IBM Security
Livre blanc

Gestion de la mobilité de l'entreprise

La théorie du Big Bang : pourquoi la gestion des dispositifs mobiles a explosé pour inclure les dispositifs, les applis et les contenus.

IBM

Introduction

Les frontières entre le travail au bureau, en déplacement et chez soi, s'estompent avec la puissance des smartphones, des tablettes et autres dispositifs mobiles. Les employés demandent de la flexibilité pour travailler sur les dispositifs qu'ils choisissent et une disponibilité permanente. Ces besoins posent généralement des problèmes aux responsables de la sécurité des réseaux et des données. Dans certaines entreprises, la réponse est simplement un refus. Mais actuellement, ces réponses sont rares. La norme actuelle est "Il faut voir". On ne peut pas non plus occulter le microcosme des divers services dans une entreprise, ce qui crée un nouveau débat sur l'étendue des accès nécessaires par rapport à la protection des données sensibles.

Pour optimiser la mobilité, la règle est d'adopter une stratégie nuancée. Pour concrétiser le potentiel transformatif de la mobilité, le service informatique doit devenir un partenaire commercial qui comprend les moteurs économiques et qui établit la feuille de route technologique pour répondre aux objectifs de chacun.

L'univers de la mobilité est complexe et en perpétuelle expansion, comme le nôtre. Le potentiel réalisable grâce à une compréhension rationnelle, analytique et extensive est une autre caractéristique commune de la mobilité et de notre univers en perpétuelle expansion.

L'explosion de la mobilité : Le Big Bang qui continue son expansion

Au début, tout était ténèbres, surtout pour ceux qui devaient travailler chez eux ou pendant des déplacements. Les employés laissaient leurs données et leurs logiciels de productivité sur leurs ordinateurs de bureau. Les ordinateurs portables ont alors permis de travailler en dehors du bureau, mais les connexions étaient coûteuses et incohérentes. En outre, dès que l'ordinateur était éteint, vous étiez bloqué dans un trou noir de non information.

Avec l'arrivée du BlackBerry, les dirigeants d'entreprise ont pu garder un contact constant avec leur bureau. Un rayon de lumière apparaissait, mais il ressemblait plus aux étoiles lointaines qu'à un phare.

Ensuite, dans une éruption d'innovation, le premier smartphone est apparu.

La lumière se diffusa, comme les dispositifs, pratiquement partout et à tous. Les dirigeants utilisaient des BlackBerries, mais soudain, de nouveaux appareils tactiles avec les systèmes d'exploitation iOS et Android gagnèrent les poches et l'espace de travail des utilisateurs.

Puis, nouvelle révolution, la tablette apparut avec des écrans plus grands permettant d'être plus productif et plus actif. Leur format plus grand et leur intelligence accrue a enfin permis d'extraire et de manipuler des données pendant tous les déplacements. Les employés étaient enchantés, mais le service informatique restait quelque peu dans l'ombre, incrédule. Quels appareils devaient accéder aux informations de l'entreprise ? Quels appareils exclure de ces accès ? Quelles ressources protéger ?

Gérer le Big Bang de la mobilité

Comment gérer le Big Bang de la mobilité ?

Gestion des dispositifs

Arrive alors MDM (Mobile Device Management), le cœur de la solution dédiée a Big Bang des services informatiques qui apporte la visibilité et des contrôles indispensables. Dans cette expansion universelle, le MDM a permis au service informatique d'appliquer un code d'accès, de connecter des ressources de l'entreprise, telles que la messagerie et les réseaux Wi-Fi, et de surveiller les dispositifs connectés.

Grâce aux interfaces API intégrées dans le système d'exploitation, le service informatique peut configurer des paramètres, activer ou désactiver des fonctions, localiser et verrouiller des appareils à distance et même effacer partiellement ou en totalité des données, selon les besoins.

D'après les estimations, les appareils gérés par des fournisseurs de services externes ont bénéficié d'une croissance de 50 % en 2015.[1]

Le service informatique déclara que c'était bon, et les utilisateurs acquiescèrent. Mais à mesure que les utilisateurs et les applis devinrent plus sophistiqués et que les documents, tels que les feuilles de calcul et les document Word purent être manipulés sur les appareils mobiles, il devint évident que les entreprises ne pouvaient plus se contenter de MDM.

Alors, une nouvelle expansion se produisit : l'avènement de solutions de gestion des applis et des contenus, mais aussi la séparation des données professionnelles et personnelles sous la forme de conteneurs.

Gestion des applis

La MAM (Mobile Application Management ou Gestion des applications mobiles) gère les différents aspects du cycle de vie, tels que la distribution, les mises à jour, les catalogues d'applis d'entreprise, la mise en liste noire/blanche et la sécurité. La MAM était nécessaire pour gérer l'explosion de l'univers des applis publiques et personnalisées.

Mais les applis ne sont pas universelles. Certaines ne sont pas écrites ou détenues par l'entreprise et la possibilité de les contrôler serait toujours limitée. Une application parfaite pour la MAM est le contrôle d'un dispositif dédié à une seule appli, ce que l'on appelle parfois le « mode Borne ». Des scénarios d'utilisation dans les magasins et hôtels ont activé ce mode pour accélérer le processus de paiement, de consultation du stock ou de commande de produits alimentaires et de boissons.

Gestion du contenu

L'univers connut alors une nouvelle expansion. Un éclair apparut et le CMC (Mobile Content Management) vit le jour. Désormais, les fichiers et les documents pouvaient être gérés de manière sélective par les membres sélectionnés d'une équipe. Certains utilisateurs sont exclusivement autorisés à voir certains documents et les réexpédier. Certains peuvent modifier des documents, enregistrer les modifications grâce au partage de fichier et permettre à tous les utilisateurs de les consulter et de les synchroniser sur leurs dispositifs. La mobilité de l'entreprise a largement bénéficié des possibilités et des contrôles apportés par la MCM. L'avenir était également plein d'espoir et de promesses : modification sécurisée, privée et simultanée de documents partagés sur des appareils mobiles, sans risque de collisions avec des astéroïdes de sécurité qui caractérisent généralement les services publics de partage de fichiers.

« Mais nous voulons montrer à nos collègues des photos de famille, de nos animaux domestiques et lire les emails professionnels avant d'arriver au travail ! » s'exclamèrent les employés.
« Peut-on faire les deux sur un même appareil ? »

Cette série d'expansions en si peu de temps plaça l'entreprise devant un éventail de choix si étourdissant pour gérer la mobilité que le service informatique replongea de lui-même pratiquement dans l'obscurité en tentant de comprendre les multiples options de gestion des points de connexion maintenant disponibles.

66 % des principaux problèmes de sécurité des responsables informatiques concernent la connexion des appareils personnels au réseau de l'entreprise.[2]

Frontières entre vie professionnelle et vie privée

Un autre éclair : désormais les utilisateurs étaient prêts à cette explosion de lumière et s'étaient munis de lunettes de soleil. C'est alors que tomba du ciel un conteneur qui renforça l'intérêt de la MAM et de la MCM et créa deux environnements indépendants.

Un conteneur fournit une approche plus fine de la gestion des applis et des contenus en fonction du contexte et de l'identité : qui ils sont, où ils sont et quel est leur rôle dans l'entreprise. Il sépare également les données personnelles de celles de l'entreprise en isolant les applis professionnelles et personnelles et en plaçant dans un bac spécifique les e-mails et documents professionnels.

Les conteneurs protègent les données personnelles des employés et offrent des contrôles séparés pour l'entreprise, tels que l'accès au réseau et la navigation Web approuvée par l'entreprise. Ils peuvent empêcher la copie des données d'un « coté » de l'appareil vers l'autre, et le conteneur de l'employeur peut être effacé ou verrouillé en cas d'activité répréhensible sans affecter l'autre « côté » de l'appareil. L'archétype de scénario d'utilisation est un employé dans un secteur très réglementé qui utilise des informations sensibles de l'entreprise.

Enterprise Mobility Management : L'univers mobile actuel et l'étape suivante

Les membres du service informatique étaient aux anges. Désormais, les utilisateurs pouvaient télécharger des applis depuis les magasins d'applis commerciales sans compromettre les systèmes de l'entreprise. Les conteneurs offraient également plus de flexibilité aux utilisateurs, car le « côté professionnel » du conteneur pouvait être simplement supprimé sans affecter le reste des données et des applis sur l'appareil.

La plupart des entreprises utilisent plusieurs plateformes logicielles et échangent constamment une multitude de types de documents sur les postes de travail et les réseaux locaux. « Et pourquoi ne pouvons-nous pas le faire en toute sécurité sur nos appareils mobiles ? » demandèrent les utilisateurs.

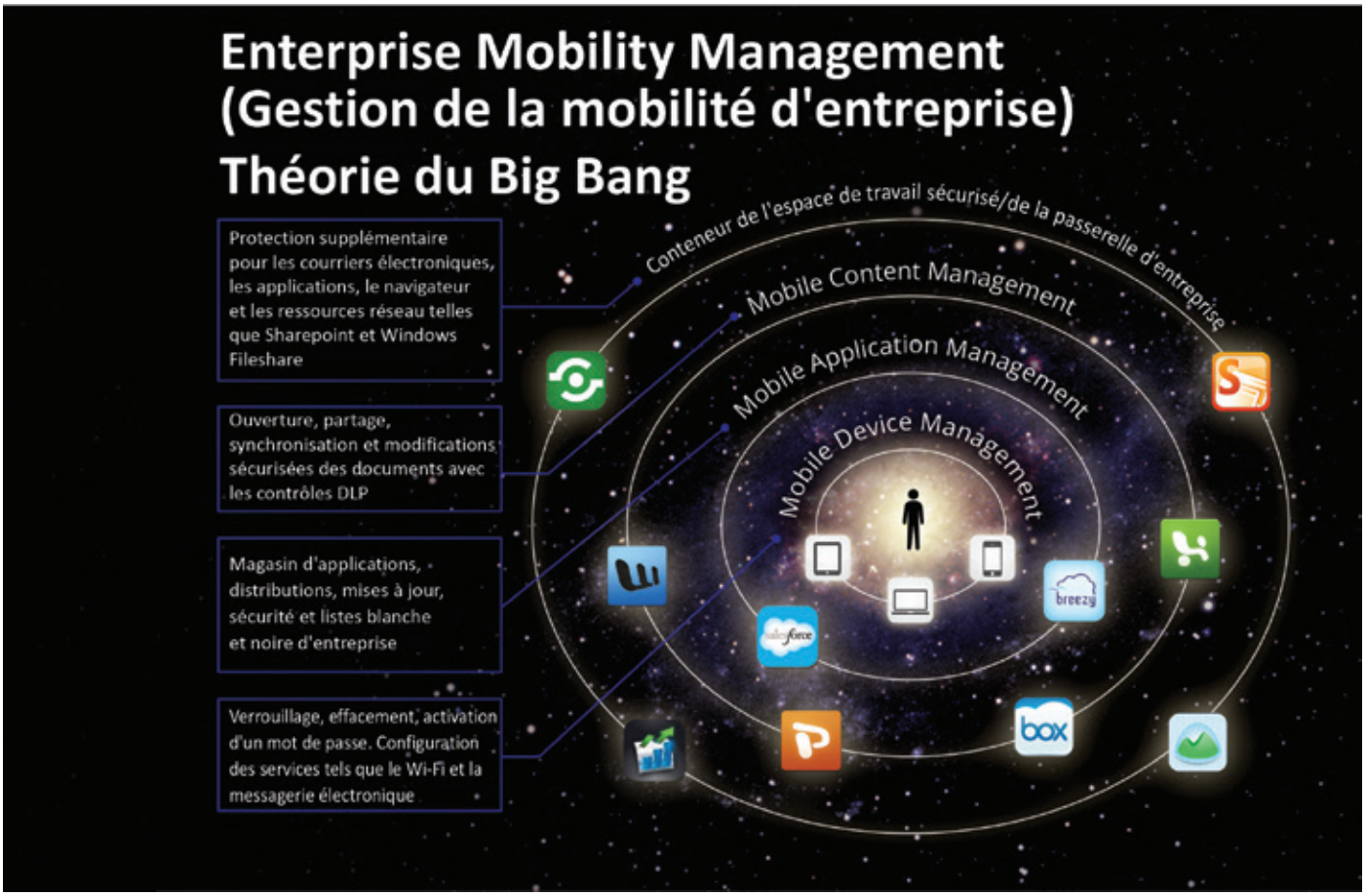

Figure 1 : Théorie du Big Bang pour la gestion de la mobilité d'entreprise

28 % des directeurs de services informatiques indiquèrent que leurs entreprises n'avaient aucune stratégie de technologie mobile.[3]

51 % des entreprises appliquent une stratégie de mobilité d'entreprise avec des projets clairement définis. Et 49 % n'en ont pas.[4]

Les entreprises sont confrontées à un autre cataclysme, mais cette fois, il s'apparente plus à une implosion qu'à une expansion. La plupart des solutions dédiées qui résolvent des aspects des problèmes de mobilité d'entreprise sont regroupées sous l'EMM (Enterprise Mobility Management) qui permet au service informatique de résoudre les problèmes d'intégrité des données et de sécurité dans l'univers mobile. L'époque actuelle s'apparente à la Renaissance après le Moyen-Âge. Elle promet d'offrir plus de choix aux grandes et petites entreprises avec une flexibilité infinie pour sélectionner les composants qui répondent aux besoins réels de l'entreprise.

L'EMM facilite la résolution des problèmes d'intégrité des données et de sécurité dans l'univers mobile.

Alors, comment passer à l'âge des lumières ? Le manque de réflexion structurée concernant ces solutions et leur intégration peut freiner les efforts des entreprises qui tentent d'extraire la valeur ajoutée d'une stratégie mobile et réaliser leur véritable potentiel. Cette situation en partiellement causée par la prolifération des fournisseurs, mais aussi par certaines variables telles que les actions des services et des utilisateurs qui échappent au contrôle du service informatique. Les entreprises doivent donc relever le défi de développer et d'appliquer une politique de gestion de la mobilité conforme à leurs activités et aisément mise en œuvre et exécutée par les utilisateurs.

Qu'est-ce qui empêche les entreprises de réaliser leur véritable potentiel grâce à la valeur ajoutée générée par une stratégie mobile ? Il peut s'agir d'un manque de réflexion structurée pour développer et intégrer ces solutions.

La dernière frontière

L'univers est maintenant entré dans l'âge du choix et de l'abondance, mais aussi dans l'âge du chaos. Aujourd'hui, les besoins des utilisateurs de solutions mobiles peuvent largement dépasser les capacités du service en termes de sécurité et de réactivité. Les employés veulent accéder aux informations professionnelles avec leurs dispositifs mobiles pendant leurs déplacements.

Les différents secteurs d'activité réalisent de plus en plus la valeur que présentent des accès contrôlés, parce qu'ils constatent que la flexibilité améliore la productivité, élimine les retards causés par l'impossibilité d'accéder aux systèmes de l'entreprise pendant des déplacements, et supprime les failles de sécurité qui peuvent mettre en danger leurs précieuses informations. C'est pourquoi les appareils personnels détenus par l'entreprise et les stratégies BYOD (Bring Your Own Device) connaissent un essor rapide.

38 % des entreprises qui envoient des applis à leurs employés utilisent des applis personnalisées.[5]

En règle générale, les utilisateurs ne veulent pas utiliser deux appareils avec des protocoles d'utilisation, des plans de données, des schémas de paiement et des numéros de téléphone différents. Certaines entreprises permettent aux dispositifs personnels d'accéder à leurs systèmes. D'autres les bloquent complètement. Certaines autorisent le développement et la distribution des applis sans tenir compte de la gestion des cycles de vie (déploiement, mise à jour, protection et mise hors service) des applis et des appareils. Ces approches sont dangereuses.

Un système de gestion plus important et holistique ainsi qu'une stratégie associée sont nécessaires pour protéger les données de l'entreprise.

Gestion aisée d'un univers en perpétuelle expansion

Sans l'EMM, l'expansion continue de l'univers mobile devient un défi pour le service informatique, et la plupart des responsables informatiques seraient bien incapables d'indiquer précisément le nombre d'applis utilisées et qui sont leurs utilisateurs. Les applis ont des cycles de développement courts et peuvent proliférer rapidement, au moins pour trois systèmes d'exploitation (ISO, Windows et Android) et pour des dizaines de fabricants d'appareils mobiles.

Pour "arranger" les choses, les services cloud facilitent le téléchargement et le développement d'applis, les transferts de fichiers, etc., parfois totalement en dehors du réseau de l'entreprise.

Le développement d'applis prolifère aussi parce qu'il est décentralisé. Imaginons que le service Marketing crée une appli en quelques semaines, la déploie sur les tablettes de son personnel dans le cadre d'un congrès, et que l'appli se connecte aux systèmes back-end. Si le service informatique ne contrôle pas la situation ou n'en a pas connaissance, un risque de sécurité et de gestion est évident. Et ce type de situation peut être identifié plusieurs fois par jour.

Tout comme le télescope Hubble, la solution EMM idéale doit procurer une visibilité sans faille de tous les appareils introduits dans la sphère des données de l'entreprise.

Les responsables informatiques savent pertinemment que la mobilité est à la fois stratégique et inévitable et veulent que leur entreprise reste compétitive. Mais les services informatiques doivent faire face à une multiplicité de plateformes et de dispositifs non standardisés et sont responsables de la protection des données de l'entreprise.

Les questions sont alors les suivantes :

- Comment les services informatiques peuvent-ils établir un équilibre entre la sécurité et la productivité ?
- Comment le plan de mobilité des services informatiques peut-il s'intégrer à ceux de plusieurs fournisseurs ?
- Comment les entreprises qui adoptent et déploient la mobilité peuvent-elles être plus compétitives et mieux protégées ?
- Comment l'approche IT de la mobilité de l'entreprise peut-elle passer du verrouillage complet des dispositifs pour éviter les problèmes à une ouverture suffisante pour tirer parti des nouvelles opportunités ?
- Comment rétablir l'équilibre dans ce monde et au grand jour ?

Enterprise Mobility Management : Enfin un univers compréhensible

L'EMM est une suite de solutions qui couvrent le large éventail d'activités et de politiques nécessaires à une informatique utilisateur mobile dans plusieurs scénarios d'utilisation. Il s'agit d'une méthodologie holistique qui peut normaliser la gestion d'un environnement multi-OS, s'intégrer aux systèmes d'entreprise existants et supporter de manière sécurisée l'avalanche de données depuis les applis jusqu'aux contenus.

L'EMM englobe tous les aspects de la gestion de la mobilité, ce qui permet au service informatique de couvrir un univers mobile en expansion continue. L'EMM élargit le débat en passant d'un modèle basé sur le dispositif à un modèle centré sur l'appli et les données qui incorpore les applis, les données, le contenu, etc. de l'entreprise dans un environnement indépendant du dispositif. La solution englobe tous les avantages MDM, MAM, MCM et de la conteneurisation dans une structure plus souple. L'EMM peut également générer un retour sur investissement, puisqu'il fournit des rapports et des analyses approfondies pour évaluer la véritable valeur ajoutée de la connectivité mobile.

Avec l'EMM, les entreprises s'émancipent du dispositif.

L'EMM évite aux entreprises d'avoir à sélectionner un dispositif et un système d'exploitation pour prendre en charge les autres, en leur permettant de se détourner des solutions dédiées qui ne répondent qu'à une partie d'un défi plus large. La solution peut incorporer les applis développées par l'entreprise et les applis tierces. Elle évite ainsi à l'entreprise de se focaliser sur la propriété intellectuelle unique incorporée dans leurs données. Cette approche homogène de la gestion des systèmes hétérogènes est la panacée de la surveillance que les responsables informatiques recherchent depuis leur premier examen de certification MS.

40 % des personnes interrogées citent le « choix du dispositif » comme la principale priorité BYOD des employés[6]

L'EMM est une solution pour un environnement d'entreprise mondial.

Il ne fait pas de doute que l'entreprise devient une entité toujours plus mondiale. Alors que les entreprises se confrontaient individuellement, les chaînes d'approvisionnement doivent aujourd'hui collaborer et affronter la concurrence à l'échelle mondiale. Cela signifie que, d'une manière générale, les employés et les partenaires voyagent, exécutent des transactions et engagent les actifs de l'entreprise dans plusieurs juridictions et cultures.

L'EMM permet de respecter les réglementations, quelle que soit la zone géographique. La solution permet aux employés en déplacement d'accéder en toute sécurité aux données de l'entreprise sur n'importe quel dispositif, y compris les dispositifs mobiles et les ordinateurs portables. La collaboration, l'échange de fichiers et la synchronisation des données dans et au-delà des limites de l'entreprise deviennent plus aisés. Quel que soit le nombre d'utilisateurs qui accèdent au réseau, la sécurité appropriée peut être appliquée.

Les applis grand public sont populaires parce qu'elles sont utiles. Mais elles n'ont pas été développées nécessairement pour interagir avec des systèmes d'entreprise comme l'ERP et le CRM. Les solutions EMM répondent à ces problèmes en adoptant une approche axée sur les données, générant ainsi un nouveau potentiel de retour sur investissement.

EMM : génération d'un retour sur investissement vertical

Le nombre des dispositifs et des applis explose, mais ce n'est rien en regard du nombre d'entreprises et des scénarios d'utilisation mobile potentiels. L'EMM peut être personnalisé en fonction des besoins de chaque entreprise, service, employé et partenaire. Analysons quelques cas d'utilisation.

Une grande entreprise utilisait un réseau d'agents et de sous-traitants externes pour vendre ses produits. La société voulait doter cette force de vente tierce d'applis pour leur permettre de vendre plus efficacement, mais la gestion de leurs dispositifs n'était pas pratique. Le but était simplement de fournir des applis sur les dispositifs personnels des vendeurs et de protéger les données dans les applis. L'EMM leur a permis de rassembler seulement les aspects nécessaires de la gestion de la mobilité (la MAM, mais pas la MDM) afin de faciliter l'administration, et sans être intrusif pour les vendeurs qui utilisent leurs propres dispositifs.

Une grande entreprise du secteur des loisirs a amélioré l'expérience client en distribuant des produits alimentaires et des boissons en quatre minutes au lieu de 20. En utilisant une appli mobile spécialisée et gérée en toute sécurité sur les tablettes du personnel, les commandes des clients sont exécutées plus rapidement. L'entreprise a ainsi augmenté son chiffre d'affaires grâce à de meilleurs volumes de commandes.

Evaluation du retour sur investissement de la mobilité

Une caserne de pompiers a doté ses équipes d'iPads contenant les plans d'étage des bâtiments de son territoire, et leur permet de recevoir des informations en direct des webcams installées dans les locaux. En quelques minutes, entre le départ de la caserne et l'arrivée sur le site, les pompiers étudient la progression de l'incendie et ont une meilleure compréhension de l'organisation du bâtiment. Pouvoir éteindre un incendie 10 minutes plus tôt grâce à une meilleure compréhension de la situation génère peut-être le meilleur de tous les retours d'investissement : des vies sauvées.

Les fonctions d'analyse, un élément moins apparent de l'EMM, peuvent être utilisées pour évaluer le retour sur investissement de la mobilité. Par exemple, historiquement, les compagnies d'assurance ont toujours généré d'énormes volumes de papier. Un grand assureur américain permet à ses employés d'accéder à leurs e-mails sur leurs dispositifs mobiles, de déterminer les heures d'envoi des courriers et d'identifier les appareils concernés. La compagnie d'assurance a constaté une augmentation significative de l'utilisation des appareils mobiles après les heures de travail et une diminution correspondante du volume de papier utilisé car les employés n'impriment plus leurs documents pour les emmener chez eux le soir ; leurs activités mobiles génèrent clairement un retour sur investissement.

D'autres entreprises utilisent l'EMM pour analyser les caractéristiques de performance et d'utilisation d'une appli ou d'un contenu, ce qui permet aux services informatiques et aux responsables sectoriels de déterminer précisément la rentabilité de l'investissement.

Conclusion

Pratiquement toutes les entreprises doivent gérer des appareils mobiles à un niveau qui n'existait même pas il y a deux ans. L'éventail des appareils, des systèmes d'exploitation, des applis et des utilisations donne le vertige compte tenu de leurs possibilités d'utilisation infinies.

Que l'entreprise nécessite l'ensemble des fonctionnalités de gestion des dispositifs, du contenu et des applis, et de la conteneurisation ou simplement quelques-unes d'entre elles, il est essentiel d'appliquer une stratégie de mobilité d'entreprise. Les entreprises qui ont déployé l'EMM ont résolu la plupart des problèmes de l'environnement actuel, répondent aux besoins d'accès des employés, protègent leurs données et enchantent les directeurs avec un nouveau potentiel de productivité et de retour sur investissement reposant sur une stratégie de mobilité. Naturellement, à l'instar de n'importe quel autre outil, l'EMM n'est pas une « potion magique » qui fonctionne en pilotage automatique. L'EMM doit être guidée par une équipe de gestion qui tient compte de l'ensemble du cycle de vie de l'adoption de la mobilité et qui connaît les défis et les opportunités que représente la mobilité pour les conditions d'exploitation de l'entreprise.

Nous recommandons à votre entreprise d'appliquer une stratégie de mobilité unifiée qui représente bien plus qu'une réaction automatique à chaque « expansion » de l'univers mobile. Le service informatique joue un rôle clé parce qu'il définit les différents contrôles et autorisations applicables aux différents groupes et qu'il gère ces contrôles sur un système commun.

Alors, l'univers mobile ne devient pas moins puissant, mais peut être, en fin de compte, plus complet, gérable et rationnel. Grâce à cette rationalité éclairée appliquée à la mobilité, vous ne pouvez plus rester dans l'ombre : vous devez foncer vers le progrès avec la certitude de savoir maîtriser cette puissance et de nouveaux potentiels.

Ce document a été créé par CITO Research et sponsorisé par Fiberlink.

CITO Research

CITO Research est une source d'actualités, d'analyse, de recherche et de connaissances pour les directeurs informatiques, les responsables des technologies et d'autres professionnels de l'informatique et de l'entreprise. CITO Research dialogue avec son audience pour identifier les tendances technologiques qui sont exploitées, analysées et communiquées afin d'aider les professionnels à résoudre les problèmes complexes de l'entreprise.

Consultez notre site à l'adresse : http://www.citoresearch.com

A propos de IBM MaaS360

IBM MaaS360 est une plateforme de gestion de la mobilité d'entreprise qui soutient la productivité et assure la protection des données en fonction des habitudes de travail individuelles. Des milliers d'entreprises font confiance au MaaS360 comme fondation de leurs initiatives mobiles. MaaS360 offre une gestion intégrale, avec de puissants contrôles de sécurité pour tous les utilisateurs, les appareils, les applis et les contenus afin de supporter tous les déploiements mobiles. Pour plus d'informations sur IBM MaaS360 et pour commencer un essai gratuit de 30 jours, visitez www.ibm.com/maas360

A propos d'IBM Security

La plateforme de sécurité IBM fournit les données de sécurité nécessaires pour aider les entreprises à gérer leurs utilisateurs, leurs données, leurs applis et leur infrastructure de manière globale. IBM propose des solutions de gestion des identités et des accès, de gestion des données et des événements relatifs à la sécurité, la sécurité des bases de données, le développement d'applis, la gestion des risques, la gestion des terminaux, la protection de dernière génération contre les intrusions, etc. IBM possède l'un des plus grands services du monde en matière de recherche, de développement et de mise en œuvre de services de sécurité. Pour en savoir plus, visitez le site : www.ibm.com/security

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

Produit aux Etats-Unis
Mars 2016

Pensez à recycler

1 Gartner : http://blogs.gartner.com/eric_goodness/2014/07/30/magic-quadrant-for-managed-mobility-services/

2 Ponemon Institute® Rapport d'étude, *2014 « Bilan sur les risques encourus par les terminaux »*, sponsorisé par Lumension® réalisé de manière indépendante par le Ponemon Institute LLD. Date de publication : Décembre 2013 ». https://www.lumension.com/Lumension/media/graphics/Resources/2014-state-of -the-endpoint/2014-State-of-the-Endpoint-Whitepaper- Lumension.pdf

3 Donavan, Fred",*Recherche : stratégie de mobilité »*,enquête de Robert Half Technology, FierceMobileIT, 26/03/14, http://www.fiercemobileit.com/story/wanted-mobile-tech-strategy/2014-03-26

4 Bernhart Walker, Molly, *« Le rapport indique que seules 50 % des entreprises ont une stratégie de mobilité, et que la sécurité est le problème le plus important »*, mandaté par Cisco/Illuminas Survey ; FierceMobileIT, 01/04/14, http://www.fiercemobileit.com/story/only-half-enterprises-have-mobile-strategy-security-biggest-challenge-says/2014-04-01

5 Données issues de *« Statistiques mobiles du MaaS360 » de Fiberlink*, mai 2014 (publication arrêtée).

6 Enquête Cisco : *« Les services informatiques disent Oui au BYOD »*, Communiqué de presse, the network, Cisco's Technology News Site, 16/05/12. http://newsroom.cisco.com/release/854754/Cisco-Study-IT-Saying-Yes-To-BYODwww.maas360.com/maasters/blog security-information/is-your-device-security-policy-leaving-your-company-vulnerable