Microsoft

Securing Applications with Azure Active Directory

Jonathan Lyon

@TheJonLyon

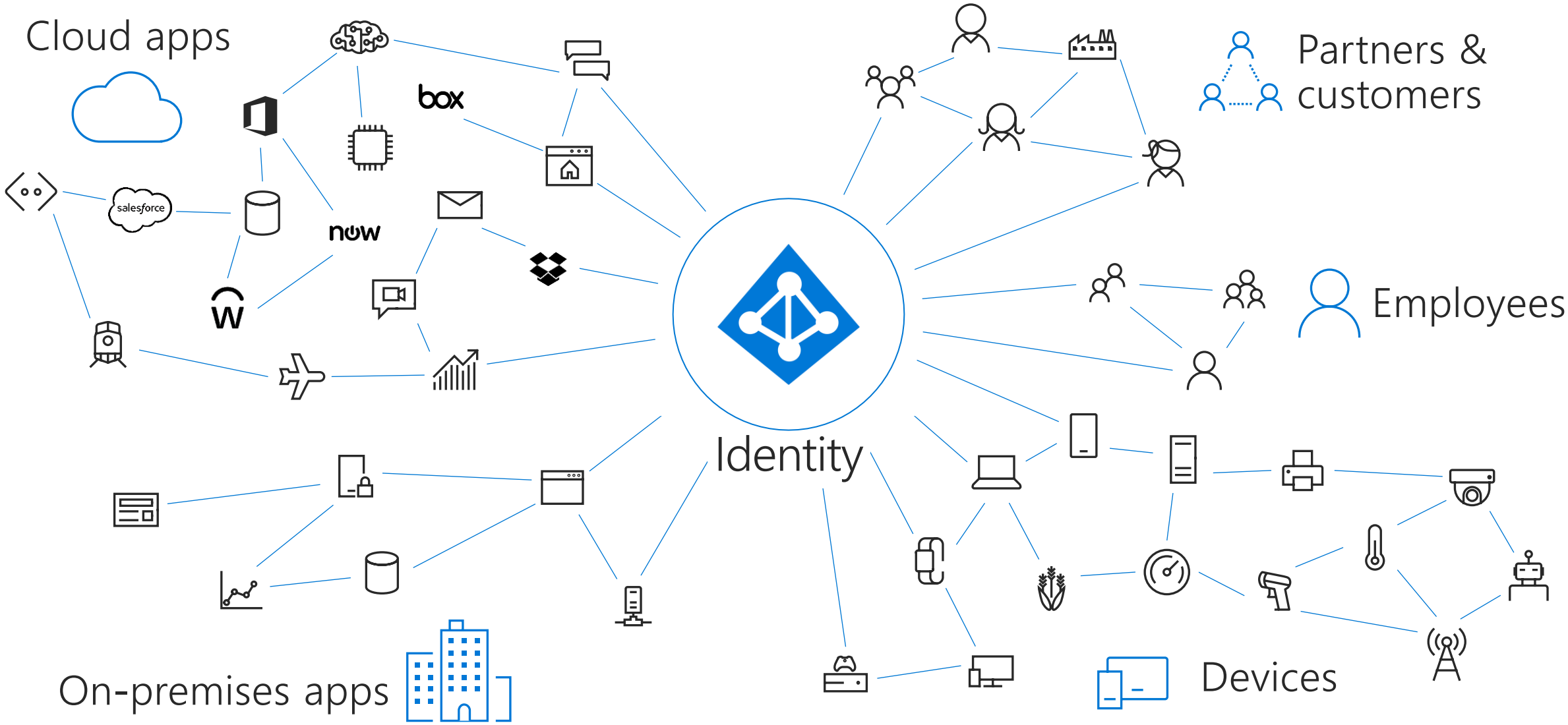
in/thejonlyon

Senior Program Manager, Microsoft Identity Engineering

To begin with, what is Azure AD?

Identity and Security solutions *from* Microsoft,
not *for* Microsoft

Identity is the control plane



Azure Active Directory

Strong usage growth

254M

Azure AD

Monthly Active Users

100K+

Enterprise customers

Using Azure AD

30B+

Daily Authentications

Using Azure AD

Azure Active Directory—the world's largest cloud identity service

Thousands of organizations, millions of active users, billions of daily requests

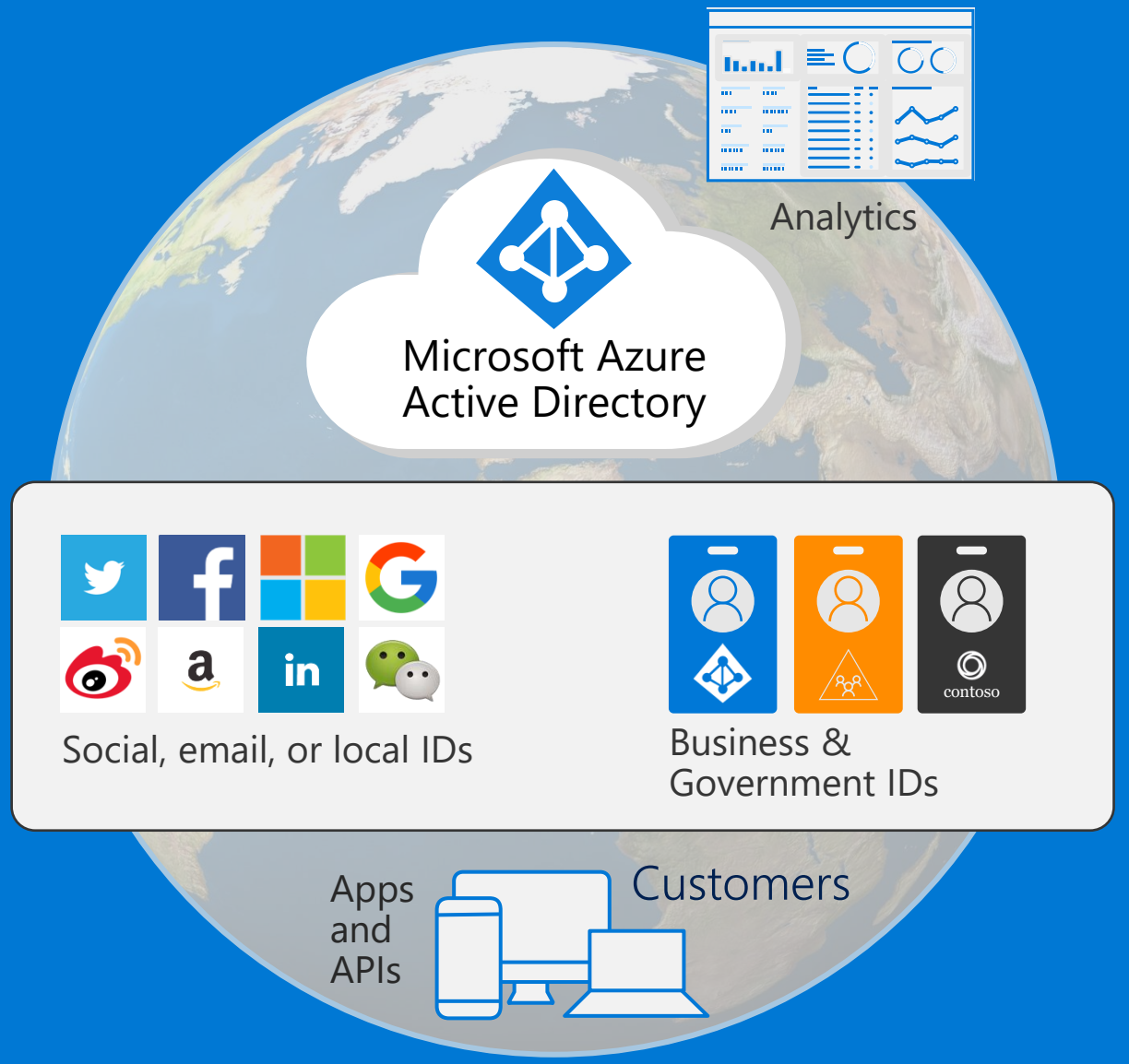
Oct 2019

CONNECT & COLLABORATE

Azure Active Directory B2C

Connect to any user on any platform

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



How is your customer authenticating with Azure AD?

Cloud authentication

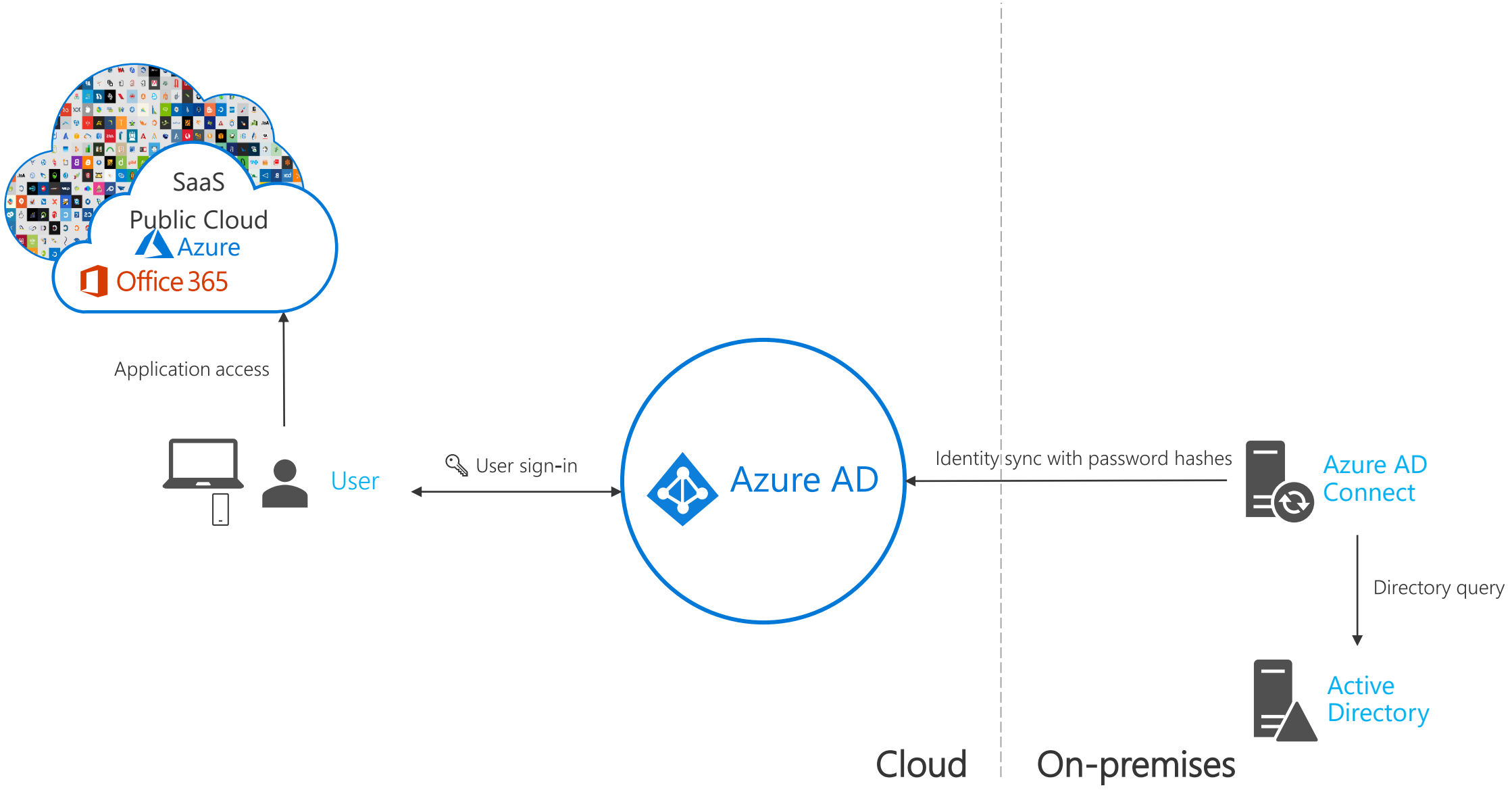
- Cloud-only
- Password Hash Sync + Seamless SSO
- Pass-through authentication + Seamless SSO

Federated authentication

- AD FS
- Third party federation providers

aka.ms/auth-options

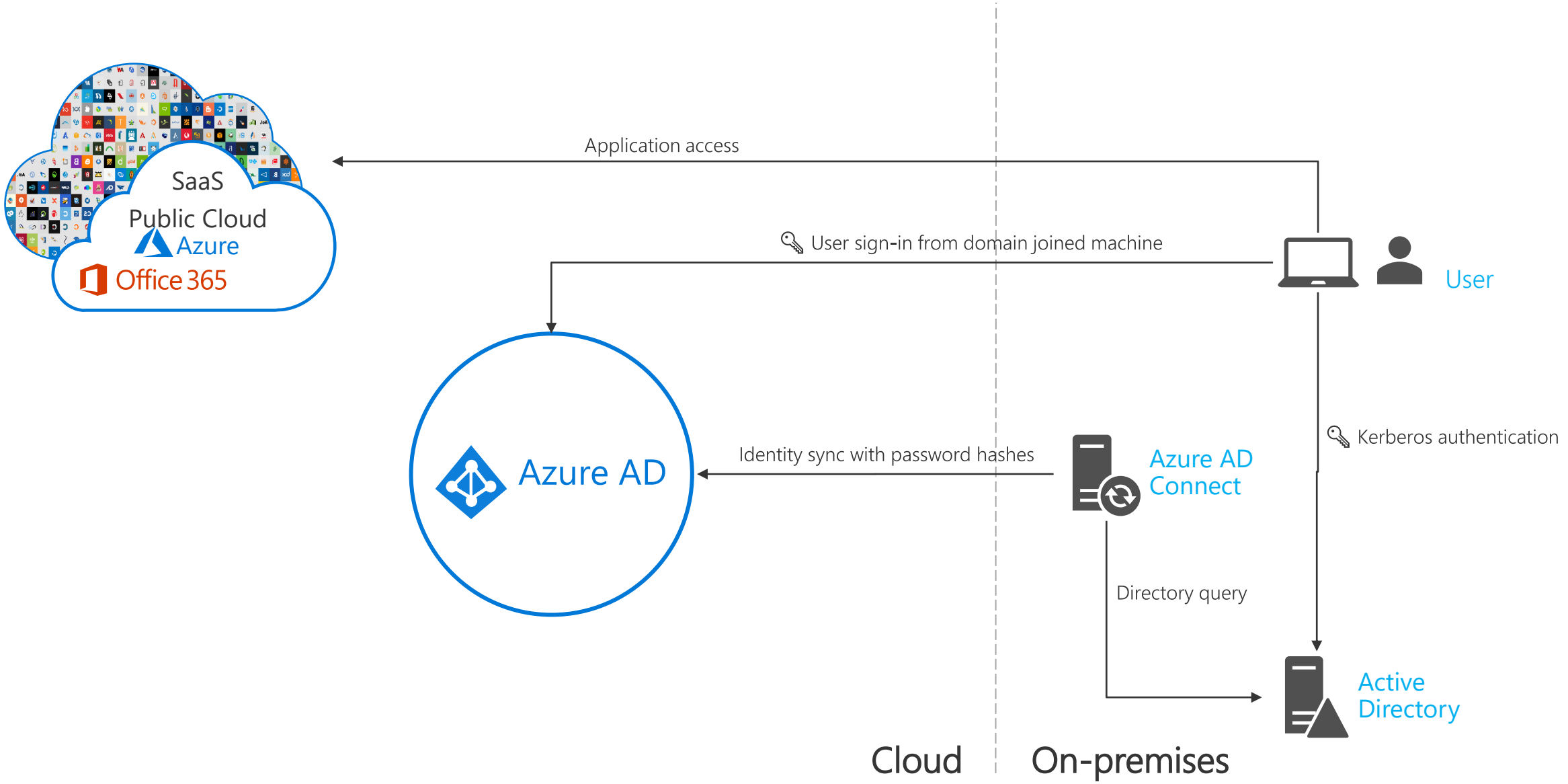
Azure AD Hybrid Identity with Password Hash Sync



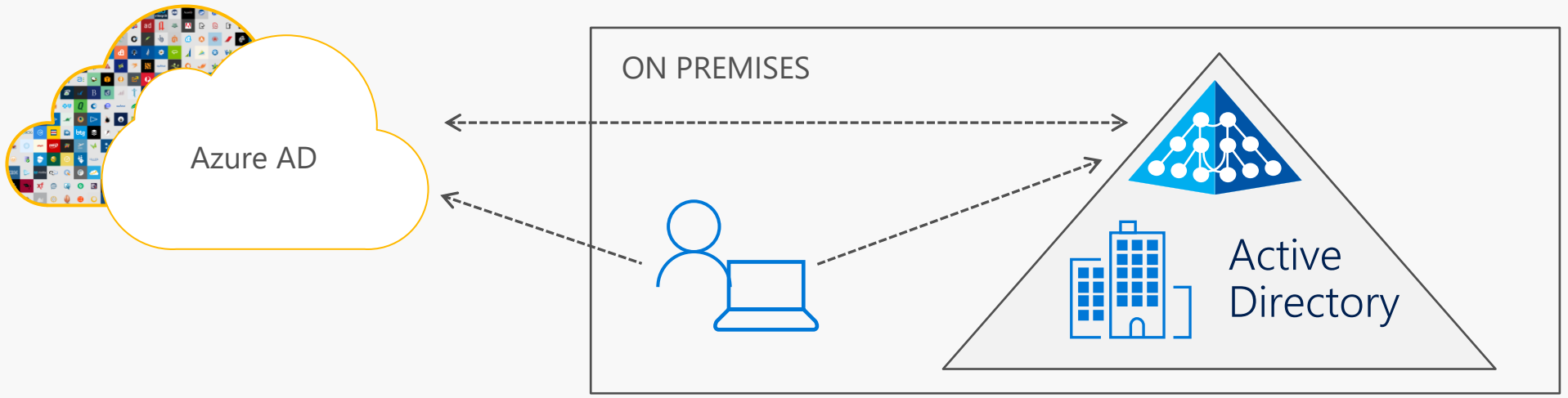
Seamless Single Sign On

- Seamless SSO creates a computer account named **AZUREADSSOACC** in your on-premises Active Directory (AD) in each AD forest.
- The **AZUREADSSOACC** computer account needs to be strongly protected for security reasons.
- Only Domain Admins should be able to manage the computer account. Ensure that Kerberos delegation on the computer account is disabled, and that no other account in Active Directory has delegation permissions on the AZUREADSSOACC computer account.
- Store the computer account in an Organization Unit (OU) where they are safe from accidental deletions and where only Domain Admins have access.

Azure Active Directory Seamless Single Sign On

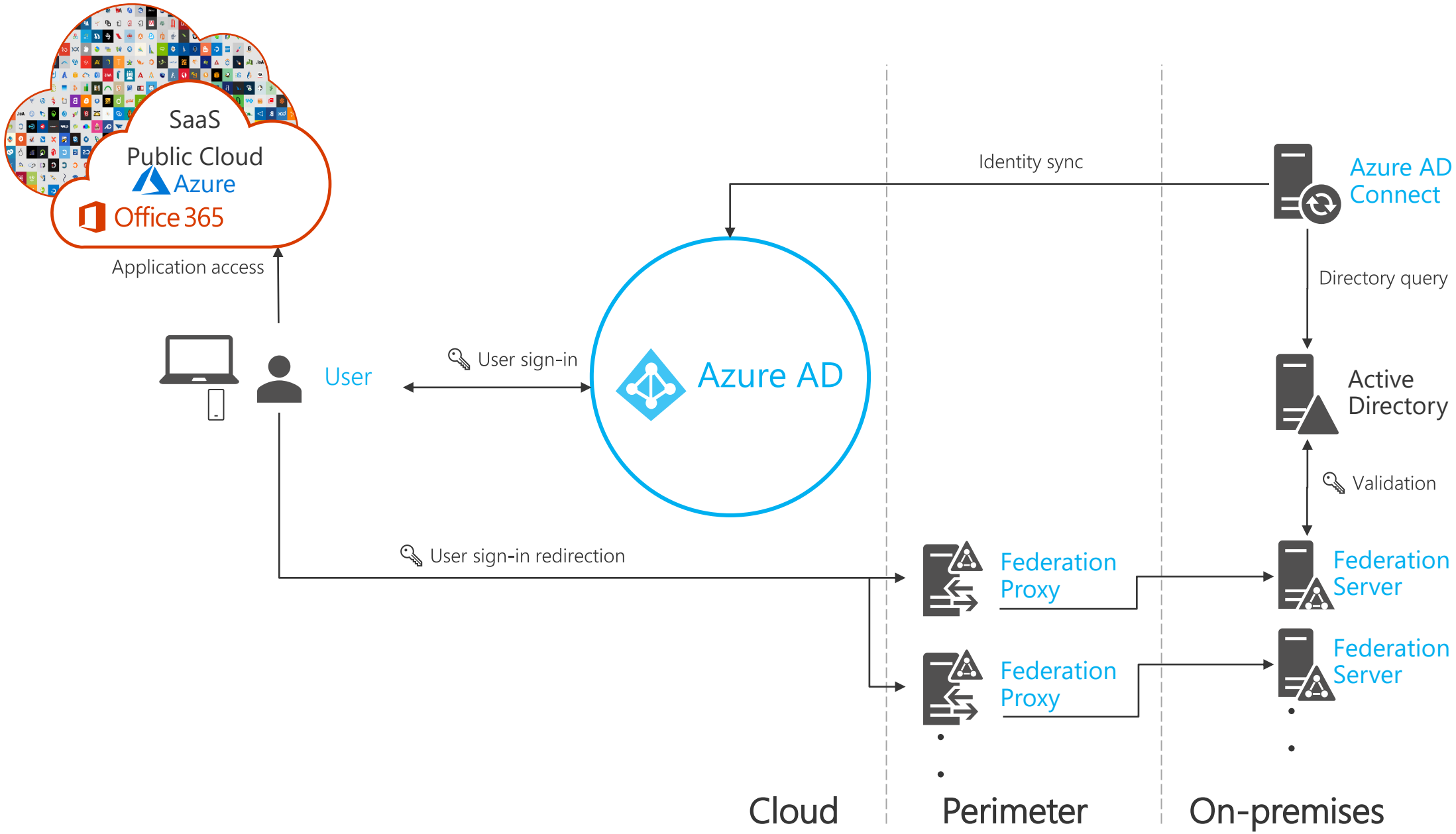


Seamless Single Sign On

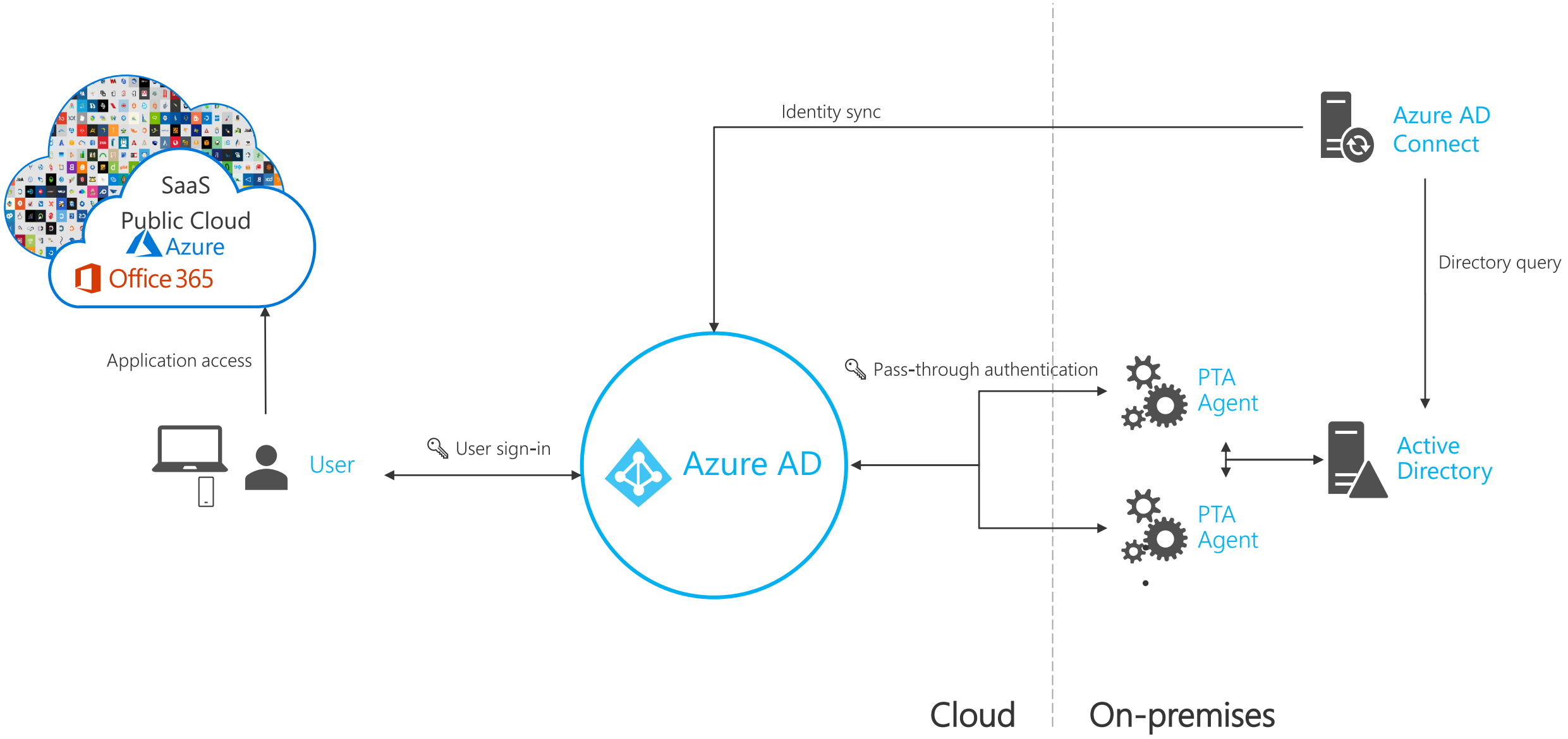


Easy to integrate	Easy to administer	Great user experience
Works with Password Hash Sync and Pass-through Authentication	No additional on-premise infrastructure	SSO experience from domain-joined devices within your corpnet
Supports Alternate Login ID	Register non-Windows 10 devices without AD FS	

Federated Authentication



Azure Active Directory Pass-through authentication



Smart Lockout

Smart lockout locks the account from sign-in attempts for one minute after 10 failed attempts. The account locks again after each subsequent failed sign-in attempt, for one minute at first and longer in subsequent attempts.

Smart lockout tracks the last three bad password hashes to avoid incrementing the lockout counter for the same password. If someone enters the same bad password multiple times, this behavior will not cause the account to lockout.

When using pass-through authentication, you need to make sure that:

- The Azure AD lockout threshold is **less** than the Active Directory account lockout threshold. Set the values so that the Active Directory account lockout threshold is at least two or three times longer than the Azure AD lockout threshold.

- The Azure AD lockout duration **in seconds** is **longer** than the Active Directory reset account lockout counter after duration **minutes**.

Important
Currently an administrator can't unlock the users' cloud accounts if they have been locked out by the Smart Lockout capability. The administrator must wait for the lockout duration to expire.

Why choose Cloud Authentication over Federated?

Less On-Premises infrastructure

- Password Hash Sync – Azure AD Connect server facilitates this process
- Pass-through Authentication - Agents deployed on existing servers (physical/virtual)
- Seamless SSO - Provided via existing AD infrastructure (computer account)

Same or better end user sign-in experience

- No smart link requirements
- Modern Authentication and KMSI for continued SSO
- Windows 10 Hybrid AADJ gives the best SSO experience regardless of authentication choice

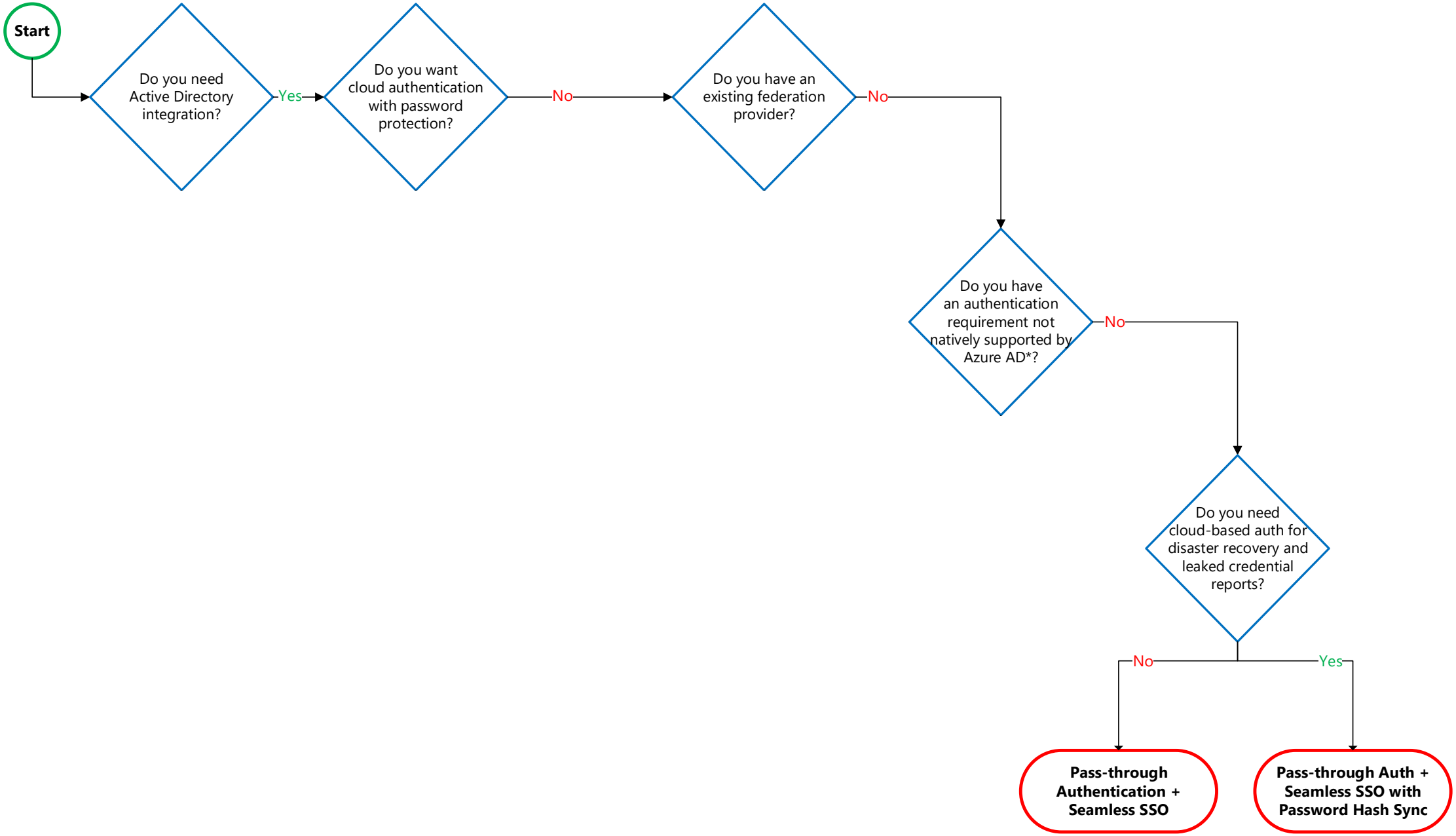
Smart Lockout

- Gain instant protection for identities
- Customizable. Lockout bad actor after X failed password attempts

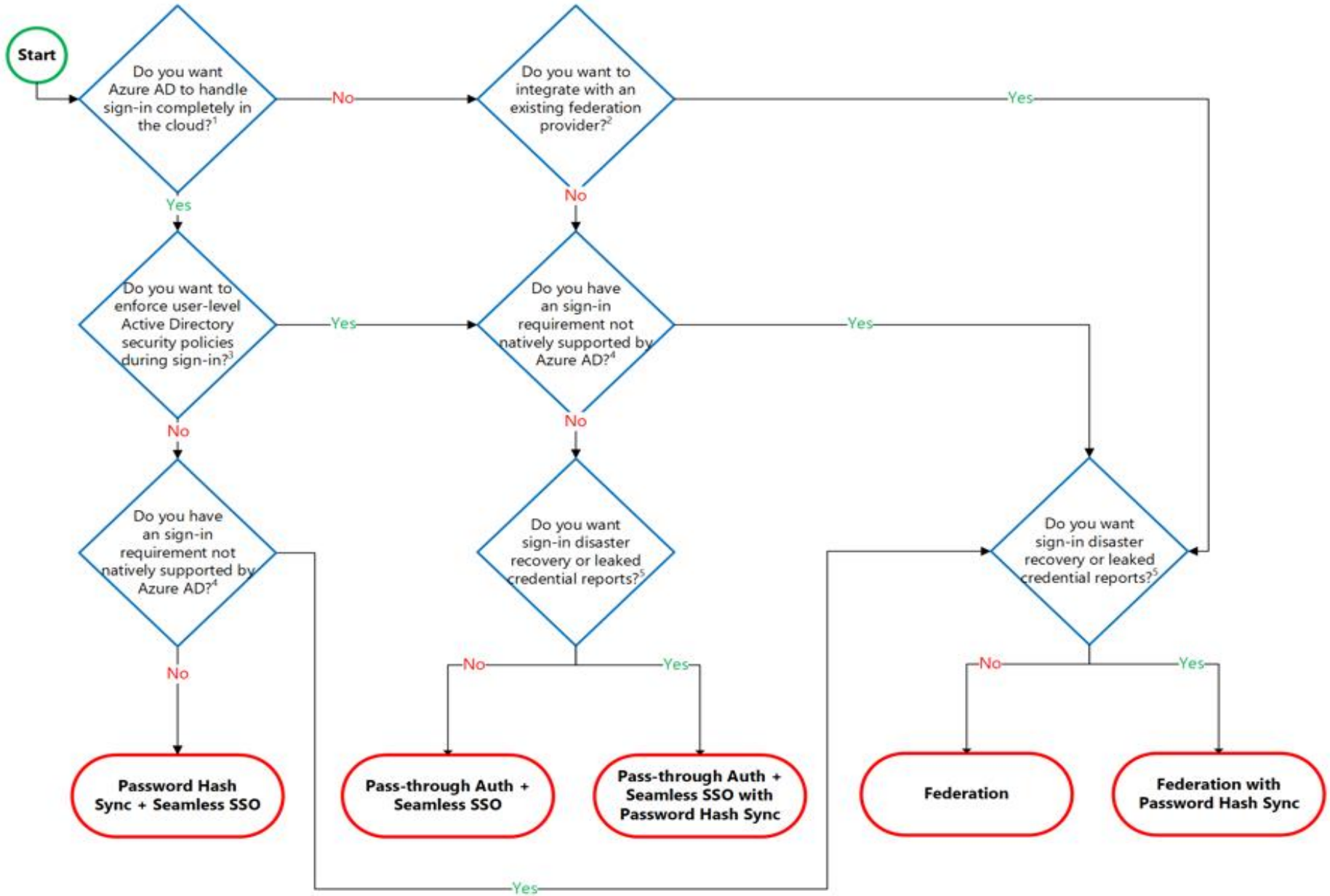
Woodgrove Bank – A national financial institution

Strong regulatory operation + Present in almost every region + 100'000 employees + Office 365 SaaS apps LOB apps

Azure AD Authentication decision tree



Azure AD Authentication decision tree



Resources

Choosing the right authentication method:

http://aka.ms/auth-options

Migration Guides:

http://aka.ms/aadauthmigrate

Azure AD Deployment plans:

http://aka.ms/deploymentplans

Hybrid Identity Framework:

Aka.ms/aadframework

Security Considerations:

Aka.ms/aaddatawhitepaper

Microsoft

Thank you.

Follow Microsoft Azure AD

 @AzureAD

aka.ms/enableMFA

…it’s free!