Lookout

MTD vs. MDM vs. MAM

Mobile Threat Defense | Mobile Device Management | Mobile App Management

Seitdem immer öfter über Mobilgeräte auf sensible Unternehmensdaten zugegriffen wird, setzen die verantwortlichen Abteilungen MDM- und MAM-Lösungen in der Hoffnung ein, dass diese ihre Unternehmen in der Cloud vor Cybersicherheitsbedrohungen schützen können.

Unternehmen setzen zunehmend auf MTD

MTD

200%

„Bis 2020 werden 30 % der Unternehmen MTD nutzen – **im Vergleich zu den weniger als 10 % im Jahr 2018 ein deutlicher Anstieg.**"[2]
[Ein Anstieg von 200 %]

MDM

30%

„Die Bereitstellung von MDM mit EMM verliert an Attraktivität – **in den nächsten 12-18 Monaten wird die Zahl der Unternehmen mit einem solchen Plan um ca. 30 % zurückgehen.**"[1]

MAM

10%

„Die Bereitstellung von MDM und MCM mit EMM verliert an Attraktivität – **in den nächsten 12-18 Monaten wird die Zahl der Unternehmen mit einem solchen Plan um ca. 10 % zurückgehen.**"[1]

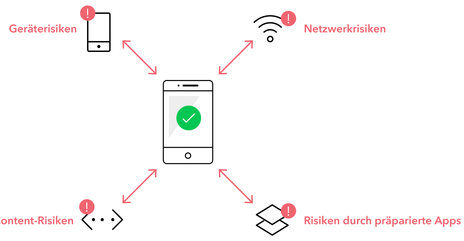
Übersicht zur Aufdeckung von Sicherheitslücken beim Mobilgeräte-Management

Diese Übersicht stellt die Cybersicherheitsfunktionen von MTD, MDM und MAM dem Spektrum an Mobilitätsrisiken gegenüber. Unter Sicherheitslücken beim Mobilgeräte-Management sind potenzielle Systemschwachstellen zu verstehen, die Unternehmen angehen sollten, um ihre Mobilgeräteflotten besser zu schützen.

Risikokomponenten	MTD	MDM	MAM
Internet- und Contentbedrohungen *Präparierte URLs, die in E-Mails, SMS, Browsern und Social-Media-Apps angeklickt werden. Sie lenken Anwender auf Websites, die sich für legitime Anmeldeseiten ausgeben.* *Eventuell verschlüsseln andere Websites Anmeldedaten nicht oder lassen Daten abfließen.*	ERFÜLLT DIE ANFORDERUNGEN Lookout bietet Phishing-Schutz für E-Mails, SMS, Browser und Apps. Lookout überwacht alle ausgehenden Verbindungen des Mobilgeräts auf Netzwerkebene und in Echtzeit.	KEINE LÖSUNG Ein MDM bietet keinen Phishing-Schutz.	KEINE LÖSUNG Ein MAM bietet keinen Phishing-Schutz.
App-Bedrohungen *Präparierte Apps, die Informationen stehlen, Daten abzielen, unbefugten Fernzugriff ermöglichen oder sogar Geräte beschädigen können.* *Hierzu zählen auch nicht präparierte Apps, die aber von Grund auf Schwachstellen aufweisen, z. B. die Möglichkeit, Kontaktlisten weiterzugeben.*	ERFÜLLT DIE ANFORDERUNGEN Dank seines Datensatzes aus mehr als 70 Millionen Anwendungen erkennt Lookout „bösartige" Apps (d. h. Apps, die eventuell Unternehmensdaten offenlegen) und präparierte Apps. Dies geschieht anhand einer Reputations- und Codeanalyse.	KEINE LÖSUNG MDM erkennt keine präparierten Apps oder Apps mit Schwachstellen.	KEINE LÖSUNG Das MAM erkennt keine präparierten oder mit Schwachstellen behafteten Apps.
Gerätebedrohungen *Ausnutzen von Schwachstellen im Betriebssystem, um umfassendere Berechtigungen zu erlangen. Potenziell besonders effektiv sind solche Angriffe zwischen Betriebssystem-Upgrades und -Patches.* *Des Weiteren können auch per Sideloading installierte Apps Gerätebedrohungen verursachen.*	ERFÜLLT DIE ANFORDERUNGEN Zum Schutz vor jailbroken/gerooteten Geräten, veralteten Betriebssystemen und riskanten Gerätekonfigurationen verfolgt Lookout anonymisierte Verhaltensmuster der Anwender, um darin etwaige Verhaltensanomalien zu entdecken.	TEILLÖSUNG MDM-Lösungen erkennen Rooting/Jailbreaks nicht in Echtzeit. Stattdessen werden Software-Updates als Gegenmaßnahme angeboten. Dadurch bleibt ein Angriffsfenster offen.	KEINE LÖSUNG MAM erkennt keine Gerätebedrohungen.
Netzwerkbedrohungen *Netzwerkbedrohungen, die Schwachstellen beim TLS-/SSL-Verbindungsaufbau von Websites oder Anwendungen über WLAN, Funk oder andere Netze ausnutzen.*	ERFÜLLT DIE ANFORDERUNGEN Lookout kann riskante Netzwerke erkennen und vor Man-in-the-Middle-Angriffen, Zertifikatfälschungen, TLS-/SSL-Stripping oder das Herabstufen von TLS-/SSL-Chiffrensammlungen schützen.	KEINE LÖSUNG Ein MDM erkennt keine Netzwerkbedrohungen.	KEINE LÖSUNG Ein MAM erkennt keine Netzwerkbedrohungen.
Beseitigung von Bedrohungen *Unmittelbare Beseitigung von Bedrohungen auf Mobilgeräten – für den durchgängig sicheren Gebrauch des Geräts und Zugriff auf Unternehmensressourcen*	ERFÜLLT DIE ANFORDERUNGEN Bei Bekanntwerden einer Bedrohung gibt Lookout dem Anwender eine Anleitung zur eigenständigen Beseitigung. 95 % der Bedrohungen werden von den Anwendern selbst beseitigt.	TEILLÖSUNG Keine Bedrohungserkennung oder eigenständige Beseitigung. Allerdings kann MDM das Gerät zurücksetzen und Bedrohungen so den Nährboden entziehen. Zur Bedrohungserkennung sind MTD-Informationen erforderlich.	TEILLÖSUNG Keine Bedrohungserkennung oder -beseitigung. MAM kann infizierte Anwendungen einschränken/entfernen. Erforderlich sind Risikoinformationen seitens der MTD-Lösung.
Bedingter Zugang *Risikobehaftete Mobilgeräte fordern den Zugriff auf Unternehmensressourcen an. Als hochriskant gelten in der Regel mit Viren oder Malware infizierte Geräte, Geräte mit Schwachstellen sowie gerootete Geräte.*	ERFÜLLT DIE ANFORDERUNGEN Lookout Continuous Conditional Access für durchgängig bedingten Zugriff überwacht den Gerätezustand, erkennt das Risikoniveau und bindet dieses Merkmal in die Authentifizierung ein.	TEILLÖSUNG Dank MTD-Informationen kann das MDM Richtlinien zur Vermeidung der Authentifizierung umsetzen. Das MDM kann den Zugriff wegen eines veralteten Betriebssystem verweigern und die Nutzung eines Geräte-Passcodes erzwingen.	TEILLÖSUNG MTD-Informationen helfen MAM-Lösungen, Richtlinien zum Schutz vor der Authentifizierung bei MAM-geschützten Apps umzusetzen. Auch im Falle veralteter App-Versionen kann MAM den Zugriff verhindern.
Anwenderdatenschutz *Schutz der Anwenderdaten und Einhaltung der Datenschutzvorschriften diverser Branchen.*	ERFÜLLT DIE ANFORDERUNGEN Für die Einrichtung benötigt Lookout nur eine E-Mail-Adresse, keine GPS-Position. Lookout bietet zudem einen erweiterten Datenschutzmodus an, über den zusätzliche Anwenderinformationen unterbunden werden.	KEINE LÖSUNG Viele MDM-Tools ermöglichen Arbeitgebern die Überwachung sämtlicher Geräteaktivitäten, z. B. private Anrufe und die Internetnutzung, und das zu jeder Zeit. Einen Privatmodus gibt es nicht.	TEILLÖSUNG Als Einzellösung verwaltet MAM nur vom Arbeitgeber geforderte Anwendungen und beschränkt die Verwendung von Anwenderinformationen. Allerdings werden viele MAM-Lösungen gemeinsam mit MDM bereitgestellt.
Benachrichtigung bei Bedrohungen *Kontinuierliche Suche nach Cybersicherheitsbedrohungen; Benachrichtigung bei Fund.*	ERFÜLLT DIE ANFORDERUNGEN Erkennt Lookout ein Cybersicherheitsereignis auf einem Mobilgerät, erhalten der Administrator und andere ausgewählte Empfänger sofort eine Mitteilung.	KEINE LÖSUNG Erkennt keine mobilen Cybersicherheitsbedrohungen	KEINE LÖSUNG Erkennt keine mobilen Cybersicherheitsbedrohungen

MTD schützt vor diversen Cybersicherheitsereignissen

MDM- und MAM-Lösungen erkennen keine Cybersicherheitsbedrohungen oder schädlichen Anwenderhandlungen und schützen auch nicht davor. Es handelt sich eher um Verwaltungstools, die Richtlinien und Verfahrensweisen für die Administration und Governance von Mobilgeräten eines Unternehmens anwenden. Schutz vor Cybersicherheitsangriffen auf Mobilgeräte bietet hingegen eine MTD-Lösung, die Bedrohungen erkennt und zum Schutze des Unternehmens blockiert. Allerdings ist die Integration von MTD in eine vorhandene MDM- und/oder MAM-Lösung zu empfehlen, da Letztere dadurch Richtlinien aufgrund der Bedrohungslage umsetzen kann.



Mehr erfahren Sie auf lookout.com/de

Lookout

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

2. Zumerle, Dionisio / Girard, John: „2018 Gartner Market Guide for Mobile Threat Defense". IDC, 2018