jamf

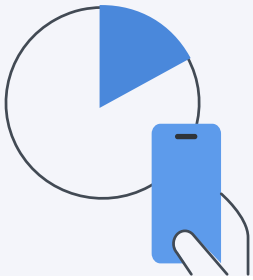
# BYOD mobile avec Jamf : **sécurité, confidentialité, simplicité.**

Selon le récent rapport **Security 360** de Jamf, « en 2022, **21 % des employésutilisaient des appareils** mal configuré et donc **à risque**. »

Les appareils qui accèdent aux ressources professionnelles doivent avoir une configuration à la hauteur.

## Les employés utilisent leur mobile – avec ou sans autorisation

**17 %** des employés **utilisent leurs appareils personnels** pour le travail sans en parler au service informatique.



SOURCE : ZIPPIA

## Le BYOD doit être utilisable, sécurisé et privé.

Si vous sécurisez la partie professionnelle des appareils, tout en facilitant l'utilisation parallèle des applications professionnelles et personnelles, vos employés seront plus enclins à les utiliser. Une chose doit être parfaitement claire : ces appareils offrent les mêmes garanties de confidentialité que ceux qui ne sont pas inscrits dans un programme BYOD. Avec Jamf, les administrateurs peuvent :

- Configurer des réglages s'appliquant uniquement aux aspects professionnels
- Sécuriser les connexions aux applications professionnelles
- S'appuyer sur la solidité du cadre de sécurité d'Apple
- Séparer les volumes professionnels et personnels pour préserver la confidentialité de l'utilisateur final.

**Avec Apple, découvrez les possibilités et les limites de la MDM.**

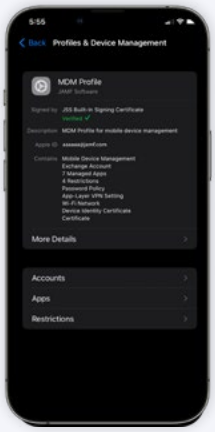
## Jamf, un atout pour le BYOD

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 volumes 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.

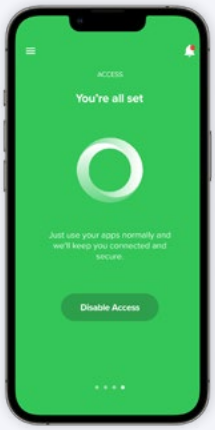
- Configurez l'accès aux services de l'entreprise : Wi-Fi, e-mail et contacts.
- Distribuez et gérez l'ensemble de la bibliothèque d'applications iOS ou iPadOS professionnelles.
- Déployez des règles pour prévenir les pertes de données et empêcher toute circulation d'informations entre applications gérées 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
- Protégez les réseaux et les appareils des logiciels malveillants
- Détectez et interceptez les attaques de type « Homme du milieu » (MitM)
- Effectuez des contrôles de sécurité pour repérer les versions obsolètes ou vulnérables des OS


jamf

www.jamf.com/fr/

Centralisez toutes ces capacités avec le forfait Business de Jamf. **Demandez une version d'essai**

Ou contactez votre représentant Jamf ou votre revendeur habituel.



*Mis à jour en février 2022*