Microsoft 365

팀즈 개발자양성 과정
1-1. M365 Architecture Overview

최은용, Solution Architect
9/27/2021

Contents

M365 Overview

Microsoft 365

A complete, intelligent, secure solution to empower employees

Unlocks creativity

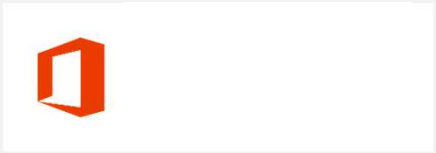
Built for teamwork

Integrated for simplicity

Intelligent security

Office 365 Enterprise | Windows 10 Enterprise | Enterprise Mobility + Security

Office 365 Enterprise capabilities



APPS Cloud Productivity & Mobility	SERVICES Rich Communication and Collaboration	SECURITY Advanced Enterprise Protection	ANALYTICS Insights for Everyone	VOICE Complete Cloud Communication
Office Pro Plus: Office apps on up to 5 PCs & Macs **Mobile Office Apps:** Office Apps for Tablet & Smartphones	**Exchange :** Business-class email & Calendar **OneDrive:** Cloud Storage and file sharing **SharePoint:** Team sites & internal portals **Skype for Business:** Online Meetings, IM, video chat **Microsoft Teams:** Chat-based Collaboration **Yammer:** Private social networking	**Advanced Threat Protection:** Zero-day threat and malware protection **Advanced Security Management:** Enhanced visibility and control **Customer Lockbox:** Enhanced customer data access controls **Advanced eDiscovery:** Identifying the relevant data quickly	**Power BI Pro:** Live business analytics and visualization **Delve Analytics:** Individual and team effectiveness	**PSTN Conferencing:** Worldwide dial-in for your online meetings **Cloud PBX:** Business phone system in the cloud **PSTN Calling:** Cost effective cloud based dial tone (add-on)

Office 365 **E3**

Office 365 **E5**

Enterprise Mobility & Security capabilities

Identity and access management	Identity Driven Security	Managed Mobile Productivity	Information Protection
Azure Active Directory Premium P1 Single sign-on to cloud and on-premises applications. Basic conditional access security System Center Configuration Manager (SCCM)	**Microsoft Advanced Threat Analytics** Identify suspicious activities & advanced attacks on premises.	**Microsoft Intune** Mobile device and app management to protect corporate apps and data on any device. Microsoft Identity Manager (MIM)	**Azure Information Protection Premium P1** Encryption for all files and storage locations. Cloud based file tracking *Existing Azure RMS capabilities*
Azure Active Directory Premium P2 Advanced risk based identity protection with alerts, analysis, & remediation.	**Microsoft Cloud App Security** Bring enterprise-grade visibility, control, and protection to your cloud applications.		**Azure Information Protection Premium P2** Intelligent classification, & encryption for files shared inside & outside your organization *Secure Islands acquisition*

EMS **E3**

EMS **E5**

Windows 10 Enterprise capabilities




The most trusted platform	More productive	More personal	The most versatile devices
Enterprise Data Protection Prevent accidental leaks by separating personal and business data	**Azure Active Directory Join** Streamline IT process by harnessing the power of the cloud	**User Experience Virtualization** (UX-V) OS and app settings synchronized across Windows instances	**Windows 10 for Industry Devices** Turn any inexpensive, off-the-shelf device, into an embedded, handheld, or kiosk experience
Windows Hello for Business Enterprise grade biometric and companion device login	**MDM enablement** Manage all of your devices with the simplicity of MDM	**Granular UX Control** Enterprise control over user experience	
Credential Guard Protects user access tokens in a hardware-isolated container	**Windows Store for Business, Private Catalog** Create a curated store experience for employee self-service		
AppLocker Block unwanted and inappropriate apps from running	**Application Virtualization** (App-V) Simplify app delivery and management		
Device Guard Device locked down to only run fully trusted apps	**Cortana Management** Create, personalize, and manage Cortana profiles through Azure Active Directory		
Advanced Threat Protection Behavior-based, attack detection Built-in threat intelligence Forensic investigation and mitigation			
Built into Windows			

Windows 10 Enterprise **E3**

Windows 10 Enterprise **E5**

Teams Voice Services

Audio Conferencing

- Use a tolled dial-in number to join meetings from any device
- Dial out to bring participants into the meeting

Phone System

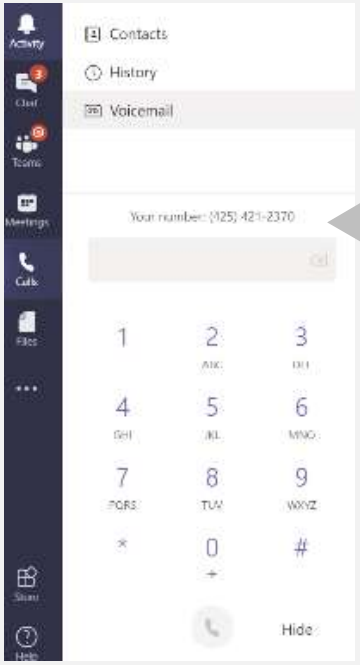
- Centrally manage users for communications, email, and content from Office 365
- Eliminate separate PBX phone systems and transition to the cloud

Calling Plan

- Subscribe to calling plans from Office 365
- Use existing phone numbers or get new ones

Audio Conferencing

x

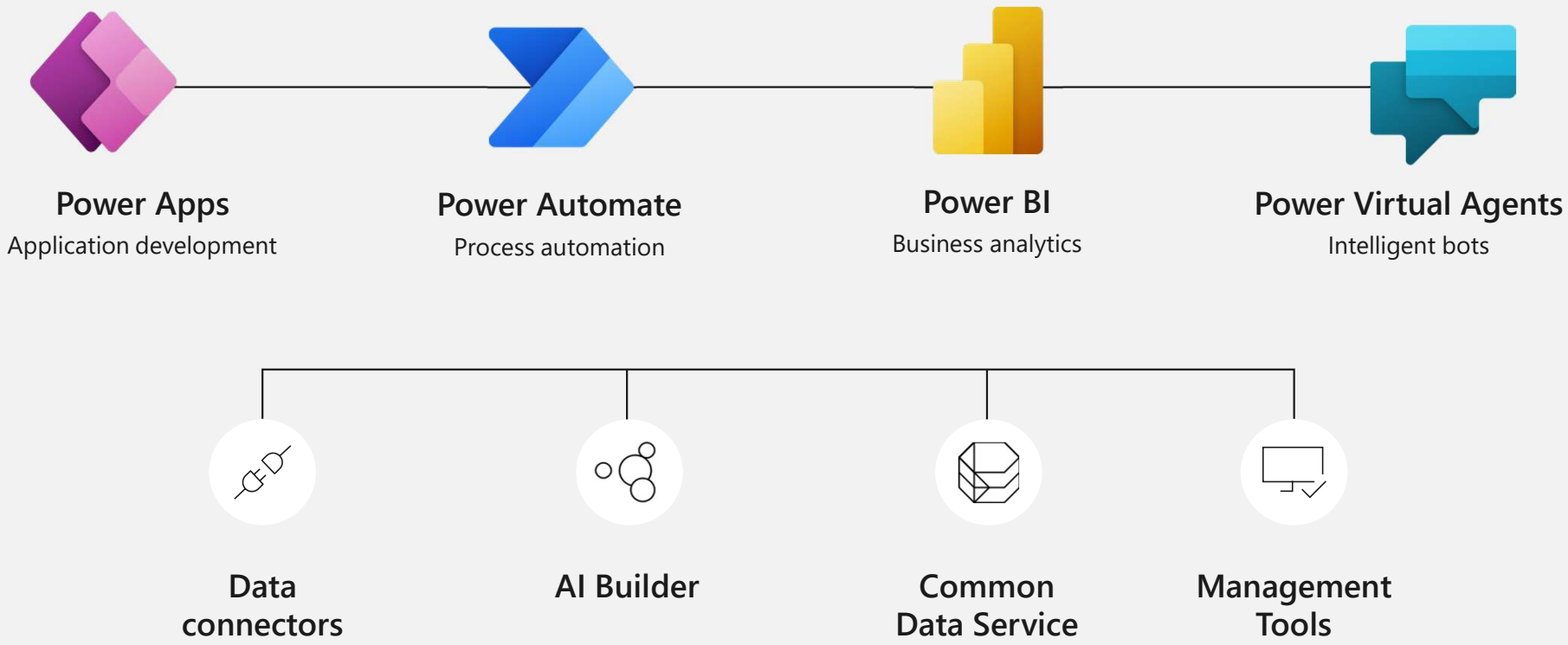


Calling Plan

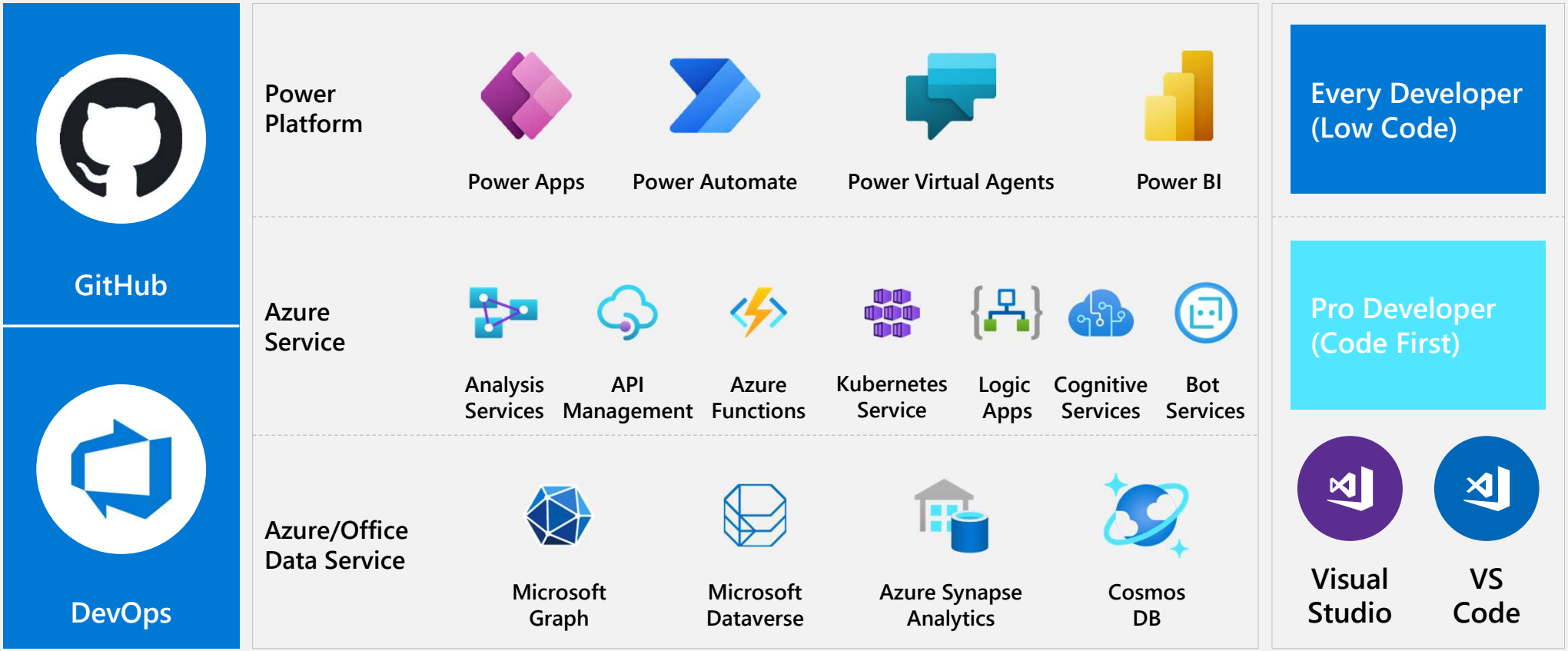
Phone System

Microsoft Power Platform

The low-code platform that spans Office 365, Azure, Dynamics 365, and standalone applications



Develop faster with a composable cloud



Power Platform for Microsoft 365, Office 365, and Windows plans

The following Microsoft 365 + Office 365 plans include limited Power Platform functionality to customize and extend Office 365 for productivity scenarios, and to delive r a comprehensive low-code extensibility platform for Microsoft Teams.

Qualifying License	Limited Use Rights Included with Qualifying License				
	Power Apps	Power Automate		Power Virtual Agents for Teams	Dataverse for Teams
		Cloud flows	Desktop flows		
Office 365 E1	•	•		•	•
Office 365 E3	•	•		•	•
Office 365 E5	•	•		•	•
Office 365 F3	•	•		•	•
Microsoft 365 Business Basic	•	•		•	•
Microsoft 365 Business Standard	•	•		•	•
Microsoft 365 Business Premium	•	•	•	•	•
Microsoft 365 F1					
Microsoft 365 F3	•	•	•	•	•
Microsoft 365 E3	•	•	•	•	•
Microsoft 365 E5	•	•	•	•	•
Windows Enterprise E3			•		
Windows Enterprise E5			•		
Office 365 A1	•	•			
Office 365 A3[1]	•	•		•	•
Office 365 A5[1]	•	•		•	•
Microsoft 365 A1[2]	•	•			
Microsoft 365 A3[1]	•	•	•	•	•
Microsoft 365 A5[1]	•	•	•	•	•
Windows Education A3[1]			•		
Windows Education A5[1]			•		

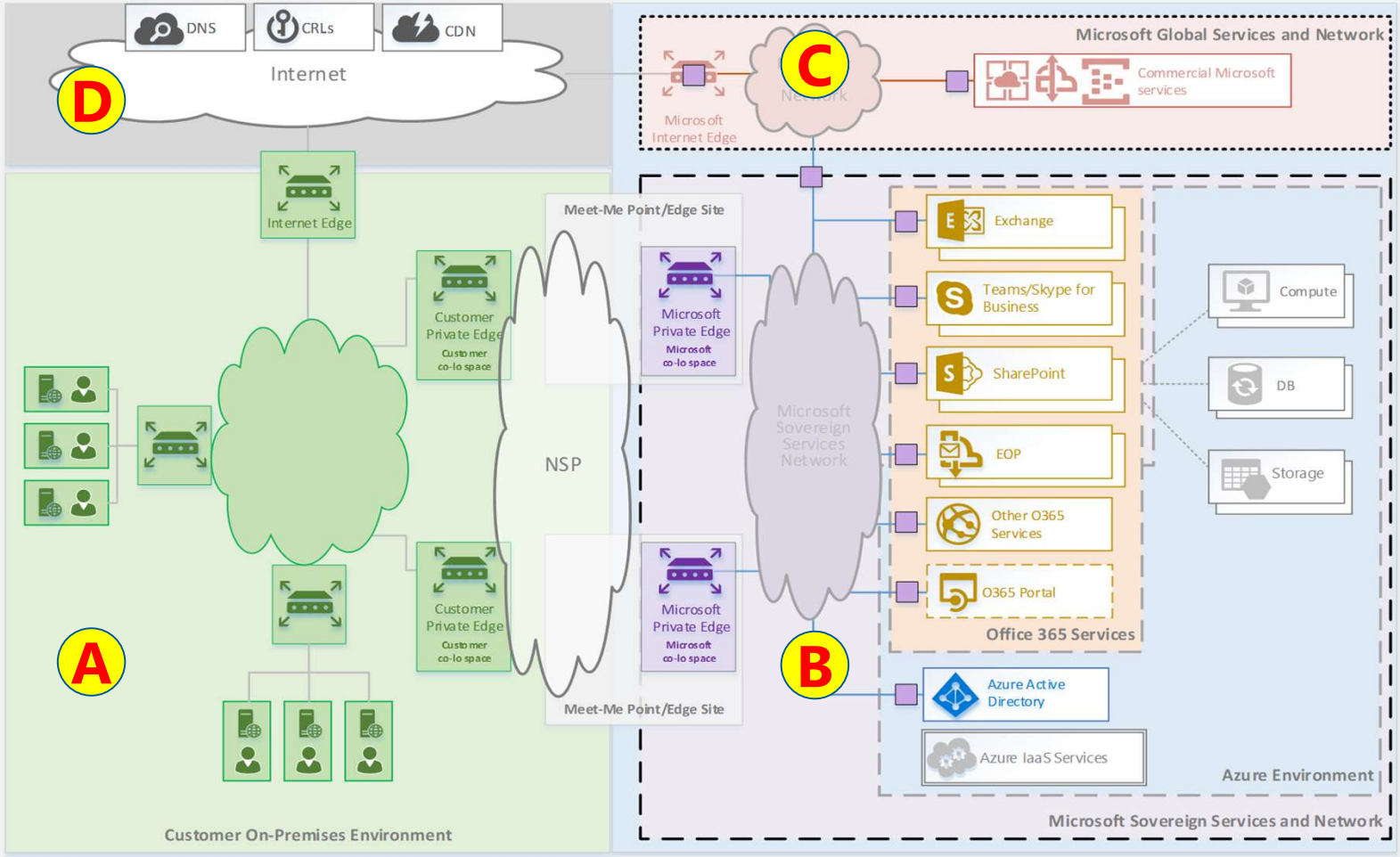
[1]Also included in Student Use Benefit
[2]Included via accompanying Office 365 A1

Microsoft 365 is governed by the License Terms of the individual products and services comprising Microsoft 365, as modified by the License Terms in the Microsoft 365 Product Entry. For more information on Microsoft 365 and Office 365 Suites licensing channels and segment availability, refer to the Product Terms and the Online Service Terms.

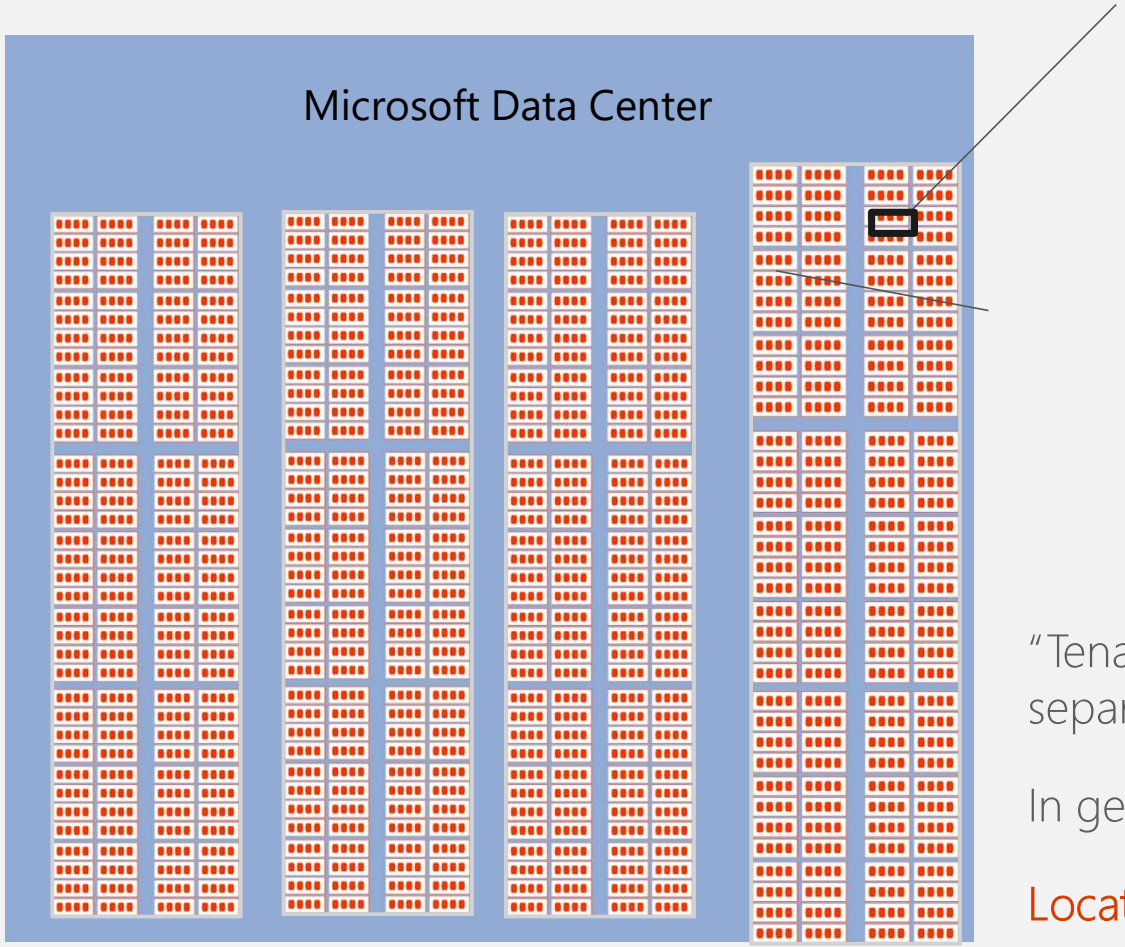
M365 Architecture

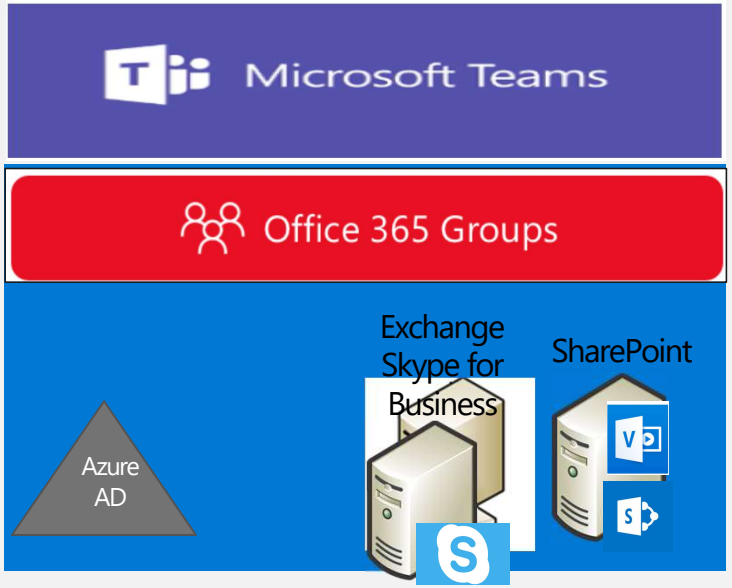
Office 365 SaaS Systems View

- 4 district areas of system significance
  - A – Customer (on-premises)
  - B – Office 365
  - C – Azure
  - D- Internet



What is “tenant” in Office 365?



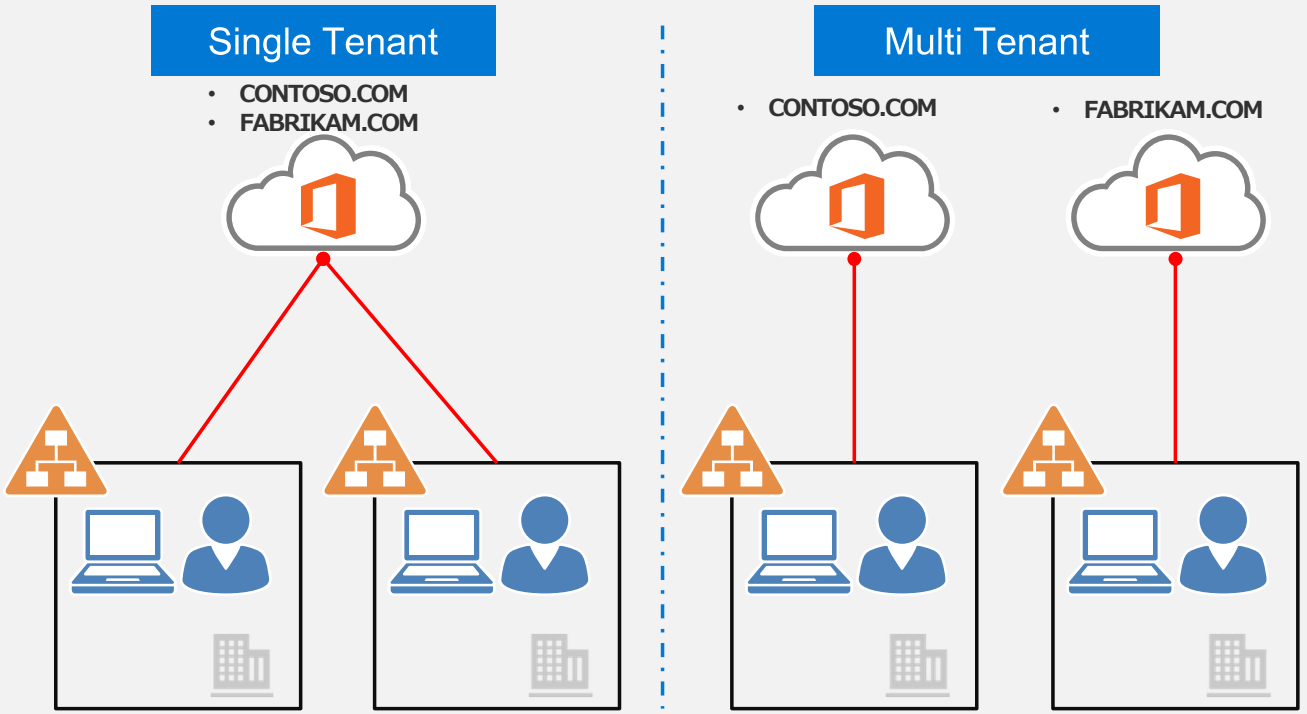


“Tenant” is a virtual instance of services which is logically separated for each customer.

In general, one tenant is provided per contract.

Location of tenant is tied to the country where contract was signed.

Tenant and Domain



Tenant and Domains

✓ If a domain registered with a tenant, same domain cannot be used in different tenant.

✓ Exchange : Use as SMTP Domain

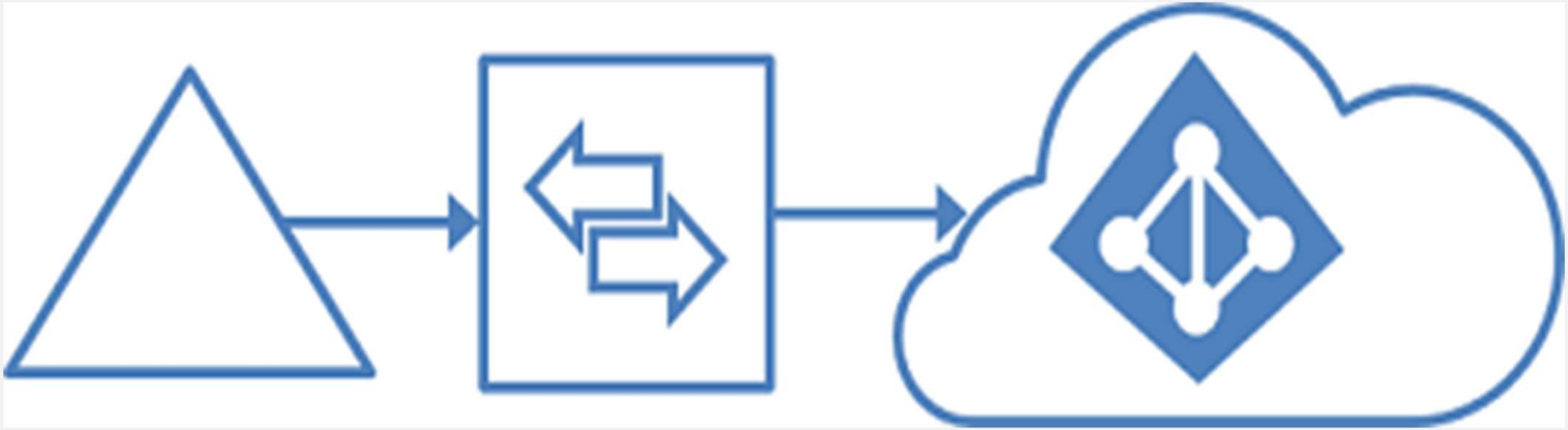
✓ example :

If “contoso.com” is registered in Tenant A, “contoso.com” cannot be used in Tenant B

(However, sub-domain, such as “SUB.CONTOSO.COM” can be registered)

Single forest and Single Azure AD Tenant

The below illustration shows a single on-premises forest, with one or multiple domains, and a single Azure AD tenant.

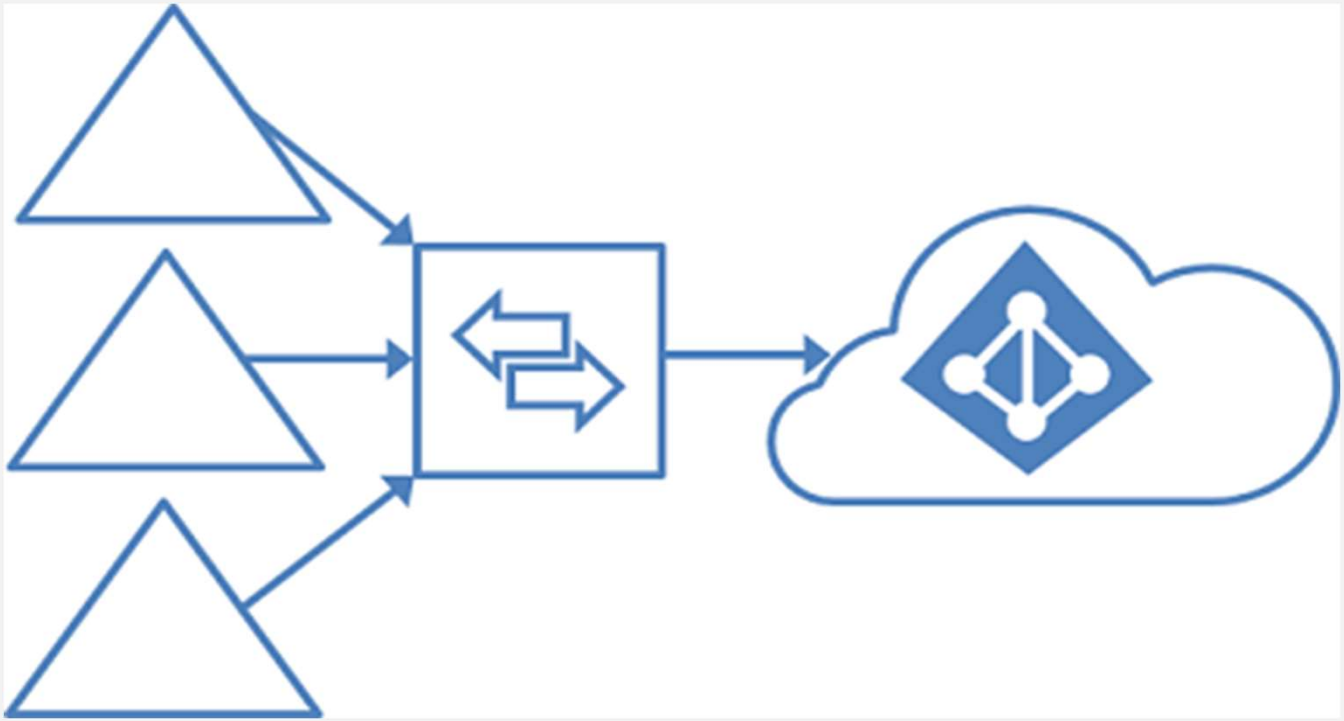


Multiple forests and Single Azure AD Tenant

The illustration below shows multiple forests.

In case of multiple forests, all forests must be reachable by a single Azure AD Connect sync server.

- Domain joined
- Server in a perimeter network (DMZ)

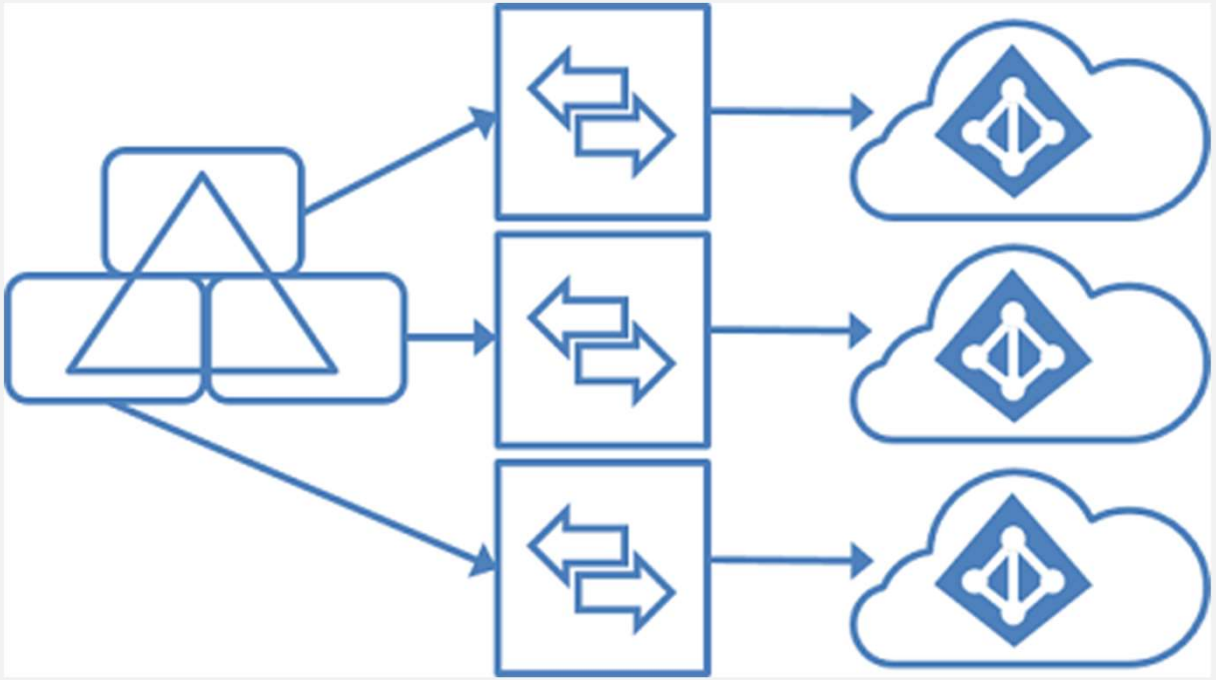


Single forests and Multiple Azure AD Tenant

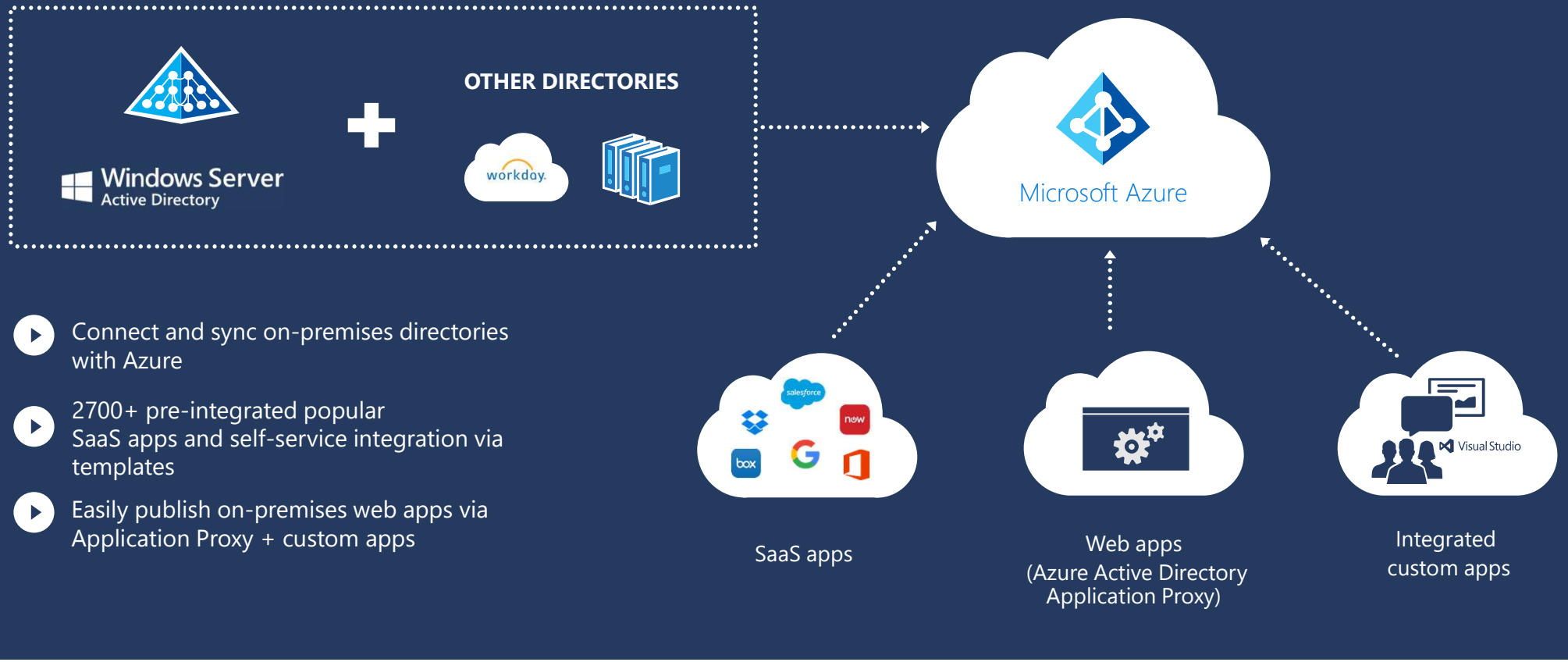
The illustration below shows multiple tenants.

The Azure AD Connect sync servers must be configured for filtering so that each has a mutually exclusive set of objects to operate on

- A DNS domain can be registered in only a single Azure AD tenant.
- The UPNs of the users in the on-premises Active Directory instance must also use separate namespaces

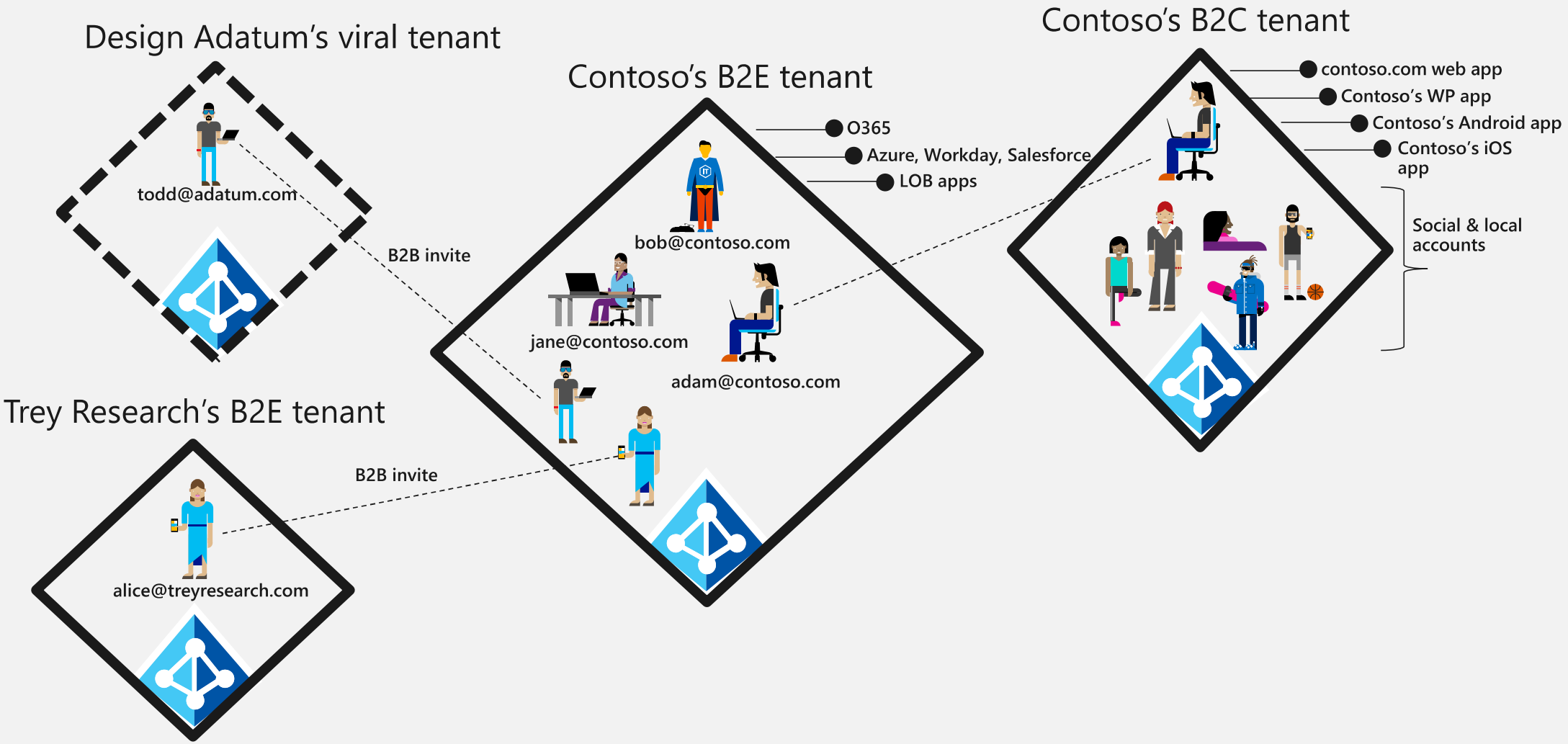


Single sign-on to any app

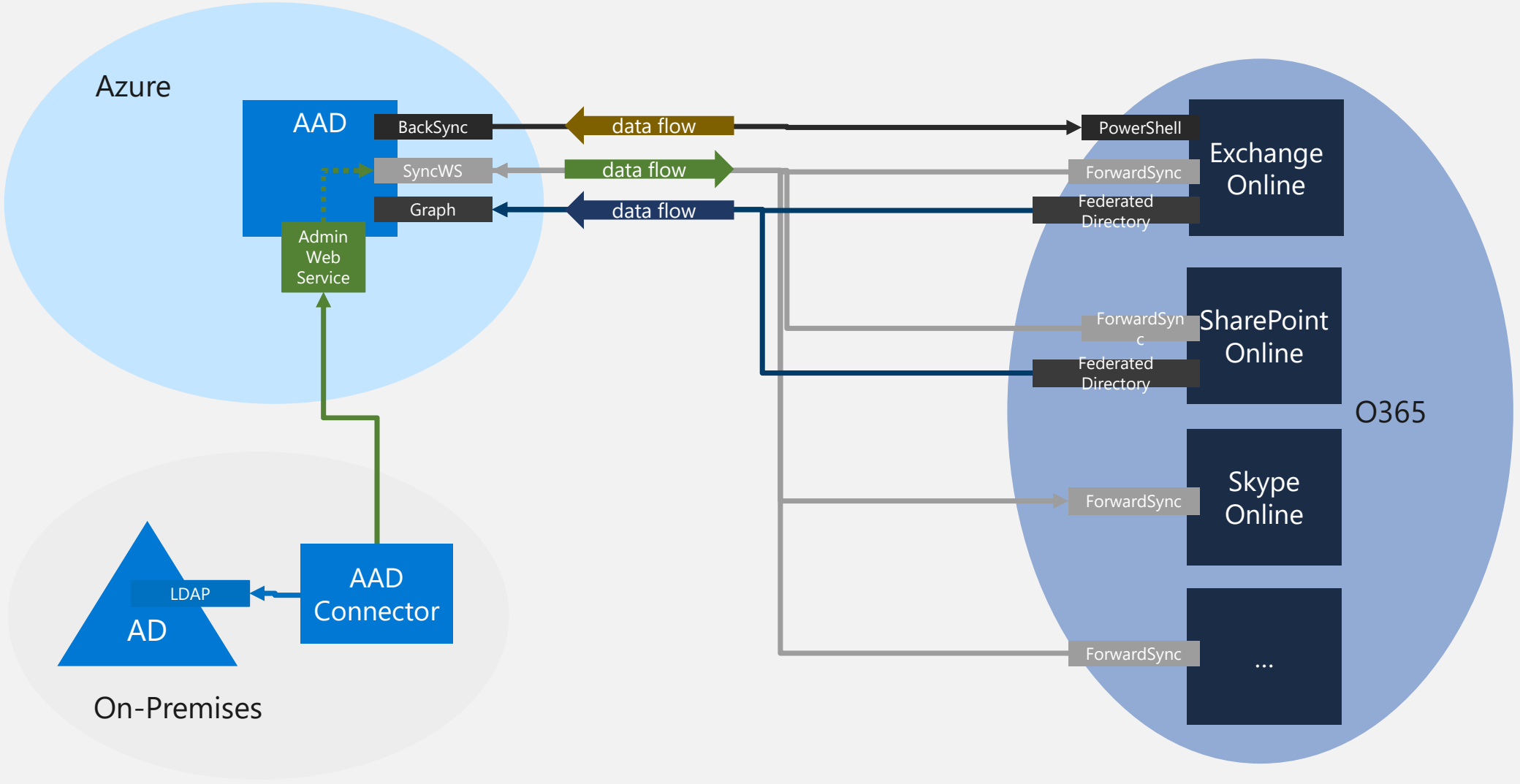


- Connect and sync on-premises directories with Azure
- 2700+ pre-integrated popular SaaS apps and self-service integration via templates
- Easily publish on-premises web apps via Application Proxy + custom apps

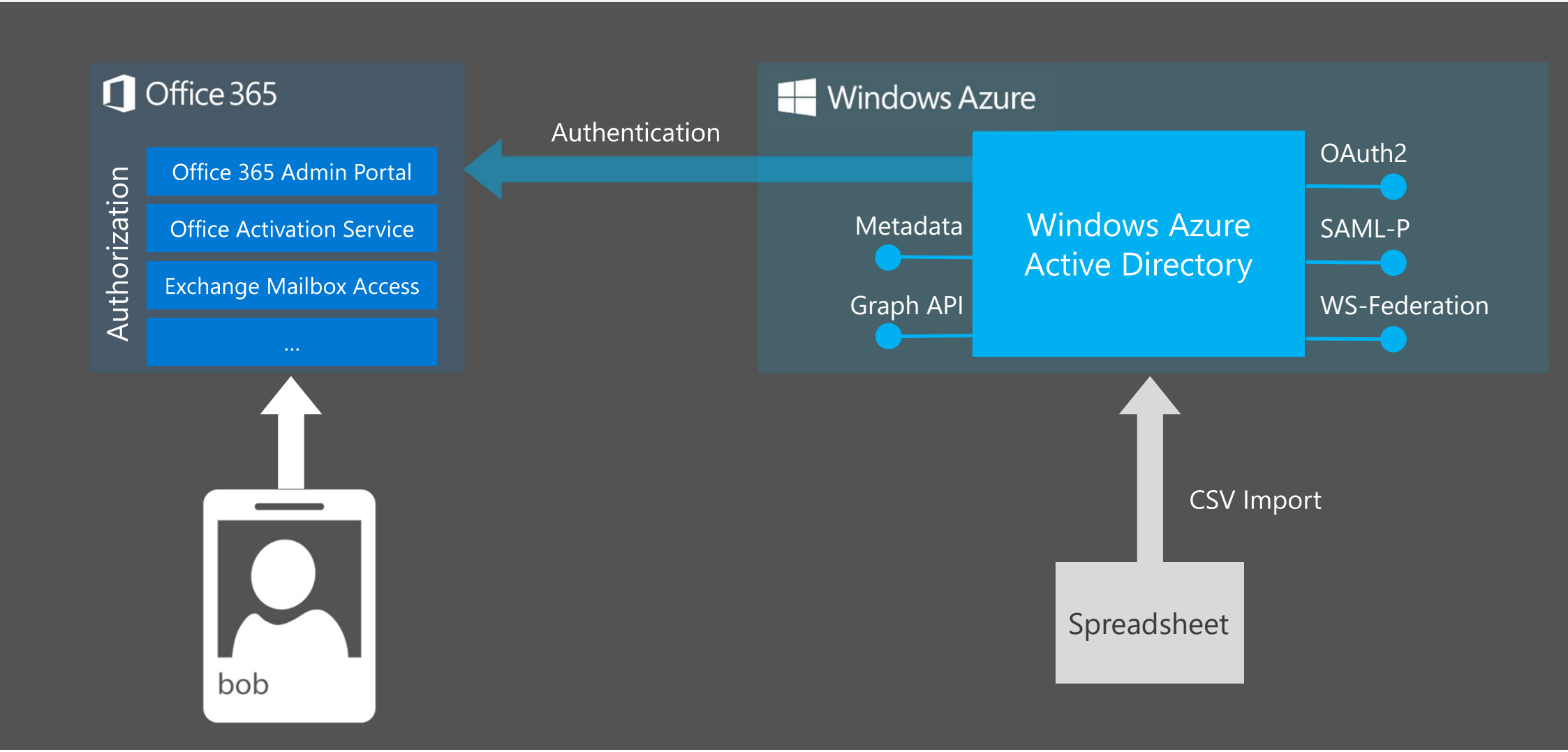
B2E vs. B2B vs. C2C



Directory Services

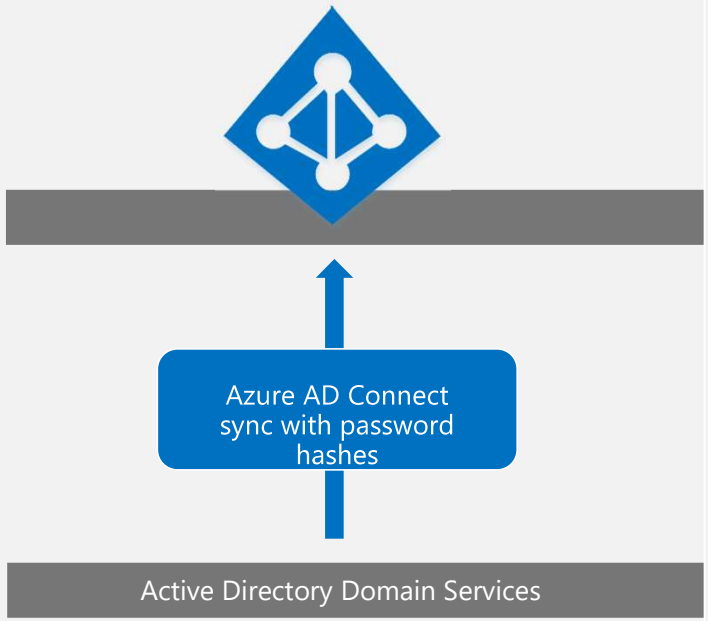


Cloud Identity



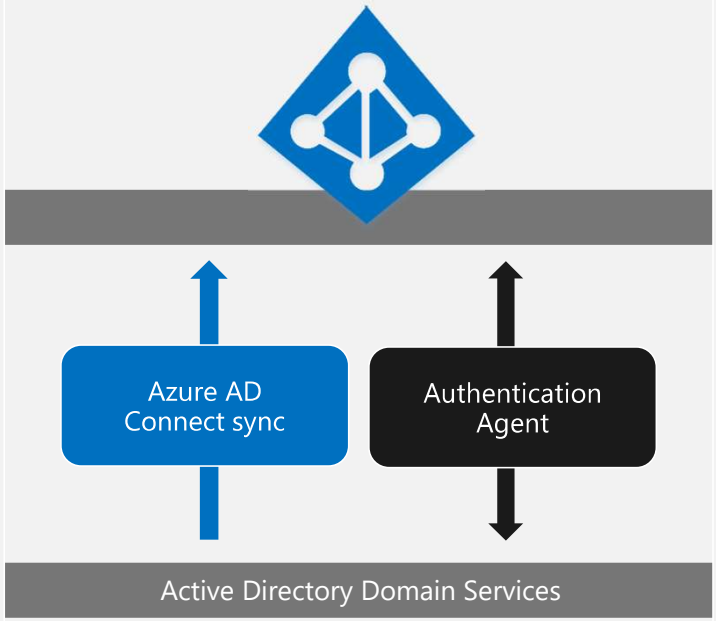
Authentication

Password Hash Synchronization



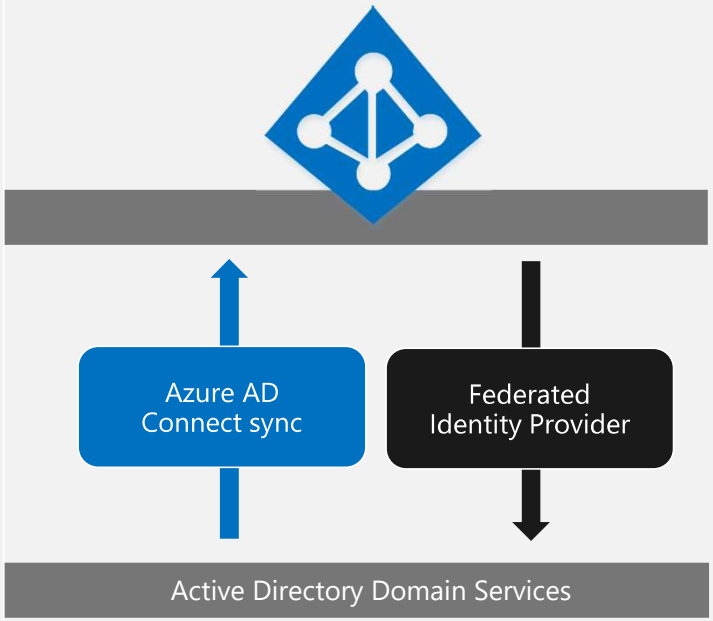
Authentication performed by Azure AD using synchronized password hashes

Pass-Through Authentication



Authentication performed by AD DS via authentication agent that looks for requests via outbound communication

Federated Authentication

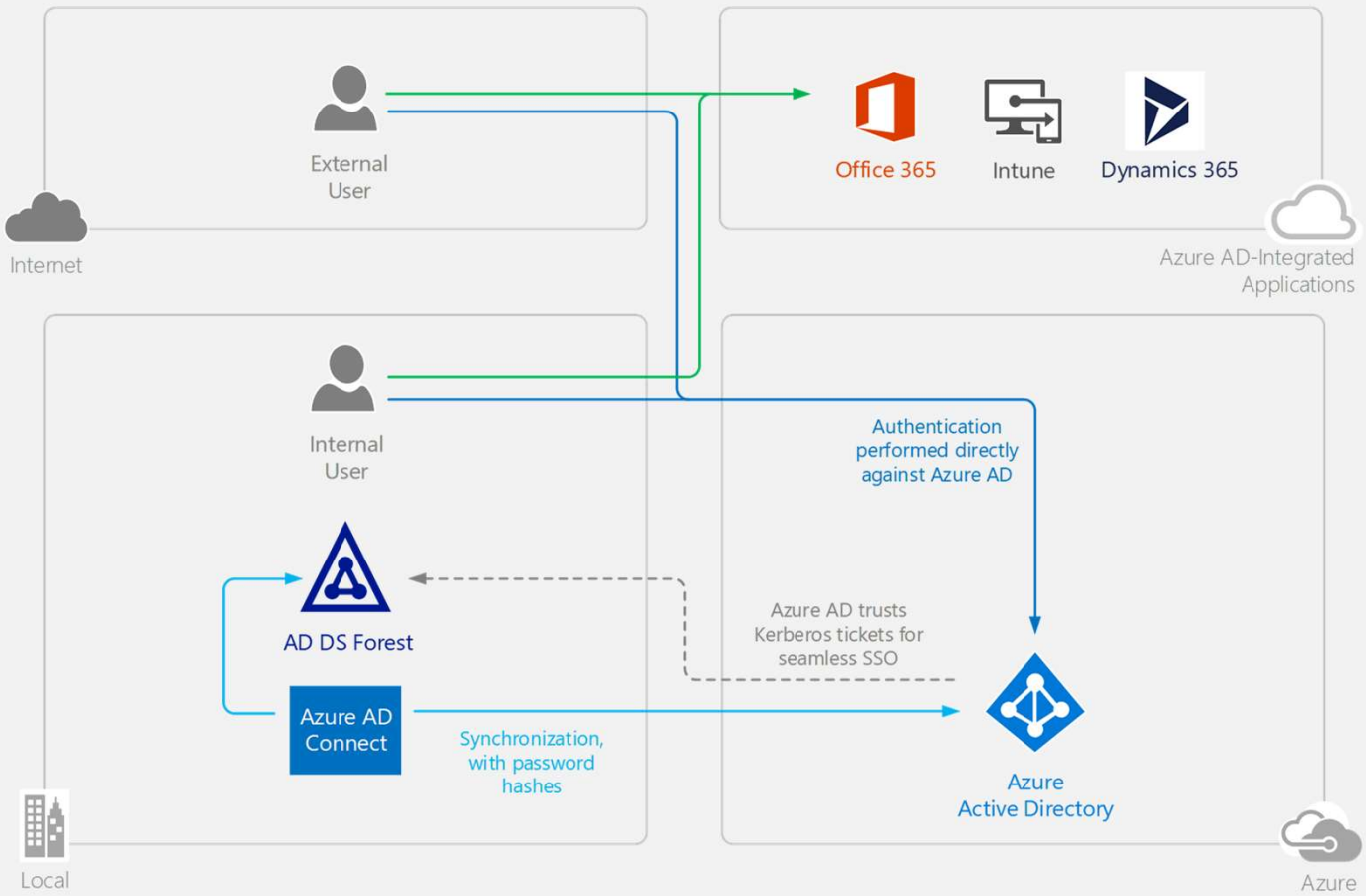


Authentication performed by AD DS via federated identity provider

Password Hash Synchronization

1. User requests access to application and is referred to Azure AD
2. Azure AD prompts for credentials and verifies password against synchronized password hash from on-prem AD DS

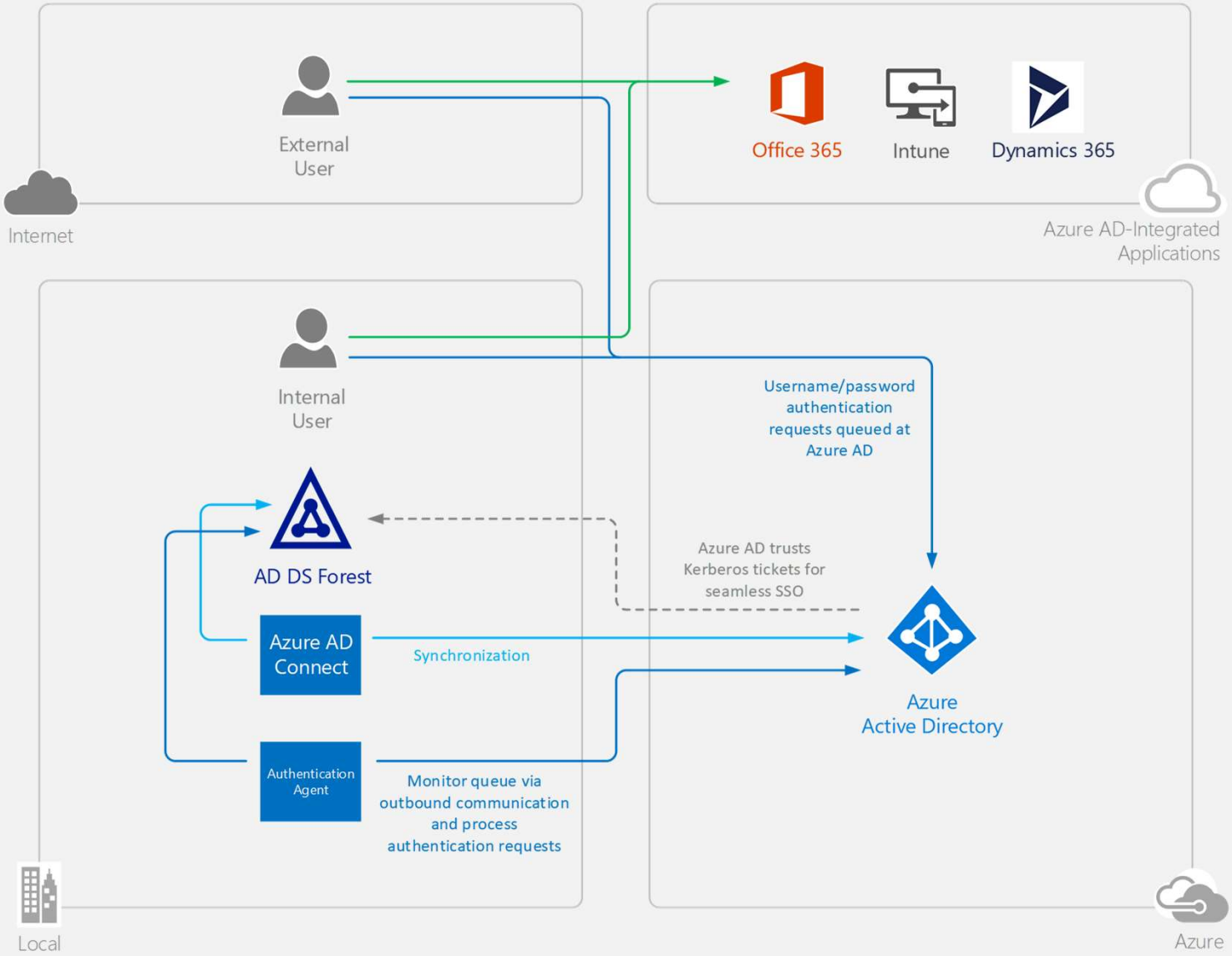
   Azure AD **Seamless SSO** available for domain-joined PCs



Pass-Through Authentication

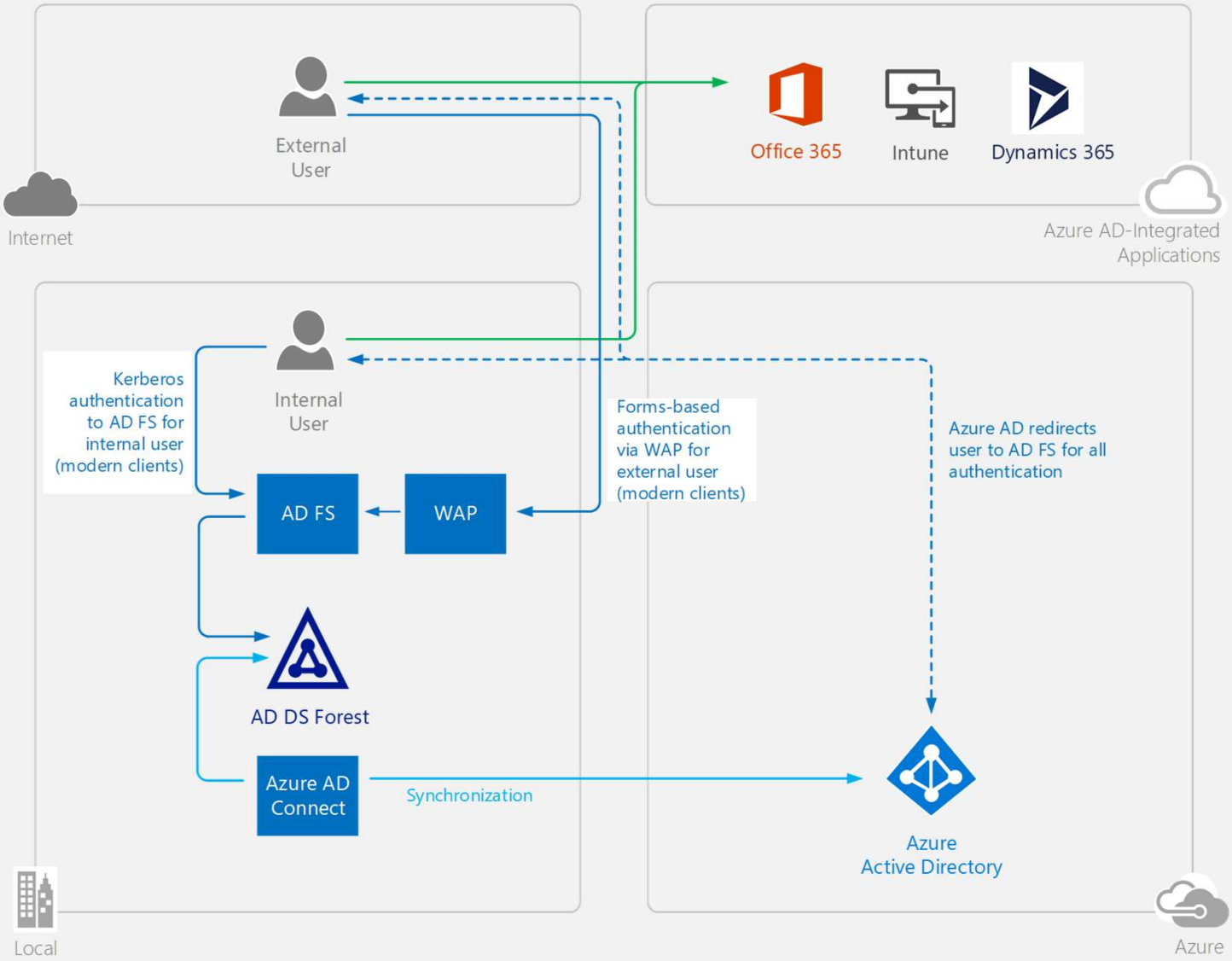
1. User requests access to application and is referred to Azure AD
2. Azure AD prompts for credentials and places UPN and encrypted password on a queue
3. Authentication agent monitors the queue via outbound communication and authenticates user against AD DS

   Azure AD **Seamless SSO** available for domain-joined PCs



Federated Authentication

1. User requests access to application and is referred to Azure AD
2. User identified to Azure AD and redirected to the federated identity provider (IdP)
3. IdP authenticates the user, via seamless SSO when possible
4. User is issued a token and returned to Azure AD
5. Azure AD verifies the token and returns the user to the application with a resource token



What is Hybrid?

Split User

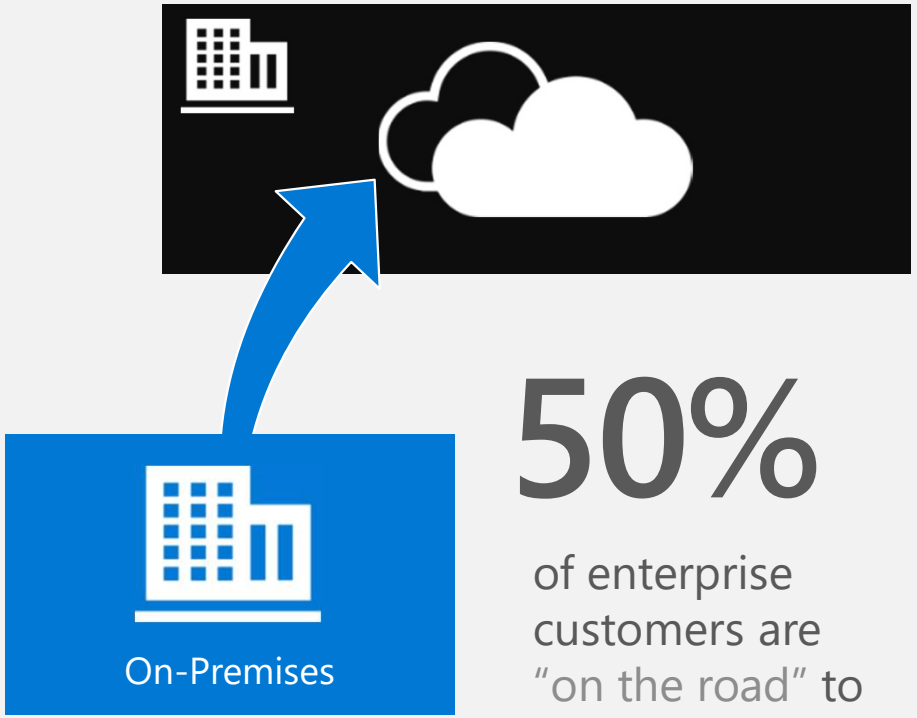
An organization splitting users within a workload (Exchange or SharePoint) between On-Premises and Online

Split Workload

Users on any of the workloads (Exchange, SharePoint or Lync) in the cloud while using other workloads On-Premises

Why Hybrid?

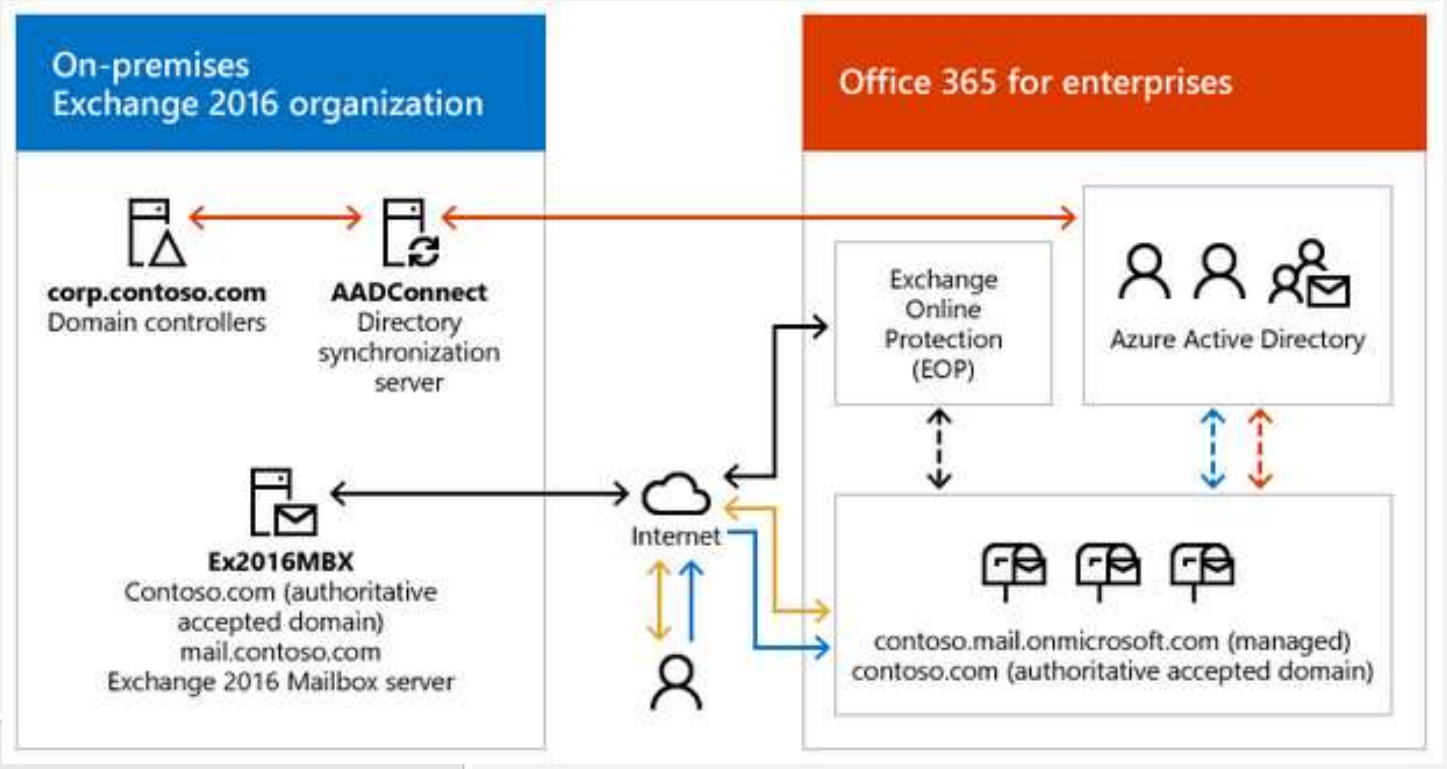
- Flexibility
- On-Premises customization
- Significant footprint in Remote locations
- Regulatory reasons
- Manageability



50%

of enterprise customers are "on the road" to cloud

Example Hybrid Topology

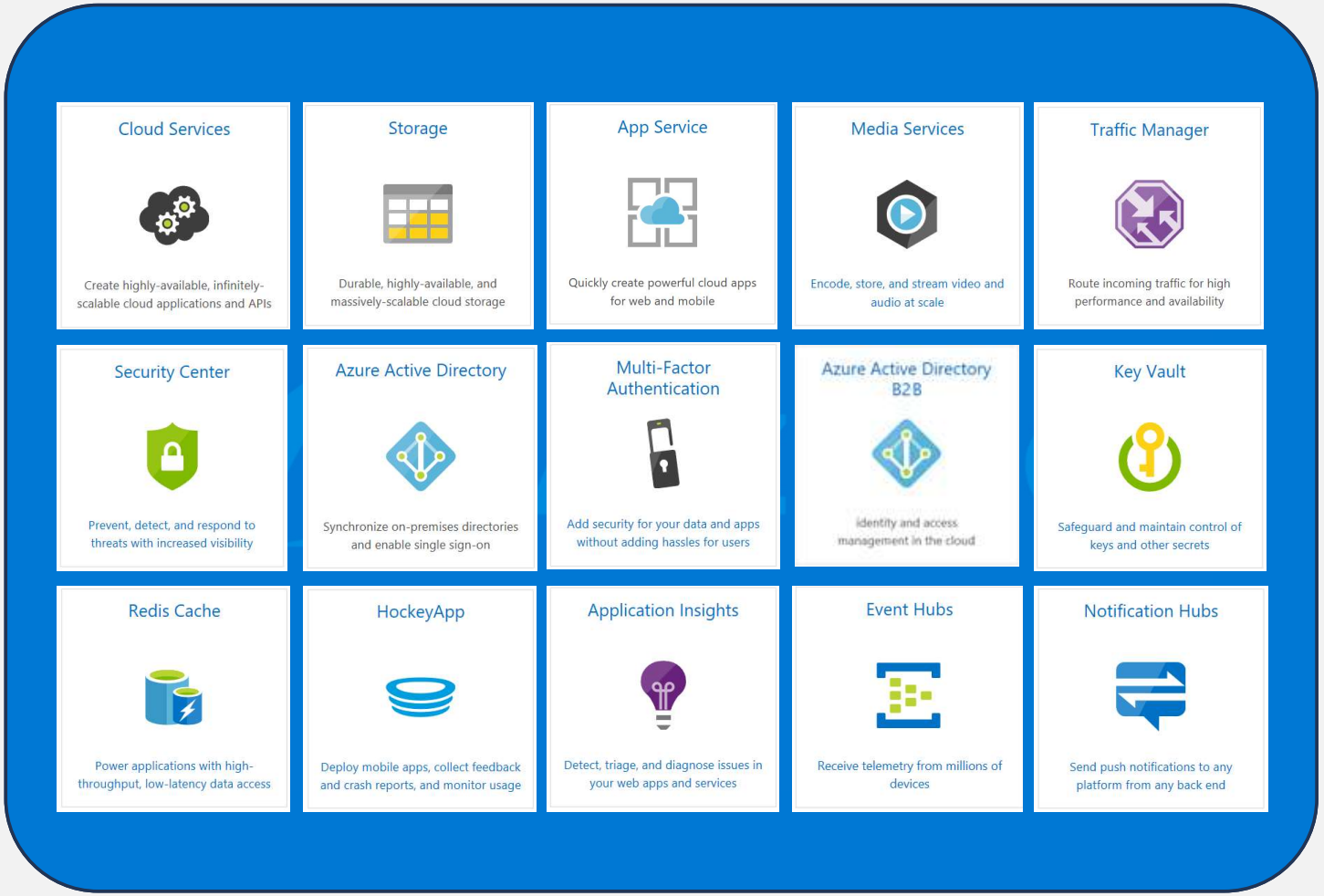


Legend

- Credentials sent from user to Exchange Online
- Credential verification between Exchange Online and Azure Active Directory
- Outlook on the web traffic
- Recipient and password synchronization between on-premises Active Directory and Azure Active Directory
- Recipient synchronization between Exchange Online and Azure Active Directory
- Mail flow to and from on-premises and the Internet, and secure mail flow between on-premises and EOP
- Secure mail transport between EOP and Exchange Online

Teams Architecture

Built on Azure



Azure is the core platform that Teams is built on

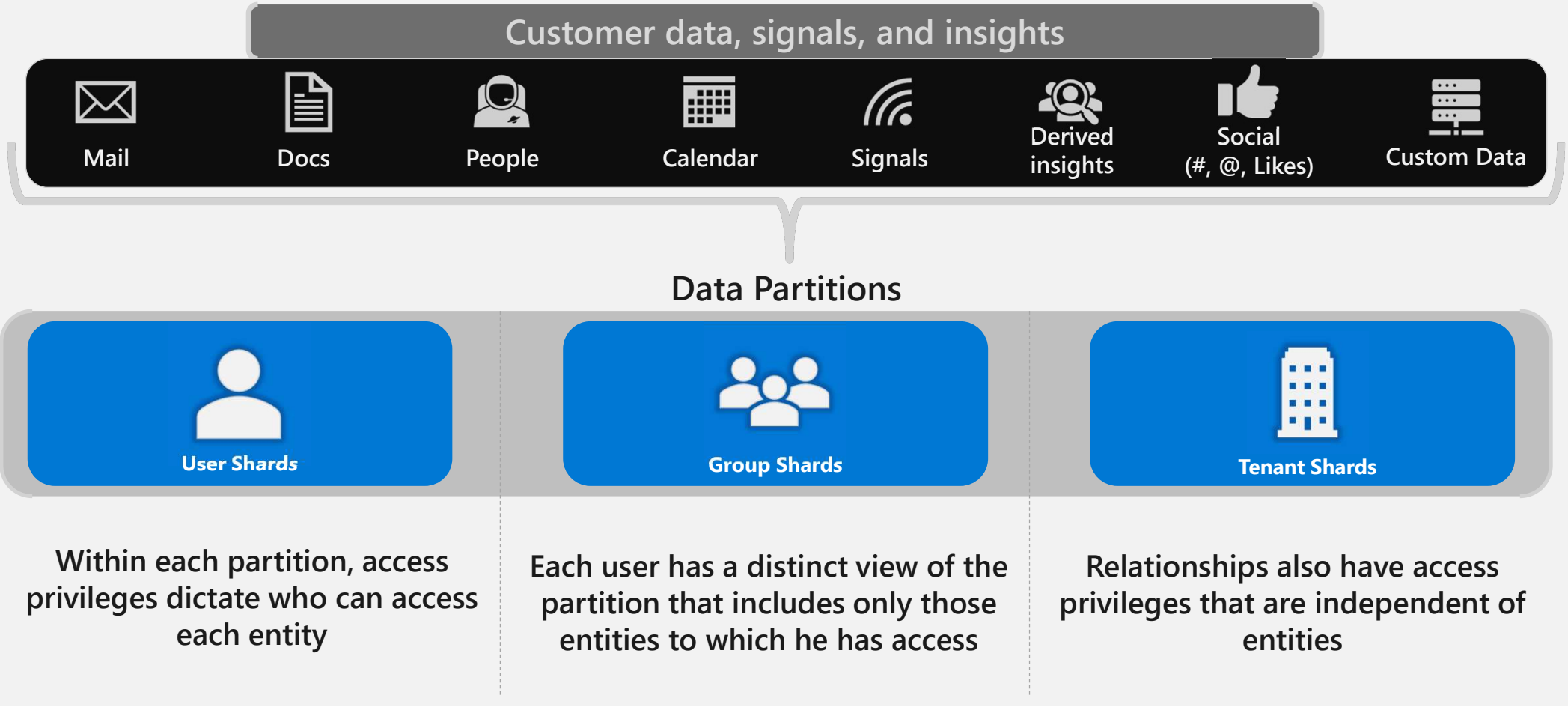
Massive scale

Global footprint

Redundancy

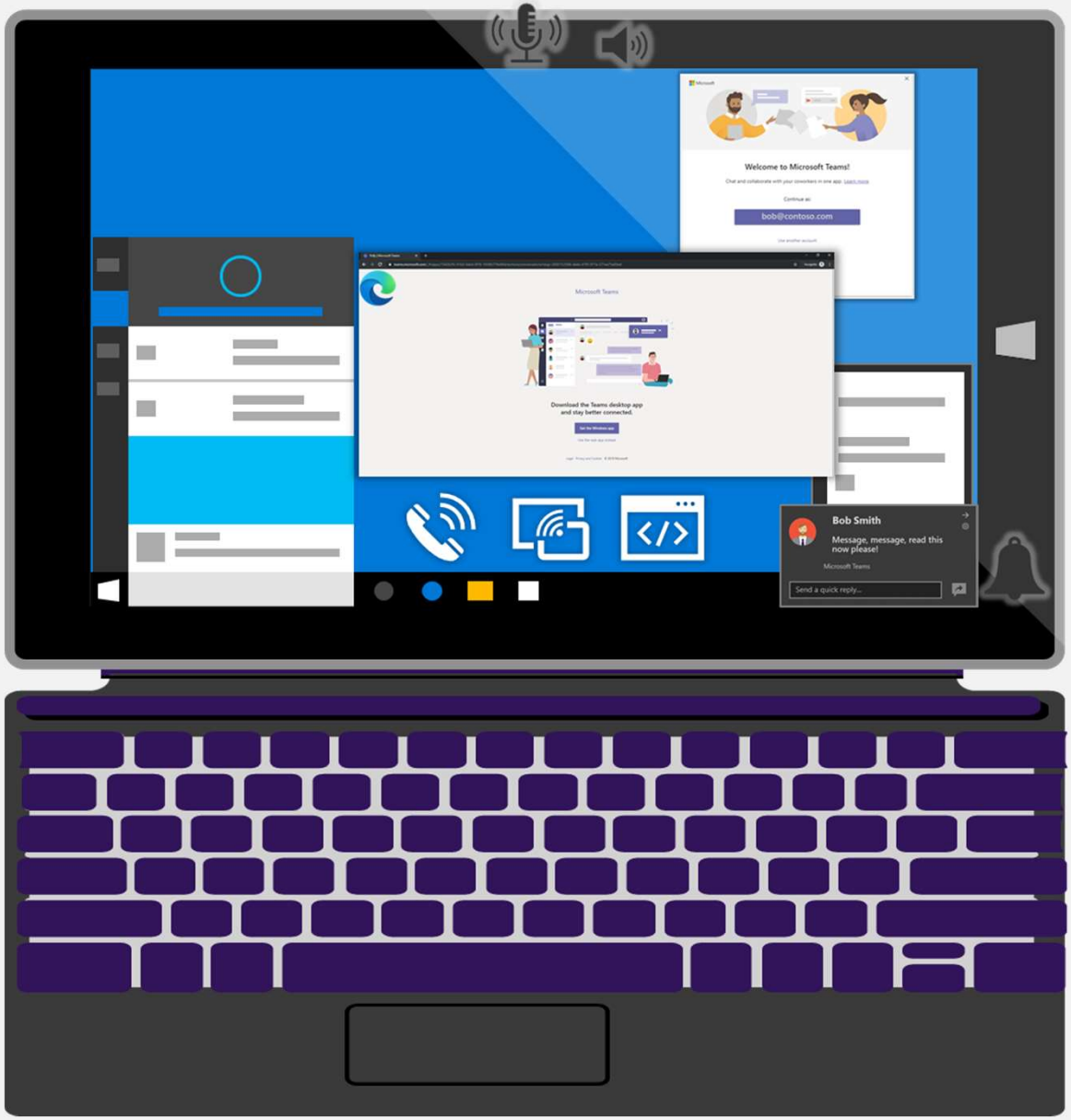
Teams and Office 365 Substrate

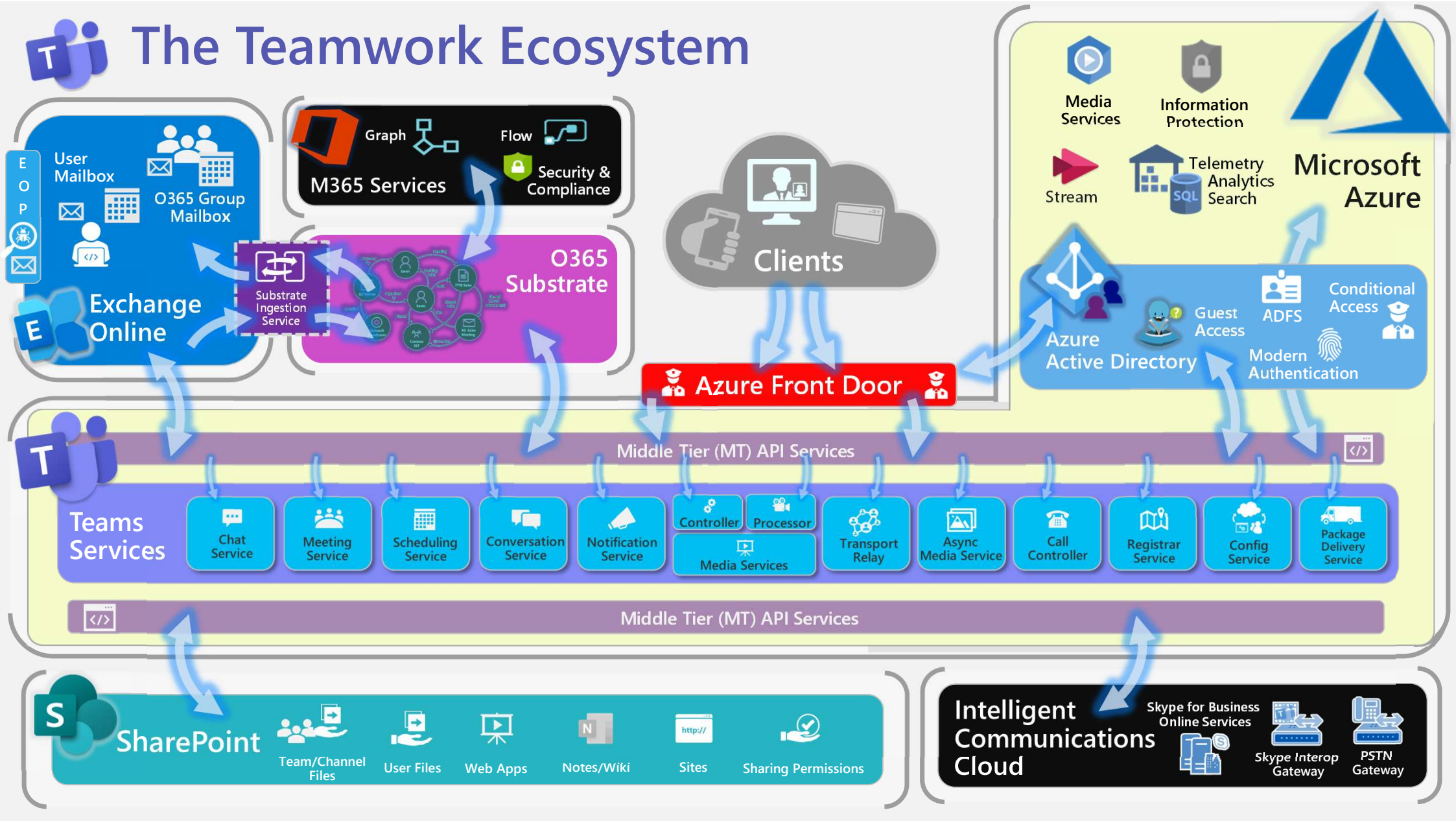
- All O365 data assets in one place



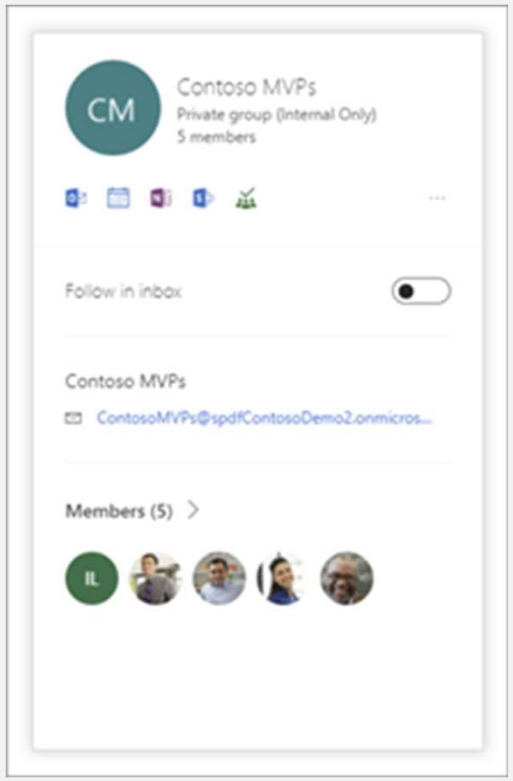
Teams client

- Electron Framework
- Open Source
- Built on Chromium
- Enables full OS functionality for web apps
  - OS level Notifications
  - Custom media components
  - System Resource Access
    - Tray
    - System Info
    - Protocol Handlers




The Teamwork Ecosystem
EOP
User Mailbox
O365 Group Mailbox
Exchange Online
Substrate Ingestion Service
Graph
Flow
M365 Services
Security & Compliance
O365 Substrate
Clients
Media Services
Information Protection
Microsoft Azure
Stream
Telemetry
Analytics
Search
Azure Active Directory
Guest Access
ADFS
Conditional Access
Modern Authentication
Azure Front Door
Middle Tier (MT) API Services
Teams Services
Chat Service
Meeting Service
Scheduling Service
Conversation Service
Notification Service
Controller
Processor
Media Services
Transport Relay
Async Media Service
Call Controller
Registrar Service
Config Service
Package Delivery Service
Middle Tier (MT) API Services
SharePoint
Team/Channel Files
User Files
Web Apps
Notes/Wiki
Sites
Sharing Permissions
Intelligent Communications Cloud
Skype for Business Online Services
Skype Interop Gateway
PSTN Gateway

What are Office 365 Groups?



A unified identity contained in AAD

Provides seamless access to other O365 Services:

Exchange Online (group mailbox and calendar):

- Only the Inbox (threaded conversations)
- Calendar folders are used

SharePoint Online

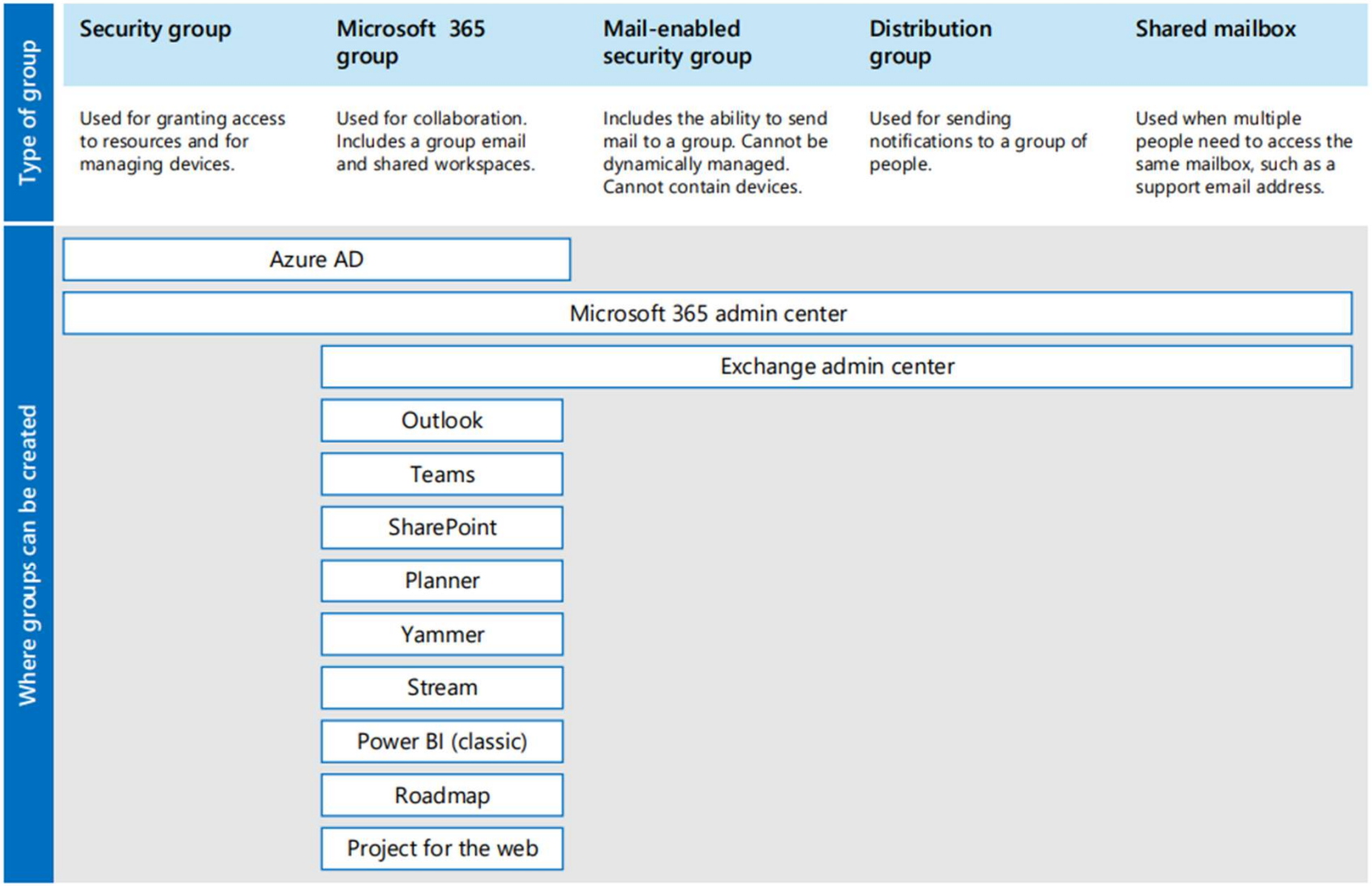
- Group document library – aka “Files” –
- Shared notebooks

The specific resources that are provided depends slightly on the groups experience your team wants to have

One size rarely fits all

Types of groups and where they are created

Groups can be created in several of the admin centers and by users from within apps.



Office 365 Groups is a membership service for Teams

Attributes

One identity

Azure AD is the master for group identity & membership

Federated resources

Office 365 services extend with their data

Loose coupling

Service notify each other of changes to a group

Work Flow

User creates new group for teamwork

Group identity created in Azure Active Directory

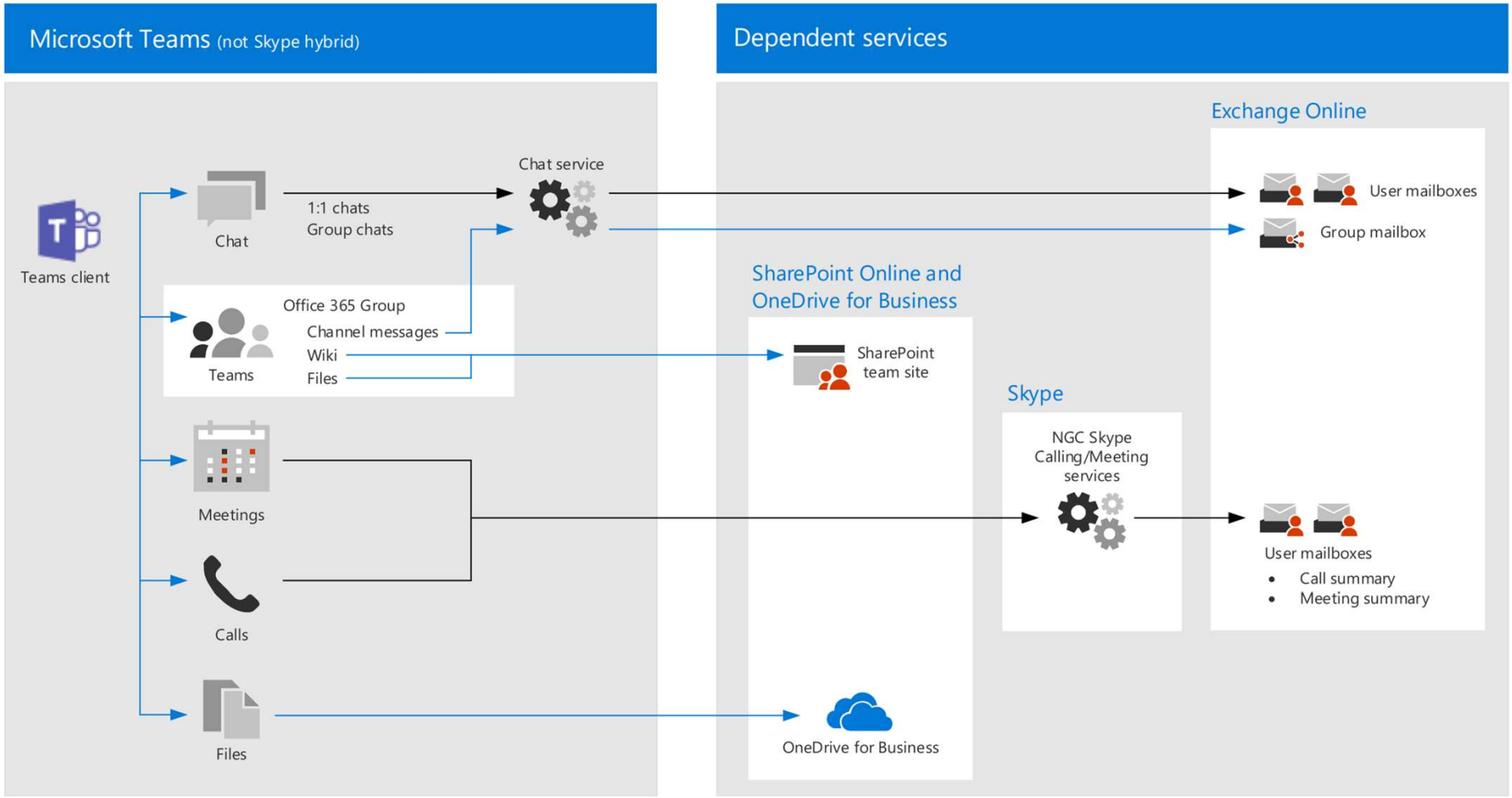
Group experience populated in app of choice

Compatibility

Azure AD

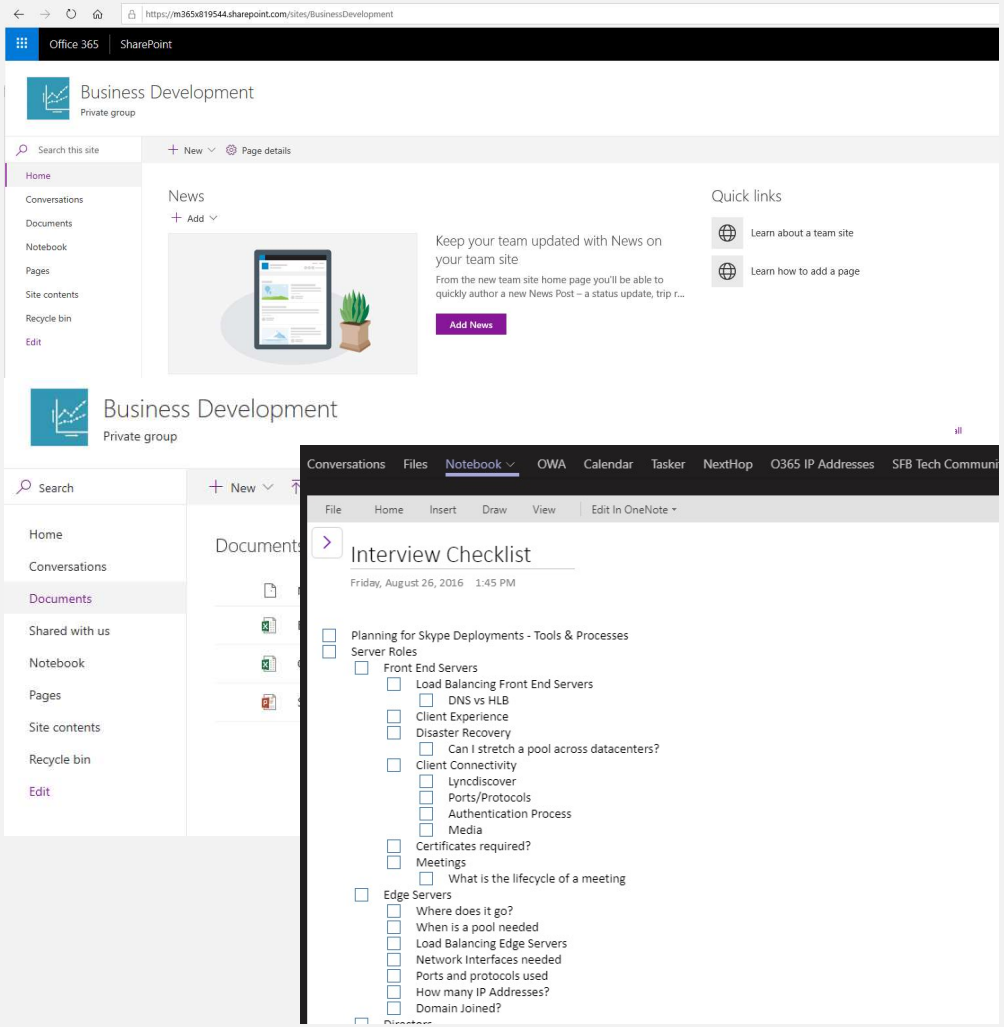
- Outlook
- Teams
- Shifts
- SharePoint
- Planner
- Dynamics CRM
- Yammer
- Stream
- Power BI

Teams 논리 구조

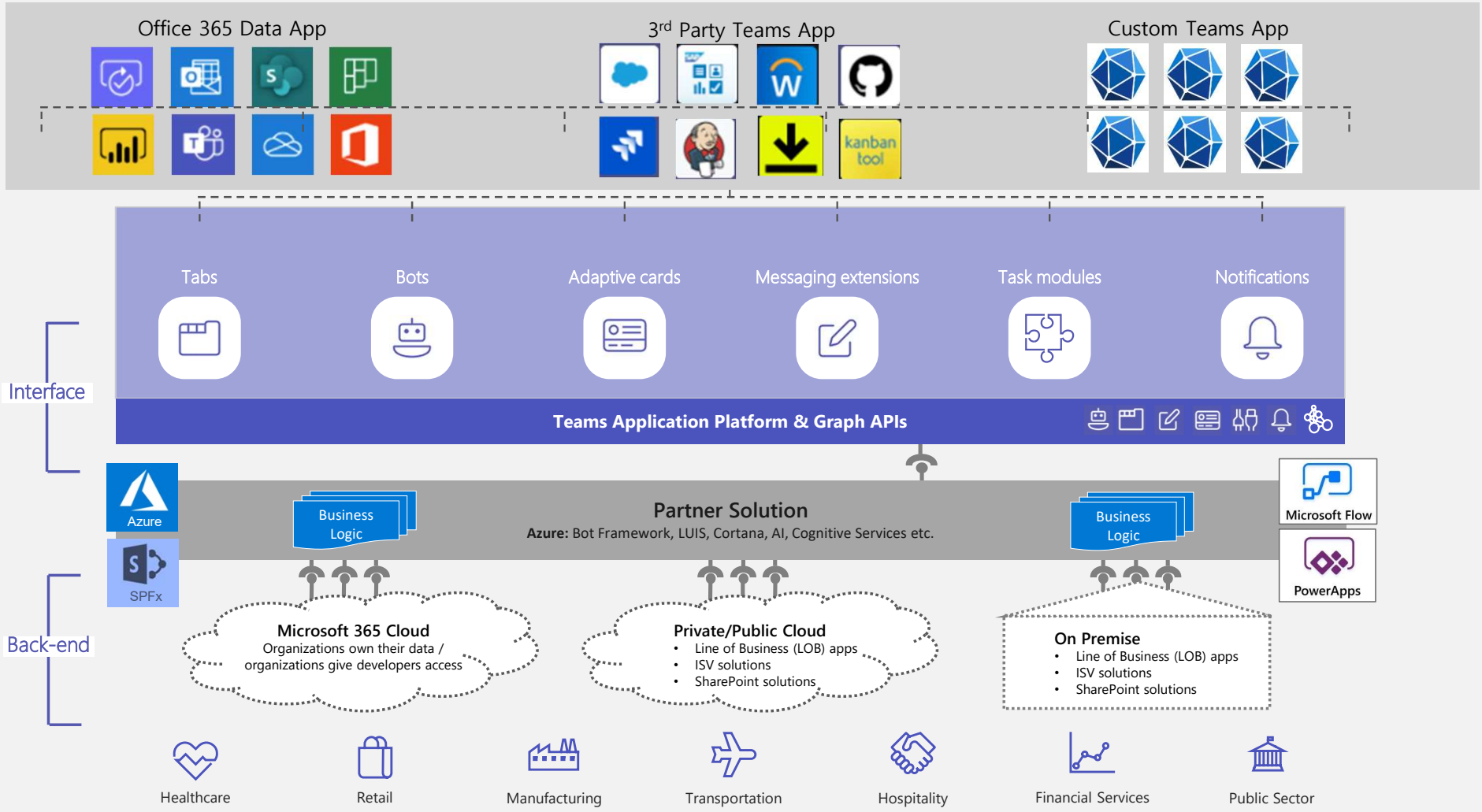

Microsoft Teams (not Skype hybrid)
Dependent services
Teams client
Chat
1:1 chats
Group chats
Chat service
Exchange Online
User mailboxes
Group mailbox
Office 365 Group
Channel messages
Wiki
Files
Teams
SharePoint Online and
OneDrive for Business
SharePoint
team site
Skype
NGC Skype
Calling/Meeting
services
Meetings
Calls
User mailboxes
Call summary
Meeting summary
Files
OneDrive for Business

How Teams uses SharePoint Online and OneDrive for Business

- SharePoint Online and OneDrive for Business are used to store files that users share in Teams
- Every Team gets a modern SharePoint Team site as part of its O365 group
  - If team with same name already exists, the SharePoint URL will include a GUID
- Team OneNote is stored in SharePoint Online
- Add tabs for any: SharePoint page, list, news, single document
- News connector posts news articles within Teams channels



Teams 확장기능 표준 아키텍처



Teams 적용 아키텍처 예시