jamf

LIVRE BLANC

La sécurité en entreprise avec Apple

Dans ce livre blanc vous découvrirez les réponses aux questions les plus fréquentes sur la sécurité et l'essentiel sur la plateforme Apple afin de vous informer sur les meilleures pratiques avant de déployer des appareils Apple dans votre entreprise.

Les sujets abordés sont les suivants:

- L'approche d'Apple en matière de gestion des appareils
- Les fonctionnalités de sécurité propres à Apple
- Les éléments à prendre en compte lors de l'implémentation de nouveaux appareils Apple
- Comment les intégrations Apple permettant de tirer davantage de votre infrastructure existante

La structure de l'écosystème Apple

Quelle approche adopter vis-à-vis de la gestion des appareils Apple?
Les plateformes iOS et macOS d'Apple sont conçues selon une approche intégrée axée sur la sécurité, qui facilite la configuration, le déploiement et la gestion des appareils. Les employés utilisant des produits Apple en entreprise s'attendent à une expérience cohérente sur tous leurs appareils. De même, les équipes informatiques devraient bénéficier de cette même cohérence lors de la gestion de macOS et iOS.

Apple propose des programmes spécifiques aux entreprises qui simplifient le déploiement et la sécurité, offrant aux utilisateurs une expérience clé en main. Le Programme d'inscription des appareils (DEP) et le Programme d'achat en volume (VPP) d'Apple, associés à la gestion des appareils mobiles (MDM), garantissent une gestion fluide et sécurisée des Mac, iPad, iPhone et Apple TV.

De nombreuses entreprises n'utilisent qu'un outil pour gérer les besoins de leurs appareils Apple, Microsoft et Google. Cela donne lieu à des lacunes en matière de gestion, d'expérience utilisateur et de sécurité. Lorsqu'un seul outil assure la gestion de plusieurs plateformes, toutes les fonctionnalités de sécurité ne sont pas exploitées, et les avantages propres à Apple sont mis de côté.

La structure Apple

Il faut commencer par les bases de la structure Apple pour comprendre sa philosophie de la sécurité.

La différence entre Apple et Microsoft du point de vue de la gestion

En quoi la gestion des terminaux de Microsoft diffère-t-elle de celle d'Apple?
La simplicité d'utilisation d'Apple est assurée par sa structure de gestion intégrée connue sous le nom de gestion des appareils mobiles (MDM). Cette solution permet aux services informatiques de créer des profils de configuration capables de définir plusieurs réglages au sein d'un système d'exploitation. Ces profils peuvent être distribués à distance, par le biais du service de notification push d'Apple (APNs). Le service de notification push maintient une connexion continue entre les appareils Apple, allégeant la charge de travail du service informatique. La solution de gestion des appareils mobiles d'Apple donne accès à des fonctionnalités que les administrateurs Windows traditionnels ne pensent pouvoir obtenir que par l'intermédiaire d'une liaison ou d'un objet de stratégie de groupe (GPO).

Le service APNs a-t-il une influence sur la posture de sécurité?
Le service APNs est un service sécurisé conçu pour transmettre des informations aux appareils iOS, watchOS, tvOS et macOS. Il constitue une couche essentielle aux programmes de déploiement Apple et aux autres fonctionnalités de sécurité, comme le verrouillage et l'effacement à distance. Les programmes d'Apple (DEP, VPP ou MDM) ne seront pas en mesure de fonctionner sans le service APNs, car ils ne peuvent pas être exploités par le biais d'une connexion proxy. Ils nécessitent l'établissement d'un canal direct avec Apple, à savoir le service APNs.

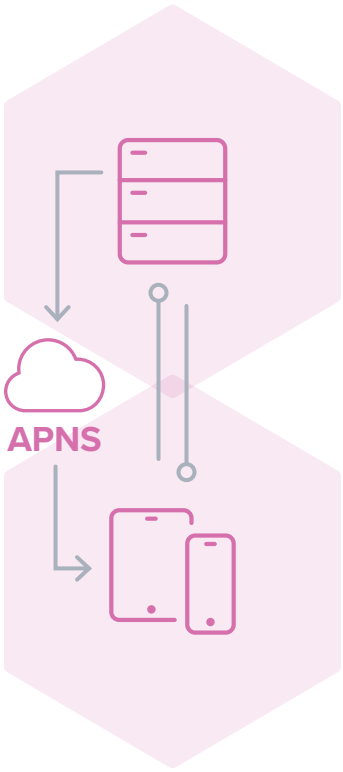
Avantages supplémentaires du service APNs :

- Amélioration de la posture de sécurité pour la gestion des ressources Apple appartenant à l'entreprise. Le service APNs permet de verrouiller ou d'effacer à distance un appareil perdu, volé ou dont la sécurité est compromise.
- La solution MDM dépend du service APNs pour l'envoi de commandes essentielles, telles que les installations de logiciels ou les mises à jour d'inventaire.
- Il est possible de distribuer les entités de profils de configuration hors ligne, mais cette méthode est nettement plus compliquée que la gestion à distance.
- Le service APNs déclenche le check-in automatique de chaque appareil auprès du serveur MDM.

Cette technologie unique, qui semble être un défi sur le plan de la sécurité, possède de nombreux avantages.
e nombreux services Google et Microsoft commencent à exiger un niveau de confiance similaire au service APNs, ainsi qu'une connexion directe. Par exemple, les solutions VOIP de Cisco pour iOS utilisent le service APNs pour les messages push et Callkit.
Le service APNs est essentiel à la sécurité et à la qualité de l'expérience utilisateur.
De plus, le fonctionnement de services comme l'App Store, l'authentification iCloud et la restauration par Internet ne sera pas entièrement assuré, voire impossible, sans le service APNs. La documentation de produit Apple vous guidera à travers les étapes d'installation pour l'ouverture des ports d'entreprise.

Pour en savoir plus, veuillez consulter le site web d'Apple: https://help.apple.com/deployment/macos/#/ior9d28751c0.

Architecture du serveur de notifications push d'Apple



Les appareils Apple nécessitent-ils l'utilisation d'un logiciel de sécurité tiers?
Les appareils Windows et Android requièrent souvent l'installation de logiciels de sécurité tiers ou complémentaires, ce qui est rarement le cas avec les produits Apple.

Les entreprises de sécurité traditionnellement axées sur l'environnement Windows tendent à être en retard sur les cycles de développement d'Apple, ce qui peut potentiellement ralentir le processus d'adoption de nouveaux systèmes d'exploitation et de nouvelles fonctionnalités de sécurité. Adopter la même approche pour la plateforme Apple que pour les autres plateformes nuit généralement aux performances des employés et dégrade la qualité de l'expérience utilisateur qui fait la renommée d'Apple. De plus, installer un logiciel Windows sur un appareil Apple peut donner lieu à une mauvaise exécution du code, des saturations de la mémoire et des paniques du noyau liées aux extensions (KEXT), ce qui ajoute une charge de travail considérable aux équipes informatiques.

Le chiffrement et l'antivirus intégrés d'Apple permettent à la majeure partie des entreprises de se passer de logiciels tiers. Certaines cherchent cependant à s'équiper de solutions de gestion des fuites de données de l'entreprise. Mais il est possible de contrôler la fuite de données de l'entreprise par le biais de la solution MDM, avec des protections supplémentaires côté réseau, en exploitant des outils comme Cisco Security Connector.

En février 2018, Cisco, Apple, Aon et Allianz ont présenté une solution inédite de gestion des risques de cyber sécurité pour les entreprises. Elle intègre à la fois les services d'évaluation de la cyber-résilience d'Aon, les technologies les plus sécurisées de Cisco et d'Apple, et des options permettant d'améliorer la couverture des assurances de cyber sécurité fournies par Allianz. Pour plus d'informations sur ce partenariat, veuillez lire l'annonce complète sur le site d'Apple.

Comment se déroule l'expérience de gestion des appareils Apple?
Auparavant, les services informatiques ne pensaient pas pouvoir trouver d'outils aussi performants pour gérer les appareils Apple que ceux destinés aux produits Windows. Cette idée préconçue, complétée par la fausse impression que la plateforme Apple serait plus complexe à gérer que les autres, a découragé beaucoup d'entreprises de proposer et de promouvoir Apple.

Des sondages ont montré que la plateforme Apple est en réalité plus simple à gérer que les autres plateformes. Un sondage de Dimensional Research a montré que 66 % des personnes interrogées trouvaient qu'il était plus simple de sécuriser un Mac qu'un PC, et 90 % pensaient qu'il était plus simple de sécuriser iOS que les autres plateformes. Des résultats similaires ont été obtenus en demandant aux participants si les appareils Apple étaient plus simples à déployer, à configurer et à dépanner.

IBM, le géant du secteur informatique, ne représente qu'une des nombreuses entreprises ayant décidé de mettre en place un programme de choix des employés avec la plateforme Apple. Fletcher Previn, le nouveau CIO d'IBM, a démontré que l'utilisation de Mac à la place de PC permettait à son entreprise de gagner de l'argent et de réaliser des économies.

66%
des entreprises trouvent qu'il est plus simple de sécuriser un Mac plutôt qu'un PC

90%
des entreprises trouvent qu'il est plus simple de sécuriser iOS plutôt que les autres plateformes

Cela prouve que l'entreprise a un besoin fondamental de cohérence du point de vue du déploiement et de l'expérience utilisateur. Or Apple offre la cohérence et la sécurité dès le départ.

Les fonctionnalités de sécurité propres à l'écosystème Apple

Quelles sont les fonctionnalités de sécurité intégrées à macOS?
La conception de macOS s'appuie sur des logiciels intégrés et sécurisés.

Les fonctionnalités de sécurité de système de macOS comportent les éléments suivants:

- **FileVault** fournit un niveau de chiffrement supplémentaire directement intégré à macOS, afin de protéger les données en cas de perte ou de vol de l'appareil.
- **Les mises à jour** logicielles viennent directement d'Apple, qui les signe électroniquement, de sorte que les entreprises et les services informatiques sachent qu'elles sont fiables.
- **La protection de l'intégrité du système (PIS)** protège les fichiers essentiels du système d'exploitation pouvant être visés par des attaques provenant de l'accès par des utilisateurs ou des applications.
- **Gatekeeper** permet aux services informatiques de définir les emplacements à partir desquels les utilisateurs peuvent télécharger leurs applications. Cet outil empêche les apps non signées et les logiciels malveillants de s'exécuter, et collabore avec XProtect pour interrompre au plus vite la diffusion des logiciels malveillants.
- **XProtect** est un utilitaire conçu pour combattre les logiciels malveillants, régulièrement mis à jour par Apple. Il empêche les logiciels malveillants et/ou les modules souvent obsolètes et vulnérables, comme Java et Flash, de s'exécuter sur le Mac.
- **Outil de suppression des logiciels malveillants** : Apple est en mesure de supprimer les rares logiciels malveillants qui réussissent à accéder au système.
- Les apps mises à disposition sur l'**App Store** sont toujours contrôlées par Apple, et seules les ressources approuvées par Apple y sont autorisées. Apple est en mesure de rendre des apps indisponibles et de révoquer les certificats de développeurs sans délai.
- Le « **sandboxing** » des apps garantit que les apps ne partagent pas (et ne volent pas) de données depuis le système ou entre elles.
- Les utilisateurs et les services informatiques peuvent définir les **contrôles de confidentialité**. Ceci s'agit d'un processus transparent qui indique aux utilisateurs quand le service de localisation est utilisé, quelles apps ont accès aux contacts ou aux calendriers, et quelles informations sont partagées avec Apple et/ou les développeurs d'apps.

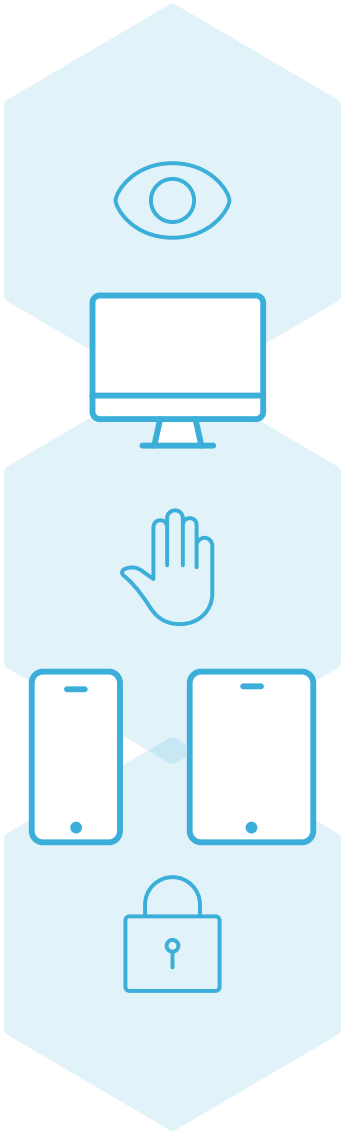
Pour consulter la liste complète des fonctionnalités de sécurité du Mac, rendez-vous sur: https://www.apple.com/macos/security/.

Pourquoi choisir FileVault pour le chiffrement de disque?
FFilevault est un outil de chiffrement de disque intégré à macOS. Cela signifie que les services informatiques n'ont pas besoin d'installer des logiciels supplémentaires pour chiffrer un disque. Il peut être activé manuellement, ou le service informatique peut l'activer à distance sur tous les Mac. Il est possible de gérer les clés de chiffrement de manière centralisée, ce qui permet au service informatique d'accéder aux données importantes lorsqu'un employé quitte l'entreprise ou oublie son mot de passe et a besoin d'aide pour se connecter. Il est également possible de configurer facilement la rotation des clés de chiffrement pour plus de sécurité.

Quelles sont les fonctionnalités de sécurité intégrées à iOS?
La plupart des fonctionnalités de sécurité essentielles du Mac sont disponibles sur iPad et iPhone, pour une expérience cohérente et sécurisée au sein de l'écosystème Apple:

- La sécurité du système intègre notamment les technologies de démarrage sécurisé, Autorisation du logiciel et une enclave sécurisée pour empêcher que le système ne soit compromis. Le service informatique a aussi la possibilité d'effacer entièrement le système d'exploitation iOS pour repartir à zéro.
- Touch ID et Face ID tirent parti de la détection d'empreinte digitale et de la reconnaissance faciale pour rationaliser le processus de connexion et s'assurer que seuls les utilisateurs autorisés peuvent accéder à l'appareil.
- Le chiffrement et la protection des données garantissent la sécurité des données personnelles et de l'entreprise, même si d'autres sections de l'appareil ont été effacées à la suite d'un vol ou d'une perte de l'appareil.
- La supervision offre un ensemble de fonctionnalités supplémentaires que le service informatique peut utiliser pour obtenir davantage de fonctionnalités de gestion dans des environnements plus contrôlés.

Pour consulter la liste complète des fonctionnalités de sécurité d'iOS, rendez-vous sur: https://www.apple.com/business/docs/iOS_Security_Guide.pdf.



Les éléments à prendre en compte lors de l'implémentation de nouveaux appareils Apple

Comment démontrer que les appareils Apple sont sûrs?
La possibilité de créer des profils de configuration est un principe fondamental de la gestion des appareils d'Apple. En créant des profils de configuration avec une solution de gestion des appareils mobiles comme Jamf Pro, les services informatiques peuvent imposer des mots de passe, restreindre des réglages, définir des protocoles réseau, configurer des réglages pour le VPN et les comptes de messagerie, entre autres. Ils peuvent ensuite déployer tous ces réglages sur les appareils gérés.

Pourquoi est-il inutile d'utiliser des conteneurs d'apps?
Les outils de gestion conçus pour Apple, comme Jamf Pro, permettent de déployer des apps certifiées sur des appareils et d'empêcher les apps non certifiées d'y

accéder. iOS a déjà la capacité de gérer des apps d'entreprise en utilisant la gestion des apps natives avec des solutions comme Jamf Pro. Cette méthode de gestion sépare les données d'entreprise des données personnelles et gère le flux de données sans avoir recours à des apps de conteneur, qui ont tendance à ralentir les performances ou à perdre en efficacité à chaque fois qu'une nouvelle version du système d'exploitation est installée.

Mis à part la structure de la solution MDM, quelles sont les autres fonctions de sécurité pour Mac?
Sur macOS, les solutions telles que Jamf Pro peuvent voir leurs capacités décuplées avec l'agent Jamf. L'agent Jamf est un fichier binaire installé lorsque le Mac est enrôlé dans la solution de gestion. Il permet au service informatique de créer un compte administrateur masqué qui donne un accès root à distance à tous les Mac gérés.

Une fois l'agent Jamf installé, le service informatique peut appliquer des règles et exécuter des scripts plus avancés, installer des logiciels disponibles en dehors de l'App Store (par exemple, Adobe), et bien plus. Il offre de nouvelles possibilités de personnalisation et étend les capacités de gestion au-delà de celles de la solution de gestion des appareils.

Comment valider, appliquer et signaler la conformité des appareils Apple au sein d'un environnement ?
Les secteurs hautement réglementés peuvent subir des audits nombreux et fastidieux. Être en mesure de démontrer que les appareils sont correctement gérés et sécurisés est donc une étape importante pour prouver la conformité de l'entreprise.

La tenue de l'inventaire est primordiale pour assurer la conformité réglementaire et sécuritaire des entreprises. Connaître le nombre d'appareils intégrés à l'environnement de l'entreprise, leurs propriétaires, l'état des mises à jour logicielles, les profils et les réglages attribués à chaque appareil, l'état actuel du chiffrement et les restrictions et configurations appliquées est essentiel à tout environnement sain et sécurisé..

Avec des solutions comme Jamf Pro, les services informatiques peuvent créer des rapports concernant toutes les catégories d'inventaire, et ainsi permettre aux entreprises de prendre des décisions plus éclairées et d'assurer leur conformité. S'il advient qu'un appareil ne soit pas conforme, le déploiement de profils de configuration permet de le remettre en conformité.

Si un ou plusieurs appareils ne sont pas conformes, ou si l'environnement doit être contrôlé dans son ensemble, vous pouvez utiliser Jamf Pro pour créer des groupes intelligents d'appareils. Les groupes intelligents s'appuient sur des critères d'inventaire avancés définis par le service informatique, et peuvent déclencher automatiquement des actions de gestion en fonction du rapport d'inventaire.

Comment gérer l'application de correctifs aux logiciels macOS tiers?
Les logiciels peuvent vite devenir obsolètes, et lorsque cela se produit, l'appareil, les données et le réseau sont exposés à des menaces internes et externes. La gestion des correctifs peut résoudre ces problèmes de vulnérabilité de manière rapide et efficace.

Grâce à la fonctionnalité de gestion des correctifs de votre solution MDM, le service informatique reçoit des alertes relatives aux correctifs lorsque de nouvelles versions de logiciels tiers sont disponibles. Il peut alors créer des paquets logiciels comportant le correctif adéquat (version à jour du logiciel), distribuer ce correctif aux appareils concernés, puis obtenir un rapport de correctif par le biais de la gestion d'inventaire pour s'assurer que le correctif a été correctement installé.

Les entreprises savent instantanément quelles apps et quels logiciels sont obsolètes, puis peuvent prendre des mesures rapides pour installer la version la plus récente et la plus sécurisée, adoptant ainsi une approche proactive des procédures de sécurité.

Pourquoi est-il déconseillé de lier les appareils Apple à Active Directory?
Les déploiements Mac ne suivent pas le schéma habituel d'un appareil par personne. Avec des outils comme Jamf Pro, Enterprise Connect et NoMAD, la liaison appartient au passé. La liaison complique les processus DEP des entreprises dont les contrôleurs de domaine ne sont pas ouverts aux réseaux externes ; en outre, les entreprises utilisant la liaison n'ont plus la possibilité d'expédier les nouveaux appareils aux utilisateurs distants. Bien que l'établissement d'une liaison reste envisageable, les entreprises exploitant une solution comme Jamf Pro sont en mesure de gérer les comptes locaux afin d'appliquer les mêmes exigences en matière de complexité et d'expiration du mot de passe sans tenir compte de la connexion ou de la synchronisation avec AD. Cela se traduit par moins de demandes de mots de passe pour vos utilisateurs finaux, et moins d'appels vers le service d'assistance informatique.

Comment les services dans le cloud fonctionnent-ils avec les appareils Apple?
De plus en plus d'entreprises migrent vers les services dans le cloud. Avec l'hébergement dans le cloud, l'accès à la base de données est limité et ne reste pas sur le serveur de votre réseau. Depuis des décennies, les entreprises érigent des « murs » autour de leurs locaux et utilisent le périmètre de leur réseau comme première ligne de défense. Avec l'apogée des espaces de travail mobiles et la circulation des données en dehors du pare-feu, les entreprises doivent trouver un modèle de sécurité plus moderne et davantage basé sur l'identité.

Microsoft transfère les données des entreprises vers le cloud avec Azure Active Directory. Afin de garantir que seuls les utilisateurs, appareils et apps de confiance puissent accéder aux données de l'entreprise dans le cloud, Microsoft et Jamf proposent une intégration exclusive permettant de bénéficier d'un accès conditionnel sans proxy.

Pour en savoir plus: https://www.jamf.com/resources/white-papers/conditional-access-going-beyond-perimeter-based-security/.

La transition vers un espace de travail mobile et le recours croissant au cloud n'est pas qu'une tendance éphémère

85%
des entreprises stockent des informations sensibles dans le cloud

80%
des employés utilisent des apps SaaS qui ne sont pas approuvées pour l'usage professionnel

41%
des employés estiment que les apps mobiles professionnelles transforment leurs méthodes de travail

Comment appliquer les normes de sécurité du secteur?
L'application dépend des normes de sécurité, ainsi que des normes de conformité qui doivent être respectées. SOC 2 est différent d'HIPAA, et PCI est différent de CIS. La première étape consiste à savoir quel modèle adopter.

Jamf Pro offre une structure flexible pour faciliter l'adoption de la plupart des normes réglementaires courantes. Les services informatiques ne peuvent pas se contenter de définir des normes applicables, de créer des profils et des règles s'y conformant, puis de les appliquer. Il peut par exemple s'agir de restreindre certaines fonctionnalités grand public comme iCloud Drive, de s'assurer que Gatekeeper autorise uniquement le téléchargement d'apps sûres, d'appliquer le chiffrement FileVault aux Mac, ou de restreindre les apps en recherchant une app restreinte (ou bien macOS) au sein des appareils Apple gérés pour la supprimer. Les services informatiques ont simplement besoin de définir des réglages et d'utiliser ces informations pour créer les profils de configuration et les règles, puis de les appliquer aux appareils.

Consultez ce livre blanc pour savoir comment respecter les consignes du Center for Internet Security (CIS): https://www.jamf.com/resources/white-papers/macos-security-checklist/.

Pourquoi utiliser les programmes de déploiement Apple?

Les programmes de déploiement Apple pour les entreprises, DEP et VPP, sont gratuits et propres à Apple. Ils permettent non seulement d'augmenter le niveau de sécurité des appareils, mais donnent aussi aux services informatiques la possibilité d'automatiser et de personnaliser la configuration des appareils à grande échelle.

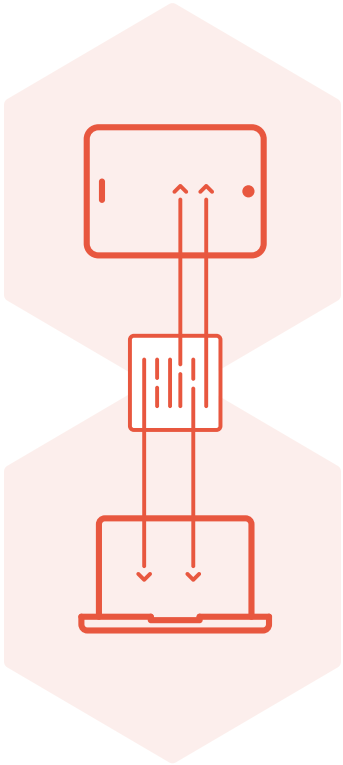
- Le programme DEP est la méthode recommandée pour gérer et sécuriser les appareils Apple appartenant à une entreprise. Il permet d'effectuer le déploiement sans intervention, ce qui signifie qu'il n'est plus nécessaire de recourir au processus traditionnel de création d'images ou à la configuration manuelle. Les utilisateurs peuvent s'enrôler eux-mêmes dans l'environnement de manière rapide et transparente, accélérant le processus d'intégration et sécurisant les terminaux en quelques clics seulement. Les appareils commandés directement auprès d'Apple ou d'un Revendeur Agréé Apple peuvent bénéficier du programme DEP et sont automatiquement enrôlés auprès de la solution de gestion au cours de la configuration initiale
- Le programme DEP donne accès à des options de gestion supplémentaires pour les appareils macOS, iOS et tvOS, offrant un niveau de gestion plus approfondi.
- Lorsqu'il est associé à la gestion des appareils mobiles, ou MDM (la structure de gestion intégrée d'Apple), il utilise une méthode dynamique pour distribuer la configuration finale aux utilisateurs selon leurs besoins, plutôt que de créer une image identique pour tous.
- Le programme VPP permet aux utilisateurs de distribuer des apps de l'App Store sous licence et des logiciels aux individus ou aux appareils. S'ils sont directement distribués aux appareils, les identifiants Apple ne sont pas requis. Les identifiants Apple authentifient les utilisateurs et leur donnent accès aux services Apple, par exemple iCloud, iTunes et l'App Store.
- Le service informatique peut gérer les apps achetées par l'intermédiaire du programme VPP et les récupérer pour les redistribuer ultérieurement lorsqu'un employé quitte l'entreprise ou n'a plus besoin d'une app spécifique.

« Toutes les solutions de gestion d'appareils Apple ne prennent pas en charge les programmes et services Apple. Vérifiez auprès de votre fournisseur qu'il prend en charge ces programmes ainsi que les améliorations progressives. »

Les intégrations Apple permettant de tirer avantage de votre infrastructure existante

Comment intégrer Apple (et Jamf) à l'ensemble des technologies existantes de l'entreprise ?

Les entreprises, services informatiques et employés ne sont pas coupés du monde. Apple a prouvé son engagement auprès des entreprises en s'associant à des partenaires informatiques comme Cisco, afin de proposer des services professionnels modernes et sécurisés.



De nombreuses entreprises ont besoin de services qui ne font pas partie de l'écosystème Apple. Grâce aux intégrations compatibles et sécurisées, elles peuvent exploiter toutes les facettes de leur environnement et intégrer toute une gamme de services pour faire croître leur activité.

Quelques exemples :

- Interface de programmation applicative, ou API, de Jamf, pour créer des intégrations destinées aux outils informatiques existants.
- Intégration de Microsoft EMS avec Jamf, pour procéder à une intégration exclusive sans proxy dans le cadre de l'accès conditionnel sur Mac.
- Cisco ISE, pour créer et appliquer des règles de sécurité et d'accès pour les appareils connectés au réseau d'une entreprise.
- Cisco Fast Lane, pour réduire l'utilisation de la bande passante réseau en hiérarchisant les apps et en configurant automatiquement la qualité du service.
- ServiceNow, pour automatiser les processus informatiques et métier dans le cadre de la gestion de l'activité.

Les entreprises modernes sont de plus en plus nombreuses à adopter des outils professionnels comme ceux de Cisco. Avec l'ajout de Jamf pour gérer les Mac, elles disposent d'une solution entièrement intégrée qui ne fait l'impasse sur aucune des plateformes prises en charge.

De plus, l'entreprise de gestion des identités Okta Inc. a récemment publié un rapport relatif à la sécurité des données qui comporte de nouvelles informations sur la popularité grandissante des applications de cyber sécurité en entreprise. Pour la première fois cette année, les outils de sécurité tels que Jamf sont tous classés dans le top 15 des apps connaissant la meilleure croissance.

Apple et Jamf : un niveau de gestion et de sécurité des appareils sans précédent

La plateforme la plus sécurisée nécessite la solution de gestion la plus performante pour garantir que toutes les fonctionnalités de sécurité existantes sont correctement appliquées et installées. Jamf est l'entreprise de gestion des appareils mobiles la mieux adaptée aux produits et aux services d'Apple, et le fournisseur le plus à même d'assurer la pérennité de votre infrastructure Apple.

C'est la raison pour laquelle les entreprises dépendant le plus de la sécurité, notamment les dix plus grandes banques américaines et neuf des dix plus grandes entreprises informatiques, font confiance à Jamf pour gérer leur environnement Apple.

Jamf offre une assistance immédiate pour tous les systèmes d'exploitation et fonctionnalités d'Apple, ce qui en fait une solution de confiance pour les entreprises souhaitant adopter les produits Apple et valoriser le travail de leurs employés.

Les outils de Jamf permettent de sécuriser 100 à 100 000 appareils Apple. Les entreprises peuvent ainsi donner la priorité à la réussite des tâches stratégiques: accélérer les procédures, améliorer l'expérience utilisateur et assurer la réussite de l'entreprise.

96 % des clients de Jamf renouvellent leur contrat d'une année sur l'autre. Pour en savoir plus sur les atouts de Jamf Pro pour la gestion de vos appareils Apple, rendez-vous sur jamf.com/fr/produits/jamf-pro.