IBM Security
Livre blanc « Thought Leadership » (Un leadership des idées)

Satisfaire votre désir de pâtisseries fines Android

Les mises à jour Android aux noms de pâtisseries améliorent-elles assez la sécurité des données et des dispositifs pour permettre des utilisations en entreprise ?

IBM

Android est prêt pour l'entreprise. Mais votre entreprise est-elle prête pour Android ?

Introduction

Android domine depuis longtemps le marché de la grande consommation. Aujourd'hui, les améliorations de sécurité les plus récentes de Google et des fabricants d'appareils, et le soutien d'Android par les principaux fournisseurs de solutions EMM, étendent sa présence dans l'entreprise. Pour assurer la sécurité et la conformité aux normes industrielles et aux réglementations publiques, les entreprises ont besoin d'une solution permettant de protéger et de gérer la gamme étendue des dispositifs disponibles, incluant les versions et les particularités du système d'exploitation le plus utilisé dans le monde.

Cette solution ne peut pas être universelle. Les services informatiques doivent examiner l'ensemble de leurs applis et dispositifs afin de définir les caractéristiques de gestion et de sécurité indispensables dans une stratégie de mobilité d'entreprise personnalisée. Grâce à des plateformes comme MaaS360®, qui offrent une approche EMM souple, les entreprises peuvent exploiter des commandes SE et matérielles natives, la conteneurisation des données, l'évolutivité dans le cloud, et adopter en toute confiance les systèmes Android.

Les entreprises autorisent les employés à utiliser des dispositifs personnels ou spécialisés, mais les services informatiques restent confrontés aux enjeux importants de la protection des données et de la normalisation de la gestion.

Android est presque partout : adaptations et retombées

Avec 84 % de part de marché des dispositifs mobiles dans le monde[1], Android est le cœur de centaines de millions d'appareils mobiles, pour le travail et les loisirs, dans plus de 190 pays. Il constitue la plus vaste base installée de toutes les plateformes mobiles... et sa croissance continue. La riche variété des dispositifs Android disponibles implique qu'ils sont souvent bien adaptés aux programmes d'équipement des entreprises. Par exemple, de nombreux employés nomades ont besoin de dispositifs Android robustes et résistants à la poussière, aux chocs, aux vibrations, à la pluie, à l'humidité, au rayons du soleil, à l'altitude, et aux températures extrêmes. D'autres veulent des dispositifs Android ayant des fonctions de capture de données idéales pour le contrôle des inventaires et les opérations en entrepôt.

Cette croissance a des conséquences inattendues, avec d'importantes répercussions pour les services informatiques. Les entreprises autorisent les employés à utiliser des dispositifs personnels ou spécialisés, mais les services informatiques restent confrontés aux enjeux importants de la protection des données et de la normalisation de la gestion.

La plateforme mobile la plus utilisée dans le monde se caractérise aussi par un historique de sécurité fluctuant.[2] Cependant, les récentes versions d'Android aux noms très appétissants 4.0 (Ice Cream Sandwich, Jelly Bean et KitKat), 5.0 (Lollipop) et 6.0 (Marshmallow) ont comblé les failles de sécurité les plus importantes. Au niveau du système d'exploitation, Android 4.0 prend en charge l'encodage, une nouvelle structure publique en anneaux pour la gestion des authentifications, la protection contre les attaques sophistiquées, telles que les exploits en mémoire. Avec Android 5.0, de nombreuses fonctions de sécurité essentielles sont automatiquement activées pour les utilisateurs, dont le verrouillage de l'écran, l'encodage du dispositif, le gestionnaire de dispositif (qui facilite la recherche et la suppression des données à distance en cas de perte). Google a aussi commandé le mode d'application de Security Enhanced Linux (SELinux), qui limite les privilèges des applis et des utilisateurs, afin de prévenir des violations de la sécurité du système. Pour faciliter l'utilisation des appareils personnels dans les environnements professionnels (BYOD), un nouveau processus d'approvisionnement géré dans Android 5.0 crée un profil Travail protégé sur chaque dispositif. Dans l'assistant de démarrage, un badge de travail est affiché avec les applis pour indiquer qu'elles sont gérées avec leurs données dans le profil Travail par un administrateur de service informatique.

Les notifications pour les deux profils Travail et Personnel sont affichées dans une vue unifiée. Les données de chaque profil sont enregistrées séparément, même lorsque les deux profils utilisent la même appli.

En outre, Android 5.0 offre un mode Invité pour les téléphones et les tablettes. Ce mode vous permet de bloquer ou de contrôler des applis avec un code PIN afin qu'un utilisateur ne

puisse pas accéder à d'autres parties du dispositif. Cette excellente méthode autorise aussi l'accès à des applis en mode Kiosque sur des dispositifs mis en vente dans des magasins.

Android for Work

Il est évident que Google a effectivement écouté les réactions et les besoins des entreprises. Alors qu'il se prépare à lancer Android for Work, Google offre aux services informatiques l'option de la conteneurisation et des contrôles de sécurité pour les entreprises. Grâce à une nouvelle plateforme de gestion conçue pour l'entreprise, Android for Work permet aux services informatiques de :

- Séparer les données personnelles et professionnelles sur des smartphones Android
- Gérer et distribuer facilement des applis Google Play payantes et gratuites

Android for Work sera automatiquement intégré dans Lollipop et disponible sous forme d'appli pour tous les dispositifs Android 4.0 et versions ultérieures.

Fabricants : sécurité intégrée et intégration EMM

De nombreux grands fabricants de dispositifs Android, tels que Samsung, HTC, LG et Amazon, ont aussi mis en œuvre sur leurs modèles les plus récents, des protections spécifiques pour les entreprises. Grâce à des fonctions intégrées, telles que le formatage à distance des cartes SD, l'encodage de fichiers, la sécurité WLAN d'entreprise, l'accès VPN et le support simultané d'informations ouvertes et encodées sur un même dispositif, de nombreux dispositifs Android répondent mieux aux attentes des entreprises.

- Samsung KNOX offre un conteneur protégé qui permet à l'utilisateur de gérer, d'actualiser et de protéger les données de l'entreprise.
- Les dispositifs certifiés HTCpro offrent un chiffrement des données de classe Administration publique, avec l'accès VPN et d'autres fonctions de sécurité avancées.
- Les dispositifs Amazon Fire combinent le chiffrement, l'accès VPN, l'authentification unique et l'enregistrement de certificat.
- Les dispositifs LG GATE offrent une fonction de gestion de la sécurité avec support de Microsoft Exchange ActiveSync avancé, le chiffrement des données et l'accès VPN.

Ces quatre fabricants (et d'autres) de dispositifs Android ont non seulement mis en œuvre des caractéristiques de sécurité essentielles, mais ils ont aussi développé des partenariats avec des fournisseurs de solutions « Enterprise Mobility Management » (EMM) leaders du marché. Les API et les intégrations EMM permettent aux entreprises de profiter de caractéristiques de sécurité et de gestion robustes sur un seul portail.

Meilleures pratiques et fonctions

Compte tenu de l'importance des améliorations de sécurité apportées par les versions 3 et 4 d'Android, les services informatiques devraient exiger que tous les dispositifs passent sous Android 4.0 et versions ultérieures, et qu'ils soient protégés par mot de passe. Ceci réduit considérablement les « risques Android traditionnels » causés par la fragmentation et l'absence de chiffrement. Alors que la flexibilité d'Android génère un haut niveau de satisfaction dans les entreprises et chez les utilisateurs, avec certains des dispositifs les mieux adaptés aux besoins, elle se traduit aussi par un niveau d'exposition accru. Les services informatiques doivent donc protéger les données de l'entreprise et mettre en place des protections contre diverses menaces, dont les logiciels malveillants et le rootage.

Rootage risqué : Inacceptable pour les entreprises

Le rootage consiste à accéder au cœur UNIX d'un dispositif Android pour y installer quasiment n'importe quelle application, comme par exemple un logiciel malveillant, et modifier les contrôles des applis. Un dispositif « rooté » peut exposer le réseau de l'entreprise au logiciel malveillant qu'il contient et contourner les protections conçues pour éviter les pertes de données.

Perte de données : L'entreprise est dans votre poche

Vous souvenez-vous du bon vieux temps ? Le risque d'exposition était bien moindre avec un bon vieil ordinateur de bureau. De nos jours, le transfert des données entre différents équipements crée de nouvelles vulnérabilités. Les appareils avec des ports USB et des cartes SD amovibles peuvent facilement perdre des données, même si elles sont chiffrées. Les données transmises dans une zone Wi-Fi non protégée sont aussi exposées à des risques. Pour les entreprises, les pertes de données et les violations de sécurité peuvent entraîner des amendes très lourdes, mais aussi une perte de fidélité et de confiance des clients.

Logiciels malveillants : toujours dangereux, qu'ils soient introduits accidentellement ou intentionnellement.

Dans son rapport sur la sécurité des applis mobiles[3], Arxan Technologies, Inc. indique que 97 % des applis payantes Android et 80 % des applis Android gratuites les plus utilisées ont été piratées à un moment ou un autre. Comme les utilisateurs Android peuvent installer n'importe quelle appli provenant de n'importe quel point de vente en ligne (n'étant pas limité à Google Play), le pourcentage des applis qui contiennent un logiciel malveillant, ou une forme d'ingénierie sociale supportant une connexion à un logiciel malveillant, est nettement plus élevé que pour tout autre système d'exploitation mobile. Arxan constate aussi que les applis mobiles piratées se généralisent, puisque le nombre d'entreprises préférant l'innovation centrée sur des applis ne cesse d'augmenter et que de plus en plus d'employés utilisent la technologie mobile.

Même des applis considérées comme inoffensives dans Google Play Store peuvent faire des ravages sur votre réseau et votre marque, provoquant des pertes de chiffre d'affaires potentielles, des accès non autorisés à des données critiques, des vols de propriété intellectuelle, des fraudes et une dégradation de l'expérience utilisateur. Par exemple, si votre enfant prend votre téléphone et télécharge le jeu Temple Run, son code peut accéder à votre système de fichiers racines, télécharge le cache ou même le contenu de la carte SD se trouvant dans votre téléphone. Il peut aussi enregistrer les signaux audio sur le microphone de l'appareil et suivre votre position géographique. Le produit IBM® MaaS360® App Risk Management permet de voir toutes ces informations sur la sécurité (dans le genre mauvaise surprise...) liées à Temple Run.

Pour éviter de telles vulnérabilités, les services informatiques ont besoin de connaître les logiciels qui ont été installés, de détecter les logiciels malveillants et les dispositifs ciblés par une opération de routage, de procéder à une mise en liste noire et de faire appliquer les règles de conformité, selon les besoins.

Comment approcher EMM dans un environnement Android

Que les appareils appartiennent à l'entreprise ou aux employés, de nombreux services informatiques gèrent plus d'un type de dispositifs, de nombreuses applis et probablement plus d'un système d'exploitation.

L'une des meilleures pratiques à adopter pour l'EMM : personnaliser pour adapter les utilisations à vos politiques de la sécurité et de l'environnement.

Les services informatiques doivent adapter la taille des investissements en gestion de mobilité en fonction des classes d'utilisateurs, services, territoires, dispositifs et applis, et appliquer une approche technologique profilée selon les besoins des différents cas d'utilisation. Par exemple, les commerciaux ont besoin d'accéder aux coordonnées des clients et aux données des produits. Par contre, les ressources humaines (RH) ont accès à des données nettement plus sensibles, présentant des risques de conformité en cas de violation. L'EMM n'offre pas de taille universelle et n'est pas égalitaire.

MaaS360 peut vous aider à satisfaire votre désir de pâtisseries fines Android

En tant que partenaire technologique, IBM collabore étroitement avec Google et divers fabricants, comme Samsung, pour garantir que les clients profitent au maximum de leur expérience Android. MaaS360 est directement intégré à Samsung KNOX et à Android for Work. Avec MaaS360, vous pouvez bénéficier d'une expérience cohérente et robuste en gérant vos différents dispositifs sur plusieurs plateformes.

En travaillant avec des fonctions Google, les fabricants de dispositifs et MaaS360, les services informatiques ont accès à une gamme étendue d'options de sécurité mobile et à une plateforme unifiée pour développer, gérer et faire évoluer un programme de sécurité multi-couche. Avec MaaS360, vous pouvez déployer uniquement ce dont vous avez besoin, choisir des solutions individuelles qui vous permettront de protéger votre environnement mobile, avec les contrôles spécifiques que vous souhaitez utiliser dans cet environnement.

MaaS360	Utilisation
IBM® MaaS360® Mobile Device Management Les caractéristiques dont vous avez besoin pendant le cycle de vie de vos dispositifs	• Contrôler les accès et mettre en quarantaine des dispositifs spécifiques ou des versions SE Android à la demande • Protéger les données en transit avec des codes d'accès, des règles de protection géographiques, et une gestion contextuelle • Détecter et restreindre les dispositifs « rootés » • Localisez, verrouillez et nettoyez à distance les terminaux perdus ou volés
IBM® MaaS360® Mobile Application Management Mise en œuvre de l'entreprise mobile intelligente	• Protection des applis de l'entreprise avec la conteneurisation • Gestion des applis mobiles avec une console centrale basée sur Internet • Identifier les applis requises, mettre des applis sur liste blanche/noire afin de bloquer les fuites de données et les attaques du réseau
IBM® MaaS360® Productivity Suite Une protection de classe mondiale à des niveaux individuels	• Séparation des données professionnelles et personnelles • Définir des politiques profilées au niveau des utilisateurs • Appliquez des contrôles de conformité en ligne et hors ligne • Effacez des conteneurs de suite, des conteneurs d'applis, des profils d'entreprises ou tous les contenus de dispositifs ciblés
IBM® MaaS360® Content Suite Collaboration sous contrôle	• Gérer à partir d'un point central la distribution documentaire, ou créer un accès protégé aux ressources de fichiers existantes de l'entreprise, tels que SharePoint, Windows File Share, IBM Connections, Box, Google Drive, sources CMIS et bien d'autres. • Permettre aux utilisateurs de voir, créer, modifier, enregistrer des documents, en toute sécurité, dans un conteneur encodé sur des dispositifs Android. • Synchroniser des contenus sur plusieurs types de dispositifs, dont iOS, Android et Windows.
IBM® MaaS360® Gateway Suite Protégez vos accès	• Accès protégés aux données d'entreprise avec des dispositifs mobiles sans utiliser de VPN • Utilisation de SharePoint, du partage de fichiers Windows et de vos sites intranet • Utilisation des tunnels VPN intégrés dans les applis pour accéder aux systèmes de votre entreprise

MaaS360	Utilisation
IBM® MaaS360® Mobile Threat Management Éliminer les attaques par anticipation.	• Détecter les applis contenant des signatures de logiciels malveillants avec une base de données constamment mise à jour. • Mettre en œuvre un moteur de règles de conformité en temps quasi-réel pour automatiser la résolution de problèmes. • Découvrir les tentatives de masquage des dispositifs « rootés » par des pirates.
MasS360 App Risk Management Permet d'éliminer des risques auxquels vos applis sont exposées	• Identifier des centaines de vulnérabilités dans le code et des comportements applicatifs dangereux grâce à des analyses en profondeur et automatisées. • Concevoir et tester des règles d'applis avant leur déploiement dans les business units, les territoires ou les groupes de travail. • Appliquer des politiques de sécurité sur des dispositifs d'utilisateurs et des magasins d'applis pour entreprises.

Android est officiellement prêt pour l'entreprise. Alors, contactez-nous sans attendre pour en savoir plus sur MaaS360 et préparer votre entreprise pour Android. Protégez vos données d'entreprise et donnez à vos utilisateurs un accès transparent à des informations professionnelles sur leur dispositif. Profitez de politiques unifiées, de gestion des menaces, de distribution des applis, de gestion des dispositifs et une infrastructure standard pour bénéficier d'une expérience cohérente sur une grande variété de dispositifs Android. Pour bénéficier tout de suite d'un essai gratuit de 30 jours d'IBM MaaS360, rendez-vous sur : **ibm.com**/maas360.

A propos de 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

1 « Les expéditions de smartphones ont approché 300 millions d'unités au deuxième trimestre. Les dispositifs Android et iOS représentent 96 % du marché global, d'après IDC », IDC Worldwide Mobile Phone Tracker, 14 août 2014 (paywall) http://www.businesswire.com/news/home/20140814005599/en/Worldwide-Smartphone-Shipments-Edge-300-Million-Units

2 Ibid, 2014.

3 « State of Mobile App Security (recherche), Apps Under Attack, Vol. 3 (Bilan de la sécurité des applis mobiles, les applis sont ciblées) (titre précédent : State of Security in the App Economy (Bilan sur la sécurité du marché des applis) », 17 novembre 2014, Arxan Technologies, Inc., https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

Compagnie IBM France
17, avenue de l'Europe
92275 BOIS COLOMBES CEDEX

Produit aux Etats-Unis Mars 2016

Pensez à recycler

WGW03108-FRFR-01