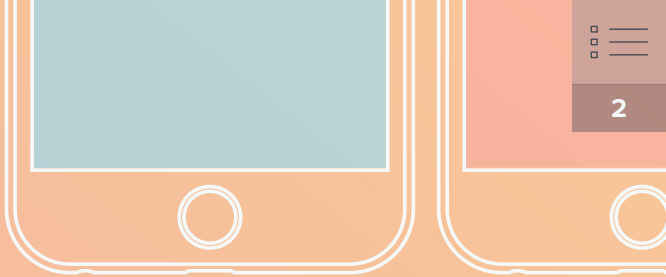
La sécurité des appareils Apple

UNE INTRODUCTION

Une cyberattaque bien planifiée ou un téléchargement accidentel de logiciel malveillant peut faire la différence entre une journée productive et une interruption totale de votre activité. Les pirates informatiques utilisant des techniques de plus en plus sophistiquées, les entreprises soucieuses de leurs résultats financiers et de la sécurité des données de leurs clients, employés ou étudiants doivent garder le contrôle de la sécurité.



Les problèmes qui touchent la sécurité Apple, comme tous les problèmes de sécurité informatique, sont bien réels.

Même si Apple a beaucoup investi dans ses fonctionnalités de sécurité, devenant rapidement le leader en matière de confidentialité et de sécurité des appareils et des données, aucun système d'exploitation n'est à l'abri.

Cela signifie que les administrateurs doivent non seulement réagir rapidement aux problèmes de sécurité, mais aussi s'en prémunir de manière proactive.

Ce guide s'adresse aux administrateurs qui veulent améliorer la sécurité de leurs appareils Apple au sein de leur entreprise. En outre, il offre des informations de base pour les nouveaux venus ou un simple rafraîchissement pour les habitués de la gestion Apple.

Introduction à la sécurité Apple

Les éléments de base

Plusieurs facteurs interagissent pour assurer la sécurité du matériel et des données de votre entreprise. Ils peuvent être classés en six catégories principales :

Sécurité native Apple

Systèmes de sécurité déjà intégrés à macOS, iOS et tvOS

Page 4

Sécurisation des appareils

Protection de vos appareils physiques et de leurs utilisateurs

Page 6

Chiffrement des données

Les bases du chiffrement des données au repos et en transit

Page 8

Surveillance de la conformité

Surveillance des appareils pour identifier les mises à jour nécessaires

Page 11

Sécurité des applications et des correctifs

Mise à jour constante des logiciels

Page 12

Déploiements sécurisés

Déploiement avec le plus haut niveau de sécurité disponible

Page 14

I. Sécurité native Apple

Optimisation grâce à la gestion des appareils

Les fonctionnalités de sécurité intégrées à macOS (système d'exploitation pour Mac), iOS (système d'exploitation pour iPad et iPhone) et tvOS (système d'exploitation pour Apple TV) sont nombreuses et présentent plusieurs avantages :

- Les systèmes d'exploitation Apple reposent sur une infrastructure UNIX éprouvée et conçue pour offrir une excellente stabilité
- Infrastructure robuste de sécurité du système d'exploitation
- Sécurité de l'appareil sous la forme d'un verrouillage et d'outils de géolocalisation
- Possibilité d'implémenter et de configurer des contrôles de sécurité grâce à des options de configuration via une solution de gestion des appareils mobiles (Mobile Device Management ou MDM)

Une solution MDM peut gérer ces configurations de sécurité existantes et les déployer (en les appliquant) sur un grand nombre d'appareils. Ainsi, vous pouvez configurer non seulement un Mac en toute sécurité, mais aussi des milliers d'autres Mac. Vous disposez également de contrôles de sécurité plus étendus grâce à un outil MDM capable de verrouiller et d'effacer les appareils perdus ou dont l'entreprise se sépare.

Détails des fonctionnalités de sécurité

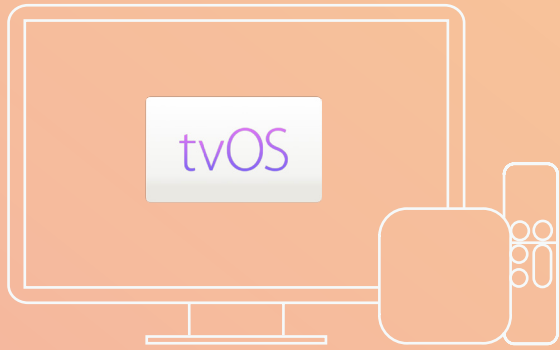
Fonctionnalités de sécurité natives pour macOS, iOS et tvOS

Fonctionnalités macOS

- Mises à jour de logiciels
- Protection de l'intégrité du système (SIP)
- Gatekeeper
- App Store
- Chiffrement FileVault
- XProtect
- Sandboxing des apps
- Réglages de confidentialité

Fonctionnalités iOS

- Mises à jour de logiciels
- Système sécurisé
- App Store
- Touch ID
- Chiffrement matériel
- Sandboxing des apps
- Confidentialité
- Supervision
- Recherche à distance des appareils perdus



Fonctionnalités tvOS

- Mises à jour directes des logiciels par Apple
- Apps de l'App Store validées et sécurisées
- Supervision (avec MDM)
- Restrictions d'apps
- Réglages et mots de passe AirPlay
- Bannière/écran par défaut

II: Sécurisation des appareils

Suivi, sécurisation et protection des appareils et des utilisateurs

L'un des moyens les plus simples de porter atteinte à la sécurité d'une entreprise, ou de compromettre la sécurité de l'utilisateur final, consiste à accéder à un seul appareil. Que votre organisation propose ses services à des étudiants, des enseignants, du personnel de santé, des salariés itinérants, des employés en magasin ou des employés souvent en déplacement, vos appareils peuvent à tout moment se trouver dans plusieurs endroits différents.

Appareils perdus ou volés

La perte ou le vol d'un iPad, d'un iPhone ou d'un Mac n'est pas seulement une perte financière : c'est un risque de sécurité majeur. Les dommages peuvent être incalculables si un voleur parvient à accéder aux données privées d'étudiants ou à l'ensemble de la base de données de l'organisation à partir d'un ordinateur portable. Ou si une ancienne employée a gardé son ordinateur portable de travail et publie des informations privées ou les communique à des concurrents. Sans oublier l'installation d'un logiciel malveillant à partir d'une source distante.

Il arrive que des appareils soient perdus ou volés. Personne n'est à l'abri d'un accident ou d'un moment d'inattention, et il est donc crucial de trouver une solution qui intègre le fait qu'un utilisateur perdra, a un moment ou un autre, un appareil.

Par ailleurs, de nombreux appareils — en particulier ceux destinés aux étudiants, aux patients, ou ceux partagés par plusieurs utilisateurs — doivent être protégés contre une mauvaise utilisation, un accès accidentel aux données d'autrui ou l'affichage d'un contenu inapproprié.

Sécurisation ou restriction manuelles des appareils :

Mac

- Exigez un code d'accès sur tous les appareils
- Activez Localiser mon Mac dans les Préférences Système — > iCloud
- Chaque utilisateur doit se connecter à iCloud et mémoriser son code d'accès
- Effectuez un suivi de tous les numéros de série des Mac
- Signalez à Apple la perte ou le vol d'un appareil
- Activez les contrôles parentaux sur l'appareil pour bloquer les sites web (ceci n'affecte que le navigateur Safari)

iPad and iPhone

- Exigez un code d'accès sur tous les appareils
- Activez Localiser mon iPhone dans les Préférences Système — > iCloud
- Chaque utilisateur doit se connecter à iCloud et mémoriser son code d'accès
- Signalez à Apple la perte ou le vol d'un appareil
- Activez les contrôles parentaux sur un appareil individuel, en créant des comptes différents pour chaque appareil

Apple TV

- Exigez un code d'accès sur toutes les Apple TV
- Restrictions d'utilisation :
  - Dans le menu principal, accédez à Réglages > Général > Restrictions
  - Sélectionnez Restrictions pour activer cette option
  - À l'invite, créez un code d'accès à quatre chiffres
  - Saisissez à nouveau les quatre chiffres pour confirmer, puis sélectionnez OK
  - Assurez-vous de bien mémoriser le code d'accès
  - Répétez cette procédure pour toutes les Apple TV

Sécurisation des appareils

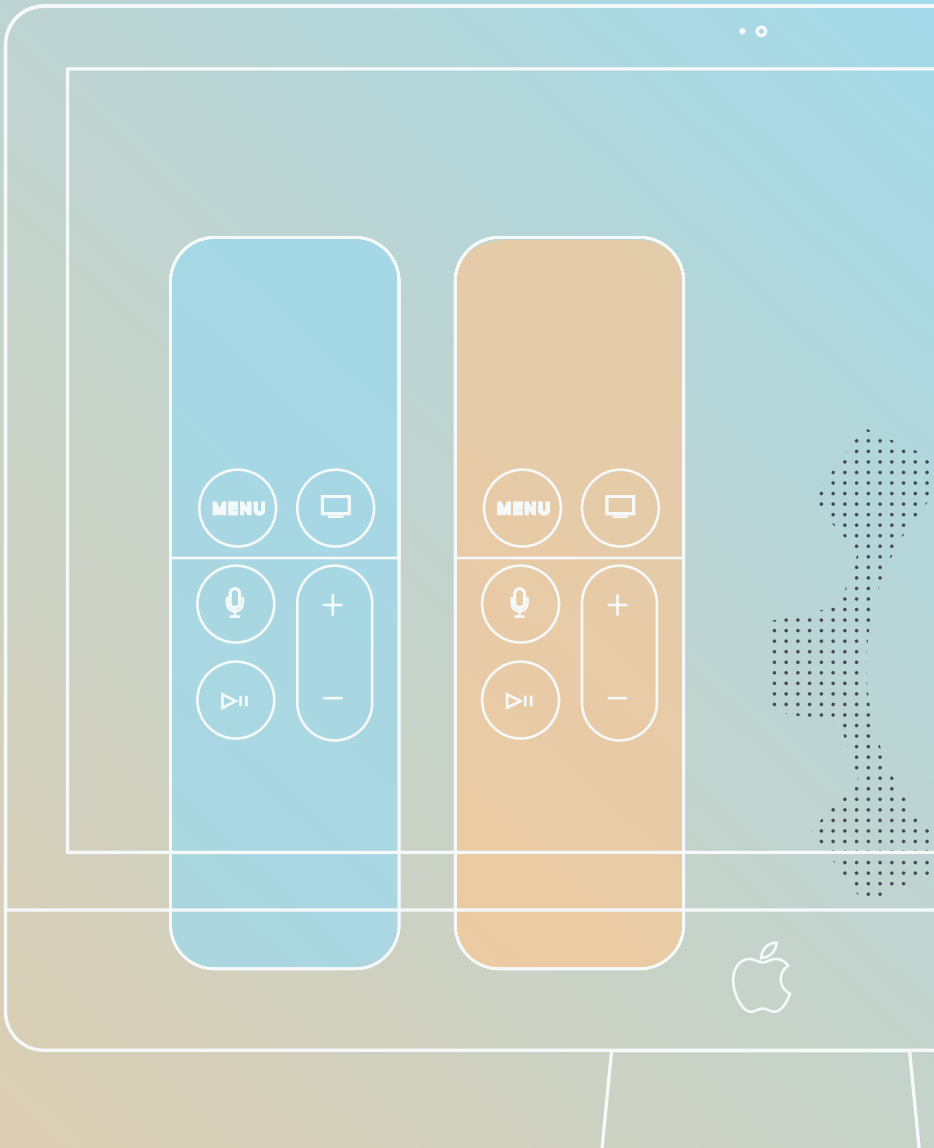
Restreindre AirPlay pour l'Apple TV :

- Dans le menu principal, accédez à Réglages — > Sélectionnez AirPlay
- Activez ou désactivez AirPlay
- Choisissez une des options suivantes :
  - Tous
  - Tout utilisateur du même réseau
- Répétez cette procédure pour toutes les Apple TV

Sécurisation ou restriction des appareils avec une solution MDM comme Jamf :

Mac, iPad, iPhone et Apple TV :

- Définissez toutes les restrictions et fonctionnalités de sécurité dès la première utilisation, ou configurez les appareils à l'aide de profils ou de règles
- Verrouillez de manière centralisée tout appareil perdu ou détourné
- Effacez de manière centralisée tout appareil perdu ou détourné
- Autorisez plusieurs utilisateurs à partager des appareils en toute sécurité, en tirant parti de leurs propres connexions avec leurs propres réglages, ou en effaçant l'appareil entre chaque utilisation, par exemple avec des patients



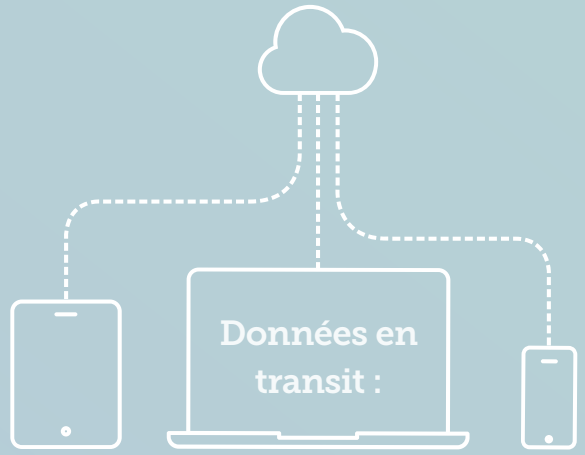
III: Chiffrement des données

Bases de données au repos et en transit, et sécurisation de ces deux types de données

Qu'il s'agisse d'une école qui protège les informations sur ses élèves, d'un établissement de santé qui protège les dossiers médicaux de ses patients ou d'une entreprise qui protège sa propriété intellectuelle, le chiffrement est essentiel pour les organisations. La meilleure stratégie dans ce domaine consiste à chiffrer toutes les données stockées sur les appareils.

Il existe deux types de données :

chiffrement du disque ou de l'appareil.



Un réseau privé virtuel (Virtual Private Network ou VPN) peut protéger les données lors de leur transfert sans fil d'un appareil à un autre service.

Chiffrement des données

Données au repos :
chiffrement du disque ou de l'appareil.

- macOS intègre déjà un chiffrement du disque : FileVault. Inutile d'installer un logiciel supplémentaire pour chiffrer un disque sur Mac.
- FileVault est certifié FIPS 140-2. Cela signifie que le système de chiffrement Apple répond aux normes de chiffrement les plus élevées définies par le gouvernement.
- Vous pouvez activer FileVault manuellement ou à distance : l'utilisateur peut choisir l'option lui-même sur un appareil, ou le service informatique peut activer FileVault (via Jamf) sur des centaines voire des milliers d'appareils.
- Jamf s'assure que les clés de chiffrement sont stockées de manière centralisée au cas où vous auriez besoin de récupérer des données, si un employé quitte l'entreprise ou si un utilisateur a oublié son code d'accès.

Pour activer manuellement FileVault :

1. Accédez aux Préférences Système —> Sécurité et confidentialité —> FileVault
2. Basculez le bouton pour activer l'option
3. Répétez la procédure pour tous les appareils

Pour activer FileVault sur tous les appareils de votre entreprise, utilisez une solution MDM afin d'automatiser, déployer et appliquer le chiffrement.

Vous pouvez déployer un profil de configuration ou une règle qui active FileVault, et le service informatique peut récupérer les clés de chiffrement si le personnel a besoin de déchiffrer un appareil en cours de route.

1. Créez un profil de configuration en sélectionnant quelques options dans Jamf
2. Déployez le profil sur autant d'appareils que vous le souhaitez
3. Il n'y a pas de 3ème étape

Jamf vous permet également de configurer la redirection de la clé de secours, même si l'utilisateur active lui-même FileVault. La clé sera alors sauvegardée dans la solution de gestion utilisée par le service informatique.

Qu'en est-il de l'iPad ou de l'iPhone ?

Le chiffrement des appareils iOS est encore plus simple puisque ces derniers intègrent déjà un chiffrement dès qu'un code d'accès est défini. Vous pouvez effectuer cette opération individuellement ou depuis Jamf, mais aussi configurer les réglages du code d'accès comme sa longueur et sa complexité.

Chiffrement des données

Données en transit :

Un réseau privé virtuel (Virtual Private Network ou VPN) peut protéger les données lors de leur transfert sans fil d'un appareil à un autre service.

Les personnes en déplacement ou qui travaillent à distance devraient utiliser un VPN pour se connecter au réseau de votre organisation. Cette bonne pratique crée une connexion sécurisée au réseau de votre organisation, ce qui garantit le chiffrement de bout en bout des données que vous envoyez.

Configuration requise

- Une connexion réseau sécurisée
- Un serveur VPN

macOS et iOS intègrent tous deux des clients VPN pour vous permettre de vous connecter à un certain nombre de fournisseurs de services VPN reconnus.

Comment activer le chiffrement ?

Pour vous connecter manuellement à un VPN :

Après avoir configuré un fournisseur de VPN :

1. Accédez à Préférences—> Réseau
2. Entrez l'adresse du serveur VPN sur l'appareil
3. Sélectionnez le VPN dans les options de votre réseau
4. Répétez la procédure pour chaque appareil

Pour connecter plusieurs appareils à un VPN :

Après avoir configuré un fournisseur de VPN :

1. Créez un profil de configuration dans une solution MDM comme Jamf pour iOS et/ou Mac
2. Déployez les configurations sur autant d'appareils que vous le souhaitez
3. Ici aussi, il n'y a pas de 3ème étape

Comment vérifier le bon fonctionnement du chiffrement ?

Une des meilleures façons d'assurer la sécurité et un chiffrement homogène consiste à héberger votre solution MDM dans le cloud. Avec un produit réputé comme Jamf Cloud, vous avez la garantie que votre serveur est sécurisé, que vos données sont protégées et que les mises à jour ou correctifs sont immédiatement disponibles.

IV: Surveillance de la conformité

S'assurer que les protocoles et les contrôles ont été installés sur tous les appareils.

La qualité d'un système de sécurité se juge avant tout par son point faible. Pour garantir une couverture optimale, les administrateurs doivent surveiller les appareils de l'entreprise et vérifier que chaque appareil est mis à jour, dispose des correctifs les plus récents et que les options de chiffrement appropriées sont activées.

Surveillance manuelle de la conformité

Pour vous assurer que tous les appareils de votre organisation sont protégés, soumettez ces appareils à un audit continu.

1. Localisez physiquement chaque appareil
2. Passez en revue chaque option individuellement pour vous assurer que :
   - Les logiciels disposent des dernières mises à jour
   - Le chiffrement est activé
   - Personne n'a installé un logiciel malveillant ou un virus
3. Vérifiez que vous avez installé les dernières mises à jour disponibles
4. Répétez régulièrement ces étapes
5. Cette procédure nécessite une vigilance constante ainsi qu'un haut niveau d'implication et de coopération de la part des utilisateurs finaux.

Surveillance de la conformité avec Jamf

Pour vous assurer que tous les appareils de votre organisation sont protégés à l'aide de la fonctionnalité de gestion de l'inventaire de Jamf :

1. Consultez des informations actualisées et en temps réel sur tous les appareils
2. Déployez des mises à jour et des configurations de sécurité sur tout appareil qui n'est pas correctement sécurisé
3. Vous l'avez deviné : il n'y a pas de 3ème étape

La possibilité d'afficher l'état des appareils aide les administrateurs à identifier quelles mises à jour envoyer et vers quels appareils, et quelles fonctionnalités de sécurité il faut configurer. Des groupes intelligents dynamiques basés sur le service, les autorisations, les appareils ou toute autre méthode de catégorisation permettent aux administrateurs de sélectionner des mises à jour ciblées ou globales.

V: Sécurité des applications et gestion des correctifs

Garantir la mise à jour des correctifs et la sécurité des applications

Sécurité des applications :
Vous devez absolument veiller à ce que vos applications ne contiennent aucun logiciel malveillant ou autre code hostile. Si les sources de vos applications ne sont pas fiables, votre sécurité est compromise.

Les applications disponibles sur la plateforme Apple intègrent des fonctionnalités spécifiques afin de garantir la sécurité de l'appareil et de l'utilisateurs lors du téléchargement et de l'utilisation :

- Elles intègrent un modèle de Sandboxing : chaque application évolue dans son propre espace et ne peut pas interagir avec d'autres applications. L'utilisateur ou l'administrateur doit autoriser les applications à lire ou à écrire les données partagées avec d'autres utilisateurs.
- Les applications de l'App Store ont été vérifiées pour limiter les risques au niveau de la sécurité. C'est le seul moyen d'obtenir des applications sur un appareil iOS en gardant le contrôle de la sécurité. Contraindre les utilisateurs Mac à passer par l'App Store pour leurs applications est un moyen pour les administrateurs de contrôler la sécurité de tous les appareils.
- Gatekeeper pour macOS est une fonctionnalité que les utilisateurs peuvent sélectionner ou que les administrateurs peuvent configurer sur tous les appareils (avec une solution MDM comme Jamf). Les utilisateurs ou administrateurs peuvent choisir parmi trois options Gatekeeper afin d'autoriser le téléchargement d'apps depuis les emplacements suivants :
  - Mac App Store
  - Mac App Store et développeurs identifiés
  - N'importe où

La meilleure stratégie consiste à autoriser le Mac App Store et les développeurs identifiés, surtout si vous créez vos propres applications ou re-packagez des applications. Signez vous-même vos applications pour les faire valider par Gatekeeper.

Bien que le Mac offre une option « N'importe où », il est recommandé de vérifier la source de l'application et si elle a été signée par un développeur fiable. Vous aurez ainsi la garantie que l'application n'a pas été modifiée depuis sa conception.

Configuration manuelle des options Gatekeeper :

1. Accédez à : Préférences—> Sécurité et confidentialité -> Général
2. Faites votre choix parmi les trois options disponibles
3. Répétez l'opération pour chacun des appareils de votre organisation

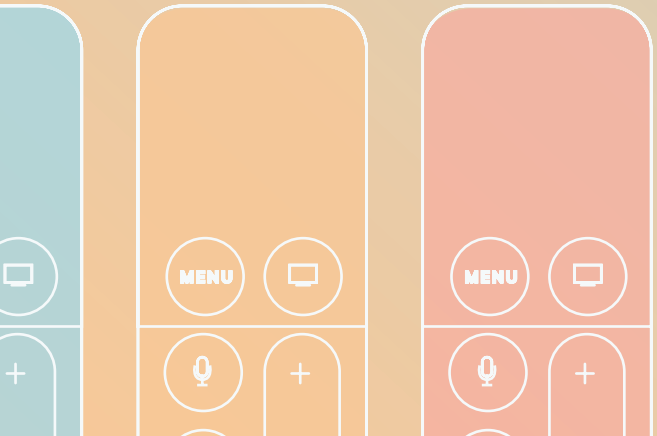
Configuration des options Gatekeeper avec Jamf :

Dans le même esprit, configurez et déployez un profil de configuration sur tous les appareils.

Sécurité des applications et gestion des correctifs

Correctifs :
Chaque logiciel contient des erreurs, parce qu'il est développé par des humains, qui risquent de faire des erreurs. Cela ne peut être évité.

C'est pourquoi il est impératif pour les organisations de mettre en œuvre une stratégie visant à intégrer une gestion des correctifs le plus rapidement possible, d'autant plus que ces bugs peuvent représenter des failles de sécurité.



Options de gestion manuelle des correctifs :

- Sensibiliser les utilisateurs à installer automatiquement les mises à jour dès qu'ils reçoivent des notifications de mise à jour sur leurs appareils.
- Lorsqu'un nouveau correctif d'une application est disponible, collectez tous les appareils puis téléchargez le correctif manuellement.
- Identifiez les appareils qui ne disposent pas des derniers correctifs lors de la surveillance manuelle de la conformité.

Toutes ces options peuvent être problématiques. Même si l'utilisateur final est bien intentionné, un manque de connaissances techniques ou un emploi du temps surchargé peut lui faire manquer une mise à jour importante. La collecte de tous les appareils chaque fois qu'une application dispose d'un nouveau correctif est un processus particulièrement chronophage. Si vous constatez que des appareils présentent des failles de sécurité non corrigées lors de la surveillance manuelle de la conformité, votre entreprise est alors vulnérable aux attaques ou aux logiciels malveillants car les appareils ne sont plus conformes.

Options de gestion des correctifs avec Jamf :

- Jamf reçoit des notifications concernant les mises à jour et les correctifs automatiques, et dispose d'outils permettant de déployer des correctifs sur tous les appareils de votre entreprise : vous ne raterez ainsi plus aucun correctif.
- Vous pouvez aider les utilisateurs à effectuer les mises à jour grâce au catalogue d'applications Self Service de Jamf, qui les avertit lorsqu'ils doivent installer une mise à jour pour pouvoir continuer à utiliser l'application.
- Vous pouvez également interdire aux personnes d'installer des mises à jour et envoyer des correctifs, grâce à des règles appliquées à tous les appareils ou à certains appareils ciblés à l'aide de groupes intelligents dynamiques.

VI: Déploiements sécurisés

Effectuez des déploiements sécurisés de vos appareils et logiciels grâce à Jamf et au programme d'inscription des appareils Apple

La première étape pour garantir des déploiements sécurisés sur tous vos appareils consiste à les enrôler dans le programme gratuit d'inscription des appareils Apple.

Avec l'enrôlement de vos appareils, vous pouvez fournir à Apple la liste des appareils appartenant à votre entreprise, en indiquant que vous souhaitez confier la gestion de ces appareils à la solution MDM de votre organisation. Puis, au premier démarrage d'un appareil enrôlé dans ce programme, l'appareil s'enrôle automatiquement auprès de la solution MDM de votre organisation, permettant des contrôles de sécurité plus stricts et des mises à jour de sécurité plus rapides, ainsi que l'application de tous les profils de configuration. Non seulement cette procédure vous fait gagner du temps, mais elle assure aussi la sécurité de votre entreprise en écartant les moindres doutes.

Jamf intègre les fonctionnalités suivantes :

Enrôlement sans intervention

Déploiement évolutif

Configurations sécurisées

Pour Mac, iPad, iPhone et Apple TV

La sécurité des appareils et des données ne doit pas être prise à la légère.

Les entreprises peuvent prévenir les attaques ou les vols en mettant en place la meilleure protection de sécurité possible via Apple. Avec Jamf, cette stratégie est encore plus facile, plus rapide et plus sûre que les protocoles de sécurité manuels.

jamf

Ne soyez pas pris par surprise et évitez toute situation pouvant entraîner une confusion. Prenez des mesures proactives pour sécuriser vos appareils et vos données afin d'assurer la sécurité et la sûreté de votre organisation et des personnes qui y travaillent.

Bénéficiez des meilleures options de sécurité pour votre entreprise en testant gratuitement un produit Jamf, ou contactez un représentant Jamf pour commencer.

Tester un produit | Nous contacter

Ou contactez votre revendeur d'appareils Apple agréé habituel pour tester Jamf.