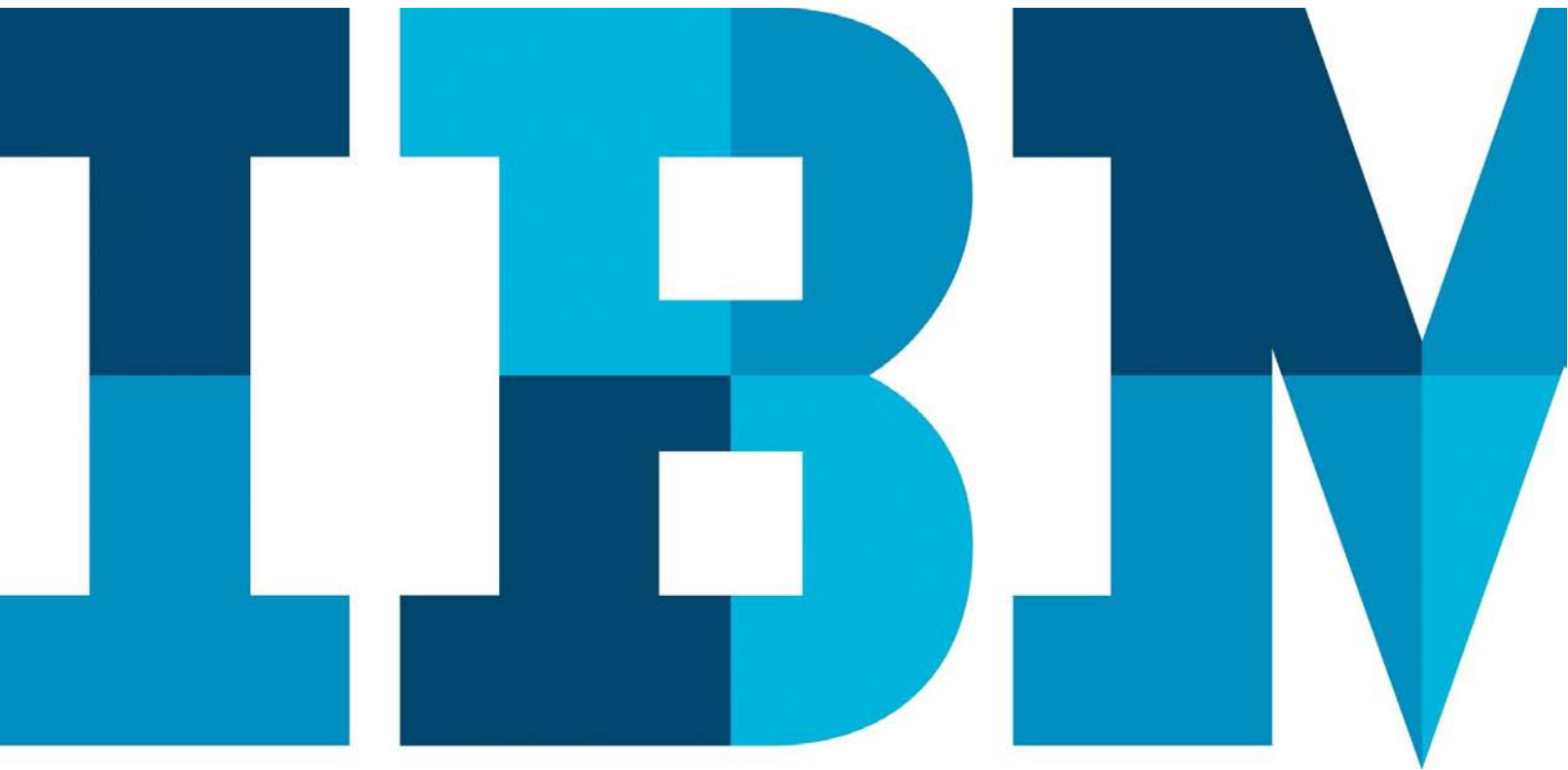


Sécurisation de la productivité mobile pour Microsoft Office 365

IBM MaaS360 vous permet de déployer les outils Microsoft en toute sécurité sur toutes les plateformes mobiles



Introduction

Des smartphones aux tablettes, en passant par les ordinateurs portables et autres appareils mobiles, les entreprises sont envahies par les technologies mobiles. Certains appareils appartiennent aux employés et peuvent même faire partie d'une initiative BYOD officielle, tandis que d'autres appartiennent à la société. Toutefois, aucune distinction n'est à faire en matière de sécurité. Les organisations informatiques doivent gérer et sécuriser tous les appareils accédant aux données, aux applications et au contenu d'entreprise.

Malgré les défis en matière de sécurité, il est judicieux d'encourager les employés à utiliser des appareils mobiles, car cela augmente leur productivité et leur satisfaction globale. Dans une enquête menée auprès d'équipes informatiques et commerciales, 67 % des participants à l'enquête ont déclaré être significativement plus productifs lorsqu'ils utilisent leurs propres appareils mobiles dans le cadre de leurs activités professionnelles.¹ L'objectif des organisations informatiques consiste à trouver la solution idéale pour améliorer la productivité des employés tout en déployant la technologie appropriée pour réduire les risques.

Depuis des années, les produits Microsoft sont largement utilisés dans le cadre de l'amélioration de la productivité des entreprises. Il devient donc très urgent de les déployer et de les sécuriser sur les appareils mobiles. IBM® MaaS360® permet aux organisations informatiques de gérer et de sécuriser les produits Microsoft dans des environnements mobiles hétérogènes. La vaste gamme de produits pris en charge comprend, entre autres, Microsoft Office 365, Microsoft Office pour les appareils mobiles, Microsoft Lync et Microsoft Skype for Business.

Ce livre blanc explique en quoi IBM MaaS360 constitue le choix idéal pour déployer et sécuriser l'environnement Microsoft sur toutes les plateformes mobiles, y compris Microsoft Windows 10. L'objectif principal consiste à permettre aux départements informatiques de gérer efficacement la productivité, la connectivité et la sécurité des entreprises dans le monde mobile d'aujourd'hui et de demain.

Travaillez en toute sécurité dans Office 365

Aujourd'hui, les organisations déploient une vaste gamme d'applications mobiles pour aider leurs employés à atteindre leurs objectifs, n'importe où, n'importe quand. Basé sur la plateforme Office, Office 365 est la solution préférée des utilisateurs parmi les logiciels de productivité. En effet, selon Microsoft, la suite de productivité dans le cloud est utilisée tous les mois par environ 50 millions d'utilisateurs professionnels.²

Office 365 offre des paramètres de sécurité de base du contrôle de l'accès mobile aux applications d'entreprise. Toutefois, en pratique, Office 365 n'est généralement pas déployé de façon isolée. Les équipes informatiques doivent pouvoir sécuriser et gérer les appareils, les applications et le contenu mobile dans un environnement composé de multiples plateformes. Elles ont besoin de flexibilité pour gérer tous les types d'appareil mobiles (appartenant aux employés et aux sociétés) à partir d'une console unique. Elles doivent également pouvoir mettre en place des normes de sécurité sans contrôler l'appareil.

Qu'est-ce qu'Office 365 ?

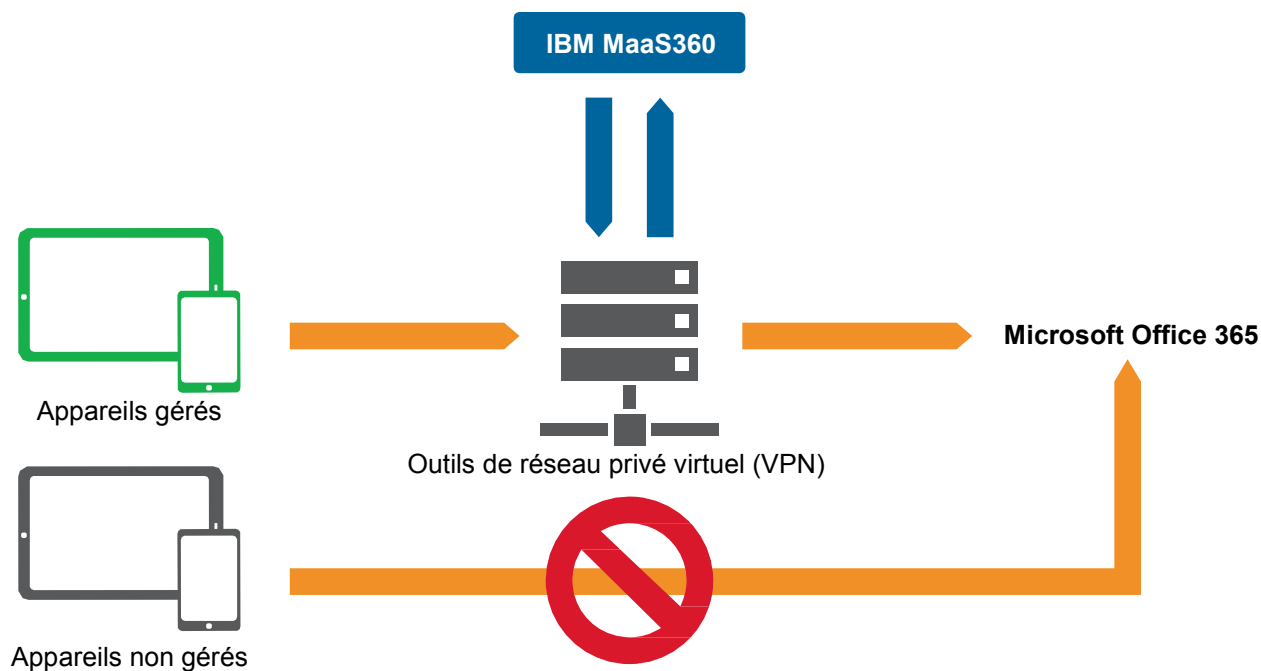
Office 365 est une solution de productivité de Microsoft qui offre un accès basé sur abonnement aux applications Office, ainsi que des services de cloud tels que la solution de cyberconférence Skype for Business, les services de collaboration Microsoft SharePoint, la solution de stockage Microsoft OneDrive et la solution de messagerie hébergée Microsoft Exchange Online.

De nombreuses offres Office 365 incluent les dernières applications Office, telles que : Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft OneNote et Microsoft Outlook. Toutes ces solutions peuvent être installées sur plusieurs appareils (PC, Mac, tablettes et téléphones Android et appareils iPad et iPhone Apple). La suite comprend également Microsoft Publisher et Microsoft Access, disponibles uniquement pour PC.

IBM MaaS360 permet aux organisations de maintenir la sécurité des appareils et du contenu grâce à une gestion avancée des appareils mobiles. Les équipes informatiques peuvent bloquer l'accès aux données d'entreprise des appareils déverrouillés ou rootés, localiser les appareils perdus ou volés, interdire les applications non sécurisées et profiter de fonctionnalités avancées de gestion des appareils mobiles accédant aux données d'entreprise sur Office 365. Grâce au support dans le cloud d'Office 365, IBM MaaS360 offre les fonctions de sécurité essentielles à la protection des données d'entreprise sensibles sur les appareils mobiles, notamment :

- Configuration à distance des profils Office 365
- Prise en charge de plusieurs systèmes d'exploitation et d'appareils dans le cadre de programmes BYOD
- Contrôle automatique des e-mails des appareils tentant d'accéder à Office 365
- Mise en quarantaine automatique des appareils nouveaux ou inconnus, jusqu'à approbation par le département informatique
- Accès sous condition à Office 365 uniquement pour les appareils gérés
- Possibilité de créer une liste noire des applications non sécurisées
- Limitation de l'utilisation de la commande « Ouvrir dans » sur les appareils Apple iOS, afin d'empêcher les applications non autorisées d'ouvrir des documents Office 365 et de faire « fuiter » des données
- Services de localisation pour suivre les appareils perdus ou volés
- Mise en place automatisée de règles et de normes de conformité
- Effacement sélectif pour supprimer exclusivement les données professionnelles, y compris les applications et les données d'Office 365, sans compromettre la confidentialité et les données personnelles de l'employé
- Accès sécurisé aux dossiers Microsoft OneDrive for Business

Accès sous condition à Microsoft Office 365 via IBM MaaS360



IBM MaaS360 s'assure que seuls les appareils autorisés accèdent à Office 365. Les appareils doivent être gérés, en toute conformité, par le département informatique.

IBM MaaS360 s'adresse particulièrement aux organisations nécessitant des contrôles stricts de la conformité et des règles de sécurité, similaires à ceux en pratique dans les secteurs de la santé et de la finance. Ses fonctions de *conteneurisation* permettent de séparer les données professionnelles (ici, les données Office 365) des autres données sur l'appareil mobile, tout en aidant à réduire les risques d'applications non autorisées sur l'appareil accédant aux données sensibles.

La messagerie mobile nécessite une approche différente

Les employés aiment consulter leurs e-mails sur leurs appareils mobiles, mais leur utilisation peut ouvrir la porte à des menaces de sécurité et des fuites de données professionnelles. Pour sécuriser l'accès mobile aux e-mails professionnels depuis Microsoft Exchange ou Office 365, IBM MaaS360 propose une application certifiée conçue pour maintenir la séparation entre les e-mails, les calendriers, les contacts et les données d'application professionnelles des applications et données personnelles. Fonctionnalités de l'application de conteneur sécurisée IBM :

- **Protection du texte et des pièces jointes des e-mails sur les appareils iOS, Android et Windows Phone**
 - **Chiffrement 256 bits conforme aux publications AES et FIPS 140-2 pour les données au repos**
 - **Application de l'authentification, de limitations en matière de couper/coller et mode d'affichage exclusif**
 - **Limitation des transferts, des déplacements et des captures d'écran**
 - **Contrôles de la conformité en ligne et hors ligne avant autorisation de l'accès aux e-mails**
-

Sécurisation du contenu mobile dans Office

De nombreuses organisations optent pour des couches de déploiement Microsoft, qui permettent de réduire les frais de licence et de simplifier les opérations. Par exemple, elles peuvent déployer Office 365 pour les utilisateurs expérimentés qui ont besoin d'une suite complète d'outils de productivité, tout en fournissant des applications Office mobiles aux autres utilisateurs afin qu'ils puissent utiliser occasionnellement des documents.

Dans un tel environnement, IBM MaaS360 permet aux organisations informatiques de gérer et sécuriser des apps Office pour les utilisateurs mobiles sur des appareils iOS, Android et Windows Phone. A partir d'une console unique, les administrateurs peuvent tout gérer de l'inscription des appareils aux règles de sécurité, en passant par le contrôle, la distribution des apps et des documents et le support client. Ils peuvent créer des règles solides visant à garantir la sécurité et la confidentialité des programmes BYOD, tout cela sans compromettre l'expérience utilisateur.

Pour être productifs à tout moment et quelle que soit leur localisation, les utilisateurs souhaitent pouvoir visualiser, créer, modifier et imprimer des documents Word, Excel et PowerPoint depuis leurs appareils mobiles. Souvent, ces documents sont envoyés sous forme de pièces jointes à leurs e-mails professionnels. Toutefois, l'utilisation de ces pièces jointes sur les appareils mobiles est traditionnellement fastidieuse et expose les appareils à des risques de sécurité.



IBM MaaS360 facilite le déploiement des applications pour tous les utilisateurs, un groupe d'utilisateurs ou un appareil spécifique, à partir d'un catalogue central d'applications.

IBM MaaS360 sécurise la productivité mobile et offre les avantages suivants aux organisations informatiques :

- Prévention des fuites de données grâce à la gestion des commandes « Ouvrir dans » sur les appareils iOS
- Extension de l'accès au stockage (au-delà de OneDrive ou Microsoft SharePoint Online) à d'autres référentiels de fichiers, tels qu'IBM Connections, Microsoft SharePoint On-Premises, Microsoft Windows File Shares, Box, Google Drive et les systèmes CMIS (Content Management Interoperability Services)
- Accès à des référentiels internes sans qu'il soit nécessaire de disposer d'un réseau privé virtuel (VPN)
- Prise en charge de l'envoi sécurisé par e-mail de documents via IBM MaaS360 Secure Mail
- Expérience de modification optimisée via IBM MaaS360 Document Editor, comprenant ce qui suit :
 - Prise en charge de toutes les plateformes et de tous les formats, notamment iOS, Android et Windows Phone
 - Prise en charge de plusieurs types de fichier au-delà des formats Office, tels que des documents PDF
 - Prévention complète des fuites de données grâce à des restrictions sur les opérations de copier/coller de contenu et de déplacement de fichiers
- Déploiement automatique de règles et de normes de conformité
- Effacement sélectif des données pour supprimer exclusivement le contenu professionnel, y compris les documents Office, sans compromettre la confidentialité et les données personnelles de l'employé

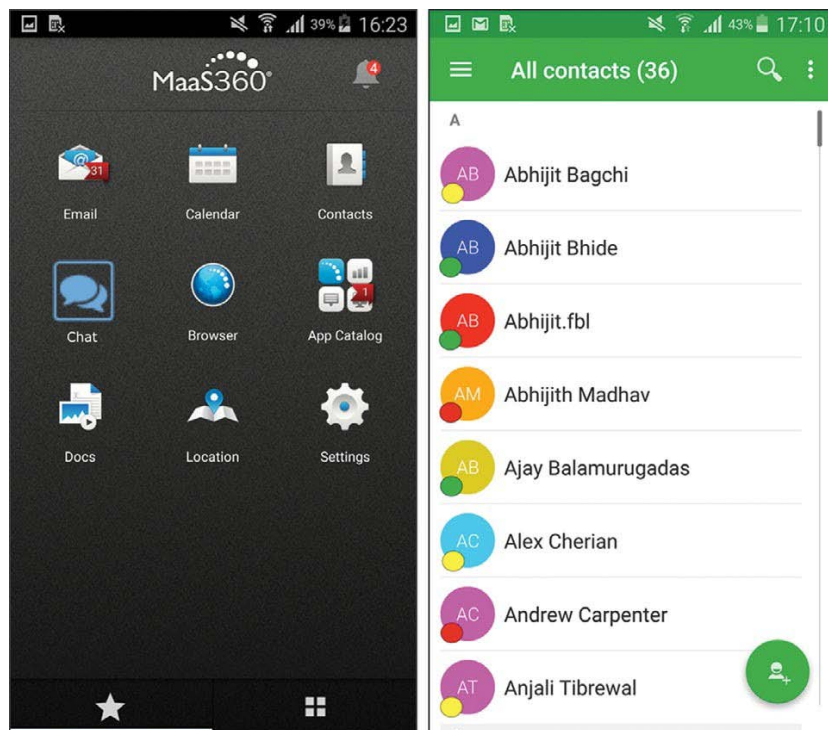
Réunir les équipes grâce à Skype for Business et Microsoft Lync

La collaboration en temps réel représente une part essentielle de la réussite des activités. C'est pourquoi de nombreuses organisations déploient Skype for Business (anciennement Microsoft Lync) pour fournir une expérience de communication unifiée. Depuis leurs applications Office, les employés peuvent collaborer à l'aide de la messagerie instantanée, d'écrans partagés, d'appels téléphoniques ou de discussions vidéo. Ils peuvent planifier des rendez-vous, consulter l'historique de la messagerie instantanée dans Outlook et lancer des réunions sur des applications telles que Word ou PowerPoint afin d'obtenir des résultats plus rapides.

Toutefois, tout comme avec Office 365 et Office pour les appareils mobiles, les équipes informatiques doivent être capables de gérer et sécuriser l'utilisation de Skype for Business. Elles doivent s'assurer que les appareils des employés sont conformes aux règles de sécurité de l'entreprise, gérer les notifications de discussion instantanée et prévenir toute fuite de données.

IBM MaaS360 propose un contrôle granulaire des fonctions de discussion instantanée de Skype for Business. Le personnel informatique et de sécurité peut donc :

- appliquer des règles pour l'authentification, les discussions en groupes, l'historique de conversation et le partage de fichiers ;
- prendre en charge les fonctions de discussion sécurisées, telles que la possibilité de voir les utilisateurs présents, de gérer les notifications et de démarrer une discussion dans IBM MaaS360 Secure Mail ;
- intégrer la solution à l'infrastructure existante via IBM MaaS360 Cloud Extender, qui comprend les éléments suivants :
 - Prise en charge de l'authentification avancée via Microsoft Active Directory, le protocole Lightweight Directory Access Protocol (LDAP), les autorités de certification et le langage Security Assertion Markup Language (SAML)
 - Prévention complète des fuites de données grâce à des restrictions sur les opérations de copier/coller de contenu et de déplacement de fichiers
- Déploiement automatique de règles et de normes de conformité
- Effacement sélectif des appareils pour supprimer uniquement le contenu professionnel, y compris les configurations de Skype for Business, sans compromettre la confidentialité des employés



IBM MaaS360 garantit une collaboration sécurisée et en temps réel et affiche la présence des utilisateurs.

Sécurité intégrée dans l'environnement Microsoft

Au fil des années, IBM MaaS360 a évolué pour prendre en charge l'environnement de produits professionnels Microsoft et permettre aux organisations de gérer et sécuriser le contenu et les applications des appareils mobiles. Autres intégrations Microsoft clés :

- **Exchange ActiveSync** : sécurisation de l'accès à la messagerie à partir d'appareils mobiles, comprenant la mise en quarantaine automatique des appareils inconnus, l'application de règles et la prise en charge de l'effacement à distance
 - **SharePoint On-Premises** : collaboration via des sites SharePoint publics et privés, tout en sécurisant le contenu via des règles d'autorisation, de chiffrement et de conteneurisation
 - **Windows File Shares** : protection de l'accès aux dossiers réseau à partir d'un conteneur sécurisé et chiffré
 - **OneDrive for Business** : conteneur sécurisé pour accéder, stocker, synchroniser et partager des fichiers de travail à partir d'un appareil géré
 - **Ordinateurs portables, ordinateurs de bureau et tablettes Windows** : prise en charge de la gestion du cycle de vie des PC Windows depuis la même interface que celles des autres appareils mobiles, y compris Windows XP, Windows Vista, Windows 7, Windows 8+ et Windows 10
 - **Windows Phone et Windows Mobile** : visibilité et contrôle des appareils mobiles Windows Phone 7, Windows Phone 8+ et Windows 10, y compris application de règles, gestion des applications et création de rapports de conformité
 - **Active Directory** : intégration des informations Active Directory à utiliser pour la gestion des appareils mobiles, la rationalisation de l'authentification des appareils et de la gestion des groupes
-

Conclusion

Des organisations de toutes tailles utilisent les programmes BYOD pour améliorer la productivité et la satisfaction des employés. Les équipes informatiques, quant à elles, doivent s'occuper de la sécurité, de la conformité et de la gouvernance des données. IBM MaaS360 simplifie la gestion de la main-d'œuvre mobile, de la prise en charge d'un grand nombre de smartphones et de tablettes avec différents systèmes d'exploitation à la distribution d'applications et de documents volumineux.

Plus encore, IBM MaaS360 propose une plateforme complète de gestion et de sécurisation de l'environnement de produits professionnels Microsoft. Grâce à la visibilité en temps réel, au contrôle continu et à l'application automatique de règles, IBM MaaS360 constitue le chemin le plus court vers la sécurité mobile pour Office 365, Office pour les appareils mobiles, Microsoft Lync et Skype for Business. IBM MaaS360 constitue le choix idéal pour gérer les exigences de la nouvelle génération de programmes BYOD en matière de mobilité.

Pour plus d'informations

Pour en savoir plus sur IBM MaaS360, contactez votre représentant ou votre partenaire commercial IBM, ou visitez le site suivant :

ibm.com/security/fr/fr/mobile/maas360.html

A propos des solutions IBM Security

IBM Security offre un portefeuille de produits et de services de sécurité professionnels des plus avant-gardistes et des plus intégrés. Ce portefeuille, étayé par la recherche et le développement IBM X-Force® de renommée mondiale, fournit des informations sur la sécurité afin d'aider les entreprises à protéger globalement leur personnel, leurs infrastructures, leurs données et leurs applications, tout en proposant des solutions de gestion de l'identité et de l'accès, de sécurité des bases de données, de développement des applications, de gestion des risques, de gestion des terminaux, de sécurité du réseau, etc. Grâce à ces solutions, les organisations sont à même de gérer efficacement les risques encourus ainsi que de mettre en place une sécurité intégrée pour les appareils mobiles, le Cloud, les réseaux sociaux et autres architectures métier.

IBM gère l'une des organisations mondiales les plus importantes en termes de prestation de services, développement et recherche sur la sécurité. La société surveille 15 milliards d'événements de sécurité par jour dans plus de 130 pays et détient plus de 3 000 brevets relatifs à la sécurité.

IBM Global Financing propose de nombreuses solutions de paiement qui vous aideront à acquérir la technologie dont vous avez besoin pour développer vos activités. Nous proposons une gestion sur la totalité du cycle de vie des produits et services informatiques, de l'acquisition à la mise au rebut. Pour plus d'informations, consultez le site : ibm.com/financing



© Copyright IBM Corporation 2016

IBM Security
17 avenue de l'Europe
92275 Bois Colombes Cedex

Imprimé en France
Mars 2016

IBM, le logo IBM, ibm.com et X-Force sont des marques d'International Business Machines Corp. déposées dans de nombreuses juridictions réparties dans le monde entier. Les autres noms de produits et services peuvent appartenir à IBM ou à des tiers. La liste actualisée des marques IBM est disponible sur Internet dans la rubrique consacrée au copyright et aux marques du site ibm.com/legal/copytrade.shtml

Cloud Extender et MaaS360 sont des marques ou des marques déposées de Fiberlink Communications Corporation, société du groupe IBM.

Microsoft et Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Le présent document est en vigueur à compter de la date de publication. Il peut être modifié à tout moment par IBM. Les offres ne sont pas toutes disponibles dans les pays où IBM est implanté.

TOUTES LES INFORMATIONS DU PRESENT DOCUMENT SONT FOURNIES « EN L'ETAT », SANS AUCUNE GARANTIE DE QUELQUE NATURE QUE CE SOIT, EXPRESSE OU IMPLICITE, Y COMPRIS TOUTE GARANTIE DE QUALITE MARCHANDE, D'ADEQUATION A UN USAGE PARTICULIER OU DE NON-CONTREFACON. Les produits IBM sont garantis conformément aux conditions des accords selon lesquels ils sont fournis.

Le client doit se conformer aux lois et réglementations en vigueur. IBM ne fournit pas de conseils juridiques ou ne garantit pas que ses services ou produits permettent au client de se conformer aux lois et réglementations en vigueur.

Déclaration de bonnes pratiques en matière de sécurité : La sécurité des systèmes informatiques consiste à protéger les systèmes et les informations par la prévention, la détection et la gestion de l'accès inapproprié au sein de l'entreprise et en dehors de celle-ci. L'accès inapproprié peut entraîner l'altération, la destruction, le détournement ou l'usage abusif d'informations, ou peut entraîner des dommages ou un usage non approprié de vos systèmes, notamment à des fins malveillantes. Aucun système ou produit informatique ne saurait être considéré comme entièrement sûr et aucun produit, service ou mesure de sécurité ne peut être complètement efficace en matière de prévention d'accès ou d'usage non approprié. Les systèmes, services et produits IBM doivent être intégrés à une approche complète en matière de sécurité. Celle-ci implique nécessairement des procédures opérationnelles supplémentaires et peut nécessiter d'autres systèmes, produits ou services pour en optimiser l'efficacité. IBM NE SAURAIT GARANTIR QUE LES SYSTEMES, PRODUITS OU SERVICES SONT ENTIEREMENT PROTEGES CONTRE LES COMPORTEMENTS MALVEILLANTS OU ILLEGAUX DE TIERS OU QU'ILS PROTEGERONT VOTRE ENTREPRISE CONTRE LESDITS COMPORTEMENTS.

¹ "Making BYOD work: Balancing productivity and security," *Harvard Business Review Analytic Services Report*, sponsored by Verizon Wireless, octobre 2014. https://hbr.org/resources/pdfs/comm/verizon/18918_HBR_Verizon_BYOD_OCT_2014.pdf

² Julie Bort, "Here's more proof that companies are jumping on Microsoft Office 365 like crazy," *Business Insider*, 24 avril 2015. <http://www.businessinsider.com/chart-shows-the-rise-of-office-365-2015-4>



Recyclable