AWS re:Invent 2024 reCap
Edge security

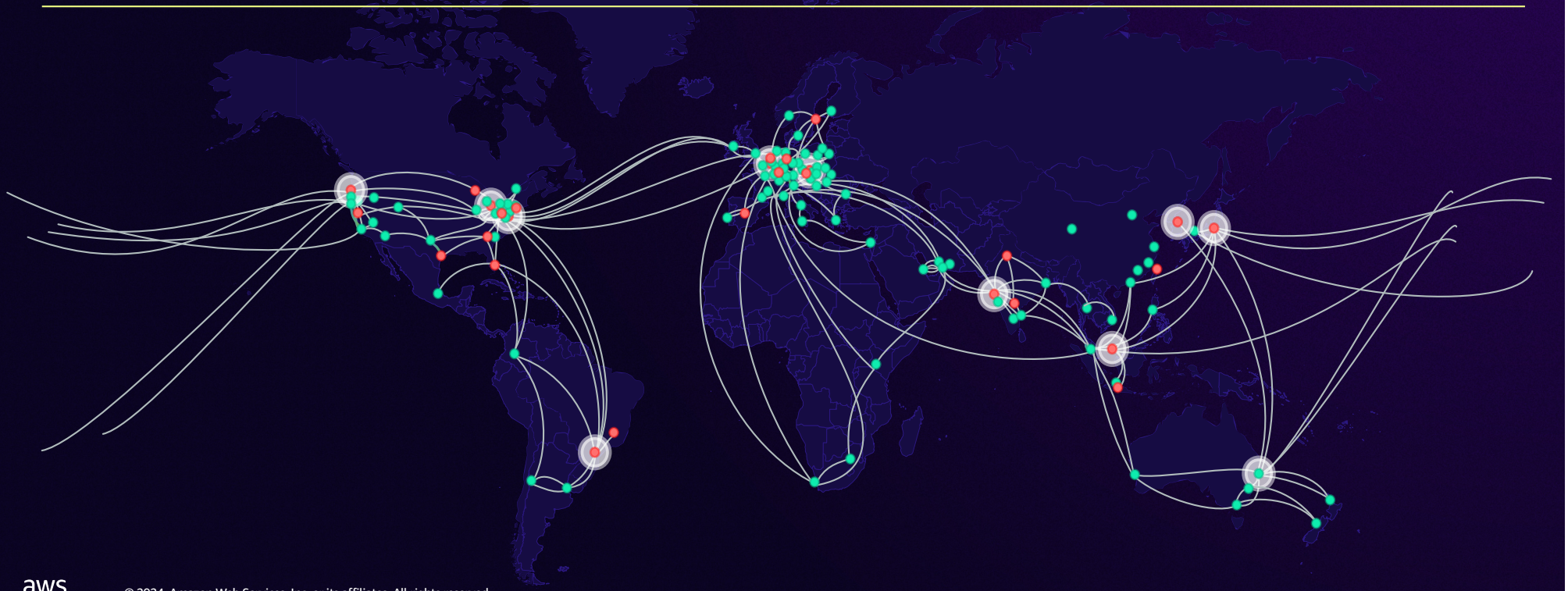
Achraf Souk
Principal Solutions Architect

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



How AWS uses active defense to protect you

MadPot	Sonaris	Mithra
Globally-distributed **network of honeypot** threat sensors with automated response capabilities	An **active defense tool** that analyzes potentially harmful network traffic	An internal **neural network graph model** that uses algorithms for threat intelligence
Observe and react to threat actors' evolving tactics, techniques, and procedures (TTPS)	Deny attempts to find unintentionally public S3 buckets and vulnerable services	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

Case Study - Anonymous Sudan

United States Attorney's Office
Central District of California

About CDCA | Find Help | Contact Us

Search

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 16, 2024

Share

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 Yousif Omer, 22, and Alaa Salah Yusuuf 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 demonstrates the resolve of the Defense Criminal Investigative Service (DCIS) to safeguard the Department of Defense from evolving cyber threats," said Kenneth A. DeChellis, DCIS Cyber Field Office, Special Agent in Charge. "Cybercriminals need to understand that if they target America's warfighters, they will face consequences."

amazon

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

News / AWS

5 min

October 16, 2024

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

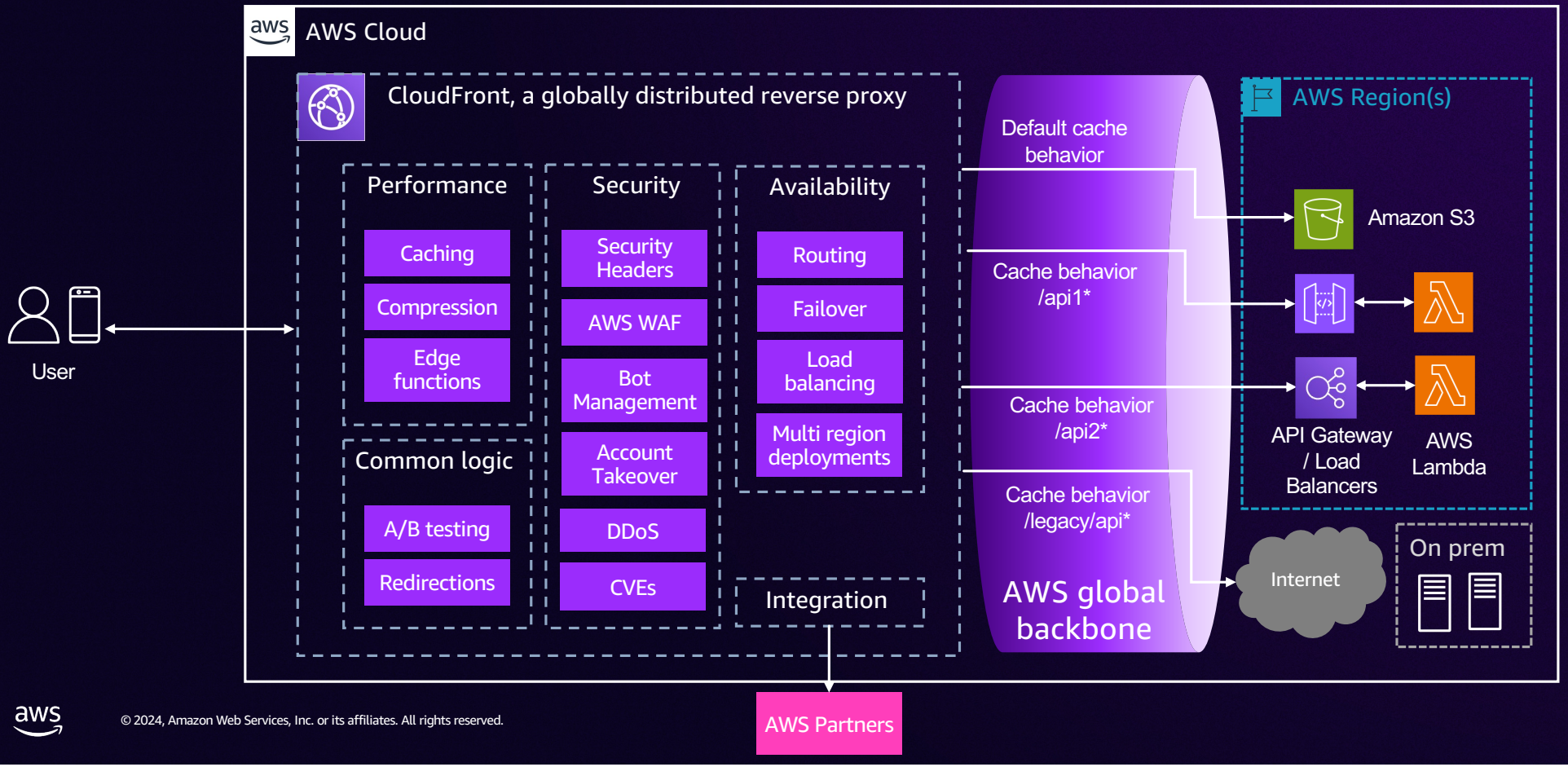
Written by Amazon Staff

5 min

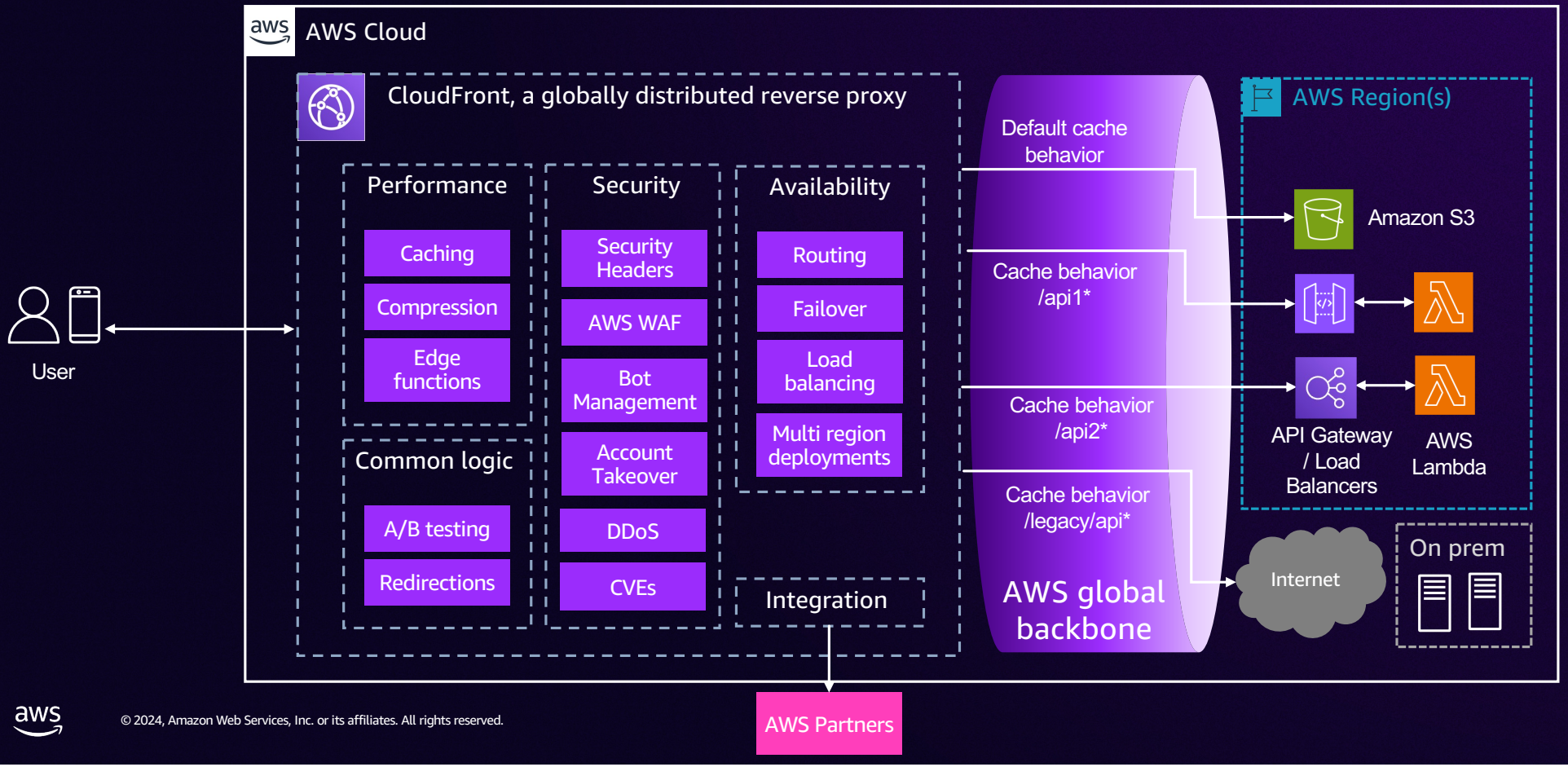
Reading:
Amazon helps the US Department of Justice thwart international

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

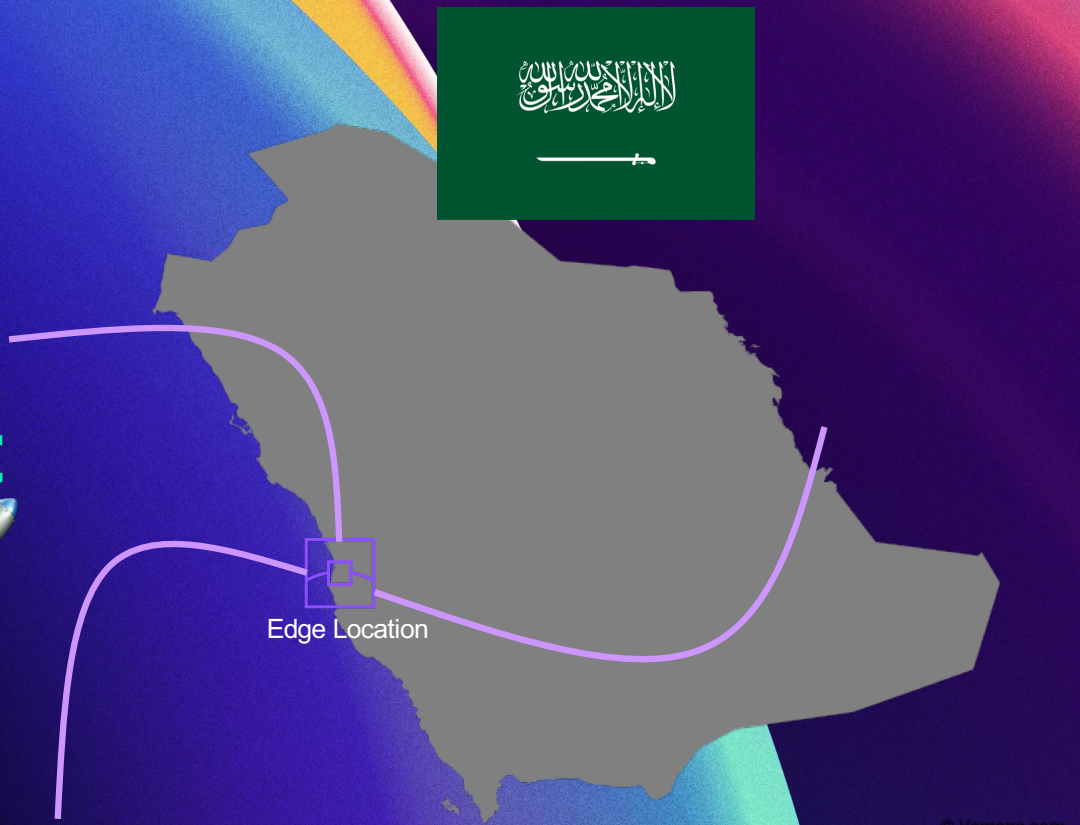
CloudFront – Mental model



What's new on the user side?



Amazon CloudFront
Expanding in KSA 🚀

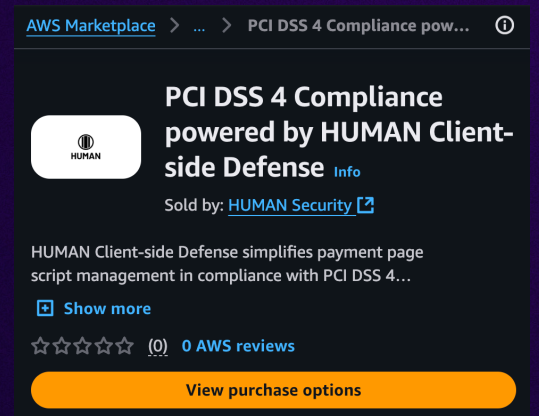


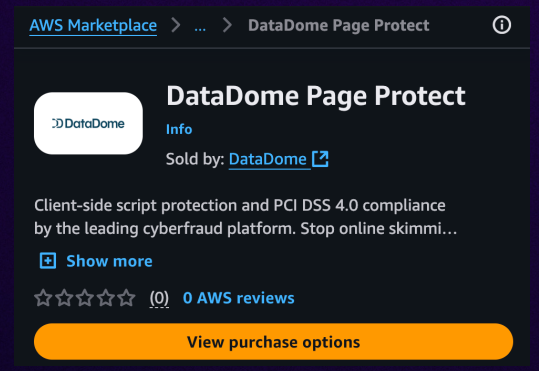
PCI DSS v4.0 embraced Client Side Protection

PCI Security Standards Council

PCI Security Standards Council

Requirements and Testing Procedures	
11.6 Unauthorized changes on payment pages are detected and responded to.	
Defined Approach Requirements	**Defined Approach Testing Procedures**
11.6.1 A change- and tamper-detection mechanism is deployed as follows: • 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: – At least once every seven days **OR**	**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. **11.6.1.b** Examine configuration settings to verify the mechanism is configured in accordance with all elements specified in this requirement. **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.





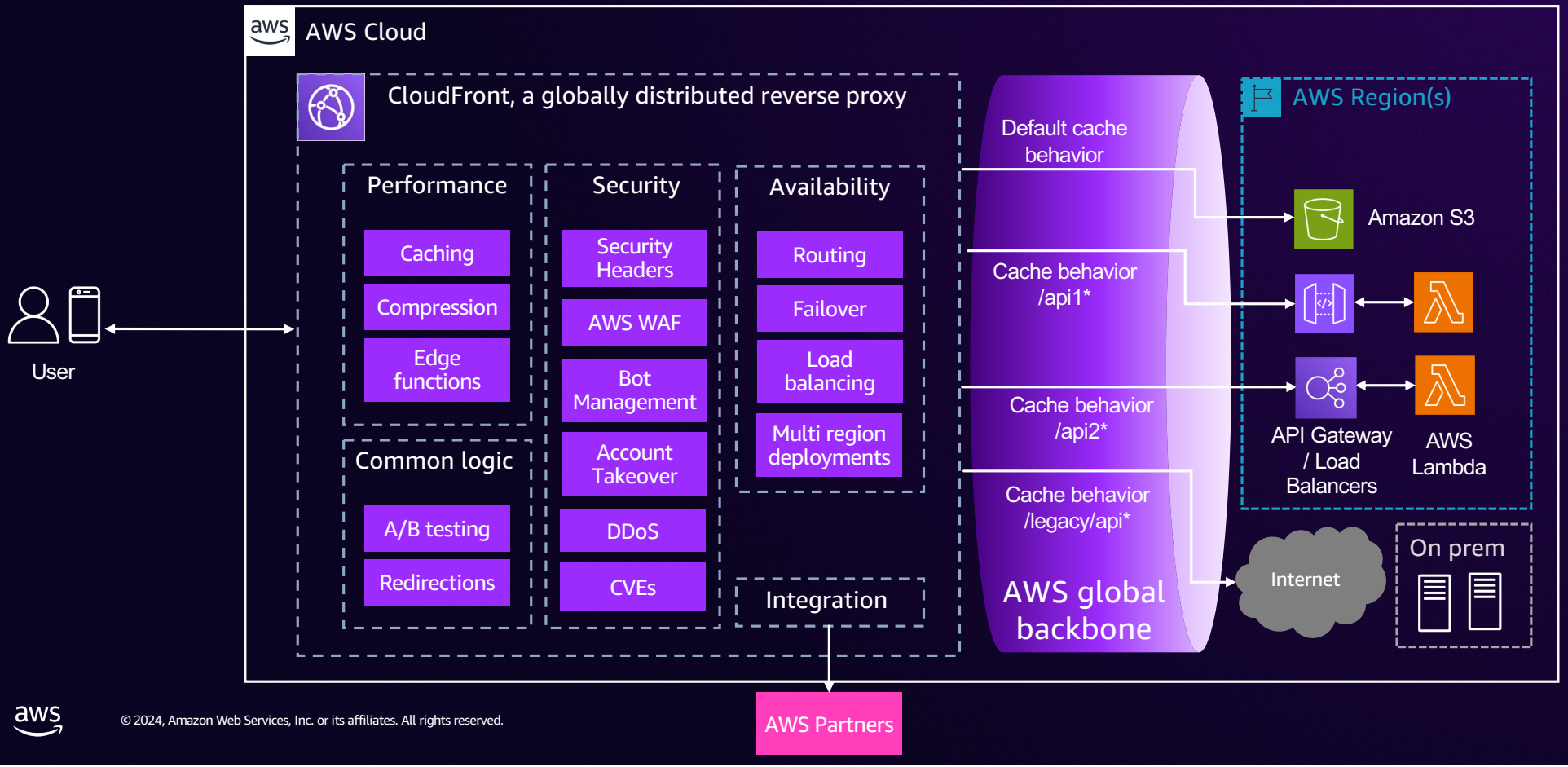
aws

Allow-list your endpoint IPs in customer firewalls

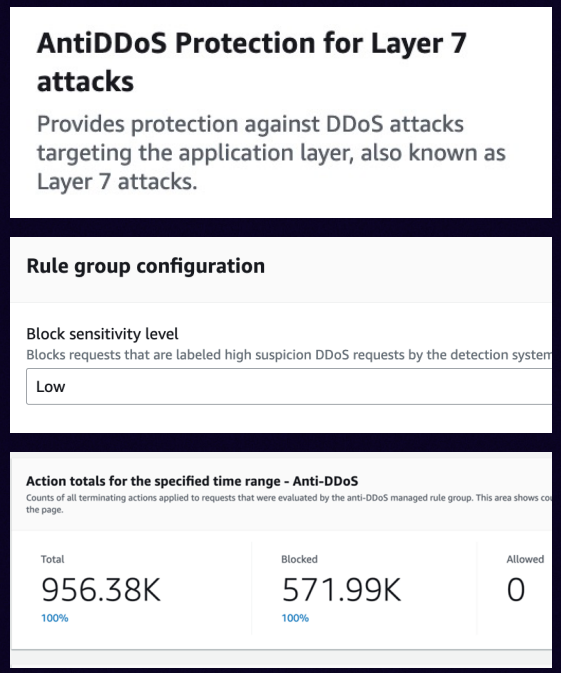
- B2B Business, e.g. SaaS or Connected devices
- How to prevent the firewall of your customers to block traffic to your CloudFront based endpoint?
- Anycast Static IPs provides a fixed, dedicated set of IPs that do not change

Enterprise Applications
Allow-Listing

What's new on AWS WAF?



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



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

in preview


CloudFront no
longer charges for
requests blocked
by AWS WAF

LLMs are hungry

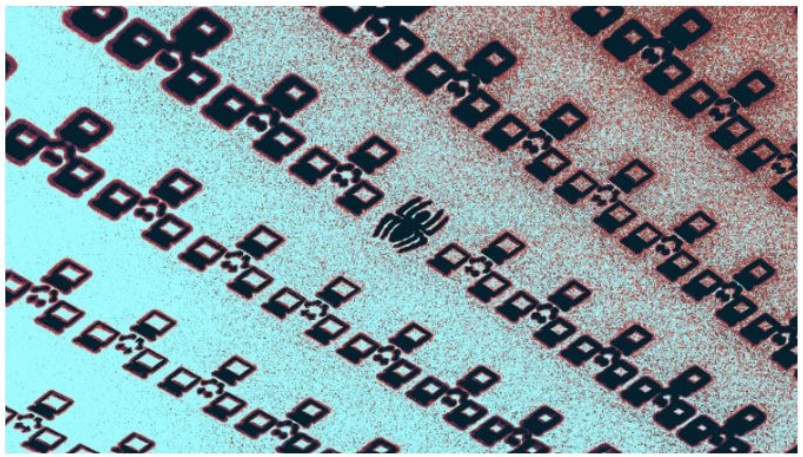
… for your public data

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.



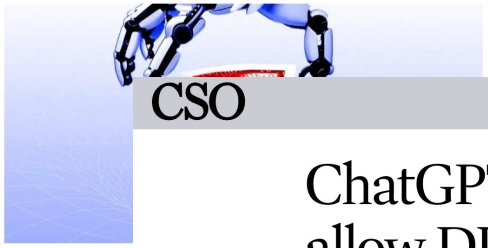
[Source Photo: Getty Images]

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



Getty Images; Alys

CSO

ChatGPT API flaws could allow DDoS, prompt injection attacks

News

21 Jan 2025 • 3 mins

APIs | DDoS | Vulnerabilities

Opting out of AI crawling

- Robots.txt
- No standard for disallowing all AI crawl
  (e.g. User-Agent: AI-Ingest)
  - Disallowing specific AI bots:

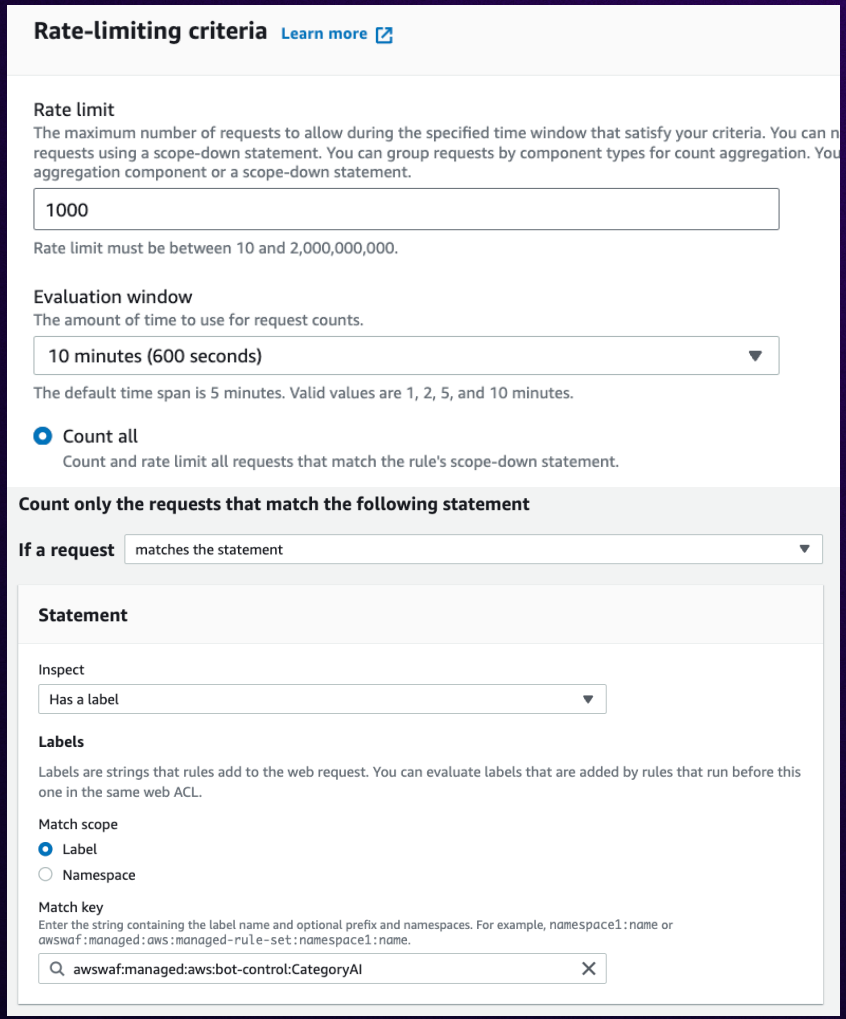
```
User-Agent: GPTBot
Disallow: /
```

  - Or Disallowing all bots, but allowing specific desired ones (e.g. Google Bot)

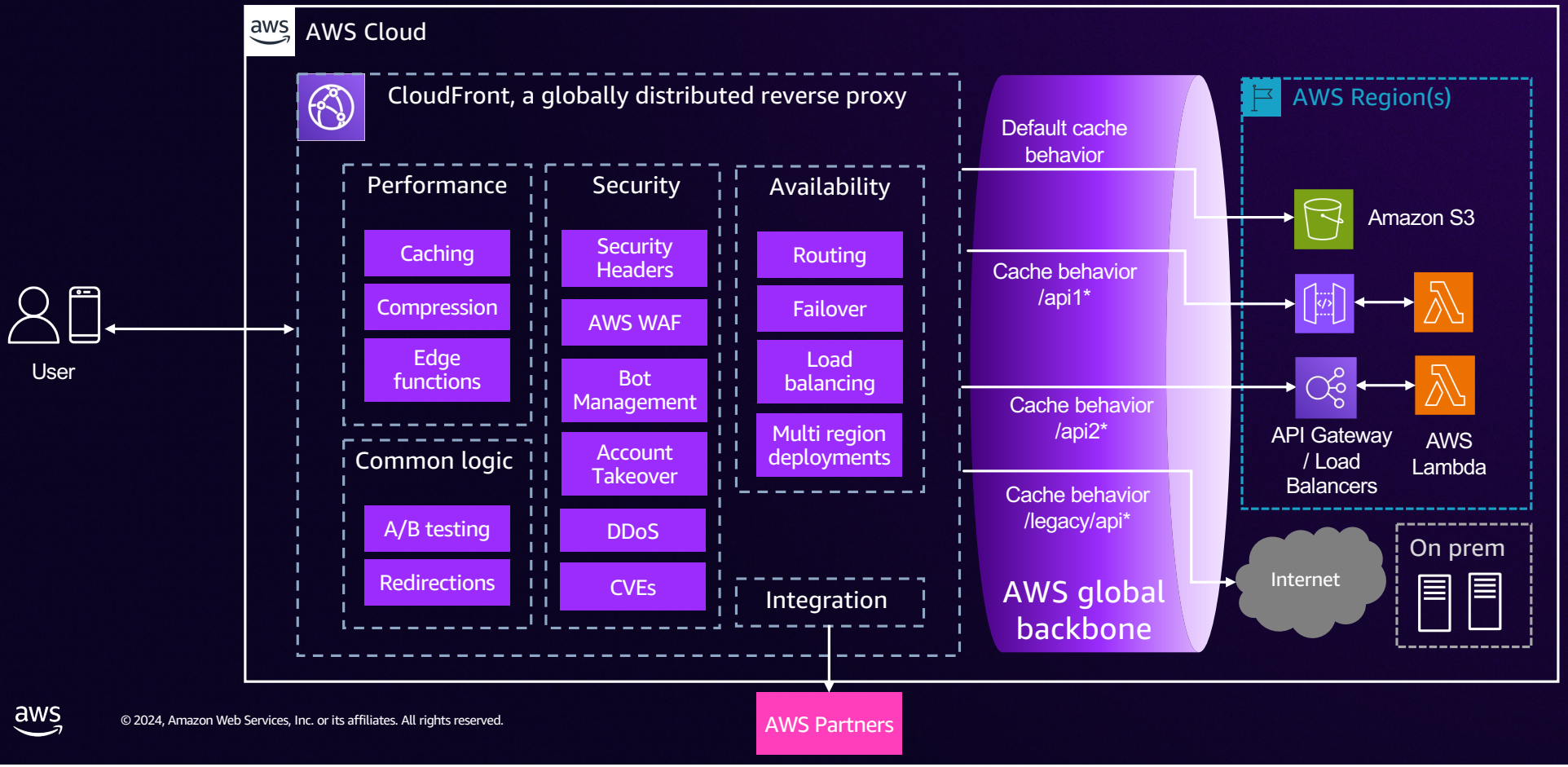
New signals for AI bots in AWS WAF Bot Control

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



What's new in origin integration?




AWS WAF
AWS Threat Intelligence
Anti-DDoS
CloudFront


Attack the origin

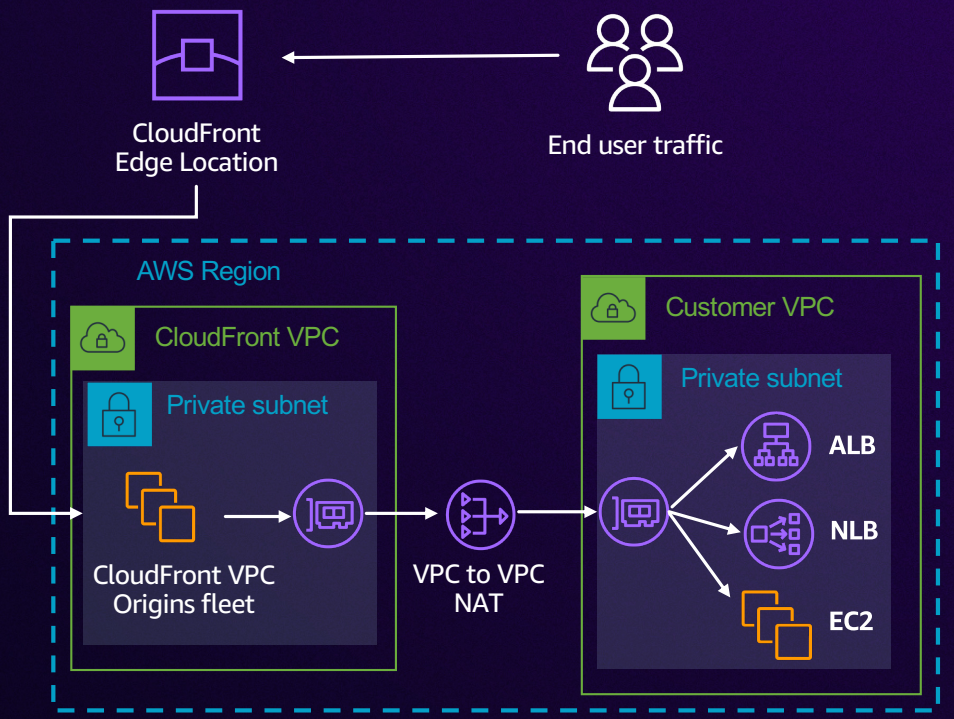
PAGE CONTENT

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 by-pa CloudFront and its security controls to attack the origin directly, using firewall block any traffic not coming from the CloudFront entry point. Origin cloaking can b

VPC origins, the ultimate Origin Cloaking

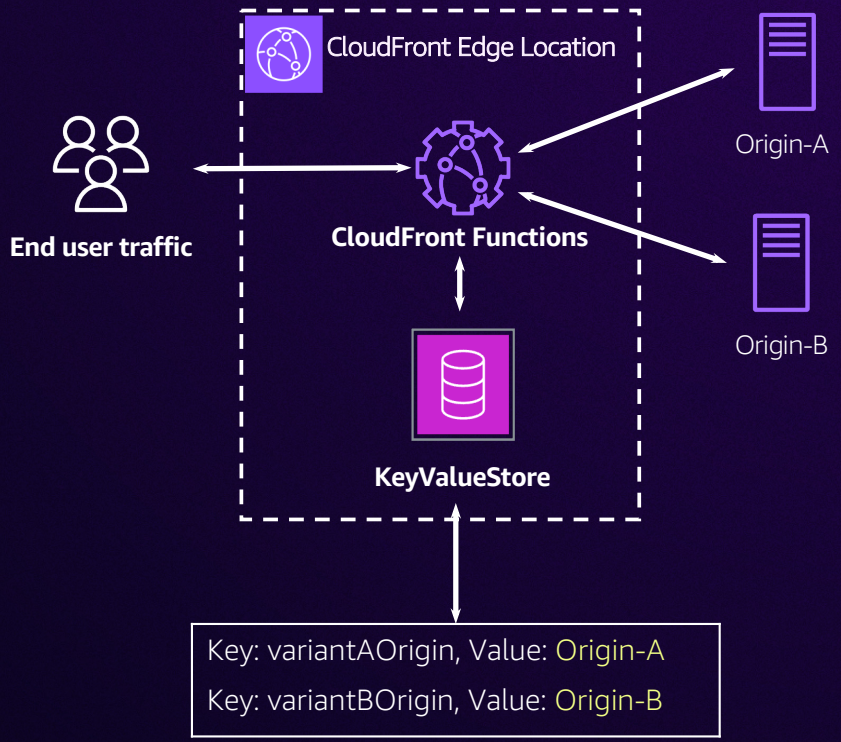
- Keep applications in private subnets of a VPC without internet access
- Restrict access to only your CloudFront distributions
- Same performance and scale



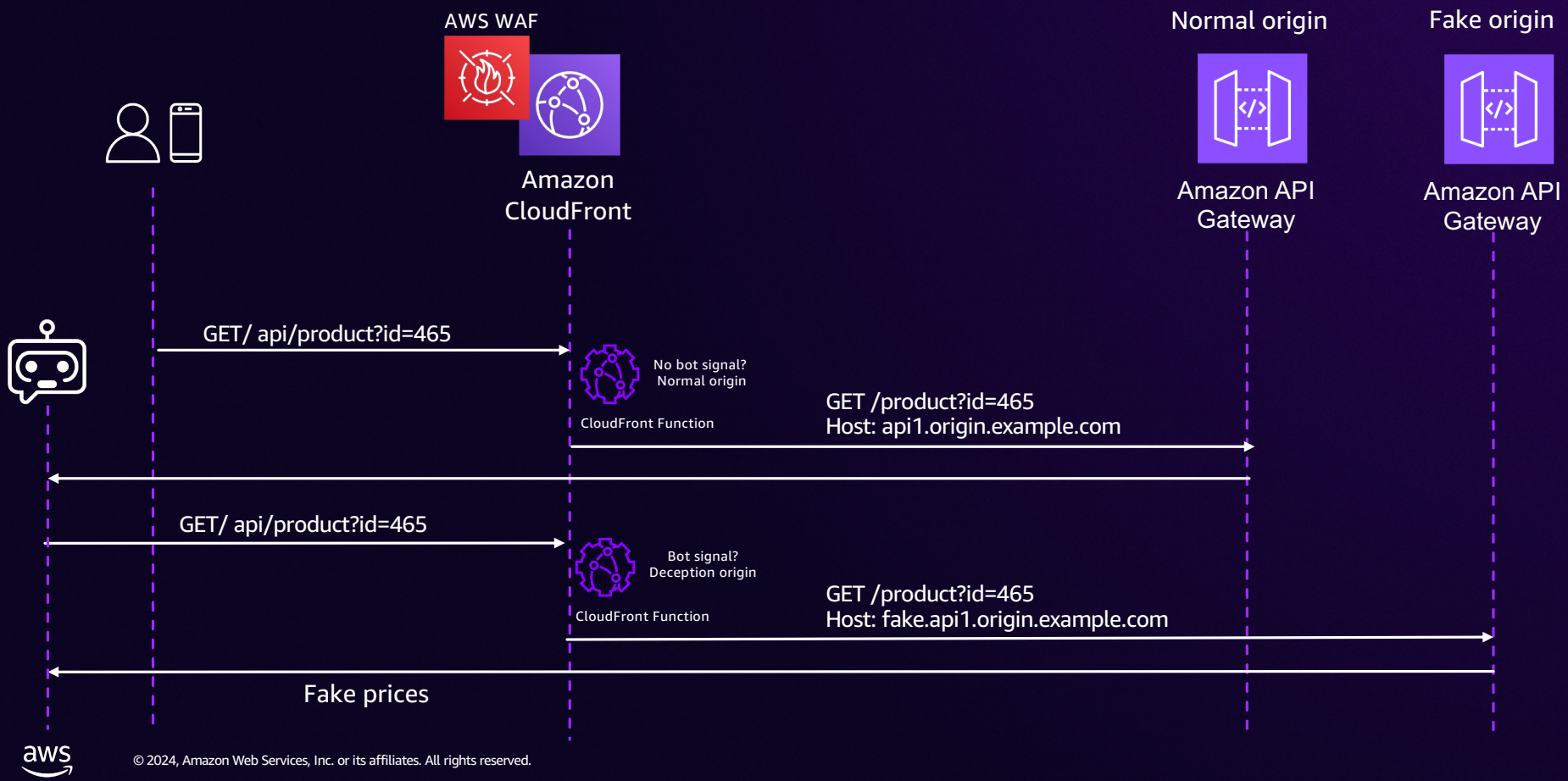
Deception

Origin selection with CloudFront Functions

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

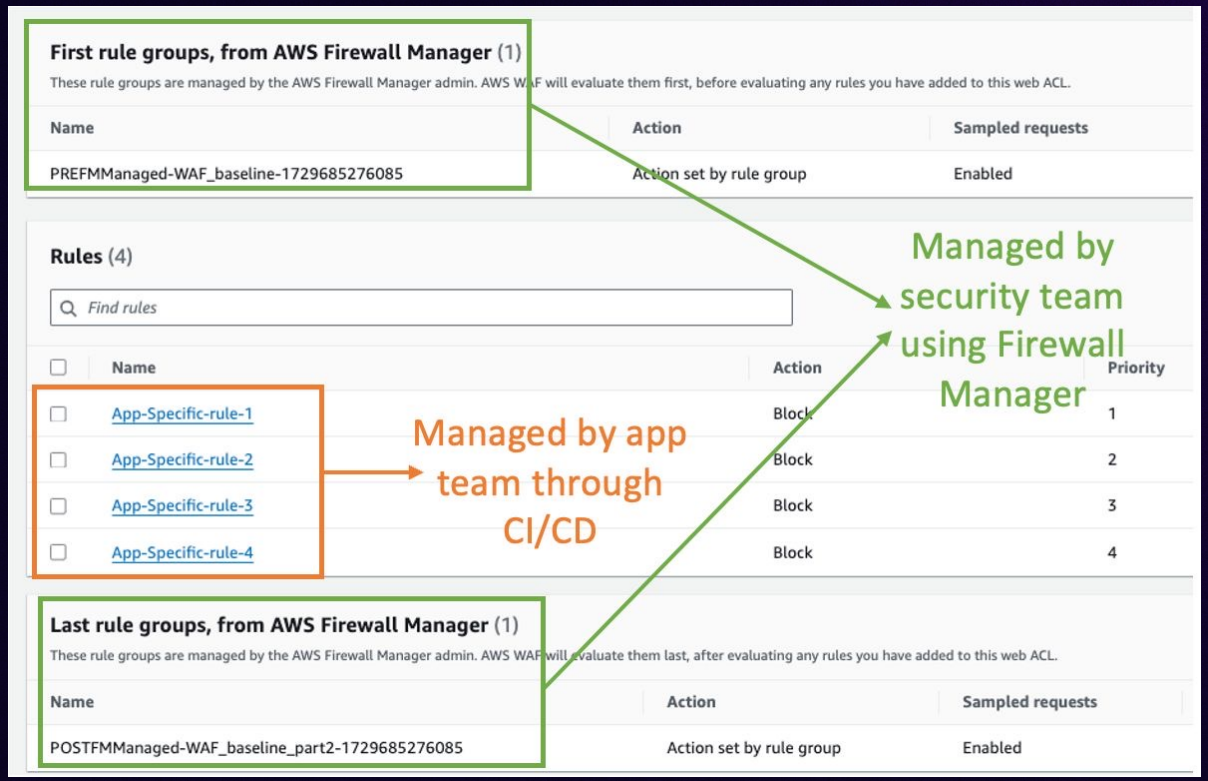


Example of deception using Origin Selection

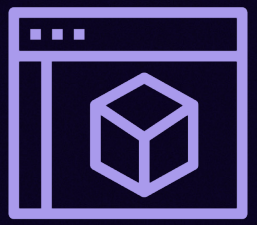


What's new in security governance?

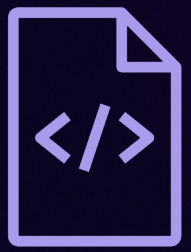
Harmonize central security with application team flexibility, AWS Firewall Manager retrofitting



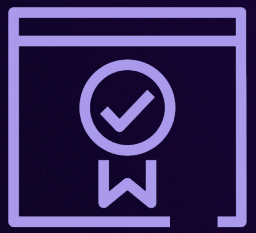
1-Click integration with ALB



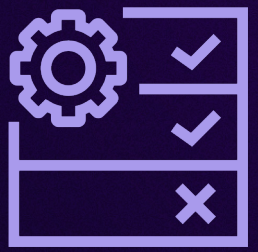
Enable CF+WAF when creating or managing an ALB



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



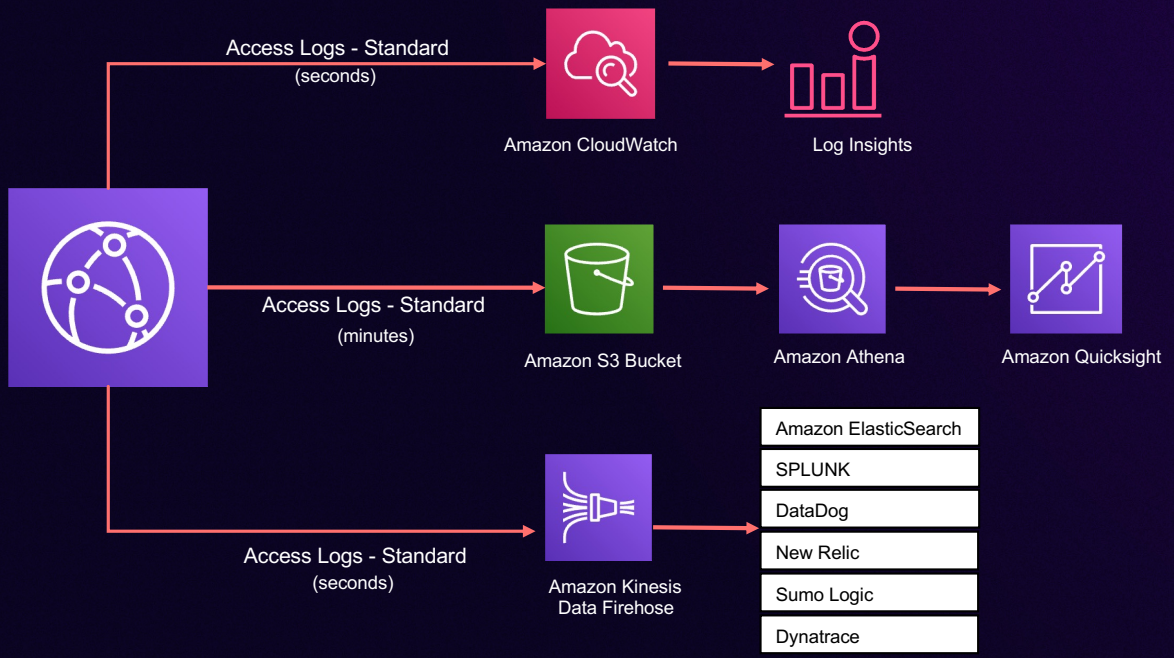
Uses ACM certificate from HTTPS listener, automatically maps custom domains to CloudFront



AWS recommended basic security protections through AWS WAF

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

Enhanced logging in CloudFront



New

New log destinations – CloudWatch Logs & Data Firehose

Apache Parquet & Hive format, Hourly partitioning

Additional fields & field selection

Thank you!

Achraf Souk

/in/achrafsouk