Microsoft

Microsoft Identity Platform
Developer Training

Modern Identity for Developers

Ronny Hansen
Cloud Solution Architect OCP

Ronny.Hansen@microsoft.com

Sander van den Hoven
Cloud Solution Architect ISV OCP

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 3rd 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

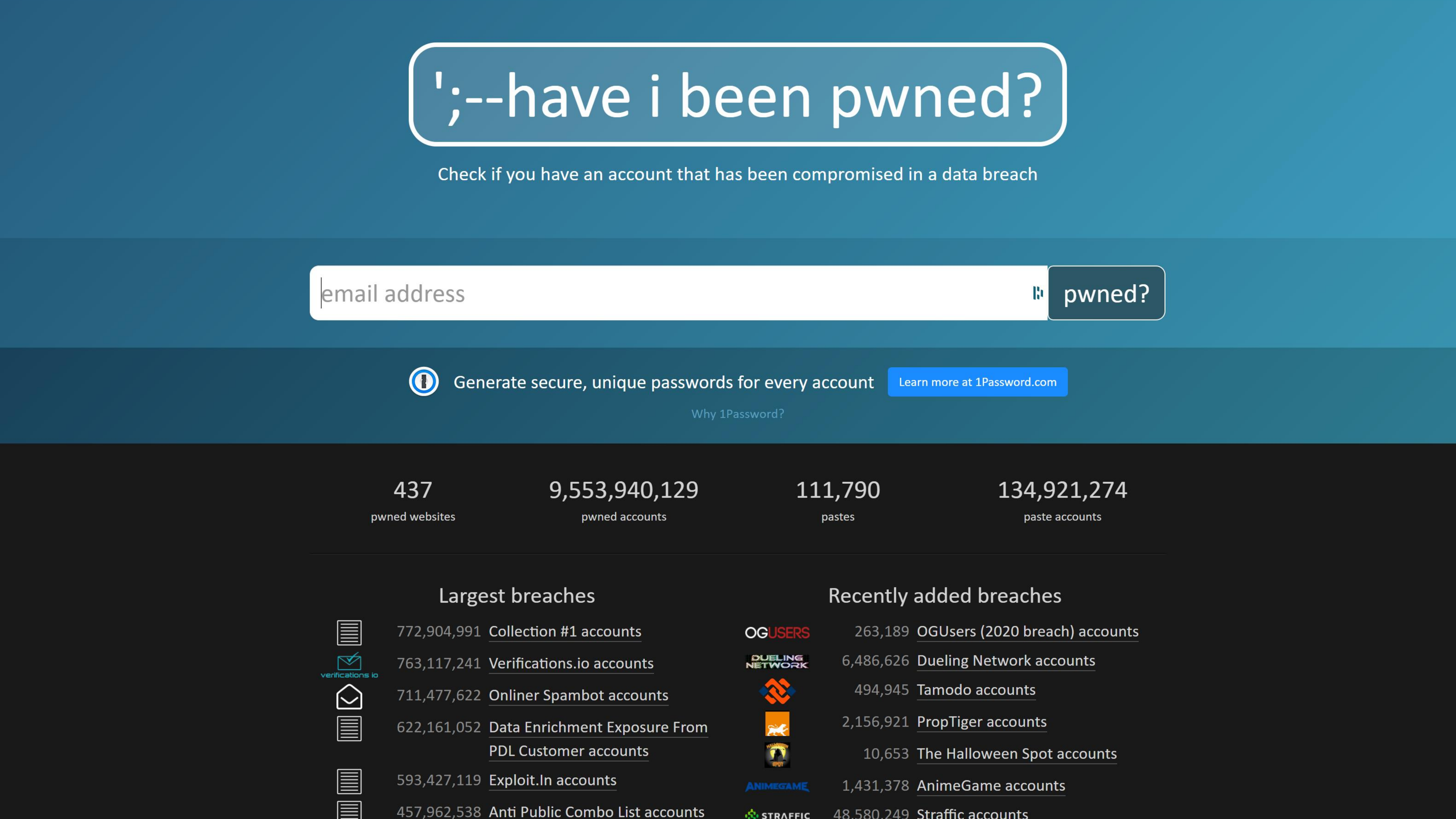
Identity History – Modern Identity

- 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

437	9,553,940,129	111,790	134,921,274
pwned websites	pwned accounts	pastes	paste accounts

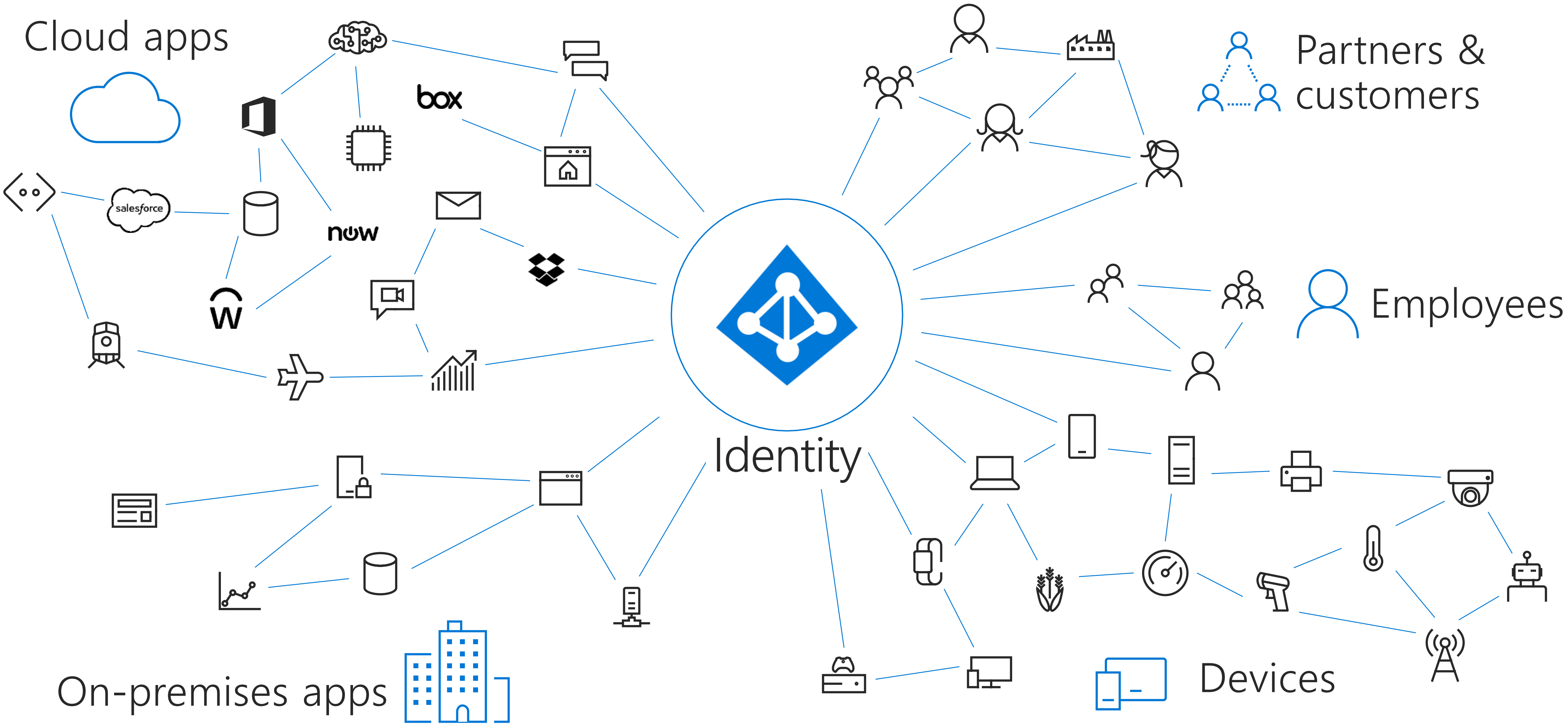
Largest breaches

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

263,189	OGUsers (2020 breach) accounts
6,486,626	Dueling Network accounts
494,945	Tamodo accounts
2,156,921	PropTiger accounts
10,653	The Halloween Spot accounts
1,431,378	AnimeGame accounts
48,580,249	Straffic accounts

Identity is the control plane



Cloud apps

Partners & customers

Employees

Identity

On-premises apps

Devices

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

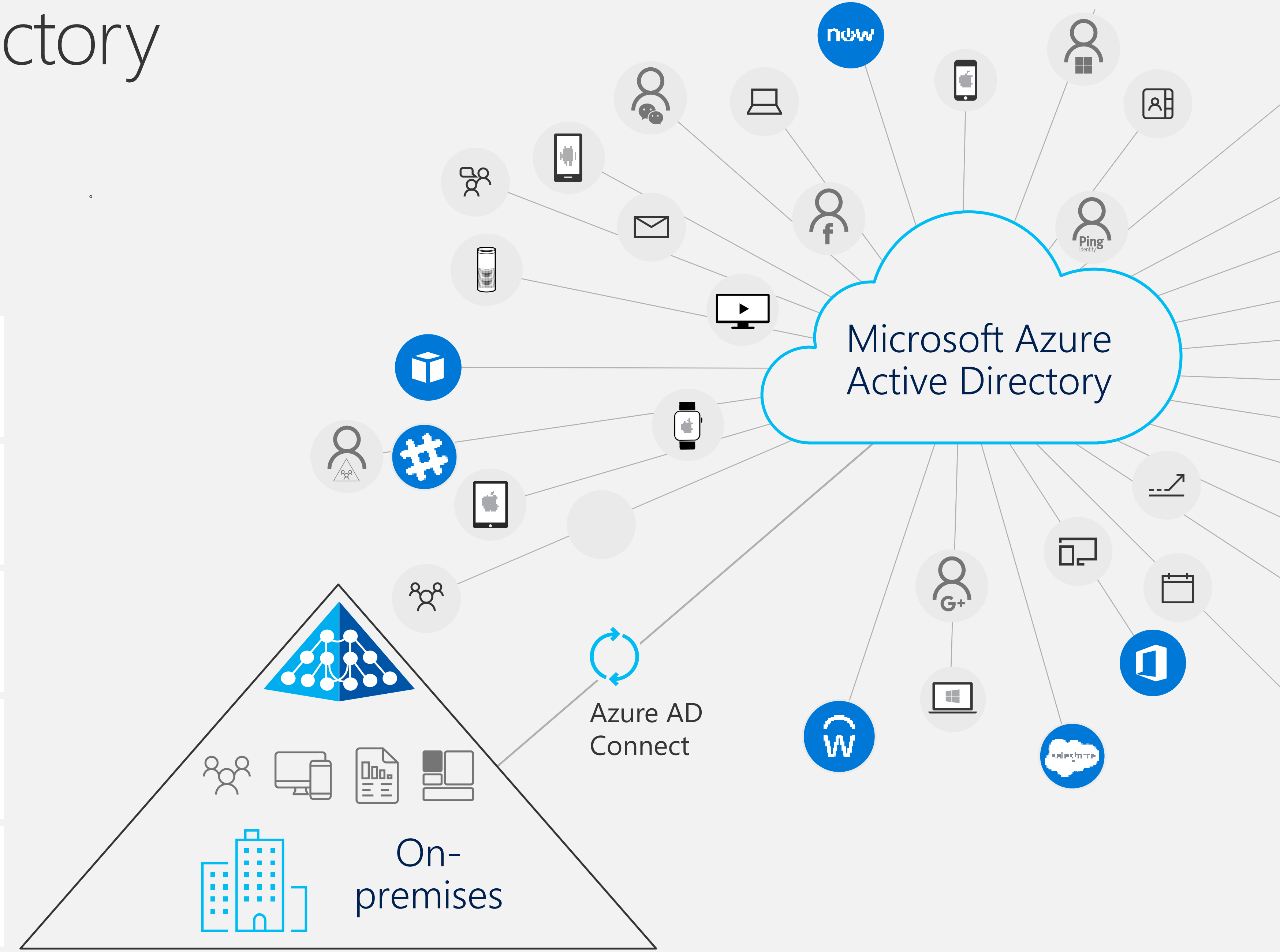
45B
daily Azure AD authentications

90%
of Fortune 500 companies

October 2019

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

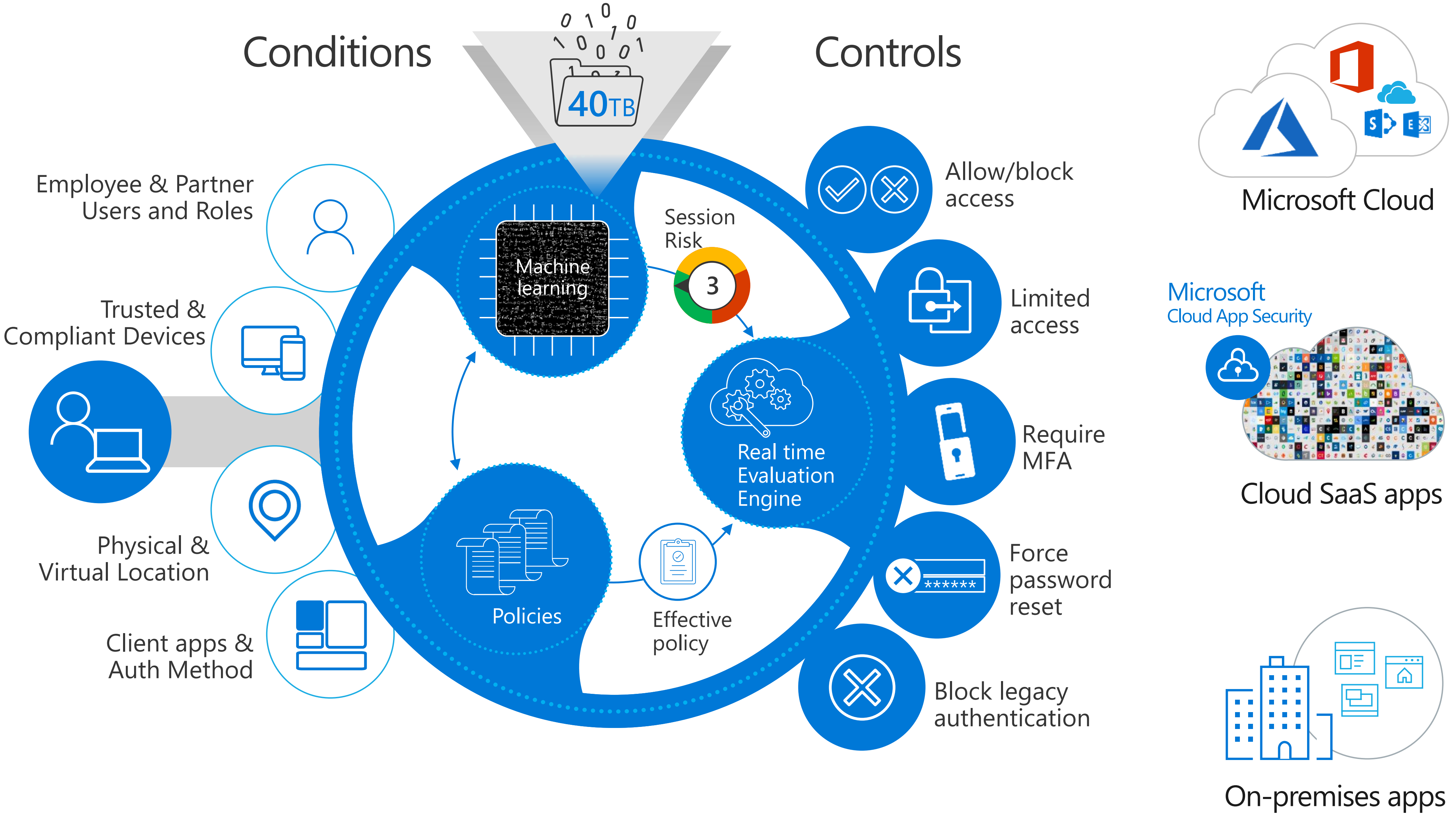


Azure AD
ADFS
MSA
Google ID

Android
iOS
MacOS
Windows
Windows Defender ATP

Geo-location
Corporate Network

Browser apps
Client apps



Conditions

Controls

40TB

Employee & Partner Users and Roles

Trusted & Compliant Devices

Physical & Virtual Location

Client apps & Auth Method

Machine learning

Session Risk

3

Real time Evaluation Engine

Policies

Effective policy

Allow/block access

Limited access

Require MFA

Force password reset

Block legacy authentication

Microsoft Cloud

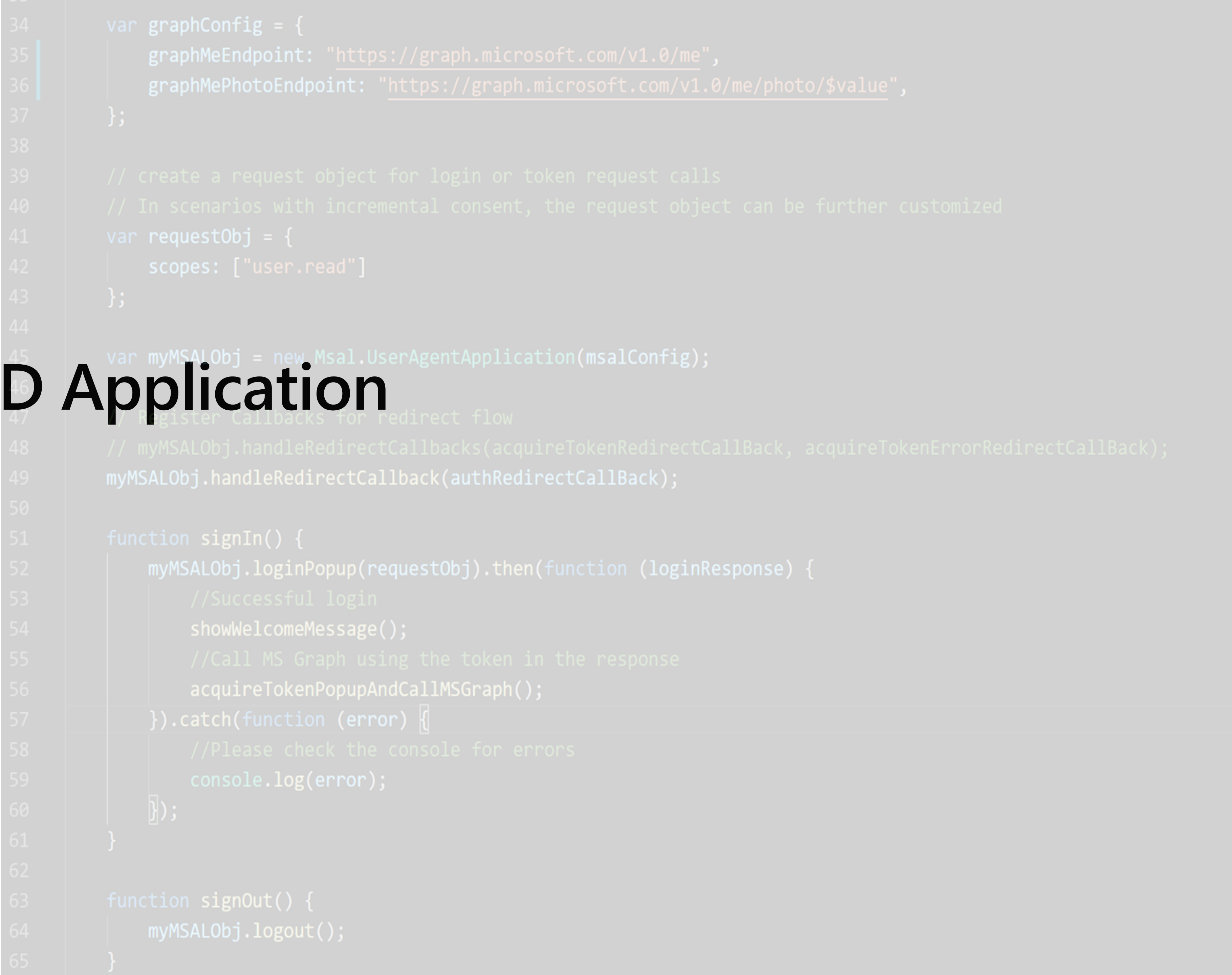
Microsoft Cloud App Security

Cloud SaaS apps

On-premises apps

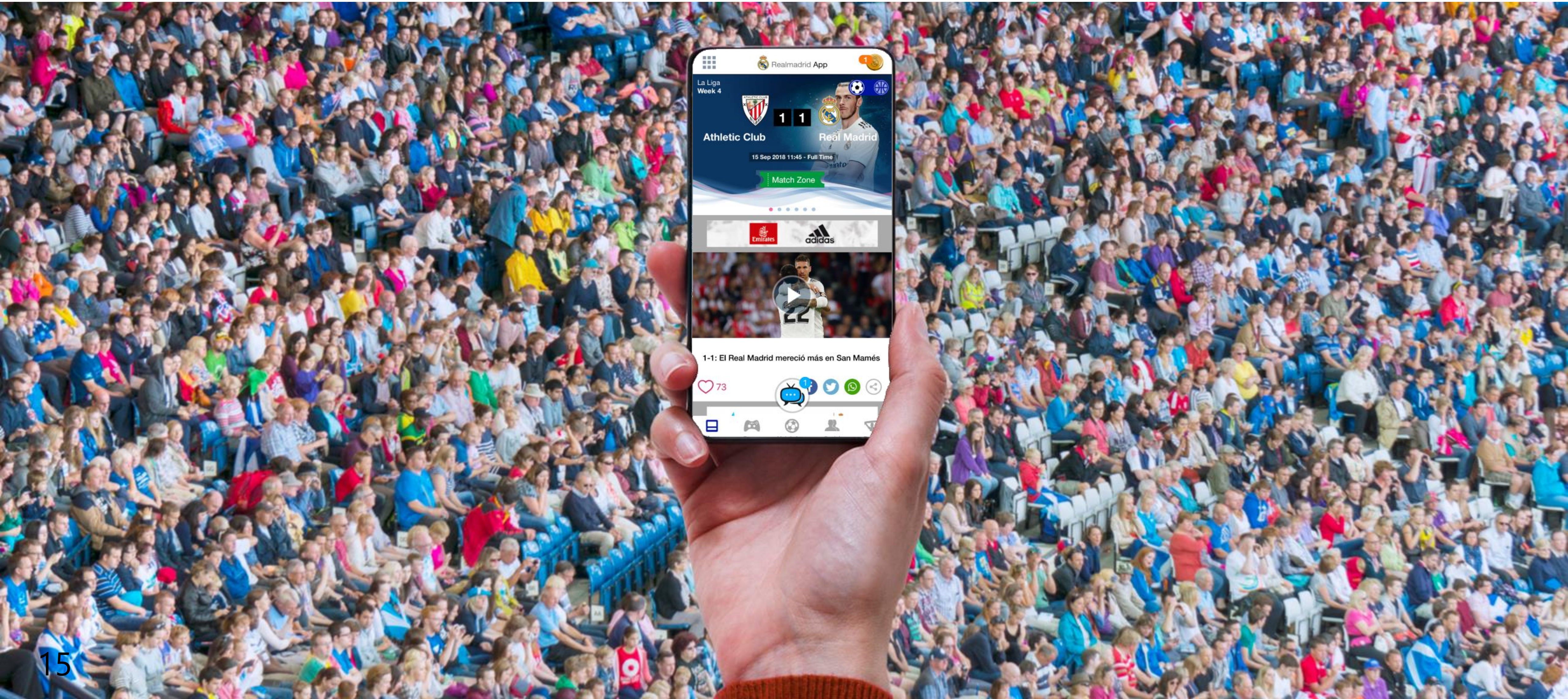
Microsoft

Demo Azure AD Application Registration

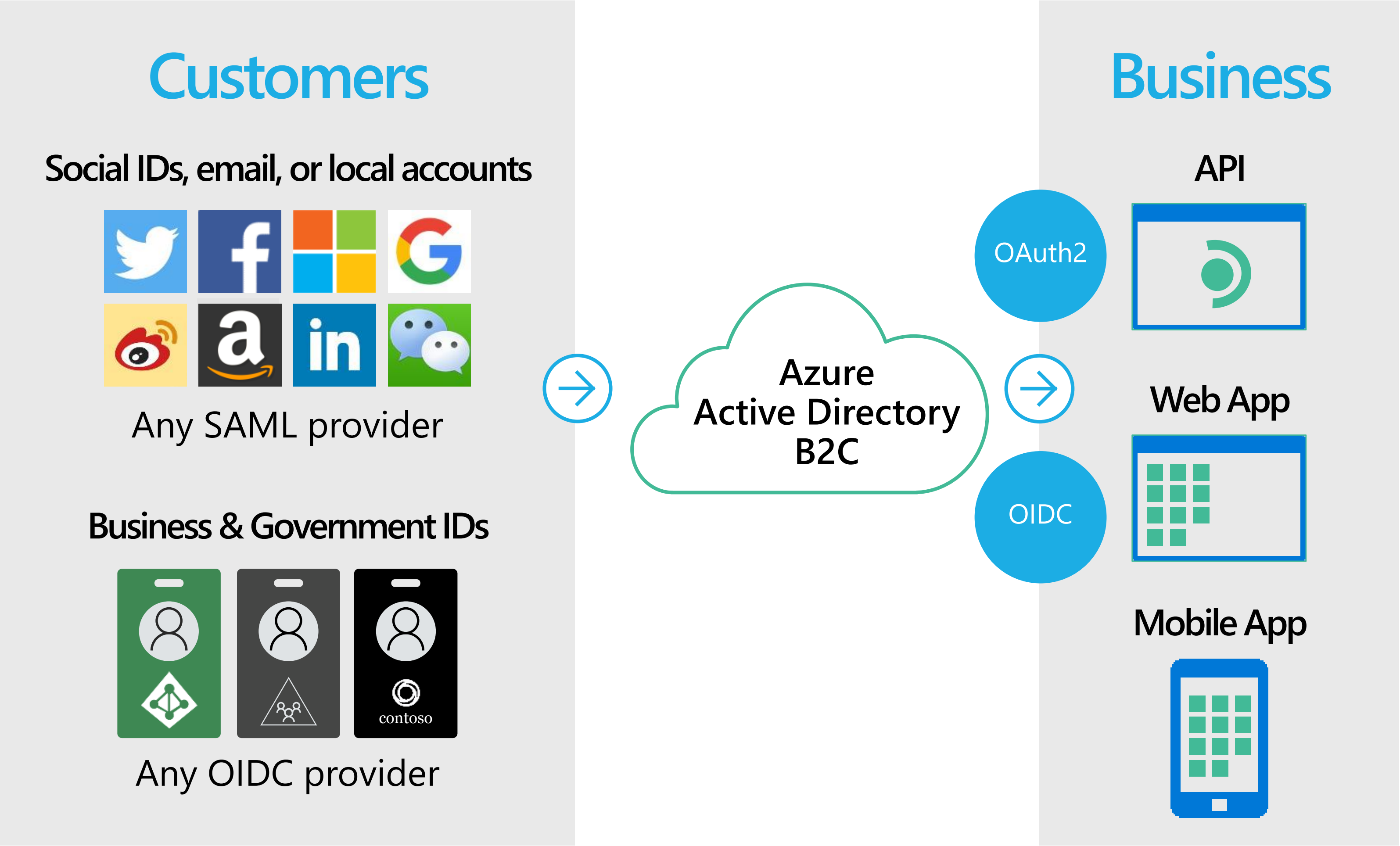


```
var graphConfig = {
    graphMeEndpoint: "https://graph.microsoft.com/v1.0/me",
    graphMePhotoEndpoint: "https://graph.microsoft.com/v1.0/me/photo/$value",
};

// create a request object for login or token request calls
// In scenarios with incremental consent, the request object can be further customized
var requestObj = {
    scopes: ["user.read"]
};

var myMSALObj = new Msal.UserAgentApplication(msalConfig);

// Register Callbacks for redirect flow
// myMSALObj.handleRedirectCallbacks(acquireTokenRedirectCallBack, acquireTokenErrorRedirectCallBack);
myMSALObj.handleRedirectCallback(authRedirectCallBack);

function signIn() {
    myMSALObj.loginPopup(requestObj).then(function (loginResponse) {
        //Successful login
        showWelcomeMessage();
        //Call MS Graph using the token in the response
        acquireTokenPopupAndCallMSGraph();
    }).catch(function (error) {
        //Please check the console for errors
        console.log(error);
    });
}

function signOut() {
    myMSALObj.logout();
}
```

Customers – Business to Customers (B2C)



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



Customers

Social IDs, email, or local accounts

Any SAML provider

Business & Government IDs

Any OIDC provider

Azure Active Directory B2C

OAuth2

OIDC

Business

API

Web App

Mobile App

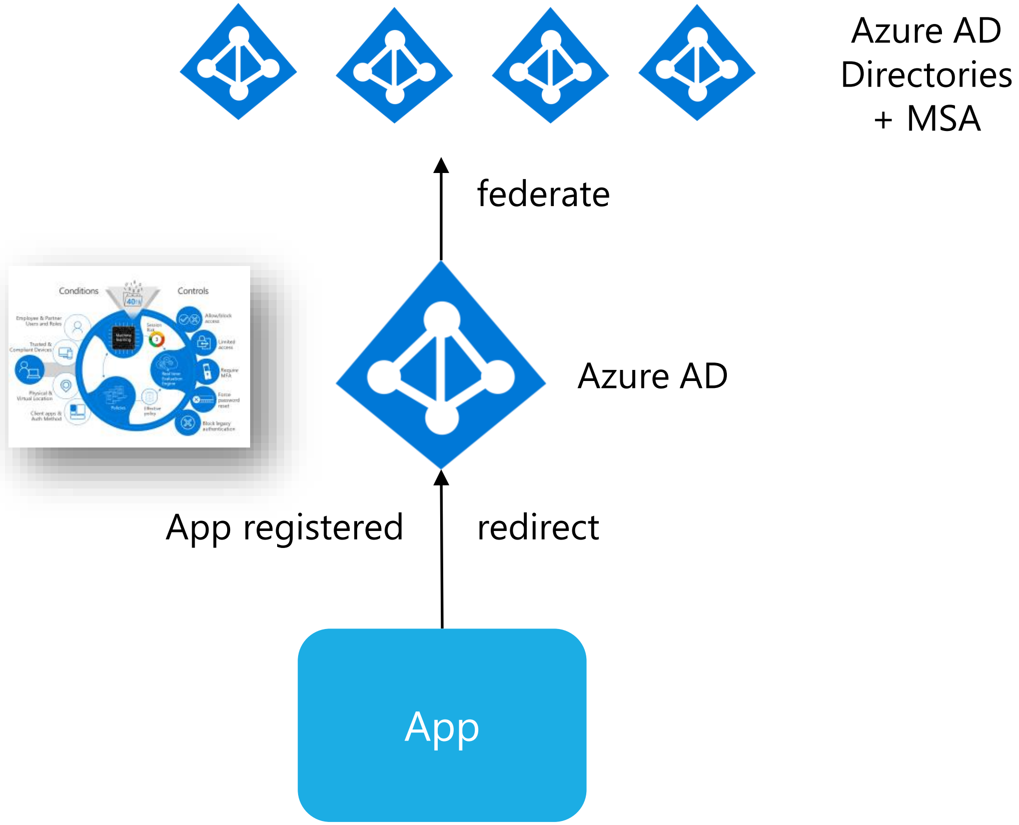
- Azure AD integration
- Connect with existing systems
- SSO to customer apps
- Social accounts
- Use your own branding
- Open standards
- Native sign-in experience
- Enrich user journeys
- Self-service capabilities
- Compliance

Azure B2C Demo

http://aka.ms/ciamdemo

```
var graphConfig = {
    graphMeEndpoint: "https://graph.microsoft.com/v1.0/me",
    graphMePhotoEndpoint: "https://graph.microsoft.com/v1.0/me/photo/$value",
};

// create a request object for login or token request calls
// In scenarios with incremental consent, the request object can be further customized
var requestObj = {
    scopes: ["user.read"]
};

var myMSALObj = new Msal.UserAgentApplication(msalConfig);

// Register Callbacks for redirect flow
// myMSALObj.handleRedirectCallbacks(acquireTokenRedirectCallBack, acquireTokenErrorRedirectCallBack);
myMSALObj.handleRedirectCallback(authRedirectCallBack);

function signIn() {
    myMSALObj.loginPopup(requestObj).then(function (loginResponse) {
        //Successful login
        showWelcomeMessage();
        //Call MS Graph using the token in the response
        acquireTokenPopupAndCallMSGraph();
    }).catch(function (error) {
        //Please check the console for errors
        console.log(error);
    });
}

function signOut() {
    myMSALObj.logout();
}
```

Azure AD versus Azure B2C for ISV



Azure AD
Directories
+ MSA

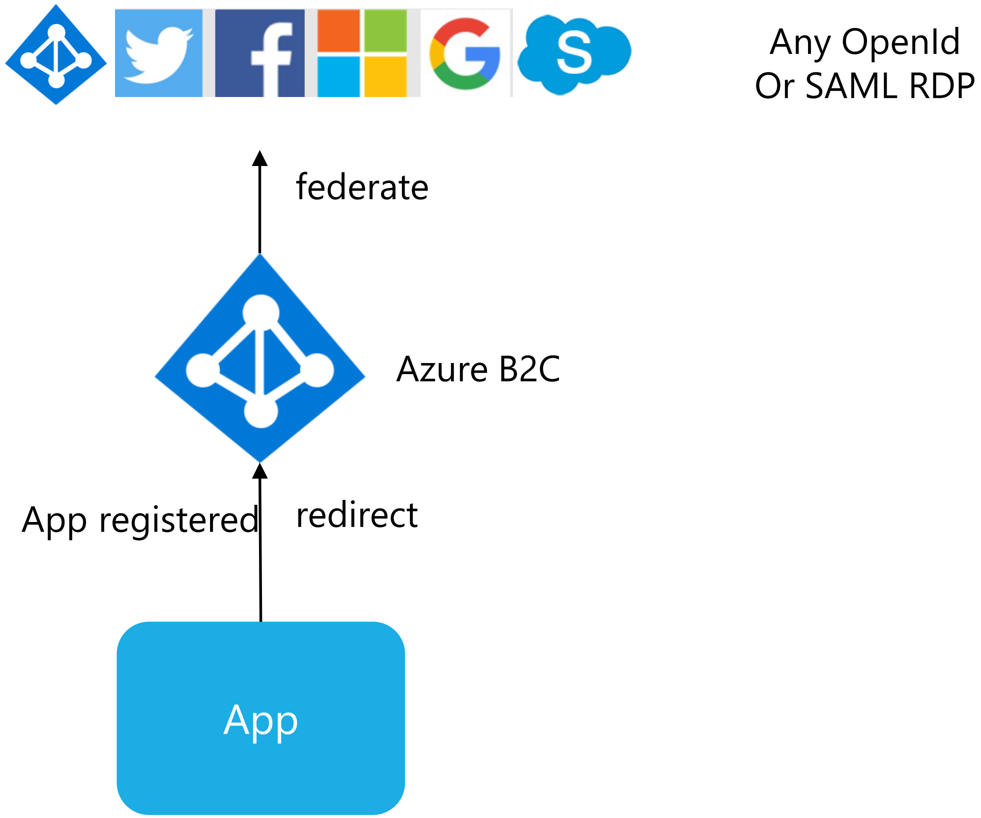
federate

Azure AD

App registered

redirect

App



Any OpenId
Or SAML RDP

federate

Azure B2C

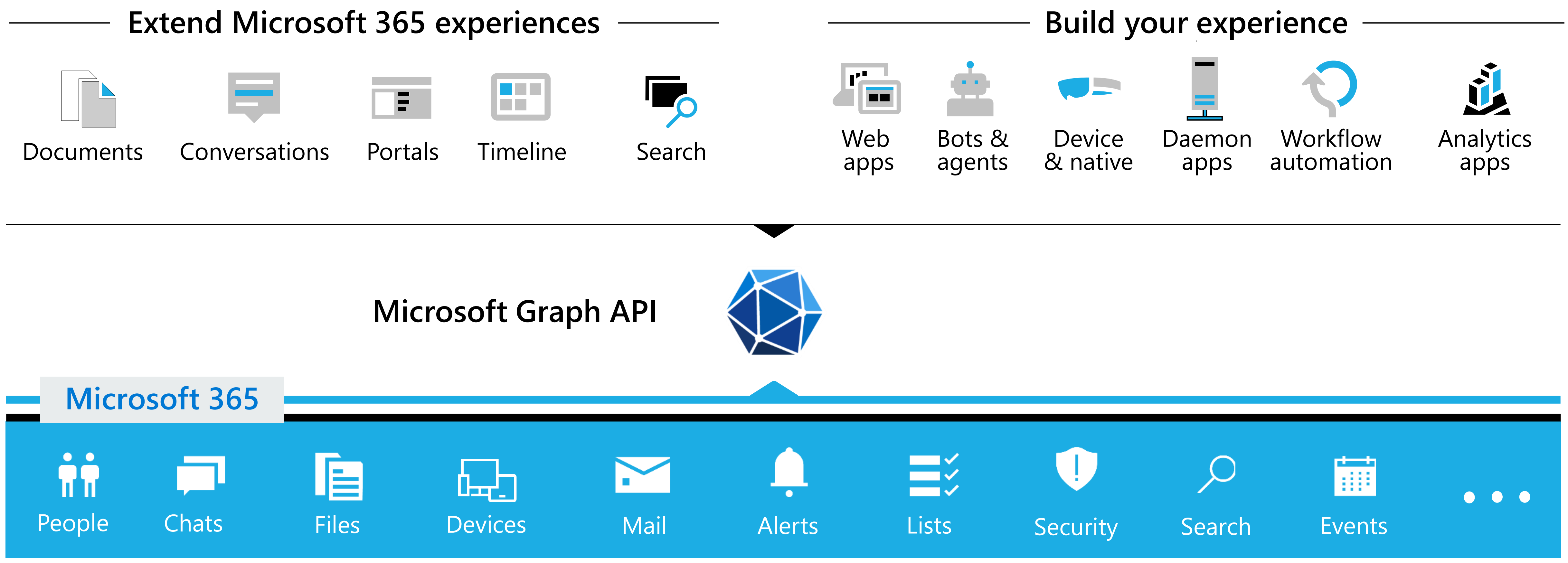
App registered

redirect

App

Integrate with Microsoft 365

Microsoft 365 Platform



Extend Microsoft 365 experiences

Documents

Conversations

Portals

Timeline

Search

Build your experience

Web apps

Bots & agents

Device & native

Daemon apps

Workflow automation

Analytics apps

Microsoft Graph API

Microsoft 365

People

Chats

Files

Devices

Mail

Alerts

Lists

Security

Search

Events

. . .

Microsoft

Graph Explorer

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

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

```
var graphConfig = {
    graphMeEndpoint: "https://graph.microsoft.com/v1.0/me",
    graphMePhotoEndpoint: "https://graph.microsoft.com/v1.0/me/photo/$value",
};

// create a request object for login or token request calls
// In scenarios with incremental consent, the request object can be further customized
var requestObj = {
    scopes: ["user.read"]
};

var myMSALObj = new Msal.UserAgentApplication(msalConfig);

// Register Callbacks for redirect flow
// myMSALObj.handleRedirectCallbacks(acquireTokenRedirectCallBack, acquireTokenErrorRedirectCallBack);
myMSALObj.handleRedirectCallback(authRedirectCallBack);

function signIn() {
    myMSALObj.loginPopup(requestObj).then(function (loginResponse) {
        //Successful login
        showWelcomeMessage();
        //Call MS Graph using the token in the response
        acquireTokenPopupAndCallMSGraph();
    }).catch(function (error) {
        //Please check the console for errors
        console.log(error);
    });
}

function signOut() {
    myMSALObj.logout();
}
```

Single tenant vs multi tenant (for Azure AD)

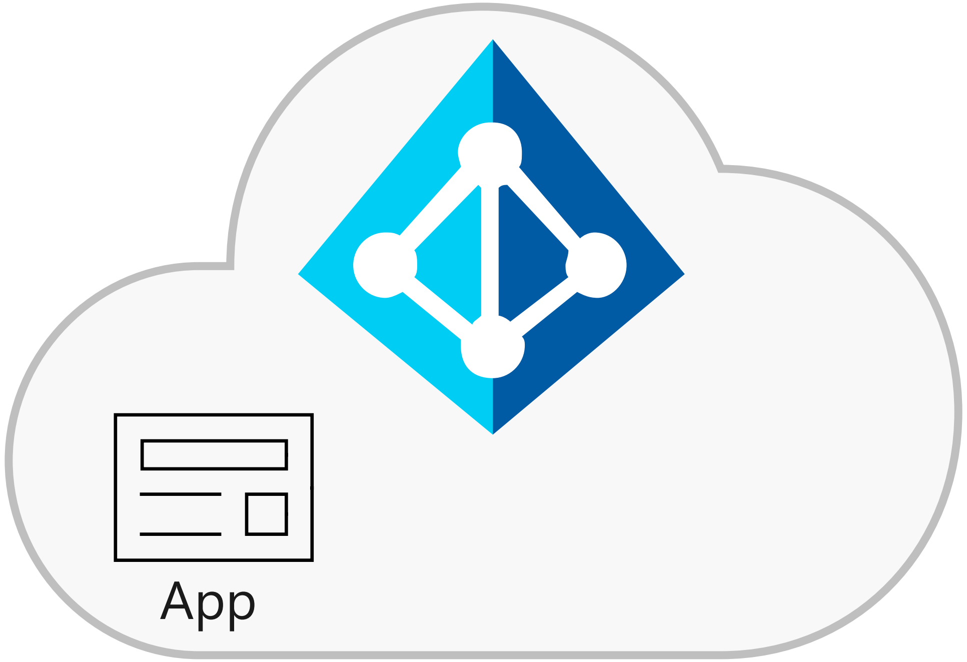
Single Enterprise App – Users come from only one enterprise

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



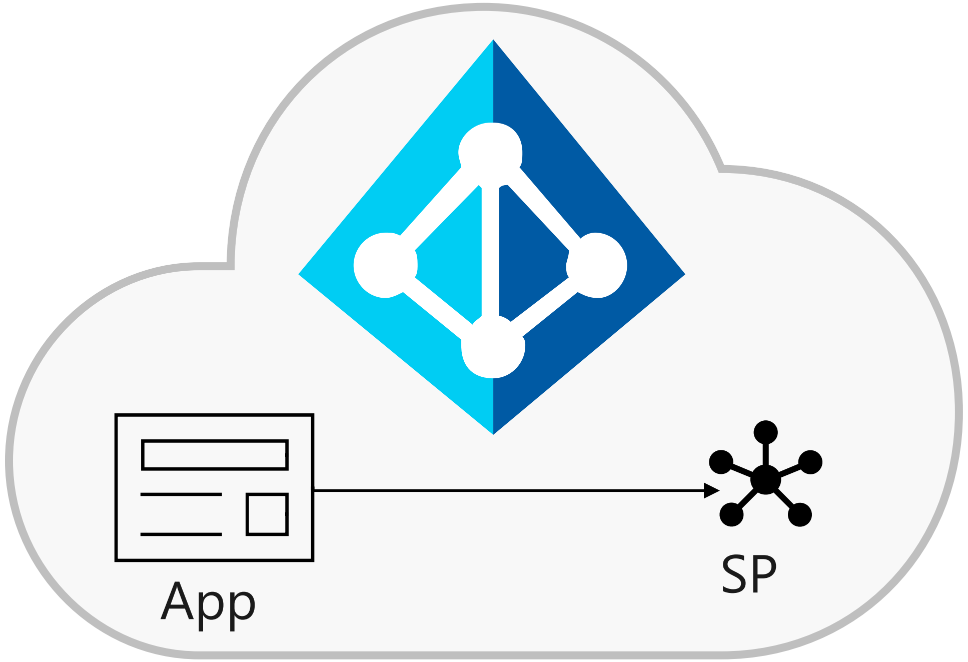
Making getting your app easier

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)

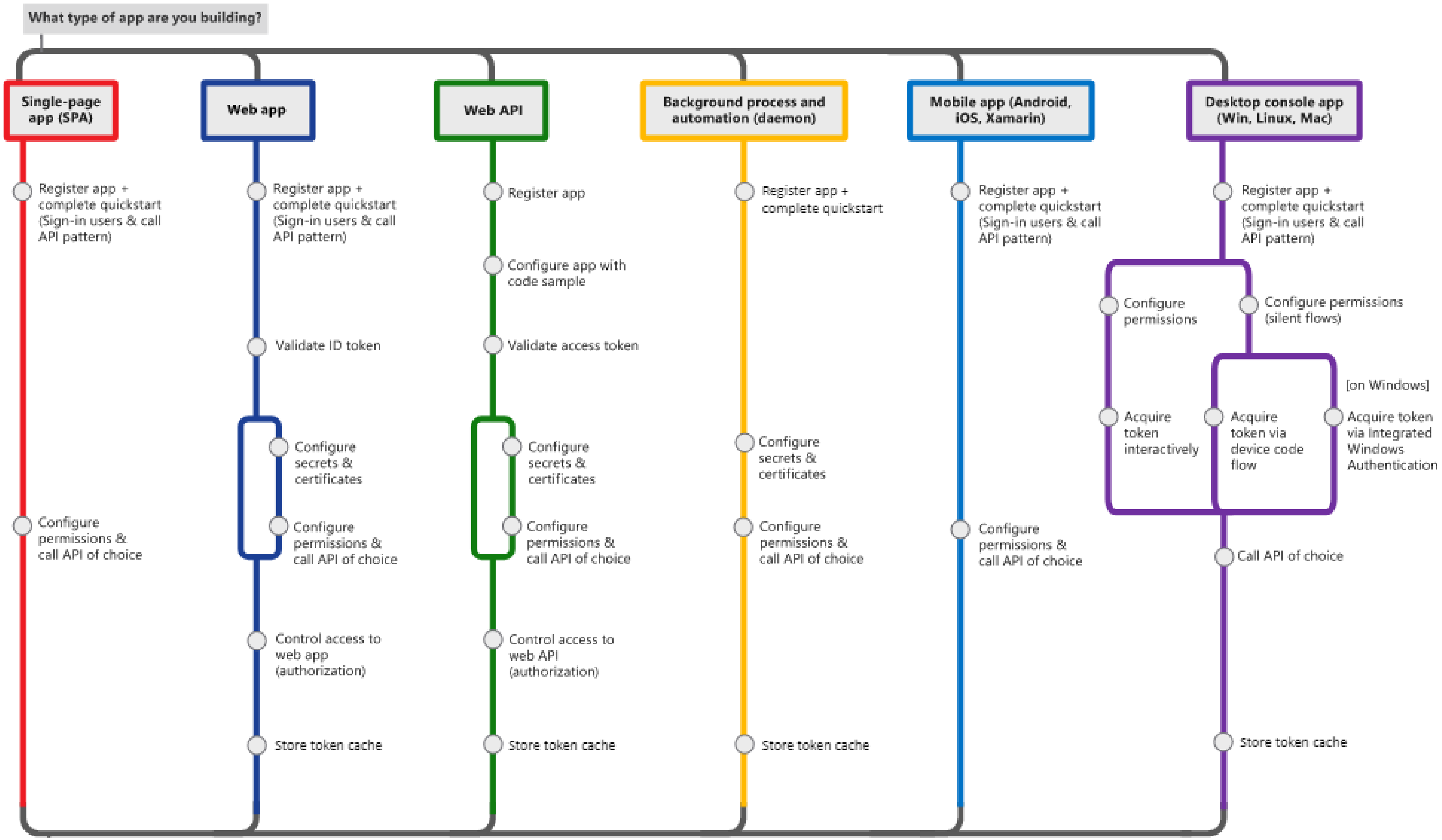
Admins decide who can consent to apps in their tenant



Microsoft Identity Platform
(evolution of Azure AD for Developers)

Microsoft identity platform

http://aka.ms/IdentityPlatform



What type of app are you building?

Single-page app (SPA)
- Register app + complete quickstart (Sign-in users & call API pattern)
- Configure permissions & call API of choice

Web app
- Register app + complete quickstart (Sign-in users & call API pattern)
- Validate ID token
- Configure secrets & certificates
- Configure permissions & call API of choice
- Control access to web app (authorization)
- Store token cache

Web API
- Register app
- Configure app with code sample
- Validate access token
- Configure secrets & certificates
- Configure permissions & call API of choice
- Control access to web API (authorization)
- Store token cache

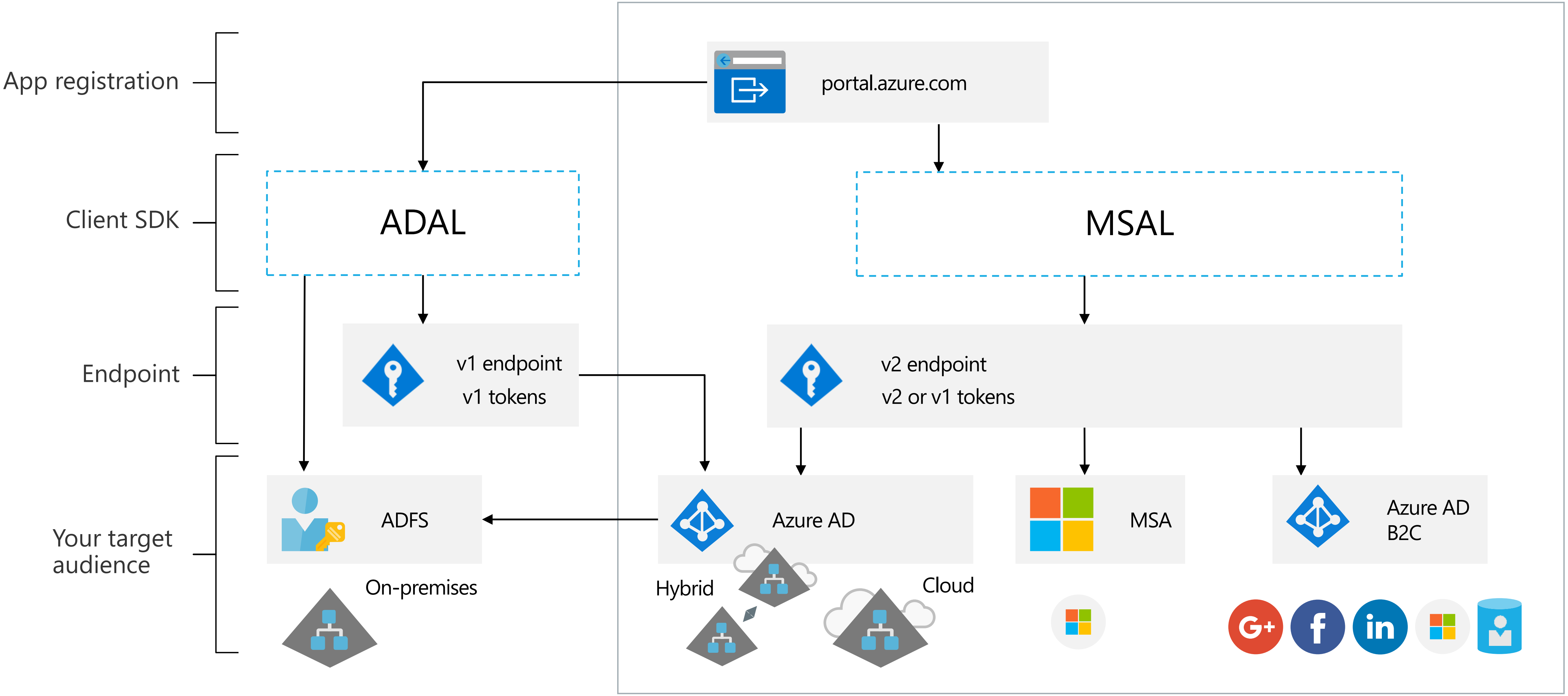
Background process and automation (daemon)
- Register app + complete quickstart
- Configure secrets & certificates
- Configure permissions & call API of choice
- Store token cache

Mobile app (Android, iOS, Xamarin)
- Register app + complete quickstart (Sign-in users & call API pattern)
- Configure permissions & call API of choice

Desktop console app (Win, Linux, Mac)
- Register app + complete quickstart (Sign-in users & call API pattern)
- Configure permissions
- Acquire token interactively
- Configure permissions (silent flows)
- Acquire token via device code flow
- [on Windows] Acquire token via Integrated Windows Authentication
- Call API of choice
- Store token cache

Microsoft Identity Platform

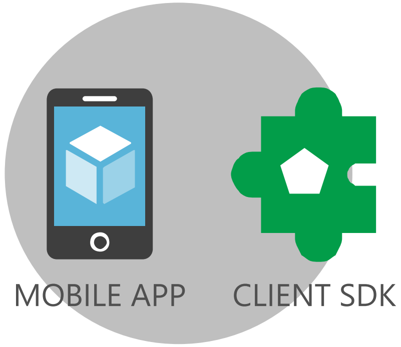
Unified toolkit for building identity-connected applications



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

PREVIEW
Angular

.NET

UWP

PREVIEW
Java

Android

iOS

Xamarin

PREVIEW
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 exercise as homework.

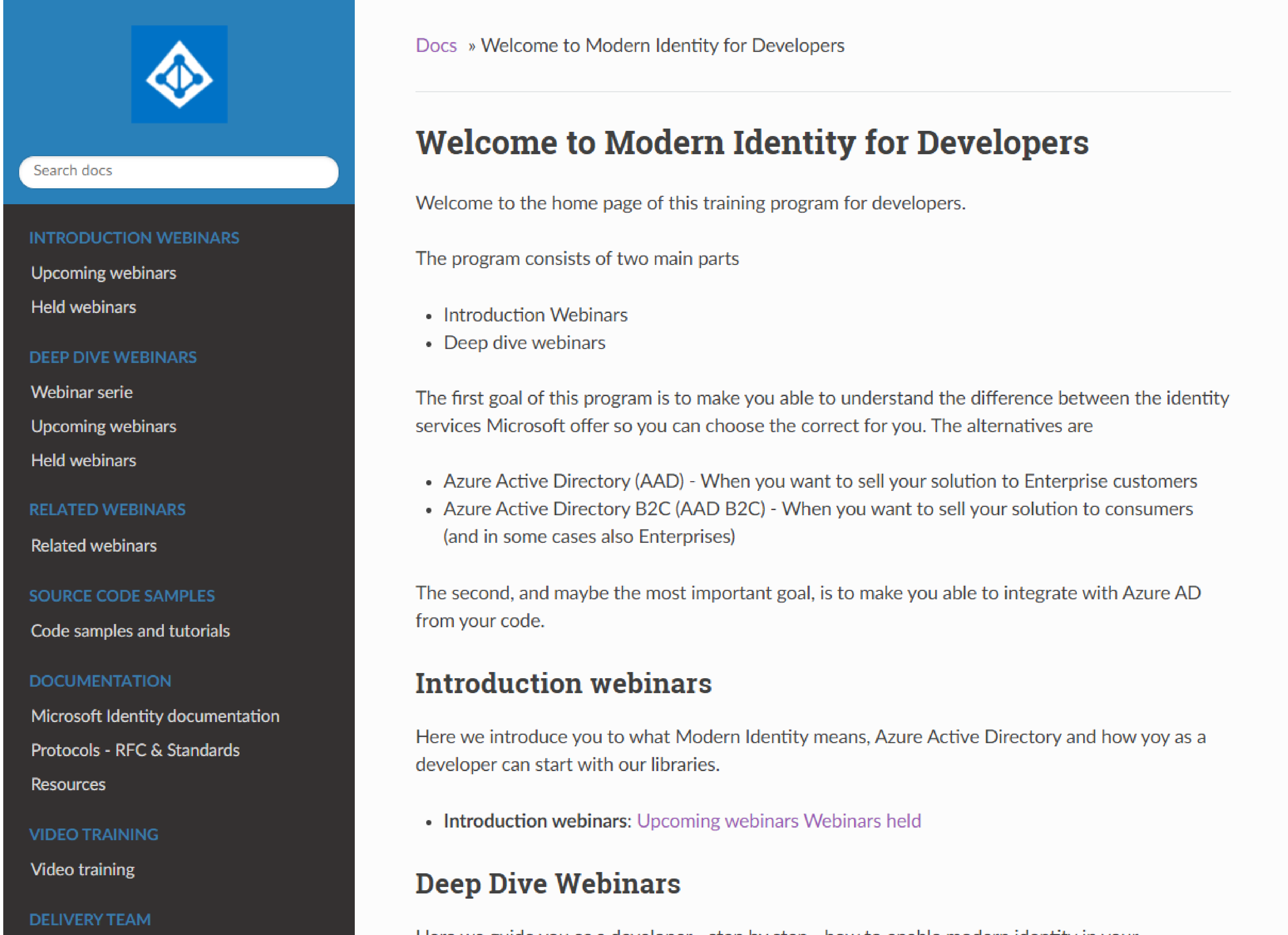
1. Adding Authentication	Week 18
2. Permission and Consent framework	Week 19
3. Accessing and protecting API’s	Week 20
4. Authorization	Week 21
5. Azure Active Directory B2C	Week 22
6. Best practices for securing your services	Week 23

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.



Search docs

INTRODUCTION WEBINARS

Upcoming webinars

Held webinars

DEEP DIVE WEBINARS

Webinar serie

Upcoming webinars

Held webinars

RELATED WEBINARS

Related webinars

SOURCE CODE SAMPLES

Code samples and tutorials

DOCUMENTATION

Microsoft Identity documentation

Protocols - RFC & Standards

Resources

VIDEO TRAINING

Video training

DELIVERY TEAM

Docs » Welcome to Modern Identity for Developers

Welcome to Modern Identity for Developers

Welcome to the home page of this training program for developers.

The program consists of two main parts

- Introduction Webinars
- Deep dive webinars

The first goal of this program is to make you able to understand the difference between the identity services Microsoft offer so you can choose the correct for you. The alternatives are

- Azure Active Directory (AAD) - When you want to sell your solution to Enterprise customers
- Azure Active Directory B2C (AAD B2C) - When you want to sell your solution to consumers (and in some cases also Enterprises)

The second, and maybe the most important goal, is to make you able to integrate with Azure AD from your code.

Introduction webinars

Here we introduce you to what Modern Identity means, Azure Active Directory and how yoy as a developer can start with our libraries.

- **Introduction webinars:** Upcoming webinars Webinars held

Deep Dive Webinars

Here we guide you as a developer - step by step - how to enable modern identity in your

Microsoft

http://aka.ms/modernIdentityForDevelopers

Ronny.Hansen@Microsoft.com