GESTION DE FLOTTE MOBILE (MDM), LE GUIDE DES BONNES PRATIQUES

Avec Kaspersky, maintenant, c'est possible !
kaspersky.fr/business

Be Ready for What's Next

KASPERSKY lab

SOMMAIRE

NOUVELLES ORIENTATIONS : GESTION ET PROTECTION DES PÉRIPHÉRIQUES MOBILES.

1. MOBILITÉ : LES NOUVEAUX DÉFIS

L'accès aux informations et aux applications de l'entreprise avec des appareils mobiles, smartphones ou tablettes, permet aux collaborateurs d'être plus productifs, ce qui renforce l'agilité et la flexibilité de l'entreprise.

Mais la mobilité a un prix. Les fonctionnalités des appareils nomades les plus prisées par les employés attirent tout autant les pirates informatiques, les usurpateurs d'identité, les auteurs de programmes malveillants et autres cyber-criminels. Au cours des 12 derniers mois, 51 % des entreprises dans le monde ont perdu des données en raison d'appareils mobiles non sécurisés.[1]

Il ne s'agit pas simplement de programmes malveillants ; la tendance qui consiste à utiliser des appareils personnels dans les entreprises de toutes tailles contribue à une prolifération de plus en plus complexe des périphériques dans l'entreprise. Dans le même temps, la frontière entre usage professionnel et usage privé devient de plus en plus floue, créant un environnement de gestion et de contrôle difficile pour les administrateurs informatiques.

Comment assurez-vous la prise en charge des appareils personnels sans que cela ne devienne un véritable casse-tête ? Comment pouvez-vous contrôler les activités de l'utilisateur lorsqu'il télécharge des applications dans une chambre d'hôtel à un fuseau horaire différent ? Que se passe-t-il s'il oublie son smartphone dans un taxi ? Êtes-vous en mesure de surveiller tout cela facilement depuis un seul point central ? Le module Mobile Device Management (MDM) peut apporter des réponses à la plupart de ces questions.

2. MOBILE DEVICE MANAGEMENT (MDM) – QU'EST-CE QUE C'EST ?

Le module Mobile Device Management offre aux professionnels de l'informatique la possibilité d'étendre leur stratégie et leurs politiques de sécurité traditionnelles à tous les périphériques, notamment les smartphones et les tablettes quel que soit le lieu où ils se trouvent. Les responsables informatiques peuvent automatiser à moindre coût des tâches de gestion et de surveillance, notamment la configuration des périphériques, les mises à jour logicielles ou la sauvegarde/restauration de données. Et ce, tout en assurant la sécurité des données sensibles de l'entreprise en cas de vol, de perte ou d'utilisation abusive.

3. CHOISIR UNE SOLUTION MDM ADAPTÉE

3.1 Support de plates-formes multiples

Android, BlackBerry, iOS, Symbian, Windows Phone… : toutes les entreprises qui adoptent la pratique du BYOD (Bring Your Own Device) savent bien ce que représente la sécurisation et la gestion de plates-formes multiples.

Une solution MDM permettant le support de plusieurs plates-formes n'est pas simplement source d'économies, elle simplifie également la gestion des systèmes multiples. En outre, elle fait gagner en flexibilité, prenant en charge non seulement vos périphériques existants mais aussi les marques et produits que vous adopterez ultérieurement.

1 Source reference: Ponemon: The Cost of a Lost Laptop (2009)

4. LES BONNES PRATIQUES À ADOPTER

4.1 Des politiques clairement définies

Établissez des politiques spécifiques aux appareils mobiles qui déterminent clairement, entre autres :

- comment les périphériques seront déployés
- à quelles données les équipes nomades accéderont
- quels individus peuvent utiliser les réseaux de l'entreprise et quelles tâches ils sont en mesure d'exécuter
- quelles seront les procédures mises en oeuvre en cas de perte ou de vol

Définissez et appliquez des politiques de manière flexible et précise (ex. : application de différentes politiques à plusieurs utilisateurs et groupes, en fonction de leurs besoins). Ce niveau de contrôle granulaire doit s'étendre à l'appareil lui-même (il est par exemple possible d'empêcher des appareils déverrouillés ou infectés d'accéder aux données de l'entreprise ou de les verrouiller à distance, rajoutant ainsi un niveau de sécurité supplémentaire).

4.2 Compartimenter les données

89 % des personnes qui utilisent un appareil personnel pour leur travail déclarent s'en servir pour accéder à des informations professionnelles indispensables et 41 % avouent utiliser des appareils personnels sur leur lieu de travail sans permission.[2]
Même les utilisateurs les plus rigoureux peuvent, par inadvertance, exposer les systèmes et les contenus de l'entreprise à des risques en téléchargeant des applications personnelles ou en accédant à du contenu personnel depuis leur appareil.
C'est là qu'intervient la compartimentation des données. Cette solution simple sépare le contenu professionnel du contenu personnel sur un appareil, ce qui permet aux départements informatiques d'exercer un contrôle total sur les contenus de l'entreprise et de les protéger des éventuels risques liés à une utilisation privée, sans toucher aux données personnelles des employés. En s'appuyant sur cette technique, les départements informatiques peuvent appliquer des politiques de sécurité et de protection des données à un « conteneur » professionnel sur un appareil personnel ou professionnel, ce qui s'avère particulièrement utile en cas d'utilisation d'appareils personnels au sein de l'entreprise.

4.3 Chiffrement

Les bonnes pratiques en matière de MDM doivent également intégrer la possibilité de chiffrer les données sensibles stockées sur l'appareil. Le chiffrement renforce ansi les dispositifs antivol. En imposant le chiffrement des données sensibles, on diminue considérablement l'impact lié au délai d'intervention nécessaire à la suppression des données d'un appareil égaré ou volé.
En veillant à ce que seules les données chiffrées soient autorisées à quitter le conteneur professionnel sur un appareil, les entreprises peuvent se protéger contre les fuites de données et remplir leurs obligations de conformité en matière de protection des données. La technologie de chiffrement de Kaspersky Lab peut être automatisée et rendue complètement transparente pour l'utilisateur final, garantissant le respect de vos politiques de sécurité.

2 Source reference: Juniper Networks, Trusted Mobility Index 2012.

4.4 Protection antivol et sécurité du contenu
La solution MDM de Kaspersky Lab intègre des fonctionnalités antivol et de protection du contenu, qui peuvent être activées à distance afin d'empêcher tout accès non autorisé aux données confidentielles, notamment :

• **contrôle de la carte SIM :** verrouillage à distance d'un téléphone en cas de perte ou de vol, même lorsque sa carte SIM est remplacée, et envoi du nouveau numéro au propriétaire légitime.
• **localisation/suivi des appareils :** utilisation de la fonctionnalité GPS, GSM ou WiFi pour localiser l'appareil.
• **suppression des données à distance/sélective :** effacement de l'intégralité des données enregistrées sur un appareil ou uniquement des informations sensibles de l'entreprise.
• **verrouillage à distance :** blocage des accès non autorisés à l'appareil, sans avoir à supprimer les données.

4.5 Protection des appareils mobiles contre les programmes malveillants
Une stratégie contre la perte ou le vol des appareils mobiles est indispensable. Car ils courent des risques même entre les mains d'utilisateurs autorisés. Les entreprises se donnent du mal pour mettre en place des solutions de protection contre les programmes malveillants et les courriers indésirables sur leurs réseaux fixes, mais déploient paradoxalement peu de moyens pour empêcher que les appareils mobiles ne deviennent la source de virus ou d'autres menaces.

Les technologies de sécurité de flotte mobile de Kaspersky Lab intègrent une solution anti-malware qui associe la détection traditionnelle à base de signatures et des technologies proactives basées sur le cloud qui garantissent un taux de détection élevé et une protection en temps réel contre les menaces. Des analyses à la demande et programmées permettent une protection optimale, d'où la nécessité d'intégrer des mises à jour automatiques « over-the-air » à une stratégie MDM.

4.6 Simplicité : contrôles centralisés
Les technologies Kaspersky Lab permettent aux administrateurs de gérer la sécurité des appareils mobiles à partir de la même console d'administration que celle qu'ils utilisent pour la sécurité de leurs réseaux et terminaux. Ils s'affranchissent ainsi de la complexité inhérente à des solutions séparées et à la multiplication de consoles souvent incompatibles. Le foisonnement technologique complique la tâche plus que nécessaire.

En simplifiant et en automatisant la configuration sécurisée de multiples appareils, vous réduisez la charge de travail de l'équipe informatique et favorisez une meilleure politique de protection de votre flotte mobile. Une fois vos politiques et règles de base mises en place, un simple clic suffit pour tout contrôler de manière centralisée, que vous gériez 10 ou 1 000 périphériques.

4.7 Trouver le bon équilibre
Le déploiement, l'administration et la sécurité de votre environnement informatique mobile doivent être simples et économiques. La solution MDM de Kaspersky Lab facilite la configuration sécurisée des appareils mobiles, tandis que l'agent installé sur les appareils apporte toute la protection dont vous avez besoin pour les protéger. Les administrateurs informatiques sont ainsi assurés que tous les appareils mobiles sont configurés avec les paramètres appropriés et sont sécurisés en cas de perte, de vol ou d'utilisation abusive.

Quelle que soit la taille de votre entreprise, si vous ne maîtrisez pas les appareils mobiles qui accèdent à vos données d'entreprise, vous allez rapidement faire face à des risques en termes de sécurité ou de perte de données. Que vous adoptiez une approche BYOD pour réduire les coûts ou que vous utilisiez une flotte d'entreprise, au bout du compte les risques sont les mêmes : une quantité exponentielle de données professionnelles sensibles se retrouvent dans les poches des employés et peuvent être oubliées à l'arrière d'un taxi, volées ou perdues.

Imaginez pouvoir allier sécurité et protection des données à la mobilité, à une productivité optimale et à davantage de simplicité. C'est possible grâce aux technologies de gestion et de protection des appareils mobiles de Kaspersky.

5. EN CONCLUSION

Les entreprises ont besoin de compter sur des technologies de sécurité intelligentes pour protéger leurs données, ainsi que sur des outils informatiques à la fois intuitifs et simples d'utilisation. Les 2 500 collaborateurs de Kaspersky Lab ont à coeur de répondre aux besoins des plus de 300 millions de systèmes dont ils assurent la protection et des 50 000 nouveaux systèmes qu'ils accueillent chaque jour.

Kaspersky MDM est une composante de Kaspersky Endpoint Security for Business. Associant logiciels de protection anti-malware primés, outils d'application des politiques informatiques, administration centralisée et protection basée sur le Cloud, les produits de sécurité d'entreprise Kaspersky répondent parfaitement aux besoins de votre entreprise.

Contactez votre revendeur informatique pour découvrir comment Kaspersky peut sécuriser la configuration de vos terminaux mobiles et bien davantage !

IDENTIFIER. CONTRÔLER. PROTÉGER.

Avec Kaspersky, maintenant, c'est possible !
kaspersky.fr/business

Be Ready for What's Next

Kaspersky Lab France
www.kaspersky.fr