

VERS LA MOBILITÉ

Développement d'une stratégie d'entreprise Mobile efficace



VERS LA MOBILITÉ

La révolution mobile a évolué. Il ne s'agit plus simplement de rendre les applications existantes accessibles à distance. Il s'agit désormais de se concentrer sur l'activation d'applications qui ne viennent pas simplement s'ajouter aux modèles d'entreprise existants, mais qui les transforment.

Aujourd'hui, de nombreuses sociétés ont clairement compris les avantages apportés par les solutions de données mobiles d'entreprise : optimisation de la productivité, efficacité et temps de réponse améliorés permettant une réduction des coûts et des opportunités d'augmentation de revenu.

Mais ces avantages comportent également des risques, dont la plupart sont liés au contrôle des données stockées sur les appareils mobiles, ainsi que sur les réseaux et applications auxquels ils se connectent. Comment les entreprises peuvent-elles conserver le contrôle de leurs données ? Garantir la conformité ? Éviter la perte ou la fuite d'informations ? Les entreprises mobiles qui ne disposent d'aucune réponse à ces questions s'exposent à des menaces pouvant avoir un impact grave sur l'ensemble de l'entreprise.

Les stratégies ad hoc ne suffisent plus pour garantir la sécurité de l'informatique mobile. L'une des meilleures méthodes de garantir la cohérence et la sécurité pour les entreprises est de développer un ensemble de stratégies complet.

POURQUOI LES STRATÉGIES SONT-ELLES IMPORTANTES ?

Les appareils informatiques mobiles et plus particulièrement ceux achetés à titre personnel, représentent un risque de sécurité significatif pour les données de la plupart des entreprises.

Ces appareils peuvent contenir des données d'entreprise sensibles et sont facilement égarés, perdus ou sujets à d'autres utilisations inappropriées. De plus, étant donné que ces appareils sont parfois achetés à titre personnel, les contrôles de spécification et d'utilisation sont plus difficiles à mettre en œuvre. Le fait que les entreprises mettent en place des dispositifs de fixation des équipements informatiques ou encore qu'elles vérifient régulièrement les numéros de série et les marques de propriété des ordinateurs portables n'est pas anodin. Toutefois, ces stratégies sont rarement appliquées à des smartphones et à d'autres appareils mobiles. Quoi qu'il en soit, l'élément ayant le plus de valeur n'est bien souvent pas l'appareil mobile lui-même, mais les données qu'il contient.

La sauvegarde de données sur des smartphones ou des PDA devient également un problème. Les appareils mobiles sont souvent perdus ou endommagés et la perte de données, ainsi que la perte de productivité associée, peuvent devenir préoccupantes. Quelques entreprises fournissent des outils, des formations ou des instructions aux employés en déplacement pour la sauvegarde de données sur ces appareils. Mais cela a un coût et il est peu vraisemblable qu'il entre dans le budget établi par ces entreprises.

Les services informatiques du monde entier luttent pour trouver un moyen de s'assurer que les employés se conforment aux stratégies de sécurité des entreprises. Parmi tous les problèmes de sécurité que peut rencontrer une entreprise, le plus préoccupant est sans doute le comportement désinvolte et risqué que peuvent avoir certains employés.

À QUI EST CET APPAREIL ?

L'une des raisons pour lesquelles les déploiements mobiles peuvent comporter des risques est qu'ils représentent une opportunité : les employés en déplacement les utilisent pour répondre à leurs propres besoins et la sécurité des données d'entreprise peut parfois passer au second plan.

Une entreprise doit pouvoir mettre en œuvre une stratégie mobile englobant l'ensemble de la société et les divers groupes et équipes qu'elle comprend. Cela ne se fera pas en une nuit et n'arrivera pas par accident. Cette mise en œuvre nécessite un ensemble de stratégies de mobilité fortes. De plus, de nombreuses entreprises ne disposent encore d'aucune stratégie.

La propriété des appareils est une première étape importante. Si l'entreprise est propriétaire de l'appareil, quand et à quelles fins les employés peuvent-ils l'utiliser ? D'un côté se trouvent les employés qui peuvent affirmer, « Il s'agit de mon smartphone BlackBerry® et je fais ce que je veux avec. » et de l'autre l'entreprise qui peut répondre « Aussi longtemps que vous travaillerez ici, vous utiliserez cet appareil uniquement de cette manière ».

Les entreprises peuvent choisir parmi quatre modèles de propriété :

- responsabilité individuelle, paiement par l'entreprise
- responsabilité individuelle, paiement individuel
- responsabilité de l'entreprise, paiement individuel
- responsabilité de l'entreprise, paiement par l'entreprise

Les entreprises doivent déterminer lequel de ces modèles correspond le mieux à leurs besoins et faire en sorte que ces stratégies soient justes et raisonnables. Par exemple, une entreprise peut demander aux employés d'acheter leurs propres appareils mobiles et en même temps imposer de lourdes restrictions quand à leur utilisation. Dans un scénario comme celui-ci les employés peuvent se sentir frustrés et il sera plus difficile de garantir l'application des stratégies de sécurité.

LA SOLUTION

Parmi ses nombreuses fonctionnalités de sécurité, BlackBerry® Enterprise Solution comprend plus de 400 stratégies informatiques conçues pour aider les services informatiques à maintenir le niveau de sécurité dont ils ont besoin.

Ces stratégies comprennent des commandes permettant aux administrateurs système de verrouiller ou de « tuer » un terminal mobile. Si un utilisateur a égaré son terminal mais qu'il espère le récupérer, l'administrateur peut le rendre temporairement inutilisable. Si le terminal a été volé, il peut être désactivé de manière permanente afin de protéger les données confidentielles qui y sont stockées.

Les stratégies mobiles doivent au minimum prendre en charge ces scénarios, mais il existe de nombreux autres aspects à prendre en considération, y compris : quelles applications les utilisateurs pourront-ils télécharger et installer ? Existe-il des restrictions à définir pour l'utilisation de la technologie Bluetooth ? Le cryptage des données doit-il être obligatoire sur tous les appareils afin de protéger les données au repos ? Quel sera votre position concernant l'utilisation des cartes multimédia, des appareils photo, du Wi-Fi® et du GPS ? Votre stratégie mobile doit prendre en compte tous ces scénarios et plus encore, elle doit protéger efficacement votre entreprise tout en garantissant une productivité optimale.

QUELLE EST LA VALEUR D'UNE STRATÉGIE ?

Lorsque vous établissez des stratégies mobiles, commencez par penser à la valeur des informations que vous essayez de protéger.

La propriété intellectuelle de votre entreprise —c'est à dire non seulement vos processus confidentiels ou informations propriétaires, mais également les connaissances de vos employés— a une très grande valeur sur le marché de l'information actuel. Mais une entreprise peut-elle mettre un prix sur les informations stockées sur le terminal mobile d'un employé ? Il s'agit d'un point délicat car il est difficile d'évaluer la valeur des données étant donné qu'elle varie de manière significative en fonction des entreprises.

QUI CONSERVE VOTRE ANNUAIRE DE CONTACTS ?

Les entreprises doivent considérer les numéros de téléphone comme un actif lorsqu'elles établissent des stratégies mobiles. Même si les employés possèdent leurs propres terminaux mobiles, les entreprises peuvent leur demander de laisser leurs numéros de téléphone lorsqu'ils quittent l'entreprise.

Le coût des services téléphoniques peut également être affecté par les stratégies mobiles. Si une entreprise possède une architecture propriétaire centralisée regroupant toutes les factures, elle peut contrôler ce type de coût avec bien plus d'efficacité. Lorsque les terminaux sont des propriétés individuelles et que les frais sont remboursés, les entreprises finissent toujours par payer beaucoup plus.

DÉMARRAGE DE L'ACTIVITÉ

Maintenant que vous comprenez certains des avantages et des failles potentielles des stratégies mobiles, il est temps de les rédiger.

Pour garantir l'efficacité des stratégies, prenez les éléments suivants en considération :

- Les stratégies ne doivent jamais être rédigées de façon isolée car les personnes à qui on demande de les utiliser ou de les mettre en œuvre peuvent avoir une opinion différente. Un rédacteur unique peut également négliger des aspects importants aux yeux des autres. Ce point n'est pas à prendre à la légère : les entreprises doivent sélectionner les bonnes personnes et inclure autant d'employés et de groupes que nécessaire.
- Un certain nombre de facteurs peuvent entraver l'adoption d'une stratégie et une entreprise doit faire de son mieux pour anticiper ces obstacles. Par exemple, les employés doivent disposer d'une formation suffisante aux stratégies et procédures et bien connaître les raisons pour lesquelles elles ont été mises en place afin de garantir la sécurité. La culture d'entreprise est également un point important. Par exemple, les employés travaillant dans des espaces de travail informels peuvent être moins disposés à adopter des stratégies mobiles restrictives.
- Les procédures de gestion doivent encourager l'adoption de ces stratégies ou leur mise en œuvre risque d'être affectée. Les responsables doivent faire particulièrement attention à ne pas utiliser leurs terminaux en contradiction avec les stratégies et montrer que la conformité avec ces dernières est un aspect qu'ils prennent au sérieux.

Il est clair que l'augmentation de la force de travail mobile accroît considérablement les demandes aux services informatiques car les employés nécessitent un accès plus large aux terminaux mobiles et aux entrepôts de données d'entreprise via ces terminaux. Les entreprises responsables reconnaissent les risques que cela implique, ainsi que l'importance de l'établissement de stratégies mobiles complètes. Elles utilisent ensuite leurs stratégies mobiles et travaillent à la mise en œuvre des solutions mobiles permettant de contrôler l'environnement mobile via l'utilisation de stratégies informatiques.

DÉCOUVREZ LES AVANTAGES DE BLACKBERRY SOLUTION

Avec plus de 400 stratégies informatiques publiées BlackBerry Enterprise Solution aide les administrateurs à contrôler leurs solutions mobiles grâce à des outils de gestion des stratégies informatiques complets et intuitifs.

STRATÉGIES INFORMATIQUES DE GROUPE

Dans une entreprise, plusieurs utilisateurs mobiles peuvent avoir différents besoins pour la sécurité et l'accès aux informations. Désormais, les stratégies uniques ne sont plus applicables à tous. Pour relever ce défi, la solution BlackBerry permet aux administrateurs de déployer des stratégies de groupe qui reflètent les besoins des divers utilisateurs et groupes présents au sein de l'entreprise.

STRATÉGIE INFORMATIQUE PAR DÉFAUT

Dès son activation, chaque smartphone BlackBerry est conçu pour être ajouté à une stratégie informatique de base personnalisable pour bénéficier d'un niveau de sécurité minimal. À partir de là, les administrateurs peuvent créer des groupes d'utilisateurs et modifier facilement les stratégies afin de répondre aux besoins de sécurité de l'entreprise.

MISE EN ŒUVRE PAR LIAISON RADIO

Les paramètres de stratégie informatique peuvent être synchronisés et attribués au smartphone BlackBerry par liaison radio. Par conséquent, les administrateurs BlackBerry® Enterprise Server devant effectuer des déploiements importants peuvent simplement modifier les stratégies informatiques au niveau de l'entreprise sans demander aux utilisateurs de placer leurs smartphones BlackBerry sur une station d'accueil.

Grâce à BlackBerry Enterprise Solution, les stratégies informatiques sont des communications unidirectionnelles sortantes initiées par le serveur. Cela aide les administrateurs à s'assurer que chaque smartphone BlackBerry est conforme — les stratégies informatiques sont conçues pour que les utilisateurs ne puissent pas intervenir ou empêcher l'application d'une stratégie une fois qu'elle a été lancée par l'administrateur. Les stratégies informatiques disposent également de signatures numériques uniques permettant de garantir que seul le serveur BlackBerry Enterprise Server défini puisse envoyer des mises à jour vers un smartphone BlackBerry.

CONTRÔLE DES APPLICATIONS MALVEILLANTES

Dans la conjoncture informatique actuelle, éviter les virus, les chevaux de Troie, les vers et les logiciels espions (regroupés sous le nom d'« applications malveillantes ») comprend deux stratégies : détection et mise en quarantaine. La détection des applications malveillantes peut nécessiter une base de données locale volumineuse régulièrement mise à jour ou un accès permanent à une base de données en ligne. Cette approche fonctionne pour les ordinateurs de bureau, mais pas pour les terminaux mobiles.

BlackBerry Enterprise Solution se concentre sur la mise en quarantaine des applications malveillantes. BlackBerry Enterprise Server dispose d'une multitude de stratégies informatiques de contrôle des applications permettant aux administrateurs de limiter les ressources et les données utilisateur disponibles pour une application donnée. Par exemple, des restrictions peuvent être imposées sur des domaines internes ou externes, un téléphone, un périphérique Bluetooth ou USB, ainsi que sur les données utilisateur telles que les e-mails et la gestion des informations personnelles (PIM). De plus, étant donné que les limitations peuvent être spécifiées pour chaque application, les administrateurs peuvent accorder des autorisations élevées à des applications approuvées.

CONTRÔLE DE BLACKBERRY ENTERPRISE SOLUTION

BlackBerry Enterprise Solution est conçue pour fournir aux administrateurs un contrôle total de la solution. Avec plus de 400 stratégies informatiques publiées, les administrateurs peuvent définir des fonctionnalités d'application concernant :

- L'obligation d'utilisation du mot de passe, la complexité du mot de passe et les délais d'expiration
- La disponibilité des applications
- Des fonctions pouvant être exécutées dans chaque application
- Les périphériques Bluetooth et la manière dont ils se connectent au smartphone BlackBerry
- Le lecteur BlackBerry® Smart Card Reader, pour une authentification à deux facteurs pour l'accès au smartphone BlackBerry
- Les disponibilités et fonctionnalités du navigateur Internet
- Les notifications de changement de stratégie informatique
- Les paramètres des informations sur le propriétaire
- L'affichage des pièces jointes et les formats pris en charge
- Les conditions et la fréquence des sauvegardes et des synchronisations
- Les fonctionnalités relatives aux SMS, MMS et aux messages PIN à PIN
- Les conditions de cryptage S/MIME et PGP®
- Le niveau de stockage de clé privée pour les messages cryptés
- Le niveau de protection du contenu
- Les paramètres de cryptage et l'utilisation de certificats
- Le contrôle de la carte SIM pour les informations liées à l'emplacement, les fonctionnalités d'appel et bien plus encore.

STRATÉGIES INFORMATIQUES BLACKBERRY

Pour obtenir une liste complète de l'ensemble des stratégies informatiques BlackBerry, consultez le Guide de référence de la stratégie BlackBerry Enterprise Server (PDF) à l'adresse :

www.blackberry.com/go/security

FACILE À DÉPLOYER, FACILE À GÉRER

Grâce à BlackBerry Enterprise Solution, les entreprises peuvent bénéficier de fonctionnalités de déploiement et de gestion permettant de simplifier l'administration.

- Fonctionnalités d'administration basées sur les rôles et les groupes - Aide à réduire les risques liés à la sécurité et au fonctionnement, ainsi que les frais administratifs en attribuant des autorisations par rôle et en créant des groupes d'utilisateurs administratifs.
- Application des stratégies informatiques mobiles par liaison radio – Aide à fournir une méthode rapide et économique pour la prise en charge des utilisateurs et la gestion des stratégies d'entreprise à distance afin que les utilisateurs puissent disposer de leurs terminaux en permanence et que les services informatiques puissent effectuer des modifications sans avoir à récupérer les terminaux.
- Suivi des statistiques clés des terminaux – Aide à surveiller facilement les applications tierces chargées, les stratégies informatiques appliquées, les modèles des terminaux, les codes PIN, les versions logicielles et les numéros de série.
- BlackBerry® Web Desktop Manager – Application basée sur le Web conçue pour réduire le coût total de possession pour BlackBerry Enterprise Solution en diminuant le nombre de composants logiciels BlackBerry installés sur les stations de travail des utilisateurs finaux et en permettant aux utilisateurs de smartphones BlackBerry d'installer des logiciels et de gérer leurs terminaux à l'aide de n'importe quel ordinateur disposant d'un navigateur.
- BlackBerry® Monitoring Service – Aide les entreprises à conserver de hauts niveaux de disponibilité et de performances dans leur infrastructure BlackBerry Enterprise Solution en fournissant aux administrateurs des fonctionnalités de surveillance, d'alerte, de dépannage et de création de rapports améliorées, ainsi qu'en activant l'identification et la résolution proactive des problèmes.

La solution BlackBerry est aujourd'hui utilisée aussi bien par des grandes entreprises multinationales que des gouvernements ou encore des petites et moyennes entreprises, et ce n'est pas surprenant. Elle offre l'infrastructure, la sécurité et les fonctionnalités pour fournir aux responsables de secteurs d'activité un accès mobiles à toute une variété d'informations d'entreprise essentielles – e-mail, données et voix de l'organisateur, analytiques d'entreprise, gestion des relations client (CRM) et autres applications d'entreprise. La solution mobile BlackBerry est idéale pour garantir la connexion et la collaboration des entreprises.

OFFRES PROMOTIONNELLES

Démarrez avec des offres promotionnelles conçues pour évaluer simplement une solution BlackBerry avant d'investir. Fournissez un confort d'utilisation et une mobilité accrue à vos utilisateurs en un minimum d'efforts.

Plus d'infos sur www.blackberry.com/go/offers

Le présent document, ainsi que tous les documents inclus en référence ci-dedans ou mis à disposition par hyperlien sont fournis ou mis à disposition « EN L'ÉTAT » et « TEL QUEL » sans condition ni garantie en tout genre de la part de Research In Motion Limited et de ses filiales (« RIM »). RIM décline toute responsabilité en cas d'erreur ou d'oubli typographique, technique ou autre inexactitude contenue dans ce document et ne peut en aucun cas être tenu pour responsable pour tout type de dommage associé à ce document ou à son utilisation, des performances ou non performances de tout logiciel, matériel, produit ou service y compris les composants et les contenus tels que les contenus protégés par copyright et/ou par des sites Web tiers (regroupés sous le nom de « Produits et services tiers »). Lorsque vous vous abonnez à des produits et services tiers vous acceptez : 1. qu'il tient de votre seule responsabilité de (a) vous assurer que votre opérateur prend en charge l'ensemble des fonctionnalités des produits ou services tiers ; (b) d'identifier et d'acquiescer toutes les licences nécessaires avant d'installer ou d'utiliser ces produits ou services tiers et de vous conformer aux conditions énoncées par ces licences ; 2. que RIM rejette toute déclaration, garantie et responsabilité de quelque nature que ce soit relative aux produits ou services tiers.

Certaines fonctionnalités mentionnées dans le présent document requièrent une version minimale des logiciels BlackBerry Enterprise Server ou BlackBerry Desktop, du logiciel du terminal BlackBerry ou des autres logiciels de RIM ou de BlackBerry.

Les limitations et exclusions mentionnées dans le présent document s'appliquent indépendamment de la nature de la cause d'action et en aucun cas un responsable, employé, agent, distributeur, fournisseur ou entrepreneur indépendant de RIM ne peut être tenu pour responsable de tout dommage lié à l'utilisation de ce document.

© 2008 Research In Motion Limited. Tous droits réservés. BlackBerry®, RIM®, Research In Motion®, SureType®, ainsi que les marques commerciales, noms et logos associés, sont la propriété de Research In Motion Limited et sont déposés et/ou utilisés aux États-Unis. et dans d'autres pays du monde. Wi-Fi® est une marque commerciale de Wi-Fi Alliance. Bluetooth est une marque commerciale de Bluetooth SIG. PGP est une marque commerciale de PGP Corporation. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs.