IBM Security
Livre blanc

Les 10 meilleures raisons qui rendent inutile la Mobile Device Management (MDM)

Un regard décalé sur les défis informatiques que posent les politiques de BYOD dans les entreprises modernes

IBM

Avouez-le

Les smartphones sont seulement une mode. Les tablettes ? Ce sont juste des smartphones indisciplinés et un peu trop futés. Qui en a besoin ?

N'avons-nous pas bien vécu et travaillé pendant toutes ces années sans ces appareils et sans cette connectivité folle et omniprésente ? Quant à l'utilisation des smartphones et des tablettes au travail, est-ce pour que les utilisateurs soient plus mobiles et plus flexibles ? Est-ce vraiment une bonne chose pour tous ces gens de travailler n'importe où, quasiment à n'importe quelle heure du jour et de la nuit ? Nous avons tous lus les statistiques : 1 milliard d'utilisateurs de smartphones dans le monde et des ventes de tablettes se calculant en millions stratosphériques. Tout cela ne serait-il pas en réalité que du matraquage marketing pour nous faire acheter toujours plus ?

Malheureusement, certaines personnes dans votre entreprise ont pu céder au matraquage et pensent que des employés veulent ces nouveaux types d'appareils pour améliorer leur mobilité et souhaitent vraiment travailler sur n'importe quel dispositif pendant leurs déplacements. Ces personnes, souvent des directeurs généraux ou autres responsables, peuvent essayer de vous convaincre que l'entreprise doit évoluer pour supporter, prolonger et amplifier ce mouvement en faveur d'une mobilité toujours accrue.

Ils vous diront que la mobilité s'inscrit dans un mode de fonctionnement moderne, et qu'elle permettra à l'entreprise d'économiser et d'accroître sa réactivité, son agilité. Ils ajouteront que les employés doivent disposer des moyens nécessaires, et même être encouragés à apporter leurs propres appareils au travail et à utiliser les mêmes dispositifs pour leurs activités professionnelles et leur vie privée. Puis ils argumenteront que les employés plus jeunes, parfois appelés la Génération Y ou Millénium, risquent d'exigerr cette liberté mobile. Ils préciseront que vous, en tant qu'administrateur ou professionnel du service informatique, devriez imaginer des solutions qui supportent ces types d'activités tout en coordonnant la gestion, la sécurité, les politiques, l'utilisation et l'évolutivité des appareils mobiles. Enfin ils vous diront que vous devez déployer une solution pour la gestion des appareils mobiles (Mobile Device Management – MDM).

Le moment est venu de prendre position

Bien que des entreprises comme IBM facilitent la centralisation de la gestion et de la sécurité des appareils mobiles divers et variés, ce n'est pas une excuse pour vous soumettre aux lubies des masses, ni pour accélérer votre carrière en essayant d'être tendance et dans le coup. Si vous permettez au progrès de s'immiscer sur ce point, vous savez très bien que l'entreprise vous demandera ensuite de passer au cloud. Où cela s'arrêtera t-il ? Ainsi, avant de passer à l'étape fatale de la mobilité, de la sécurité, du BYOD (Bring Your Own Device : apporter votre dispositif personnel) et de la flexibilité, lisez attentivement ces 10 meilleures raisons qui rendent inutile la gestion des dispositifs mobiles.

1. Il est tout de même plus sympathique d'aller rendre visite à son service d'assistance informatique que d'aller à Disney World® et à Las Vegas

Si vous déployez une solution MDM, vous pourrez facilement et simplement prendre en charge des dispositifs, déployer des correctifs et des caractéristiques de sécurité, gérer l'évolutivité et les mises à niveau, et appliquer des mises à jour et des modifications pour vos politiques. Toutes ces activités peuvent être réalisées par liaison directe sans fil, sans que votre service d'assistance n'ait même à toucher ne serait-ce qu'un appareil ou à intervenir sur place pour aider les employés. Souhaitez-vous véritablement infliger cela à vos employés du service d'assistance et les priver du bonheur de provisionner les appareils un par un ?

2. La technologie ne doit pas sortir de l'espace de travail

Il est évident que les employés savent parfaitement comment utiliser les ordinateurs au bureau. Ils apprendront même à utiliser leurs appareils portables si cela s'avérait utile à l'entreprise. Mais personne n'a envie d'utiliser la technologie à la maison, n'est-ce pas ? Les employés délaissent la technologie dès 17 h et, s'ils doivent respecter une échéance importante, ils préfèrent largement rester au bureau plutôt que de rentrer chez eux pour être en famille. De même, un professionnel en déplacement préfère lire les vieux magazines de l'aéroport, au lieu d'utiliser ce temps d'attente de manière productive. S'il doit travailler pendant des déplacements, il peut utiliser un ordinateur portable, voire mieux : un ordinateur de bureau léger pour disposer de davantage de puissance de traitement. Il fera ainsi l'exercice et le service informatique pourra être fier de son niveau de normalisation.
Et les réseaux sociaux, demandez-vous ? Juste une autre mode pour les adolescents. Affirmer que la majorité des inscrits sont des adultes n'est qu'un écran de fumée pour doper les introductions en bourse. Il suffit de demander au service marketing. Ils vous diront bien que les réseaux sociaux n'ont aucun rôle dans la recherche de contacts et d'opportunités commerciales.

3. Les smartphones ne devraient servir qu'à téléphoner

D'accord, admettons que cette folie des smartphones soit plus qu'une mode et que les employés envisagent de les utiliser au travail. Leur seul intérêt professionnel réel est bien de pouvoir téléphoner, non ? Certes, il existe plus d'un million d'applications mobiles sur le marché. Et il serait vrai que les entreprises, quel que soit leur secteur, utilisent des applications mobiles pour transformer le travail des employés et les interactions entre les clients et les entreprises. Et il faut bien admettre que des solutions Mobile Device Management dans le cloud comme IBM® MaaS360® peuvent aider votre service informatique à gérer le déploiement, la protection, l'attribution et la désinstallation de ces applications. Mais vous devez poser les bonnes questions : Si les employés utilisent toutes ces applications si intéressantes sur leurs smartphones, ne seront-ils pas un peu trop enthousiastes et productifs ? Ne serait-il pas judicieux de limiter leurs attentes ? Après tout, ce ne sont que des smart-phones et pas des smart-ordinateurs, peu importe leur niveau d'intelligence.

4. Vous croyez encore qu'une tablette n'est qu'un smartphone passé sous un rouleau compresseur

C'est déjà assez pénible d'avoir à intégrer les smartphones au travail. Et, maintenant, c'est au tour des tablettes ? Elles sont vendues dans plusieurs formats et différents systèmes d'exploitation. Pourquoi devriez-vous supporter tous ces systèmes d'exploitation, même si le MaaS360 vous permettrait de gérer l'ensemble à partir d'une fenêtre unique ? Et, pourquoi des tablettes d'ailleurs ? Certes, elles offrent aux utilisateurs. de nombreuses applications mobiles supplémentaires. Certes, elles peuvent augmenter la productivité des employés et optimiser la réactivité de l'entreprise. Certes, elles peuvent être gérées simplement et centralisées grâce à un service MDM cloud. Mais même si elles sont des outils géniaux, que les utilisateurs les adorent, qu'elles prolifèrent rapidement, qu'elles risquent de supplanter les ordinateurs portables et qu'elles peuvent être gérées de manière simple et efficace : est-ce suffisant pour les accueillir à bras ouvert dans l'entreprise ? Non, les tablettes doivent s'en tenir à leur rôle initial : rediffuser les épisodes de « La petite maison dans la prairie ».

5. Vous n'embauchez que des employés modèles

Une solution MDM, plus particulièrement une solution MDM cloud, risque de vous rendre la tâche trop aisée pour protéger vos dispositifs mobiles. Il suffira d'un claquement de doigts pour définir et mettre en œuvre les politiques de mobilité dans toute l'entreprise. Les utilisateurs auront beaucoup trop de mal à vous prouver qu'ils ne feront jamais rien qui risque de nuire à l'entreprise, soit de façon malintentionnée, soit par négligence. S'ils perdent leur téléphone, se le font voler ou essaient par quelque moyen que ce soit de détourner les données de l'entreprise, MDM dispose de fonctions et de politiques qui surveillent les dommages potentiels, avertissent le service informatique et aident à mettre en œuvre des solutions correctives à déploiement instantané. Mais, étant donné que votre entreprise n'embauche que des employés modèles incapables de commettre la moindre erreur et aveuglément fidèles à l'entreprise en toutes circonstances, pourquoi devriez-vous installer des mesures de contrôle ? Pourquoi ne pas simplement accepter que les travailleurs seront toujours parfaits, loyaux et dignes de confiance ?

6. Votre secteur d'activité est libre de toute surveillance ou réglementation

Oui, vous avez de la chance. Vous êtes dans une entreprise qui n'est pas soumise à la surveillance de l'administration publique ou à des réglementations nationales. Vous ne faites partie du secteur de la santé, de l'éducation, de l'administration, de la distribution, de la fabrication, des médias, de l'aéronautique, de la chimie, de l'agriculture, de la pharmacie, des transports, des sciences, des finances ou d'aucun autre secteur soumis à la surveillance du gouvernement ou de l'industrie. En fait, vous vendez des poupées Barbie sur eBay, c'est ça ? Donc, en effet, chanceux comme vous êtes, ne vous préoccupez pas des politiques, des audits ou de la gestion MDM.

7. Le service informatique adore examiner et manipuler tous les appareils qu'il contrôle

C'est vrai au fond. Si vous ne pouvez pas le voir ni le toucher... peut-être que cela n'existe pas. Vous y avez déjà réfléchi ? En outre, l'équipe du service informatique préfère largement traiter un à un chaque dispositif (même ceux des utilisateurs) plutôt que de s'asseoir confortablement derrière une console unique et se contenter d'ajuster les politiques, de surveiller l'utilisation et de faire tout son travail rapidement, simplement et en temps réel. Imaginez seulement à quel point l'équipe informatique pourrait s'amuser sans la surveillance centralisée. Elle pourrait distribuer un numéro à chaque utilisateur pour qu'ils viennent tous un par un au bureau faire configurer leur appareil : « John Forman des RH, vous êtes le numéro 1327. Le prochain rendez-vous de mise à niveau disponible est le 22 octobre 2018. Nous serons heureux de vous revoir. Jusqu'à cette date, ne touchez à rien ! »

8. Vos employés sont des êtres cybernétiques et la technologie est gravée dans leur peau

En effet, vous avez bien compris qu'embaucher des employés de science fiction provenant d'une autre planète ou d'une autre civilisation vous apporterait des avantages indiscutables. Grâce à cette main d'œuvre unique en son genre, vous n'avez plus à vous préoccuper des pertes ou des vols d'appareils. Ainsi, quel est l'intérêt de même penser à une gestion centralisée de la sécurité mobile avec des fonctions de suivi à distance, d'effacement à distance et de chiffrement ?

9. Les entreprises fonctionnent mieux quand elles restent complètement à l'écart des informations

Les dirigeants adorent jeter l'argent par les fenêtres. Le « retour sur investissement » n'est qu'une simple expression utilisée à tort et à travers par des élites universitaires qui enseignent les théories de la gestion d'entreprise. Le retour sur investissement n'est pas d'actualité dans l'entreprise moderne et, même s'il l'était, nous savons qu'il ne s'appliquerait pas à l'informatique. Et seriez-vous prêt à croire que les solutions MDM actuelles, telles que MaaS360 IBM Security, proposent des fonctions de gestion des dépenses des mobiles ? A partir d'un site central et en quelques minutes, vous pouvez surveiller et suivre proactivement les utilisateurs qui déploient des applications mobiles. Vous pouvez également vérifier s'ils utilisent leurs appareils pour des activités professionnelles ou personnelles. Quelle perte de temps et d'énergie ! Il y a un vieux proverbe : « Ce que vous ne savez pas ne peut pas vous faire de mal ». Il est impressionnant de voir à quel point ce proverbe reste d'actualité, abstraction faite des découvertes scientifiques de ces 500 dernières années.

10. Vous vous réveillez chaque matin avec la certitude que cette folie « mobile » ne tardera pas à s'essouffler

Vous ne croyez pas aux tendances et c'est tant mieux. Ou à la réalité, tant qu'à faire... Vous savez en votre âme et conscience que cet engouement pour la mobilité finira par faire pschitt. C'est juste une question de temps. Alors enfin, vous n'aurez plus à subir cette pression pour déployer une solution MDM ou autre qui faciliterait la mobilité. Vous ne devrez pas vous soucier de la sécurité mobile, du BYOD ou de la réactivité de l'entreprise. Vous n'aurez pas vous soucier de la prise en charge d'un large éventail d'appareils et d'applications mobiles, ni de créer et de mettre en œuvre des politiques couvrant une multitude de dispositifs. Le cloud ne sera plus une initiative informatique de dernière génération : ce sera votre état d'esprit permanent. Vous serez ravi de vous réveiller tous les matins avec cette belle image teintée de cloud en vous disant que vous aviez raison et que les défenseurs de la mobilité avaient tort.

Vous avez changé d'avis et vous souhaitez découvrir comment le BYOD peut vous aider ?

Dans ce cas, consultez la page www-03.ibm.com/security/mobile/maas360.html et commencez à utiliser MaaS360 gratuitement pendant 30 jours. MaaS3360 étant basé sur le cloud, votre environnement d'essai peut devenir automatiquement un environnement de production sans aucune perte de données

A propos d'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 des utilisateurs. 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, rendez-vous sur 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

WGW03114-FRFR-01