Florian Bienvenu (Good Technology) : « Il est vain d'interdire l'usage des terminaux personnels en entreprise »

Good Technology propose des solutions de gestion et sécurisation des données mobiles. Notamment avec deux produits principaux : Good for Entreprise, qui gère l'*e-mail* et les PIM (*Personal Information Manager*, données propres à l'agenda, contacts, etc.), et Good Dynamics qui répond à tous les autres besoins à travers une offre SaaS (*Software as a service*). Si Enterprise répond depuis plusieurs années aux problématiques du BYOD (*Bring Your Own Device*), Dynamics se présente comme une extension qui permet de développer et déployer des applications, standard ou tierces et spécifiques aux métiers de l'entreprise, et une infrastructure de gestion de manière sécurisée.

Fort de cette expertise en matière de gestion des données mobiles, **Florian Bienvenu**, vice-président Europe du Sud et Centrale de Good Technology, revient pour *Silicon.fr* sur les enjeux pour les entreprises confrontées à l'usage grandissant des terminaux personnels à des fins professionnelles au sein des organisations.

La problématique du BYOD est-elle une réalité en Europe, en France notamment ?

En tant que responsable Europe du Sud et Centrale, je constate deux grandes tendances entre deux grands pays, la France et l'Allemagne, où il existe un petit décalage de maturité dans le concept d'embrasser le BYOD. En Allemagne, toutes les entreprises du top 30 ont un programme BYOD. En France, la moitié des sociétés du CAC40 ont un programme, mais elles cherchent avant tout à gérer les terminaux de l'entreprise, que ce soit des iPhone, iPad, ou Android, pas les terminaux personnels.

Or, la consumérisation est propre au fait que tout le monde veut utiliser ses propres terminaux au travail. Les salariés les amènent dans l'entreprise, qu'ils en aient le droit ou pas. Les données professionnelles se retrouvent sur les terminaux personnels, que les DSI le veuillent ou non. D'ailleurs, en France, 55 % des DSI utilisent leurs terminaux personnels pour les usages professionnels.

Dans ces conditions, est-il utile de lutter contre le phénomène ?

Certains le font via le *blacklisting* des applications interdites. Mais ce type de défense n'est plus valable car il y a toujours quelqu'un qui trouve la parade en proposant une application non encore référencée et donc pas bloquée. De plus, avoir une adoption forte d'applications mobiles pour optimiser la productivité est dans l'intérêt de l'entreprise. Donc, il est vain de chercher à l'interdire. Au mieux, cela réduit la productivité, au pire bloquer les *devices* risque de poser des problèmes d'accès aux données personnelles. Il faut s'interroger sur les solutions à mettre en place sans mettre en danger les données professionnelles, ni personnelles.

En quoi l'offre de Good Technologies se distingue-t-elle ?

Nous avons une approche différente de la plupart des offres qui misent sur la sécurisation du terminal. Car ce n'est pas en sécurisant le réseau qu'on protège les données. Une fois entrée dans le VPN, une application peut accéder à toutes les données du terminal. Nous privilégions donc la sécurité au niveau de l'application plutôt que du terminal *via* une approche par *container* (bac à sable). Ce qui rend chaque application hermétique de l'autre et rend impossible le copier-coller. Pour effacer les données à distance, on efface le *container*, pas l'ensemble des données du terminal.

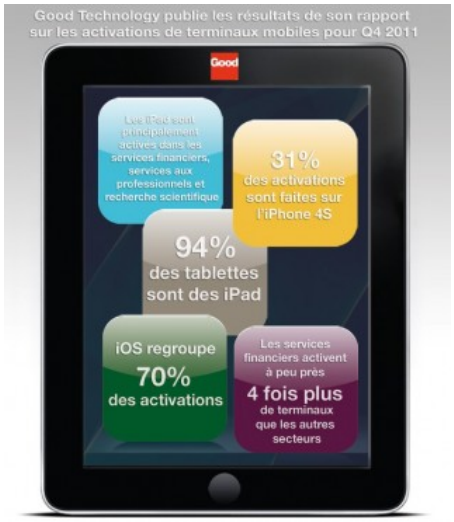
Notre architecture permet un transport sécurisé de bout en bout de la donnée et évite la connexion directe avec les données d'entreprise via notre NOC (*Network Operations Center*) *datacenter* qui assure le filtrage en « reconnaissant » le terminal, provisionné et non déverrouillé (*jailbreaké*) en vérifiant s'il dispose de la bonne version de la plate-forme, etc. Bref, que le terminal est conforme à la politique de sécurité de l'entreprise. Ensuite le *datacenter* fait la connexion entre le terminal et le réseau de l'entreprise depuis un lien bidirectionnel. La connexion sortante de bout en bout est chiffrée avec domaine de chiffrement de niveau militaire aux États-Unis, et bientôt en Europe.

Cette architecture n'impacte-t-elle pas les performances ? Et quels sont les risques si le datacenter est attaqué ?

Nous ne stockons aucune donnée sur le *datacenter* qui assure un rôle de transit uniquement. Il n'y a pas de latence, ou bien son impact reste mineur. Nous travaillons avec tous les *providers* les plus importants de la planète. Notre offre Good Dynamics ne fait que reprendre les politiques de sécurisation des *devices* de l'entreprise pour accéder à leur réseau. Enfin, il est possible de tester la solution en usage réel. Plus de 80 % des clients testent nos solutions sur un nombre réduit d'utilisateurs (généralement les VIP) avant de sauter le pas.

Quels sont les terminaux supportés par Good Technology ?

Nous couvrons toutes les plates-formes sauf BlackBerry. Ce sont certes des solutions reconnues sur le marché avec une architecture proche de la nôtre *(Balance, NDLR)*. Mais les entreprises cherchent à trouver une alternative à RIM (*Research in Motion*) aujourd'hui. Car les succès de l'iPhone et d'Android viennent de la richesse et de l'accès au catalogue applicatif. Or, les BlackBerry n'apportent pas suffisamment d'applications. On constate que, plutôt que de renouveler leur parc de terminaux BlackBerry, les entreprises regardent les autres solutions.



Pourtant, les BlackBerry sont plus présents en entreprises que les Windows Phone…

Il y a une vraie demande du marché sur Windows Phone. Notamment le Lumia de Nokia. Il est fort probable que les employés adhèrent à ces nouveaux *smartphones* qu'il faut certifier. Et ce n'est pas forcément lié à la capacité d'intégrer la plate-forme avec les applications de l'entreprise. D'autant que des partenaires développent des solutions qui permettent d'accéder à des applications type SharePoint de manière sécurisée quelle que soit la plate-forme.

Pour nous, la question est : *« Qu'est-ce que les utilisateurs adoptent ? »*, afin de prendre en compte la tendance du marché du BYOD. On constate en tout cas une grosse demande alternative à BlackBerry. L'iPhone reste le premier des *smartphones* activé, et Android connaît une grosse progression. Côté tablette l'iPad s'impose toujours. Android tourne autour de 5-6 % (voir infographie ci-contre).

Est-ce qu'il y a des terminaux plus sécurisés que d'autres ?

Nous ne regardons pas au niveau du terminal qui, avec nos solutions, convergent vers un même niveau de sécurité quelle que soit la plateforme. Nous nous assurons de pouvoir les certifier (au niveau de la combinaison terminal – opération téléphonique) et regardons si nous sommes capables de créer un environnement sécurisé sur le terminal. Par exemple, les premières versions de Windows Phone n'en étaient pas capables. Nous avons attendu que Microsoft sorte une version plus professionnelle de son OS pour certifier les Windows Phone. Nous n'utilisons pas les applications natives du *smartphone* et développons des clients complets pour chaque plate-forme.

Il n'en reste pas moins qu'il est toujours possible, pour le salarié, de se renvoyer par email un contenu professionnel vers une boîte personnelle…

Les risques de renvoi des données vers la messagerie personnelle sont réels. Et l'entreprise a un rôle pédagogique à jouer pour en expliquer les enjeux. Mais au-delà, si les employés font ce genre de démarche, c'est parce que l'employeur ne leur a pas donné les moyens de travailler dans de bonnes conditions. Le meilleur moyen de gérer les employés, c'est de leur donner une liberté totale d'accès aux applications de l'entreprise.

Propos recueillis le 7 février 2012.