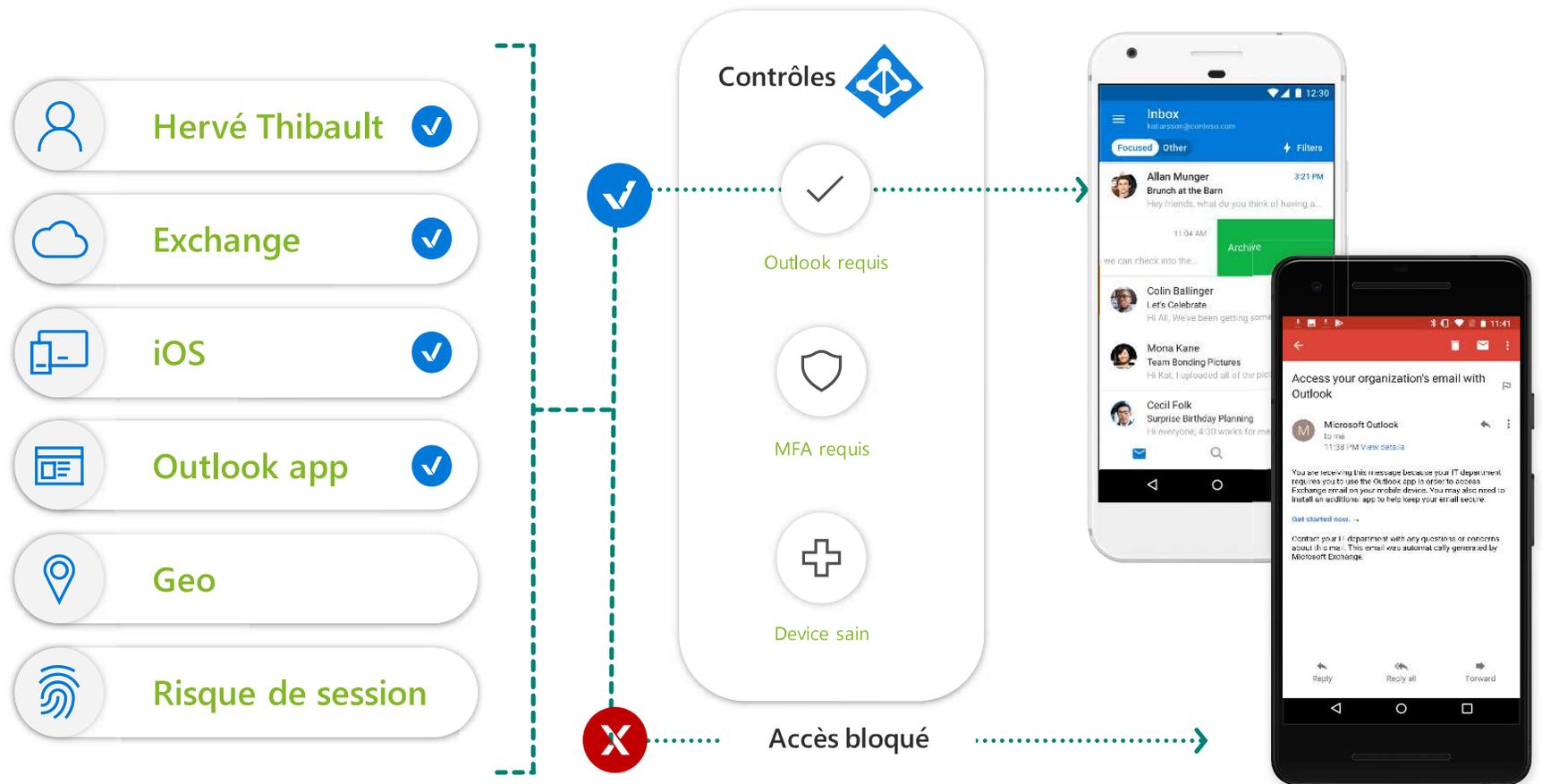


Accès conditionnel avec Azure AD Premium

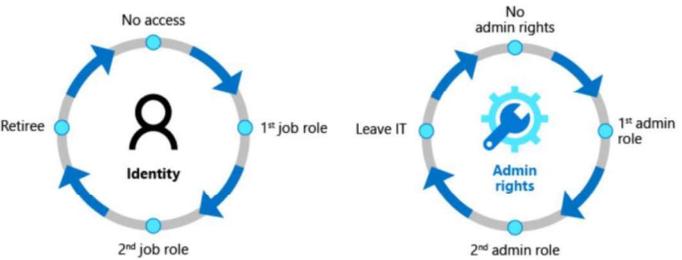
Autoriser l'accès à Exchange Online depuis Outlook uniquement



Modern Workplace : Identity Gouvernance

- Gouverner le cycle de vie des identités
- Gouverner le cycle de vie des accès
- Sécuriser l'administration

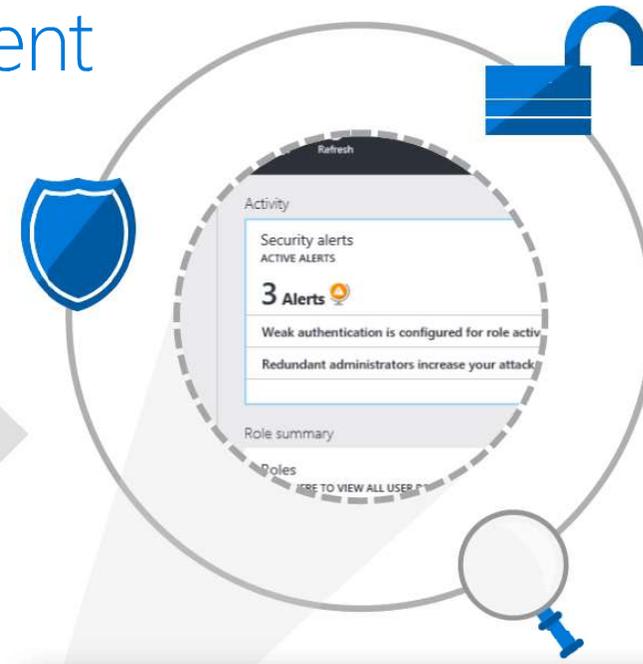
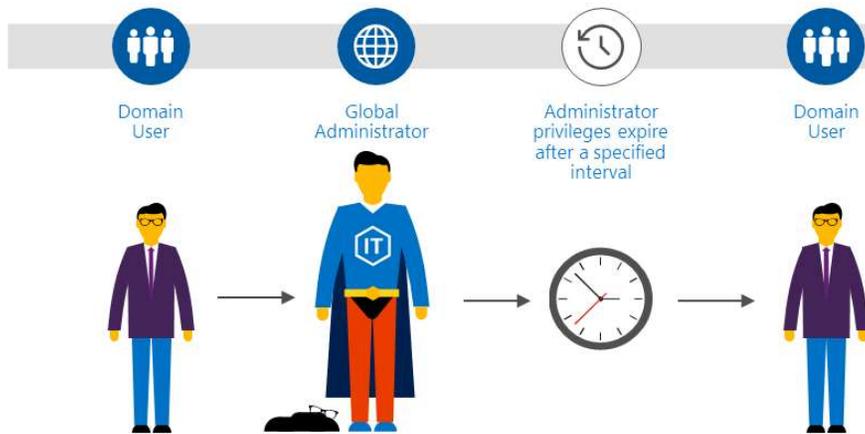
<input type="checkbox"/>	Administrateur d'authentification	A accès pour afficher, définir et réinitialiser les informations de méthode d'authentific...
<input type="checkbox"/>	Administrateur d'authentification	Autorisé à afficher, définir et réinitialiser les informations de méthode d'authentificati...
<input type="checkbox"/>	Administrateur d'utilisateurs	Peut gérer tous les aspects des utilisateurs et groupes, notamment la réinitialisation ...
<input type="checkbox"/>	Administrateur de conformité	Peut lire et gérer la configuration de la conformité et les rapports dans Azure AD et ...
<input type="checkbox"/>	Administrateur de facturation	Peut effectuer des tâches de facturation courantes, telles que la mise à jour des infor...
<input type="checkbox"/>	Administrateur de fournisseur d'id...	Peut configurer les fournisseurs d'identité pour une utilisation dans la fédération dire...
<input type="checkbox"/>	Administrateur de jeu de clés IEF B...	Peut gérer les secrets pour la fédération et le chiffrement dans Identity Experience Fr...
<input type="checkbox"/>	Administrateur de l'accès conditio...	Peut gérer les fonctionnalités d'accès conditionnel.
<input type="checkbox"/>	Administrateur de la sécurité	Peut lire des rapports et des informations de sécurité, ainsi que gérer la configuratio...
<input type="checkbox"/>	Administrateur de licence	Possibilité d'attribuer, de supprimer et de mettre à jour des attributions de licence.
<input type="checkbox"/>	Administrateur de mot de passe	Peut réinitialiser les mots de passe pour les administrateurs de mot de passe et les ut...
<input type="checkbox"/>	Administrateur de recherche	Peut créer et gérer tous les aspects des paramètres Microsoft Search.
<input type="checkbox"/>	Administrateur de rôle privilégié	Peut gérer les attributions de rôles dans Azure AD et tous les aspects de Privileged Id...
<input type="checkbox"/>	Administrateur de service	Peut lire des informations sur l'intégrité du service et gérer les tickets de support.
<input type="checkbox"/>	Administrateur de stratégie IEF B2C	Peut créer et gérer les stratégies de framework de confiance dans Identity Experience...
<input type="checkbox"/>	Administrateur des communicatio...	Peut gérer les fonctionnalités d'appel et de réunions au sein du service Microsoft Tea...
<input type="checkbox"/>	Administrateur des données de co...	Permet de créer et de gérer le contenu de conformité.
<input type="checkbox"/>	Administrateur du flux utilisateur ...	Peut créer et gérer tous les aspects des flux utilisateur.
<input type="checkbox"/>	Administrateur du service Teams	Peut gérer le service Microsoft Teams.
<input type="checkbox"/>	Administrateur du support techniq...	Peut réinitialiser les mots de passe pour les administrateurs de mot de passe et les ut...
<input type="checkbox"/>	Administrateur Dynamics 365	Peut gérer tous les aspects du produit Dynamics 365.
<input type="checkbox"/>	Administrateur Exchange	Peut gérer tous les aspects du produit Exchange.
<input type="checkbox"/>	Administrateur général	Peut gérer tous les aspects d'Azure AD et des services Microsoft qui utilisent des ide...
<input type="checkbox"/>	Administrateur Intune	Peut gérer tous les aspects du produit Intune.



Comme pour tout projet, la gouvernance est clé !

Privileged Identity Management

- Just In Time Administration (JITA)
- Just Enough Administration (JEA)



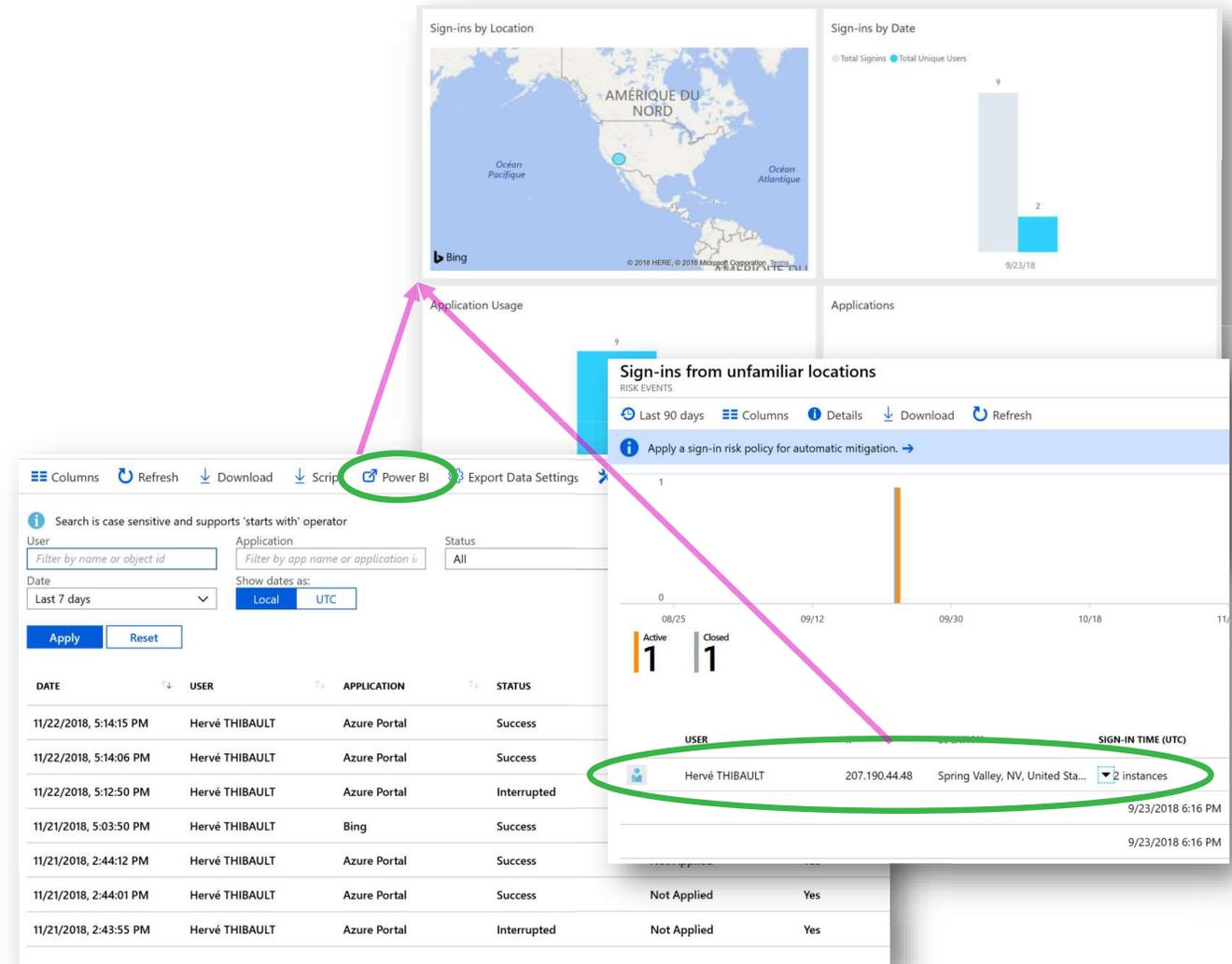
The screenshot shows the Privileged Identity Management (PIM) console interface. The main heading is "Gérer votre accès privilégié" (Manage your privileged access). Below this, there are three main sections:

- Gérer l'accès** (Manage access): Les utilisateurs disposant d'un accès excessif sont vulnérables en cas de compromission d'un compte. Assurez-vous que votre organisation gère le moindre privilège en examinant, en renouvelant ou en étendant l'accès aux ressources.
- Activer juste-à-temps** (Activate just-in-time): Réduisez le risque de mouvement latéral en cas de compromission d'un compte en éliminant l'accès permanent aux rôles et ressources privilégiés. Appliquez l'accès juste-à-temps aux rôles critiques avec PIM.
- Découvrir et surveiller** (Discover and monitor): Il est courant que l'accès aux ressources critiques ne soit pas détecté. Vérifiez que vous savez qui a accès à quoi et recevez des notifications lorsque de nouvelles attributions sont accordées aux comptes de votre organisation.

The interface also includes a sidebar with navigation options like "Mes rôles", "Mes demandes", "Approuver les demandes", "Revoir l'accès", "Gérer", "Rôles Azure AD", "Rôles personnalisés Azure AD", "Ressources Azure", "Activité", "Mon historique d'audit", "Dépannage + support", "Dépanner", and "Nouvelle demande de support".

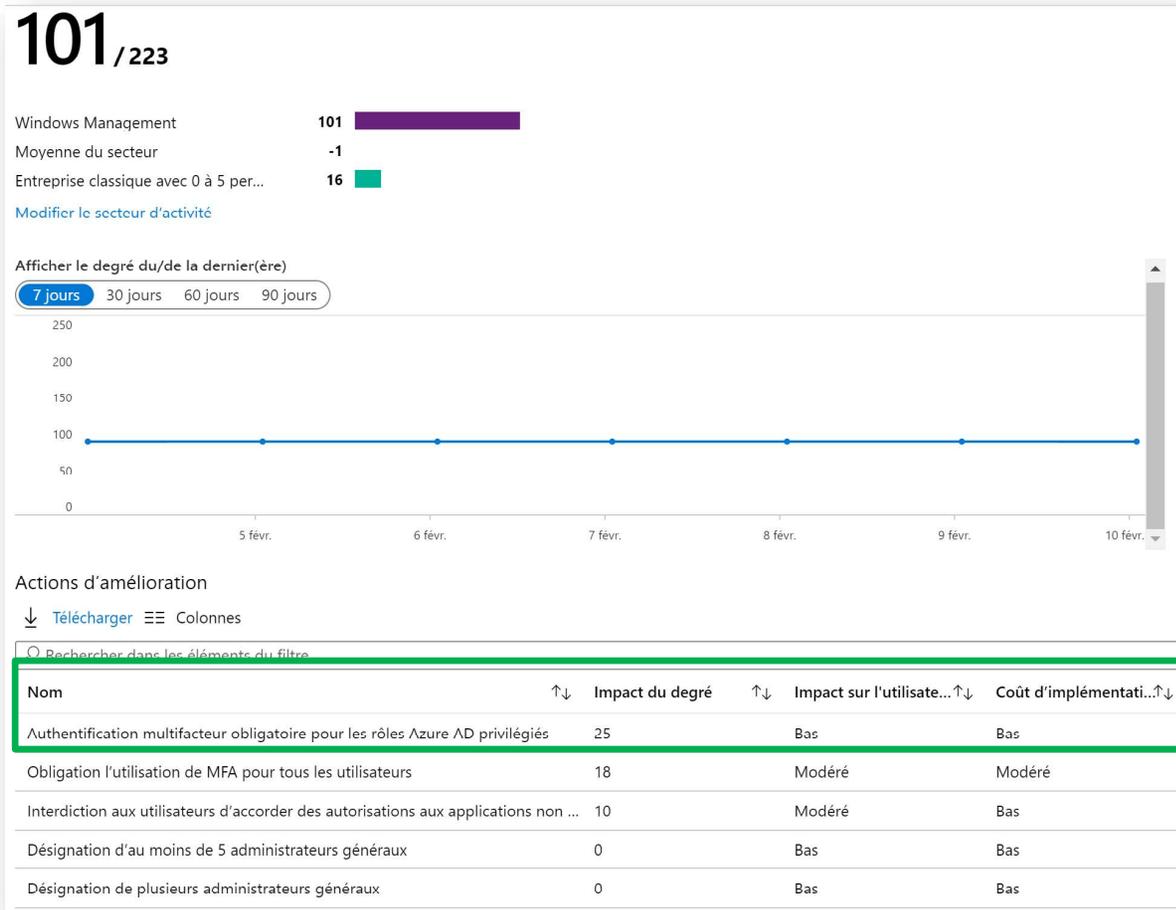
Rapports de sécurité & d'activité

- **Rapports de sécurité :**
Identification des utilisateurs "à risque", des connexions "suspectes" (@IP anonymes, endroits inhabituels ou "impossibles", devices compromis, ...)
- **Rapports d'activité :**
changements de groupe, reset de mot de passe, connexions authentifiées, ...



Secure Score

Identifier les axes d'amélioration de la sécurité en un coup d'œil



Action d'amélioration

Authentification multifacteur obligatoire pour les rôles Azure AD privilégiés

IMPACT DU DEGRÉ ⓘ
+25

DEGRÉ ACTUEL ⓘ
25

DEGRÉ MAXIMAL ⓘ
50

STATUT ⓘ

Par défaut

DESCRIPTION ⓘ

Exiger l'authentification multifacteur pour tous les comptes Azure Active Directory dotés de rôles privilégiés complique l'accès des attaquants aux comptes. Les rôles privilégiés possèdent des autorisations plus élevées que les utilisateurs normaux et incluent tous les rôles d'administrateur (Administrateur général, Administrateur SharePoint, Administrateur Exchange, etc.). Si l'un de ces comptes est compromis, des appareils et données critiques pourront faire l'objet d'attaques. 1 compte(s) sur 2 doté(s) de rôles privilégiés n'utilise(nt) pas l'authentification multifacteur.

IMPACT SUR L'UTILISATEUR ⓘ
Bas

COÛT D'IMPLÉMENTATION ⓘ
Bas

QUE SUIS-JE SUR LE POINT DE CHANGER ? ⓘ

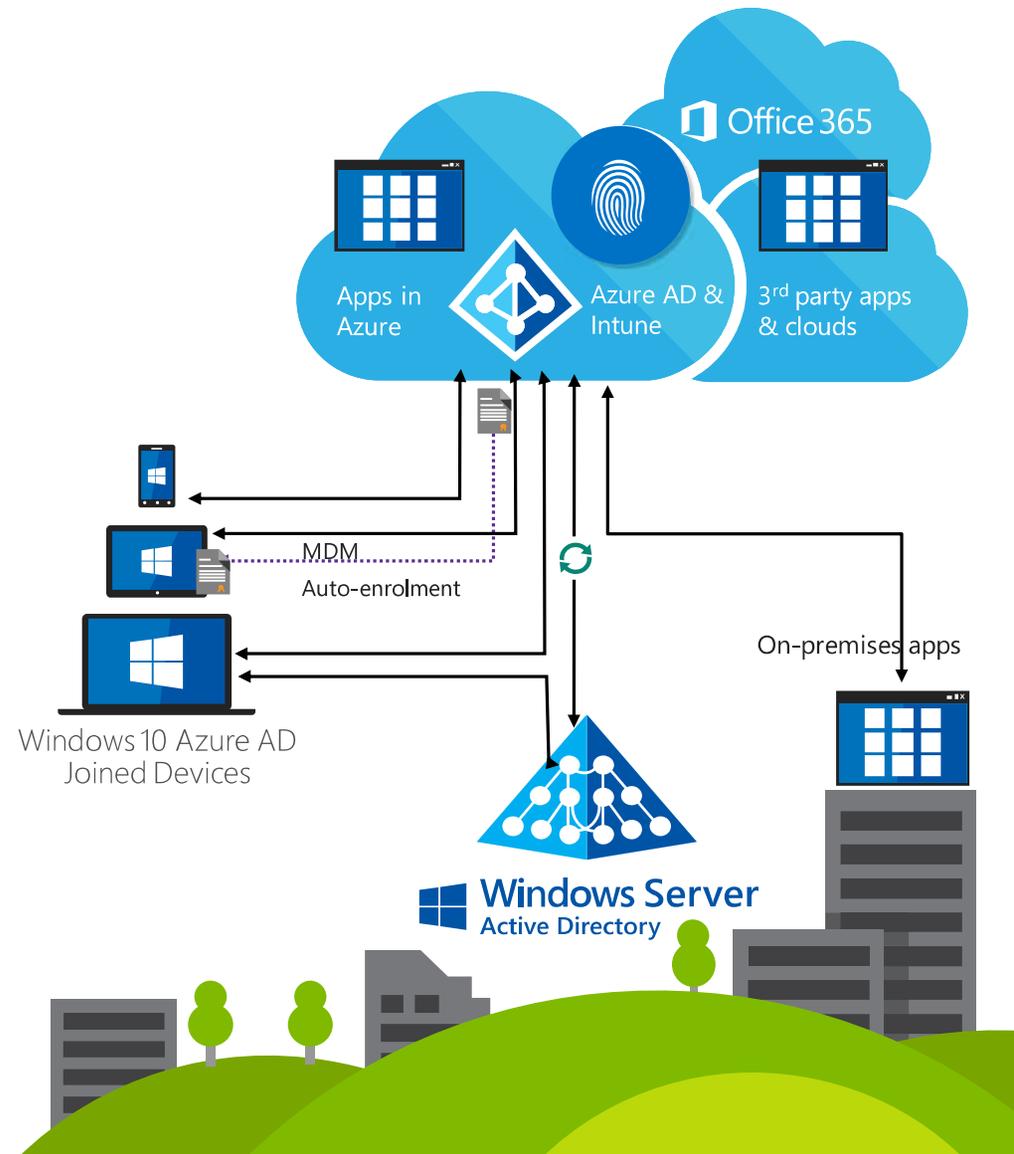
Créez une stratégie via le [portail d'accès conditionnel Azure AD](#) pour exiger l'authentification multifacteur pour tous vos rôles privilégiés :

1. Sélectionnez **+ Nouvelle stratégie**
2. Accédez aux Affectations > Utilisateurs et groupes > Inclure > **Sélectionnez des utilisateurs et des groupes** > cochez

La mise à jour des degrés de sécurisation peut prendre jusqu'à 48 heures.

Azure AD Join & Windows 10

- Azure AD Join permet de connecter un appareil Windows 10 device dans l'Azure Active Directory de votre organisation.
- Les utilisateurs peuvent se connecter à Windows avec les identifiants stockés dans le cloud et profiter de la nouvelle expérience moderne de Windows.
- SSO
- Accès Education / Business Store
- Enrôlement automatique dans un MDM
- Support d'environnement hybride



Azure AD Join & Windows 10

 **Hervé THIBAUT**
Architecte technique
Enterprise Workplace
Experience

Email : herve.thibault@infeeny.com
Téléphone: (téléphone portable)

Gérer le compte

- Changer le mot de passe
- Configurer la réinitialisation du mot de passe en libre-service
- Vérification de sécurité supplémentaire
- Vérifier les conditions d'utilisation

[Se déconnecter partout](#)

Appareils et activité

Appareil	OS	Statut
Windows-Phone	Windows	Désactiver l'appareil
HUAWEIFRD L09	Android	Désactiver l'appareil
SURFACELAPTOPHT	Windows	Obtenir des clés Bitlocker
SURFACELAPTOPHT	Windows	Désactiver l'appareil
SURFACEPRO-HTT	Windows	Désactiver l'appareil
SURFACEBOOK2-HT	Windows	Désactiver l'appareil

Accueil

Rechercher un paramètre

Comptes

- Vos informations
- E-mail et comptes
- Options de connexion
- Accès Professionnel ou Scolaire
- Autres utilisateurs
- Synchroniser vos paramètres

Accès Professionnel ou Scolaire

Accédez à des ressources comme la messagerie, les applications et le réseau. En vous connectant, vous acceptez que votre entreprise ou votre établissement puisse contrôler certains éléments de votre appareil, par exemple les paramètres que vous êtes autorisé à modifier. Pour plus d'informations à ce sujet, posez la question.

Se connecter

- Connecté au domaine Azure AD de Infeeny
- Connecté par herve.thibault@infeeny.com
- [Gérer votre compte](#)

Informations | Déconnecter

Microsoft Store pour Entreprises

Effectuer des achats pour mon groupe | Windows Management | Gérer | Rechercher un fournisseur de solutions

+ Ajouter une collection

Windows Management (11)

- SNCF
- Microsoft To-Do
- Forza Hub
- Mon Office
- Word Mobile
- OneDrive
- Sway
- Excel Mobile
- OneNote

Les incontournables Infeeny (4)

- SNCF
- Portail d'entreprise
- Mon Office
- Microsoft To-Do

En synthèse

Azure Active Directory Premium :

- **Des utilisateurs** : Créés dans le cloud, importés depuis un fichier, synchronisés depuis un annuaire LDAP
- **Des groupes** : Pour donner accès à des applications (Cloud ou on-premise)
- **Une identité sécurisée** (MFA, rapports d'activité, protection de l'identité, ...)
- Mais ... pas de stratégies systèmes (GPOs)
 - Il faut utiliser **Microsoft Intune** (ou autre solution de MDM) !

Modern Management



Secure Device, OS & Applications



- UEFI/secure Boot
- Device Health Attestation
- BitLocker
- Applocker
- Exploit Guard
- Credential Guard
- Application Guard
- Windows Hello (clé de sécurité Fido2)
- Windows Sandbox
- Windows Defender Advanced Threat Protection

The image shows a screenshot of Windows settings. On the left, the 'Windows Hello' settings are visible, including options for face recognition, fingerprint, PIN, security key, password, and picture password. On the right, the 'Paramètres d'Application Guard' (Application Guard settings) are shown, with several options set to 'Désactivé' (Disabled): 'Enregistrer les données', 'Copier et coller', 'Imprimer des fichiers', 'Caméra et microphone', and 'Exporter le filtrage d'adresses (EAF)'. The 'Paramètres du programme: Application Guard' section is also partially visible, showing options for 'Désactiver les appels système Win32k', 'Ne pas autoriser les processus enfants', and 'Forcer la randomisation des images'.

Gestion MDM dans Windows 10 – OMA-URI

- OMA-URI = Open Mobile Alliance - Uniform Resource Identifier : Paramètres standards utilisés par de nombreux fabricants d'appareils mobiles pour contrôler les fonctionnalités des appareils
 - Permet de contrôler les fonctionnalités des appareils Windows 10 sans GPO Active Directory ou GPO locales
 - Via WCD, SCCM, Intune, Airwatch, ...
 - Librairie de référence des paramètres qui peuvent être utilisés avec Windows 10 : <https://docs.microsoft.com/fr-fr/windows/client-management/mdm/configuration-service-provider-reference>
- **Nom du paramètre** : Affectez un nom unique au paramètre OMA-URI pour mieux l'identifier dans la liste des paramètres.
 - **Description du paramètre** : Si vous le souhaitez, entrez une description du paramètre.
 - **Type de données** : Choisissez parmi :
 - Chaîne
 - Chaîne (XML)
 - Date et heure
 - Entier
 - Virgule flottante
 - Booléen
 - **OMA-URI (sensible à la casse)** : Spécifiez l'identificateur OMA-URI pour lequel vous voulez fournir un paramètre.
 - **Valeur** : Spécifiez la valeur à associer à l'identificateur OMA-URI que vous avez entré.

Ajouter ou modifier le paramètre OMA-URI ✕

* Nom du paramètre :

Description du paramètre :

* Type de données :

* OMA-URI (sensible à la casse) :

* Valeur :