AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

NET319

Migrating large-scale websites to Amazon CloudFront

Hector Ibarra
Principal Solutions Architect
AWS

Jeremy Labadie
Sr. Cloud Infrastructure Architect – Edge Services
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- Why AWS edge services?
- Frequent migration challenges
- Typical migration plan and lessons learned
- Dive deep into the most common solutions
- Migration architecture examples
- Enhancing flexibility for security migration
- Takeaways

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why AWS edge services

WHAT CUSTOMERS MIGRATING TO AMAZON CLOUDFRONT TELL US

Speed of innovation

"We've been able to move more quickly because a broader range of people have been able to work on the problems that fit at the CDN layer. Relying on Amazon CloudFront, we can iterate faster on features at the CDN layer."

Michael Smith, Principal Engineer – Reach plc

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why AWS edge services

WHAT CUSTOMERS MIGRATING TO AMAZON CLOUDFRONT TELL US

Fast and reliable

"At Arqiva we are using CloudFront Functions to enable us to easily implement a bespoke authentication solution for a consumer-facing API serving over 50,000 requests/second at peak. This allows us to secure the platform in a highly performant and scalable way, fully leveraging the power and reliability of the CloudFront CDN."

Matthew Huntington, Director of Product – Arqiva

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why AWS edge services

WHAT CUSTOMERS MIGRATING TO AMAZON CLOUDFRONT TELL US

AWS integrations

"We love the way CloudFront seamlessly integrates with the rest of AWS and allows us to be very efficient in the ways we develop, deploy, and manage our infrastructure."

Udi Nir, VP of Engineering – Instacart

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why AWS edge services

WHAT CUSTOMERS MIGRATING TO AMAZON CLOUDFRONT TELL US

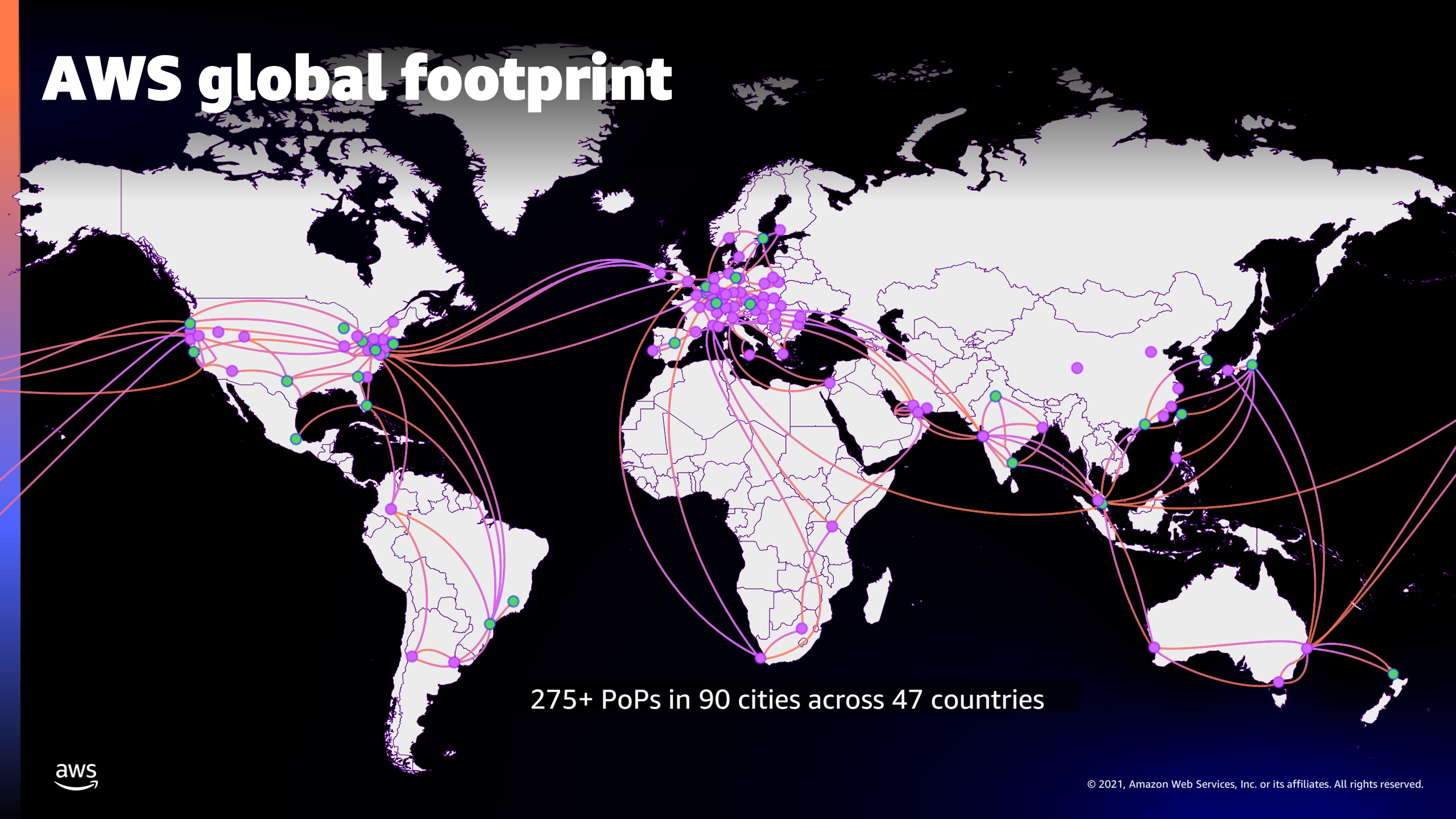
Cost-effective

"ProSiebenSat.1 Media chose Amazon CloudFront primarily for the cost advantage the cloud service provides . . . our digital offerings decreased their operational costs by more than 50 percent. In particular, the cost-free exchange between Amazon S3 and CloudFront allowed savings in the six-digit range per year."

Boris Radke, CIO – ProSiebenSat.1 Media SE

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

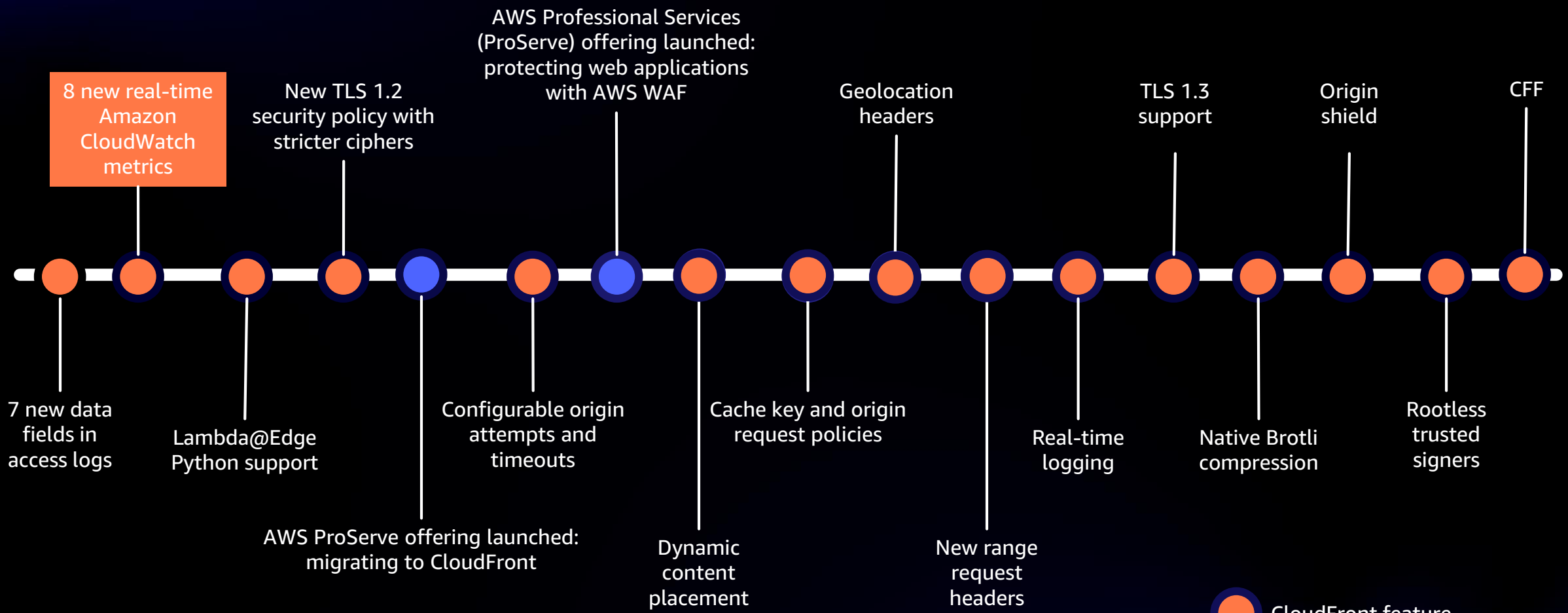
AWS global footprint



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudFront

LATEST UPDATES

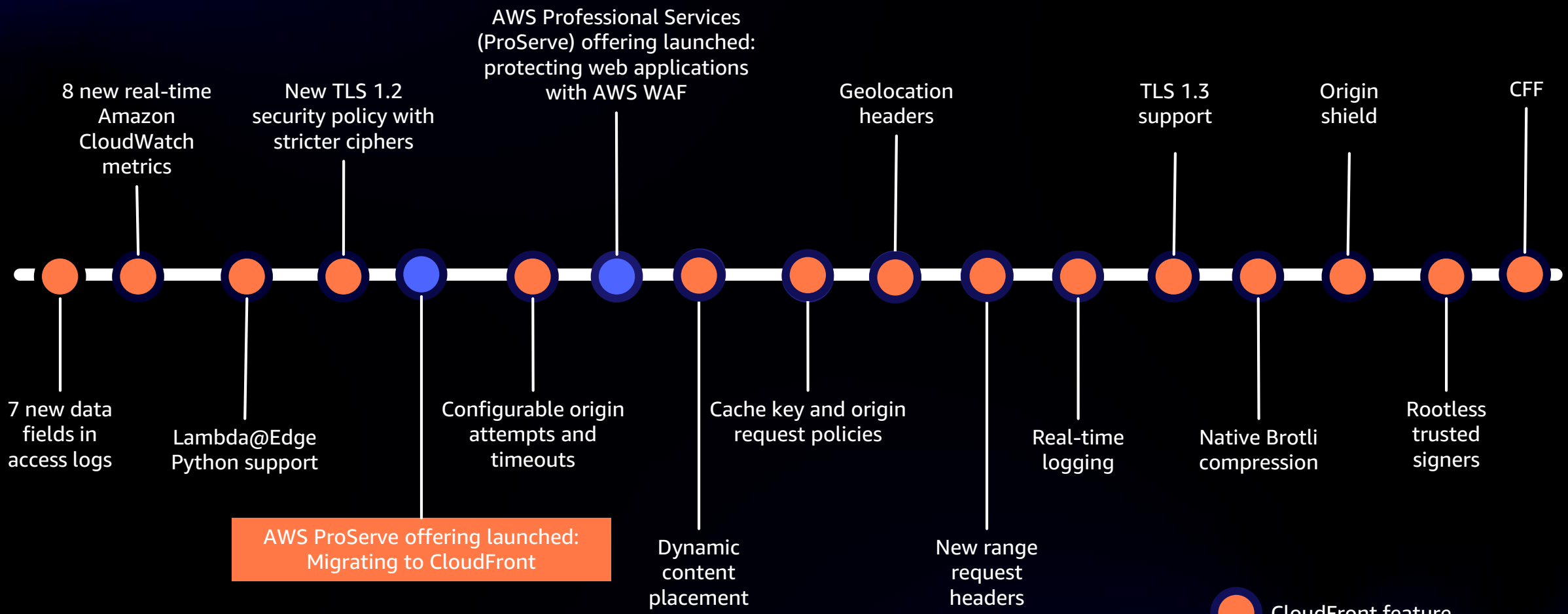


The updates are in random order

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudFront

LATEST UPDATES

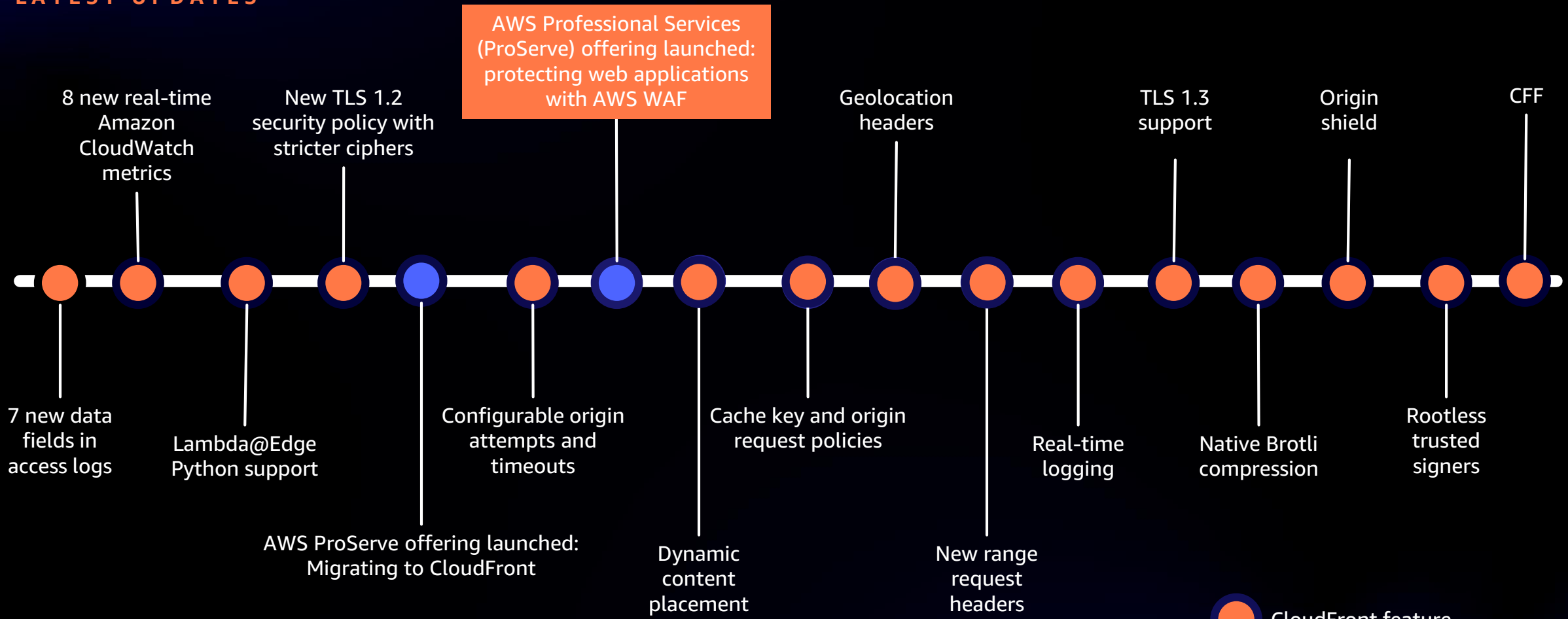


The updates are in random order

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudFront

LATEST UPDATES

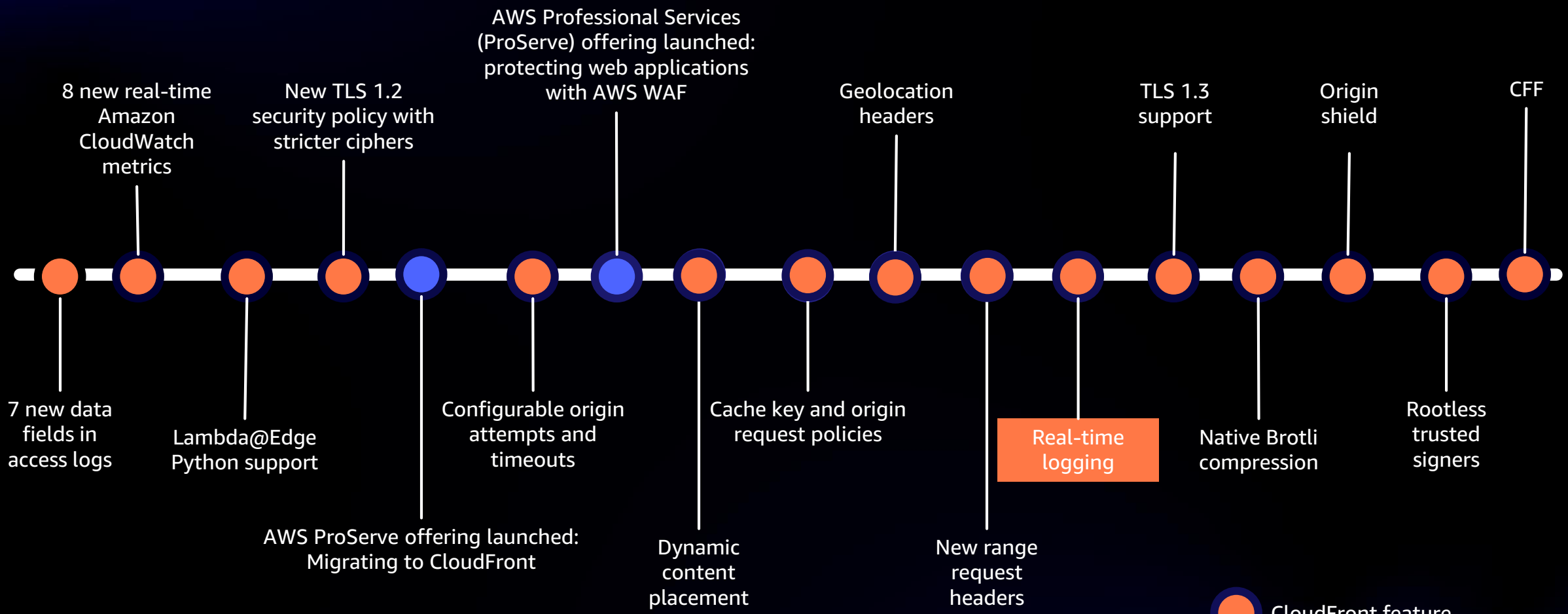


The updates are in random order

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudFront

LATEST UPDATES

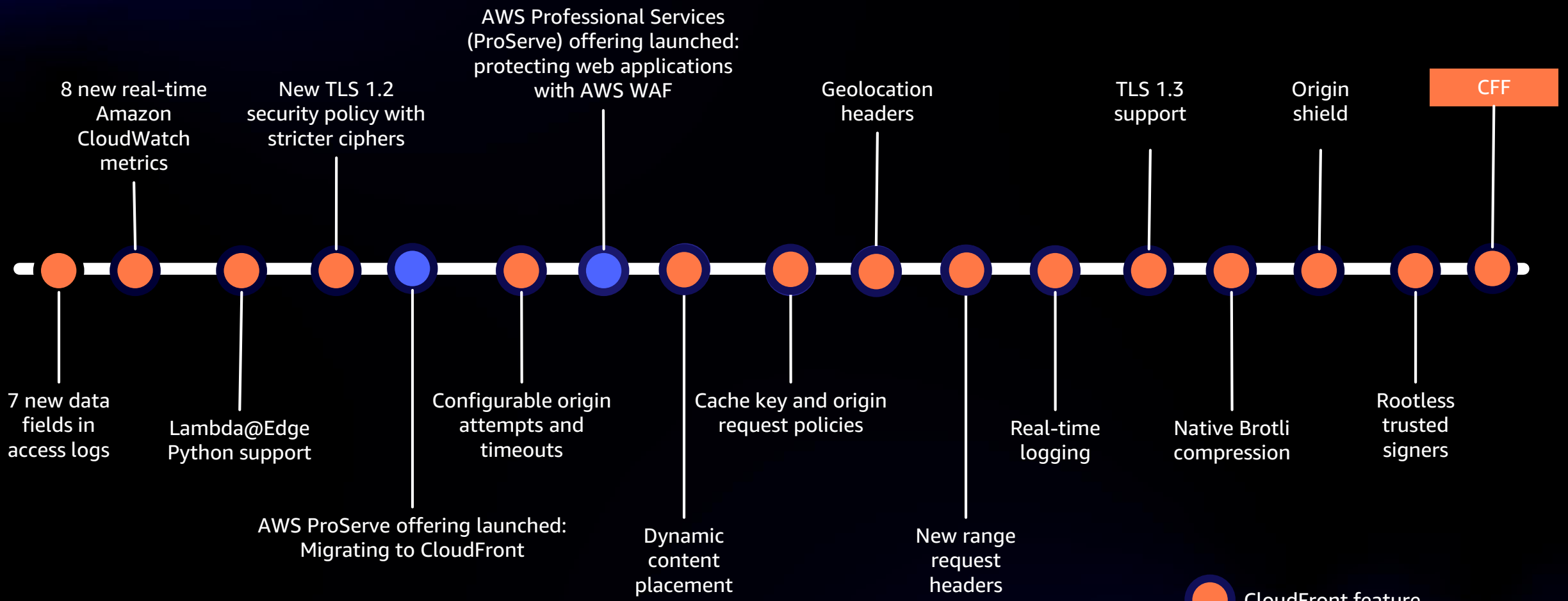


The updates are in random order

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudFront

LATEST UPDATES



The updates are in random order

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Migration challenges

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Most frequent customer challenges

WE ARE HEARING FROM CUSTOMERS

- Limited agility
  - Remove dependency of professional services
  - Empower internal builders
- How to optimize cost
  - CDN and security
  - Data Transfer Out (DTO)
- Platform standardization
  - Leverage a single UX experience
  - Reduce complexity of automation and abstraction layers
- Security flexibility – Better fit for the purpose of fraud mitigation

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Most frequent customer challenges

WE ARE HEARING FROM CUSTOMERS

- Innovation speed
  - Increase innovation speed with AWS pace of innovation
  - Better integration with AWS services
- Better insights
  - Maintain full control of the solution
  - Access real-time logs, integrate easily with existing SIEM
- Migration expertise
  - Edge specialists for builders
  - AWS Professional Services or AWS Partners

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Migration best practices

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

"AWS simplifies the work so much that you can build a solution to fit your organization without much effort if properly planned."

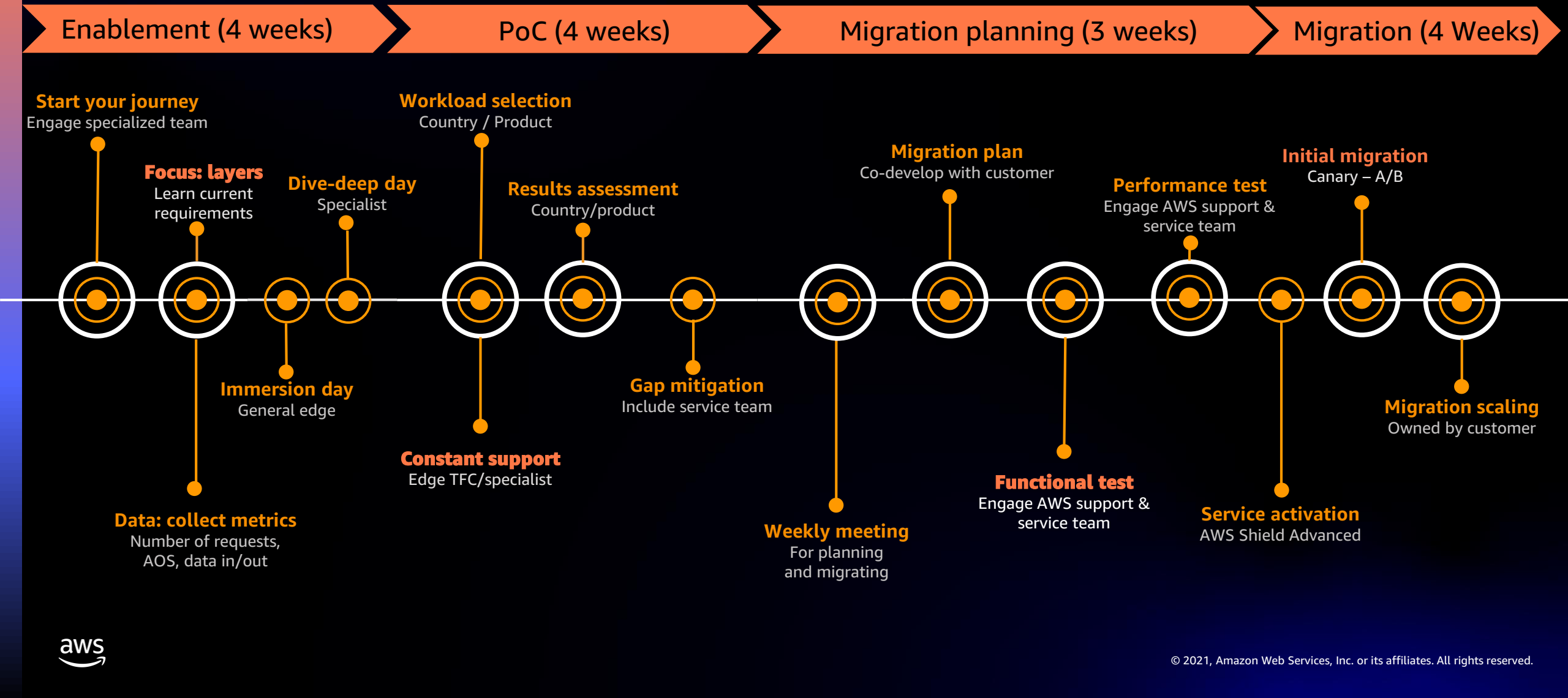
Daniel Loureiro

Lead Security Engineer – OLX Group

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Migration path

ENTERPRISE MIGRATION IN LESS THAN 4 MONTHS



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Phase: Enablement

Customers are comfortable with their current solution – and proud, as in some cases they invested years to configure and optimize it. However, customers are also concerned about low agility, high solution cost, and poor observability control.



Blockers

- Technical teams proud of their solution
- Lack of AWS experience with service updates
- Advanced bot protection
- Vendor lock-in
- Regulatory and compliance requirements
- Desire to have a fully managed solution
- Lack of service-utilization data
- Media assets management & optimization



Initiatives

- Share your current architecture
- Engage specialized edge team
- Collect service utilization data
- Take an edge services immersion day
- Take a full-day dive-deep workshop to answer all the questions



Expected outcomes

- Clear service-utilization data
- Upskilled teams
- No hard technical questions left

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Phase: PoC

The customer wants to drive a PoC, but it is hard for them to define the workload and know how to architect and how to measure success.



Blockers

- Complex architectures (want to conduct a PoC for each)
- Technical limitations like domain name utilization
- Lack of experience with collecting the right metrics
- Lack of or limited hands-on experience
- Working in isolation, no partners engaged



Initiatives

- AWS can help to define the scope and success metrics
- Engage your TAM
- Jointly architect the solution
- AWS can assist you to understand/assess the metrics
- Engage AWS service teams if needed



Expected outcomes

- Successful PoC
- Clear gaps in understanding (if any)
- Customers with hands-on experience
- Customers ready to make a decision

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Phase: Migration Planning

Customers are committed to migration. However, a more complex plan is required. They feel insecure about their technical experience and their ability to plan and run the migration.



Blockers

- Resource availability
- Technical challenges
- Remediation time



Initiatives

- Engage the customer TAM
- Schedule weekly meetings
- Assist the customer to create the migration plan
- Execute a function test
- Execute a performance test
- Activate AWS Shield Advanced (if required)



Expected outcomes

- Migration plan
- Successful function and performance tests
- Onboarded to AWS Shield Advanced

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Phase: Migration

The customer is ready, but the main concern is production impact.



Blockers

- Poor change windows
- Application not scaling
- Service limits
- Undetected issues



Initiatives

- Infrastructure Event Management (IEM) scheduling
- Create a configuration pipeline
- Define the migration team
- Schedule daily checkpoint calls
- Focus on observability



Expected outcomes

- Successful migration

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Planning your migration

5 common migration challenges to plan for *before* you start building

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Planning for your migration

QUESTIONS TO ASK

1. Where do I start?
2. Which AWS services will I need?
3. How should I design my CDN configurations?
4. How will I deploy and manage everything?
5. Where should I deploy?

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The first challenge

WHERE DO I START?

Start by taking inventory of your current CDN environment

Your goals are to

- Create an inventory of all CDN configurations that need to be migrated
- Identify logic that is reused between configurations (i.e. caching, redirects, etc.)
- Try to gauge complexity (small, medium, large)
- Keep it simple!

Configuration Name	Application Family	Environment	Complexity	Caching	Redirects
app1.example.com	App1	Prod	Medium	Y	Y
uat.app1.example.com	App1	UAT	Medium	Y	Y
api1.example.com	API	Prod	Low	N	N

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

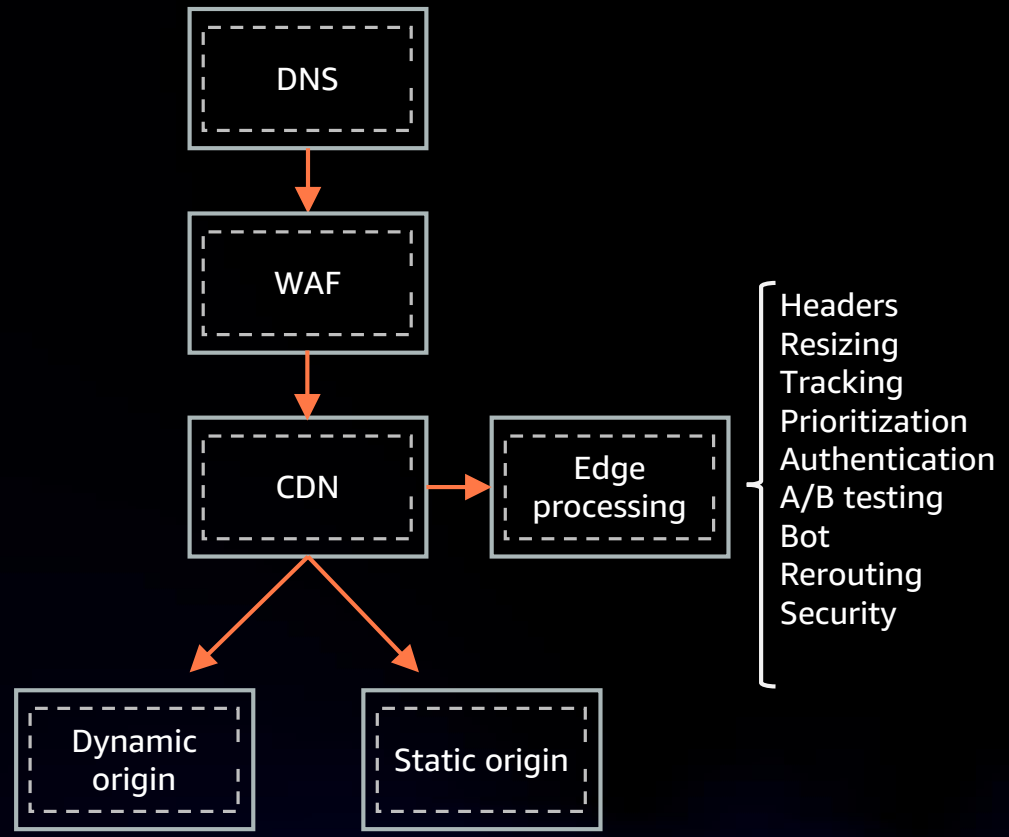
The second challenge

WHICH AWS SERVICES WILL I NEED?

Which products and support services do you use with your current CDN?

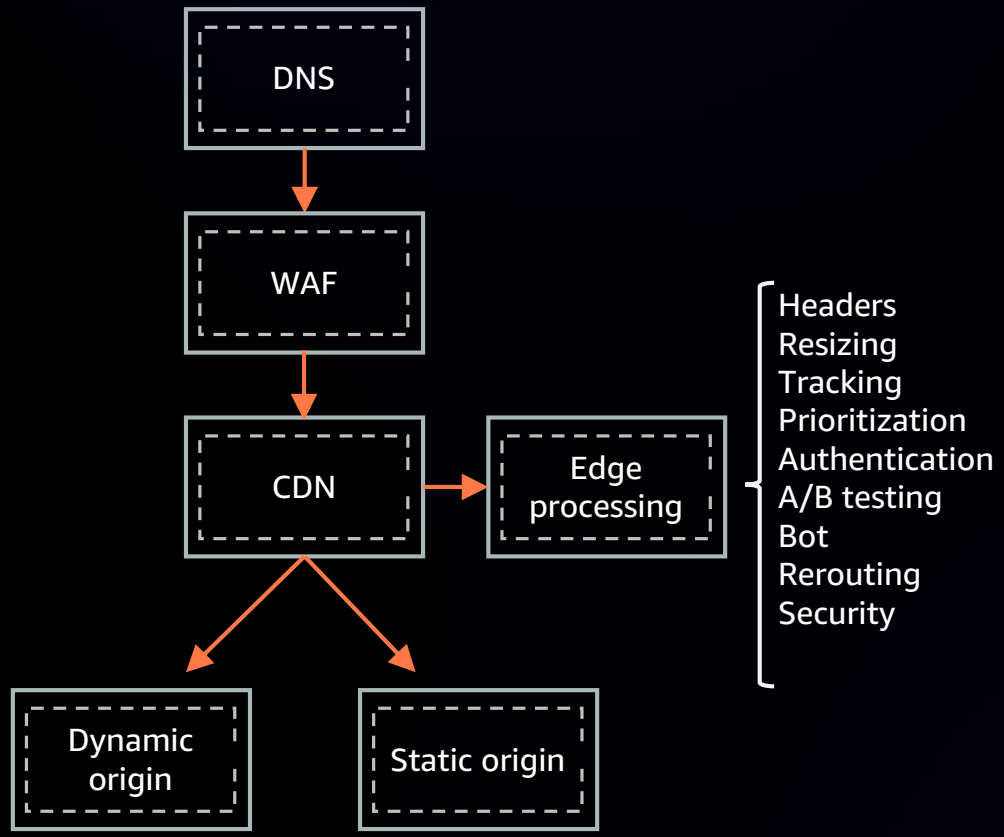
- Are there any accessory products or modules (i.e., AWS WAF or DNS)?
- How do you use reports and dashboards? How do you review logs?

Your goal: Create a reference architecture that works for all applications

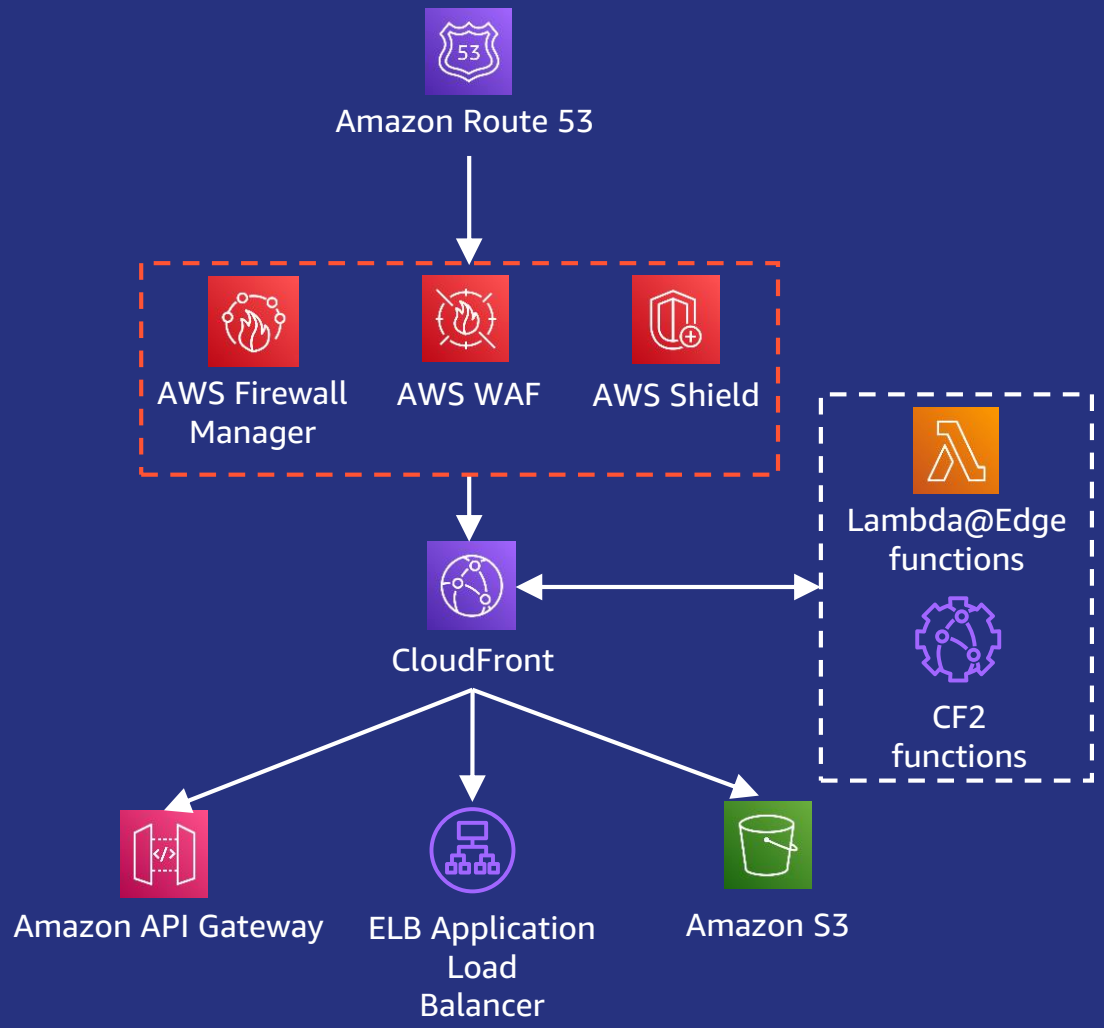


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

From this



to this



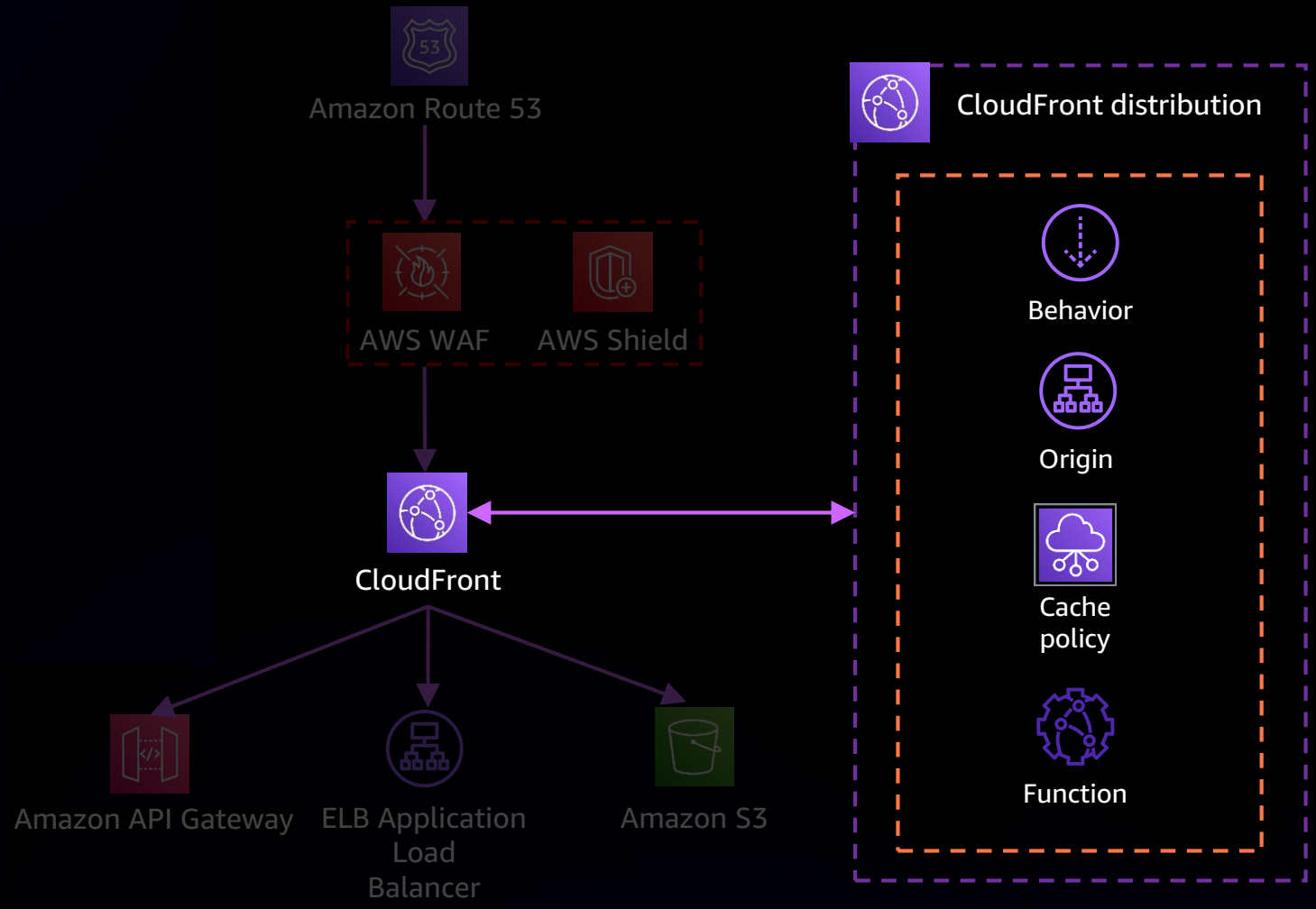
The third challenge

HOW SHOULD I DESIGN MY CDN CONFIGURATIONS?

Create a repeatable design pattern before building; understand the concepts of distributions, origins, behaviors, policies, and functions

Your goals

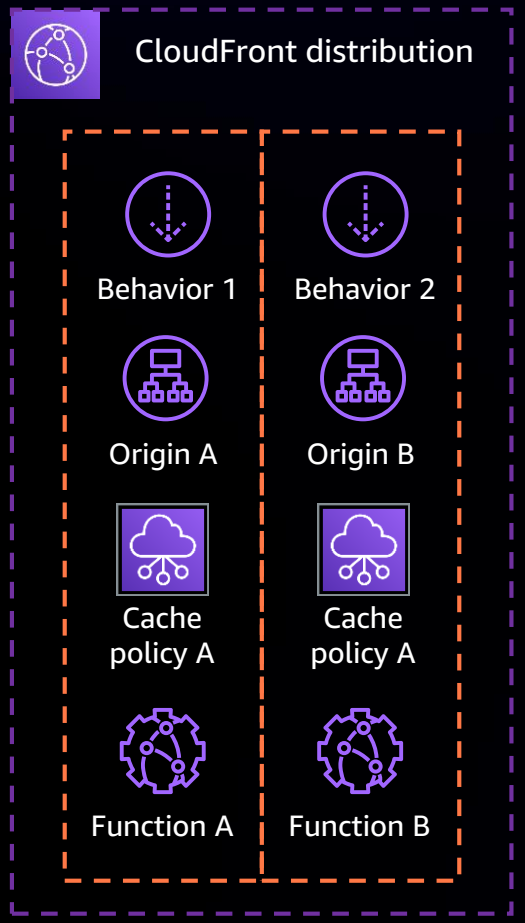
- Create a reference design that can be used for all applications
- Try to account for single uses and corner cases



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The third challenge

KEY DESIGN CONCEPTS – CLOUDFRONT COMPONENTS



Distribution

- Main CDN configuration
- Houses top-level components like hostnames, certs, and logging details

Behavior

- Handles simple logic – allows for path-based matching
- Can select origins, policies, and functions to tie to the behavior

Origin

- Origin definition
- Can define origin connection settings and custom origin headers

Policy

- Define cache TTLs and modify cache keys
- Forward or strip items to origin, and enable compression

Function

- Handles complex logic
- CloudFront Function or Lambda@Edge function
- Written in common languages like JavaScript or Python

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The third challenge

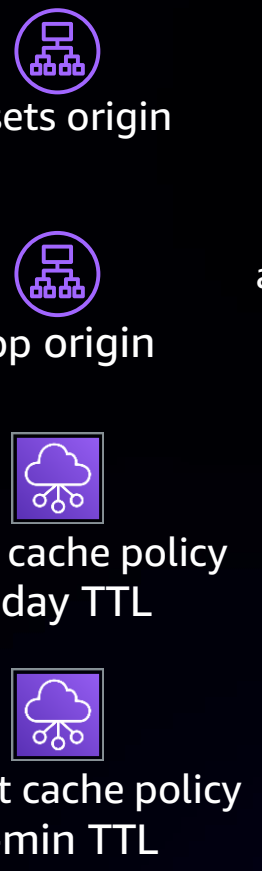
KEY DESIGN CONCEPTS – CLOUDFRONT COMPONENTS

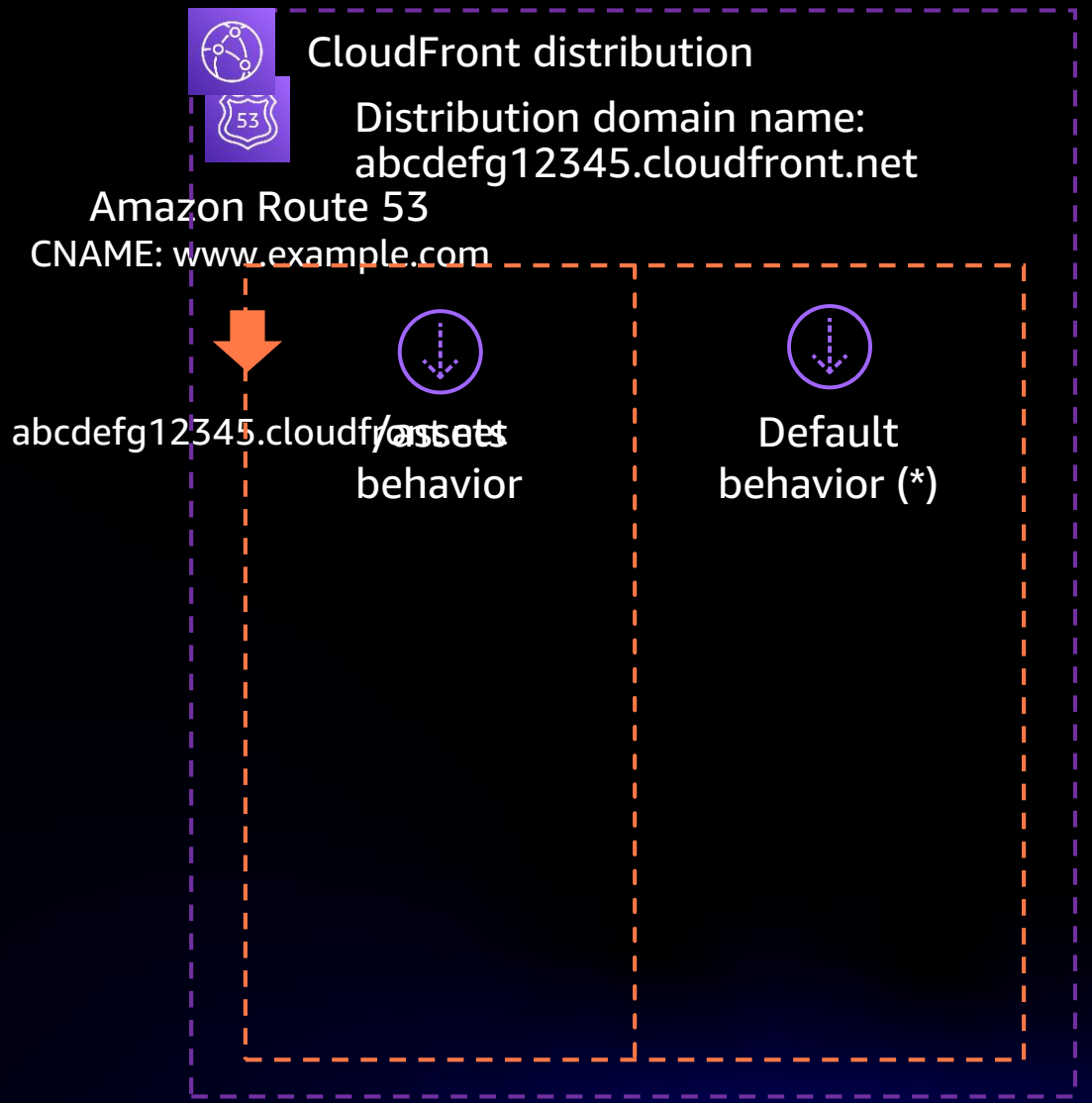
Scenario: www.example.com

Application	ALB Origin	5 min TTL
Assets	S3 Origin	1 day TTL

Steps

1. Create a distribution
2. Define origins
3. Create policies
4. Create behaviors
5. Update DNS CNAME



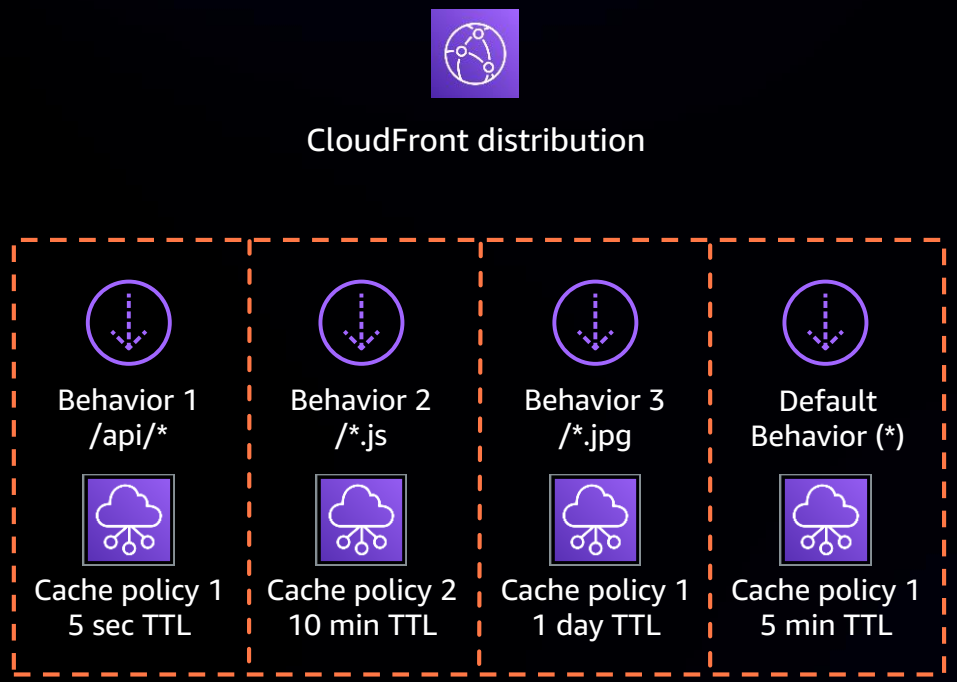


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

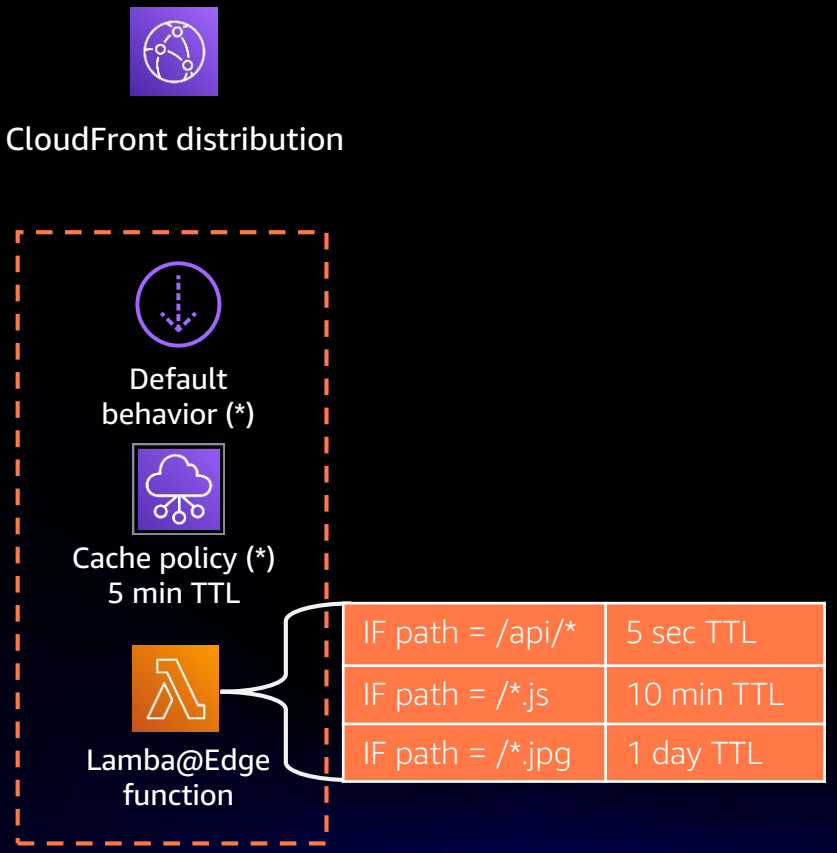
The third challenge

KEY DESIGN CONCEPTS – EXAMPLE 1: CACHE TTLS

Behavior-focused



Function-focused

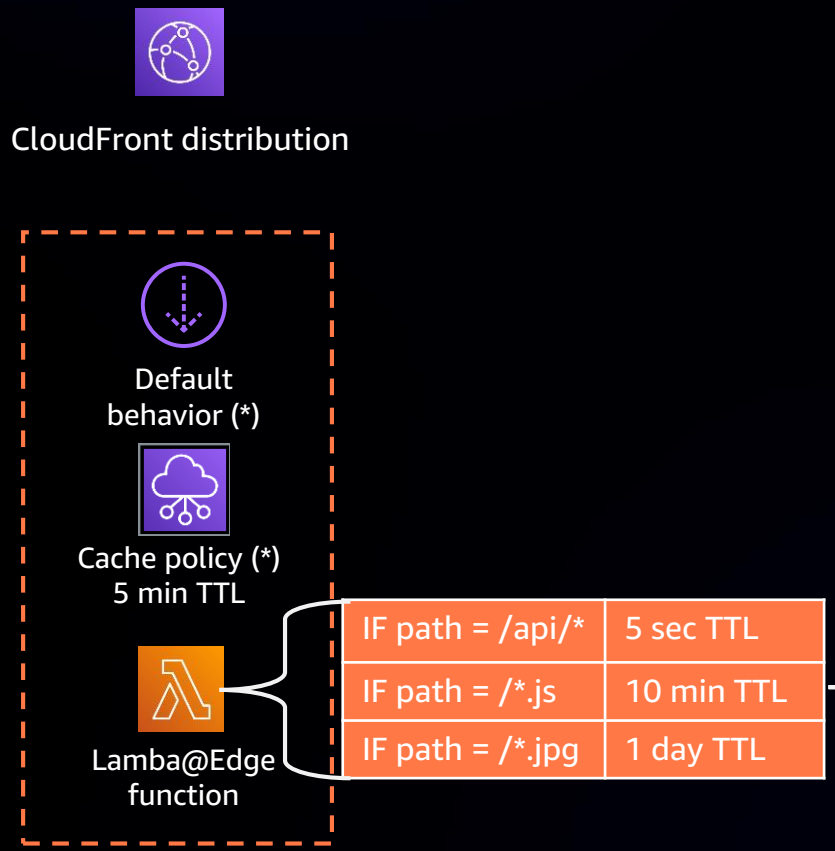


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The third challenge

KEY DESIGN CONCEPTS – EXAMPLE 1: CACHE TTLs

Function-focused




```
exports.handler = async (event, context) => {
    const request = event.Records[0].cf.request;
    const response = event.Records[0].cf.response;
    const respHeaders = response.headers;
    const cacheControlHeader = 'Cache-Control';

    if (request.uri.match(/^\/api\/.*$/)) {
        respHeaders[cacheControlHeader] = [{
            key: cacheControlHeader,
            value: 'max-age=5',
        }];
    } else if (request.uri.match(/^\/.*\.js$/)) {
        respHeaders[cacheControlHeader] = [{
            key: cacheControlHeader,
            value: 'max-age=600',
        }];
    } else if (request.uri.match(/^\/.*\.jpg$/)) {
        respHeaders[cacheControlHeader] = [{
            key: cacheControlHeader,
            value: 'max-age=86400',
        }];
    }

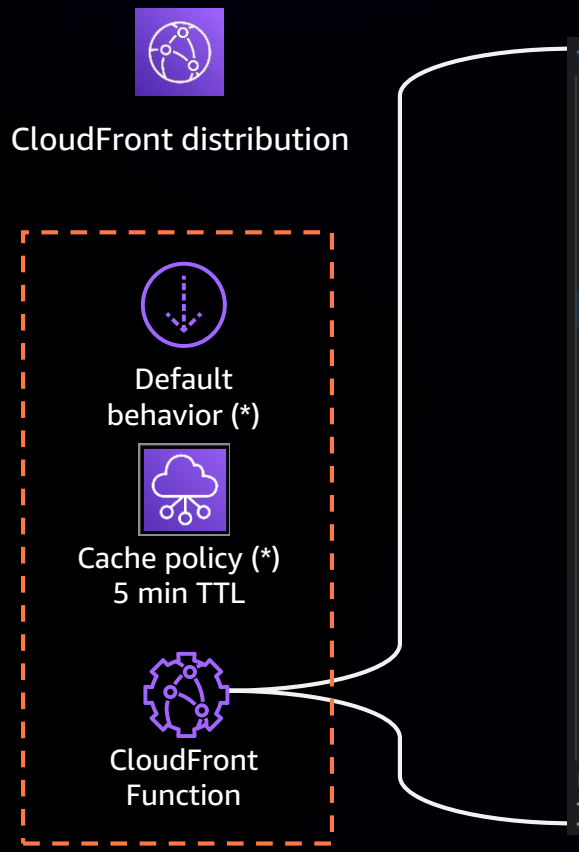
    return response;
};
```

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The third challenge

KEY DESIGN CONCEPTS – EXAMPLE 2: REDIRECTS

Function-focused




```
function handler(event) {
    var request = event.request;
    var querystring = request.querystring;
    var includeQuerystring = true                    // Include the query string in the redirect?
    var match = request.uri.match('/path')           // Redirect when this path matches
    var targetUrl = `https://www.yourtargeturl.com` // Set a redirect target URL

    function qsNormalizer(querystring) {…
    }

    var response = {
                statusCode: 301,
                statusDescription: 'Moved Permanently',
                headers:
                    { "location": { "value": targetUrl + qsNormalizer(querystring)} }
                }

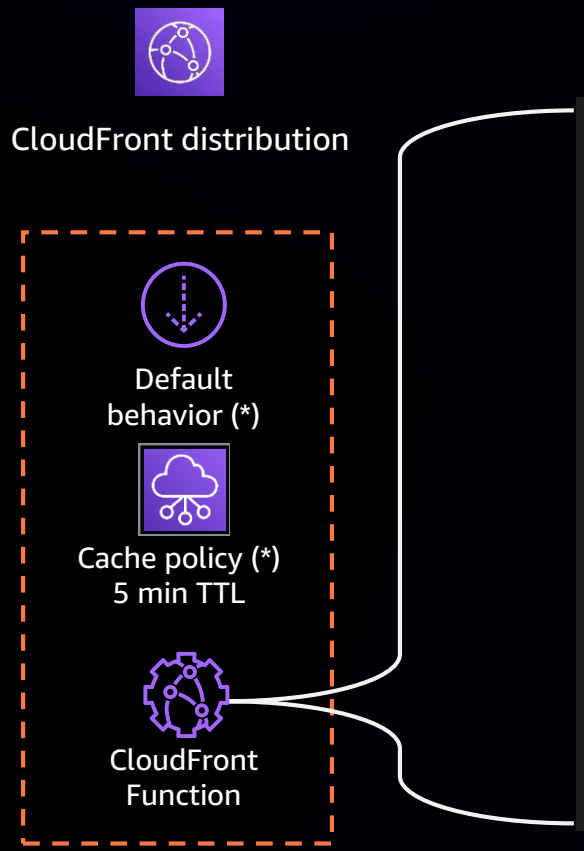
    if (match) {
        return response;
    }
return request;
}
```

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The third challenge

KEY DESIGN CONCEPTS – EXAMPLE 3: SETTING A COOKIE

Function-focused




```
function handler(event) {
    var request = event.request;
    var response = event.response;
    var reqHeaders = request.headers;
    var respCookies = response.cookies;
    var country = reqHeaders['cloudfront-viewer-country'];
    var region = reqHeaders['cloudfront-viewer-country-region'];
    var city = reqHeaders['cloudfront-viewer-city'];

    if (country) respCookies.Country = { "value": country.value};
    if (region) respCookies.State = { "value": region.value};
    if (city) respCookies.City = { "value": city.value};

    return response;
}
```

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The fourth challenge

HOW SHOULD I DEPLOY, MANAGE, AND MONITOR MY ENVIRONMENT?

1	Infrastructure as code	Use CloudFormation or Terraform
2	AWS CDK	Programmatically generate templates and configurations
3	AWS Cloud9	Cloud IDE
4	AWS CodeCommit	Use version control for templates and functions
5	Amazon OpenSearch Service	Real-time logging

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The fifth challenge

WHERE SHOULD I DEPLOY?

AWS account

Determine where to deploy

Centrally managed? Create new accounts for CloudFront

Distributed management? Deploy in your existing application accounts

Account bootstrapping

Prep your account for shared resources

Create shared resources first

- S3 buckets
- IAM roles and policies
- Setting up ACM

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Planning for your migration

WHAT WE COVERED

1

Where to start
- Take an inventory
- Know what to migrate

2

Which AWS services you will need
- Understand what you use today
- Build a reference architecture

3

How to design your CDN configurations
- Behaviors or functions
- Build a reference design

4

How to deploy your environment
- Use Infrastructure as code
- Use CloudFront metrics or Amazon OpenSearch Service

5

Which AWS accounts to use
- Consider new AWS accounts
- OR deploy with your applications

aws

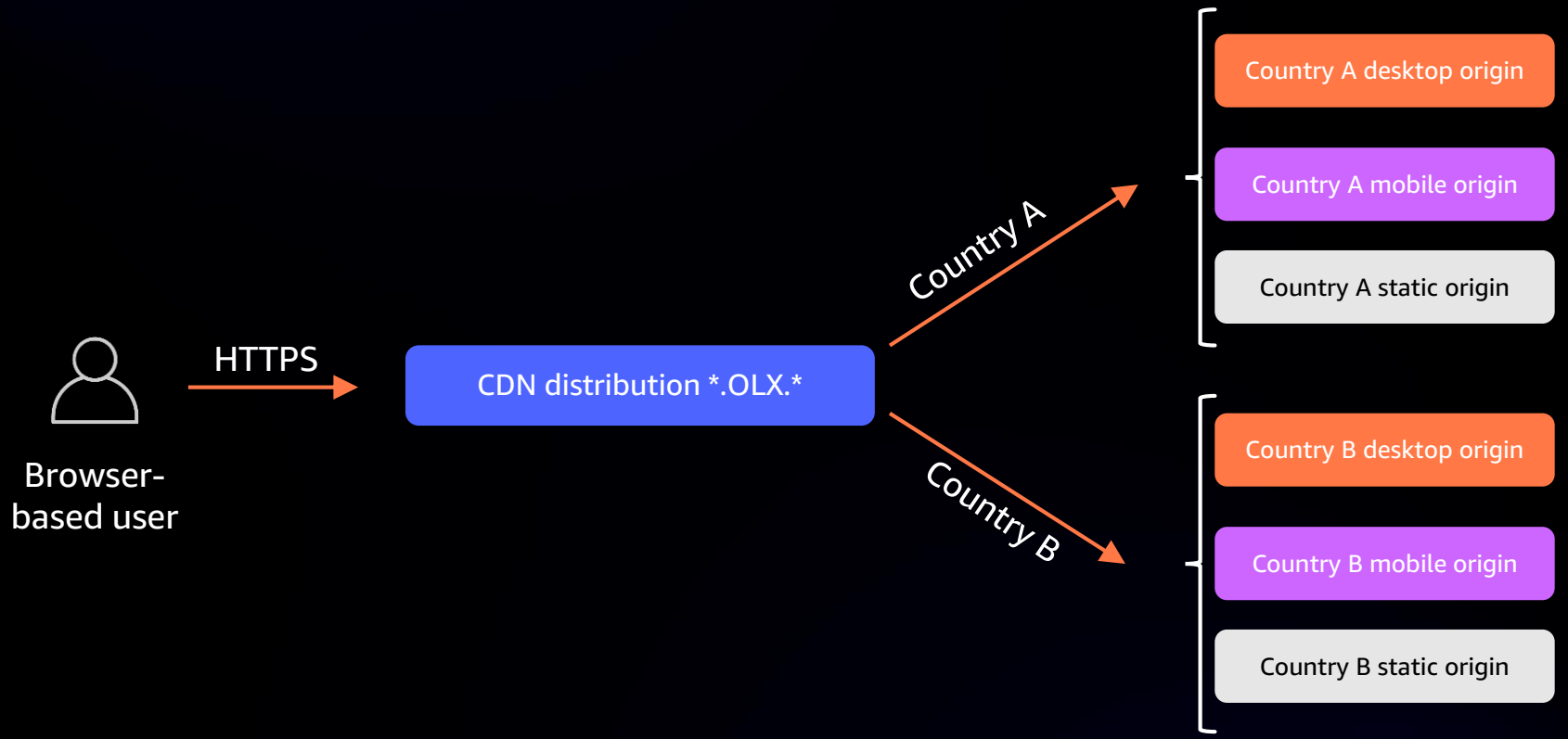
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Migration architectures

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Migration architecture

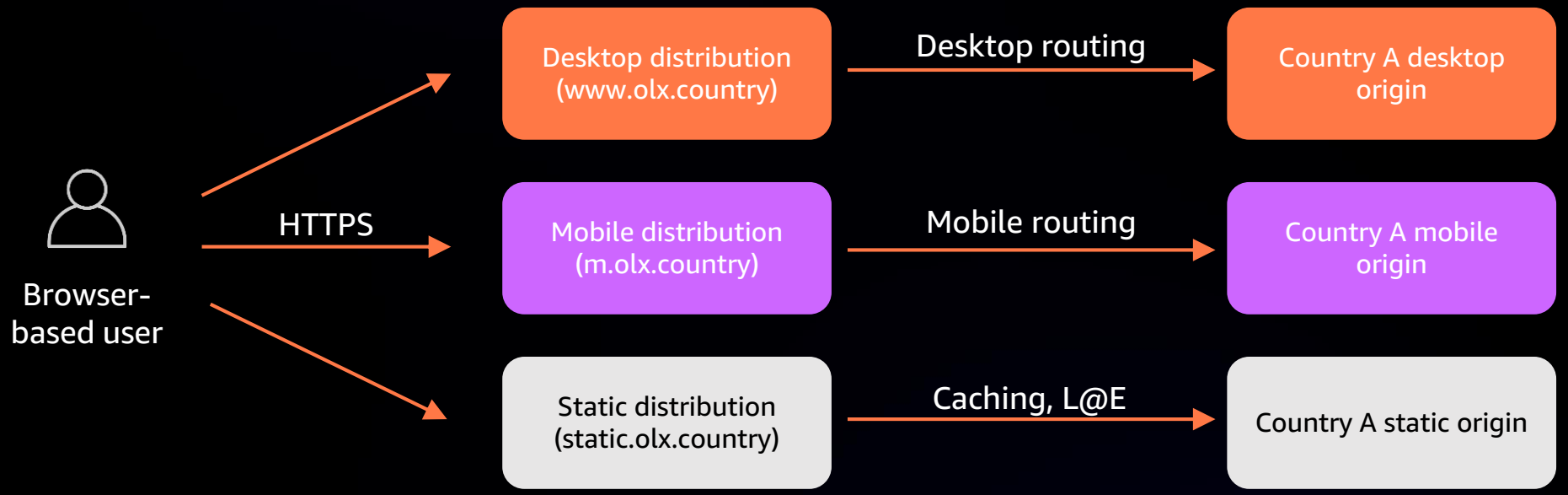
OLX GROUP EU



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Migration architecture

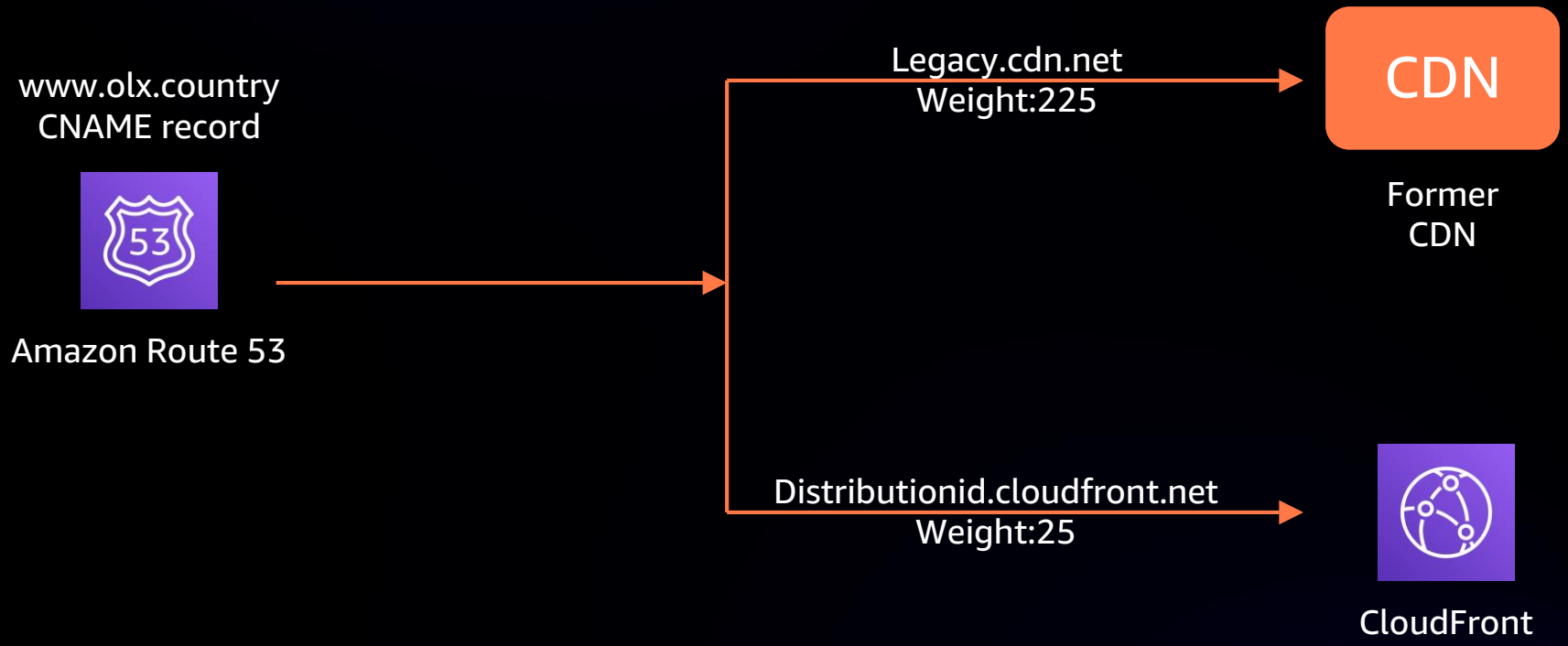
OLX GROUP EU



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Migration architecture

OLX GROUP EU



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security aspects

FRAUD

Account takeover (ATO)
Malicious access to an online account in which a fraud service or unauthorized user gains control of an account and makes unauthorized transactions

Credential cracking attacks (CCA)
An event beginning with a list of user names but without a password

Credential stuffing (CSA)
An event beginning with a list of user names and passwords collected from the dark web; then a bot automatically enters various websites simultaneously (known 0.5%–3% success rate)

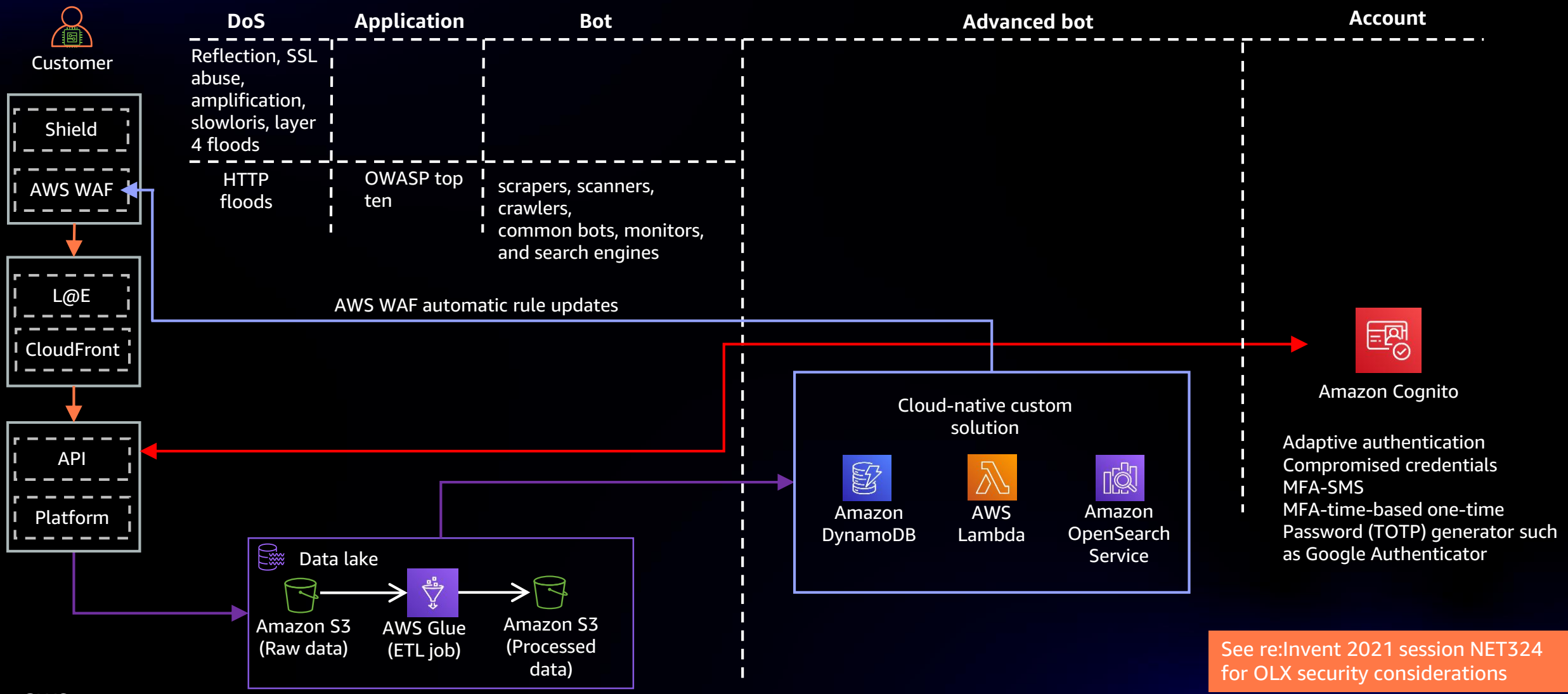
Account creation (AC)
Mass account creation using similar name, email, location (street, zip, city, country), order addresses, article data, customer account and order creation data

Content scraping (CS)
Extraction of data from a website which is collected and then exported to a format that is more useful to the user

Content spam
A term referencing a broad category of spambot or spammer postings which abuse web-based forms to post unsolicited advertisements as comments on forums, blogs, wikis, and online guest books

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

OLX security architecture



See re:Invent 2021 session NET324 for OLX security considerations

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudFront

ROBUST END-TO-END SECURITY

Encrypted connections

1. ACM integration – Certificate issuance/mgmt
2. Strict protocol enforcement TLS v1.0 to 1.3
3. Advanced ciphers with several TLS policy options
4. Field-level encryption
5. OCSP stapling
6. Session tickets
7. Perfect forward secrecy

Access control

1. Custom origin protection (header and ACL)
2. Amazon S3 origin access identity
3. Content restriction
4. Signed URL/cookies (with new key groups)
5. Geoblocking
6. Edge compute = token auth, watermarking, etc.
7. IAM/tag-based ACL to create/edit CF resources

Native integrations with AWS security services

AWS Shield Standard

Protects AWS services against common DDoS attacks

AWS WAF

Protects web applications by allowing you to write custom rules or choose managed rules from AWS or the AWS Marketplace

AWS Shield Advanced

Managed threat protection that blocks DDoS attacks, vulnerability exploitation, and bad bots

AWS Firewall Manager

Centrally configure and manage security rules across accounts and applications

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Takeaways

- Yes, it is possible to migrate in 4 months
- We can help you with experience and expertise
- You can optimize complex solutions
- Learn from our customers' migration experience
- Migrate your security while enhancing flexibility

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Hector Ibarra
hectorib@amazon.com

Jeremy Labadie
jdlab@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.