

# MobileIron Access

Services cloud sécurisés sur mobile



## Repenser la sécurité dans un univers cloud mobile

Avec la consomérisation de l'informatique, l'utilisation d'applications et d'appareils mobiles personnels dans le cadre professionnel a tendance à se généraliser. Dans le même temps, les entreprises du monde entier transfèrent leurs processus métier vers des applications et des services cloud tels que Box, G Suite, Microsoft Office 365 et Salesforce. Ainsi, de plus en plus de collaborateurs accèdent à des ressources cloud professionnelles par simple saisie d'un nom d'utilisateur et d'un mot de passe dans une application ou un appareil personnel, ce qui met en péril les données de l'entreprise.

La méthode du nom d'utilisateur/mot de passe s'est avérée efficace tant qu'il s'agissait de sécuriser les services cloud sur des PC d'entreprise, mais elle ne suffit plus aujourd'hui pour protéger des données professionnelles dans l'univers cloud mobile. Désormais, pour sécuriser l'accès au cloud depuis les applications mobiles, il faut non seulement vérifier l'identité de l'utilisateur, mais aussi disposer d'une infrastructure permettant de contrôler le statut de l'appareil et les autorisations des applications, de sorte que les ressources de l'entreprise soient accessibles depuis le cloud uniquement aux utilisateurs, appareils et applications de confiance.

## MobileIron Access : la solution pour sécuriser l'accès aux données cloud depuis les applications mobiles

MobileIron Access est une solution de sécurité cloud qui permet de conditionner l'accès aux services cloud à partir des applications et des navigateurs mobiles. Contrairement aux approches de sécurité classiques, MobileIron Access met en corrélation l'identité de l'utilisateur avec des informations uniques telles que le statut de l'appareil ou l'état de l'application. MobileIron garantit que les données professionnelles restent dans les limites fixées par le service informatique et ne puissent pas être stockées sur des appareils non sécurisés, connectées à des applications non gérées ou partagées avec des services cloud non approuvés. Avec MobileIron Access, les organisations bénéficient d'une approche basée sur les normes capable de sécuriser tout service cloud, y compris Office 365, sans nécessiter aucune intégration propriétaire.

## Sécuriser les données de l'entreprise avec MobileIron Access

MobileIron Access contribue à éliminer le risque lié aux applications mobiles et au cloud dans les scénarios courants suivants :

- 1. Appareil non géré :** une collaboratrice souhaite consulter des informations sur Salesforce, mais elle a laissé l'iPad de la société au bureau. Avec la méthode du nom d'utilisateur/mot de passe, elle peut saisir ses identifiants dans l'application Salesforce sur son iPad personnel, puis consulter et enregistrer des contenus professionnels sur un appareil non sécurisé. Avec MobileIron Access, cette collaboratrice ne peut accéder aux données qu'une fois son appareil enregistré et sécurisé via MobileIron.

### Le défi

- Les applications mobiles sont devenues le principal moyen par lequel les utilisateurs professionnels accèdent aux services cloud.
- Les solutions de sécurité classiques basées sur PC ne sont plus suffisantes pour protéger vos données dans le cloud.



401 East Middlefield Road,  
Mountain View, CA 94043,  
États-Unis

info@mobileiron.com  
www.mobileiron.com

Tél. : +1 877 819 3451  
Fax : +1 650 919 8006

- 2. Application non gérée :** un collaborateur télécharge par inadvertance PowerPoint de la suite Office 365 à partir d'un magasin d'applications tiers au lieu de passer par le magasin d'applications professionnelles sécurisé. Avec une solution de sécurité classique basée sur l'identité, ce collaborateur peut utiliser la version non gérée de PowerPoint pour accéder aux données de l'entreprise. Ces données peuvent également être partagées avec d'autres applications non sécurisées, ainsi qu'avec des services cloud non autorisés. De plus, les données d'application ne peuvent pas être supprimées en cas de perte ou de vol de l'appareil. MobileIron Access permet de prévenir facilement le risque de perte de données en invitant l'utilisateur à télécharger la version gérée de PowerPoint à partir du magasin d'applications professionnelles.
- 3. Services cloud non approuvés :** un collaborateur découvre une nouvelle application de productivité et la connecte à son compte Box professionnel en utilisant seulement son ID utilisateur et son mot de passe. Malheureusement, il s'agit d'une application malveillante qui utilise les API Box publiques pour copier des fichiers sensibles de l'entreprise dans un service cloud non autorisé. Avec MobileIron Access, aucun service cloud non approuvé ne peut se connecter aux services cloud de l'entreprise, ce qui élimine le risque de fuite de données.

#### Pourquoi MobileIron Access :

- Protéger les données à l'aide d'autorisations conditionnelles basées sur le statut de l'appareil, de l'application et du cloud
- Simplifier l'authentification avec une authentification unique transparente
- Accélérer les processus de correction pour garantir la productivité en continu
- Disposer de journaux détaillés pour créer des rapports d'audit et de conformité
- Adopter une approche basée sur les normes pour déployer une sécurité cloud de pointe et évolutive
- Profiter d'une plateforme end-to-end pour la sécurité cloud mobile

## Favoriser l'adoption avec un accès cloud transparent via l'authentification unique

La nécessité de mémoriser et de saisir constamment des mots de passe est une grande source d'insatisfaction pour les utilisateurs, notamment parce qu'ils utilisent toujours plus d'applications mobiles et cloud au travail. De plus, les mots de passe ne sont pas faciles à saisir sur les petits écrans des mobiles. Les erreurs sont fréquentes et donnent parfois lieu à des verrouillages de comptes, ce qui a pour effet de multiplier le nombre d'appels au service d'assistance et de réduire la productivité des collaborateurs.

MobileIron Access prend en charge l'authentification unique (SSO) pour les applications mobiles cloud et internes, sachant que cela ne requiert aucune intégration ni modification spécifique de l'application elle-même. Avec MobileIron Access, les utilisateurs profitent de l'authentification unique, et le service informatique peut protéger la vie privée des utilisateurs, simplifier l'accès aux applications et aux données mobiles de l'entreprise, et proposer un système de sécurité transparent qui protège les données professionnelles sans pour autant freiner la productivité mobile.

## S'offrir une meilleure visibilité avec MobileIron Access

Alors que de plus en plus d'entreprises s'appuient sur une combinaison de services cloud, d'applications et d'appareils, les services informatiques ont besoin d'un système centralisé et évolutif permettant d'appliquer des règles et de suivre, contrôler et documenter la conformité.

Grâce aux fonctionnalités de génération de rapports et de journalisation de MobileIron Access, ils peuvent voir combien d'utilisateurs sont connectés aux services cloud, afficher les types d'appareils et d'applications mobiles utilisés, et vérifier que ces derniers sont sécurisés. Les administrateurs peuvent aisément accéder aux données détaillées des rapports, entre autres pour identifier les utilisateurs dont les applications sont obsolètes.

## Protéger les données dans le cloud est plus facile que vous ne le pensez

MobileIron Access combine des informations uniques sur le statut de l'appareil et de l'application avec un cadre basé sur des normes pour fournir un accès transparent et sécurisé à tout service cloud sur tout appareil mobile. Pour découvrir comment résoudre les problèmes liés à la sécurité des applications mobiles et cloud, rendez-vous sur le site [mobileiron.com/access](https://mobileiron.com/access).