AWS re:Inforce

JUNE 10 - 12, 2024 | PHILADELPHIA, PA

NIS306

How Catch uses AWS WAF Bot Control on their ecommerce platform

Robbie Cooray
Sr. Solutions Architect
Amazon Web Services

Cameron Hall
Platform Engineering Lead
Catch

Etienne Münnich
Sr. Edge Specialist SA
Amazon Web Services

Speakers

Robbie Cooray

Sr. Solutions Architect
Amazon Web Services

Cameron Hall

Platform Engineering Lead
Catch

Etienne Münnich

Sr. Edge Specialist SA
Amazon Web Services

Agenda

01 Threat landscape

02 How AWS WAF helped **Catch** improve their security posture

03 How you can protect your web applications today

Last 12 months statistics

THREAT LANDSCAPE

Last 12 months statistics

THREAT LANDSCAPE

212k

Total DDoS attacks

Last 12 months statistics

THREAT LANDSCAPE

212k

Total DDoS attacks

155M RPS

Largest request flood attack

Last 12 months statistics

THREAT LANDSCAPE

212k

Total DDoS attacks

155M RPS

Largest request flood attack

842 Gbps

Largest bandwidth heavy attack

Last 12 months statistics

THREAT LANDSCAPE

212k

Total DDoS attacks

155M RPS

Largest request flood attack

842 Gbps

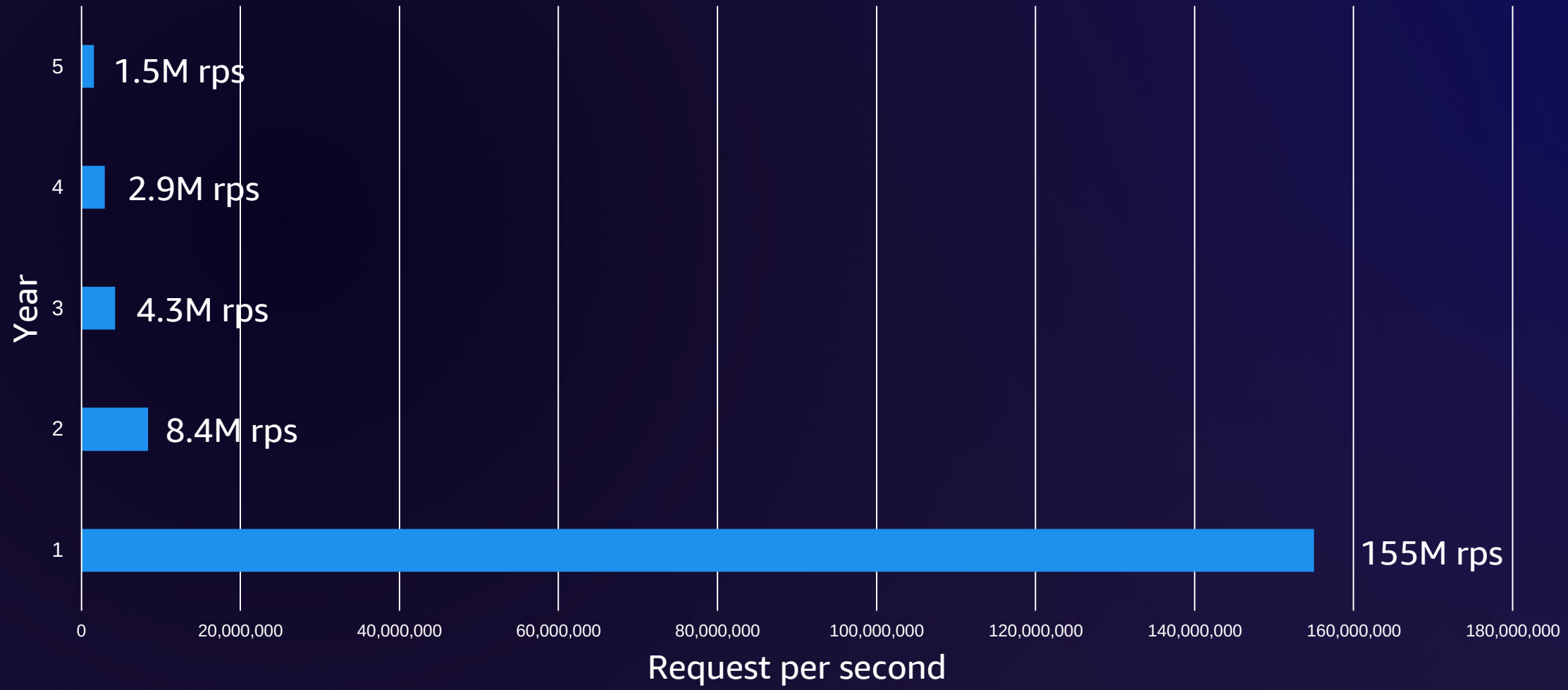
Largest bandwidth heavy attack

221M PPS

Largest packet attack

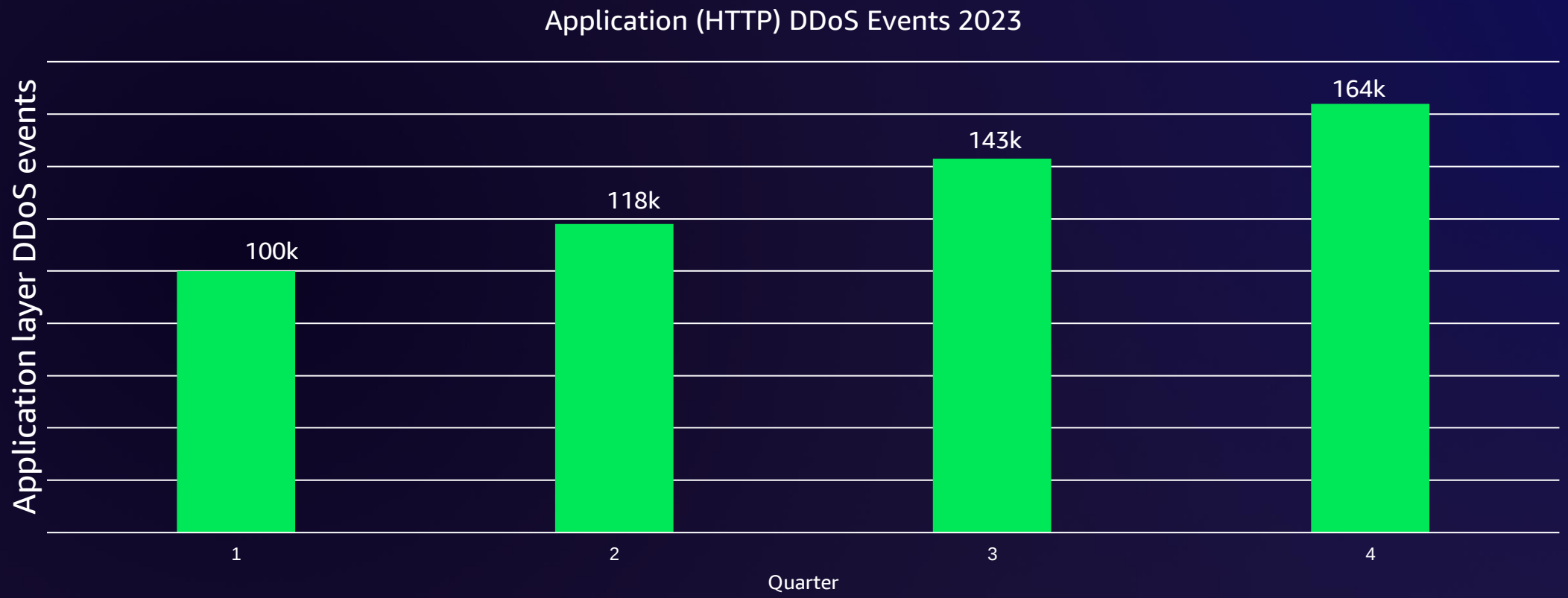
Largest request flood events by year, as seen by AWS

THREAT LANDSCAPE



Application (HTTP) layer DDoS events rising

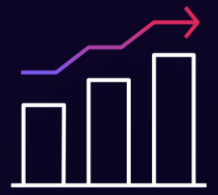
THREAT LANDSCAPE



Application (HTTP) DDoS events
526,000 events detected in 2023
52.1% YoY increase

Performance matters

THREAT LANDSCAPE



70%

Influenced by page speed [1]

17%

Decreased conversion every additional second [1]

15%

Frustrated with slow checkout [2]

1 Tooltester. (2023, Aug). Website Loading Time Statistics (2023).
2 PYMNTS, Checkout.com (2022) Checkout Conversion Index (2022)

Bot attack vectors

THREAT LANDSCAPE

Bot attack vectors

THREAT LANDSCAPE

More than

47%

of all internet traffic is bots

Bot attack vectors

THREAT LANDSCAPE

More than

47%

of all internet traffic is bots

Common Bad bot activity

Impacting user experience and reputation

Bot attack vectors

THREAT LANDSCAPE

More than

47%

of all internet traffic is bots

Common Bad bot activity

Impacting user experience and reputation

Content scraping

Bot attack vectors

THREAT LANDSCAPE

More than

47%

of all internet traffic is bots

Common Bad bot activity

Impacting user experience and reputation

Content scraping

Credential stuffing / Account takeover fraud

Bot attack vectors

THREAT LANDSCAPE

More than

47%

of all internet traffic is bots

Common Bad bot activity

Impacting user experience and reputation

Content scraping

Credential stuffing / Account takeover fraud

Card Cracking

Bot attack vectors

THREAT LANDSCAPE

More than

47%

of all internet traffic is bots

Common Bad bot activity

Impacting user experience and reputation

Content scraping

Credential stuffing / Account takeover fraud

Card Cracking

Account creation fraud

Bot attack vectors

THREAT LANDSCAPE

More than

47%

of all internet traffic is bots

Common Bad bot activity

Impacting user experience and reputation

Content scraping

Credential stuffing / Account takeover fraud

Card Cracking

Account creation fraud

Scalping

Bot attack vectors

THREAT LANDSCAPE

More than

47%

of all internet traffic is bots

Common Bad bot activity

Impacting user experience and reputation

Content scraping

Credential stuffing / Account takeover fraud

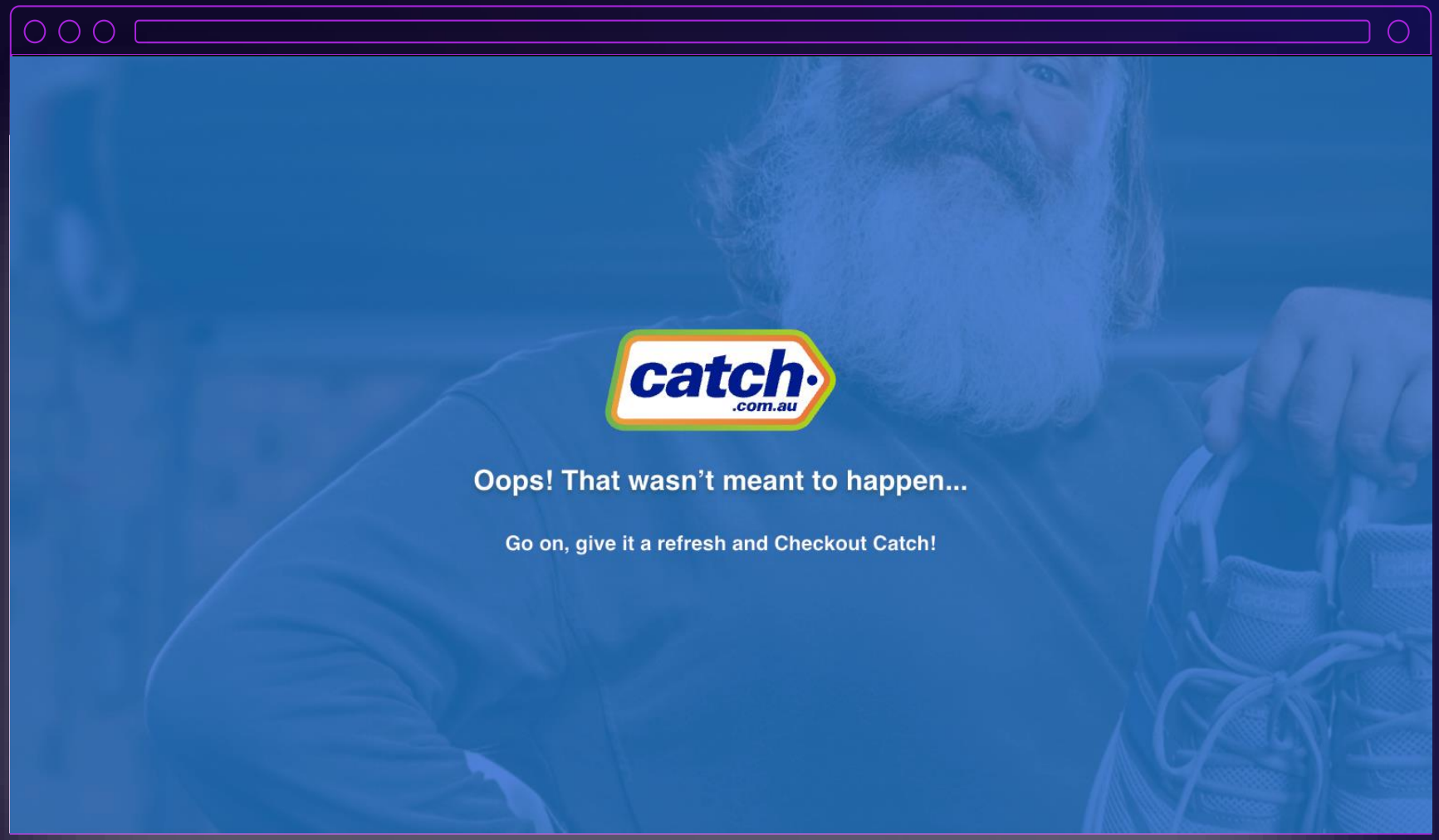
Card Cracking

Account creation fraud

Scalping

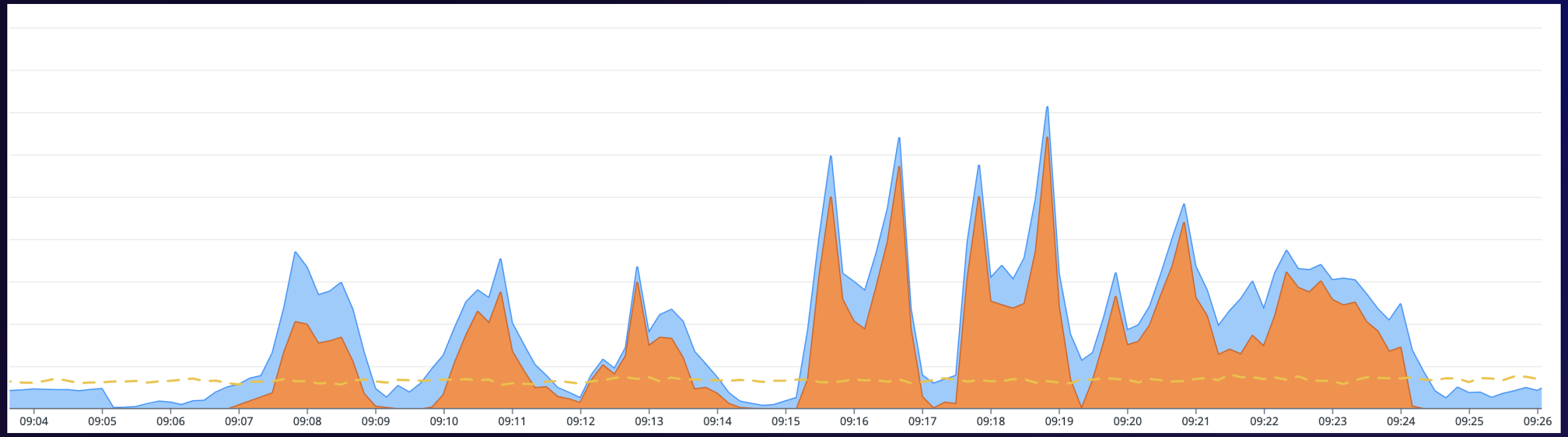
Denial of Service

A busy day in October



Impact to the website and APIs

11x EXPECTED TRAFFIC REQUEST VOLUMES



Requests per second (RPS)
Errors per second
Previous day RPS

How Catch improved their security posture

Incident response

Implemented a generous rate limit and reduced the threshold as we analyzed traffic patterns

Created a simple IP blocklist rule and created a related playbook

Creating a “break-glass” Geo-Block rule to restrict traffic to Australia and New Zealand

Post-incident review

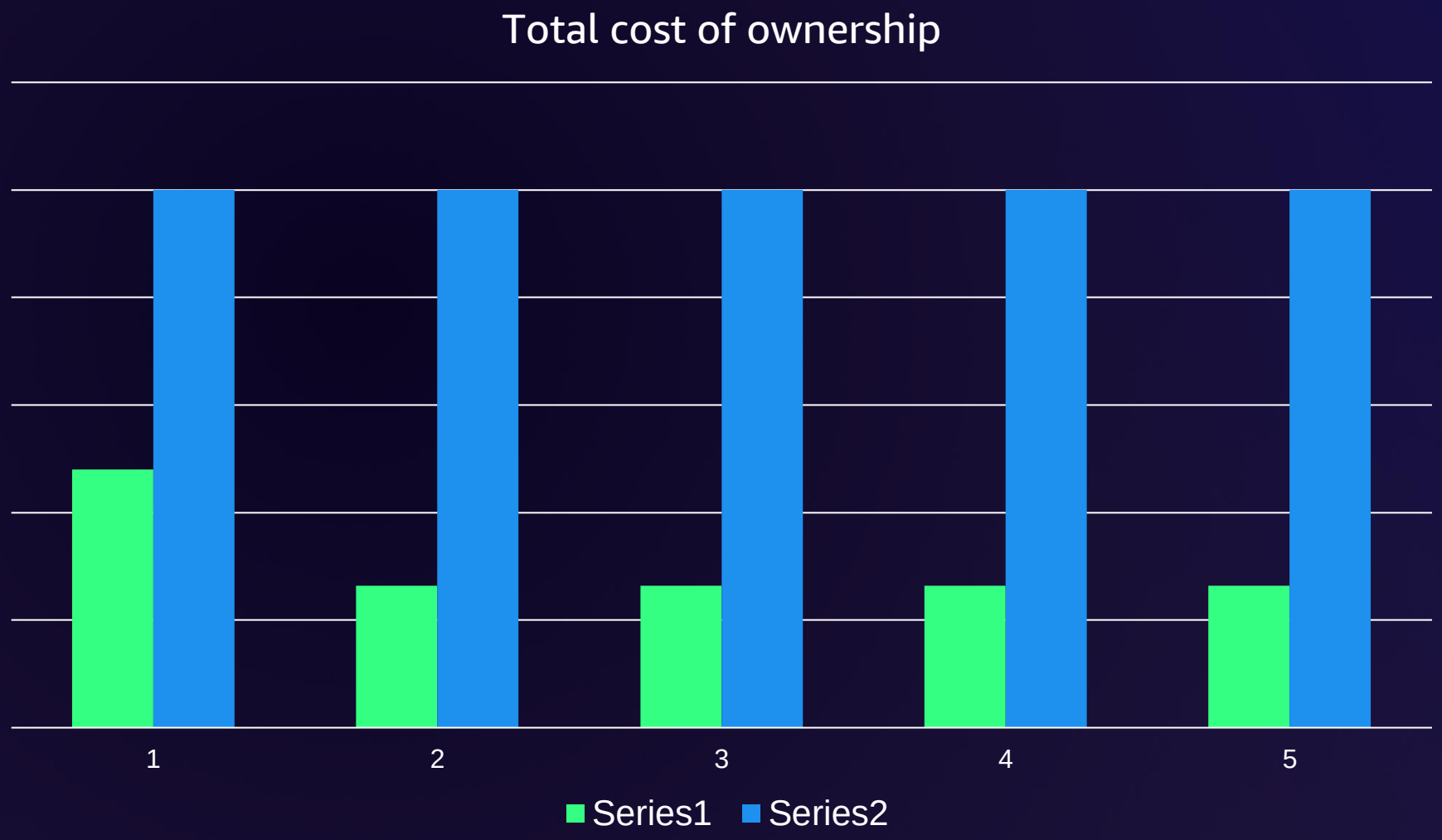
Post-mortem

Went to market

Proof of concept

Operating model

It’s not just about request costs



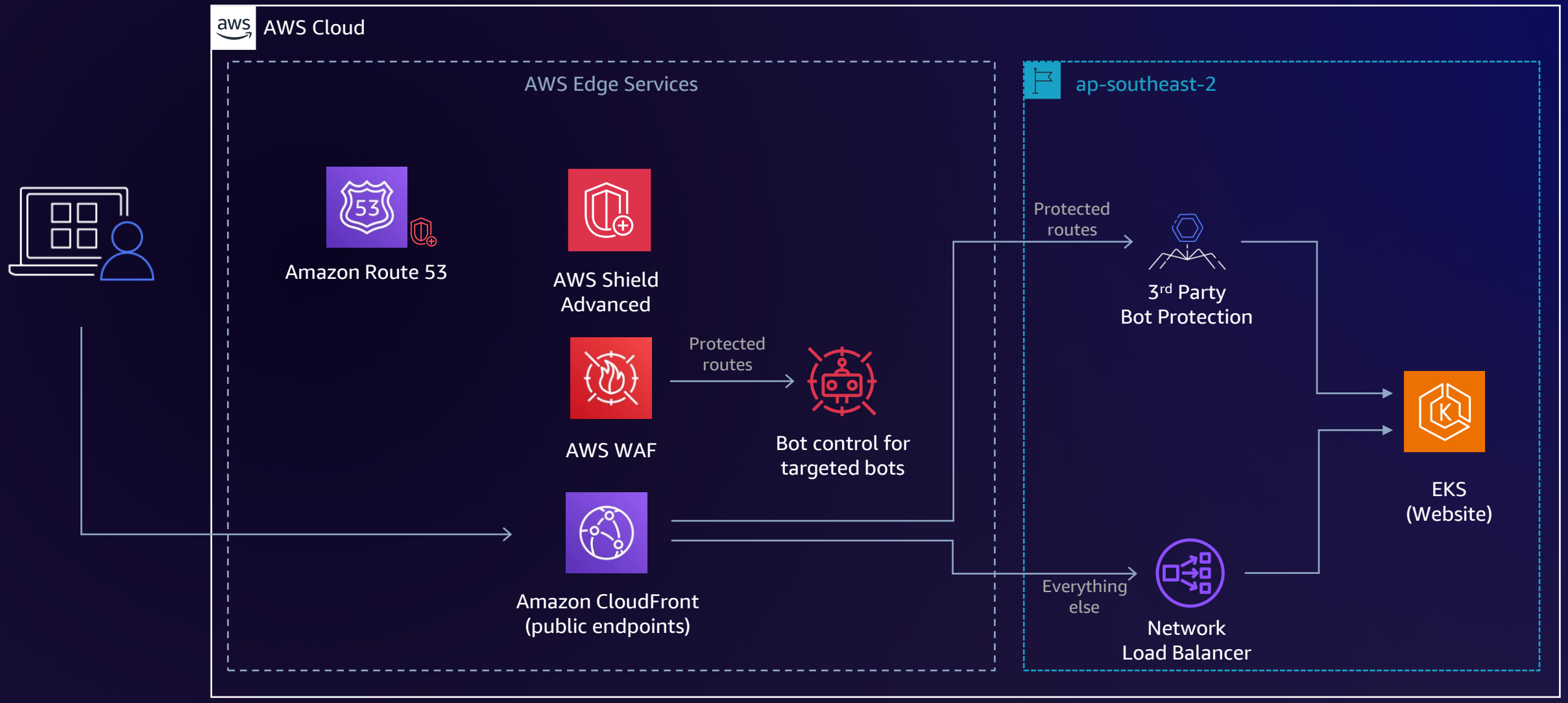
2x

Savings in Year 1

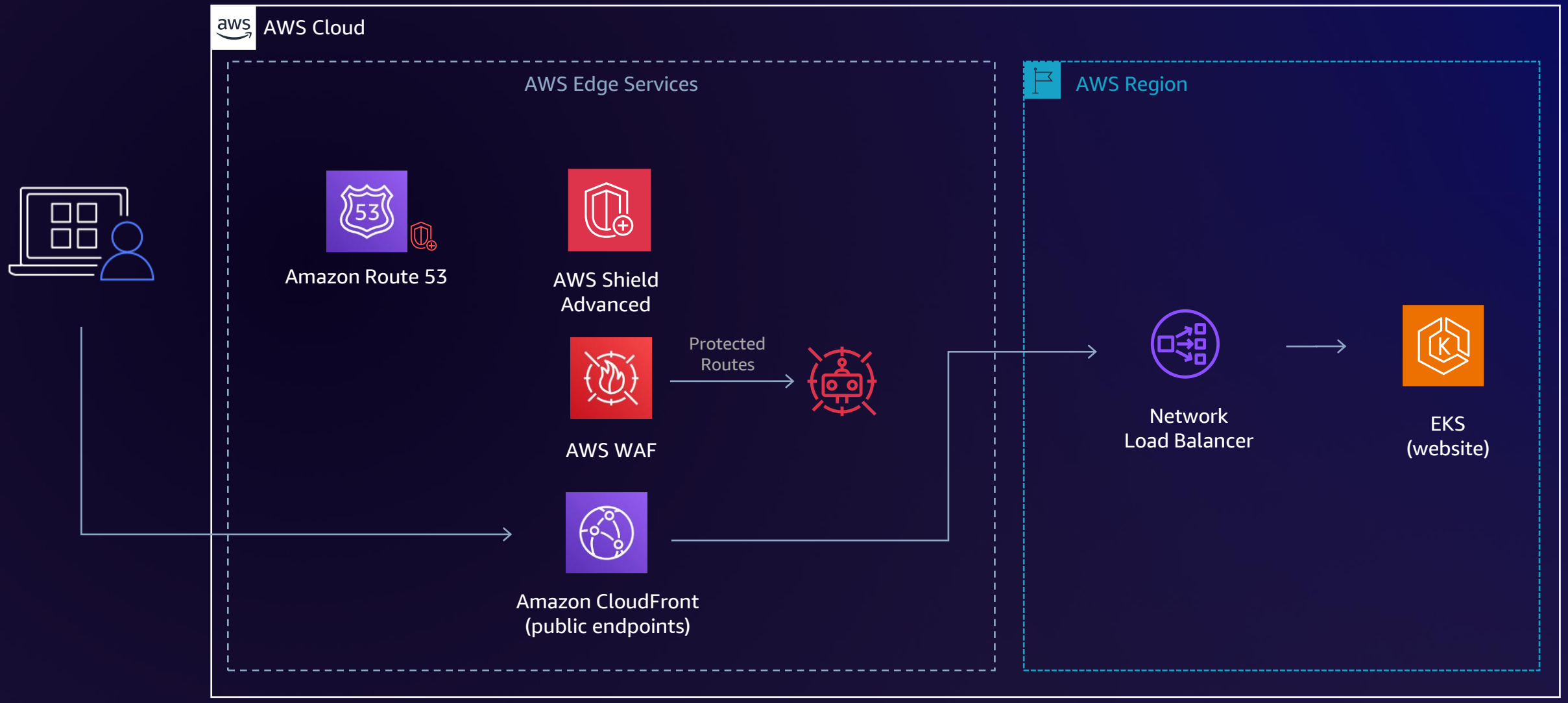
4x

Savings each year thereafter

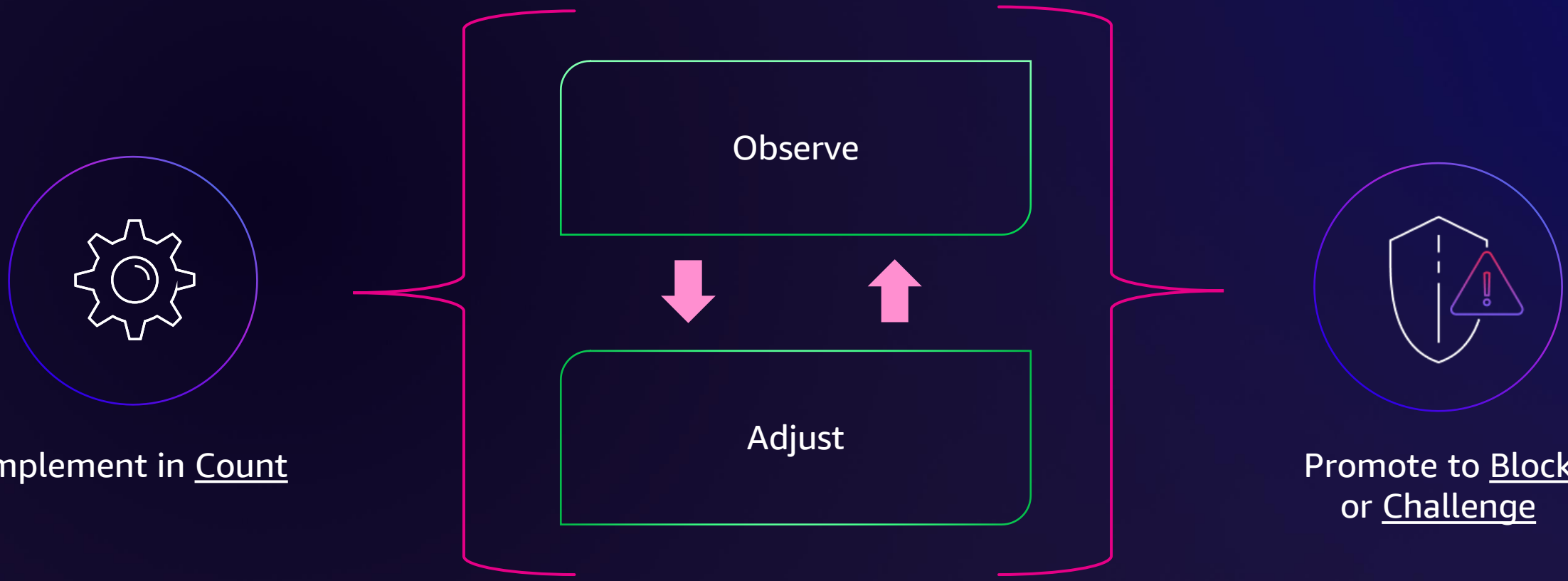
Migration state



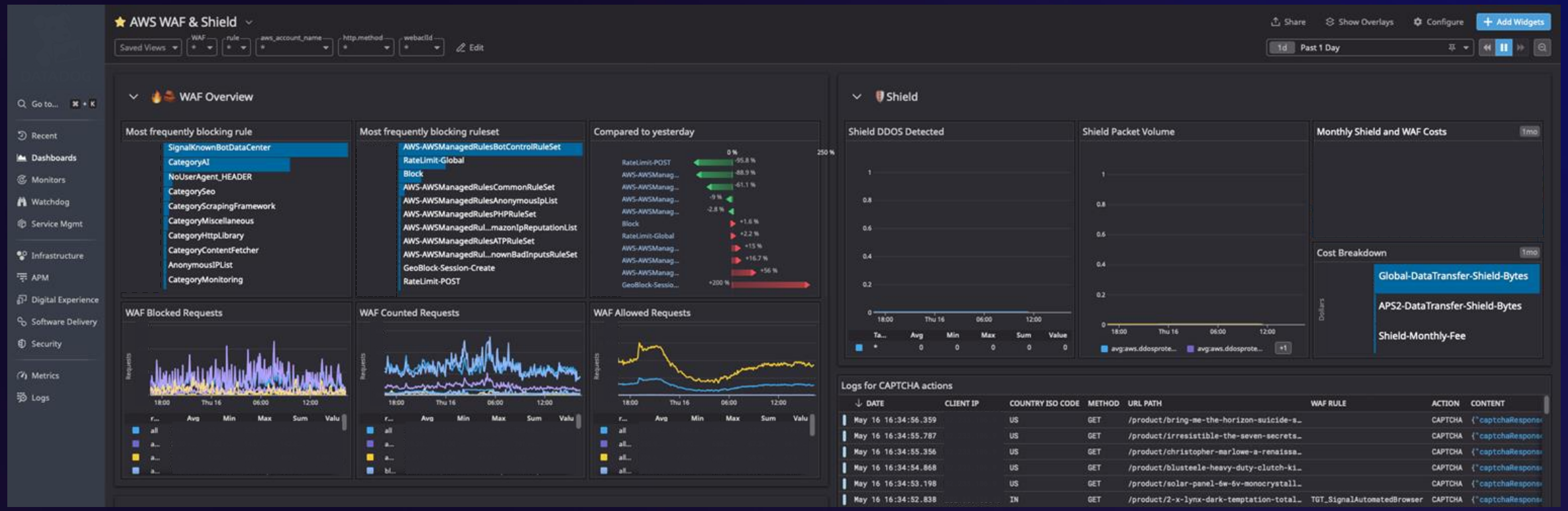
End-state architecture



How did we implement new rules?



Understanding traffic patterns



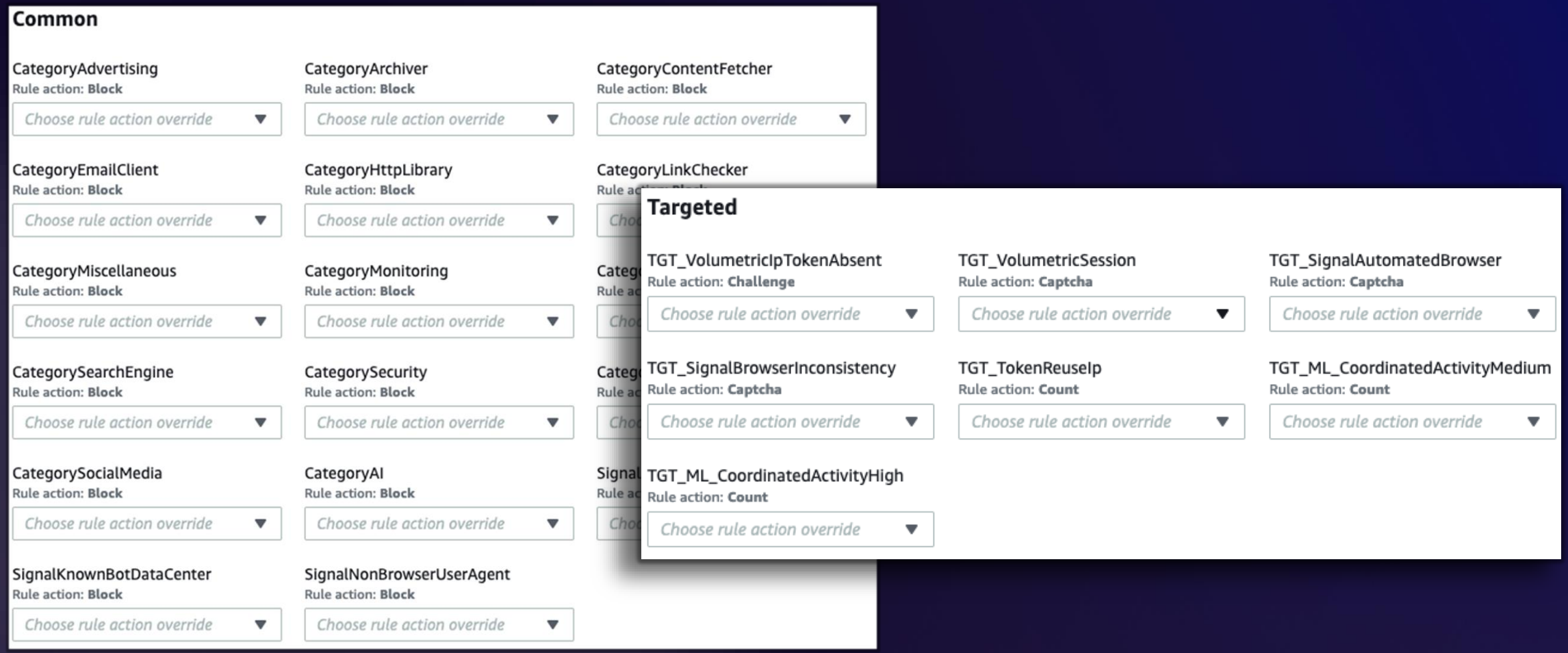
AWS WAF bot mitigation

AWS WAF offers two levels of bot to help manage how our application responds to bots

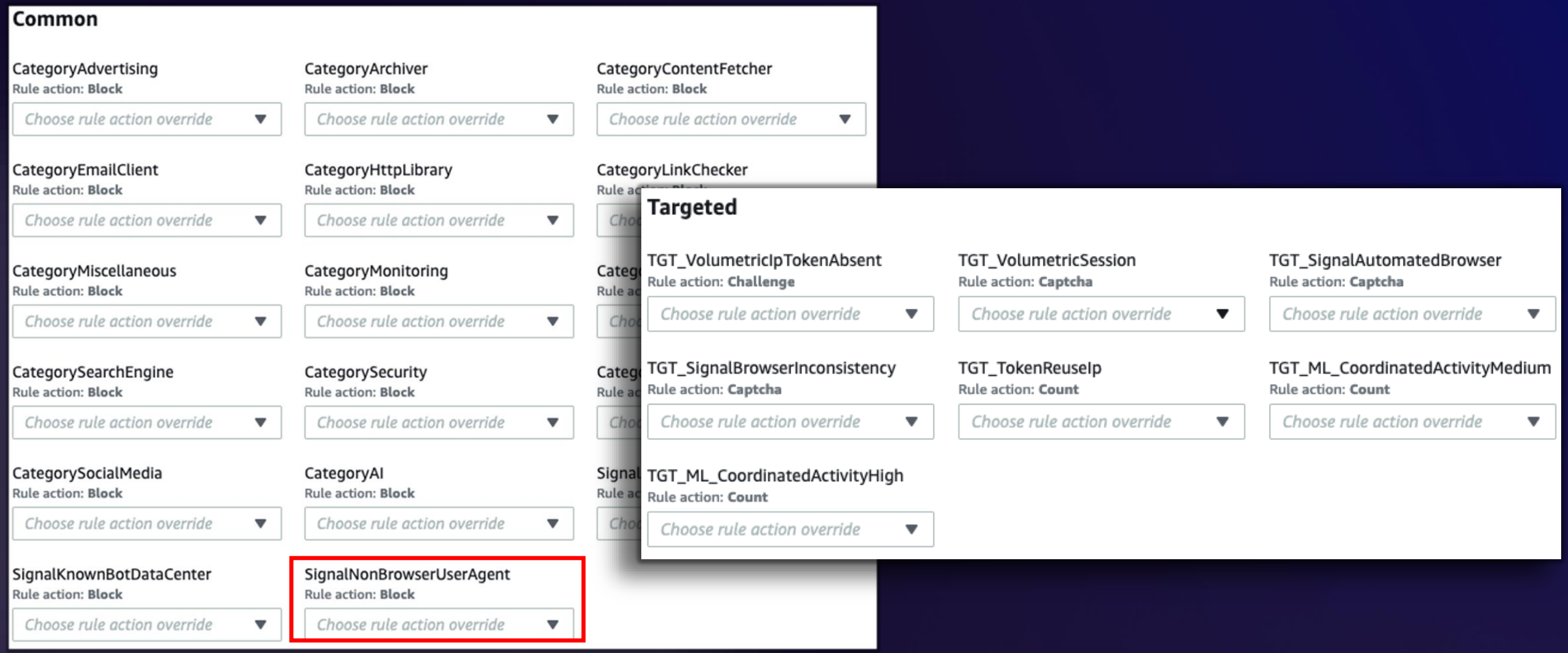
	Common bots	Targeted bots
Use cases	Detects self-identifying and simple bots. Allow listing of known good bots	Detects bots that try to evade detection by mimicking human behavior
Detection capabilities	Signature-based detection	Behavior-based and ML detection
Detection techniques	IP reputation lists, request headers, reverse DNS lookup, user agent validations	Browser fingerprinting and interrogation, dynamic rate-limiting, automation detection and fallback to CAPTCHA

AWS WAF launches Challenge rule action and Bot Control for Targeted Bots, Oct 2022

Managed bot protection



Managed bot protection



Lesson learned

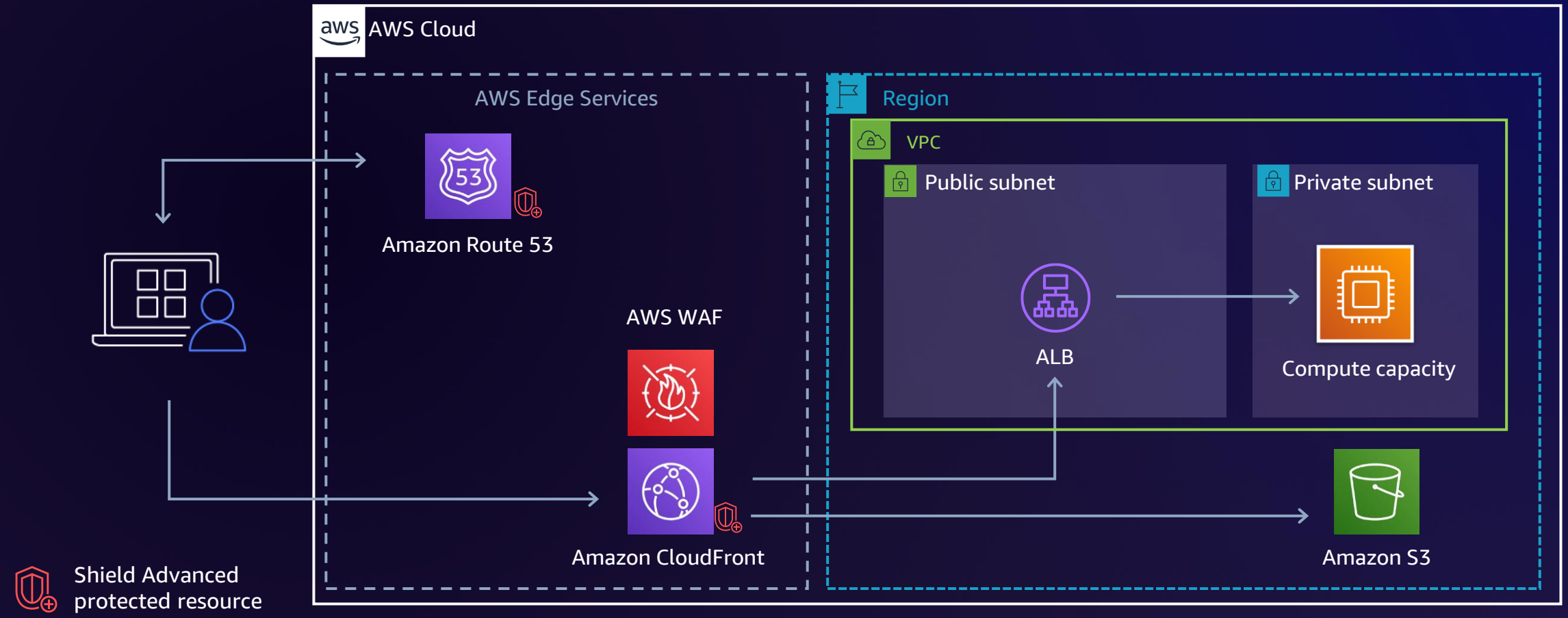
Use count actions when testing new rules

Address false positives by using scope down statements

Ensure you’re ingesting and analyzing the WAF logs

How you can protect your website today

Work toward well-architected applications



Build effective AWS WAF rules

Build effective AWS WAF rules

- Block lists
- IP reputation lists
- Shield auto mitigation

Build effective AWS WAF rules

- Block lists
- IP reputation lists
- Shield auto mitigation
- Baseline & use-case specific rule groups

Build effective AWS WAF rules

- Block lists
- IP reputation lists
- Shield auto mitigation
- Baseline & use-case specific rule groups
- Rate-based rules

Build effective AWS WAF rules

- Block lists
- IP reputation lists
- Shield auto mitigation
- Baseline & use-case specific rule groups
- Rate-based rules
- Bot and fraud control rules

Build effective AWS WAF rules

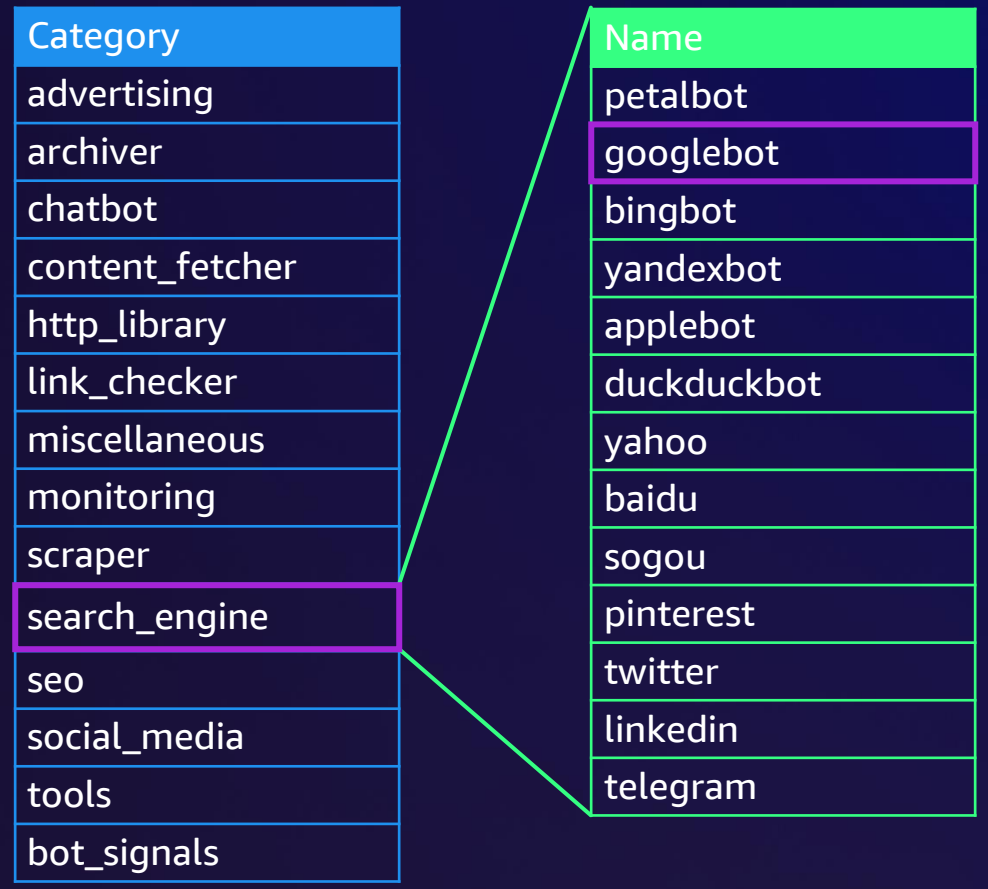
- Block lists
- IP reputation lists
- Shield auto mitigation
- Baseline & use-case specific rule groups
- Rate-based rules
- Bot and fraud control rules

Rich metadata added based on detections

Multiple labels are provided, based on categories and the specific bot detected:

For example:

```
awswaf:managed:aws:bot-control:bot:category:search_engine
awswaf:managed:aws:bot-control:bot:name:duckduckbot
awswaf:managed:aws:bot-control:bot:name:duckduckgo_favicons_bot
```



You can start detecting bots today

01 One-click AWS WAF deploy

02 Add bot control for targeted bots in count mode

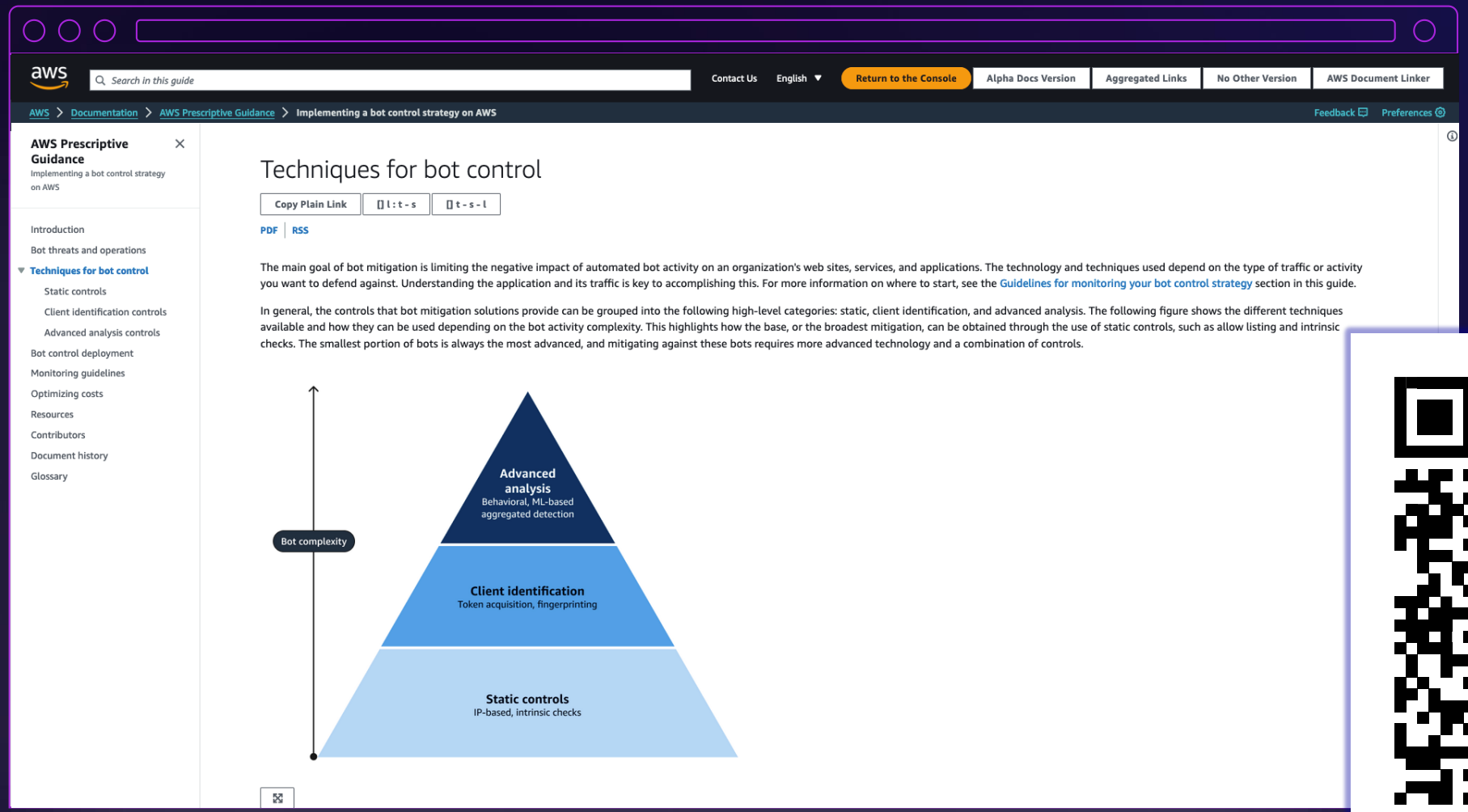
03 If protecting authentication pages, add account takeover protection ruleset

04 Use the AWS WAF dashboards to review risks detected

05 Change to blocking, challenge and CAPTCHA actions for categories of bots

06 Create scope down statements to limit inspection to specific URLs or dynamic content

AWS bot control prescriptive guidance



Additional resources

BOOKMARK THESE FOR LATER

Amazon CloudFront Pricing and Cost Optimization Guide

Cost-effective ways for securing your web applications using AWS WAF

CloudFront security savings bundle

AWS best practices for DDoS resiliency