

AWS re:Inforce

JUNE 10 - 12, 2024 | PHILADELPHIA, PA

N I S 3 0 6

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



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

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

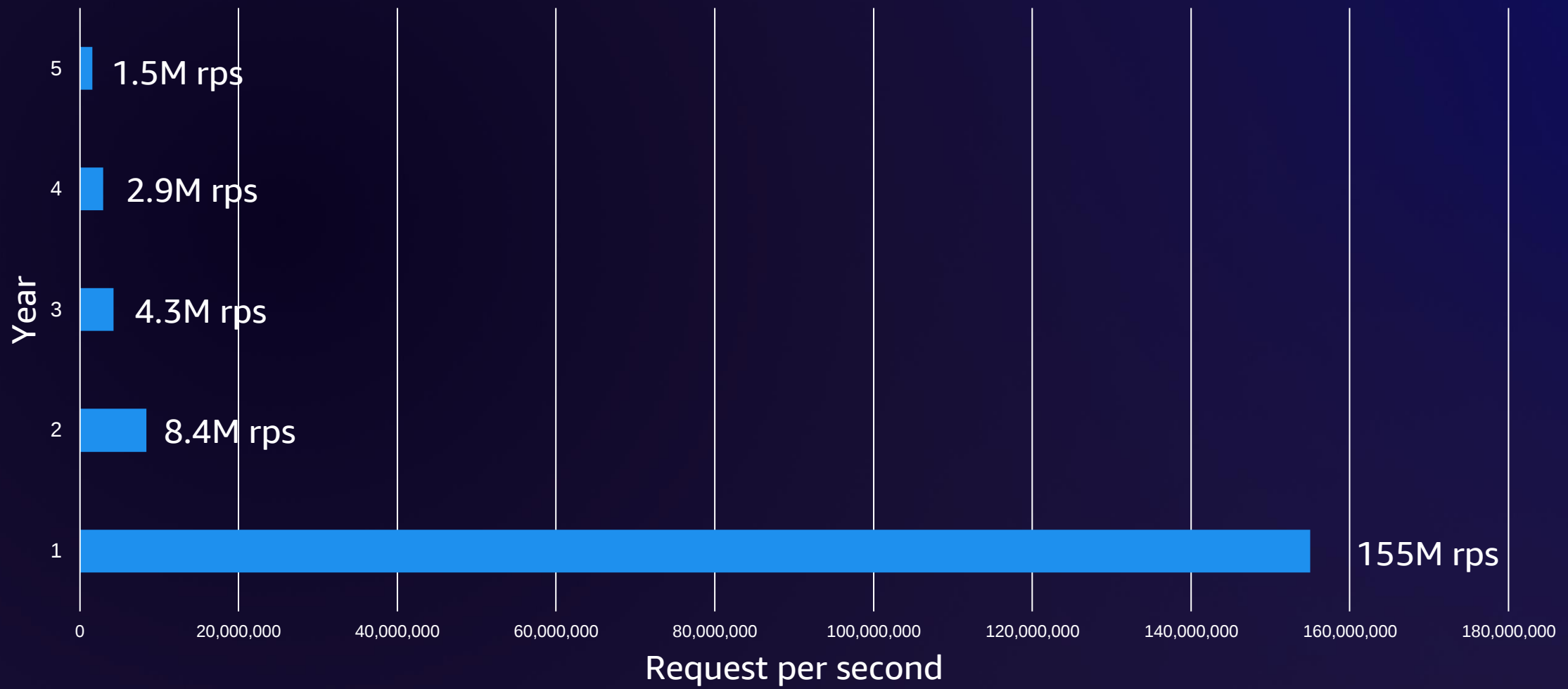


221M PPS

Largest packet
attack

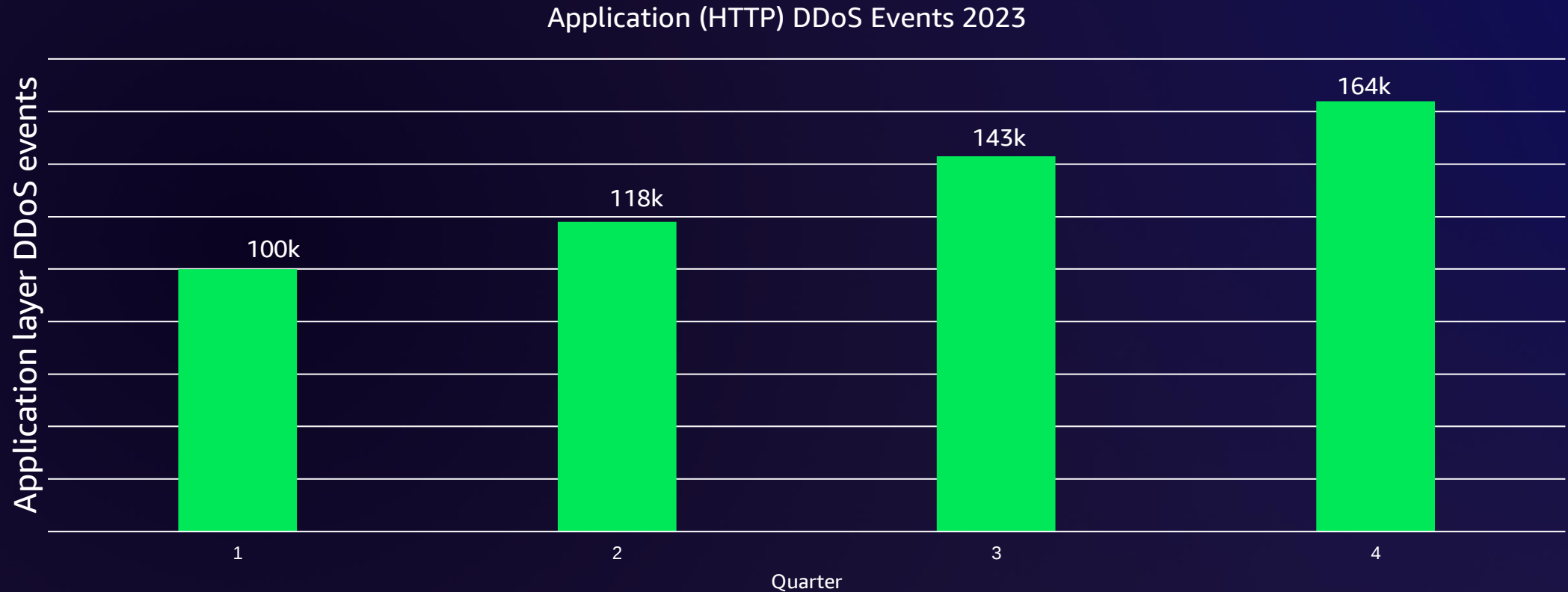
Largest request flood events by year, as seen by AWS

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

Bot attack vectors

THREAT LANDSCAPE



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

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



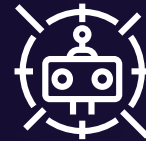
Content scraping



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



Catch Mobile

CareersGift CardsHelpTrack My Order

Search for new balance

AccountOnePassFree deliveryFlybuys\$2 = 1 point

Shop All CategoriesOnePassToday's DealsClearanceCatch FestWinterBulk BuysAnkoRefurbished StoreCatch ConnectAppleTarget

CATCH FEST

UP TO 50% off

SALE NOW LIVE

Selected Products

Shop Now

*Selected Products only. Ends 11:59PM AEST 19 May 2024. While stocks last.

Deal of the Day24 HOURS ONLY

Black Lord Walking Pad

Offer applies to products sold by Aussie Union Group* only
*Offer ends 16/05/2024 11:59AM AEST.

Don't Pay \$219.85
\$149
\$70.85 off RRP



From \$7

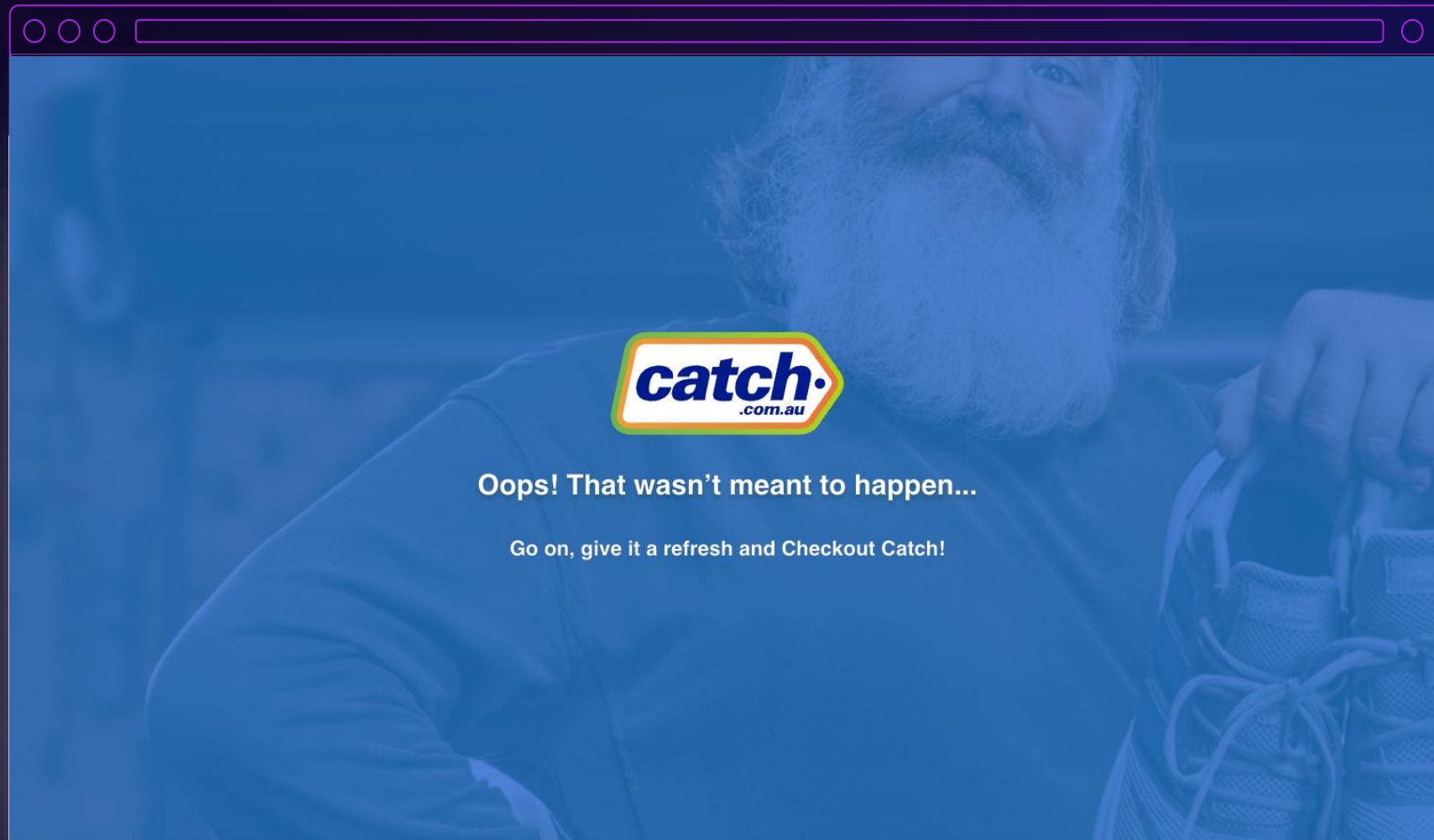


\$59 & Under



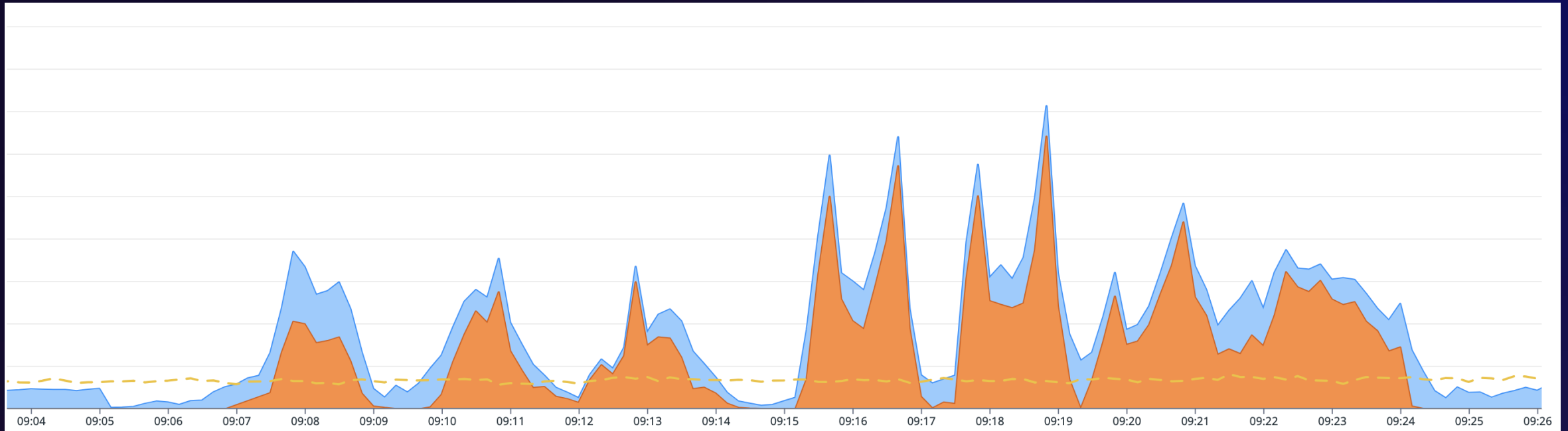
Offer limited to products sold by Catch in this event. Excludes third party marketplace seller products. Offer ends 19/05/2024 AEST 11:59pm. While stocks last.

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



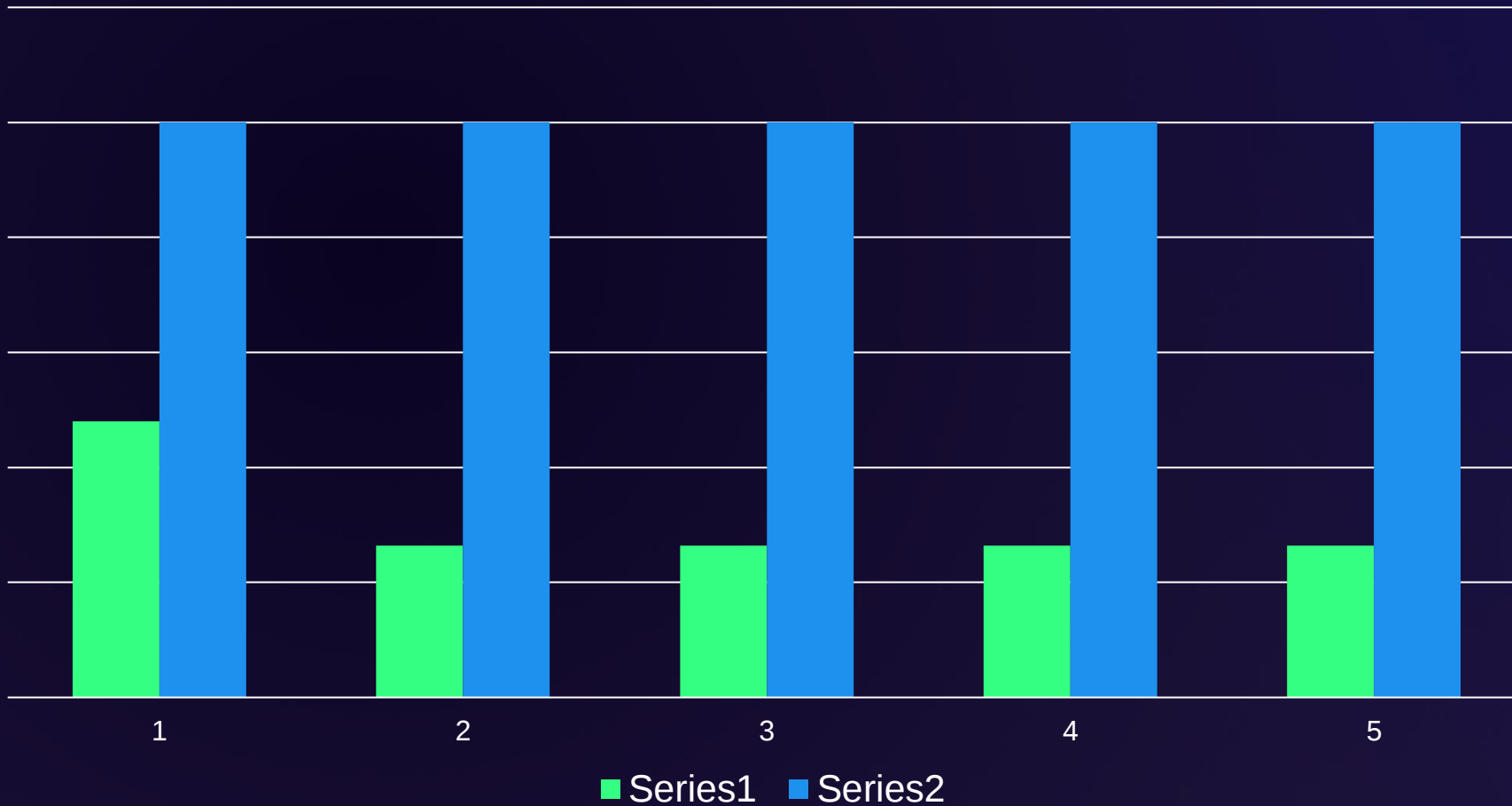
Proof of concept



Operating model

It's not just about request costs

Total cost of ownership



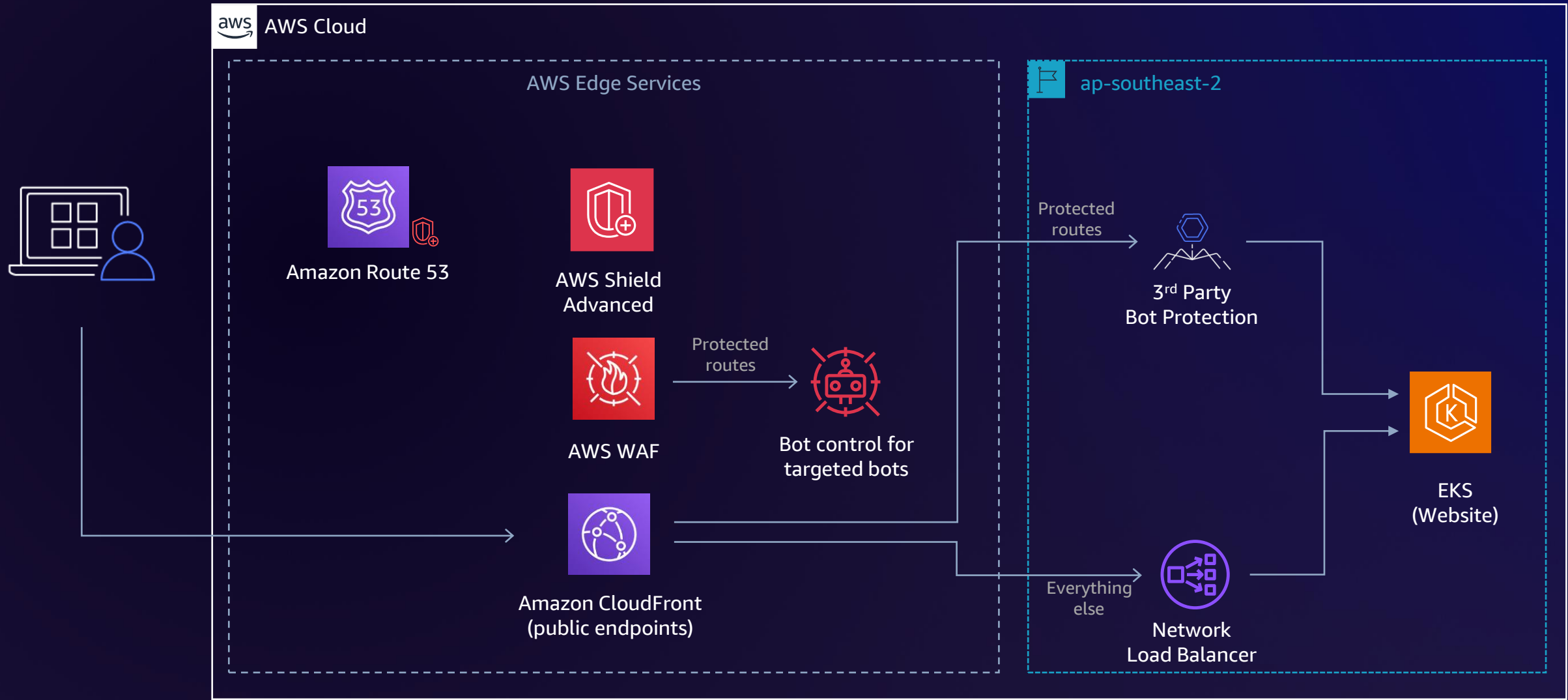
2x

Savings in Year 1

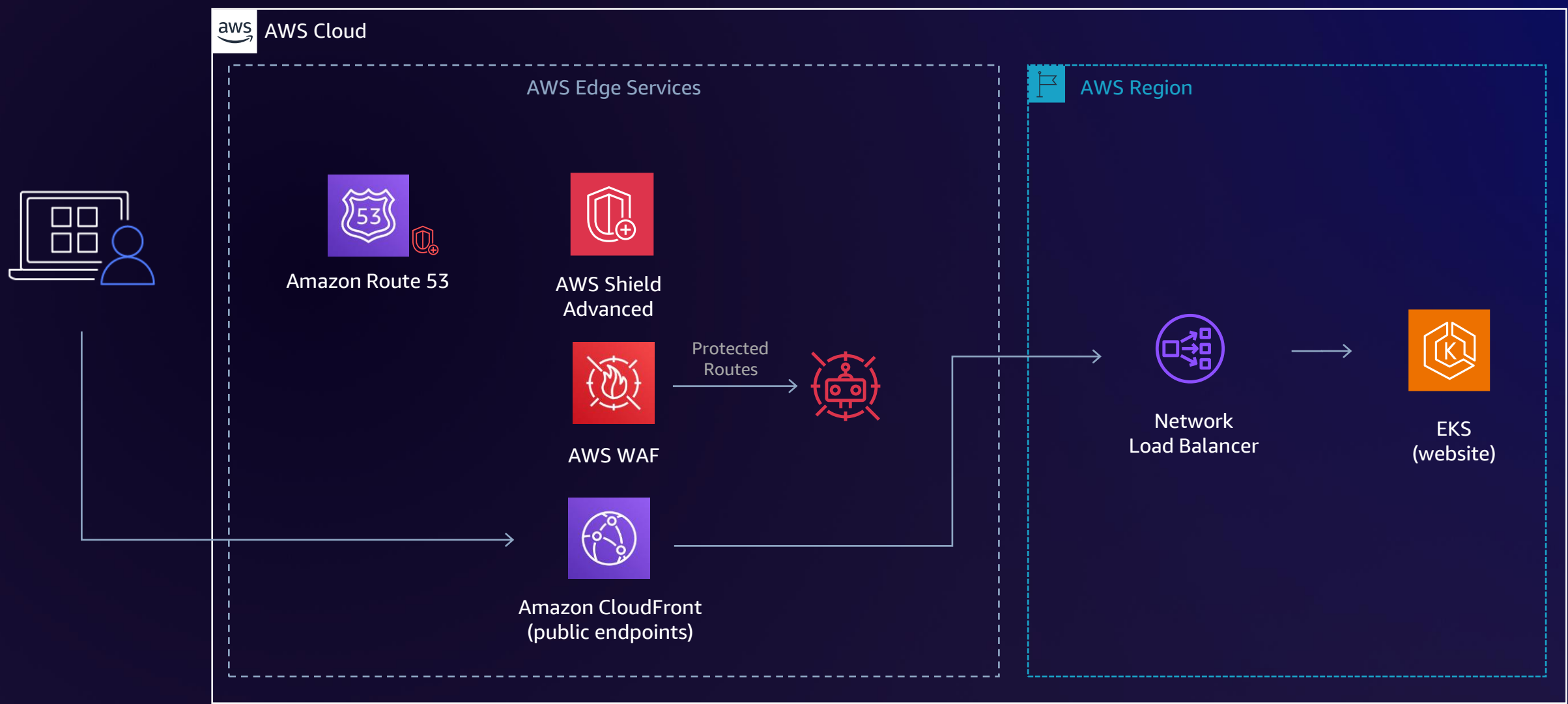
4x

Savings each year thereafter

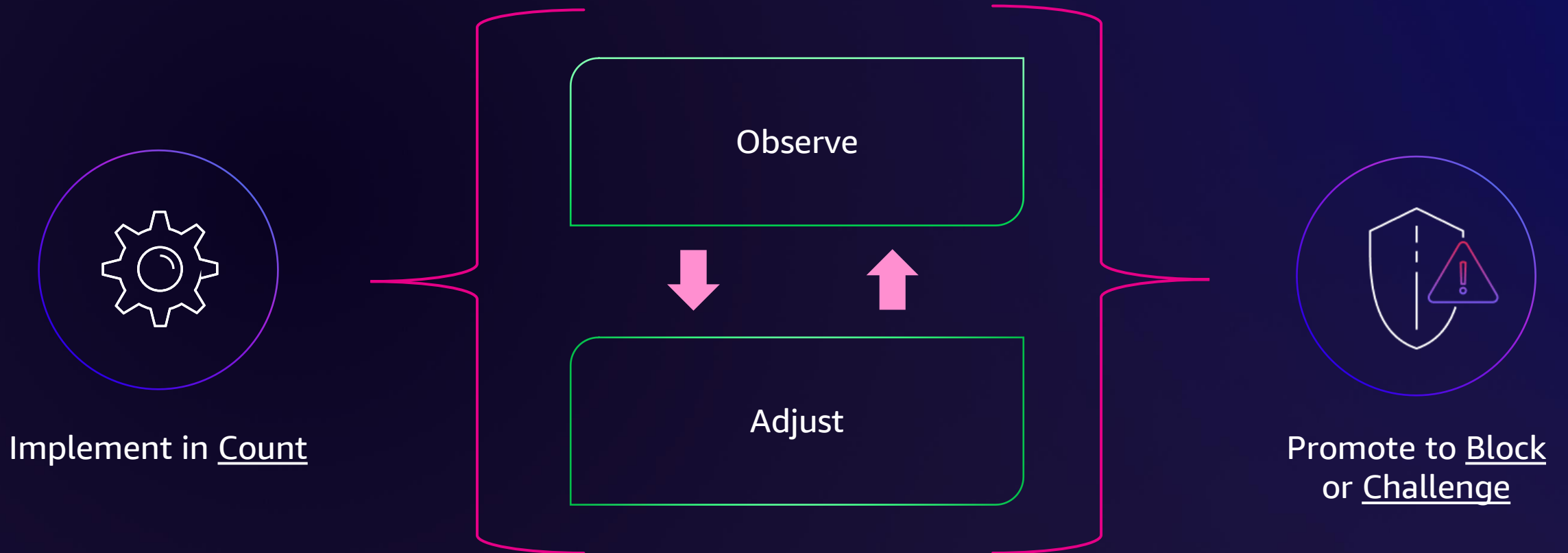
Migration state



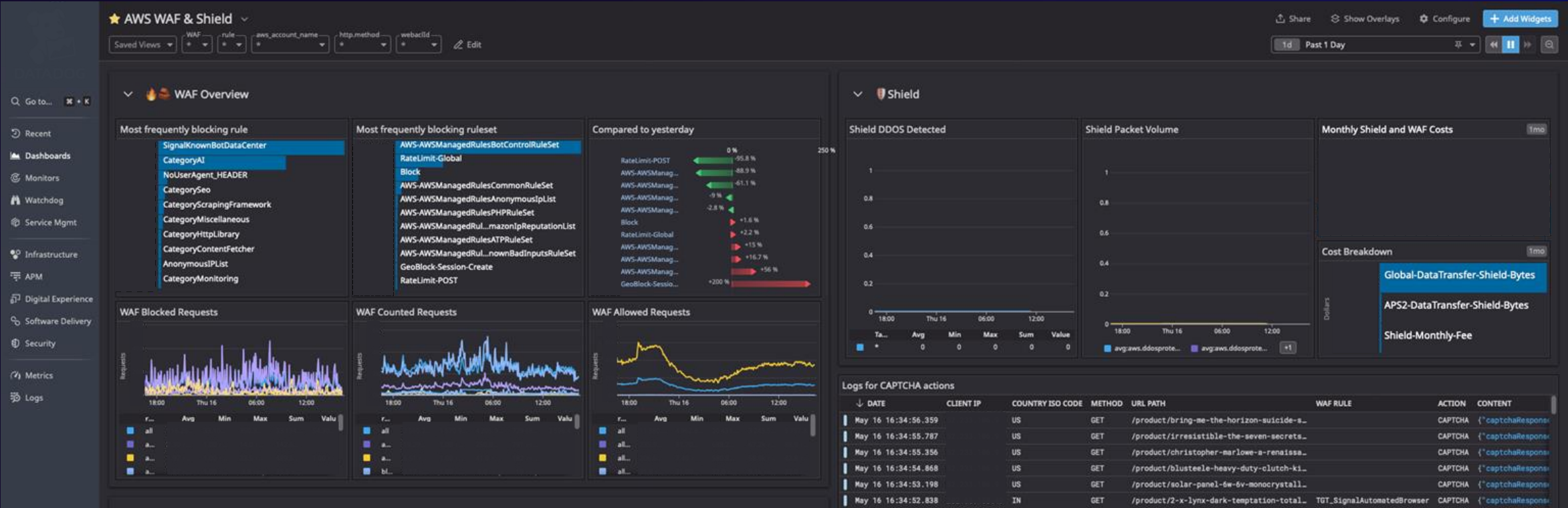
End-state architecture



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

Managed bot protection

Common

CategoryAdvertising Rule action: Block Choose rule action override ▼	CategoryArchiver Rule action: Block Choose rule action override ▼	CategoryContentFetcher Rule action: Block Choose rule action override ▼
CategoryEmailClient Rule action: Block Choose rule action override ▼	CategoryHttpLibrary Rule action: Block Choose rule action override ▼	CategoryLinkChecker Rule action: Block Choose rule action override ▼
CategoryMiscellaneous Rule action: Block Choose rule action override ▼	CategoryMonitoring Rule action: Block Choose rule action override ▼	CategorySearchEngine Rule action: Block Choose rule action override ▼
CategorySecurity Rule action: Block Choose rule action override ▼	CategorySocialMedia Rule action: Block Choose rule action override ▼	CategoryAI Rule action: Block Choose rule action override ▼
SignalKnownBotDataCenter Rule action: Block Choose rule action override ▼	SignalNonBrowserUserAgent Rule action: Block Choose rule action override ▼	

Targeted

TGT_VolumetricIpTokenAbsent Rule action: Challenge Choose rule action override ▼	TGT_VolumetricSession Rule action: Captcha Choose rule action override ▼	TGT_SignalAutomatedBrowser Rule action: Captcha Choose rule action override ▼
TGT_SignalBrowserInconsistency Rule action: Captcha Choose rule action override ▼	TGT_TokenReuselp Rule action: Count Choose rule action override ▼	TGT_ML_CoordinatedActivityMedium Rule action: Count Choose rule action override ▼
TGT_ML_CoordinatedActivityHigh Rule action: Count Choose rule action override ▼		



Managed bot protection

Common

CategoryAdvertising

Rule action: Block

Choose rule action override ▼

CategoryArchiver

Rule action: Block

Choose rule action override ▼

CategoryContentFetcher

Rule action: Block

Choose rule action override ▼

CategoryEmailClient

Rule action: Block

Choose rule action override ▼

CategoryHttpLibrary

Rule action: Block

Choose rule action override ▼

CategoryLinkChecker

Rule action: Block

Choose rule action override ▼

CategoryMiscellaneous

Rule action: Block

Choose rule action override ▼

CategoryMonitoring

Rule action: Block

Choose rule action override ▼

CategorySearchEngine

Rule action: Block

Choose rule action override ▼

CategorySecurity

Rule action: Block

Choose rule action override ▼

CategorySocialMedia

Rule action: Block

Choose rule action override ▼

CategoryAI

Rule action: Block

Choose rule action override ▼

SignalKnownBotDataCenter

Rule action: Block

Choose rule action override ▼

SignalNonBrowserUserAgent

Rule action: Block

Choose rule action override ▼

Targeted

TGT_VolumetricIpTokenAbsent

Rule action: Challenge

Choose rule action override ▼

TGT_VolumetricSession

Rule action: Captcha

Choose rule action override ▼

TGT_SignalAutomatedBrowser

Rule action: Captcha

Choose rule action override ▼

TGT_SignalBrowserInconsistency

Rule action: Captcha

Choose rule action override ▼

TGT_TokenReuselp

Rule action: Count

Choose rule action override ▼

TGT_ML_CoordinatedActivityMedium

Rule action: Count

Choose rule action override ▼

TGT_ML_CoordinatedActivityHigh

Rule action: Count

Choose rule action override ▼

Lesson learned



Use count actions when testing new rules



Address false positives by using scope down statements

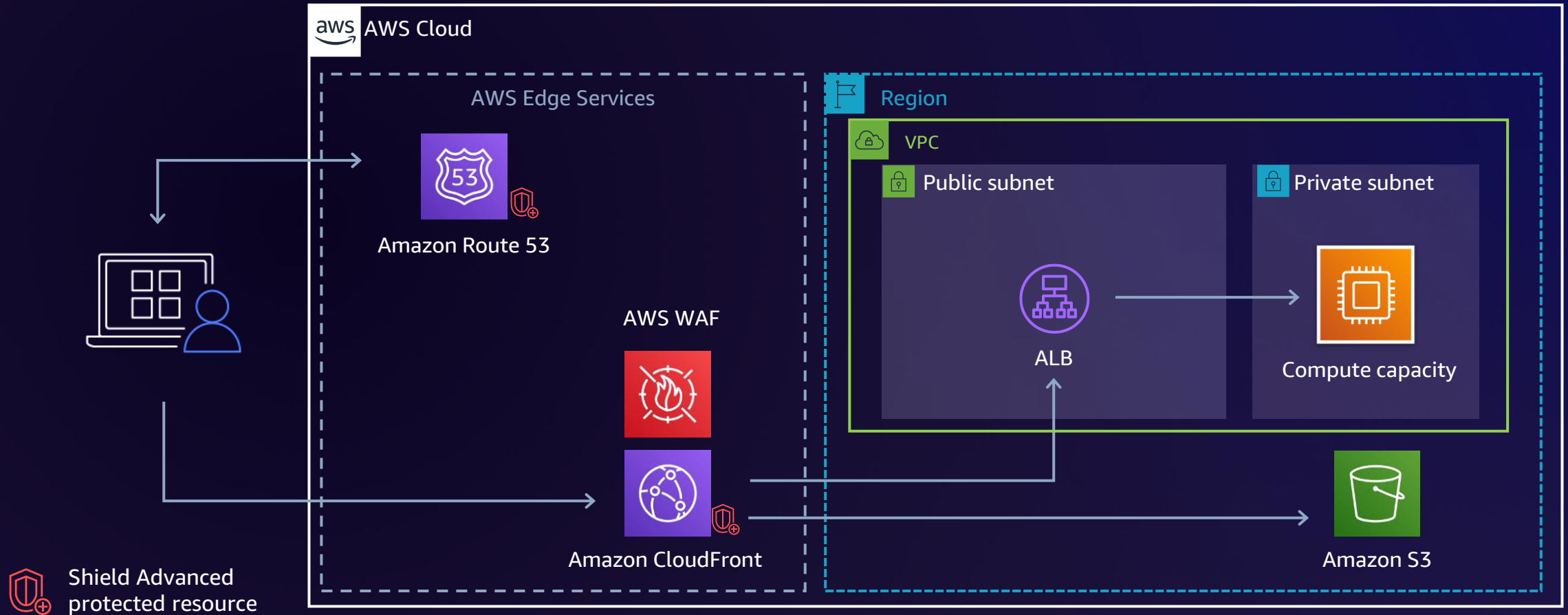


Ensure you're ingesting and analyzing the WAF logs

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:

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

Category
advertising
archiver
chatbot
content_fetcher
http_library
link_checker
miscellaneous
monitoring
scraper
search_engine
seo
social_media
tools
bot_signals

Name
petalbot
googlebot
bingbot
yandexbot
applebot
duckduckbot
yahoo
baidu
sogou
pinterest
twitter
linkedin
telegram



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

AWS Prescriptive Guidance

Implementing a bot control strategy on AWS

Introduction

Bot threats and operations

Techniques for bot control

Static controls

Client identification controls

Advanced analysis controls

Bot control deployment

Monitoring guidelines

Optimizing costs

Resources

Contributors

Document history

Glossary

Search this guide

Contact UsEnglishReturn to the ConsoleAlpha Docs VersionAggregated LinksNo Other VersionAWS Document Linker

AWS > Documentation > AWS Prescriptive Guidance > Implementing a bot control strategy on AWSFeedbackPreferences

Techniques for bot control

Copy Plain Linkt - s t - s - l

PDFRSS

The main goal of bot mitigation is limiting the negative impact of automated bot activity on an organization's web sites, services, and applications. The technology and techniques used depend on the type of traffic or activity you want to defend against. Understanding the application and its traffic is key to accomplishing this. For more information on where to start, see the Guidelines for monitoring your bot control strategy section in this guide.

In general, the controls that bot mitigation solutions provide can be grouped into the following high-level categories: static, client identification, and advanced analysis. The following figure shows the different techniques available and how they can be used depending on the bot activity complexity. This highlights how the base, or the broadest mitigation, can be obtained through the use of static controls, such as allow listing and intrinsic checks. The smallest portion of bots is always the most advanced, and mitigating against these bots requires more advanced technology and a combination of controls.

Bot complexity

Advanced analysis
Behavioral, ML-based aggregated detection

Client identification
Token acquisition, fingerprinting

Static controls
IP-based, intrinsic checks



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