***CybersÃ©curitÃ© : Quelles solutions pour vos mobiles ?***
**MobilitÃ©**
PostÃ© par : JulieM
PubliÃ©e le : 28/6/2021 13:00:00

Les cyberattaques sont de plus en plus frÃ©quentes. Le tÃ©lÃ©travail et la mobilitÃ© permanente des collaborateurs sont devenus incontournables et exposent les entreprises Ã de nouveaux dÃ©fis en termes de sÃ©curitÃ© mobile. Dans ce contexte, 80 % des entreprises ont dÃ©jÃ subi des cyberattaques contre leurs systÃ¨mes.

Et pourtant, moins de 25 % des tÃ©lÃ©phones mobiles dâ□□entreprise sont sÃ©curisÃ©s alors que les terminaux mobiles font partie des principales causes de fuites de donnÃ©es informatiques dâ□□entreprise. En ce sens, MDM, EMM, UEM, ou encore MTD sont autant de concepts souvent Ã©voquÃ©s. Mais Ã quoi correspondent-ils exactement ?

## Quâ□□est-ce quâ□□un MDM ?

Un MDM, Mobile Device Management permet la gestion technique de lâ□□ensemble des appareils mobiles (smartphones, tablettes) Ã partir dâ□□une mÃªme et seule plateforme. Lorsque lâ□□on possÃ¨de une flotte de nombreux terminaux mobiles, cet outil centralise la gestion de celle-ci et apporte un vÃ©ritable gain de temps. GrÃ¢ce Ã lâ□□utilisation dâ□□un MDM, il est possible de bÃ©nÃ©ficier d'une flotte de mobiles harmonisÃ©e.

Plus concrÃ¨tement, un MDM permet dâ□□optimiser le fonctionnement et la sÃ©curitÃ© des appareils mobiles au sein de lâ□□entreprise tout en protÃ©geant le rÃ©seau de lâ□□entreprise. Il permet de gÃ©rer les appareils Ã distance et de proscrire certaines actions par les utilisateurs.

L'effacement des donnÃ©es Ã distance en cas de vol ou de perte de l'appareil est ainsi possible avec ce type de logiciel. C'est l'outil nÃ©cessaire afin d'appliquer une politique de sÃ©curitÃ© harmonisÃ©e sur l'ensemble des tÃ©lÃ©phones et d'effectuer une surveillance en temps rÃ©el des terminaux.

Le MDM s'avÃ¨re Ãªtre un vÃ©ritable atout dans la mise en conformitÃ© du RGPD afin de protÃ©ger ses appareils mobiles professionnels ainsi que ses donnÃ©es d'entreprise. Les fonctionnalitÃ©s d'un MDM ont pour domaines d'expertise l'approvisionnement et le regroupement des appareils, la sÃ©curitÃ© des appareils et leurs localisations, ainsi que la surveillance de l'Ã©tat de l'appareil.

## Les EMM :

En rÃ©alitÃ©, le MDM est une catÃ©gorie de logiciels dont les fonctionnalitÃ©s peuvent Ãªtre regroupÃ©es au sein d'un EMM (Enterprise Mobility Management) avec d'autres catÃ©gories de logiciels.

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

â□¢ MDM (Mobile Device Management) pour la gestion de terminaux mobiles et de leurs paramÃ¨tres
â□¢ MAM (Mobile Application Management) pour les dÃ©ploiements et mises Ã jour des applications
â□¢ MIM (Mobile Identity Management) pour la gestion des processus dâ□□identification et

dâ□□accÃ¨s aux donnÃ©es

Il sâ□□agit en fait dâ□□une solution plus complÃ¨te de gestion des terminaux mobiles dâ□□entreprise, intÃ©grant le MDM.

## Et l'UEM, alors ?

Lâ□□UEM correspond Ã  la gestion unifiÃ©e des points de terminaison, Unified Endpoint Management, en anglais. Plus simplement, l'UEM permet aux entreprises d'ouvrir la plateforme de gestion Ã  un plus large Ã©ventail de pÃ©riphÃ©riques tels que les ordinateurs portables, les mobiles, les tablettes, les PC, les appareils IoT, les imprimantes et les appareils portables Ã  l'aide dâ□□une seule solution EMM Ã©tendue.

Que ce soit l'UEM, l'EMM ou encore le MDM, ces logiciels facilitent la gestion et lâ□□application de la stratÃ©gie de sÃ©curitÃ© Ã  distance et en masse dâ□□une flotte mobile. En revanche, ils ne protÃ¨gent pas directement des cybermenaces.

## Qu'est-ce qu'un MTD ?

Les Mobile Threat Defense sont des solutions de protection poussÃ©e contre les cybermenaces sur les appareils mobiles. Le logiciel agit sur les appareils, sur les applications ainsi que sur les rÃ©seaux. Les solutions de Mobile Threat Defense permettent de sÃ©curiser les connexions rÃ©seau et la lÃ©gitimitÃ© du contenu en temps rÃ©el. Il est alors aisÃ© dâ□□identifier les anomalies pour garantir que toute activitÃ© malveillante soit bloquÃ©e de maniÃ¨re proactive sans nÃ©cessiter lâ□□action de lâ□□utilisateur.

Le MTD est un complÃ©ment indispensable au MDM afin de pouvoir contrÃ´ler les usages professionnels des terminaux tout en laissant ses collaborateurs utiliser leurs mobiles pour des besoins personnels en toute sÃ©rÃ©nitÃ©. Un MTD est un alliÃ© indispensable dans le cas du BYOD.

Certaines entreprises permettent aux employÃ©s dâ□□utiliser les terminaux mobiles personnels pour le travail. Cela implique d'Ãªtre exposÃ© Ã  de plus nombreux dangers. Ainsi, les logiciels de type MTD apportent une solution efficace dans le cadre de cette pratique pour plus de sÃ©rÃ©nitÃ©.

Les solutions de sÃ©curitÃ© MTD agissent au niveau du terminal en protection contre le phishing, identification des malwares mobiles basÃ©s sur lâ□□analyse comportementale des applications et blocage de lâ□□extraction de donnÃ©es sensibles. Il permet de rÃ©agir rapidement face Ã  la menace et de dÃ©jouer les attaques avant quâ□□elles prennent de lâ□□ampleur et engendrent des dÃ©gÃ¢ts importants.

Pour conclure, il est possible de distinguer les solutions de gestion centralisÃ©e de son parc dâ□□une part et les logiciels spÃ©cialisÃ©s dans la sÃ©curitÃ© accrue des mobiles pour lutter contre les cyberattaques dâ□□autre part. Ces deux solutions sont complÃ©mentaires pour avoir une sÃ©curitÃ© mobile optimale.

SÃ©bastien REVERDY, CEO de BetooBe