Gestion des appareils et des données d’entreprise

Aperçu

Table des matières

Les données sont l’un des actifs les plus précieux d’une entreprise. Séparer ses données personnelles de celles de l’entreprise est un bon moyen de les protéger contre les attaques et les mauvaises manipulations, qu’on y accède depuis sa propre machine ou depuis celles fournies par l’organisation. Apple aide les équipes des TI à mettre en place différents mécanismes de gestion des appareils, tout en favorisant la productivité du personnel.

Dans le cas des appareils appartenant à l’entreprise, les TI peuvent utiliser Apple Business Manager pour automatiser leur inscription : la distribution du matériel se fait alors rapidement et facilement, sans qu’aucune manipulation ou préparation ne soit nécessaire. Avec la supervision, les TI profitent d’options que les autres modèles de déploiement n’offrent pas, comme des configurations de sécurité supplémentaires, l’inscription irrévocable à la GAM ou la gestion des mises à jour logicielles.

Pour les appareils personnels administrés via l’inscription par l’utilisateur ou l’utilisatrice, les données privées et celles de l’entreprise sont réparties entre, respectivement, un identifiant Apple personnel et un identifiant Apple géré. Ainsi, les données de l’organisation sont protégées et séparées des données personnelles. Et quand quelqu’un quitte son emploi ou n’a plus besoin d’accéder à une app, les données d’entreprise sont supprimées.

Gestion des appareils Apple

Apple dote les équipes des TI des outils dont elles ont besoin pour réussir à exercer un contrôle efficace qui ne compromet pas la convivialité. Cet équilibre est atteint grâce à la parfaite symbiose entre le cadre de gestion d'Apple et la solution de gestion des appareils mobiles (GAM) de l'entreprise.

La gestion des appareils selon Apple

Apple intègre un cadre de gestion à iOS, iPadOS, tvOS et macOS pour permettre aux équipes des TI de configurer et de mettre à jour les réglages, de déployer des apps, de vérifier la conformité, d'interroger les appareils, et de les verrouiller ou d'en effacer le contenu à distance. Ce cadre, qui fonctionne aussi bien avec les appareils appartenant à l'entreprise qu'avec ceux appartenant au personnel, est à la base de la stratégie de déploiement et de gestion. Puisque le cadre est intégré aux systèmes d'exploitation d'Apple, les organisations peuvent gérer discrètement les éléments nécessaires, et non seulement limiter ou désactiver des fonctionnalités. Les équipes des TI disposent ainsi du contrôle requis sans nuire à l'expérience d'utilisation ni compromettre la vie privée.

Qu'est-ce que la GAM?

Ensemble, les outils d'Apple et votre solution de GAM facilitent le déploiement du matériel, la distribution d'apps et de livres, la configuration des réglages et la protection des appareils.

La solution de GAM permet la configuration d'apps, de comptes et de données sur chaque appareil, ce qui inclut des fonctionnalités intégrées comme l'imposition de mots de passe et de politiques. Ces interventions demeurent transparentes et préservent la confidentialité des renseignements personnels. Et en cas de perte ou de vol, les équipes des TI peuvent effacer le contenu des appareils à distance et en toute sécurité.

Selon qu'une entreprise opte pour l'infonuagique ou pour un serveur installé sur place, il existe sur le marché un éventail de solutions de GAM à différents prix et avec toutes sortes de fonctionnalités, pour une flexibilité incomparable.

D'autres méthodes peuvent désigner différemment les fonctionnalités de GAM et parler notamment de gestion de la mobilité d'entreprise (EMM) ou de gestion unifiée des terminaux (UEM). Ces solutions ont toutefois le même objectif : encadrer les appareils et les données d'une organisation à distance.

L'incidence de la GAM sur les utilisateurs et utilisatrices

Apple permet aux équipes des TI de déployer et de gérer des appareils sans compromettre la vie privée des personnes ni perturber leurs tâches quotidiennes. Les fonctionnalités et appareils ne sont donc pas bloqués ni désactivés à grande échelle, et la collecte et l'utilisation de données sont restreintes, que le matériel appartienne à l'entreprise ou aux membres du personnel.

Ce système fonctionne, car Apple sépare les apps et données selon si elles sont destinées à un usage professionnel ou personnel. Grâce à la compatibilité avec la plupart des solutions de GAM tierces, les équipes des TI peuvent interagir avec un appareil Apple en ayant un accès limité à certains réglages et informations. Quel que soit le modèle de déploiement choisi, le cadre de GAM n'a jamais accès aux renseignements personnels, y compris les courriels, les messages et l'historique de navigation.

Les fonctionnalités de GAM sont restreintes sur les appareils personnels.

- ✓ Configurer des comptes
- ✓ Configurer le VPN par app
- ✓ Installer et configurer des apps
- ✓ Exiger un code d'accès
- ✓ Imposer certaines restrictions
- ✓ Voir la liste des apps professionnelles
- ✓ Effacer des données d'entreprise
- ✗ Accéder aux données personnelles
- ✗ Voir la liste des apps personnelles
- ✗ Effacer des données personnelles
- ✗ Recueillir des fichiers journaux
- ✗ Prendre le contrôle d'apps personnelles
- ✗ Exiger un code d'accès complexe
- ✗ Effacer à distance toutes les données de l'appareil
- ✗ Connaître la position de l'appareil

Modèles de déploiement

Les appareils appartiennent soit à l'organisation, soit au personnel. Le matériel appartenant à l'entreprise est le plus souvent distribué de façon individuelle, ce qui signifie que chaque personne se voit attribuer une machine dont la configuration est assurée par l'équipe des TI. Les outils peuvent aussi être partagés entre plusieurs collègues. Dans un modèle de distribution partagée, un appareil sera par exemple utilisé en alternance par des personnes travaillant selon des quarts différents, ou servira de point de vente mobile à l'équipe d'une boutique. Les appareils appartenant à l'entreprise peuvent être gérés au moyen de la supervision : l'équipe des TI dispose alors d'un contrôle supplémentaire sur la configuration et les restrictions, sans avoir besoin de limiter l'utilisation du matériel.

Dans le cas d'outils appartenant aux personnes (on parle aussi de modèle « Apportez votre appareil »), la gestion se fait via l'inscription par l'utilisateur ou l'utilisatrice. Cette méthode de gestion permet aux membres du personnel d'utiliser leurs propres appareils à des fins professionnelles.

Dans les deux cas, Apple propose divers mécanismes de gestion tout en protégeant la vie privée, en assurant la sécurité et en veillant à la séparation des données.

Les équipes des TI ont un meilleur contrôle sur les appareils Apple supervisés.

- ✓ Configurer des comptes
- ✓ Configurer des serveurs mandataires
- ✓ Installer, configurer et supprimer des apps
- ✓ Exiger un code d'accès complexe
- ✓ Imposer toutes les restrictions voulues
- ✓ Voir la liste des apps installées
- ✓ Effacer à distance toutes les données de l'appareil
- ✓ Gérer les mises à jour logicielles
- ✓ Supprimer des apps système
- ✓ Modifier le fond d'écran
- ✓ Limiter l'utilisation à une seule app
- ✓ Contourner le verrouillage d'activation
- ✓ Forcer l'activation du Wi-Fi
- ✓ Activer le mode Perdu

Appareils appartenant à l'entreprise

Les appareils appartenant à l'entreprise peuvent être configurés par les équipes des TI de sorte qu'ils ne contiennent que les données, apps et réglages nécessaires aux tâches du personnel. Il est possible de les déployer automatiquement via la solution de GAM. Les appareils achetés directement auprès d'Apple ou d'un revendeur agréé Apple peuvent être automatiquement inscrits à Apple Business Manager et déployés à distance : les équipes des TI n'ont ainsi plus besoin d'intervenir sur chaque machine.

Quand les appareils appartiennent à l'entreprise, celle-ci peut exercer un plus grand contrôle sans pour autant sacrifier la confidentialité ni la convivialité. L'inscription d'une machine appartenant à l'organisation permet à l'équipe des TI de configurer le Wi-Fi, le VPN, la messagerie et le calendrier, mais aussi d'installer divers comptes et restrictions. Ces dernières sont par exemple mises en place pour empêcher les utilisateurs et utilisatrices d'ajouter leurs propres comptes sur les appareils.

S'il est possible d'utiliser un identifiant Apple géré, un identifiant Apple personnel, voire aucun identifiant sur un appareil appartenant à l'entreprise, la première option reste toutefois celle à privilégier. Les identifiants Apple gérés sont propres à votre organisation et distincts des identifiants Apple créés pour un usage personnel. Ce sont les gestionnaires des TI qui gèrent les services auxquels les personnes peuvent accéder avec leur identifiant Apple géré, ce qui n'est pas le cas pour les identifiants Apple personnels. Par ailleurs, la supervision donne aux TI des moyens de contrôle qui ne sont pas possibles dans les autres modèles de déploiement. Il s'agit notamment de configurations de sécurité supplémentaires, de l'inscription irrévocable à la GAM ou de la gestion des mises à jour logicielles.

Que les appareils appartenant à l'entreprise soient assignés individuellement ou partagés entre plusieurs personnes pour réaliser des tâches communes, toutes les données qu'ils contiennent peuvent être facilement sécurisées et protégées.

Appareils personnels

Lorsque des membres du personnel utilisent leurs propres appareils au travail, les données d'entreprise consultées peuvent être gérées via l'inscription par l'utilisateur ou l'utilisatrice. Conçu exclusivement pour les programmes « Apportez votre appareil », ce type d'inscription protège la vie privée des gens, tout en séparant et en sécurisant les données d'entreprise. Il est ainsi possible d'aller plus loin avec la personnalisation des appareils. Les équipes des TI peuvent alors appliquer certains réglages, surveiller le respect des politiques et supprimer uniquement des données et apps d'entreprise. En revanche, elles ne peuvent pas effacer le contenu d'un appareil à distance, obtenir sa position, ni accéder aux apps et renseignements personnels qui y sont stockés. En plus de pouvoir supprimer un profil de GAM, et donc toutes les apps et données d'entreprise associées, quand ils le souhaitent, les utilisateurs et utilisatrices disposent d'une plus grande marge de manœuvre sur les mises à jour et autres configurations qu'avec des appareils appartenant à l'organisation.

Avec l'inscription par l'utilisateur ou l'utilisatrice, les personnes doivent ajouter elles-mêmes leur appareil à la solution de GAM de l'entreprise. Cela leur permet ainsi d'accéder aux ressources organisationnelles, de définir différents réglages ainsi que d'installer un profil de configuration et des apps d'entreprise.

Ce type d'inscription permet à un identifiant Apple géré et à un identifiant Apple personnel de coexister sur un appareil. L'identifiant Apple personnel sert à gérer toutes les données iCloud de l'utilisateur ou de l'utilisatrice. L'identifiant Apple fourni par l'organisation permet quant à lui de regrouper toutes les données iCloud d'entreprise dans Notes et le service iCloud Drive géré.

Avec iOS 15 et iPadOS 15, les utilisateurs et utilisatrices peuvent maintenant inscrire leur appareil directement à partir de l'app Réglages. À cet endroit, après avoir cliqué sur Général, il suffit de sélectionner VPN et gestion de l'appareil, puis Se connecter au compte professionnel ou scolaire. Une fois l'identifiant Apple géré et le mot de passe saisis, le processus d'authentification commence.

Ce type de gestion des données renforce l'autonomie des gens, tout en sécurisant davantage les données de l'entreprise, puisqu'elles sont stockées de manière cryptographique sur un volume Apple File System (APFS) distinct dans Notes et iCloud Drive. La sécurité, la protection de la vie privée et l'expérience d'utilisation dans le cadre des programmes du type « Apportez votre appareil » s'en trouvent donc améliorées. Et si une personne change d'appareil ou quitte l'entreprise, toutes les données du volume APFS sont détruites dès la désinscription de l'appareil.

Outils pour séparer les données d'entreprise

Apple propose divers outils qui facilitent la séparation des données personnelles et d'entreprise sur les appareils, quel que soit le modèle de déploiement. Dans cette section, vous découvrirez comment gérer les données de différents éléments supervisés, tels que les apps, les livres, les réglages ou les comptes.

Apps gérées

Pour se faire assigner des apps par votre organisation, les appareils doivent être inscrits à la solution de GAM. Une fois qu'une app est attribuée à un appareil, elle lui parvient par l'intermédiaire de la solution de GAM. Sur les appareils détenus par l'entreprise et gérés au moyen de la supervision, les apps sont installées en arrière-plan, sans que l'utilisateur ou l'utilisatrice ait à intervenir ou à saisir un identifiant Apple.

Les données stockées dans une app gérée, que l'appareil appartienne ou non à l'entreprise, sont supprimées dès que la machine est désinscrite de la GAM (par l'équipe des TI ou par l'utilisateur ou l'utilisatrice). Les équipes des TI peuvent aussi empêcher les apps gérées de sauvegarder des données dans le Finder, sur iTunes ou dans iCloud. Cela évite que les données d'une app gérée soient récupérées, si celle-ci est supprimée via la solution de GAM, puis réinstallée.

Livres gérés

Les livres achetés via Apple Business Manager peuvent être assignés à une personne utilisant un identifiant Apple géré ou un identifiant Apple personnel. Les livres attribués sont soumis aux mêmes restrictions géographiques de téléchargement que les apps.

Comme pour les apps gérées, la solution de GAM peut empêcher la sauvegarde des ouvrages. Mais contrairement aux apps, il n'est pas possible de retirer l'accès à des livres gérés ou de les réassigner.

Réglages gérés

Une fois que les utilisateurs et utilisatrices sont inscrits à la GAM, ils peuvent facilement voir depuis Réglages les apps, livres et comptes gérés, ainsi que les restrictions mises en place. Tous les réglages, comptes et contenus d'entreprise installés par l'intermédiaire de la GAM sont indiqués comme étant gérés. Cela inclut les paramètres de configuration du Wi-Fi et du VPN, et les exigences de mot de passe. Tous les réglages peuvent être mis à jour ou supprimés en tout temps.

Restrictions

Empêcher l'accès à des options de partage ou le téléchargement de certaines apps est une façon pour les équipes des TI de sécuriser les données d'entreprise. Avec les outils Apple et la solution de GAM, les spécialistes des TI peuvent exercer un niveau de contrôle plus élevé sur les appareils appartenant à l'organisation en recourant à la supervision. Cette méthode s'accompagne de contrôles de gestion supplémentaires, comme l'inscription irrévocable à la solution de GAM, qui ne sont pas offerts par les autres modèles de déploiement. En outre, les équipes peuvent imposer diverses restrictions, comme la désactivation d'iCloud, de Siri ou de la caméra d'iPhone.

Comptes gérés

En gérant les adresses courriel, les calendriers et les contacts professionnels sur les appareils, les équipes des TI aident les membres du personnel à se mettre au travail plus rapidement. La gestion des comptes empêche les utilisateurs et utilisatrices d'ajouter leurs propres adresses courriel, calendriers et contacts, ce qui limite la personnalisation, mais permet aux équipes des TI de mieux protéger les données stockées localement.

Extensions gérées

Avec les extensions, les développeurs tiers peuvent ajouter des fonctionnalités à des apps, voire à des systèmes clés intégrés aux systèmes d'exploitation, ce qui fait naître de nouveaux processus de travail entre les apps. La gestion des extensions permet d'éviter que des fonctionnalités non encadrées n'interagissent avec des apps gérées. Parmi les extensions, on trouve par exemple les extensions de gestion de fichiers, qui permettent aux apps de productivité d'ouvrir des documents à partir de divers services infonuagiques; les extensions de partage, qui offrent une solution pratique pour transmettre du contenu à d'autres entités; et les extensions d'action, qui permettent de visionner ou de manipuler du contenu dans une app différente.

Gestion des autorisations d'ouverture pour iOS et iPadOS

La gestion des autorisations d'ouverture s'appuie sur trois volets distincts pour protéger les données d'entreprise :

- **Autorisation de l'envoi de documents provenant de sources non gérées vers des destinations gérées.** Imposer ce type de restriction permet d'éviter que les sources et comptes personnels d'un utilisateur ou d'une utilisatrice n'ouvrent des documents dans les destinations gérées de votre organisation. Par exemple, il serait impossible de consulter un PDF issu d'un site externe sur l'app de lecture de PDF de votre entreprise.

- **Autorisation de l'envoi de documents provenant de sources gérées vers des destinations non gérées.** En imposant ce type de restriction, on évite que les sources et comptes gérés d'une organisation n'ouvrent des documents dans des destinations personnelles. Ainsi, une pièce jointe confidentielle liée à un compte de messagerie géré ne pourrait pas être ouverte dans des apps personnelles.

- **Presse-papiers géré.** Sous iOS 15 et iPadOS 15 et les versions ultérieures, cette restriction permet de contrôler le collage de contenu entre les destinations gérées et non gérées. Lorsque ce type de restriction est mis en place, le collage de contenu est conçu pour respecter les règles des autorisations d'ouverture définies entre les apps tierces et les apps Apple comme Calendrier, Fichiers, Mail et Notes. Les apps ne peuvent pas non plus demander d'éléments du presse-papiers lorsque le contenu outrepasse les règles définies.

Plus concrètement, ces trois fonctionnalités permettent de diviser l'appareil géré en deux environnements : l'un pour les apps et données d'entreprise gérées, et l'autre pour les apps et données personnelles non gérées.

Le recours à la gestion des autorisations d'ouverture pour isoler les données améliore sensiblement l'expérience d'utilisation. Plutôt que de limiter l'ensemble des capacités d'un appareil, les équipes des TI peuvent opter pour l'approche plus conviviale d'Apple, qui leur offre la visibilité nécessaire pour gérer les sources et les destinations des données sans la lourdeur habituelle.

Domaines gérés pour iOS et iPadOS

Les équipes des TI peuvent gérer des URL et des sous-domaines précis sur iPhone et iPad. Par exemple, si une personne télécharge un PDF à partir d'un domaine géré, celui-ci va requérir que le document soit conforme à tous les réglages définis pour l'ouverture de documents. Les chemins empruntés par le domaine sont gérés par défaut.

Appareils perdus ou volés

Il arrive malheureusement que les appareils soient perdus ou volés. Grâce aux outils Apple et à votre solution de GAM, ces situations ne permettront pas à des individus d'accéder librement à vos données d'entreprise. Votre solution de GAM peut établir un système de protection des données qui s'active automatiquement à la saisie d'un code. Par ailleurs, le niveau de complexité des codes peut être renforcé sur l'ensemble des appareils au moyen des réglages gérés.

Les équipes des TI peuvent facilement verrouiller à distance un appareil macOS égaré ou activer le mode Perdu sur un appareil iOS ou iPadOS qui manque à l'appel. Dans les deux cas, la machine reste verrouillée jusqu'à ce que le bon code ou le bon mot de passe soit saisi. Si l'appareil ne peut pas être localisé, votre solution de GAM peut le verrouiller et en effacer le contenu à distance. De cette façon, personne ne pourra accéder à vos données d'entreprise sensibles.

Gestion des identités

Dans les organisations qui déploient des appareils Apple à petite comme à grande échelle, les identités sont au cœur des mécanismes permettant d'accéder aux appareils, aux sites web, aux apps et aux services. Elles sont ainsi étroitement intégrées à l'ensemble des systèmes d'exploitation. C'est ce qui rend l'expérience d'utilisation complètement fluide. Et c'est ce qui soutient le travail à distance, tout en offrant aux équipes des TI la visibilité et le contrôle dont elles ont besoin. En mettant en place des balises solides pour la gestion des identités, le personnel des TI peut prévenir les fuites de données et s'appuyer sur une stratégie de réponse claire, si ces événements venaient à se produire. Apple a développé de nombreux outils et technologies qui facilitent cet encadrement, notamment ceux décrits ci-après.

Authentification sur les appareils

La gestion des identités sur les appareils Apple commence par l'authentification, sur l'écran verrouillé ou la fenêtre de connexion, et s'étend à toutes les fonctionnalités. Si plusieurs personnes utilisent un iPad ou un Mac partagé, chacune peut sélectionner son compte, entrer ses renseignements de connexion et accéder à une expérience sur mesure. L'authentification sur les appareils donne aux équipes des TI une vision détaillée de la chaîne de possession des données : qui a accédé à quels fichiers, et à qui ceux-ci ont été transmis. L'authentification sur un iPad partagé requiert un identifiant Apple géré. Sur un Mac partagé, les comptes sont soit locaux, soit issus du réseau.

Extensions d'authentification unique (SSO)

Configurées via la solution de GAM, les extensions d'authentification unique (SSO) permettent aux apps natives et à WebKit de fournir une expérience d'authentification unique plus fluide. Les utilisateurs et utilisatrices peuvent alors utiliser leurs identifiants existants pour accéder de manière sécurisée à des apps, sans avoir à créer de comptes ou de mots de passe supplémentaires. Les équipes des TI sont capables de configurer ces extensions sur des iPad partagés dotés d'iPadOS 14 ainsi que sur des Mac dotés de macOS Big Sur. D'autres outils de macOS, tels que l'extension SSO Kerberos, permettent d'intégrer les politiques et fonctionnalités d'Active Directory sans devoir associer de comptes mobiles aux appareils. La solution de GAM peut gérer des certificats provenant d'autorités de certification internes et externes. Ainsi, des certificats clients peuvent servir à s'authentifier de manière transparente auprès de services fiables.

Identifiants Apple gérés

Les équipes des TI utilisent les identifiants Apple gérés pour encadrer les appareils des organisations et les achats d'apps dans Apple Business Manager. Avec ce type d'identifiant, les équipes peuvent aussi tirer parti de l'authentification fédérée, une architecture de gestion des identités simple et sécurisée. Ce dispositif permet aux organisations inscrites à Apple Business Manager de continuer à utiliser leur système de gestion des identités existant. Les utilisateurs et utilisatrices reçoivent automatiquement un accès aux services Apple, sans devoir obtenir de nouveaux identifiants. Quand une personne ouvre pour la première fois une session sur son appareil Apple au moyen de l'authentification fédérée, l'identifiant Apple géré requis pour accéder aux services Apple est automatiquement créé. En plus de simplifier la gestion des comptes pour les TI comme pour les utilisateurs et utilisatrices, ce type d'authentification garantit l'application uniforme des politiques de gestion des identités pour tous les services et apps de l'entreprise.

Conclusion

Vos données suivent les membres de votre personnel. Il est donc crucial d'assurer leur protection. Grâce au cadre de gestion d'Apple et à votre solution de GAM, vos équipes ont tous les outils nécessaires pour fournir un travail exceptionnel, où qu'elles se trouvent.

À mesure que vous améliorez la gestion de votre parc et que vous mettez en place un cadre de séparation des données, ne perdez pas de vue ces points essentiels :

- Les appareils appartenant à l'entreprise sont ceux qui offrent le plus grand niveau de contrôle et de protection des données organisationnelles.
- La gestion des appareils appartenant au personnel via l'inscription par l'utilisateur ou l'utilisatrice permet de sécuriser les données professionnelles sans compromettre les données personnelles, et donc de protéger la vie privée des gens.
- La vie privée et la sécurité des personnes sont tout aussi importantes que la protection des données d'entreprise.
- La gestion des appareils et des données est une responsabilité commune, et les meilleures équipes des TI privilégient une approche conviviale.

Ressources supplémentaires

En savoir plus sur le déploiement des appareils Apple :
support.apple.com/guide/deployment/welcome/web

En savoir plus sur Apple Business Manager :
support.apple.com/guide/apple-business-manager/welcome/web

En savoir plus sur les identifiants Apple gérés pour les entreprises :
apple.com/ca/fr/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

En savoir plus sur Apple at Work :
apple.com/ca/fr/business

En savoir plus sur les fonctionnalités pour les TI :
apple.com/ca/fr/business/it

En savoir plus sur la sécurité des plateformes Apple (en anglais) :
support.apple.com/guide/security/welcome/web

Parcourir les programmes AppleCare :
apple.com/ca/fr/support/professional

En savoir plus sur les formations et les certifications Apple (en anglais) :
training.apple.com

Communiquer avec les Services professionnels Apple :
consultingservices@apple.com