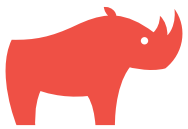
Synapsys

LIVRE BLANC

BYOD : gérer les appareils personnels dans Intune



Synapsys

Sommaire

Introduction : les enjeux du BYOD

Dans un monde professionnel en constante évolution, marqué par l'innovation technologique et les changements dans les modes de travail, le concept de « Bring Your Own Device » a gagné en popularité.

Ce modèle, qui permet aux employés d'utiliser leurs propres appareils à des fins professionnelles, offre une flexibilité sans précédent, mais soulève également d'importants défis en termes de sécurité et de gestion.

Le BYOD est un sujet d'actualité pour beaucoup d'entreprises qui souhaitent basculer vers un environnement de travail plus moderne et flexible, tout en réduisant les coûts.

Contrairement aux idées reçues, le BYOD se prête à de nombreux secteurs, parfois très réglementés comme la banque ou l'énergie, dans la mesure où il permet d'instaurer un cadre d'usage strict.

Mais l'intégration du BYOD en entreprise ne se fait pas sans défis, notamment en termes de sécurité des données et de gestion des appareils.

Dans ce livre blanc, nous proposons une exploration approfondie de cette tendance, en abordant ses avantages, ses défis, ainsi que les meilleures pratiques pour une mise en œuvre réussie.

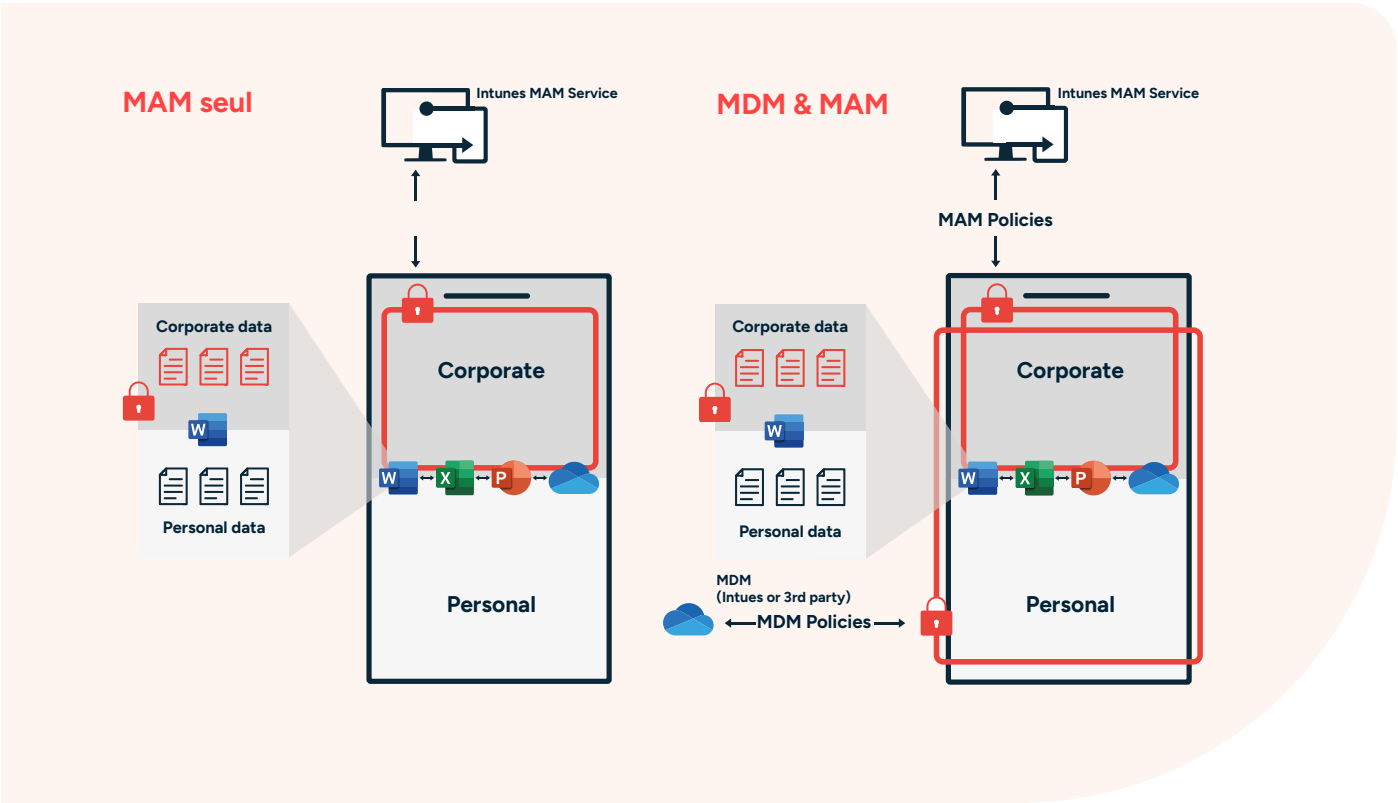
MDM / MAM,
de quoi parle-t-on ?

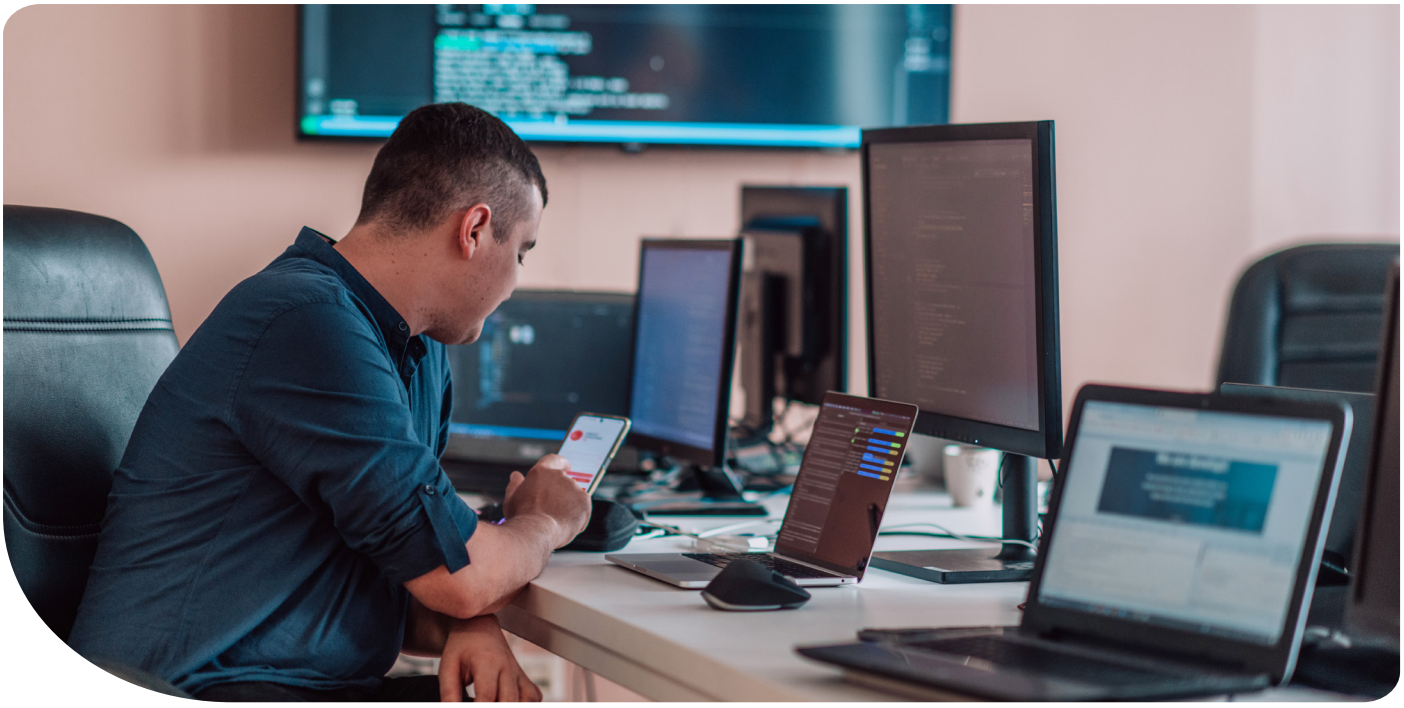
Pour bien appréhender le BYOD, il est important de distinguer deux concepts: le Mobile Device Management (MDM) et le Mobile Application Management (MAM). Le MAM et le MDM sont deux stratégies de gestion des technologies mobiles en entreprise qui se concentrent sur des aspects différents.

Le MDM est axé sur la gestion des appareils mobiles eux-mêmes. Il permet aux entreprises de contrôler et de sécuriser l'ensemble de l'appareil, y compris les applications, les données, et les paramètres de configuration.

Le MAM, en revanche, se concentre spécifiquement sur la gestion des applications mobiles. Il permet aux entreprises de contrôler l'accès aux applications d'entreprise, de gérer les mises à jour, de configurer les paramètres au sein des applications, et de protéger les données d'entreprise qui y sont stockées, sans avoir un contrôle complet sur l'appareil entier.

En résumé, le MDM gère l'appareil dans son ensemble, tandis que le MAM se concentre uniquement sur la gestion des applications. Notons qu'il est possible de gérer un appareil personnel dans un MDM tout en appliquant une politique MAM.





Checklist : différences entre MAM et MDM

MAM (Mobile Application Management)	MDM (Mobile Device Management)
• Contrôler et gérer les applications d'entreprise présentes sur les appareils qu'ils soient personnels (BYOD) ou fournis par l'entreprise. • Appliquer les normes de sécurité spécifiques aux applications, telles que le chiffrement des données, les restrictions d'accès... • Séparer les données d'entreprise des données personnelles sur les appareils. • Supprimer à distance les données d'entreprise des applications sans effacer les données personnelles de l'utilisateur. • Gérer l'accès aux applications d'entreprise selon le profil de l'utilisateur. • Réaliser du suivi et du reporting sur l'utilisation des applications.	• Gérer des appareils en appliquant des politiques de sécurité et de configuration globales. • Déployer des configurations comme les paramètre Wi-Fi, VPN, les mises à jour de sécurité, et les restriction d'appareils. • Sécuriser l'accès aux ressources d'entreprise comme le courriel, les fichiers, et les applications, en fonction du statut de conformité de l'appareil. • Effacer à distance les données d'un appareil en cas de perte ou de vol. • Faire respecter les normes de conformité et les politiques de l'entreprise. • Avoir des rapports sur l'état des appareils, leur conformité et les statistiques d'utilisation.

Feuille de route d'un projet MAM

Mettre en place une politique de Mobile Application Management (MAM) nécessite une approche structurée pour garantir non seulement la sécurité des données d'entreprise, mais aussi pour répondre aux besoins des utilisateurs et respecter leur vie privée.

Étape 1

Analyse des besoins

- Identifier les besoins de l'entreprise concernant l'utilisation des applications mobiles.
- Identifier les applications nécessitant une gestion et une sécurisation.
- Recueillir des informations sur les préférences et les habitudes des employés.
- Établir les objectifs de la politique de MAM en termes de sécurité, de flexibilité et de facilité d'utilisation.

Étape 2

Choix de la solution de MAM

- Comparer les fonctionnalités, la facilité d'utilisation et la compatibilité avec les systèmes existants.
- Considérer les aspects de sécurité, comme le chiffrement des données et la protection contre les fuites d'informations.

Étape 3

Élaboration des politiques et règles

- Définir les politiques de sécurité.
- Établir des règles de Conditional Access pour l'utilisation des applications, le stockage des données et l'accès aux ressources d'entreprise.

Étape 4

Informer les utilisateurs

- Informer les utilisateurs sur l'utilisation sécurisée des applications mobiles.
- Mettre en place des conditions générales d'utilisation à lire et accepter par les employés.

Étape 5

Déploiement et configuration

- Installer et configurer la solution sur les appareils cibles.
- Appliquer les règles de Conditional Access sur les applications concernées.

Étape 6

Surveillance et Maintenance

- Surveiller l'efficacité de la politique.
- Evaluer le respect des politiques et identifier les problèmes potentiels.
- Réviser régulièrement les politiques en fonction des retours d'expérience.

L'importance du juridique

La dimension légale est importante lorsqu'il s'agit de BYOD ou de MAM.

Bien que l'entreprise ne soit pas tenue d'informer les utilisateurs sur les contrôles qui sont fait dans le cadre d'une politique MAM, il est tout de même important de sensibiliser et d'expliquer ce qui a été mis en place. Cela permet à l'utilisateur de comprendre ce qu'il peut et ne peut plus faire dans le cadre professionnel.

Pour ce qui est du MDM, l'entreprise a la nécessité d'informer les utilisateurs avec les conditions générales d'utilisation. Cela permet de protéger juridiquement l'entreprise et d'informer les utilisateurs sur ce à quoi l'entreprise à accès ou non sur l'appareil personnel. Avoir des conditions générales d'utilisation à lire et accepter lors de la phase d'enrôlement du mobile, dans le cas d'un MDM ou d'un BYOD, n'est pas à négliger d'un point de vue juridique.

Les règles de Conditional Access

Les règles de Conditional Access permettent de contrôler l'habilitation d'un utilisateur sur une application depuis le device.

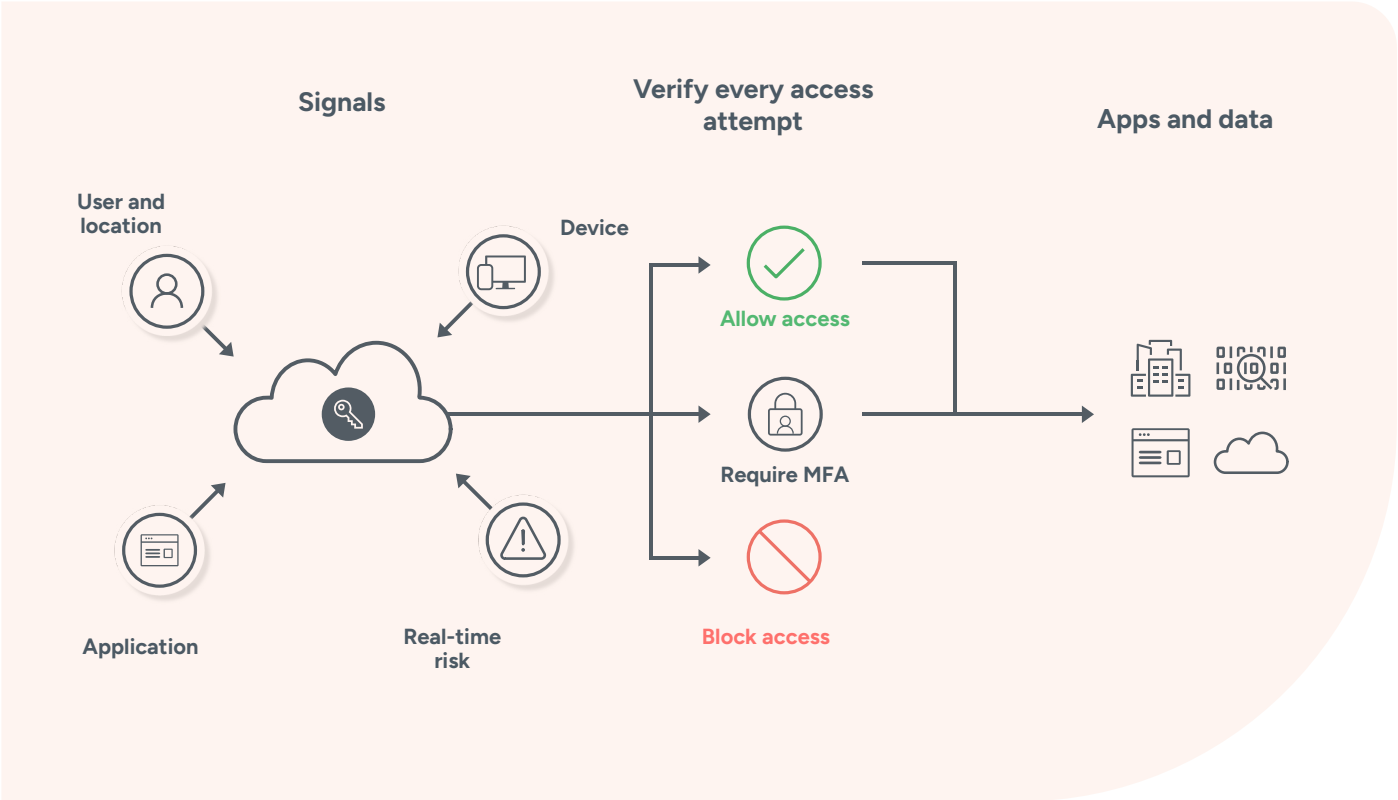
A titre d'exemple, un utilisateur pourra accéder à Teams seulement si l'appareil en question est enrôlé dans le tenant Intune et respecte un certain nombre de règles qu'on appelle des règles de compliance.

Les règles de Conditional Access veillent à sécuriser techniquement l'accès à la donnée suivant les scénarios définis en amont.

Beaucoup d'entreprises ont capitalisé sur les règles de Conditional Access pour stopper l'utilisation de certaines applications d'entreprises sur les devices non enrôlés.
A titre d'exemple, une entreprise peut décider de verrouiller l'utilisation des Mac qui concernait généralement une population moins nombreuse et moins critique.

Suite à l'activation de la règle d'enrôlement, les entreprises constatent de nombreux enrôlements immédiats par les utilisateurs qui ne peuvent d'un coup plus accéder aux applications. Cet exemple souligne qu'il existe toujours une masse silencieuse au sein des entreprises qui utilise les applications entreprises officieusement.

De la même manière, il existe des logs Microsoft 365 qui permettent de savoir qui utilise les données sur des devices non managés. Cela permet d'estimer l'impact d'une règle de Conditional Access avant son déploiement.



TOP 8

de règles de Conditional Access

1 Authentification à deux facteurs (2FA) obligatoire

L'authentification à deux facteurs demeure la première ligne de défense incontournable. Cette règle impose la validation par deux moyens distincts, créant ainsi une barrière robuste contre les accès non autorisés.

2 Restriction géographique

La restriction géographique limite l'accès en fonction de la localisation de l'utilisateur. En définissant des règles basées sur les plages d'adresses IP, elle renforce la sécurité en restreignant l'accès depuis des zones non autorisées. La cartographie peut être assez complexe à définir mais ça en vaut la chandelle.

3 Contrôle basé sur la conformité

Les critères de conformité sont définis dans votre MDM Intune. Ce sont des règles de compliance. Selon le résultat de cette compliance, l'utilisateur peut accéder aux ressources ou non.
Très pratique, attention toutefois, vous êtes en train de dire que l'appareil sera nécessairement enrôlé dans votre MDM Intune.

4 Intégration avec Microsoft Defender

L'intégration avec Microsoft Defender constitue un bouclier avancé contre les menaces. En exploitant les fonctionnalités avancées et ce Secure Score depuis la compliance Intune, elle renforce la capacité à identifier et à neutraliser les menaces potentielles en temps réel.

Attention toutefois aux actions d'admins que vous pouvez réaliser sur le poste, Defender peut avoir tendance à monter votre score si vous accéder à des fichiers sensibles ou exécutez des commandes à privilège.

5 Acceptation des Conditions d'Utilisation (Terms of Use)

Intégrer la règle d'acceptation des Conditions d'Utilisation (TOU) est une pratique moderne et qui responsabilise. Avant d'accorder l'accès, les utilisateurs doivent explicitement accepter les conditions et les politiques de sécurité, renforçant la conformité et la transparence dans l'utilisation des ressources IT.

6 Restreindre l'accès aux OS identifiés

Vous n'avez pas d'appareils macOS en entreprise, pourquoi permettre l'accès à vos ressources depuis un mac ? Vous voulez implémenter une règle forçant les appareils mobiles à être conforme ?
Ou tout simplement interdire aux mobiles l'accès à des ressources sensibles ? Pensez donc à restreindre l'accès sur les types d'OS que vous avez authentifié.

7 Bloquer l'Authentification de Base/Legacy

Le blocage de l'authentification de base ou legacy est une mesure cruciale. En éliminant les méthodes d'authentification obsolètes, cette règle renforce la sécurité en réduisant les vulnérabilités potentielles.

8 Exiger une Politique de Protection des Applications (App Protection Policy)

L'exigence d'une politique de protection des applications implémentée dans Intune ajoute une dimension de sécurité spécifique aux applications.
Cette règle garantit que les applications respectent des normes strictes de sécurité, renforçant ainsi la protection des données.

L'implication des métiers

Il est pertinent d'impliquer des pilotes métiers lors des tests d'un projet BYOD. Effectivement, engager les métiers dans une démarche BYOD permet de trouver le bon niveau de protection afin d'éviter de se heurter plus tard à des résistances.

A noter qu'il s'agit de devices personnels. Plus on met de règles lourdes, plus on impacte l'expérience utilisateur. Complexifier l'utilisation d'un device personnel peut être mal perçu. Effectivement, on observe l'abandon de projets à cause de règles trop restrictives.

Il y a une vraie réflexion à mener en amont autour de la politique de protection et le choix des règles de Conditional Access. De manière générale, il est conseillé d'y aller avec légèreté pour fluidifier l'expérience.

Le BYOD a l'avantage de réduire le nombre de devices gérés et donc de réduire le coût de renouvellement des flottes d'appareils.

A contrario, il faut accepter une plus grande diversité dans le parc de l'entreprise, bien qu'il soit aussi possible de limiter l'autorisation des applications sur un certain type d'appareils ou sur des appareils respectant une version minimale.

Synapsys

A propos de Synapsys

Synapsys est un acteur de référence spécialisé dans la transformation des infrastructures digitales. Depuis plus de 10 ans, nous accompagnons nos clients tout au long du cycle de vie des projets d'infrastructure à travers nos expertises en Digital Workplace, Cloud et DevOps.

Synapsys propose à ses clients un service technologique de qualité, grâce à l'esprit collectif et engagé de ses 180 talents répartis à Paris, Lille, Lyon et Kuala Lumpur.

Nous sommes fiers d'être considérés comme un partenaire de confiance et plébiscités pour la réalisation de projets de transformation structurants. Nos clients grands comptes nous sollicitent pour bâtir des infrastructures agiles et résilientes afin de relever les défis de transformation digitale de demain. Convaincus que tout projet doit apporter le progrès et toute collaboration, la confiance, nous avons à cœur de proposer une vision de l'entreprise inclusive et équitable.Nous faisons du développement des hommes un véritable modèle d'entreprise qui guide nos orientations stratégiques, notre culture et notre mode de fonctionnement.

Chez Synapsys, c'est la force du collectif, l'engagement, l'équité et l'authenticité qui priment. Nous mettons tout en œuvre pour que chacun ait l'opportunité de se développer professionnellement dans un climat de confiance autour d'un projet commun.

www.synapsys-groupe.com

Auteurs :
Tom Machado, Modern Workplace Technical Expert
Nathalie Hoyos, Directrice Marketing & Communication

Crédit image : Synapsys & Adobe Stock