

Les plus grandes entreprises du monde s'appuient sur MobileIron pour opérer en toute sécurité leur transition Mobile First. Notre plateforme globale de gestion unifiée des terminaux (UEM, Unified Endpoint Management) est spécialement conçue pour sécuriser les environnements multi-OS grâce à des fonctionnalités innovantes de gestion des appareils, des contenus et des applications mobiles. Nos clients bénéficient en outre d'un accès garanti à notre technologie UEM et à nos services d'intégration partout dans le monde grâce à notre réseau de partenaires international.

Parce que nous proposons une plateforme UEM très modulable et une expertise globale, de plus en plus d'organisations se tournent vers MobileIron pour accélérer leur adoption d'Android. Avec deux milliards d'appareils actifs tous les mois, Android est devenu le premier système d'exploitation mobile grand public. En entreprise, Android équipe le plus grand éventail de déploiements, des solutions à utilisation unique aux outils de productivité haut de gamme.

Premier fournisseur à proposer une boutique d'applications professionnelles, des contrôles de la confidentialité BYOD et la gestion des identités à l'aide de certificats pour Android, MobileIron est également l'un des premiers fournisseurs UEM à prendre en charge la plateforme Android pour les entreprises.



## Défi

- Renforcer la sécurité des données sensibles sous Android
- Sécuriser et configurer les applications Android
- Inscrire les appareils détenus par l'entreprise, une opération qui requiert des connaissances techniques
- Déployer les appareils Android, en propre et en BYOD
- Harmoniser à grande échelle la gestion informatique d'appareils de divers fabricants

## Solution

- MobileIron pour Android

## Fonctionnalités

- Élargir la prise en charge des appareils par l'intégration sécurisée des appareils et applications Android
- Inscrire les appareils mobiles d'entreprise sans contact
- Distinguer données personnelles et données professionnelles sur l'appareil
- Appliquer des règles de sécurité et de confidentialité
- Protéger les données statiques par le chiffrement et les contrôles DLP
- Préserver l'expérience native pour satisfaire les employés
- Assurer un contrôle précis au niveau des applications durant tout leur cycle de vie
- Sécuriser et protéger les appareils Android dédiés en mode kiosk

## De la flexibilité pour répondre à vos besoins

MobileIron pour Android gère un large éventail de scénarios d'utilisation pour répondre au mieux aux besoins de votre organisation. Ces cas d'utilisation vous permettent de segmenter vos utilisateurs en fonction de leur rôle et du détenteur de leurs appareils (l'entreprise ou l'employé). Ils concernent aussi bien des appareils grand public utilisés par les travailleurs du savoir (BYOD, par exemple) que des appareils dédiés aux travailleurs à la tâche. Avec MobileIron pour Android, les entreprises peuvent accroître la productivité de leurs collaborateurs en mettant à leur disposition les outils et les appareils nécessaires pour réussir en toute sécurité la transformation du paysage mobile.

## Une gestion informatique cohérente à grande échelle sur différents types d'appareils

Android pour les entreprises offre aux entreprises un modèle de sécurité plus exhaustif et cohérent, modèle pris en charge par MobileIron. Avec la console UEM de MobileIron, les services informatiques peuvent distribuer des applications d'entreprise et des configurations sur des appareils équipés d'Android pour



les entreprises. Grâce à une distribution et à une sécurité cohérentes des applications, ces fonctions inédites simplifient la gestion informatique et réduisent la fragmentation d'Android.

## Une base sécurisée pour Android en entreprise

MobileIron pour Android répond aux inquiétudes des entreprises en matière de sécurité en créant une entité entreprise qui sépare les applications et les contenus personnels et professionnels, sans modifier l'expérience utilisateur native. Qu'un appareil appartienne à l'entreprise ou soit détenu par un employé dans le cadre d'un programme BYOD, le conteneur d'entreprise est entièrement contrôlé par le service informatique. L'administrateur peut définir et gérer des règles pour les applications et les données, et procéder à des effacements sélectifs ou complets sur le conteneur.

MobileIron pour Android fournit aux services informatiques les contrôles de sécurité des données nécessaires tout en assurant une expérience utilisateur cohérente sur tous les appareils. Fonctionnalités incluses :

### Sécurité des appareils

- Sécurisation des appareils Android à l'aide de règles de codes d'accès, dont la gestion d'options biométriques
- Protection contre les accès non autorisés par le verrouillage des accès matériels
- Verrouillage avec le mode kiosque et prise en charge des appareils partagés

### Sécurité des données

- Chiffrement distinct des données d'applications
- Sécurité basée sur les certificats pour la messagerie, le Wi-Fi et le VPN
- Authentification unique sécurisée
- Effacement sélectif des données d'applications d'entreprise

### Prévention contre la perte des données (DLP)

- Contrôle des pièces jointes chiffrées
- Contrôle des captures d'écran
- Contrôle de la fonction copier/coller

### Accès sécurisé au réseau

- Tunneling des applications
- Configuration d'un réseau Wi-Fi d'entreprise
- Configuration d'un VPN d'entreprise

## Une gestion avancée des applications pour Android, axée sur la productivité

En proposant la plateforme de gestion des applications mobiles la plus exhaustive qui soit pour le système Android, MobileIron permet aux utilisateurs d'être productifs sur leurs appareils mobiles. La distribution et la recherche d'applications sont disponibles avec Google Play d'entreprise ou Apps@Work, la sécurité des données est assurée par le biais de conteneurs d'entreprise natifs ou AppConnect, et la configuration des applications d'entreprise est sécurisée dans le respect des normes du secteur grâce à AppConfig.

MobileIron pour Android compartimente les applications d'entreprise dans un conteneur sécurisé dont les données sont chiffrées, protégées contre tout accès non autorisé et effaçables. Un code unique sécurise l'accès aux applications d'entreprise, et les utilisateurs peuvent facilement accéder aux données de ces applications et les partager. Toutes les applications conteneurisées sont gérées via la plateforme MobileIron de gestion centralisée des règles qui prend en charge les processus Android natifs et offre une expérience mobile favorisant la productivité des utilisateurs. Fonctionnalités de productivité incluses :

### Gestion PIM sécurisée

MobileIron pour Android propose différentes solutions pour accéder de façon sécurisée aux applications de gestion des informations personnelles (personal information management, PIM). En effet, les services informatiques peuvent utiliser la plateforme MobileIron pour configurer et distribuer facilement des applications conteneurisées, telles que la messagerie, les contacts, l'agenda et la liste de tâches. Avec Android pour les entreprises, il est également possible d'installer et de supprimer des applications publiques de manière silencieuse.

	MobileIron Email+ pour Android	Gmail
Configuration par l'équipe informatique	✓	✓
Messagerie	✓	✓
Agenda	✓	✓
Contacts	✓	✓

### Gestion sécurisée des contenus

MobileIron Docs@Work permet aux utilisateurs d'accéder à différents référentiels de contenus facilement et en toute sécurité. Ils peuvent utiliser leurs appareils mobiles pour télécharger des contenus, consulter, annoter et modifier des fichiers ou des dossiers distants, et enregistrer les modifications effectuées. Docs@Work offre aux administrateurs informatiques la possibilité de gérer l'accès aux référentiels de contenus de façon centralisée, de préremplir des noms d'utilisateur et des chemins d'accès aux dossiers, et d'autoriser des appareils extérieurs au réseau approuvé à accéder aux référentiels de contenus internes via MobileIron Sentry. Docs@Work sécurise la connexion à un large éventail de serveurs de contenus différents. (Pour plus d'informations, consultez la fiche technique de Docs@Work.)

### Navigation sécurisée

Web@Work, la solution de navigation sécurisée de MobileIron, crée des tunnels propres aux navigateurs afin d'accéder aux ressources Web de l'entreprise sans passer par un VPN étendu à l'appareil. Android pour les entreprises comprend également Google Chrome, un navigateur conteneurisé sécurisé, deux outils que la plateforme MobileIron est en mesure de gérer.



MobileIron met à disposition des entreprises du monde entier, quelle que soit leur taille, un socle de sécurité pour le travail moderne. Pour plus d'informations, visitez le site [www.mobileiron.com/android](http://www.mobileiron.com/android) ou contactez votre représentant commercial MobileIron.



« Android Enterprise Recommended », un programme Google, valide les offres de produits EMM (Enterprise Mobility Management, ou Gestion de la mobilité en entreprise) qui intègrent des fonctionnalités avancées d'Android pour les entreprises et qui sont proposées par des partenaires capables de fournir des conseils fiables et une assistance professionnelle.