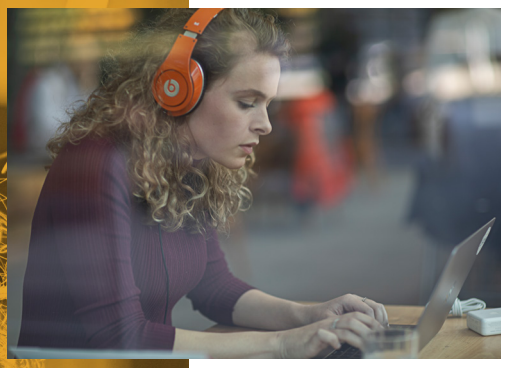
jamf

Jamf et Apple : une **meilleure approche** du BYOD

Encouragez l'adoption du BYOD en équilibrant sécurité informatique et respect de la vie privée et des données des utilisateurs.



En s'affirmant comme les champions inégalés de la productivité personnelle, l'iPhone et l'iPad ont permis l'avènement d'une génération de professionnels modernes, mobiles et toujours connectés. Et cela représente un défi de taille pour la gestion informatique.

Les éléments clé du succès du BYOD

Réduire les problèmes de sécurité informatique + Réduire les coûts et la complexité des programmes + Garantir la confidentialité des utilisateurs + Offrir une expérience utilisateur familière = Augmenter l'adoption par les utilisateurs

Les appareils mobiles sont partout, et la plupart des employés apportent leur appareil personnel au travail, que ce soit pour des raisons professionnelles ou personnelles. Mais les tentatives faites ces dernières années pour exploiter leur potentiel n'ont pas toujours été couronnées de succès. De nombreux programmes BYOD (utilisation des appareils personnels en entreprise), excellents dans leur conception, restent imparfaits dans leur mise en œuvre. Les employés fournissent le matériel, les organisations fournissent l'accès, mais cette pratique a deux écueils opposés : l'excès de gestion ou le manque de service aux utilisatuers.

En effet, le contrôle exercé par le cadre de gestion des appareils mobiles peut s'avérer trop étroit : le service informatique voit toutes les applications présentes sur l'appareil, qu'elles soient professionnelles ou personnelles. Il a également la capacité de verrouiller, déverrouiller ou effacer l'ensemble de l'appareil. De toute évidence, le propriétaire n'aime pas renoncer au contrôle total de son appareil personnel, et encore moins que sa vie privée soit exposée – même si ce n'est qu'une impression.

Il existe une autre méthode de gestion des appareils BYOD : la gestion des applications mobiles. Elle permet à l'informatique d'appliquer des règles d'entreprise à des applications spécifiques fournies sur l'appareil. Mais cette approche est limitée : impossible, pour l'informatique, de fournir d'autres services comme la configuration sécurisée du WiFi et du VPN, ou d'imposer l'utilisation de codes d'accès et d'autres réglages de sécurité. Toutes ces mesures sont pourtant indispensables pour donner aux employés un accès fiable et sécurisé aux ressources dont ils ont besoin. En l'absence de règles d'entreprise de base, ces employés se sentent mal servis et l'informatique craint les vulnérabilités de sécurité.

En réalité, le succès – ou l'échec – d'un programme BYOD dépend à la fois du confort de l'organisation et de l'utilisateur. Il faut trouver un juste équilibre entre le contrôle informatique, sécurisation des appareils et respect de la vie privée. Ce document présente une stratégie pour trouver cet équilibre et assurer le succès du BYOD.

Les utilisateurs tiennent au respect de leur vie privée.

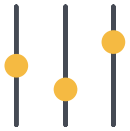
Nos appareils personnels contiennent les données les plus confidentielles : correspondance personnelle, photos, contacts, documents. Même le choix des apps installées sur l'appareil peut révéler des informations très privées sur nos passe-temps, nos habitudes et notre mode de vie. En inscrivant leur appareil personnel dans un système de gestion des appareils mobiles (MDM) contrôlé par le groupe informatique de leur organisation, la plupart des employés craignent de donner accès à ces informations. Et on comprend qu'ils soient réticents.

Lorsqu'elles se traduisent par un refus, ces réticences sont une raison fréquente de l'échec des programmes BYOD, même si les administrateurs informatiques n'ont pas réellement accès aux données personnelles. C'est un sujet crucial, et les utilisateurs sont de plus en plus sensibles à toute compromission de la confidentialité au nom du contrôle informatique.

La sécurité, une priorité pour l'informatique

Pour le responsable informatique, l'idée que des appareils personnels puissent accéder librement aux ressources internes, sans connaître leur configuration ni leurs réglages de sécurité, est un véritable cauchemar. **Les appareils mobiles sont couramment la cible d'attaques par logiciels malveillants ou par hameçonnage**. Ils représentent un vecteur potentiel d'intrusion lorsqu'ils sont connectés au réseau d'une organisation.

Sans aucune visibilité ni aucun contrôle sur ces terminaux, il est impossible de mettre en œuvre une sécurité informatique efficace. C'est cet impératif de sécurité qui incite les organisations à utiliser la MDM pour leur programme BYOD. Elles doivent donc demander à leurs employés d'enrôler leur appareil personnel avant de leur donner accès au réseau interne, à la messagerie, aux calendriers, au VPN et autres outils.



Quelques contrôles de gestion BYOD

Les administrateurs informatique peuvent :

- Verrouiller l'appareil
- Appliquer les configurations de l'entreprise – Wi-Fi, VPN, messagerie et codes d'accès
- Installer et supprimer les apps et livres de l'entreprise et les données associées
- Collecter des informations de sécurité à partir de l'appareil
- Ajouter/supprimer des restrictions pour protéger les données de l'entreprise

Les administrateurs informatiques ne peuvent pas :

- Effacer les données personnelles – photos, courrier personnel, contacts, etc.
- Supprimer des apps personnelles
- Consulter des données privées (ce qui inclut le nom des apps personnelles)
- Limiter l'utilisation de l'appareil ou l'installation d'apps personnelles
- Suivre la localisation de l'appareil
- Supprimer ce qui a été installé par l'utilisateur
- Recueillir les informations de l'utilisateur à partir de l'appareil

Trouver le juste équilibre

Les préoccupations des employés sont aussi valables que celles de l'informatique. Les premiers ne veulent avoir qu'un seul appareil, mais sans donner ni accès ni contrôle sur leurs données privées. L'informatique cherche à réduire les coûts en achetant moins d'appareils d'entreprise, mais doit assurer la sécurité de l'organisation. Dans de nombreuses entreprises, ces tiraillements ont signé l'échec du programme BYOD.

Pourtant, on peut répondre à ces deux préoccupations en repensant le rôle de la MDM dans le cadre du BYOD. Plutôt qu'une approche générique, les responsables informatiques peuvent choisir une MDM conçue pour le BYOD. Cette solution protègera la vie privée des employés tout en fournissant des contrôles de sécurité solides pour répondre aux besoins de l'informatique.

Le BYOD pour les équipes d'aujourd'hui

Les entreprises les plus en pointe choisissent un ensemble de fonctionnalités spécialement conçues pour le BYOD. L'objectif : répondre aux besoins des deux parties, sans complexités inutiles ni coûts supplémentaires. Il est important que l'informatique et l'utilisateur final comprennent bien les avantages d'un programme BYOD conçu pour eux. Assurer la réussite du programme exige également de communiquer les avantages d'un programme BYOD et de faire preuve de transparence auprès des employés : on apaisera ainsi toute tension liée à l'utilisation d'un appareil personnel au travail. Voici quelques avantages clés d'un programme BYOD bien pensé, pour l'entreprise comme pour ses employés.

Tout le monde doit y gagner

Avantages pour les employés

Une expérience familière, à la fois personnelle et professionnelle, dans un seul appareil :

- Transparence des capacités de gestion informatique des appareils personnels avant l'enrôlement, pour garantir la protection des données personnelles de l'utilisateur.
- Accès sécurisé aux ressources d'entreprise – e-mails, calendriers, Wi-Fi et apps – pour favoriser la productivité.

Avantages pour l'organisation

Un équilibre entre sécurité et respect de la vie privée, dans un seul appareil :

- Sécurisation de l'appareil et de l'accès aux données et ressources de l'entreprise, pour préserver les employés et leur productivité
- Contrôle des coûts grâce à la baisse des acquisitions d'appareils

Le BYOD avec Jamf et Apple

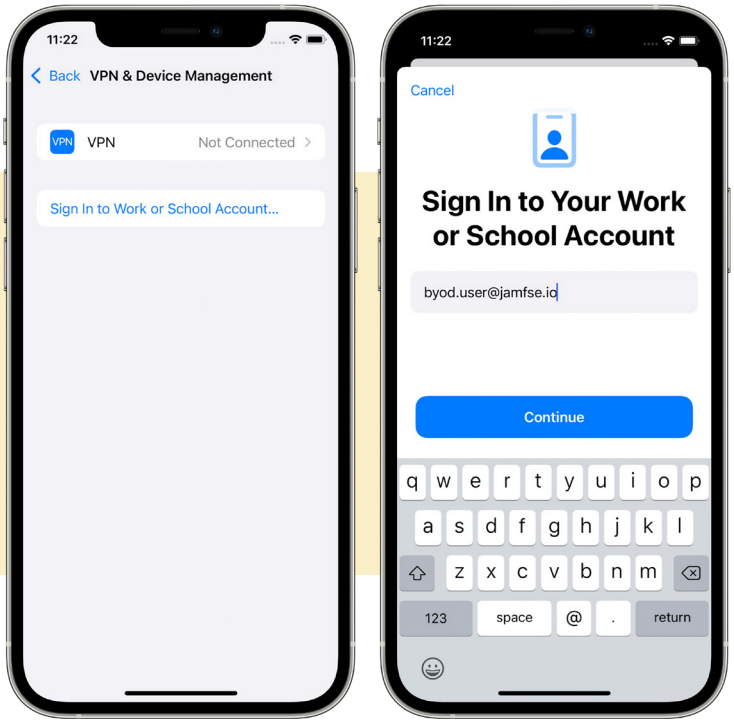
Comme le souligne cet article, l'objectif est de trouver un juste milieu pour les appareils personnels. Sans tomber dans un excès de gestion, l'informatique doit avoir les moyens de bien servir ses utilisateurs et son organisation, en offrant un accès facile et sécurisé aux logiciels et aux apps utiles. C'est dans cette optique que Jamf prolonge les capacités et les atouts d'Apple pour optimiser les programmes BYOD.

L'**enrôlement des utilisateurs basée sur le compte** d'Apple met l'accent sur la sécurité et la confidentialité. Cette méthode BYOD, axée sur les appareils iOS et iPadOS, rationalise le processus d'inscription des utilisateurs pour leur donner un accès entreprise, tout en préservant le caractère confidentiel de leur appareil personnel. Grâce à ce nouveau workflow, les entreprises peuvent enrôler les appareils mobiles de leurs employés exploitant iOS ou iPadOS 15 et plus avec Jamf Pro (à partir de la version 10.33).

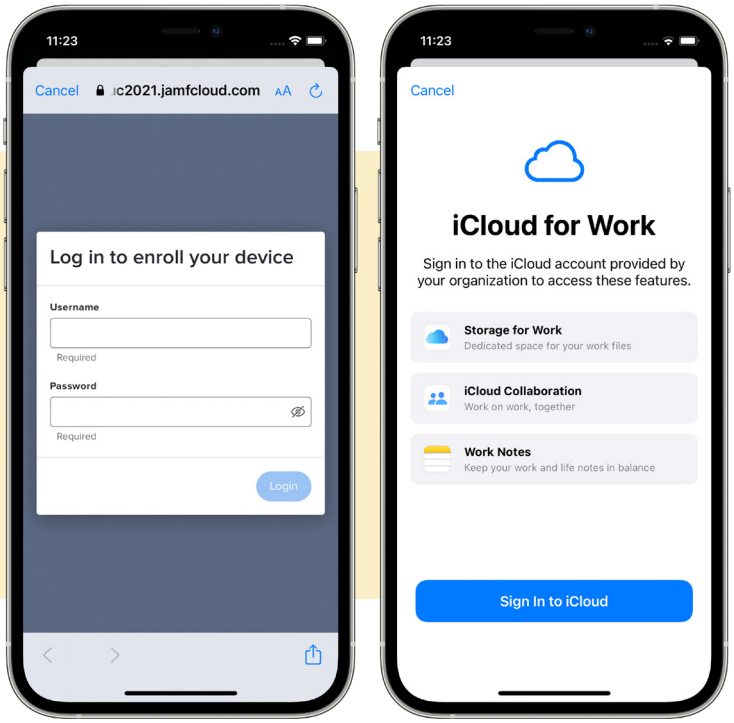
L'enrôlement des utilisateurs basé sur le compte sépare les données personnelles des données institutionnelles en leur associant deux identifiants différents : un Apple ID personnel pour les premières, et un Apple ID géré pour les secondes. Jamf Pro a adopté la fonction de découverte des services d'Apple : elle permet d'exploiter différentes configurations qui associent la gestion à l'employé et son usage professionnel de l'appareil plutôt qu'à l'appareil proprement dit. L'utilisateur accède ainsi à ses données d'entreprise de manière sécurisée, sans que l'informatique n'ait à toucher l'appareil ni à lui envoyer un lien d'inscription. L'employé bénéficie même du Jamf Self Service pour installer des applications d'entreprise. Il n'a qu'une opération très simple et familière à réaliser : ouvrir les réglages généraux. Cette expérience a l'avantage d'inspirer confiance à l'utilisateur. Elle se rapproche également du déploiement zero-touch pour l'informatique, avec l'intérêt d'un accès sécurisé aux ressources de l'organisation.

Voici comment cela fonctionne :

1 L'utilisateur s'authentifie sur l'appareil à l'aide d'un identifiant Apple géré en accédant à Réglages > Général > VPN et gestion des appareils, puis se connecte à son compte professionnel ou scolaire avec son identifiant Apple géré. Après avoir saisi l'Apple ID géré, il appuie sur Continuer.



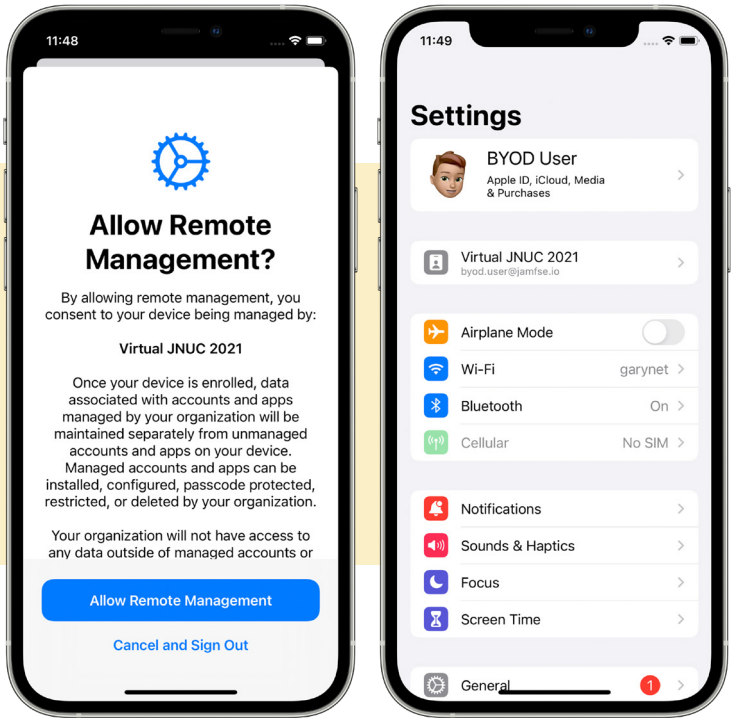
2 Le portail d'enrôlement s'affiche et invite l'utilisateur à saisir son compte utilisateur Jamf Pro ou ses identifiants d'annuaire (LDAP ou Azure AD, par exemple). Il appuie ensuite sur Connexion. L'utilisateur se connecte alors à iCloud avec l'adresse e-mail de son identifiant Apple géré et son mot de passe lorsqu'il y est invité.



3

Il est ensuite invité à autoriser la gestion à distance et le téléchargement du profil MDM sur l'appareil.

Et c'est tout ! C'est une expérience simple pour l'utilisateur final, mais elle assure à l'organisation une sécurité de niveau entreprise.



Une couche de protection supplémentaire

Le **Relais privé** est un nouveau service iCloud qui protège la confidentialité d'une personne en masquant son adresse IP et sa localisation aux sites web qu'elle visite. L'introduction du Relais privé fait suite au lancement de Jamf Private Access, la solution Jamf qui sécurise l'accès aux applications professionnelles sans les problèmes de performance, de confidentialité et de sécurité des connexions VPN. À présent, avec le Relais privé et **Jamf Private Access**, les utilisateurs sont protégés lors de leurs navigations privées et professionnelles. Jamf peut être déployé sur des appareils personnels pour protéger et router le trafic professionnel. La navigation personnelle, acheminée via le Relais privé, reste confidentielle.

Avec le Relais privé et Jamf Private Access, les employés sont protégés par une sécurité de niveau entreprise qui respecte leur vie privée. En utilisant à la fois Jamf Private Access et le Relais privé iCloud+, ils bénéficient d'une approche optimale de la confidentialité et de la sécurité, sans compromis sur les performances.

Conclusion

Un programme BYOD réussi est un avantage pour les employés comme pour les administrateurs informatiques. Avec la bonne solution MDM, l'informatique peut se consacrer aux besoins critiques de l'entreprise sans subir les frictions de la technologie ou des utilisateurs. Les utilisateurs bénéficient d'une expérience confortable et familière sur leur appareil personnel, sans ressentir l'intrusion de l'informatique.

Découvrez-en plus sur l'**enrôlement des utilisateurs BYOD** et voyez comment Jamf avec Apple peut donner vie à vos plans BYOD en **demandant une version d'essai.**