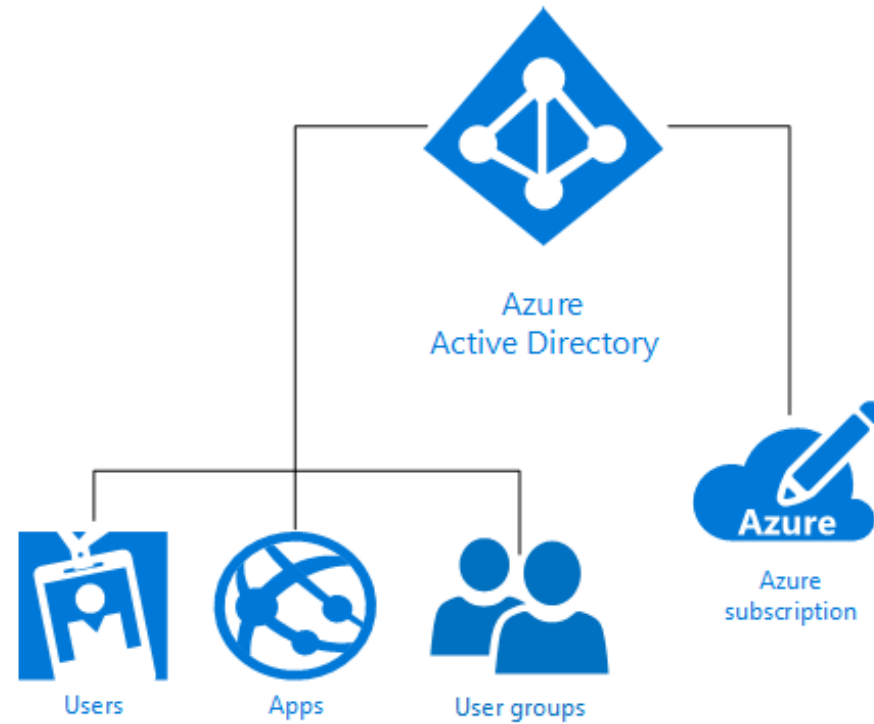


Identity and Access Essentials

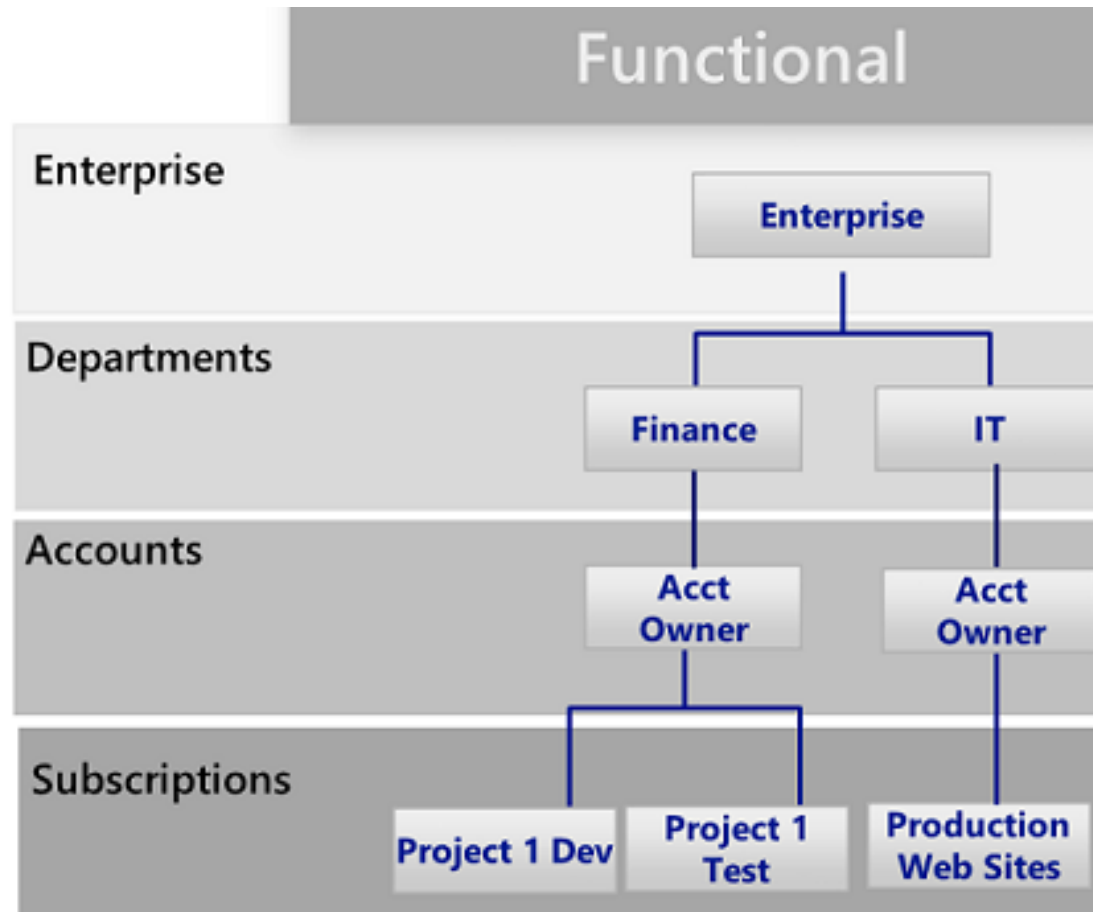
Terms to Know

- Azure Subscription
- Azure Tenant
- Azure AD Directory
- Custom Domain
- Azure Subscription Administrator
- Azure AD Global Administrator

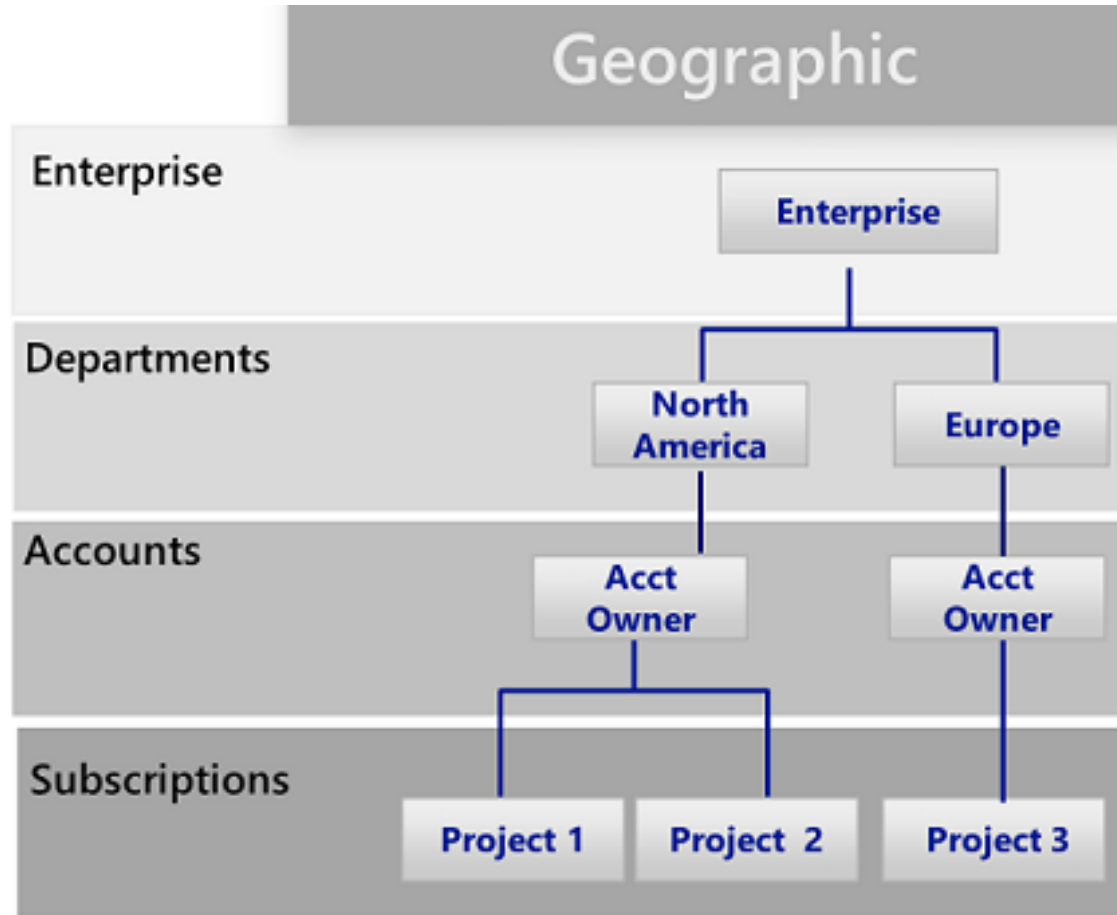
Tenant, Subscription, Administrator...



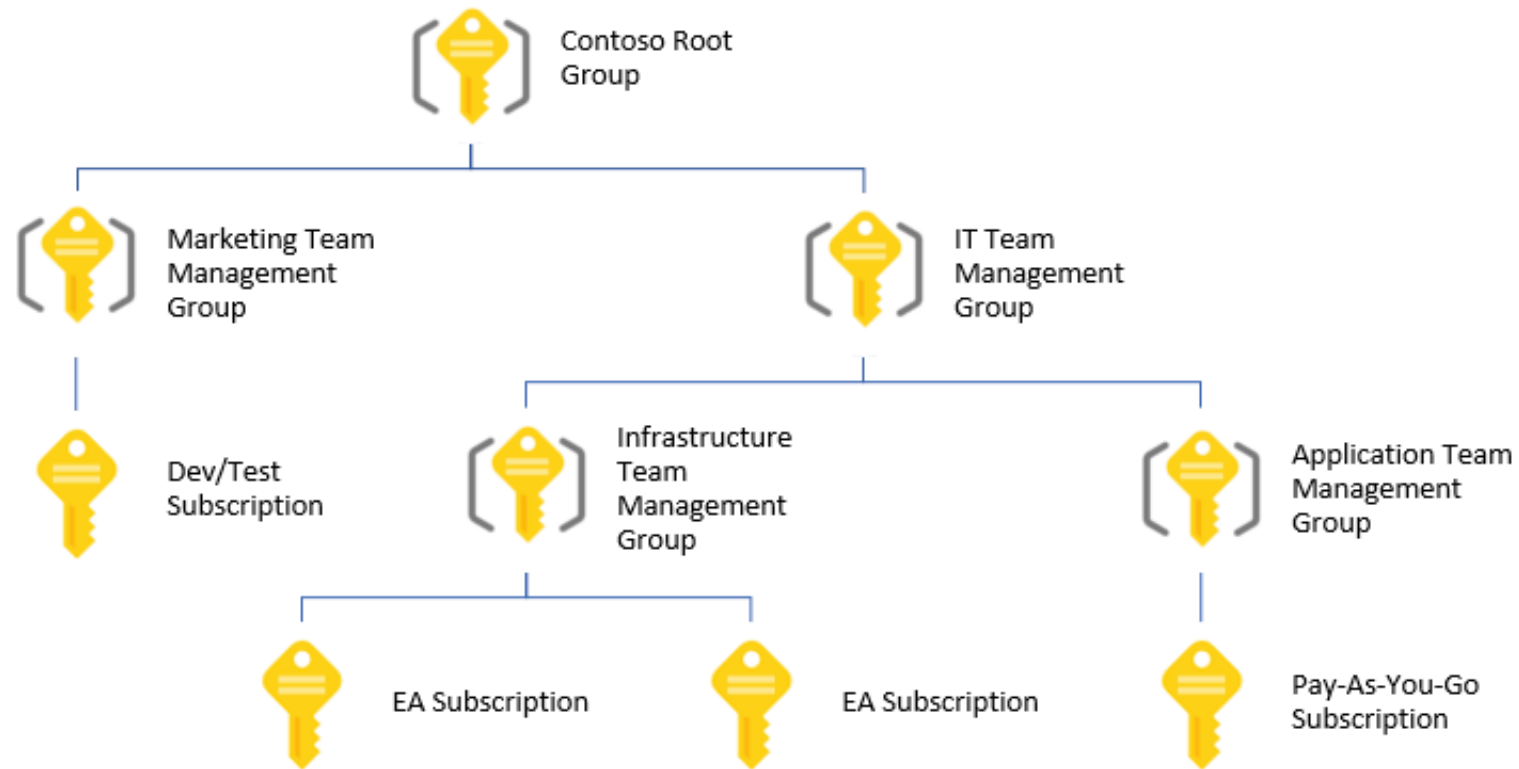
Subscription Governance



Subscription Governance



Management Groups



Management Groups

- Organize subscriptions into containers called "management groups"
- Apply governance conditions to the management groups
- All subscriptions within a management group automatically inherit the conditions applied to the management group
- Max six levels deep (total 10,000 management groups)

Subscription Governance

- P &P Guidance
 - <https://docs.microsoft.com/en-us/azure/architecture/best-practices/naming-conventions>
- Resource Tags
 - Billing
 - Service Context Identification
- Policies

Policies and Auditing

- **Geo-compliance/data sovereignty** - ensure resources are created close to the end consumers of the resources
- **Cost management** - ensure that standard subscriptions avoid using unnecessarily large resources
- **Default governance through required tags** ensure that a resource is appropriately tagged. Department, Resource Owner, and Environment type (for example - production, test, development)

Why Azure AD?



SSO to SaaS

Single-sign On to thousands of 3rd party SaaS application from any device



Azure AD Connect

More options for authentication than any other vendor.



Office 365 App Launcher

Office 365 Integration



Remote Access to on-premises apps

Secure remote access to on-premises apps.



Identity Protection

Unique Risk-based Identity Protection



Conditional Access

Conditional

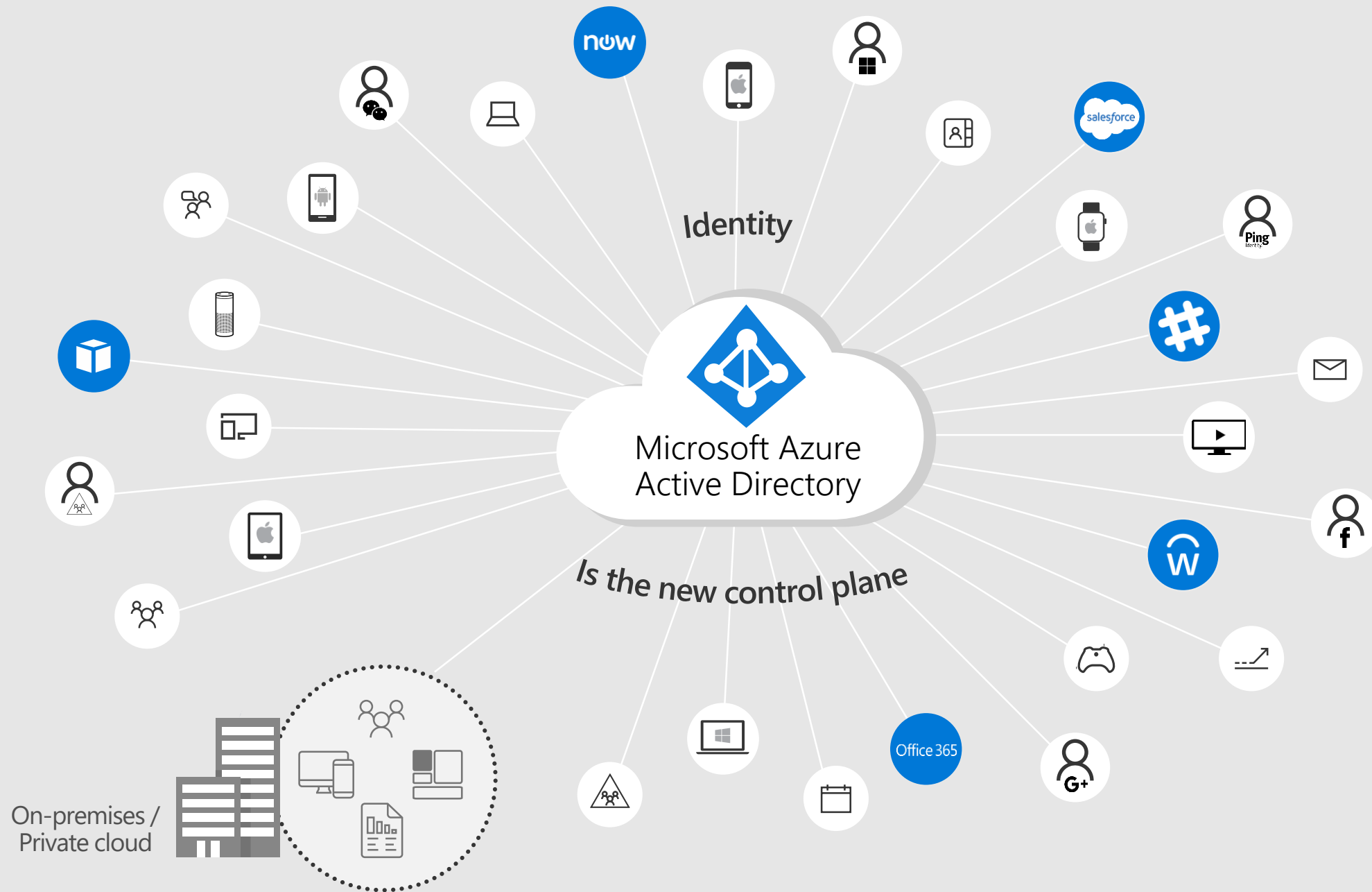


Security Reporting

Advanced Security Reporting



Holistic security solution with Enterprise Mobility + Security (EMS)



Azure Active Directory in the Marketplace

— Every Office 365 and Microsoft Azure customer uses Azure Active Directory —

14.2_M

organizations

+30%
YoY

1.01_B

identities

+35%
YoY

334_k

3rd party apps
in Azure AD

+150%
YoY

64_k

paid Azure AD /
EMS customers

























+65%
YoY

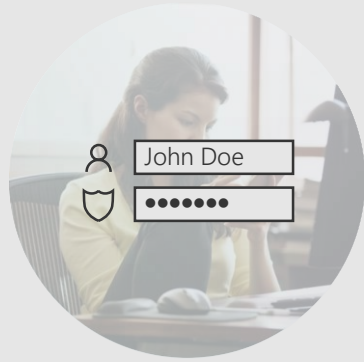
90%

of Fortune 500
companies use
Azure AD

Azure Active Directory

— Identity and access management for employees, partners, and customers —

 B2B collaboration	 Provisioning-Deprovisioning	 Addition of custom cloud apps	 Access Panel/MyApps	 Dynamic Groups	 Identity Protection
 Self-Service capabilities	 Connect Health	 Remote Access to on-premises apps	 Azure AD B2C	 Group-Based Licensing	 Privileged Identity Management
 Azure AD Connect	 Conditional Access	 Microsoft Authenticator - Password-less Access	 Azure AD Join	 MDM-auto enrollment / Enterprise State Roaming	 Security Reporting
 SSO to SaaS	 Multi-Factor Authentication	 Azure AD DS	 Office 365 App Launcher	 HR App Integration	 Access Reviews



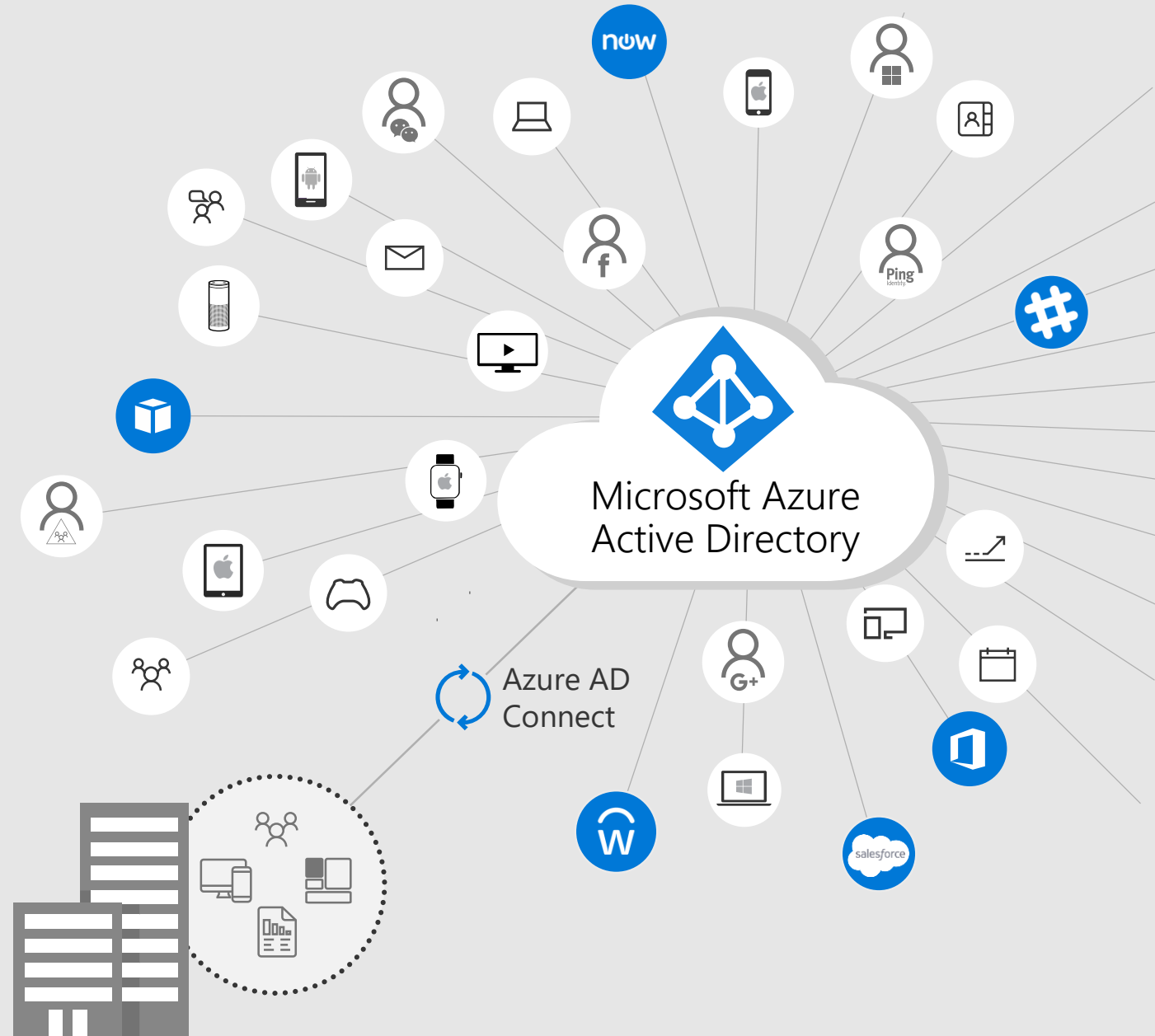
I want to provide my employees access to every app from any location and any device

Hybrid

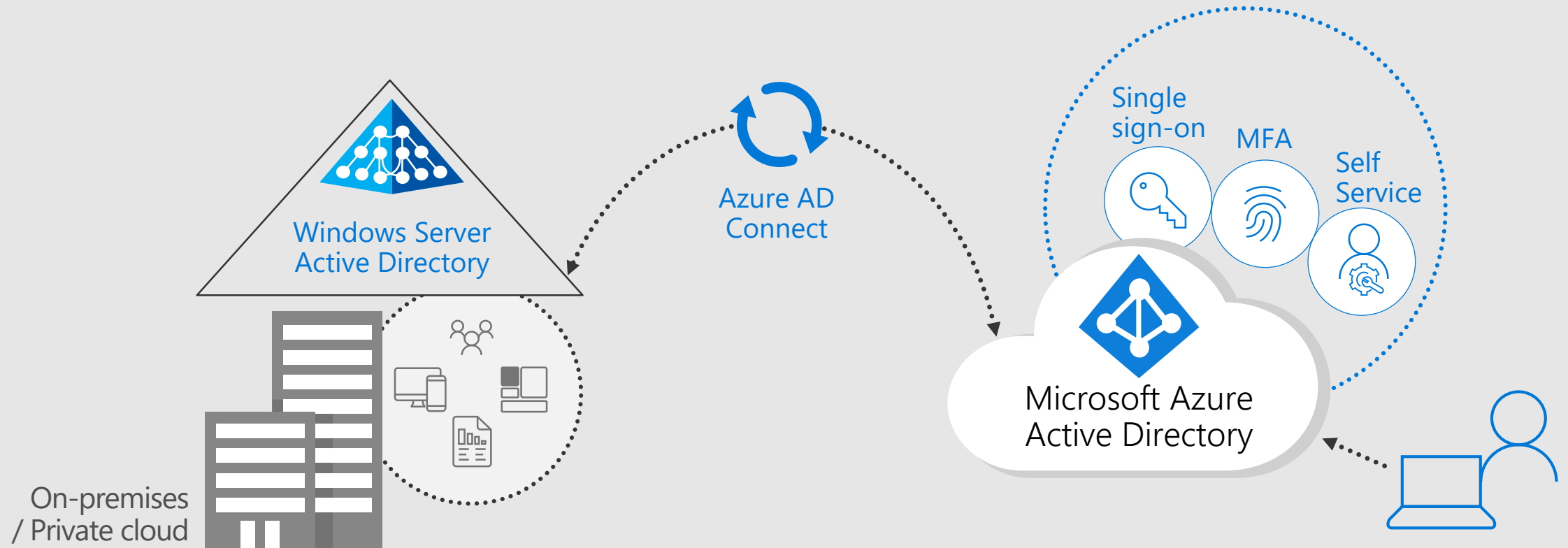
1 Identity

Multiple apps

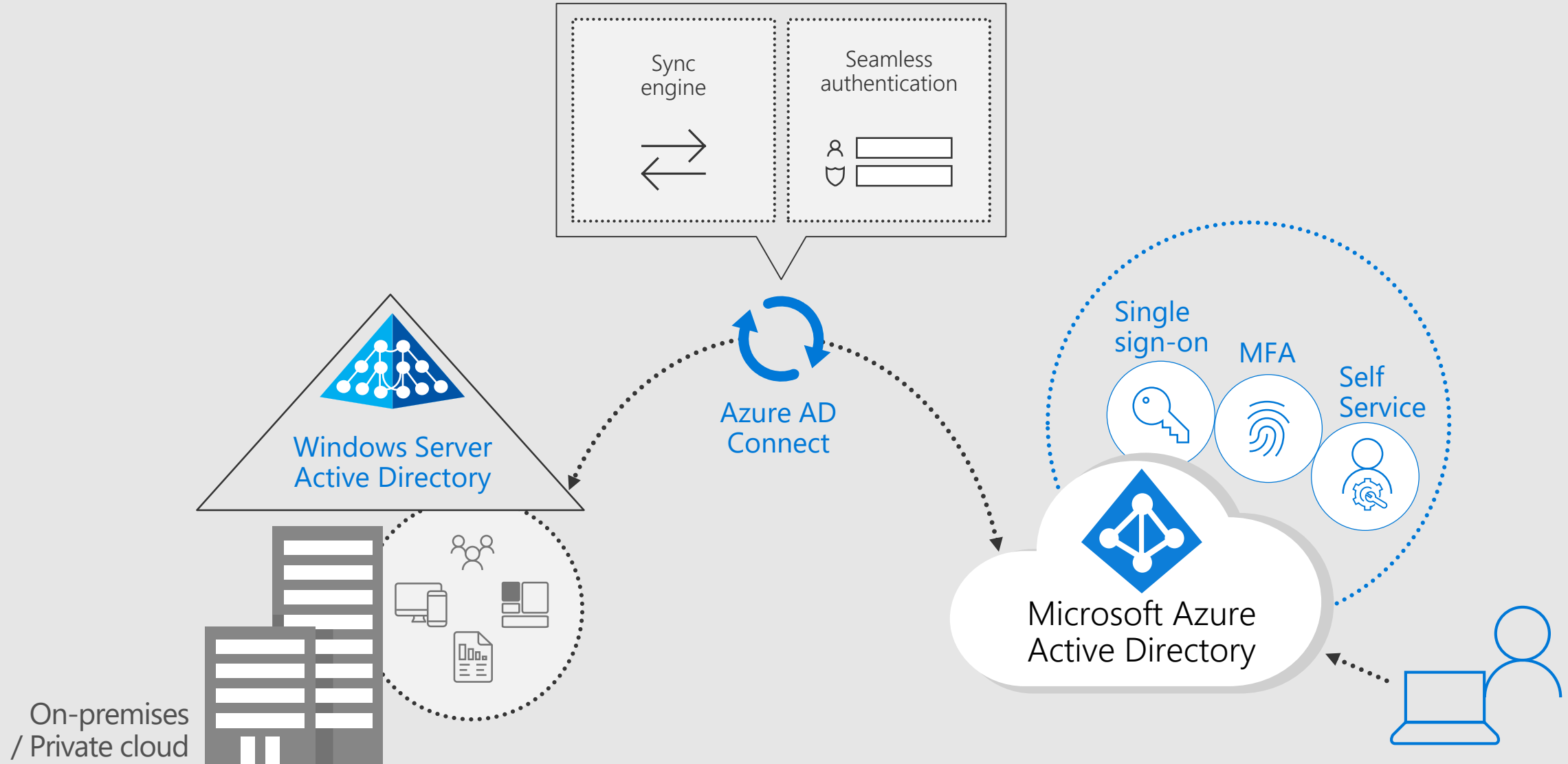
On-premises /
Private cloud



Hybrid

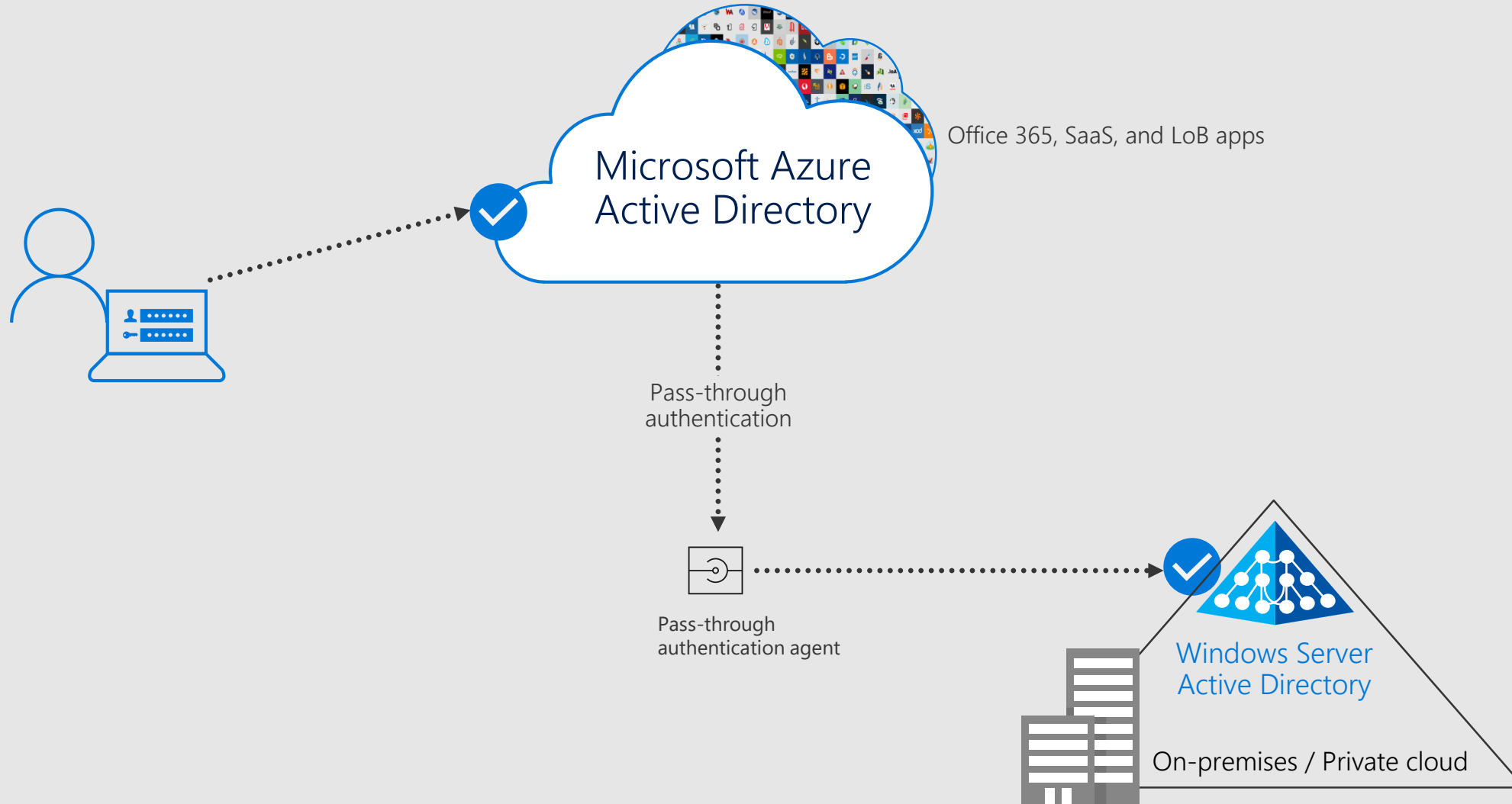


1 Identity



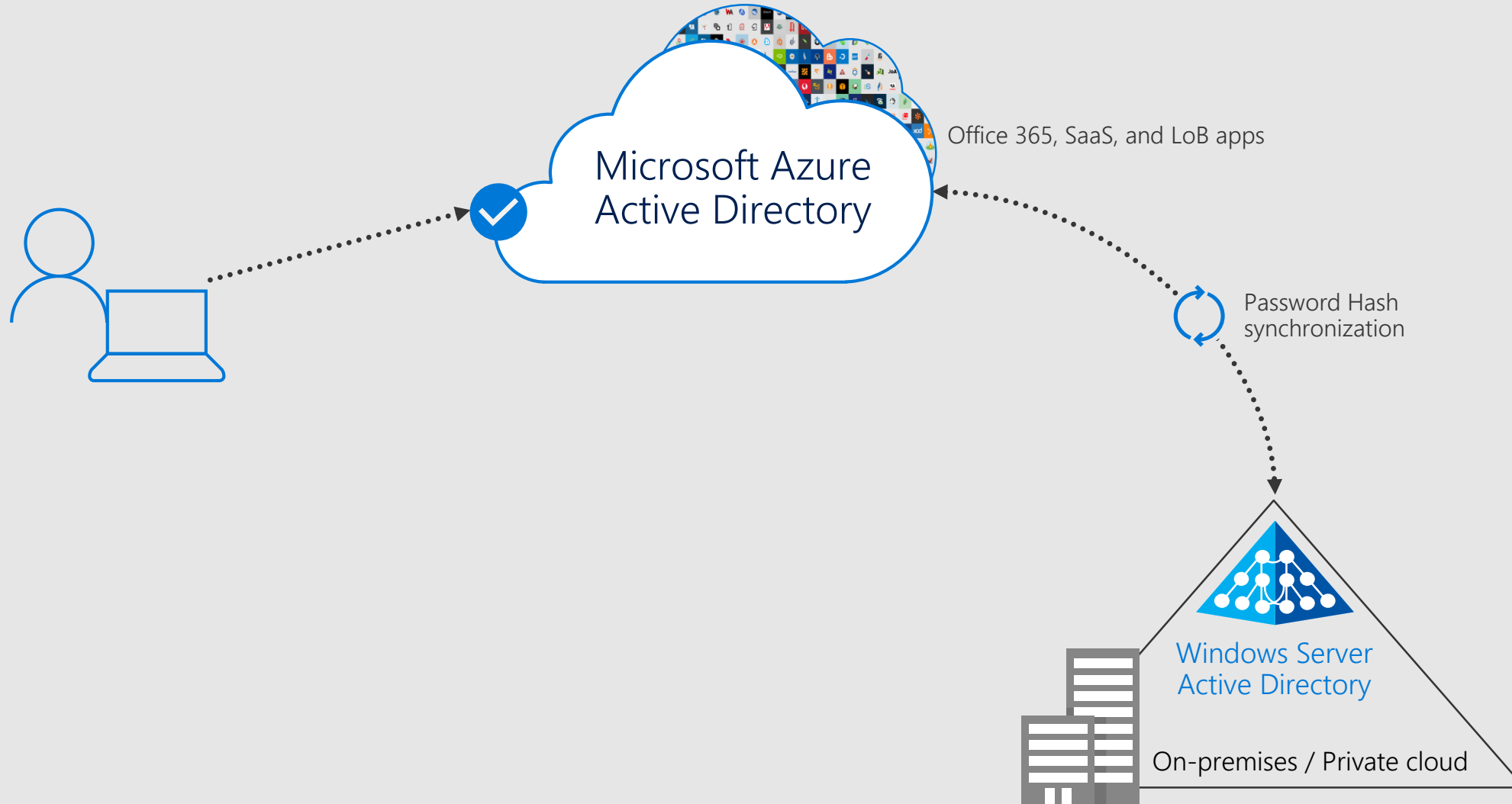
Azure AD Connect authentication options

Pass-through authentication



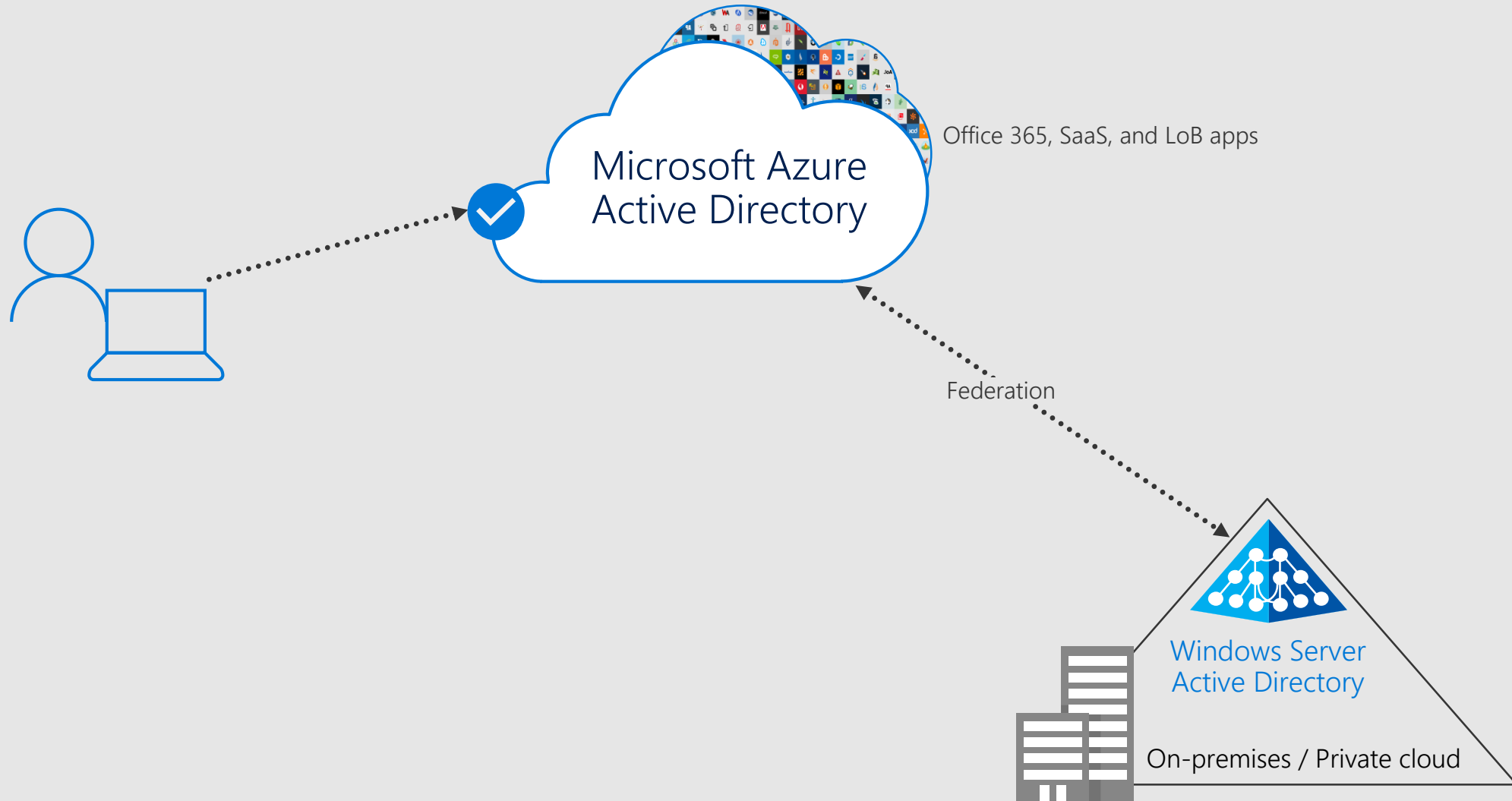
Azure AD Connect authentication options

Password Hash synchronization

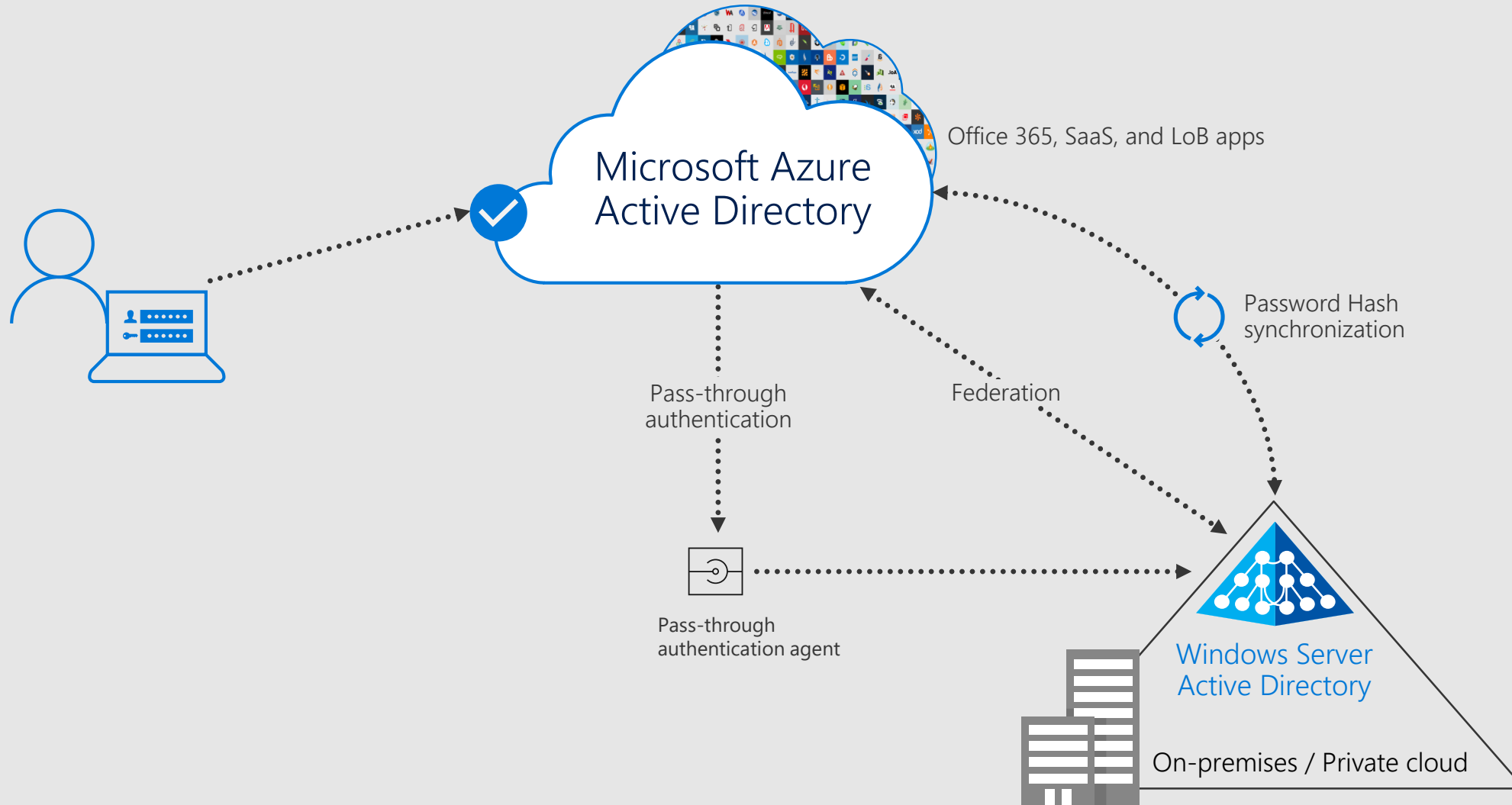


Azure AD Connect authentication options

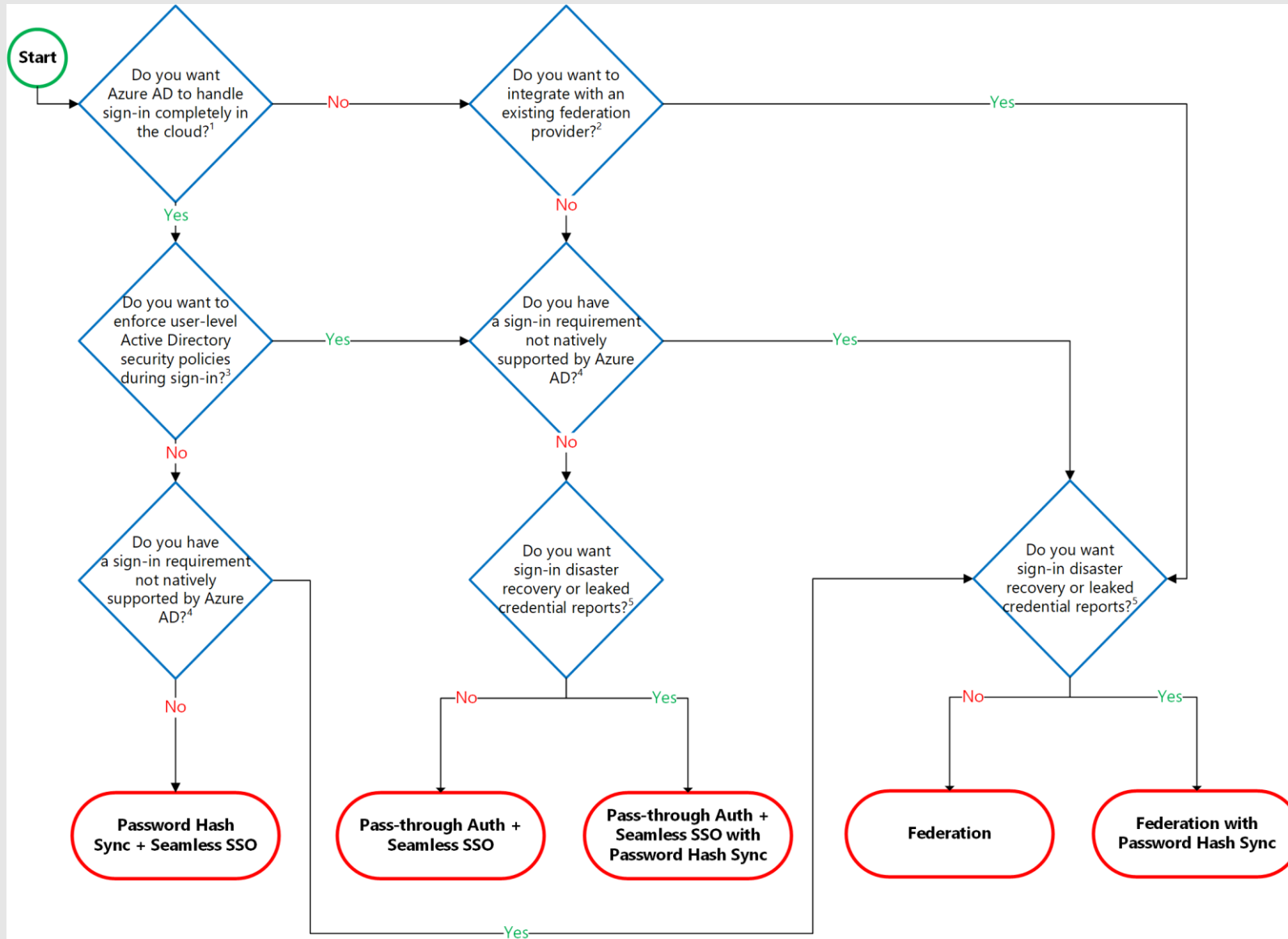
Federation via ADFS



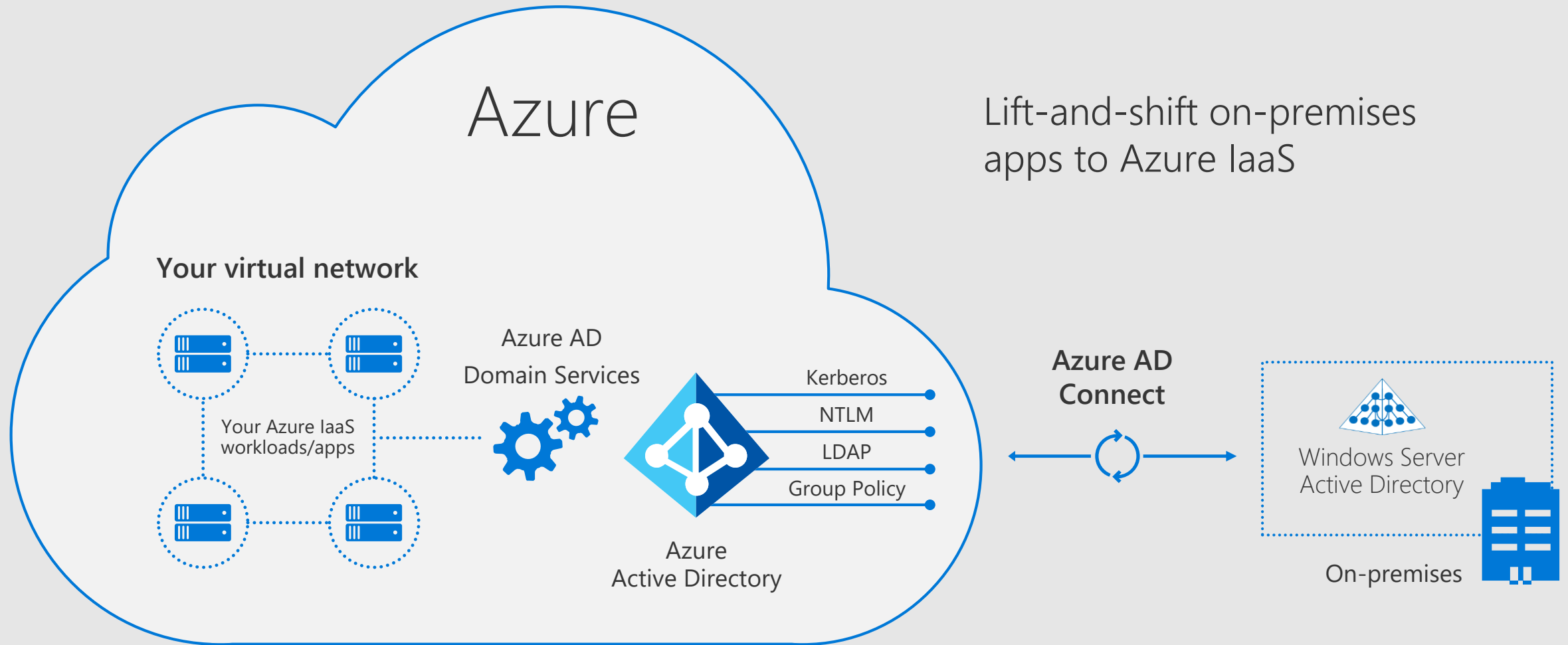
Hybrid authentication options



Hybrid Decision Tree



Azure Active Directory Domain Services



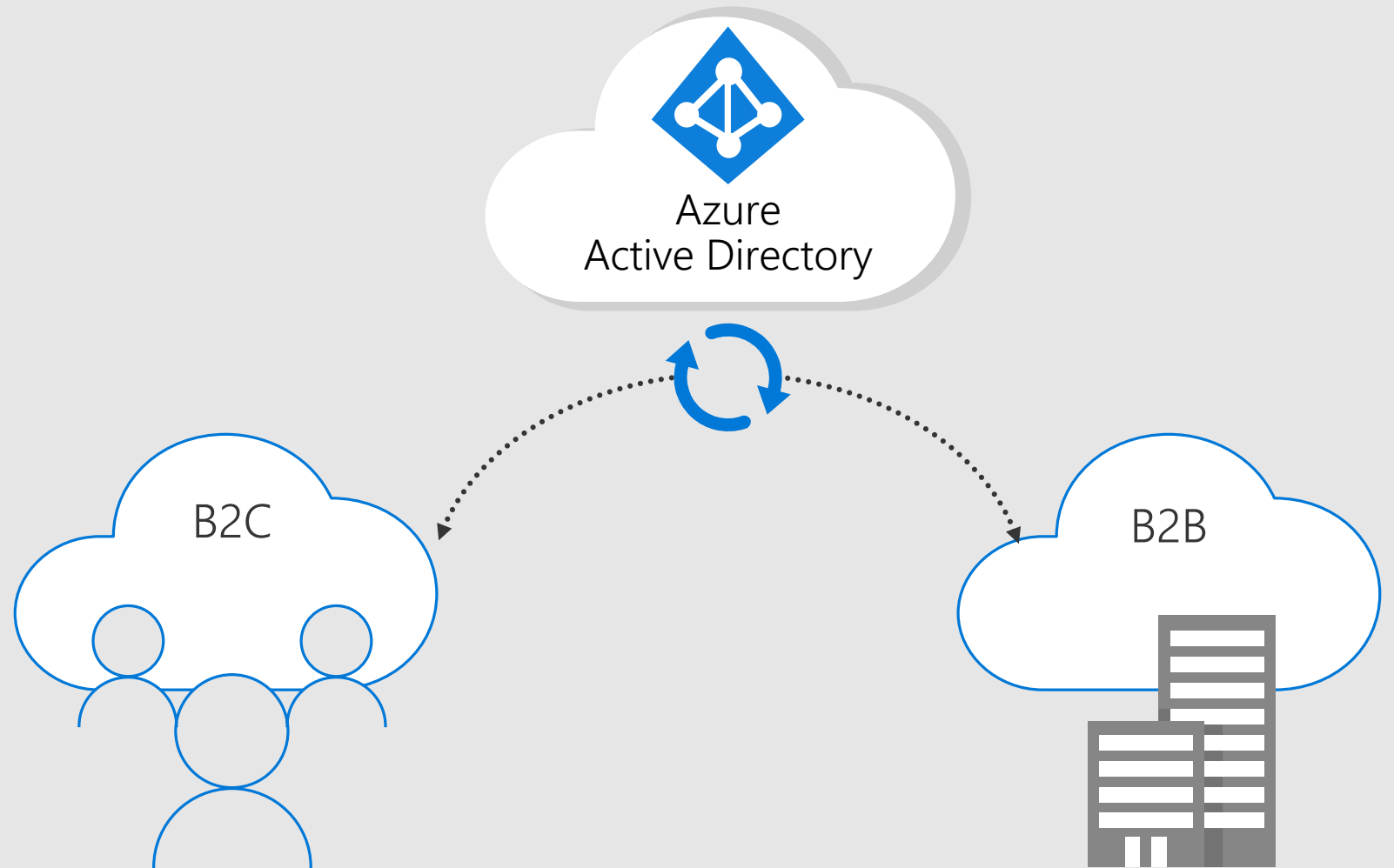


I want my customers
and partners to access
the apps they need

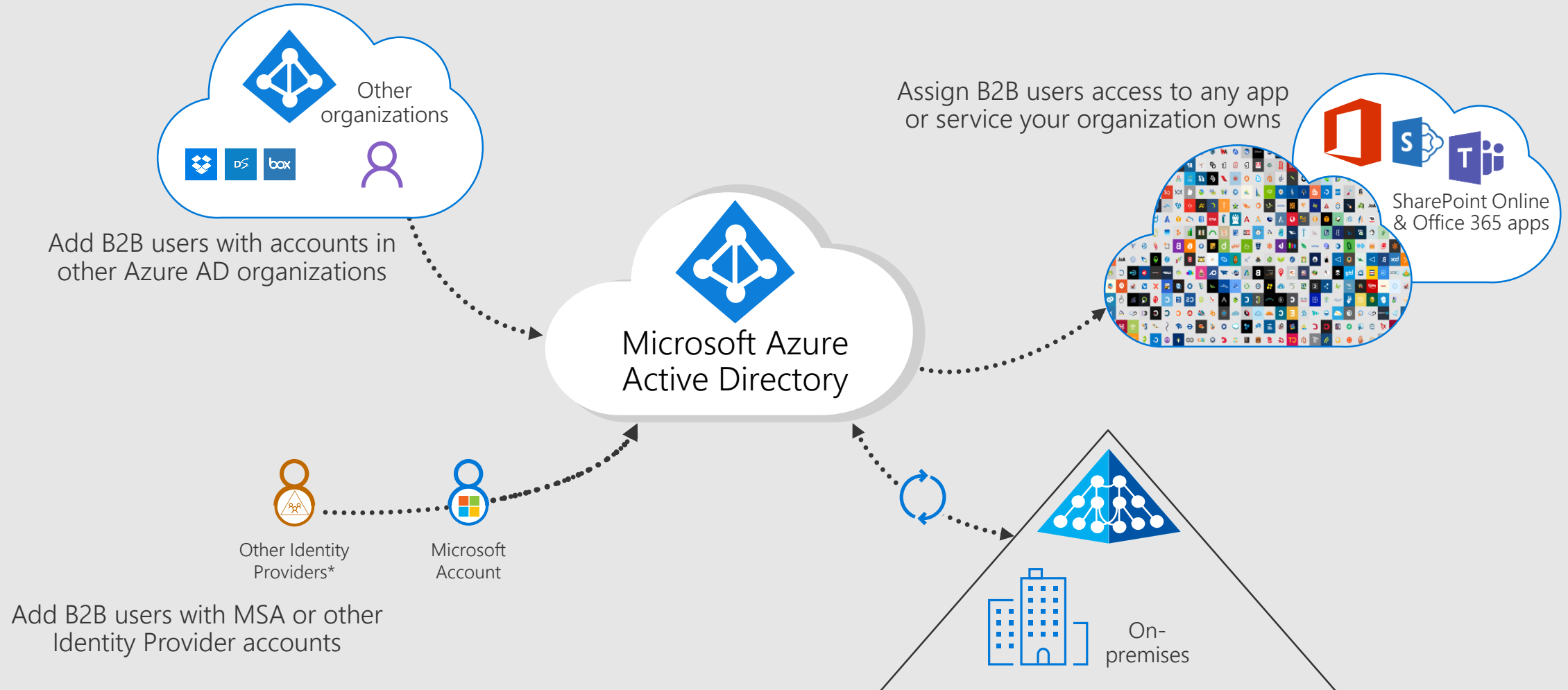
Secure collaboration

Simple sign-in and sign-up

Branded experience



Azure AD B2B collaboration



Azure Active Directory B2C

- ➔ 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



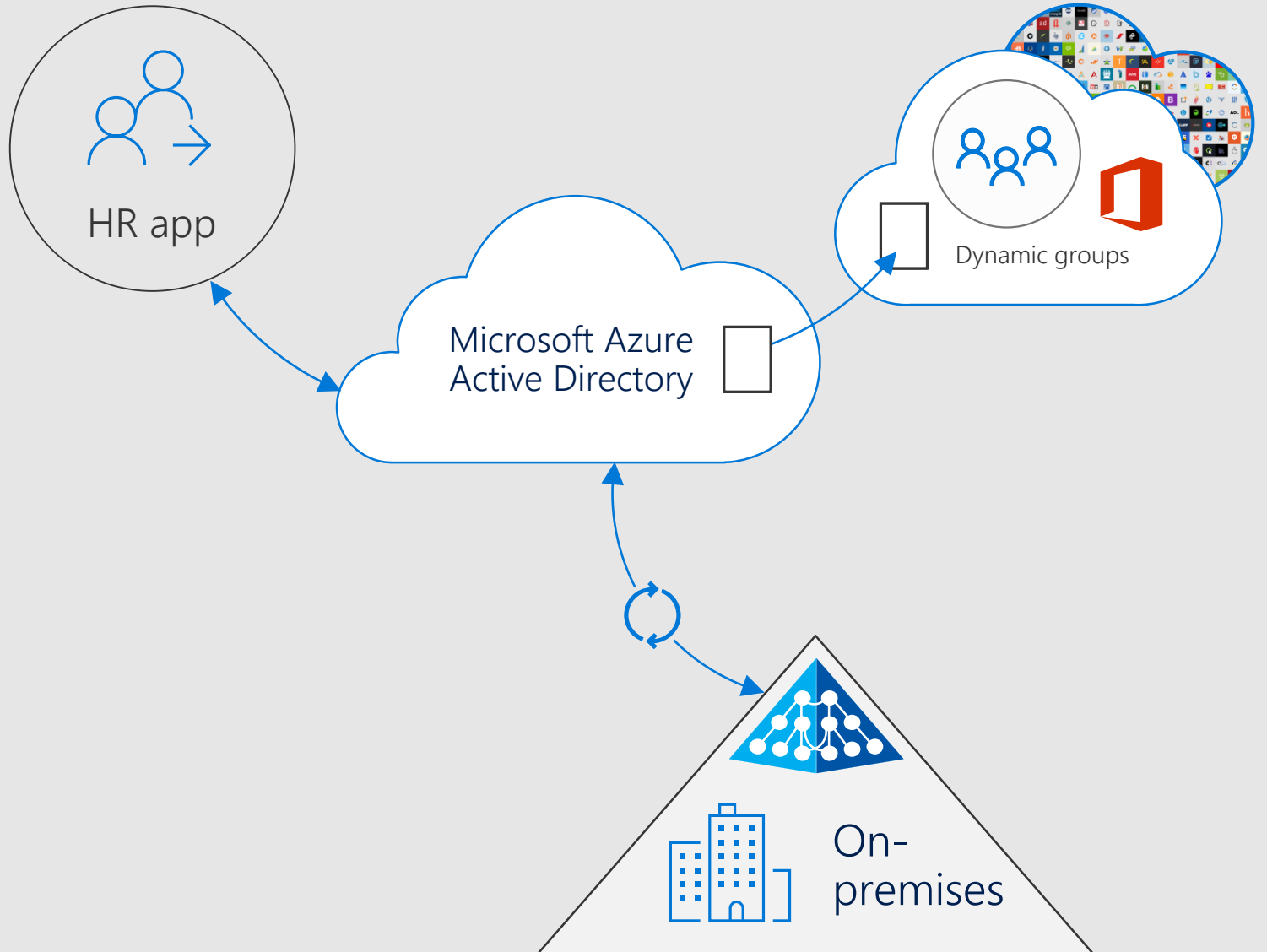


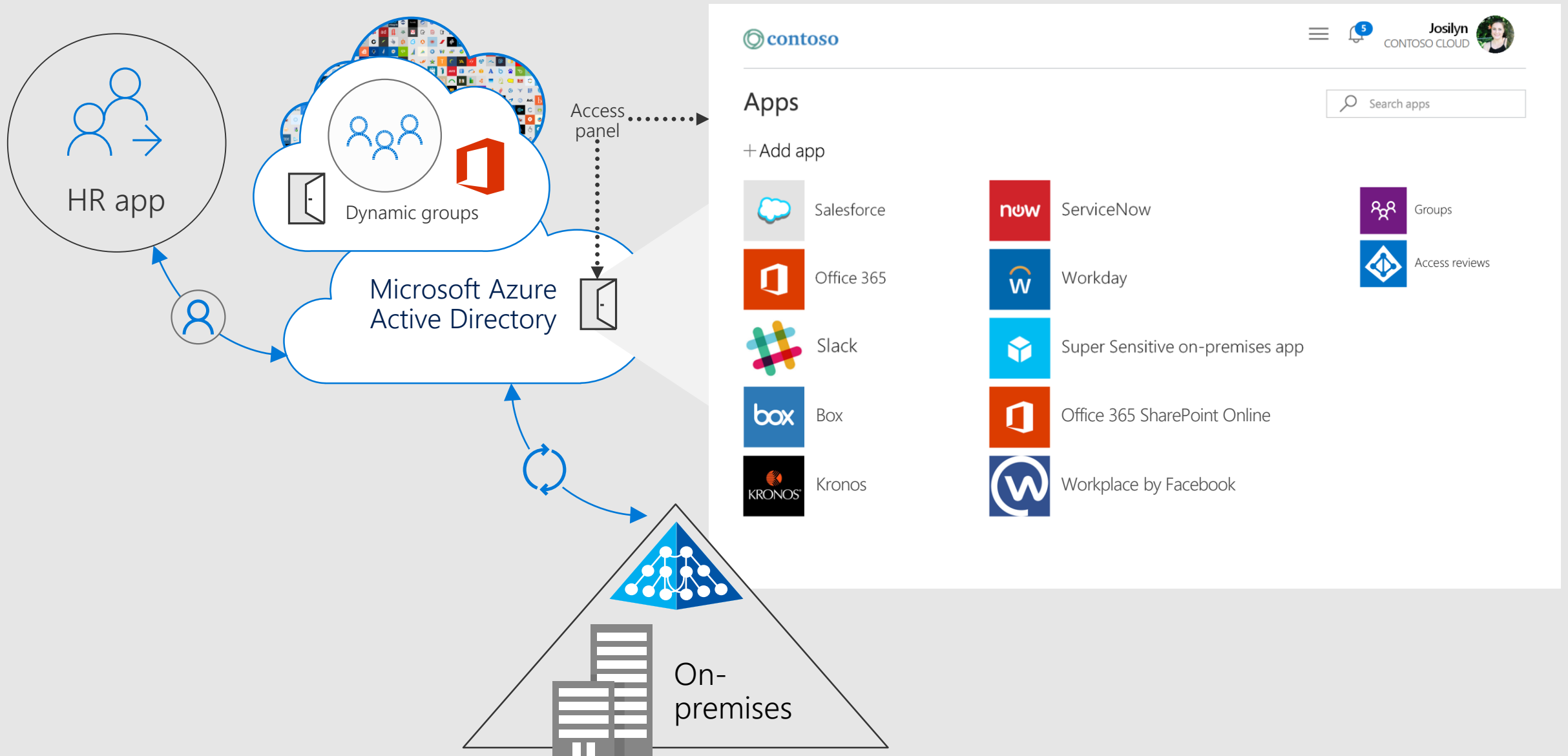
I want to automate the user identity lifecycle and cut down on helpdesk costs

Join/Move/Leave

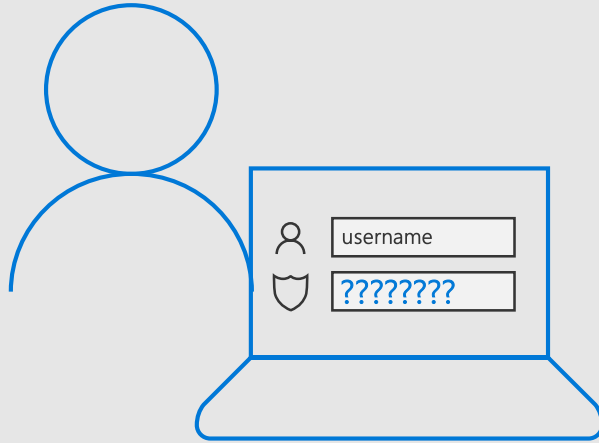
Self-service capabilities

Access reviews





Self service password reset



- Resolving password issues for users is one of the largest IT costs
- Self-service password reset empowers users and reduces administration costs

A screenshot of a web application for 'contoso'. The header includes the 'contoso' logo, a hamburger menu, a notification bell with a blue circle containing the number '5', and a user profile for 'Josilyn' with a circular avatar and the text 'CONTOSO CLOUD'. The main heading is 'change password'. Below it, a message states: 'Strong password required. Enter 8-16 characters. Do not include common words or names. Combine uppercase letters, lowercase letters, numbers, and symbols.' The form includes the following fields: 'User ID' (pre-filled with 'josilync@contoso.com'), 'Old password', 'Create new password', 'Password strength' (a sub-field under 'Create new password'), and 'Confirm new password'. At the bottom are two buttons: a green 'submit' button and a blue 'cancel' link.

Azure Active Directory Join for Windows 10

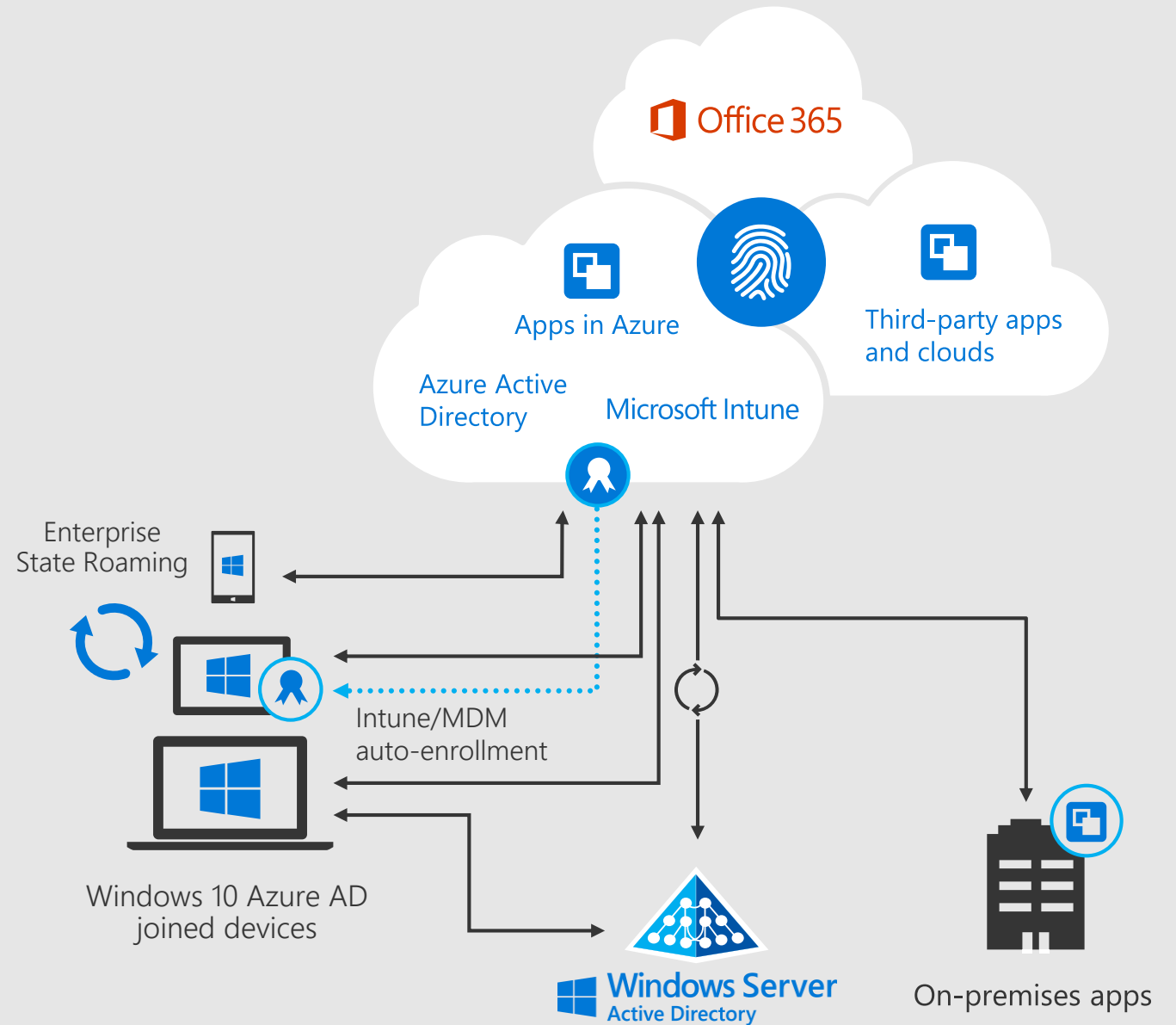
Azure Active Directory Join makes it possible to connect work-owned Windows 10 devices to your company's Azure Active Directory

Enterprise-compliant services

SSO from the desktop to cloud and on-premises applications with no VPN

MDM auto-enrollment

Support for hybrid environments





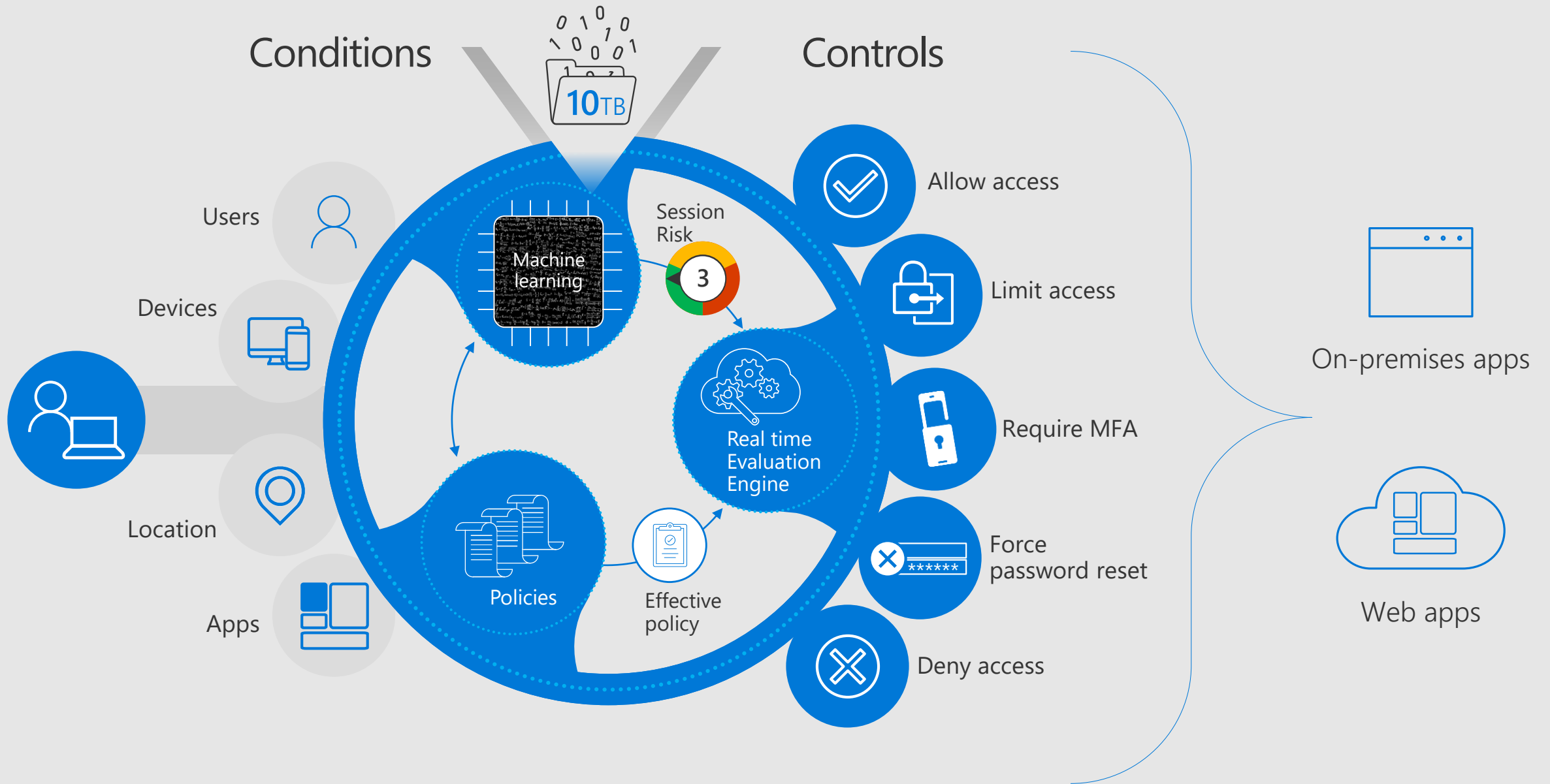
I want to protect access to my resources from threats

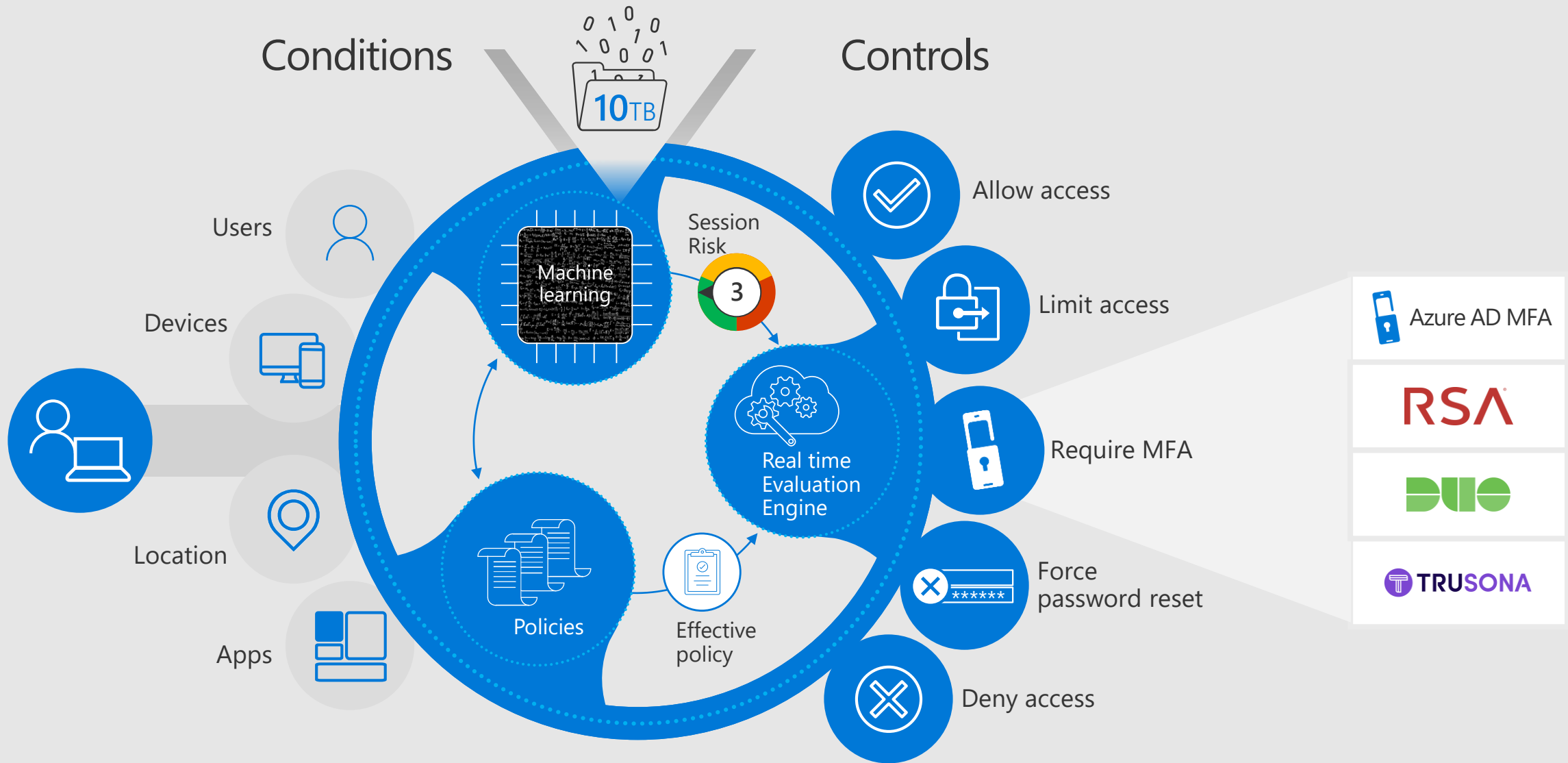
Cloud intelligence

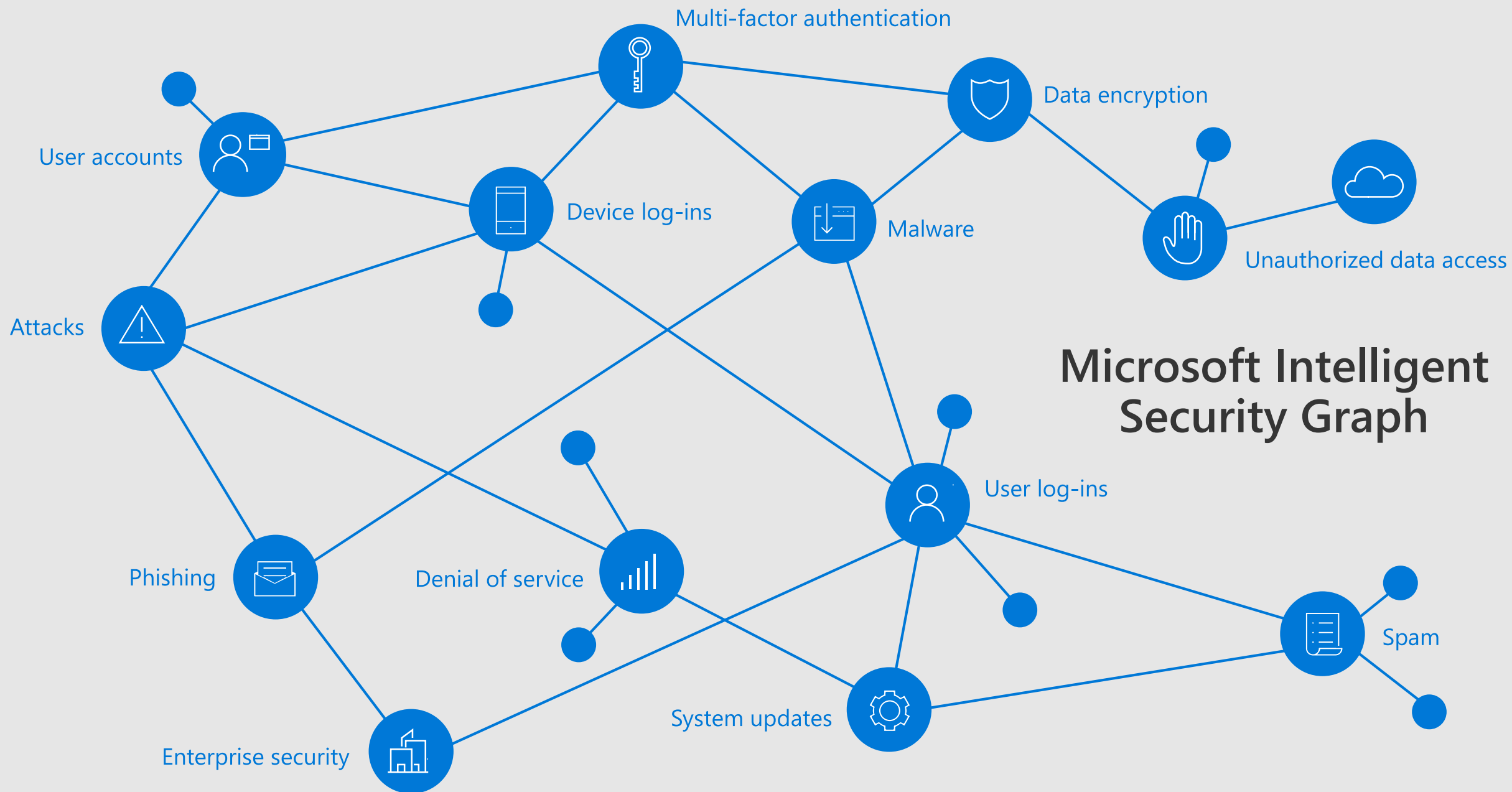
Dynamic protection

Machine learning



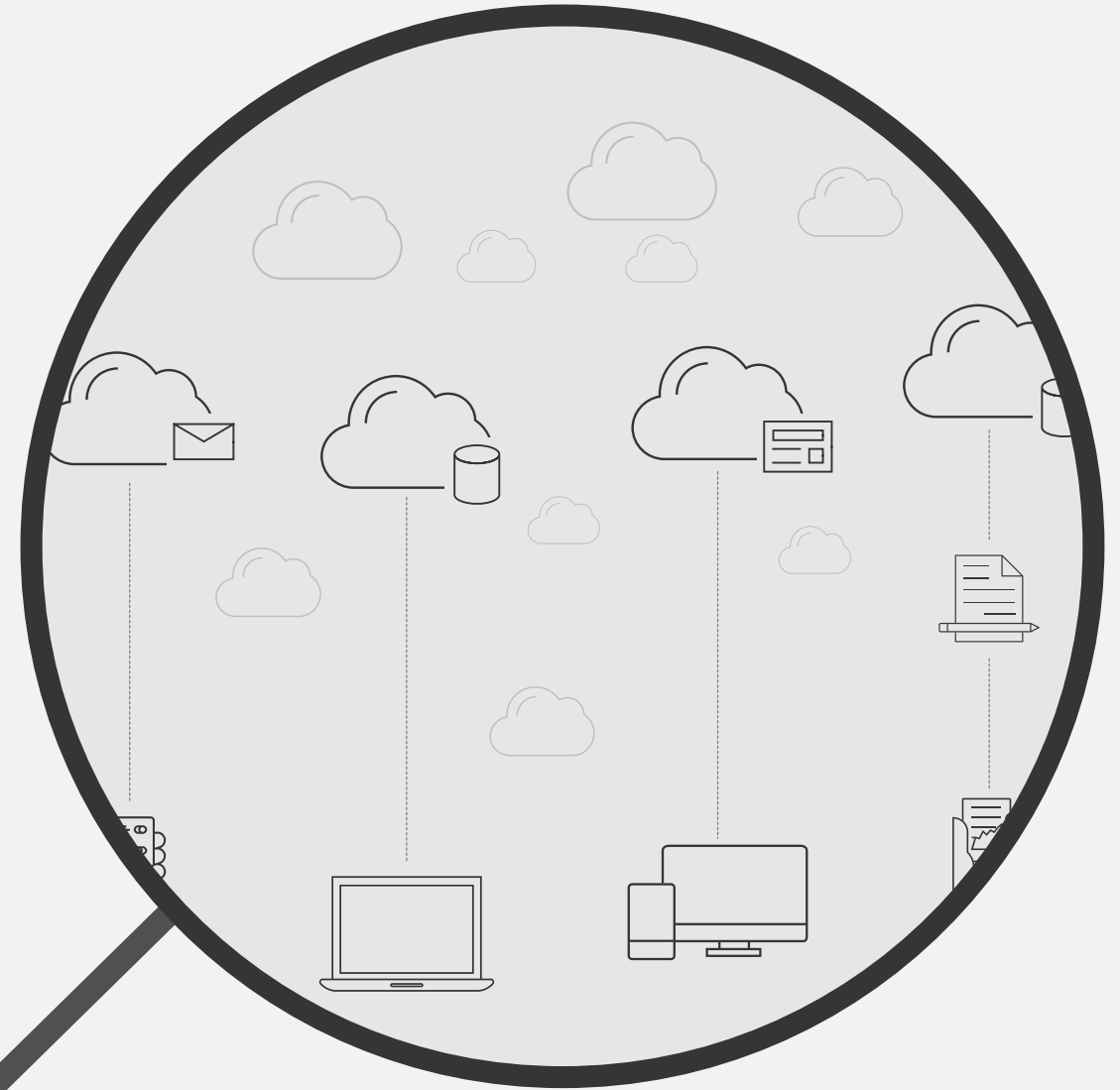






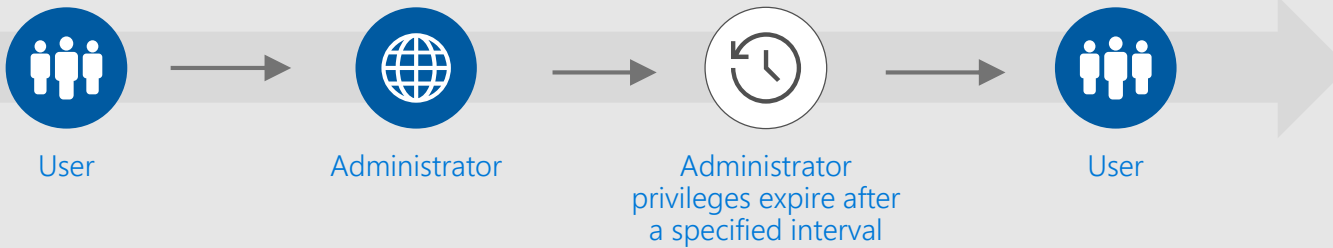
Cloud App Discovery

- ➔ Discover the cloud apps being used on your network
- ➔ View user and app based usage information
- ➔ Powered by Microsoft Cloud App Security

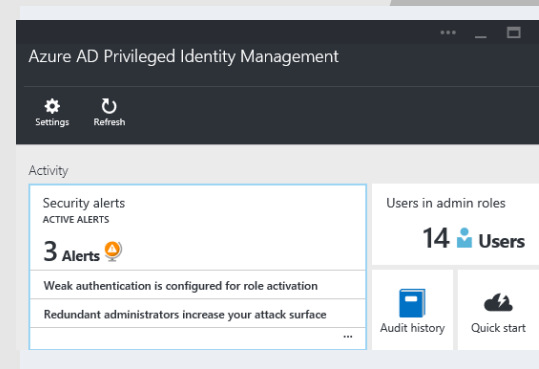


Privileged Identity Management

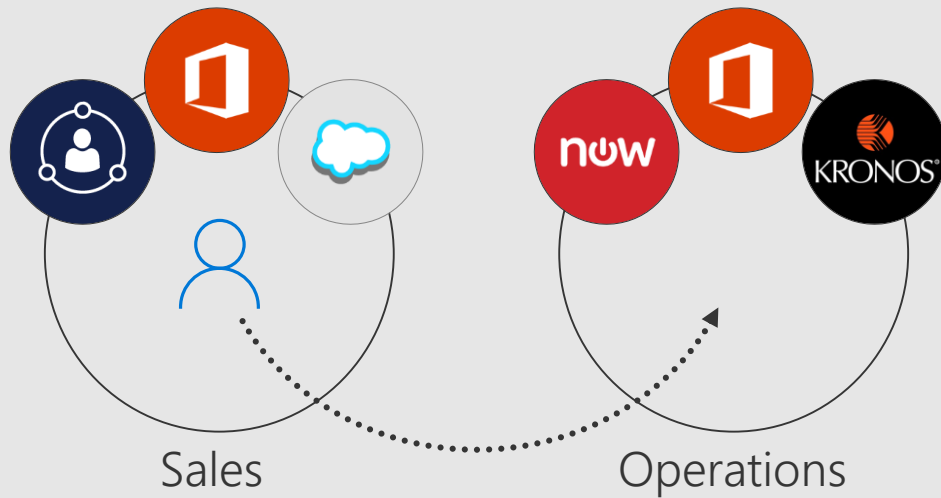
Discover, restrict, and monitor privileged identities




- ➔ Enforce on-demand, just-in-time administrative access when needed
- ➔ Ensure policies are met with alerts, audit reports and access reviews
- ➔ Manage admins access in Azure AD and also in Azure RBAC



Access Reviews



- Provide oversight for which users have access to what resources
- Prompts users to ensure their access is limited to the resources they need
- Applies to employees and guest users

 **Douglas Fife**
douglas.fife@litware.com


Access info


This user has signed in at least once in the last 30 days.


Review result

Don't know, on September 21, 2017 9:12 AM by Lee Sperry

Action to take

 Approve
(Recommended)

 Deny

 Don't know

Reason *

Still using Salesforce

Save changes

Cancel

[Reset](#)

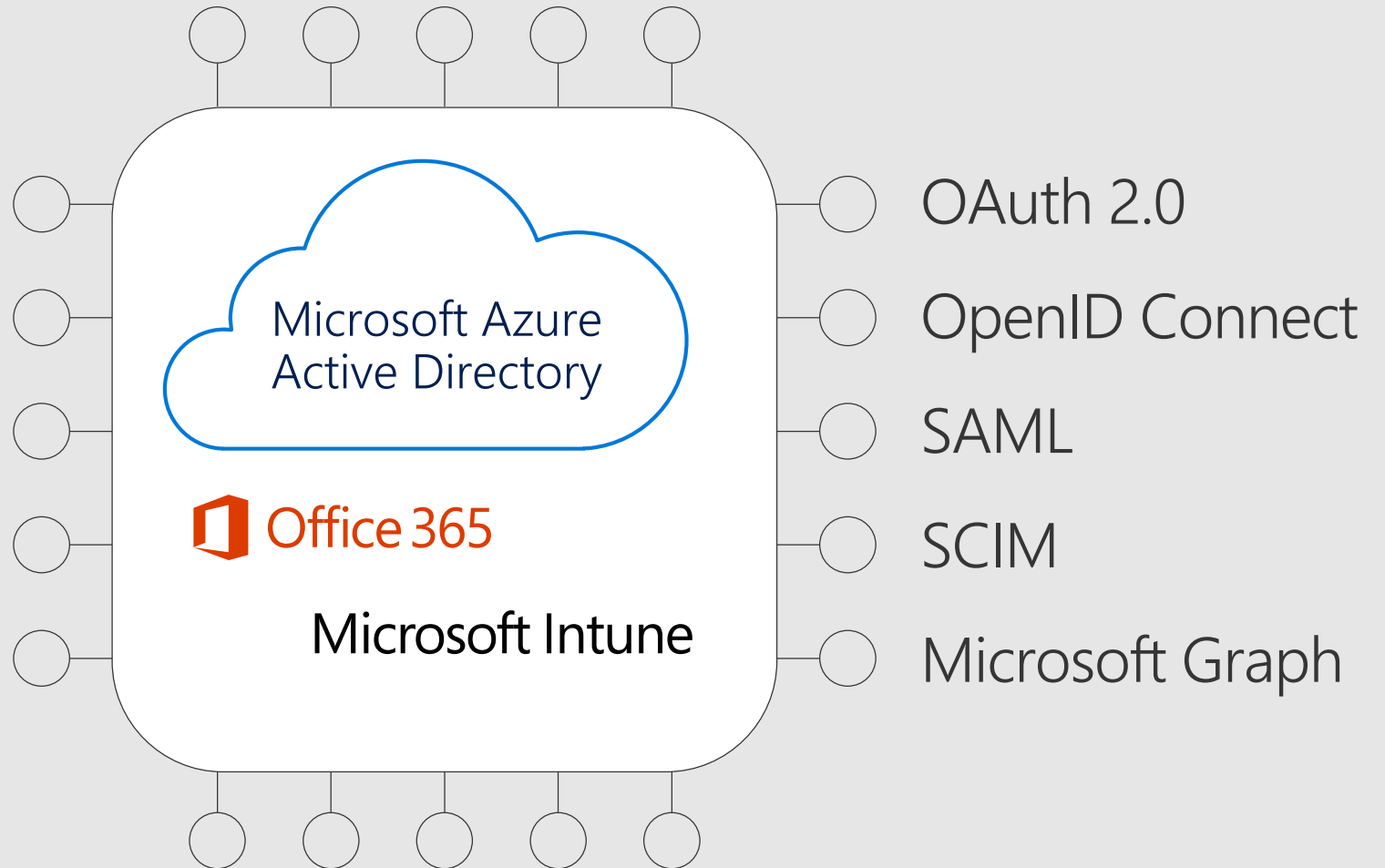


I want to build apps that work with corporate identities in Azure AD

Open Standards

Microsoft Graph

Customer Journeys



Microsoft Graph

[HTTPS://GRAPH.MICROSOFT.COM](https://graph.microsoft.com)



Azure AD



Excel



Intune



Outlook



OneDrive



OneNote



SharePoint



Planner

Single API that proxies multiple Microsoft services

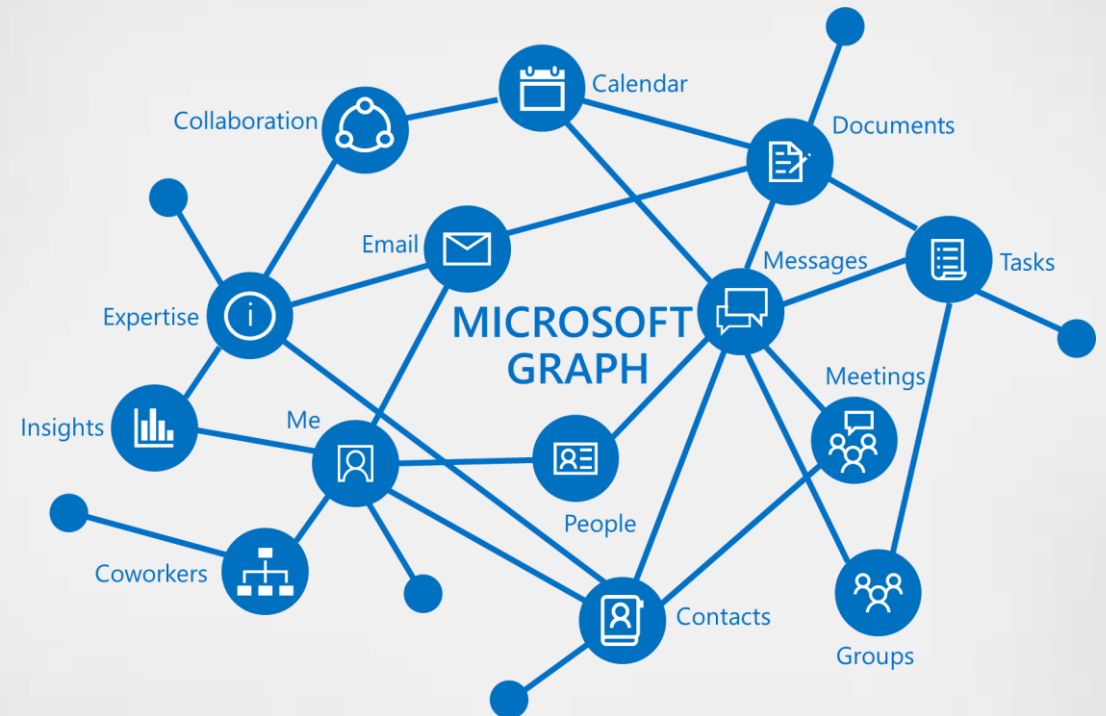
Allows for **easy traversal** of objects and relationships

Eliminates the need to discovery endpoints

Only **one** access token needed

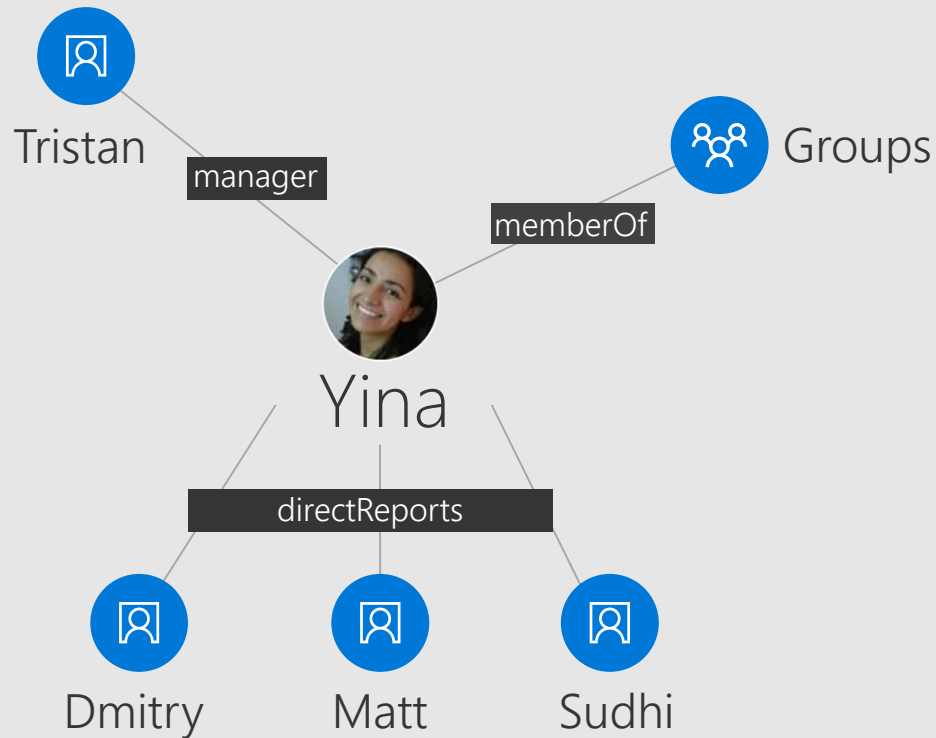
For **both** personal and work and school accounts

Exposing **User** data, **Group** data and **Organizational** data



With Microsoft Graph

Get the user **profile**



```
GET: /users/yina
{
  "displayName": "Yina",
  "jobTitle": "PRINCIPAL PM MANAGER"
}
```

```
GET: /users/yina/photo/$value
Stream image/jpeg
```

```
GET: /users/yina/manager
{"displayName": "Tristan", ...}
```

```
GET: /users/yina/directReports
"value" : [
  {"displayName": "Matt", ...},
  {"displayName": "Dmitry", ...},
]
```

```
GET: /users/yina/memberOf
"value" : [
  {"displayName": "Office engineering", ...},
  {"displayName": "Women in tech", ...}
]
```