

Securing Our Application with Azure AD B2C



Mark Heath

MICROSOFT MVP

@mark_heath www.markheath.net



Overview



User identity

- Authentication – who are they?
- Authorization – what can they do?

Serverless authentication

- Third party identity providers

Azure AD B2C

- Issues access tokens
- Verified by Azure Functions

“Who’s Playing” demo app

- Enable “Easy Auth”



The Story so Far

Email containing
personalized URL



Single Page
Application
(SPA)



Event Admin
Page



Get Event
Azure
Function



Update
Event
Azure
Function



Create Event
Azure
Function



Login
Function?



Database
(Azure Table
Storage)



User Details
Database



The Story so Far

Email containing
personalized URL



Single Page
Application
(SPA)



Event Admin
Page



Get Event
Azure
Function



Update
Event
Azure
Function



Create Event
Azure
Function

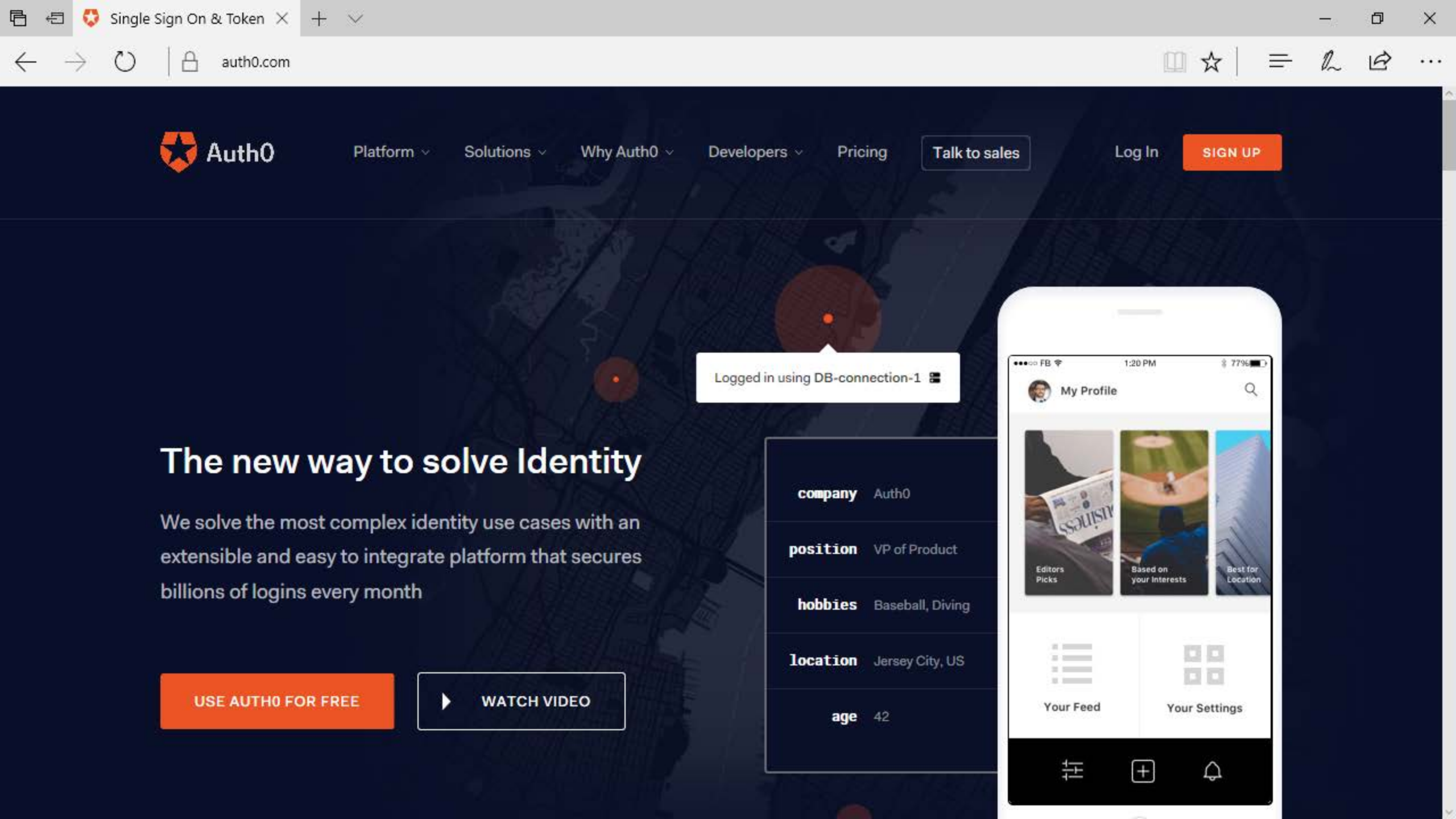


Auth as a
Service



Database
(Azure Table
Storage)





Platform ▾

Solutions ▾

Why Auth0 ▾

Developers ▾

Pricing

Talk to sales

Log In

SIGN UP

The new way to solve Identity

We solve the most complex identity use cases with an extensible and easy to integrate platform that secures billions of logins every month

USE AUTH0 FOR FREE



WATCH VIDEO

Logged in using DB-connection-1

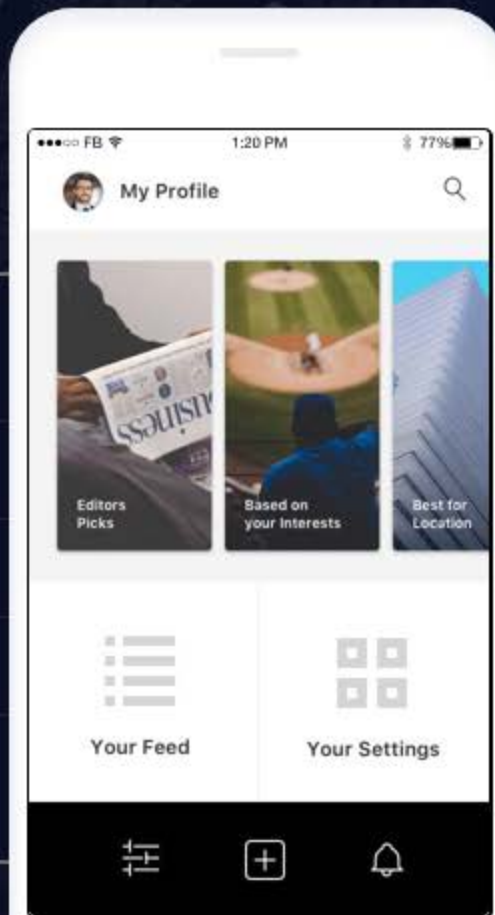
company Auth0

position VP of Product

hobbies Baseball, Diving

location Jersey City, US

age 42

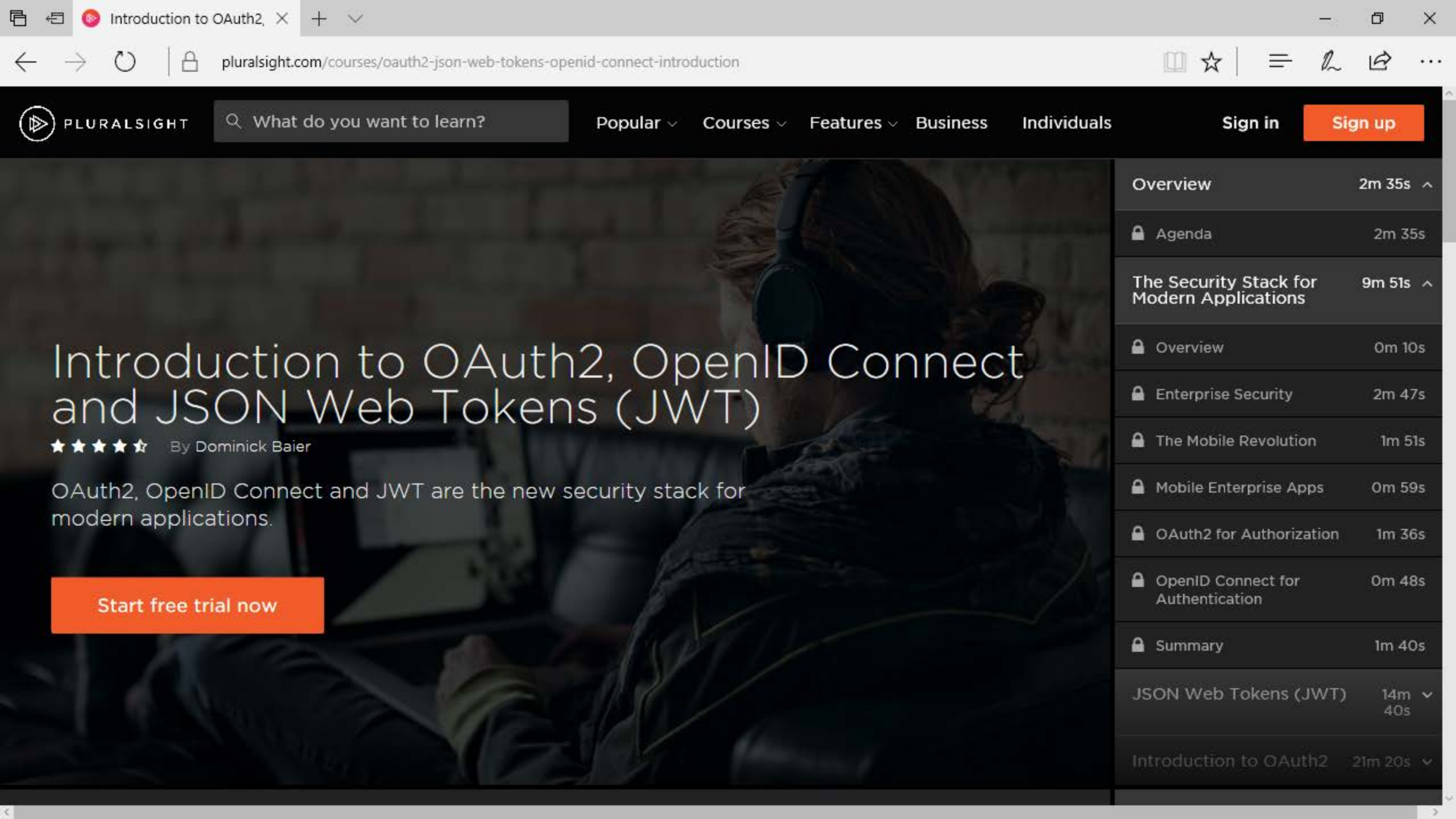


OAuth 2.0

OpenID

JSON Web
Tokens





PLURALSIGHT

What do you want to learn?

Popular v

Courses v

Features v

Business

Individuals

Sign in

Sign up

Introduction to OAuth2, OpenID Connect and JSON Web Tokens (JWT)

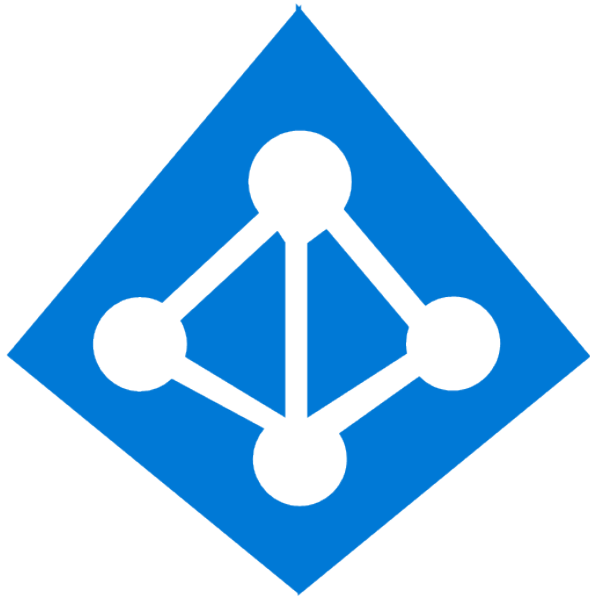
★★★★★ By Dominick Baier

OAuth2, OpenID Connect and JWT are the new security stack for modern applications.

Start free trial now

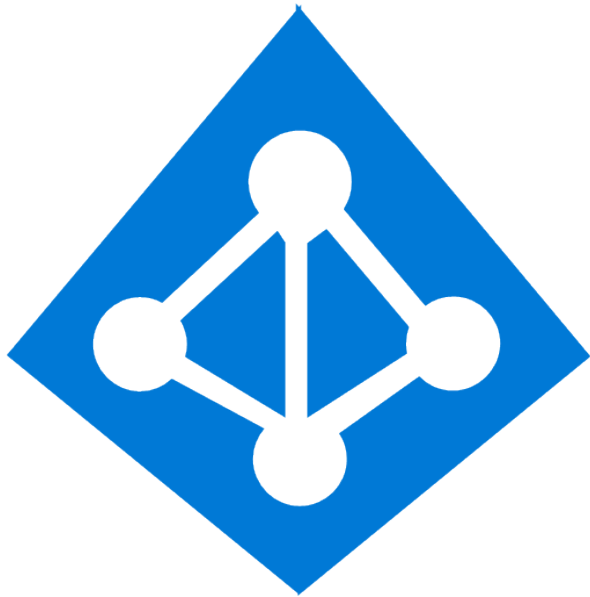
Overview	2m 35s ^
🔒 Agenda	2m 35s
The Security Stack for Modern Applications	9m 51s ^
🔒 Overview	0m 10s
🔒 Enterprise Security	2m 47s
🔒 The Mobile Revolution	1m 51s
🔒 Mobile Enterprise Apps	0m 59s
🔒 OAuth2 for Authorization	1m 36s
🔒 OpenID Connect for Authentication	0m 48s
🔒 Summary	1m 40s
JSON Web Tokens (JWT)	14m 40s v
Introduction to OAuth2	21m 20s v

Identity Providers in Azure



Azure Active Directory B2C
- Business to Consumer

Azure Active Directory B2C



User and login management

- Minimize the code you need to write

Social identity provider integration

Customizable

Serverless pricing model

Integrating AD B2C with Serverless Apps



Client side

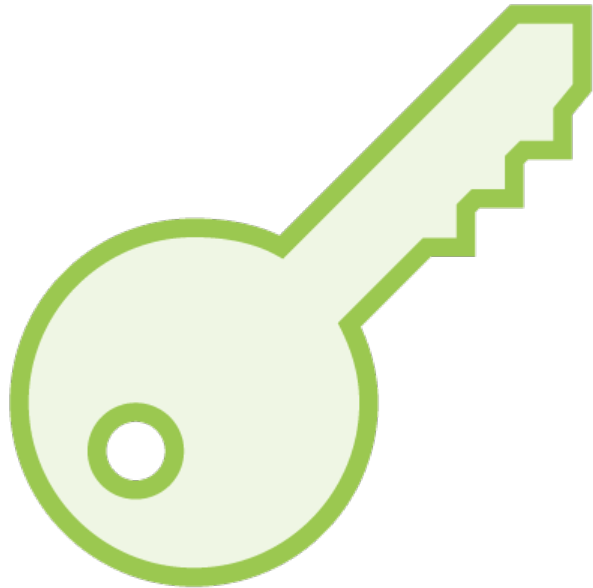
- Manage tokens issued by AD B2C

Server side

- Validate tokens

Sample implementations

Easy Auth and Azure Functions



Requires authentication on every incoming request

- Redirects unauthorized users to login

Whole site is protected

- admin.whosplaying.eu
- www.whosplaying.eu

Configuring Easy Auth

- Enable it for the Function App
- Use Azure Function proxies for HTML

Demo



Creating a new AD B2C tenant

- Create a sign-up & sign-in policy



Demo



Secure Azure Function App with AD B2C

- Use App Service “Easy Auth” feature
- Use Azure Functions proxies
- Admin site requires login
- Securely pass JWT to Azure Functions



Recap: Securing Azure Functions with AD B2C



Create Azure B2C Tenant

- Create a sign-up or sign-in policy
- Create an AD B2C application

Set up Azure Functions proxies

- For static HTML, CSS & JavaScript

Enable EasyAuth

- Connect it to AD B2C
- Application ID, and policy URL

Inspect Azure Function request headers

- Access the JSON Web Token contents



Use the JWT contents to
perform authorization



Taking It Further

Customize the AD B2C Login UI

Enable social logins

Enable two factor authentication

Use JWT to make authorization decisions



Summary



Securing serverless applications

- Don't roll your own security
- Build on established standards

Use a 3rd party authentication service

- Azure AD B2C
- Others are available (e.g. Auth0)
- Manages logins and passwords for you

Who's Playing demo app

- Secured with AD B2C and Easy Auth

Microsoft Auth Samples

- <https://github.com/Azure-Samples>



Automating deployment

