Sécurité ou expérience utilisateur : faut-il vraiment choisir ?

Igexin, … autant de noms qui ont marqué les esprits ces derniers mois. Cette multiplication récente des cyberattaques de grande ampleur rappelle aux dirigeants, DSI et RSSI l'importance de l'enjeu sécuritaire, s'il en était besoin.

Dans un monde où le digital devient la norme, protéger les données exploitées en mobilité est essentiel. Pour ce faire, une méthode : **la conteneurisation**. Elle consiste à **isoler les données professionnelles des données personnelles sur le terminal mobile pour mieux les protéger**. Il existe aujourd'hui deux technologies, conteneur « propriétaire » ou « natif », chacune avec une approche différente.

La tentation de donner priorité absolue à la sécurité au détriment de l'expérience utilisateur est forte. Or, en matière de mobilité, une bonne expérience utilisateur est un facteur clé de succès essentiel. Alors comment faire le bon choix ?

Le conteneur propriétaire : la sécurité par la contrainte

Proposé par les éditeurs de solutions EMM/MAM, le conteneur propriétaire consiste en une surcouche applicative permettant d'**isoler et de chiffrer les données professionnelles** sur le terminal **pour les rendre inaccessibles**, même en cas de compromission de l'OS mobile (Root / Jailbreak).

Pour les équipes IT, le conteneur propriétaire est difficile à maintenir de par l'évolution rapide des OS mobiles, et impose des contraintes sur les technologies de développement.

Pour les collaborateurs, il **complexifie l'accès aux applications professionnelles** en créant une bulle professionnelle distincte de l'espace personnel sur le terminal, ce qui peut être rédhibitoire pour l'adoption des outils digitaux de l'entreprise !

Le conteneur natif OS : adhésion garantie !

Proposé par les éditeurs d'OS mobiles, le conteneur natif (iOS, Android et Windows 10) est intégré directement dans le système d'exploitation du terminal mobile. Il accède aux applications professionnelles en exploitant les applications natives du terminal (mail, navigateur, …). Avec cette technologie, **les utilisateurs conservent leurs habitudes quel que soit leur usage** (professionnel ou personnel). L'adoption des applications professionnelles est grandement favorisée !

Conscients de l'importance de l'expérience utilisateur, les éditeurs EMM/MAM (Vmware Airwatch, IBM MaaS360, MobileIron et Jamf) ont créé la communauté « AppConfig » pour promouvoir les technologies natives avec plusieurs éditeurs d'applications professionnelles (exemples : Salesforce 1, Box, Concur, …).

Nicolas Raison

Practice manager chez digital dimension, il est expert dans le domaine des OS et des infrastructures EMM. Il se passionne tout particulièrement pour les nouvelles technologies destinées à améliorer les usages en entreprise

Côté sécurité, le conteneur natif est souvent moins bien considéré que le conteneur propriétaire car il est plus **exposé à une faille du système d'exploitation du terminal**. Les technologies proposées par les éditeurs d'OS mobile ont pourtant largement progressé pour intégrer les besoins des entreprises : c'est le cas pour Apple depuis iOS 7, pour Google avec Android Enterprise depuis Marshmallow (6.0) et pour Windows avec WIP (Windows Information Protection).

On notera que **les conteneurs natifs ne peuvent exister sans les solutions EMM** qui permettent de piloter les politiques de conformité du système d'exploitation, mais surtout de réaliser des actions de remédiation en cas de compromission de l'OS mobile (exemple : effacement automatique des données professionnelles du terminal), élément indispensable d'une politique de sécurité.

La sécurité : encore plus fort !

Etant donné l'importance et la criticité de l'enjeu sécuritaire, des éditeurs spécialisés comme Checkpoint, Lookout ou Skycure vont aujourd'hui plus loin en proposant **des solutions de « MTD » (Mobile Threat Defense)**. Leur rôle : analyser le comportement des applications, des connexions réseau et de l'OS pour remonter des alertes en cas d'anomalie et ainsi permettre à l'entreprise d'agir.

Ces solutions très poussées apportent une vraie complémentarité aux technologies de conteneurisation. Elles sont particulièrement efficaces pour **prévenir les attaques ciblées et le risque d'espionnage**. Ces besoins ne concernent toutefois pas la totalité des entreprises.

Que retenir ?

Haut niveau de sécurité et expérience utilisateur de qualité ne sont pas contradictoires. Pour garantir le succès d'un projet, la DSI peut – et doit – concilier ces deux éléments.

Il n'y a toutefois pas de « bon choix », tant l'importance des critères à prendre en compte varie : exigences et résistance au changement des utilisateurs, besoins applicatifs des métiers, criticité des données exploitées sur les terminaux mobiles, importance de l'exposition au risque d'attaque, … A chaque entreprise sa réponse !