# 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

# Gardez le contrôle avec Azure AD Conditional Access

Xuan AHEHEHINNOU
& Hakim TAOUSSI

# AGENDA DE LA CONFÉRENCE

Xuan AHEHEHINNOU

**Microsoft 365 Solution Architect**
Abalon

Hakim TAOUSSI

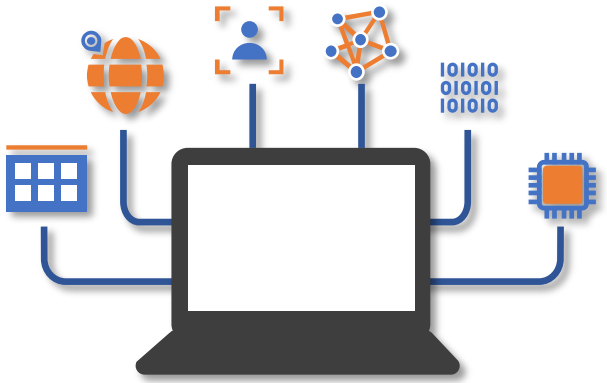
**Senior Architect /**
**MVP Office Apps & Services**
Insight

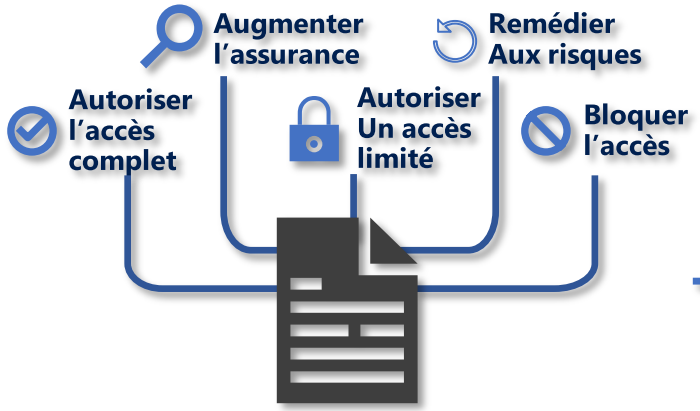
- Vue d'ensemble
Azure AD Conditional access

- Cas d'usage
Les stratégies les plus pertinentes pour sécuriser les accès

# Vue d'ensemble
# Azure AD Conditional access

# Vue d'ensemble Conditional Access






## Signal

*pour prendre une décision éclairée*

**Risque Appareil**
- Gestion des appareils
- Détection des menaces
- et plus encore...

**Risque Utilisateur**
- Authentification multifacteur
- Analyse du comportement
- et plus encore...

## Décision

*en fonction de la politique de l'organisation*

**Evaluation des demandes entrantes**

**Réévaluation pendant la session**

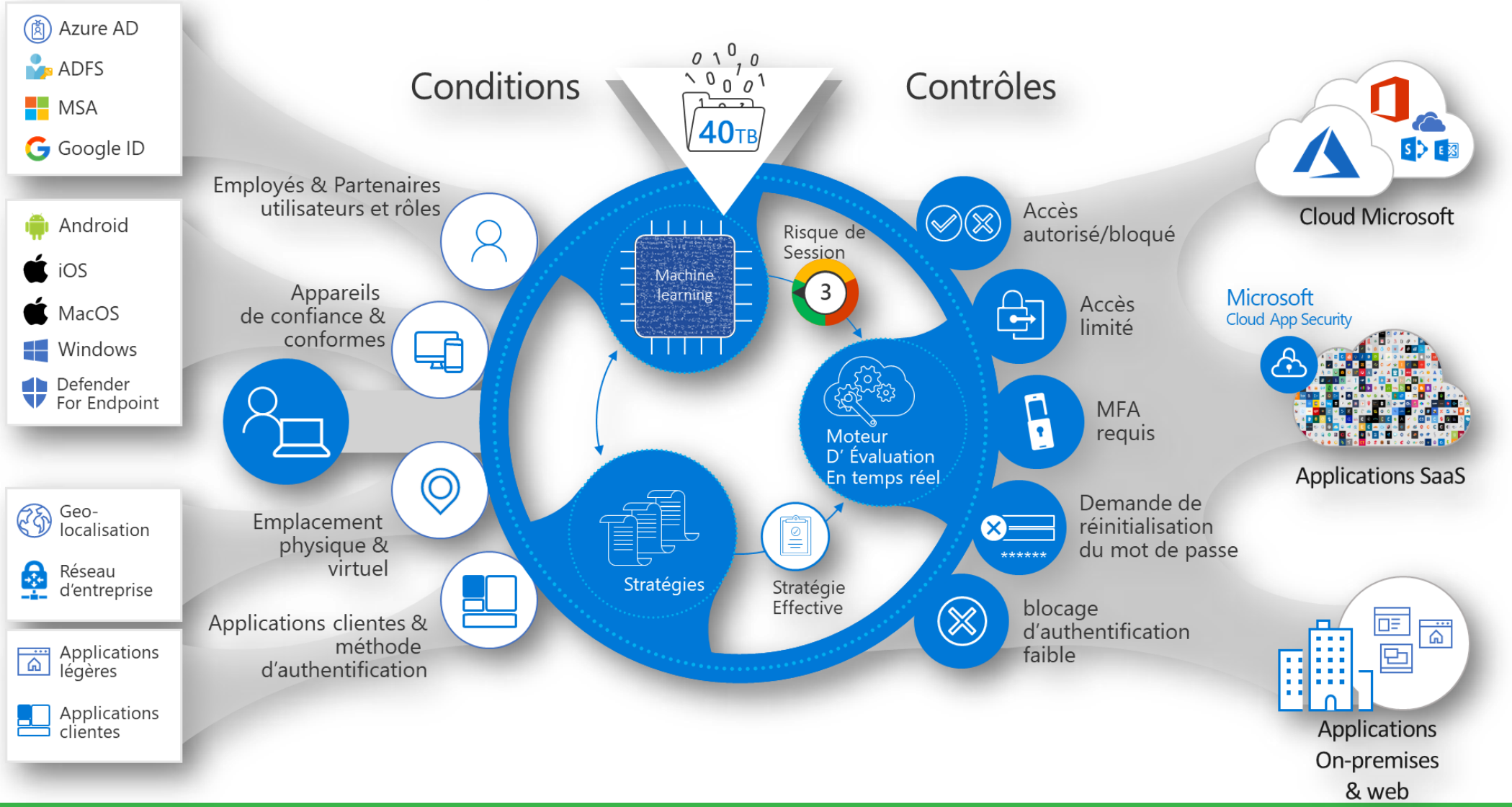
## Application

*de la politique sur l'ensemble des ressources*

**Applications Modernes**
**Applications SaaS**
**Applications Legacy**
**Et plus encore...**

# Vue étendue

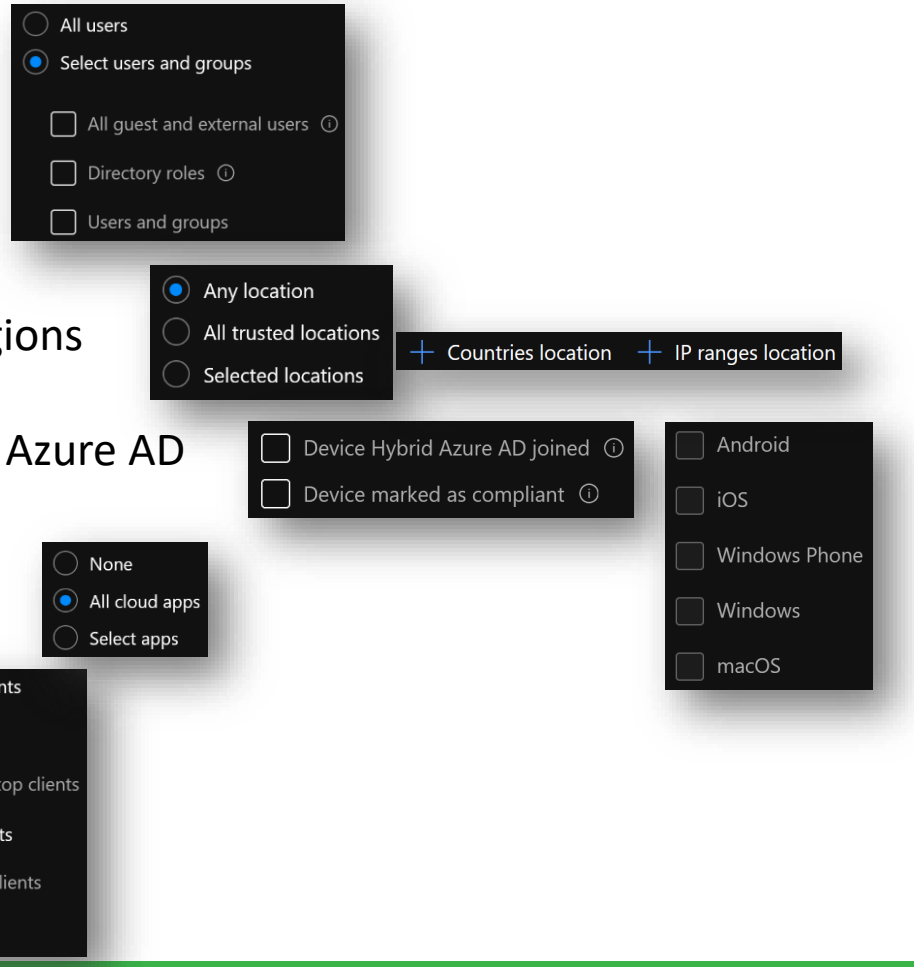
# Conditional Access



# Fonctionnalités Conditional Access

## Signaux basiques

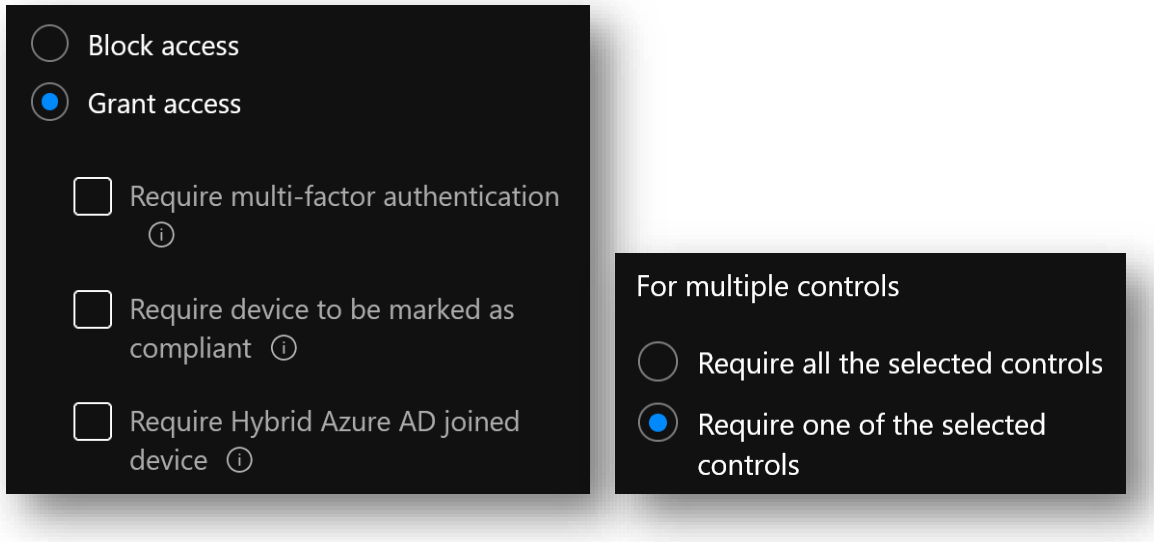
- Utilisateurs, groupes spécifiques, rôles spécifiques
- Emplacements réseau : plages d'adresses IP, pays/régions
- Etat de l'appareil : plateforme, conformité, jointure à Azure AD
- Ensemble des applications, applications spécifiques
- Application cliente : moderne, legacy



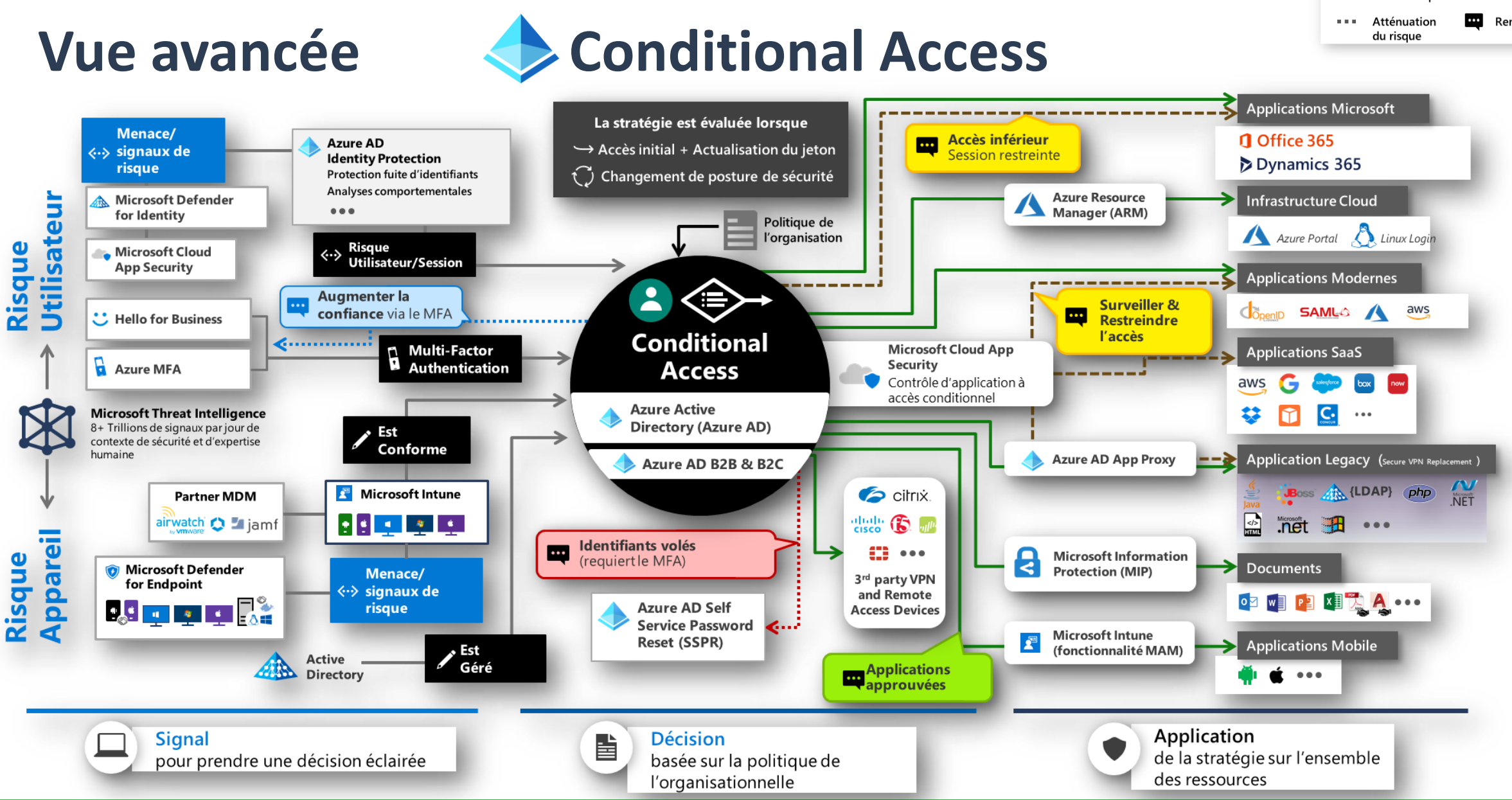
# Fonctionnalités Conditional Access

## Décisions basiques

- Bloquer l'accès
- Autoriser l'accès
  - Exiger le MFA
  - Exiger la conformité de l'appareil
  - Exiger que l'appareil soit joint à Azure AD



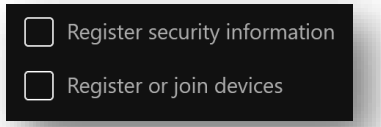
# Vue avancée Conditional Access



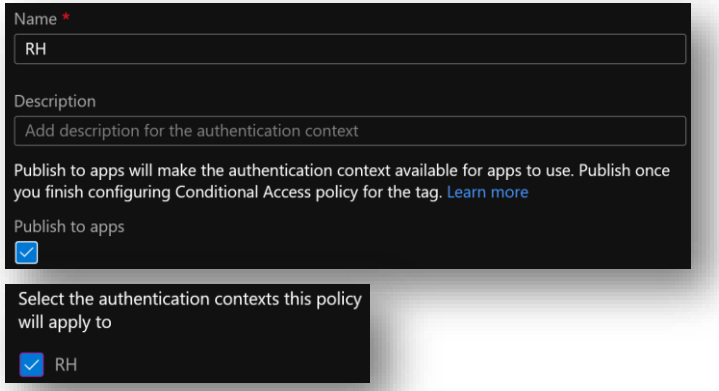
# Fonctionnalités Conditional Access

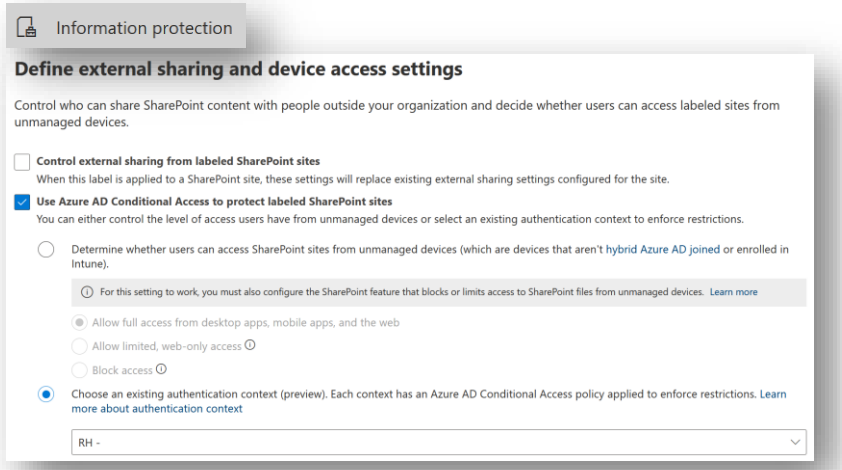
## Signaux avancés 1/4

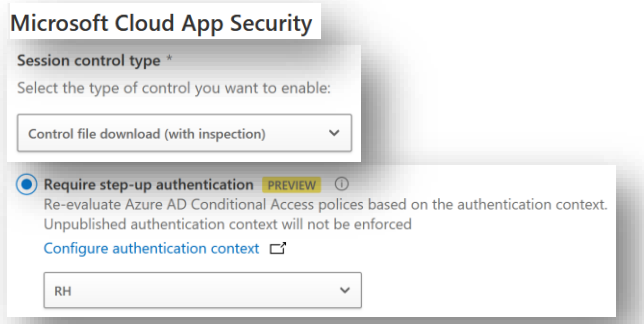
- Actions de l'utilisateur
  - Enregistrer des informations de sécurité
  - Enregistrer ou joindre des périphériques




- Contextes d'authentification



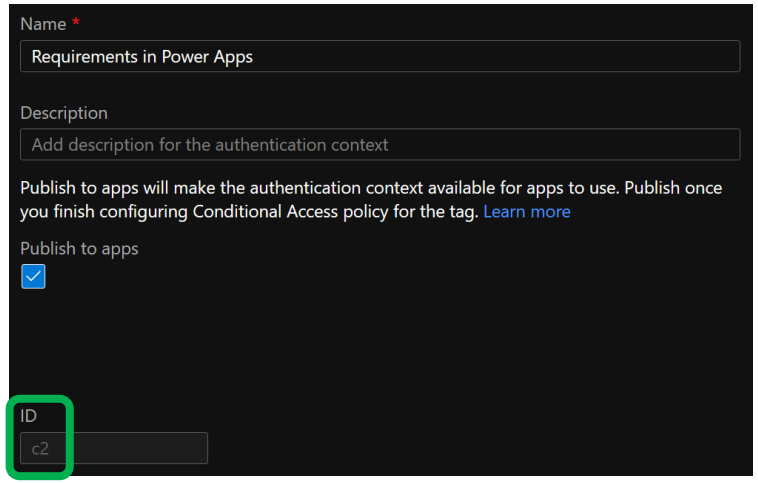



# Fonctionnalités Conditional Access

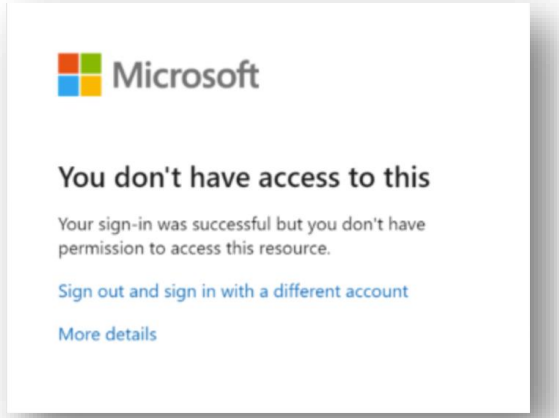
## Signaux avancés 2/4

- Contextes d'authentification
  - Par Application Power Apps (preview)




```
Set-AdminPowerAppConditionalAccessAuthenticationContextIds
-EnvironmentName <EnvironmentName> -AppName <AppName> -
AuthenticationContextIds c2
```

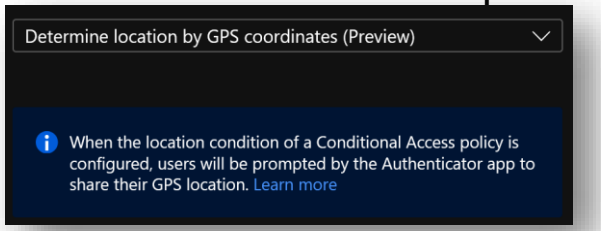
https://apps.powerapps.com/play



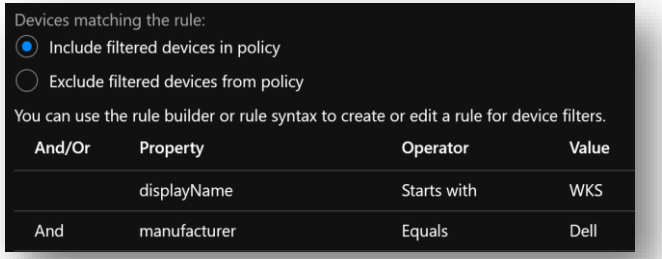
# Fonctionnalités Conditional Access

## Signaux avancés 3/4

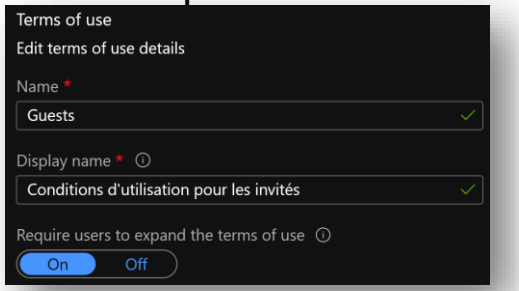
- Localisation déterminée par les coordonnées GPS



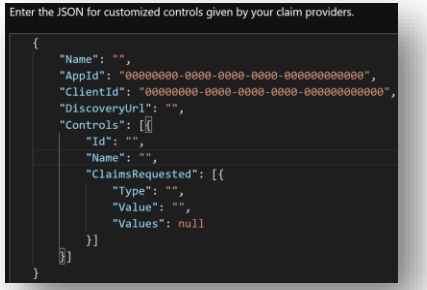

- Attributs de périphérique




- Contrôle personnalisé



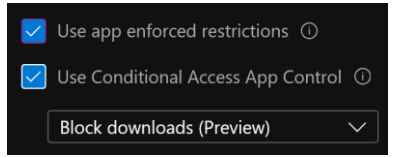

- Conditions d'utilisation

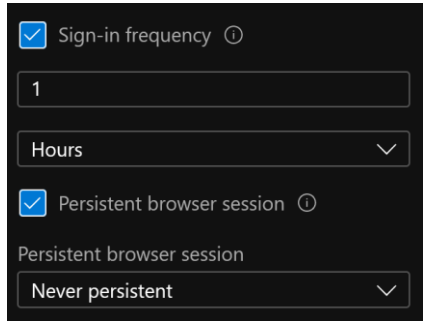


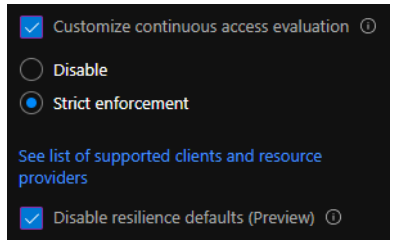
# Fonctionnalités Conditional Access

## Signaux avancés 3/4

- Contrôle de session
  - Restrictions appliquées par l'application
  - Contrôle d'application par accès conditionnel
  - Fréquence de connexion
  - Persistance des sessions de navigation
  - Évaluation de la stratégie d'accès conditionnel (*Preview*)
  - Désactivation de la résilience (*Preview*)



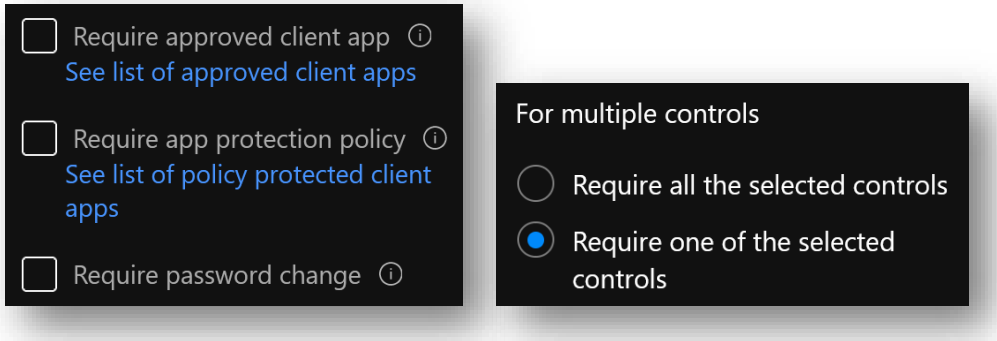




- *Contrôles de session dans une stratégie d'accès conditionnel - Azure Active Directory | Microsoft Docs*
- *Protéger avec le contrôle d'application par accès conditionnel Microsoft Cloud App Security | Microsoft Docs*
- *Configurer la gestion de la session d'authentification - Azure Active Directory | Microsoft Docs*
- *Configurer la gestion de la session d'authentification - Azure Active Directory | Microsoft Docs*
- *Évaluation de l'accès continu dans Azure AD | Microsoft Docs*
- *Valeurs de résilience par défaut pour l'accès conditionnel Azure AD | Microsoft Docs*

# Fonctionnalités Conditional Access

## Décisions avancées

- Autoriser l'accès
  - Demander une application cliente approuvée
  - Exiger une stratégie de protection des applications
  - Exiger un changement du mot de passe



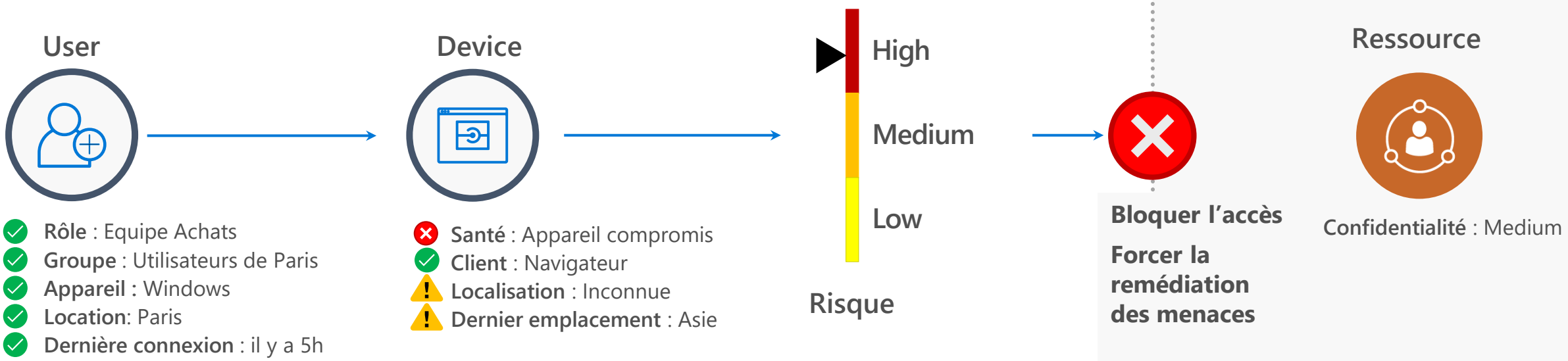

*Application clientes approuvées*

- https://docs.microsoft.com/fr-fr/azure/active-directory/conditional-access/concept-conditional-access-grant#require-approved-client-app

*Application clientes prise en charge par les stratégies de protection des applications*

- https://docs.microsoft.com/fr-fr/azure/active-directory/conditional-access/concept-conditional-access-grant#require-app-protection-policy

# Exemple Conditional Access




Activité malicieuse détectée sur l'appareil

IP Anonyme

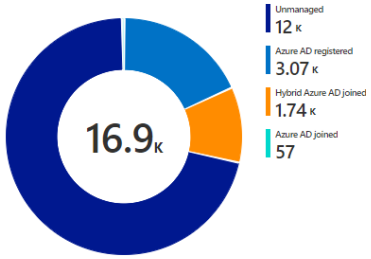
Localisation inhabituelle pour cet utilisateur

# Insights et rapports Conditional Access

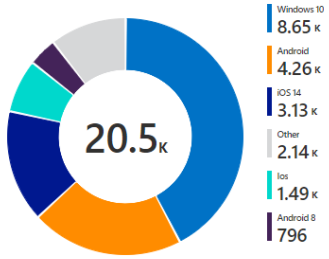
**Breakdown per condition and sign-in status**

*Download results to Excel or open query in Log Analytics by clicking the icons in the upper right corner of each query.*

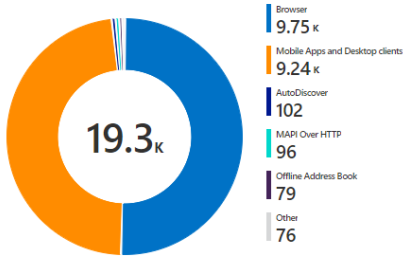
Device State - Total



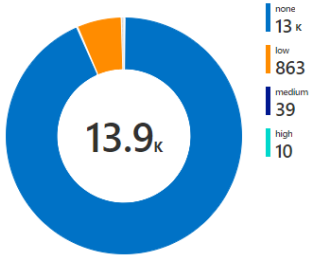

Device platform - Total



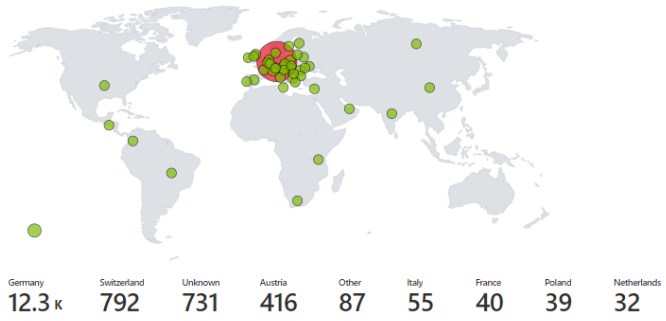

Client app - Total




Sign-in risk - Total




Location - Total




Applications - Total

| AppDisplayName | Count |
|---|---|
| Microsoft Teams | 7665 |
| Office 365 Exchange Online | 5958 |
| Office365 Shell WCSS-Client | 5732 |
| Office 365 SharePoint Online | 4017 |
| Microsoft Teams Web Client | 3946 |

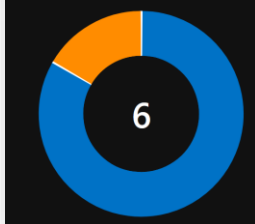
Results were limited to the first 250 rows.

**Activity Details: Sign-ins**

Basic info | Location | Device info | Authentication Details | Conditional Access | Report-only

| Policy Name | Grant Controls | Session Controls | Result |
|---|---|---|---|
| CA - MFA Forced | require multi-factor authentic... | | Success |
| CA - POC BitLocker | | | Disabled |
| CA - Test New Feature | | | Disabled |
| CA - Admin account | require multi-factor authentic... | | Not Applied |
| CA - Block EAS | block | | Not Applied |
| Combined Security Info Registration on Trusted | | | Disabled |
| Teams only for calendar | | | Disabled |
| CA - Block Legacy | block | | Not Applied |

Client app - Success




Run | Time range : Last 24 hours | Save | Share | New alert rule | Export | Pin to dashboard | Format query

```
1  SigninLogs
2  | where TimeGenerated > ago(1d)
3  | project ConditionalAccessStatus, UserDisplayName, AppDisplayName, DeviceDetail
4  | where "All users" == "All users" or UserDisplayName contains "All users"
5  | where "All apps" == "All apps" or AppDisplayName contains "All apps"
6  | project-away AppDisplayName
7  | extend filterResult = case("Total" == "Total", "", "Total" == "Success", "success", "Total" == "Failure", "failure", "notApplied")
8  | where ConditionalAccessStatus contains filterResult
9  | extend deviceState = case(DeviceDetail["trustType"] == "", "Unmanaged", DeviceDetail["trustType"])
10 | summarize count() by UserDisplayName, deviceState
11 | summarize count() by deviceState
```

| ConditionalAccessStatus | UserDisplayName | ClientAppUsed |
|---|---|---|
| success | Xuan Ahehehinnou | Browser |
| success | Xuan Ahehehinnou | Browser |
| success | Hakim Taoussi | Browser |
| success | Hakim Taoussi | Browser |

# Cas d'usage
# Les stratégies les plus pertinentes pour sécuriser les accès

# Principes et bonnes pratiques Conditional Access

- Appliquer les principes de l'approche « Zero Trust »
- Bloquer l'authentification legacy
- Protéger les utilisateurs privilégiés dans tous les systèmes RBAC M365
- Protéger les systèmes privilégiés (comme Azure Management)
- Exiger le MFA dans le maximum des contextes
- Tester les scénarios positifs et négatifs
- Utilisation limitée du blocage général, uniquement si / où cela est nécessaire
- S'assurer que toutes les applications sont protégées (CA n'a pas de « refuser tout » par défaut)
- Exiger la modification du mot de passe et le MFA pour les utilisateurs et les connexions à haut risque
- Restreindre l'accès à partir d'appareils à haut risque (stratégie de conformité Intune avec vérification de conformité dans l'accès conditionnel)
- Empêcher les sessions de navigateur persistantes pour les administrateurs et sur les appareils non approuvés
- Restreindre l'accès à partir de plates-formes d'appareils inconnues ou non prises en charge
- Restreindre l'enregistrement des informations sécurité
- Utiliser le mode « report-only » avant de mettre une stratégie en production.

- Exclure les comptes « bris de glace » de toutes les stratégies
- Exclure les comptes de service Azure AD Connect des stratégies qui l'empêcheraient de se synchroniser en utilisant le rôle « Directory Synchronization Accounts »
- Utiliser des groupes de sécurité pour les exclusions (les groupes basés sur le cloud sont optimaux car les modifications apportées à ces groupes seraient appliquées rapidement par opposition à un groupe synchronisé à partir d'un groupe local)
- Créer un groupe d'exclusion pour chaque stratégie ou par type de stratégie, qui est normalement vide et est utilisé pour fournir des exclusions temporaires via des dérogations. Les exclusions statiques sont affectées en tant qu'affectation d'exclusion directe en plus des exclusions temporaires.
- Faire des revues régulières des membres des groupes d'exclusion
- Attention au navigateur Chrome qui nécessite l'extension « Windows 10 Accounts »

# Convention de nommage  Conditional Access

Il est recommandé de commencer à utiliser un modèle de dénomination cohérent

Assurer une convention de dénomination stricte des politiques, du type :

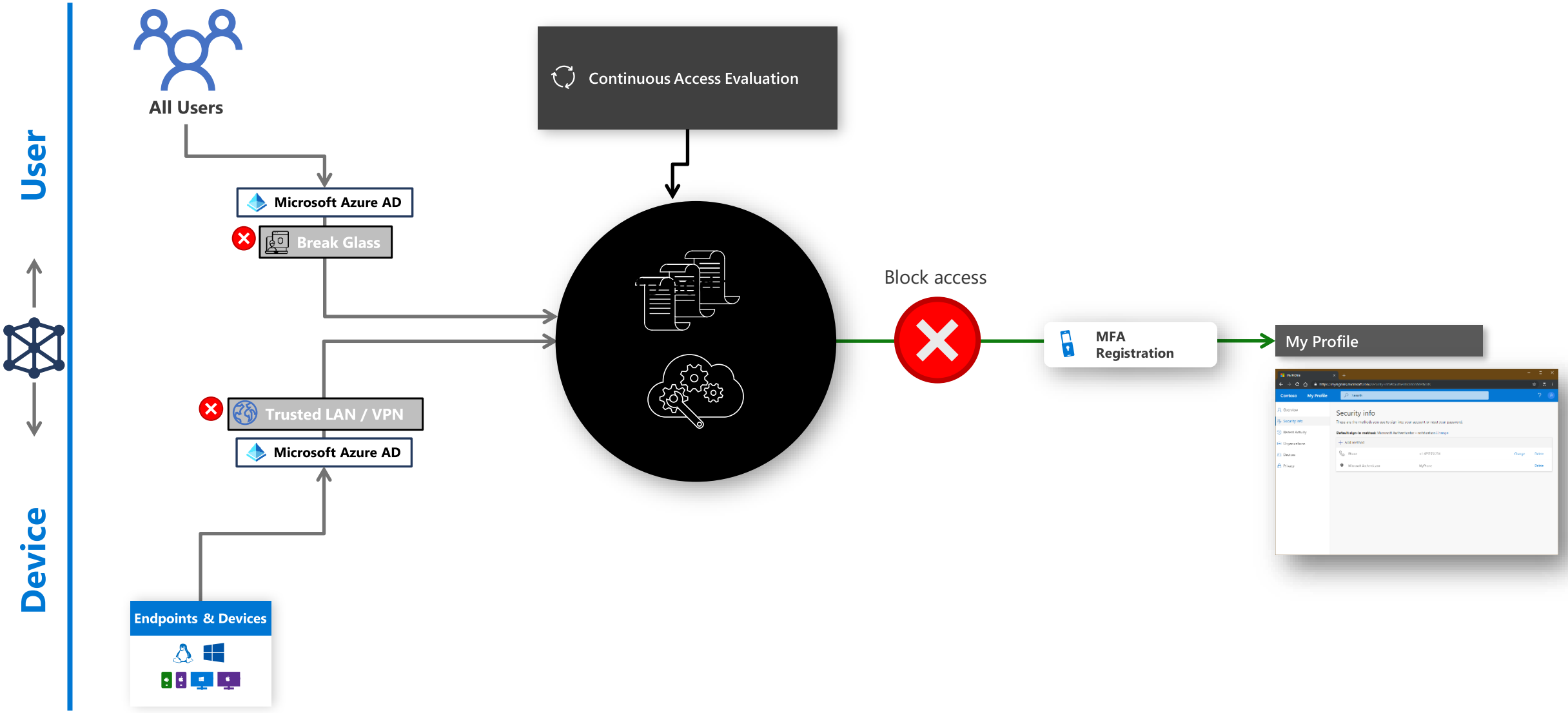
*<CAnumber>-<Persona/User type>-<Policy Type>-<App>-<Platform>-<Grant>-<Optional Description>*

- Exemples :
  - CA001-Global-BaseProtection-AllApps-AnyPlatforms-AADJorCompliant
  - CA002-Global-IdentityProtection-AllApps-AnyPlatforms-Block-BlockLegacy
  - CA101-Admins-AttackSurfaceReduction-AllApps-Unknown-Block
  - CA200-Internals-AppProtection-O365-Windows10-AADHJ
  - CA201-Internals-AppProtection-O365-Windows10-Unmanaged
  - CA202-Internals-DataProtection-O365-Windows10-Unmanaged-DLPSessioncontrol
  - CA203-Internals-AppProtection-O365-iOSAndroid-AppProtection
  - CA204-Internals-AppProtection-SPO-iOSAndroid
  - CA301-Guests-Compliance-AllApps-AllDevices-RequireTermsOfUse

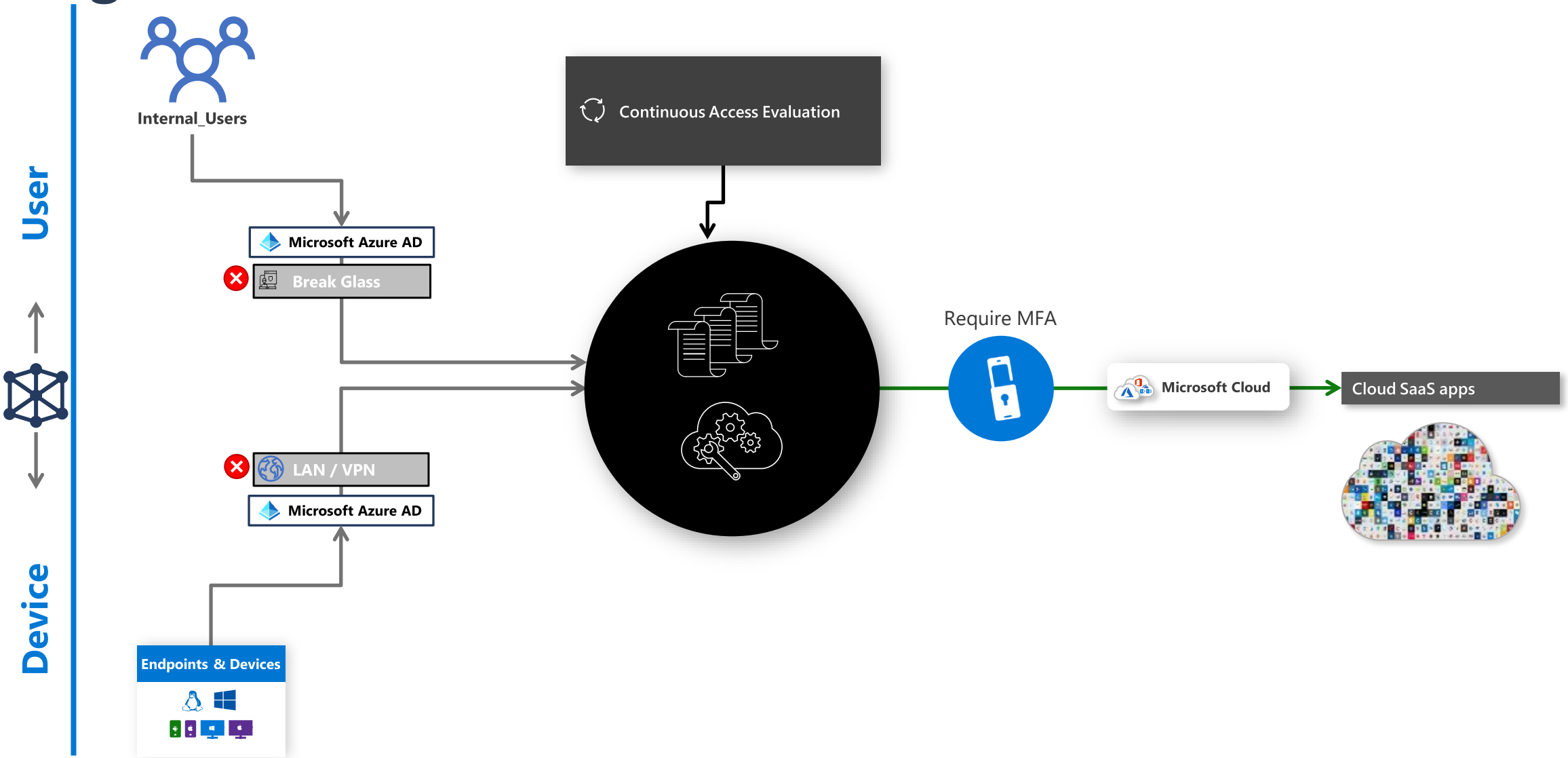
# Exemples de stratégies pertinentes  Conditional Access

- Exiger le MFA en dehors du bureau
- Exiger le MFA pour les administrateurs
- Exiger le MFA pour les invités
- Exiger le MFA pour la gestion Azure
- Exiger un appareil conforme
- Exiger un appareil géré
- Protéger les données des applications mobiles
- Exiger l'acceptation des conditions d'utilisation pour les invités
- Accès basé sur les risques de connexion
- Accès basé sur les risques de l'utilisateur
- Fréquence de l'authentification
- Persistance des sessions de navigation
- Restreindre l'enregistrement d'informations de sécurité
- Bloquer les authentifications legacy
- Bloquer l'accès depuis certains emplacements
- Bloquer les comptes des services
- Bloquer l'accès à des applications spécifiques
- Bloquer les clients mobiles pour les invités et externes
- Bloquer l'accès web depuis des appareils non gérés
- Bloquer du téléchargement depuis des appareils non gérés

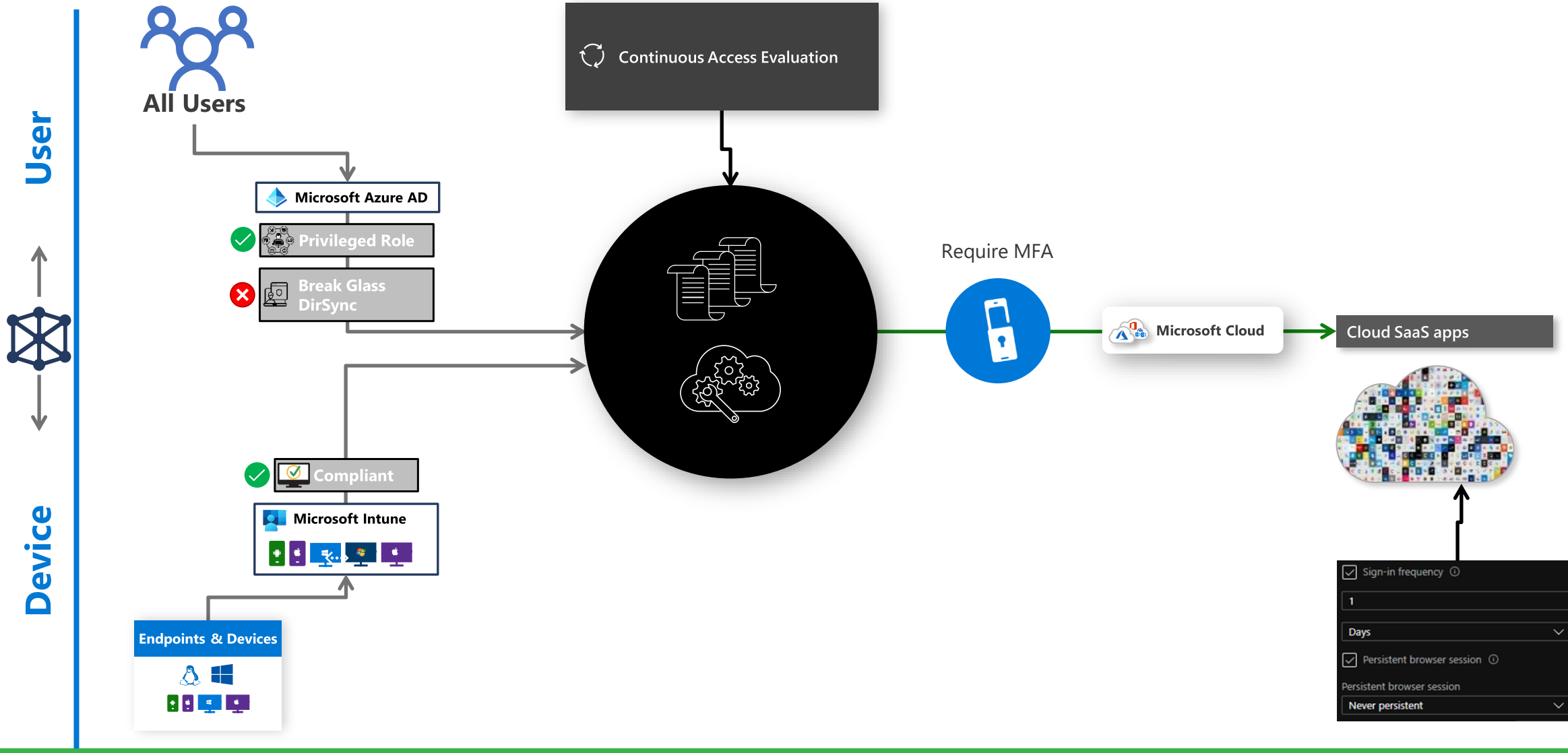
# Restreindre l'enregistrement des informations de sécurité



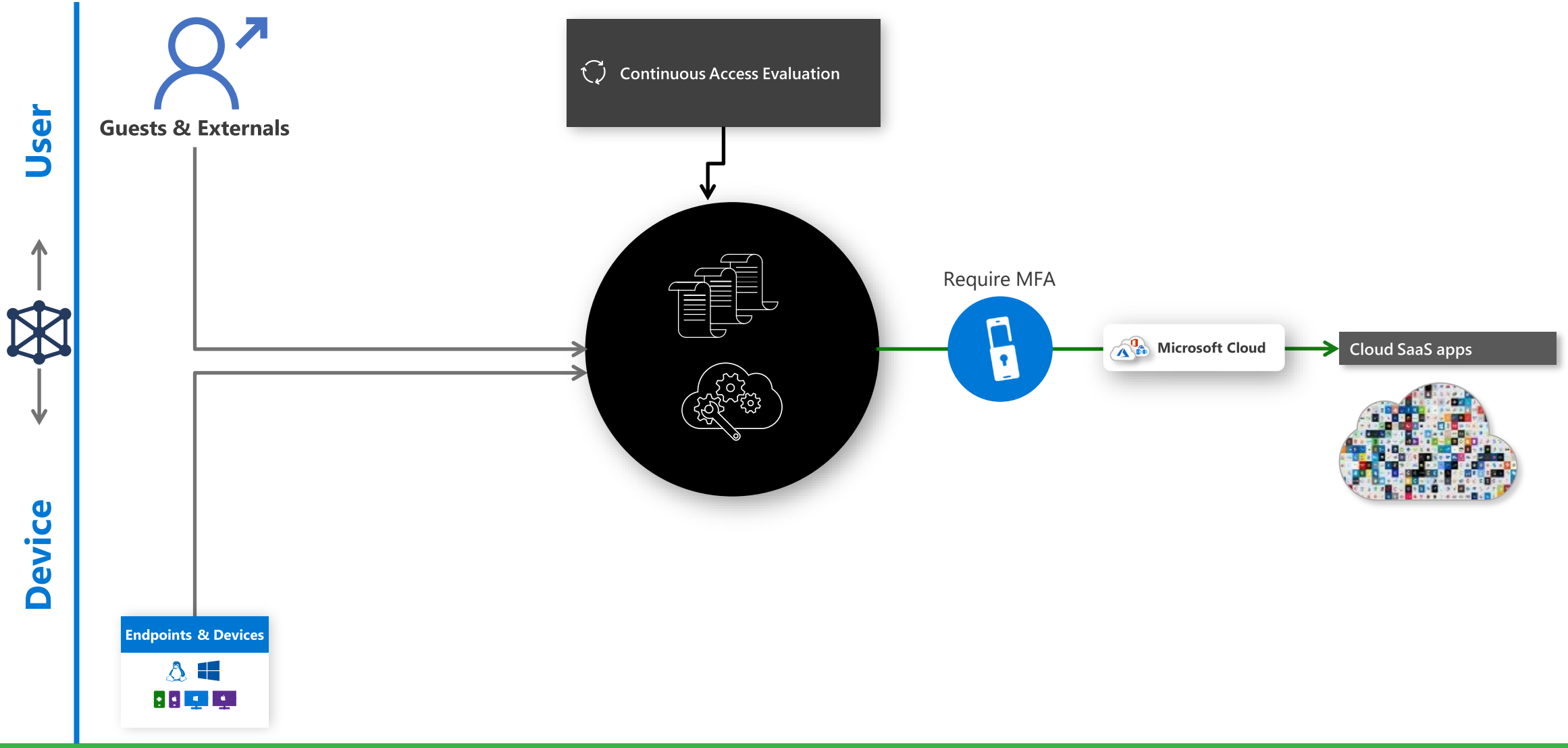
# Exiger le MFA en dehors du bureau



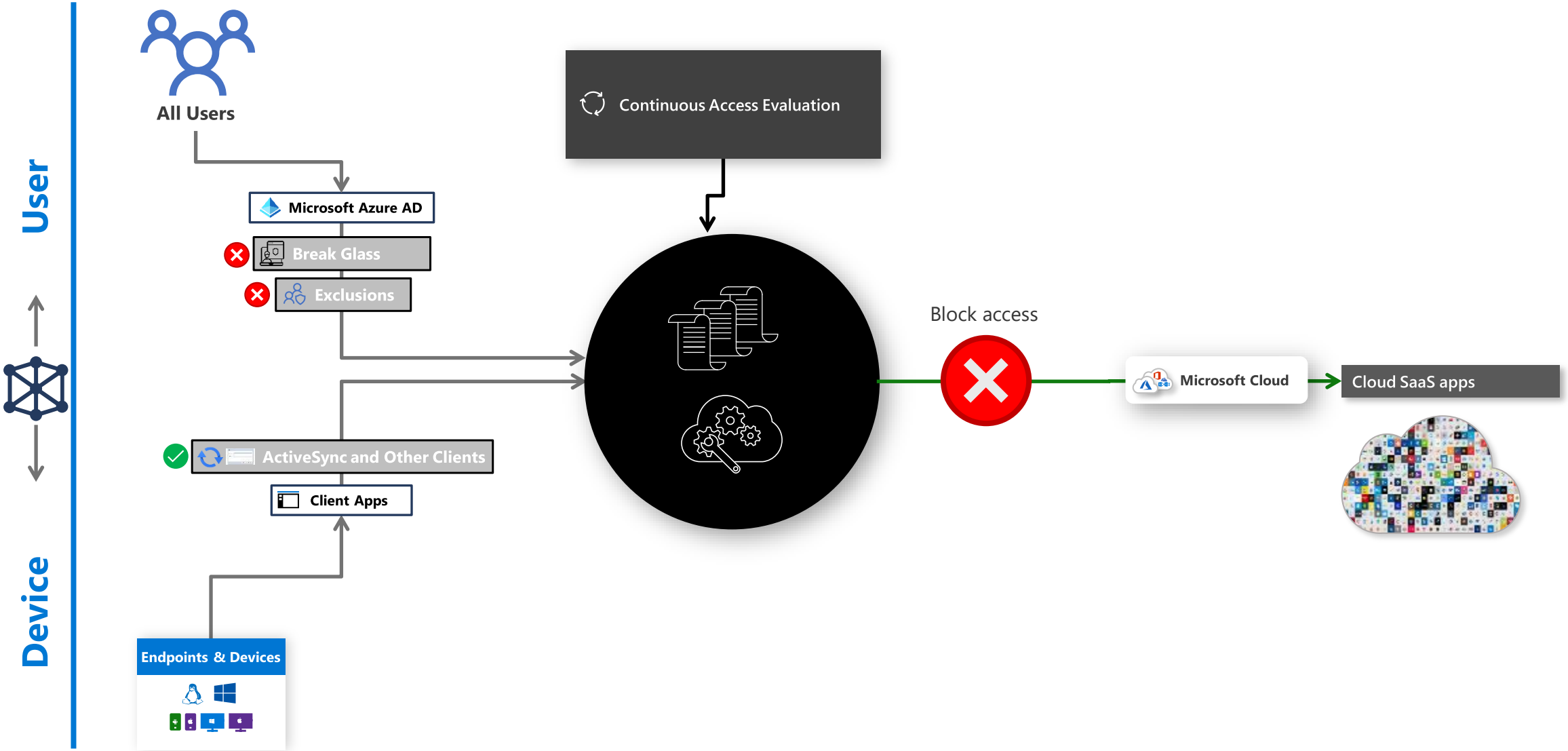
# Exiger le MFA pour les administrateurs



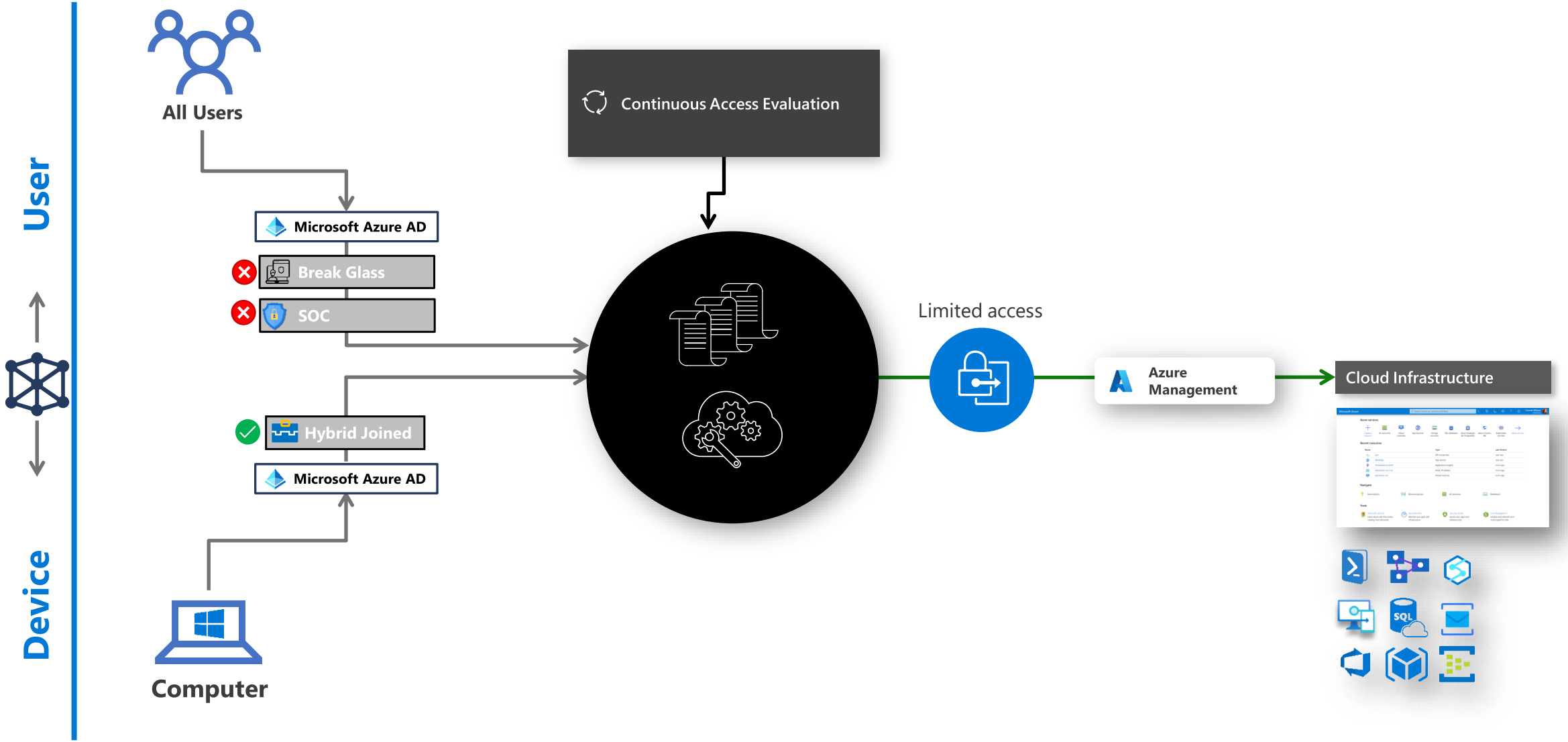
# Exiger le MFA pour les invités et externes



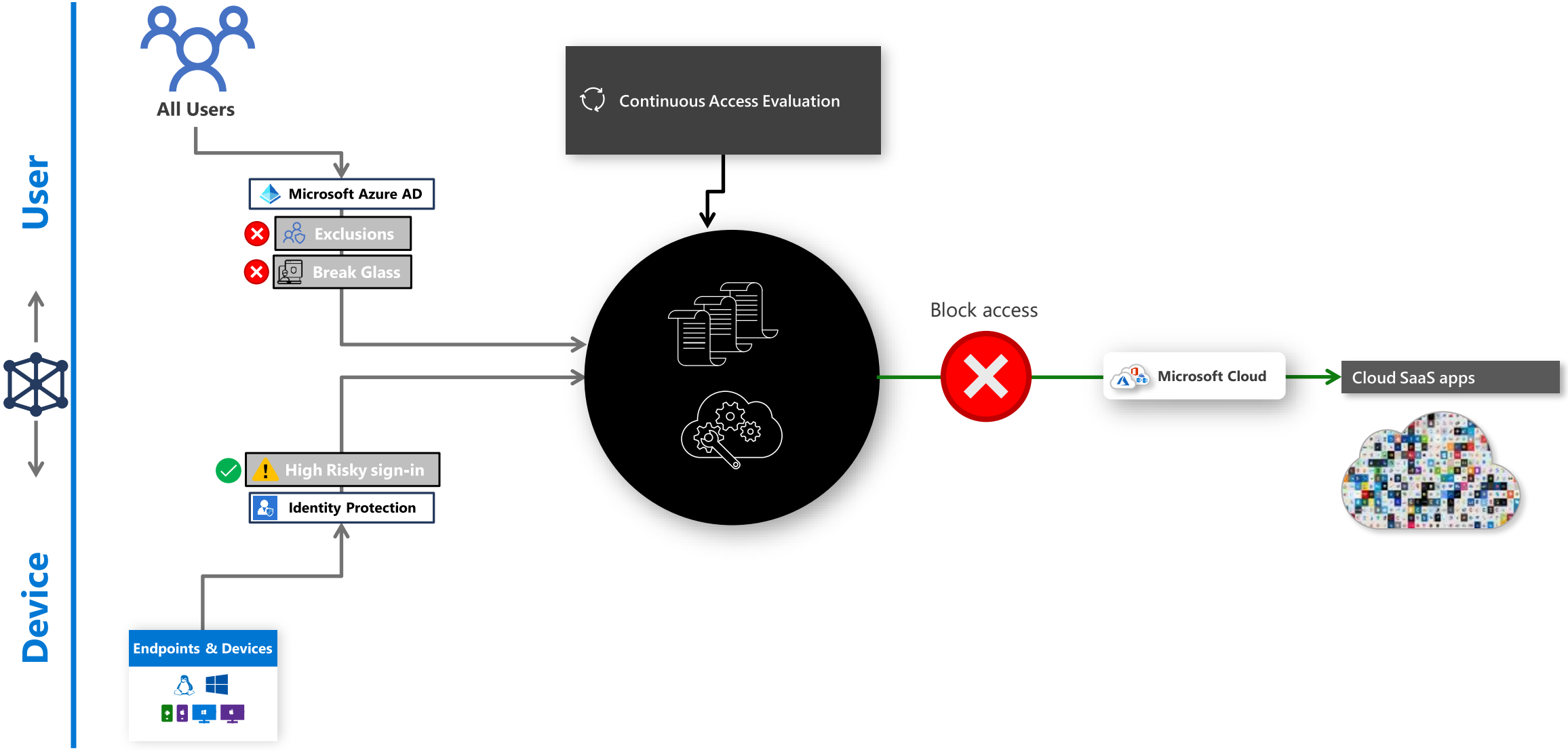
# Bloquer des authentifications & clients « Legacy »



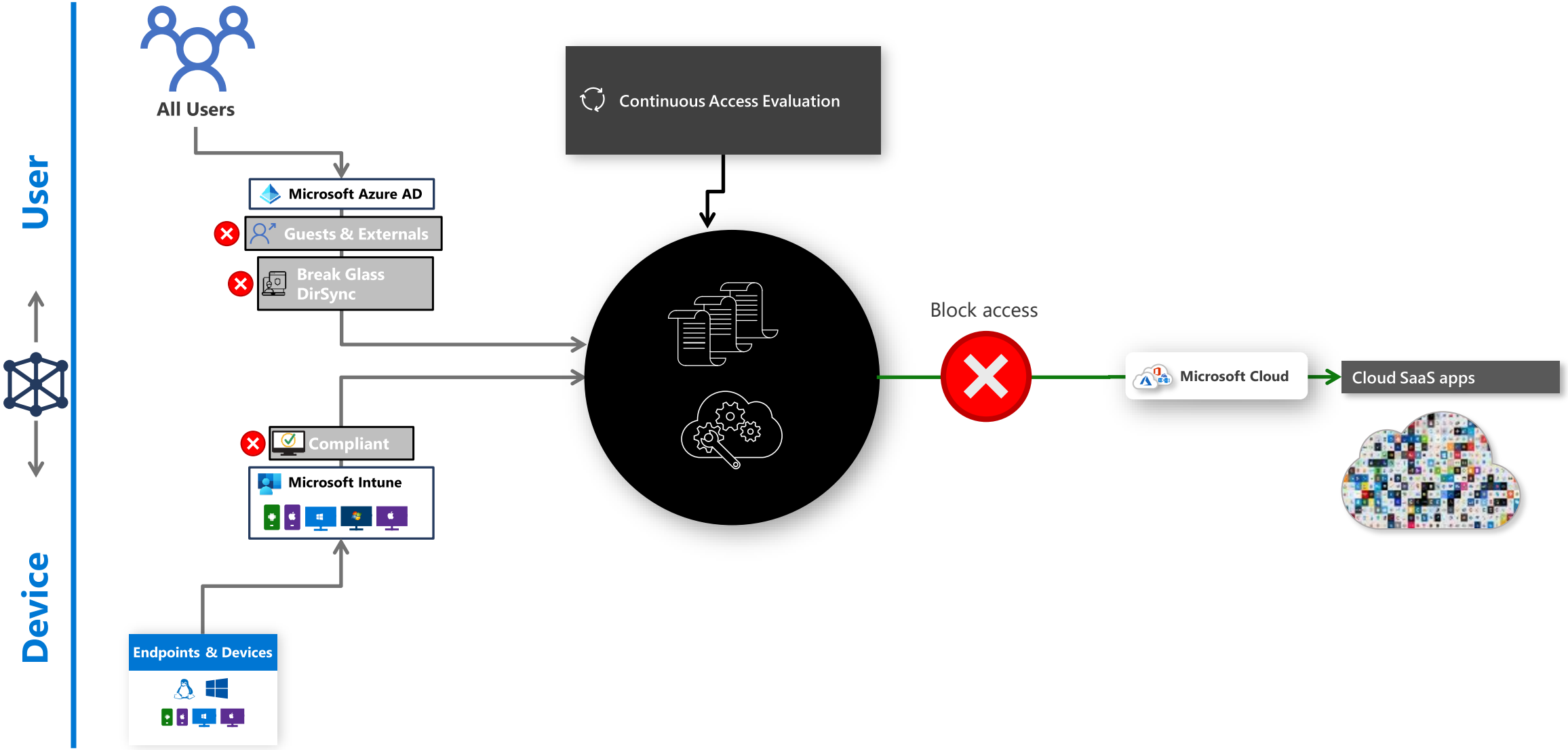
# Restreindre l'accès à la gestion Azure



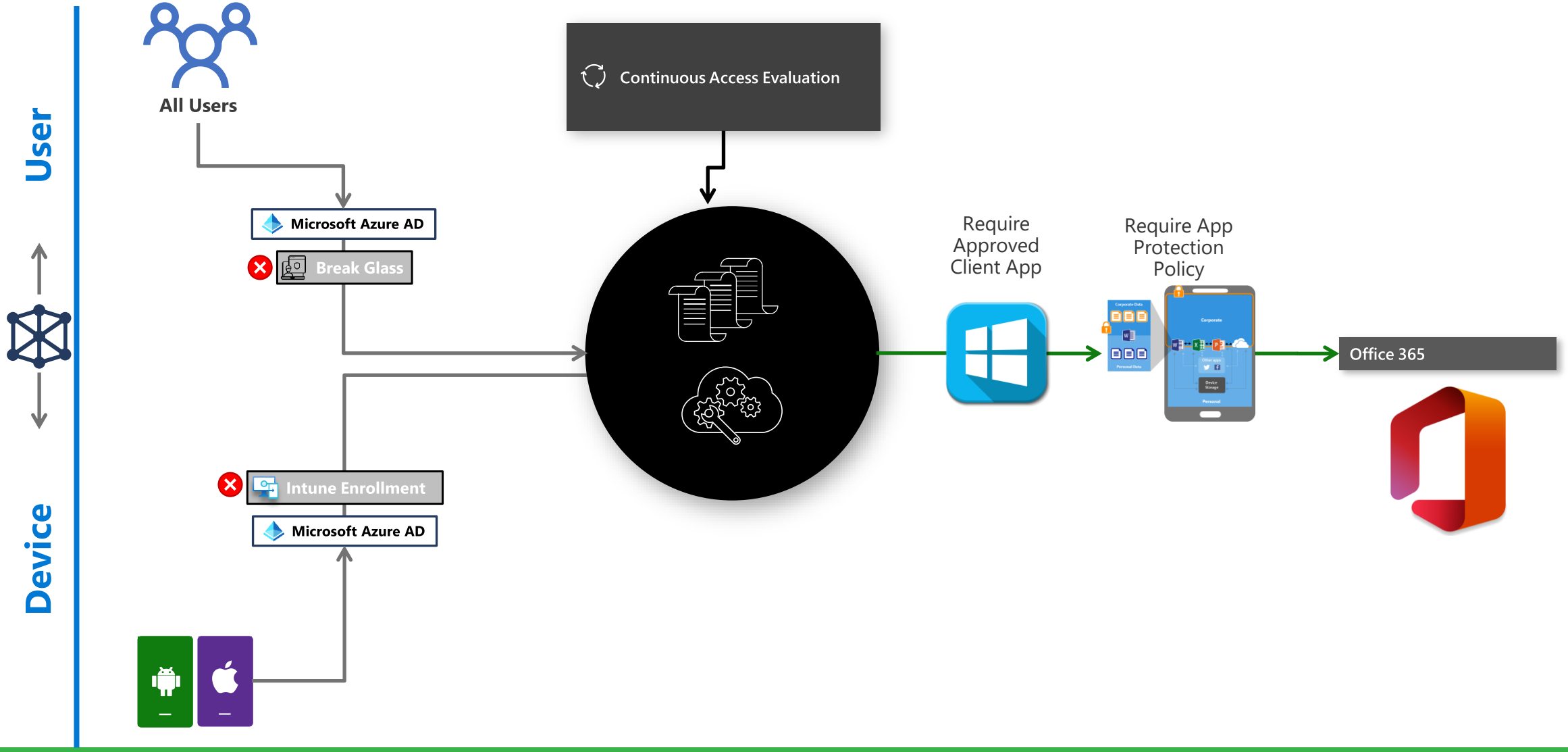
# Bloquer les connexions à risque élevé



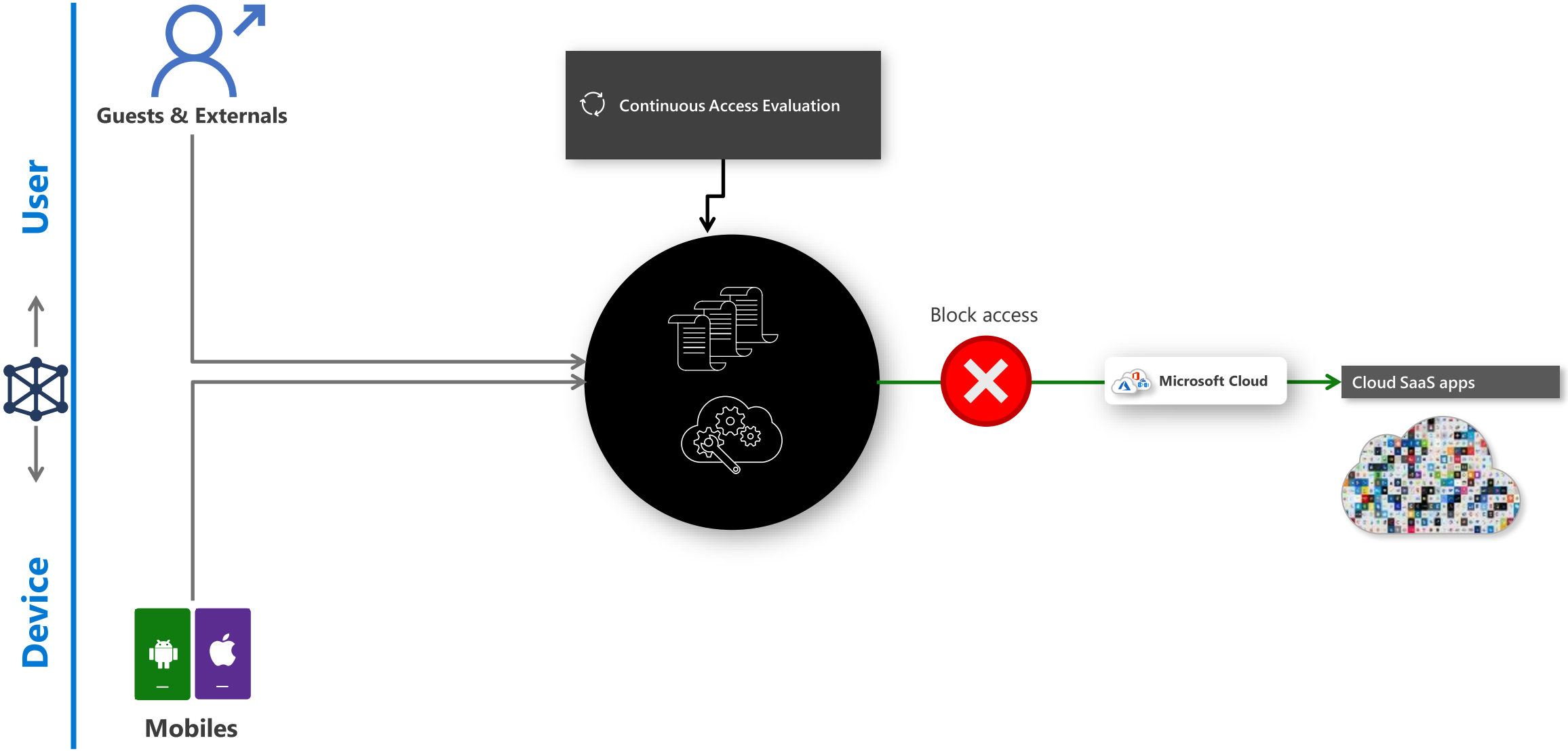
# Bloquer les appareils non conformes



# Protéger les données des applications mobiles (BYOD)



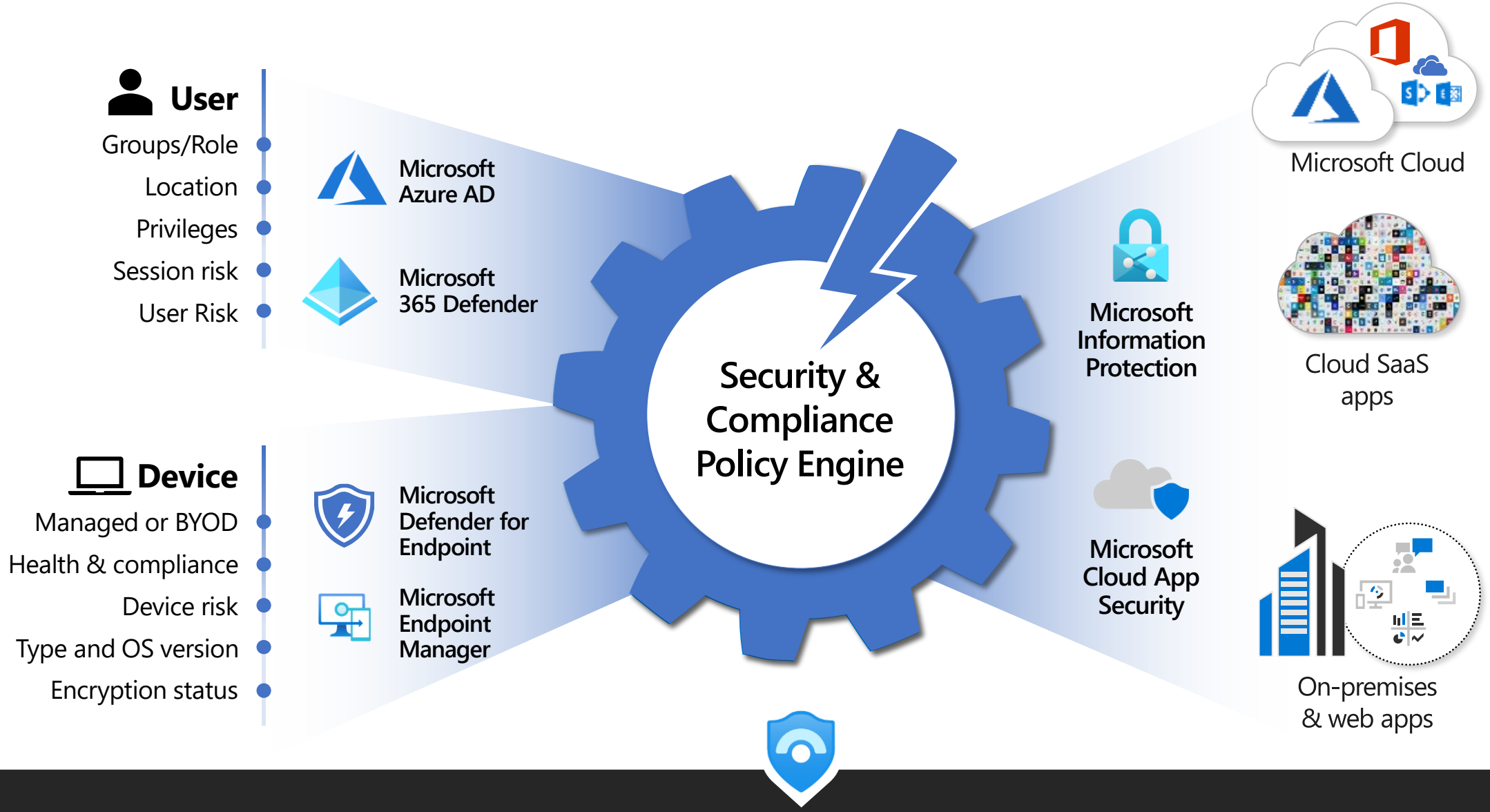
# Bloquer les clients mobiles pour les invités et externes



# CONCLUSION

# Protégez vos actifs où que vous soyez avec Zero Trust

Vérifier **explicitement** | Appliquer **le principe du moindre privilège** | Supposer **une brèche**




aka.ms/zerotrust


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