

AWS  
re:Invent

WIN317

# Demystifying identity, AuthN, and AuthZ for .NET apps on AWS

## **Justin Yancey**

Senior Systems Dev Engineer  
Amazon Web Services

## **Kevin Higgins**

Senior Cloud Infrastructure Architect  
Amazon Web Services

# Agenda

User authentication fundamentals

How to approach .NET authentication on AWS

Learn how customers are implementing identity management for their serverless apps using

- Amazon Cognito user pools
- Amazon Cognito identity pools
- Application Load Balancers
- Amazon API Gateway
- AWS Lambda
- AWS Identity and Access Management (IAM)

# Principle

## **Federate everything**

Every. Single. App.

## Single sign-on standards

OpenID Connect and OAuth

SAML

## Make it easy to do the right thing

... and difficult to do it wrong

# Multiple approaches/choices

## No-infrastructure compute

- Lambda (serverless)
- AWS Fargate (containers on Amazon ECS)

## No-infrastructure storage

- Amazon S3
- Amazon DynamoDB

## Identity management (authentication)

- Amazon Cognito
- Third-party IdP
- Build your own . . .

# Amazon Cognito

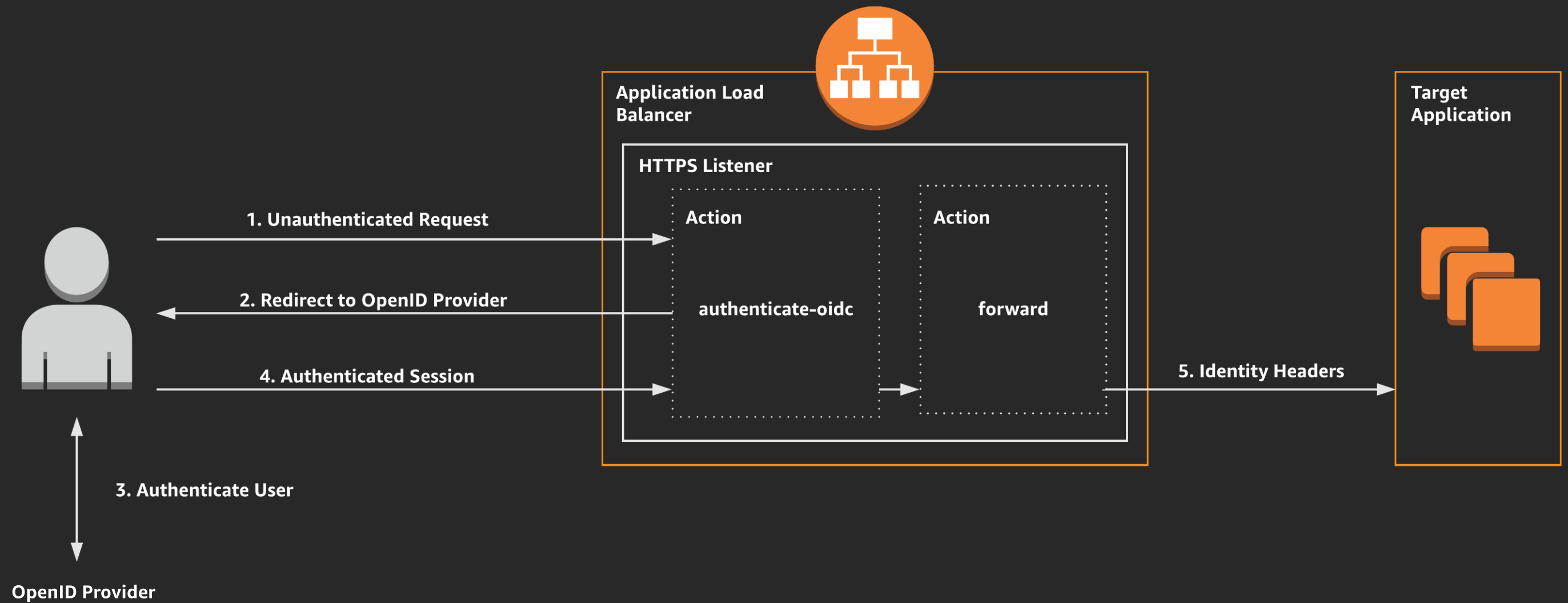
## Use API Gateway w/integrated Amazon Cognito authorization

- Pros: Can vary authorization by request type (GET/PUT/POST/etc.)
- Cons: Need additional service, complicates service-to-service auth

## Use ALB Amazon Cognito authorization feature

- Pros: It's a feature of ALB
- Cons: Authorization is per-path only (e.g., per microservice)

# ALB authentication



# Thank you!

**Justin Yancey**

yancej@amazon.com

**Kevin Higgins**

kevhiggi@amazon.com





Please complete the session survey in the mobile app.