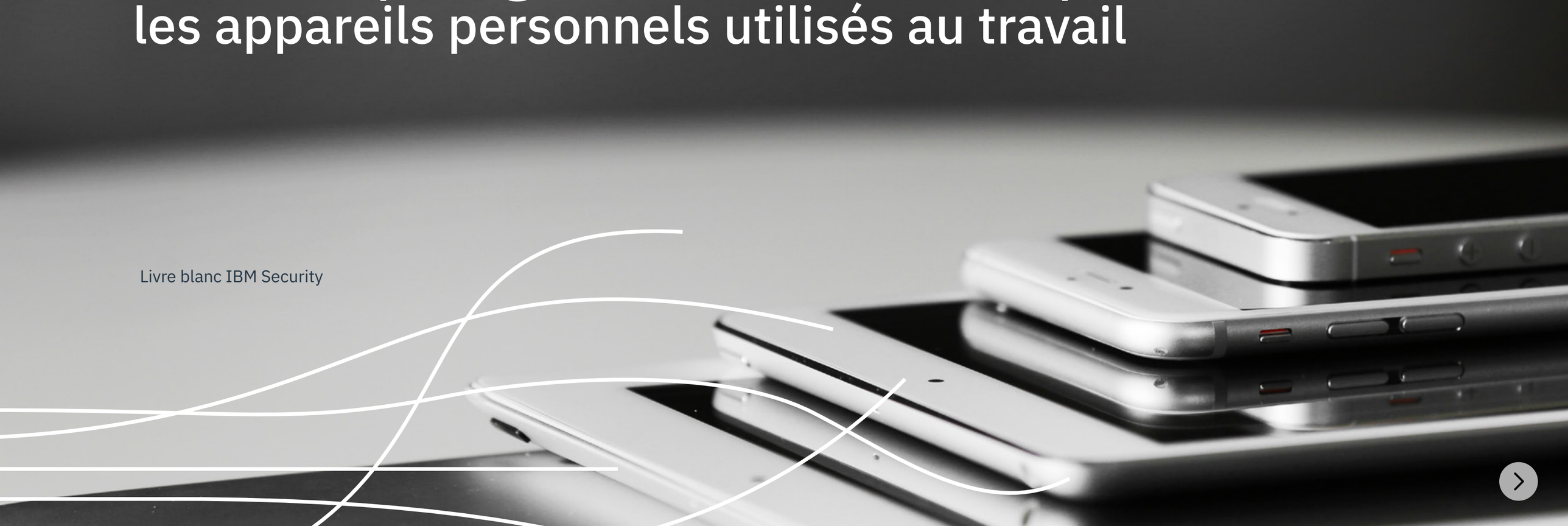
IBM Security

POUR UN AFFICHAGE OPTIMAL, VEUILLEZ UTILISER ACROBAT READER

Les 10 règles du BYOD

Comment protéger les données d'entreprise sur les appareils personnels utilisés au travail

Livre blanc IBM Security



Devez-vous autoriser un BYOD en milieu de travail ?

Pour de nombreux dirigeants informatiques, la prolifération rapide des appareils mobiles sur le lieu de travail a eu l'effet d'un coup de foudre. Les appareils mobiles et leurs applications ont transformé nos modes de vie, notre façon de communiquer, de voyager, d'acheter, de travailler et bien plus encore. Cette transformation mobile a été tellement révolutionnaire qu'il est désormais difficile d'envisager la vie sans ces appareils.

Avec le BYOD, les utilisateurs peuvent travailler n'importe quand, n'importe où et utiliser les appareils qu'ils ont payés eux-mêmes.

Ceci pose l'inévitable question : Comment épauler cette demande à l'avenir, tout en permettant aux utilisateurs de faire preuve de productivité en se servant des fonctionnalités de messagerie, d'applis et de contenu, cela dans un environnement sécurisé à même de protéger les données d'entreprise ? Suivez les « dix règles du BYOD » pour créer un environnement mobile serein, protégé et productif.

Les dix règles du BYOD

1. Définissez votre politique avant d'acquérir la technologie
2. Identifiez les appareils qui accèdent aux ressources de l'entreprise
3. Simplifiez leur enregistrement
4. Configurez vos appareils dans la foulée
5. Aidez vos utilisateurs à se servir
6. Protégez la confidentialité de vos utilisateurs
7. Séparez les données de l'entreprise des données personnelles
8. Gérez la consommation des données
9. Surveillez les appareils en continu pour vérifier leur conformité
10. Profitez du retour sur investissement engendré par le BOYD

Saviez-vous que...

La gestion de la mobilité d'entreprise (EMM) prend appui sur la gestion des appareils mobiles (MDM) pour offrir des capacités de gestion d'applications, de contenu et des dépenses. De surcroît, la gestion unifiée des terminaux (UEM) prend en charge les terminaux, les utilisateurs et tout ce qui se situe entre les deux, y compris la gestion des menaces et des identités.

1

Définissez votre politique avant d'acquérir la technologie

Comme pour tout autre projet informatique : d'abord la définition des politiques, puis l'achat des technologies... oui, même dans le cloud. Si vous voulez être sûr que votre technologie MDM ou EMM est utilisée efficacement sur les appareils des employés, vous devez en passer par la définition de politiques. Ces politiques ne concernent pas uniquement le service informatique : elle touchent les RH, le service juridique, la sécurité et tous les composants de l'entreprise qui utilisent les appareils mobiles, les applis et le contenu au nom de la productivité.

Etant donné que tous les services sont concernés par la politique BYOD, il est impossible de s'isoler dans un monde technologico-informatique pour la définir. Vu les attentes différentes des usagers, le service informatique doit veiller à prendre en compte chaque individu au moment de créer la politique. Puisqu'il n'existe pas de politique BYOD idéale, voici quelques questions à se poser au moment de développer la vôtre :

- **Appareils :** Quels seront les types d'appareils supportés ? Smartphones, tablettes, ordinateurs portables, objets connectés portables ? Seulement certains ou tous ceux suggérés par les employés ?
- **Conformité :** Quels sont les règlements auxquels votre organisation doit être en conformité ? Il convient d'envisager la loi HIPAA (The Health Insurance Portability and Accountability Act), la loi HITECH (the Health Information Technology for Economic and Clinical Health Act), l'autorité de surveillance des marchés financiers (la FINRA - Financial Industry Regulatory Authority) et le RGPD (Règlement général sur la protection des données de l'Union européenne) parmi d'autres. Veillez à faire des recherches sur celles qui correspondent à votre secteur ou région et faites en sorte de comprendre ce qui les relie à votre stratégie mobile.
- **Sécurité :** Quelles sont les mesures de sécurité nécessaires ? La protection de mot secret ? L'Encodage ? Le confinement ? La détection du débridage/rootage ? La protection contre les logiciels malveillants ? Un accès conditionnel ? Ce ne sont que quelques uns des nombreux éléments à prendre en compte
- **Applications :** Allez-vous créer une liste verte pour les applications approuvées ou une liste rouge pour celles qui sont interdites ? Comment allez-vous rendre les applications accessibles sur les types divers d'appareils au sein de votre environnement (par ex., smartphones, tablettes et ordinateurs portables) tout en préservant une expérience utilisateur cohérente ?
- **Accords :** Existe-t-il un accord d'usage acceptable (AUA) pour les appareils des employés accédant aux données de l'entreprise ?
- **Accès au réseau de l'entreprise :** À quelles ressources de l'entreprise vos employés peuvent-ils accéder via un appareil mobile ? La messagerie électronique, le calendrier et les contacts ? Les partages de fichiers et référentiels de documents ? Les sites intranet ? Les réseaux Wi-Fi ? Les réseaux privés virtuels (VPN) ?
- **Confidentialité de l'utilisateur :** Vous devrez protéger la confidentialité de vos utilisateurs. Quelles sont les données personnelles collectées à partir des appareils des employés ? Quelles sont les données personnelles jamais collectées ? De quelle manière allez-vous communiquer cette information à l'entreprise ?
- **Plans de données mobiles :** L'entreprise paiera-t-elle pour les plans de données mobiles ? Allouerez-vous un forfait ou l'employé doit-il soumettre des notes de frais ?

Aucune question n'est absurde lorsqu'il s'agit de BYOD. Le dialogue doit être franc et honnête sur l'utilisation des appareils et sur les capacités du service informatique à répondre aux attentes tout en protégeant les données d'entreprise.

2

Identifiez les appareils qui accèdent aux ressources de l'entreprise

Il est probable que le nombre d'appareils accédant à votre réseau est plus important que vous ne voulez l'admettre. Ne vivez pas dans le déni. Dans l'idée que « ce que vous ne savez pas ne vous touche pas ». Etudiez votre environnement mobile actuel avant d'élaborer une stratégie immuable.

Pour ce faire, vous devrez vous appuyer sur un outil capable de communiquer en permanence avec votre environnement de messagerie et de détecter tous les appareils connectés à votre réseau d'entreprise. N'oubliez pas que si Microsoft ActiveSync est activé sur une boîte de messagerie, il n'y a généralement aucun problème pour synchroniser plusieurs appareils sans que le service informatique le sache. Votre projet de mobilité doit englober tous les appareils mobiles. De même, les propriétaires de ces appareils doivent être avertis de l'entrée en vigueur de nouvelles politiques de sécurité.

Vous savez peu de choses sur la technologie UEM ?
Elle vous permet de gérer tous types d'appareils sur une plateforme unique : ordinateurs portables, ordinateurs de bureau, smartphones, tablettes, objets connectés portables et Internet des objets (IoT).

3

Simplifiez leur enregistrement

Après avoir identifié les appareils que vous devez enregistrer, votre programme BYOD doit employer une technologie à la méthodologie simple et à interaction réduite pour l'inscription des usagers, afin de réduire les processus fastidieux et manuels (tout en vous permettant d'être évolutif).

Vous voulez soit enregistrer les appareils en masse, soit demander aux utilisateurs qu'ils les enregistrent eux-mêmes. Vous devez également être en mesure d'authentifier les employés à l'aide d'un processus d'authentification de base, tel qu'un mot de passe à usage unique, ou d'utiliser les répertoires d'entreprise existants tels que Microsoft Active Directory/Lightweight Directory Access Protocol (AD/LDAP).

Tous les appareils neufs tentant d'accéder à des ressources de l'entreprise doivent être placés en quarantaine. Ainsi, le service informatique pourra choisir de bloquer l'appareil ou, s'il l'autorise, de lancer un workflow d'enregistrement en bonne et due forme afin de garantir la conformité aux politiques de l'entreprise. Comparez votre programme BYOD à un contrat prénuptial qui encadrerait une union harmonieuse entre utilisateurs et politiques informatiques. Des instructions simples mais détaillées devraient aider les utilisateurs à s'enregistrer dans le programme BYOD.

Celles-ci doivent être envoyées par courrier électronique ou SMS et être accompagnées d'un lien qui dirige vers une création de profil MDM sur leur propre appareil. N'oubliez pas de joindre le très important accord AUA.

4

Configurez vos appareils dans la foulée

S'il est bien un effet que la politique BYOD ne doit pas produire, c'est orienter davantage d'utilisateurs vers le service d'assistance. Vos appareils doivent être configurés dans la foulée (over the air - OTA) pour gagner du temps et obtenir une efficacité optimale, à la fois pour le personnel informatique et les utilisateurs.

Une fois que les utilisateurs ont terminé leur enregistrement, votre plateforme MDM ou EMM devrait prendre en charge une livraison dans la foulée de tous les profils, identifiants et paramètres dont l'employé a besoin, notamment :

- La messagerie électronique, les contacts et le calendrier
- Les profils VPN et Wi-Fi
- Le contenu de l'entreprise
- Les applis internes et publiques
- Les politiques de sécurité (par ex., conteneur).

Voyez ce qu'ils voient

Trouver un outil doté de capacités intégrées de support à distance peut faire gagner du temps et minimiser les efforts sur le long terme. C'est particulièrement utile lorsque vous avez besoin de mener des opérations de dépannage pour les utilisateurs sur le terrain.

5

Aidez vos utilisateurs à se servir

Les utilisateurs veulent un appareil qui fonctionne et vous voulez éviter de faire perdre du temps au service d'assistance. Une plateforme libre-service bien conçue permet aux utilisateurs de réaliser directement les actions suivantes :

- lancer des réinitialisations en cas d'oubli de codes Pin et mots de passe actuels ;
- géolocaliser un appareil perdu à partir d'un portail internet, en utilisant un outil cartographique ;
- effacer à distance le contenu d'un appareil pour supprimer les données d'entreprise sensibles ;
- comprendre ce qui peut les amener à ne plus être en conformité.

La sécurité, la protection des données de l'entreprise et la conformité sont des responsabilités partagées. Cela peut être difficile à accepter pour les employés, mais il est impossible d'atténuer les risques sans leur coopération.

Avez-vous une méthode *imprenable* pour distribuer vos applis ?

Vous devrez réfléchir à la meilleure façon de télécharger les applications sur les appareils. Un catalogue d'applis universel vous permet de le faire sur tous les formats. En adoptant cette approche, les utilisateurs peuvent voir quelles applications ont été approuvées à l'usage quel que soit l'appareil sur lequel ils travaillent. Vous pouvez faire un suivi des utilisateurs qui les ont installées, voir quels appareils disposent de la version la plus récente de l'application et qui doit installer une version actualisée. Les catalogues d'applications les mieux conçus ressembleront exactement aux boutiques d'applications publiques. De plus, les utilisateurs pourront recommander et noter celles qu'ils utilisent.

6

Protégez la confidentialité de vos utilisateurs

Un programme BYOD bien conçu soustraira les données personnelles des employés de votre écran. Les informations d'identification personnelle peuvent également servir à identifier, à contacter ou à localiser une personne. Certaines lois sur la vie privée interdisent aux entreprises de collecter ces données. Transférez la politique de confidentialité aux employés et précisez clairement ce qui peut ou ne peut pas être collecté sur leurs appareils. Par exemple, une solution MDM ou EMM devrait pouvoir restreindre la collecte de :

- courriers électroniques, contacts et calendrier personnels ;
- emplacement ;
- photos ;
- données d'application et SMS ;
- journal des appels et messagerie vocale.

En revanche, expliquez aux utilisateurs tous les éléments que vous collectez, l'utilisation que vous en ferez et l'intérêt que cela représente pour eux.

Une solution avancée garde l'emplacement et les informations sur le logiciel à l'abri des regards. Cela permet aux entreprises de mieux se conformer aux réglementations sur les informations d'identification personnelle. De même, les employés en tirent un certain confort puisque les données personnelles contenues dans leurs smartphones et tablettes ne peuvent pas être visualisées. Ils peuvent, par exemple :

- désactiver les rapports d'inventaire d'applications pour ne pas laisser les administrateurs ; voir les applications personnelles
- désactiver les services de localisation pour empêcher l'accès aux indicateurs d'emplacement tels que l'adresse physique, les coordonnées géographiques, l'adresse IP et l'identificateur SSID (Service Set Identifier) Wi-Fi.

7

Séparez les données de l'entreprise des données personnelles

En bref, les applis, les documents et les autres ressources de l'entreprise doivent être protégés par le service informatique si l'employé décide de quitter la société. Par contre, la messagerie, les applis et les photos personnelles doivent demeurer hors de portée.

On obtient cet équilibre grâce à la technologie de confinement disponible dans les solutions EMM de pointe. Non seulement la liberté conférée par cette approche sera appréciée par les utilisateurs, mais elle facilitera considérablement la vie du service informatique. Ce dernier pourra exécuter une réinitialisation sélective après le départ de l'employé, notamment du courrier électronique, du calendrier, des contacts, des applis et de toutes les données de l'entreprise. De même, selon les circonstances, il sera possible d'effacer tous le contenu de l'appareil s'il venait à être perdu.

De quoi un conteneur doit-il être composé pour le rendre exceptionnel ?

Un conteneur sur appareil et protégé par mot secret abrite toutes les données de l'entreprise. Les applis contenues dedans comprennent le courrier électronique, les contacts, les documents, le chat d'entreprise et même un navigateur sécurisé. Vous pouvez offrir aux utilisateurs leurs ressources de travail pertinentes en un seul endroit. C'est particulièrement utile pour les sous-traitants. Toutes les ressources nécessaires sont à leur disposition. Puis, une fois leur projet fini et après leur départ, vous pouvez tout effacer.

Vous n'avez pas besoin de gérer l'appareil, ou seulement le contenu ? Les conteneurs les mieux adaptés peuvent être déployés de façon autonome, éliminant ainsi le besoin d'enregistrer l'appareil MDM.

8

Gérer l'utilisation des données

Si vous payez un plan de données, un suivi des données peut vous être utile. Dans le cas contraire, vous pouvez néanmoins aider les utilisateurs à suivre leur consommation de données. Vous devez être en mesure de suivre la consommation de données des appareils, aussi bien sur le réseau qu'en itinérance, et de générer des alertes si un utilisateur dépasse un certain seuil.

Vous pouvez définir des limites en mégaoctets pour le réseau et l'itinérance, et personnaliser les rapports de facturation afin de créer des notifications basées sur le pourcentage utilisé. Il est recommandé d'expliquer aux utilisateurs les avantages d'utiliser une liaison Wi-Fi lorsqu'ils en ont la possibilité. Une configuration Wi-Fi automatique permet de s'assurer que les appareils se connectent au Wi-Fi dès qu'ils entrent dans le périmètre de l'entreprise.

Si le forfait attribué couvre uniquement 50 USD ou 200 Mo de données par mois, les employés apprécieront de recevoir un avertissement indiquant qu'ils sont responsables de tout dépassement.

9

Surveillez les appareils en continu pour vérifier leur conformité

Une fois l'appareil enregistré, tout dépend du contexte. Dans certains cas, les appareils doivent être surveillés en continu et des politiques automatisées doivent être mises en place. Voici quelques problèmes courants qui doivent être traités dans vos politiques :

'**Pas de MDM pour moi !**' Certains utilisateurs pourraient essayer de supprimer la gestion d'entreprise de leur appareil. Votre politique devrait le détecter et restreindre immédiatement l'accès aux ressources d'entreprise.
'**Je m'introduis dans la place !**' Pour contourner les restrictions liées au système d'exploitation (SE), les employés débrident (jailbreakent) (Apple iOS) ou rootent (Google Android) parfois un appareil, ce qui laisse la porte ouverte aux logiciels malveillants susceptibles de voler les informations. Si un appareil est débridé ou rooté, la solution MDM ou EMM doit prendre les mesures nécessaires, telles que l'effacement sélectif et immédiat sur l'appareil du conteneur, des applis de l'entreprise et de toutes données sensibles.
'**Je n'arrive pas à suivre toutes les nouveautés technologiques.**' Votre politique BYOD devrait avoir une stipulation au sujet des mises à jour des versions de SE. De même, il vous faudra tenir les utilisateurs informés des dernières et meilleures versions de SE publiées par tous les fournisseurs majeurs, notamment Apple, Google et Microsoft. En limitant l'utilisation de versions SE obsolètes, il devient plus facile de garantir la conformité et d'optimiser le fonctionnement de l'appareil.

Partez en guerre contre les logiciels malveillants

Les applis peuvent être fauteurs de trouble. Vous devez reconnaître la présence de logiciels malveillants sur vos appareils et réagir immédiatement pour éviter leur propagation. Faites preuve de discernement au moment de choisir votre EMM ou UEM. La solution doit vous donner le moyen de détecter les applis comportant des signatures de logiciels malveillants et un comportement nuisible, afin de pouvoir prendre des mesures pour les stopper dans les plus brefs délais.

10

Profitez du retour sur investissement engendré par le BOYD

Il n'existe pas de solution universelle, mais une politique BYOD minutieusement élaborée peut vous apporter tous les atouts nécessaires pour gérer efficacement les appareils mobiles.

Bien sûr, des améliorations de la productivité sont souvent constatées lorsque les employés sont mobiles et connectés en permanence. Le BYOD est une excellente solution pour étendre ces améliorations de productivité à de nouveaux utilisateurs qui n'ont pas le droit d'utiliser des appareils de l'entreprise. Lorsque vous définissez votre politique, tenez compte de son impact sur le retour sur investissement. Ceci inclut la comparaison des approches, comme indiqué ci-dessous :

Modèle avec dispositifs appartenant à l'entreprise

- Combien vous coûterait chaque dispositif ?
- Coût d'un plan de données entièrement subventionné
- Coût du recyclage des appareils après quelques années
- Plans de garanties
- Temps et main d'œuvre consacrés par le service informatique dans la gestion du programme.

BYOD

- Coût d'un plan de données partiellement subventionné
- Suppression du coût de l'achat des appareils
- Coût de la plateforme de gestion de la mobilité.

Mais ce n'est pas tout !

Lorsqu'une solution UEM est combinée à la gestion d'identité et d'accès (IAM), le partenariat donne des résultats magnifiques. Il offre aux utilisateurs un accès protégé, à authentification unique (SSO) au cloud et aux applis web nécessaires pour le travail. L'utilisateur est moins irrité, car il n'a pas besoin d'avoir à se souvenir de plusieurs mots de passe pour chaque appli. Il obtient l'accès dont il a besoin sans compromettre la sécurité des données.

Un résultat net

Le BYOD est devenu une pratique déterminante pour toutes les entreprises, ce qui n'est pas surprenant. Il donne aux employés la liberté de travailler sur leurs propres appareils, tout en allégeant les charges financières et de gestion pour le service informatique et les responsables de la sécurité. Cependant, s'il n'est pas encadré par une politique bien formulée et une plateforme d'administration solide, le BYOD ne peut pas tenir sa promesse de rationaliser la gestion et de réduire les coûts. Si vous commencez tout juste à élaborer votre stratégie mobile, IBM® MaaS360® with Watson™ propose un vaste éventail de ressources éducatives. Si vous décidez que le BYOD convient à votre entreprise, cliquez ici pour tester gratuitement MaaS360 pendant 30 jours. MaaS3360 étant basé sur le cloud, votre environnement de test peut devenir automatiquement un environnement de production sans entraîner de perte de données.

Pour progresser, passez au niveau supérieur

La gestion des terminaux, outre celle de leurs utilisateurs et données, est une activité chronophage si l'on emploie des solutions MDM et EMM conventionnelles. La gestion UEM cognitive met à votre disposition des connaissances, une analyse contextuelle et des capacités de benchmarking Cloud pour appréhender les problèmes que vous rencontrez au quotidien avec les appareils mobiles, tout en protégeant vos terminaux, les utilisateurs, les applis, les documents et les données associées à partir d'une plateforme unique.

IBM MaaS360 | With Watson

A propos de MaaS360 with Watson

Des milliers d'entreprises de toutes tailles, de tous les secteurs, font confiance à MaaS360 comme pilier de leur transformation digitale avec des appareils mobiles. Avec Watson, MaaS360 offre une UEM cognitive dotée de puissants contrôles de sécurité pour tous les utilisateurs, les appareils, les applis et les contenus afin de supporter tous les déploiements de terminaux et mobiles. Fourni depuis un cloud IBM de premier ordre sur une plateforme mature et fiable, MaaS360 permet de gérer une grande variété d'appareils pour de multiples utilisateurs à partir d'une console unique et d'intégrer les solutions d'Apple, de Google, de Microsoft et d'autres fournisseurs d'outils de gestion. IBM travaille de concert avec ces fournisseurs non seulement pour l'intégration, mais aussi pour veiller à ce qu'elle soit appliquée dès que de nouveaux outils ou de nouvelles mises à jour des outils existants sont disponibles.

Complément d'information

Pour plus d’informations sur MaaS360 et pour commencer un essai gratuit de 30 jours, visitez : **ibm.com/fr-fr**/maas360-trial

A propos des solutions de sécurité d'IBM

IBM Security propose l’un des portefeuilles les plus développés et intégrés en matière de produits et de services de sécurité pour les entreprises. Supporté par la recherche et le développement IBM X-Force® de réputation internationale, ce portefeuille offre un service de renseignement dédié à la sécurité pour aider les entreprises à protéger de manière globale leurs employés, leurs infrastructures, leurs données et leurs applications. Il offre des solutions pour la gestion des identités et de l’accès, la sécurité des bases de données, le développement d’applications, la gestion des risques, la gestion des terminaux, la sécurité des réseaux, etc. Ces solutions permettent aux entreprises de gérer efficacement les risques et de mettre en œuvre une sécurité intégrée aux architectures mobiles, cloud, de réseaux sociaux et d'autres types. IBM dispose de l’un des services de recherche, de développement et de mise en œuvre les plus importants au monde, surveille 30 milliards d’événements de sécurité par jour dans plus de 130 pays et détient plus de 3 000 brevets relatifs à la sécurité.

De plus, IBM Global Financing offre de nombreuses options de financement vous permettant d'acquérir la technologie dont vous avez besoin pour la croissance de votre entreprise. Nous nous chargeons de la gestion complète du cycle de vie des produits et services informatiques, depuis leur acquisition jusqu’à leur mise au rebut. Pour en savoir plus, allez sur **ibm.com/fr-fr**/financing

Compagnie IBM France
17, avenue de l’Europe,
92275 Bois-Colombes Cedex
France

IBM Irlande
Oldbrook House
24-32 Pembroke Road
Dublin 4

IBM Ireland est enregistrée en Irlande sous le numéro de société 16226

WGW03341-FRFR-01