AWS
re:Invent

Agenda

The challenge: Unified customer experience, many microservices

The AWS toolbox

Common design patterns

The challenge: Competing demands

The customer wants …

Consistent authN/authZ experience

GET /orders/{orderId}

Consistent metering

DELETE /cart/{orderId}

Understandable throttling

…

service1.domain.com
service2.domain.com

OR

domain.com/orders
domain.com/cart

The developers want …

Autonomy

Agility

Easy to do things "the right way"

The security team wants …

Consistent security standards

Firewall rules

DDoS protection

Payload validation
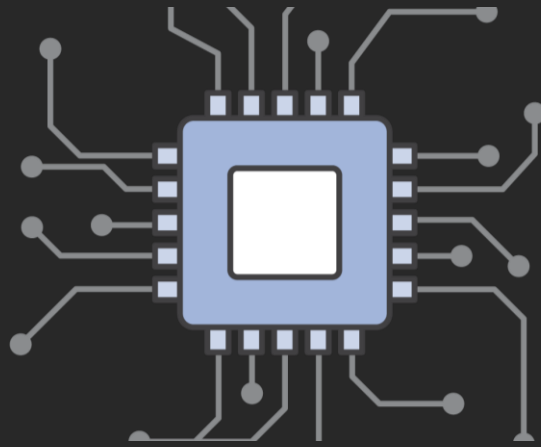
AuthN/Z integration

Logging

Visibility

AWS toolbox

aws

Amazon API Gateway

Create a unified API frontend for multiple microservices

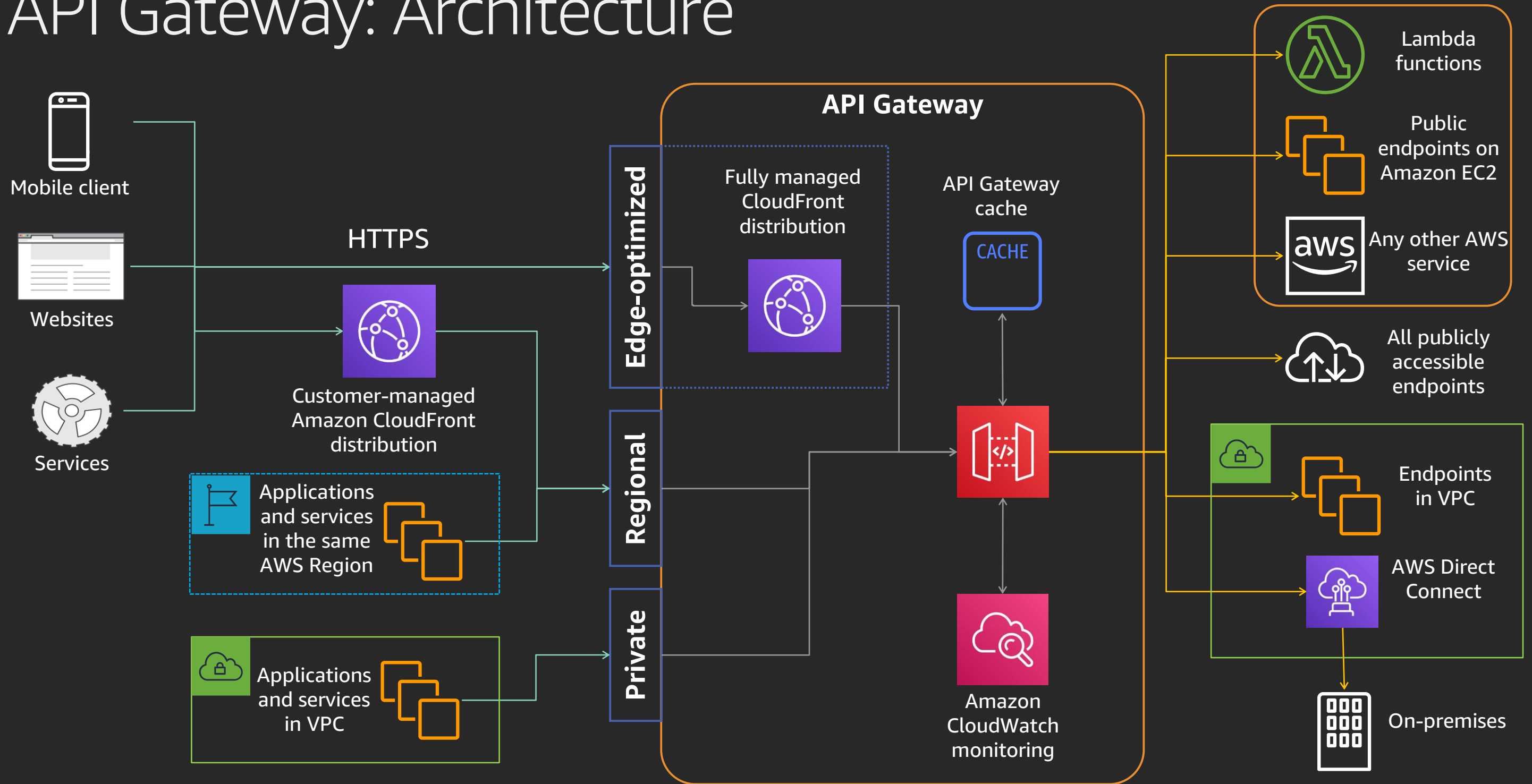DDoS protection and throttling for your backend
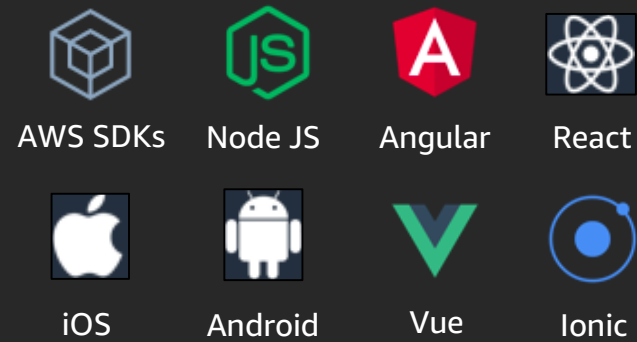

Authenticate and authorize requests to a backend

Throttle, meter, and monetize API usage by third-party developers

API Gateway: Architecture

Amazon Cognito

Flexible and scalable API and SDK support

AWS SDKs   Node JS   Angular   React

iOS   Android   Vue   Ionic

Built-in UI for applications

iOS   Android   Web   SPA

Amazon Cognito

Secure and available

Adaptive auth   Compromised password DB   MFA   99.9% SLA

Extensible AuthN and AuthZ:

AWS Lambda   Application Load Balancer   API Gateway
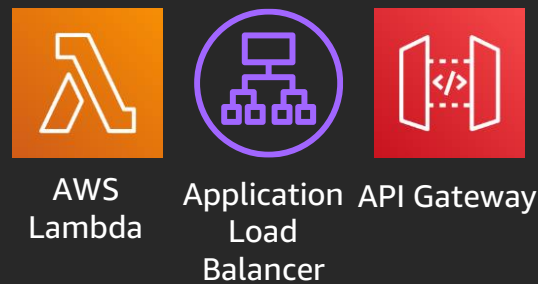
Out-of-the-box support for open standards

SAML   OAuth2   OIDC
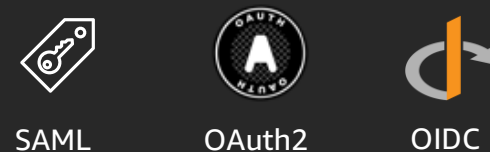
Out-of-the-box support for social federation

Google   Facebook   Amazon

AWS X-Ray

AWS X-Ray
AWS X-Ray helps you analyze and debug modern applications built using microservices and serverlesss architecture and quantify customer impact

Collect traces
Collect data about the request from each of the underlying application services it passes through

Record traces
X-Ray combines the data gathered from each service into singular units called traces

View service map
View the service map to see trace data such as latencies, HTTP statuses, and metadata for each service

Analyze issues
Drill into the service showing unusual behavior to identify the root issue

AWS Service Catalog

AWS product/service

Customer-created
AWS-based solution

AWS Marketplace
third-party products

JSON, YML, or
Terraform

✓ Constrains
✓ Security controls
✓ Parameter validation
✓ IAM assignment
✓ Tag enforcement

Admin

Standardizes best practices

AWS Service
Catalog

Amazon CloudWatch

Amazon CloudWatch
Complete visibility into your cloud resources and applications

Collect
Metrics and logs from all your AWS resources, applications, and services that run on AWS and on-premises servers

Monitor
Visualize applications and infrastructure with CloudWatch dashboards; correlate logs and metrics side by side to troubleshoot and set alerts with CloudWatch Alarms

Act
Automate response to operational changes with CloudWatch Events and Auto Scaling

Analyze
Up to 1-second metrics, extended data retention (15 months), and real-time analysis with CloudWatch Metric Math

Application Monitoring

System-wide Visibility

Resource Optimization

Unified Operational Health

Common architectures

Single AWS account

Single AWS account

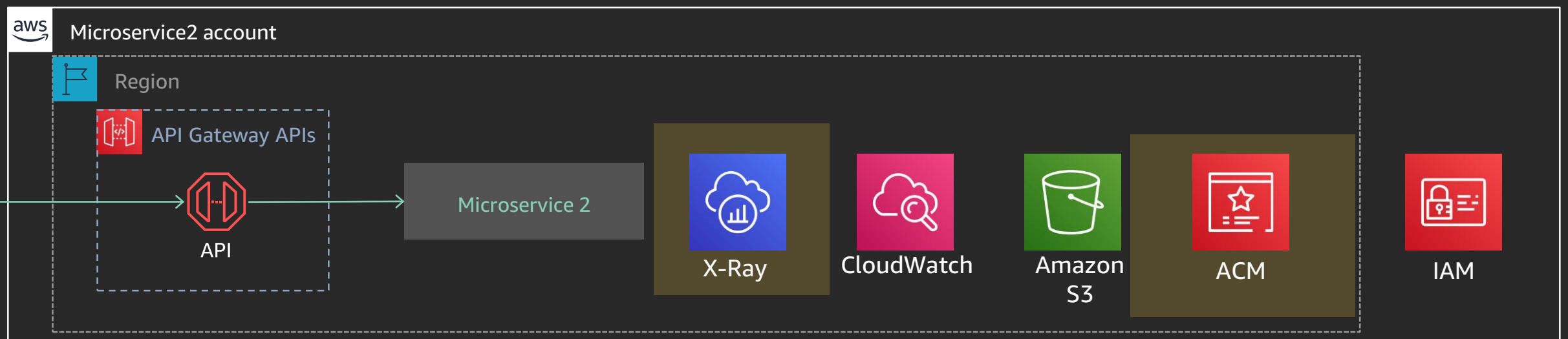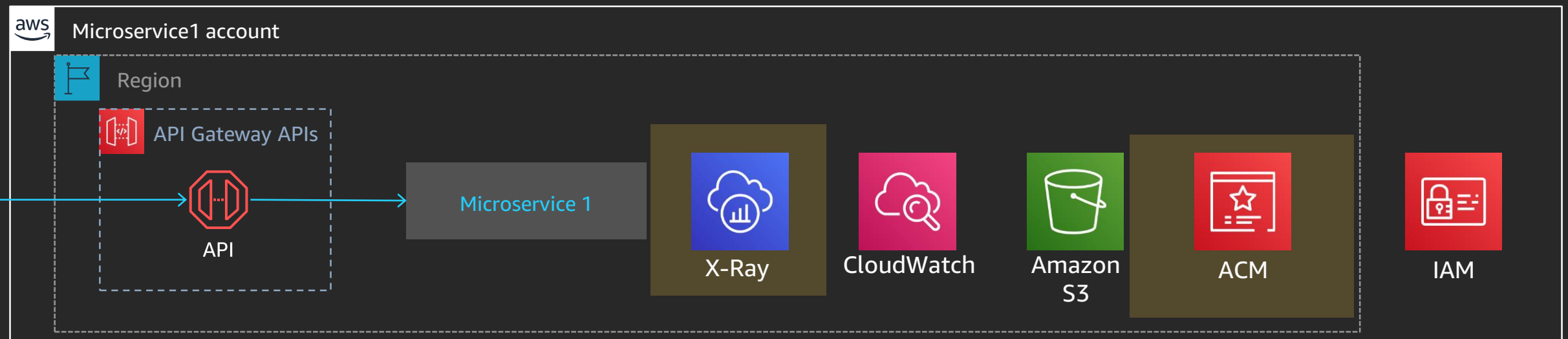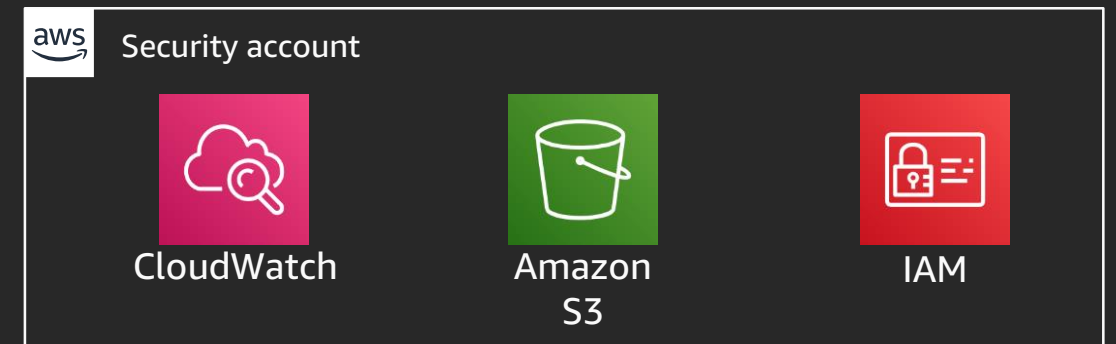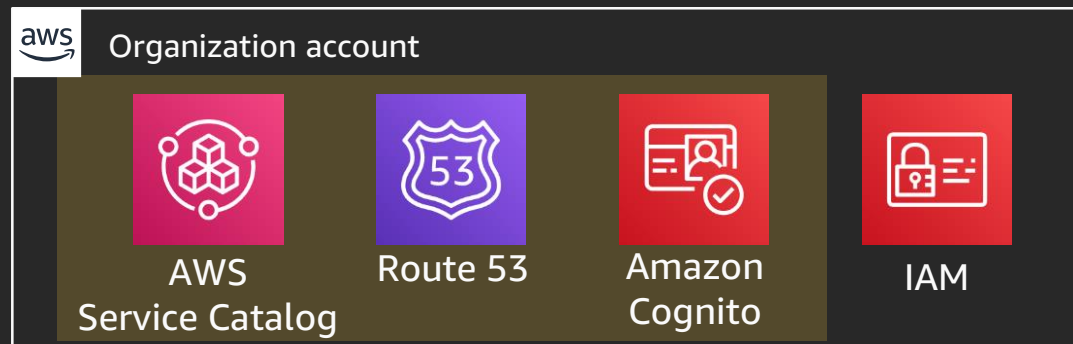## Benefits

Easier to get started

Shared networking topology

Shared API Gateway configuration

Throttling

Metering

Payload validation

AuthN/Z

Support for both subdomains and
path-based routing

Central TLS certificate management

Complete X-Ray traces

Complete CloudWatch dashboards

Challenges

Large blast radius

Shared AWS service quotas

Blended costs for shared resources

Multiple AWS accounts

Organization account

| AWS Service Catalog | Route 53 | Amazon Cognito | IAM |

Security account

| CloudWatch | Amazon S3 | IAM |

Microservice1 account

Region

API Gateway APIs

sub1.domain.com → API → Microservice 1 → X-Ray | CloudWatch | Amazon S3 | ACM | IAM

Microservice2 account

Region

API Gateway APIs

sub2.domain.com → API → Microservice 2 → X-Ray | CloudWatch | Amazon S3 | ACM | IAM

Multiple AWS accounts

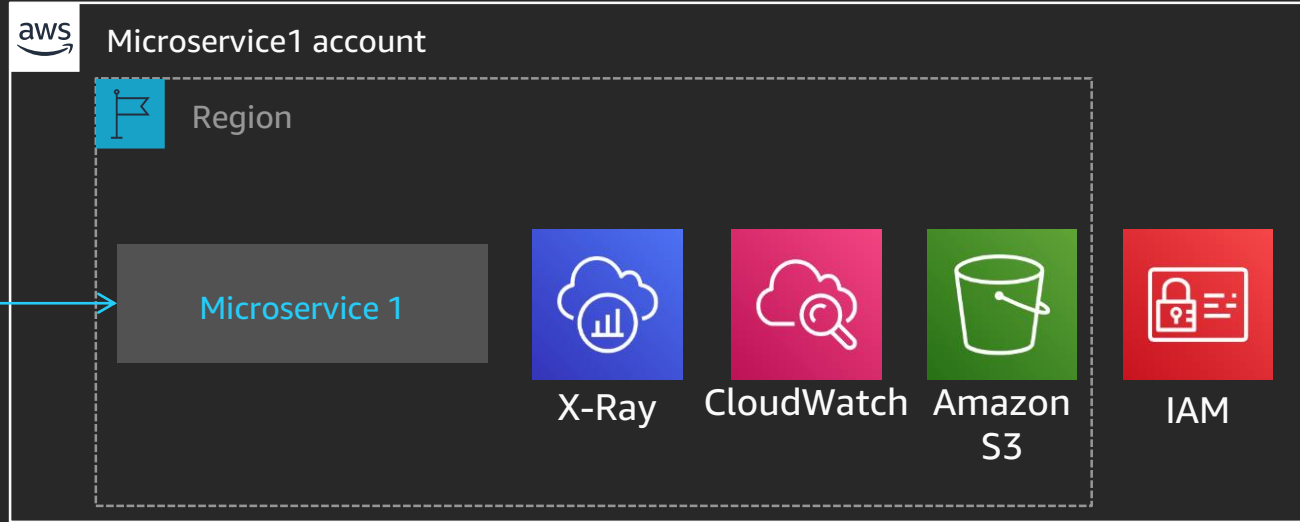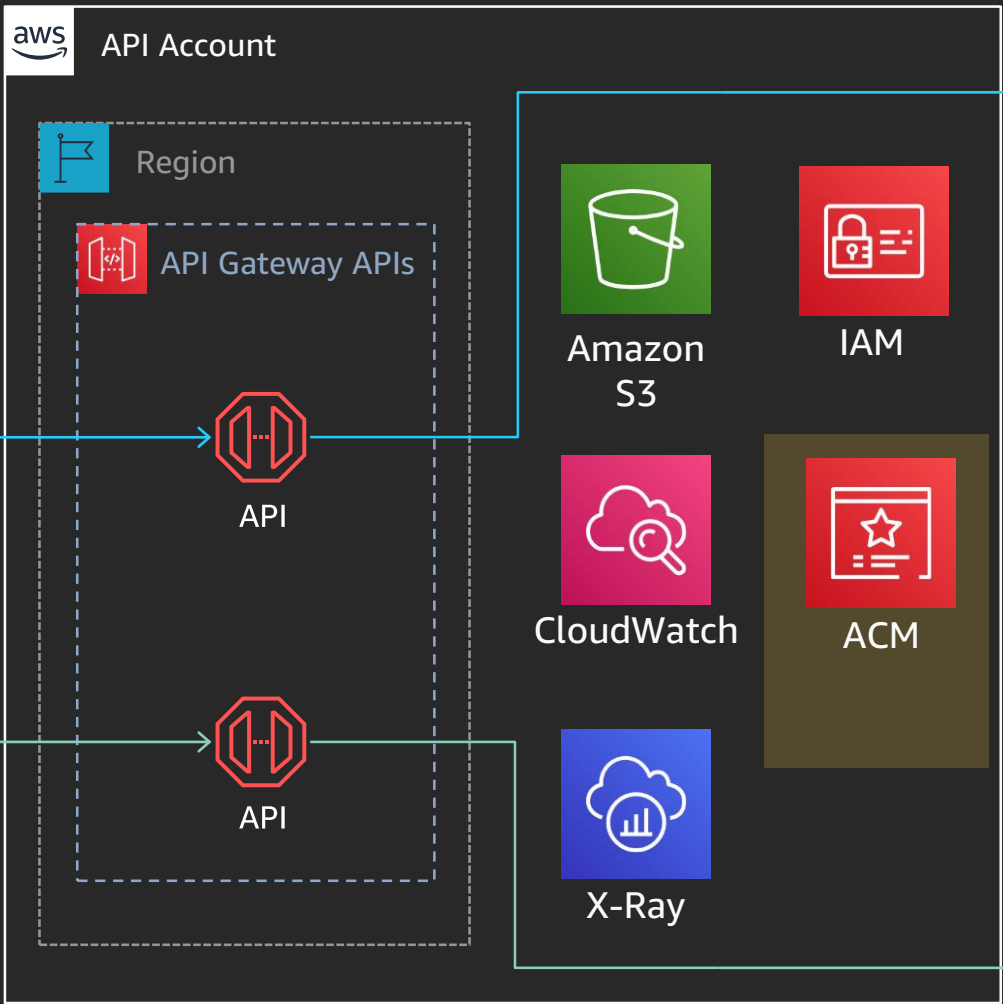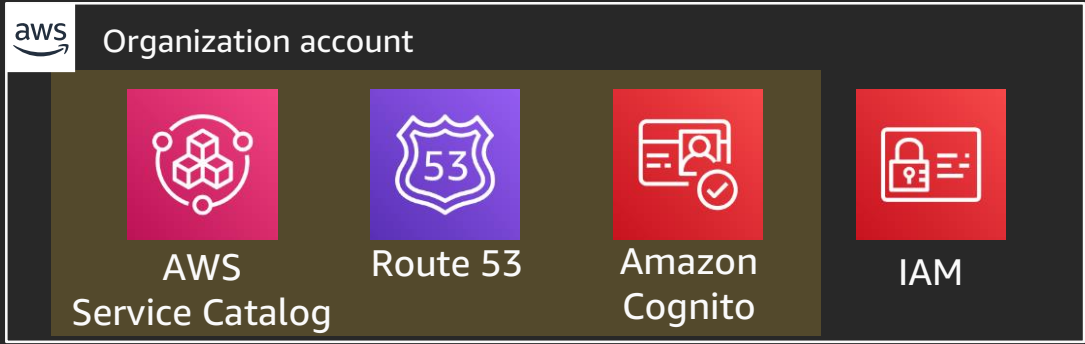## Benefits

Limited blast radius

Cost isolation

Complete X-Ray traces

Complete CloudWatch dashboard per microservice

Challenges

Multi-account strategy

Subdomain routing only (unless you add CloudFront)

Cross-account observability

Cross-service authN/Z

Cross-service API metering and throttling

Shared API Gateway account
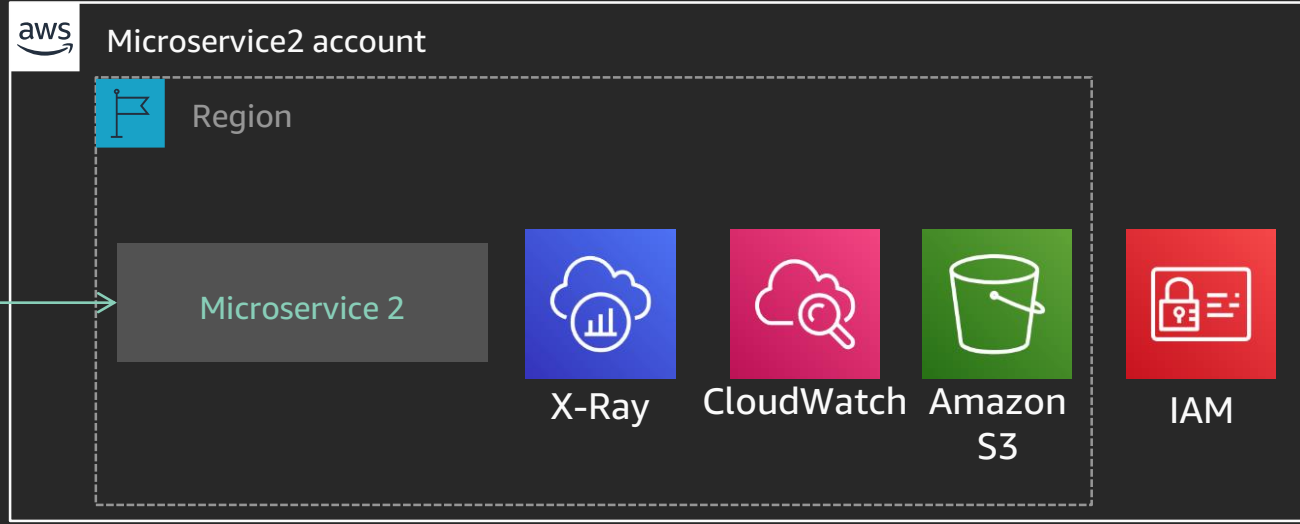
Shared API Gateway account

Benefits

Shared API Gateway configuration

Throttling

Metering

Payload validation

AuthN/Z

Support for both subdomains and path-based routing

Central TLS certificate management

Reduced blast radius

Improved cost isolation
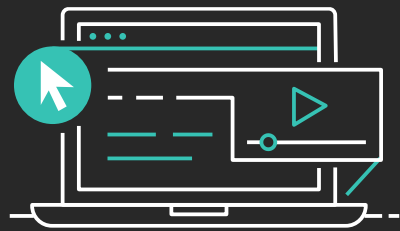
Challenges

Multi-account strategy

Full-service traces

Cross-account observability

Discussion

aws

Learn serverless with AWS Training and Certification

Resources created by the experts at AWS to help you learn modern application development

Free, on-demand courses on serverless, including

- Introduction to Serverless Development

- Getting into the Serverless Mindset

- AWS Lambda Foundations

- Amazon API Gateway for Serverless Applications

- Amazon DynamoDB for Serverless Architectures
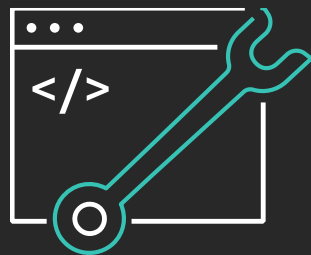
Additional digital and classroom trainings cover modern application development and computing

Visit the Learning Library at https://aws.training

aws training and certification

Thank you!

AWS re:Invent

aws

Please complete the session survey in the mobile app.