Spécial Mobilité: 3-La gestion des devices et des applications est transformée

La stratégie de gestion d'un parc d'appareils mobiles semblait naguère tracée. Il suffisait d'appliquer les méthodes éprouvées dans le monde du PC, en contrôlant globalement leurs mises à jour et leurs paramètres de sécurité. Ainsi naissaient les outils de **MDM** (*mobile device management*), qui avaient le mérite de supporter les parcs hétérogènes – iOS, Android, BlackBerry OS et autres Windows Phone.

La consumérisation rend l'approche traditionnelle caduque

Née en grande partie autour des smartphones et tablettes, la consumérisation de l'IT vient tout balayer. Les terminaux sont de plus en plus souvent personnels (cf. concept du BYOD, *bring your own device*). Et plus généralement, les utilisateurs sont habitués à une certaine liberté, qu'ils vivent au quotidien sur les 'App Stores' et autres Google Play. Ils veulent choisir leurs applications et les installer quand ils le souhaitent. Dès lors, difficile d'imposer l'installation d'un agent logiciel permettant à la DSI de contrôler entièrement leur smartphone ou leur tablette. « *Le MDM permet de modifier le système d'authentification ou de verrouiller la partie téléphone pour obliger l'utilisateur à passer par l'entreprise lorsqu'il veut ajouter des applications, ce qui est pas acceptable dans le cas d'une démarche BYOD* », affirme ainsi **François-Xavier Levy**, directeur technique d'Arkama, un intégrateur spécialisé dans la mobilité. Cela dépend toutefois des entreprises et des pays. « *Le MDM appliqué au BYOD n'est pas envisageable en Allemagne mais il est pratiqué par certaines entreprises françaises* », pondère ainsi **Rémy Mandon**, WebSphere France Country Leader chez IBM.

La gestion par les applications s'impose mais ne suffit pas

Pour autant, les entreprises souhaitent conserver la maîtrise de la sécurité et des mises à jour. Fort de ces constats, les outils de MAM (*mobile application management*) se concentrent sur la gestion des applications. Ils permettent de mettre en œuvre un magasin privé accueillant des logiciels spécifiques ou sur étagère, dont certains peuvent provenir d'un magasin public. « *On peut aussi spécifier les applications accessibles par l'employé et gérer l'aspect sécurité, notamment en imposant un niveau de version* », résume François-Xavier Levy. Pour la sécurité, chaque application est intégrée dans un package – baptisé bulle par les uns, micro-conteneur par les autres – qui gère l'authentification et le chiffrement des données, uniquement pour cette application.

Pour autant, il peut être utile de cumuler MAM et MDM afin de renforcer la sécurité. Ainsi, un agent MDM peu intrusif permettra d'identifier les terminaux et leurs propriétaires, et on pourra ainsi vérifier s'ils présentent un risque, par exemple s'ils ont été déverrouillés ('*jailbreakés*' ou '*rootés*'). En fonction de ces critères, les utilisateurs seront autorisés, ou pas, à installer telle ou telle application,

le MAM prenant ensuite le relais. « *Il est intéressant de séparer MAM et MDM car ils adressent des populations différentes. Le premier est géré par le développeur tandis que le second concerne plutôt la cellule sécurité* », explique François-Xavier Levy. D'ailleurs, dans certaines offres, le MAM est partiellement embarqué dans l'environnement de développement.

Partager les données non structurées en situation de mobilité

Un autre type de service,s né dans la sphère grand public, est demandé par les utilisateurs. Il s'agit des plates-formes de partage de fichiers de type Dropbox. Elles ont tout leur sens dans l'entreprise car elles permettent de partager des données non structurées (qui représentent 80 % des données de l'entreprise) et d'y accéder en situation de mobilité. « *Cela permet d'emmener les derniers contrats, les conditions tarifaires ou une documentation technique* », donne en exemple **Frédéric Puche**, responsable de l'offre mobilité chez SAP. Mais là encore, pas question pour les DSI de sacrifier la sécurité. La solution : déployer une plate-forme privée en mode SaaS ou '*on premise*'. On parle alors de MFM (*mobile file management*) ou de MCM (*mobile content management*). Dans certaines solutions, cette notion vient s'intégrer au MDM ou au MAM, notamment afin de gérer globalement des politiques de sécurité.

___
Auteur: *Thierry Lévy-Abégnoli* . – ***[A suivre]***
_____ *DOSSIER : Mobilité* __ *Autres articles à lire:* _____

- Spécial Mobilité : 1 – Des défis technologiques à la mesure des enjeux business
- Spécial Mobilité : 2 – Tous ces enjeux business qui pèsent sur la DSI…
- Spécial Mobilité: 3-La gestion des devices et des applications est transformée
- Spécial Mobilité : 4 – Le développement d'applications mobiles s'impose en multi-OS
- Spécial Mobilité : 5 – Gestion des applications mobiles : une offre pléthorique
- Spécial Mobilité : 6 – Applications mobiles multi-OS : les MEAP résolvent un casse-tête