Cybersécurité : Quelles solutions pour vos mobiles ?

Mobilité

Posté par : JulieM

Publié le : 28/6/2021 13:00:00

Les cyberattaques sont de plus en plus fréquentes. Le télétravail et la mobilité permanente des collaborateurs sont devenus incontournables et exposent les entreprises à de nouveaux défis en termes de sécurité mobile. Dans ce contexte, 80 % des entreprises ont déjà subi des cyberattaques contre leurs systèmes.

Et pourtant, moins de 25 % des téléphones mobiles d'entreprise sont sécurisés alors que les terminaux mobiles font partie des principales causes de fuites de données informatiques d'entreprise. En ce sens, MDM, EMM, UEM, ou encore MTD sont autant de concepts souvent évoqués. Mais à quoi correspondent-ils exactement ?

Qu'est-ce qu'un MDM ?

Un MDM, Mobile Device Management permet la gestion technique de l'ensemble des appareils mobiles (smartphones, tablettes) à partir d'une même et seule plateforme. Lorsque l'on possède une flotte de nombreux terminaux mobiles, cet outil centralise la gestion de celle-ci et apporte un véritable gain de temps. Grâce à l'utilisation d'un MDM, il est possible de bénéficier d'une flotte de mobiles harmonisée.

Plus concrètement, un MDM permet d'optimiser le fonctionnement et la sécurité des appareils mobiles au sein de l'entreprise tout en protégeant le réseau de l'entreprise. Il permet de gérer les appareils à distance et de proscrire certaines actions par les utilisateurs.

L'effacement des données à distance en cas de vol ou de perte de l'appareil est ainsi possible avec ce type de logiciel. C'est l'outil nécessaire afin d'appliquer une politique de sécurité harmonisée sur l'ensemble des téléphones et d'effectuer une surveillance en temps réel des terminaux.

Le MDM s'avère être un véritable atout dans la mise en conformité du RGPD afin de protéger ses appareils mobiles professionnels ainsi que ses données d'entreprise. Les fonctionnalités d'un MDM ont pour domaines d'expertise l'approvisionnement et le regroupement des appareils, la sécurité des appareils et leurs localisations, ainsi que la surveillance de l'état de l'appareil.

Les EMM :

En réalité, le MDM est une catégorie de logiciels dont les fonctionnalités peuvent être regroupées au sein d'un EMM (Enterprise Mobility Management) avec d'autres catégories de logiciels.

L'EMM est la combinaison d'un MDM, d'un MAM et d'un MIM :

à MDM (Mobile Device Management) pour la gestion de terminaux mobiles et de leurs paramètres

à MAM (Mobile Application Management) pour les déploiements et mises à jour des applications

à MIM (Mobile Identity Management) pour la gestion des processus d'identification et

d'accès aux données

Il s'agit en fait d'une solution plus complète de gestion des terminaux mobiles d'entreprise, intégrant le MDM.

Et l'UEM, alors ?

L'UEM correspond à la gestion unifiée des points de terminaison, Unified Endpoint Management, en anglais. Plus simplement, l'UEM permet aux entreprises d'ouvrir la plateforme de gestion à un plus large éventail de périphériques tels que les ordinateurs portables, les mobiles, les tablettes, les PC, les appareils IoT, les imprimantes et les appareils portables à l'aide d'une seule solution EMM étendue.

Que ce soit l'UEM, l'EMM ou encore le MDM, ces logiciels facilitent la gestion et l'application de la stratégie de sécurité à distance et en masse d'une flotte mobile. En revanche, ils ne protègent pas directement des cybermenaces.

Qu'est-ce qu'un MTD ?

Les Mobile Threat Defense sont des solutions de protection poussées contre les cybermenaces sur les appareils mobiles. Le logiciel agit sur les appareils, sur les applications ainsi que sur les réseaux. Les solutions de Mobile Threat Defense permettent de sécuriser les connexions réseau et la limite du contenu en temps réel. Il est alors aisé d'identifier les anomalies pour garantir que toute activité malveillante soit bloquée de manière proactive sans nécessiter l'action de l'utilisateur.

Le MTD est un complément indispensable au MDM afin de pouvoir contrôler les usages professionnels des terminaux tout en laissant ses collaborateurs utiliser leurs mobiles pour des besoins personnels en toute sécurité. Un MTD est un allié indispensable dans le cas du BYOD.

Certaines entreprises permettent aux employés d'utiliser les terminaux mobiles personnels pour le travail. Cela implique d'être exposé à de plus nombreux dangers. Ainsi, les logiciels de type MTD apportent une solution efficace dans le cadre de cette pratique pour plus de sécurité.

Les solutions de sécurité MTD agissent au niveau du terminal en protection contre le phishing, identification des malwares mobiles basés sur l'analyse comportementale des applications et blocage de l'extraction de données sensibles. Il permet de réagir rapidement face à la menace et de déjouer les attaques avant qu'elles prennent de l'ampleur et engendrent des dégâts importants.

Pour conclure, il est possible de distinguer les solutions de gestion centralisée de son parc d'une part et les logiciels spécialisés dans la sécurité accrue des mobiles pour lutter contre les cyberattaques d'autre part. Ces deux solutions sont complémentaires pour avoir une sécurité mobile optimale.

Sébastien REVERDY, CEO de BetooBe