



# Sécurisation de macOS à l'ère du travail moderne

Les entreprises mondiales sont entrées dans une nouvelle ère du travail moderne, où les individus doivent prendre des décisions avisées à la volée, en utilisant les outils qu'ils connaissent et qu'ils aiment. Cette tendance est alimentée par la génération Y, qui représente un pourcentage croissant du personnel des entreprises d'aujourd'hui. Ces employés souhaitent pouvoir choisir les meilleurs outils sans que leur expérience mobile ou la confidentialité de leurs informations personnelles soient compromises et inondent les entreprises de leurs appareils et applications préférés. La popularité d'Apple auprès de la génération Y a entraîné une augmentation



401 East Middlefield Road  
Mountain View, CA 94043, États-Unis  
[globalsales@mobileiron.com](mailto:globalsales@mobileiron.com)  
[www.mobileiron.com](http://www.mobileiron.com)  
Tél. : +1 877 819 3451  
Fax : +1 650 919 8006

considérable des appareils iOS et, plus récemment, des ordinateurs macOS dans les entreprises. En effet, au 4e trimestre 2017, les expéditions d'appareils Mac ont augmenté de 7,3 % par rapport à l'année précédente, dépassant largement le marché des PC dans son ensemble, qui n'a augmenté que de 0,7 %<sup>1</sup>.

Il n'y a pas si longtemps, les ordinateurs portables et de bureau Mac dans les entreprises étaient essentiellement utilisés par des utilisateurs de niche, tels que des experts en conception graphique et des producteurs de vidéos. Le nombre de postes de travail Mac à gérer étant faible, beaucoup de services informatiques ne sécurisaient pas ces terminaux ou les sécurisaient via une solution distincte, qui ne s'inscrivait pas dans une infrastructure de gestion unifiée des terminaux (UEM). Alors que les solutions autonomes représentent une option intéressante à court terme, elles n'offrent pas la stratégie de long terme ou le modèle de sécurité multicouche nécessaire pour s'adapter aux déploiements croissants d'ordinateurs Mac à l'échelle de l'entreprise. Par conséquent, la gestion des ordinateurs Mac par le biais de solutions autonomes peut menacer les terminaux et créer des failles de sécurité au sein de l'entreprise dans son ensemble.

Il est nécessaire d'adopter une approche stratégique de l'UEM, qui simplifie et réduit le coût des opérations informatiques, prend en charge divers systèmes d'exploitation, notamment iOS, macOS, Android et Windows 10, et offre aux utilisateurs une expérience transparente, sécurisée et productive dans l'environnement de travail moderne d'aujourd'hui. Une plateforme UEM complète, comme le propose MobileIron, permet aux utilisateurs d'opter pour l'innovation mobile et cloud en toute sécurité, et ainsi de prendre des décisions rapides et avisées entraînant des actions significatives au bon moment. Aucune solution autonome n'est en mesure d'offrir tout cela.



<sup>1</sup> <https://9to5mac.com/2018/01/12/mac-market-share-2017/>

## Pourquoi l'UEM est la solution idéale pour sécuriser macOS

L'heure est venue d'adopter une approche plus mature de la gestion des Mac au sein de l'entreprise. C'est particulièrement le cas pour les entreprises qui ont une solution de gestion unifiée des terminaux actuellement déployée, mais qui continuent de gérer macOS via un produit distinct. En déployant tous ces appareils sous l'égide de l'UEM, les services informatiques peuvent les gérer avec un niveau de sécurité plus élevé et optimiser deux domaines de gestion clés :

**Amélioration de l'efficacité opérationnelle.** Avec la gestion des terminaux unifiée, les administrateurs des services informatiques sont en mesure de déployer facilement les paramètres de réseau et d'appareil, les applications, les certificats ainsi que les configurations sur les ordinateurs Mac à partir d'une console centralisée. En continuant à gérer le déploiement des ordinateurs Mac via des solutions autonomes, les services informatiques doivent répéter ces tâches plusieurs fois avec différents outils de gestion qui ne communiquent pas entre eux.

**Gestion solide et complète de la conformité.** Grâce à une plateforme commune, un seul ensemble de règles doit être défini. Une fois cet ensemble de règles approuvé par le responsable de la sécurité de l'entreprise, il peut être appliqué à tous les terminaux afin de garantir la conformité. Le processus est alors simplifié et le travail des services informatiques facilité. À l'inverse, avec les systèmes autonomes, les services informatiques doivent définir différentes règles dans divers systèmes afin de respecter les directives de conformité et de sécurité de l'entreprise. Étant donné le fonctionnement différent de chaque système, certaines règles de conformité risquent d'être négligées. Par exemple, lorsque les réglementations changent, les règles peuvent devenir obsolètes sans que les services informatiques le sachent. Il peut également s'avérer difficile de produire des rapports d'audit complets sans moyen uniforme de les visualiser pour chaque solution.

## Choisissez MobileIron pour gérer les déploiements de vos ordinateurs Mac de manière sécurisée

MobileIron offre un modèle d'accès et de sécurité multicouche pour macOS, qui renforce l'efficacité opérationnelle et facilite la conformité en simplifiant la gestion de tous les terminaux de l'entreprise, quel que soit le format de l'appareil ou le système d'exploitation. L'agent macOS MobileIron facilite l'enregistrement des utilisateurs dans la solution UEM et aide également à l'exécution des scripts pour les tâches qui ne relèvent pas du protocole MDM. Par ailleurs, il peut être déployé comme n'importe quelle autre application sur des appareils déjà enregistrés et n'a pas d'impact sur la gestion existante afin de fournir aux terminaux une fonction d'« exécution de script ».

### Sécurité renforcée

Grâce à un contrôle plus précis et à une meilleure visibilité, les entreprises sont en mesure de respecter les règles de conformité et de protéger les données sur les ordinateurs de bureau Mac détenus par l'entreprise ou par l'employé, tout comme les autres appareils sous divers systèmes d'exploitation. Avec MobileIron, les entreprises peuvent tirer profit du chiffrement des appareils et des paramètres de prévention contre la perte de données, mais aussi mettre en place un accès conditionnel aux services cloud, tels qu'Office 365 et Salesforce.com.

### Facilité de gestion

Les services informatiques bénéficient d'une gestion plus efficace avec un faible niveau d'intervention qui permet aux administrateurs de configurer n'importe quel appareil à distance et de fournir un accès sécurisé aux applications d'entreprise, à la messagerie, au Wi-Fi, au VPN, et à d'autres applications de productivité et référentiels de contenu, tels que SharePoint et Box. Désormais, la gestion des Mac avec MobileIron est aussi simple

que celle des appareils iOS ou autres, car elle ne nécessite ni courbe d'apprentissage, ni intervention manuelle, ni formation des administrateurs.

Les services informatiques gagnent également en productivité grâce à une architecture de sécurité des applications mobiles qui permet aux administrateurs de distribuer, de protéger et de gérer les applications à grande échelle. La confidentialité des informations personnelles des employés est également protégée par la séparation des applications et données personnelles et professionnelles qui figurent sur les ordinateurs de bureau détenus par les employés. Point tout aussi important, les services informatiques peuvent gérer les appareils tout au long de leur cycle de vie, notamment en déployant, en administrant et en excluant les appareils lorsque des employés quittent l'entreprise ou remplacent leurs ordinateurs de bureau.

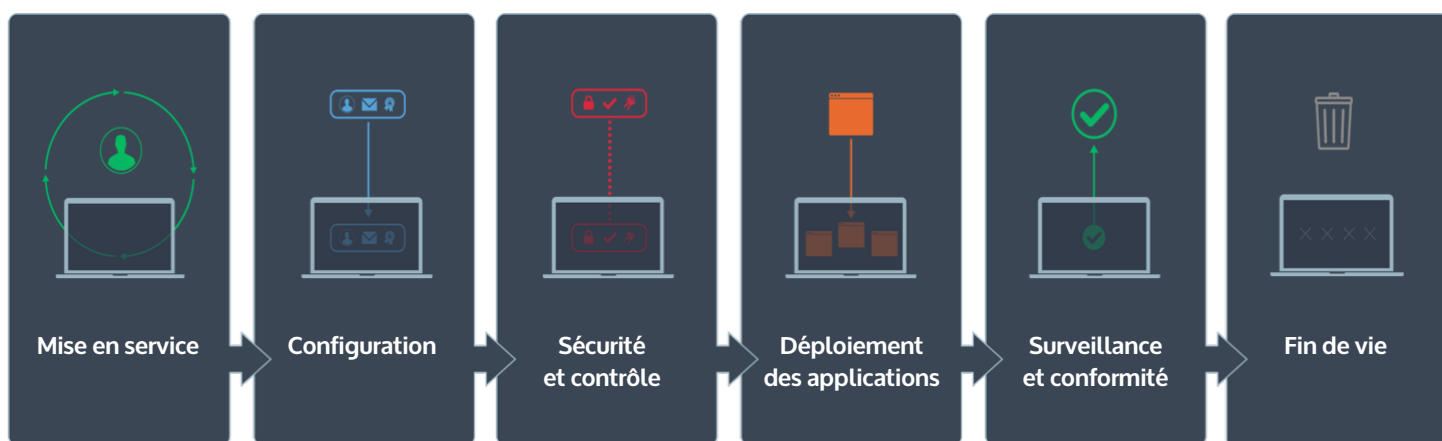
### Meilleure expérience utilisateur

MobileIron aide les services informatiques à accroître la productivité en permettant aux utilisateurs d'être opérationnels en quelques minutes sur n'importe quel appareil. Le personnel contractuel et à distance peut accéder rapidement aux applications et au

contenu de l'entreprise à partir d'un ordinateur de bureau Mac intégralement provisionné, où qu'il travaille. Grâce à des options de dépannage et de libre-service facilement accessibles, MobileIron aide les utilisateurs à résoudre les problèmes par eux-mêmes, réduisant ainsi le nombre d'appels à l'assistance. Par ailleurs, les utilisateurs bénéficient de la même expérience intuitive MobileIron sur tous leurs appareils, des smartphones aux tablettes en passant par les ordinateurs de bureau. Les employés n'ont pas à naviguer entre plusieurs interfaces de gestion sur différents appareils. En enregistrant les appareils d'entreprise dans MobileIron, les utilisateurs bénéficient d'une expérience transparente sur tous ces appareils.

## MobileIron sécurise les Mac tout au long du cycle de vie de leur gestion

MobileIron fournit une solution complète de gestion des ordinateurs de bureau Mac à chaque étape du cycle de vie de gestion des appareils. Si les entreprises utilisent déjà MobileIron pour sécuriser et gérer des appareils sous iOS, Android ou Windows 10, elles peuvent facilement étendre ces fonctionnalités aux postes de travail Mac.



### **Mise en service**

MobileIron prend en charge le programme d'inscription des appareils (DEP) d'Apple pour faciliter la mise en service et la configuration de nouveaux appareils détenus par les entreprises, notamment les ordinateurs Mac. Comme indiqué précédemment, l'agent macOS MobileIron offre davantage de contrôles précis qui vont au-delà des fonctionnalités de sécurité prises en charge via le protocole MDM, mais il sert également de point d'inscription.

### **Configuration**

Les services informatiques ont accès à la console MobileIron facile à utiliser afin de configurer tous les terminaux modernes par le biais de paramètres, de certificats, du Wi-Fi, de VPN et bien d'autres. L'agent macOS permet aux administrateurs d'exécuter des scripts complexes qu'ils auraient pu utiliser avec des systèmes existants ou des solutions ad hoc pour prendre en charge des cas d'utilisation de niche.

### **Sécurité et contrôle**

La sécurisation des ordinateurs Mac avec MobileIron n'est pas différente de celle des autres appareils. Les entreprises peuvent protéger leurs données au sein de services cloud, tels qu'Office 365 et Salesforce, en bloquant les appareils non conformes grâce à MobileIron Access. MobileIron protège aussi les données lorsqu'elles quittent un ordinateur Mac en sécurisant la connexion via MobileIron Tunnel, qui fournit un VPN par application et évite le recours à un VPN tiers distinct. Les services informatiques ont également la possibilité de déployer et de mettre à jour des applications antivirus et anti-logiciels malveillants standard sur tous les ordinateurs Mac par le biais de la console MobileIron.

### **Déploiement des applications**

MobileIron prend en charge une gamme complète de fonctionnalités de distribution et de cycle de vie des applications sur les ordinateurs macOS, notamment le programme d'achat en volume (VPP) d'Apple. Il est possible d'organiser les

applications provenant de l'App Store d'Apple tout comme les applications internes dans Apps@Work et de les déployer sur chaque ordinateur Mac. Diverses applications peuvent être mises à la disposition de différents utilisateurs dans Apps@Work selon les règles de l'entreprise. Les utilisateurs finaux ont simplement à télécharger, puis à installer, les applications qu'ils souhaitent, en les sélectionnant dans Apps@Work. Par le biais de la console MobileIron, les administrateurs peuvent définir des règles qui limitent le téléchargement des applications par les employés sur leurs appareils et empêchent les applications d'effectuer des actions malveillantes.

### **Surveillance et conformité**

Afin de garantir la conformité de tous les appareils, y compris les Mac, les administrateurs doivent avoir une visibilité sur l'état de conformité de chaque appareil. Grâce à MobileIron, les services informatiques sont en mesure de définir une infrastructure de sécurité et de la mettre en œuvre de façon cohérente sur l'ensemble des appareils mobiles et ordinateurs via un moteur de règles intuitif. Les appareils non conformes peuvent rapidement être identifiés et se voir refuser l'accès aux ressources de l'entreprise, le cas échéant. La précision des paramètres et des configurations disponibles pour définir des règles de sécurité et de conformité permet également aux services informatiques de les adapter et de les mettre à jour à mesure que les réglementations et les exigences de l'entreprise, telles que le RGPD, la norme PCI DSS ainsi que la loi HIPAA, évoluent.

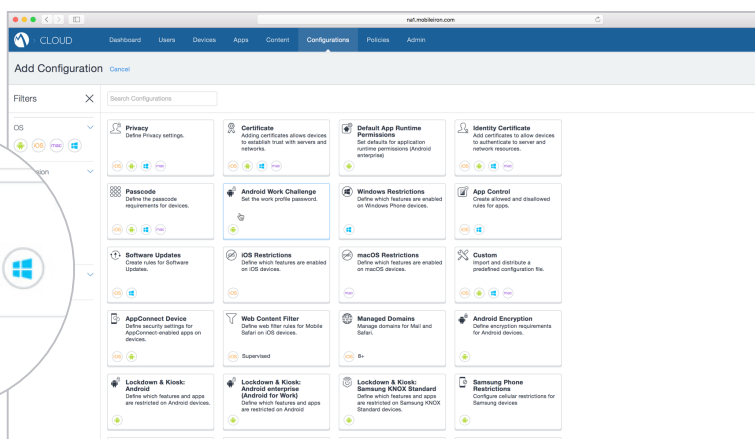
### **Fin de vie**

Lorsqu'un ordinateur Mac arrive en fin de vie ou qu'un employé quitte l'entreprise, les services informatiques ont la possibilité de supprimer à distance toutes les applications, les données et les configurations de l'entreprise, et de rétablir les paramètres d'usine de l'ordinateur. Dans le cas d'un ordinateur Mac détenu par un employé, les services informatiques peuvent simplement supprimer les applications et les données de l'entreprise tout en gardant intacts les applications et les contenus personnels sur l'ordinateur.

# Le travail moderne nécessite un modèle de sécurité moderne

Le paysage des entreprises a changé de façon radicale avec l'arrivée de la génération Y, et de ses appareils favoris, dans le monde du travail. Par conséquent, les ordinateurs Mac, autrefois limités à des utilisations de niche, se développent désormais au sein des entreprises à vitesse grand V. Ces ordinateurs exigent le même niveau de sécurité et de surveillance que les autres appareils. Si elles ne sécurisent pas les ordinateurs Mac ou se contentent de les gérer avec des produits individuels, les entreprises s'exposent à des failles de sécurité qui les rendent vulnérables aux cyberattaques ainsi qu'aux violations de la conformité.

La bonne nouvelle, c'est que, grâce à MobileIron, sécuriser les ordinateurs Mac devient aussi simple que de gérer les autres appareils de l'entreprise. Aucune intégration, aucune formation supplémentaire ni aucun temps d'adaptation n'est nécessaire. L'heure est venue d'adopter une approche moderne de la gestion des ordinateurs Mac, invisible aux yeux des utilisateurs finaux, qui améliore l'efficacité opérationnelle et simplifie les opérations informatiques tout au long du cycle de vie des appareils. C'est possible grâce à MobileIron.



Avec MobileIron Cloud, sécurisez les ordinateurs de bureau Mac en même temps que les terminaux sous d'autres systèmes d'exploitation.

## Pour en savoir plus

Pour découvrir comment MobileIron offre une sécurité moderne des terminaux macOS, consultez notre [page](#).