

# Modern Identity for Developers

Ronny Hansen

Cloud Solution Architect OCP

[Ronny.Hansen@microsoft.com](mailto:Ronny.Hansen@microsoft.com)



Sander van den Hoven

Cloud Solution Architect ISV OCP

[sandervd@microsoft.com](mailto:sandervd@microsoft.com)



# Identity History – Legacy identity

- Windows Applications
  - Local windows accounts
  - Domain user accounts
  - Applications may use windows accounts or some other solution (the apps database or 3<sup>rd</sup> party like LDAP)
- Web applications
  - Integrated with Windows Domain User accounts (local network)
  - Have their own Identity store (username and password in a database)
    - Session cookie stored their login state
    - Works with a web front end – REST API's cannot read the cookie
  - 3rd party (proprietary, X.500, LDAP, + +)
- Mobile applications and Web Applications using API's

# Identity History – Modern Identity

- Modern protocols
  - Security Assertion Markup Language (SAML)
  - OAuth 2.0 – Authorization
  - OpenID Connect – Authentication (a layer on top of OAuth 2.0)
- Identity Providers
  - Common for these protocols is that you have ONE Identity Provider (IdP) to handle the credentials and logins, no need to create accounts everywhere
- Can I run my own Identity Provider ?
  - Yes, for example IdentityServer4
    - IdentityServer is a free, open source OpenID Connect and OAuth 2.0 framework for ASP.NET Core.
- Considerations
  - Scaling and SLA
  - Security (Securing your backend services, adding MFA, AI to detect security issues, ++)
  - Cost for hosting (compute + storage), scaling and operations/backup/++

# ';--have i been pwned?

Check if you have an account that has been compromised in a data breach

 pwned?



Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

[Why 1Password?](#)

437

pwned websites

9,553,940,129

pwned accounts

111,790

pastes

134,921,274

paste accounts

## Largest breaches



772,904,991 [Collection #1 accounts](#)



763,117,241 [Verifications.io accounts](#)



711,477,622 [Onliner Spambot accounts](#)



622,161,052 [Data Enrichment Exposure From PDL Customer accounts](#)



593,427,119 [Exploit.In accounts](#)



457,962,538 [Anti Public Combo List accounts](#)

## Recently added breaches

OGUSERS

263,189 [OGUsers \(2020 breach\) accounts](#)

DUELING NETWORK

6,486,626 [Dueling Network accounts](#)



494,945 [Tamodo accounts](#)



2,156,921 [PropTiger accounts](#)



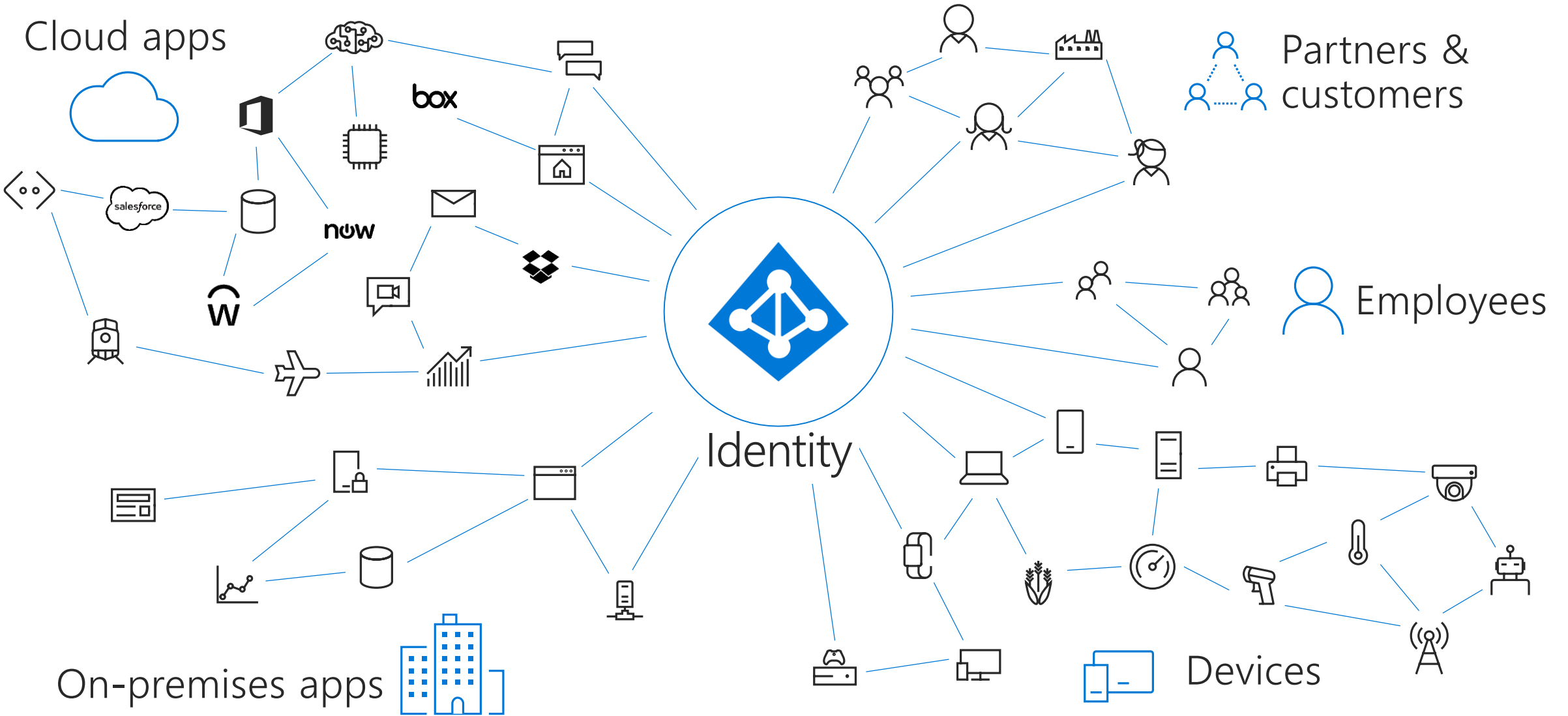
10,653 [The Halloween Spot accounts](#)

ANIMEGAME

1,431,378 [AnimeGame accounts](#)

STRAFFIC

48,580,249 [Straffic accounts](#)



# Why build with the Microsoft identity platform

Unified toolkit to reach any Microsoft identity – personal Microsoft accounts to Azure AD accounts



## Reach consumers and enterprises

Let your users sign in with their Microsoft personal account or work or school account provisioned by Azure AD



## Protect your app and users

Comply with IT policy and extend the security benefits to your app for customers who use Azure AD



## Create powerful apps

Build the next generation of apps and experiences by connecting to the Microsoft Graph



## Integrate with ease

Build with confidence using our authentication libraries and open industry standards on a trusted, reliable platform



# Partners – Business to Business (B2B)





# Azure Active Directory by the numbers

The world's #1 enterprise identity service

22.5M

organizations



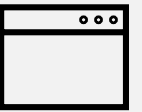
1.3B

identities



1.4M

third-party apps



100M

paid Azure AD/EMS  
seats



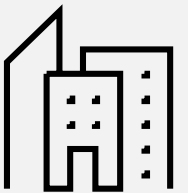
45B

daily Azure AD  
authentications













90%

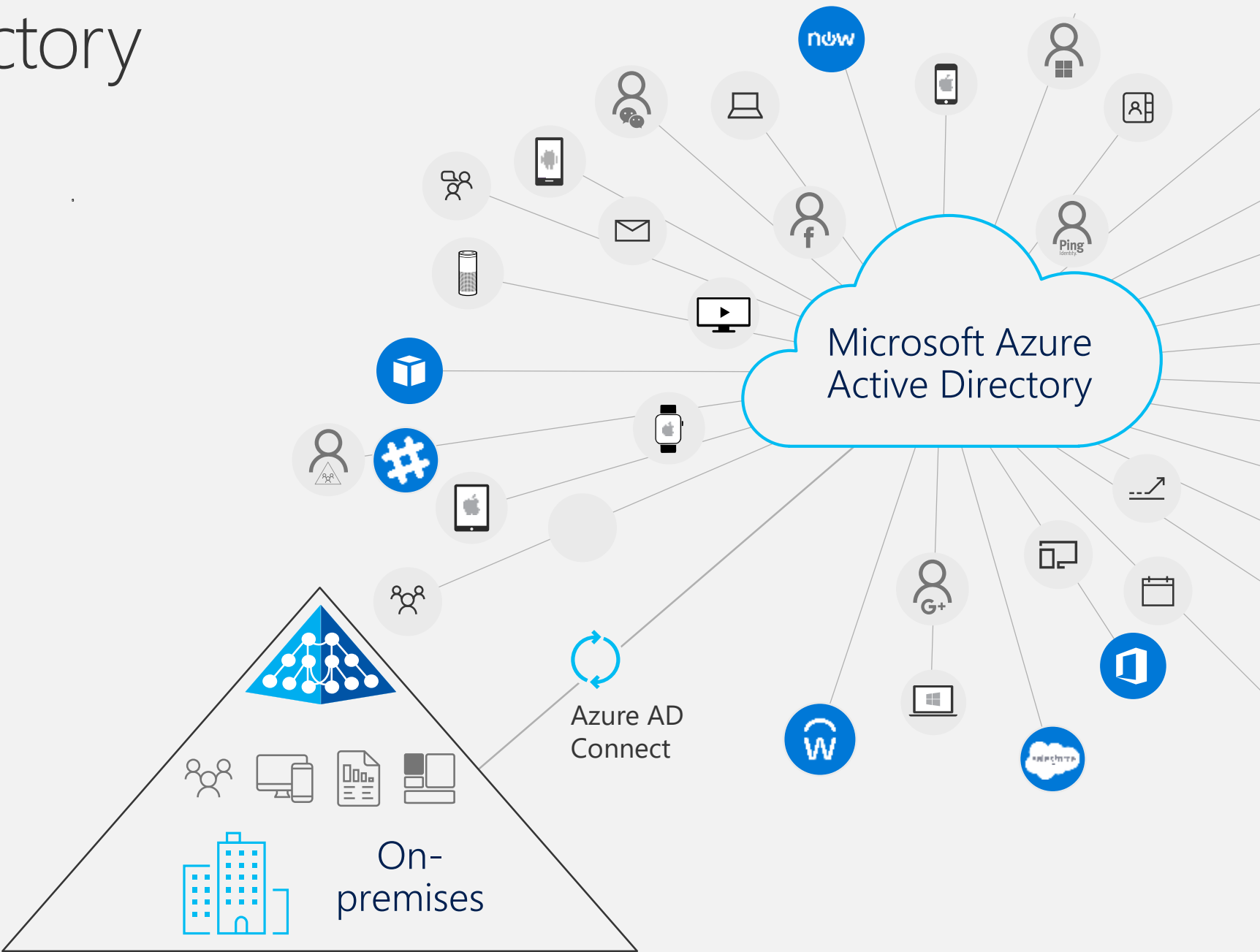
of Fortune 500  
companies





# Azure Active Directory

 Azure AD Connect	 Azure AD DS
 SSO to SaaS	 Self-Service capabilities
 Remote Access to on-premises apps	 Access Panel/MyApps
 Microsoft Authenticator - Password-less Access	 Conditional Access
 Office 365 App Launcher	 Multi-Factor Authentication

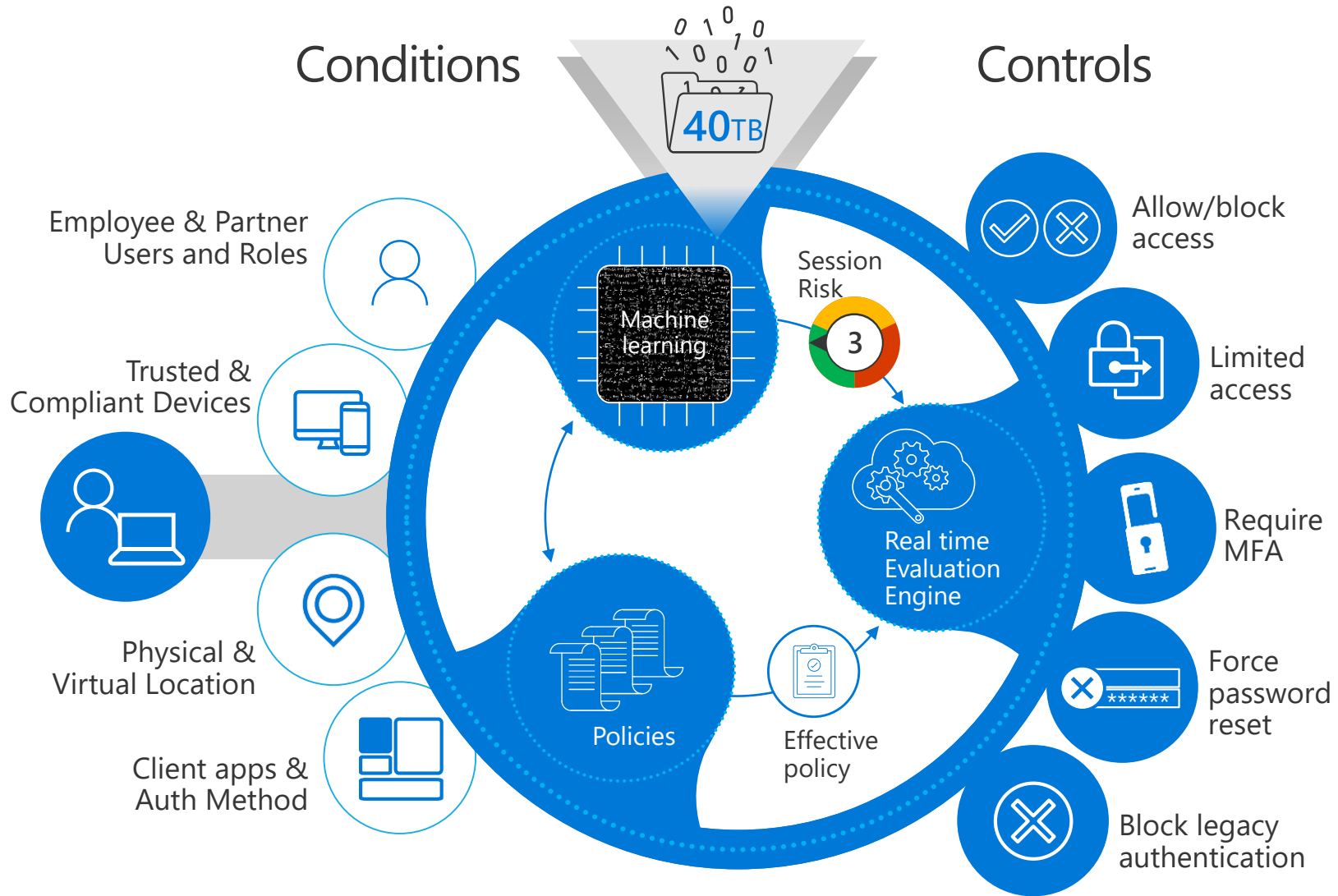


- Azure AD
- ADFS
- MSA
- Google ID

- Android
- iOS
- MacOS
- Windows
- Windows Defender ATP

- Geo-location
- Corporate Network

- Browser apps
- Client apps



Microsoft Cloud

Microsoft  
Cloud App Security



Cloud SaaS apps



On-premises apps

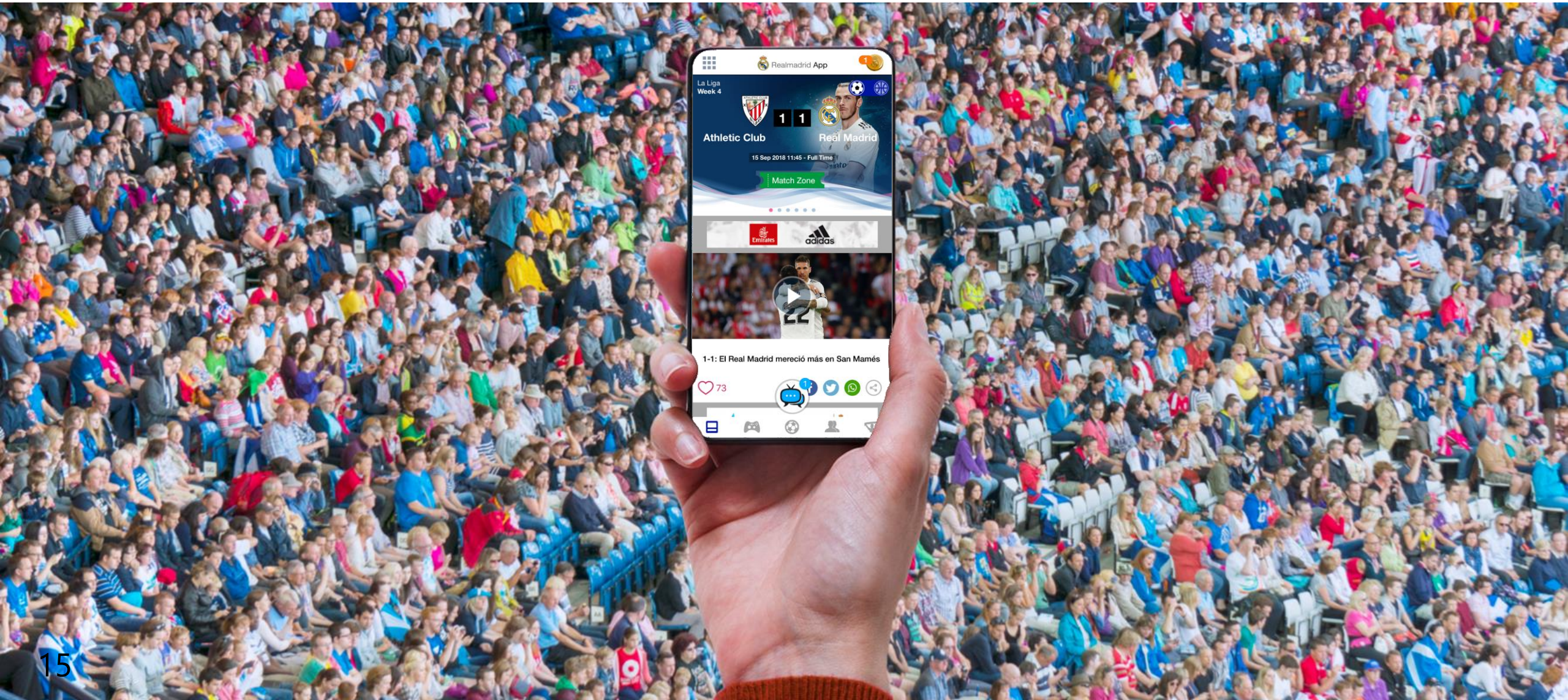


# Demo Azure AD Application Registration

```
34     var graphConfig = {
35         graphMeEndpoint: "https://graph.microsoft.com/v1.0/me",
36         graphMePhotoEndpoint: "https://graph.microsoft.com/v1.0/me/photo/$value",
37     };
38
39     // create a request object for login or token request calls
40     // In scenarios with incremental consent, the request object can be further customized
41     var requestObj = {
42         scopes: ["user.read"]
43     };
44
45     var myMSALObj = new Msal.UserAgentApplication(msalConfig);
46
47     // register Callbacks for redirect flow
48     // myMSALObj.handleRedirectCallbacks(acquireTokenRedirectCallback, acquireTokenErrorRedirectCallback);
49     myMSALObj.handleRedirectCallback(authRedirectCallback);
50
51     function signIn() {
52         myMSALObj.loginPopup(requestObj).then(function (loginResponse) {
53             //Successful login
54             showWelcomeMessage();
55             //Call MS Graph using the token in the response
56             acquireTokenPopupAndCallMSGraph();
57         }).catch(function (error) {
58             //Please check the console for errors
59             console.log(error);
60         });
61     }
62
63     function signOut() {
64         myMSALObj.logout();
65     }
```

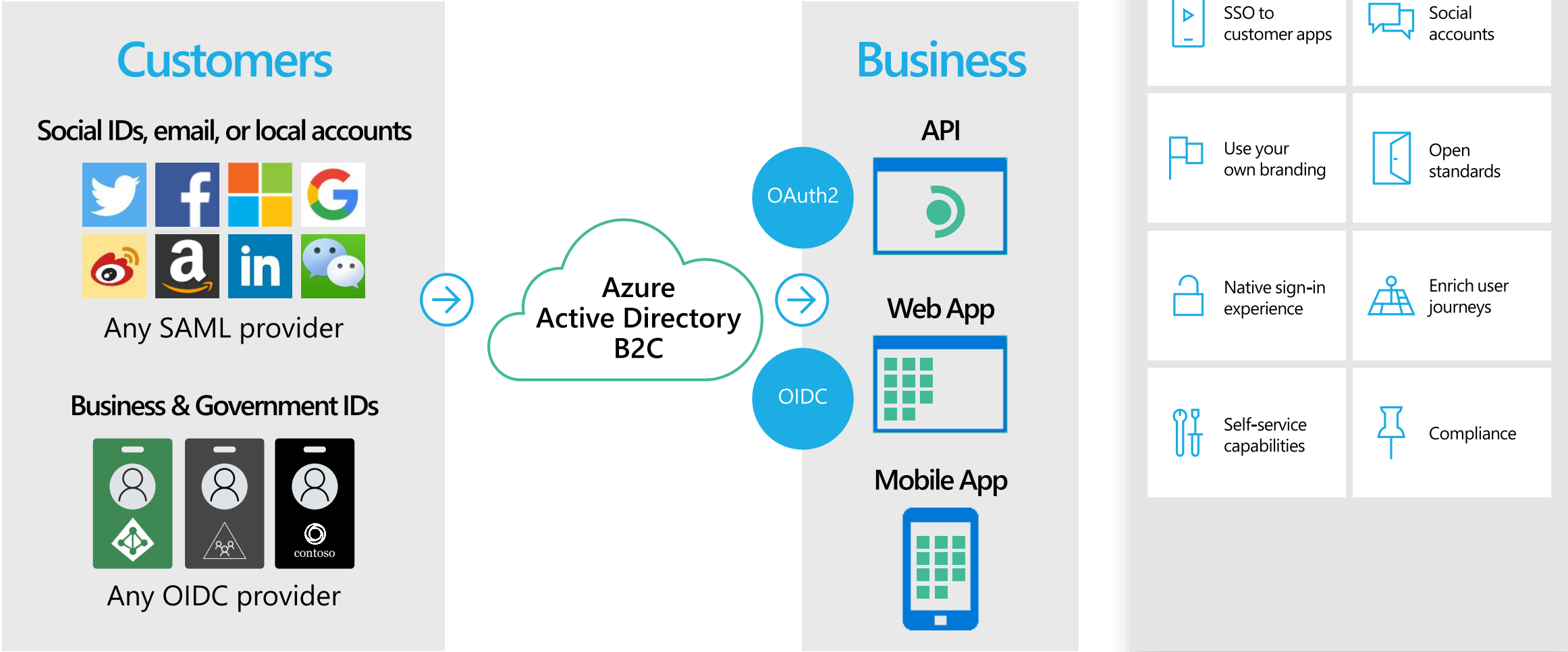


# Customers – Business to Customers (B2C)





B2C provides simple, reliable and secure, SSO access to customer-facing apps with social or business IDs .



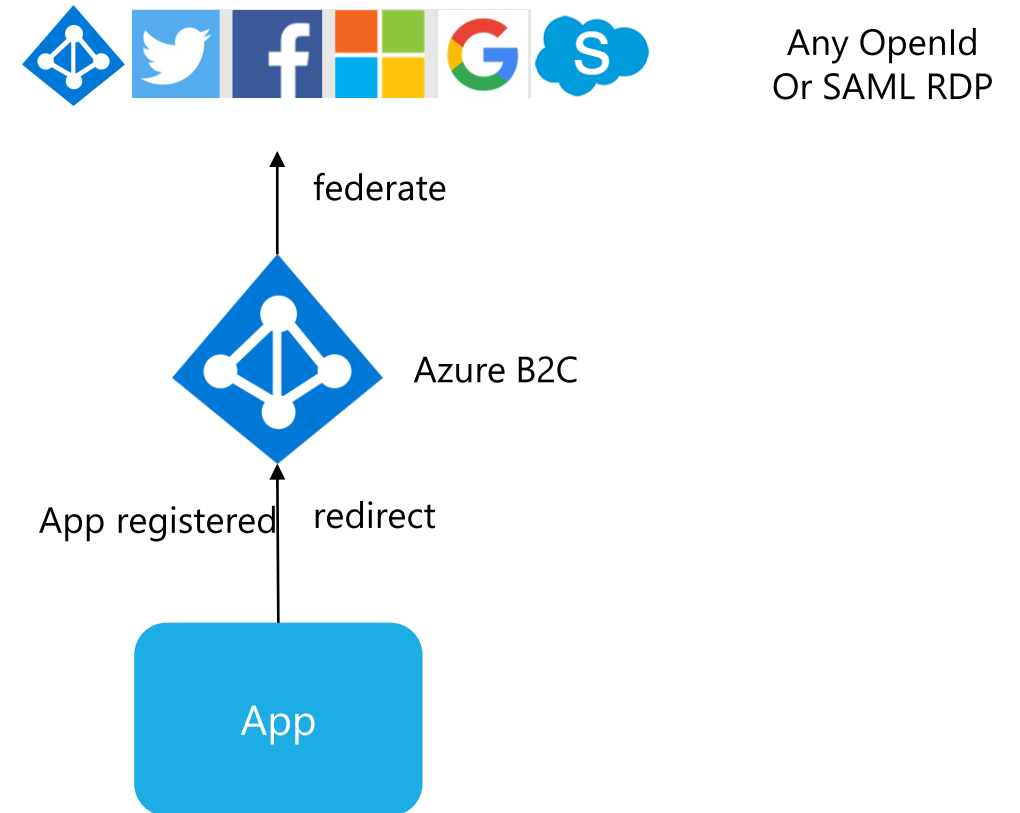
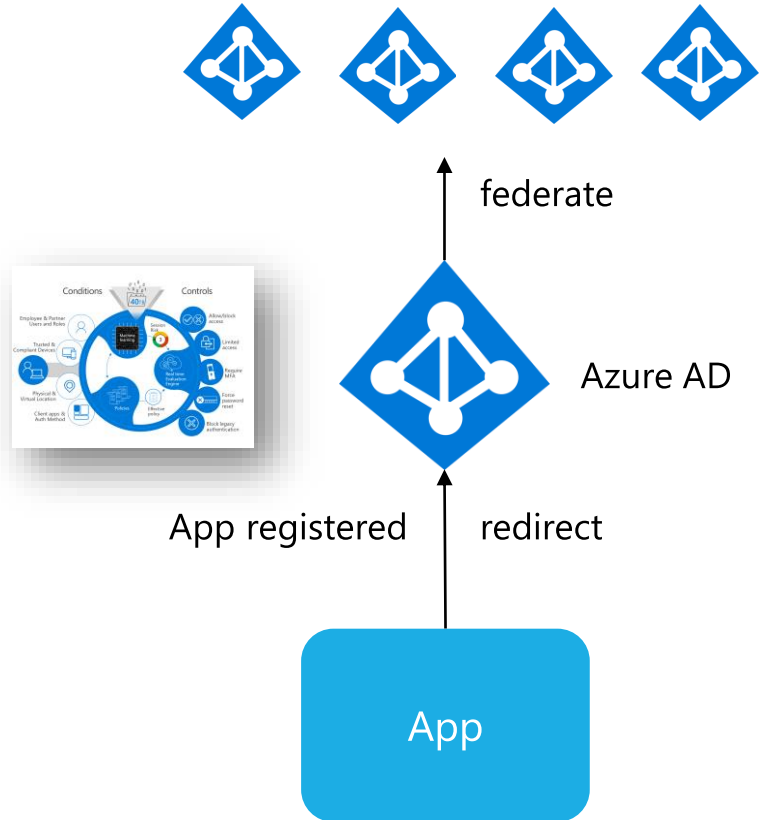


# Azure B2C Demo

<http://aka.ms/ciamdemo>

```
34 var graphConfig = {
35     graphMeEndpoint: "https://graph.microsoft.com/v1.0/me",
36     graphMePhotoEndpoint: "https://graph.microsoft.com/v1.0/me/photo/$value",
37 };
38
39 // create a request object for login or token request calls
40 // In scenarios with incremental consent, the request object can be further customized
41 var requestObj = {
42     scopes: ["user.read"]
43 };
44
45 var myMSALObj = new Msal.UserAgentApplication(msalConfig);
46
47 // Register Callbacks for redirect flow
48 // myMSALObj.handleRedirectCallbacks(acquireTokenRedirectCallback, acquireTokenErrorRedirectCallback);
49 myMSALObj.handleRedirectCallback(authRedirectCallback);
50
51 function signIn() {
52     myMSALObj.loginPopup(requestObj).then(function (loginResponse) {
53         //Successful login
54         showWelcomeMessage();
55         //Call MS Graph using the token in the response
56         acquireTokenPopupAndCallMSGraph();
57     }).catch(function (error) {
58         //Please check the console for errors
59         console.log(error);
60     });
61 }
62
63 function signOut() {
64     myMSALObj.logout();
65 }
```

# Azure AD versus Azure B2C for ISV



# Integrate with Microsoft 365



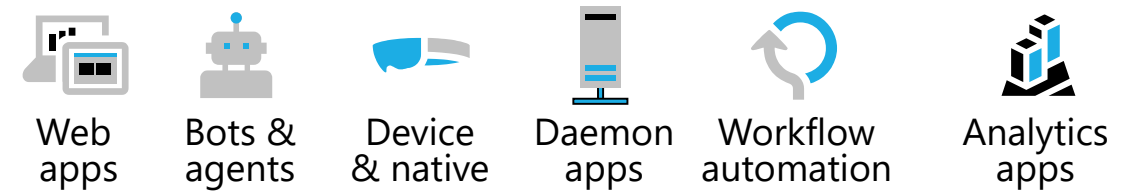


# Microsoft 365 Platform

## Extend Microsoft 365 experiences



## Build your experience



## Microsoft Graph API



## Microsoft 365





# Graph Explorer

<https://developer.microsoft.com/en-us/graph/graph-explorer/preview>

<https://developer.microsoft.com/en-us/graph/quick-start>

```
34 var graphConfig = {
35     graphMeEndpoint: "https://graph.microsoft.com/v1.0/me",
36     graphMePhotoEndpoint: "https://graph.microsoft.com/v1.0/me/photo/$value",
37 };
38
39 // create a request object for login or token request calls
40 // In scenarios with incremental consent, the request object can be further customized
41 var requestObj = {
42     scopes: ["user.read"]
43 };
44
45 var myMSALObj = new Msal.UserAgentApplication(msalConfig);
46
47 // Register Callbacks for redirect flow
48 // myMSALObj.handleRedirectCallbacks(acquireTokenRedirectCallback, acquireTokenErrorRedirectCallback);
49 myMSALObj.handleRedirectCallback(authRedirectCallback);
50
51 function signIn() {
52     myMSALObj.loginPopup(requestObj).then(function (loginResponse) {
53         // Success for login
54         showWelcomeMessage();
55         //Call MS Graph using the token in the response
56         acquireTokenPopupAndCallMSGraph();
57     }).catch(function (error) {
58         //Please check the console for errors
59         console.log(error);
60     });
61 }
62
63 function signOut() {
64     // Sign out logic
65 }
```

# Single tenant vs multi tenant (for Azure AD)

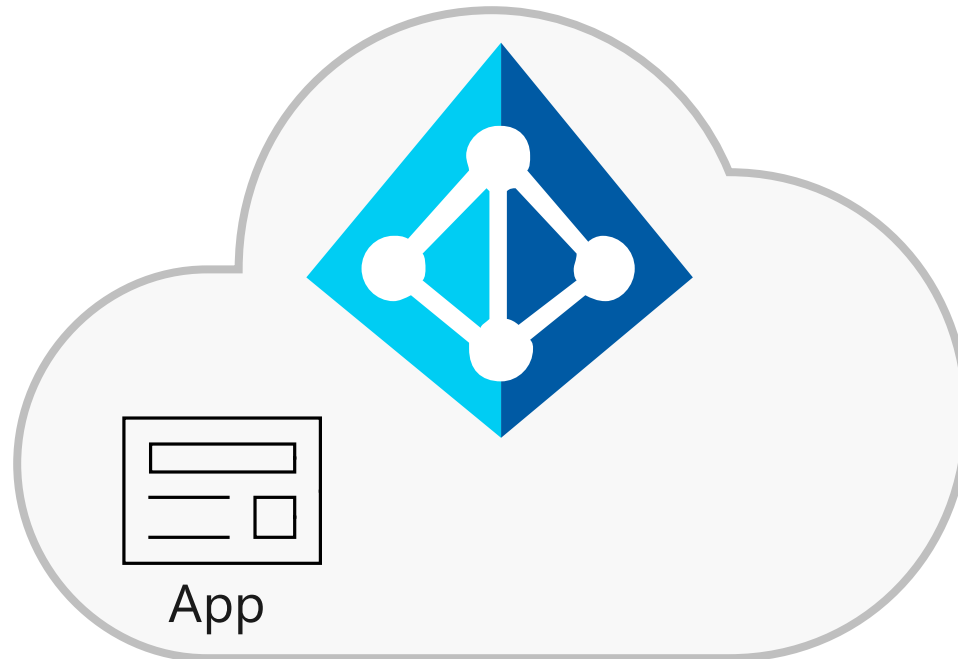
# Single Enterprise App – Users come from only one enterprise

App registered for a specific Azure AD directory

*Single-tenant*

Registered with Azure Portal, script, automation provided by developer

Admins decide who can register apps in their tenant





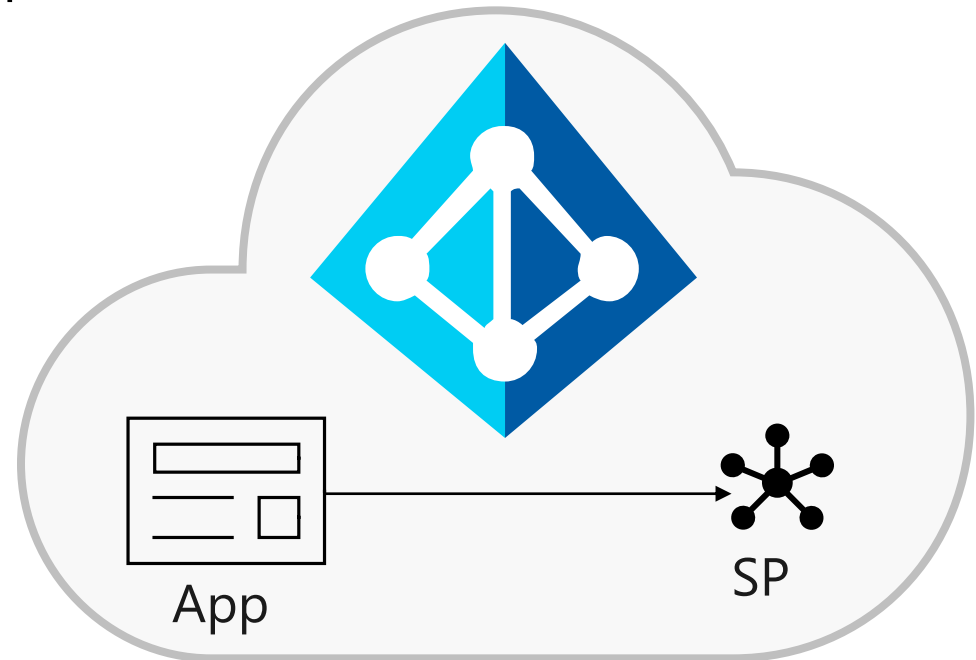
# Making getting your app easier

App registered for use in any Azure Directory or any Azure AD and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

## *Multi-tenant*

Registered in its “Home” directory (same process as single-tenant)

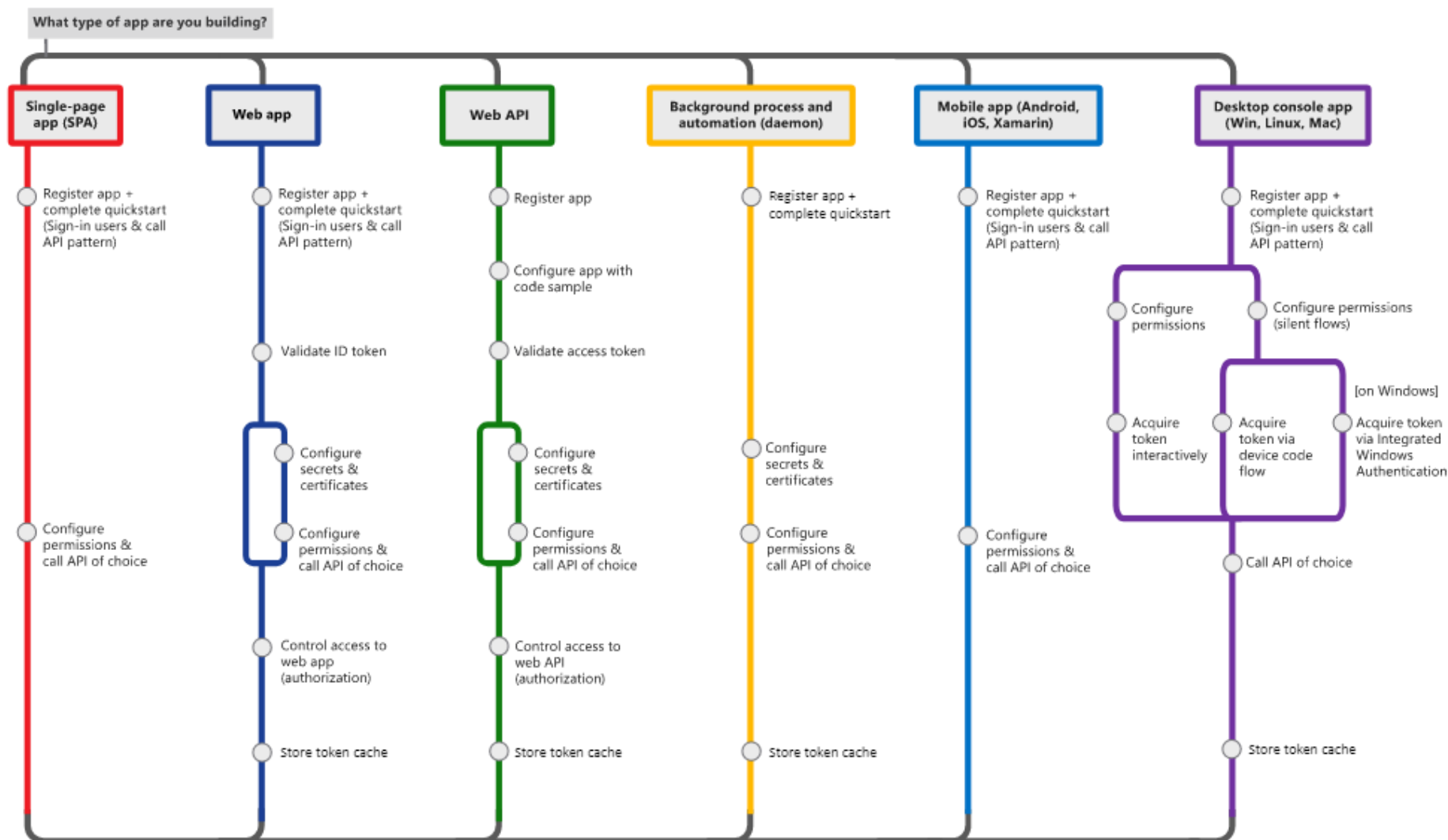
Admins decide who can consent to apps in their tenant



# Microsoft Identity Platform (evolution of Azure AD for Developers)

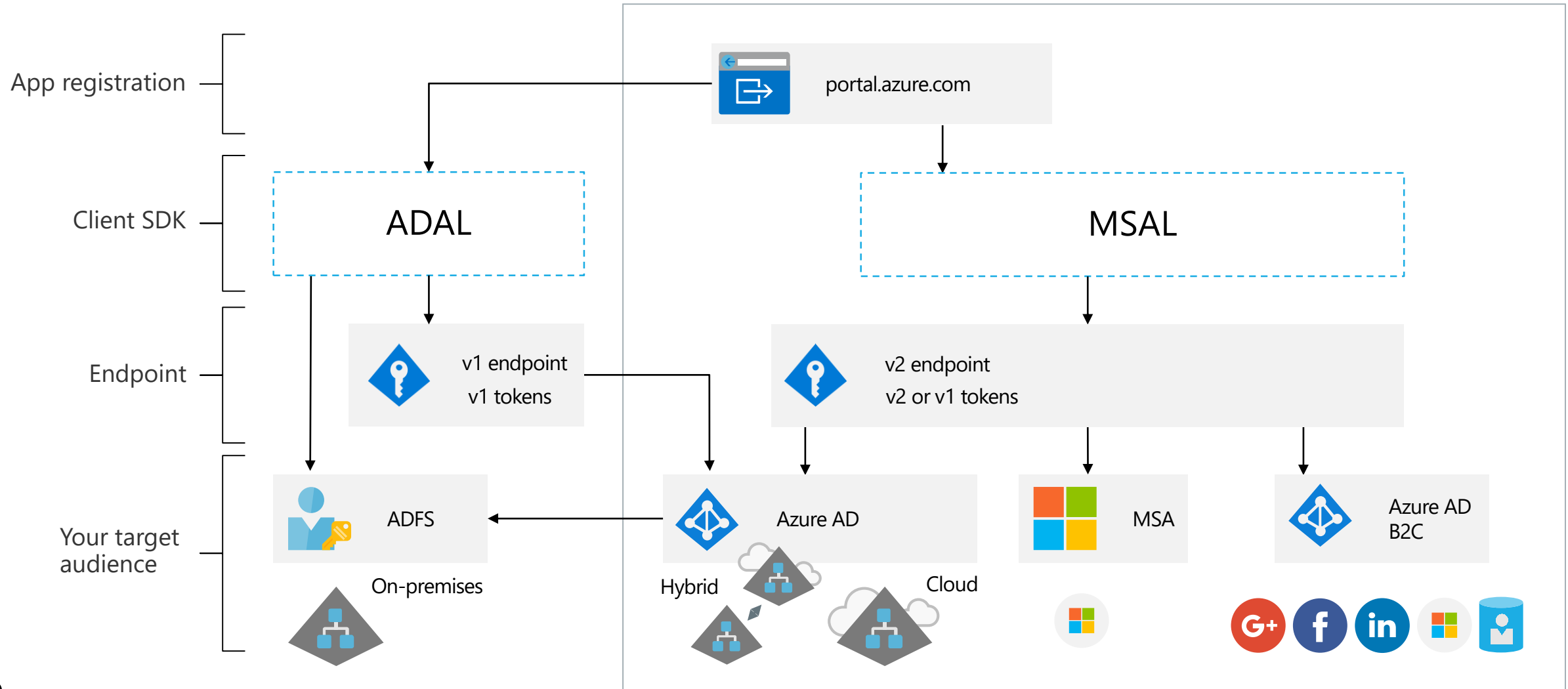
# Microsoft identity platform

<http://aka.ms/IdentityPlatform>



# Microsoft Identity Platform

Unified toolkit for building identity-connected applications





# Fast and simple integration

## Authentication libraries

- Secure access to users and data made simple
  - Microsoft's world (Microsoft Graph, other APIs)
  - Your own APIs
- MSAL - best in class auth libs
  - Built for v2 endpoint, reach any audience
  - Follows Microsoft Security Development Lifecycle
- Update at your own pace
  - ADAL based apps continue to work
  - Portfolio of ADAL and MSAL apps get Single Sign On



# Microsoft Authentication Libraries (MSAL)

.NET, JS GA at Build

Updates frequently

Adding new features to MSAL only, security updates for ADAL



JavaScript



Angular



.NET



UWP



Java



Android

iOS

iOS



Xamarin



Python

# Modern Identity – Deep Dive Webinar Serie

Repeat topic Monday and Thursday – One topic pr week

Format: 45 minutes presentation. Intro to homework, Q&A. Listeners get a coding excercise as homework.

- |  |         |
|--|---------|
| 1. Adding Authentication                     | Week 18 |
| 2. Permission and Consent framework          | Week 19 |
| 3. Accessing and protecting API's            | Week 20 |
| 4. Authorization                             | Week 21 |
| 5. Azure Active Directorey B2C               | Week 22 |
| 6. Best practices for securing your services | Week 23 |

# 1:1 Hands on Modern Identity Enablement for select ISV's

Accelerate partner competence and help them integrate their products with Azure Active Directory for managing their identity through a 4-step virtual engagement

1. Architecture Design Session (ADS)
2. Make the ISV Application multitenant (Guidance on how to architect and implement the solution to be multi-tenant)
3. Enable ISV application to integrate with Azure AD (Hands on training and guidance to do the integration through our toolkits)
4. Register the application in Azure Active Directory App Gallery

This offer is only valid to managed partners that has a multitenant app or that want to make their application multitenant.

# Resources

Accelerate adoption and protect your application

## SERVICE & SUPPORT

[Stack Overflow](#) | [Support](#)

## DOCS

[Azure Active Directory](#) | [Microsoft Identity Platform](#) | [Microsoft Graph](#)

## TOOLS

[Quick Starts](#) | [Graph Explorer](#) | [MSAL Libraries](#)

## PRODUCT INFLUENCE

[UserVoice](#) | [MSAL Survey](#)

## Bookmark or subscribe



[developer.microsoft.com/identity/blogs/](https://developer.microsoft.com/identity/blogs/)



[azure.microsoft.com/services/active-directory](https://azure.microsoft.com/services/active-directory)



[github.com/AzureAD](https://github.com/AzureAD)



[aka.ms/MsIdStackOverflow](https://aka.ms/MsIdStackOverflow)



[@AzureAD](#), [@msiddev](#)

Get your completed integrations listed into our app gallery by submitting it to [aka.ms/AzureADAppGallery](https://aka.ms/AzureADAppGallery)

<https://aka.ms/identityplatform>

Ronny.Hansen@Microsoft.com