PROTECTION POUR CHAQUE ENTREPRISE : COMMENT FONCTIONNE LA SÉCURITÉ BLACKBERRY

Ce document procure une vue d'ensemble de la sécurité de BlackBerry® sur le plan IT, en expliquant comment nous couvrons l'intégralité des besoins de l'entreprise en matière de sécurité multiplateforme, avec une protection contre les fuites de données, le chiffrement certifié, la conteneurisation et plus encore.

BlackBerry®

Conçu pour optimiser la performance de votre business

Pourquoi la sécurité est plus importante que jamais

La plupart des experts en informatique sont d'accord pour dire que le phénomène BYOD (apportez votre propre terminal) est la tendance en matière de mobilité la plus importante pour les entreprises d'aujourd'hui. Toutefois, la consumérisation est assortie d'une combinaison d'utilisations personnelles et d'utilisations professionnelles – et les terminaux conçus exclusivement pour les consommateurs ne contiennent aucune protection intégrée contre la fuite de données d'entreprise par les canaux personnels.

Au fur et à mesure que les processus d'affaires deviennent de plus en plus mobiles, un volume toujours croissant de données sensibles transite par les terminaux et y réside.

Pendant ce temps, les usages personnelles, assorties d'un risque inhérent, ne cessent d'augmenter :

- Réseaux sociaux
- Courriel personnel
- Applis personnelles non sécurisées
- Messagerie instantanée, SMS/MMS, autre messagerie P2P
- Navigation sur le Web
- Stockage sur MicroSD
- Connectivité USB

Aujourd'hui, les entreprises savent bien qu'elles ont besoin d'une stratégie de sécurité et d'une plateforme de mobilité robustes pour protéger leurs données, leurs activités et leurs utilisateurs.

Pour aborder ces problèmes en détail, la plateforme BlackBerry a été conçue depuis le début pour procurer aux utilisateurs une expérience de premier rang, tout en répondant aux besoins complexes et toujours changeants de la sécurité de l'entreprise. Dans ce document, nous nous pencherons sur les caractéristiques suivantes :

- BlackBerry® Balance™ (pour la séparation des données personnelles et des données d'entreprise au niveau de la plateforme)
- BlackBerry® World™ for Work (une vitrine pour les applications d'entreprise)
- Connectivité sécurisée BlackBerry®
- Authentification sur BlackBerry 10
- Le système d'exploitation BlackBerry 10
- Gestion de la mobilité en entreprise ; règles en matière d'IT et établissement des politiques

Toutes ces caractéristiques et ces fonctions sont contrôlées et activées par l'entremise de la plateforme BlackBerry Enterprise Service 10, que les administrateurs IT peuvent utiliser pour gérer non seulement les terminaux BlackBerry 10, mais également les terminaux iOS et Android,™ pour une véritable gestion de la mobilité miltiplateforme sur une seule console unifiée.

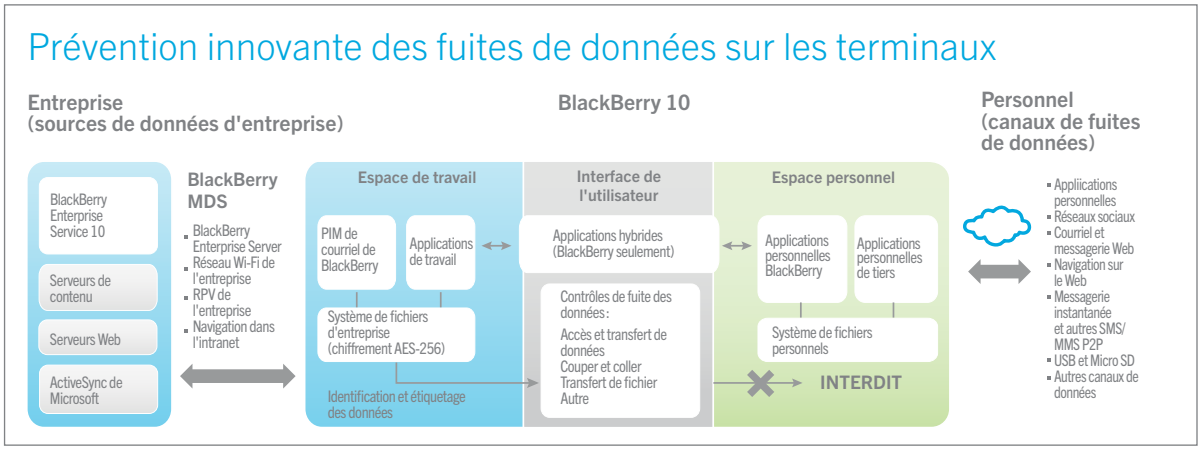
Comment fonctionne BlackBerry Balance

Autrefois, si vous vouliez une meilleure sécurité mobile, vous deviez sacrifier l'expérience utilisateur, et vice versa. Avec BlackBerry Balance, tout cela est fini.

BlackBerry Balance maximise la productivité des employés et la satisfaction des utilisateurs grâce à une interface utilisateur transparente, élégante et intuitive. De plus, il contrôle les risques pour la sécurité en offrant :

- une protection complète sur tous les canaux et mécanismes de fuite de données
- une architecture à l'épreuve de l'altération, qui protège contre les abus et les attaques

BlackBerry Balance cloisonne les données d'entreprise et les données personnelles grâce à deux systèmes de fichiers entièrement séparés. Pour mieux comprendre l'architecture de BlackBerry Balance, jetez un coup d'œil au diagramme ci-dessous.



Espace de travail (bleu)

Les applications d'entreprise résident dans le système de fichiers d'entreprise.

- Les applications et les données d'entreprise sont toujours protégées par le système de fichiers d'entreprise avec chiffrement AES-256.
- Seules les applications qui résident dans le système de fichiers d'entreprise peuvent se connecter par l'entremise de canaux de communication d'entreprise, y compris BlackBerry Enterprise Service 10, le service sans fil de l'entreprise, les VPN de l'entreprise et le navigateur Internet.
  (Si vous souhaitez permettre au trafic dans l'espace personnel d'utiliser les options de connectivité d'entreprise, vous pouvez le faire.)
- Les canaux de communication appropriés sont provisionnés automatiquement afin de protéger vos données d'entreprise sensibles.

Espace personnel (vert)

Les applications personnelles résident dans le système de fichiers personnels.

- Parmi les applications personnelles, on peut citer les applications BlackBerry personnelles comme BBM™ et les applications personnelles de tiers utilisées pour des fonctions comme le courriel, les jeux et les réseaux sociaux.
- Les applications qui résident dans le système de fichiers personnels n'ont accès qu'aux canaux de communication personnelle (figurant sur le côté droit du diagramme), que l'on appelle souvent canaux de fuite de données. Ici encore, vous pouvez autoriser les applications personnelles à utiliser les options de connectivité d'entreprise, si vous le souhaitez.

Interface utilisateur (gris)

La clé de BlackBerry Balance est son interface.

- Les données provenant d'une ressource d'entreprise sont automatiquement identifiées comme données d'entreprise, et toutes les autres données comme données personnelles.
- Les données d'entreprise ne peuvent pas être copiées ou collées dans un canal de données personnelles et les fichiers ne peuvent pas être transférés d'un système de fichiers à l'autre.
- L'interface utilisateur permet l'affichage simultané d'une certaine partie du contenu d'entreprise et du contenu personnel afin que l'utilisateur puisse bénéficier d'une expérience idéale, par exemple dans le cas du BlackBerry Hub ; toutefois, une « couche d'abstraction » évite toute fuite de données entre l'espace de travail et l'espace personnel.
- Comme l'espace de travail et l'espace personnel ont des fonds d'écran différents, les utilisateurs peuvent toujours voir d'un coup d'œil dans quel espace ils se trouvent.

Conteneurisation pour iOS et Android : Secure Work Space

BlackBerry Balance est une solution de pointe permettant de séparer les données d'entreprise et les données personnelles sur les terminaux BlackBerry 10. Toutefois, dans un environnement multiplateforme, il faut tenir compte des mêmes problèmes sur différents terminaux. Secure Work Space est une nouvelle option de conteneurisation, d'enveloppe d'applications et de connectivité sécurisée qui procure un niveau de contrôle et de sécurité plus élevé pour les terminaux iOS et Android,™ le tout géré par l'entremise de la console d'administration BlackBerry Enterprise Service 10. Les applications gérées sont sécurisées et séparées des applis et des données personnelles ; en outre, les utilisateurs peuvent accéder à une appli intégrée pour le courriel, le calendrier et les contacts, à un navigateur sécurisé au niveau de l'entreprise, en plus de la consultation et de la modification sécurisées de pièces jointes grâce à Documents To Go.™ L'utilisateur doit s'authentifier pour accéder aux applis sécurisées et les données d'entreprise ne peuvent pas être partagées hors de Secure Work Space.

Votre vitrine pour les applis d'entreprise : BlackBerry World for Work

BlackBerry World for Work fournit un outil simple, gérable et évolutif pour le déploiement sécurisé d'applications d'entreprise. Il installe les applications, qui sont sécurisées par défaut, dans l'espace de travail des terminaux BlackBerry 10 de vos utilisateurs. De là, BlackBerry Balance vous protège contre les fuites de données et toute tentative malicieuse d'accéder aux données d'entreprise.

BlackBerry World for Work vous donne deux options en matière de déploiement de vos applications d'entreprise : le push obligatoire ou le téléchargement facultatif.

Push obligatoires

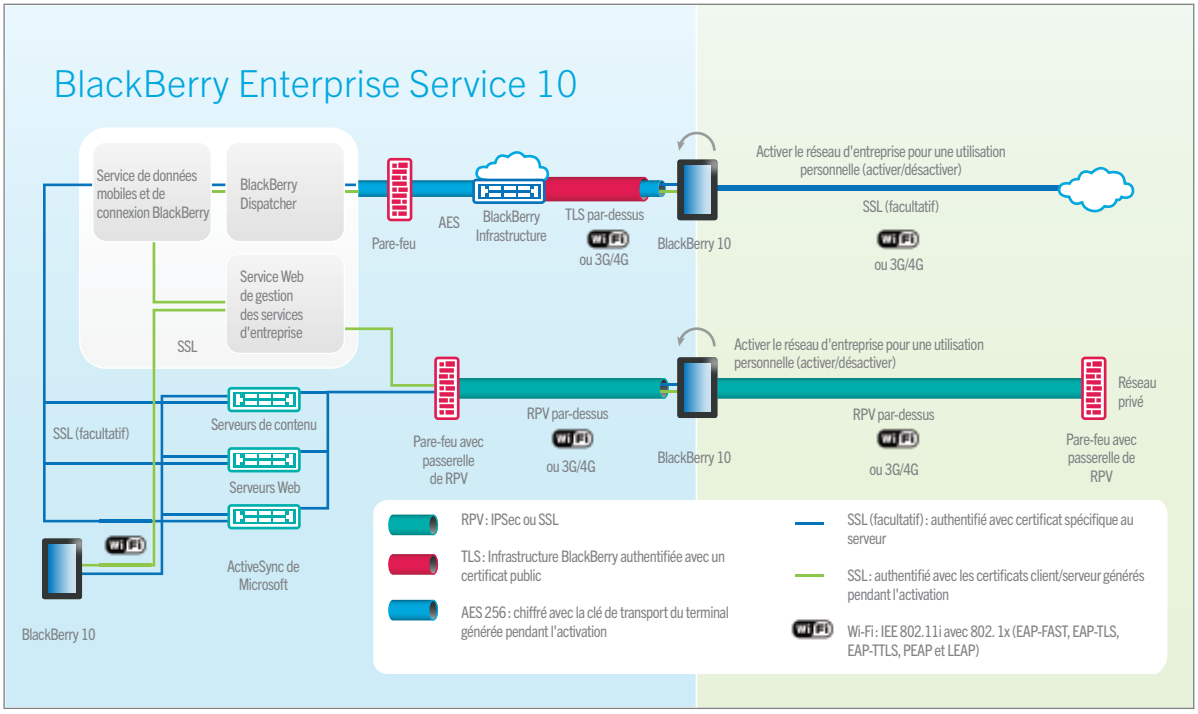
- Vous pouvez les configurer par l'entremise de la console d'administration de BlackBerry 10.
- Ces applis d'entreprise sont livrées et mises à jour automatiquement – les utilisateurs n'ont absolument rien à faire.

Téléchargements facultatifs

- Remplissez votre catalogue d'entreprise d'applis utiles, éprouvées, que vos employés peuvent choisir de télécharger.
- Vous pouvez même choisir de créer une liste d'applis approuvées sur votre boutique d'applications BlackBerry World pour le travail à partir du BlackBerry World publiquement accessible.

La référence en matière de connectivité sécurisée

Depuis des années, BlackBerry® est connu comme la référence en matière de connectivité sécurisée. Rien ne change avec BlackBerry Enterprise Service 10 et BlackBerry 10.



Vous savez peut-être déjà que BlackBerry 10 prend en charge ActiveSync.™ Il faut toutefois noter que le protocole ActiveSync est protégé par le chiffrement de transport familier et sécurisé de BlackBerry avec AES-256. Tandis qu'ActiveSync propose une performance, une résilience et une évolutivité excellentes, BlackBerry aborde donc les préoccupations relatives à la sécurité avec son chiffrement de transport renommé.

Jetons un coup d'œil aux terminaux qui chevauchent le fond bleu et le fond vert du diagramme. Il s'agit des terminaux BlackBerry 10 à connexion d'entreprise (les connexions d'entreprise se trouvent à gauche et les connexions personnelles à droite).

Options de connectivité d'entreprise (fond bleu)

- Hors de l'entreprise, toute connexion à BlackBerry Enterprise Service 10 par l'entremise de l'infrastructure BlackBerry, via le réseau Wi-Fi ou cellulaire, utilise AES-256, qui protège également la connexion à Microsoft Exchange et à tout autre serveur de contenu d'entreprise.
- L'étape allant de l'infrastructure BlackBerry au terminal ajoute une couche supplémentaire de Transport Layer Security (TLS) pour authentifier l'infrastructure BlackBerry.
- Hors de l'entreprise, il est possible de contourner l'infrastructure BlackBerry en se connectant directement à BlackBerry Enterprise Service 10 via VPN, réseau Wi-Fi ou cellulaire.
- Le VPN du terminal prend en charge IPsec et SSL.
- Dans l'entreprise, le terminal se connecte directement à BlackBerry Enterprise Service 10 et au LAN par l'entremise du réseau Wi-Fi.

Remarque : pour toutes ces options, la sécurité Wi-Fi est la norme de l'industrie indiquée dans la légende. Pour plus de sécurité, le SSL de bout en bout est pris en charge entre les terminaux BlackBerry 10 et les serveurs de contenu.

Options de connectivité personnelle (à droite)

- L'espace personnel et les applis personnelles de l'utilisateur peuvent se connecter directement au réseau Wi-Fi et au réseau cellulaire, avec SSL si vous le souhaitez.
- Les utilisateurs peuvent également se connecter au VPN de leur réseau privé.
- Tel que mentionné ci-dessus, il est également possible de permettre au trafic de l'espace personnel d'utiliser les options de connectivité d'entreprise (ce qui peut facilement être désactivé si les politiques IT le demandent).

Authentification : options flexibles en matière de mots de passe et de certificats

BlackBerry 10 prend en charge deux options d'authentification : les mots de passe et les certificats. Les mots de passe sont généralement utilisés pour l'authentification des terminaux.

Des politiques relatives aux mots de passe flexibles et personnalisées peuvent être appliquées :

- À l'espace de travail : l'administrateur peut exiger que l'utilisateur saisisse un mot de passe pour avoir accès à l'espace de travail.
- À tout le terminal : l'administrateur peut également exiger la saisie d'un mot de passe pour avoir accès à tout le terminal BlackBerry 10 (ce qui est essentiel pour bon nombre d'environnements réglementés et à sécurité stricte).

BlackBerry 10 prend également en charge l'inscription de certificats et le renouvellement automatique, au moyen du Simple Certificate Enrollment Protocol (SCEP), la norme dans le secteur.

- SCEP procure une inscription et un renouvellement faciles et évolutifs des certificats.
- L'authentification s'adresse généralement aux réseaux Wi-Fi, aux VPN ou aux intranets.
- Tous les certificats sont chiffrés et protégés dans la base de stockage des clés de BlackBerry 10.

Pourquoi le système d'exploitation BlackBerry 10 est le plus sécurisé

Le système d'exploitation est incontestablement le composant le plus important de la sécurité des terminaux, mais il est souvent oublié. Contrairement aux outils, aux contrôles et aux fonctions de sécurité ou aux sandbox d'entreprise, la sécurité du système d'exploitation est généralement moins visible pour l'observateur. Le code source du système d'exploitation n'est généralement pas partagé et même s'il l'est, il est difficile d'évaluer la sécurité de millions de lignes de code.

Tout d'abord, BlackBerry 10 est basé sur le micronoyau QNX. Qu'est-ce que cela signifie pour vous ? Cela signifie plusieurs avantages pour la sécurité de votre enterprise.

Les avantages pour la sécurité du micronoyau QNX

Il contient moins de code (environ 150 000 lignes) :

- Cette petite empreinte contribue à éliminer les vulnérabilités, car la vérification et les essais de sécurité sont ainsi plus faciles et plus robustes.

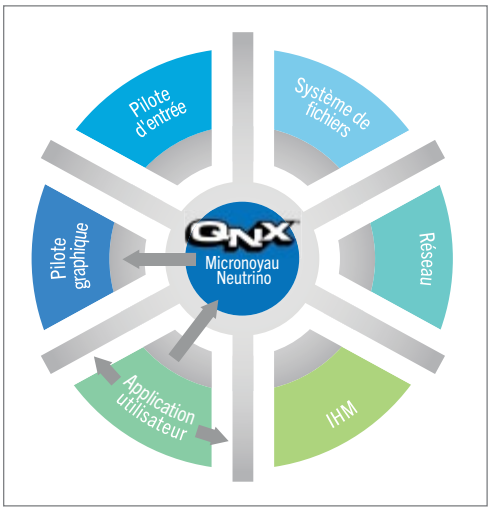
Il est conçu pour être résilient :

- Le micronoyau isole les processus dans l'espace utilisateur.
- Les processus qui ne réagissent pas sont redémarrés sans affecter les autres, ce qui empêche les applications de faire planter le système d'exploitation.

Il minimise tous les processus système :

- Seuls les processus les plus essentiels de BlackBerry fonctionnent comme processus système.
- Les processus système ne sont pas disponibles aux parties autres que BlackBerry, ce qui rend le système d'exploitation moins vulnérable aux risques pour la sécurité.

Le diagramme du micronoyau QNX, ci-dessous, illustre le fait que les processus utilisateurs ne peuvent pas accéder directement à d'autres processus.



Contenu et contraint : contrôles des applications et des maliciels

La meilleure façon de protéger votre entreprise contre les malware consiste à utiliser un système d'exploitation conçu pour leur résister. BlackBerry 10 a recours à une architecture qui « contient et impose des contraintes » afin de minimiser les risques présentés par les malware.

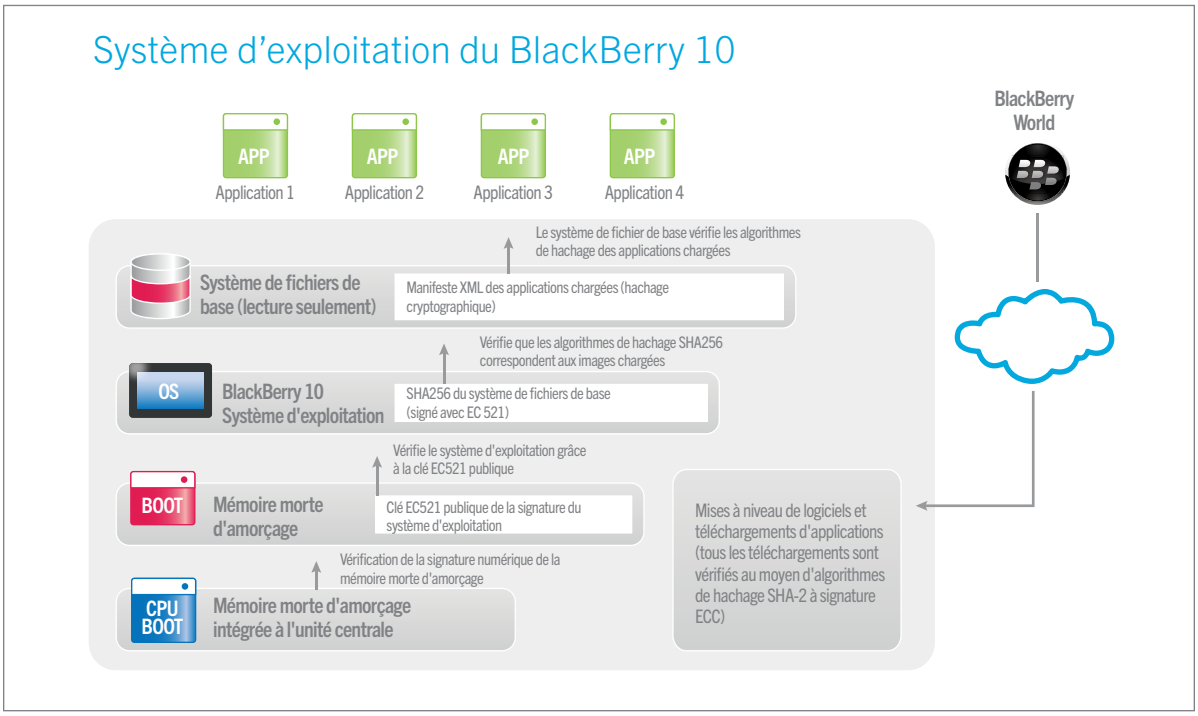
En confinant l'espace utilisateur dans conteneur sécurisé, BlackBerry 10 peut bloquer les comportements malveillants :

- Des contraintes sont imposées aux processus dans l'espace utilisateur et le micronoyau supervise attentivement la communication entre les processus.
- La mémoire à laquelle accède l'espace utilisateur est également autorisée par le micronoyau.
- Tout processus qui tente d'adresser une partie non autorisée de la mémoire est automatiquement redémarré ou arrêté.

Contrôle des applications personnelles

- L'accès aux ressources de l'espace personnel est limité et fonctionne sur une base « appli par appli » et selon les besoins.
- L'utilisateur obtient les bons renseignements au bon moment pour prendre une décision éclairée concernant les permissions à accorder.

Le diagramme ci-dessous présente le processus d'alimentation du terminal et la « chaîne de confiance » de BlackBerry. Ce processus sécurisé est centré sur l'authentification, afin d'offrir une protection contre les attaques persistantes sur le système d'exploitation et les programmes malveillants furtifs.



Dans le diagramme suivant, vous verrez quelques exemples des mécanismes de sécurité intégrés au système d'exploitation BlackBerry 10 pour assurer une protection contre les attaques et l'exécution arbitraire de code.

Mécanisme de protection	Description
Pile et tas non exécutables	Les zones de pile et de tas en mémoire ne peuvent pas exécuter le code machine, dans ce segment de la mémoire, empêchant tout assaillant d'exploiter un dépassement de la mémoire tampon
Protection cookie empilé	Protection contre les dépassements de la mémoire tampon pour éviter l'exécution arbitraire de code
Mises en œuvre de tas robustes	Une forme de protection contre la corruption de la zone de tas en mémoire qui peut entraîner l'exécution arbitraire de code
Randomisation de la disposition de l'espace d'adresse (ASLR)	Allocation aléatoire de l'espace d'adressage d'un procédé qui rend plus difficile l'exécution arbitraire de code
Renforcement du code source au niveau du compilateur	Une option du compilateur remplace les constructions de code non sécuritaire, lorsque c'est possible
Pages de garde	Une forme de protection contre un dépassement de la mémoire tampon des tas et l'exécution arbitraire de code

Compatibilité avec S/MIME

Une note importante. S/MIME est la norme la plus courante de chiffrement des courriels entre l'expéditeur et le destinataire. C'est une excellente solution pour la sécurité robuste des communications par courriel à l'extérieur de l'entreprise. Si votre entreprise en a besoin, vous serez heureux de savoir que BlackBerry 10 prend en charge automatiquement les courriels chiffrés et signés avec S/MIME.

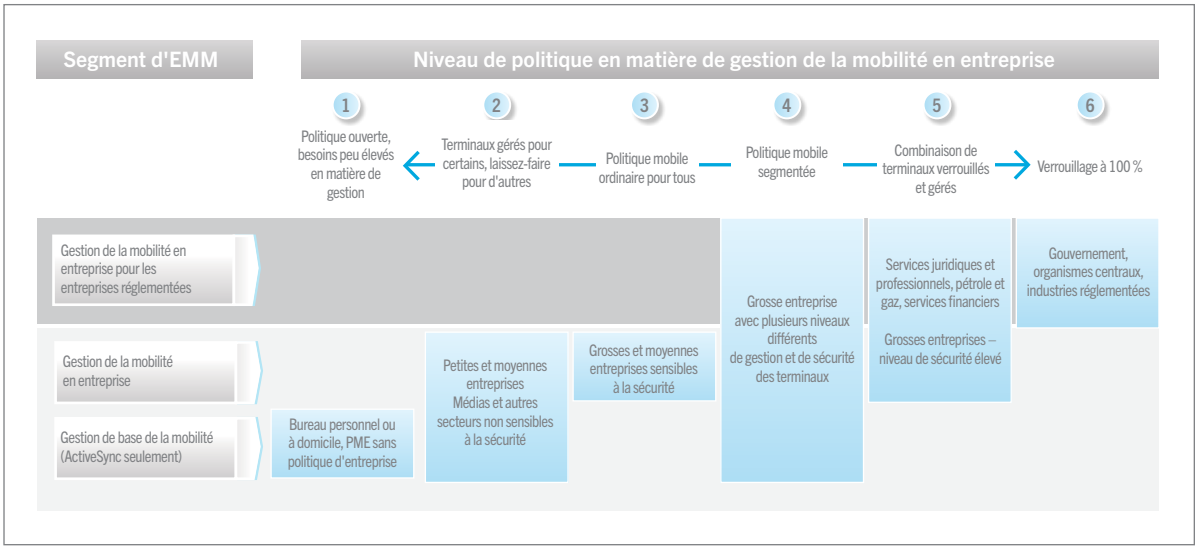
Gestion de la mobilité en entreprise

BlackBerry 10 avec BlackBerry Enterprise Service 10 est compatible avec toute la gamme de besoins en matière de gestion de la mobilité en entreprise, du BYOD de base à un niveau de sécurité élevé.

La prise en charge du protocole ActiveSync par BlackBerry 10 répondra aux besoins des entreprises qui ont une approche décontractée de la gestion des terminaux et de la sécurité, afin de permettre la synchronisation avec leur plateforme de courriel et la gestion de base des terminaux.

À un niveau plus haut, nous proposons la solution Gestion de la mobilité en entreprise (EMM), qui fait partie de BlackBerry Enterprise Service 10. Elle s'adresse aux entreprises qui sont plus sensibles à la nécessité de sécuriser leurs données et qui ont besoin de capacités plus importantes en matière de sécurité et de gestion des terminaux.

Les organismes publics à réglementation stricte et les entreprises qui prennent la sécurité très au sérieux ont besoin d'un contrôle plus rigoureux sur leurs terminaux et auront besoin de faire appliquer des politiques de sécurité sévères. Pour ces organisations, nous proposons la gestion de la mobilité en entreprise pour les environnements réglementés, qui est également administrée par l'entremise de BlackBerry Enterprise Service 10. Cette option vous offre toute une gamme de politiques qui vous permettront de contrôler pratiquement tous les aspects des terminaux.



Règles en matière de TI et établissement des politiques

Comme avec BlackBerry® OS 7 et les versions précédentes, BlackBerry 10 vous permet d'avoir recours aux politiques des TI pour contrôler et gérer les terminaux dans l'environnement de votre organisation. Et tandis que BlackBerry 10 peut activer les différentes politiques requises par les organisations réglementées à niveau de sécurité élevée, il n'est pas nécessaire de mettre en place des centaines de contrôles informatiques granulaires pour boucher les fuites de données : grâce à BlackBerry Balance, votre entreprise est automatiquement protégée.

Si vous souhaitez obtenir des renseignements plus détaillés sur les sujets que nous venons d'aborder, consultez la vue d'ensemble technique sur la sécurité de BlackBerry 10 ou visionnez cette webémission sur demande concernant la sécurité de BlackBerry 10.

Et pour obtenir des renseignements supplémentaires sur différents aspects de BlackBerry 10 et de BlackBerry Enterprise Service 10 :

- Rendez-vous sur http://blackberry.com/fr/blackberry10ready
- Ne ratez pas le reste de notre série de webémissions sur BlackBerry 10
- Et lisez le BlackBerry Biz Blog pour toutes les nouvelles les plus récentes

Vous êtes prêt à commencer avec BlackBerry Enterprise Service 10 ?
Téléchargez l'essai gratuit pendant 60 jours de BlackBerry Enterprise Service 10[1]

[1]Offre d'essai gratuit de 60 jours : Offre de durée limitée soumise à modifications. Limitée à 1 essai par client. L'essai démarre au moment de l'activation, et est limité à 50 licences EMM Entreprise et 50 licences Secure Work Space. Au terme de l'essai, le client doit acheter le service pour continuer à utiliser le produit. Non disponible dans tous les pays. La mise à niveau d'un système d'essai vers un système de production est possible à tout moment en ajoutant une clé de production, obtenue soit par le programme d'échange BES10 v10.1 soit à l'achat auprès d'un revendeur agréé. Lors de la mise à niveau d'un système pour une utilisation en production, les licences d'essai ne sont plus disponibles. L'option Secure Work Space nécessite BES10 v10.1.

Android est une marque de commerce de Google Inc.

© 2013 BlackBerry. Tous droits réservés. BlackBerry®, BBM™ ainsi que les marques déposées, les noms et les logos qui leur sont associés sont la propriété de BlackBerry Limited et sont enregistrés et/ou utilisés aux États-Unis et dans les pays du monde entier.

BlackBerry®