Lookout

MTD vs MDM vs MAM

Mobile Threat Defense | Mobile Device Management | Mobile App Management

Avec la montée en puissance du BYOD pour accéder aux données d'entreprise, de nombreuses entreprises déploient des solutions du type MDM et MAM en pensant que ces solutions sont suffisamment robustes pour protéger efficacement leurs données.

Les entreprises adoptent de plus en plus le MTD

MTD

200 %

« D'ici à 2020, 30 % des entreprises auront installé un MTD, **soit une augmentation de moins de 10 % par rapport à 2018.** »[2]
[Une augmentation de 200 %]

MDM

30 %

« Le déploiement de MDM avec EMM va **diminuer d'environ 30 % dans les entreprises au cours des 12 à 18 prochains mois.** »[1]

MAM

10 %

« Le déploiement de solutions MAM et MCM via un EMM va **diminuer d'environ 10 % dans les entreprises au cours des 12 à 18 prochains mois.** »[1]

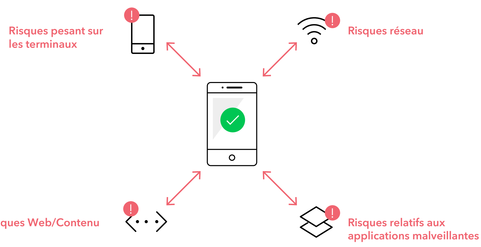
Guide pour identifier les carences de sécurité dans la gestion mobile

Ce guide compare les fonctionnalités de cybersécurité du MTD, du MDM et du MAM par rapport au spectre des risques mobiles. Les failles dans la gestion mobile démontrent les vulnérabilités d'un système que les entreprises doivent améliorer pour renforcer la sécurité de leurs terminaux mobile.

Les composantes du risque	MTD	MDM	MAM
Menaces Web & Contenu *Ouverture d'URL malveillantes provenant d'un e-mail, d'un SMS, d'un navigateur et d'une application de réseau social. Ces URL peuvent orienter les utilisateurs vers des sites Web se faisant passer pour les pages de connexion d'un site officiel.* *D'autres sites Web peuvent ne pas chiffrer leurs identifiants de connexion ou peuvent dévoiler des données.*	RÉPOND AUX EXIGENCES Lookout protège vos e-mails, SMS, navigateurs et applications contre le phishing. Lookout inspecte en temps réel toutes les connexions sortantes de votre terminal mobile au niveau du réseau.	AUCUNE SOLUTION Le MDM ne fournit aucune protection contre le phishing.	AUCUNE SOLUTION Le MAM ne fournit aucune protection contre le phishing.
Menaces applicatives *Applications malveillantes pouvant dérober des informations, divulguer des données, obtenir un accès à distance non autorisé à d'autres systèmes et même détériorer des terminaux.* *Sont également concernées les applications non malveillantes présentant des vulnérabilités intrinsèque, telles que leur capacité à divulguer des coordonnées.*	RÉPOND AUX EXIGENCES Grâce à un corpus de données de plus de 90 millions d'applications, Lookout identifie les applications susceptibles d'exfiltrer les données d'une entreprise ainsi que les applications malveillantes, en analysant leur réputation et leur code.	AUCUNE SOLUTION Le MDM n'est pas capable de détecter des applications malveillantes ou vulnérables.	AUCUNE SOLUTION Le MAM n'est pas capable de détecter des applications malveillantes ou vulnérables.
Menaces pesant sur les terminaux *Menaces exploitant les vulnérabilités d'un système d'exploitation pour obtenir des autorisations supplémentaires. Ces attaques peuvent être particulièrement efficaces pendant la fenêtre de vulnérabilité entre l'installation de mises à niveau et de correctifs au niveau du système d'exploitation.* *Les applications sideloadées peuvent aussi être des vecteurs de menaces pour les terminaux.*	RÉPOND AUX EXIGENCES Pour assurer une protection contre les terminaux jailbreakés/rootés, les systèmes d'exploitation obsolètes et les configurations de terminaux à risque, Lookout recourt à la détection d'anomalies comportementales en suivant des modèles d'utilisation reconnaissables.	SOLUTION PARTIELLE Les solutions MDM ne peuvent pas détecter des roots/jailbreaks en temps réel. Elles incitent plutôt à télécharger des mises à jour logicielles pour gérer toute menace, laissant ainsi une fenêtre de vulnérabilité ouverte aux attaques.	AUCUNE SOLUTION MAM n'est pas capable de détecter les menaces pesant sur les terminaux.
Menaces réseau *Menaces exploitant les vulnérabilités de sites Web ou d'applications lors de l'établissement de sessions TLS/SSL sur les réseaux Wi-Fi, mobiles ou autres.*	RÉPOND AUX EXIGENCES Lookout peut détecter des réseaux à risque et fournir une protection contre les attaques man-in-the-middle, les usurpations de certificats, le TLS/SSL stripping ou les versions inférieures de suites cryptographiques TLS/ SSL.	AUCUNE SOLUTION Le MDM n'est pas capable de détecter des menaces réseau.	AUCUNE SOLUTION Le MAM n'est pas capable de détecter des menaces réseau.
Correction des menaces *Correction immédiate des menaces sur un terminal mobile pour garantir son utilisation continue et sécurisée et son accès aux ressources de l'entreprise.*	RÉPOND AUX EXIGENCES Lors de la détection d'une menace, Lookout suggère aux utilisateurs de la corriger eux-mêmes. Les utilisateurs peuvent ainsi résoudre 95 % des menaces eux-mêmes.	SOLUTION PARTIELLE Aucune détection ou correction automatique des attaques. Toutefois, le MDM peut effacer le contenu d'un terminal en cas d'une attaque de haute importance. Nécessite une solution MTD pour identifier les attaques.	SOLUTION PARTIELLE Aucune détection ou correction des menaces. MAM peut restreindre/supprimer une application suite à la détection de son infection. Nécessite une solution MTD pour lui envoyer des informations concernant le niveau de risque d'une application.
Accès conditionnel *Les terminaux mobiles présentant des risques élevés essaient d'accéder aux ressources d'entreprises. Les terminaux contenant des logiciels malveillants, des vulnérabilités ou ayant ont été rootés sont généralement considérés comme étant particulièrement à risque.*	RÉPOND AUX EXIGENCES Lookout Continuous Conditional Access surveille la santé de votre terminal, lui assigne un niveau de risque et transmet ces informations à l'entreprise pour valider l'authentification.	SOLUTION PARTIELLE Grâce à une solution de MTD, le MDM peut mettre en place des politiques empêchant l'accès. Le MDM peut empêcher l'accès d'un mobile dont le système d'exploitation est obsolète et exiger la saisie d'un mot de passe sur le terminal.	SOLUTION PARTIELLE La solution MTD va permettre au MAM de mettre en place des politiques pour empêcher l'authentification des applications en cas de détection de risque avéré. MAM peut également empêcher tout accès basé sur des versions d'applications obsolètes.
Respect de la vie privée des utilisateurs *Protection de la vie privée des utilisateurs et respect des réglementations en termes de protection de la vie privée dans différents secteurs.*	RÉPOND AUX EXIGENCES Une adresse e-mail suffit pour configurer Lookout et aucune localisation GPS n'est utilisée. Lookout fournit aussi un mode de confidentialité avancé pour supprimer toute information utilisateur inutile.	AUCUNE SOLUTION De nombreux outils MDM permettent aux employeurs de surveiller en permanence toutes les activités des terminaux, y compris les appels personnels et le trafic Web. Mode de confidentialité indisponible.	SOLUTION PARTIELLE En tant que solution autonome, MAM gère uniquement les applications requises par l'employeur et limite l'utilisation des informations concernant les utilisateurs. Cependant, de nombreuses solutions MAM sont déployées avec MDM.
Notification d'attaque *Surveillance permanente et notification des événements de cybersécurité.*	RÉPOND AUX EXIGENCES Lors de la détection d'une attaque mobile, Lookout en informe immédiatement l'administrateur et les personnes concernées.	AUCUNE SOLUTION Ne peut pas détecter des attaques sur mobile	AUCUNE SOLUTION Ne peut pas détecter des attaques sur mobile

Le MTD protège les entreprises contre les différents vecteurs d'attaques

Les solutions MDM et MAM ne fournissent aucune détection ou protection contre les attaques ou les comportements à risques de leurs utilisateurs. En revanche, ces outils de « gestion » peuvent appliquer des politiques et procédures pour administrer et gérer les terminaux mobiles utilisés au sein d'une entreprise. Pour assurer une protection contre les attaques mobiles, une solution MTD devra être installée pour détecter et bloquer toute menace afin de protéger l'entreprise. Cependant, il est judicieux d'intégrer une solution MTD avec une solution MDM et/ou MAM, car ces outils de gestion pourront appliquer des politiques basées sur des informations relatives aux menaces.



Pour en savoir plus, rendez-vous sur lookout.com/fr

Lookout

1. Hochmuch, Phil. 2018 Enterprise Mobility Decision Maker Survey: Software, Management and Security Highlights. IDC. 2018 (MCM = Mobile Content Management)

2. Zumerle, Dionisio and Girard, John. 2018 Gartner Market Guide for Mobile Threat Defense. IDC. 2018