ANTHONY VAN DEN BOSSCHE
TECHNICAL CONSULTANT HYBRID CLOUD

O365 Authentication Demystified Securing Identities

CHAPTERS

1. Possible authentication methods
2. Which authentication method to choose
3. Securing Identities
4. Demo

REALDOLMEN
a Gfi Group company

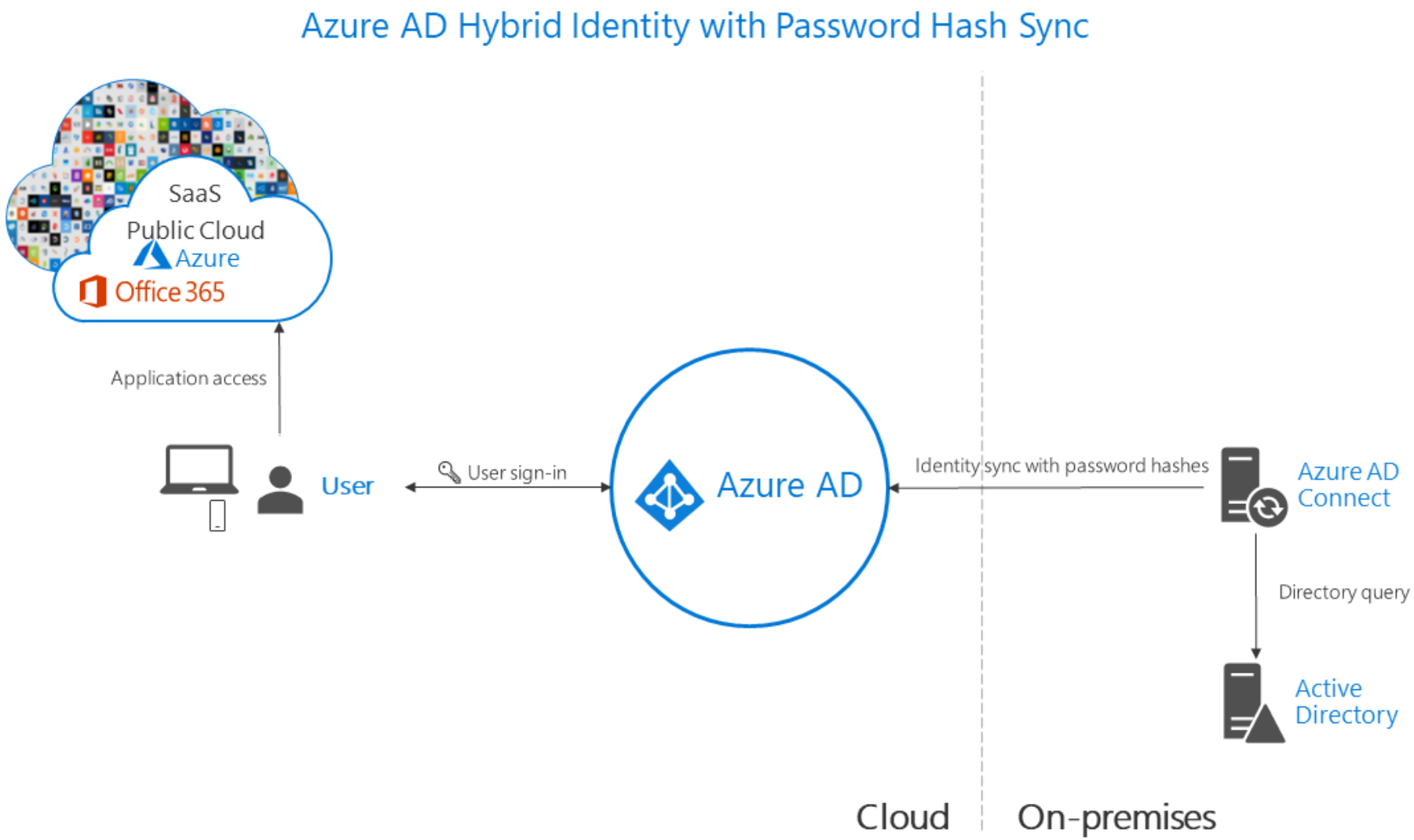
Office 365 authentication demystified

Different authentication possibilities

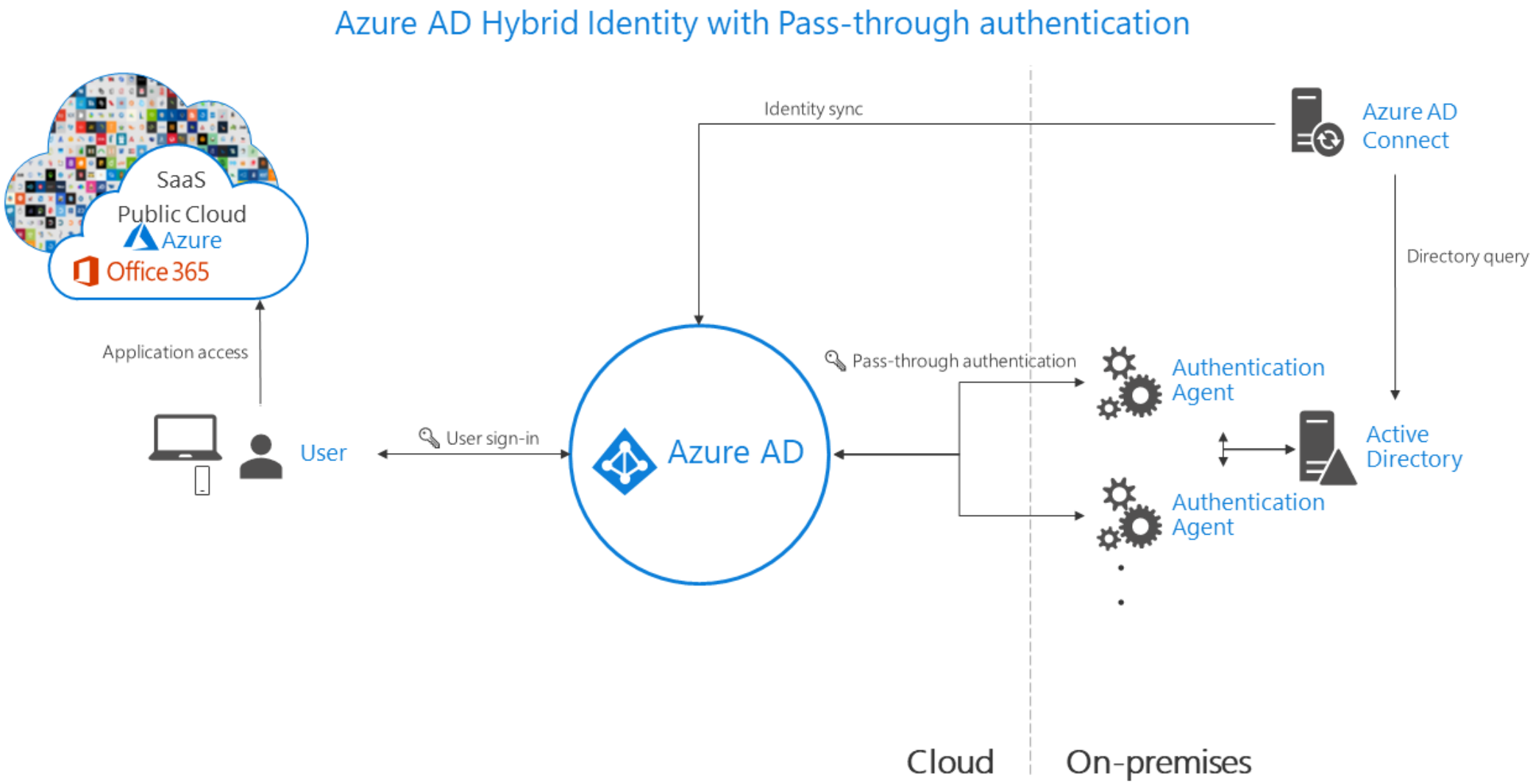
- 3 major types of **identities**
  - Cloud Identities (requires zero on-premises infrastructure) – not very common
  - Synchronized Identities (requires onprem AD + Azure AD Connect) – very common
  - Federated Identities (requires onprem AD and a Security Token Service) – implemented the most!
- A number of different **models**
  - Cloud Authentication
    - Password **Hash** Synchronization
    - Pass-through authentication
  - Federated Authentication
- Additional configuration options available
  - Seamless Single Sign On

- **Careful consideration is needed before moving forward!**

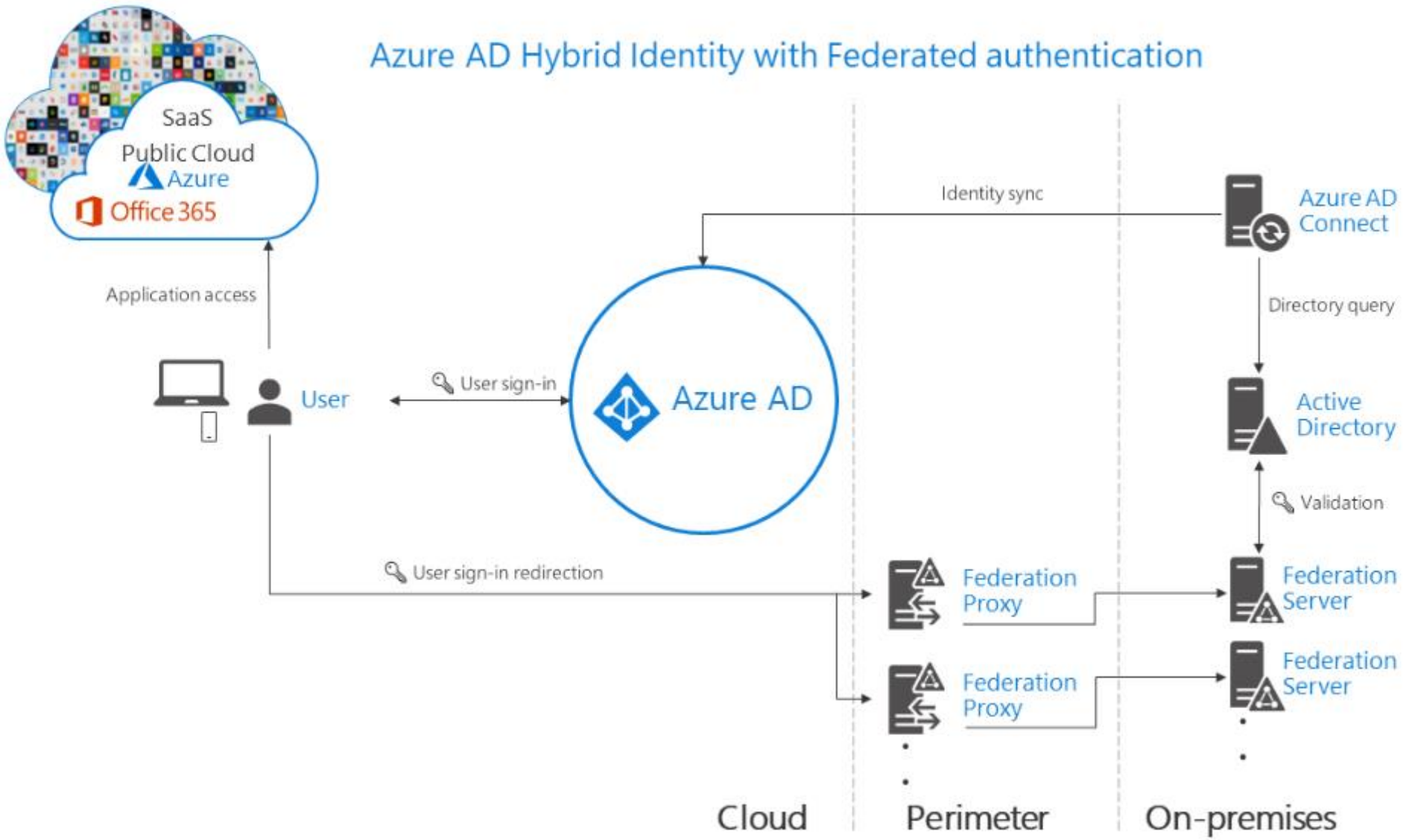
AUTHENTICATION ARCHITECTURE – PASSWORD HASH SYNCHRONIZATION



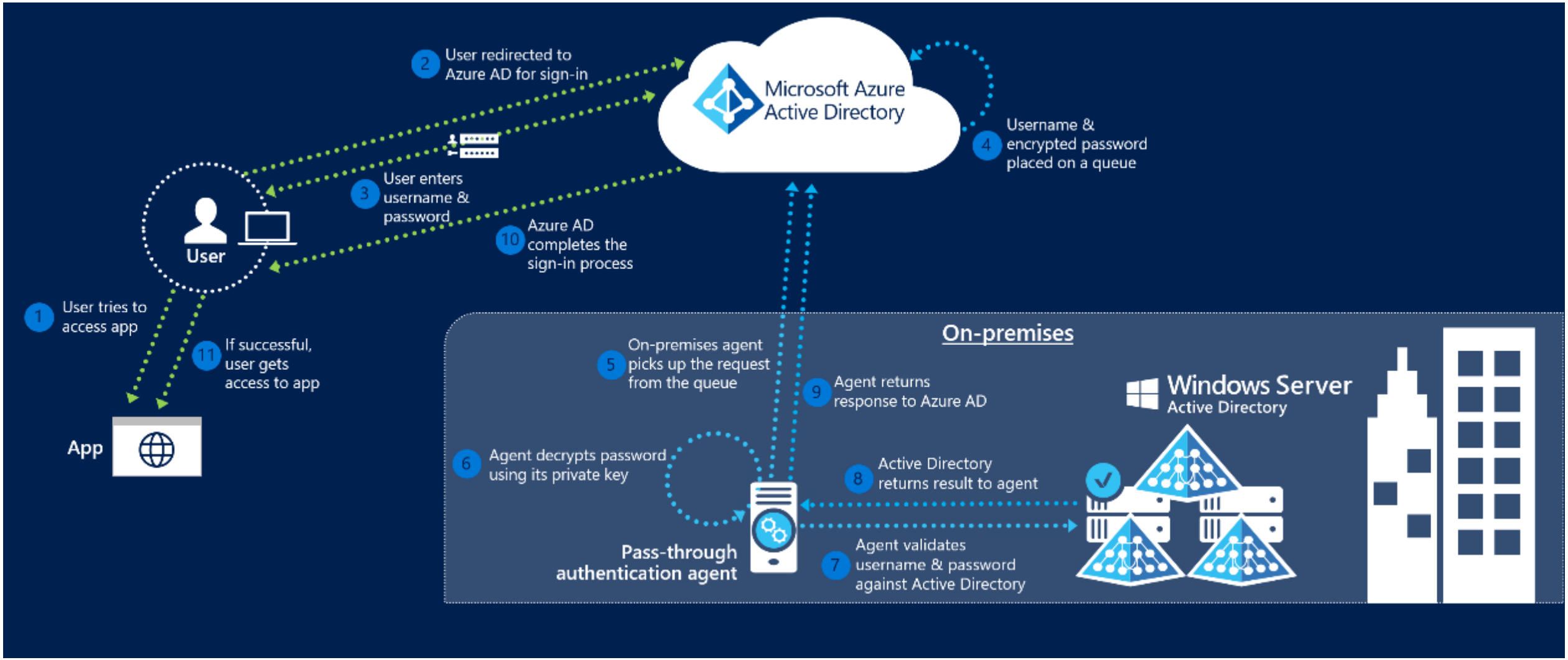
AUTHENTICATION ARCHITECTURE – PASS-THROUGH AUTHENTICATION



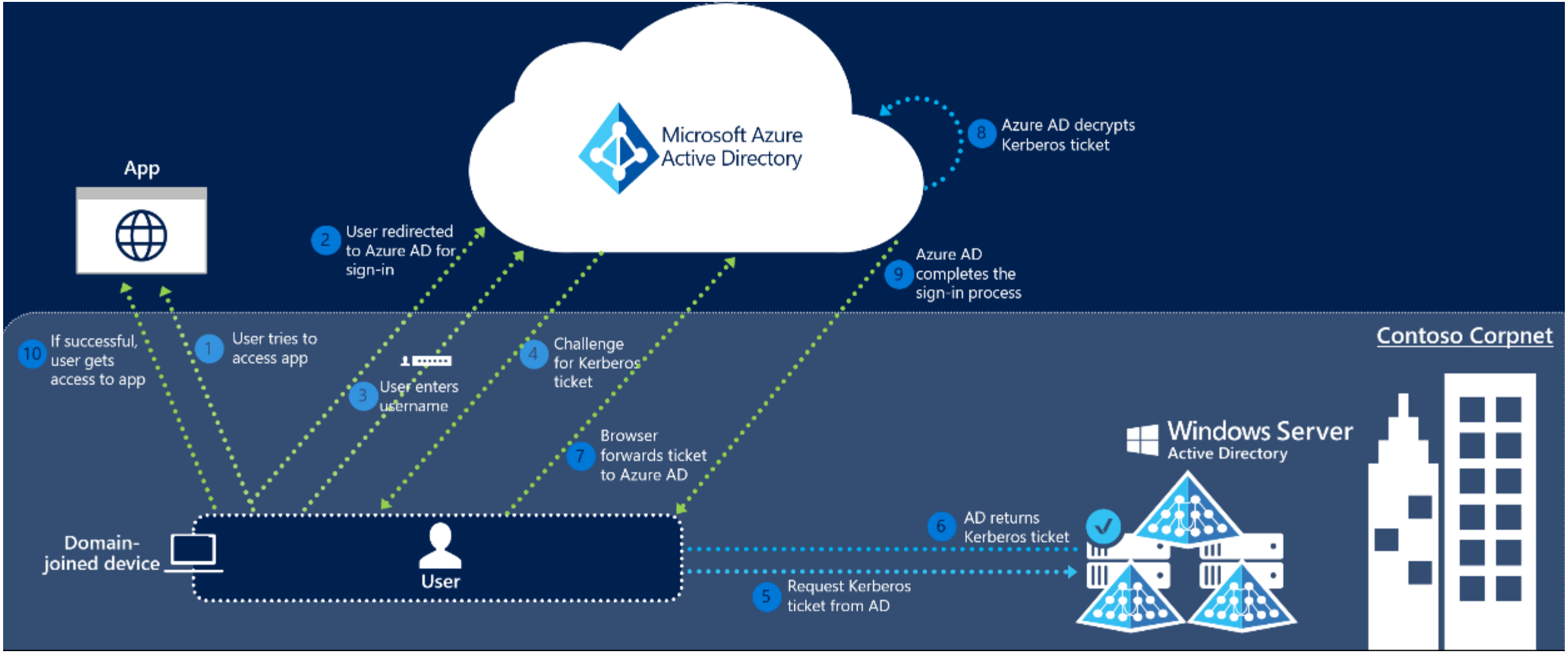
AUTHENTICATION ARCHITECTURE - FEDERATION



CONCEPTUAL INFO - PASS-THROUGH AUTHENTICATION



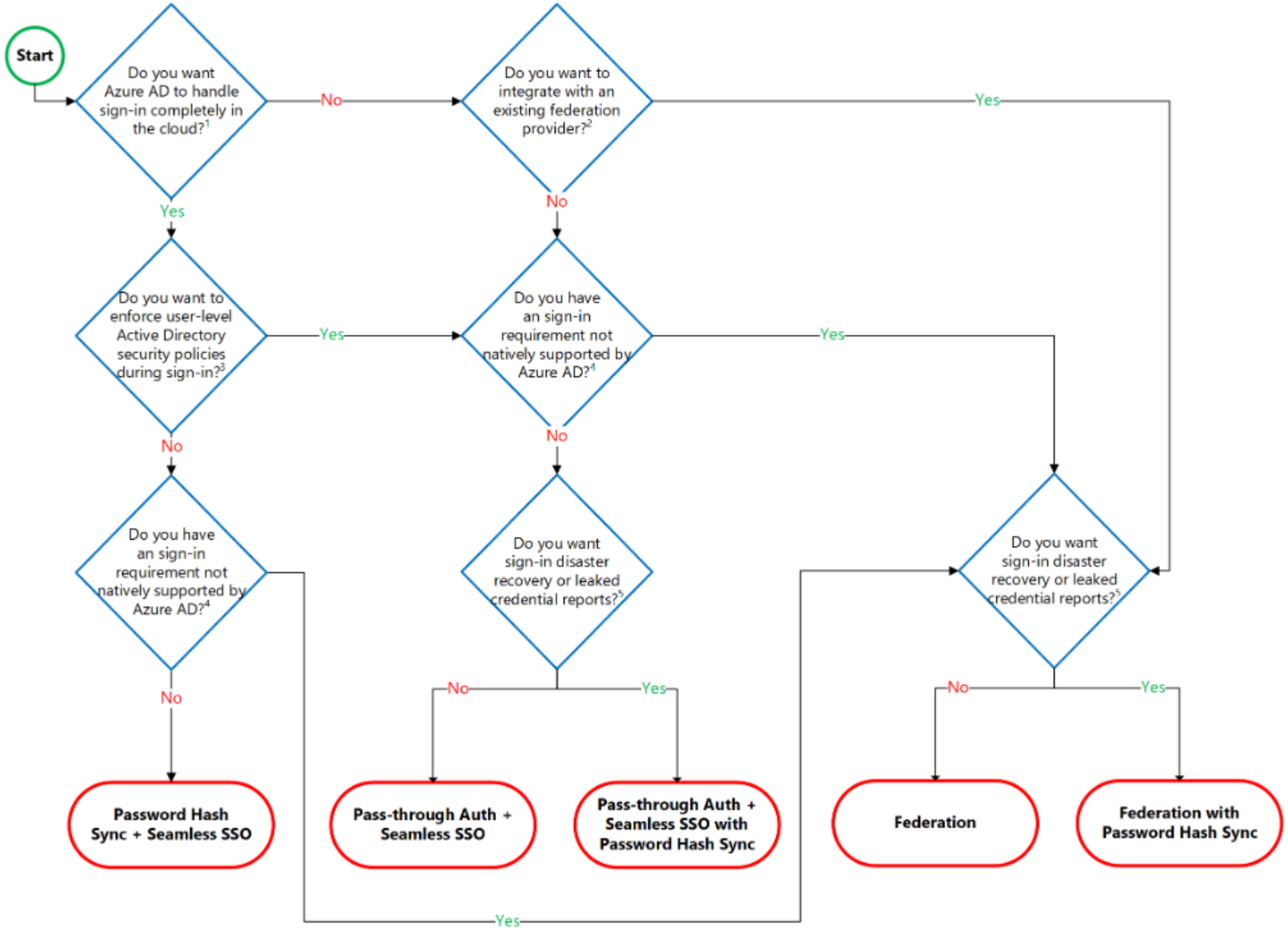
CONCEPTUAL INFO - SEAMLESS SINGLE SIGN ON



DECISION TAKING QUESTIONS

- How complex can my authentication method be?
  - Password Hash Sync only requires Azure AD Connect to configure
- How important is my end-user experience?
  - Use Azure AD Seamless Single Sign On to reduce authentication prompts
- How many infrastructure do I want to maintain to support authentication in the cloud?
  - PTA requires agents (self updating), ADFS needs 4 servers + Load Balancing
- Can I store password hashes in Azure AD?
  - If not, PTA and ADFS without Password Hash Sync are the only options
- Do I want to enjoy cloud driven, identity protection?
  - With Password Hash Sync, leaked credentials reports can be used (also Password Protection!)
- Do I want disaster recovery for my authentication method?
  - Have Password Hash Sync to fall back to
- Do I want Seamless Single Sign on? (Password-less signon)
  - ADFS and Azure AD SSSO leverage IWA to have SSSO

AUTHENTICATION METHODS – DECISION TREE



What about applications outside of office365

- Do we still need ADFS for Single Sign On? **No, we don't!**
- Azure AD is also a Security Token Service supporting SAML, OpenID, Oauth..
- Move applications to Azure AD
- Requires Premium P1 licenses on Azure AD
- Customers without P1 licenses can still rely on ADFS

SECURING IDENTITIES

Securing identities

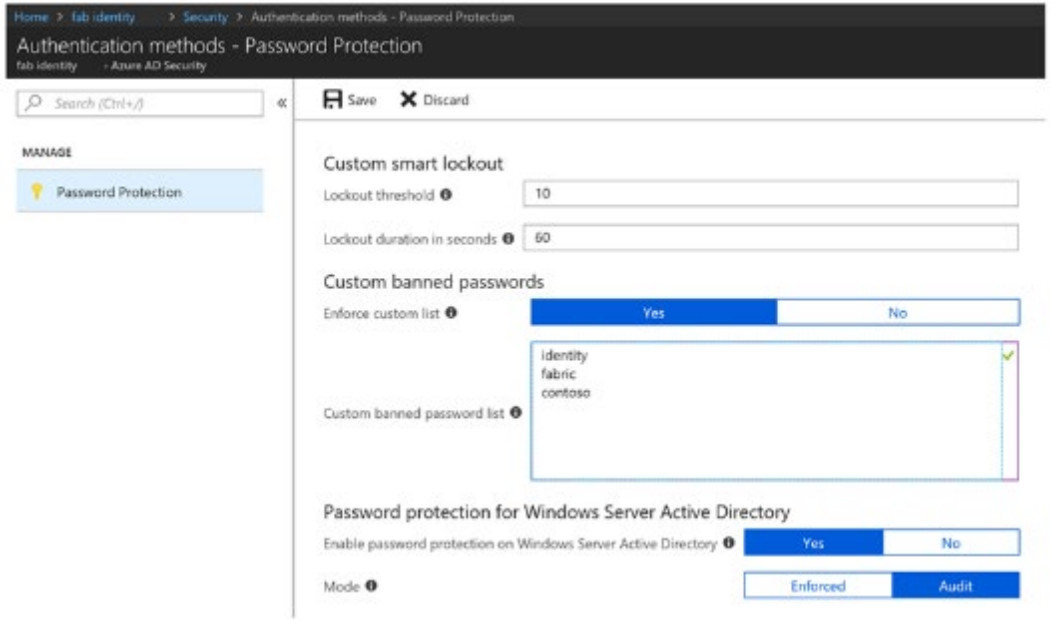
- As long as we've had passwords, people have tried to guess them
- 1 weak password is enough for a hacker
- Users tend to use predictable passwords and reuse them accross services
- Susceptible to brute force attacks like **password spraying**
  - Tools like mailsniper to learn about all users in an organization
  - Makes it look like isolated failed login attempts
  - Only have a success ratio of 0.5% is effective
- Which tools are present to prevent these kinds of attacks?
  - Use **Cloud authentication**! (Pass Hash Sync, PTA – ADFS with upgrade)
    - Smart lockout, IP lockout, Attack simulations
  - **Multifactor authentication** (what else ☺)
    - Risk based (Identity Protection), MFA Primary Auth,
  - **Better passwords**
    - SSPR (banned passwords), **custom banned passwords (Cloud + onprem)**, password never expire (?)

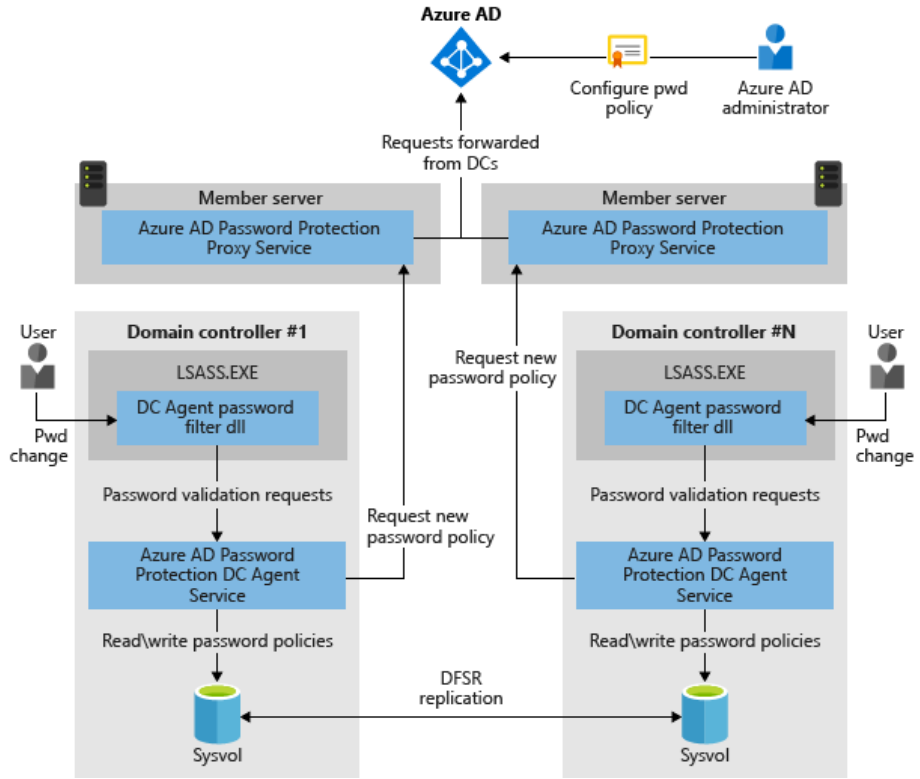
Target User	Target Password
User1@org1.com	Password1
User2@org1.com	Password1
User1@org2.com	Password1
User2@org2.com	Password1
…	…
User1@org1.com	P@$$w0rd
User2@org1.com	P@$$w0rd
User1@org2.com	P@$$w0rd
User2@org2.com	P@$$w0rd

SECURING IDENTITIES

PASSWORD PROTECTION & SMART LOCKOUT (PUBLIC PREVIEW!)

- Prevent users from using most commonly used passwords, plus over 1 million character substitution variations of those passwords
- Can be leveraged in both Azure AD as on premises AD
- Create own banned password list with company specific keywords
- Audit and enforcement mode





SECURING IDENTITIES

EASY CONFIGURATION

- Download Azure AD Password Protection Proxy service & Domain Controller Agent Service
- Install Proxy Service
  - Register proxy with the Azure AD tenant
  - Register AD Forest with the Azure AD tenant
- Install Domain Controller agent
- Configure using the Azure AD portal
- **Best practices**
  - 2 or more Proxy services for HA
  - Proxy services not on Domain Controllers (need Internet access)
- **Requirements**
  - Minimum Server 2012 for DC agent and 2012 R2 for Proxy service

SECURING IDENTITIES

HOW ARE PASSWORDS CHECKED?

- Step 1: normalization – **consider banned password "blank"**
  - Uppercase >> lowercase (B >> b) and letter substitution ($ >> s)
  - Users try **Bl@nk** which is converted to blank and thus matches
- Step 2: fuzzy matching - **consider banned password "blank"**
  - Normalized password put through matching process with an edit distance of 1
  - **"blanky"** is tried and the edit distance of 1 reduces it to blank and thus matches
- Step 3: substring matching
  - Check for usage of firstname, lastname, tenantname
  - User is called **John Blank**, tries **Blank123!** Which substring matches to the user's lastname
- Step 4: score calculation – **consider banned passwords "blank" and "password"**
  - Passwords changes are given a score based on matches and leftover characters
  - User tries **BlankPassword12**, 2 banned passwords scores 2 points, 2 leftover characters score 2 points
  - If score under 5 points, then it's rejected

Demo: password protection

To get there, together

REALDOLMEN

HQ Realdolmen Huizingen
A. Vaucampslaan 42
B-1654 Huizingen
+32 2 801 55 55

www.realdolmen.com