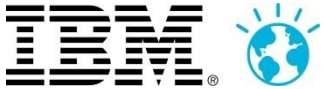
IBM Technical Summit 2013

Démarquez-vous

17 octobre | IBM Client Center Paris



IBM Technical Summit 2013

Démarquez-vous

17 octobre | IBM Client Center Paris

IBM MobileFirst Security

L'approche d'IBM pour la sécurité des terminaux mobiles

Serge RICHARD - CISSP®

Security Solution Architect, Security Systems

IBM

Agenda

- Point de vue des utilisateurs…et des entreprises
- Etat des lieux sur la sécurité des infrastructures mobiles
- L'approche IBM pour la sécurité des infrastructures mobiles
- Les offres logicielles et de services IBM

Agenda

- Point de vue des utilisateurs…et des entreprises
- Etat des lieux sur la sécurité des infrastructures mobiles
- L'approche IBM pour
- Les offres logicielles

Le terminal mobile est un objet personnel !!!

91 %
Gardent leur téléphone à portée de mains H24

60 %
Prennent leur portable à proximité de leur lit

33 %
Préfèrent perdre leur portefeuille plutôt que leur portable

On prête rarement son mobile,
On éteint rarement complètement son mobile, ..

A quel âge, le premier mobile ?

11 ans 1/2

Source : Baromobile 2011 OmnicomMedia Group

http://www.slideshare.net/WSIdee/mettez-votre-entreprise-dans-le-tlphone-de-vos-clients

Que pouvons nous faire avec un terminal mobile ?

- Téléphone
et...

- Internet
- Jeux
- Musiques
- Localisation et Navigation
- Organisateur personnel
- Paiement
- Photos et Vidéos
- Réseau Sociaux
- SMS et Messagerie
- Travail
...

Et plus encore…

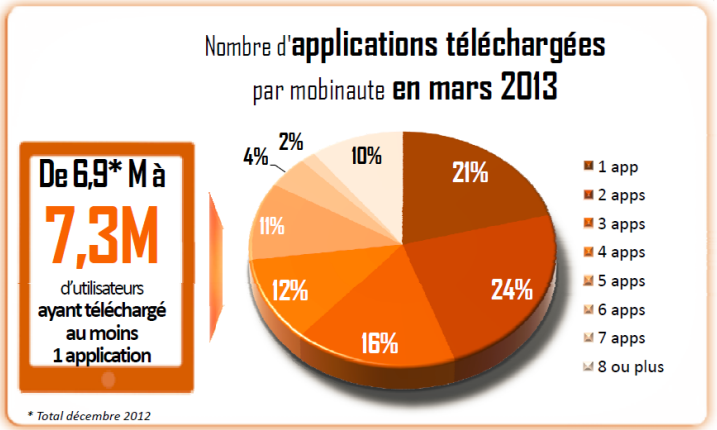
IBM

Les applications mobiles : Fer de lance des terminaux mobiles !!!

Une application mobile est un logiciel applicatif développé pour être installé sur un appareil électronique mobile, tel qu'un assistant personnel, un téléphone portable , un « smartphone », ou un baladeur numérique.

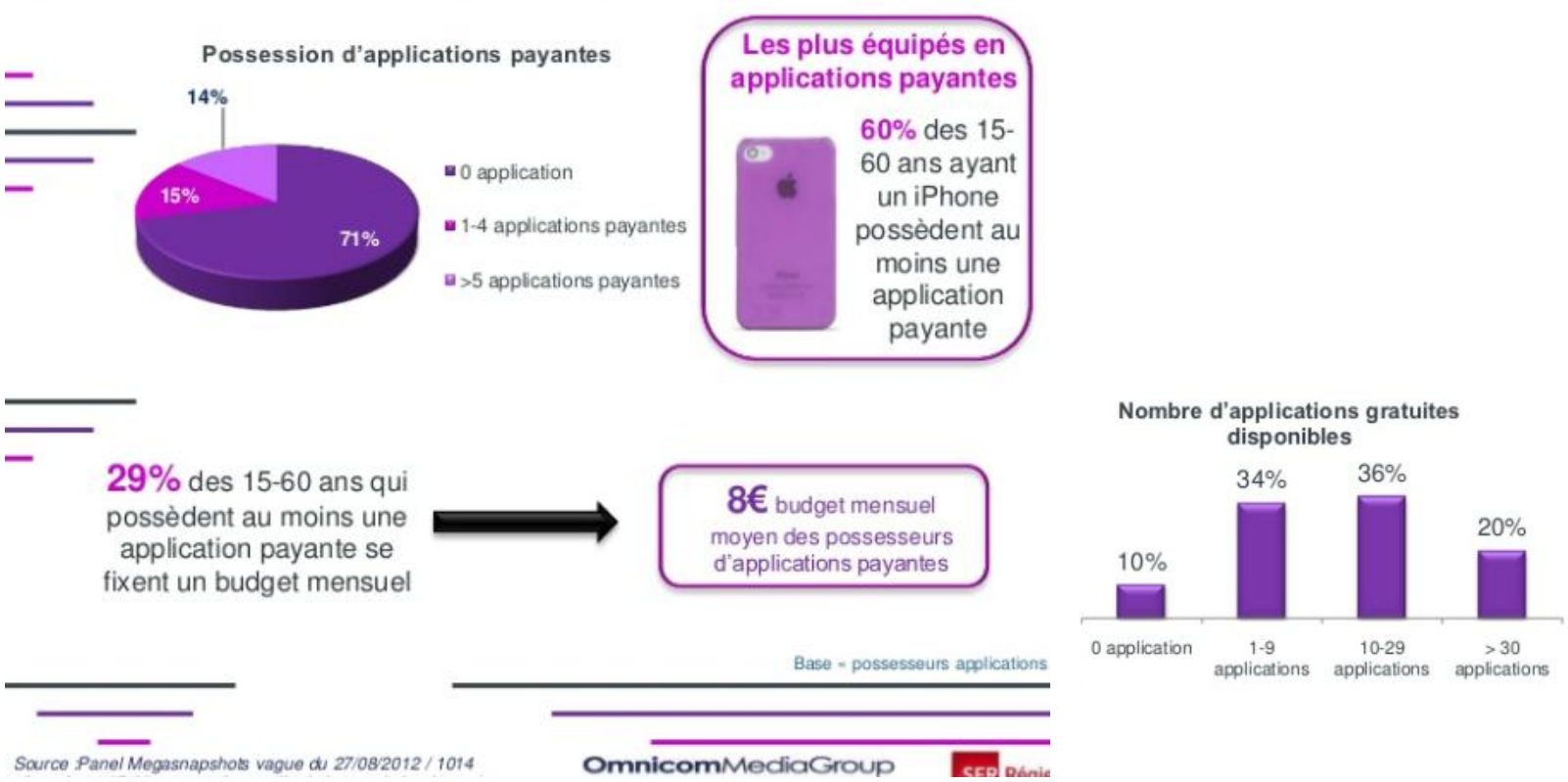
Une telle application peut être installée sur l'appareil dès la conception de celui-ci ou bien, si l'appareil le permet, téléchargée par l'utilisateur par le biais d'une boutique en ligne :

Une partie des applications disponibles sont gratuites tandis que d'autres sont payantes. […Wikipédia]



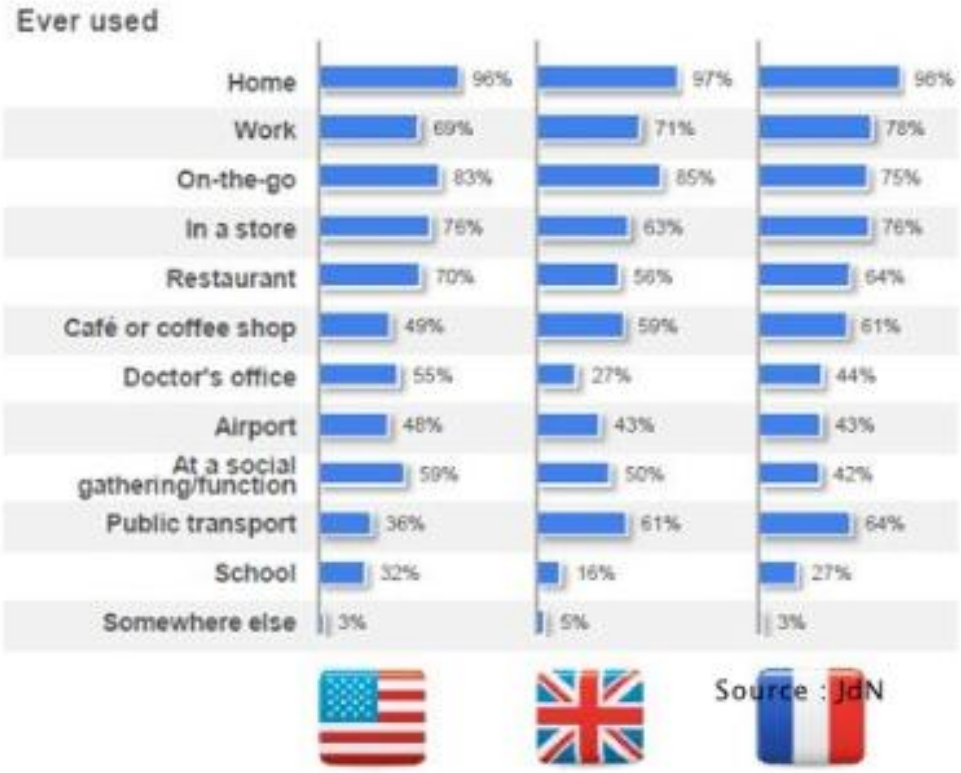
http://www.mmaf.fr/barometre-trimestriel-du-marketing-mobile-en-france-0

Le règne de l'application gratuite !!!



http://www.slideshare.net/omnicommediagroup_fr/baromobile-2012-le-barometre-de-linternet-mobile-omnicom-media-group-sfr-regiegroup-presse

Ou est ce que j'utilise mon terminal mobile ?



Problématiques de l'entreprise…

Le type de terminaux ainsi que le type d'applications sont très hétéroclites.

Les utilisateurs privilégient la facilité d'utilisation des terminaux en fonction de leurs préférences.

Les appareils mobiles sont le plus souvent utilisés en dehors du réseau de l'entreprise et sur une grande variété de réseaux pour l'accès aux comptes utilisateurs.

Dans le but de saisir de nouvelles opportunités, les lignes métiers mettent en place de nouvelles applications sur les terminaux.

Pour de nombreux utilisateurs, l'intérêt des terminaux mobiles réside dans leur capacité d'interaction et les nombreuses applications.

Les terminaux mobiles sont partagés et donc peuvent avoir de multiples utilisations.

Une entreprise ne peut développer toutes les applications demandées par les lignes métiers et doit donc supporter des applications tierces.

Nouvelles technologies pour construire des applications natives, hybrides et web pour les terminaux mobiles.

Les utilisateurs ont en moyenne plus d'un terminal, les données de l'entreprise peuvent se trouver sur ceux-ci.

Augmentation drastique du nombre de terminaux à gérer.

Un contexte dans lequel les appareils mobiles peuvent changer considérablement d'une session à l'autre.

Les applications des terminaux mobiles ont souvent recours à plusieurs services de collaboration et de canaux de communications.

Les différentes approches mises en œuvre par les entreprises

	Stratégie	Impacts avec la stratégie
	Autoriser les terminaux mobiles non contrôlés et non sécurisés	• Perte ou vol des terminaux avec les données de l'entreprise • Vol des données de l'entreprise aux travers d'applications vulnérables
	Ne pas autoriser les terminaux mobiles non contrôlés et non sécurisés	• Coût du terminal mobile à fournir à l'employé • Insatisfaction de l'employé (productivité) • Utilisation de terminaux mobiles non autorisés
	Fournir un service de messagerie au travers des terminaux mobiles : email, calendrier, contacts,...	• Gestion uniquement de la politique de mot de passe et de l'effacement des données (global) • Pas de contrôle du « jailbreak » et de l'installation des applications
	Mise en place d'une solution de Mobile Device Management (MDM) pour gérer et sécuriser les terminaux mobiles	• Nécessite la mise en place d'un nouvel outil • Nécessite de trouver les ressources et les fonds nécessaires pour le déploiement de la solution (ROI risques vs coûts)

Bring Your Own Device (BYOD) Vs Corporate Owned Personally Enabled (COPE)

Le COPE : un BYOD à l'envers

Le COPE (Corporate owned, personally enabled) consiste à mettre à disposition des salariés des terminaux achetés et configurés par l'entreprise pour un usage professionnel mais compatibles avec un usage personnel. Celui-ci sera par exemple rendu possible dans un conteneur étanche (ou sandbox).

Déploiement et sécurité : avantage au COPE

Liberté de l'utilisateur : avantage au BYOD mais...

Coût pour l'entreprise : avantage très théorique au BYOD

Séparation des usages et respect de la vie privée : égalité

Des démarches qui peuvent être complémentaires

http://www.indexel.net/management/byod-ou-cope-6-points-cles-pour-definir-une-strategie-de-mobilite-3730.html

Agenda

- Point de vue des utilisateurs…et des entreprises
- Etat des lieux sur la sécurité des infrastructures mobiles
- L'approche IBM pour la sécurité des infra
- Les offres logicielles et de services IBM

Les recommandations du gouvernement Français

DAT-NT-010/ANSSI/SDE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité
des systèmes d'information

Paris, le 19 juin 2013

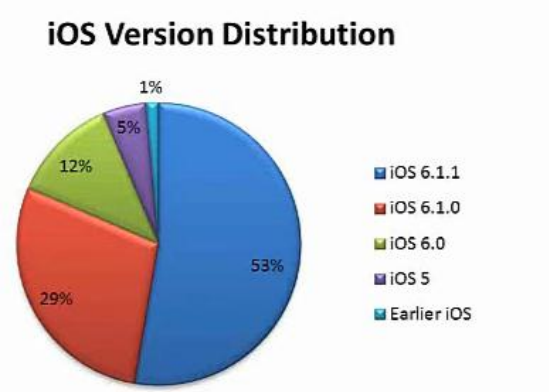
N° DAT-NT-010/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 10

NOTE TECHNIQUE

RECOMMANDATIONS DE SÉCURITÉ RELATIVES AUX ORDIPHONES

Les applications, le principal vecteur de risque ?

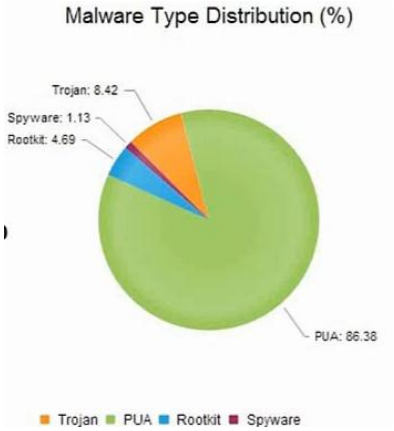


Risques associés avec les applications mobiles malicieuses :

- ✓ Vol d'information
- ✓ Facturation SMS
- ✓ Suivi activité utilisateurs
- ✓ Rootkits

Conséquences avec les applications mobiles malicieuses :

- ✓ Hameçonnage
- ✓ Vol d'identité
- ✓ Perte financière
- ✓ Compromission de l'infrastructure



http://banners.spiceworks.com/banners/webroot/june_2013/S-Webroot_MMA_Webinar.html

La réputation des applications mobiles

Figure 2. App Categories: Which Apps Put Data At Risk?

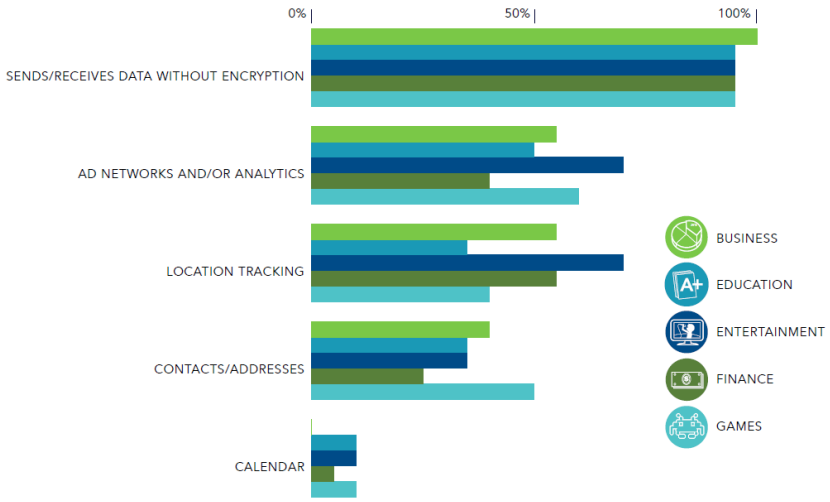
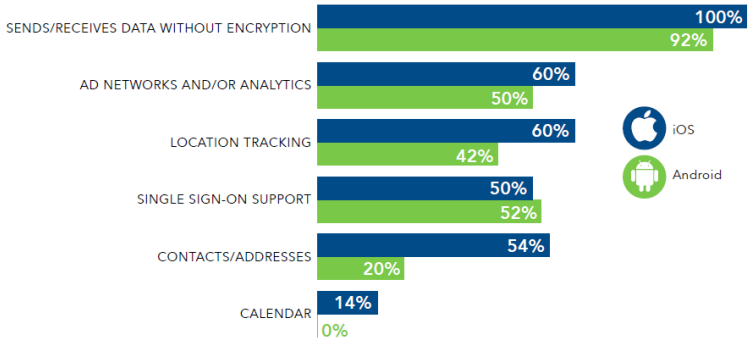


Figure 1. Risky App Behaviors: iOS vs. Android



https://www.appthority.com/appreport.pdf

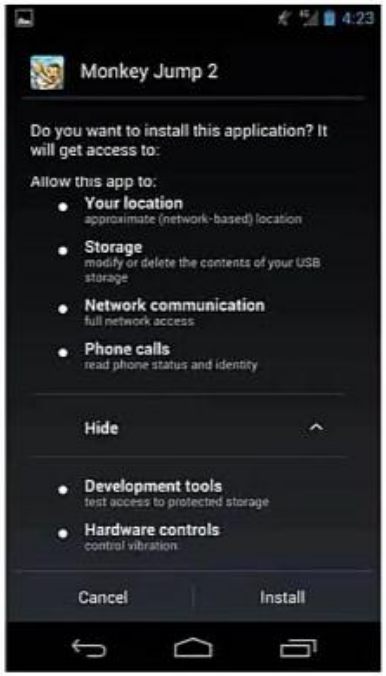
Exemple d'application malicieuse : Trojan/Rootkit

Un exemple classique d'une application malicieuse qui demande plus de droit que nécessaire.

Le fait que le terminal soit « rooté » ou « jailbreaké » ajoute des risques.

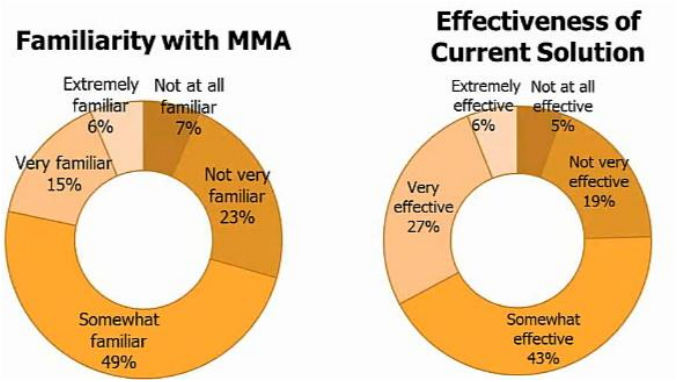
Nous pouvons nous apercevoir que la même application demande des droits supplémentaires.

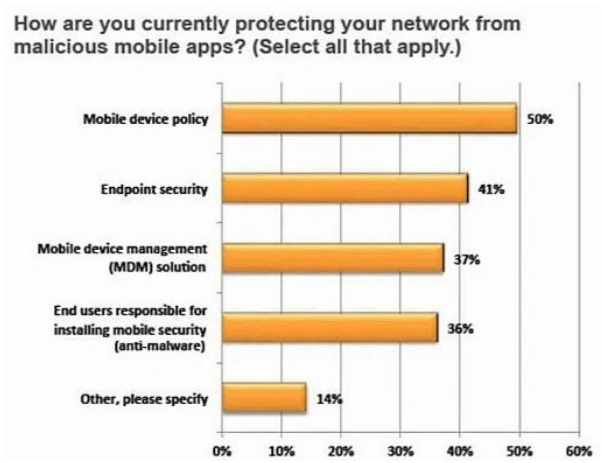
→ Démonstration

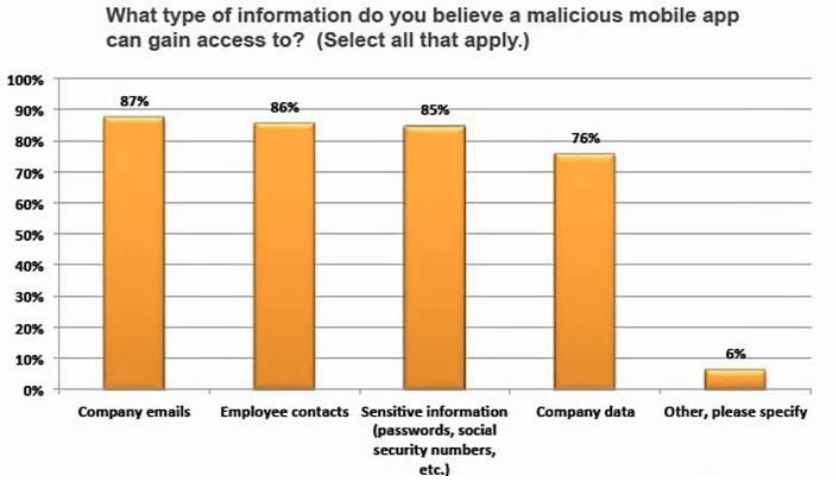


http://banners.spiceworks.com/banners/webroot/june_2013/S-Webroot_MMA_Webinar.html

Appréciation des risques (Malicious Mobile Apps) par les entreprises…





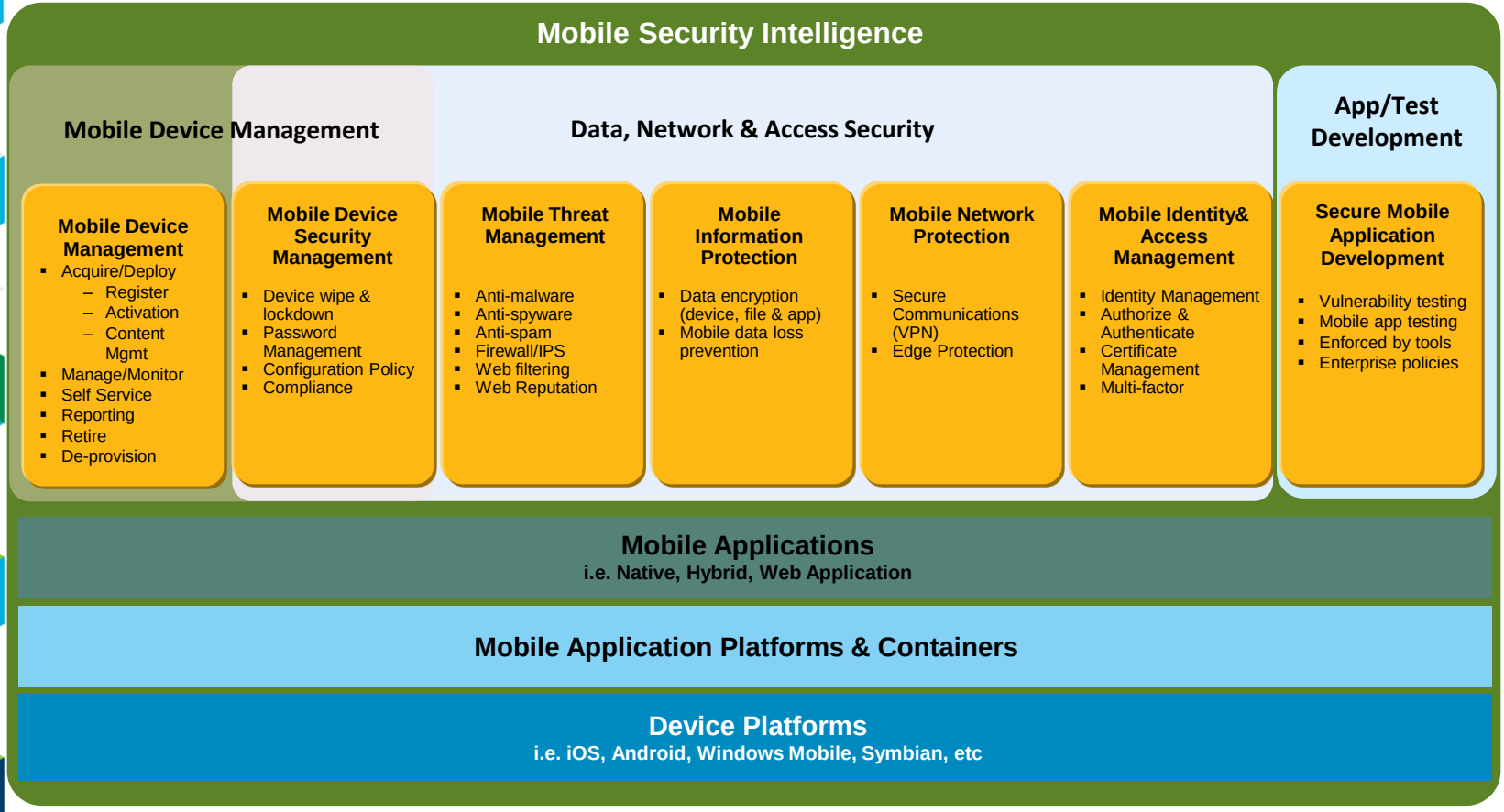


http://banners.spiceworks.com/banners/webroot/june_2013/S-Webroot_MMA_Webinar.html

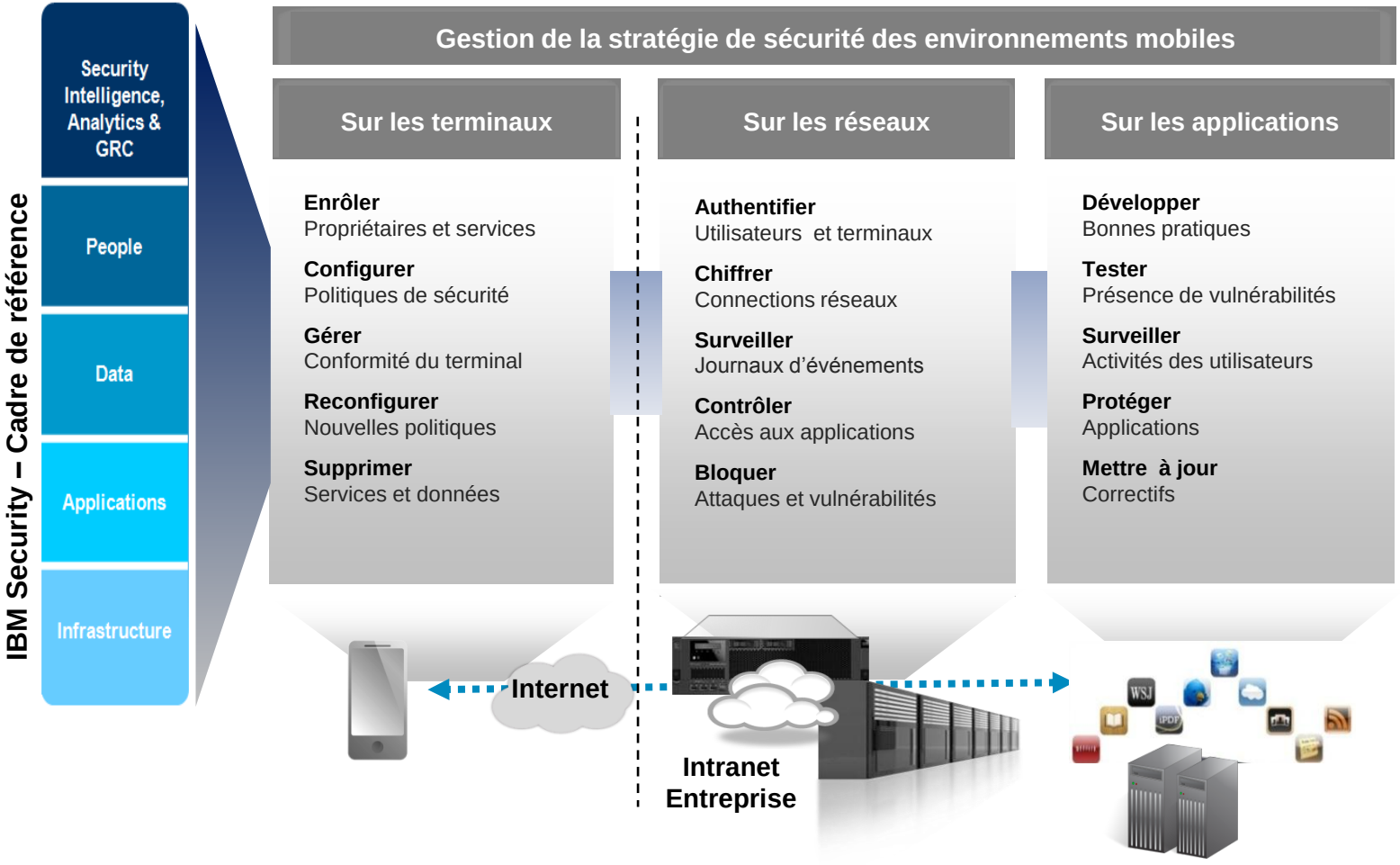
Agenda

- Point de vue des utilisateurs…et des entreprises
- Etat des lieux sur la sécurité des infrastructures mobiles
- L’approche IBM pour la sécurité des infrastructures mobiles
- Les offres logicielles et de services IBM

La sécurité des environnements des terminaux mobiles adresse des dimensions multiples dans le but d'être conforme aux politiques de sécurité de l'entreprise



Comment sécuriser les environnements des terminaux mobiles ?



Agenda

- Point de vue des utilisateurs…et des entreprises
- Etat des lieux sur la sécurité des infrastructures mobiles
- L'approche IBM pour la sécurité des infrastructures mobiles
- Les offres logicielles et de services IBM

L'offre IBM MobileFirst

L'offre IBM MobileFirst Security

IBM MobileFirst Security

Pour les entreprises qui ont besoin de :

- ➢ Protéger les données et les terminaux
- ➢ Sécuriser les communications
- ➢ Avoir un accès sécurité
- ➢ Développer des applications sécurisées
- ➢ Préserver la facilité d'utilisation sans compromettre la sécurité de l'entreprise

IBM MobileFirst Security offre:

- ✓ Un contrôle d'accès basé sur une évaluation des risques du contexte de connexion
- ✓ Une protection contre les menaces
- ✓ Une gestion des accès sécurisé
- ✓ Une analyse des vulnérabilités des applications
- ✓ Gestion des incidents et événements de sécurité sur les terminaux, les réseaux et les comportements des utilisateurs

Nouveautés !

- Une grande qualité dans l'analyse des vulnérabilités des applications pour l'environnement des terminaux mobiles
  - Support natif de l'environnement iOS
  - Prise en charge améliorer pour l'analyse du code JavaScript pour les applications hybrides
- Support de l'environnement IBM Worklight pour l'intégration de la notion des risques liés au contexte de connexion

IBM AppScan

IBM Tivoli EndPoint Manager

IBM Security Access Manager for Mobile and Cloud

IBM QRadar

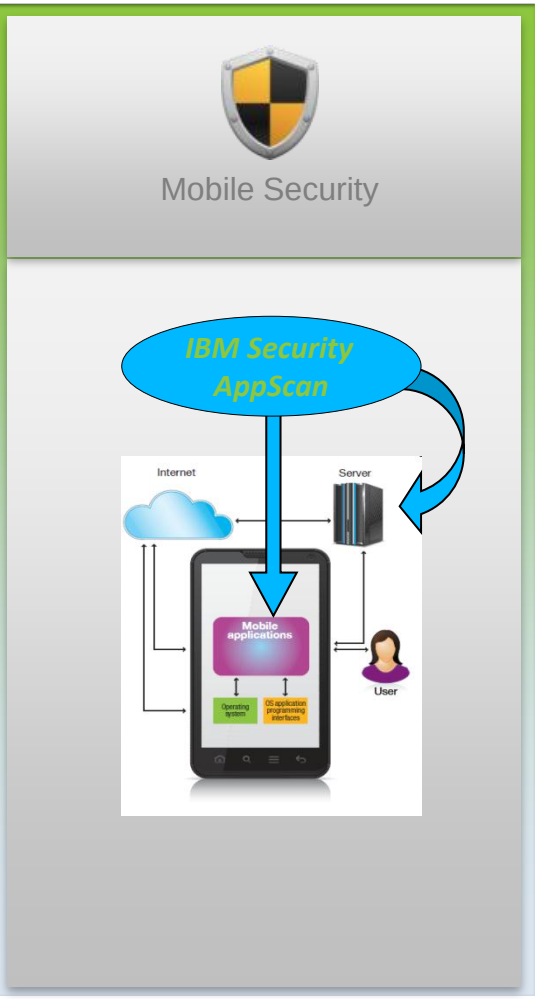
IBM Security AppScan

Adresser la sécurité et la confidentialité tout au long du cycle de vie des applications mobiles afin de protéger les actifs sensibles de l'entreprise

IBM Security AppScan 8.next

Nouveautés

- **Accélérer l'utilisation d'iOS** au seine des entreprises
- **Supporter des analyses de vulnérabilités pour les applications iOS** développées sous Objective C, Java ou JavaScript
- **Permettre une approche "secure by design"** durant le cycle de développement des applications mobiles
- Répondre aux besoins réglementaires **(US Federal Government)**



IBM Endpoint Manager for Mobile Devices

Visibilité et contrôle sur les terminaux mobiles

IBM Endpoint Manager for Mobile Devices

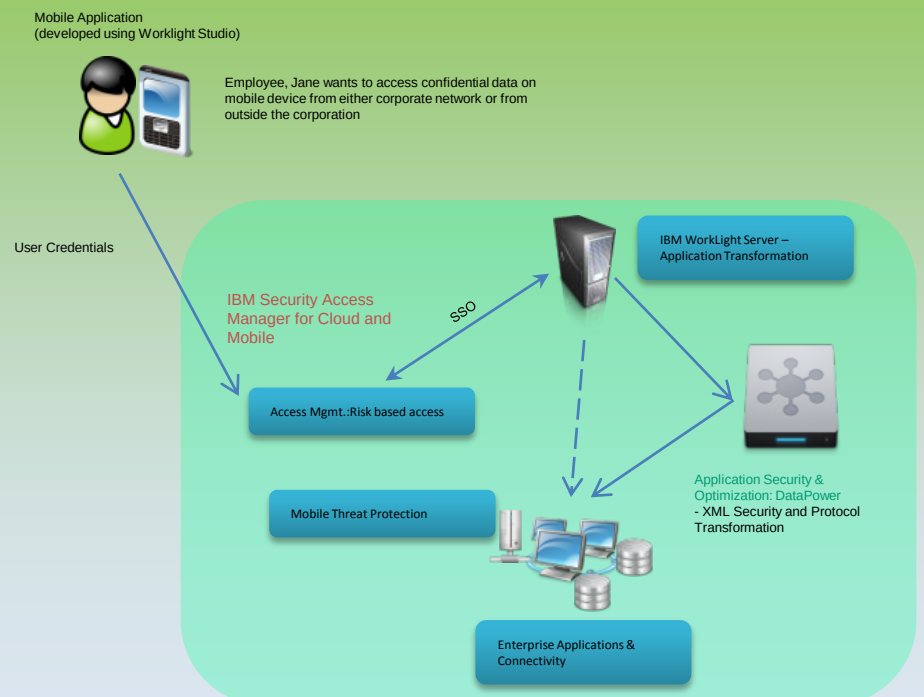
Nouveautés

- **FIPS 140-2 Certified Encryption Module**
  – Conformité aux standards du gouvernement US
- **Gestion de la conformité pour l'accès à la messagerie**
  – Autoriser ou interdire automatiquement l'accès à la messagerie en fonction de la conformité du terminal mobile aux politiques de l'entreprise.
- **Intégration des politiques de sécurité IBM Lotus Notes Traveler**
  – Facile l'administration de la sécurité par le pilotage au travers des la console d'administration Endpoint Manager
- **Dans l'optique BYOD support des plateformes**
  – BlackBerry 10, Microsoft Windows Phone 8, Windows RT, Apple iOS 6.1

IBM Security Access Manager for Cloud and Mobile

Améliorer les possibilités d'identifier les risques liés au contexte de connexion

IBM Security Access Manager for Cloud and Mobile



Mobile Security

Fonctionnalités

Identifier les risques lors de la connexion

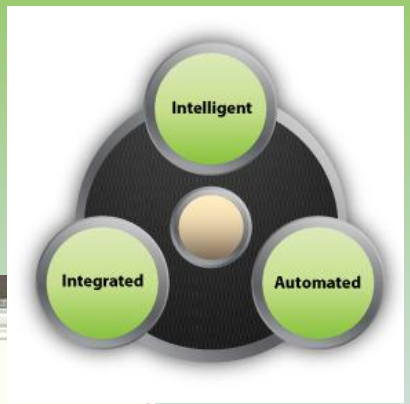
- Evaluation dynamique des risque lors d'un demande d'accès
- Quickly enforce Risk-Based Access
- S'assurer que l'utilisateur et le terminal sont authentifiés et autorisés
- Authentification forte : user id/password, OTP, biométrie, certificate, autres
- Protection des application contre les menaces par analyse du trafic réseau

IBM Security Qradar Plateform Intelligence

Un niveau de protection adaptée

IBM QRadar Plateform Intelligence

Fournir un pilotage complet de la sécurité sur l'environnement de l'infrastructure des terminaux mobiles



Mobile Security

Besoins

Besoin de visibilité sur l'ensembles des événements de sécurité dans le but de gérer les menaces, les besoins de conformité ainsi que les risques de l'entreprise.

Fonctionnalités

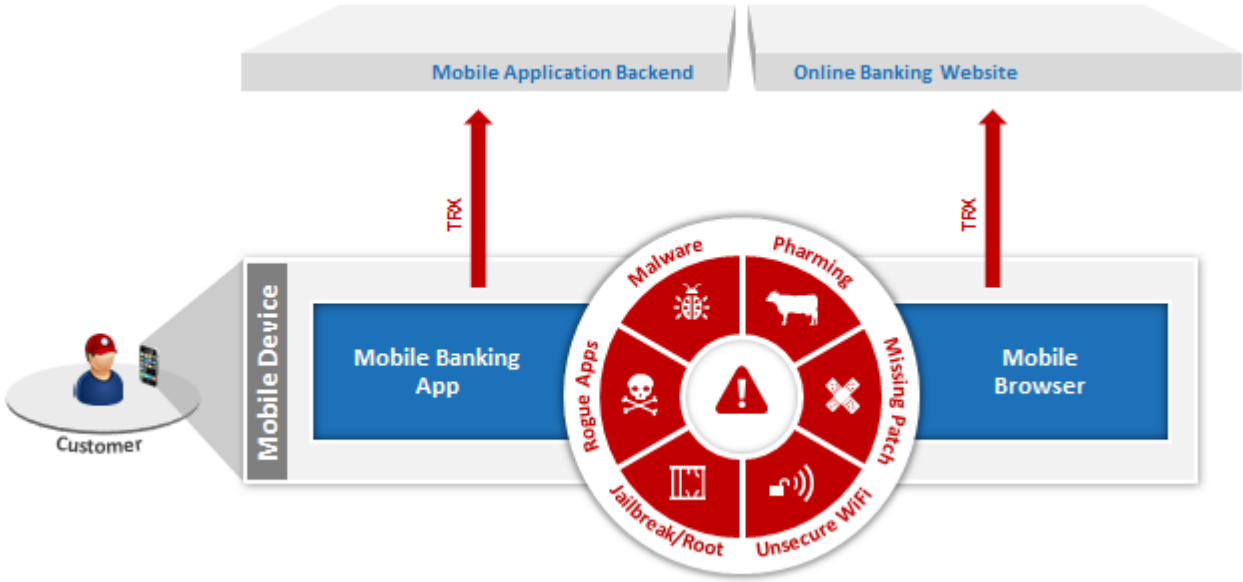
- Plateforme évoluée :
  - Recherche
  - Filtre
  - Ecriture des régles
  - Rédaction de rapport
- Une seule console utilisateur :
  - Gestion des Logs
  - Modélisation des riques
  - Priorisation des vulnérabilités
  - Détection des incidentes
  - Analyse d'impact

Trusteer
an IBM Company

IBM

Controlling Mobile Risk
Detecting compromised devices

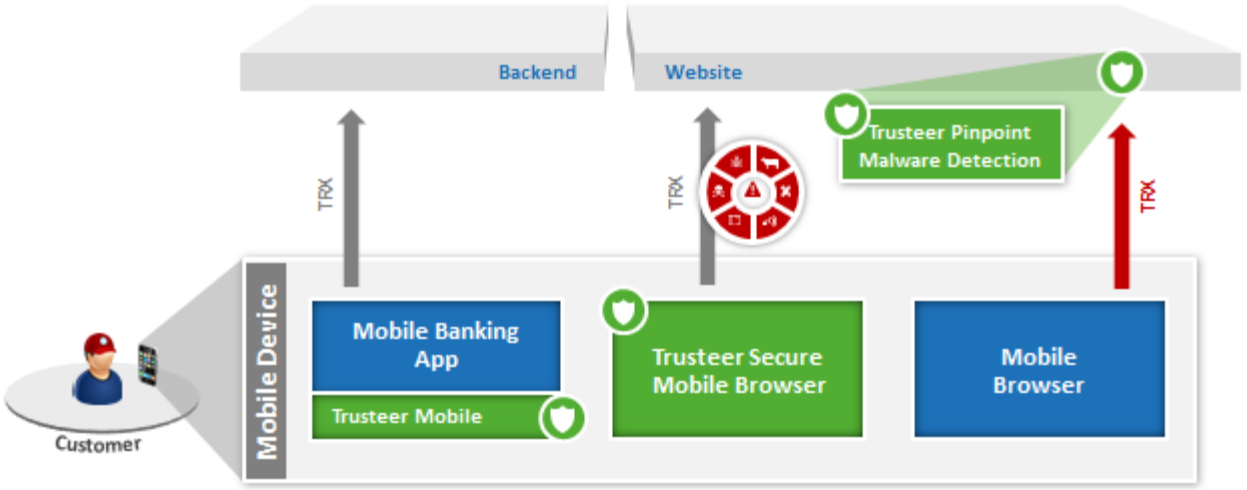
Trusteer
an IBM Company



IBM

Controlling Mobile Risk
Detecting compromised devices

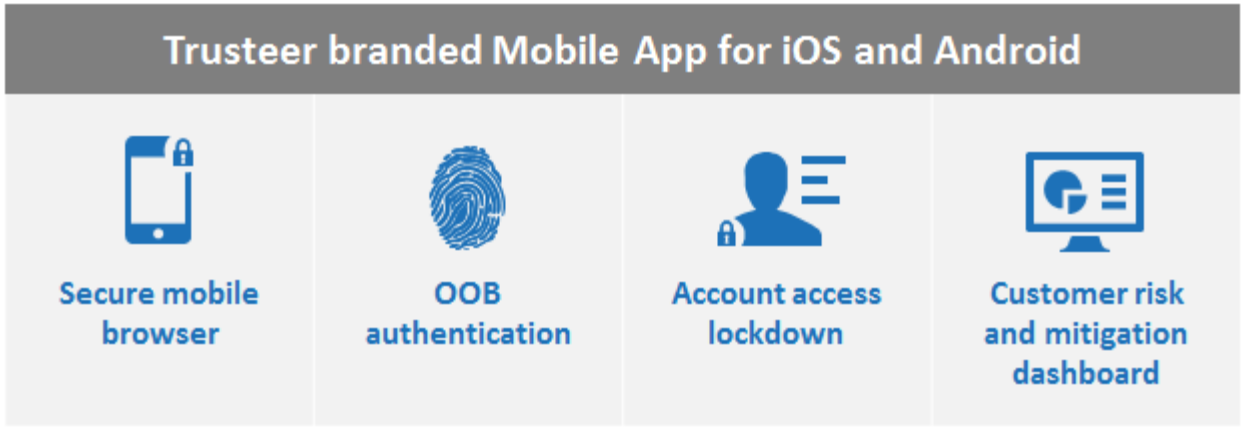
Trusteer
an IBM Company



IBM

Trusteer Mobile Application

Trusteer
an IBM Company



- Powered by Trusteer Mobile SDK
- Supports multiple FIs and multiple accounts

IBM

Trusteer Mobile Application

Secure Mobile Browser

IBM MobileFirst Offering Portfolio - Services

IBM Mobile Enterprise Services for Managed Mobility

Challenge : Gestion complète du cycle de vie de l'environnement des terminaux mobiles incluant Mobile Device Management, applications et support des utilisateurs

IBM fournis des recommandations, effectue des installations, configure et pilote les infrastructures mobiles

- Mobile device lifecycle management
- Mobile devices management (MDM)
- Mobile application platform management
- Mobile messaging
- End-user support
- Apple iOS, Google Android, RIM BlackBerry, Microsoft Windows Mobile smartphones, tablets and rugged devices managed with subscription-based pricing