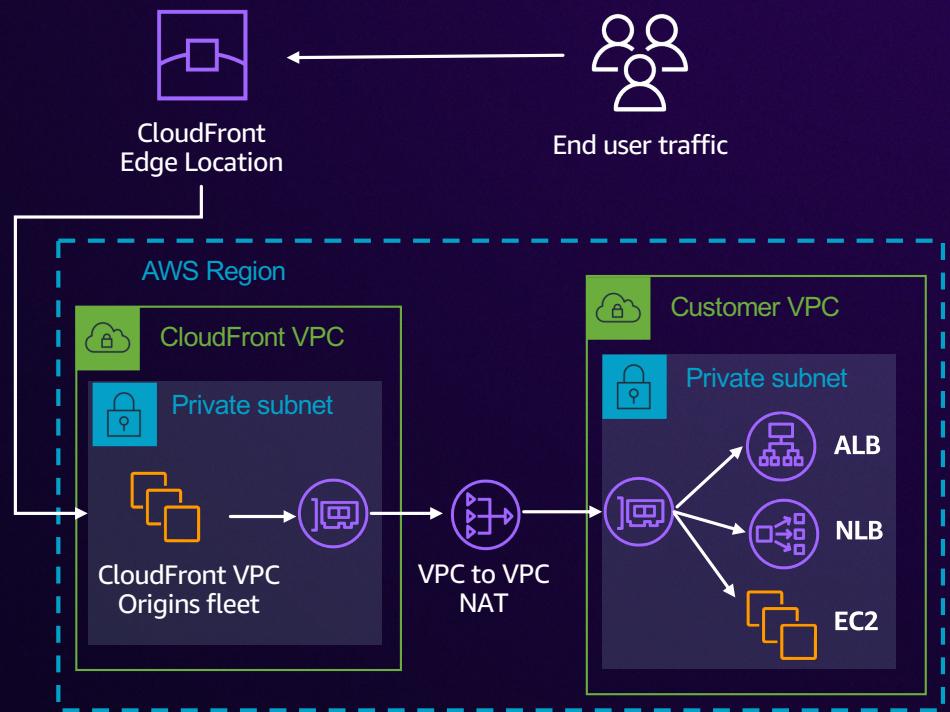
[At application layer](#)

Overview

Origin cloaking is a set of techniques aiming at reducing the attack surface of web applications. It's a best practice to use CloudFront as a single-entry point to web applications, where security controls, such as protections against DDoS attacks and undesired bots, are applied. Origin cloaking stops malicious actors from bypassing CloudFront and its security controls to attack the origin directly, using firewall rules to block any traffic not coming from the CloudFront entry point. Origin cloaking can be implemented at the network layer or at the application layer.

VPC origins, the ultimate Origin Cloaking

- Keep applications in private subnets of a VPC without internet access
- Restrict access to only your CloudFront distributions
- Same performance and scale



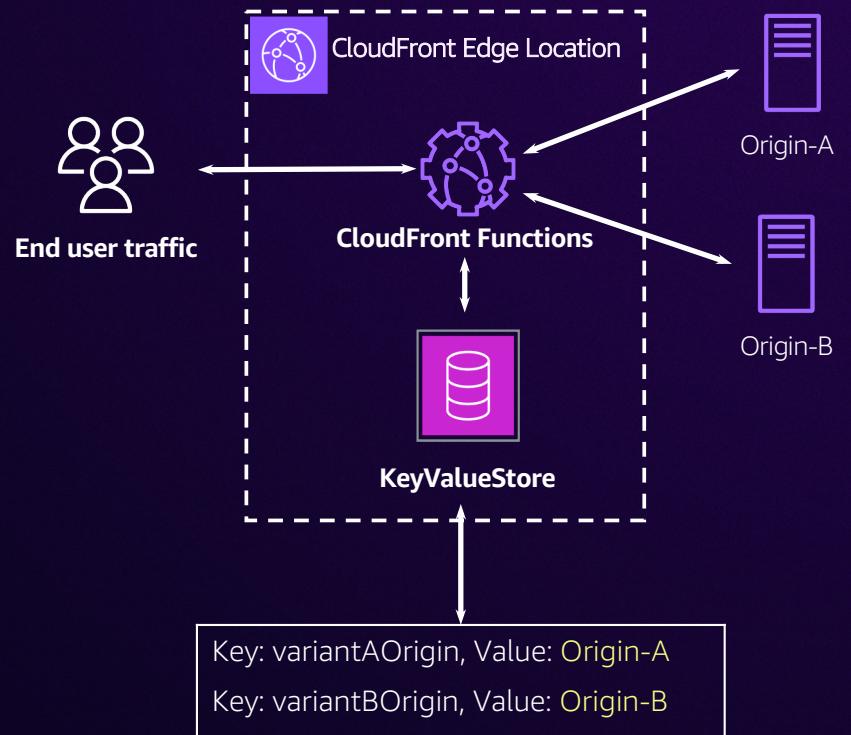
Deception



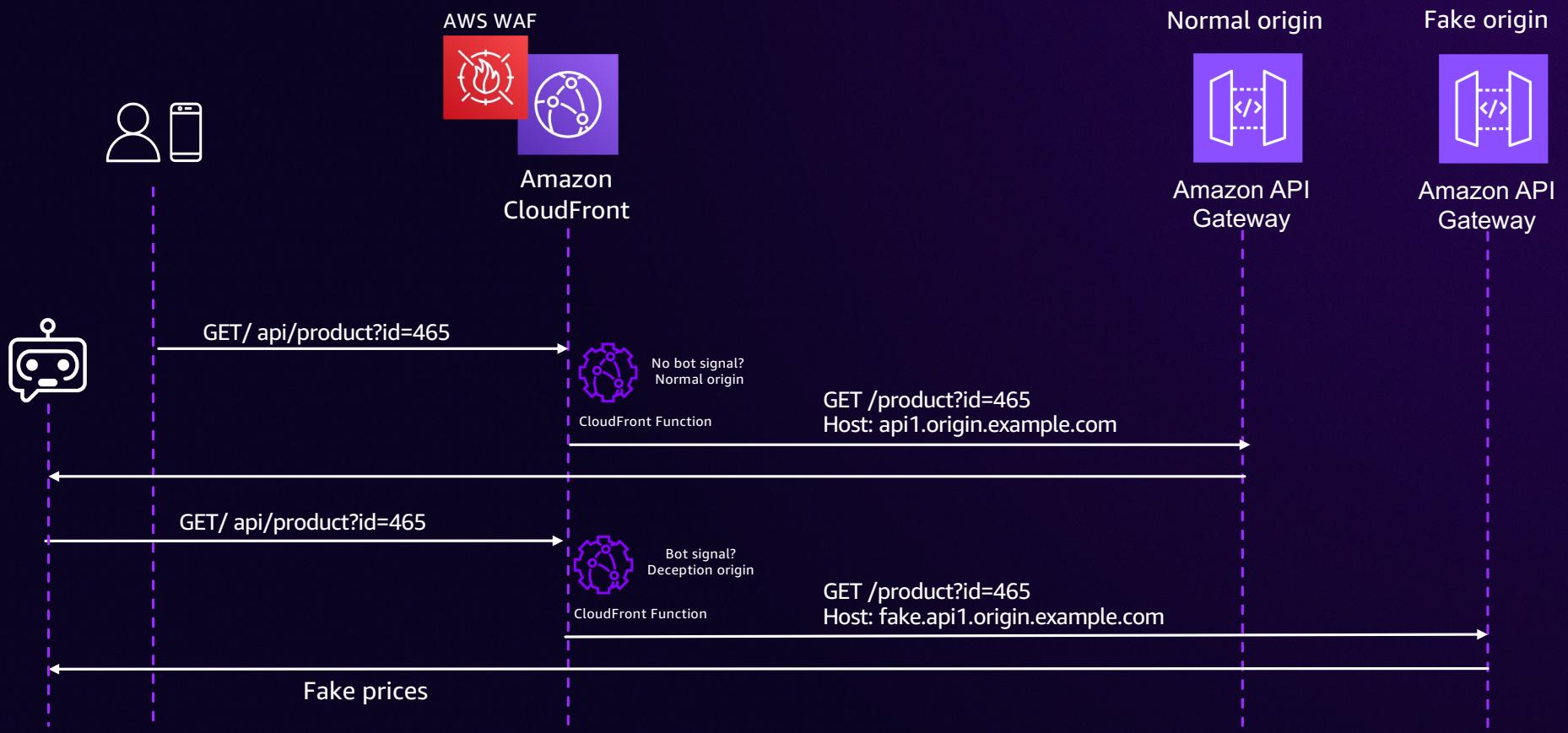
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Origin selection with CloudFront Functions

Now you can change,
modify, update origins
on each request using
CloudFront Functions



Example of deception using Origin Selection



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

What's new in **security** governance?



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

Harmonize central security with application team flexibility, AWS Firewall Manager retrofitting

First rule groups, from AWS Firewall Manager (1)

These rule groups are managed by the AWS Firewall Manager admin. AWS WAF will evaluate them first, before evaluating any rules you have added to this web ACL.

Name	Action	Sampled requests
PREFMManaged-WAF_baseline-1729685276085	Action set by rule group	Enabled

Rules (4)

Find rules

Name	Action	Priority
App-Specific-rule-1	Block	1
App-Specific-rule-2	Block	2
App-Specific-rule-3	Block	3
App-Specific-rule-4	Block	4

Last rule groups, from AWS Firewall Manager (1)

These rule groups are managed by the AWS Firewall Manager admin. AWS WAF will evaluate them last, after evaluating any rules you have added to this web ACL.

Name	Action	Sampled requests
POSTFMMManaged-WAF_baseline_part2-1729685276085	Action set by rule group	Enabled

Managed by security team using Firewall Manager

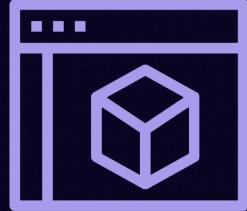
Managed by app team through CI/CD

```
graph TD; A["First rule groups, from AWS Firewall Manager (1)"] --> B["Rules (4)"]; B --> C["Last rule groups, from AWS Firewall Manager (1)"]
```



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

1-Click integration with ALB



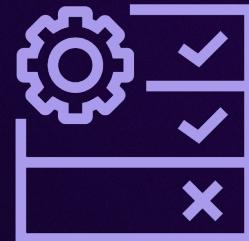
Enable CF+WAF when creating or managing an ALB



Out-of-the-box CDN config optimized for dynamic applications



Uses ACM certificate from HTTPS listener, automatically maps custom domains to CloudFront

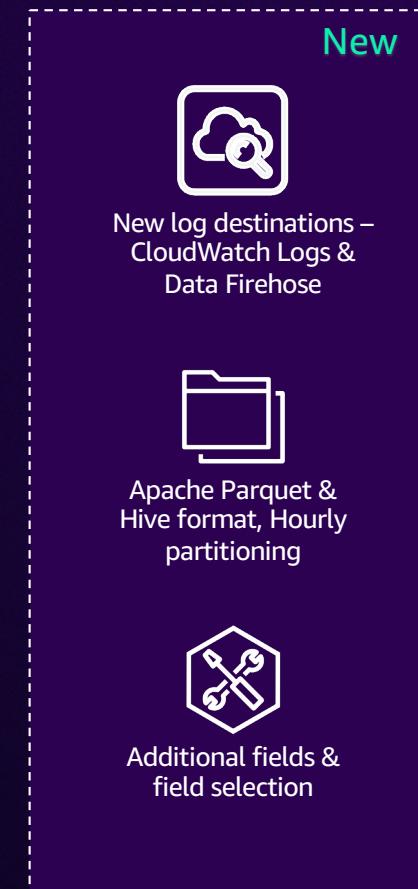
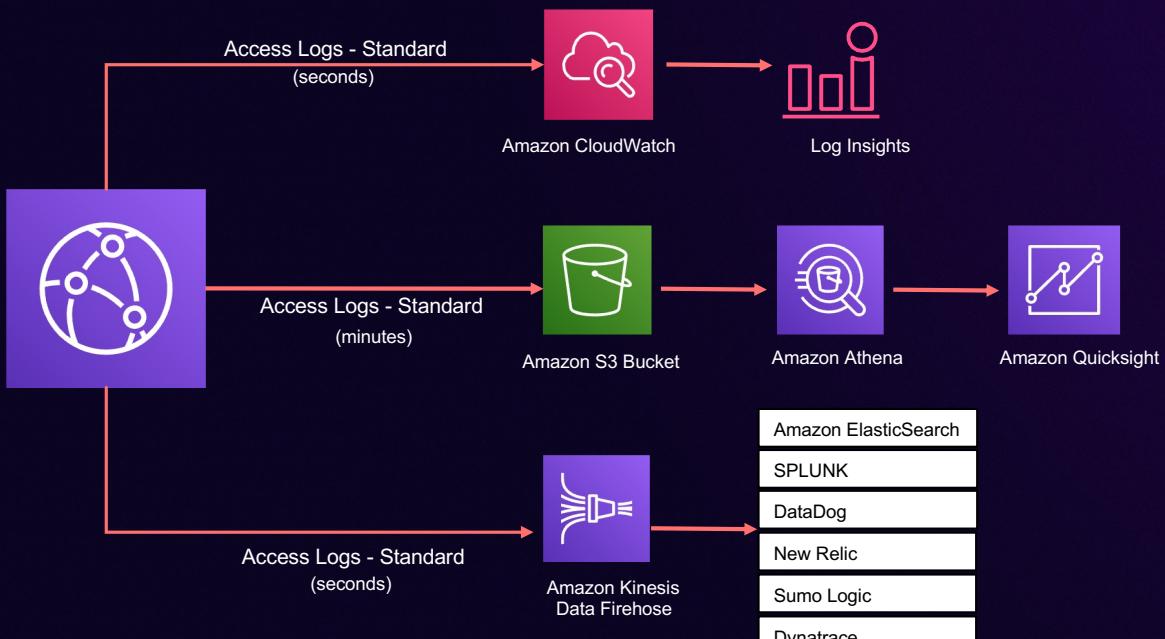


AWS recommended basic security protections through AWS WAF



Optionally attach security group to limit traffic to CF IP Prefix List

Enhanced logging in CloudFront



Thank you!

Achraf Souk

 /in/achrafsouk



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