Thomas Naunheim

Manage and Secure Your Customer Identities with Azure AD B2C!

GERMAN 13:00

#ScottishSummit2021

Our Sponsors

ScriptRunner®
The #1 for PowerShell Management

DQ GLOBAL
DRIVING DATA QUALITY

PROXIMO 3
Microsoft Consulting Specialists

Redspire

Agilisys

Hitachi Solutions

Thomas Naunheim

Cloud Architect

Speaker & Blogger

Work and live in Koblenz, Germany

Focus on Identity + Security in Microsoft Azure

Member of „Azure Meetup Bonn“ Orga Team

@Thomas_Live

www.cloud-architekt.net

Microsoft MVP

Agenda

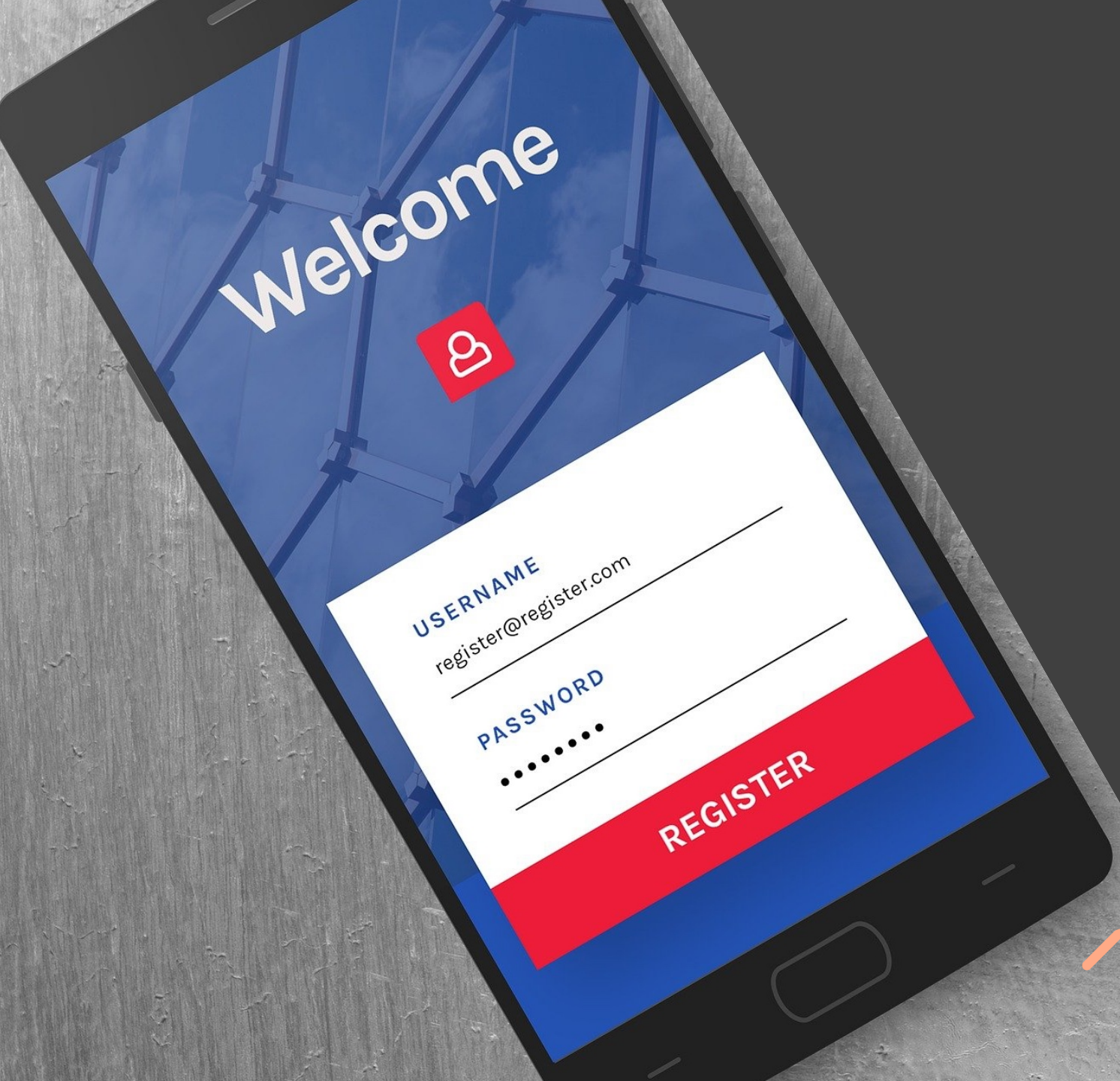
Overview and B2C Tenant

User Flows and App Integration

Branding and Customizing

Protection of B2C Identities

Monitoring and Operations



Azure AD B2C

Overview and B2C Tenant

Scottish Summit 2021

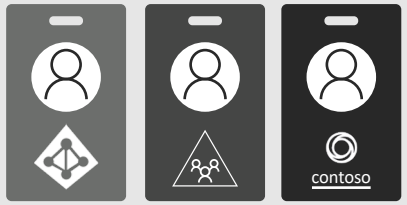
Azure Active Directory B2C

Customers

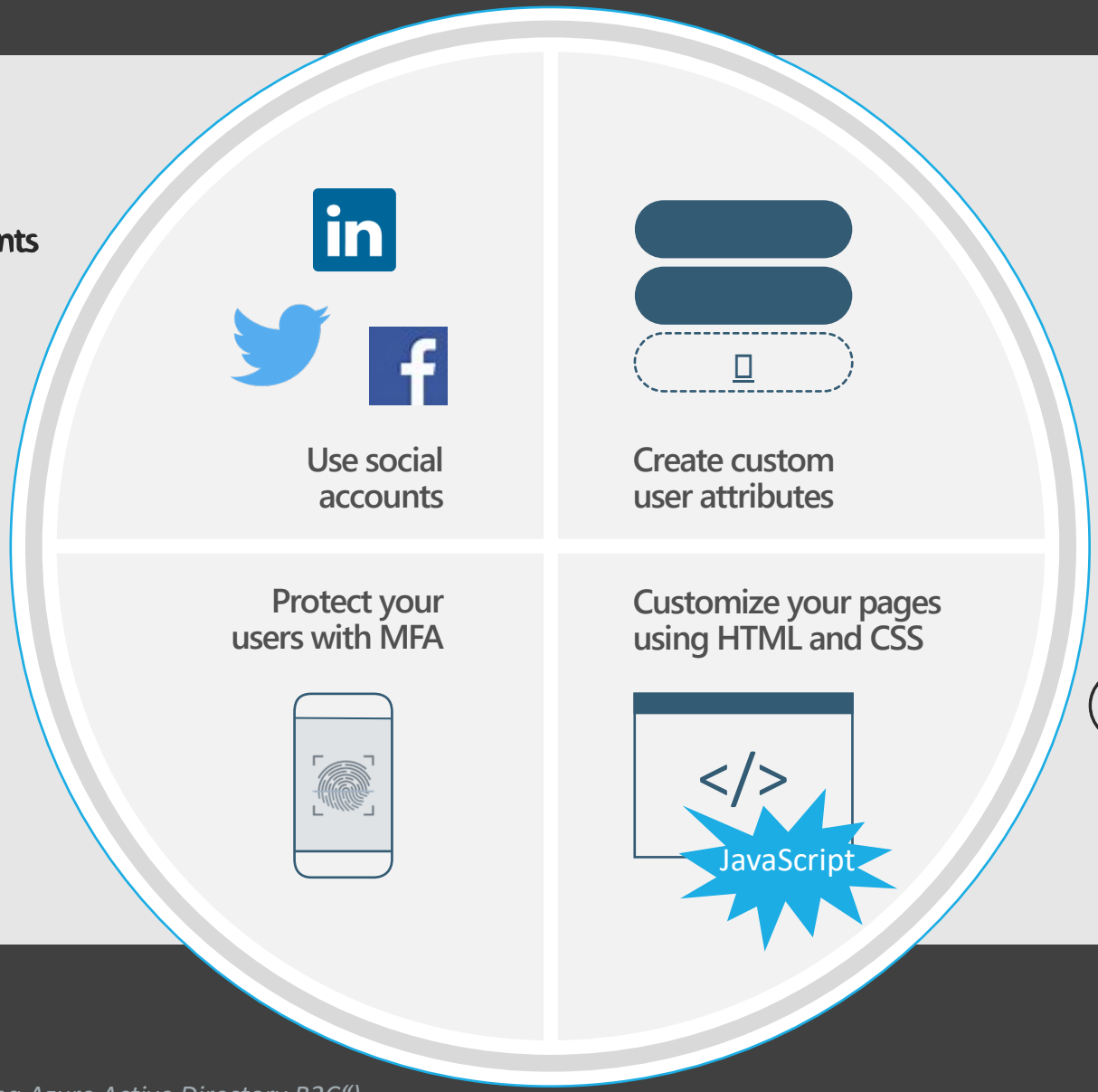
Social IDs, email, or local accounts

Any SAML Provider

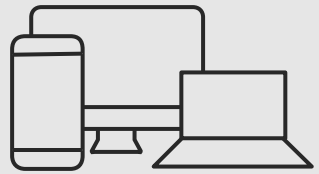
Business & Government IDs



Any OIDC Provider

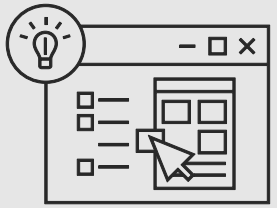


Business



Apps and APIs
OAuth2 / SAML

Analytics

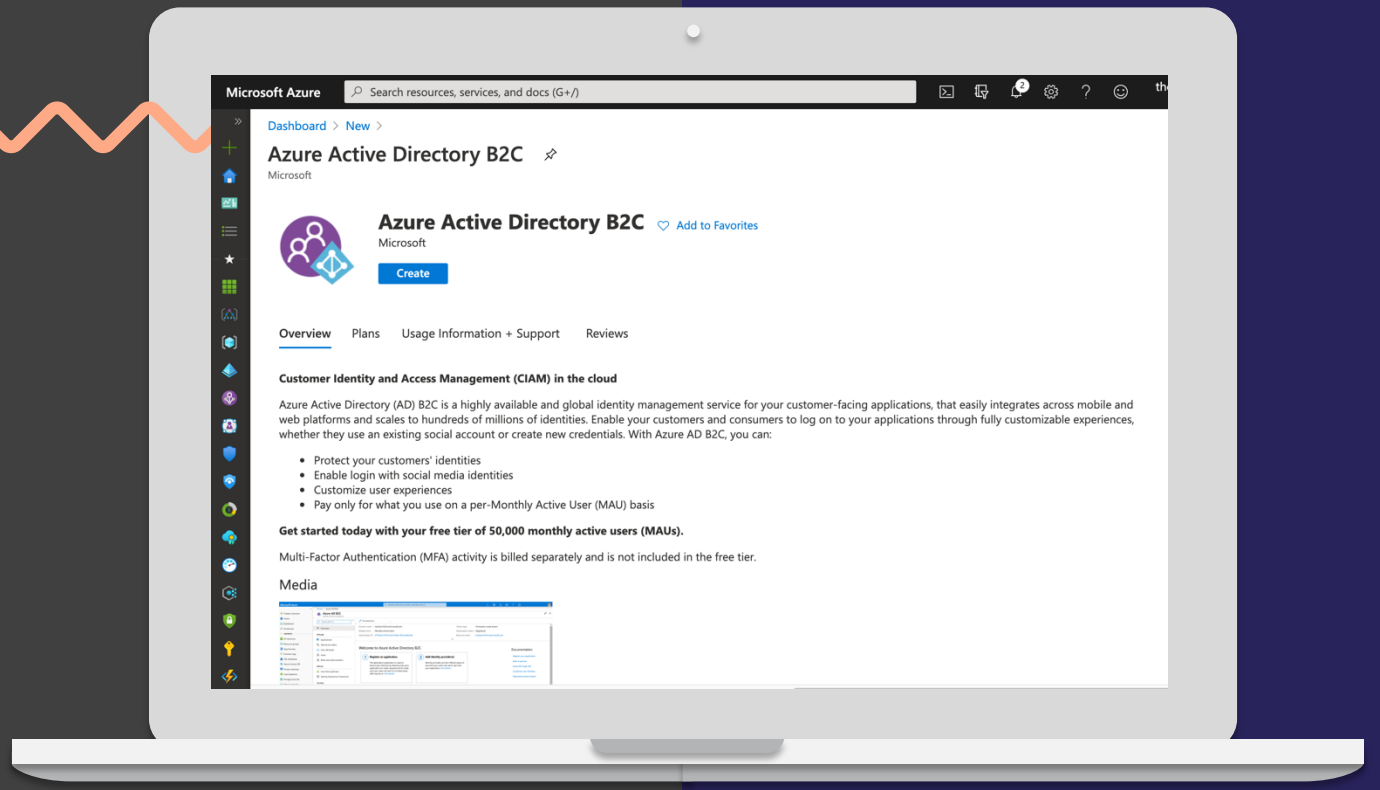


Integration with other systems

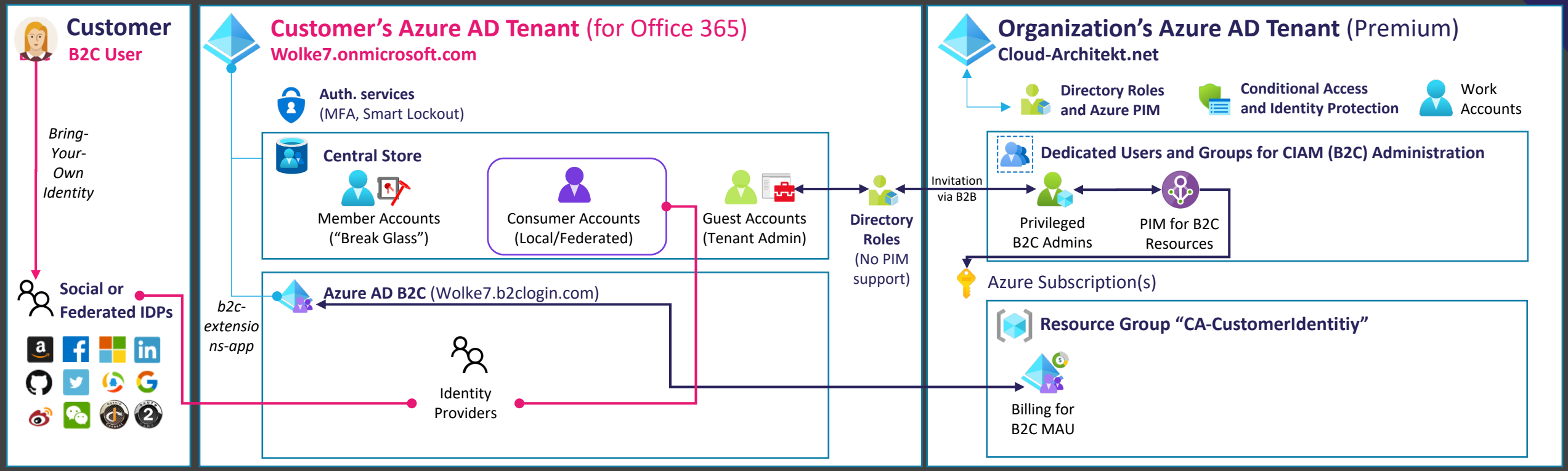
Source: Microsoft (BRK3240 „Secure CIAM using Azure Active Directory B2C“)

Azure AD B2C

Overview of B2C Tenant



Azure AD (B2C) Tenant(s)

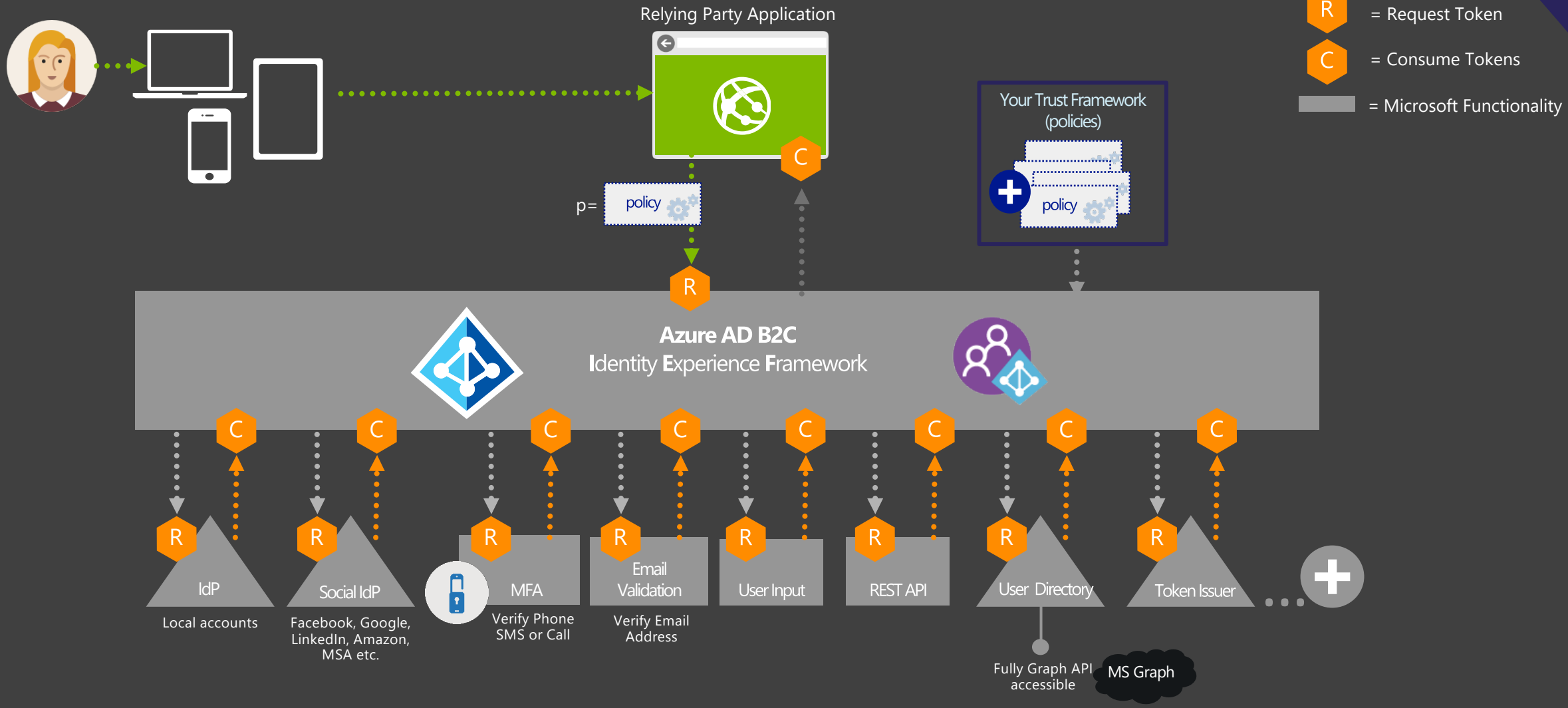


Azure AD B2C

App Integration and User Flows

Scottish Summit 2021

Orchestration and Flows



Source: Microsoft (BRK3240 „Secure CIAM using Azure Active Directory B2C “)

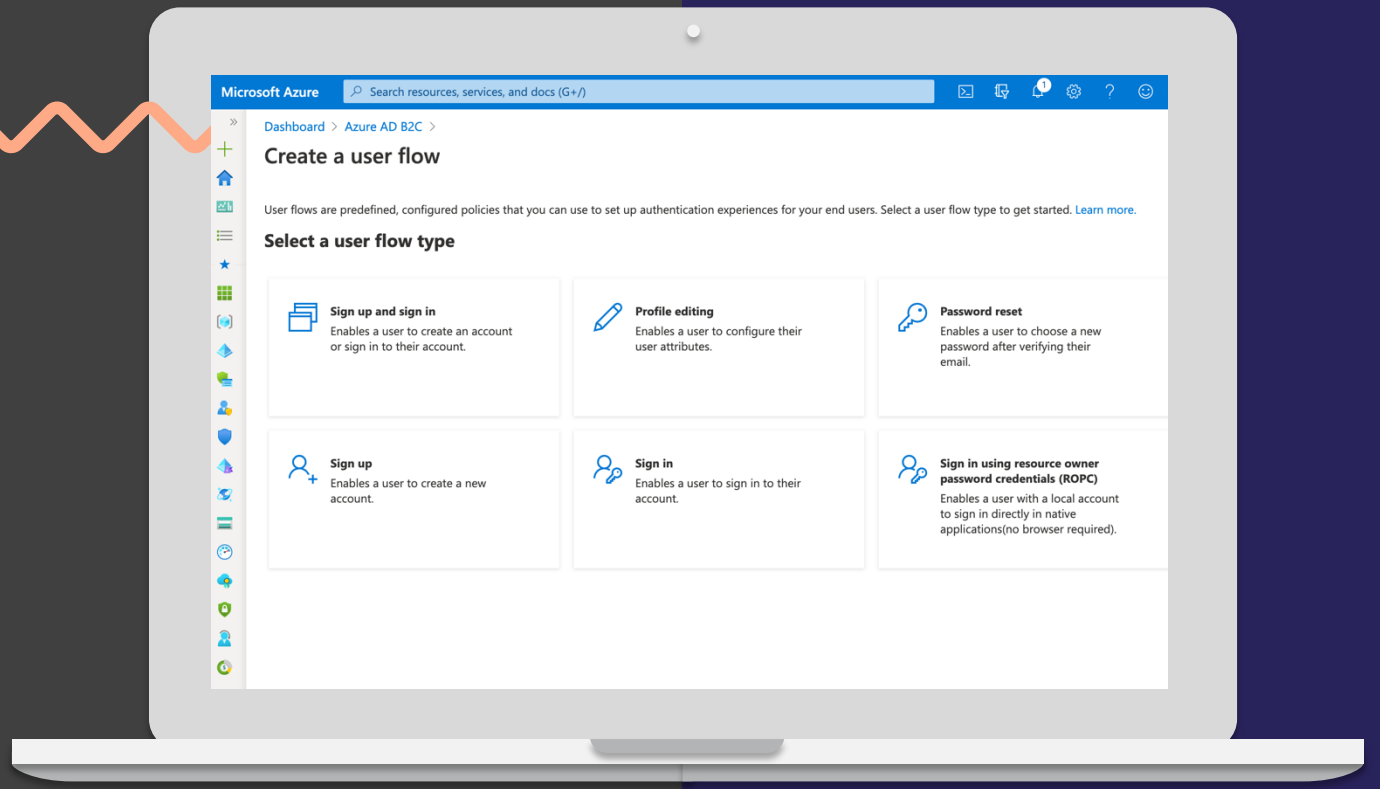
Error Codes and Throttling

- **Error Codes returned by B2C Service**
  - "AADB2C90118": Returned to app for invoking SSPR flow
  - Reference list of error codes

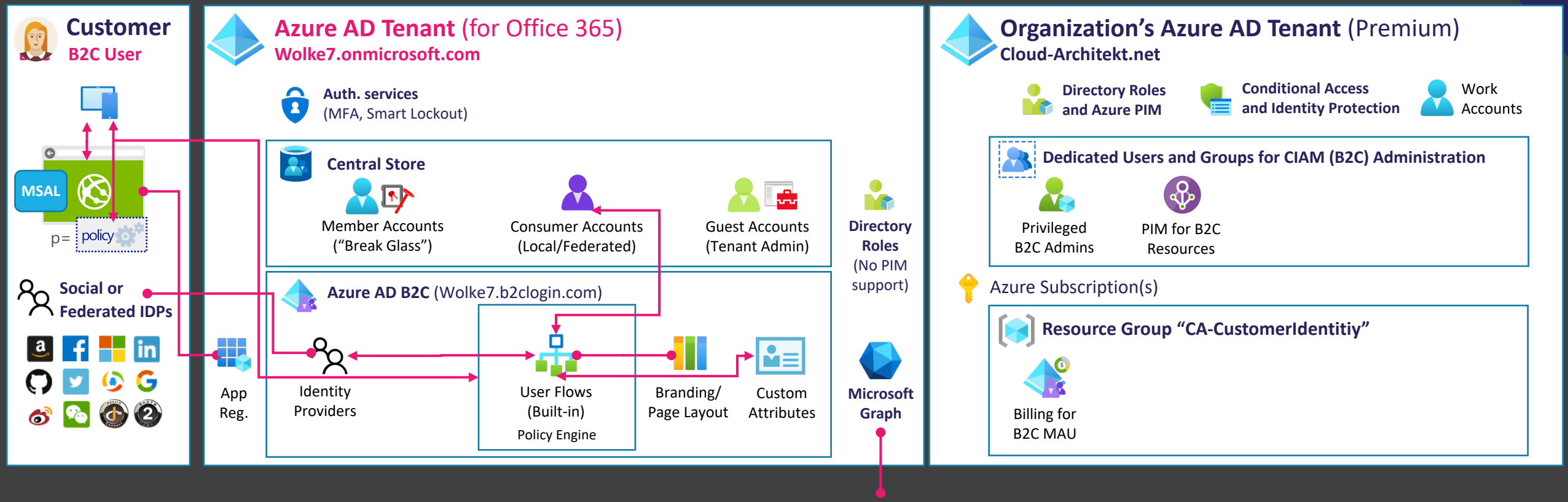
- **Throttling**
  - B2C throttles traffic if too many requests are sent (from the same source in a short period of time).
  - **Monitoring and handle error code** "AADB2C90229"

Azure AD B2C

Built-in User Flow Capabilities (Zero-Code)



User Flows and App Integration



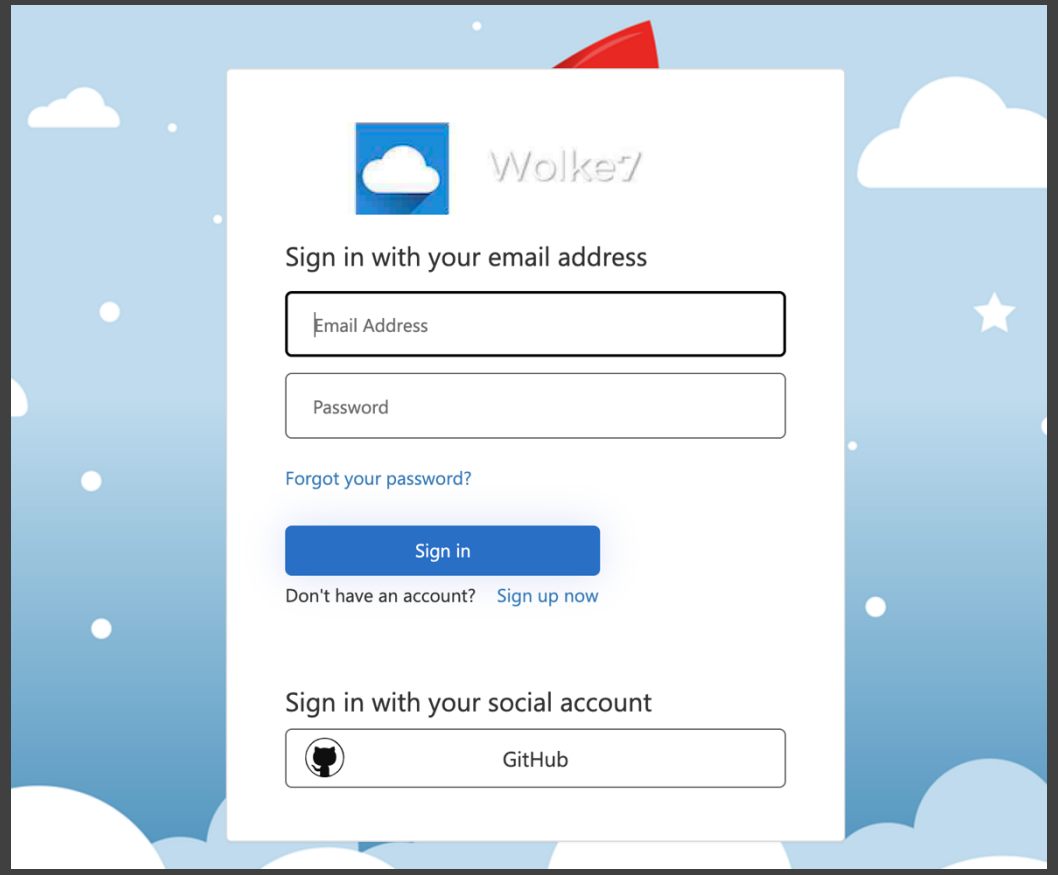
Azure AD B2C

Branding and Customizing

Scottish Summit 2021

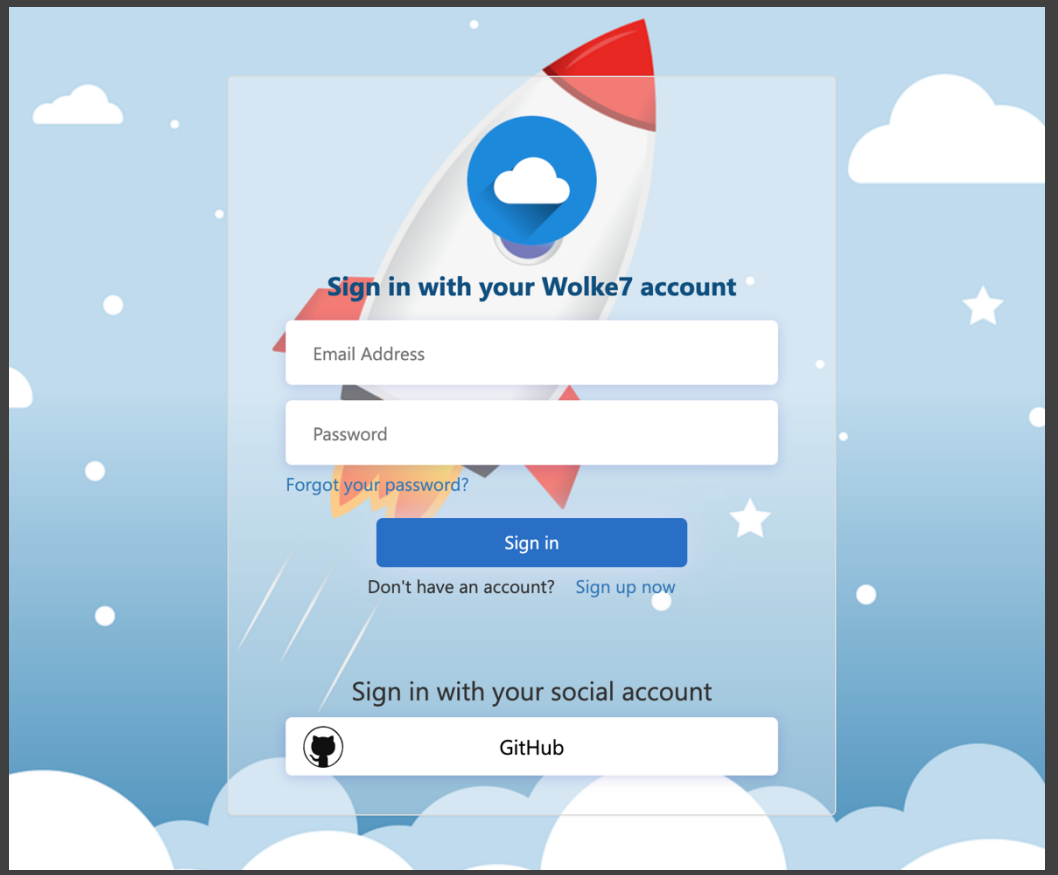
Options for UI Customizing

Company Branding (Recommended Policies)



Limitation of Azure AD's Company Branding

Custom Page Layout (All Policies)



Customizing of Template "Ocean Blue"

Options for UI Customizing

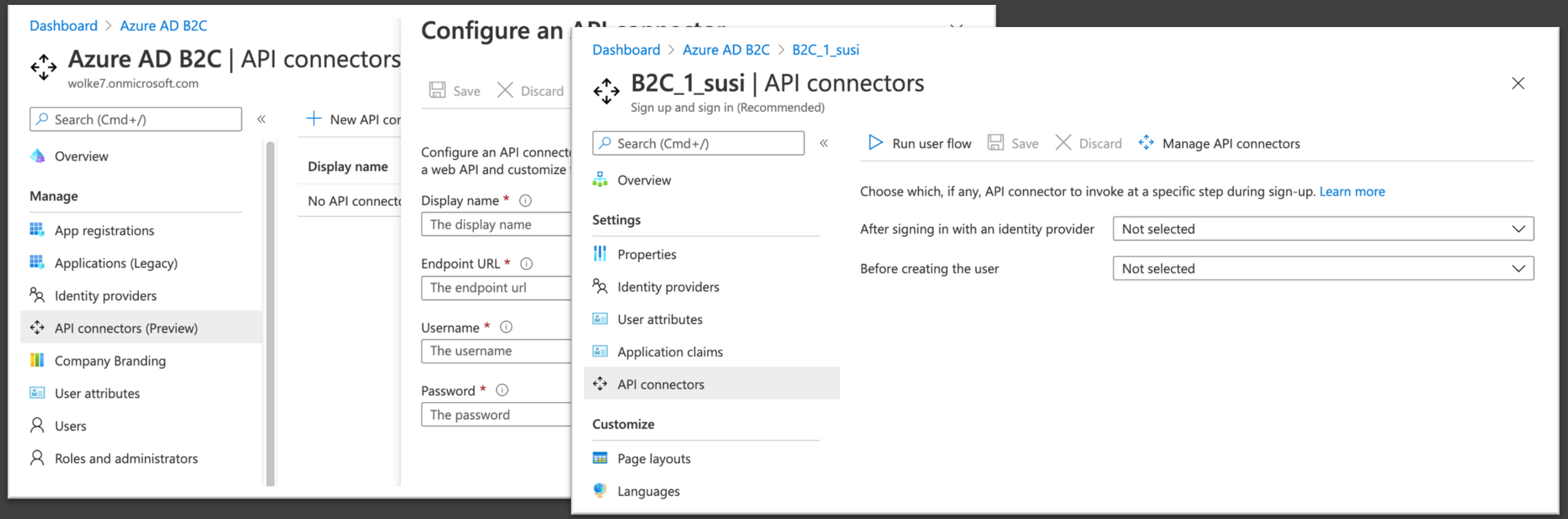
- **Custom Page Layout**
  - Customize UI with (hosted) HTML/CSS files
    - Sample HTML and CSS files available on GitHub
    - Hosting the page content (publicly available HTTP endpoint that supports CORS, CDN recommended)
  - Your own JavaScript client-side code, consider guidelines!
- **Domain Customization**
  - Default: https://{your-tenant-name}.b2clogin.com/{your-tenant-id}
  - Customer-Owned Domains: Announced as Public Preview in 2021 → UserVoice

Custom email verification (Custom Policies only)

- Send customized email using 3rd party provider (SendGrid, Mailjet,…)

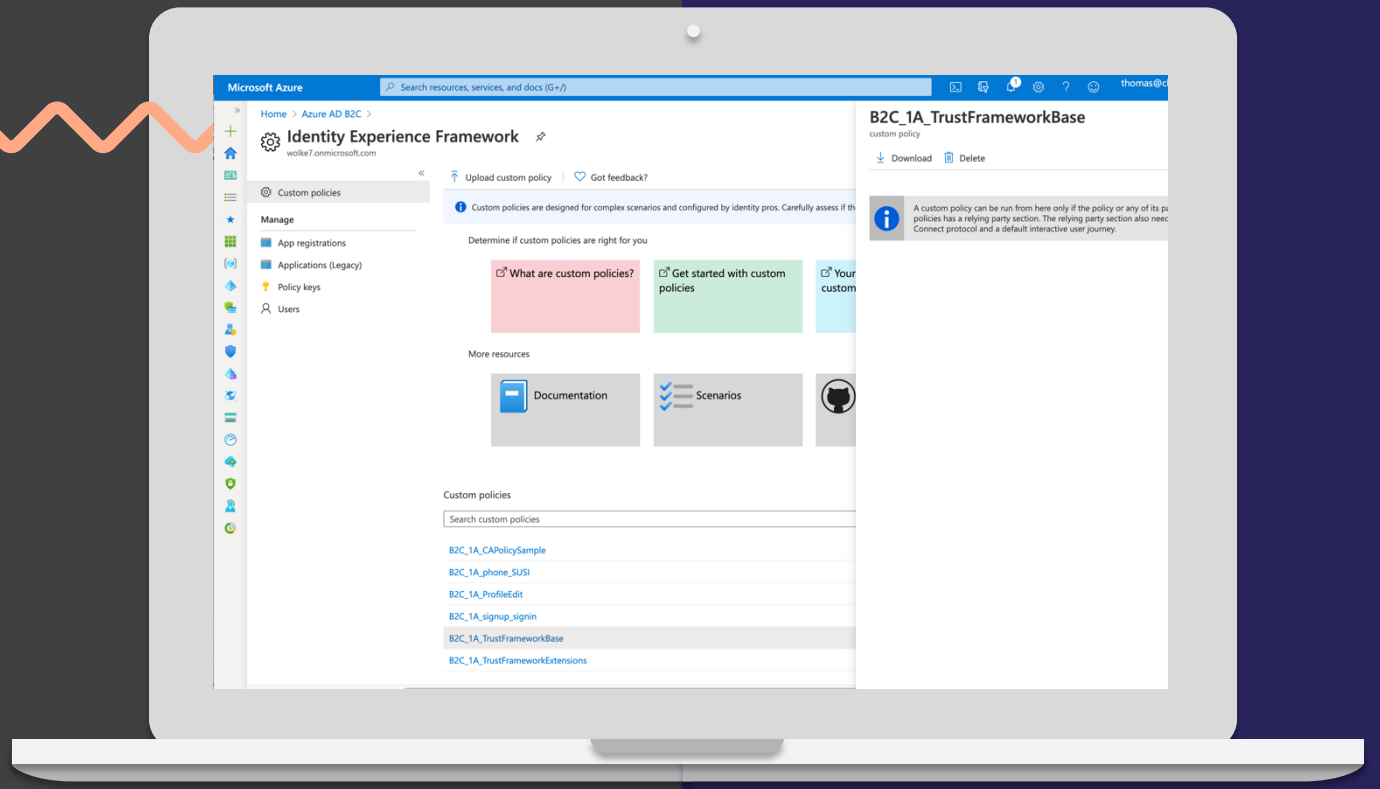
API Connectors (Preview)

- **Simple and secure customization and extension of user flows** for
  - Protect against automated fraud abuse (CAPTCHA)
  - Use invitation codes or perform identity verification
  - Reformat of attribute values or update from/to corporate database

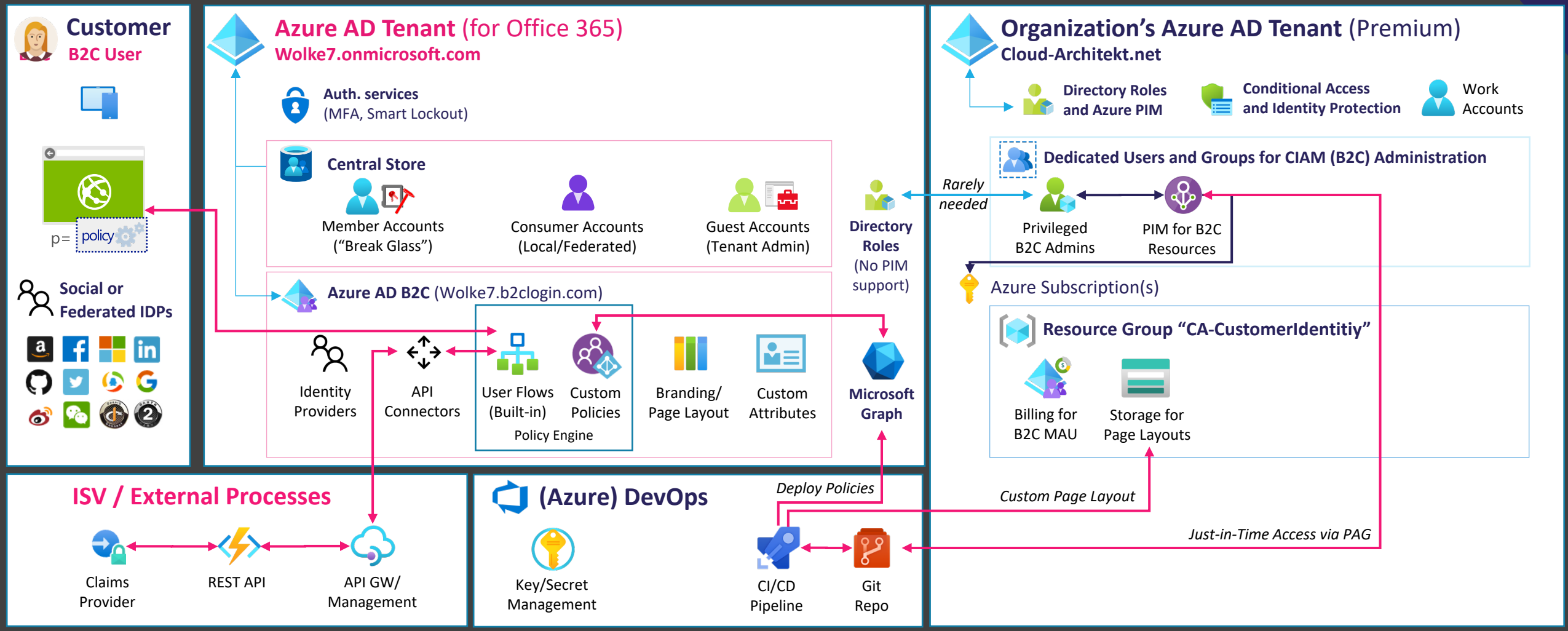


Azure AD B2C

Custom Policies (Templates) & Deployment



Branding and Customizing



Azure AD B2C

Protection of B2C identities

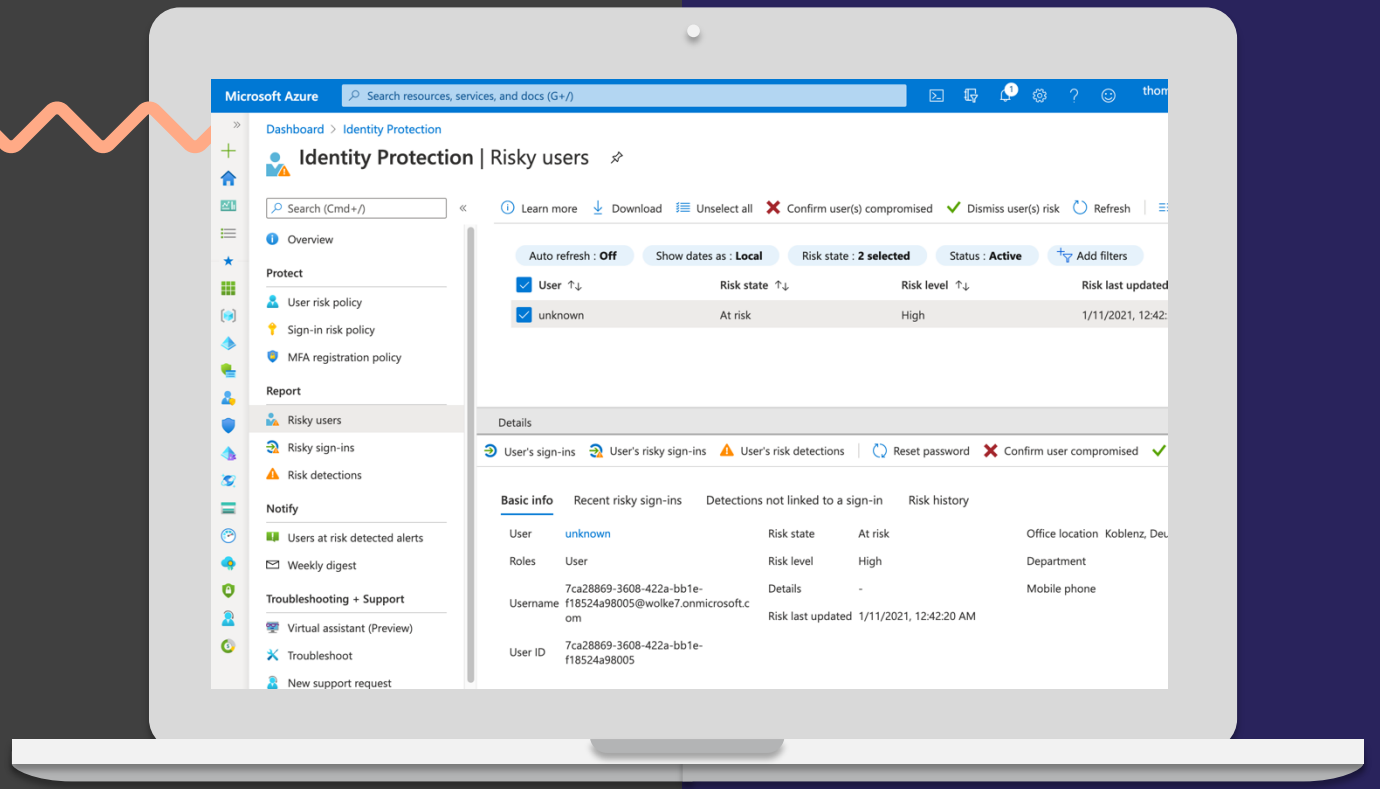
Scottish Summit 2021

Conditional Access in B2C

Source: Microsoft (Leveraging Advanced Security in Azure AD B2C)

Azure AD B2C

Identity Protection & Conditional Access



Protection of B2C identities

Customer
B2C User

MSAL
p= policy

Social or Federated IDPs

Azure AD Tenant (for Office 365)
Wolke7.onmicrosoft.com

Auth. services (MFA, Smart Lockout)

Identity Protection (excl. Social IdPs)

Conditional Access (for Customers/Admins)

Central Store
Member Accounts ("Break Glass")

Consumer Accounts (Local/Federated)

Guest Accounts (Tenant Admin)

Azure AD B2C (Wolke7.b2clogin.com)
App Reg.

Identity Providers

API Connectors

User Flows (Built-in)

Custom Policies

Policy Engine

Branding/ Page Layout

Custom Attributes

Directory Roles (No PIM support)

Microsoft Graph

Organization's Azure AD Tenant (Premium)
Cloud-Architekt.net

Directory Roles and Azure PIM

Conditional Access and Identity Protection

Work Accounts

Dedicated Users and Groups for CIAM (B2C) Administration
Privileged B2C Admins

PIM for B2C Resources

Azure Subscription(s)
Resource Group "CA-CustomerIdentitiy"
Billing for B2C MAU

Storage for Page Layouts

ISV / External Processes
Claims Provider

REST API

API GW/ Management

(Azure) DevOps
Key/Secret Management

CI/CD Pipeline

Git Repo

Azure AD B2C

Monitoring and Operations

Scottish Summit 2021

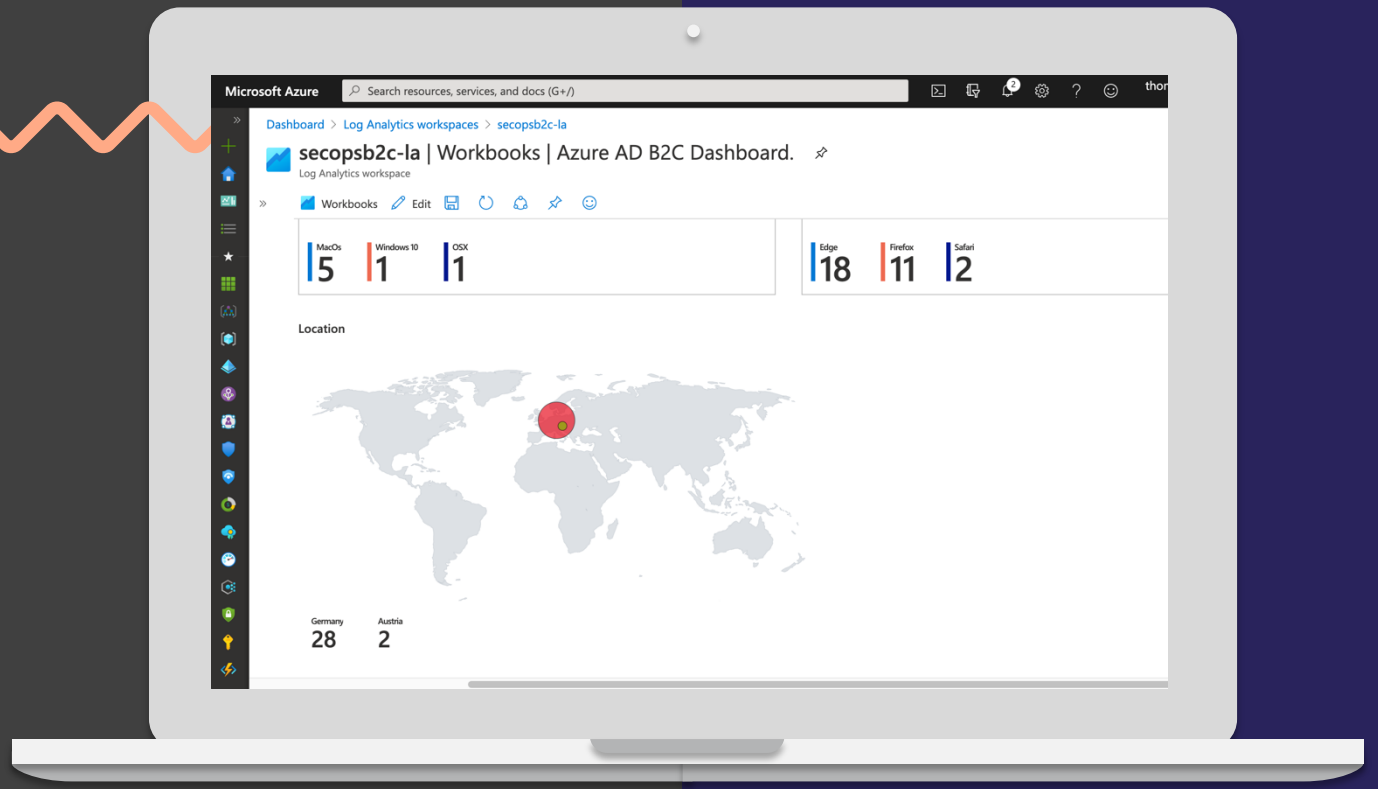
Monitoring

- **Route logs to “Azure Monitor”**, Storage (Long-term use) or 3rd Party SIEM (EventHub)

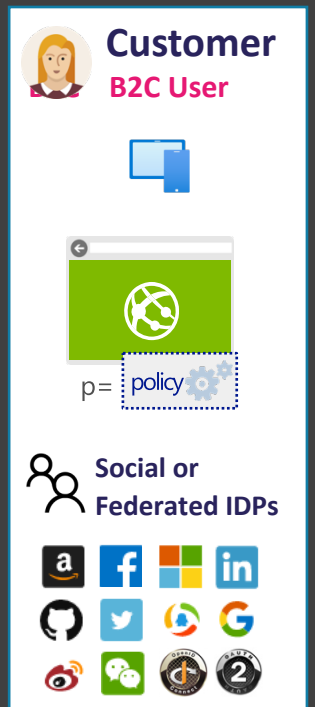
  Service Health Alerts of B2C Platform and dependencies (incl. CDN, Functions, etc.)

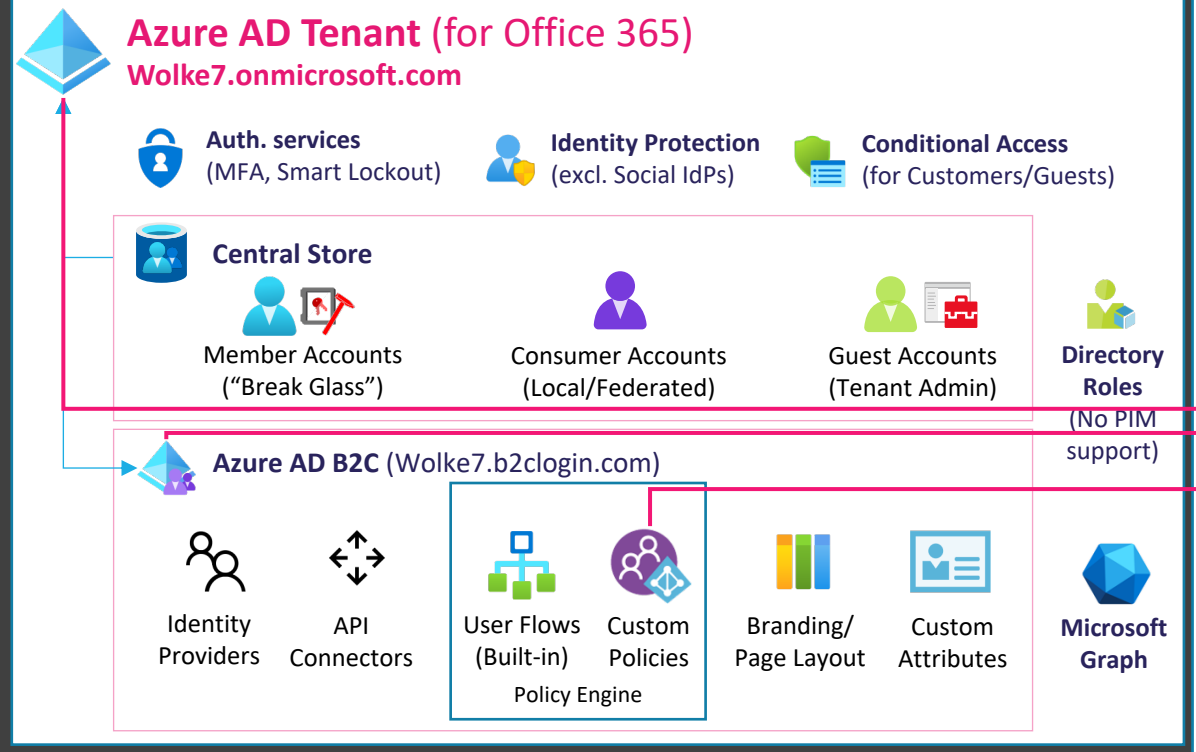
- **Track “user behavior” (Usage Analytics) in Custom Policies with “Application Insights”**

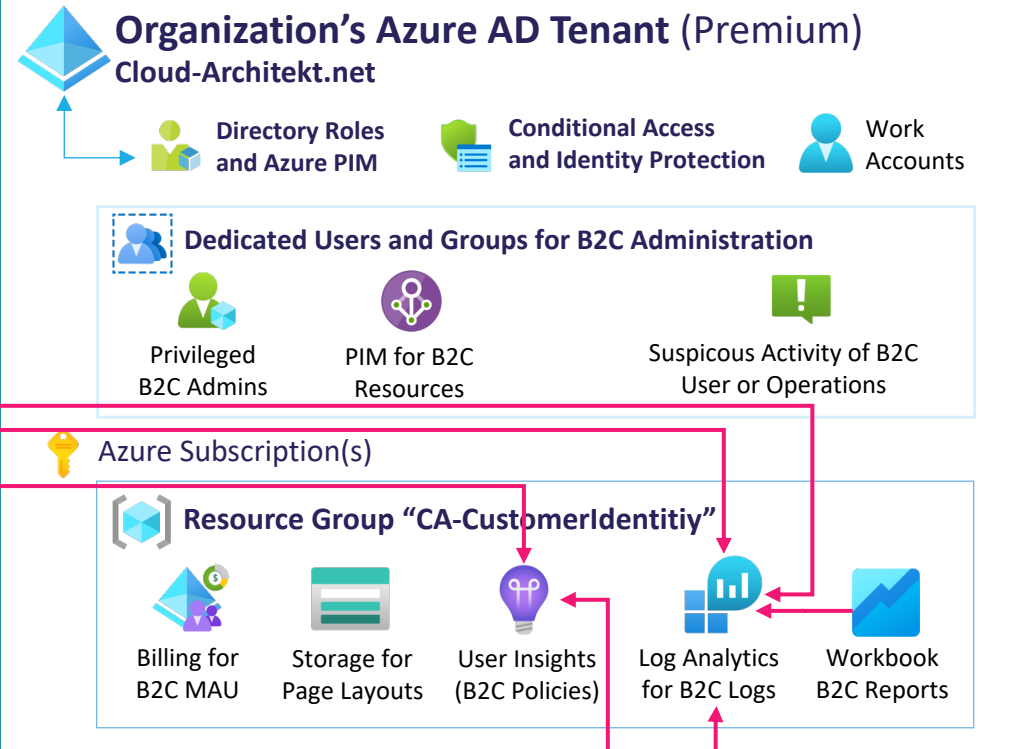
Azure AD B2C
Dashboard
for Operations

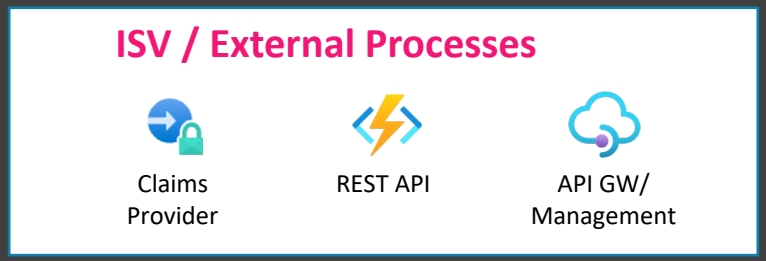


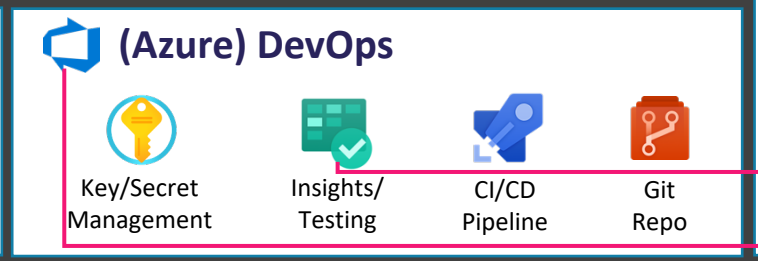
Management and Operations











Usage analytics and policy insights

Auditing of Repo, Service connections and Pipelines

#ScottishSummit2021

Thank You