The Imperative to Modernize

Saying Goodbye to ADFS and Going Beyond AD

David Gregory

Director of Product Marketing

TJ Cutting

Sr. Identity Product Marketing Manager

What is your current stance on moving Identity and Access Management to the cloud?

1. Skeptical
2. Optimistic
3. Convinced

Reality Check

- **On-premises footprint is going to be around for a while**
  - Large surface area
  - Technical and non-technical challenges
  - Focus on breaking the surface area in smaller problems

- **The good news**
  - You can migrate a lot of identity functions to the cloud at your own pace… right now!

Benefits

Microsoft Entra expands beyond identity and access management

Better Security

- Better credentials: MFA, passwordless, modern password policies
- Modern Access Control
- Better signals to measure risk, based on AI/ML

Conditional Access

Identity Protection

Better Productivity

- Optimized for remote work
- Single Sign On across any user and any app
- Automated lifecycle management
- Self-service

Provisioning-Deprovisioning

Identity Governance

.. with better ROI

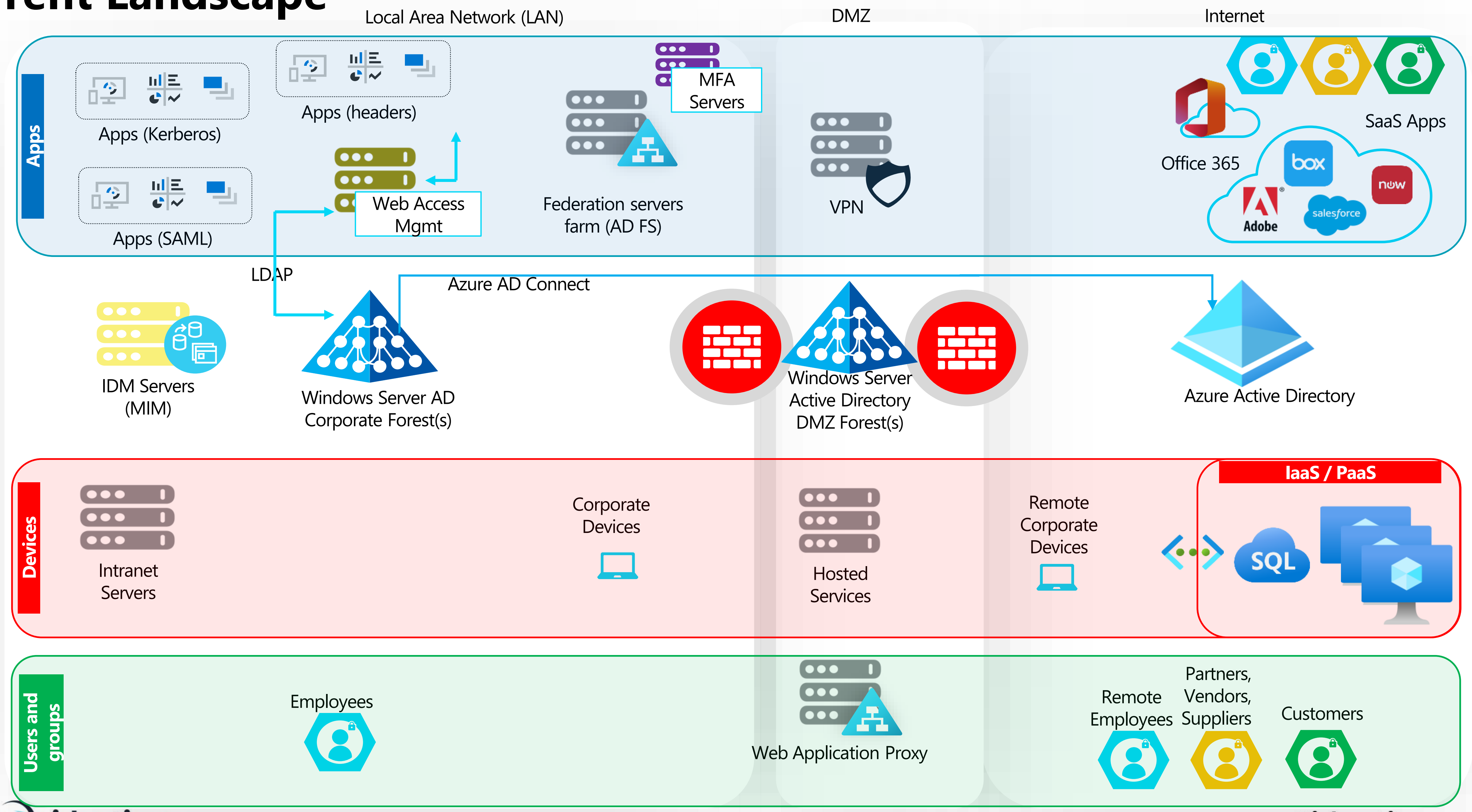
- Reduction of complex and costly 3rd party products and integration
- Reduction of the cost of procuring and maintaining aging infrastructure
- Shorter time to value

Retire Infrastructure

Resiliency

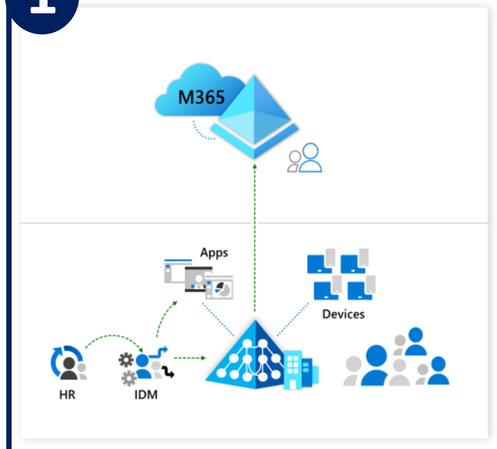
The Basics

Current Landscape

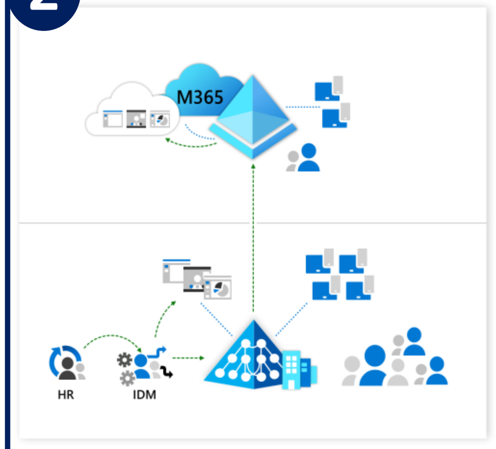


States of Transformation

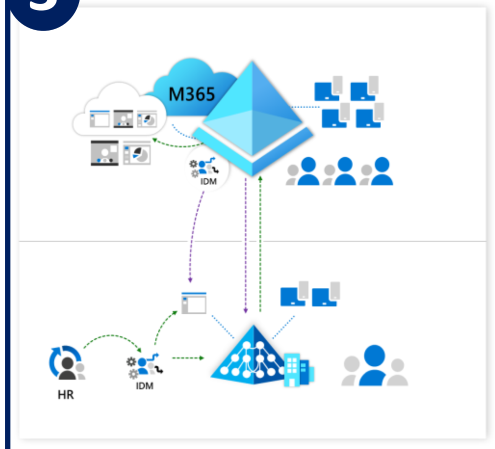
1 Attach to cloud



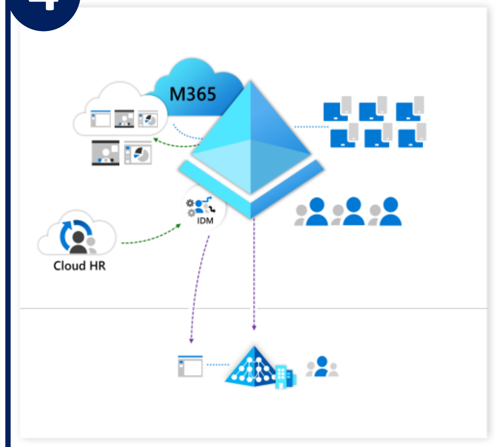
2 Get Hybrid



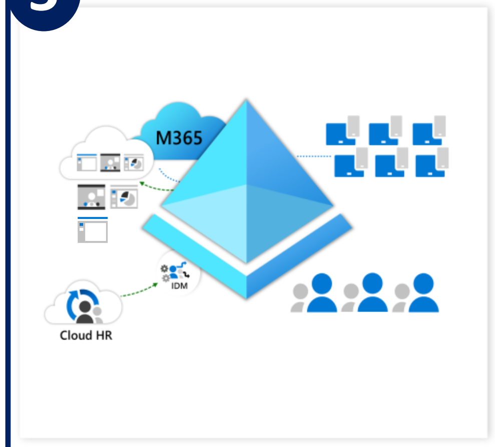
3 Decouple from on-prem



4 Cloud-Centric, AD minimized



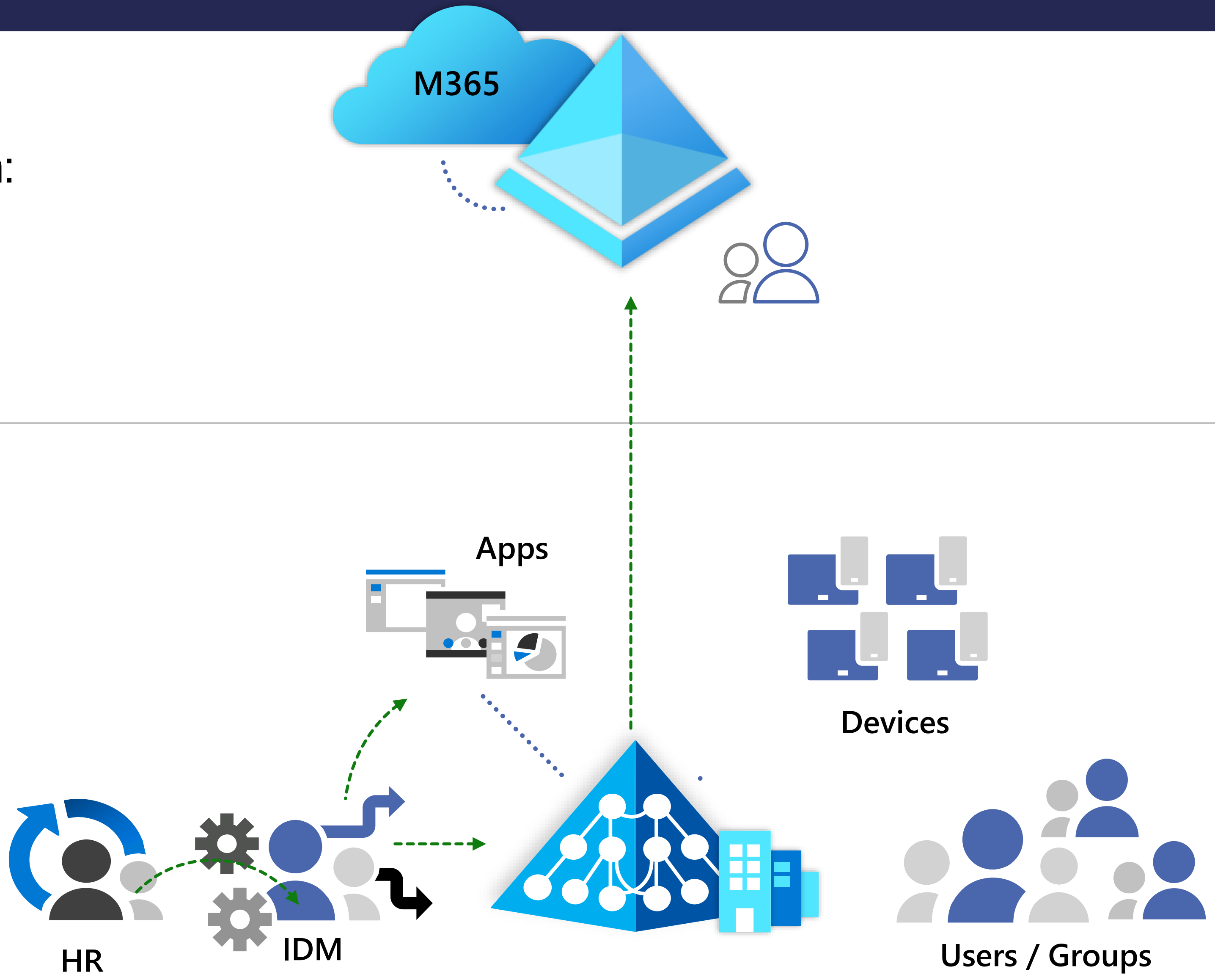
5 100% Cloud



1 Cloud Attached

Environment stays as-is, no transformation:

- Synchronization and hybrid auth established
- Goal is to enable workloads in the cloud

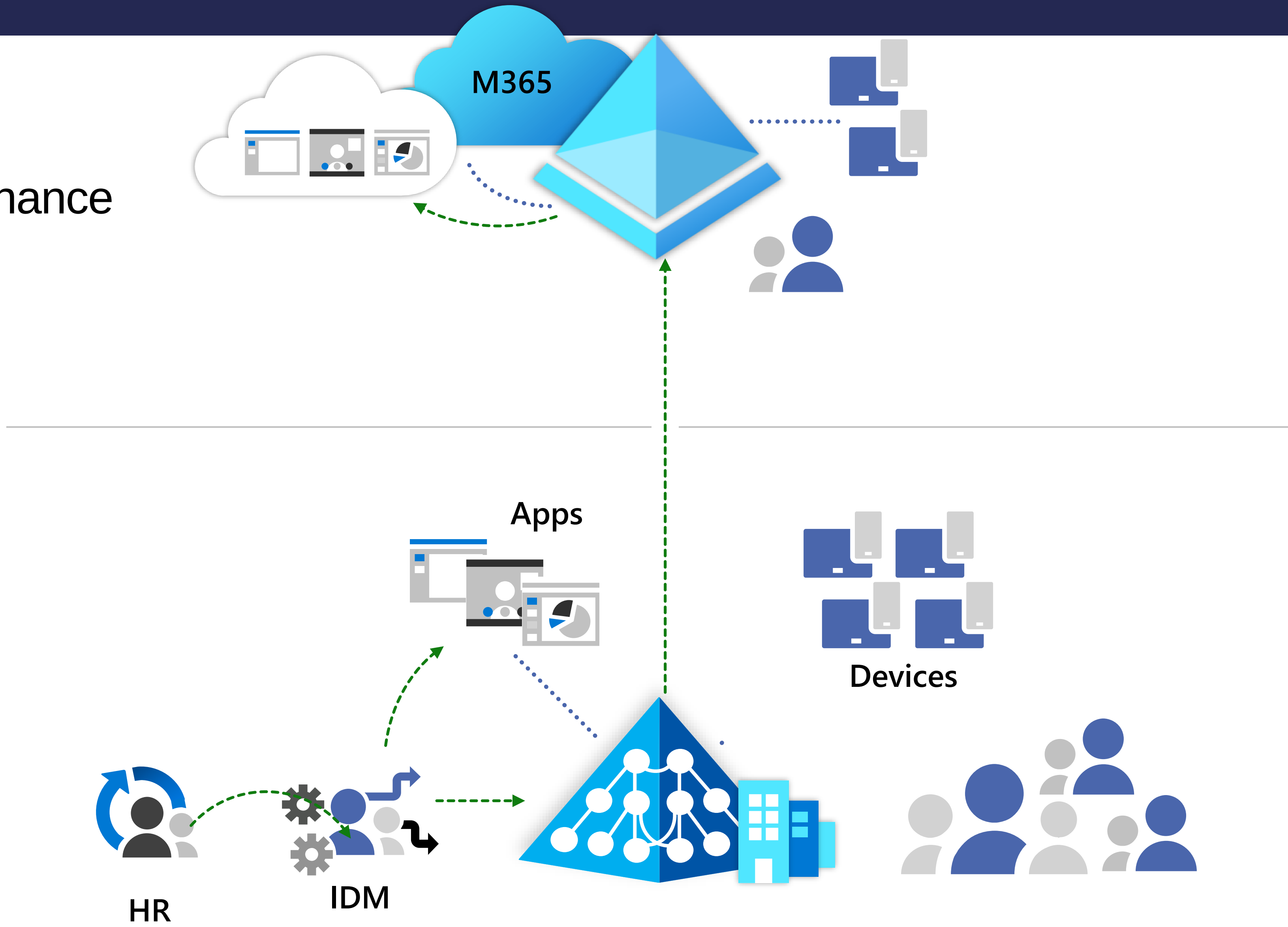


Key:
IDM: Identity Management System
HR: Human Resources System

2 Hybrid

IAM capabilities are enabled to enhance existing on-prem environment:

- Hybrid AD Join
- Password management
- App proxy

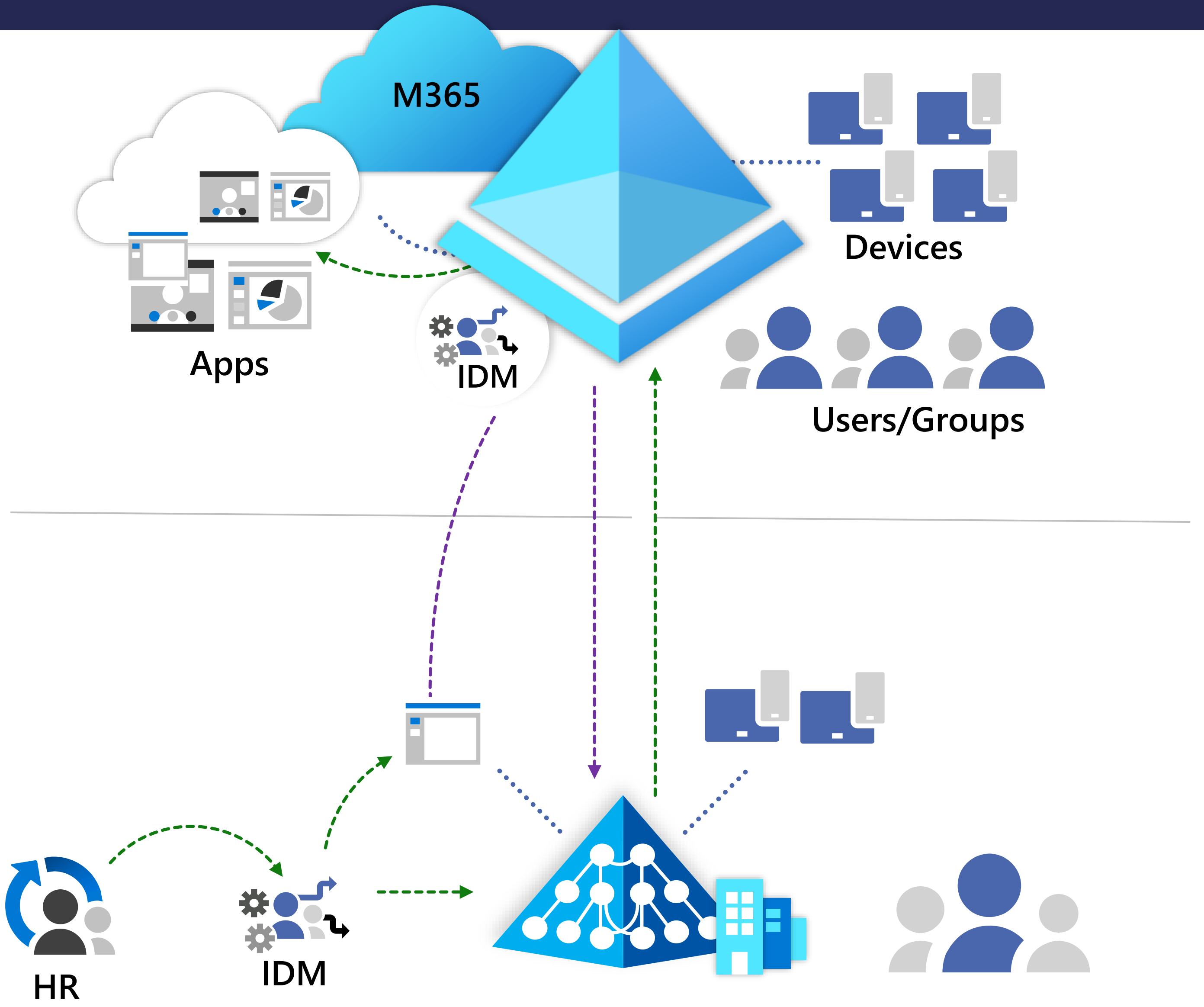


Key:
IDM: Identity Management System
HR: Human Resources System

3 Cloud First

Cloud native capabilities become the default:

- AD FS / other on-prem federation and WAM infrastructure deprecated
- New Windows devices Azure AD joined and managed with Intune
- App provisioning
- New groups are created in the cloud
- No AD accounts for externals

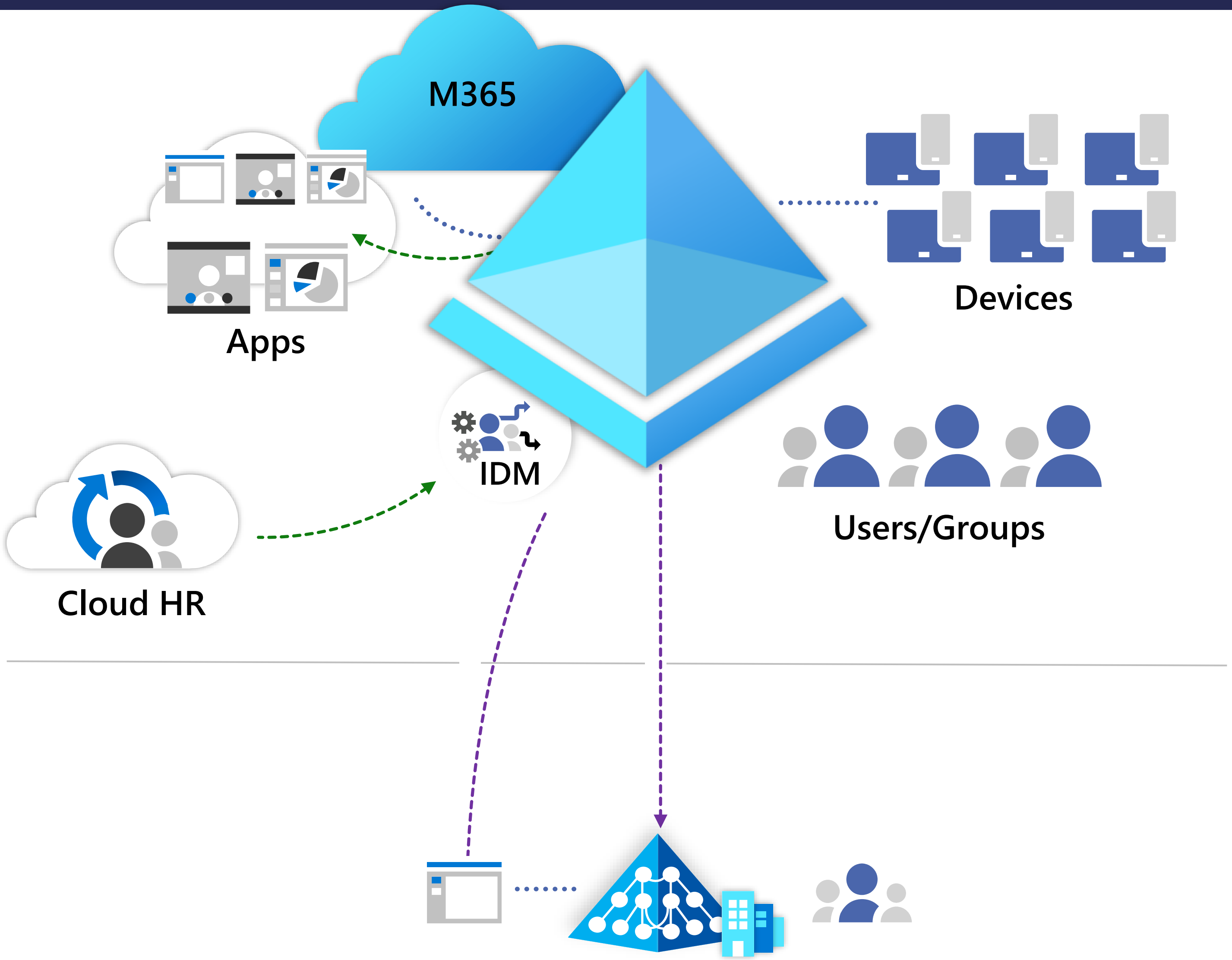


Key:
IDM: Identity Management System
HR: Human Resources System

4 AD Minimized

AD footprint is contained to a subset of legacy scenarios:

- New users are provisioned cloud-only accounts
- On-premises workloads replaced with cloud alternatives if available

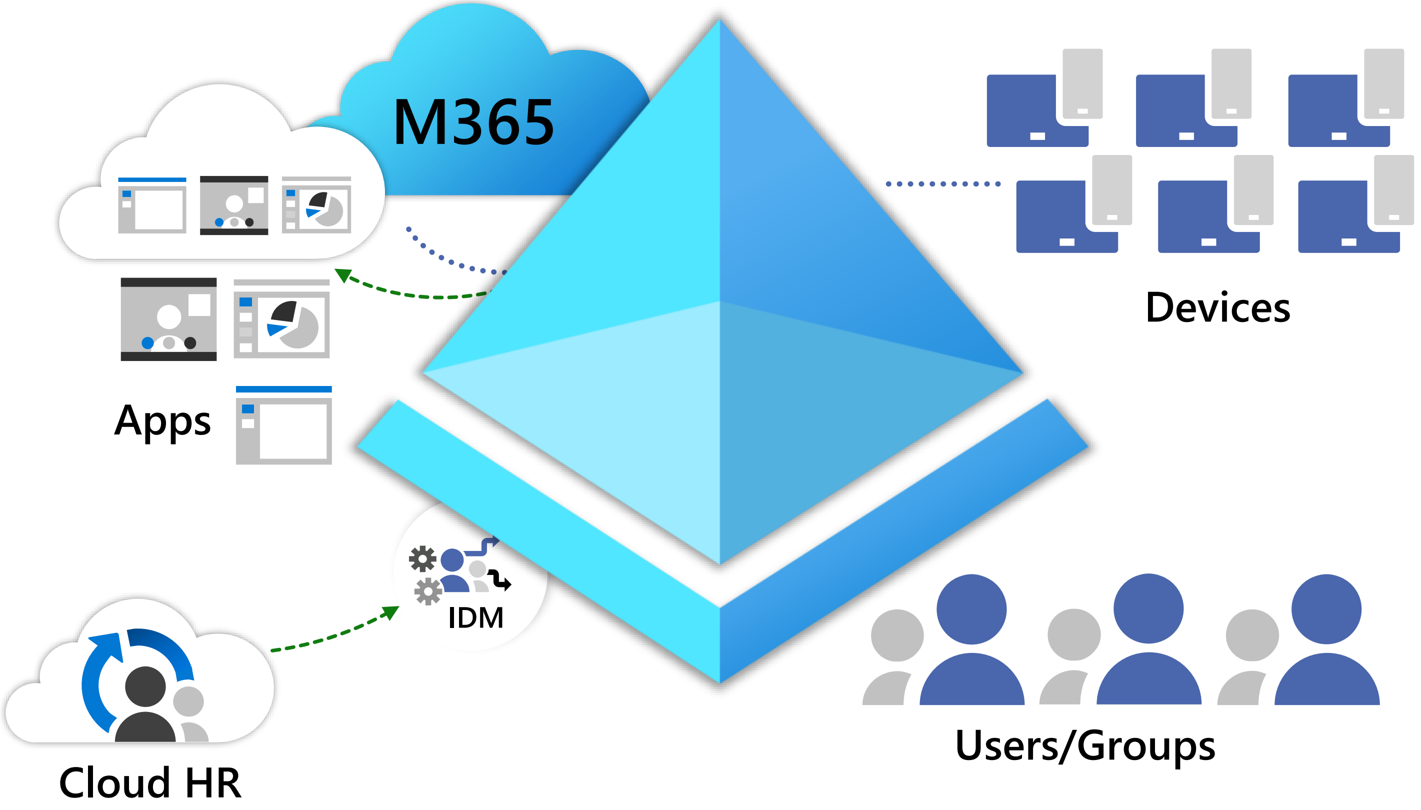


Key:
IDM: Identity Management System
HR: Human Resources System

5 100% Cloud

No on-premises IAM footprint:

- User identity lifecycle managed with Azure AD
- All users and groups are cloud native
- Relocate network services that rely on AD

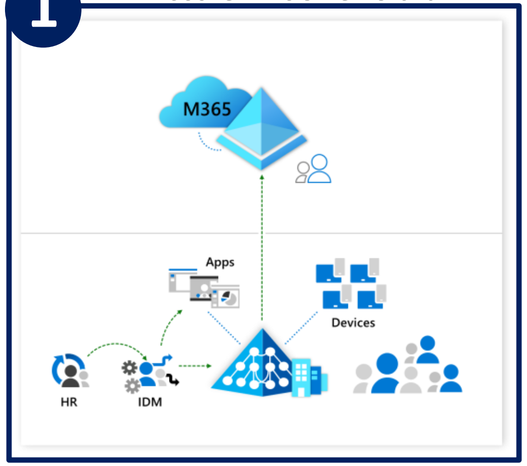


Key:
IDM: Identity Management System
HR: Human Resources System

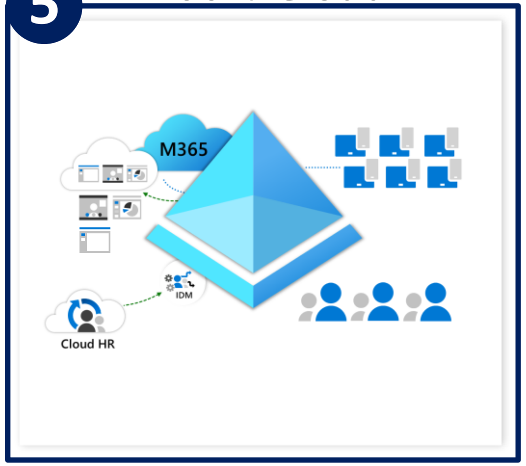
Note: *This stage includes Azure AD future investments.*

States of Transformation – A Journey

1 Attach to cloud



5 100% Cloud



Multi-Year Effort

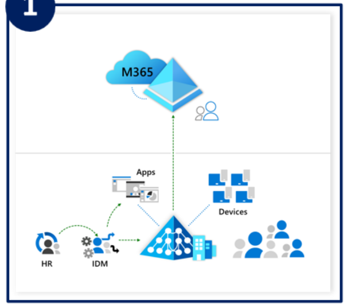
- For both you (adopt) and Microsoft (enhance the product)
- You will get value right now!
  - Don’t spend cycles w/on-prem clean ups
- Unknowns are expected

Azure AD is not “AD in the cloud”

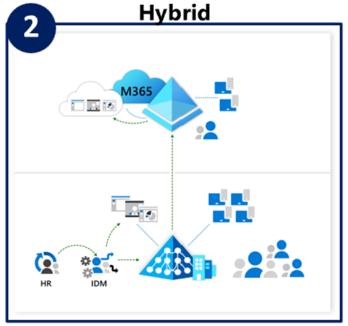
- Azure AD is an identity management system
- Focus on mapping requirements/outcomes, not features

Question

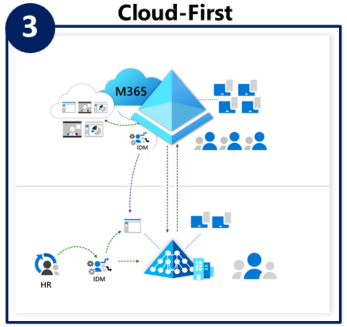
1 Cloud attached



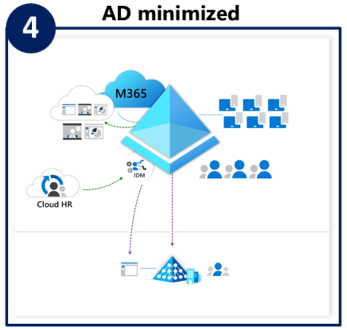
2 Hybrid



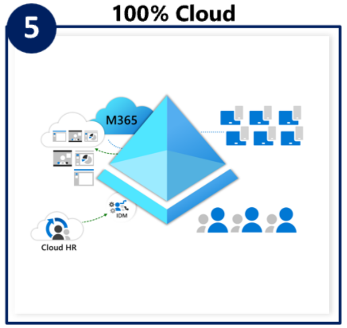
3 Cloud-First



4 AD minimized



5 100% Cloud



What state would you classify your organization today?

What state would you like to target?

Moving off AD is a long journey - not a sprint

When embarking on your journey

- Begin with the easy wins
- Inventory and plan for challenges
- Create project plans that include all stakeholders

Cloud First Approach

Cloud First Approach

Applications

App Buy / Build Guidance

- Prioritize cloud native alternatives with no on-prem infrastructure
- Require modern AuthN protocols (OIDC/OAuth2, SAML)
- Support modern provisioning (SCIM 2.0)
- No LDAP dependencies

Users/Groups

- Enrich user attributes in the cloud for
  - App provisioning
  - App authorization
  - Dynamic Group membership population
- Use External Identities for cross-company collaboration
- Use cloud groups for new app access
  - Dynamic group for automated group membership management
  - Self-service group management for user driven manual membership management
  - Evaluate Group Writeback for new groups that need to be on-premises

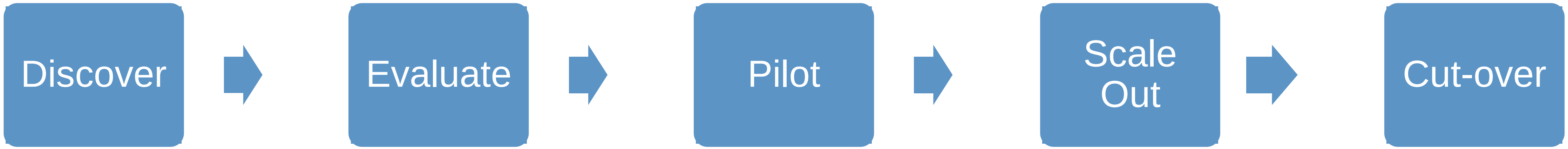
Devices

- Hybrid join existing domain-joined Windows clients
- Azure AD join for new Windows clients
- Apple SSO Extension
- Azure AD Passwordless
- Manage Windows clients with cloud-native unified endpoint management

  E.g., Microsoft Intune

  https://aka.ms/gpo2intune
- Autopilot to streamline device onboarding and provisioning

Migration Planning Framework



Discover

Evaluate

Pilot

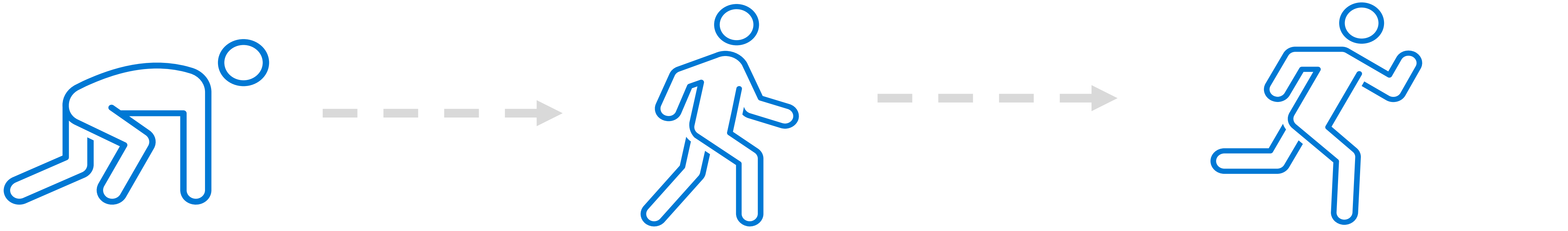
Scale Out

Cut-over

- Optimize for specific on-prem reduction goals
- Run multiple projects concurrently, based on your resources and change tolerance
- Identify and plan for dependencies between projects
- Project Management is key for success

Go-Dos

Read https://aka.ms/ad2azuread



One Month – Secure

Check your basics aka.ms/securitysteps and aka.ms/azureadsecops

Deploy Password protection

Turn on Password Hash Sync

Six Months – Transform

Azure AD Join new devices

Stop building/buying legacy auth apps

Deploy passwordless for privileged accounts

In Twelve Months – Scale

Scale out migration of modern auth apps to Azure AD

Scale out passwordless to all users

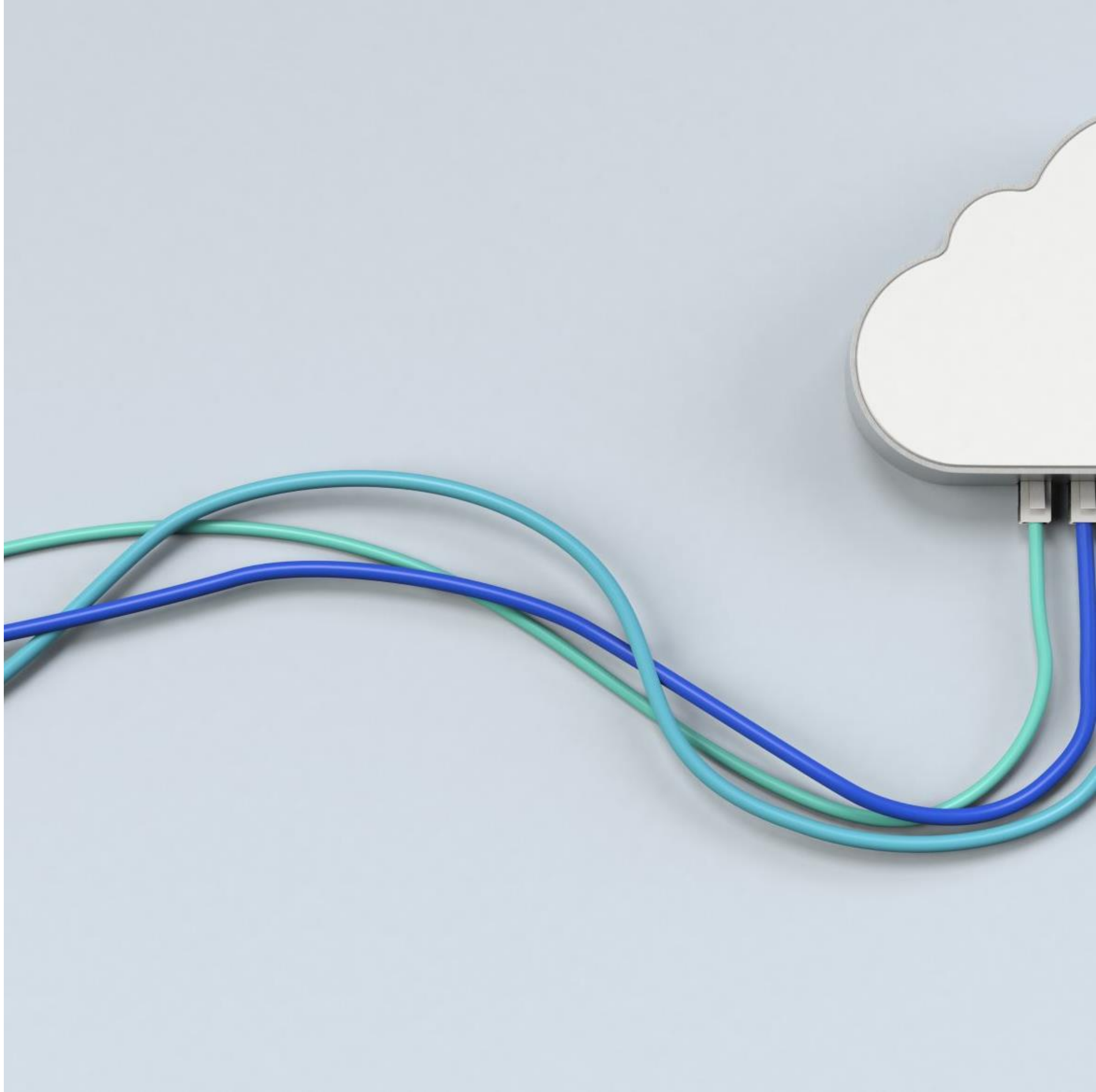
Organizations that pursue an all-in-one strategy to hybridization and eventual cloud migration of their enterprise directory will find Azure AD and adjacent Microsoft cloud technologies appealing.”

Gartner

“Active Directory in Transition” Report

AD Roadmap

- Focus of the team is around cloud investments to keep customers more secure against modern threats
- We are not deprecating AD at this time.
- Microsoft continues to fix security issues to keep you secure
- Go to the cloud!



THANK YOU!