CIAM/External Identity Management made easy

→ Jamie Vaughan – External Identity Architect,

Harsha Doddamane – Senior External Identity Consultant

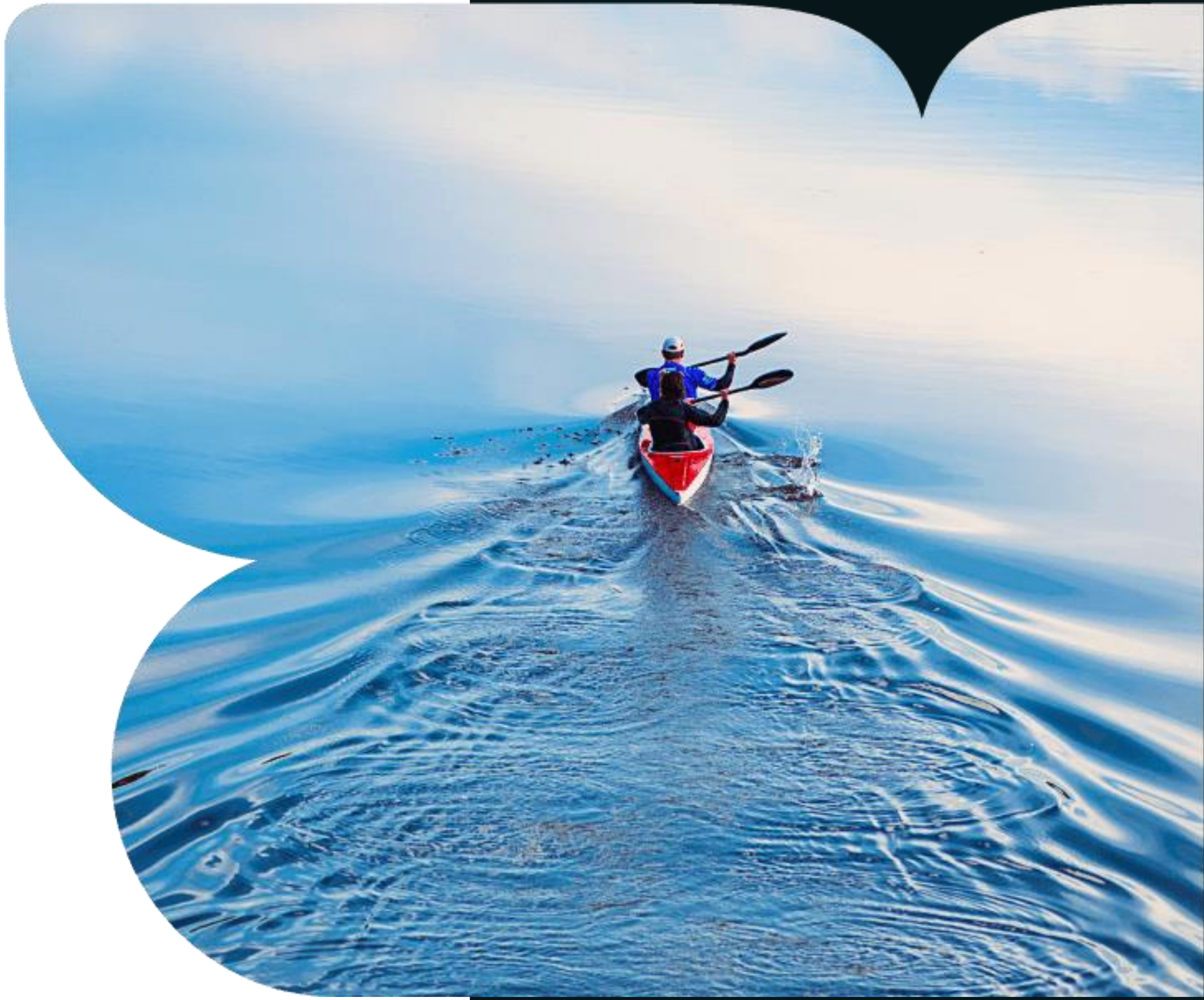
Jas Suri – Senior Program Manager, Microsoft

Kocho

BECOME GREATER

Agenda

- → Introduction
- → Azure AD B2C
- → Authentication Protocols
- → Challenges
- → Workshop



Introductions

Numbers Game

43

Trillion threat signals
processed every day

130

130 Billion authentications per day
Up from 60Billion a month (Jan 2017)

34,740

Password attacks every minute

70

Billion attacks prevented

26

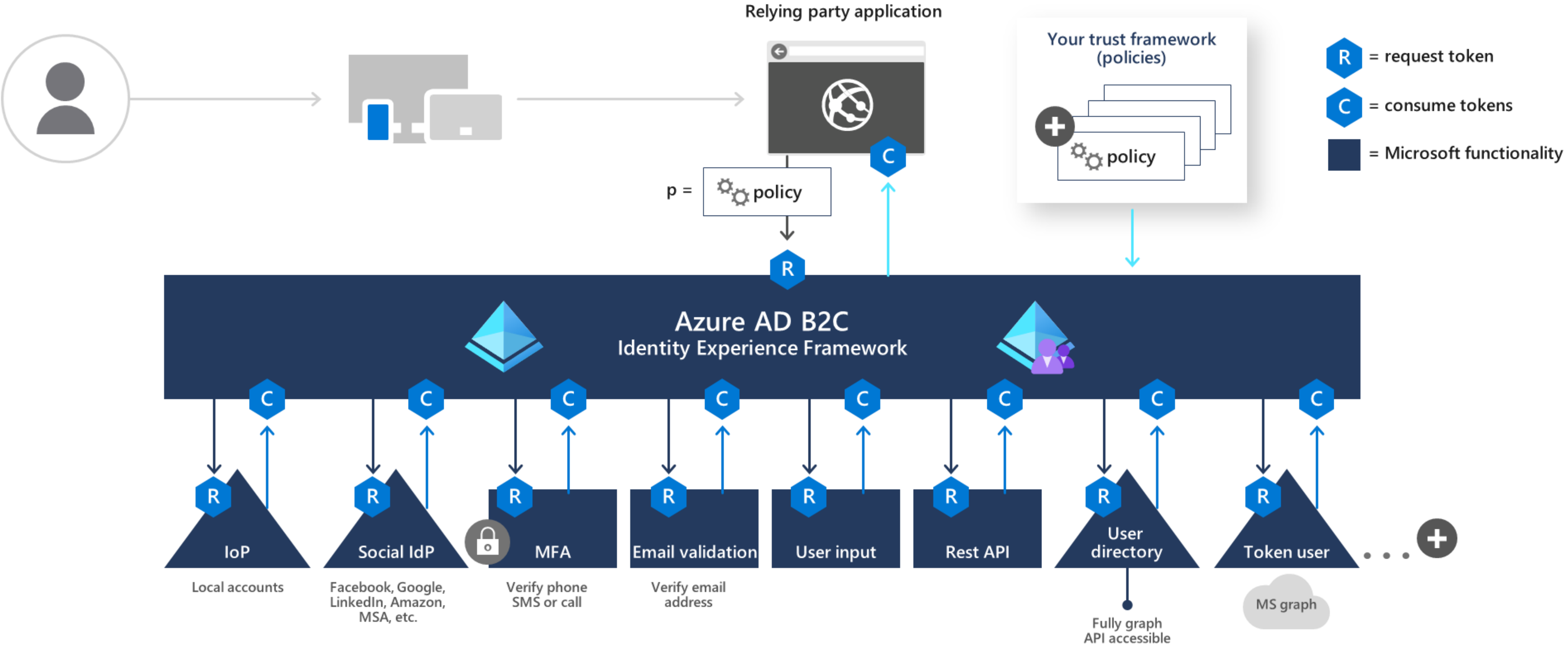
% of companies turned on MFA

20

$20 billion Microsoft investment
in Security over the next 5 years

Azure AD B2C

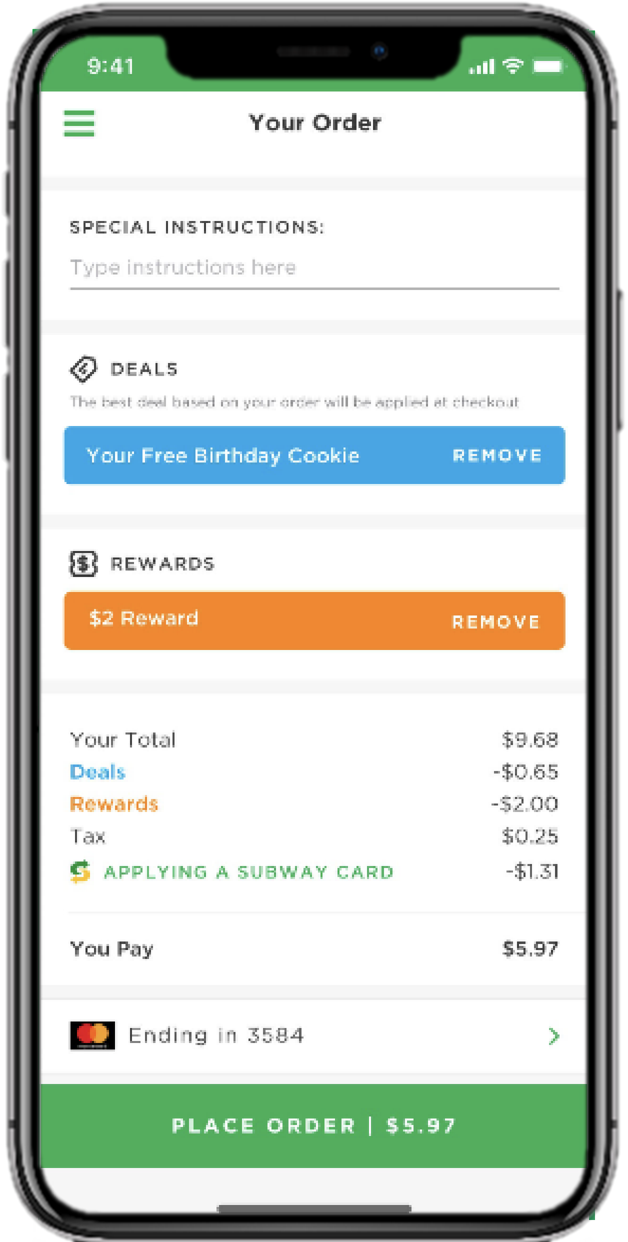
Microsoft’s identity experience framework



Fraud Detection and Protection

- Integrate with third part solutions such as Dynamics 365 Fraud Protection or Arkose Labs
  - Validate traffic during signup and signin
  - Uses signals collected in the web browser and server
  - Real time risk validation
- Complements Identity protection

User Experience



9:41

Your Order

SPECIAL INSTRUCTIONS:

Type instructions here

DEALS

The best deal based on your order will be applied at checkout

Your Free Birthday Cookie REMOVE

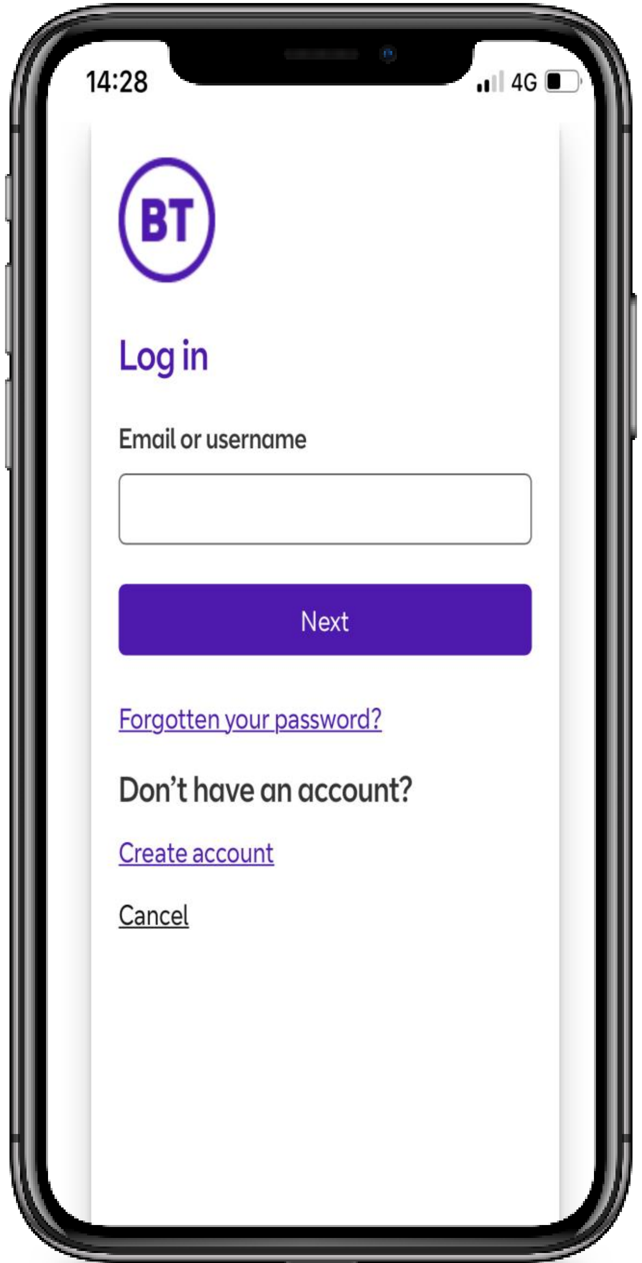
REWARDS

$2 Reward REMOVE

Your Total	$9.68
Deals	-$0.65
Rewards	-$2.00
Tax	$0.25
APPLYING A SUBWAY CARD	-$1.31
You Pay	$5.97

Ending in 3584

PLACE ORDER | $5.97



14:28 4G

BT

Log in

Email or username

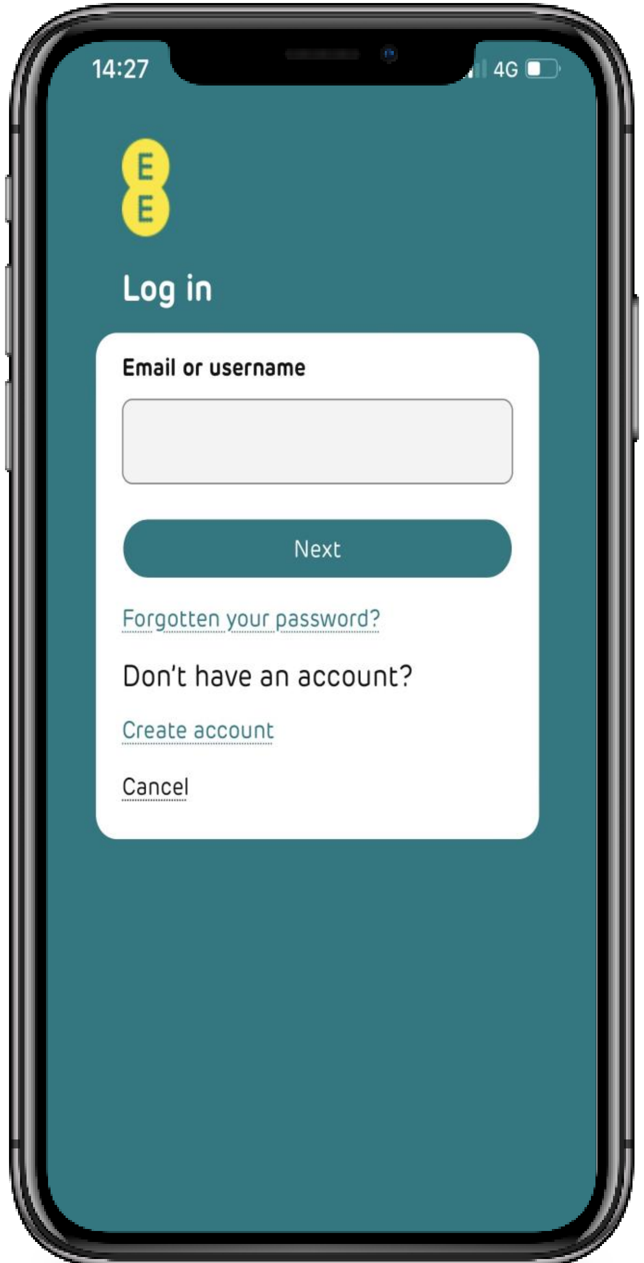
Next

Forgotten your password?

Don't have an account?

Create account

Cancel



14:27 4G

EE

Log in

Email or username

Next

Forgotten your password?

Don't have an account?

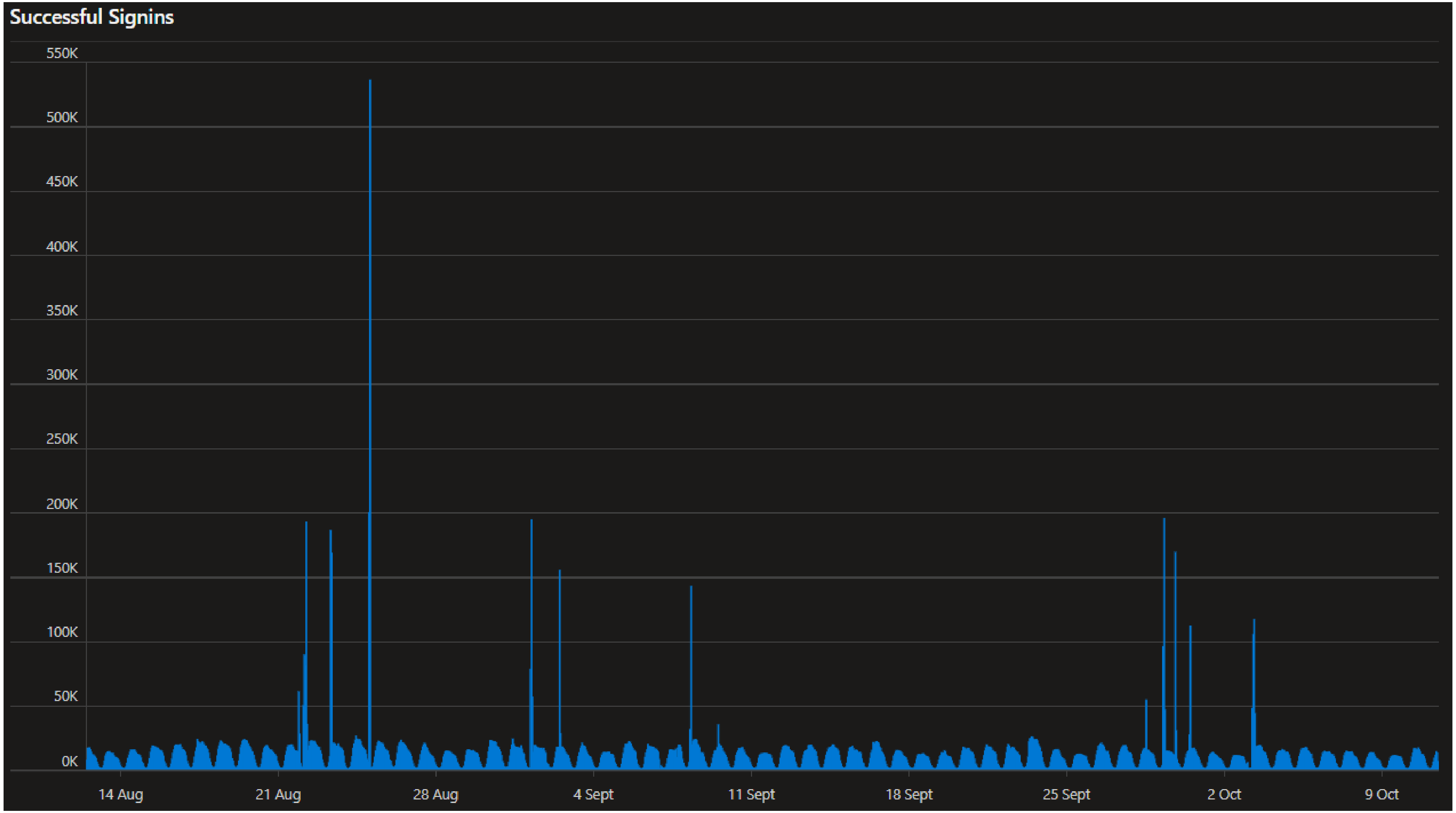
Create account

Cancel

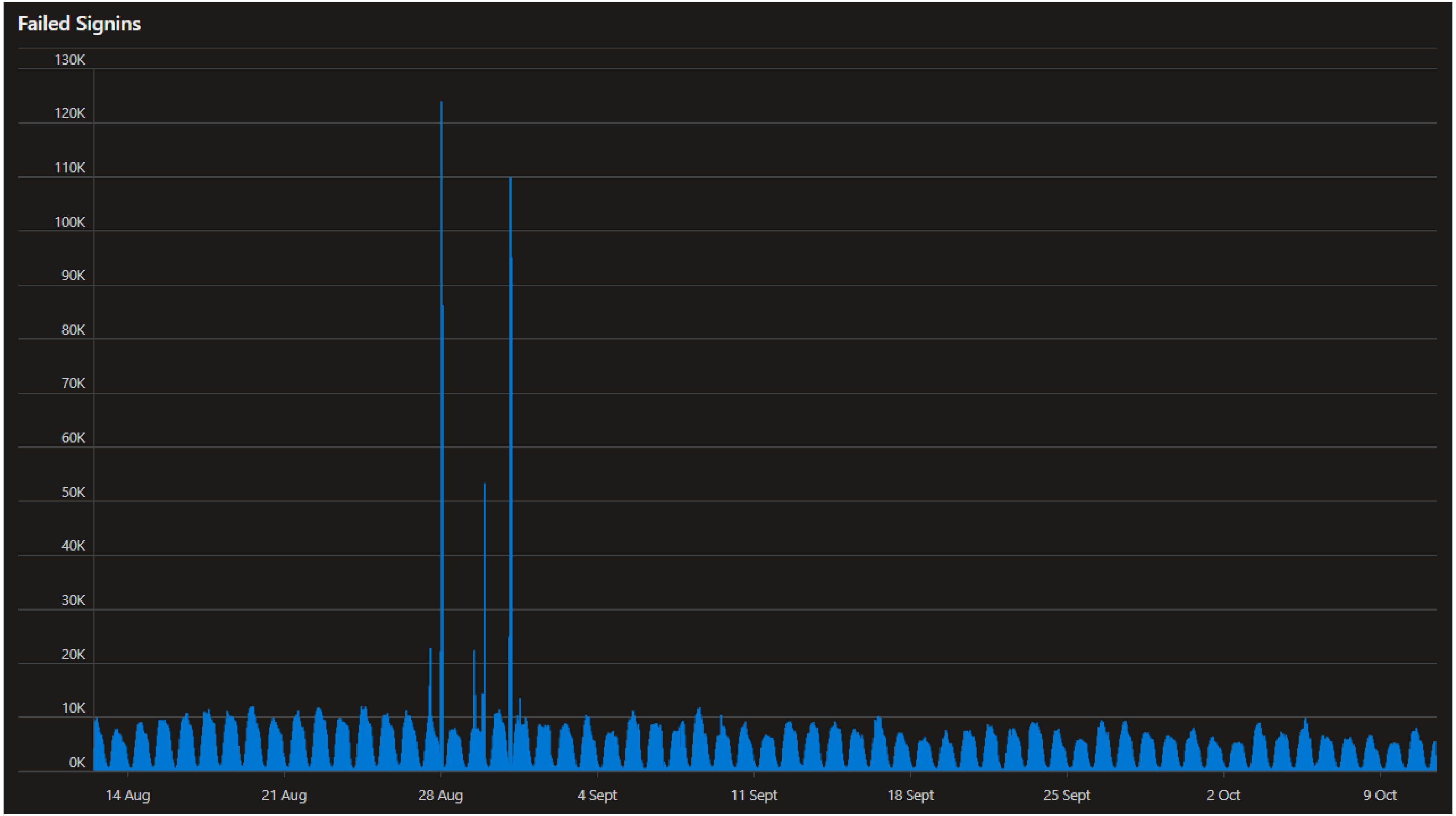
Monitoring & SEIM

- Stream to Log Analytics
- Setup events with Azure Monitor
- Threat hunting with Sentinel
- User Insights

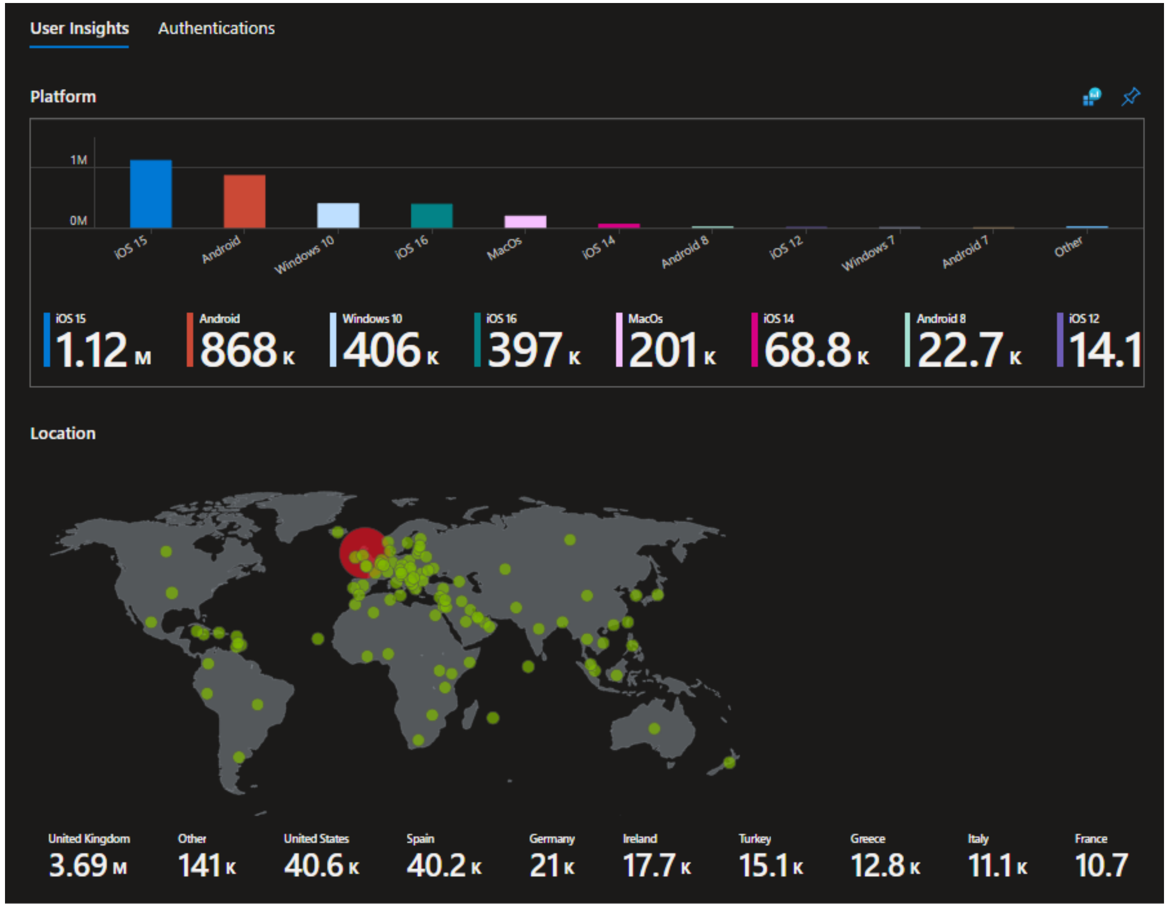
Successful Signins



Failed Signins



User Insights

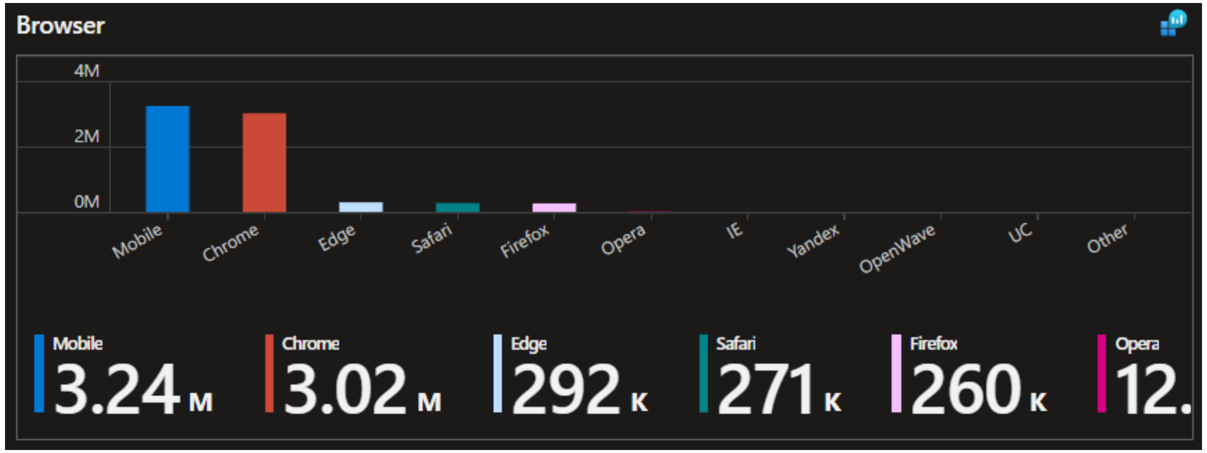


Platform

iOS 15	Android	Windows 10	iOS 16	MacOs	iOS 14	Android 8	iOS 12
1.12 M	868 K	406 K	397 K	201 K	68.8 K	22.7 K	14.1

Location

United Kingdom	Other	United States	Spain	Germany	Ireland	Turkey	Greece	Italy	France
3.69 M	141 K	40.6 K	40.2 K	21 K	17.7 K	15.1 K	12.8 K	11.1 K	10.7

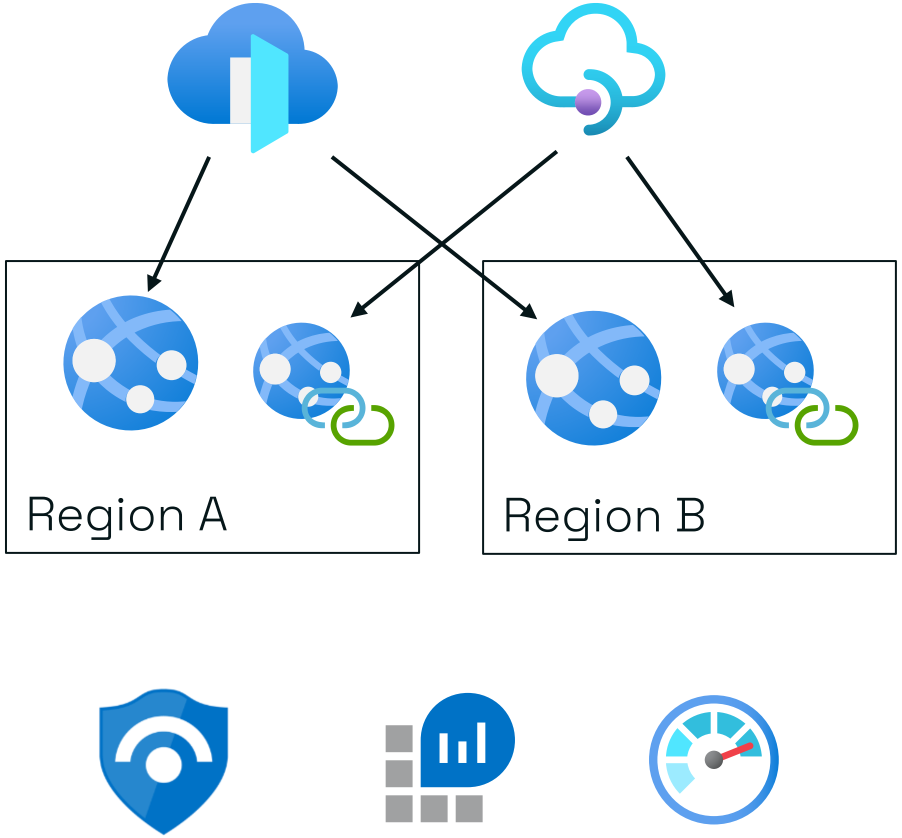


Browser

Mobile	Chrome	Edge	Safari	Firefox	Opera
3.24 M	3.02 M	292 K	271 K	260 K	12.

Scaling your service

- → Leverage Front Door and API Management
- → Scale app services according to your traffic and across regions for redundancy – use auto scaling
- → Monitor with Azure Monitor and Log Analytics
- → Integrate Sentinel for threat hunting



Authentication Protocols

Lamesville -> Awesometown

Authentication Protocols

Resource
Owner

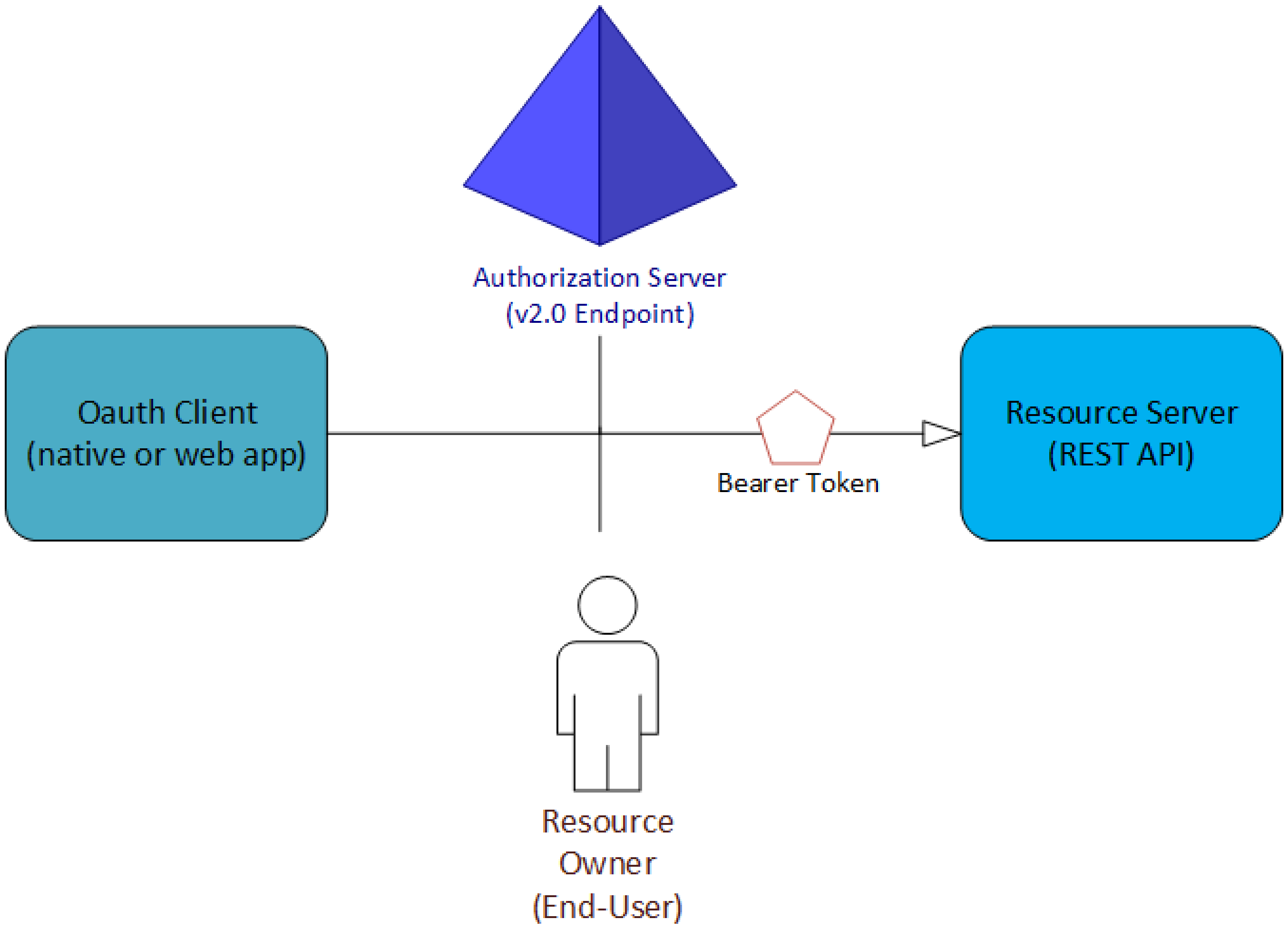
Resource
Server

Authorization
Server

Toke
n

Authentication Protocols

- → Open ID Connect (OIDC)
- → Oauth 2.0
- → SAML 2.0

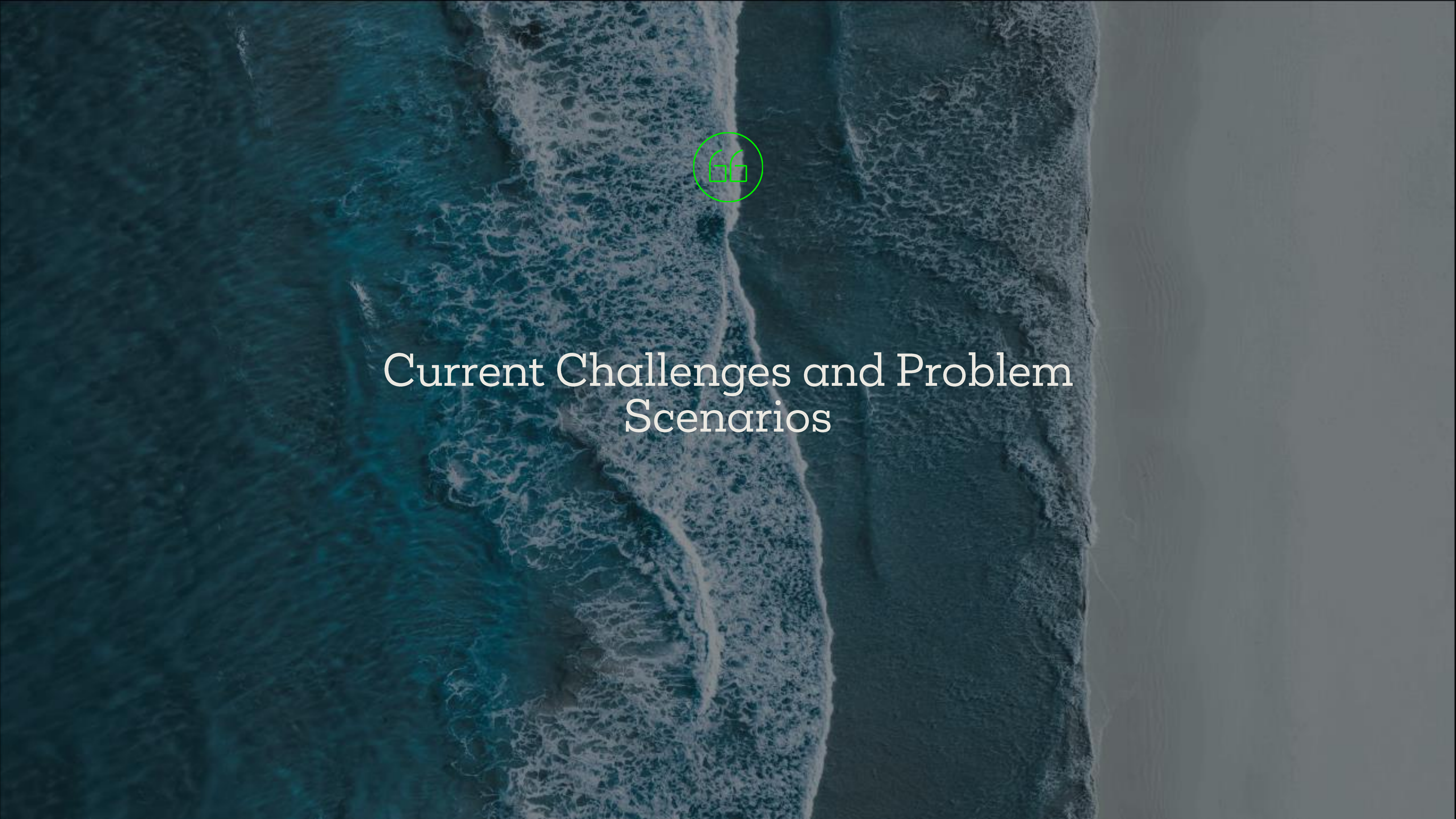


Application Integration

- Always use a production tested library
- OIDC is the preferred protocol
  - Code Grant with PKCE is the preferred flow
- Libraries exist for most dev flavours
- Always use a production tested library
- Always use a production tested library
  - Majority of application vulnerabilities uncovered from developers rolling their own auth.

- Microsoft.Identity.Web for ASP.Net web and API apps
- MSAL.JS for SPA – REACT and Angular wrappers
- Lots of third party approved libs too
  - Apache and NGINX
  - Java
  - PHP

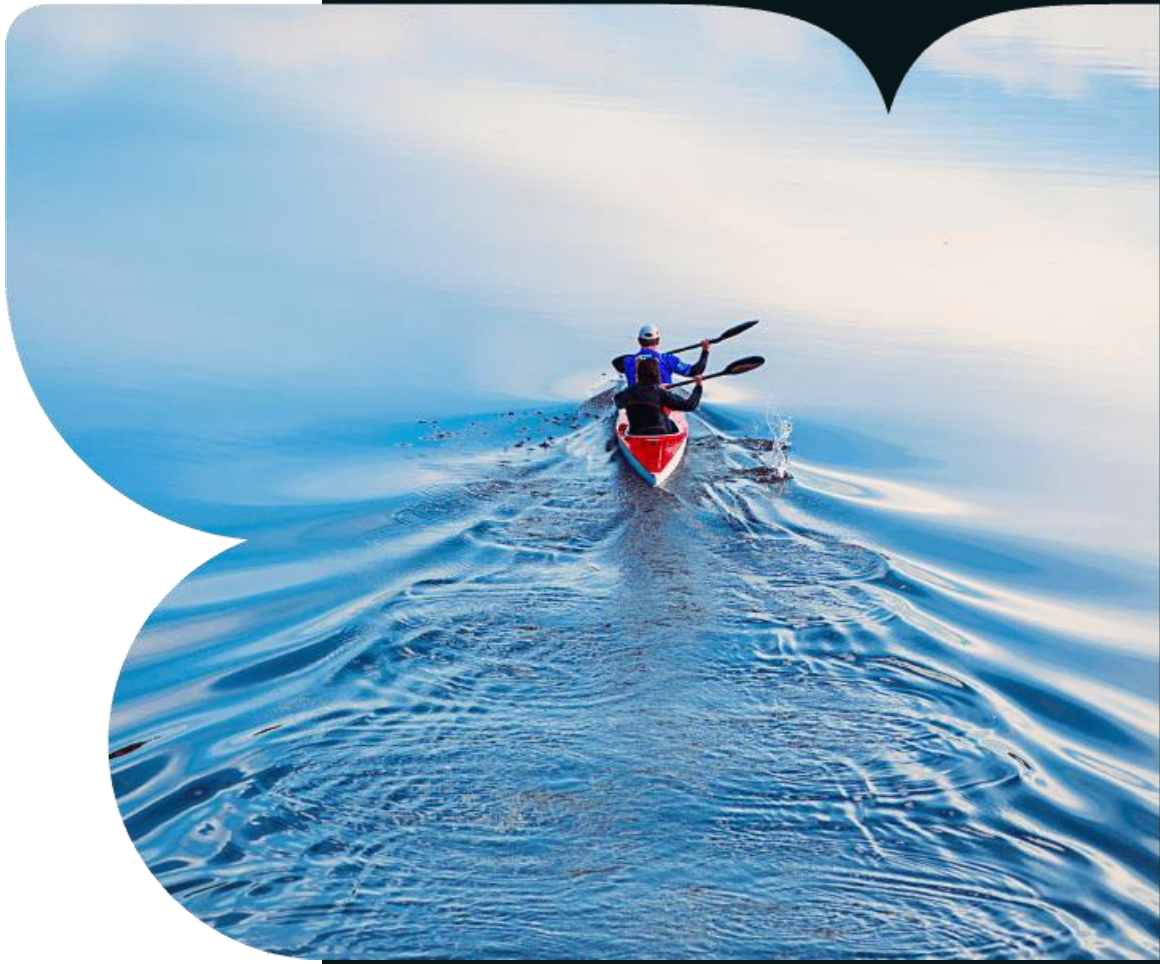
https://openid.net/developers/certified



Current Challenges and Problem Scenarios

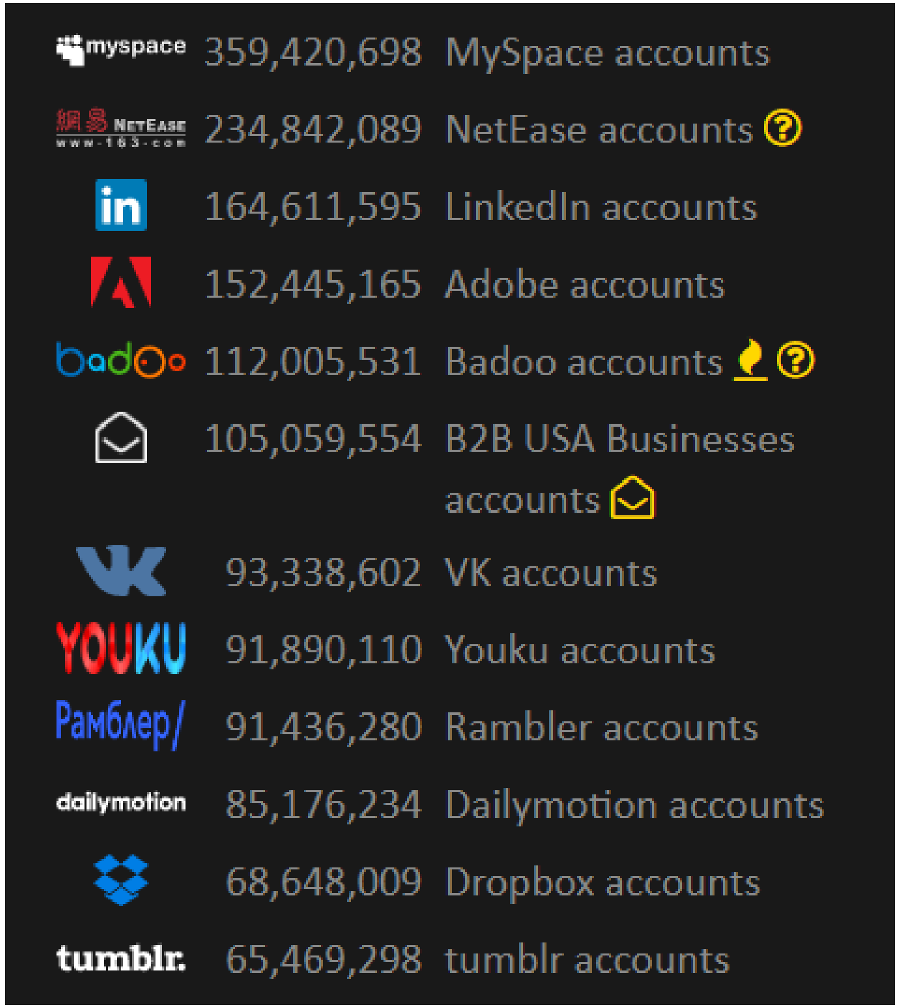
Stopping password reuse

- → Why?
  - → Credential Stuffing attacks are on the rise – 921 password attacked per second
- → How?
  - → Remove complexity – It doesn't help
  - → Increase minimum length to 12
  - → Implement Identity Protection & Conditional Access
  - → Implement password blocklist checking with HaveIBeenPwned.com

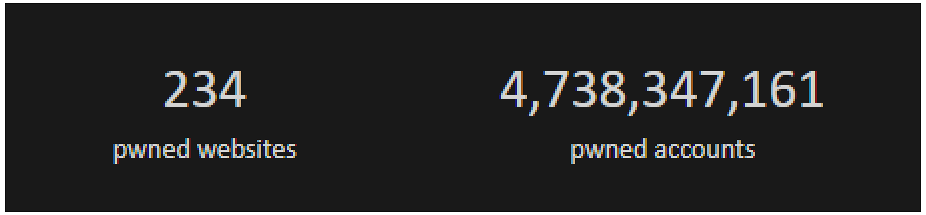


HaveIBeenPwned.com – Stopping password reuse

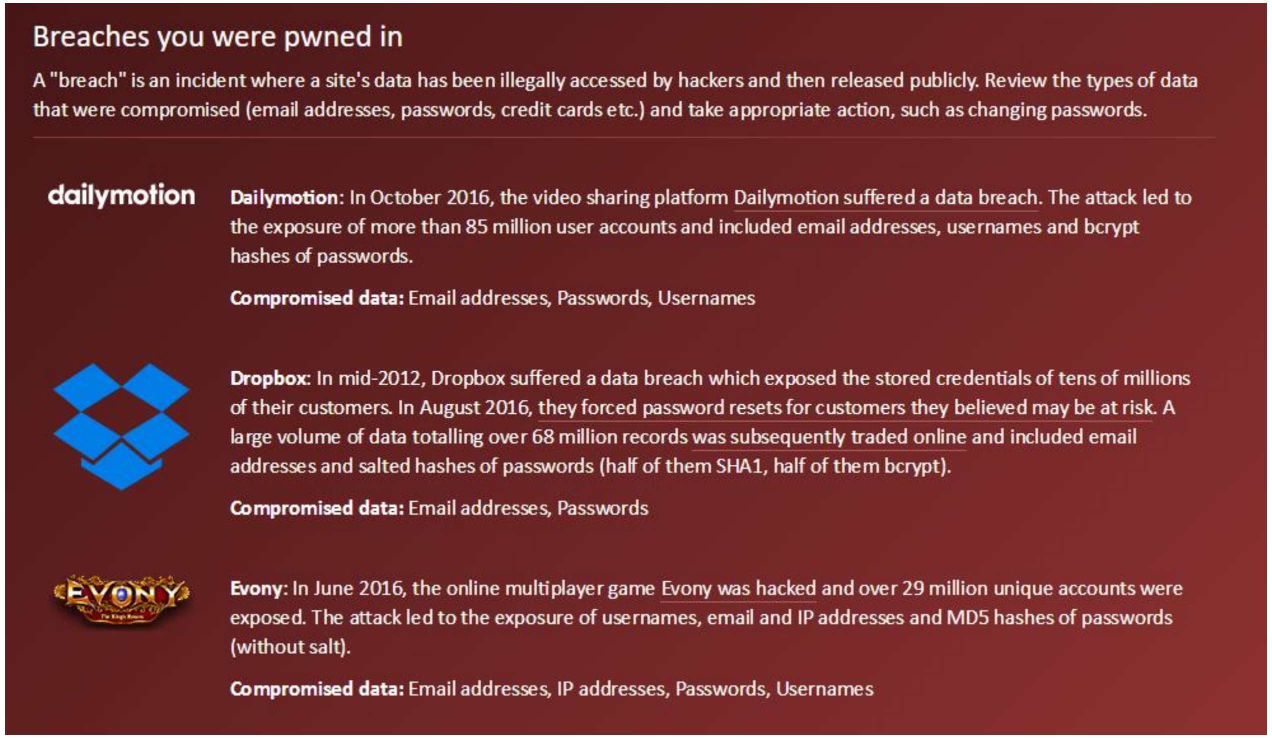
2017



359,420,698	MySpace accounts
234,842,089	NetEase accounts
164,611,595	LinkedIn accounts
152,445,165	Adobe accounts
112,005,531	Badoo accounts
105,059,554	B2B USA Businesses accounts
93,338,602	VK accounts
91,890,110	Youku accounts
91,436,280	Rambler accounts
85,176,234	Dailymotion accounts
68,648,009	Dropbox accounts
65,469,298	tumblr accounts



234	4,738,347,161
pwned websites	pwned accounts



Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

Dailymotion: In October 2016, the video sharing platform Dailymotion suffered a data breach. The attack led to the exposure of more than 85 million user accounts and included email addresses, usernames and bcrypt hashes of passwords.

Compromised data: Email addresses, Passwords, Usernames

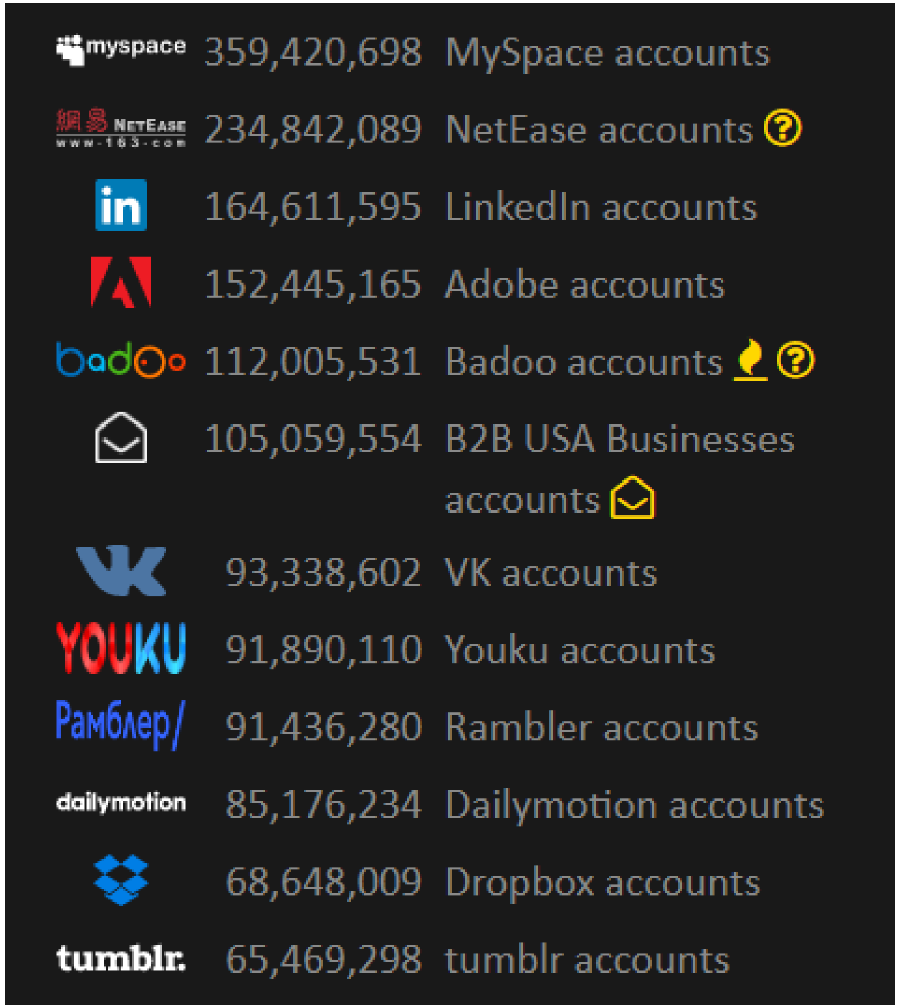
Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

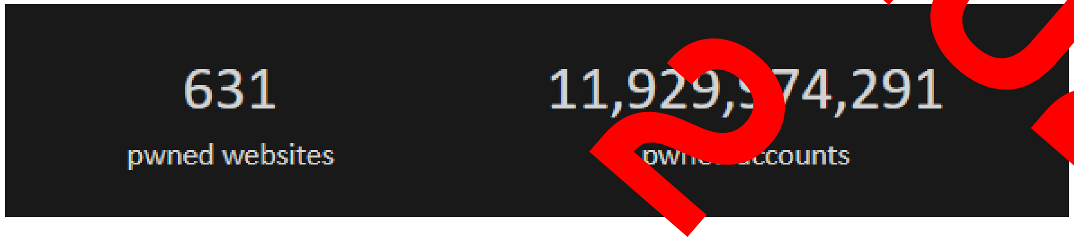
Evony: In June 2016, the online multiplayer game Evony was hacked and over 29 million unique accounts were exposed. The attack led to the exposure of usernames, email and IP addresses and MD5 hashes of passwords (without salt).

Compromised data: Email addresses, IP addresses, Passwords, Usernames

HaveIBeenPwned.com – Stopping password reuse

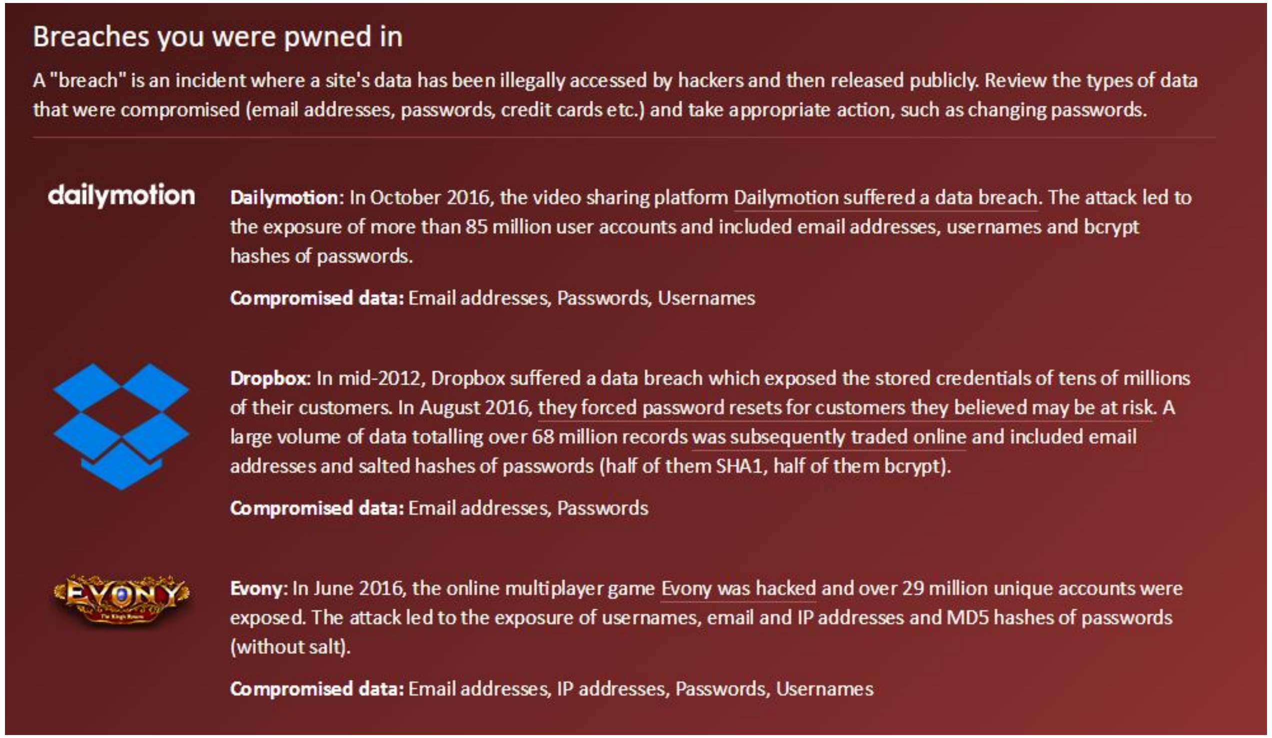


myspace	359,420,698	MySpace accounts
網易 NetEase www.163.com	234,842,089	NetEase accounts ❓
in	164,611,595	LinkedIn accounts
	152,445,165	Adobe accounts
badoo	112,005,531	Badoo accounts 🔥 ❓
✉	105,059,554	B2B USA Businesses accounts ✉
VK	93,338,602	VK accounts
YOUKU	91,890,110	Youku accounts
Рамблер/	91,436,280	Rambler accounts
dailymotion	85,176,234	Dailymotion accounts
	68,648,009	Dropbox accounts
tumblr.	65,469,298	tumblr accounts



631
pwned websites

11,929,974,291
pwned accounts



Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

dailymotion

Dailymotion: In October 2016, the video sharing platform Dailymotion suffered a data breach. The attack led to the exposure of more than 85 million user accounts and included email addresses, usernames and bcrypt hashes of passwords.

Compromised data: Email addresses, Passwords, Usernames

Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

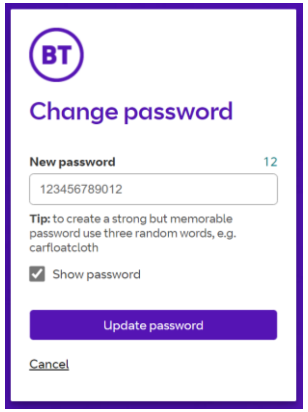
Compromised data: Email addresses, Passwords

EVONY

Evony: In June 2016, the online multiplayer game Evony was hacked and over 29 million unique accounts were exposed. The attack led to the exposure of usernames, email and IP addresses and MD5 hashes of passwords (without salt).

Compromised data: Email addresses, IP addresses, Passwords, Usernames

HaveIBeenPwned.com – Stopping password reuse



BT

Change password

New password 12

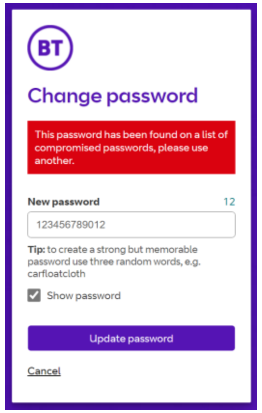
123456789012

Tip: to create a strong but memorable password use three random words, e.g. carfloatcloth

☑ Show password

Update password

Cancel



BT

Change password

This password has been found on a list of compromised passwords, please use another.

New password 12

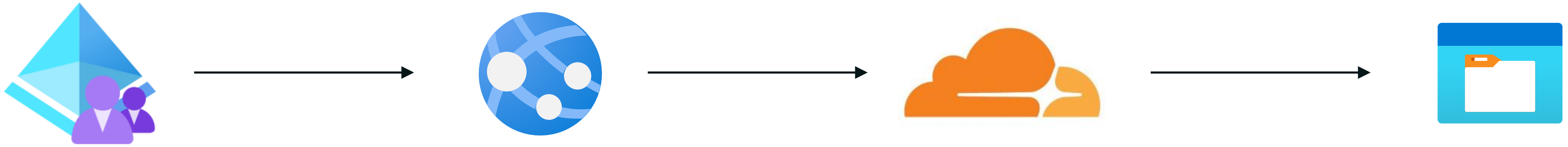
123456789012

Tip: to create a strong but memorable password use three random words, e.g. carfloatcloth

☑ Show password

Update password

Cancel



Azure AD B2C

Azure App Service

Create SHA 1

CloudFlare Cache

https://api.pwnedpasswords.com
/range/86EBA

Azure Storage Account

```
0018A45C4D1DEF81644B54AB7F969B88D65:1
00D4F6E8FA6EECAD2A3AA415EEC418D38EC:2
011053FD0102E94D6AE2F8B83D76FAF94F6:1
012A7CA357541F0AC487871FEEC1891C49C:2
0136E006E24E7D152139815FB0FC6A50B15:2
```

Workshop

Workshop Scenarios

→ Just in time Migration

→ Fraud Prevention using Netacea

Kocho

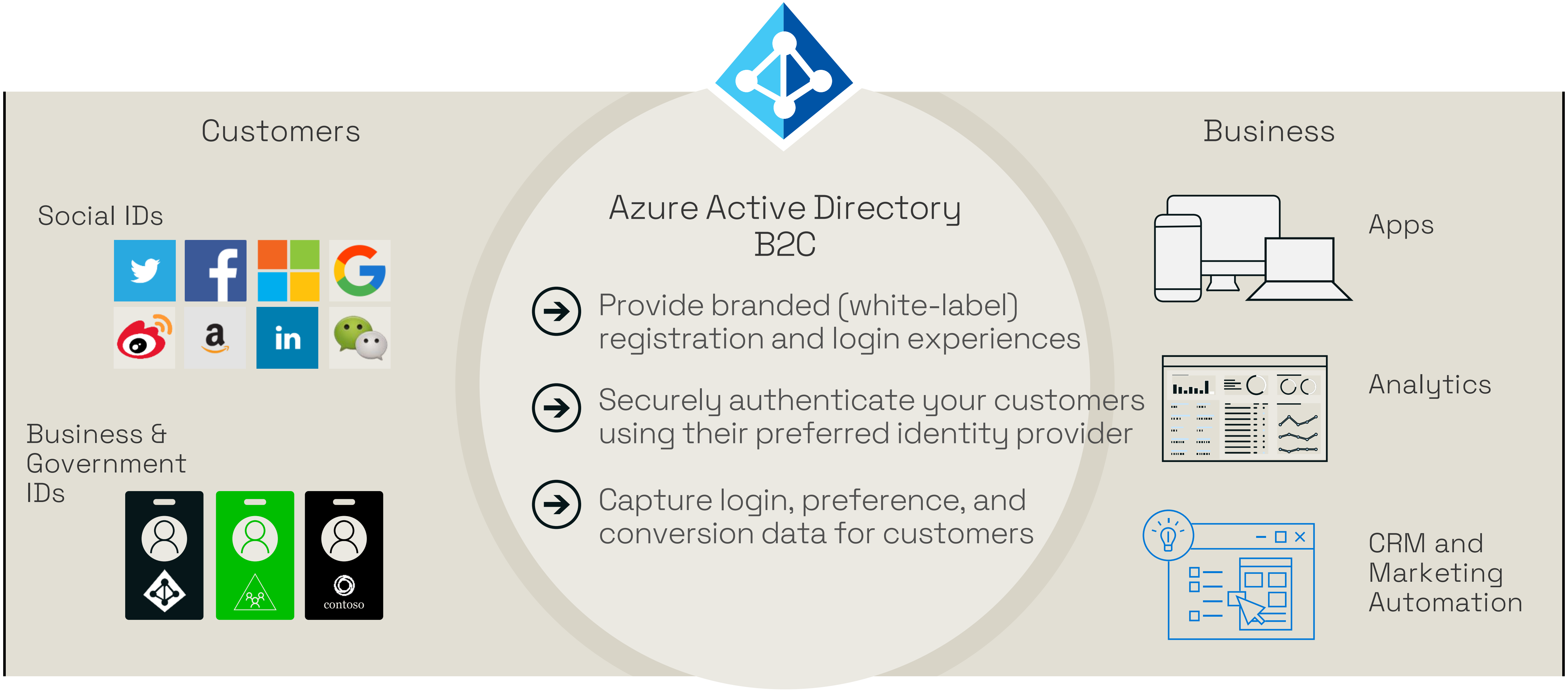
BECOME GREATER

Thank you

→ Any questions?

B2C

Azure Active Directory B2C



Customers

Social IDs

Business & Government IDs

Azure Active Directory B2C

- Provide branded (white-label) registration and login experiences
- Securely authenticate your customers using their preferred identity provider
- Capture login, preference, and conversion data for customers

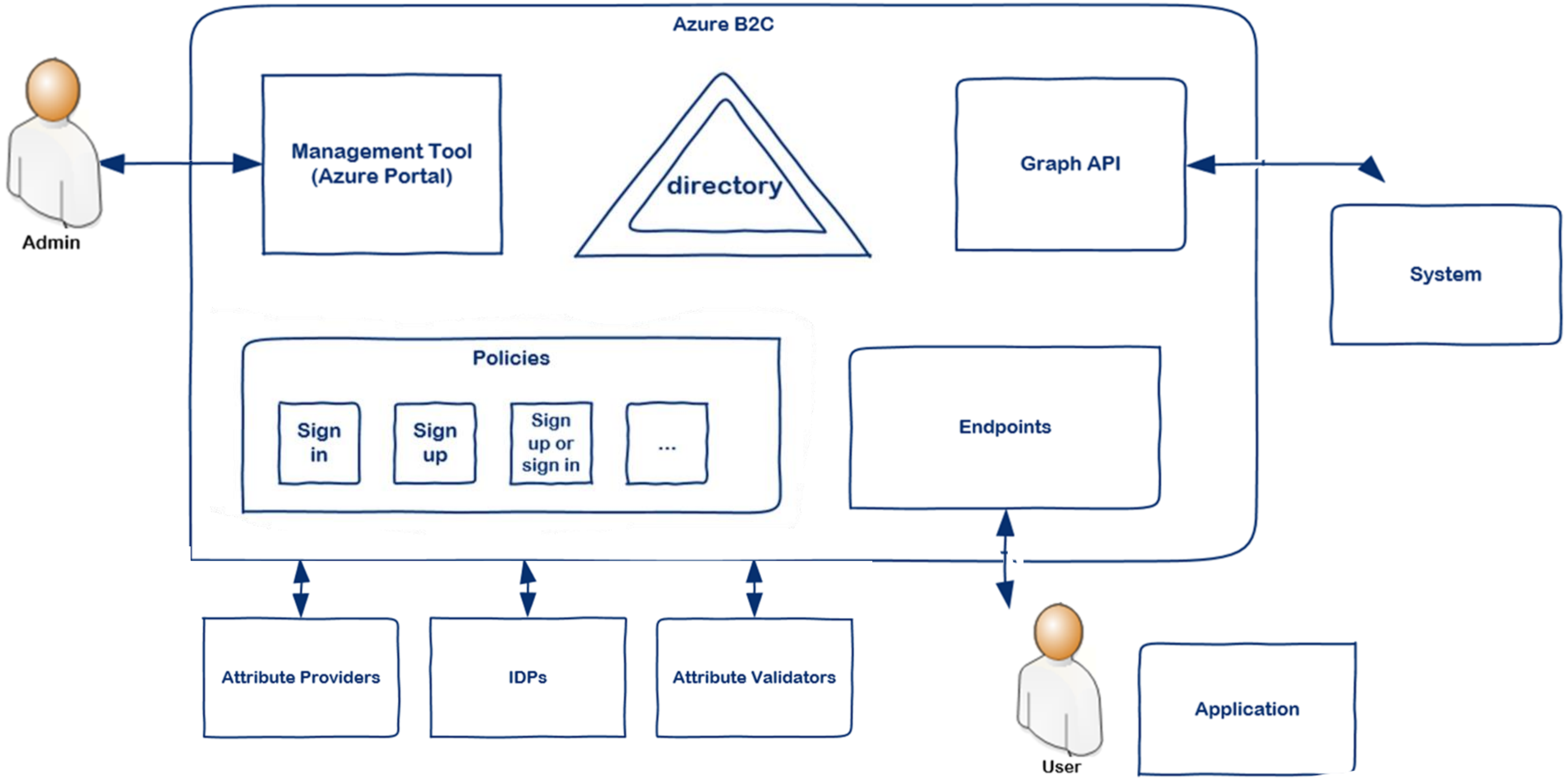
Business

Apps

Analytics

CRM and Marketing Automation

B2C


Azure B2C
Admin
Management Tool (Azure Portal)
directory
Graph API
System
Policies
Sign in
Sign up
Sign up or sign in
...
Endpoints
Attribute Providers
IDPs
Attribute Validators
User
Application

Support for multiple identity providers

Cloud Identity Providers

- amazon
- facebook
- Google
- Microsoft
- LinkedIn
- 新浪微博 weibo.com
- twitter
- WeChat

Federation Services / Other Services

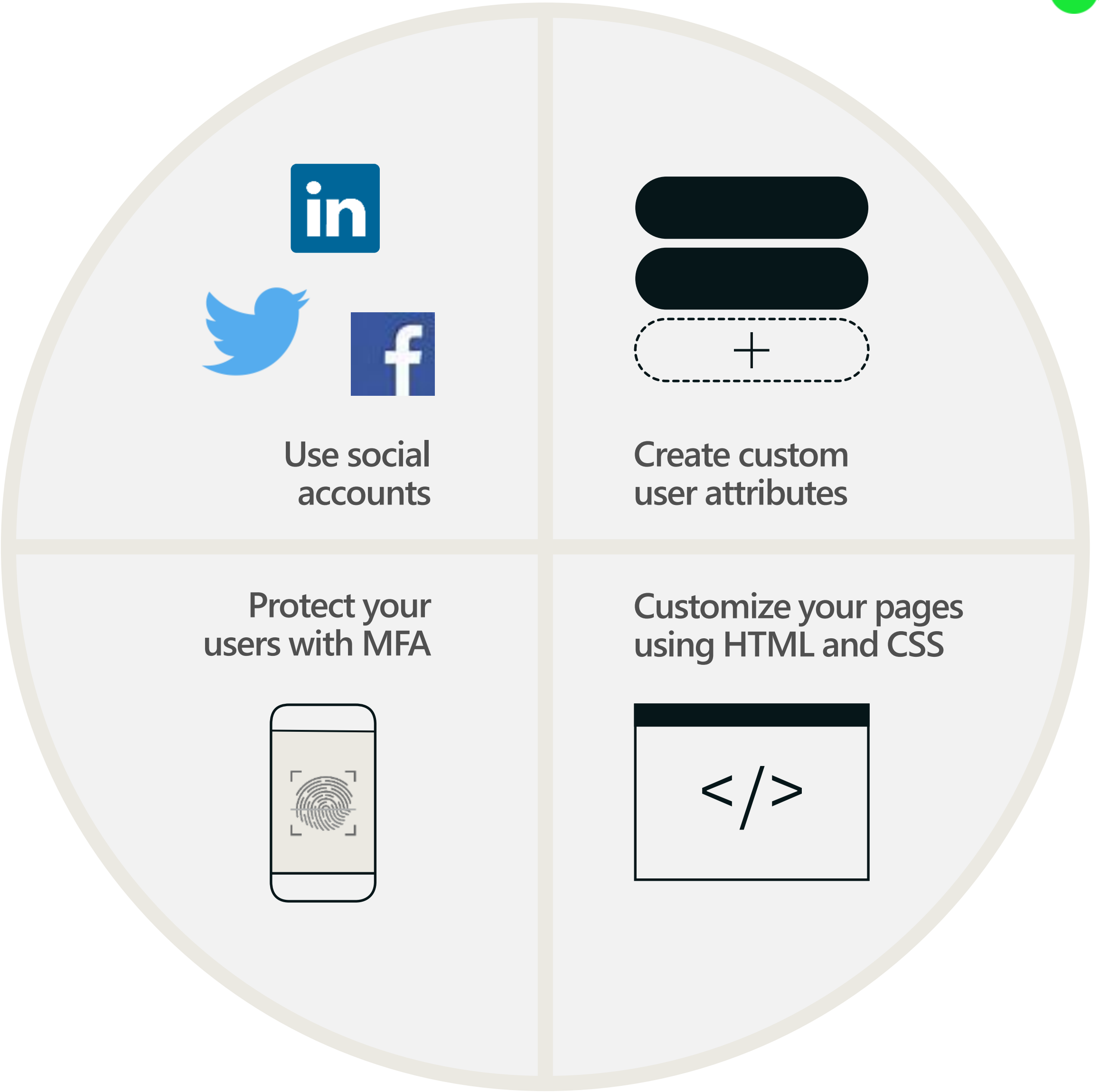
- PingFederate®
- SailPoint
- Centrify®
- ca technologies Siteminder
- ca technologies Secure Cloud
- RADIANT LOGIC™ RadiantOne CFS 3.0
- onelogin
- AuthAnvil Single Sign On
- Shibboleth.
- ilex www.ilex.fr Sign&go Global SSO
- Hewlett Packard Enterprise IceWall Federation
- Windows Server Active Directory Federation Services
- DELL One Identity Cloud Access Manager v7.1
- Optimal IdM Virtual Identity Server Federation Services
- SECUREAUTH® IdP 7.2.0
- NetIQ. Access Manager 4.0.1
- IBM® Tivoli. Federated Identity Manager 6.2.2
- f5 BIG-IP | Access Policy Manager
- vmware® Workspace Portal

Build your solution your way

for App Developers

App developers

- Sign-in any user. Any identity provider,
  social or email, consumer and enterprise
- Customize each pixel. Your brand, your HTML and CSS
- Use built-in, self-service, user journeys
  or define custom ones
- Scale to 100s of millions of users, enterprise ready, secure, cost effective



Use social accounts

Create custom user attributes

Protect your users with MFA

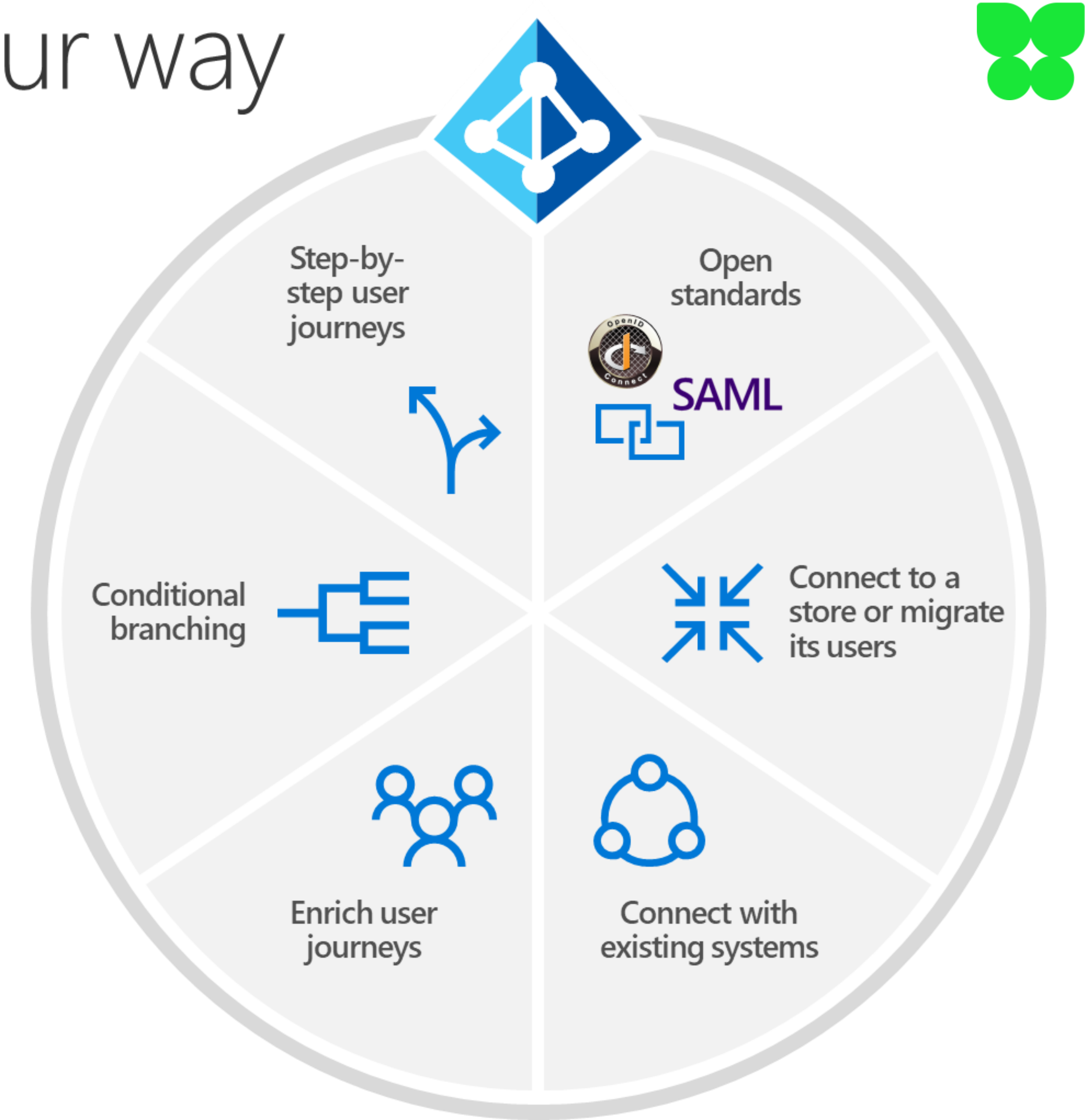
Customize your pages using HTML and CSS

Build your solution your way

for Identity Experts

Identity Experts

- Integrate with any SAML, OIDC, WsFed, or WsTrust-based identity provider
- Connect to your existing user stores or migrate from those systems seamlessly
- Connect with existing CRM systems, marketing tools, and databases
- Use REST APIs to enrich claims and empower user journeys
- Customize your user journeys with conditional branching
- Define user journeys between claims providers step-by-step

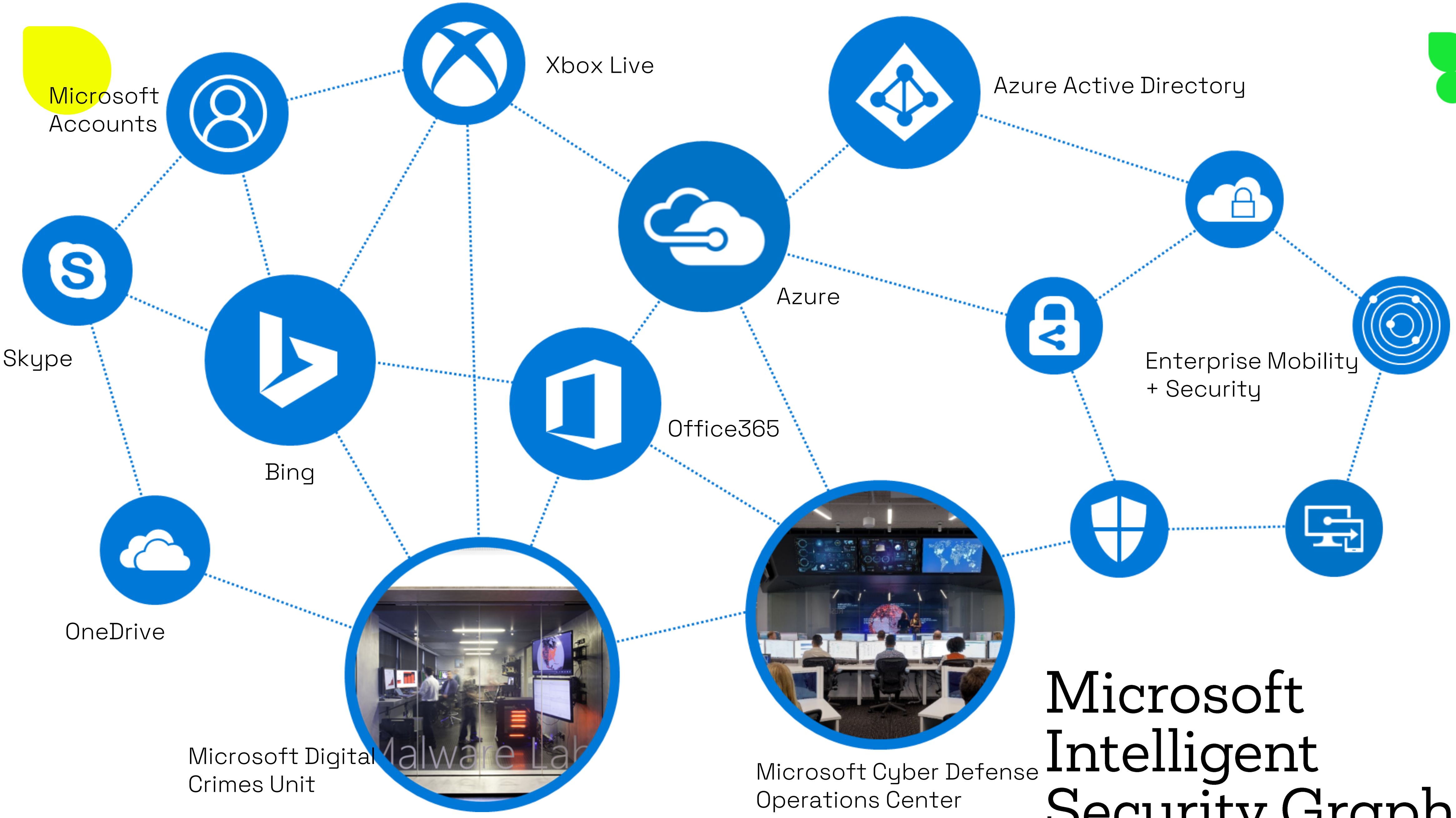

Step-by-step user journeys
Open standards
SAML
Conditional branching
Connect to a store or migrate its users
Enrich user journeys
Connect with existing systems

How does this fix the Issues?

Security

Security and Privacy

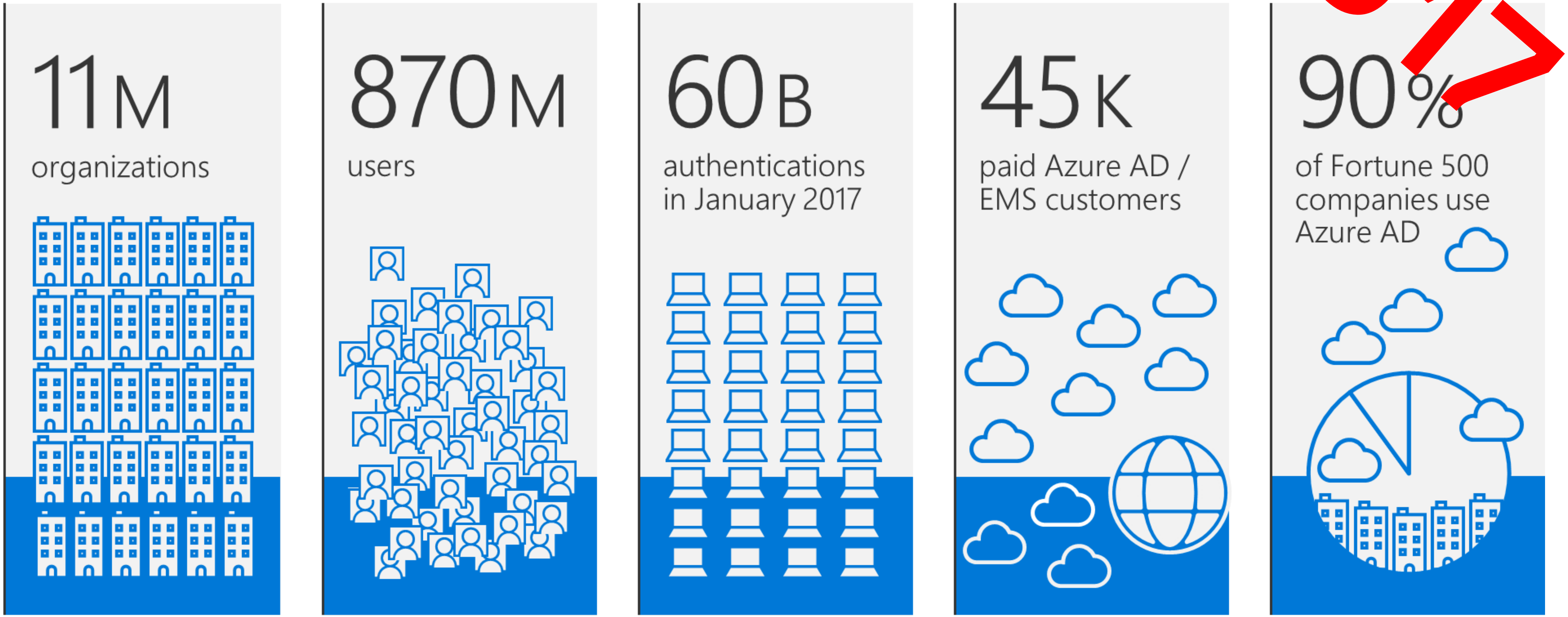
- → Secure Infrastructure
- → Blocking unauthorised traffic
- → Analysis
- → Proactive measures
- → Reduced risk of credential theft attacks


Microsoft Accounts
Xbox Live
Azure Active Directory
Skype
Azure
Enterprise Mobility + Security
Bing
Office365
OneDrive
Malware Lab
Microsoft Digital Crimes Unit
Microsoft Cyber Defense Operations Center

Microsoft Intelligent Security Graph

Built on the same proven platform used by Office 365 and Azure AD

2017



11M organizations

870M users

60B authentications in January 2017

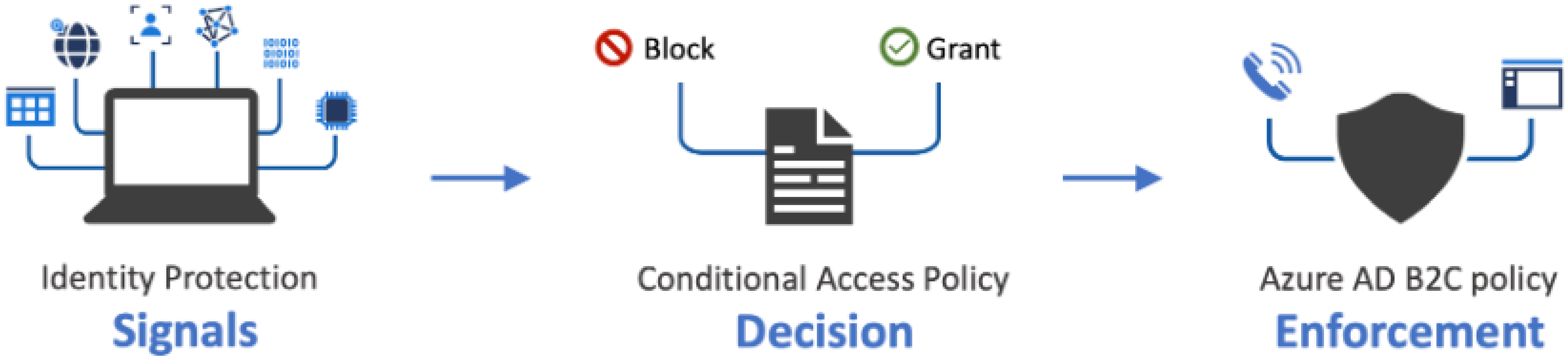
45K paid Azure AD / EMS customers

90% of Fortune 500 companies use Azure AD

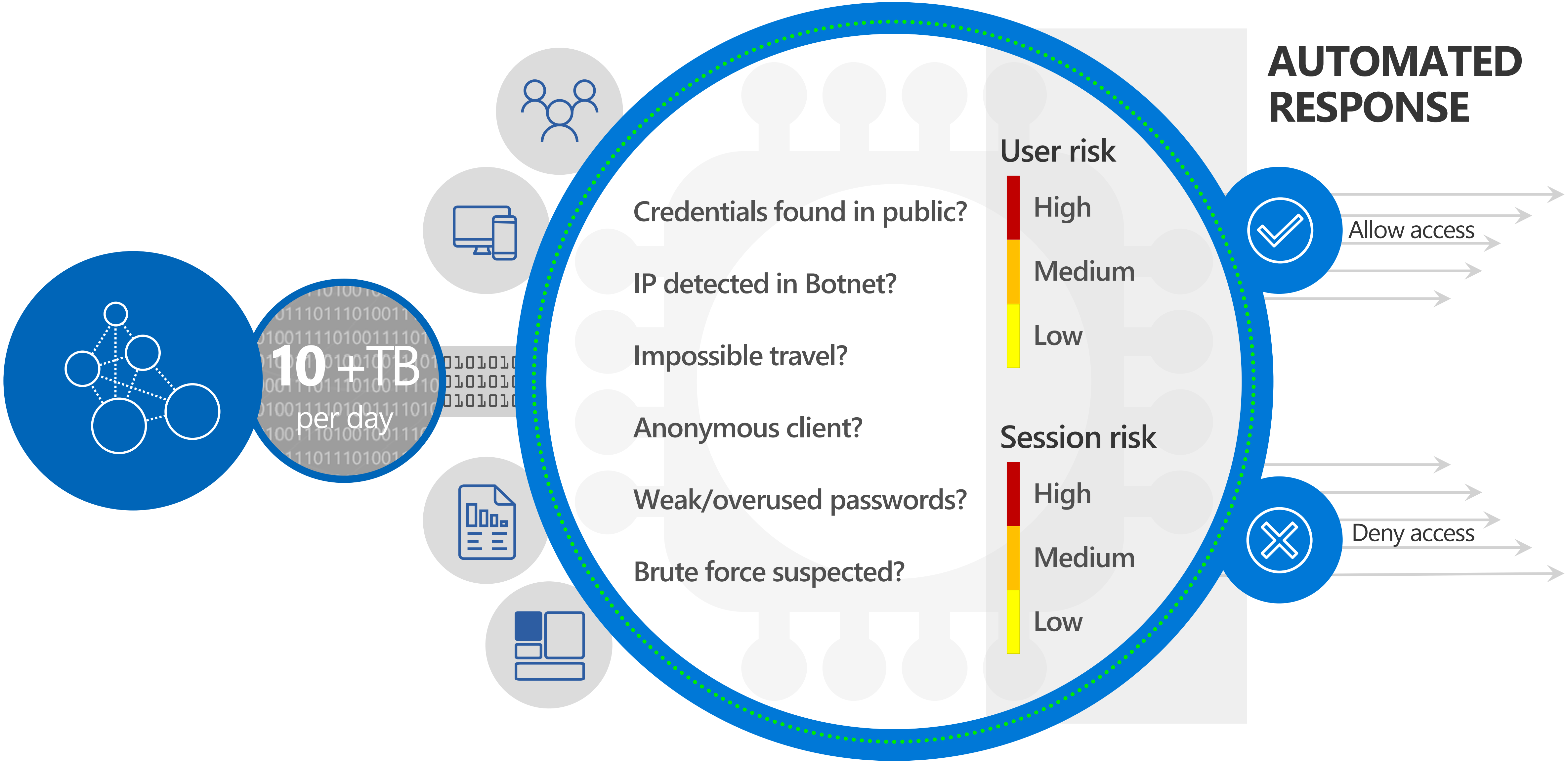
Stats

- 130 billion authentication each day
- Analysing 43 Trillion threat signals each day
- Blocked 70 Billion attacks in 2021
- Tracking 250+ unique Cyber criminals, nation states and other threat actors

Conditional Access & Identity Protection



43 Trillion/Day



CONDITIONS

Credentials found in public?

IP detected in Botnet?

Impossible travel?

Anonymous client?

Weak/overused passwords?

Brute force suspected?

User risk

- 🟥 High
- 🟧 Medium
- 🟨 Low

Session risk

- 🟥 High
- 🟧 Medium
- 🟨 Low

AUTOMATED RESPONSE

✓ Allow access

☒ Deny access

Intelligent protection with Azure Active Directory

For MSA

9.8M
users marked as compromised monthly

115.5M
blocked login attempts or 15.8M credentials daily

1.7M
users protected by real-time detection and challenges each day

For Azure AD

1M
users marked as Med/High risk monthly across 50K tenants

2.4M
users marked as at risk monthly over 100K tenants

10K
users confirmed to be compromised each month

Secure and reliable

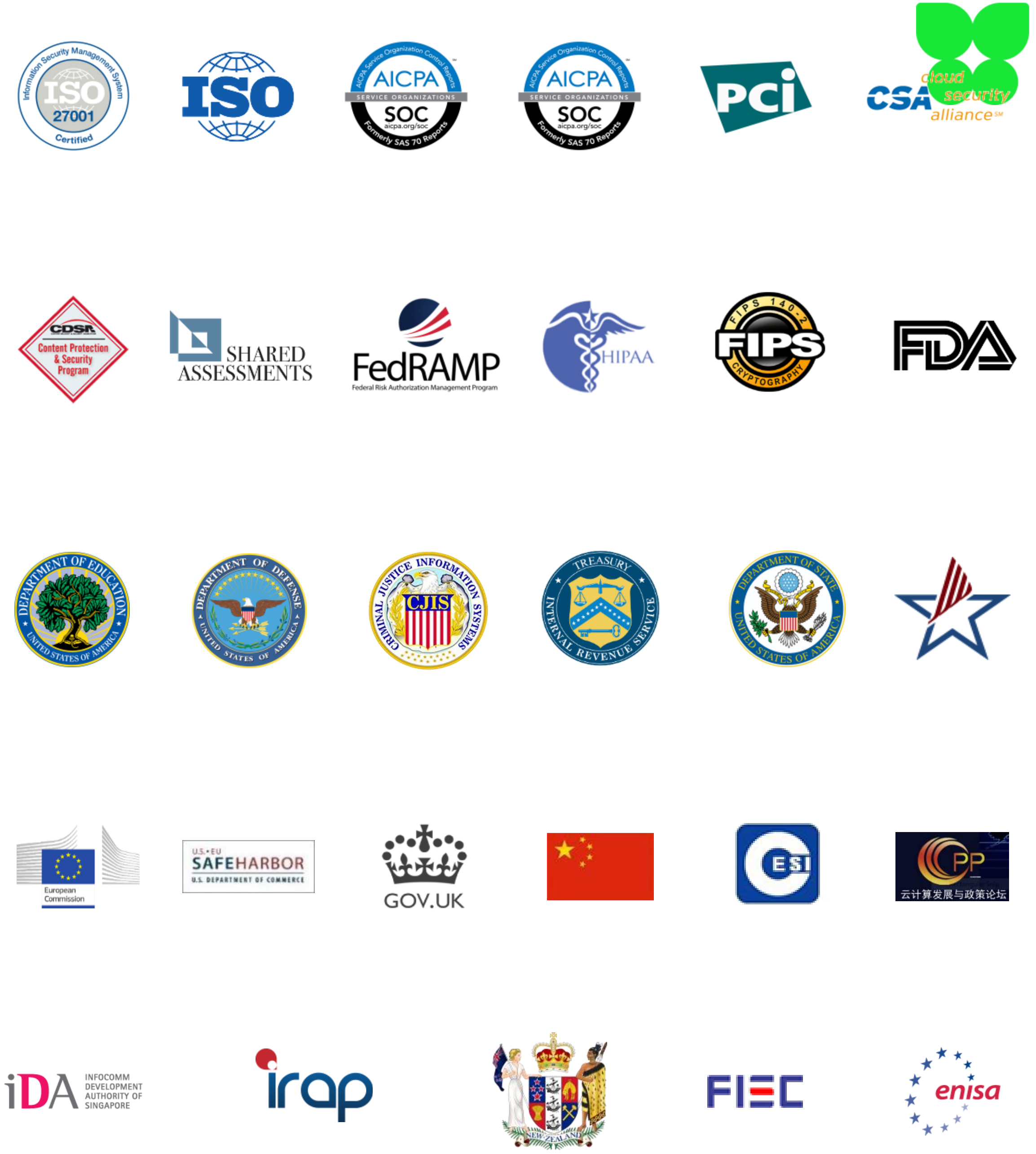
Certified and more trusted

More certifications than any other cloud provider

Industry leader for customer advocacy and privacy protection

Unique data residency guarantees

Microsoft is committed to GDPR compliance

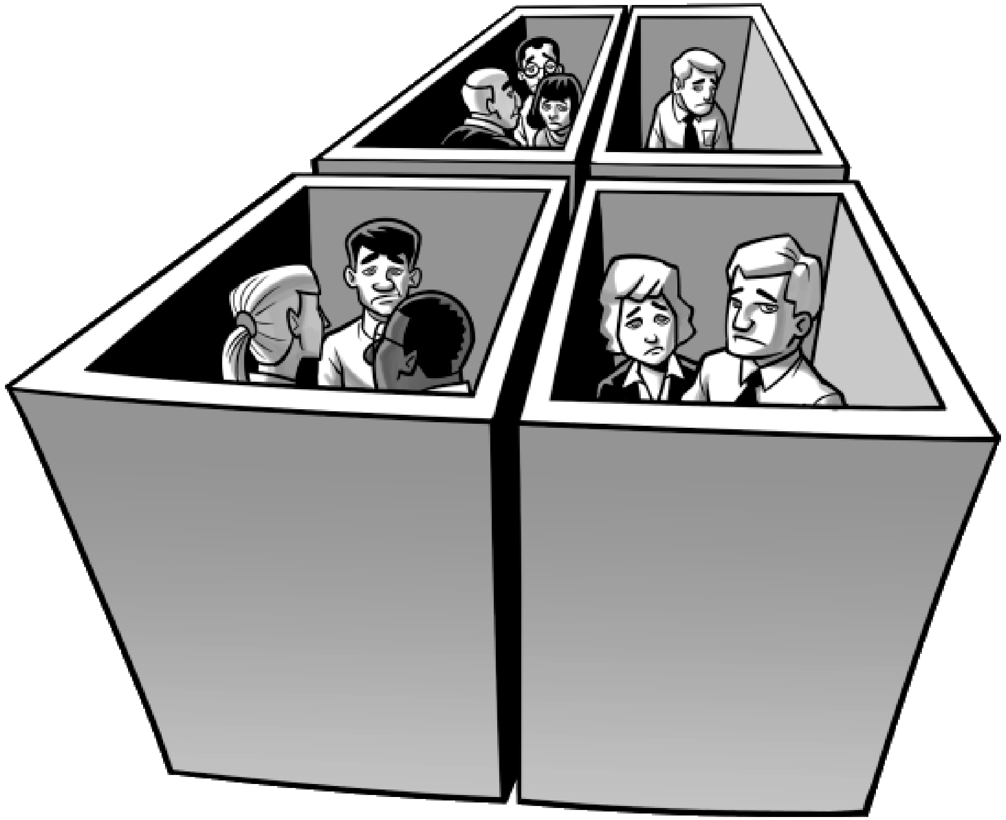


ISO 27001 Certified
ISO
AICPA SOC
AICPA SOC
PCI
CSA cloud security alliance
CDSA Content Protection & Security Program
SHARED ASSESSMENTS
FedRAMP
HIPAA
FIPS 140-2 CRYPTOGRAPHY
FDA
DEPARTMENT OF EDUCATION UNITED STATES OF AMERICA
DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA
CRIMINAL JUSTICE INFORMATION SYSTEMS CJIS
TREASURY INTERNAL REVENUE SERVICE
DEPARTMENT OF STATE UNITED STATES OF AMERICA
European Commission
U.S.-EU SAFEHARBOR U.S. DEPARTMENT OF COMMERCE
GOV.UK
ESI
CCPP 云计算发展与政策论坛
iDA INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE
irap
NEW ZEALAND
FIEC
enisa

MFA when you need it

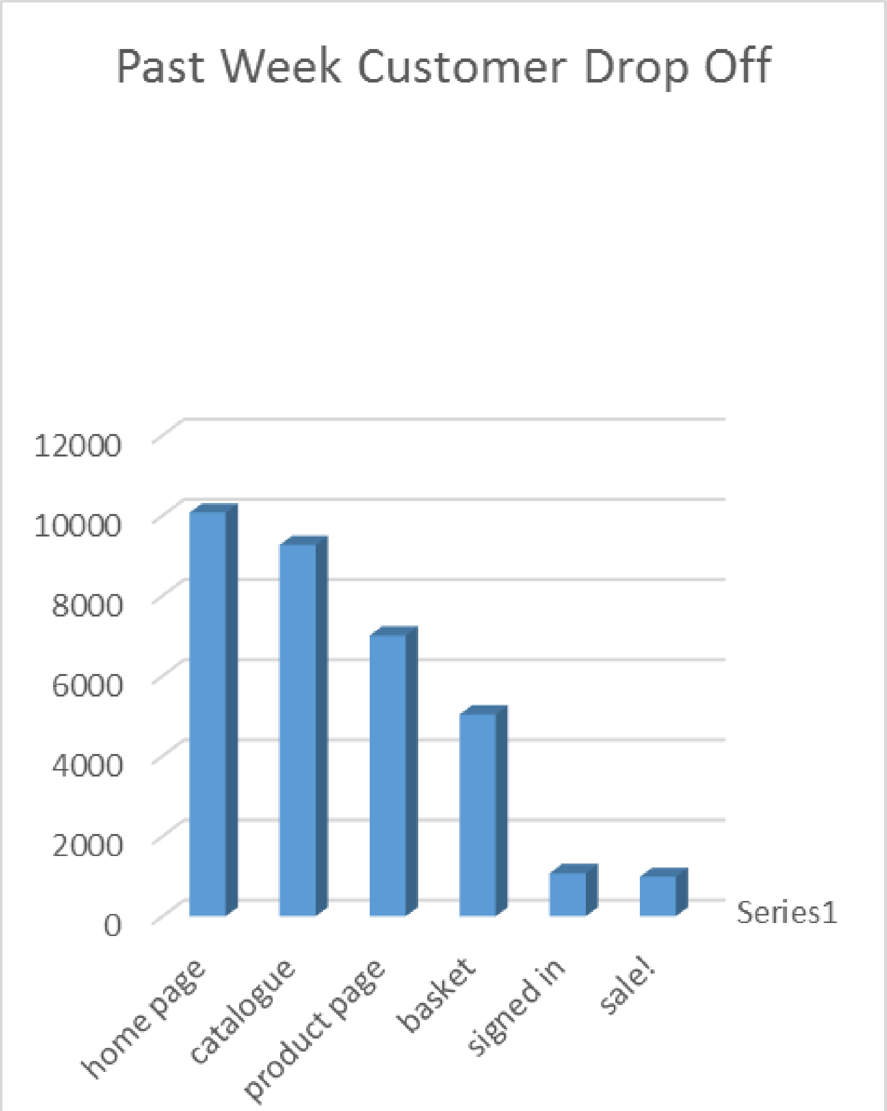
- → For higher level of authentication
- → Phone Call
- → SMS
- → TOTP (e.g Google or Microsoft authenticator)

Removing Silos



- → Unify applications Single User Directory
- → Web
- → Mobile
- → ASP.Net
- → Java
- → PHP

Reducing friction



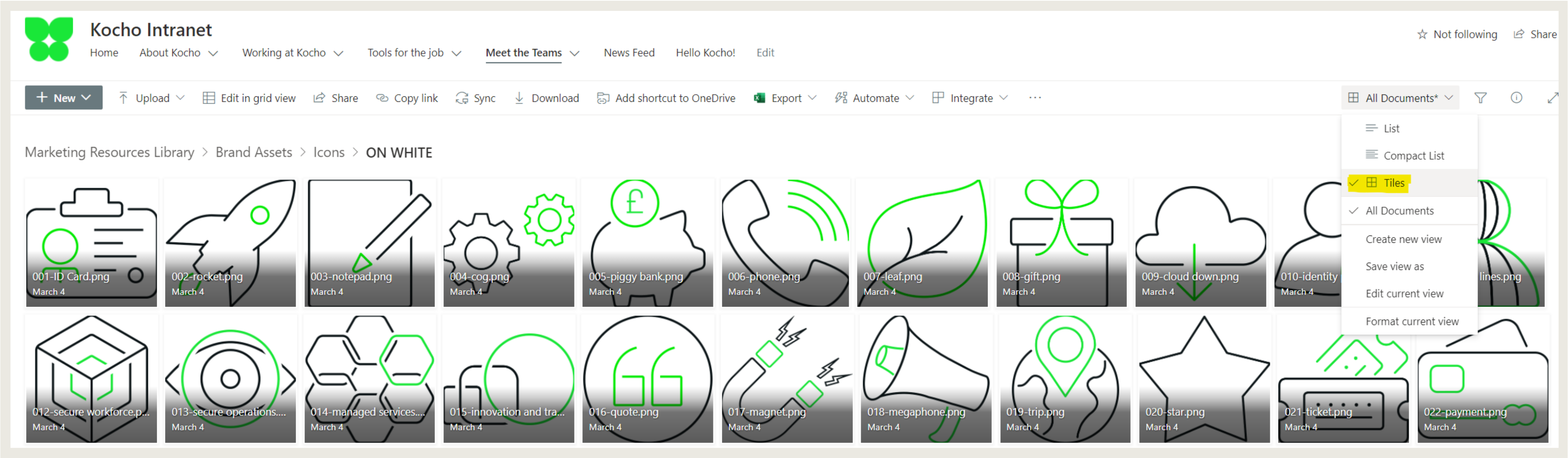
- → Improved UX
- → Sign up or sign in
- → Social login
- → Reduced form filling
- → Reduced password fatigue

Customisation

- Cross Origin Resource Sharing
- <div id=”api”></div>

Marketing Assets (Read then delete this slide)

Please click on the links below to find other Kocho marketing assets to support your PowerPoint deck styling.
When viewing in SharePoint, make sure to change viewing to tiles so that you can see the visuals clearly like below:



→ [Marketing Resources Library (Intranet)]

→ Kocho Logos

→ Kocho Icons

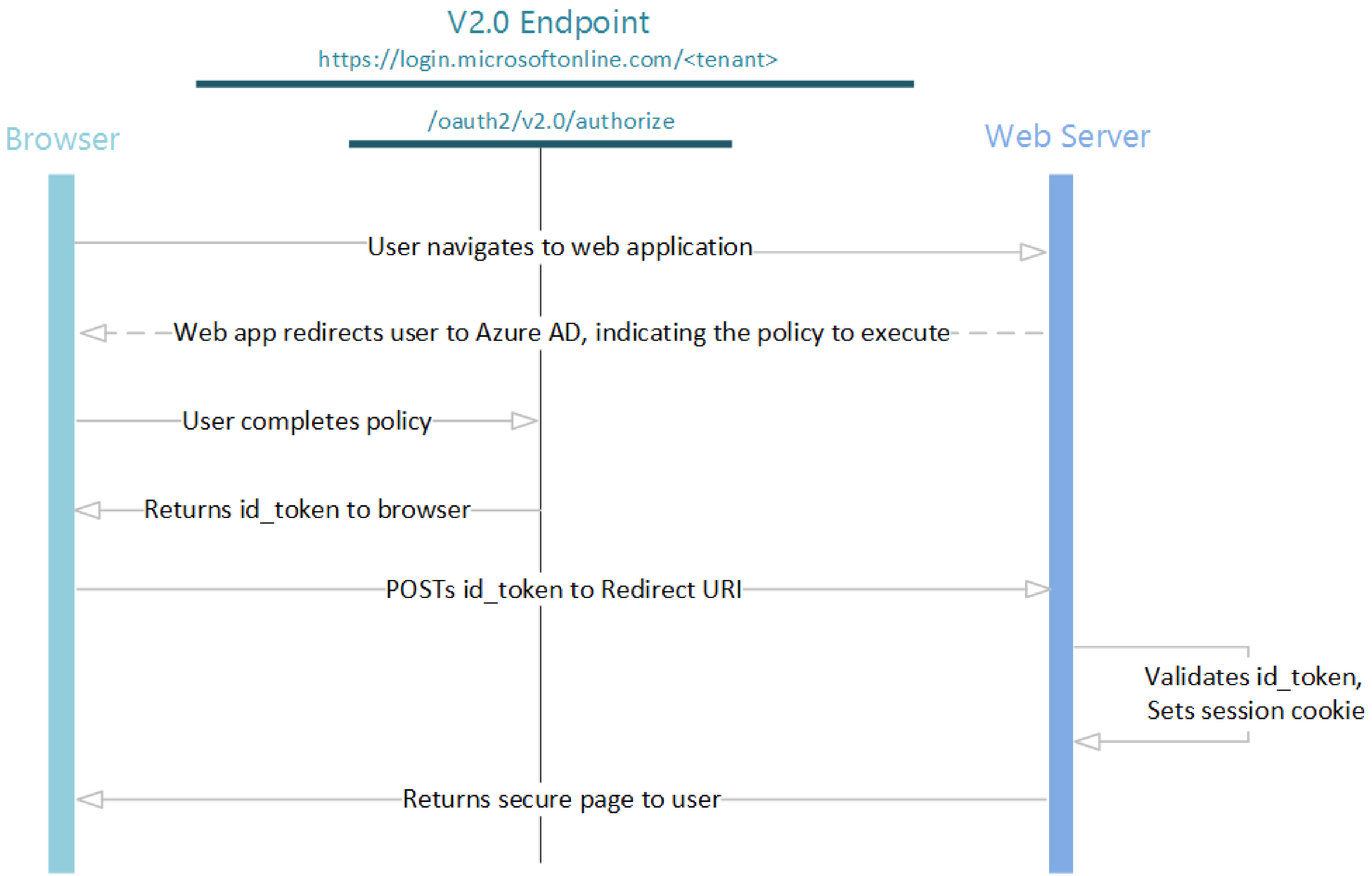
→ Kocho Photography

→ Other brand assets

ENJOY

DEMO

Flow



V2.0 Endpoint

https://login.microsoftonline.com/<tenant>

/oauth2/v2.0/authorize

Browser

Web Server

User navigates to web application

Web app redirects user to Azure AD, indicating the policy to execute

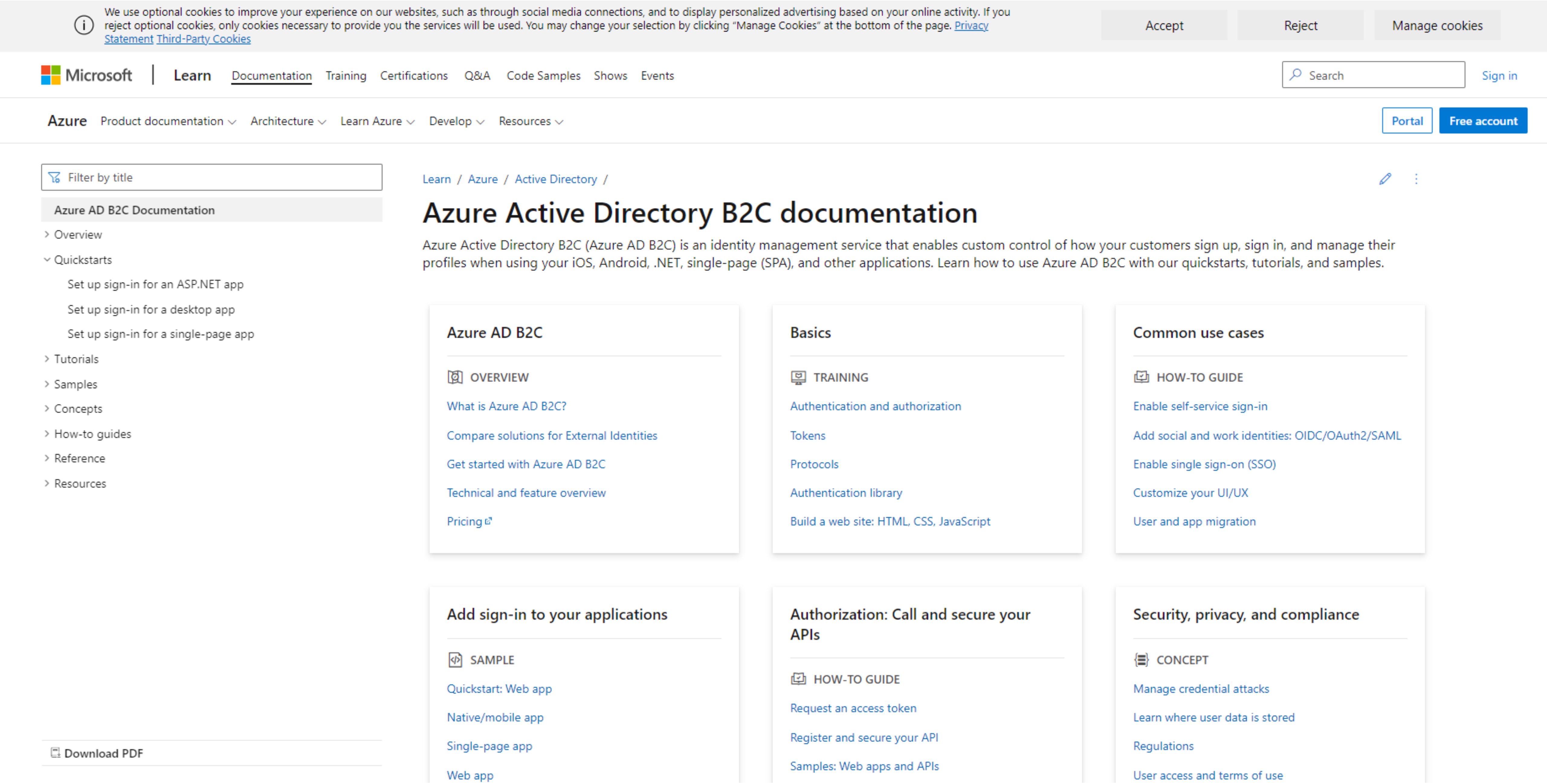
User completes policy

Returns id_token to browser

POSTs id_token to Redirect URI

Validates id_token,
Sets session cookie

Returns secure page to user



- Azure AD B2C Documentation
- Overview
- Quickstarts
  - Set up sign-in for an ASP.NET app
  - Set up sign-in for a desktop app
  - Set up sign-in for a single-page app
- Tutorials
- Samples
- Concepts
- How-to guides
- Reference
- Resources

Download PDF

Learn / Azure / Active Directory /

Azure Active Directory B2C documentation

Azure Active Directory B2C (Azure AD B2C) is an identity management service that enables custom control of how your customers sign up, sign in, and manage their profiles when using your iOS, Android, .NET, single-page (SPA), and other applications. Learn how to use Azure AD B2C with our quickstarts, tutorials, and samples.

Azure AD B2C

OVERVIEW

- What is Azure AD B2C?
- Compare solutions for External Identities
- Get started with Azure AD B2C
- Technical and feature overview
- Pricing

Basics

TRAINING

- Authentication and authorization
- Tokens
- Protocols
- Authentication library
- Build a web site: HTML, CSS, JavaScript

Common use cases

HOW-TO GUIDE

- Enable self-service sign-in
- Add social and work identities: OIDC/OAuth2/SAML
- Enable single sign-on (SSO)
- Customize your UI/UX
- User and app migration

Add sign-in to your applications

SAMPLE

- Quickstart: Web app
- Native/mobile app
- Single-page app
- Web app

Authorization: Call and secure your APIs

HOW-TO GUIDE

- Request an access token
- Register and secure your API
- Samples: Web apps and APIs

Security, privacy, and compliance

CONCEPT

- Manage credential attacks
- Learn where user data is stored
- Regulations
- User access and terms of use