



Principaux avantages

- Protection des applications de l'entreprise avec la conteneurisation
 - Hausse de la productivité des utilisateurs et de la satisfaction
 - Gestion des applications mobiles avec une console centrale basée sur Internet
 - Support du BYOD en toute sécurité
 - Réduction des risques de fuite de données sensibles
 - Application d'un contrôle d'accès intégré et conformité aux politiques et aux réglementations
 - Possibilité d'effacement sélectif du catalogue et des applications gérées
 - Utilisation de commandes d'administration granulaire et de rapports graphiques interactifs
 - Réduction de la charge du réseau et renforcement des performances des applications et de l'évolutivité
-

IBM MaaS360 Mobile Application Management

Déployez, gérez et sécurisez vos applications mobiles en toute simplicité

Offre un accès protégé aux applications

Les smartphones et les tablettes transforment les entreprises en développant la productivité et en améliorant l'efficacité ainsi que la satisfaction des utilisateurs. Toutefois, la prolifération des appareils mobiles doit être contrôlée pour sécuriser les données sensibles de l'entreprise, surtout aujourd'hui à l'époque du « BYOD » (Bring Your Own Device).

Le contrôle des e-mails et la gestion des appareils ne suffisent plus. Les applications mobiles dévoilent le véritable potentiel des appareils mobiles.

Toutefois, ces applications mobiles constituent des sources grandissantes de vulnérabilité pour les entreprises, et ce, pour diverses raisons : gestion inadéquate du stockage des données, logiciels malveillants, accès non autorisés, absence de chiffrement et fuite de données lors des synchronisations.

Il existe plus d'un million d'applications mobiles différentes que vos employés peuvent installer et utiliser sur leurs smartphones et leurs tablettes.¹

Les entreprises doivent pouvoir distribuer, gérer et assurer la sécurité des applications mobiles stratégiques, à la fois sur les appareils personnels et ceux de l'entreprise.

IBM® MaaS360® Mobile Application Management simplifie la gestion des applications mobiles en offrant un catalogue d'applications d'entreprise intuitif avec une sécurité robuste et la gestion du cycle de vie opérationnel des applications.

« En 2017, 25 % des entreprises posséderont une boutique d'applications permettant de gérer les applications approuvées par l'entreprise sur des PC et des appareils mobiles. »² - Gartner



Catalogue des applications d'entreprise

- Offre un catalogue d'applications d'entreprise intuitif et personnalisable pour les périphériques iOS, Android et Windows Phone.
- Garantit une expérience utilisateur exceptionnelle
- Permet instantanément aux utilisateurs de voir les applications disponibles, d'installer des applications et de recevoir des alertes de mise à jour des applications
- Distribue des applications publiques et d'entreprise sélectionnées
- Utilise une console protégée, basée sur Internet, pour la gestion et la distribution des applications



Figure 1 : Exemple d'un catalogue d'applications d'entreprise sur un appareil mobile

Gestion du cycle de vie des applications mobiles

- Utilisez des processus de gestion des applications mobiles issues des meilleures pratiques
- Distribuez les applications et surveillez leur installation en connexion sans fil pour l'ensemble des utilisateurs, groupes d'utilisateurs ou périphériques individuels
- Publiez des mises à jour des applications
- Référenciez en permanence les rapports d'inventaire des applications
- S'intègre aux boutiques d'applications publiques tels que l'Apple Store, Google Play et Windows Phone Store en toute transparence.

App	Name	Type	Category	Device Type	VPP Codes	Installations
Skype	Skype	Apple	Social Networking	Tablet, Smartphone	1	1
Cisco WebEx Meetings	Cisco WebEx Meetings	Android	Business	Smartphone	1	1
Salesforce Mobile	Salesforce Mobile	Android	Business	Smartphone	1	1
iBooks	iBooks	Apple	Book	Tablet, Smartphone	1	1
iTunes U	iTunes U	Apple	Education	Tablet, Smartphone	0	0
AnyConnect ICS+	AnyConnect ICS+	Android	Business	Smartphone	0	0
ACME ERP	ACME ERP	Apple	Internal Apps	Tablet, Smartphone	0	0
CDW Events	CDW Events	Apple	Social Networking	Tablet, Smartphone	0	0
LinkedIn	LinkedIn	Android	Social	Smartphone	0	0

Figure 2 : Exemple d'un catalogue d'applications sur le portail MaaS360

IBM® MaaS360® Mobile Application Security

- Utilisez un simple encapsuleur d'applications ou un kit de développement de logiciels (KDL) comme une extension de sécurité pour MaaS360 Mobile Application Management
- Authentifiez les utilisateurs avant qu'ils n'accèdent aux applications
- Appliquez des contrôles de conformité des appareils
- Limitez les actions de copier-coller, ainsi que les sauvegardes de données locales et sur le cloud
- Recevez des alertes quasiment en temps réel en cas d'infractions à la conformité
- Protégez l'accès aux données de l'entreprise sans utiliser de périphérique VPN grâce à la tunnellation au niveau des applications

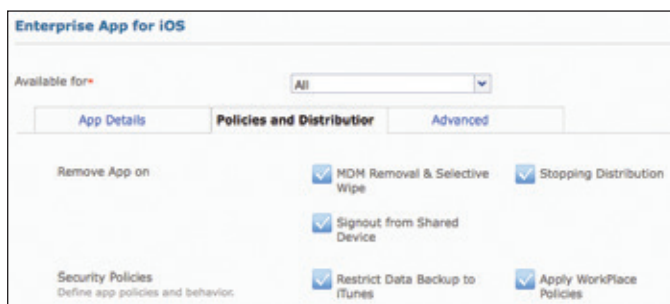


Figure 3 : Exemple d'options de sécurité pouvant être définies pour une application

Mise en conformité et exécution des applications mobiles

- Établissez une liste noire, une liste blanche et définissez les applications requises
- Limitez les applications natives sur un appareil (par ex. YouTube)
- Limitez l'accès des appareils débridés/jailbreakés
- Configurez des mesures automatisées de mise en conformité
- Réagissez immédiatement par des interventions manuelles ou automatiques pour bloquer l'accès à la messagerie, limiter les ressources réseau (par ex. à VPN) et exécuter une opération d'effacement à distance
- Affichez des rapports graphiques de sécurité et d'historique de conformité



Figure 4 : Exemple montrant comment placer une application en liste noire pour empêcher son installation sur un appareil

Conteneur d'applications mobiles d'entreprise

MaaS360 Mobile Application Management simplifie la gestion des applications mobiles en offrant un catalogue d'applications d'entreprise facile à utiliser avec une sécurité robuste et une gestion opérationnelle du cycle de vie des applications.

Catalogue des applications d'entreprise

Un catalogue des applications d'entreprise intuitif et personnalisable pour iOS, Android et Windows Phone.

Gestion du cycle de vie des applications mobiles

Une plateforme pour distribuer, mettre à jour, gérer et protéger les applications mobiles publiques et d'entreprise.

MaaS360 Mobile Application Security

Un conteneur d'applications mobiles pour les applications d'entreprise avec une gestion intégrée de la sécurité en extension facultative de MaaS360 Mobile Application Management.

Mise en conformité des applications mobiles

Règles de sécurité établissant une liste noire, une liste blanche et une liste des applications requises. Mise en oeuvre automatisée de règles pour alerter les administrateurs, bloquer les e-mails, limiter les ressources du réseau et effectuer des nettoyages à distance.

IBM® MaaS360® Content Service

Une option pour héberger et distribuer vos applications mobiles d'entreprise sur un réseau de distribution des applications optimisé à l'échelle mondiale.

Programme d'achat en volume

Prise en charge de licences d'applications en lots pour les employés.

Pour en savoir plus sur les solutions de prévention des fraudes d'IBM Security, contactez votre ingénieur ou partenaire commercial IBM. Vous pouvez également consulter le site Web suivant : ibm.com/security/fr-fr.



© Copyright IBM Corporation 2016

Compagnie IBM France
17, avenue de l'Europe
92275 BOIS COLOMBES CEDEX

Produit aux États-Unis
Août 2016

IBM, le logo IBM, ibm.com et X-Force sont des marques d'International Business Machines Corp. déposées dans de nombreuses juridictions à travers le monde. BYOD360™, Cloud Extender™, Control360®, E360®, Fiberlink®, MaaS360®, MaaS360® et appareil, MaaS360 PRO™, MCM360™, MDM360™, MI360®, Mobile Context Management™, Mobile NAC®, Mobile360®, Secure Productivity Suite™, Simple. Secure. Mobility.®, Trusted Workplace™, Visibility360® et We do IT in the Cloud.™, et appareil, sont des marques ou des marques déposées de Fiberlink Communications Corporation, une société IBM. D'autres noms de produits et services peuvent être des marques commerciales d'IBM ou d'autres sociétés. Une liste actualisée des marques IBM est disponible sur le Web à la section « Copyright and trademark information » sur ibm.com/legal/copytrade.html

Apple, iPhone, iPad, iPod touch et iOS sont des marques commerciales ou déposées d'Apple Inc. enregistrées aux États-Unis et dans d'autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

Les informations contenues dans ce document sont correctes à la date de leur publication initiale et peuvent être modifiées par IBM à tout moment. Toutes les offres ne sont pas disponibles dans tous les pays. Les données de performances et les exemples citant des clients ne sont présentés qu'à titre d'illustration. Les résultats de performances réels peuvent varier selon les configurations et les conditions de fonctionnement spécifiques. Il incombe à l'utilisateur d'évaluer et de vérifier le fonctionnement de tout autre produit ou programme avec les produits et programmes IBM.

LES INFORMATIONS CONTENUES DANS CE DOCUMENT SONT FOURNIES « EN L'ÉTAT », SANS AUCUNE GARANTIE, EXPRESSE OU TACITE, NOTAMMENT SANS AUCUNE GARANTIE OU CONDITION DE QUALITÉ MARCHANDE OU D'APTITUDE A UN EMPLOI SPÉCIFIQUE ET SANS AUCUNE GARANTIE DE NON-CONTREFAÇON. Les produits IBM sont garantis conformément aux conditions de leur contrat de vente.

Le client est tenu de s'assurer du respect des lois et réglementations en vigueur. IBM ne fournit aucun conseil juridique et ne garantit pas que ses produits ou services assurent la conformité du client aux lois et réglementations en vigueur.

Toutes les déclarations relatives aux orientations futures d'IBM sont sujettes à modification ou retrait sans préavis. Elles n'expriment que les intentions et les objectifs d'IBM.

Déclaration de bonnes pratiques en matière de sécurité : La sécurité des systèmes informatiques implique la protection des systèmes et des informations en prévenant, détectant et réagissant aux accès non autorisés, qu'ils proviennent de l'entreprise ou de l'extérieur. Les accès non autorisés peuvent entraîner l'altération, la destruction ou l'utilisation inappropriée des informations, et ainsi causer des dommages ou une utilisation abusive de vos systèmes, par exemple pour attaquer des tiers. Aucun système ou produit informatiques ne doit être considéré comme entièrement sécurisé. Aucun produit ni aucune mesure de sécurité ne peut être totalement efficace contre les accès non autorisés. Les systèmes et produits IBM s'inscrivent dans une approche de sécurité complète qui implique des procédures opérationnelles supplémentaires et peuvent demander aux autres systèmes, produits ou services d'être plus efficaces. IBM ne garantit pas que ses systèmes et ses produits sont invulnérables face aux comportements malveillants ou illégaux provenant de tiers.

1 Nombre d'applications disponibles dans les principaux magasins d'applications à partir de juillet 2014, Statista, <http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/>

2 "Gartner Says That by 2017, 25 Percent of Enterprises Will Have an Enterprise App Store," Gartner Group Press Release, 12 février 2013, <http://www.gartner.com/newsroom/id/2334015>



Recyclable