Android vs iOS en entreprise : qui gagne ?

Présentation

Leader en entreprise, iOS n'est pas le seul choix. Et si Apple continue, année après année, de faire progresser son système d'exploitation mobile en réponse aux besoins des entreprises, Google n'est pas en reste.

Android avance régulièrement dans la même direction, profitant notamment des apports de Knox de Samsung.

Et s'il reste miné par la fragmentation de son écosystème, il dispose de nombreux arguments pour séduire. A commencer, justement, par le choix qu'il offre en matière de terminaux à des prix des variés.

De quoi convaincre, pour les applications métiers ou encore les environnements où s'imposent des appareils durcis par exemple.

LeMagIT a donc réalisé ce guide pour vous aider à choisir, en abordant des questions clés telles que les différences fonctionnelles entre les deux plateformes, la protection des données et la distribution des applications, mais également quelques retours d'expériences concrètes.

• Valéry Marchive

Android 5.0 vs iOS 8 : quel OS est le plus adapté à l'entreprise ?

De nombreuses DSI préfèrent iOS à Android en raison de l'ouverture de ce dernier, qui le rend plus susceptible d'être pris pour cible par des logiciels malveillants et des attaques. Mais cela ne signifie pas que la compétition entre les deux environnements mobiles soit terminée.

Les DSI peuvent ne pas tout apprécier dans iOS 8, mais au moins offre-t-il un unique environnement d'exploitation mobile homogène. Un atout non négligeable pour les DSI, en termes d'administration.

Mais Google a travaillé avec détermination à répondre aux préoccupations des services informatiques en matière de sécurité et d'administration d'Android. Android 5.0 Lollipop est le fruit de ces efforts. Peut-être de quoi amener les DSI à changer progressivement leur regard sur le système d'exploitation mobile de Google.

Les DSI adorent l'uniformité

Apple peut compter sur la vaste population d'utilisateurs étant passés à iOS 8. C'est le cas de plus de 80 % d'entre eux à ce jour : cela constitue une base installée uniforme de terminaux signés Apple à activer, provisionner, administrer et superviser. En comparaison, seulement des 3,3 % des smartphones et des tablettes Android sont sous Android 5.0. Et la disponibilité relativement limitée de terminaux compatibles devrait retarder sa progression.

Où cette situation trouve-t-elle son origine ? Chez Samsung, HTC, Motorola, LG et autres constructeurs qui apportent généralement leurs propres modifications à l'OS de Google avant de rendre disponible un nouveau firmware. Et il n'est pas rare que ces constructeurs bloquent de manière permanente certains modèles sur une unique version d'Android.

Tout cela signifie que la DSI n'a pas à administrer qu'une seule version d'Android, comme avec iOS ; elle doit composer avec des dizaines de smartphones qui exploitent différentes versions – sinon variantes – d'Android.

Le lancement d'Android for Work a légèrement amélioré la situation en créant un environnement administré en conteneur pour les applications d'entreprise, qui offre les mêmes capacités d'administration pour tous les terminaux compatibles.

Mais Android for Work n'est natif que pour Android 5.0.

Sur les anciens terminaux restés sur Android 4.0 ou 4, il doit être installé comme une application.

Mais même si un terminal exécute Android 5.0, la DSI doit encore composer avec les capacités matérielles spécifiques des terminaux : certains ne supportent pas Android for Work du fait de l'absence de capacités de chiffrement matériel.

Contrôle et automatisation

Apple, de son côté, travaille avec les DSI depuis l'introduction d'interfaces de MDM natives dans iOS 4, leur offrant le contrôle sans fil de leurs iPhones et iPads.

Ces API de MDM continuent de gagner en profondeur, étendue et maturité, et de nombreux produits de MDM tiers peuvent enrôler et configurer des terminaux iOS 8 et leurs applications.

De la même manière, le programme d'enrôlement de terminaux (DEP, *Device Enrollment Programm*) d'Apple permet d'automatiser l'enrôlement et la configuration de terminaux iOS achetés par l'entreprise. Le DEP d'Apple permet également d'empêcher les utilisateurs de supprimer des contrôles MDM pré-installés.

Les appareils personnels, utilisés dans le cadre d'un programme de BYOD, ne peuvent être enrôlés qu'avec l'accord de leurs propriétaires, mais les DSI peuvent néanmoins bien maîtriser le cycle de vie des terminaux iOS 8.

Avec Android 5.0, Google essaie de rattraper son retard, en ajoutant des API de MDM permettant le contrôle à distance par des outils de MDM tiers, via l'application Device Policy Client. Les services de MDM tiers sont disponibles depuis longtemps pour les terminaux Android, mais Google ne fournissait pas suffisamment d'API d'administration pour qu'ils s'avèrent réellement efficaces.

Avec Android for Work, Google a rendu possible pour un éventail limité mais croissant de produits de MDM tiers d'enrôler et de configurer en masse des profils Work.

Ceux-ci sont utilisés par les DSI pour gérer les conteneurs chiffrés abritant les données et applications métiers. Contrairement aux capacités MDM natives d'iOS, ces conteneurs sont visuellement et virtuellement

séparés de tout ce qui se trouve sur le terminal : la démarcation est claire entre éléments professionnels et personnels.

Les entreprise ne voulant pas d'outils de MDM tiers peuvent adminsitrer les appareils iOS 8 et Android 5.0 avec Exchange Active Sync (AES) de Microsoft – toutefois, les DSI doivent prendre là gare aux spécificités apportées à Android par les constructeurs ; elles sont susceptibles de compliquer l'administration via AES.

Apple continue en outre de supporter son outil autonome Apple Configurator pour administrer de petits ensembles d'iPhone et iPad. De la même manière, Google propose Android Device Manager et Google for Work.

Qui plus est, de nombreux constructeurs d'appareils Android proposent leurs propres services d'administration, à commencer par Samsung avec Knox. Toutefois, les entreprises qui veulent Android for Work doivent de doter d'une solution de MDM tierce et suivre un processus d'enrôlement en ligne auprès de Google ; le tout implique de modifier leur site Web ou leurs réglages DNS pour faire la démonstration de la propriété du nom de domaine.

Administrer les applications sur iOS et Android

Alors que les smartphones et les tablettes deviennent plus répandus, les DSI ne doivent plus simplement contrôler les terminaux mobiles, mais aussi chercher à en profiter pour industrialiser leurs processus métiers. La gestion des applications mobiles (MAM) joue là un rôle critique, aidant les DSI à déployer, superviser et supporter les applications recommandées ou supportées par l'entreprise.

Apple a jouté le support natif du MAM à iOS depuis sa version 4 ; de quoi disposer d'une sérieuse avance face à Google.

Avec les API d'iOS et service MAM tiers, les DSI peuvent déployer en toute sécurité des applications de l'Apple Store et des applications internes. Le programme d'achat en volume peut là encore aider, en permettant aux entreprises d'acheter et d'administrer des flottes de licences applicatives pour leurs terminaux mobiles.

En outre, les profils applicatifs permettent de provisionner les applications. iOS 8 supporte en outre des

réseaux privés virtuels par application, renforçant ainsi le contrôle des accès réseau.

Il existe déjà des produits de MAM pour Android. Mais Android for Work ajoute des capacités de MAM natives. De quoi permettre aux DSI de contrôler les applications déployées dans le conteneur Android for Work : les utilisateurs ne peuvent pas installer leurs propres applications non administrées dans le conteneur.

En outre, Google Play for Work permet aux DSI de créer leur propre magasin applicatif et d'identifier les applications du Play Store a installer automatiquement sur les terminaux des utilisateurs.

Android for Work intègre également des applications de productivité et de gestion des comptes à privilèges, afin d'aider à superviser et à protéger ces comptes sensibles. Enfin, Android for Work permet aux DSI de configurer les applications, jusqu'à définir des règles relatives à l'utilisation de VPNs d'entreprise.

Conclusion : une différence de moins en moins tranchée

En définitive, la différence entre iOS 8 et Android 5.0, pour l'entreprise, n'est pas aussi tranchée qu'avec les versions antérieures. Android 5.0 montre que Google avance dans la bonne direction et répond aux attentes des DSI, tout en restant en retard sur iOS.

Les DSI risquent donc encore de privilégier iOS, mais il est temps de commencer à appréhender Android comme une sérieuse alternative.

• Valéry Marchive

Tous les apports d'iOS 9 pour l'entreprise

Depuis la version 4.0 de son système d'exploitation mobile – appelé iPhone OS avant d'être rebaptisé iOS, Apple n'a cessé, à chaque nouvelle mouture, de multiplier les efforts à l'intention des entreprises. La version 7.0 s'était d'ailleurs montrée particulièrement pensée pour le monde professionnel, tout comme iOS 8 un an plus tard. Pour MobileIron, c'est bien simple : la « valeur d'iOS 9 est supérieure à celle de la somme de ses apports ».

Une administration simplifiée

Le nouvel opus d'iOS doit tout d'abord simplifier la déploiements d'applications en entreprise et la gestion des licences.

Il s'accompagne en effet d'une nouvelle version du programme d'achat en volume (VPP) qui autorise les DSI à décorréler les déploiements massifs d'applications des identifiants Apple des utilisateurs.

Le VPP permet d'acheter des applications iOS en volume pour les distribuer aux terminaux des utilisateurs. Jusqu'ici, les DSI ne pouvait affecter des applications qu'à l'Apple ID d'un utilisateur spécifique. Avec iOS 9, il devient possible d'attribuer des applications à des appareils précis sans le moindre lien avec les identifiants Apple.

Le contrôle de l'entreprise sur les appareils s'en trouve renforcé : les utilisateurs finaux ne peuvent pas, seuls, procéder au moindre changement ; même si leur terminal est associé à un identifiant Apple, les applications n'apparaîtront pas dans l'historique d'achat de celui-ci, puisqu'elles n'y sont associées.

Mais il y a une limite : les développeurs d'applications peuvent choisir d'autoriser ou non leur affectation par terminaux, dans le cadre du VPP.

Il est donc possible que tous ne le fassent pas.

En outre, Apple a ajouté la distribution de l'applications multinationale au VPP : les DSI vont pouvoir acheter une application dans un pays et la distribuer aux utilisateurs dans d'autres pays, à condition que cette application soit disponible dans l'App Store de ces pays.

Des terminaux mieux maîtrisés

Le programme d'enrôlement de terminaux (DEP)

d'Apple, qui permet aux organisations de configurer leurs terminaux iOS avant de les distribuer à leurs utilisateurs, est également rafraîchi à l'occasion d'iOS 9. Les DSI peuvent ainsi empêcher l'utilisation des appareils enrôlés jusqu'à ce que tous les réglages, les comptes et les restrictions soient effectivement configurés.

Ce changement devrait renforcer la sécurité : les utilisateurs ne pourront pas changer quoi que ce soit sur un terminal administré avant que les administrateurs n'aient fini de le configurer.

Surtout, les solutions de MDM (gestion des terminaux mobiles) vont permettre aux administrateurs de parcs de transformer des applications installées par les utilisateurs finaux en applications administrées par la DSI.

De nouveaux contrôles sont d'ailleurs accessibles aux outils de MDM pour, par exemple, restreindre le recours à la fonctionnalité de partage de contenus sans fil AirDrop, ou encore désactiver le téléchargement automatique d'applications, le support d'iCloud Photo Library, l'appairage avec une Apple Watch, les captures d'écran, ou encore l'utilisation de raccourcis clavier.

Parallèlement, iOS 9 apporte plusieurs dispositifs permettant de renforcer la sécurité des terminaux et de leurs applications, avec notamment le recours, par défaut, à un mot de passe à six chiffre au lieu de quatre.

Des applications plus sûres

Le chargement d'applications en dehors du magasin applicatif du constructeur doit aussi gagner en sûreté.

Ainsi, avec les versions antérieures d'iOS, l'iPhone ou l'iPad se contente de demander à l'utilisateur s'il souhaite faire confiance à un tiers qui n'est pas reconnu par Apple comme un développeur de confiance.

Avec iOS 9, l'utilisateur doit entreprendre d'aller dans les réglages de son appareil pour consulter les certificats suspects, et décider ou non de faire confiance aux développeurs ayant émis ces certificats.

L'utilisateur ne peut pas accorder sa confiance à un développeur non validé sans passer par cet écran, et iOS ne permet pas d'exécuter ses applications sans cela.

Les entreprises qui distribuent des applications développées en interne et poussées via un outil de MDM ne sont toutefois pas concernées.

Et activer l'accès à l'App Store n'est plus nécessaire pour pouvoir pousser des applications aux terminaux administrés.

Mais ce n'est pas tout. Apple a également prévu dans iOS 9 un dispositif permettant de renforcer la sécurité des communications entre applications mobiles et serveurs applicatifs. Baptisé App Transport Security, ce dispositif actif par défaut pour les applications iOS 9 et OS X 10.11, s'appuie sur TLS 1.2, des certificats signés avec SHA256 ou mieux et une clés RSA 2048 bits ou mieux, ou une clé ESS 256 bits ou plus. Apple détaille par ailleurs les 11 algorithmes de chiffrement qu'il accepte pour la liaison TLS.

A noter au passage que le support d'IPv6 est désormais obligatoire pour les applications distribuées via l'App Store.

Le système de micro-VPN applicatif introduit précédemment dans iOS a également été améliorés avec le support du trafic UDP, pour les flux audio et vidéo.

En outre, la connexion VPN était juste là conditionnée par la connexion réseau existante ; désormais, les outils d'EMM peuvent indiquer des routes réseaux ou des réglages DNS spécifiques pour ces connexions micro-VPN.

Des gains de productivité

Les utilisateurs et leurs outils de productivité n'ont pas été oubliés. Les fichiers PDF et graphiques en pièce jointes peuvent désormais être annotés dans le client de courrier électronique d'iOS, Mail, avant leur envoi. Et tous les types de pièces jointes sont désormais supportés – et non plus uniquement les images. Les utilisateurs peuvent enregistrer les pièces jointes reçus dans iCloud Drive… à moins que l'administrateur n'ait décidé de désactiver cette option.

iOS 9 supporte par ailleurs Exchange ActiveSync 16, avec à la clé une plus grande fiabilité, le support des pièces jointes et la possibilité de créer des invitations à des réunions depuis iOS.

Le nouvel opus de l'OS mobile d'Apple apporte en outre des capacités de recherche plus avancées et transparentes : en cas d'appel d'un numéro absent du carnet d'adresses, iOS peut chercher dans les correspondances électroniques pour trouver le contact correspondant et en afficher le nom.

Enfin, iOS 9 introduit de nouvelles capacités de multi-tâche pour les iPad. La première, dite Slide Over, permet d'ouvrir une seconde application sans quitter celle que l'on utilise, pour ensuite revenir rapidement à la première.

La seconde fonction, Split View, permet d'aller plus loin et d'avoir deux applications ouvertes et actives à l'écran en même temps. Slide Over est accessible à partir de l'iPad Air et de l'iPad mini 2. Split View n'est disponible que sur les iPad Pro, Air 2 et mini 4.

Mais c'est peut-être sur l'iPad Pro que Split View sera le plus convaincant. Et tant pis si, au passage, la firme à la pomme brouille un peu plus les lignes entre tablette et ordinateur portable.

• Valéry Marchive

De nouveaux dispositifs de sécurité dans Android M

Android for Work n'aura pas profité d'un lifting à l'occasion de la conférence Google I/O 2015. Les plateformes de gestion de la mobilité d'entreprise devront donc continuer de se contenter de ce qui est offert depuis l'année en matière d'EMM avec Android. Mais Google a toutefois annoncé de nouveaux dispositifs de sécurité pour son système d'exploitation mobile.

Tout d'abord, le géant du Web a présenté Smart Lock Passwords, une fonction qui permet aux terminaux Android de stocker les noms d'utilisateur et mots de passe pour les applications. Cela signifie que les utilisateurs d'appareils Android n'auront plus à se souvenir que d'un seul mot de passe. De qui permettre l'adoption de mots de passe spécifiques aux applications plus complexes : « en intégrant Smart Lock for Passwords à votre application Android, vous pouvez authentifier automatiquement les utilisateurs avec les identifiants qu'ils ont enregistrés », explique ainsi Google dans un guide du développeur.

Smart Lock fait partie de la nouvelle Identity Platform de Google et sera intégré à la version 7.5 des services Google Play : il sera disponible sous la forme d'une mise à jour automatique pour les terminaux fonctionnant sous Android 2.3 et ultérieur. Plusieurs applications – dont Netflix et LinkedIn – le supporteront immédiatement, mais les développeurs vont probablement ajouter le support d'autres applications au fil du temps.

Mais Google a également annoncé qu'Android M, la toute dernière version de son système d'exploitation mobile, sera la première à supporter les capteurs d'empreintes digitales : les utilisateurs d'Android pourront utiliser leurs doigts pour déverrouiller leurs appareils, comme le font déjà ceux de certains appareils iOS. Les applications Android seront également capables d'utiliser les empreintes digitales pour certaines opérations comme l'autorisation d'achats.

Android intègrera également des contrôles plus fins côté utilisateurs pour la détermination des droits des applications en matière d'accès aux données.

Ce système d'exploitation mobile est conçu pour permettre aux utilisateurs de choisir à quelles données les applications tierces ont le droit d'accéder, en continu et non plus seulement au moment de l'installation et de manière définitive.

Le contrôles des permissions applicatives après installation est probablement l'évolution la plus significative en matière de sécurité pour Android : l'authentification par empreinte digitale reste d'une fiabilité discutable et certains utilisateurs pourront ne pas vouloir confier leurs mots de passe à Google.

Toutefois, les utilisateurs soucieux de la confidentialité de leurs données pourront toujours choisir de recourir à un gestionnaire de mots de passe tiers tel que Dashlane. Ce dernier supporte les capacités de reconnaissance d'empreintes digitales d'Android M et ses API d'authentification.

Ainsi, les utilisateurs de Dashlane pourront s'authentifier dans l'application avec leurs doigts, sans saisir de mot de passe.

• Valéry Marchive

BYOD : pourquoi opter pour une stratégie combinant iOS et Android

L'attrait d'une stratégie de BYOD est indéniable. Quelle entreprise souhaite obliger ses collaborateurs à transporter deux smartphones, dont l'un risque d'être perçu comme encombrant et difficile à utiliser ? Et pourquoi les entreprises devraient-elles réaliser d'importants investissements dans des appareils considérés comme inutiles par les utilisateurs ?

De la même manière, pourquoi dépenser de l'argent dans des abonnements de téléphonie mobile alors que les employés disposent déjà d'un vaste éventail d'appareils mobiles pour lesquels ils seraient heureux de recevoir un remboursement partiel ?

Le BYOD s'apparente à un véritable accord gagnant-gagnant, peut-être plus qu'aucun autre.

Mais les inconvénients du BYOD sont par ailleurs nombreux.

En laissant de côté la sécurité – tout en admettant que celle des données sensibles sur des terminaux personnels est un défi évident et bien documenté –, l'administration et le support arrivent en tête de liste. Alors comment réduire les coûts de support – et la perte de productivité résultant d'une indisponibilité durant une phase de résolution de problème – lorsque les utilisateurs peuvent utiliser leurs propres smartphones, tablettes et PC au bureau ?

Le groupe Farpoint recommande de longue date d'encadrer toutes les initiatives de mobilité avec un engagement profond en faveur des objectifs et des politiques internes, au nombre desquels la sécurité.

Mais l'élément technologique demande ici également une certaine attention, notamment en ce qui concerne le nombre et le type de terminaux BYOD autorisés.

Tout autoriser revient à créer un scénario dans lequel les équipes de sécurité et de support risquent d'être dépassées par le nombre de terminaux, et où les besoins en connaissances techniques, processus opérationnels, outils, services de support et de formation, vont au-delà du raisonnable.

D'où la recommandation de n'autoriser qu'un ensemble limité de terminaux – en relevant au passage que si BYOD se traduit par « venez avec votre propre appareil », cela ne signifie pas « venez avec n'importe

quel appareil » ni « venez avec n'importe quel appareil doté de n'importe quelle version de logiciel »…

De fait, chaque plateforme logicielle induit des coûts spécifiques en raison de ses capacités fonctionnelles d'administration et de support. Ce qui se traduit par des outils spécifiques d'administration des terminaux, des applications,et des données. Et plus les combinaisons sont nombreuses, plus la complexité est grande, ainsi que le risque d'erreur et les coûts.

La plupart des entreprises ont retenu Android et iOS comme plateformes par défaut pour leurs initiatives de BYOD, en raison de leur popularité auprès des consommateurs et de leur large adoption par les éditeurs de solutions d'administration de mobilité.

Ces deux facteurs valident à eux seuls le choix consistant à n'accepter qu'iOS et Android dans le cadre de la stratégie de BYOD.

Il est également tout à fait raisonnable de n'accepter que les plus récentes versions de systèmes d'exploitation mobiles, afin de minimiser les risques liés à des bugs ou des logiciels malveillants.

Des exploits significatifs ont été découverts pour les deux plateformes, mais chaque nouvelle version apporte son lot de correctifs renforçant fiabilité et sécurité, voire même performances.

Le support d'autres plateformes de BYOD – dont BlackBerry 7 et 10, ou encore Windows Phone 7 et Windows 8 – s'avère en revanche plus problématique. Certes, elles embarquent aussi des capacités de MDM.

Mais leur adoption est bien moindre dans l'industrie du MDM. Et leur support peut induire des coûts supplémentaires pour les entreprises.

La question est ici de savoir si Microsoft et BlackBerry offrent des capacités d'administration et de sécurité présentant un ratio coût/bénéfices favorable au point d'en justifier le support.

En outre, puisqu'il est plus que possible de supporter iOS et Android de manière sûre et économique, pourquoi s'encombrer de plateformes alternatives ?

Reste que de nouvelles technologies sont susceptibles, à terme, d'encourager justement à l'élargissement. La

virtualisation peut être ainsi une approche efficace de l'isolation et de la protection des données d'entreprise.

L'authentification multi-facteurs, via Bluetooth ou d'autres jetons matériels, peut renforcer la protection des terminaux mobiles. L'ouverture automatique de liens VPN, combinée avec le chiffrement en local, permet de sécuriser de bout en bout l'information et, peut-être, atteindre le Graal de la mobilité : confort, productivité, transparence, simplicité, et coûts de support réduits.

• Craig Mathias, Farpoint Group

AUTEURS

Lire aussi :

Le Guide Essentiel « MDM : un levier pour le BYOD »

Le document consulté provient du site www.lemagit.fr

Cyrille Chausson | *Rédacteur en Chef*

Valéry Marchive | *Journalistes*

Linda Koury | *Directeur Artistique*

Neva Maniscalco | *Designer*

TechTarget
22 rue Léon Jouhaux, 75010 Paris
www.techtarget.com