Le BYOD mobile avec Jamf et Apple

N'importe quel appareil peut devenir un appareil de travail.

Et on ne parle pas seulement des appareils d'entreprise.

Les appareils professionnels d'un employé ne se limitent pas à l'ordinateur portable que lui a fourni l'entreprise. Ce sont tous les appareils avec lesquels il accède aux ressources de l'entreprise, ce qui inclut son smartphone ou sa tablette personnelle. C'est ce qu'on appelle le « Bring Your Own Device » (BYOD). Que vous ayez ou non un programme formel de BYOD, des employés peuvent utiliser un appareil personnel à des fins professionnelles.

Une étude récente de ZIPPIA a d'ailleurs montré que **17% des employés** utilisent leurs appareils personnels pour le travail sans en parler au service informatique.

Les utilisateurs utilisent déjà leurs appareils personnels au travail, et vous n'y pouvez rien.

Mais cela pose un sérieux problème de sécurité. L'informatique ne peut pas protéger les appareils dont elle ignore l'existence. Par exemple, selon le récent rapport **Security 360** de Jamf, « en 2022, 21 % des employés utilisaient des appareils mal configuré, ce qui les exposaient à des risques. »

En revanche, vous êtes libre de proposer un programme BYOD formel et complet, conçu pour préserver la sécurité des données et des réseaux. Cette solution donnerait satisfaction aux utilisateurs et leur permettrait d'être productifs, tout en protégeant aussi bien leur confidentialité que vos données.

Quels sont les besoins d'un appareil de travail personnel ?

Le BYOD doit être utilisable, sécurisé et privé.

Le gain de sécurité doit également s'accompagner d'une excellente expérience utilisateur. Vos équipes doivent être aussi productives que possible et utiliser les appareils de la manière la plus sécurisée qui soit. Voyons comment leur faciliter la tâche.

Les organisations doivent configurer et sécuriser la partie professionnelle des appareils sans gêner l'utilisation des applications personnelles. Et une chose doit être parfaitement claire : ces appareils offrent les mêmes garanties de confidentialité que ceux qui ne sont pas inscrits.

Les options BYOD traditionnelles

Les organisations et les employés peuvent avoir des réticences face aux solutions BYOD traditionnelles. Des questions de confidentialité, de qualité d'expérience et de sécurité pour l'organisation peuvent entraver le déploiement du BYOD.

Et la gestion des applications mobiles (MAM) ?

Lorsque la MAM est utilisée seule :

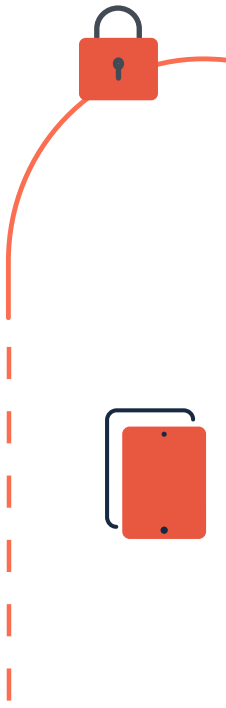
- Le service informatique ne peut pas configurer le Wi-Fi et l'e-mail, ni installer automatiquement des applications, même achetées en volume.
- Les utilisateurs doivent télécharger eux-mêmes les applications et ont souvent un choix limité.
- Les coûts de développement sont plus élevés : les apps doivent être développées spécifiquement pour la MAM.

Gestion complète des appareils :

- Les cadres de gestion complète des appareils sont beaucoup trop invasifs et violent la confidentialité des utilisateurs. Aucun employé ne souhaite ce type de modèle BYOD.

Sans solution, des appareils clandestins :

- Les employés accèdent aux ressources de l'entreprise à l'aide de leurs appareils personnels à l'insu de l'équipe de sécurité et du service informatique de l'organisation.



Jamf et Apple forment une solution BYOD idéale.

Les fonctionnalités Apple qui assurent la sécurité des données de l'entreprise mettent également celles de l'utilisateur hors de portée de son employeur. Il y a, pour ainsi dire, deux appareils en un.

Comment le BYOD est-il pris en charge dans Jamf ?

En utilisant les workflows d'**inscription utilisateur** natifs d'Apple et un identifiant Apple géré (MAID) pour configurer un compte professionnel et un compte personnel distincts, et ainsi protéger la vie privée des employés. Jamf aide ensuite les organisations à sécuriser et à configurer le compte professionnel de l'appareil. L'équipe informatique s'assure que les appareils sont conformes aux règles de l'entreprise et attribue des autorisations d'accès et des applications en fonction des besoins de l'utilisateur ou de son service.

Jamf s'appuie sur la solide posture de sécurité d'Apple et sur ses fonctions exceptionnelles de protection de la vie privée pour :

- Protéger rigoureusement la confidentialité des employés
- Fournir un accès aux ressources d'entreprise sans interrompre l'expérience de l'utilisateur
- Se prémunir contre les menaces qui pèsent sur les applications et les données de l'entreprise
- Sécuriser les connexions aux applications professionnelles

Apple accorde une très grande importance à la confidentialité des données personnelles.

Grâce au processus d'inscription utilisateur et aux fonctions de protection de la vie privée d'Apple, les administrateurs Apple ne peuvent que configurer le compte professionnel d'un appareil. Il leur est impossible d'accéder au compte personnel et ce, quelles que soient les circonstances.

Apple impose des limites infranchissables à ce que les organisations peuvent faire avec la gestion des appareils mobiles (MDM).

Avec une MDM

Le service informatique peut :

- Configurer les comptes
- Accéder à l'inventaire des applications gérées
- Supprimer uniquement les données gérées
- Installer et configurer des applications
- Exiger un code d'accès de six caractères
- Appliquer certaines limitations
- Configurer le VPN par application

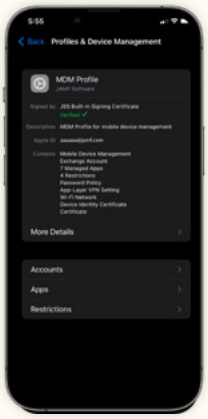
Le service informatique ne peut pas :

- Consulter les données personnelles, les données d'utilisation ou les journaux
- Accéder à l'inventaire des applications personnelles
- Supprimer des données personnelles
- Prendre le contrôle de la gestion d'une application personnelle
- Exiger un code secret ou un mot de passe complexe
- Accéder à la localisation de l'appareil
- Accéder aux identifiants uniques des appareils
- Effacer à distance l'intégralité de l'appareil
- Gérer le verrouillage d'activation
- Accéder à l'état d'itinérance
- Activation du mode Perdu

SOURCE : APPLE. « INSCRIPTION DES UTILISATEURS ET MDM. »

Jamf, un atout pour le BYOD

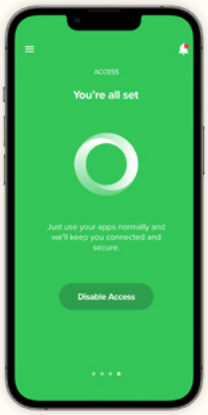
Nos solutions se coordonnent pour gérer et sécuriser les applications, les données et les connexions professionnelles selon le principe **Trusted Access**. Quant aux utilisateurs, ils ont la garantie que leur vie privée est préservée.



Une méthode d'inscription des appareils qui protège la vie privée

Jamf Pro sépare les comptes professionnels et personnels grâce à l'inscription par l'utilisateur d'Apple. L'organisation n'a ainsi aucune visibilité ni aucun contrôle sur les données personnelles.

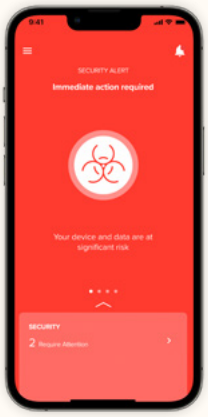
- Configurez l'accès aux services de l'entreprise : Wi-Fi, e-mail et contacts.
- Distribuez et gérez l'ensemble de la bibliothèque d'applications iOS ou iPadOS professionnelles.
- Déployez des règles pour prévenir les pertes de données et empêcher toute circulation d'informations entre applications gérées et non gérées.
- Offrez aux utilisateurs l'expérience Apple qu'ils attendent, lors de l'inscription comme au quotidien.



Sécurisez les connexions et l'accès

Jamf Connect veille à ce que seuls des utilisateurs autorisés, munis d'appareils gérés, puissent accéder aux applications et aux données de l'entreprise. Jamf Trust est l'application de Jamf Connect destinée à l'utilisateur final.

- Chiffrez et sécurisez la connexion aux applications de l'entreprise avec l'accès réseau zero-trust (ZTNA).
- Gérez le trafic réseau à l'échelle de chaque application et redoublez la protection de la confidentialité grâce au VPN par application



Protection des terminaux mobiles

Jamf Protect renforce le cadre de sécurité déjà solide d'Apple pour protéger les données de l'entreprise. Jamf Trust est l'application de Jamf Protect destinée à l'utilisateur final.

- Gérez les risques liés aux applications grâce à des workflows de validation qui suppriment les logiciels vulnérables et mal sécurisés
- Détectez et interceptez les attaques de type « Homme du milieu » (MitM)
- Effectuez des contrôles de sécurité pour repérer les versions obsolètes ou vulnérables des systèmes d'exploitation (OS)

Expérience des employés

Offrez aux utilisateurs Apple l'expérience qu'ils attendent lorsqu'ils accèdent aux ressources professionnelles.

Le BYOD ne fonctionne que si les employés savent que leur organisation n'a pas accès à leurs données personnelles et si leur expérience utilisateur est intacte. Jamf et Apple font les deux.

Inscription des utilisateurs avec Jamf Pro :

- Assure la transparence de la façon dont l'informatique gère les appareils personnels, avant et pendant l'inscription.
- Permet aux employés d'utiliser les applications Apple natives à des fins personnelles et professionnelles en toute simplicité.
- Donne aux employés la liberté de télécharger eux-mêmes des applications approuvées grâce au **Self Service**
- Les utilisateurs conservent leur identifiant Apple personnel pour leurs propres données et reçoivent identifiant Apple géré pour celles de l'entreprise.
- Réduit le risque de phishing grâce à l'inscription des utilisateurs basée sur le compte : les utilisateurs s'authentifient à l'aide d'un ID Apple géré avec l'application Réglages.

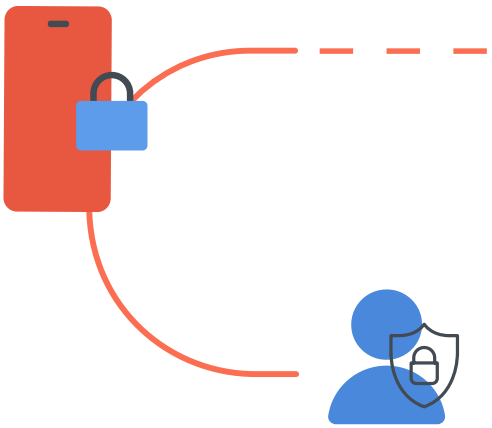
Jamf Trust : sécurité du BYOD mobile

Pour préserver la sécurité et la productivité de tous, il faut de la simplicité. Les administrateurs déploient **Jamf Trust** sur les appareils des employés. C'est cette application unique qui délivre les fonctionnalités d'accès et de sécurité de Jamf Connect et Jamf Protect sur les appareils mobiles. Jamf Trust ne fonctionne que sur le compte professionnel de l'appareil, préservant ainsi la confidentialité du compte personnel.

Jamf connaît Apple.

Les solutions de BYOD doivent impérativement être spécifiques aux OS pour garantir la sécurité de l'organisation et des accès, et permettre la configuration des appareils. La convivialité, la sécurité et les fonctionnalités de confidentialité d'Apple offrent aux organisations et à leurs équipes un environnement idéal pour inscrire des appareils en BYOD. Et personne ne connaît mieux Apple que Jamf.

Contactez votre représentant Jamf ou votre revendeur habituel pour découvrir comment Jamf peut renforcer à la fois la sécurité de votre organisation et la confidentialité de vos employés.



Demander une version d'essai