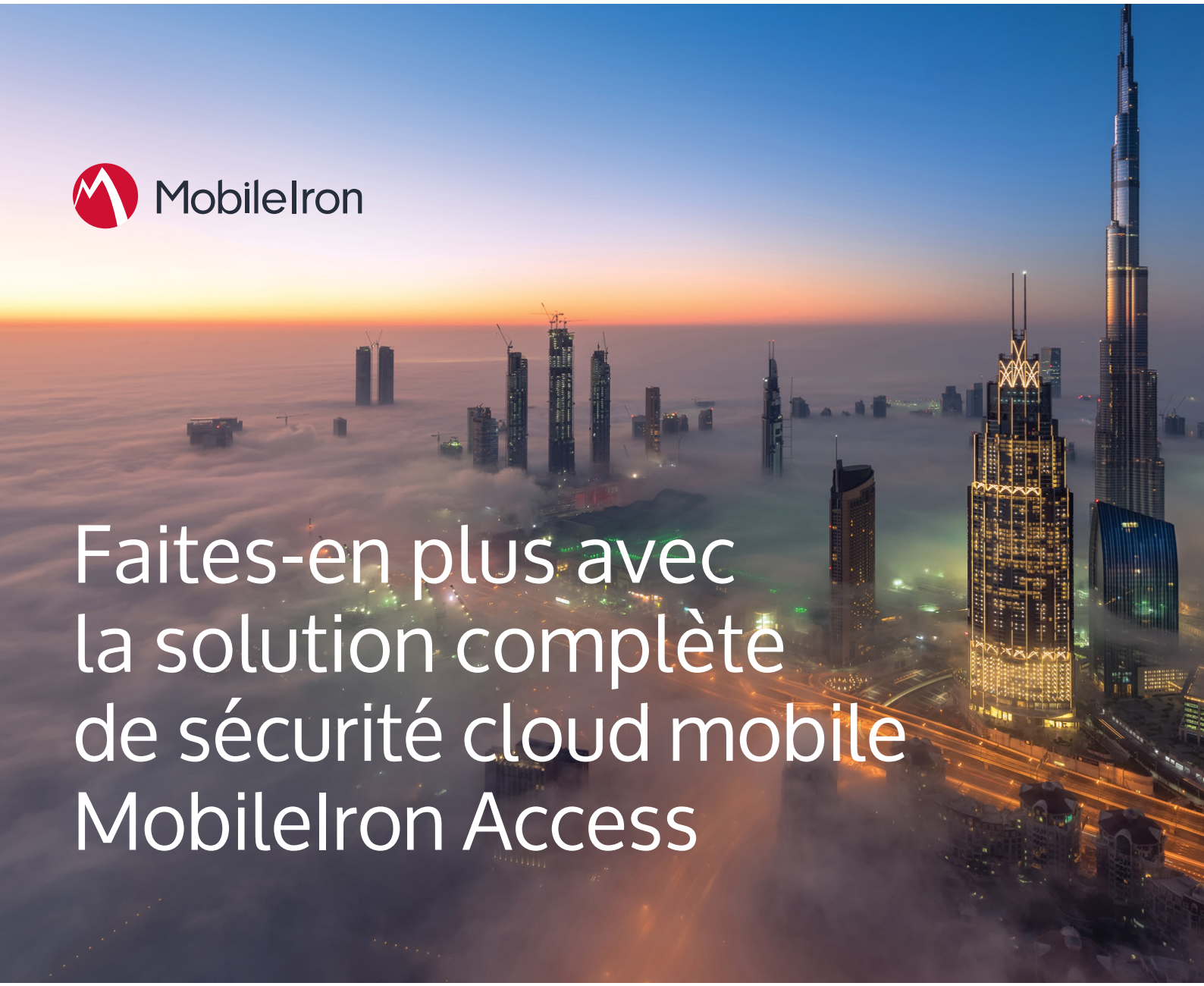


Faites-en plus avec la solution complète de sécurité cloud mobile MobileIron Access

MobileIron Access : un système complet de sécurité dans le cloud

Une solution exhaustive de sécurité. MobileIron Access utilise le statut des appareils et des applications, l'identité des utilisateurs, les données de localisation et d'autres informations pour garantir que seuls des appareils, applications et utilisateurs de confiance peuvent accéder aux services cloud de l'entreprise.

Une plateforme unifiée. MobileIron Access est une plateforme unique et unifiée facile à déployer qui aide les organisations à sécuriser leurs applications et données professionnelles stockées dans le cloud et sur des appareils mobiles.

Une solution de sécurité compatible avec les normes en vigueur. MobileIron Access s'intègre facilement aux meilleurs fournisseurs d'identité et sécurise tous les services cloud compatibles avec la norme SAML 2.0, sans qu'aucune tâche d'intégration personnalisée ne soit nécessaire.

La sécurité cloud mobile : un véritable défi

Partout dans le monde, l'évolution des entreprises vers les services cloud et les technologies de terminaux mobiles connaît un rythme sans précédent. Les modèles de sécurité basés sur les ordinateurs de bureau n'étant plus adaptés, l'adoption des technologies cloud mobiles contraint les organisations à repenser entièrement leur organisation, de l'architecture des centres de données à la sécurité des terminaux.

À l'époque où les ordinateurs de bureau contrôlés par le service informatique étaient la norme, les organisations pouvaient se reposer exclusivement sur l'approche nom d'utilisateur/mot de passe pour sécuriser l'accès aux informations. Dans le monde cloud mobile d'aujourd'hui, ce modèle n'est plus suffisant, parce qu'il ne propose aucun mécanisme de vérification de l'état de l'appareil ou de l'application, et parce qu'il encourage les comportements non sécurisés et complique l'expérience utilisateur. Par exemple, il ne permet pas de détecter si un utilisateur accède à une application d'entreprise à partir d'un appareil mobile jailbreaké, un comportement susceptible de menacer les données de l'entreprise. De plus, les utilisateurs risquent de créer des mots de passe peu sécurisés et faciles à mémoriser, ou de les stocker dans des emplacements facilement accessibles mais peu sûrs, tels qu'un document Google personnel. En outre, la saisie de mots de passe complexes sur les écrans mobiles de petite taille peut être une source de désagrément pour les utilisateurs qui tentent d'accéder aux documents et aux données de leur entreprise depuis leur appareil mobile. Si des identifiants erronés sont saisis un trop grand nombre de fois, le compte correspondant risque également d'être verrouillé.

Ce document présente certaines des failles de sécurité auxquelles les entreprises cloud mobiles d'aujourd'hui doivent faire face :

- **Des appareils non sécurisés.** Sur un appareil non sécurisé, un utilisateur peut facilement accéder aux données de l'entreprise depuis des applications mobiles ou des services cloud : il lui suffit de saisir ses identifiants dans une application ou un navigateur installé sur l'appareil en question. Dès lors qu'elles se trouvent sur l'appareil, les données risquent d'être piratées ou partagées avec des sources externes non autorisées. Par exemple, les appareils sur lesquels sont installés des systèmes d'exploitation récents tels qu'iOS, Android ou Windows 10 et qui ne sont pas inscrits à une plateforme de gestion des appareils mobiles (MDM) sont des appareils non sécurisés. Une machine Windows 7 non connectée à un domaine peut également être vulnérable aux failles de sécurité.
- **Des applications non gérées.** Par applications non gérées, on entend généralement des applications d'entreprise, telles que les applications de productivité Office 365, que l'utilisateur a téléchargées depuis le magasin d'applications personnelles et non depuis le magasin d'applications professionnelles. Ces applications ne sont donc pas contrôlées par le service informatique, mais elles peuvent néanmoins être utilisées pour accéder à des contenus de l'entreprise dès lors que l'utilisateur saisit ses identifiants. Le service informatique n'ayant aucune visibilité ni aucun contrôle sur les applications mobiles non gérées, ces données peuvent alors être partagées avec d'autres appareils et applications.
- **Des services cloud non approuvés.** La plupart des services cloud d'entreprise sont associés à des écosystèmes d'applications et de services dont l'intégration est assurée via des API. Alors qu'un service cloud d'entreprise peut être approuvé, les applications et services de l'écosystème correspondant ne le sont pas forcément. Par conséquent, les utilisateurs peuvent utiliser leurs identifiants pour connecter des services tiers non approuvés à des services cloud d'entreprise. Il devient alors possible d'accéder aux données de l'entreprise, ou de partager ces données, via un service cloud non approuvé sans que le service informatique ne le sache ni ne puisse le contrôler.

Meilleures pratiques en matière de sécurité cloud mobile

Pour limiter les failles de sécurité dans une infrastructure cloud mobile, il est nécessaire de recourir à un ensemble de meilleures pratiques reconnues offrant au service informatique des outils appropriés de contrôle et de visibilité, sans nuire aux performances ni à la productivité. Les organisations doivent rechercher une solution complète de sécurité cloud mobile qui intègre de manière transparente ces meilleures pratiques à sa plateforme.

Mettre en œuvre des règles contextuelles sur tous les services cloud et systèmes d'exploitation mobiles

Les utilisateurs professionnels ayant de plus en plus fréquemment recours à des appareils mobiles pour accéder aux applications et services cloud de l'entreprise, les services informatiques ne peuvent plus se contenter d'une solution de sécurité basée sur l'identité des utilisateurs pour bloquer les appareils non sécurisés, les applications non gérées et les services cloud non approuvés. La sécurité cloud mobile requiert une plateforme moderne à plusieurs systèmes d'exploitation qui aide le service informatique à définir et mettre en place des règles de contrôle des accès conditionnels en fonction du type et du statut des appareils, de l'état de l'application mobile, du type de service cloud et de l'identité de l'utilisateur.

Faciliter l'authentification des utilisateurs via la procédure d'authentification unique simplifiée

L'accroissement de la productivité des employés est l'une des principales raisons pour lesquelles les organisations transfèrent leurs processus métier vers le cloud. Demander aux utilisateurs de saisir un mot de passe à chaque fois qu'ils accèdent à un service cloud revient à leur bloquer l'accès aux ressources dont ils ont besoin pour effectuer leur travail. S'il arrive aux utilisateurs d'oublier leur mot de passe, ils font aussi souvent des erreurs lors de la saisie de leurs identifiants sur des écrans mobiles de petite taille et se retrouvent bloqués après plusieurs tentatives, ce qui rend nécessaire l'intervention du service d'assistance. Non seulement ces incidents freinent la productivité des employés, mais ils entraînent une augmentation des coûts liés à l'assistance et un recul de l'efficacité. Les organisations ont donc tout intérêt à simplifier les procédures d'accès sécurisé à l'aide de technologies telles que l'authentification unique.

Suivre et gérer la création de rapports de conformité

Outre le besoin de déployer des services cloud, des applications et des appareils sécurisés, les services informatiques doivent également disposer d'un système centralisé et évolutif permettant d'appliquer des règles de sécurité et de suivre, contrôler et documenter la conformité. Les solutions traditionnelles ne parviennent pas à garantir une visibilité suffisamment fiable sur le statut et l'état des appareils et applications utilisés par les employés pour se connecter aux services cloud de l'entreprise. De plus, le service informatique est généralement chargé de collecter des journaux relatifs à chaque service cloud et de les mettre en corrélation manuellement avec les journaux provenant d'autres sources afin d'identifier les appareils et applications non conformes. Cette approche trop fragmentée manque d'évolutivité. Des directives plus strictes en matière de conformité ayant été introduites via des règles telles que le règlement général sur la protection des données (RGPD), les organisations doivent mettre en œuvre une plateforme consolidée de création de rapports qui facilite les tâches de création de rapports, d'audit et de correction.

Pourquoi les approches traditionnelles ne suffisent plus

Aujourd'hui, diverses solutions sont proposées sur le marché pour aider les organisations à résoudre différents aspects du défi que représente la sécurité cloud mobile, mais elles ne sont pas compatibles avec l'ensemble des meilleures pratiques décrites ci-dessus.

- **Gestion des identités et des accès (IAM, Identity Access Management)**
  Les solutions IAM ont pour principal objectif de gérer les identités et de contrôler les accès. Elles proposent des fonctions de contrôle d'accès sur la base de l'identité pour les services cloud, mais elles ne permettent pas d'autoriser ou de refuser un accès en fonction du statut d'un appareil ou d'une application.

- **Gestion des appareils mobiles (MDM, Mobile Device Management)**
  La gestion des appareils mobiles est centrée sur la sécurisation de ces appareils. Il est important de noter que tous les fournisseurs de solutions MDM ne proposent pas d'offre satisfaisante en matière de sécurité cloud et qu'ils sont nombreux à ne pas résoudre les problèmes liés aux applications non gérées et aux services cloud non approuvés décrits ci-dessus.
- **Passerelles d'accès sécurisé au cloud (CASB, Cloud Access Security Brokers)**
  Ces passerelles apportent aux utilisateurs la visibilité dont ils ont besoin et des outils précis de contrôle des accès au niveau des fichiers pour les services cloud. Toutefois, leurs fonctionnalités sont très limitées lorsqu'il s'agit de définir le profil ou de déterminer le statut des appareils, et d'empêcher les appareils non conformes et les applications non approuvées d'accéder aux services cloud de l'entreprise.

Si ces solutions exécutent généralement bien les fonctions qui leur sont propres, elles sont trop cloisonnées pour pouvoir être intégrées facilement, ce qui entraîne des failles de sécurité et la vulnérabilité des données de l'entreprise.

Avec MobileIron Access, bénéficiez d'une solution unifiée de sécurité cloud mobile

Les organisations qui utilisent des services cloud professionnels tels que Box, G Suite, Office 365 et Salesforce doivent mettre en place un contrôle des accès conditionnels pour tous ces services. Avec MobileIron Access, les utilisateurs bénéficient d'un processus d'authentification unique (SSO) sécurisé et simplifié et d'une visibilité totale, qui permet de réserver l'accès aux données de l'entreprise stockées dans le cloud aux appareils sécurisés, applications gérées et services cloud approuvés.

Contrairement aux produits concurrents, MobileIron Access offre une plateforme unifiée compatible avec les normes en vigueur qui sécurise les services cloud tout en permettant aux utilisateurs de conserver le même niveau de productivité, où qu'ils soient et sur n'importe quel appareil. Ainsi, la sécurité des données professionnelles est assurée lors de leurs transferts depuis le cloud ou vers celui-ci.

Prévenir les risques de pertes de données

Il est essentiel de prévenir les risques de pertes de données dues à des actions intentionnelles ou accidentelles des employés. Par exemple, comment le service informatique peut-il empêcher un utilisateur de télécharger des fichiers depuis Salesforce et de les copier dans un dossier Dropbox personnel ? A-t-il la possibilité de bloquer l'accès à des données Salesforce via un navigateur Web Cydia Store installé sur un appareil iOS jailbreaké ?

MobileIron Access réduit ce risque de perte de données grâce à des règles d'accès conditionnel selon lesquelles les services et données cloud de l'entreprise ne sont accessibles qu'aux personnes de confiance utilisant des appareils conformes, des applications gérées et des services cloud approuvés. Cela signifie qu'un employé ne peut pas partager de fichiers ni de données depuis un service cloud géré, tel qu'Office 365, avec une application non gérée, telle qu'un Google Drive personnel.

Améliorer l'expérience de l'utilisateur final

Grâce à un processus d'authentification unique (SSO) sécurisé et simplifié qui permet à vos collaborateurs d'accéder instantanément aux données de l'entreprise sans avoir à saisir constamment un nom d'utilisateur et un mot de passe propres à chaque application mobile et service cloud, MobileIron Access améliore l'expérience des utilisateurs. Contrairement à l'authentification unique simple, MobileIron Access fonctionne parfaitement avec l'ensemble des applications mobiles et offre une couche supplémentaire de sécurité en empêchant les utilisateurs de se connecter à partir d'applications non sécurisées.

En rendant facultative la saisie des identifiants, le processus d'authentification unique MobileIron Access réduit le nombre de verrouillages de compte liés à des erreurs de saisie. Les organisations peuvent également augmenter leur productivité en mettant en place des processus de correction intuitifs permettant aux utilisateurs de corriger les problèmes eux-mêmes, sans avoir à recourir à l'assistance.

Simplifier la création de rapports de conformité

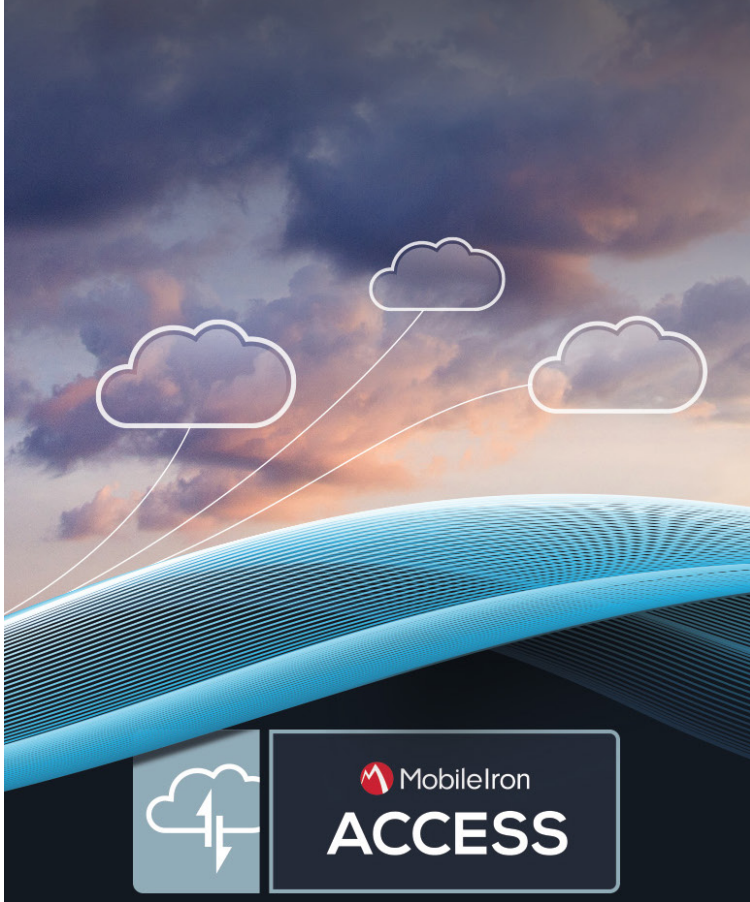
Grâce à la visibilité parfaite et aux fonctionnalités d'audit offertes par son moteur avancé de création de rapports permettant de suivre l'ensemble des appareils, applications, services, données de localisation et utilisateurs qui se connectent aux services cloud de votre entreprise, MobileIron Access améliore le niveau de conformité de votre organisation. Ce degré très poussé de visibilité facilite l'identification des utilisateurs et appareils non conformes par les organisations et offre à ces dernières les outils nécessaires pour les remettre en conformité. Point tout aussi important, les fonctionnalités de journalisation et de création de rapports de MobileIron Access permettent de simplifier les procédures d'audit et la surveillance de la conformité.

MobileIron Access : comment sécuriser l'évolution des entreprises vers les technologies du cloud

L'adoption des technologies mobiles et cloud est à l'origine de grands bouleversements au sein des organisations du monde entier. Ces nouvelles technologies permettent aux organisations de rationaliser leurs processus d'entreprise, de réduire leurs coûts et d'aider leurs collaborateurs à conserver le même niveau de productivité, où qu'ils soient. Toutefois, les solutions traditionnelles de sécurité basées sur les PC ne suffisent pas à garantir la sécurité des applications mobiles et des services cloud, auxquels elles ne sont pas adaptées.

Les entreprises d'aujourd'hui ont besoin d'une plateforme complète et unifiée telle que MobileIron Access, conçue dès le départ pour sécuriser les applications et appareils mobiles, ainsi que les services cloud. En effet, MobileIron accompagne les entreprises dans leur transformation en sécurisant leurs ressources les plus importantes, notamment les ordinateurs de bureau, les appareils mobiles, les applications et les services cloud, à partir d'un point unique de contrôle.

Pour en savoir plus sur MobileIron Access, consultez la page mobileiron.com/access.



MobileIron

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