

The background of the image features a dark blue gradient on the left, transitioning into a large, vibrant, abstract shape on the right. This shape is composed of overlapping curved segments in shades of orange, pink, and purple, creating a dynamic, modern aesthetic.

AWS re:Invent

NOV. 27 – DEC. 1, 2023 | LAS VEGAS, NV

NET 322

Evolve your web application delivery with Amazon CloudFront

Tino Tran

World Wide Tech Leader,
Edge Services
AWS

Kevin Gaynor

Distinguished Engineer
Capital One

Harish Kathpalia

Distinguished Engineer
Capital One



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



15 years of innovation with Amazon CloudFront

2008	2010	2012	2013	2015	2016	2017	2020	2021	2022	2023
Amazon CloudFront launched	Adds HTTPS support	Dynamic content support	Geo restriction Support for POST/PUT and other HTTP Methods	AWS WAF integration	HTTP/2 support Regional edge caches	Lambda@Edge 100 edge locations	200 edge locations Origin Shield	CloudFront Functions	400 edge locations HTTP3 powered by QUIC Continuous deployment	One-click AWS WAF integration 600+ edge locations KeyValueStore

Amazon CloudFront Global Edge Network

GLOBAL NETWORK

Redundant 400 GbE network and private capacity between all regions except for the AWS China*

EDGE NETWORKING

600+ PoPs in 50 countries and 100+ cities, with direct peering to all major ISPs

KEY

- Edge location
- Multiple edge locations
- Regional Edge caches

Our customers



GLOBAL
BUSINESS
TRAVEL



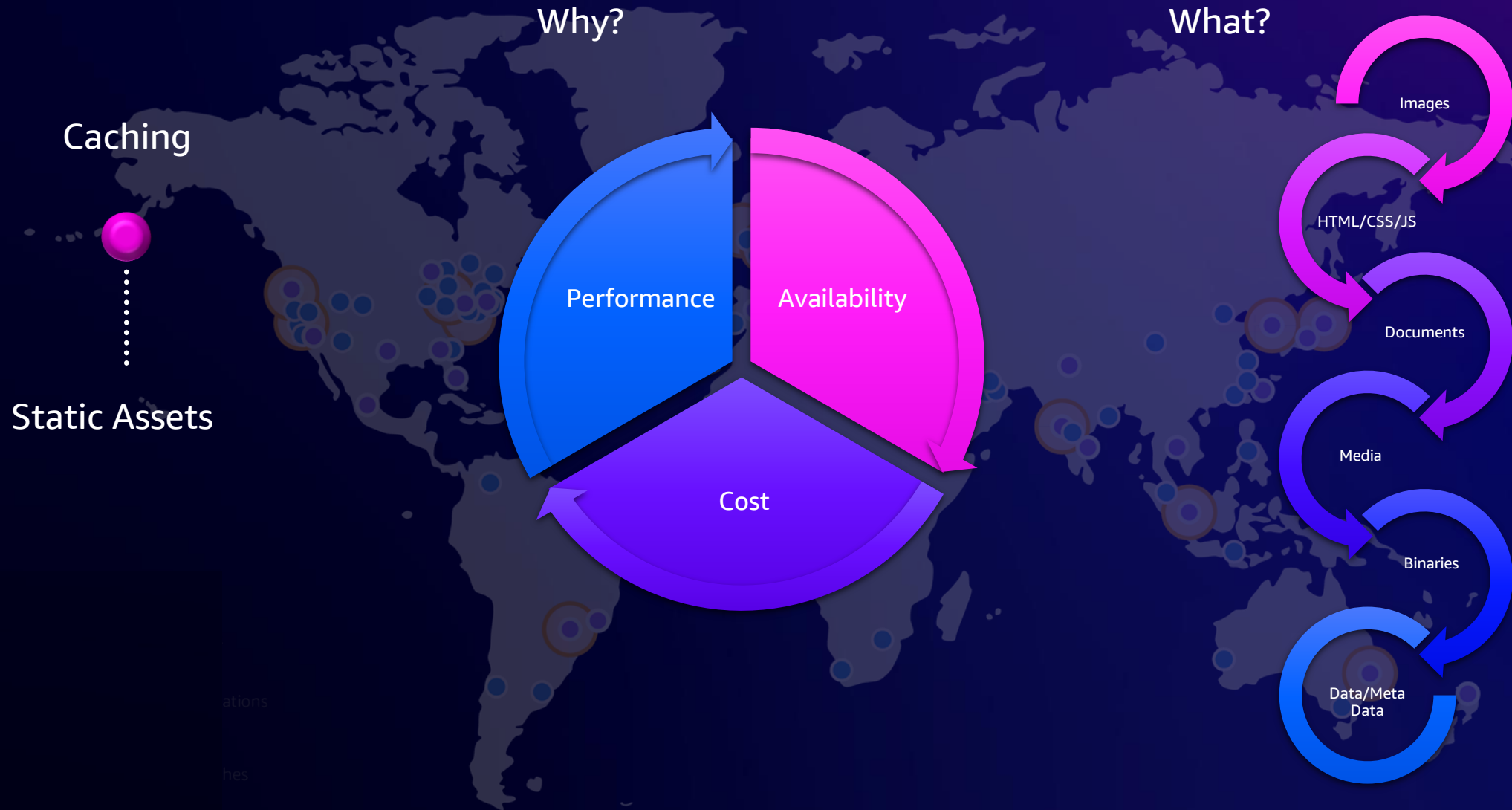
TRUECar.



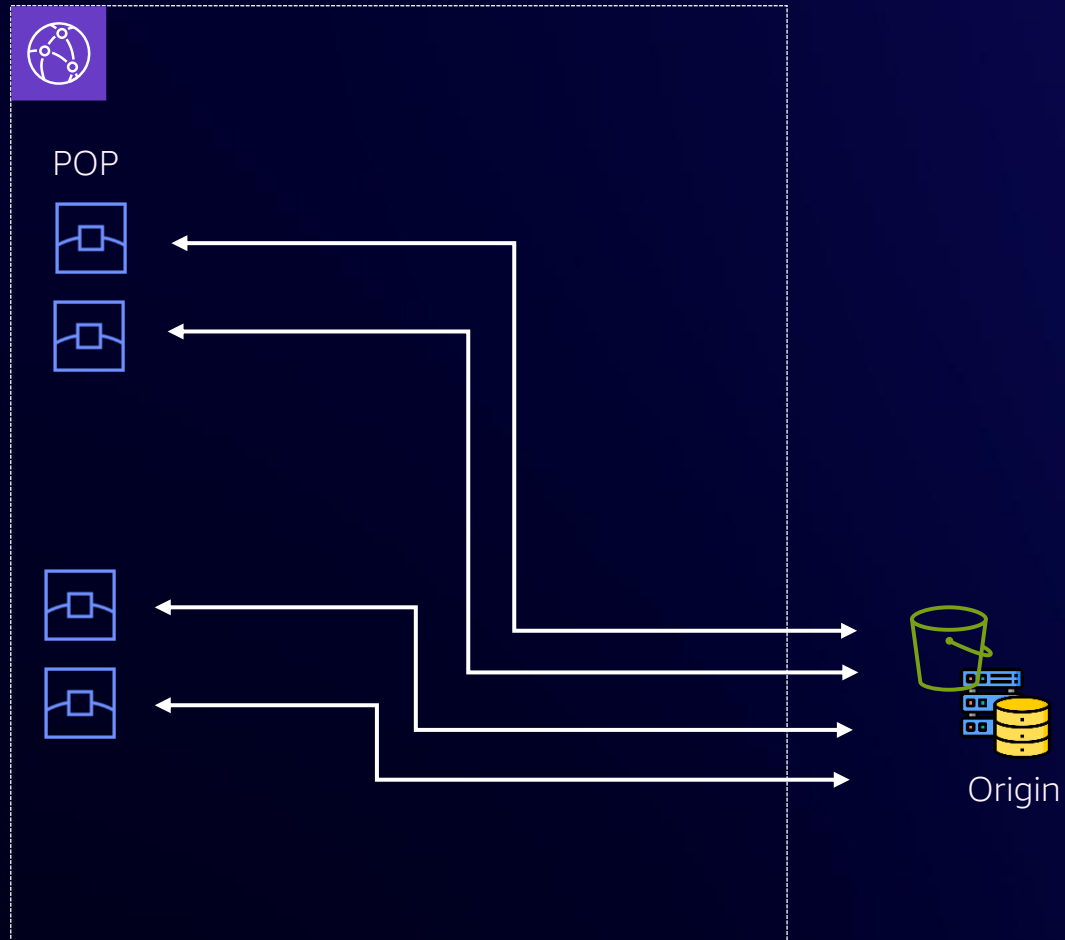
upsoft




15 years of evolving requirements



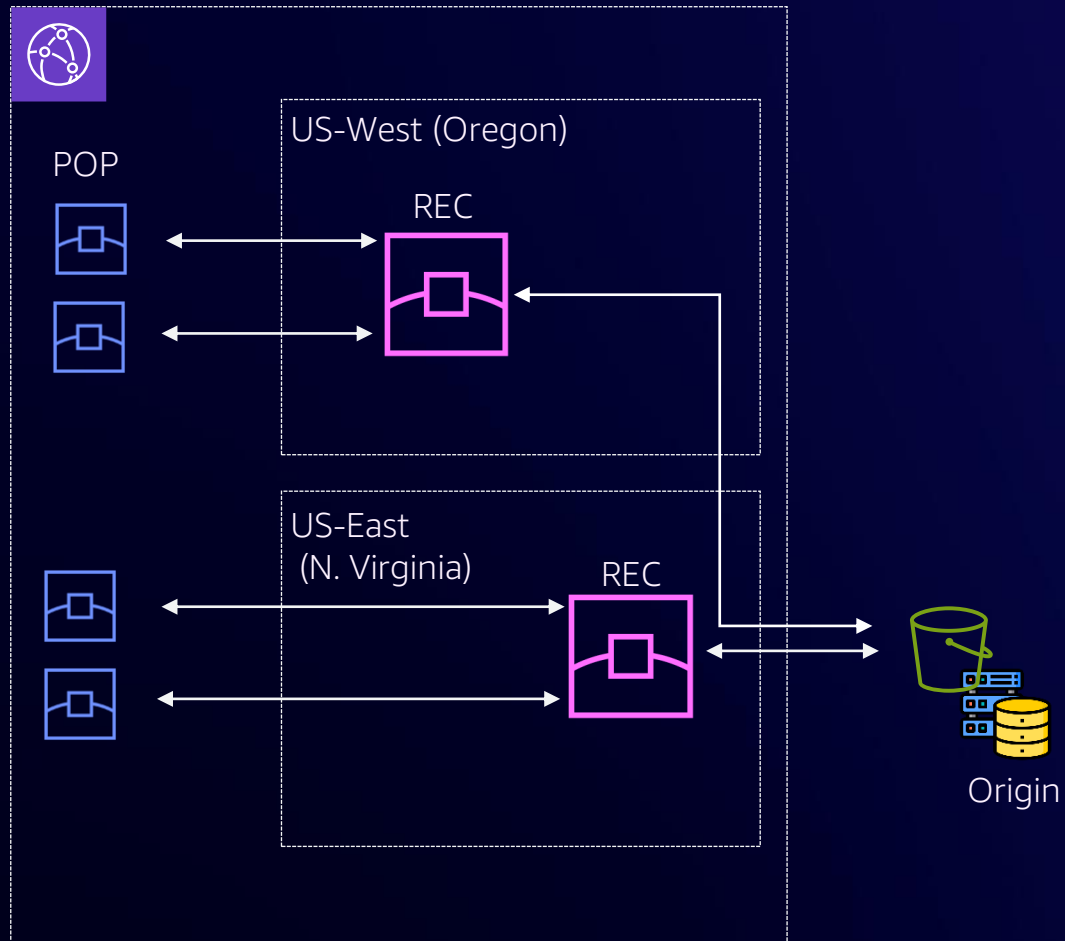
Caching strategy



 Point of Presence (POP)

 Regional Edge Cache (REC)

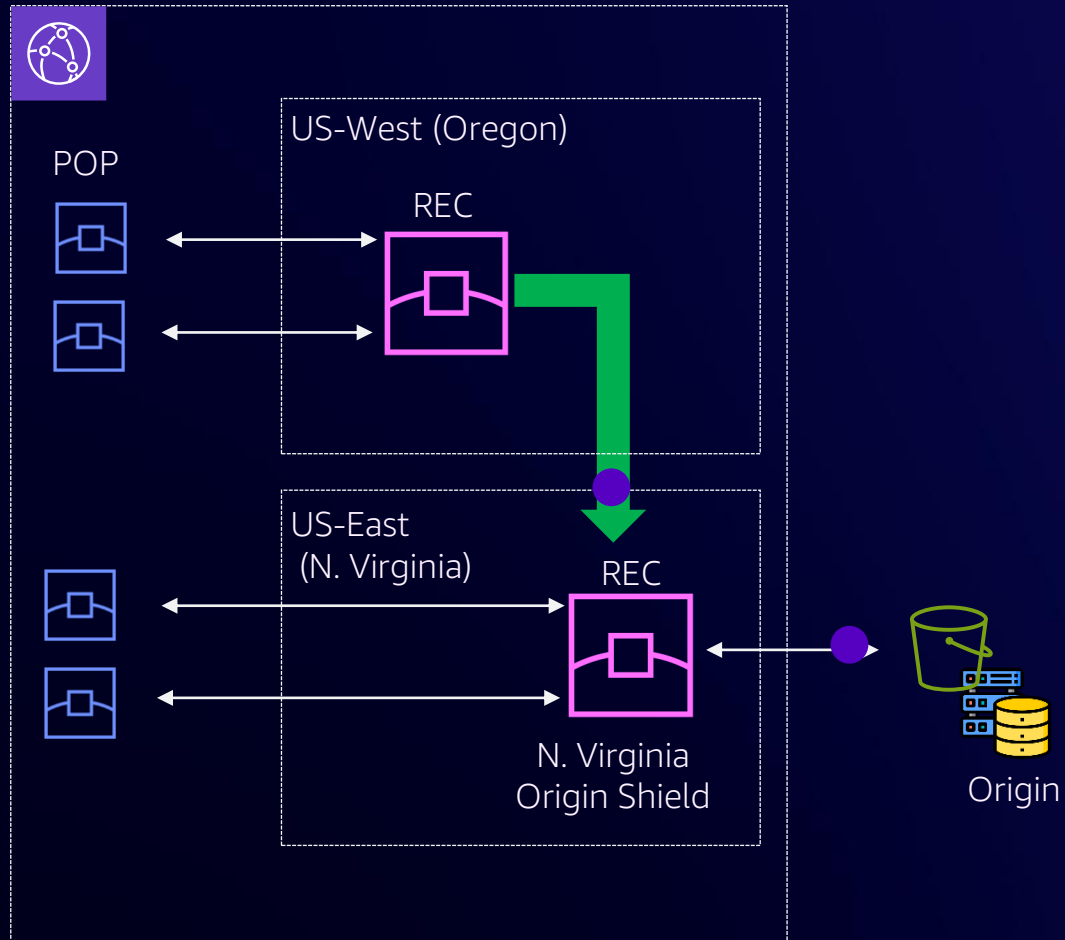
Caching strategy



 Point of Presence (POP)

 Regional Edge Cache (REC)

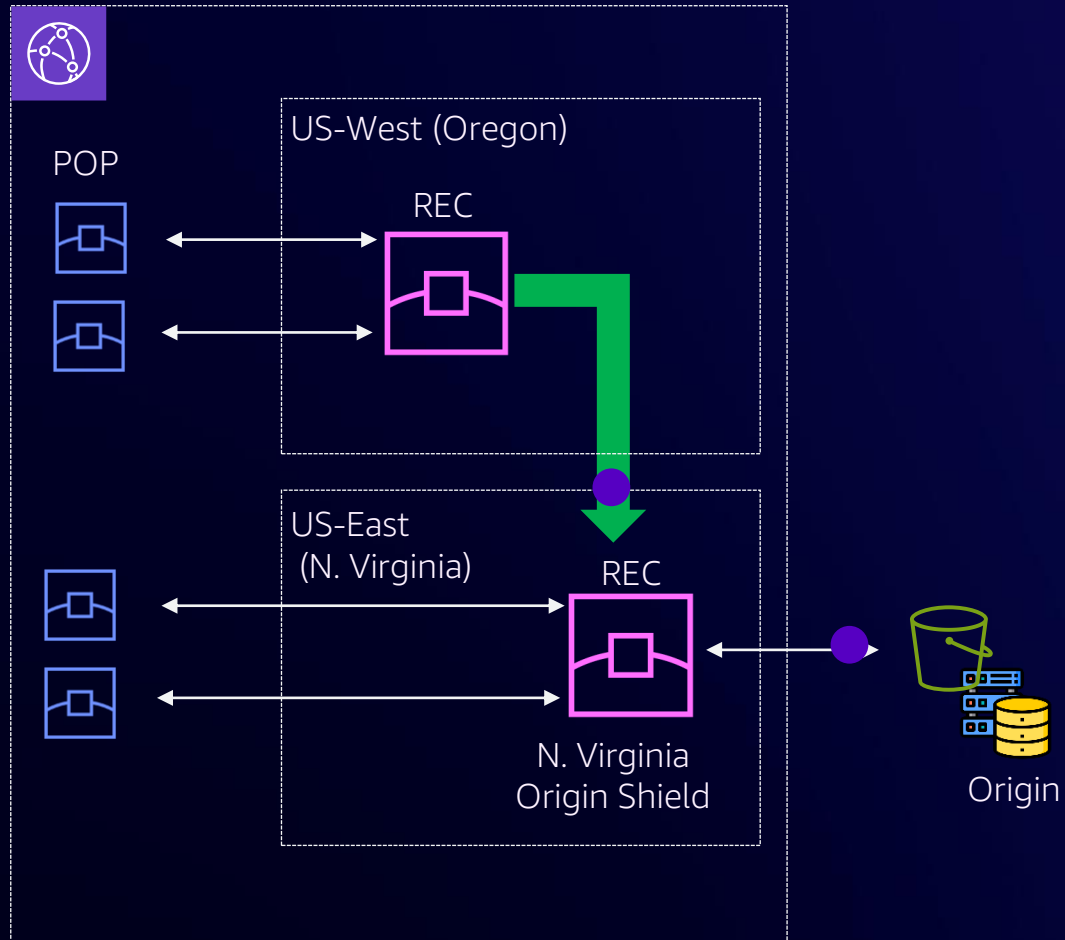
Caching strategy



 Point of Presence (POP)

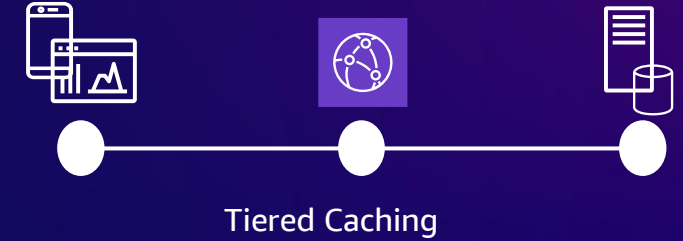
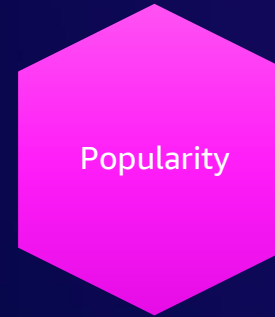
 Regional Edge Cache (REC)

Caching strategy

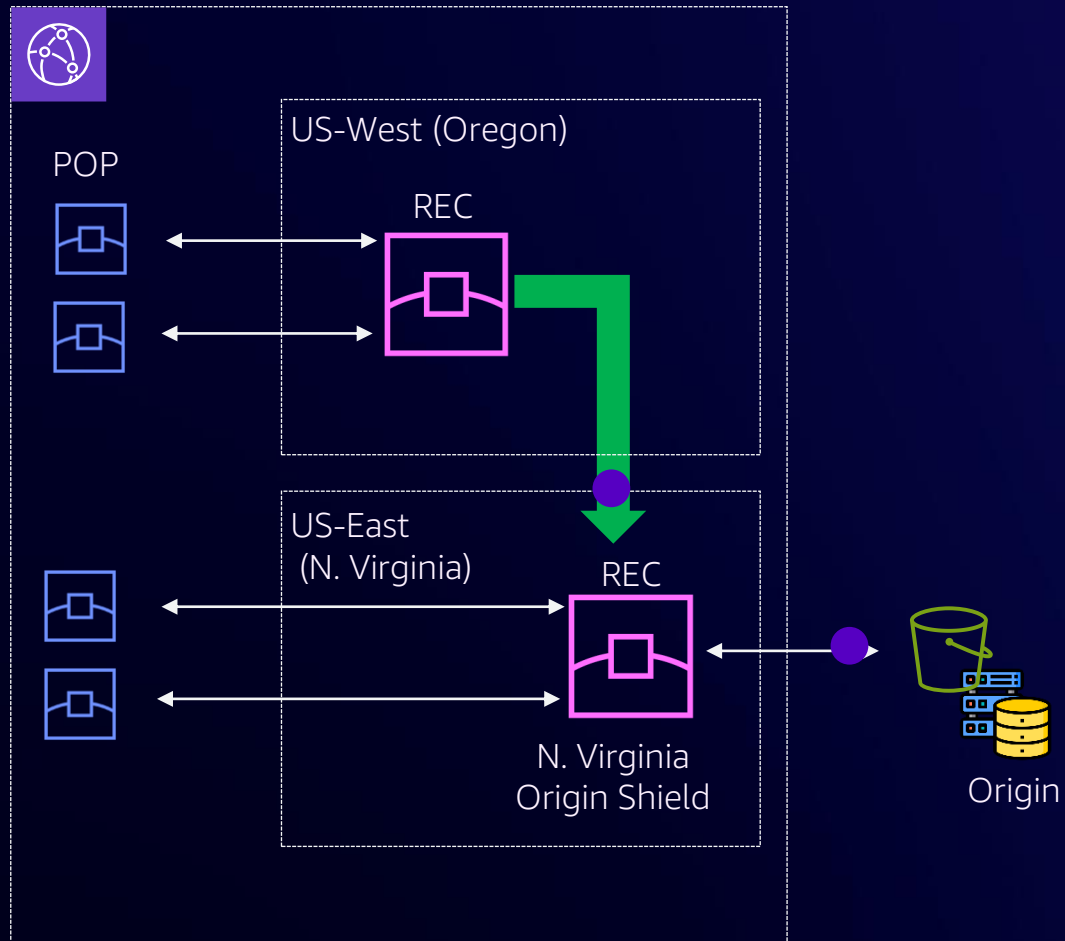


 Point of Presence (POP)

 Regional Edge Cache (REC)

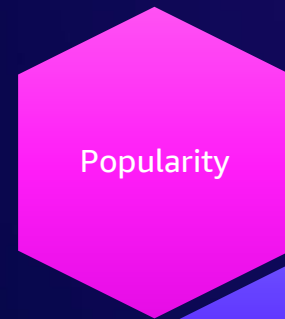


Caching strategy



 Point of Presence (POP)

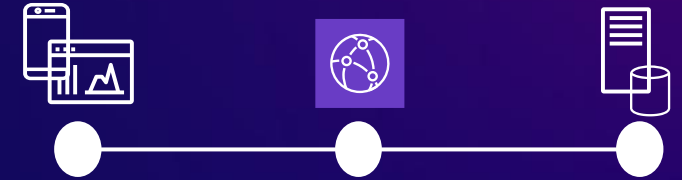
 Regional Edge Cache (REC)



Popularity



Mutability

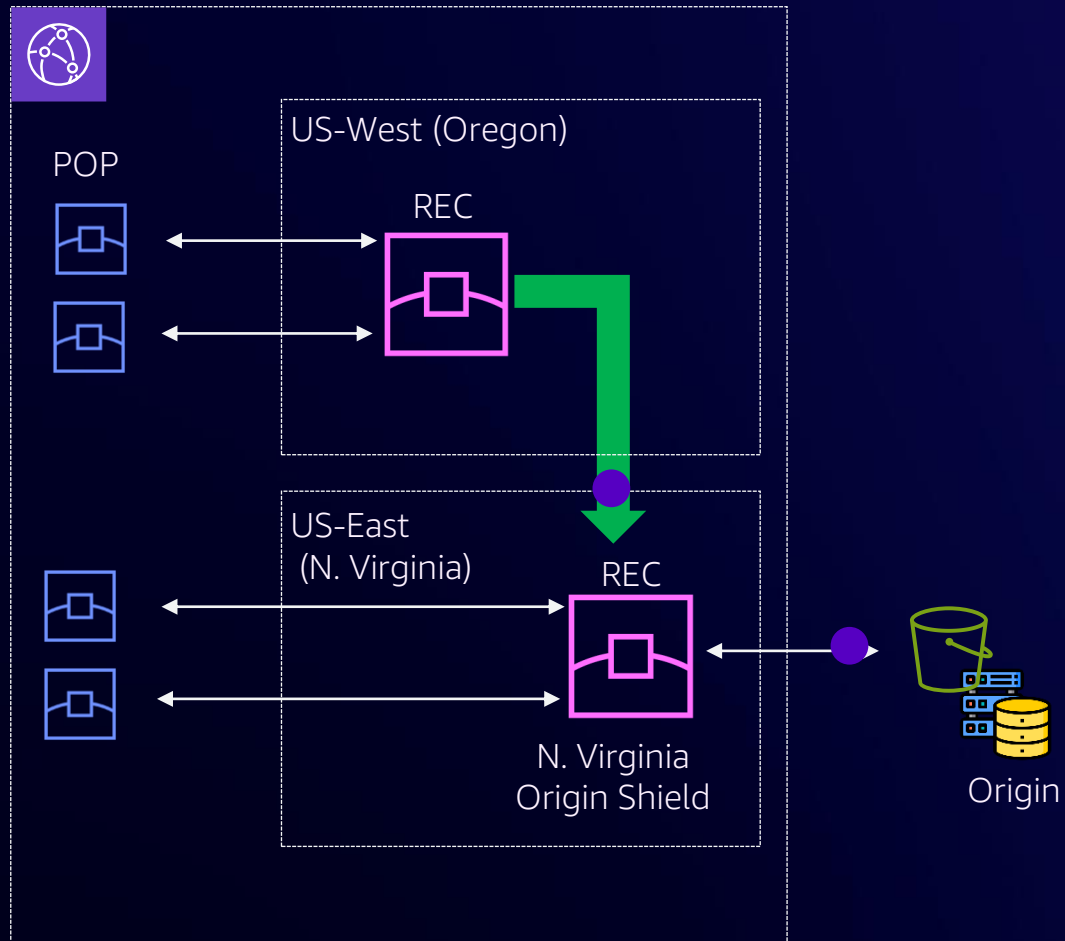




Tiered Caching

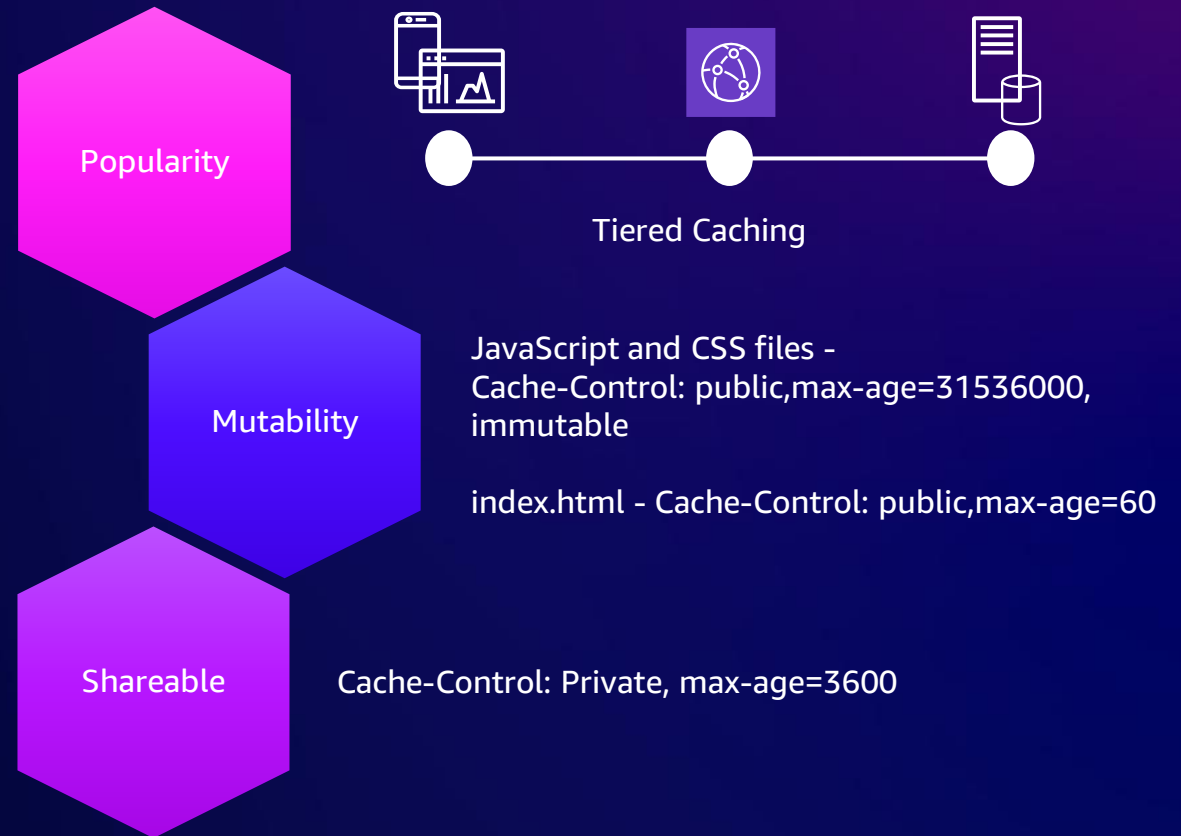
JavaScript and CSS files -
Cache-Control: public,max-age=31536000,
immutable

index.html - Cache-Control: public,max-age=60

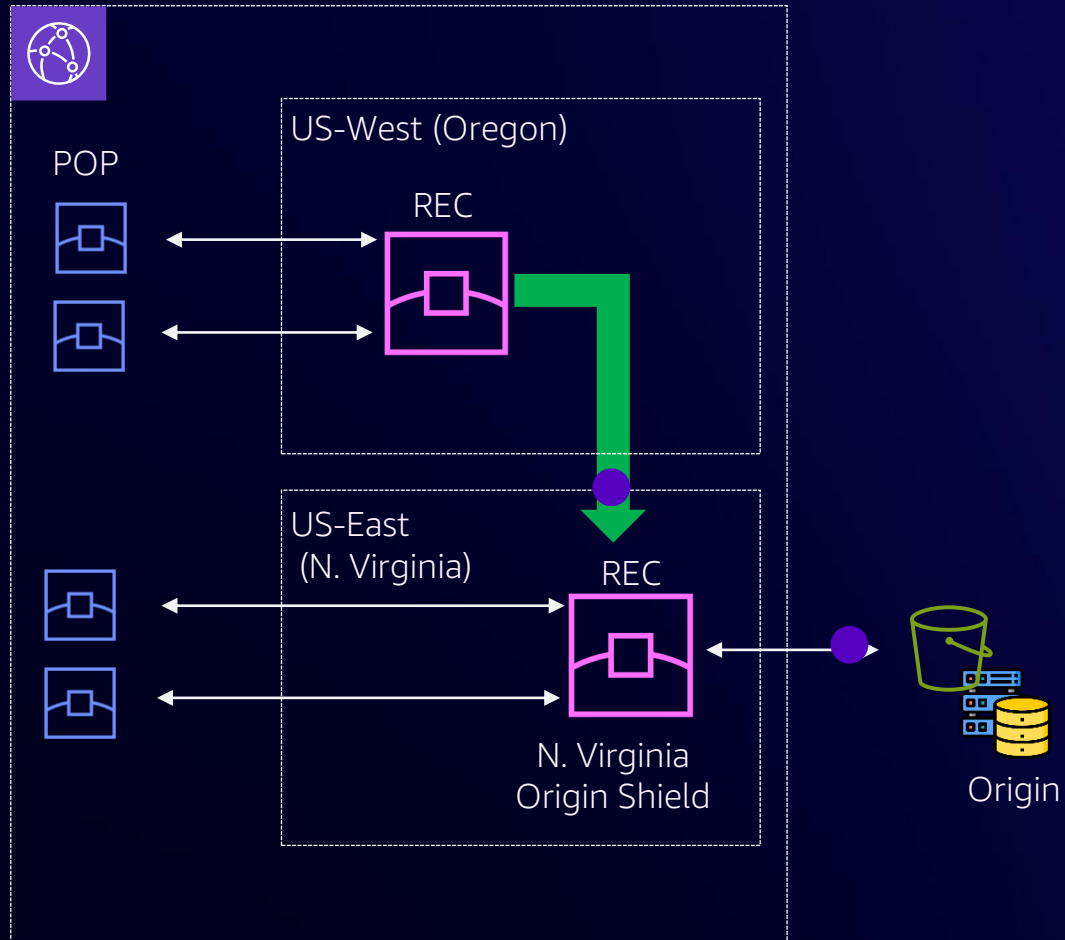
Caching strategy





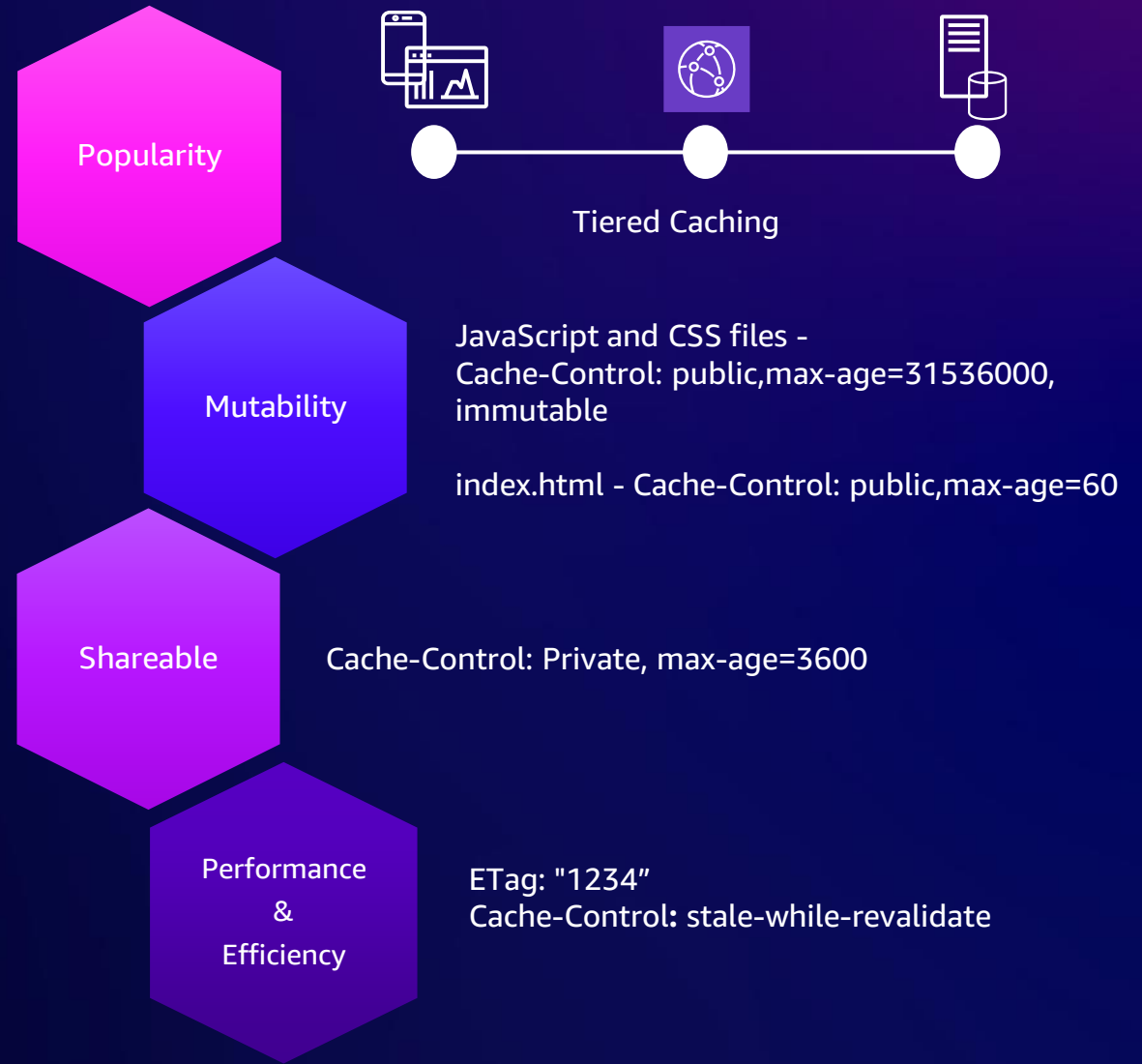
-  Point of Presence (POP)
-  Regional Edge Cache (REC)



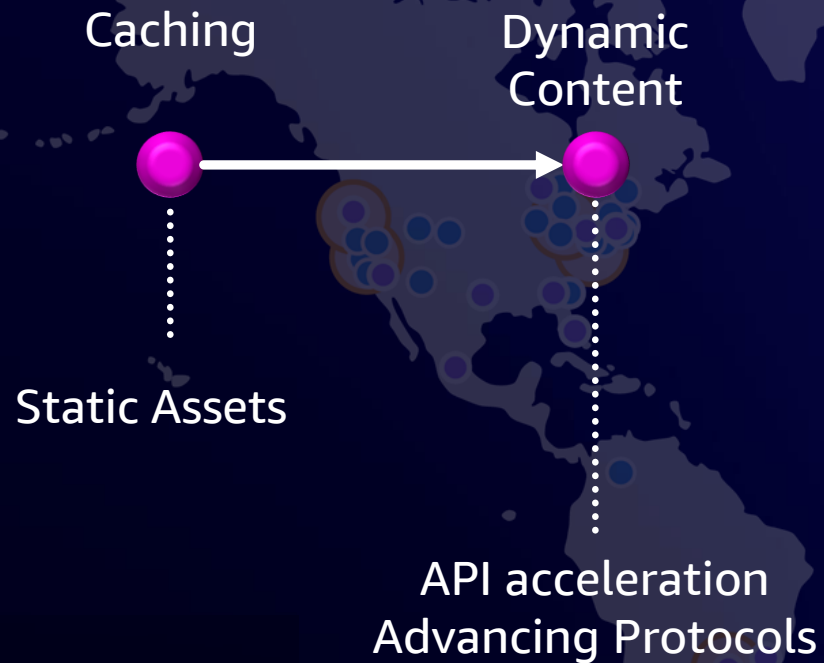
Caching strategy



-  Point of Presence (POP)
-  Regional Edge Cache (REC)



15 years of evolving requirements

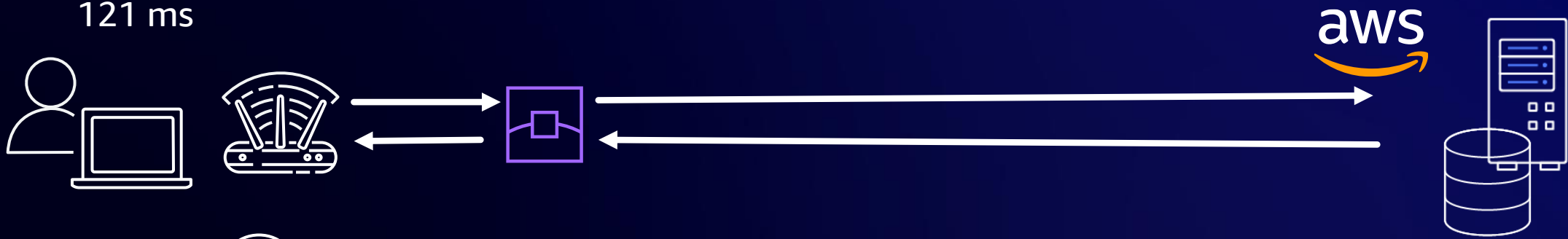


Dynamic Content Acceleration

20KB Object
393 ms



20KB Object
121 ms



Dynamic Content Acceleration

20KB Object
393 ms



20KB Object
121 ms

Optimized
TLS Termination

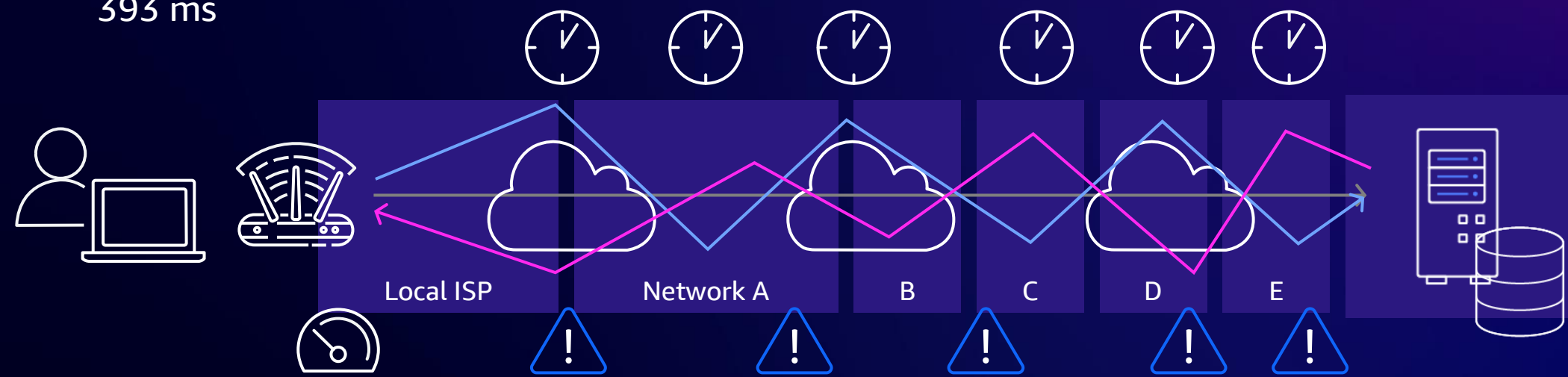
Persistent Connection Reuse

aws

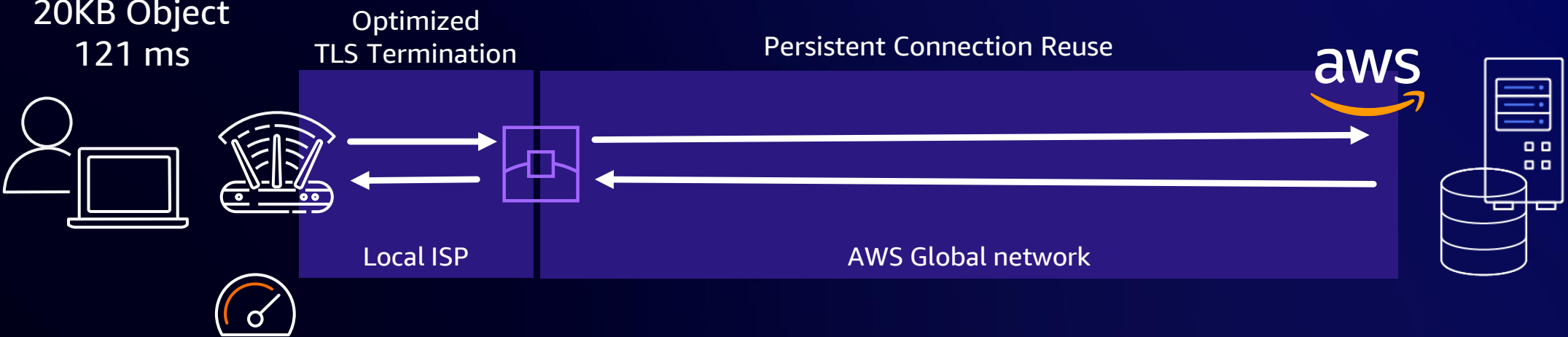


Dynamic Content Acceleration

20KB Object
393 ms



20KB Object
121 ms



Protocol Progression

HTTP 1.0/1.1/2.0
TCP + TLS 1.1/1.2

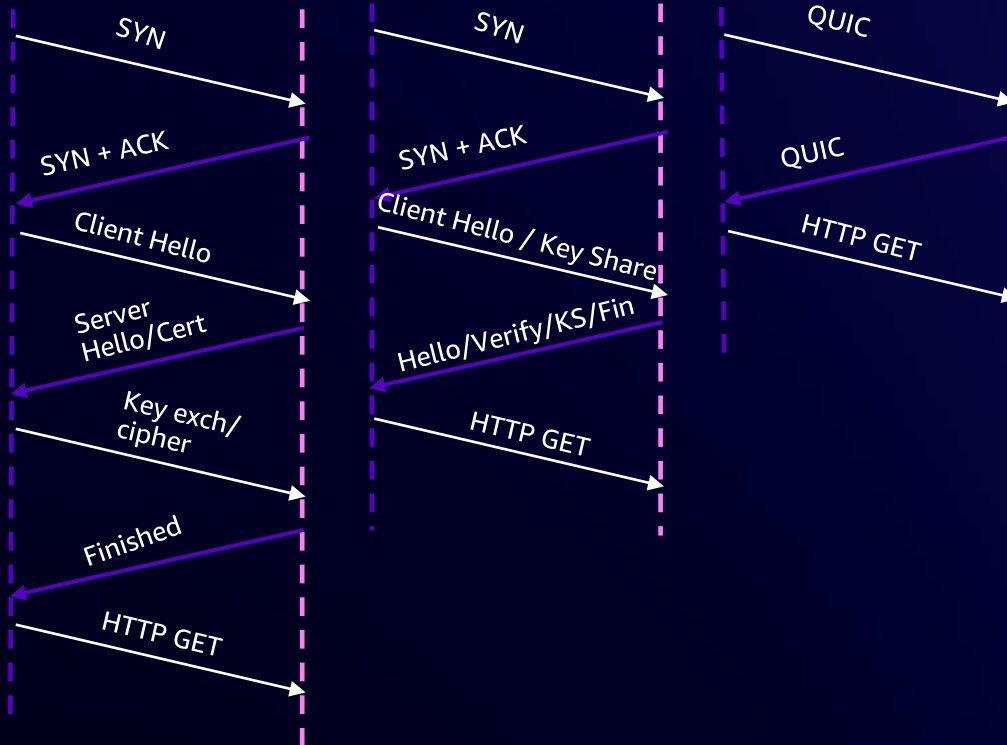
3RTT

HTTP 1.0/1.1/2.0
TCP+TLS1.3

2RTT

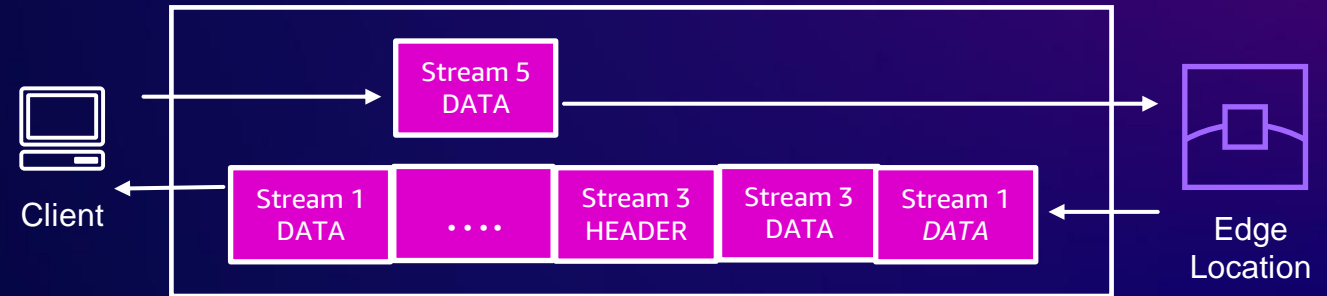
HTTP/3
QUIC + TLS1.3

1RTT



*Additional optimizations (not pictured)
TCP Fast Open
TLS Session Resumption

HTTP 2.0 Connection



WebSocket Protocol

GET /chat HTTP/1.1
Host: server.example.com
Upgrade: websocket Connection:
Upgrade Sec-WebSocket-Key: bsZSBub25jZQ==
Origin: https://example.com
Sec-WebSocket-Protocol: chat, superchat
Sec-WebSocket-Version: 13

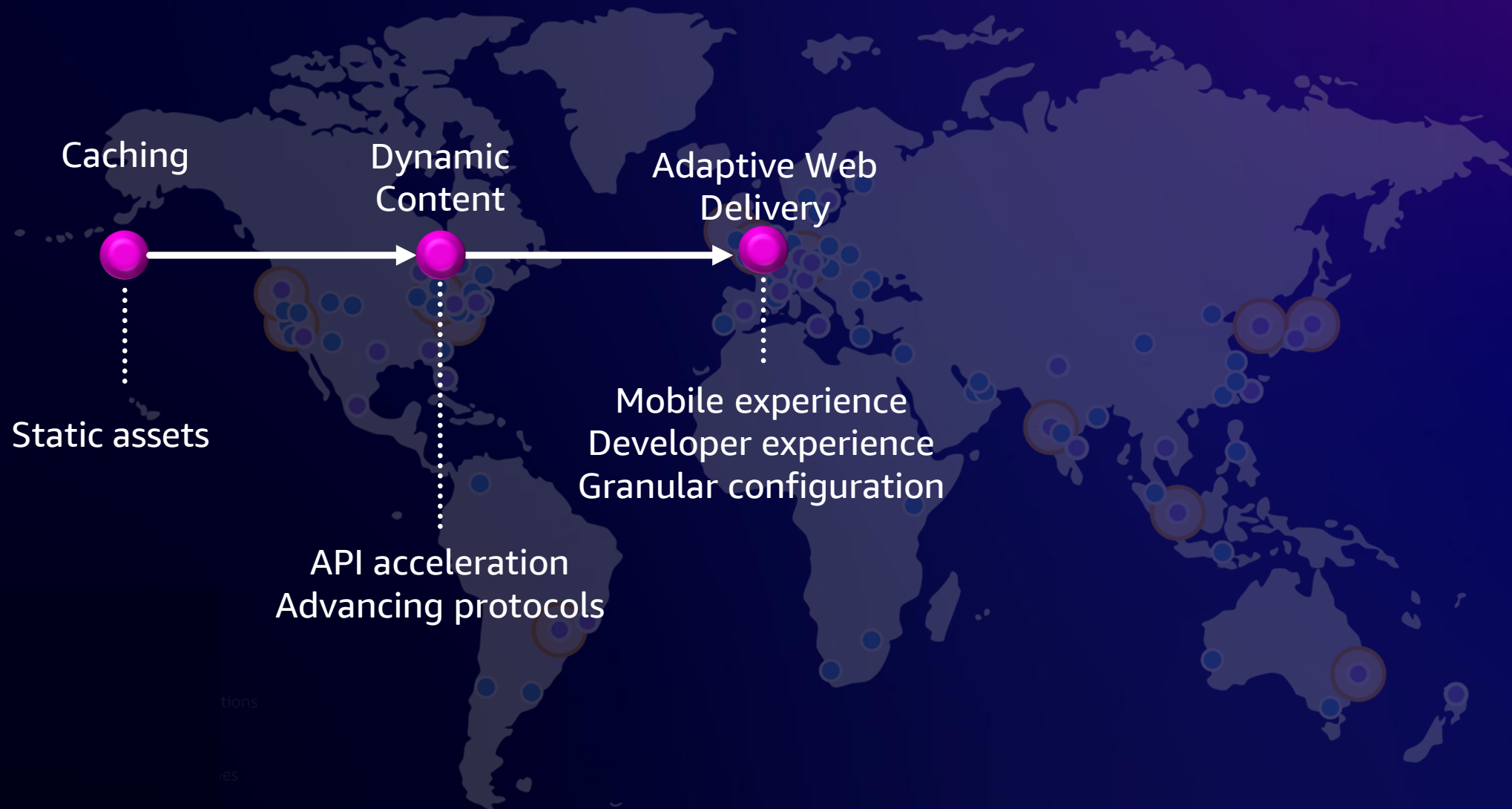
gRPC / HTTP2

```
message HelloRequest {  
    string firstName = 1;  
    string lastName = 2;  
}
```

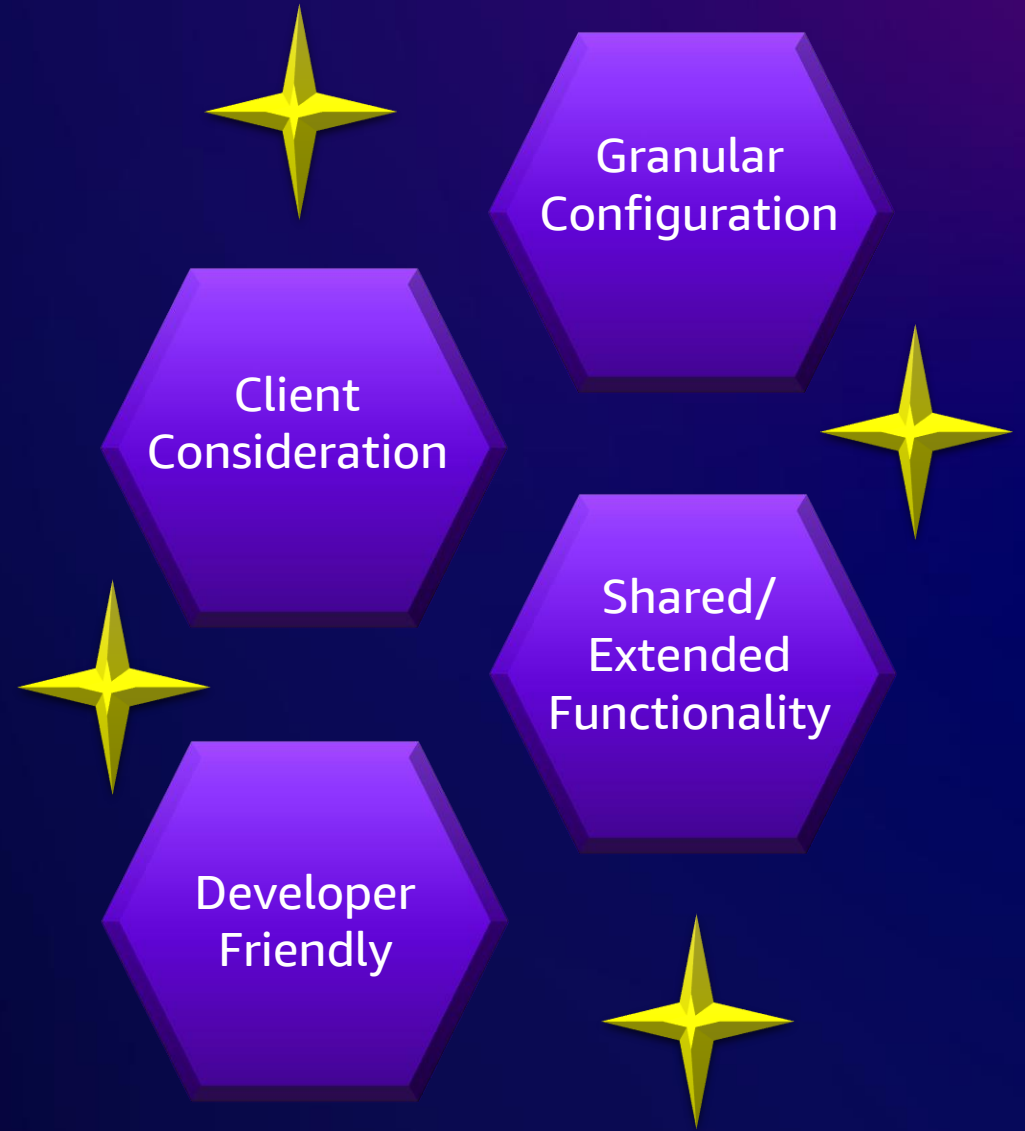


Deliver great experience with QUIC on
Amazon CloudFront

15 years of evolving requirements



Adaptive Web Delivery



Granular Configuration with Edge Functions

Request/Response Manipulation

Cache Key Normalization

URI Re-write

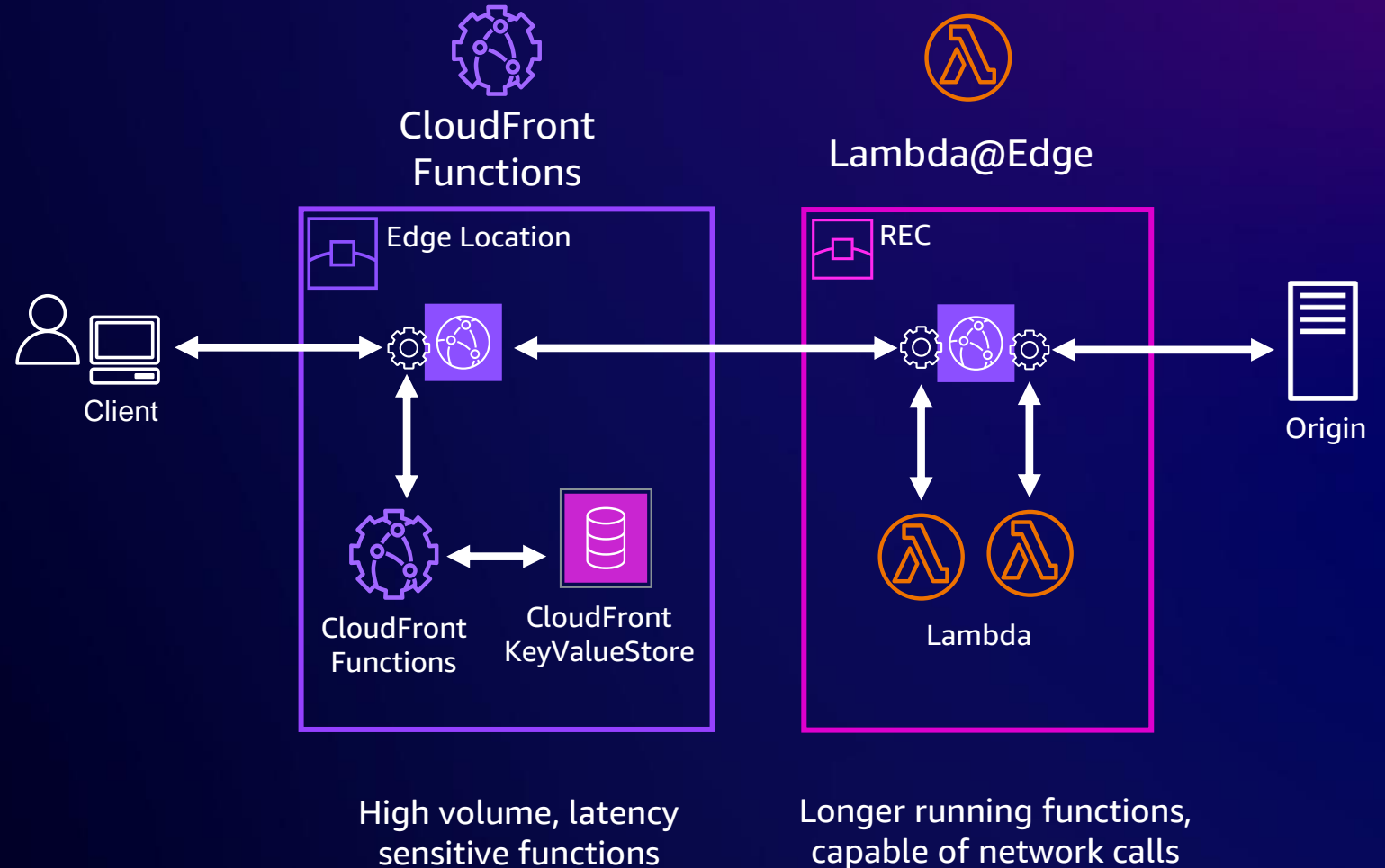
Sophisticated Routing

Redirect

Custom Response Generation

Software Integration

Javascript/Python



CloudFront KeyValueStore

Ultra-fast, instantly scalable data access from CF Functions

Key features

- Data propagated to all 600+ edge locations
- **Read** directly from within functions in microseconds.
- **Decouple code from data** needed inside the function, 5MB default limit
- CRUD APIs, batch import from S3

Maintain URL rewrites and redirects

- Redirect users to a specific country site based on geo-location. Storing and updating these geo-based URLs in a separate KV store simplifies the management of the URLs.

A/B Testing and Feature flags

- Run experiments by assigning a percentage of traffic to a specific version of website

Access Authorization

- Implement access control and authorization by creating and validating user-generated tokens, HMAC/JWT

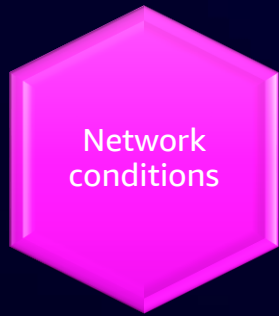
Implement custom rules

- Evaluate the incoming HTTP request against a list of known sites stored in KeyValueCollection and only allow traffic from validated

Video watermarking

- Maintain a list of user sessions in the KV store that should not have access to the livestream

Adaptive web delivery

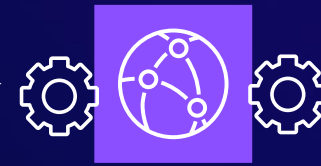


Network
conditions

`nw_path_is_expensive()`



Mobile client

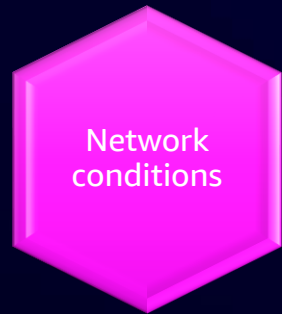


Amazon
CloudFront



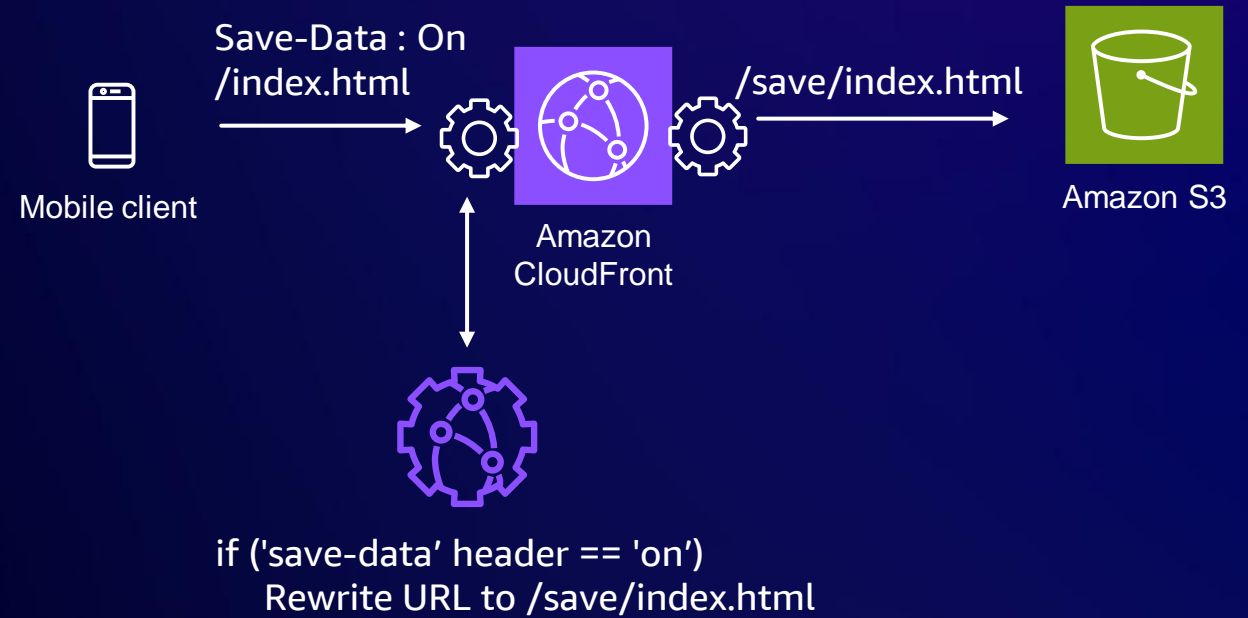
Amazon S3

Adaptive web delivery

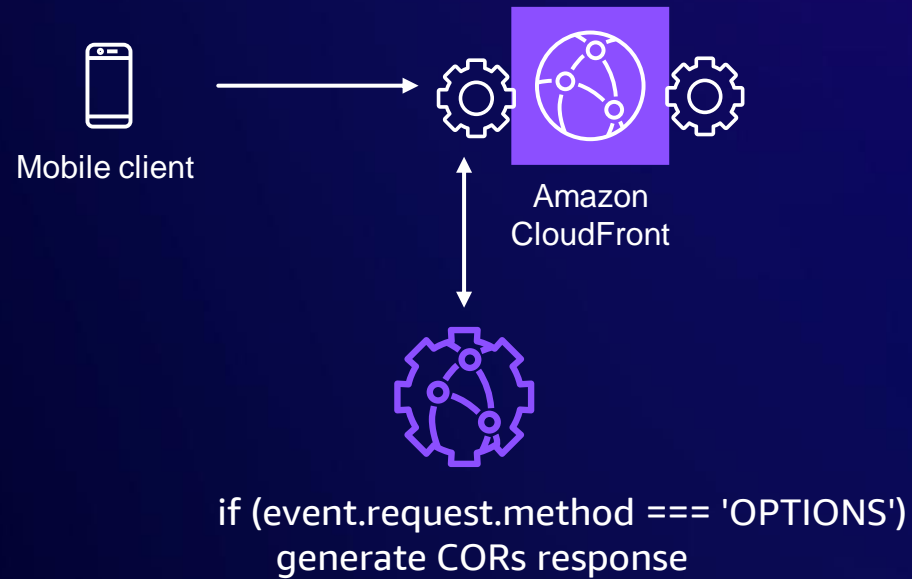
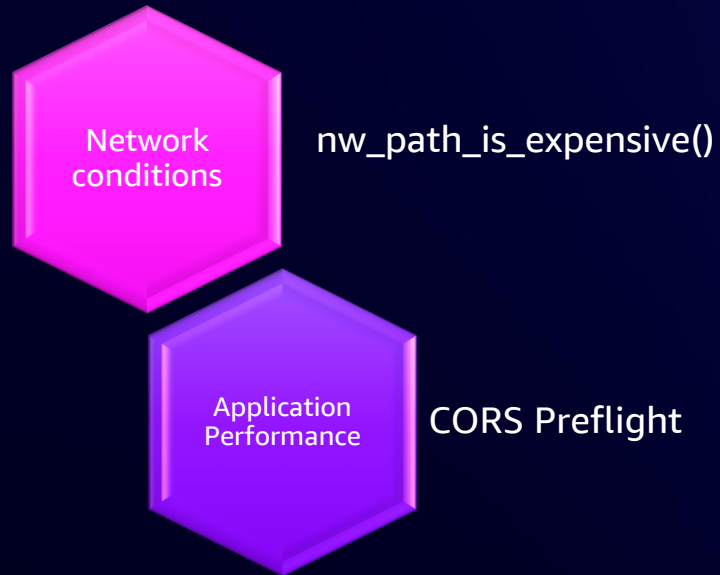


Network
conditions

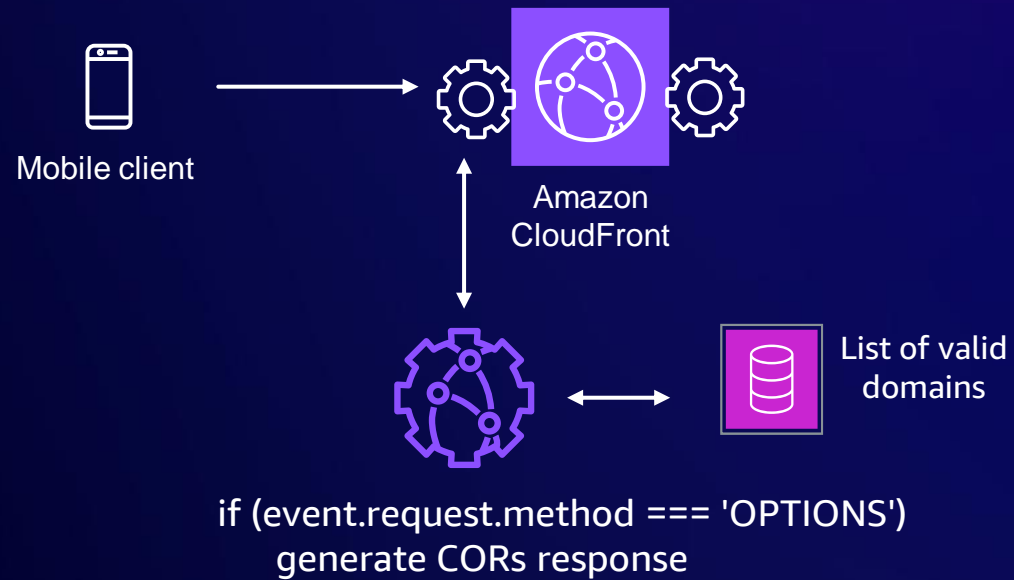
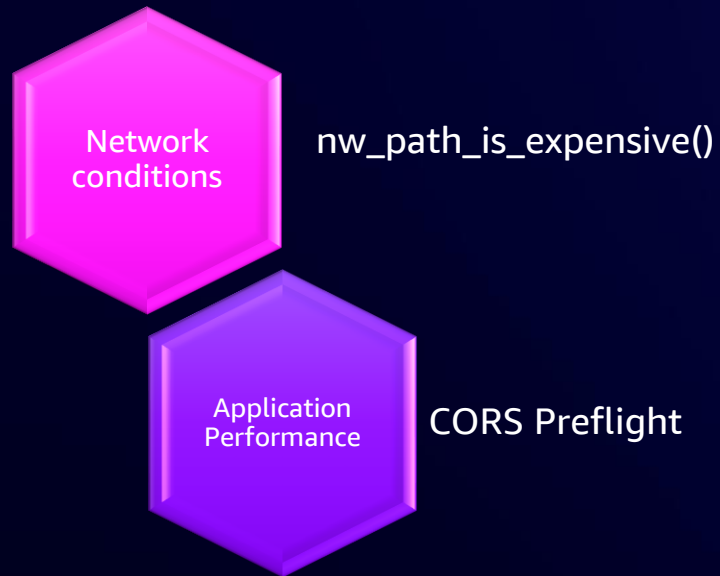
`nw_path_is_expensive()`



Adaptive web delivery

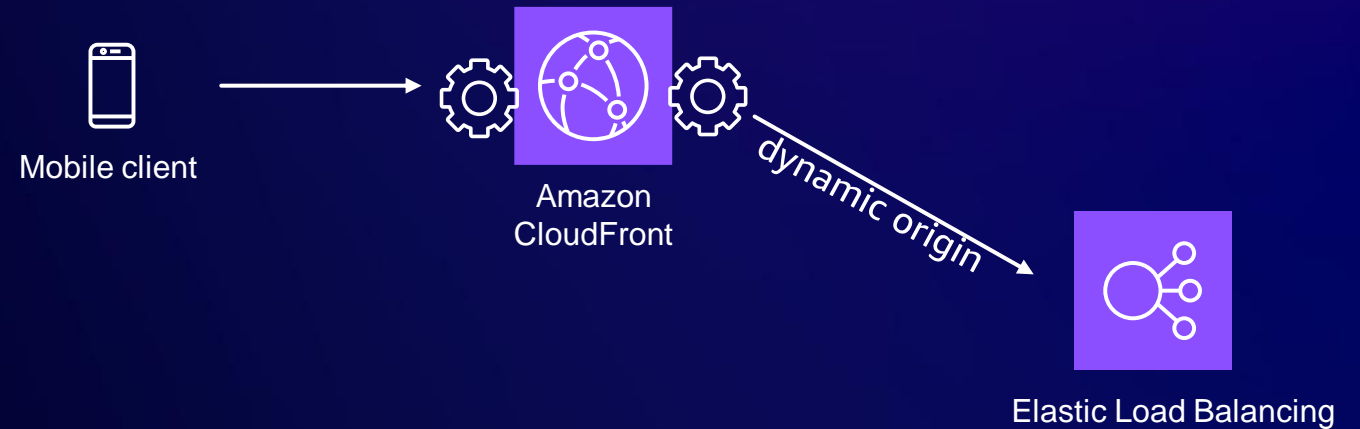
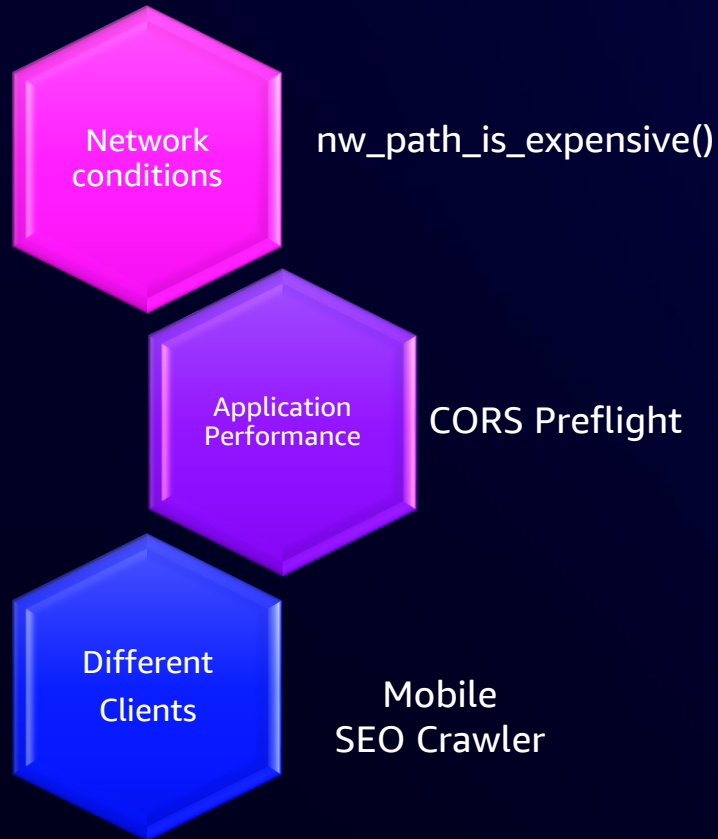


Adaptive web delivery

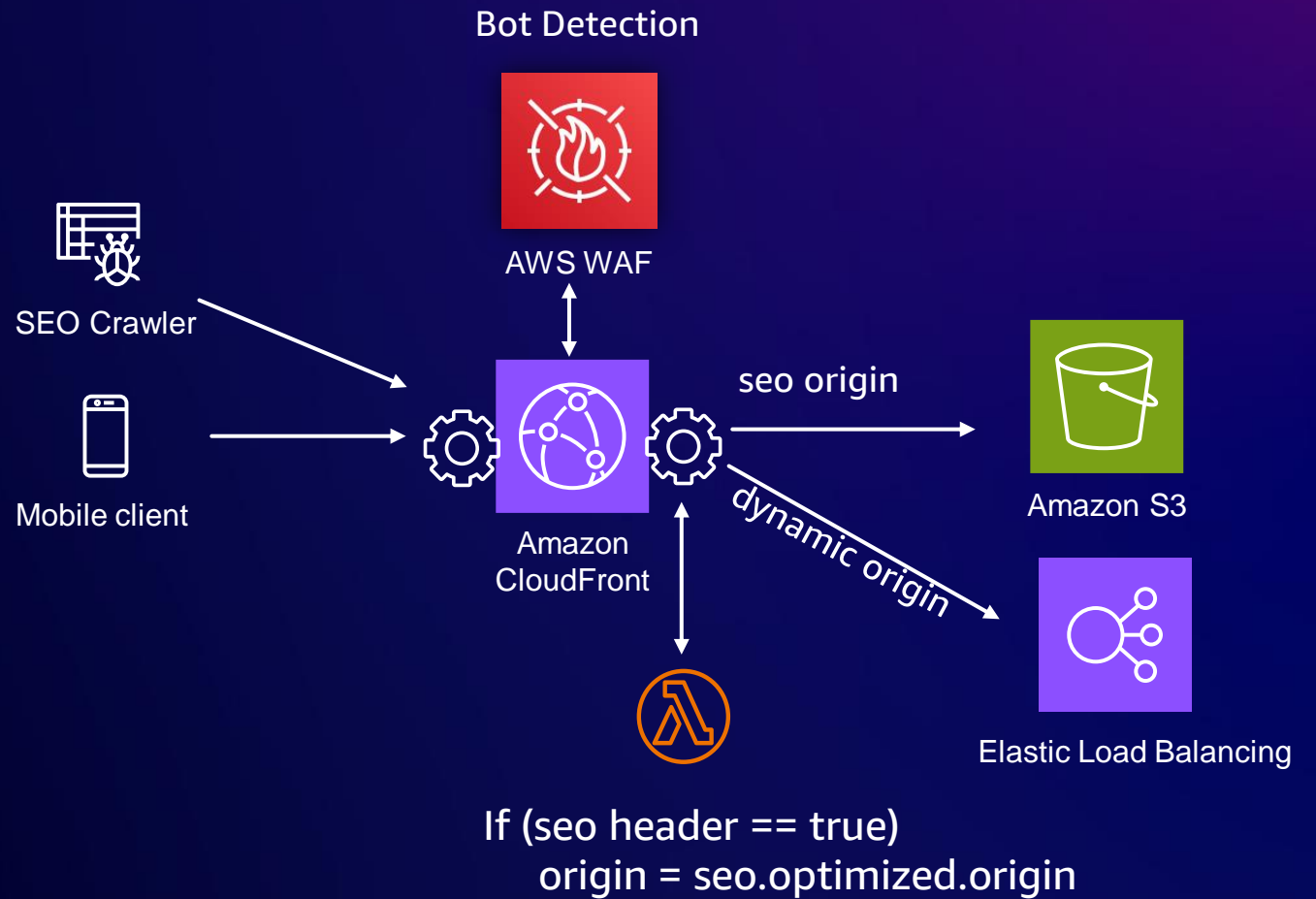
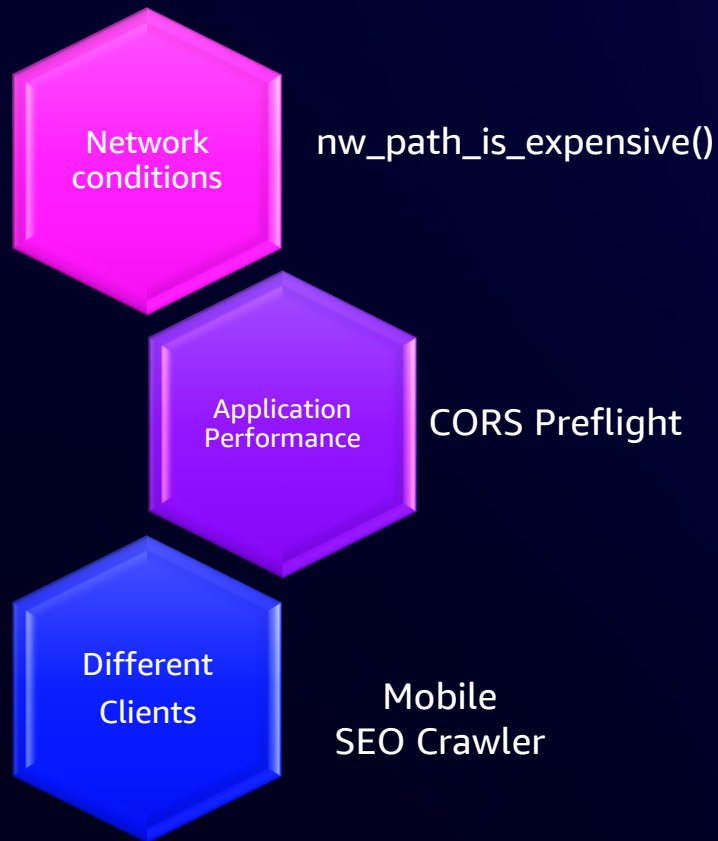


Adaptive web delivery

CloudFront-Is-Android-Viewer
CloudFront-Is-Desktop-Viewer
CloudFront-Is-IOS-Viewer
CloudFront-Is-Mobile-Viewer
CloudFront-Is-SmartTV-Viewer
CloudFront-Is-Tablet-Viewer



Adaptive web delivery



Capital One Auto Navigator

Banking should leave you with the same great feeling you get when you drive casually on a weekend afternoon. And that's how I feel when writing helpful tips and reviews – passionate about cars and passionate about financing and everything in between when buying a new ride.



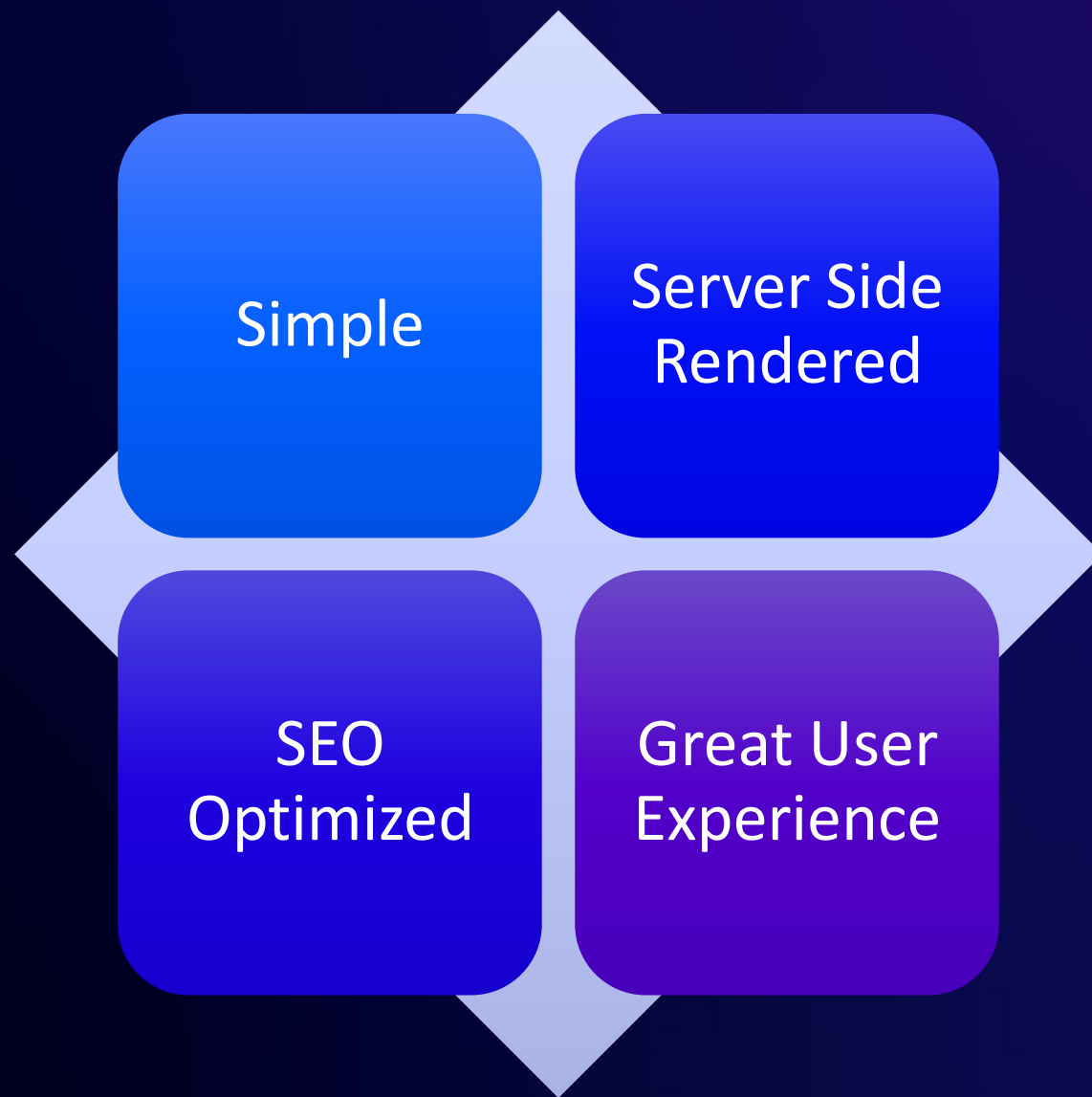
Business Goals

- Effectiveness of the UX design
- Gather learnings
- Validate and measure the customer outcomes

A/B Testing framework requirements

- Quick to Plan
- Easy to Execute

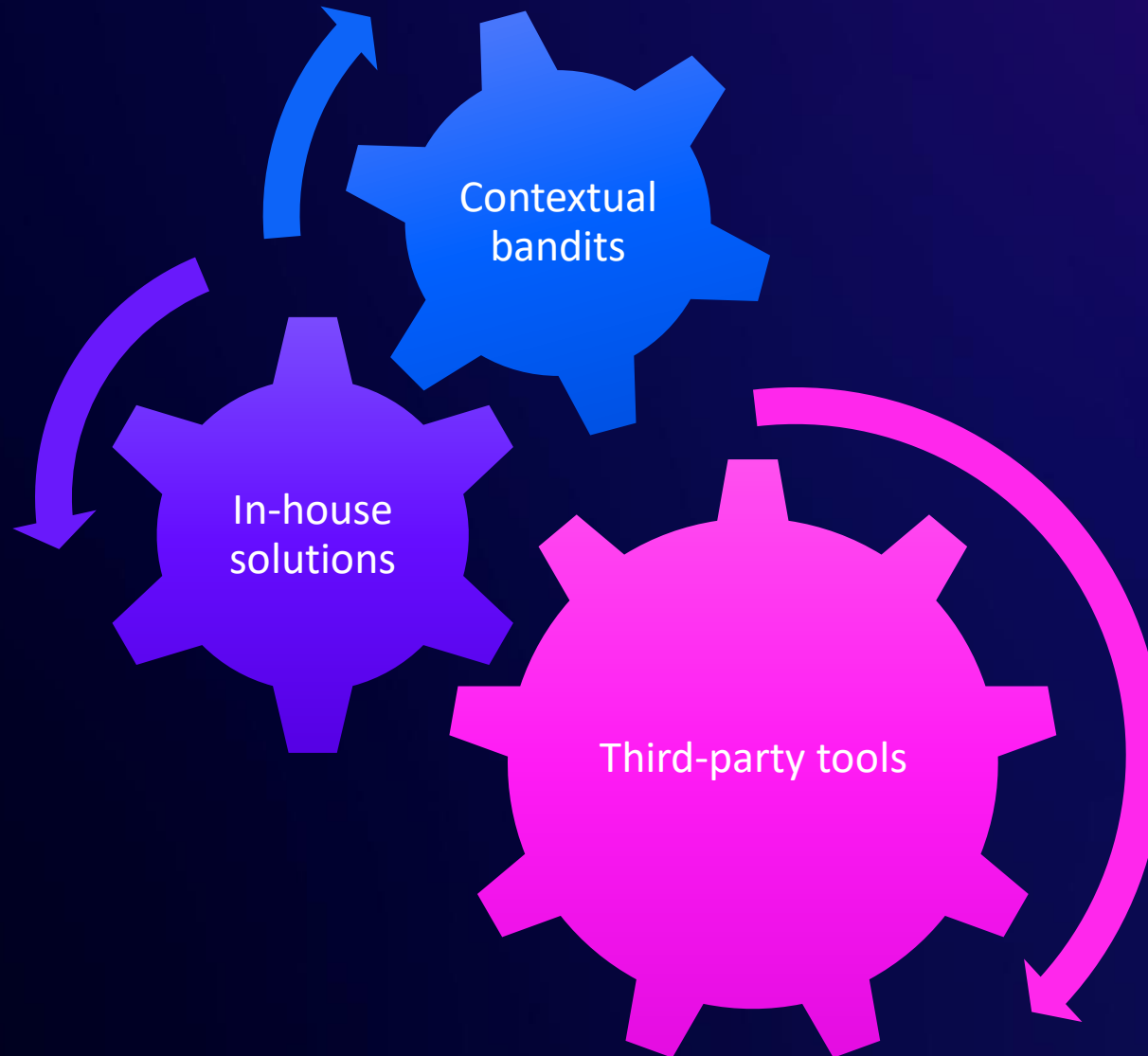
- Generate more traffic
- Crawlable by search engines



- Faster loading
- Less wait time for the user

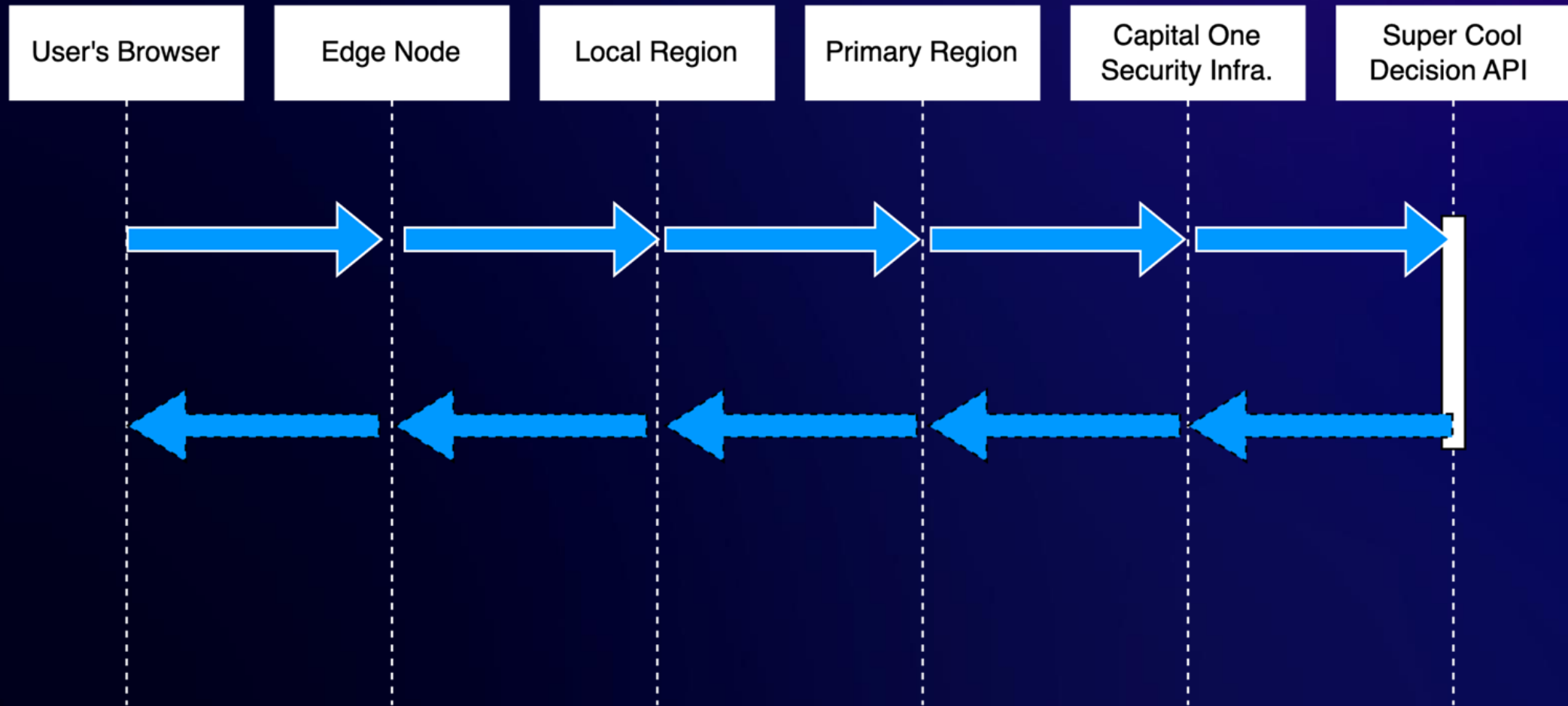
- Clear and intuitive navigation
- Responsive Design
- Engaging Content

Other solutions considered

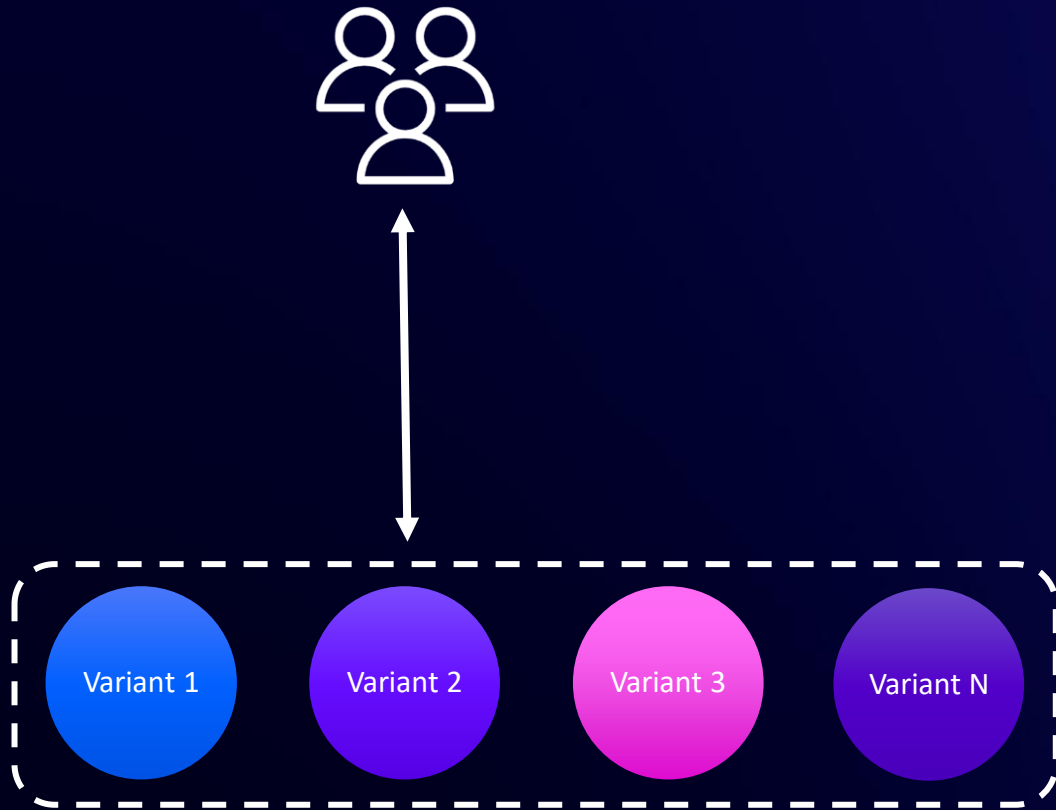


Common issue in these solutions

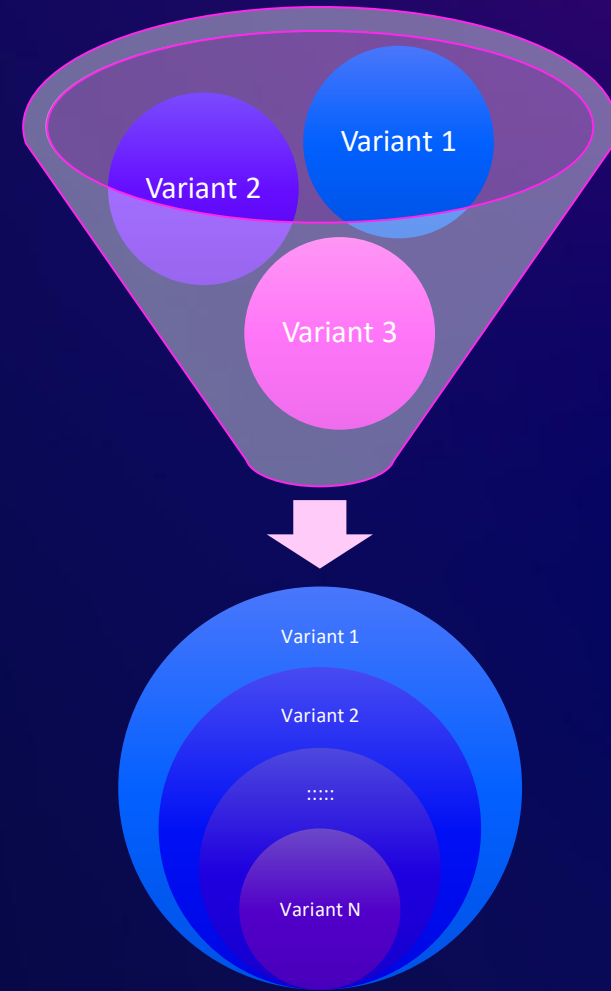
No Caching – Round trip for EVERY call, every time.



Comparing testing frameworks



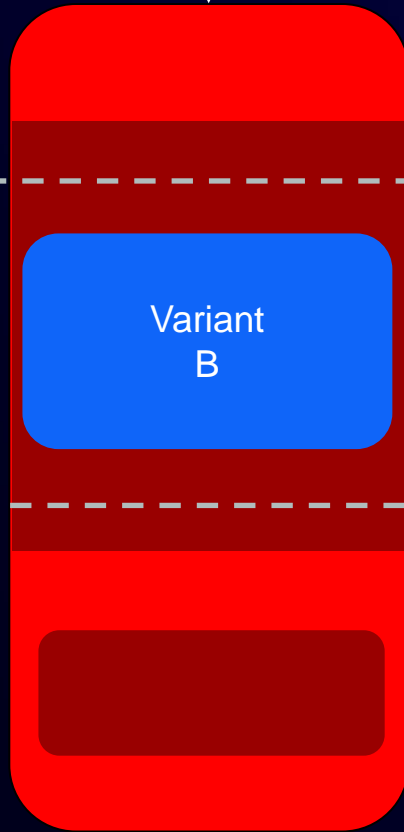
Independent variants lead to true comparisons



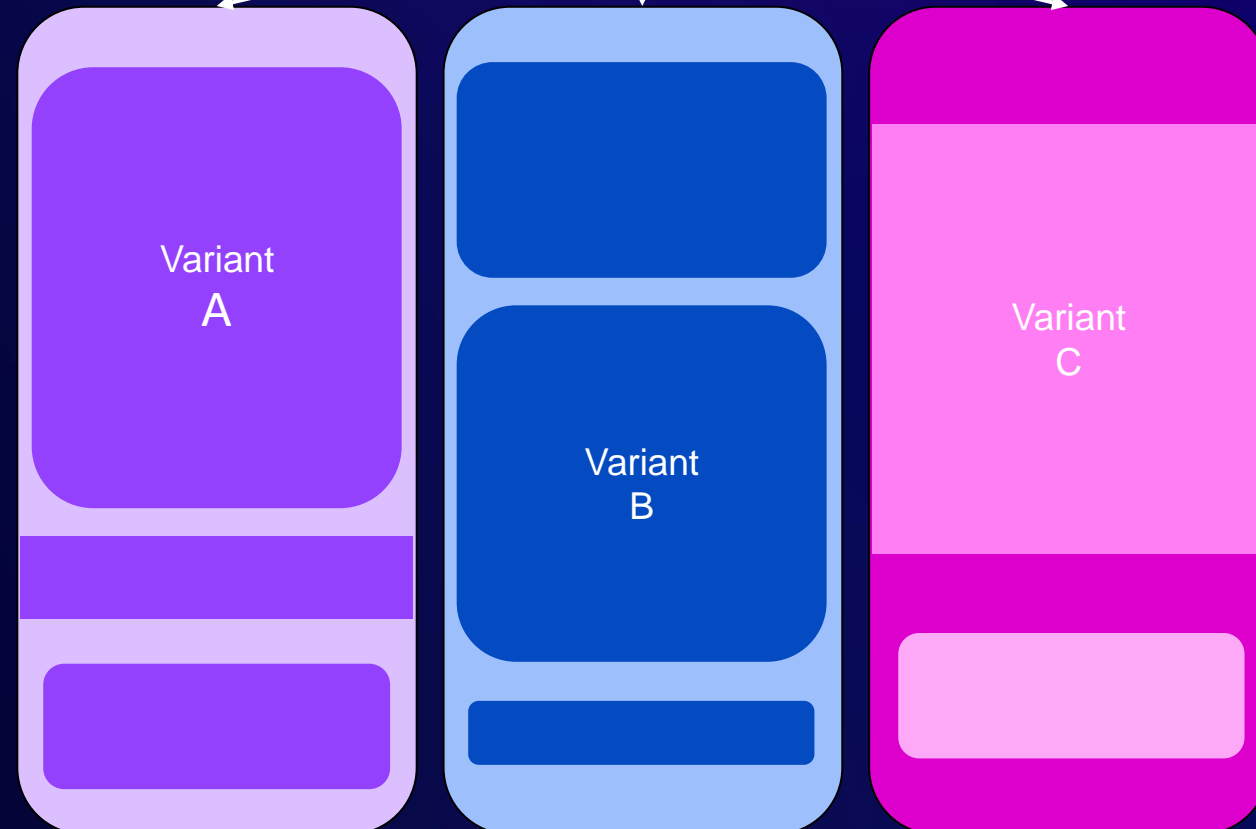
More variants led to larger packages

User experience testing

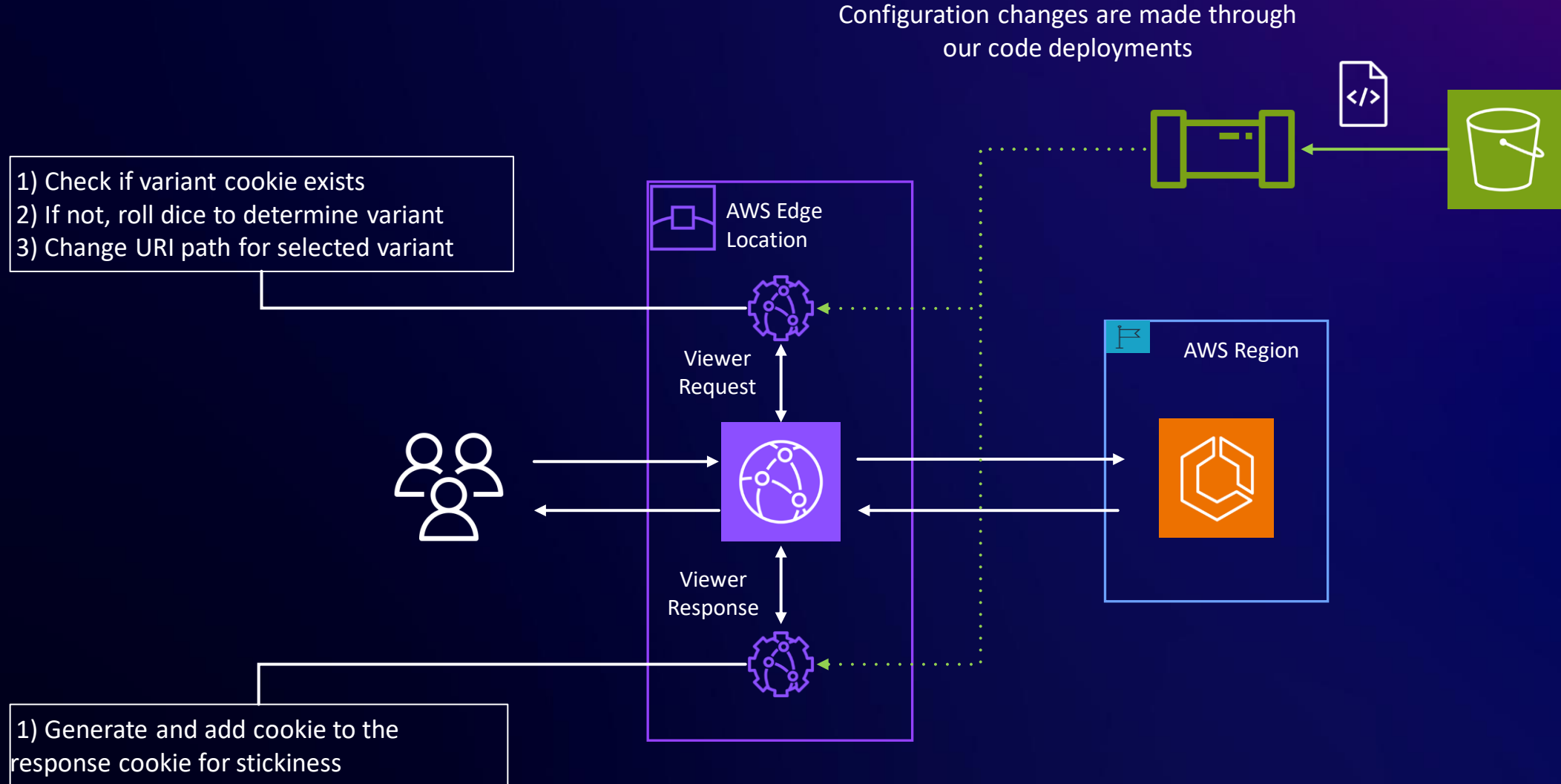
API driven
A/B Testing



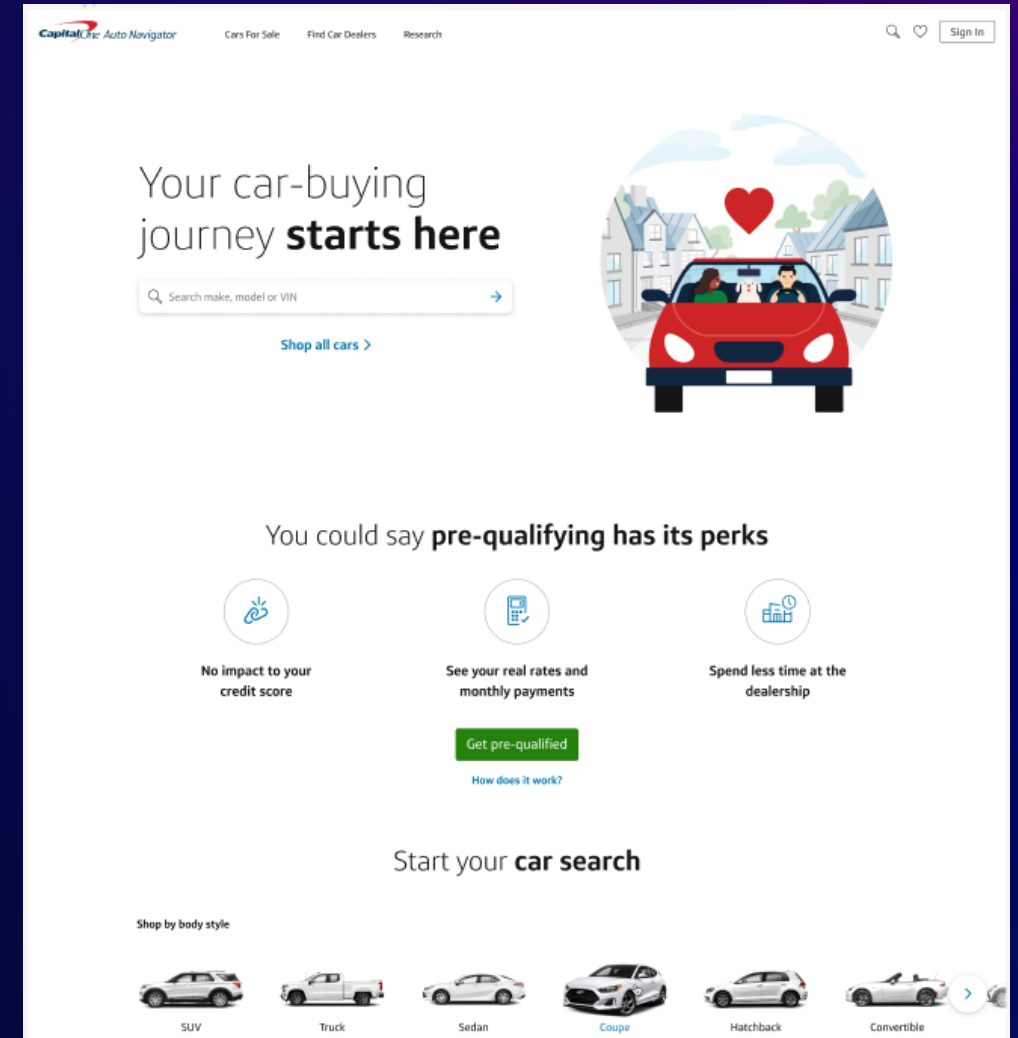
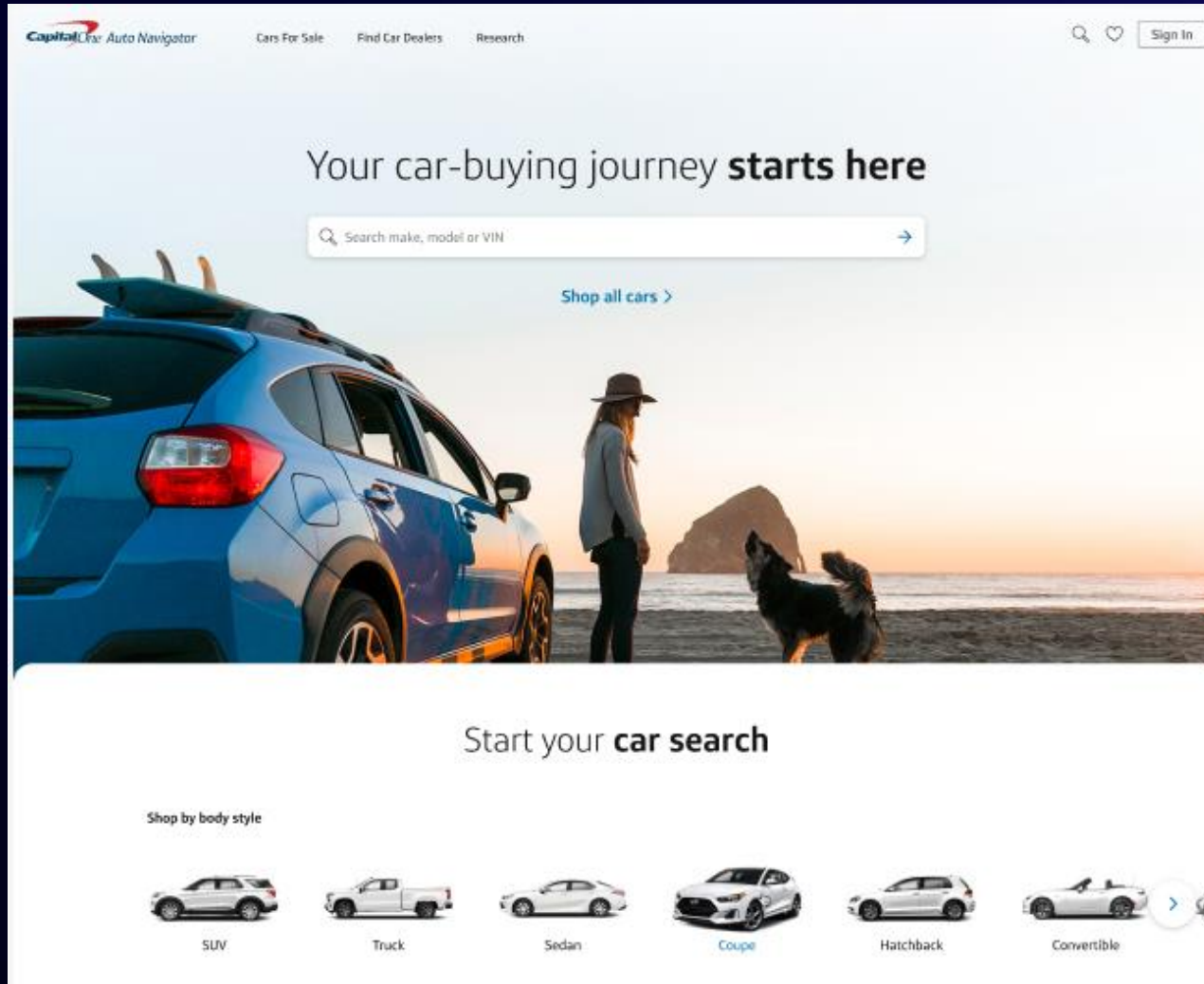
CloudFront driven
A/B Testing



Architecture



Full page testing



Results

Performance



3×

Organic Traffic



4×

Time on Site



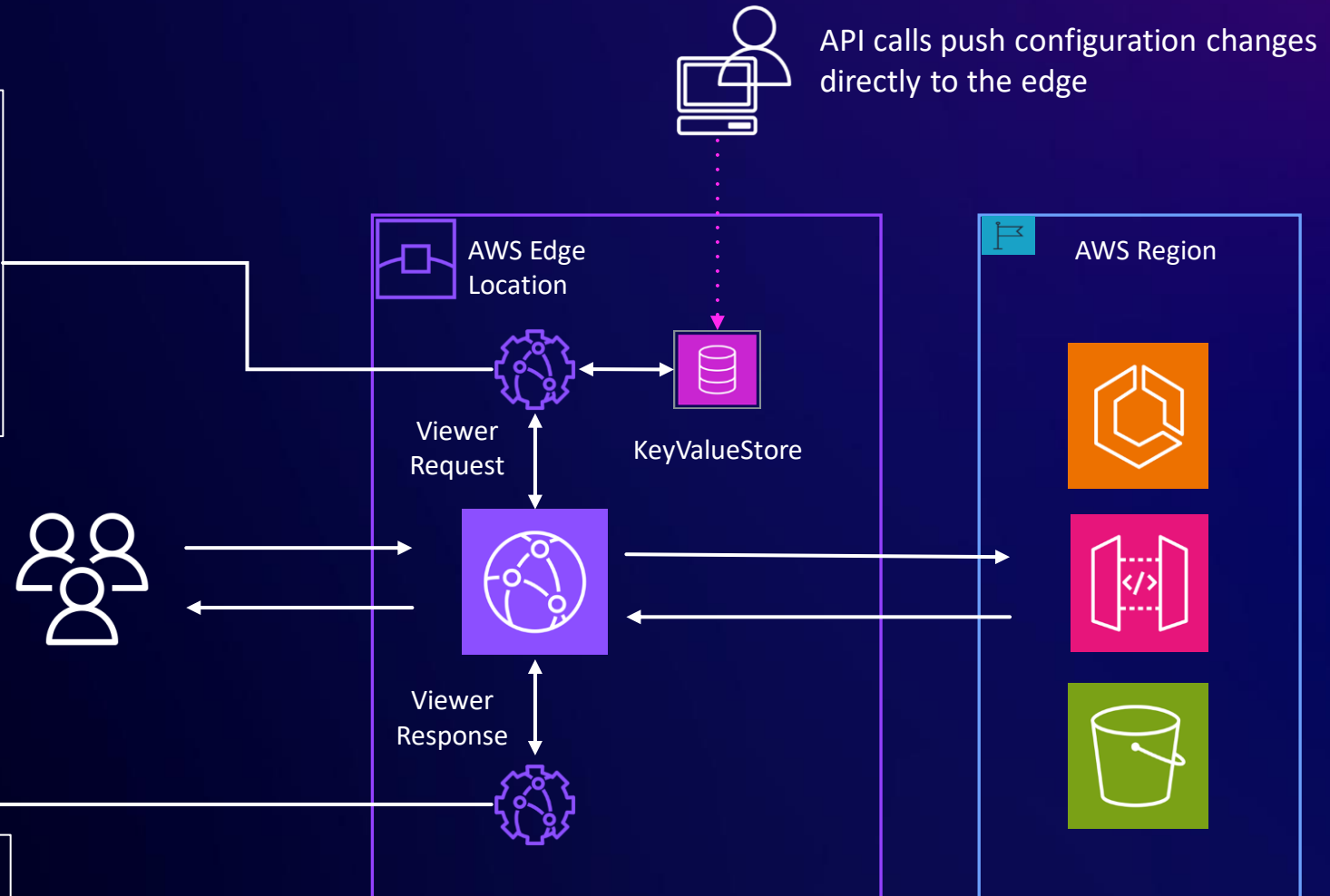
6×

Evolving Architecture - KeyValueStore

- 1) Check if variant cookie exists
- 2) If not, roll dice to determine variant
- 3) Change URI path for selected variant

Improvements:

- 1) Load variant configurations from KeyValueStore
- 2) Update/Set Response Body





- 1) Generate and add cookie to the response cookie for stickiness

No Code Testing (HTML Injection)

Take out the guesswork. See your real payment while you search.

Get Pre-qualified





Dealer Partner


2011 Chevrolet Equinox LTZ

\$11,895 ①

Gasoline

Used 61,138 mi

WBM of Arlington 5 mi away



Dealer Partner


2015 Kia Sorento LX

\$5,995 ①

Gasoline

Used 116,096 mi

Auto Buying Service 5 mi away



Dealer Partner


2012 Infiniti G37 Journey

\$6,995 ①

Gasoline

Used 114,803 mi

Auto Buying Service 5 mi away



Dealer Partner


2013 Hyundai Sonata Limited PZEV

\$8,995 ①

Gasoline

Used 124,115 mi

Auto Buying Service 5 mi away



Dealer Partner

2015 BMW 3 Series 328i xDrive

\$9,895 ①


Gasoline


Used 124,012 mi

Auto Buying Service 5 mi away

Take out the guesswork. See your real payment while you search.

Get Pre-qualified





Dealer Partner

2012 Audi A7 3.0 Premium Plus

\$10,163 ①

Gasoline

Used 128,456 mi


Auto Buying Service 5 mi away

Auto Navigator - Search Results Page

Build a **custom deal** on a car you'll love.

Personalize your deal


Less guessing, more knowing.



Sell your car with confidence, get your estimate today.

Get started


Dealer-trusted valuations.



Add your trade-in to see lower monthly payments.

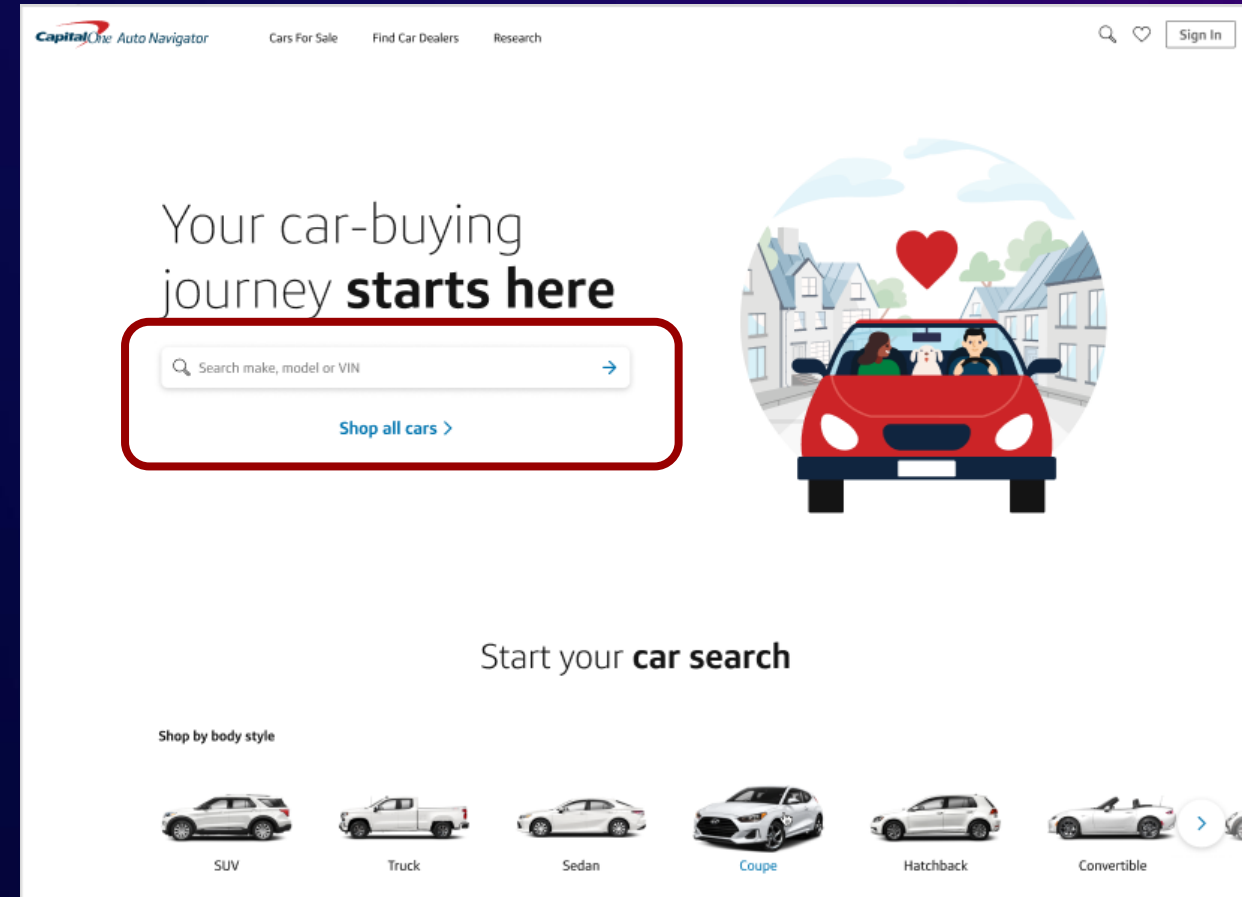
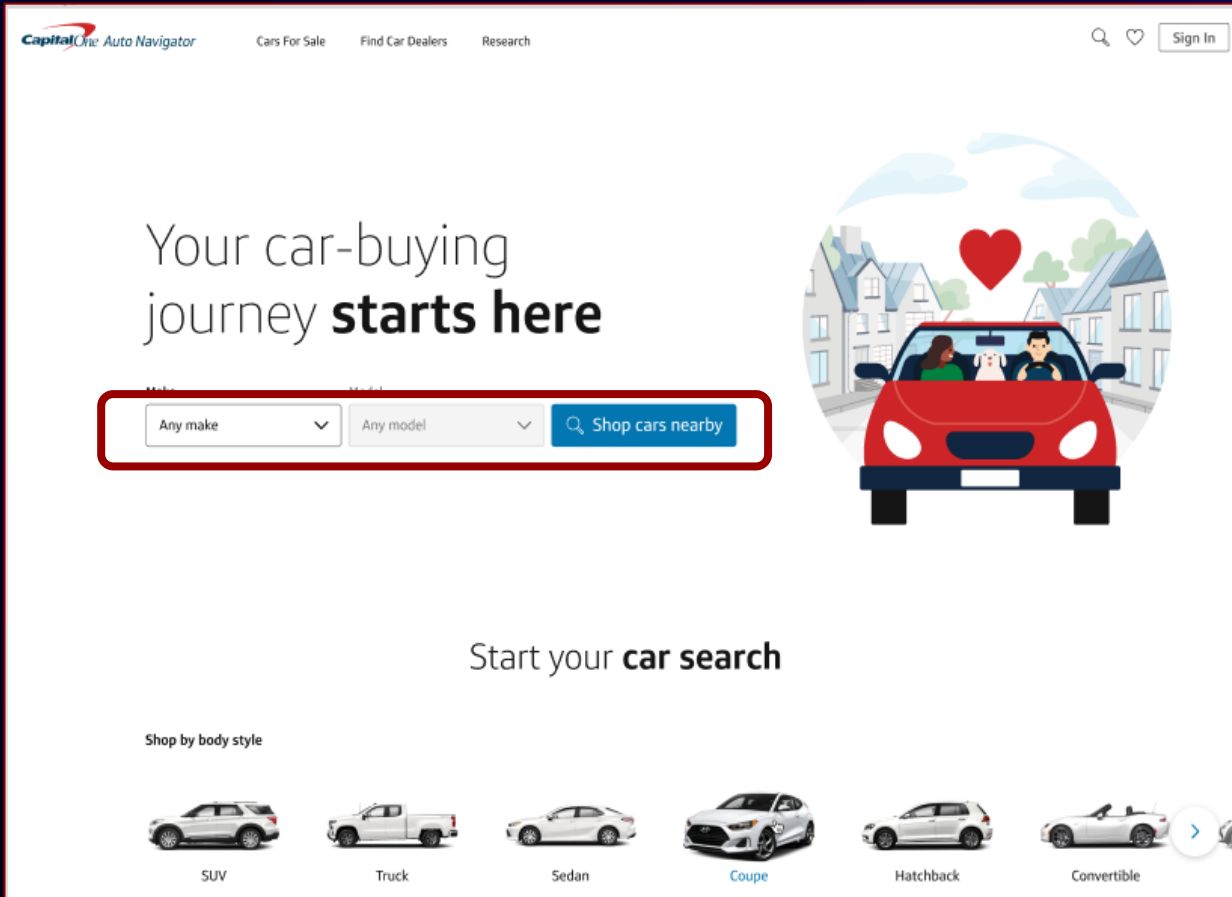
Add trade-in

Boost your down payment.



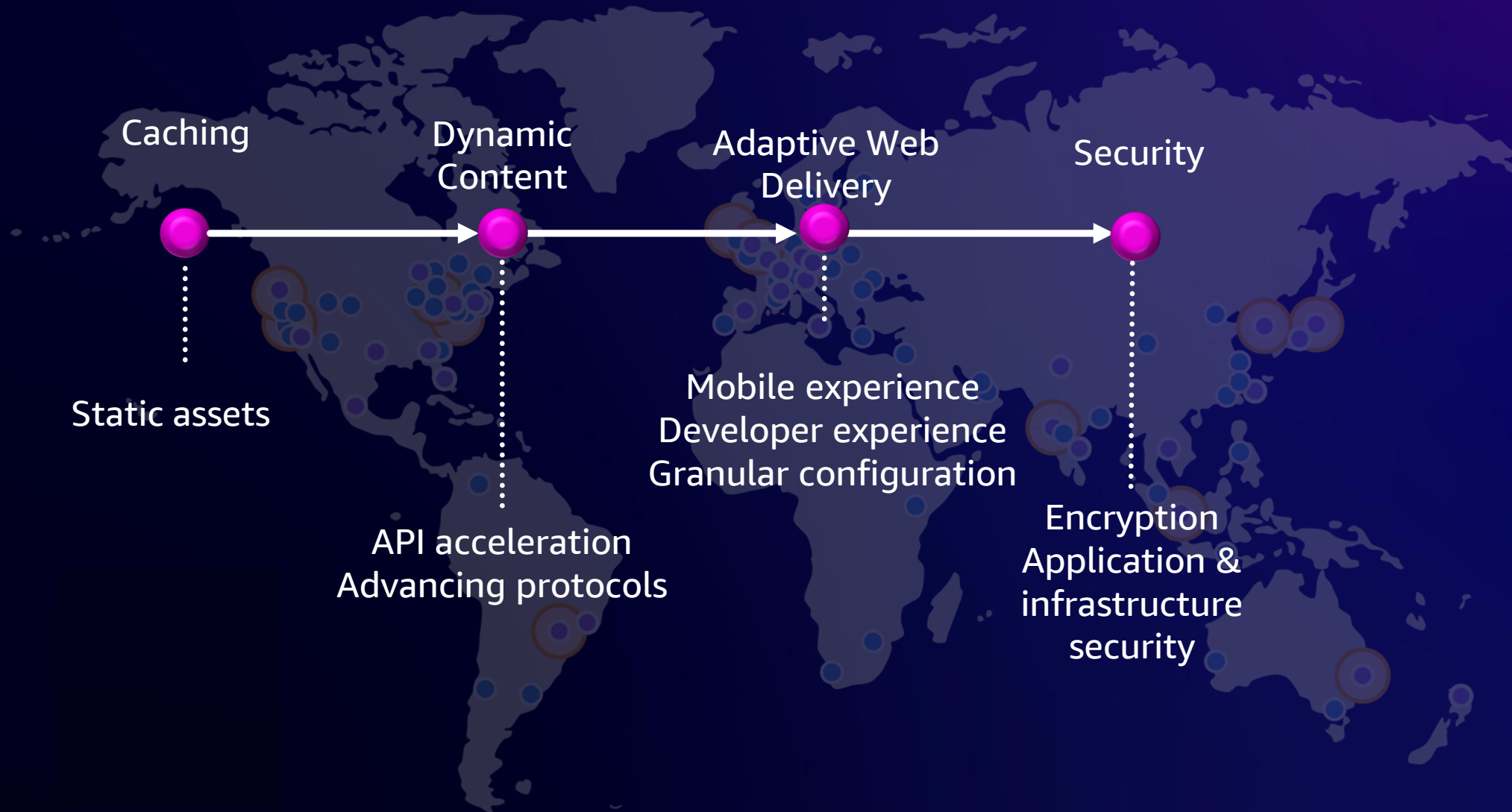
Possible Card Variants

Component Testing - Single Package



When it just can't be helped - Simple Changes

15 years of evolving requirements



Built-in security



Infrastructure Security

Shield Integration
DDOS protection
Syn Proxy
Slowloris
HTTP2 Rapid Reset
HTTP Desync
Packet Inspection
Protocol Filtering



Application Security

WAF Integration
Recommendations
Visibility



Secure Connections

ACM Integration
TLS
Free certificates
Domain Fronting
OCSP Stapling



Secure Access

Origin Access Control
Signed URLs
Signed Cookies
Field Level Encryption
VPC Prefix List
Geo Protection

Establishing a secure perimeter

Layer 3/4

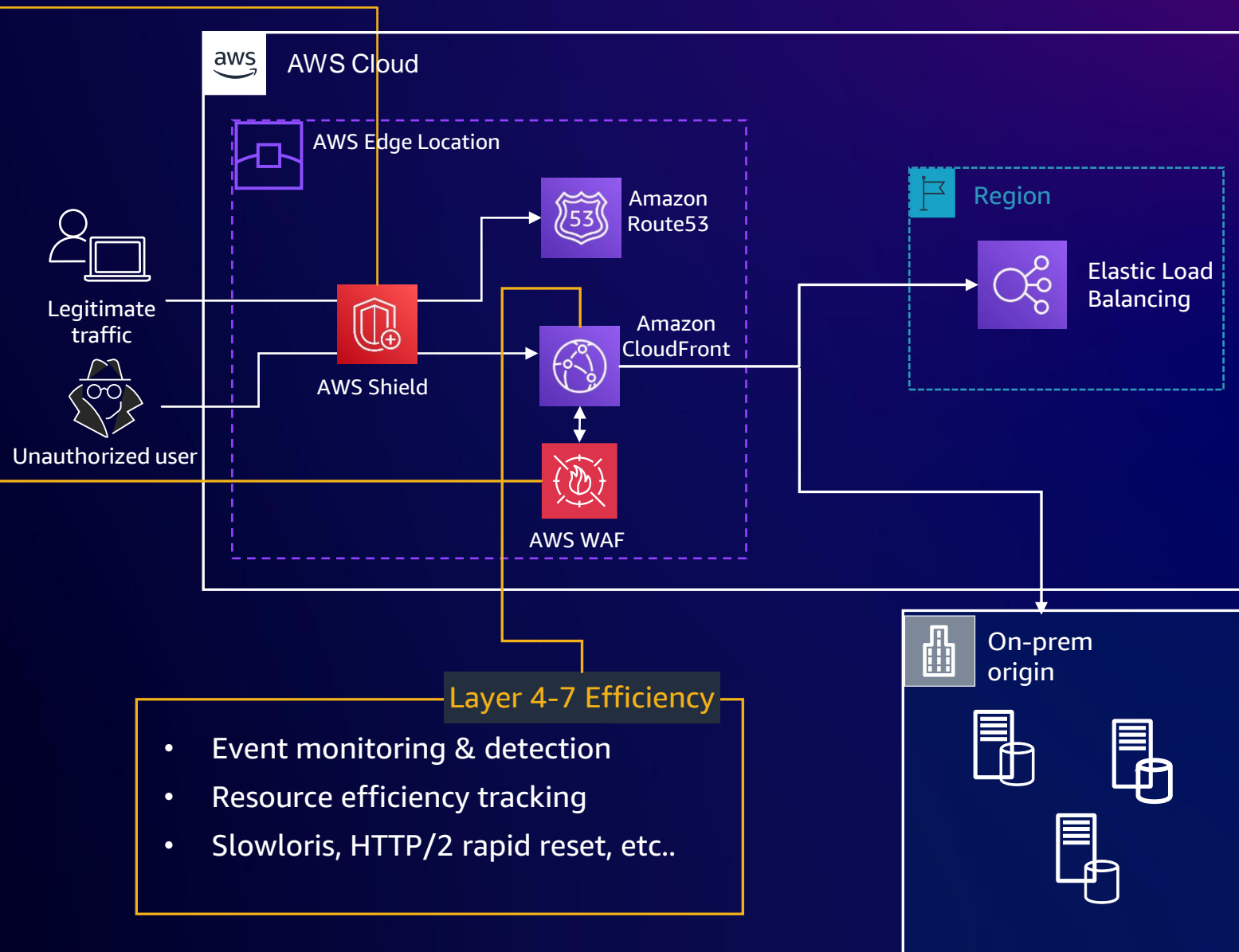
- Black Watch
- SYN Proxy
- Continuous inspection (inline)
- Packet validation
- Distributed scrubbing capacity
- Automated routing policies to absorb large attacks

Layer 7

- Bot Management
- RateLimiting
- Managed Rules (OWASP)
- Custom Rules
- Security Automation

Layer 4-7 Efficiency

- Event monitoring & detection
- Resource efficiency tracking
- Slowloris, HTTP/2 rapid reset, etc..



One click application security with recommendations, visibility, and actionable app-centric insights

Web Application Firewall (WAF) [Info](#)

AWS WAF is enabled on this distribution. [View details of your configuration](#).

Select this option if your application does not need AWS WAF security protections.

▼ Additional protections for WordPress applications **Recommended**

Blocks malicious request patterns associated with the exploitation of vulnerabilities specific to WordPress, PHP, and SQL databases.

Block HTTP flood attacks, also known as Denial of Service (DoS), that can affect availability, compromise security, or consume excessive resources. This rule rate limits requests for a given IP address that exceeds the allowed rate for your application.

▼ Price estimate

- Enabling WordPress protections will add \$3/mo to your AWS WAF bill.
- Enabling rate limiting protections will add \$1/mo to your AWS WAF bill.

Cancel

Save changes

▼ Security trends for August 18, 2024 (All requests) [Info](#)

123.9 MM ▲ 3%
Total requests

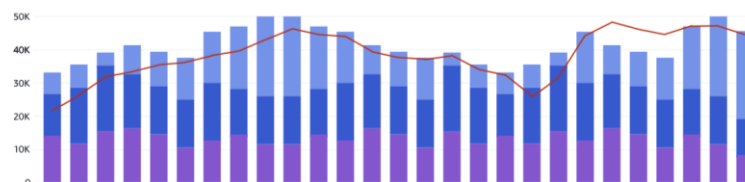
92.5 MM
■ Allowed requests

31.0 MM
Blocked requests

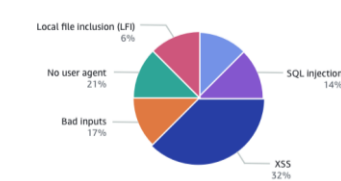
980ms ▲ 19%

■ Origin latency

Requests

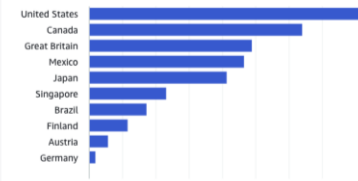


Attack types



Top countries

Manage blocked countries (2)

Requests (160) [Info](#)

< 1 2 3 4 > ⚙

	Rule action	Host	Path	IP Address	Country	User agent
	Allow	example.com	/	174.136.248.184	United States	Mozilla/5.0 (Macintosh ...
	Block	example.com	/api/me	216.185.53.123	North Korea	Mozilla/5.0 (Windows ...
	Allow	example.com	/xmircp.php	23.160.208.166	Ireland	Mozilla/5.0 (Android ...



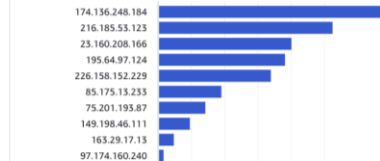
Top URI paths

Manage blocked URI paths (0



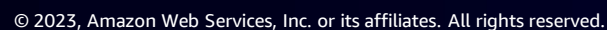
Top IP addresses

Manage blocked IP addresses (3)

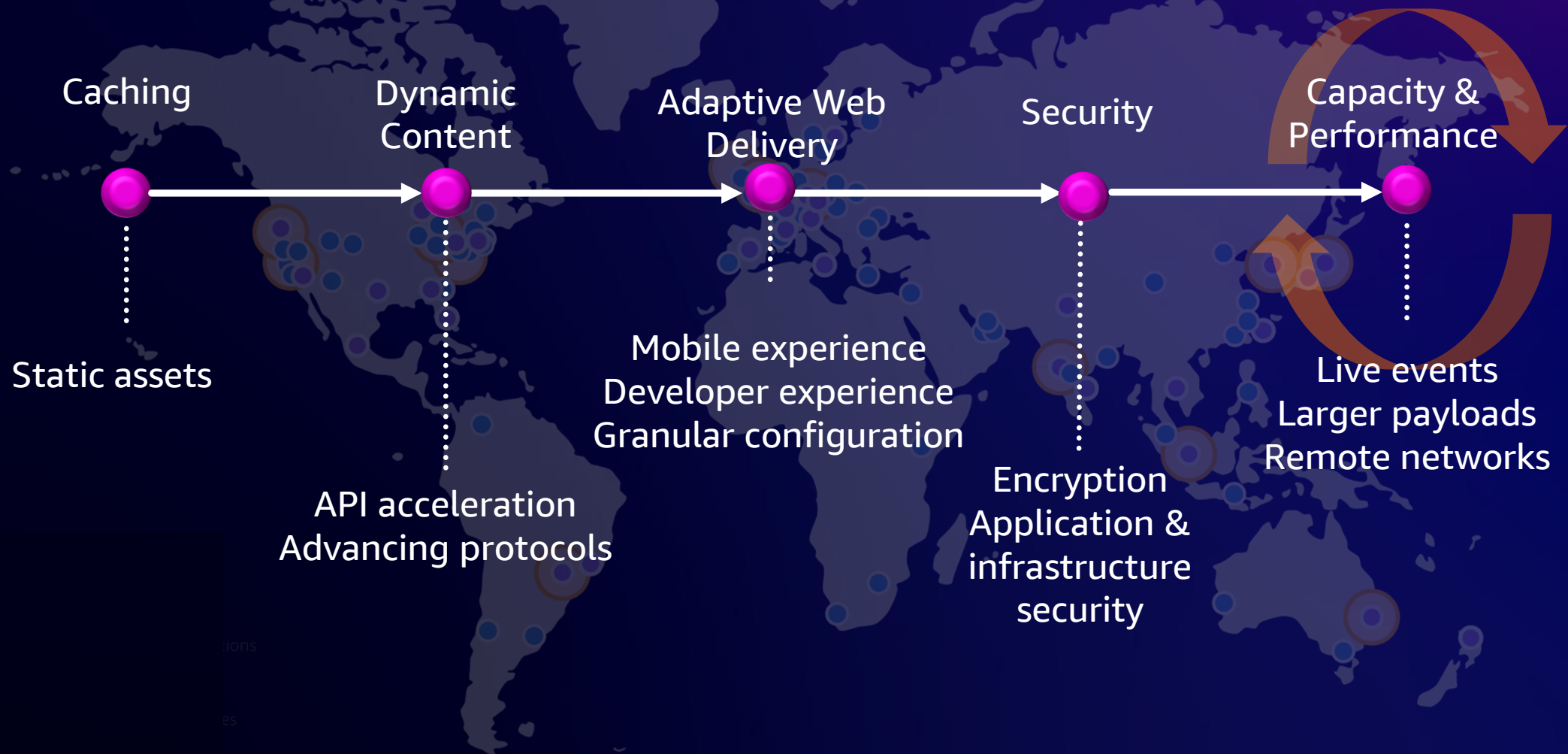


Top countries

Manage blocked countries (2)

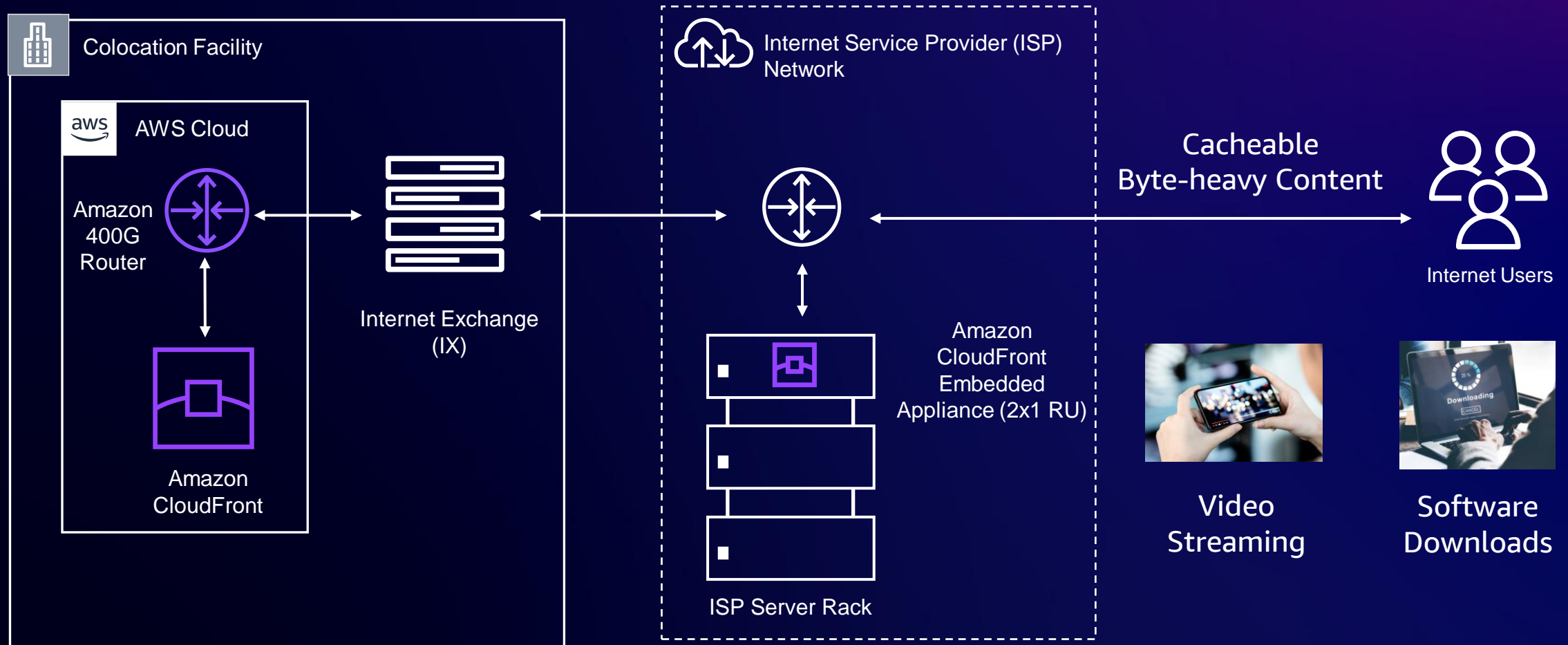


15 years of evolving requirements



Embedded POP

95% Offload
65% FBL reduction



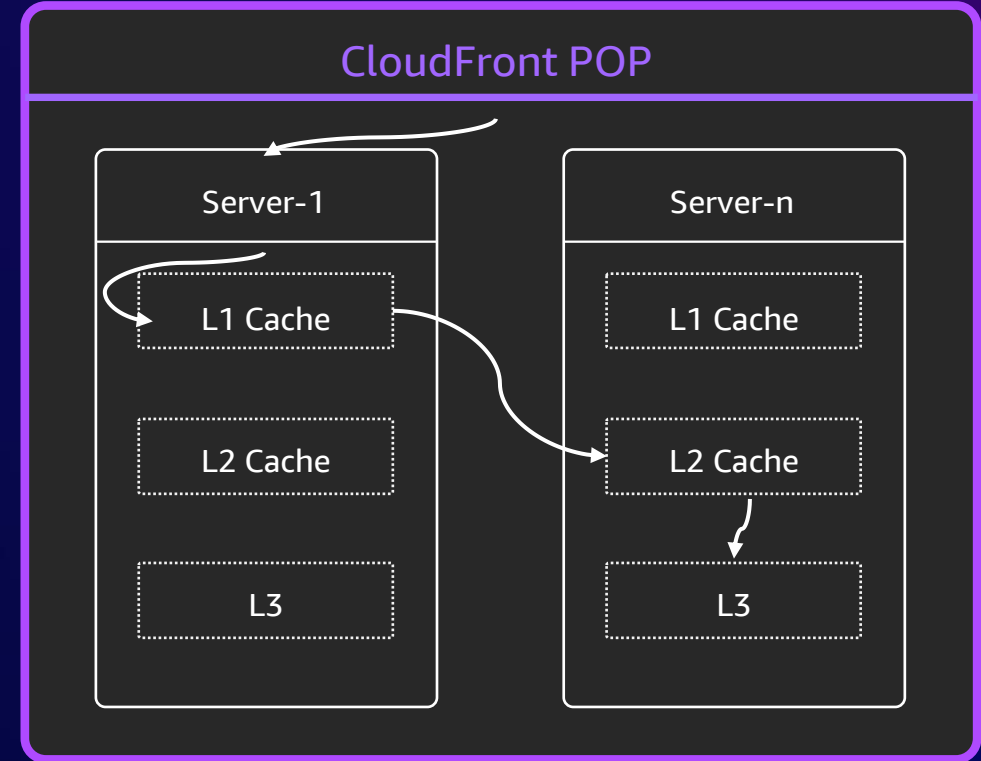
CloudFront POP architecture

Technology Stack

NGINX SQUID

Challenges

- Designed for out dated protocols
- Suboptimal for CPU expensive requests
- Contains capabilities not relevant to CDN
- Difficult to update with latest security features

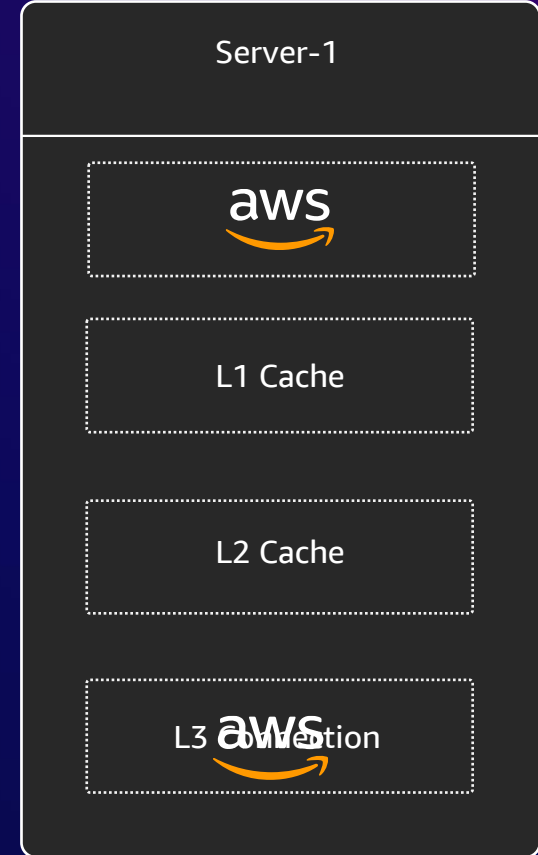


Optimizing for performance:
Every millisecond counts!

Re:Inventing Amazon CloudFront



- AWS Built server
- Built on Tokio Runtime maintained by AWS engineers
- Built to enable QUIC HTTP/3
- Multi-threaded, work stealing scheduler
- Written Rust



100ms improvement for HTTP2/3 connections

Thank you!



Please complete the session survey in the mobile app

Tino Tran

 [linkedin.com/in/tinot-aws](https://www.linkedin.com/in/tinot-aws)

Kevin Gaynor

 [linkedin.com/in/kevin-gaynor-7892a6a/](https://www.linkedin.com/in/kevin-gaynor-7892a6a/)

Harish Kathpalia

 [linkedin.com/in/harish-k-821b7810/](https://www.linkedin.com/in/harish-k-821b7810/)

