BUSINESS TECHNOLOGY
SUMMIT 2024

Ditching Active Directory

A Whirlwind Tour of Modernizing Identity & Access Management using Entra ID

BUSINESS TECHNOLOGY

SUMMIT 2024

Housekeeping

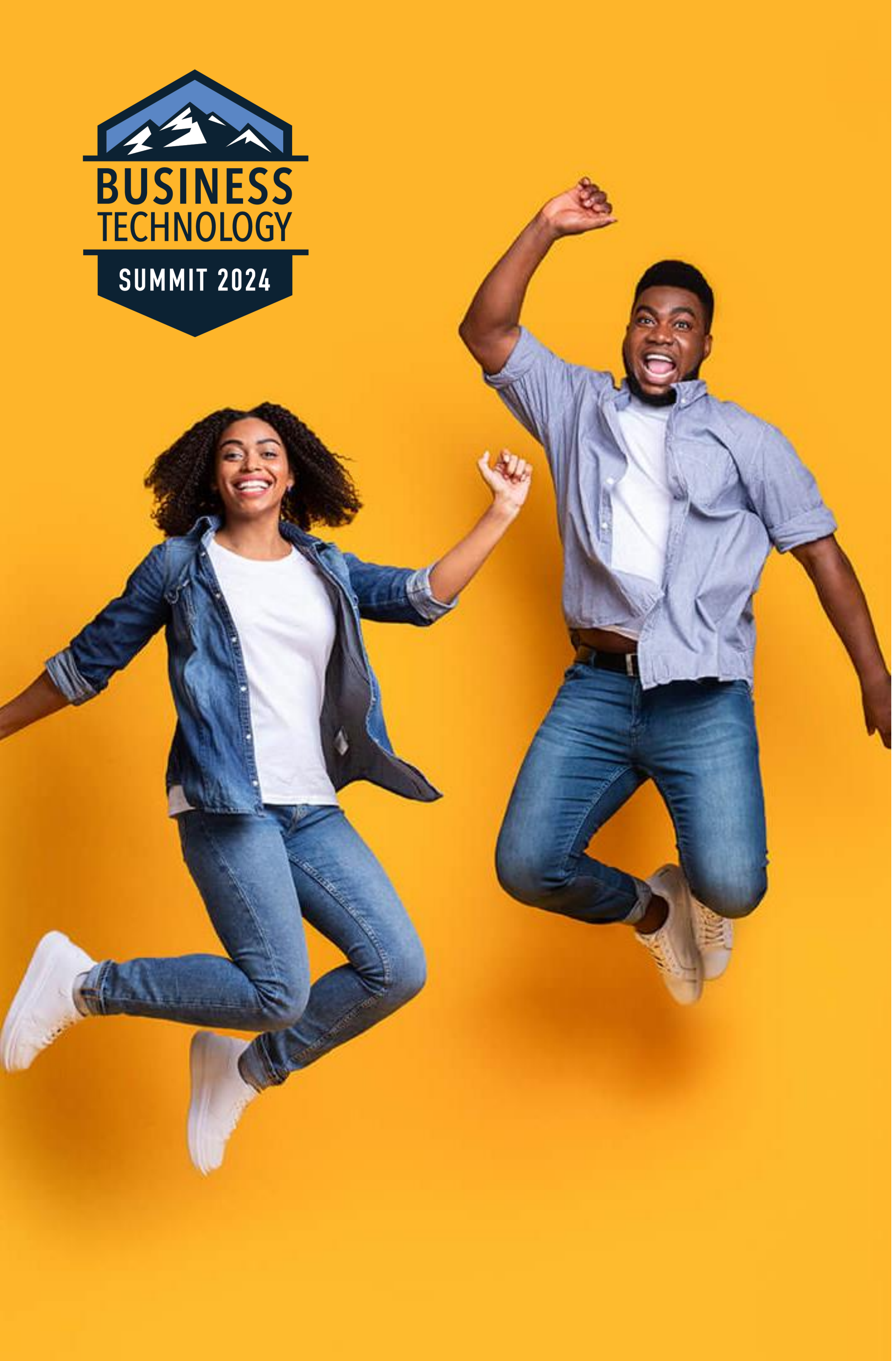
- Please silence your phones. If you need to take a call, feel free to step outside and come back in.
- Sessions are being recorded and will be available after.
- Please use this QR code to take the session survey before heading to the next session.
- Survey responses get you more entries into the raffle at the end of the day. (prizes included Surface headphones, Smart Ray Bans, RayBan Meta Smart Bluetooth Glasses, and lots more).
- Wifi Info: BusinessTechnologySummit

Password: journeyteam!

Presenters

ERIC RAFF

MODERN WORK & SECURITY DIRECTOR



BUSINESS TECHNOLOGY SUMMIT 2024

Agenda

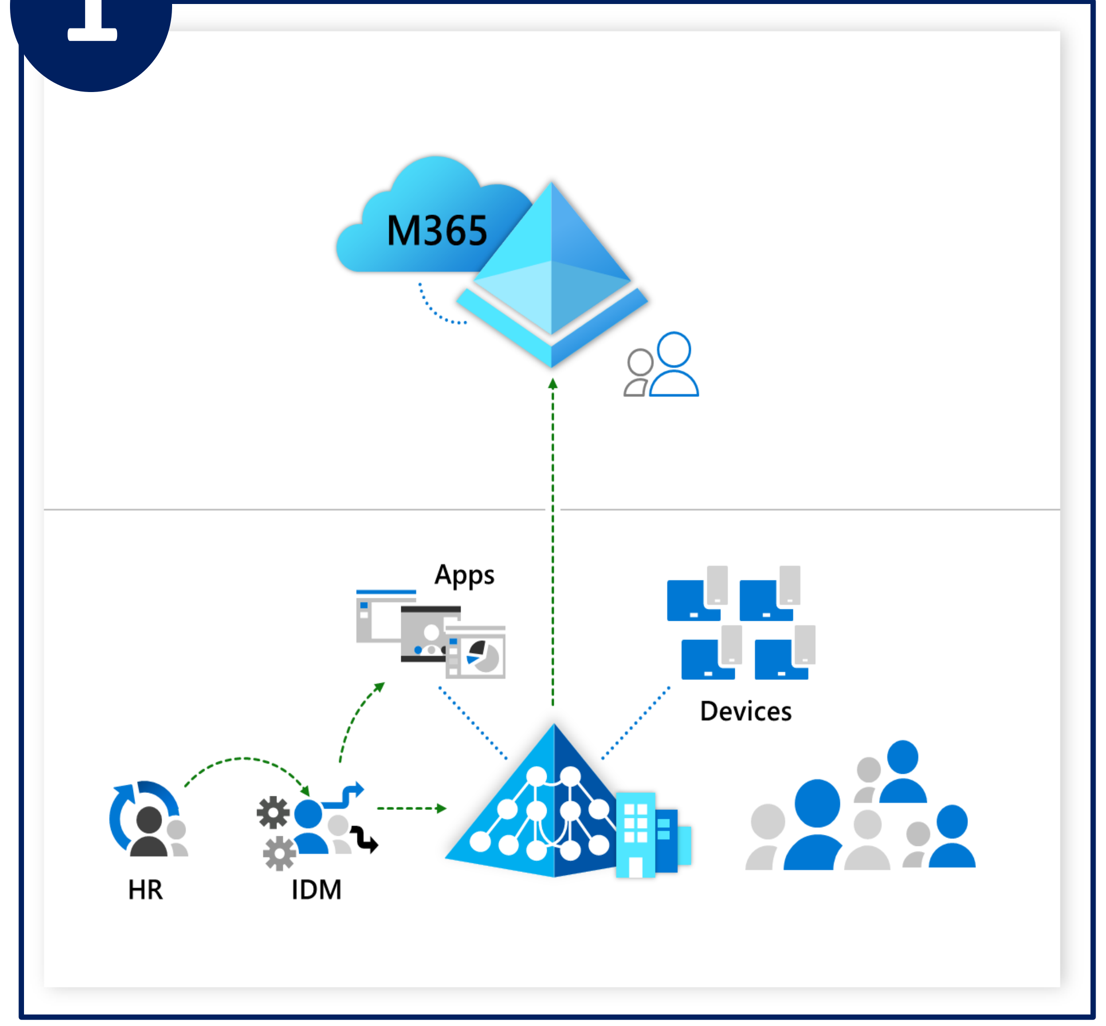
- Why this Matters – Guiding Principles
- Order of Events
- Important Considerations / Key Updates
- Workstream Considerations – “Then” (2021) vs “Now” (2024)

Why This Matters

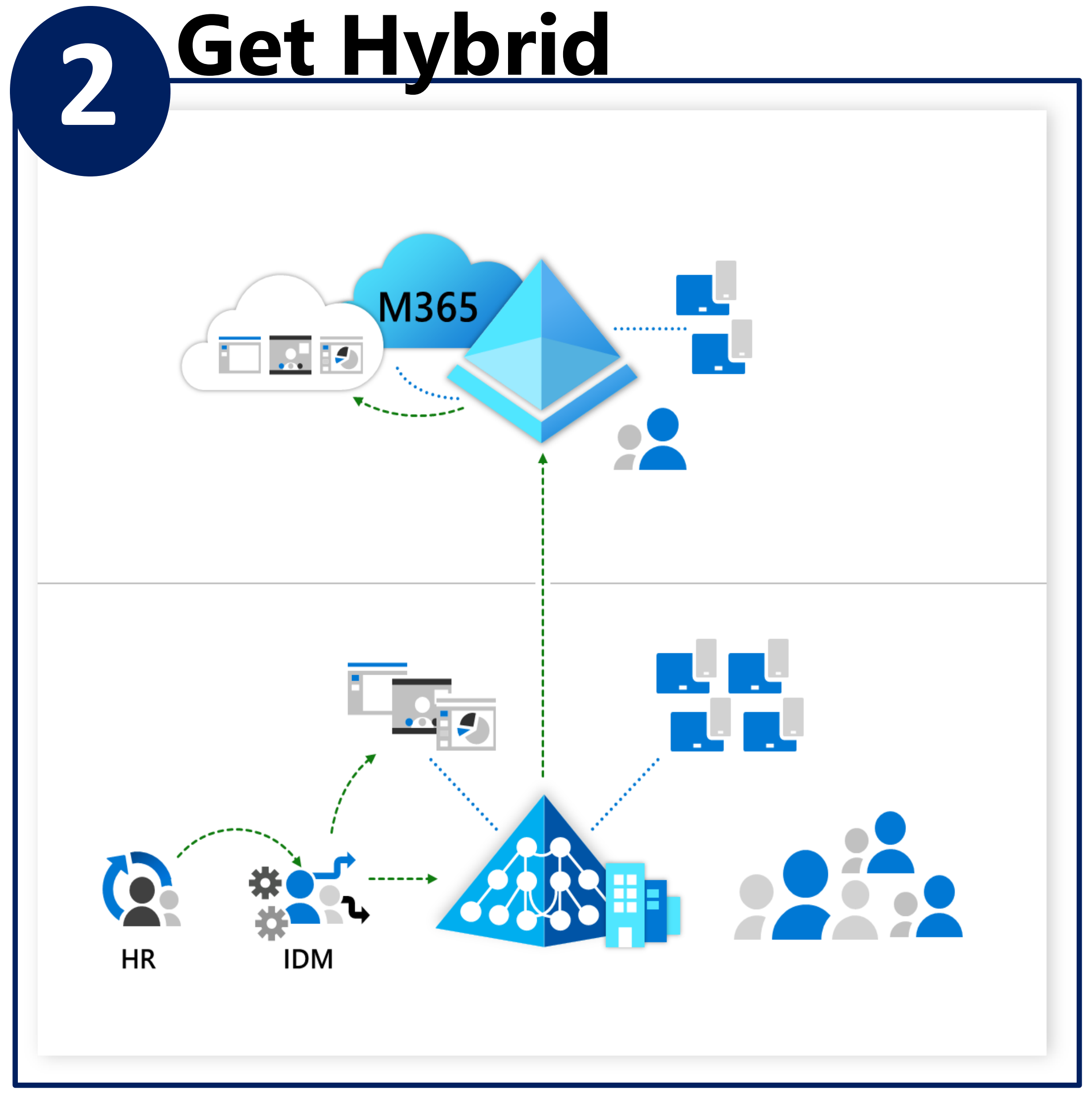
- Cloud Strategy
  - Shifting to Cloud sourced identities, groups and processes vs AD sourced
- Legacy patters are not maturing
  - Legacy onboarding and management of IAM services
  - AI is all going to be cloud based on data and services in the cloud
  - Device is a factor
- Effort and investment is going to the Cloud vs On-Prem
- A fresh point of view – what would a green field deployment look like?

Order of Events

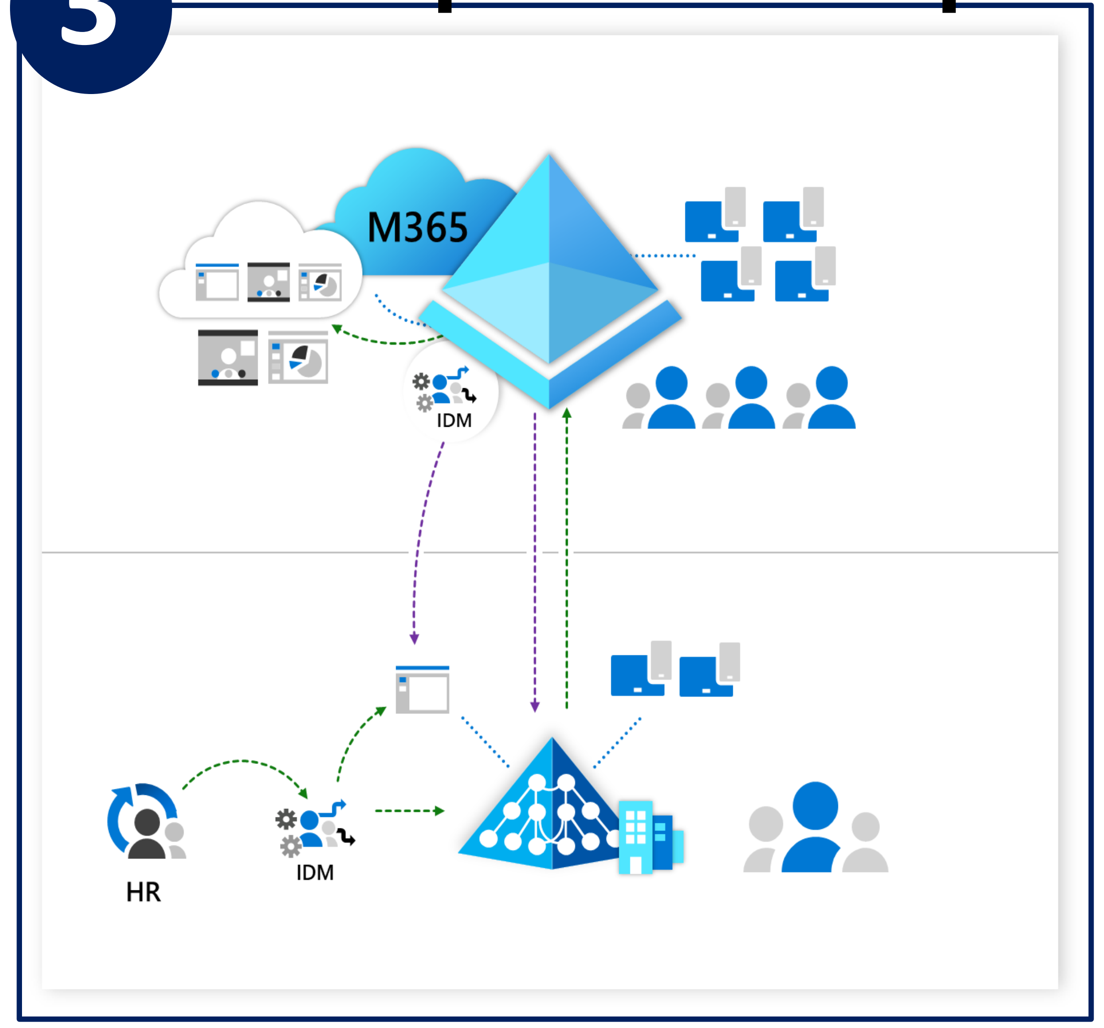
1 Attach to cloud



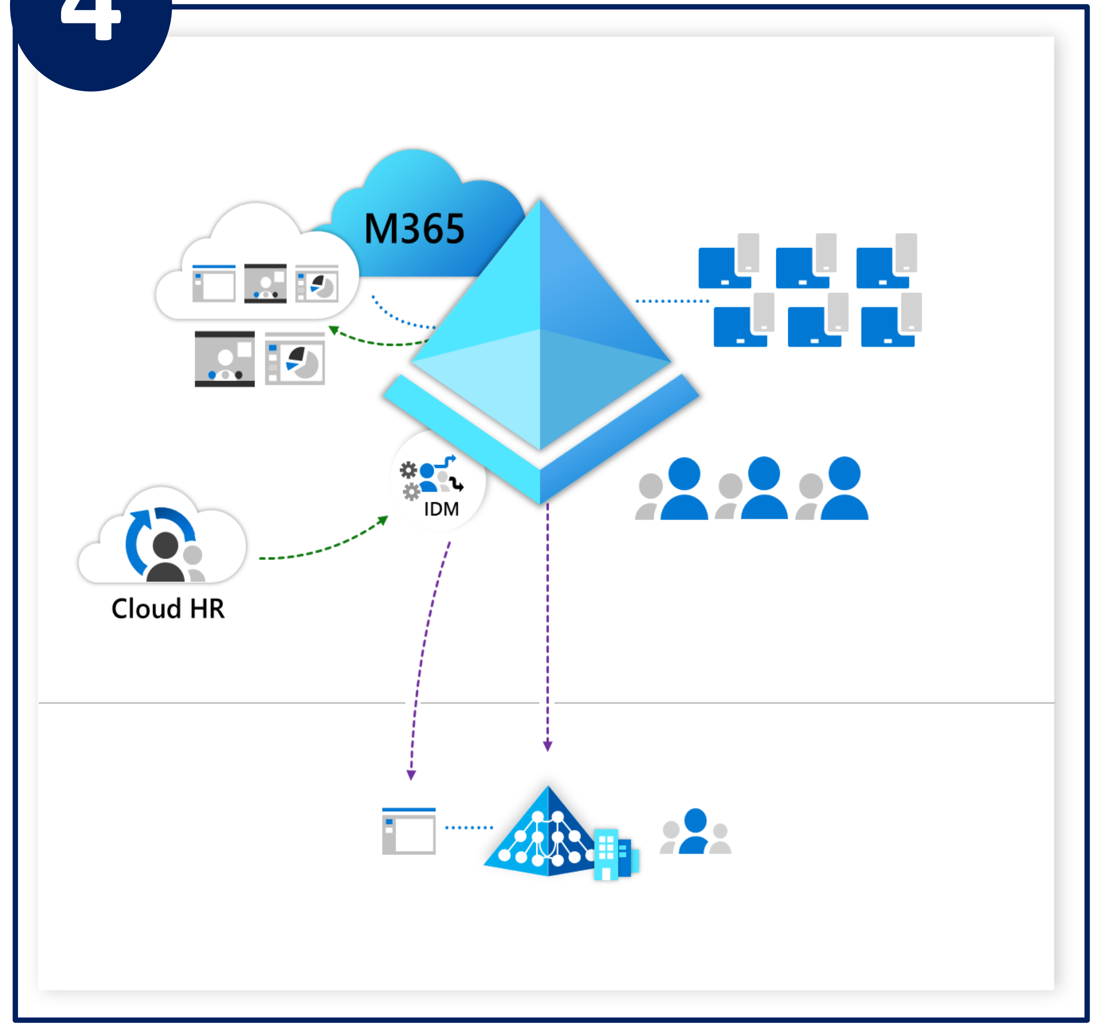
2 Get Hybrid



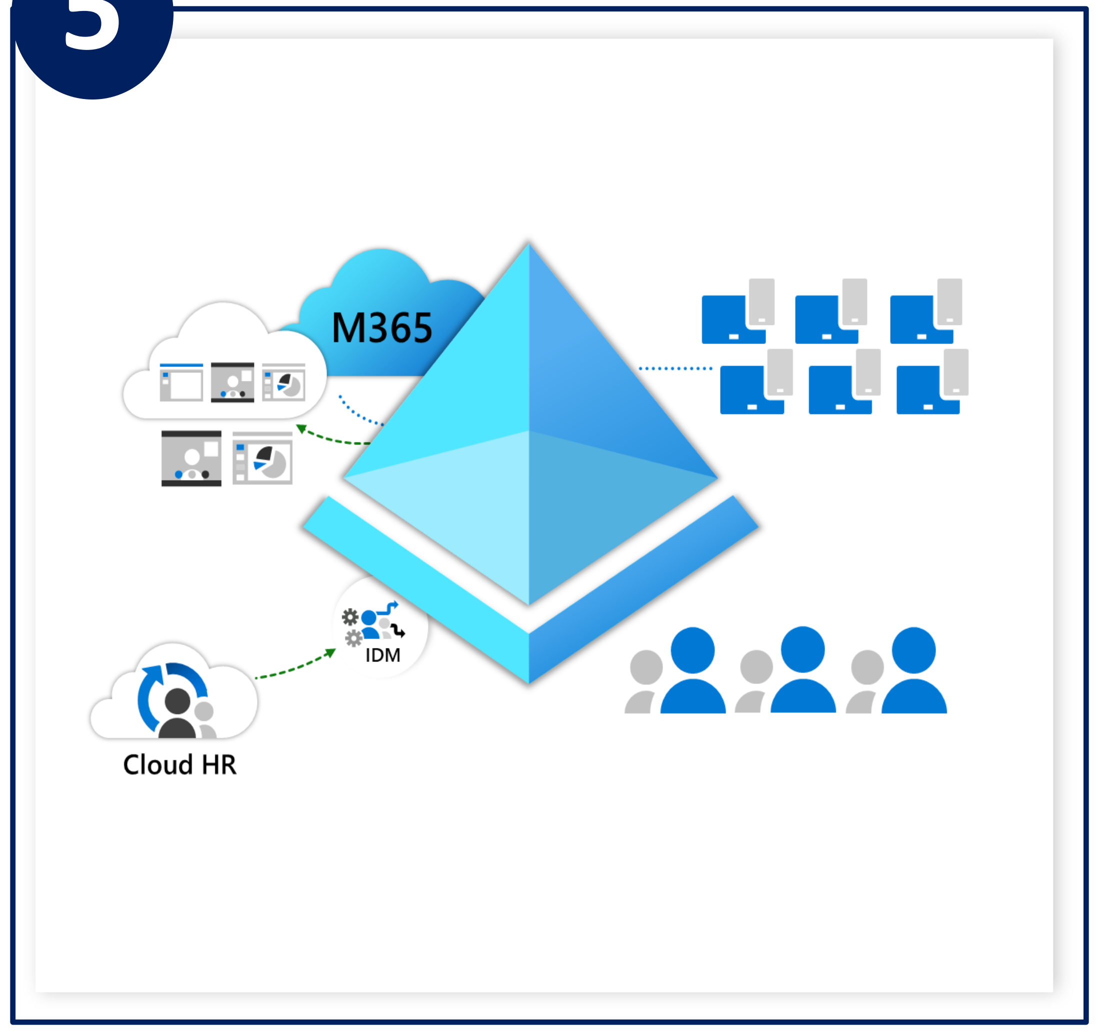
3 Decouple from on-prem



4 Cloud-Centric, AD minimized

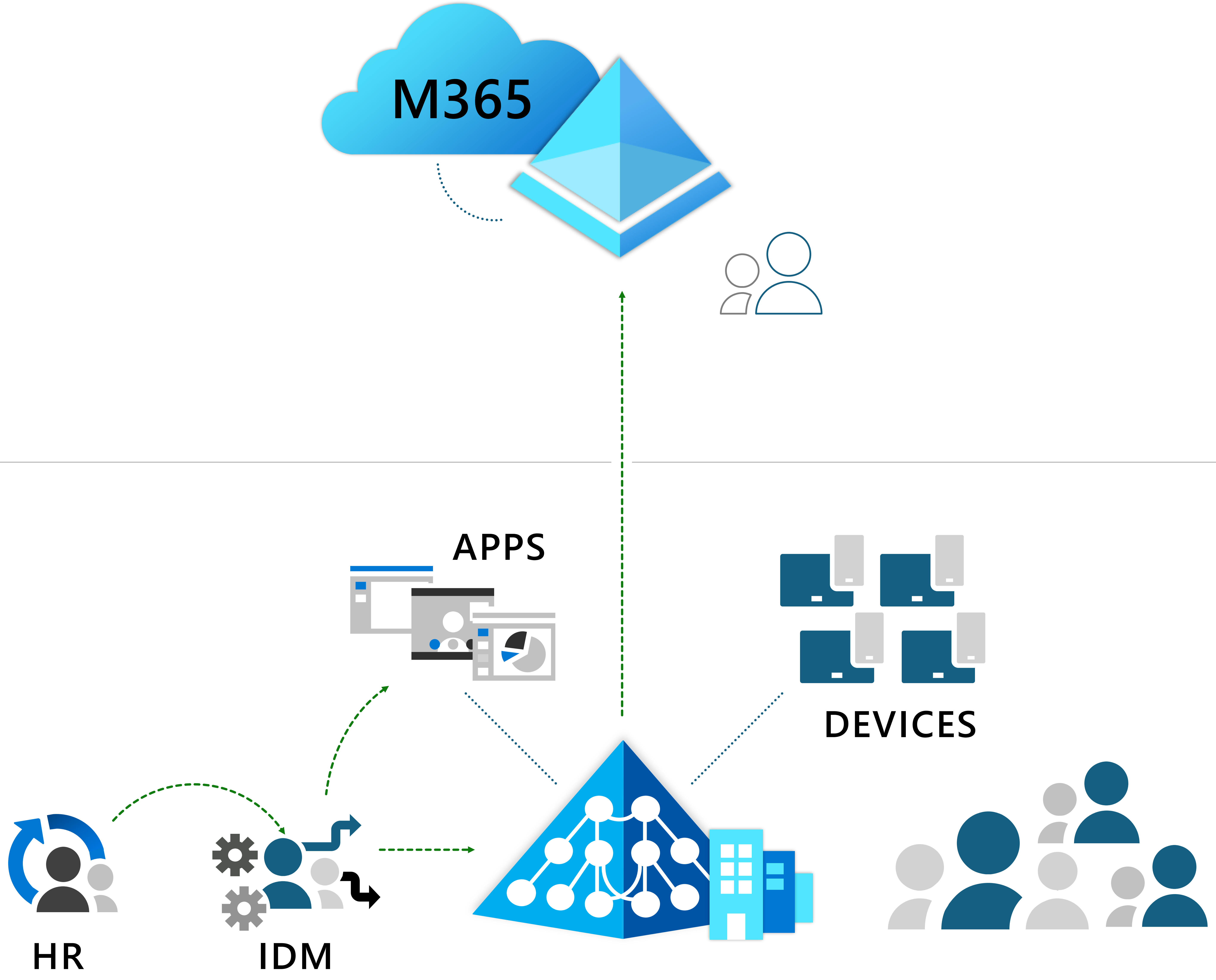


5 100% Cloud



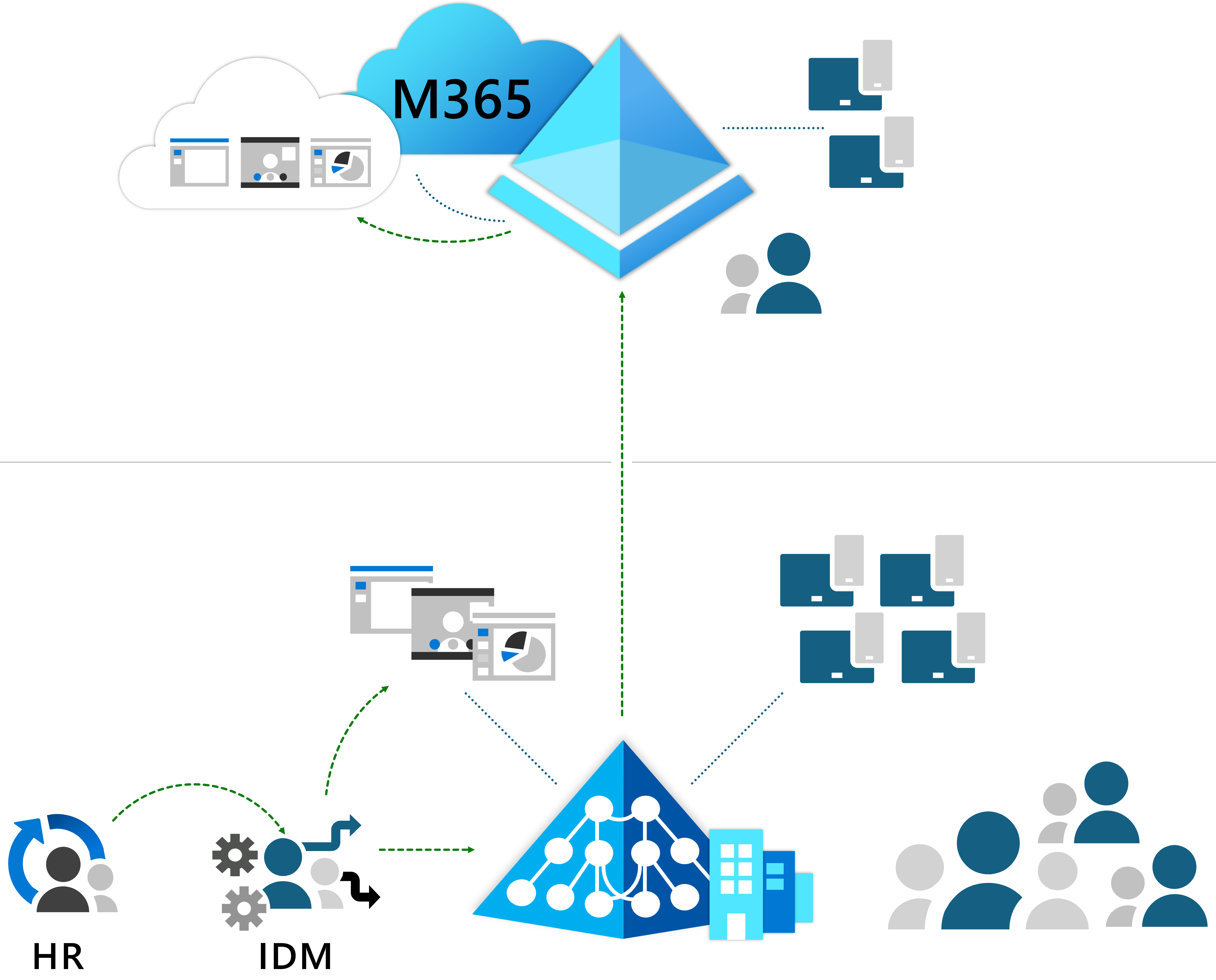
1 Attach to Cloud

- Domain joined devices
- Users managed in AD, provisioned via on-premises IDM from on-premises HR systems or manually
- Users synced to the cloud for office 365
- Apps authenticate to AD, or federation servers (e.G., AD FS, Okta etc.)



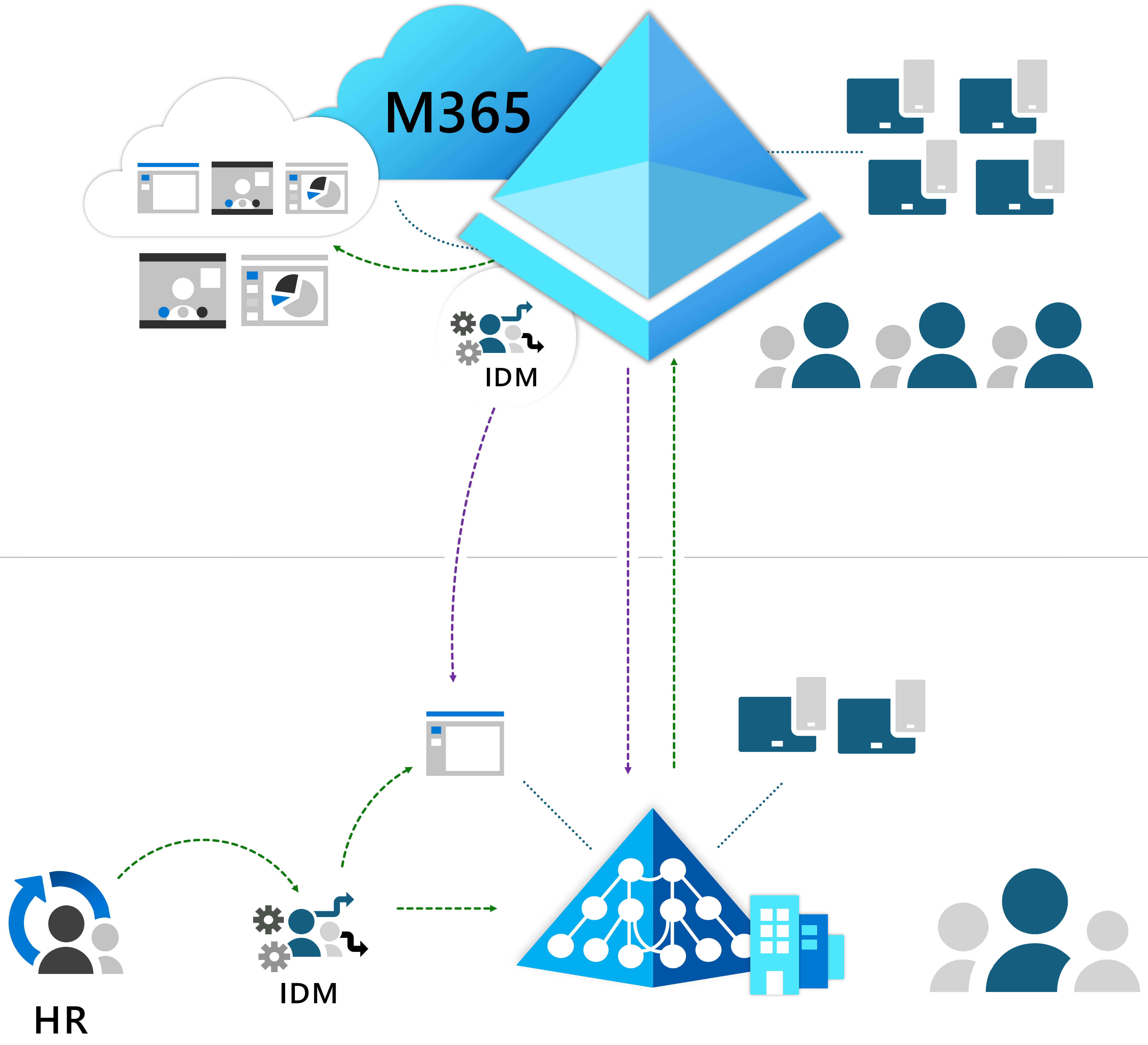
2 Get Hybrid

- Devices become hybrid Entra joined
- Lift some apps to the cloud with Entra ID DS
- Authenticate legacy apps to Entra ID via app proxy
- Enable SSPR for users



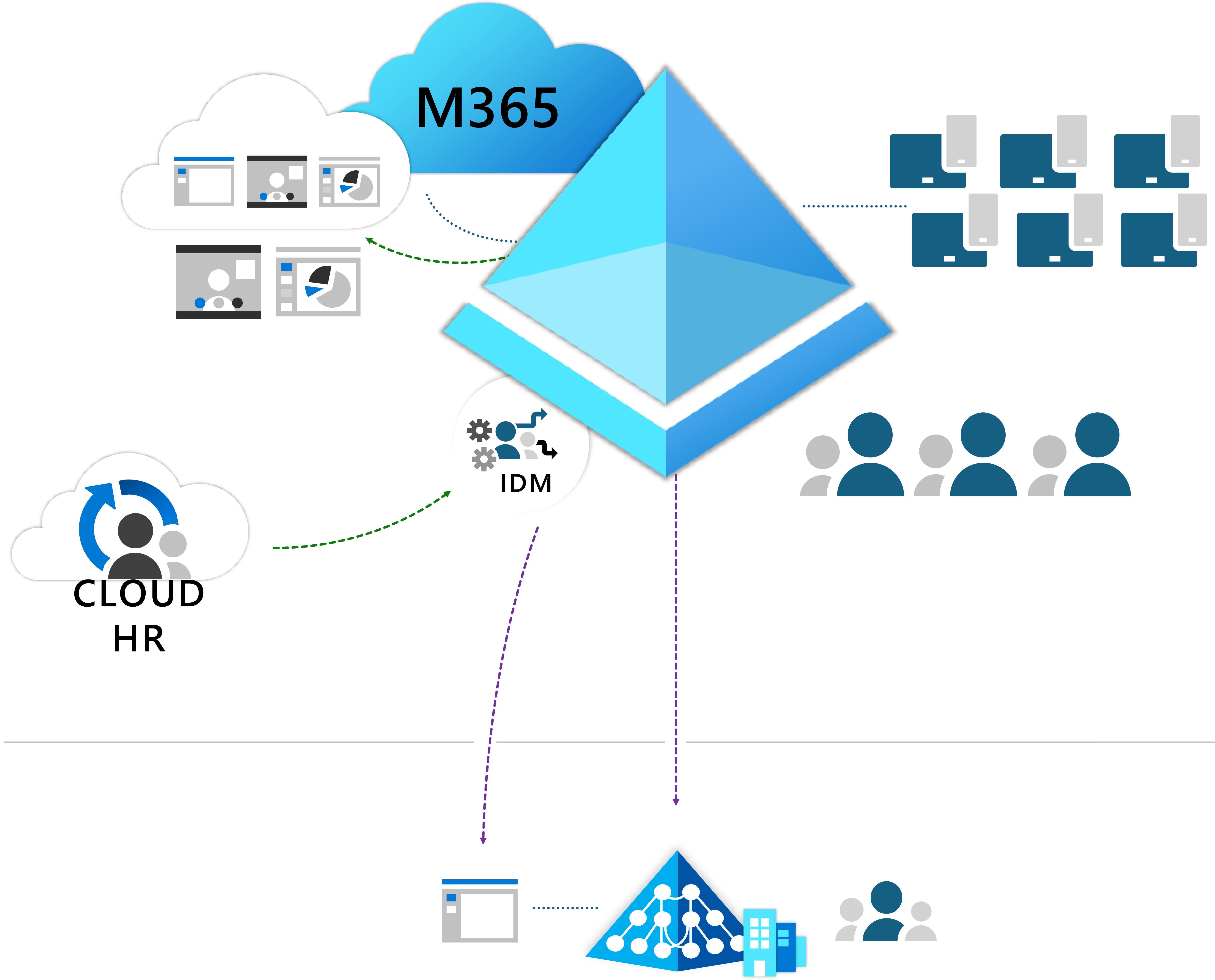
3 Decouple from on-premises

- Join new devices to Entra and provision them with Intune.
- Use connectors for app provisioning
  - 3rd party or ECMA
- Migrate federated apps to Entra ID
- Manage legacy apps in the cloud using Entra ID DS and app proxy
- Begin moving file servers and printers to the cloud +



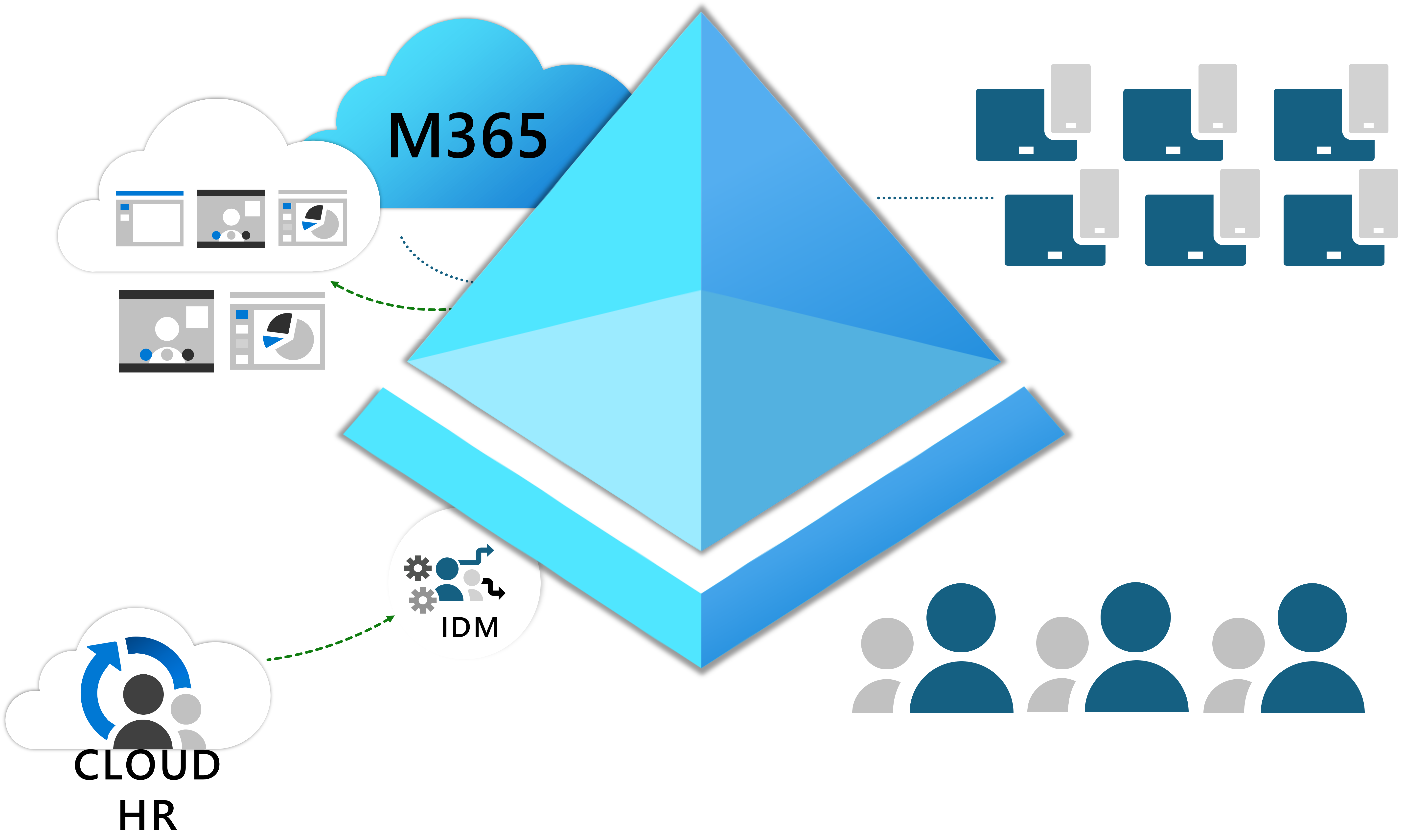
4 Cloud Centric - Minimize AD

- Move HR system to SaaS
- Manage users as cloud-first—only write-back if needed
- Modernize apps or replace them with SaaS
- Manage legacy apps in the cloud with Entra ID DS + Entra ID app proxy
- Replace on-premises workloads with Microsoft 365, Windows 365, Azure files, cloud print, Azure SQL



5 100% Cloud

- All devices modern managed
- No on-premises IAM footprint required
- Azure AD provides all IDM features
- All apps use modern authentication against Entra ID or in cloud with Entra ID DS and app proxy



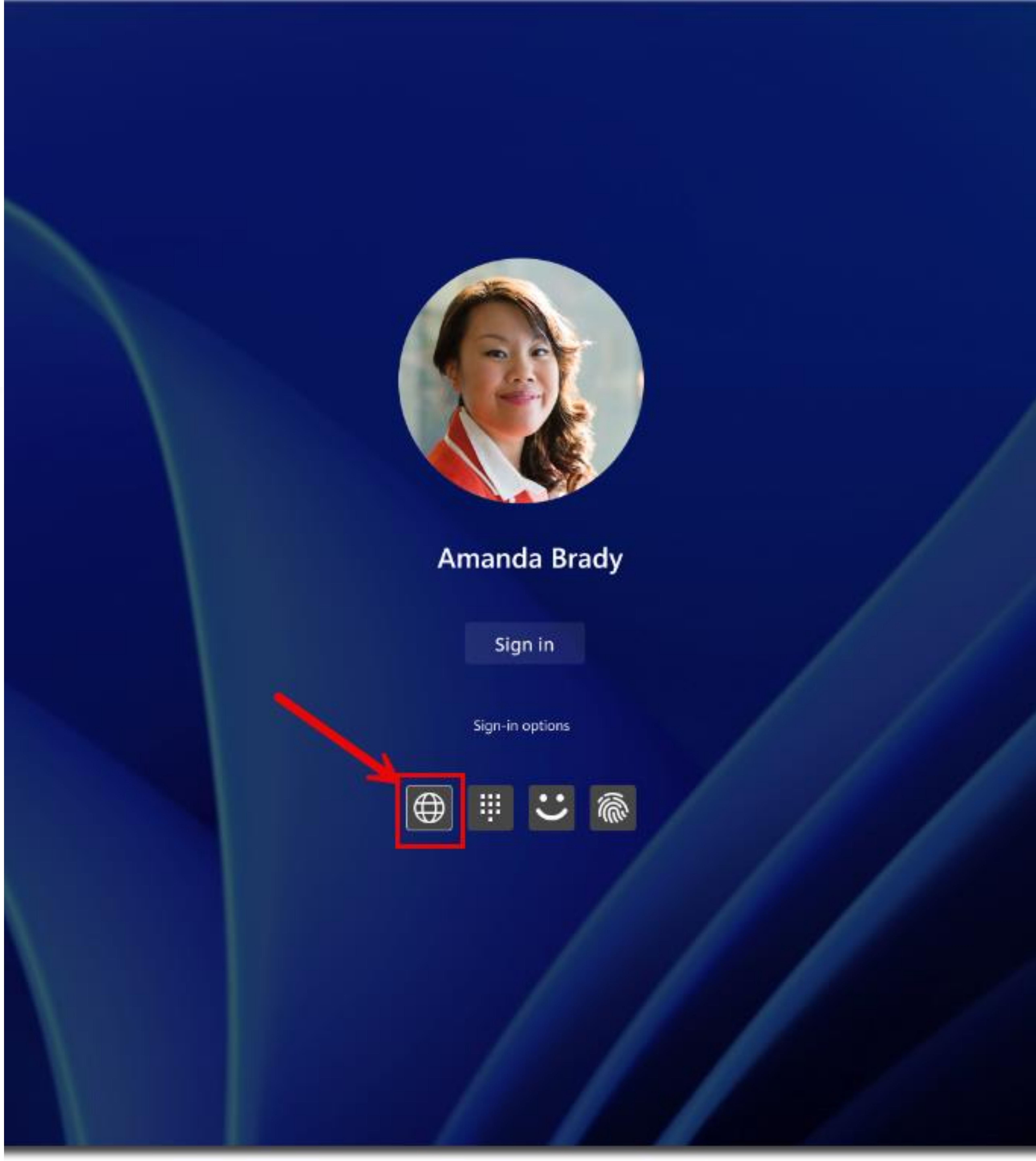
Entra ID Key Updates & Tips as of Feb 2024

Will discuss the following 5 updates and tips

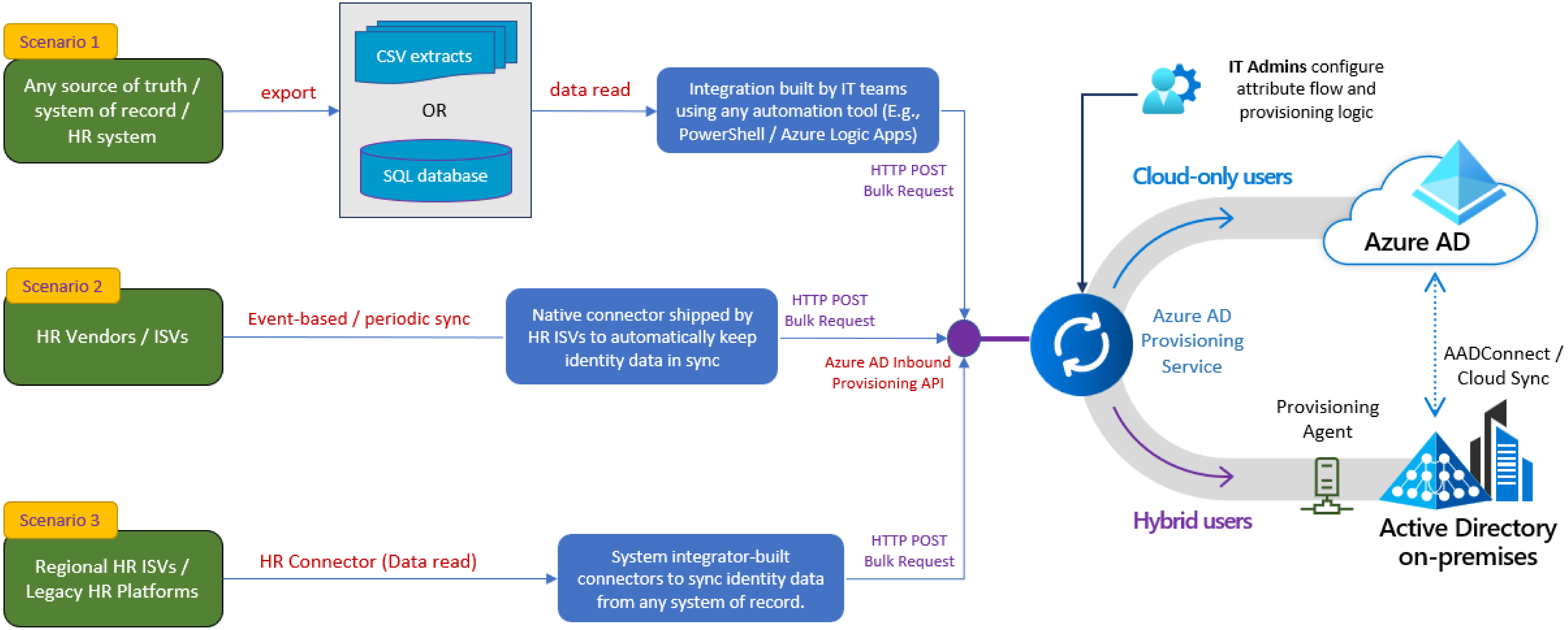
- Windows 11 Web sign-in for Windows (GA)
- Entra ID Group Provision to AD / Write Back (GA)
- Entra ID API based Provisioning (Preview)
- Cross Tenant Sync for B2B use cases (GA)
- Disconnecting your AD from Entra ID (the fun part)

Windows 11 Web Sign In

- Need Internet Access
- No Cached Creds
- Modern AuthN at runtime natively to Entra ID
- WILL support Federated AuthN to external IdP’s (ADFS, Okta, Ping, etc.)



Entra ID API Provisioning Options (preview)



Scenario 1

Any source of truth / system of record / HR system

export

CSV extracts

OR

SQL database

data read

Integration built by IT teams using any automation tool (E.g., PowerShell / Azure Logic Apps)

HTTP POST Bulk Request

Scenario 2

HR Vendors / ISVs

Event-based / periodic sync

Native connector shipped by HR ISVs to automatically keep identity data in sync

HTTP POST Bulk Request

Azure AD Inbound Provisioning API

Scenario 3

Regional HR ISVs / Legacy HR Platforms

HR Connector (Data read)

System integrator-built connectors to sync identity data from any system of record.

HTTP POST Bulk Request

IT Admins configure attribute flow and provisioning logic

Azure AD Provisioning Service

Cloud-only users

Azure AD

AADConnect / Cloud Sync

Provisioning Agent

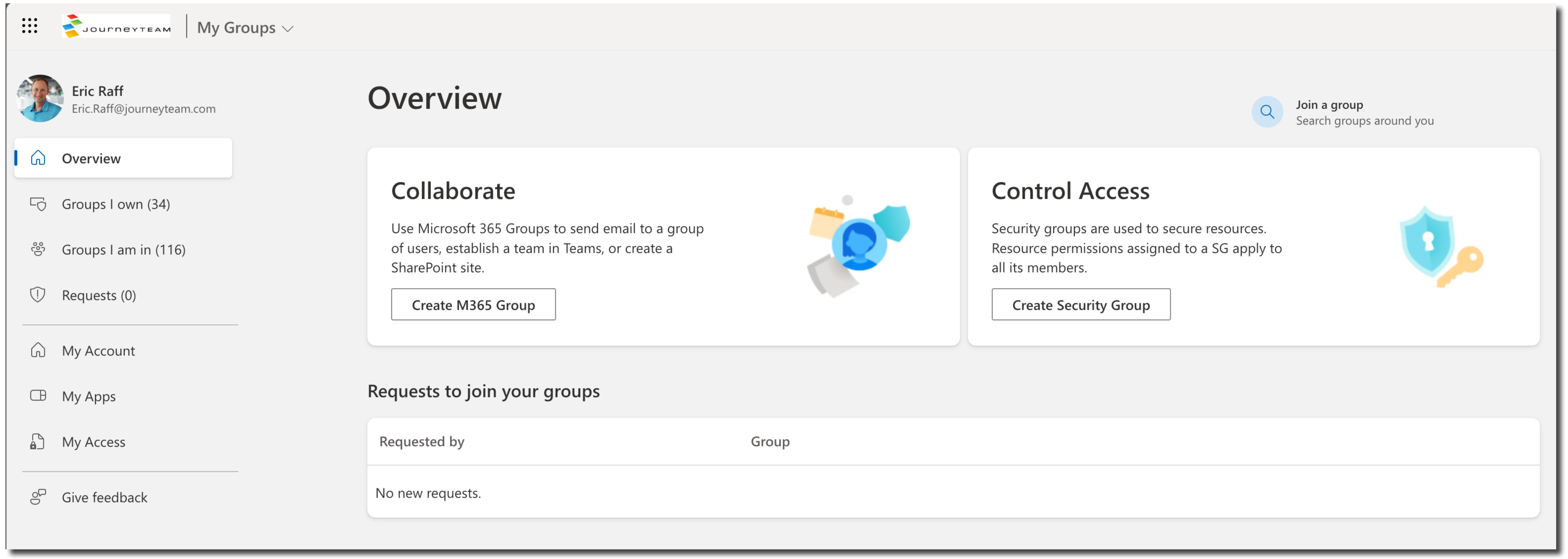
Hybrid users

Active Directory on-premises

Entra ID Group Provision to AD

Group writeback V2 using Entra ID Connect Sync (Azure AD Connect Sync) is dead after June 30 2024

- Master groups in the cloud, take advantage of Entra management, governance, flexibility
- Don’t forget about your B2B Guest use cases and Authorization points in the cloud
  - Cannot add a Guest user to an AD mastered group
- Native cloud groups enable self service capabilities
  - mygroups.microsoft.com
- Write Entra ID groups BACK to AD if required – not the other way around



Overview

Collaborate

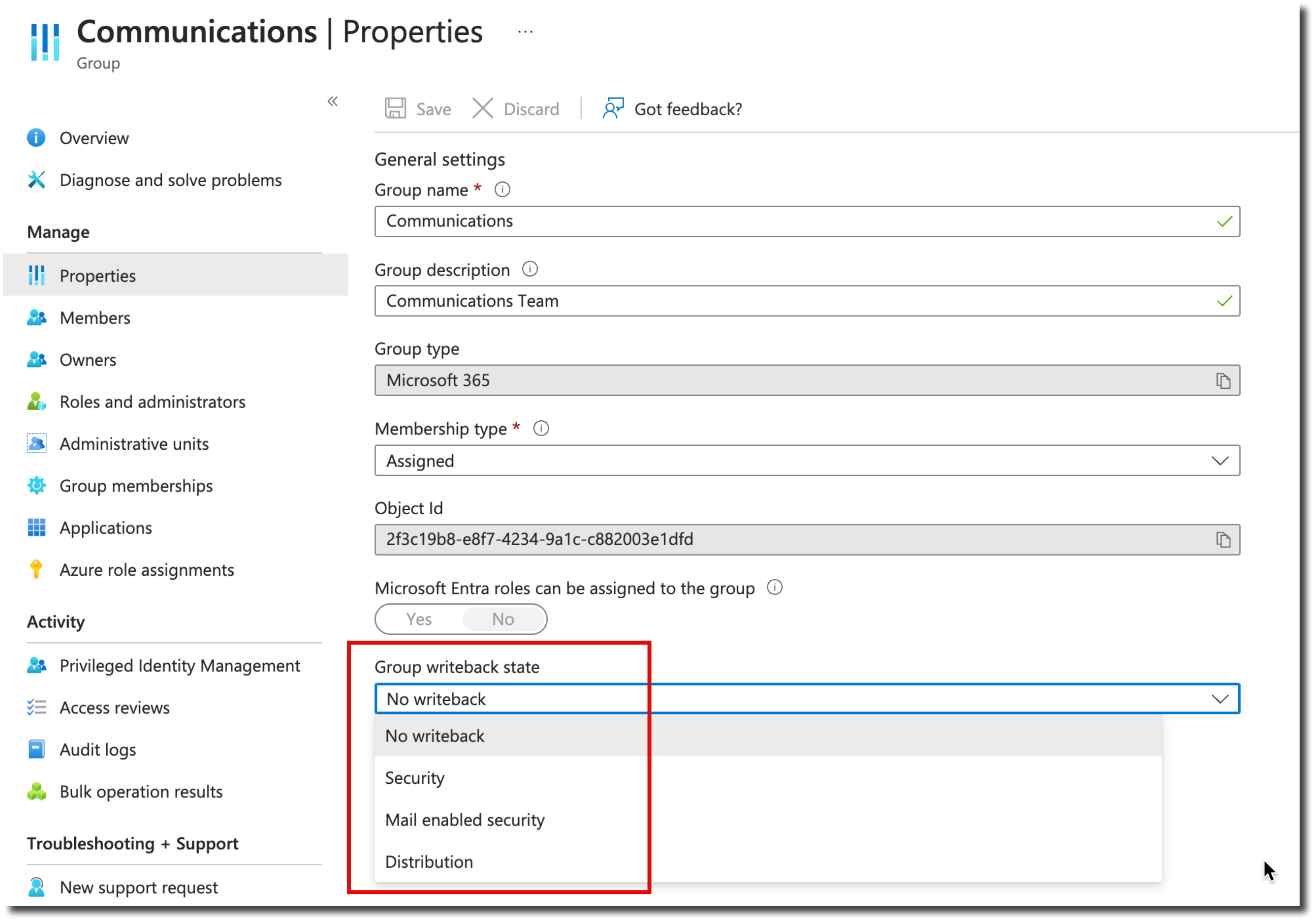
Use Microsoft 365 Groups to send email to a group of users, establish a team in Teams, or create a SharePoint site.

Control Access

Security groups are used to secure resources. Resource permissions assigned to a SG apply to all its members.

Requests to join your groups

Requested by	Group
No new requests.	



Communications | Properties

General settings

Group name *: Communications

Group description: Communications Team

Group type: Microsoft 365

Membership type *: Assigned

Object Id: 2f3c19b8-e8f7-4234-9a1c-c882003e1dfd

Microsoft Entra roles can be assigned to the group: Yes [✓ No]

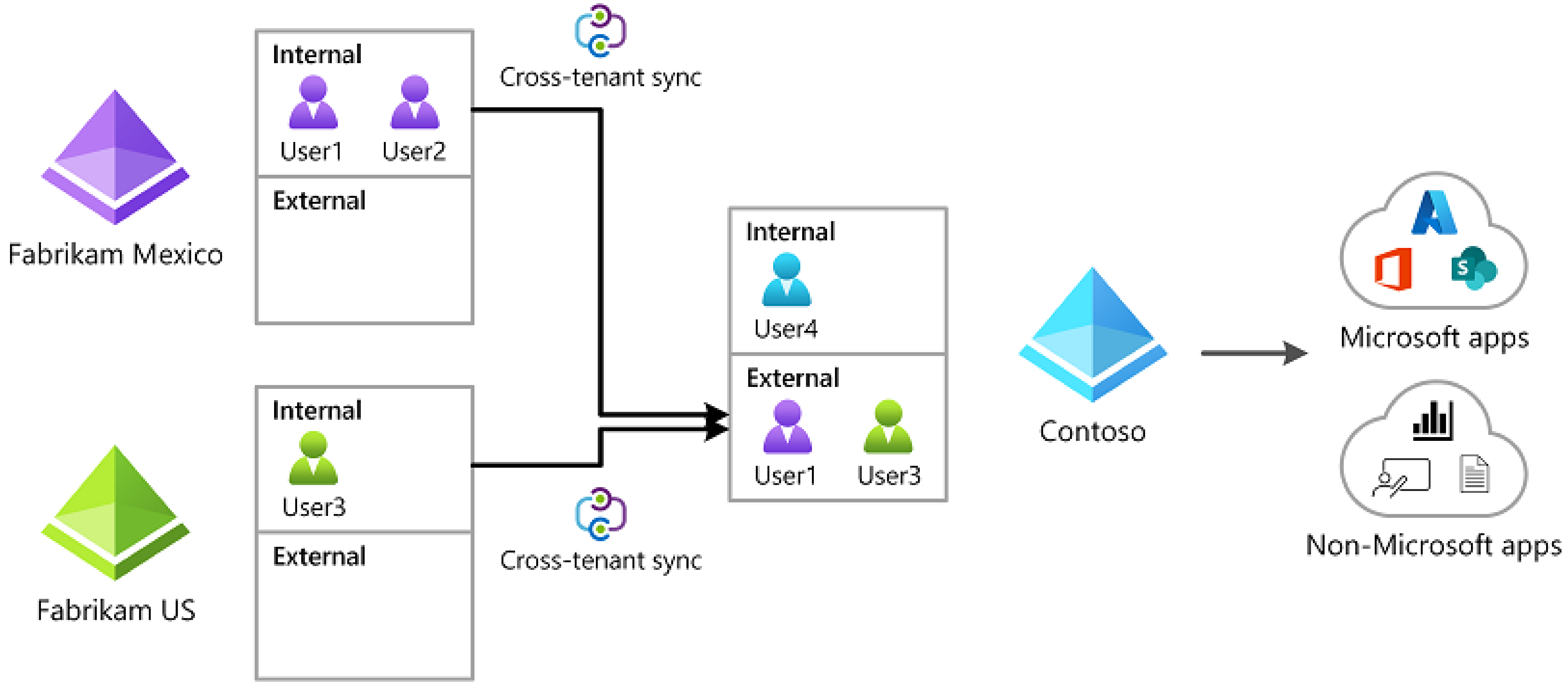
Group writeback state: No writeback

- No writeback
- Security
- Mail enabled security
- Distribution

Entra ID Cross Tenant Sync

Multi-Tenant org enablement

- Automatically provision guest users from source ”home” tenant to target tenant
- Map and sync user attributes between tenants
- Full lifecycle management based on home tenant user status
- Service integration is a moving target
  - Teams is leading the way
  - Email is a unique use case
- ONLY valuable for cloud sourced services and integrations



Disconnecting your AD from Entra ID – Exchange Use Case

I WANT TO COMPLETELY GET OFF ANY REFERENCE OR NEED FOR EXCHANGE ON-PREM

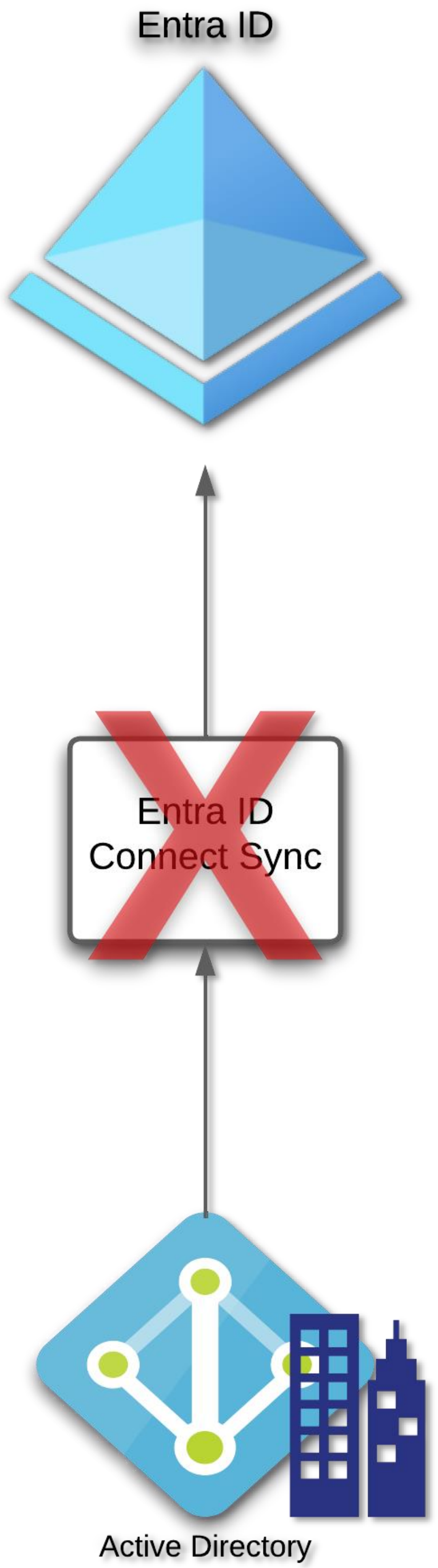
- Get off your last exchange server – 0 mail flow dependencies
- Stop needing to “enable-remotemailbox” – let Entra ID/EXO provision mailboxes and you have no need for an on-prem GAL
- Identity ALL exchange related object types and what OU they are in AD for:
  - Distribution Lists
  - Shared Mailboxes
  - Conf Rooms
  - Ex-Employees that need mailbox retention
  - SUMMARY: ANY Exchange object that there is no need for an AD object in the end after a partial cut
- Stop Sync
- Disable Sync for entire tenant - start waiting
- MOVE exchange AD objects to an OU that is NOT included in Sync Scope
- Install NEW* Entra ID Connect Sync service and exclude OU of “Legacy” exchange AD objects
- User & Security group objects are re-connected back up

*** THERE IS ANOTHER OPTION, BUT CONTACT US IF INSTALLING NEW ENTRA ID CONNECT SYNC SERVICE IS A SHOW STOPPER**

Disconnecting Your AD from Entra ID – ALL IN

Current State and Experiences of disconnecting AD from Entra ID

- TODAY: Only “supported” way to disconnect AD from Entra ID is to:
  - Set-MsolDirSyncEnabled -EnableDirSync $false
- TOMORROW: Wait and see what Microsoft *may* provide in the future
- But what about the recycle bin trick you ask?
  - Microsoft does not like it and it *could* cause issues with some M365 services (Teams VOIP/SIP)
  - I don’t suggest doing this
- You should be able to create NEW users in the cloud and they have full functionality BEFORE you are ready to turn sync completely off
  - Operations and support and ready for this change
  - User onboarding and provisioning are ready for this change
  - Tooling is different for mass and bulk operations
- It feels GREAT!



Migration Patterns

Pattern	Explanation
Migrate	Fully move to Azure AD
Go Hybrid	Move to Azure AD, can't deprecate on-prem yet but management plane is in Azure AD. In some cases, Management Plane is in on prem, but can be used in the cloud
Go Hybrid with partner integration	Use Entra ID capabilities + Partnership integrations
Evaluate	Can evaluate capabilities that are early in the cycle (e.g., Public Previews)
Wait	Entra ID does not have capability today, but it may come later. "Soon"
Revisit Approach	Re-design the underlying capability, let footprint die by attrition or decommission and replace with modern alternatives.

Migration Pattern Guidance

- Then (2021) and Now (2024)
- Migration Patterns/State
- Guidance around specific workloads
  - Apps
  - Users
  - Devices
  - Data
- Timing and state of affairs as of today

Apps – Migration Pattern Guidance (Then & Now)

Area	2021 Recommended Pattern	2024 Recommended Pattern
User Access & Authentication		
Federated Apps	Migrate	Migrate
Web Access Management App	Migrate	Migrate
Windows Integrated Auth Web Apps	Migrate	Migrate
Windows Integrated Auth non-web apps	Migrate	Migrate
Rich client apps	Evaluate	Evaluate – (Consider Entra Private access)
Internet-Resilient Mission Critical Apps	Wait	Wait
Access to Directory Data		
Applications using LDAP interface to AD	Evaluate	Entra ID Domain Services / 3rd party proxy (Strata)
Applications using LDAP interface to 3rd Party Directory	Wait or Revisit approach	Revisit approach
Provisioning		
Cloud Applications	Migrate	Migrate
On-Prem Applications	Hybrid with Partner or Evaluate	Hybrid-Group write back with cloud sync, partner

Apps – Migration Pattern Guidance (Then & Now)

Area	2021 Recommended Pattern	2024 Recommended Pattern
User Access & Authentication		
Federated Apps	Migrate	Migrate
Web Access Management App	Migrate	Migrate
Windows Integrated Auth Web Apps	Migrate	Migrate
Windows Integrated Auth non-web apps	Migrate	Migrate
Rich client apps	Evaluate	Evaluate – (Consider Entra Private access)
Internet-Resilient Mission Critical Apps	Wait	Wait
Access to Directory Data		
Applications using LDAP interface to AD	Evaluate	Entra ID Domain Services / 3rd party proxy (Strata)
Applications using LDAP interface to 3rd Party Directory	Wait or Revisit approach	Revisit approach
Provisioning		
Cloud Applications	Migrate	Migrate
On-Prem Applications	Hybrid with Partner or Evaluate	Hybrid-Group write back with cloud sync, partner
Infrastructure		
Daemons & Services	Evaluate	Evaluate
Application Server Infrastructure	Evaluate	Evaluate (SaaS, PaaS)
VPN with RADIUS or PKI	Migrate	Migrate (Entra ID, NPS)
DNS / DHCP	Evaluate	**Migrate to networking platform**
Wi-Fi with RADIUS and PKI	Wait	Wait
Printing	Evaluate or Hybrid with Partner	**Migrate**
Governance		
Access Reviews	Migrate	Migrate
Access Requests	Migrate	Migrate

Users – Migration Pattern Guidance (Then & Now)

Scenario	2021 Recommended Pattern	2024 Recommended Pattern
Provisioning		
Cloud HR	Go Hybrid	Evaluate
Disconnected AD Forests to Entra ID	Evaluate	Evaluate
GAL Sync between Exchange deployments with disconnected AD forests	Wait	Evaluate (Cross Tenant Sync)
On-Premises HR	Wait	Evaluate (Entra ID API Provisioning)
External Identities	Migrate (consider AAD B2C)	Migrate (Entra ID external Identities)
Cloud-Only employees	Evaluate	Evaluate (Entra ID API Provisioning)
Groups		
Access	Go Hybrid	Migrate (Group Write back)
Collaboration	Go Hybrid	Migrate
Recertification of membership	Go Hybrid	Migrate (Access Reviews)
Distribution	Migrate	Migrate
Admin Management		
On-Premises Privilege Identities	Wait	Wait/3rd Party
Credential Management		
Passwords	Go Hybrid	Evaluate (Passwordless)
Certificates / Smart Cards	Wait or Evaluate FIDO2	Migrate (Entra ID Certificate AuthN)
Multi-Factor	Migrate	Migrate (Passwordless)

Devices - Migration Pattern Guidance

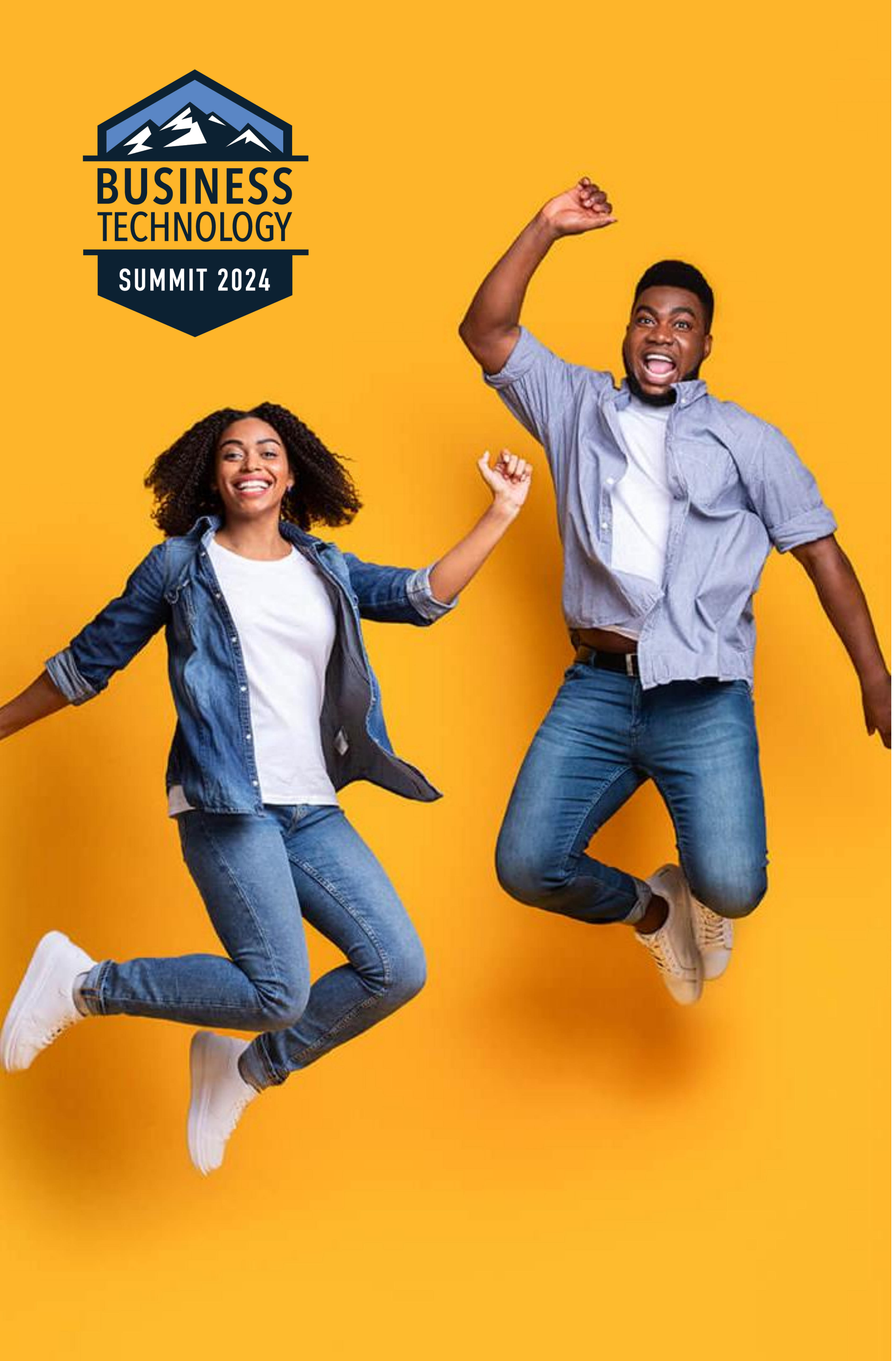
Area	2021 Recommended Pattern	2024 Recommended Pattern
Windows 10+		
Existing workstation	Go Hybrid	Migrate
New workstation	Migrate	Migrate (Web Authentication)
Virtual Desktop	Wait or Evaluate (Windows 365)	Migrate (Windows 365)
Privileged Admin Workstation	Go Hybrid	
Local Admin Management	Evaluate (LAPS lite approach)	Migrate (Windows LAPS to Entra ID)
Non Win10 Workstations		
Windows 7/8x	Revisit Approach	Revisit Approach
Windows Server OS (used as workstation)	Migrate	Migrate
MacOS	Migrate	Migrate (Native login today)
Linux/Unix workstation	Wait	Wait

Data - Migration Pattern Guidance

Area	2021 Recommended Pattern	2024 Recommended Pattern
File Shares		
User File Shares		Migrate to SPO/Teams
Application File Shares		Migrate to SPO/Azure Files
Virtual Desktop access to shares		Migrate (with VDI platform)
Database		
SQL		Evaluate
NoSQL		Evaluate

Summary:

- Migrate Data with source of access use case
- Consider governance and compliance implications
- Entra ID native Kerberos AuthN for Entra Joined device use case (Azure Files, SQL)



Call to Action

- JourneyTEAM offers a simple $3,000 ”Foundational Identity Assessment” of your environment.
- Helps you see where you are at today and what areas you can adopt and improve on in this journey.
- BTS participants will get 2 FREE FIDO2 Security keys when you commit to our Foundational Identity Assessment by end of day Friday March 1st.
  - Request through feedback survey…..

BUSINESS TECHNOLOGY

SUMMIT 2024

Feedback is a Gift

(And I love gifts ;-)

Please complete the session survey for **an extra giveaway raffle ticket!**

BUSINESS TECHNOLOGY SUMMIT 2024

Thank You!

Let's Connect:

Eric Raff

info@journeyteam.com