IDENTITY DAYS

28 octobre 2021 - PARIS

@IdentityDays #identitydays2021

Merci à tous nos partenaires !

zscaler onelogin SailPoint METSYS Auth0 FUSION DIRECTORY

Microsoft Vorteks make IT work, make IT free

tenable yubico ManageEngine WALLIX CYBERSECURITY SIMPLIFIED Exakis Nelite Magellan Partners Alphorm.com

Un système d'information sans AD ?

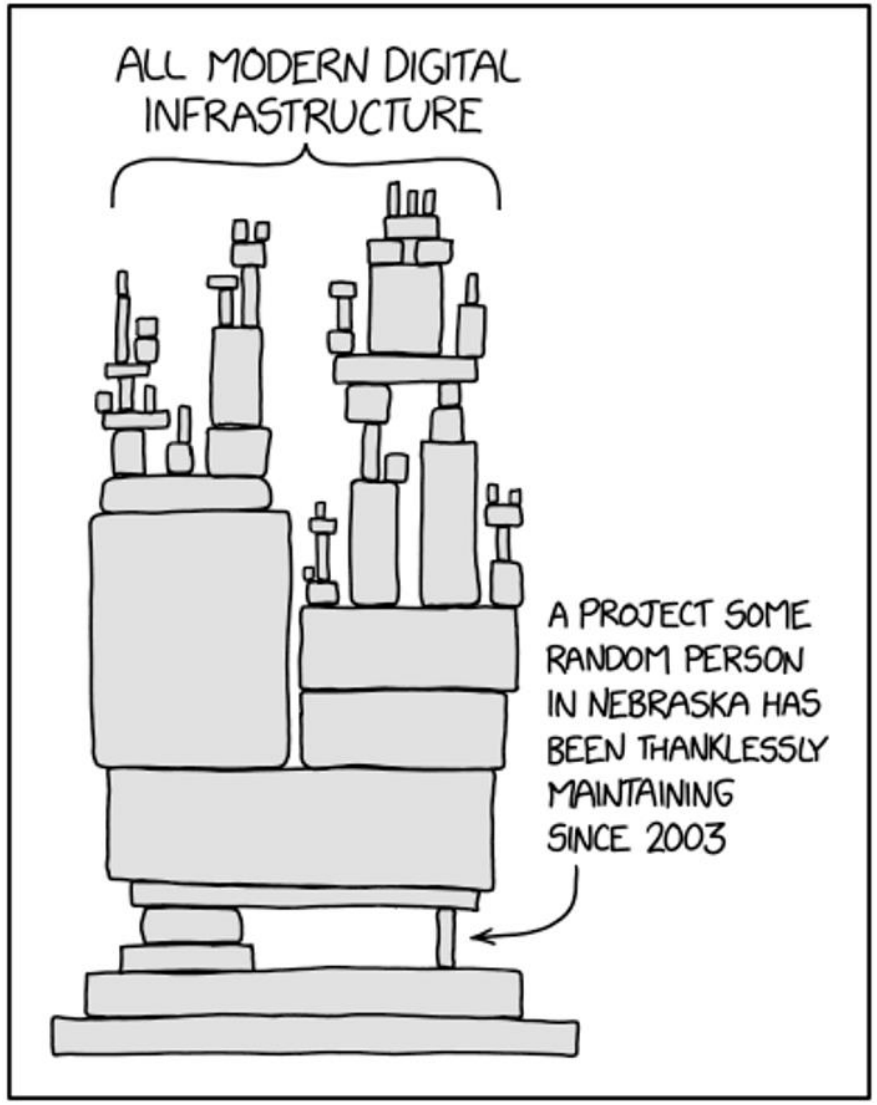
Guillaume Aubert
Yann Duchenne

Microsoft Security

Un système d'information sans AD ?

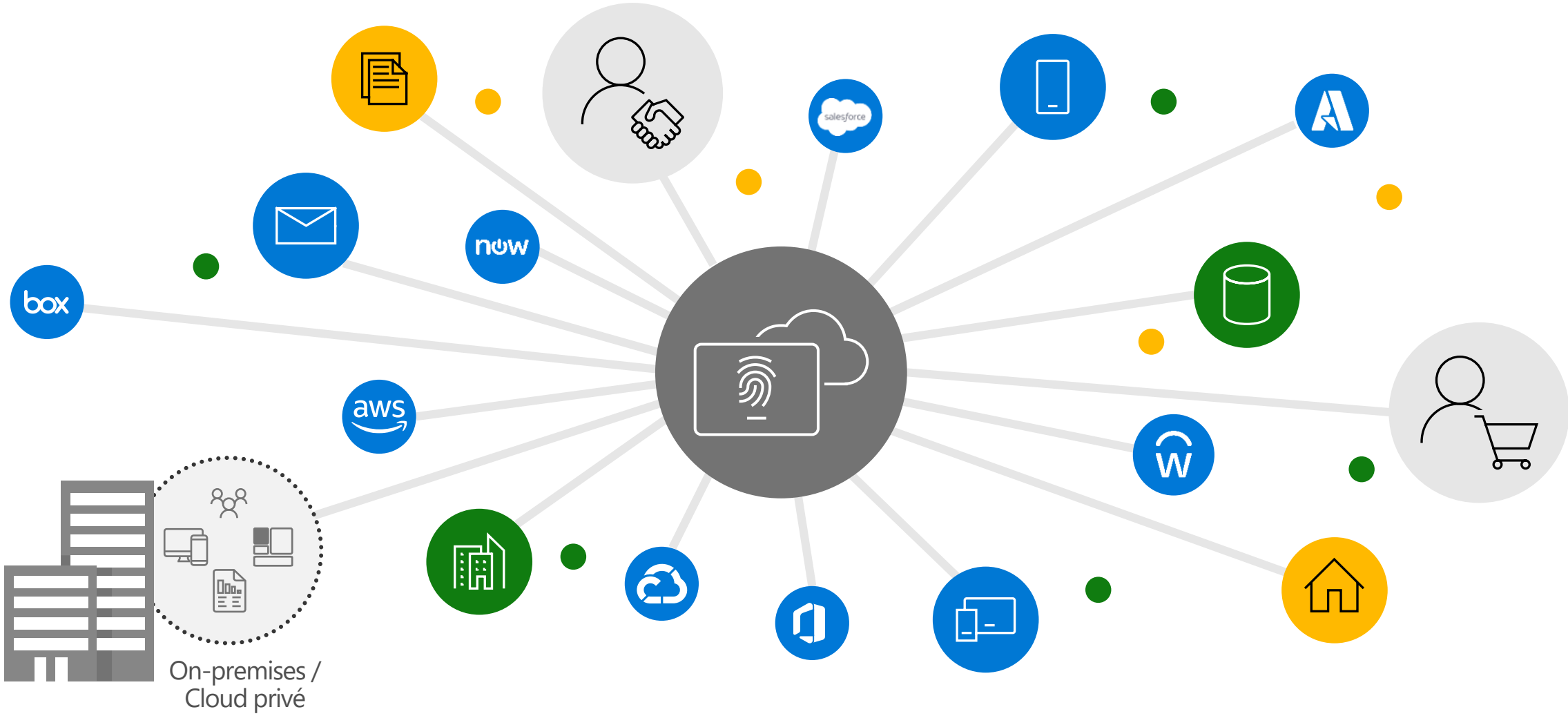
Guillaume Aubert – Security CSA
Yann Duchenne – Zero Trust GBB

Active Directory en 2021



Crédit:
https://xkcd.com/2347/

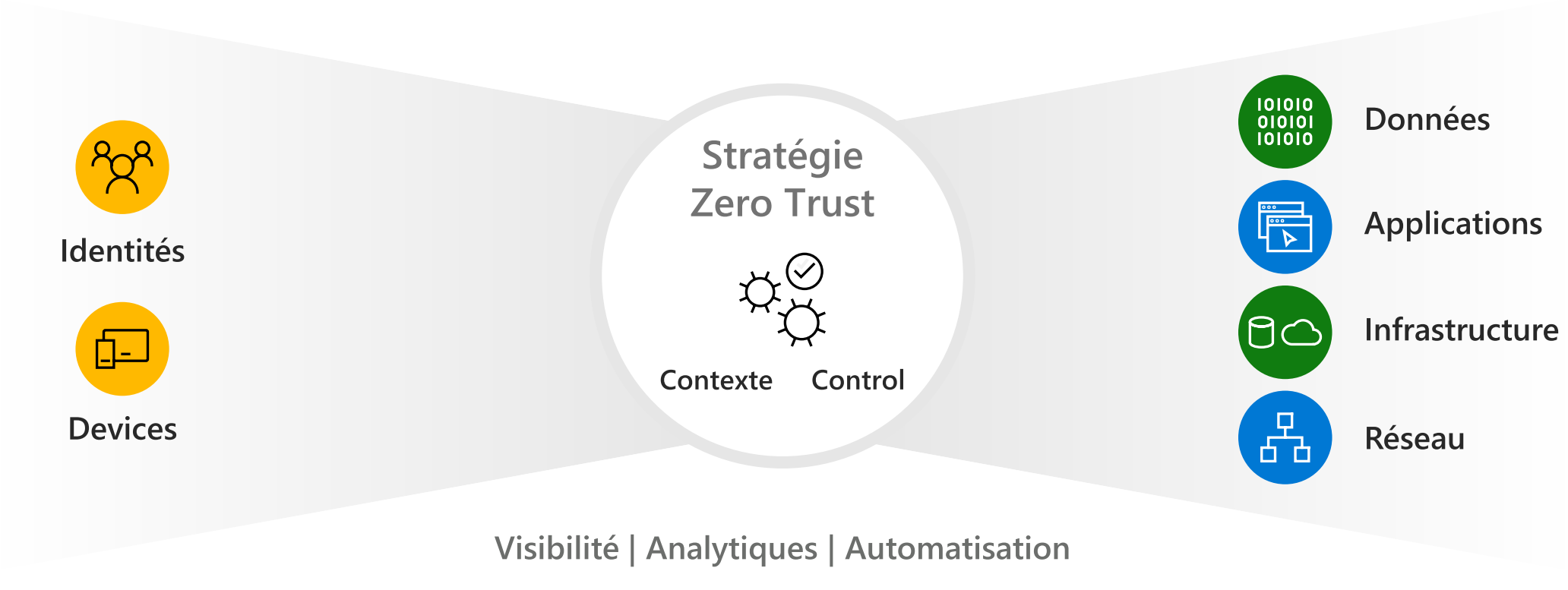
L’identité dans un monde connecté



Les principes d'une approche Zero Trust

Un cadre de sécurité moderne fondé sur l'identité

Vérifier explicitement | Limites les privilèges | Supposer la compromission



Quelques rappels utiles à propos d'Active Directory

Quels services rendent AD et Azure AD ?

Active Directory

- identités des utilisateurs
- identités des postes de travail
- identités des serveurs Windows
- configuration des postes et serveurs

Azure AD

- ~~AD dans le Cloud~~
- ~~IAM cloud pour les services Microsoft~~
- identités des utilisateurs
- identités des devices

Applications

Comptes de service

Service Principals / Managed Identities

Porte les protocoles :

LDAP, NTLM, Kerberos 5

OIDC/Oauth2, SAML, SCIM

Les challenges liés à l'AD

Historique et dette technique

- Avec souvent plus de 20 ans d'existence, AD charrie beaucoup **d'éléments historiques difficile à supprimer**
- Les **montées de version** d'OS des contrôleurs de domaines ne redéfinissent pas la configuration de votre annuaire
- Les **relations d'approbation** ne sont qu'un élément d'une problématique technique plus vaste

Sécurité

- L'AD est **une cible fréquente** (et souvent facile) **d'attaque**
- Le **durcissement** nécessite une analyse d'impact délicate
- Les **innovations sécurité** (i.e. protected admins, silos d'authentification, …) sont peu utilisées

Complexité et manque d'agilité

- L'héritage amène à des schémas de **permissions difficile** à comprendre et à gérer
- AD a toujours répondu difficilement aux scénarios de **fusions/acquisition et cessation**
- Les **migrations** sont complexes et couteuses

Manque de ressources et d'outils

- « **L'AD, ça fonctionne tout seul** » : équipes réduites et budgets limités
- Une **réelle expertise** est indispensable
- Les outils tiers peuvent aider principalement sur le monitoring et la détection mais pas sur **l'impact** d'activer ou désactiver des fonctionnalités (i.e. NTLM, LDAP signing, …)

Les opportunités offertes par Azure AD

La sécurité

- Accès conditionnel
- Identity protection
- Privileged Identity Management

MFA/ Passwordless

- Windows Hello
- Microsoft Authenticator
- FIDO2

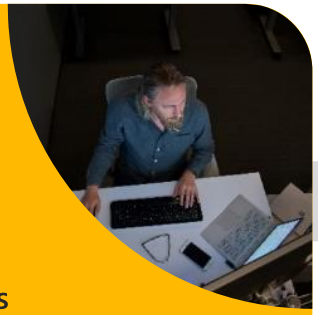
Collaboration Interne/externe

- B2B/B2C
- Teams/SharePoint
- Applications SaaS et maison

Modern Management

- Autopilot
- Microsoft Endpoint Management

Support des Architectures microservices

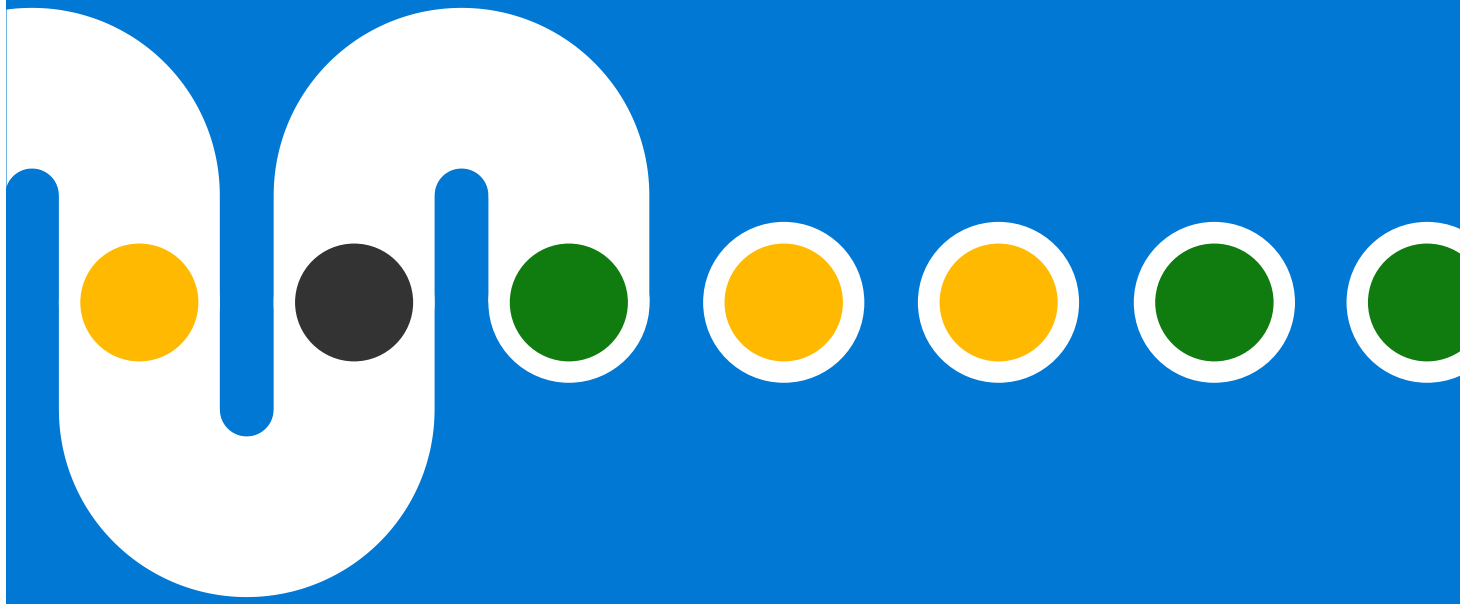


- Services Principals
- Managed Identities

Agilité

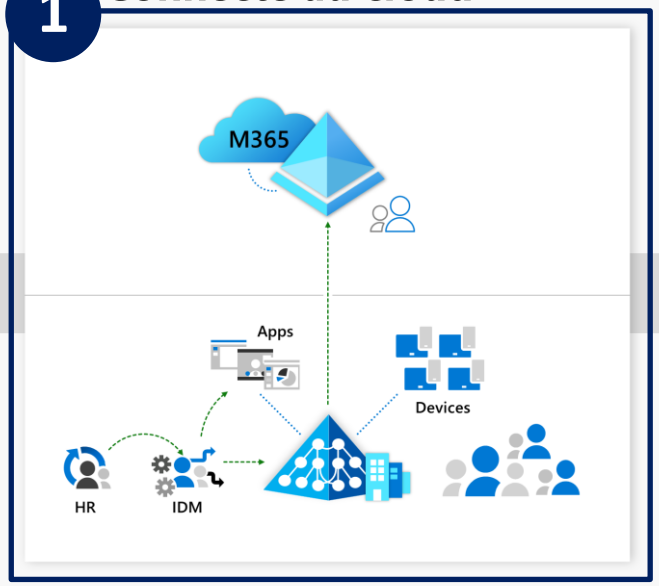
- Applications SaaS
- Services Cloud
- Firstline workers

A quoi pourrait ressembler cette transformation ?



Une proposition de feuille de route

1 Connecté au cloud

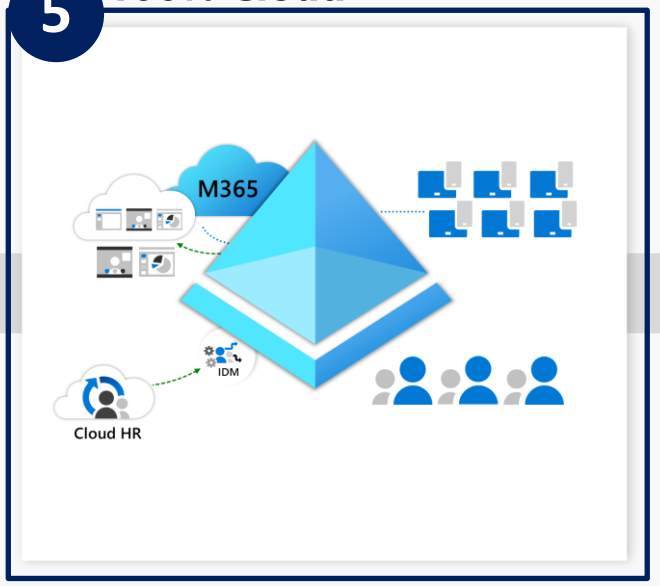


2

3

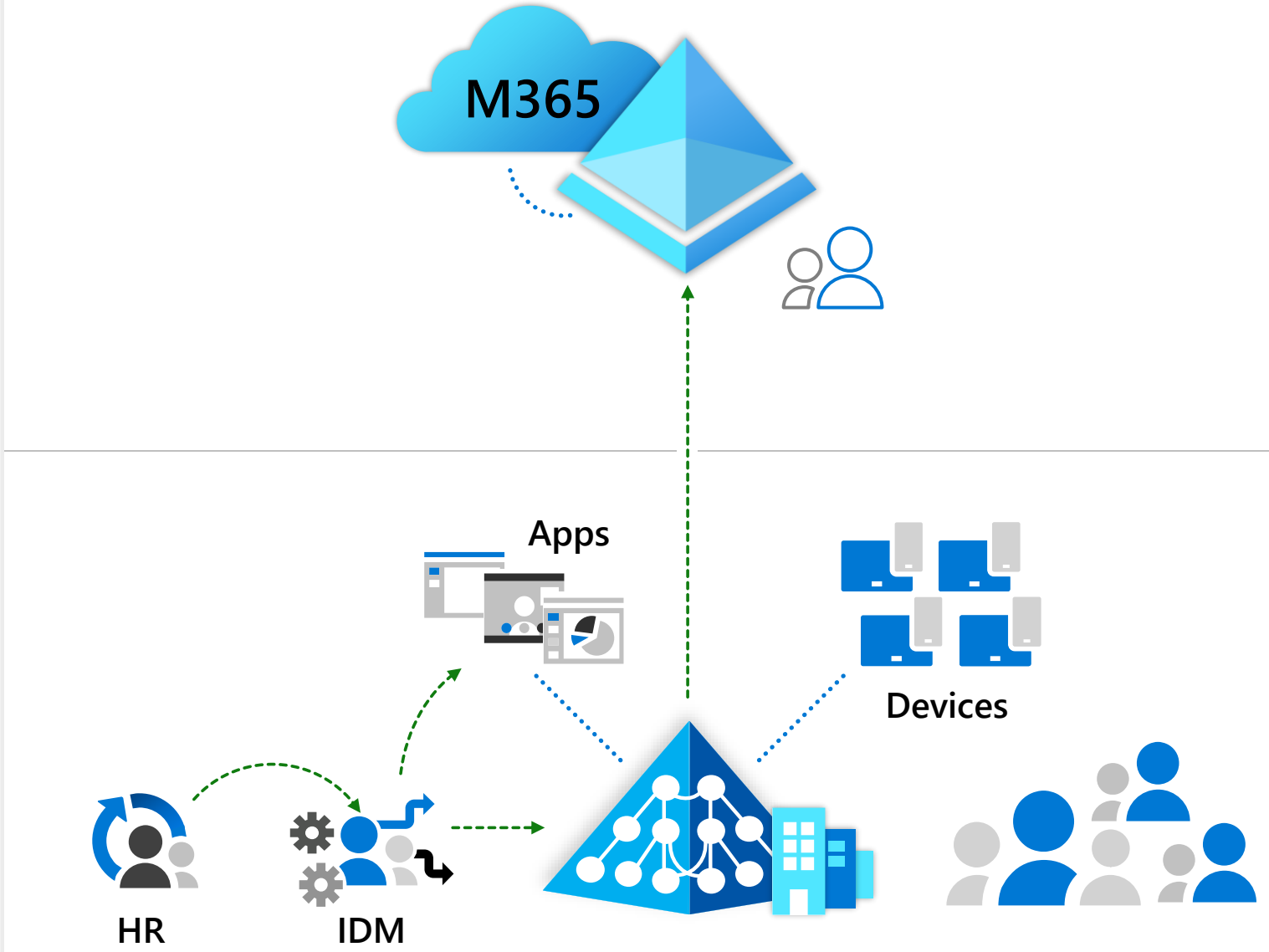
4

5 100% Cloud



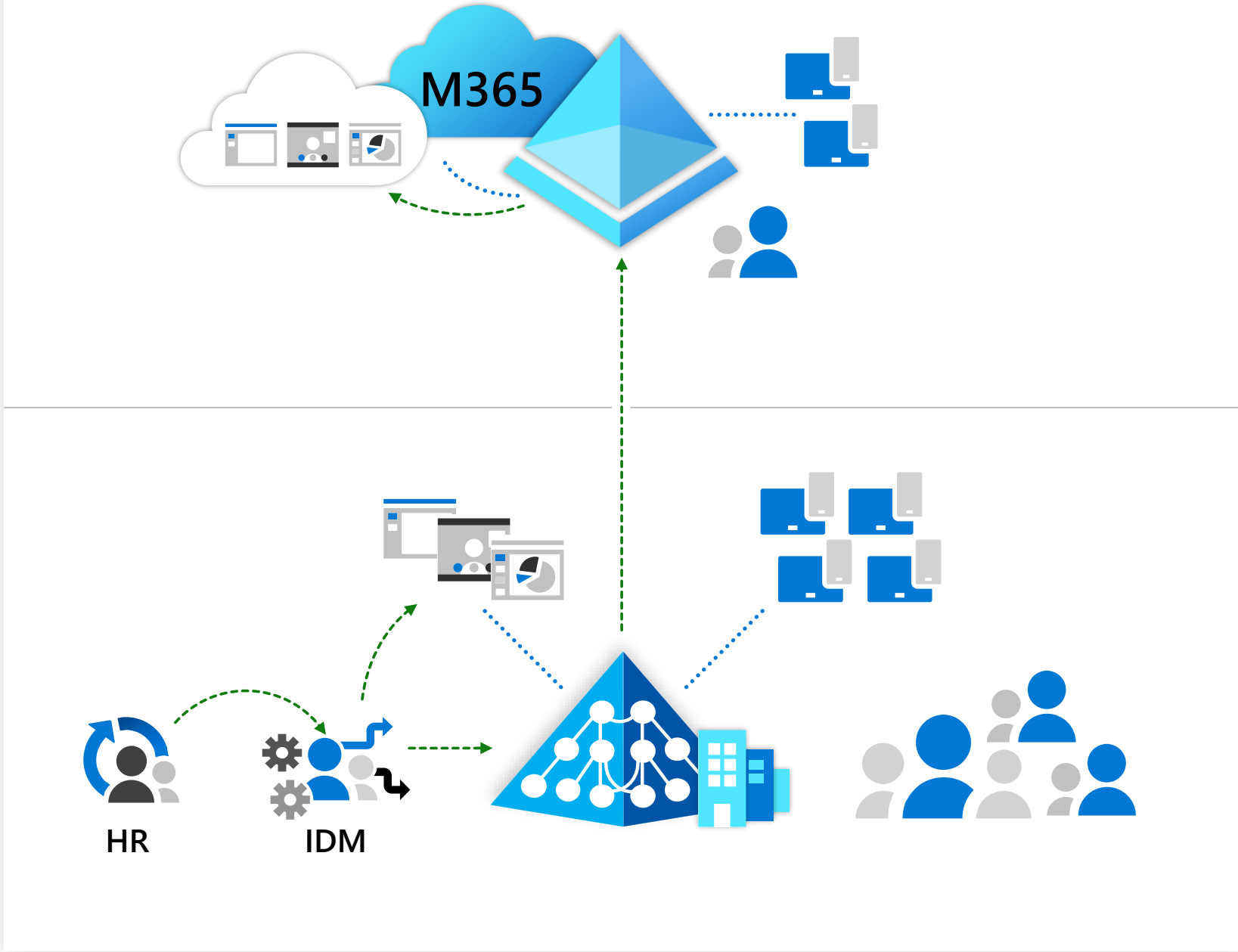
1 Connecté au Cloud

- Devices joints à l'AD
- Utilisateurs gérés dans l'AD, provisionnés par une solution IDM on-prem liée à la base RH
- Utilisateurs synchronisés vers le cloud pour Salesforce ou Office 365
- Applications basées sur l'authentification AD, ou serveurs de fédération (ex: AD FS, Ping Federate)



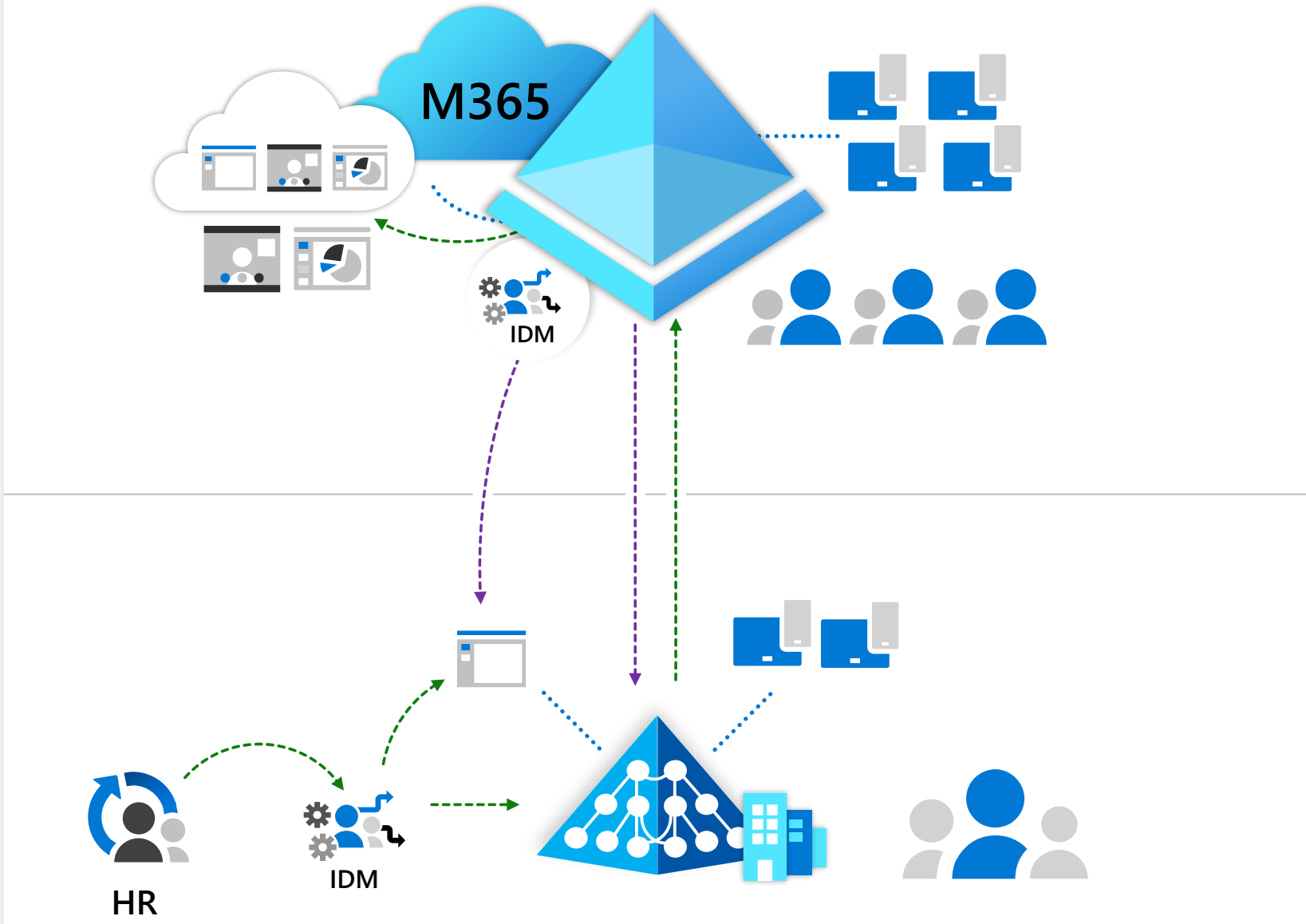
2 Hybridation

- Les devices deviennent “hybrid Azure AD joined”
- Des applications sont migrées dans Azure et utilisent Azure AD DS
- Les applications historiques sont “Saasifiées” grâce à Azure AD App Proxy (ou solutions partenaires)
- Services “Self-service” aux utilisateurs (Password Reset et Group Management)



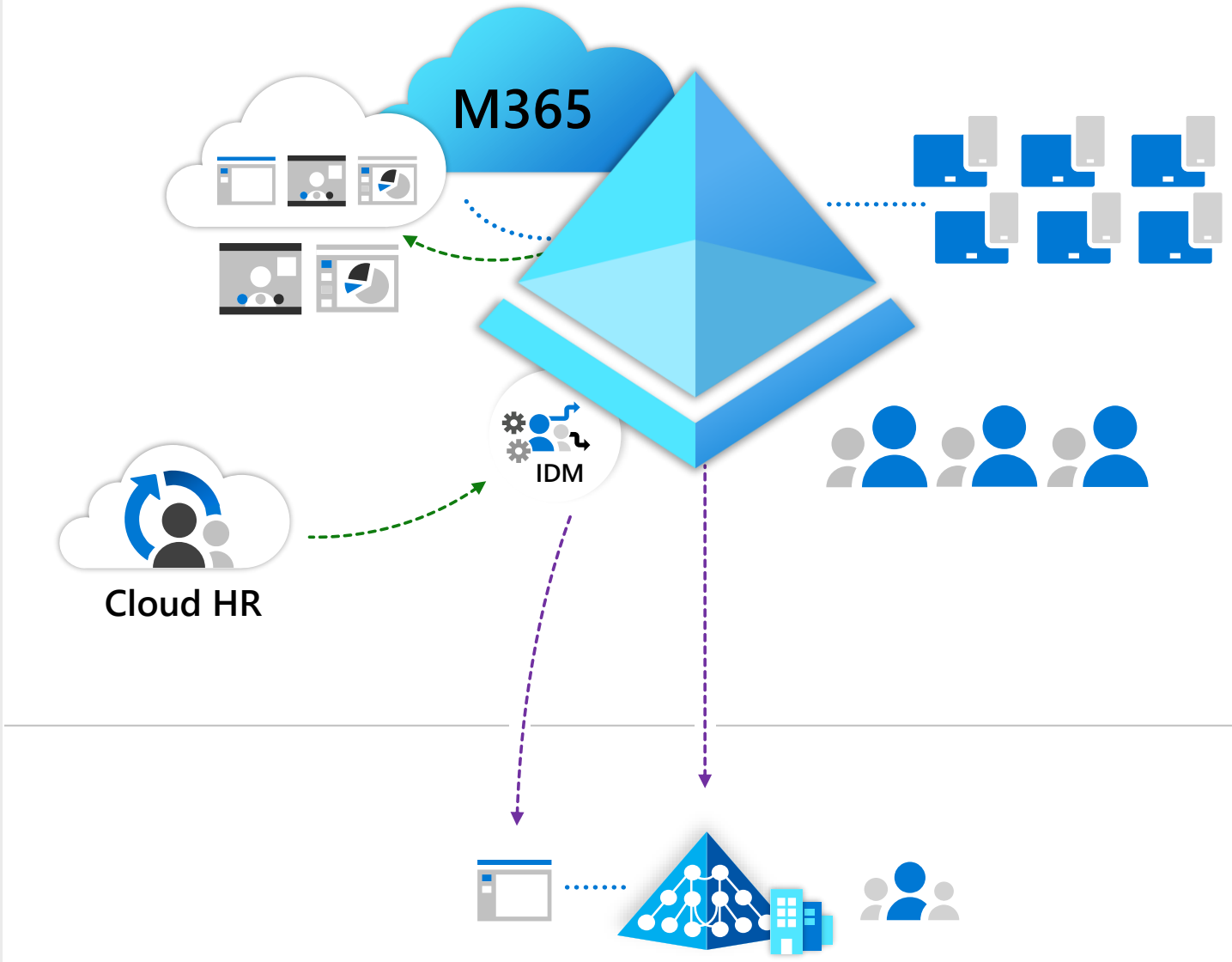
3 Dissociation cloud/on-prem

- Les nouveaux devices joints à Azure AD et gérés par MEM
- Les applications fédérées sont migrées vers Azure AD
- Les applications historiques peuvent fonctionner grâce à Azure AD DS et Azure AD Application Proxy
- Le réseau devient un simple accès internet, même au bureau
- Les serveurs de fichiers et d'impression migrent dans le cloud
- Azure AD B2B porte les besoins de collaboration
- Les connecteurs ECMA permettent un provisioning on-prem



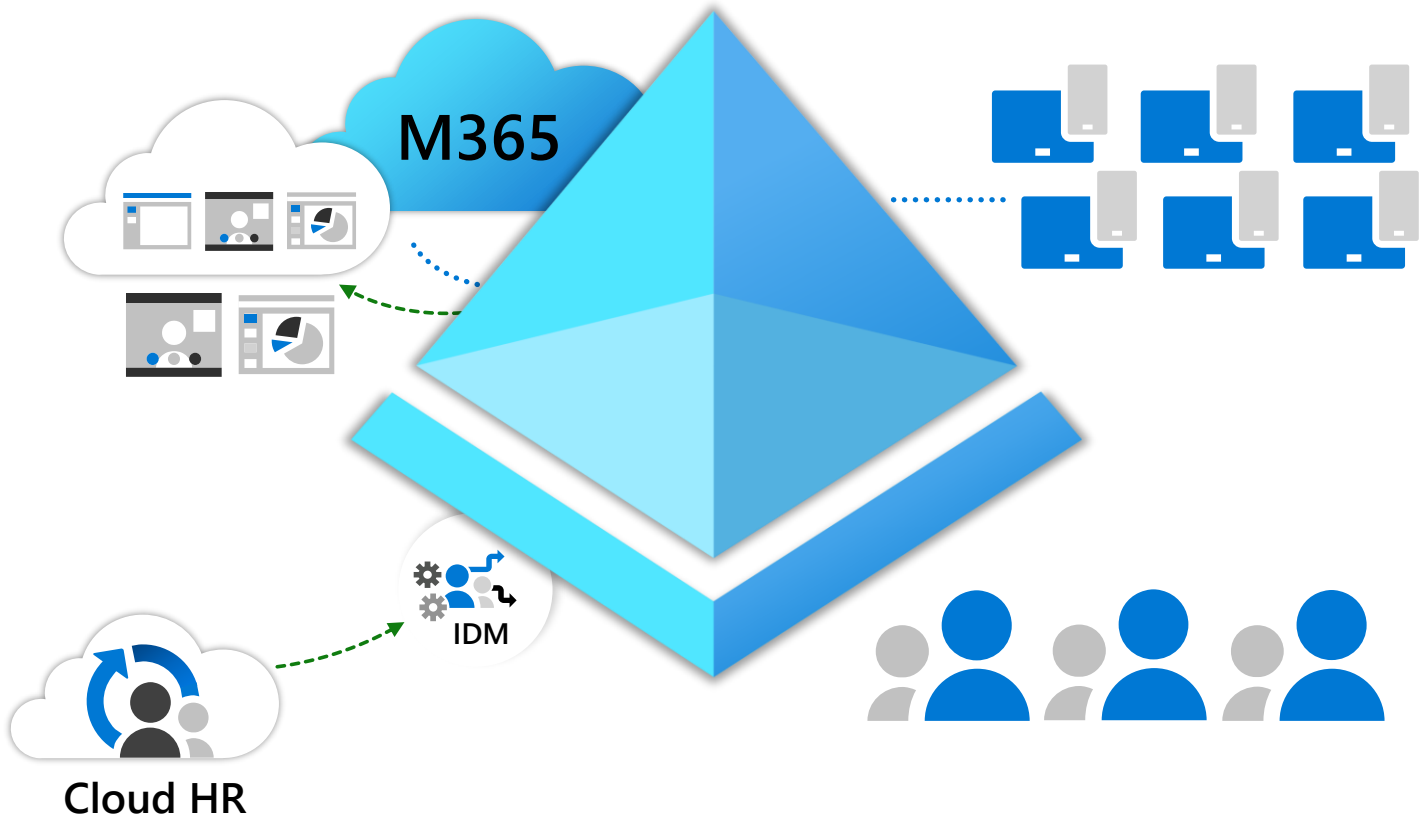
4 Cloud au centre, AD réduit

- La base RH passe en mode SaaS
- Les utilisateurs sont gérés dans le cloud — Réécriture on-prem si besoin
- Applications modernisées ou SaaS
- Les applications historiques peuvent fonctionner grâce à Azure AD DS et Azure AD Application Proxy
- Les derniers workloads on-premises sont migrés dans le cloud (Azure Virtual Desktop, Azure Files, Cloud Print, etc)



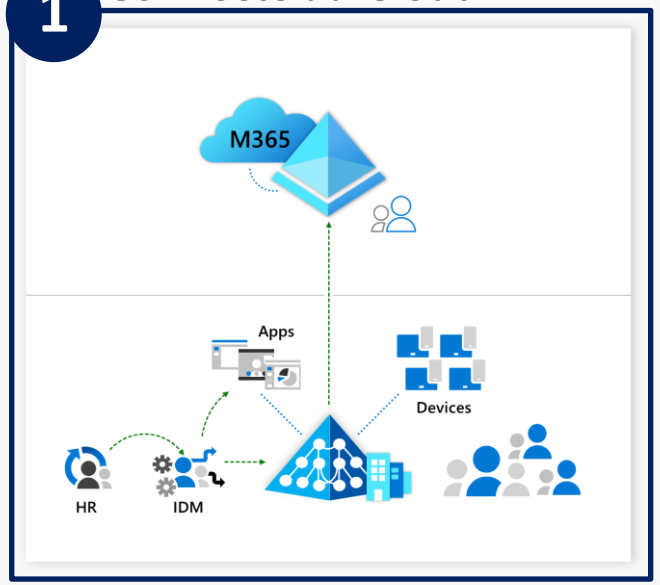
5 100% cloud

- Plus aucun IAM on-prem
- Azure AD porte toutes les fonctions de gestion des identités
- Toutes les applications ont été modernisées et reposent sur Azure AD
- Tous les devices sont en “modern management”

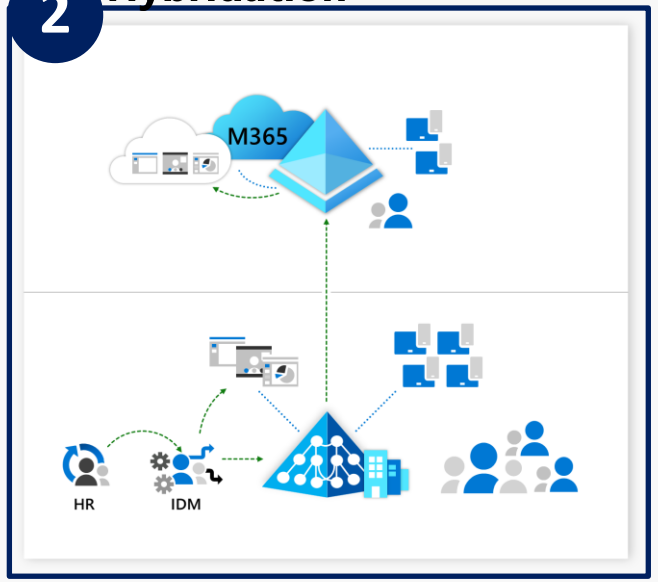


Une proposition de feuille de route

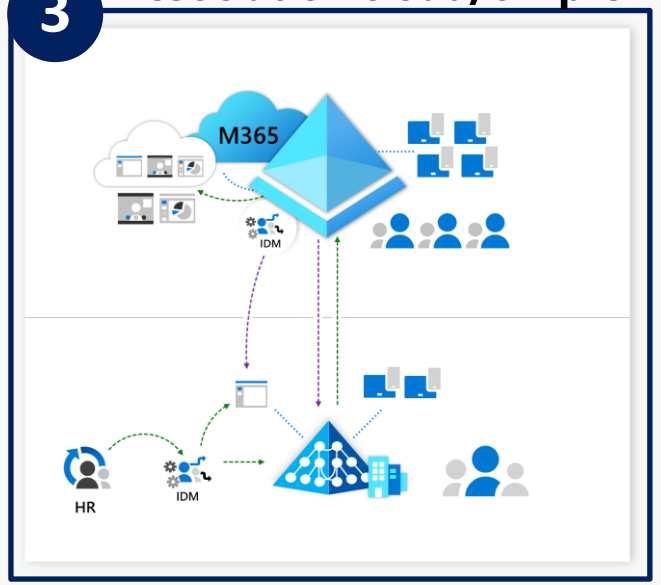
1 Connecté au Cloud



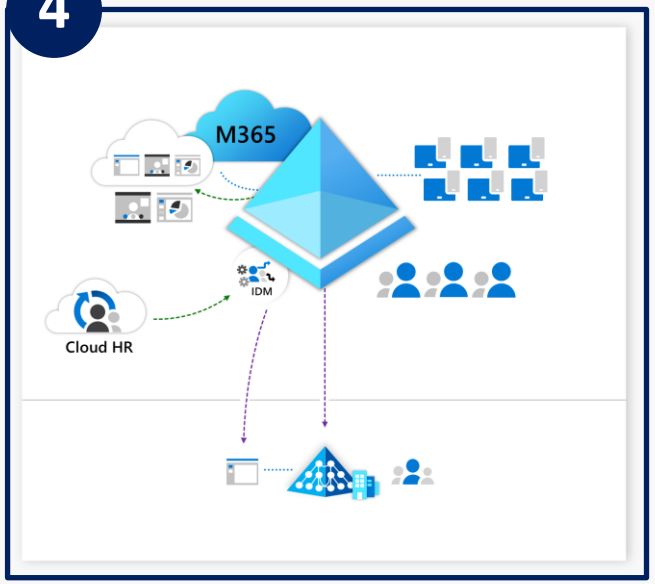
2 Hybridation



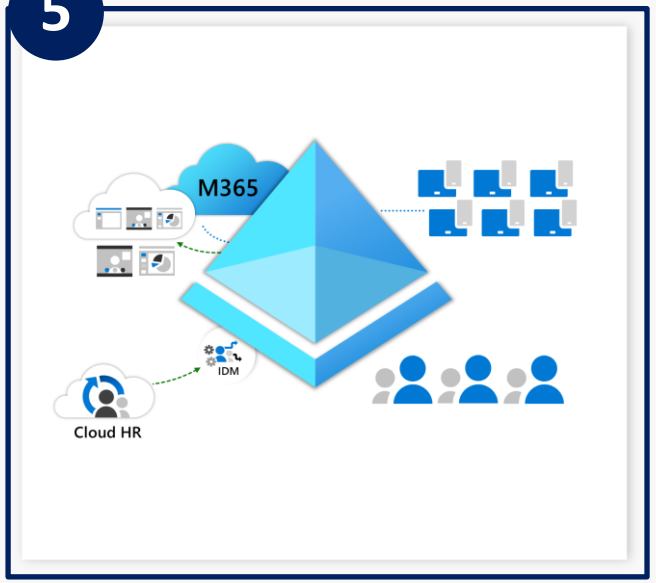
3 Dissociation cloud/on-prem



4 Cloud au centre, AD réduit



5 100% Cloud



Un projet irréaliste ?

MARC

Nouvel employé

- Collaboration
- Autopilot
- Modern Management

Etape 5

ALAIN

Ingénieur DevOps

- Collaboration
- Azure Devops
- Github
- Terraform

Etape 3

JAMES

Commercial à distance

- Collaboration
- CRM (Cloud)
- HR/Finance tools

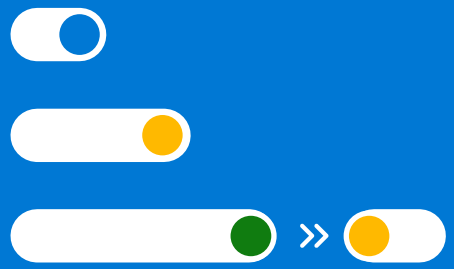
Etape 4

GREGORY

Data Scientist (stagiaire)

- Collaboration
- Azure
- Data sets
- Jupiter Notebooks

Etape 5



Cadre de sécurité modern aligné sur les principes du Zero Trust

Quelques recommandations

A-t-on encore besoin d'Active Directory ?

…mais il restera un composant clé de vos SI pour encore quelques années
le cloud vous permet dès à présent de réduire son emprunte

AD répond mal aux **nouveaux usages** et aux **exigences modernes de sécurité …**

Tant qu'il est présent, **la sécurité de l'AD doit rester une priorité**

La voie du succès :

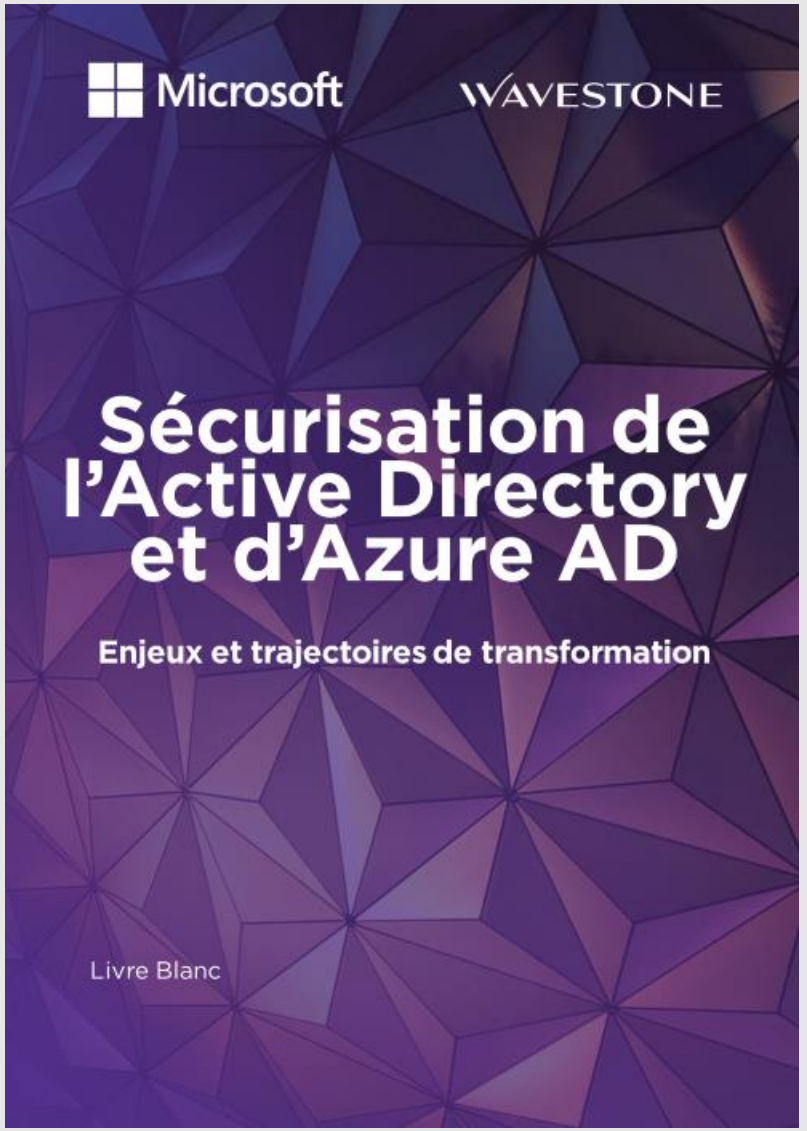
- Think big
- Start small
- Move fast

Qui vous permettra un jour d'exécuter cette commande:

Apocalypse-now.ps1

```
PS C:\Users\admin> Uninstall-ADDSDomainController
-LastDomainControllerInDomain -LocalAdministratorPassword
(ConvertTo-SecureString -AsPlainText "p7t$/CIT}NV^t:!" -Force)
-RemoveApplicationPartitions
```

Merci a tous!



Publication conjointe de Microsoft et Wavestone