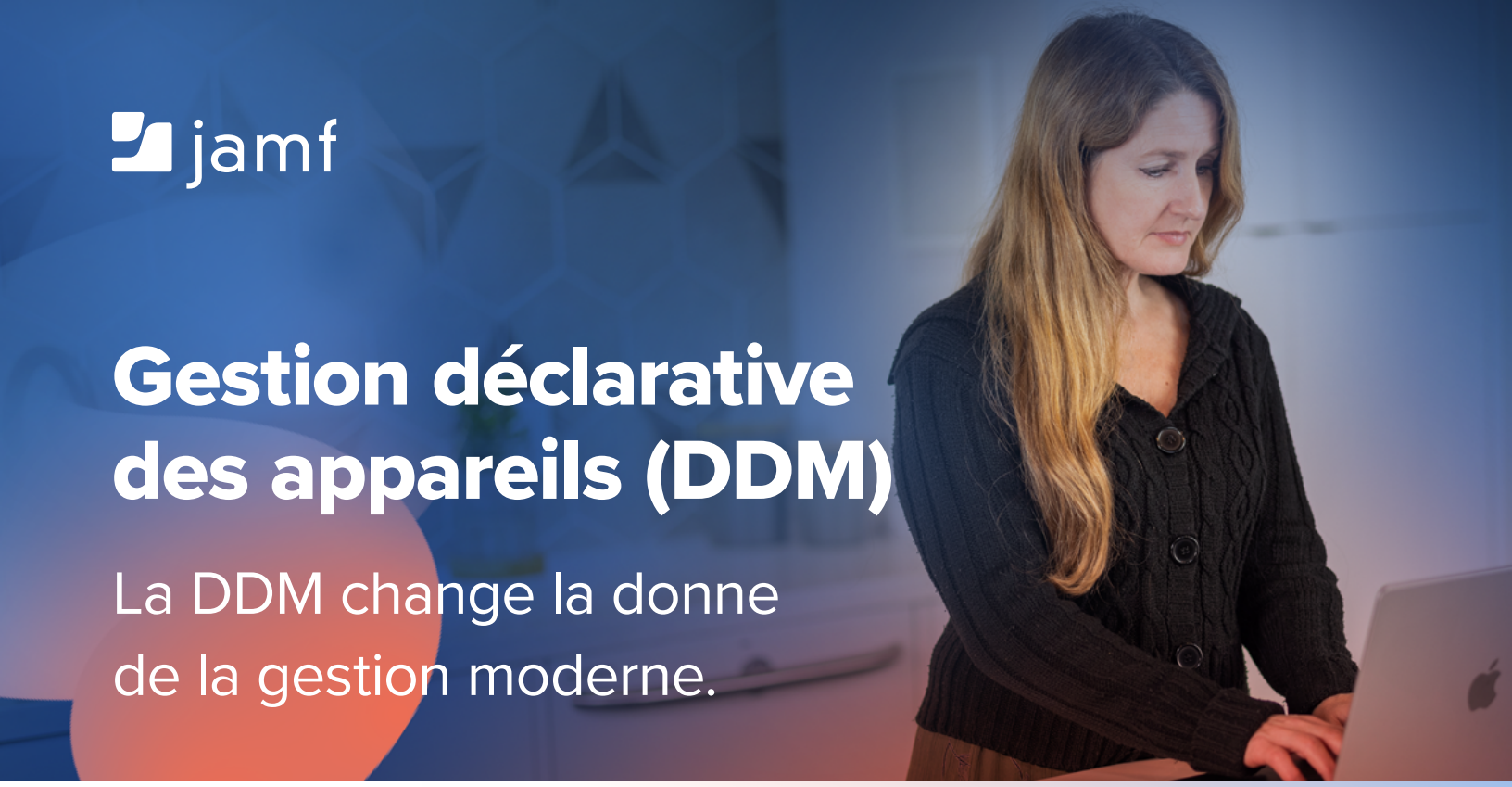


# Gestion déclarative des appareils (DDM)

## La DDM change la donne de la gestion moderne.

### La gestion des appareils mobiles (MDM) est déjà un outil puissant.

Sous l'égide de Jamf, la gestion des appareils mobiles (MDM) pour Apple a considérablement évolué. Ce qui était au départ une méthode de gestion forcée reposant sur un binaire est aujourd'hui une solution flexible, puissante et conviviale qui dépasse tout ce qu'on pouvait imaginer.

La MDM a donné aux administrateurs Apple une visibilité et des possibilités d'automatisation et de contrôle qu'ils n'avaient jamais connus. Elle réduit les tâches répétitives, élimine les facteurs d'erreur humaine et favorise l'adoption de mesures de sécurité rigoureuses.

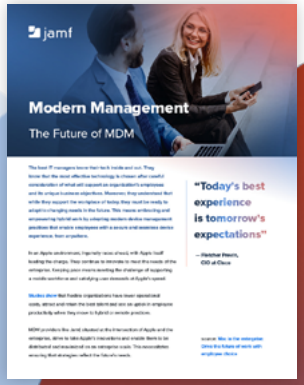
Mais le travail a changé : les équipes ont quitté les bureaux et sont dispersées dans le monde entier. Pour répondre à ces nouveaux besoins, les organisations doivent modifier leurs pratiques de gestion pour adopter un modèle plus souple, portable et sécurisé : la **gestion moderne**.

### Qu'est-ce que la gestion moderne ?

La gestion moderne est une stratégie qui s'adapte aux réalités actuelles du travail et anticipe l'environnement de travail de demain.

Elle s'appuie sur le cloud pour gérer et sécuriser les appareils, les utilisateurs, les systèmes d'exploitation et les applications. L'intégration de ces éléments améliore la sécurité, la gestion et la connaissance de la situation pour les services informatiques. Cette approche holistique offre davantage de visibilité et de réactivité.

Lisez notre article détaillé sur la gestion moderne . >



## En quoi la gestion moderne est-elle un progrès par rapport à la gestion traditionnelle des appareils ?

La gestion traditionnelle des appareils se concentre sur les appareils que l'entreprise remet aux employés. Seuls ces appareils autorisés peuvent accéder au réseau interne de l'organisation. Et cette approche a fait ses preuves pendant de longues années.

Mais le lieu de travail a changé de manière spectaculaire. Le télétravail est aujourd'hui monnaie courante, et même les entreprises qui ont encore un environnement de bureau traditionnel doivent aider chaque type d'utilisateur à rester productif sans mettre en danger leurs données.

La gestion moderne déplace tout vers le cloud et mise sur des connectivités plus sécurisées et chiffrées. Les déploiements dans le cloud offrent un certain nombre d'avantages sur le plan de la sécurité :

- **Inscription vérifiée.** L'utilisation de méthodes d'inscription intégrées garantit l'intégrité de chaque appareil géré au sein de votre organisation.
- **Gestion des identités et des accès.** Le service informatique contrôle qui a accès à quoi, en fonction de l'identité cloud de chaque individu.
- **Gestion des privilèges.** Les utilisateurs n'ont accès qu'aux ressources dont ils ont besoin afin de protéger les données plus sensibles.
- **Règles d'accès granulaires aux applications et aux données.** Elles limitent l'accès aux applications et aux données aux seuls utilisateurs autorisés et minus des appareils fiables afin de renforcer la sécurité.
- **Sécurisation du trafic réseau.** Les technologies de chiffrement sécurisé empêchent les accès non autorisés.
- **Accès conditionnel.** L'accès peut être automatiquement coupé en fonction de seuils de risques liés aux données afin de sécuriser les réseaux.

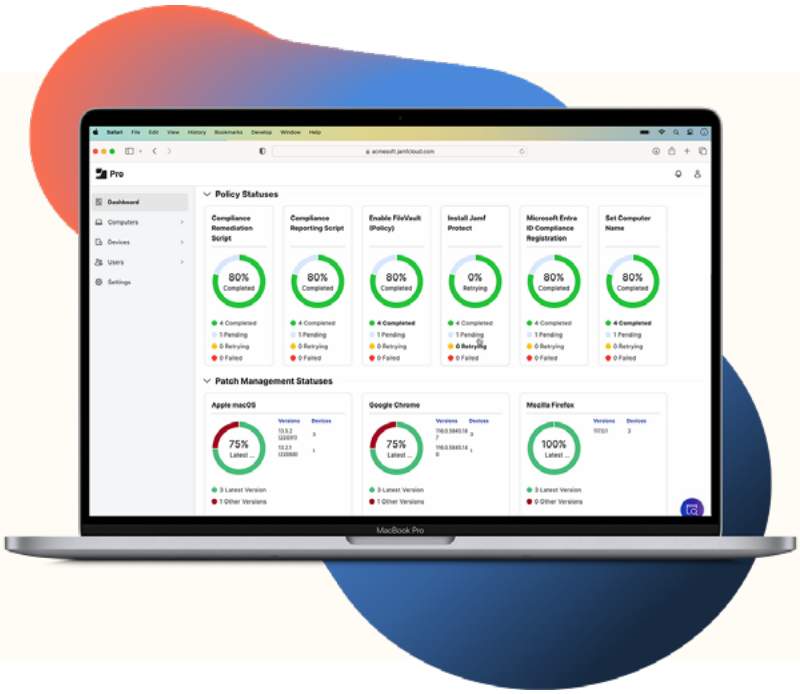
La gestion moderne offre une très grande flexibilité en matière de localisation, d'horaires de travail ou même de modèle de propriété (appareils d'entreprise ou BYOD).

Mais il a fallu atteindre la gestion déclarative des appareils (DDM) d'Apple pour que l'avenir de la gestion moderne prenne réellement forme.

## Qu’est-ce que la gestion déclarative des appareils (DDM) ?

Selon les mots d’Apple, la DDM est une « mise à jour transformatrice » du protocole MDM existant qui permet aux appareils d’agir de manière proactive et autonome.

> **« La gestion déclarative (DDM) est l’avenir de la gestion des appareils »**
>
> **– Apple à la WWDC 2021**




Chez Jamf, nous sommes tout à fait d’accord. C’est pourquoi nous sommes prêts à prendre en charge la DDM dès le premier jour.

**La gestion déclarative des appareils repose sur un principe : des appareils proactifs et autonomes.** Un appareil autonome a reçu des instructions pour réagir à ses propres changements d’état. Il applique ensuite une logique de gestion programmée pour prendre les mesures nécessaires.

Par exemple, s’il n’est plus conforme ou enregistre une activité potentiellement malveillante, il peut agir immédiatement. Il n’a plus besoin d’attendre que le serveur lui demande son état, d’envoyer un rapport, puis d’attendre que le serveur lui indique les étapes à suivre.

Cette approche a trois avantages majeurs :

1. Elle allège le trafic entre le serveur et l’appareil, ce qui a un effet positif sur les performances
2. Elle accélère le processus de mise en sandbox et de correction en cas de soupçon de logiciel malveillant, ce qui renforce la sécurité
3. Elle peut donc être appliquée à grande échelle en consommant moins de ressources

## Comment fonctionne la DDM ?

Le DDM repose principalement sur trois piliers : **les déclarations, le statut et l'extensibilité**.

### Déclarations

Les déclarations sont des charges utiles définies par le serveur et envoyées aux appareils. Elles définissent les règles (comptes, réglages, restrictions, etc.) à appliquer directement sur les appareils. Ceux-ci peuvent être distribués à tous les utilisateurs, à des groupes plus restreints, et même à un utilisateur ou un appareil isolé.

Les déclarations possèdent **obligatoirement** trois propriétés !

1. **Type :** définit la règle qu'une configuration représente.
2. **Clé d'identification :** identifie une déclaration spécifique au sein d'un ensemble. Elle sert à synchroniser les déclarations avec le serveur.
3. **Valeur :** limite les données à une certaine plage ou à un ensemble spécifique de valeurs. Il peut s'agir de chaînes de caractères, de nombres, de valeurs booléennes, de tableaux ou de dictionnaires.

### Types de déclaration

#### Activations

Les activations sont des ensembles de configurations et d'actifs référencés qui sont appliqués automatiquement et doivent tous être valides. Par exemple, une action peut n'être valide que sur un type d'appareil, un OS ou une version d'OS spécifique. La charge du serveur est ainsi transférée à l'appareil, à qui il appartient de choisir les actifs à appliquer selon les critères définis.

#### Actifs

Les actifs désignent les données dont les configurations ont besoin pour fonctionner. Si les données sont volumineuses, la déclaration des actifs fournit l'URL d'un serveur (le serveur MDM ou un autre serveur de distribution de contenu) pour les télécharger. Les actifs peuvent prendre de nombreuses formes : noms, adresses e-mail, mots de passe, certificats, etc.

#### Configurations

Les configurations sont similaires aux profils MDM et décrivent les règles à appliquer à l'appareil (comptes, réglages et restrictions).

#### Gestion

Les déclarations de gestion déterminent l'état général de gestion de chaque appareil. Elles transmettent des informations statiques sur le serveur et l'organisation.

## Canal d'état

Le canal d'état suit les changements d'état de l'appareil. Les appareils envoient des rapports d'état au serveur, qui peut les filtrer en s'abonnant uniquement aux mises à jour qui le concernent directement, comme les versions d'OS, les activités inhabituelles ou les cas de non-conformité.

L'appareil envoie ensuite des rapports incrémentiels : après le rapport d'état initial, seuls les changements sont signalés ; l'appareil n'envoie plus de description complète de son état. Le résultat : des informations plus pertinentes sont délivrées beaucoup plus rapidement. Les mises à jour asynchrones, déclenchées par les appareils, permettent aux serveurs de superviser étroitement les appareils en éliminant les informations inutiles et une grande partie du trafic réseau. **Cette approche améliore considérablement les performances.**

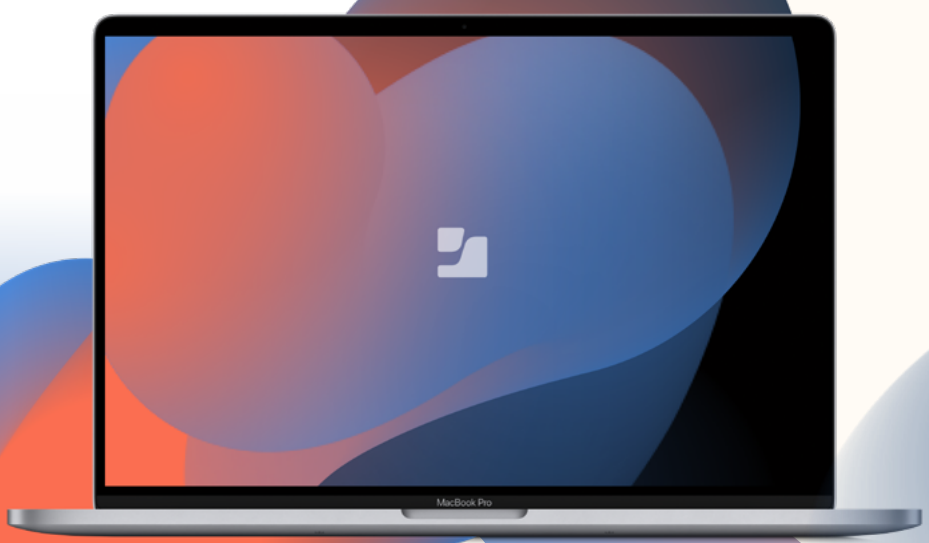
## Extensibilité

Les flottes des organisations sont rarement constituées d'un seul type de produits Apple ou d'une seule version d'OS. N'oubliez pas que les produits Apple restent utiles pendant longtemps. Pour tirer le meilleur parti de votre investissement, vous devez maintenir la compatibilité entre les différentes versions des logiciels et les capacités des appareils.

Avec la DDM, les appareils et les serveurs communiquent spontanément les changements : tous sont donc immédiatement informés lors de la sortie de nouvelles fonctionnalités. Nul besoin de coder en dur les versions de logiciels ou les dépendances matérielles.

Prenons un exemple : lorsque le service informatique met le serveur à niveau, elle synchronise automatiquement les nouvelles capacités avec l'appareil, qui peut alors les utiliser immédiatement. L'inverse est également vrai : lorsqu'un appareil se met à jour, le serveur sait immédiatement quelles sont les nouvelles fonctions intéressantes de l'appareil.

**Grâce à l'extensibilité inhérente au modèle de données déclaratives, vous savez que votre structure est pensée pour les besoins d'aujourd'hui et prête pour ceux de demain.**



## Un nouvel horizon avec la DDM

Nous ne sommes qu'au début de l'évolution de la DDM et de la MDM. Imaginez les possibilités d'une approche qui :

- Prend en charge de nouvelles stratégies de gestion complexes d'une manière simple et uniformisée
- Améliore l'expérience utilisateur sur les appareils gérés, qu'ils soient professionnels ou personnels
- Offre une expérience plus réactive et plus fiable aux utilisateurs
- Accélère le déploiement
- Libère les équipes informatiques des tâches répétitives et fastidieuses pour lui permettre d'innover et de se concentrer sur les fonctionnalités de gestion des appareils les plus utiles

**Que pourrait faire votre service informatique s'il avait le temps d'élaborer des projets ambitieux ?**

Quand vous optez pour une stratégie de DDM, de nouvelles possibilités s'ouvrent à votre organisation. Votre activité peut se développer au rythme de l'évolution de la DDM, à la vitesse d'Apple.

Quel potentiel voyez-vous à l'horizon pour votre organisation ? Pour vos propres objectifs ? Pour le monde du travail lui-même ?

Nous pensons que nous ne faisons qu'entrevoir le potentiel de cette technologie, qui peut transformer le travail et répondre aux besoins toujours changeants de la gestion moderne. Voici un petit aperçu de ce qui nous attend.

## Comment la DDM va-t-elle façonner l'avenir de la MDM ?

Sans lire dans une boule de cristal, on peut imaginer sans risque de se tromper qu'Apple va élargir le champ des possibles avec les capacités DDM. Voici quelques domaines qui, selon nous, sont appelés à se développer pour tous ceux qui utilisent et gèrent les appareils Apple.

### Sécurité

Si l'on combine les capacités de la DDM avec d'autres changements récents, une tendance se dessine.

Apple Silicon a, pour ainsi dire, bloqué toute possibilité de mise à jour non surveillée déclenchée par un script ou un agent local disposant de privilèges Root. Cela ferme la porte à certaines stratégies prisées des pirates et décourage les pratiques dangereuses telles que l'utilisation d'extensions du noyau, qui met en péril l'intégrité de l'OS.

À l'avenir, il faut s'attendre à ce que les actions administratives exigent de plus en plus des outils spécialisés et conçus pour réduire les risques.

### Un accès plus nuancé

Il est raisonnable de supposer que les organisations, en s'appuyant sur les identifiants Apple gérés, vont exercer un contrôle plus étroit sur l'accès aux services (et aux installations) grâce aux trousseaux iCloud et à la prise en charge du portefeuille Apple.

Cela ne signifie pas nécessairement qu'elles seront plus sévères. La DDM permet aux administrateurs Apple de contrôler les accès de façon bien plus nuancée.

### Une meilleure prise en charge des identités améliore l'expérience utilisateur

Apple Business Manager et Apple School Manager facilitent la prise en charge d'identités personnalisées. Un fournisseur d'identité tel que Microsoft, Google, Okta ou Open ID/SKIM peut désormais se connecter et créer facilement des identifiants gérés – et c'est la meilleure façon de gérer les appareils et les utilisateurs Apple. Quand une seule clé suffit à accéder à tous les outils de travail, les utilisateurs sont plus heureux et, accessoirement, mieux protégés.

Ces évolutions et ces perspectives nous permettent d'affirmer que la MDM sera :

- **Plus sûre**, en permettant de définir la conformité dès le départ à l'aide de déclarations et en limitant les interactions programmatiques avec les binaires de bas niveau
- **Plus native**, en invitant l'utilisateur à interagir sur la base des déclarations
- **Plus utile** dans le temps, en apportant des améliorations successives à la base déjà robuste de la MDM grâce à la DDM

Pour plus d'informations sur les implications de cette profonde transformation, regardez la présentation de la JNUC 2023 : **« MDM : quelle est la prochaine étape ? »** *(en anglais)*

## L’avenir, c’est maintenant.

Et l’un des aspects les plus enthousiasmants de cette évolution majeure est que les fournisseurs de MDM peuvent déjà utiliser les fonctionnalités de gestion déclaratives. Nul besoin de perturber les méthodes de travail avec un nouveau protocole ou une nouvelle infrastructure de serveur : les déclarations et le canal d’état peuvent fonctionner parallèlement aux commandes et aux profils MDM existants. **La DDM n’a aucun impact sur le comportement de la MDM.**

Autrement dit, une équipe informatique peut adopter la MDM à son rythme, sans avoir à modifier soudainement tous les workflows MDM en place.

**Surtout, cela signifie que vous pouvez vous lancer tout de suite !**

## Comment la DDM est-elle prise en charge par Jamf ?

Du fait de l’étroite collaboration entre Jamf et Apple, nous sommes toujours prêts à prendre en charge les innovations d’Apple dès le premier jour.

### Prise en charge dès le départ

Jamf Pro a automatiquement activé les capacités de gestion déclarative pour les appareils gérés compatibles dès octobre 2022. Les appareils concernés signalent automatiquement leurs changements d’état au serveur MDM. Certains changements sont ajoutés aux informations d’inventaire des appareils. Les administrateurs peuvent personnaliser ces états.

### Prise en charge de trois nouveaux champs dans le canal d’état

Trois nouveaux champs ont été ajoutés à la prise en charge du canal d’état DDM dans Jamf Pro 10.46 :

`SupplementalBuildVersion`

`SupplementalOSVersionExtra`

`Passcode Compliance`

Ces nouveaux éléments du canal d’état sont automatiquement activés afin que les appareils puissent dès maintenant communiquer leur état à Jamf Pro en toute autonomie.

### Prise en charge spécifique à iOS

Les possibilités de la DDM sont immenses et elle évolue très rapidement ! Voici quelques exemples concrets de l’utilisation de la DDM permettant d’améliorer la convivialité et la sécurité :

- Sur les appareils iOS, les mises à jour utilisent le code secret de l’écran de verrouillage pour générer un jeton d’autorisation qui expire après un certain temps pour plus de sécurité.
- Une fois activé par l’utilisateur final, ce jeton autorise les mises à jour sans qu’il faille déverrouiller son appareil.
- Les appareils qui n’ont pas été déverrouillés pendant une période définie ne reçoivent plus ces mises à jour ; l’utilisateur sera invité à les autoriser explicitement lorsqu’il déverrouillera son appareil.

### Gestion des mises à jour logicielles par DDM

Avant qu’Apple n’introduise les fonctions de DDM, les administrateurs de Jamf envoyaient soit une action de masse, soit une règle. Les mises à jour des logiciels gérées par DDM offrent de nouvelles possibilités :

- La configuration du plan de mise à jour des logiciels est beaucoup plus simple
- Les utilisateurs finaux disposent d’options de report nuancées
- De nouvelles fonctions d’automatisation et d’application donnent davantage de contrôle aux administrateurs informatiques.
- Les rapports spontanés des appareils sur l’avancement des mises à jour offrent aux administrateurs une plus grande visibilité.

## L'avenir

Jamf va suivre étroitement l'expansion du protocole DDM pour en faire le meilleur usage possible et le prendre en charge à chaque étape. Notre engagement à suivre le rythme d'Apple s'est récemment illustré par la prise en charge de nouveaux types d'appareils au travail, comme Apple Vision Pro et Apple Watch, pour que les utilisateurs finaux puissent adopter les outils avec lesquels ils sont le plus productifs.

## La gestion des appareils Apple n'a jamais été aussi passionnante.

La gestion déclarative des appareils a donné un formidable coup d'accélérateur au passage à une gestion moderne.

Nous avons rompu avec la gestion traditionnelle des appareils. Du jour au lendemain, nous avons abandonné les innombrables pings et les échanges volumineux entre les appareils gérés, Apple et le serveur MDM pour des appareils qui agissent de façon autonome. Nous avons adopté avec enthousiasme les technologies d'avenir.

L'avenir de la gestion et de la MDM se construit en ce moment même, et nous avons la chance d'y participer !

L'ère de la gestion moderne est arrivée.

Les organisations qui sauront tirer parti de cette période de croissance sans précédent seront prêtes pour l'avenir, et c'est en adoptant une flotte Apple qu'elles y parviendront.

## Les critères essentiels

Examinez votre stratégie technologique actuelle. Est-elle flexible ? Est-elle portable ? Reflète-t-elle une approche moderne de la gestion et de la sécurité des appareils ?

Si ce n'est pas le cas, quels avantages pourrait vous apporter une approche moderne de la gestion ? La capacité à grandir rapidement ? Pour pivoter en un instant ? Pour attirer les meilleurs talents et faire en sorte que tout le monde soit connecté et protégé ?

Quels sont les risques si vous prenez du retard ?

L'ère de la gestion moderne est arrivée. Il ne tient qu'à vous de saisir cette opportunité et de voir où elle vous mène.

Et Jamf vous soutiendra à chaque étape.

Si vous êtes prêt à **rejoindre Apple et Jamf** sur la voie de la **gestion moderne**, et si vous souhaitez profiter des avantages du cloud et de la DDM, **nous pouvons vous aider !**

jamf