Lookout

MTD vs MDM vs MAM

Mobile Threat Defense | Mobile Device Management | Mobile App Management

With employees accessing sensitive business data from mobile devices many organizations deploy MDM and MAM with the belief that these solutions will protect enterprises in the cloud from cybersecurity threats.

Organizations increasingly adopt MTD

MTD

200%

"By 2020, 30% of organizations will have MTD in place, **an increase from less than 10% in 2018.**"[2] [An increase of 200%]

MDM

30%

"Organizations looking to deploy MDM in conjunction with EMM will **decrease by approximately 30% in the next 12-18 months.**"[1]

MAM

10%

"Organizations looking to deploy MAM and MCM in conjunction with EMM will **decrease by approximately 10% in the next 12-18 months.**"[1]

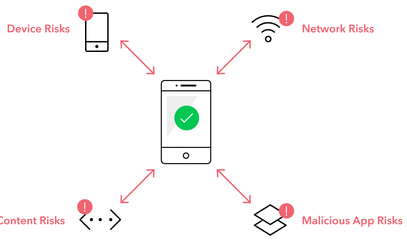
Guide to Identifying Security Gaps in Mobile Management

This guide compares the cybersecurity capabilities of MTD, MDM, and MAM relative to the spectrum of mobile risk. Security gaps in mobile management are emphasized to highlight potential system vulnerabilities that organizations should address to strengthen their mobile security posture.

Component of Risk	MTD	MDM	MAM
Web & Content Threats *Malicious URLs opened from email, SMS,browsers, and social apps. These can direct users to websites that purport to be official login pages.* *Other websites may not encrypt login credentials or can leak data.*	MEETS REQUIREMENTS Lookout provides phishing protection across email, SMS, browser, and apps. Lookout inspects all outbound connections made from the mobile device at the network level in real-time.	NO SOLUTION MDM does not provide any phishing protection.	NO SOLUTION MAM does not provide any phishing protection.
App Threats *Malicious apps that can steal information, leak data, gain unauthorized remote access to other systems, and even damage devices.* *This includes non-malicious apps that have inherent vulnerabilities such as the ability to leak contact lists.*	MEETS REQUIREMENTS With a data corpus of more than 70 million applications, Lookout identifies "leaky" apps (meaning apps that can put enterprise data at risk) and malicious apps, through reputation scanning and code analysis.	NO SOLUTION MDM has no ability to detect malicious or vulnerable apps.	NO SOLUTION MAM has no ability to detect malicious or vulnerable apps.
Device Threats *Threats that exploit the operating system to gain heightened permissions. Such attacks can be especially effective during the vulnerability window between OS-level upgrades and patches.* *Additionally, sideloaded apps can introduce device threats.*	MEETS REQUIREMENTS To protect against jailbroken/rooted devices, outdated OS, and risky device configurations, Lookout leverages behavioral anomaly detection by tracking expected and acceptable use patterns.	PARTIAL SOLUTION MDMs cannot detect root/jailbreaks in real-time. Instead they push software updates to handle the threat. This leaves a vulnerability window for attack.	NO SOLUTION MAM has no ability to detect device threats.
Network Threats *Network threats that take advantage of weakness in how web sites or applications establish TLS/SSL sessions over Wi-Fi, cellular, or other networks.*	MEETS REQUIREMENTS Lookout can detect risky networks and protect against man-in-the-middle, certificate impersonation, TLS/SSL stripping, or TLS/ SSL cipher suite downgrades.	NO SOLUTION MDM has no ability to detect network threats.	NO SOLUTION MAM has no ability to detect network threats.
Threat Remediation *Immediate threat remediation on the mobile device to ensure continued safe mobile operation and access to corporate resources.*	MEETS REQUIREMENTS Upon detection of a threat, Lookout provides user instruction for self-remediation. 95% of threats are user-remediated.	PARTIAL SOLUTION No threat detection or self-remediation. However, MDM can wipe the device to mitigate risk of a threat. Requires input from MTD to identify threats.	PARTIAL SOLUTION No threat detection or remediation. MAM can restrict/remove an application if identified as infected. Requires input from MTD to receive application risk level.
Conditional Access *High-risk mobile devices attempt to access corporate resources. Devices containing viruses, malware, vulnerabilities, or that have been rooted are typically considered high-risk.*	MEETS REQUIREMENTS Lookout Continuous Conditional Access monitors device health, assigns a risk level, and provides this information to the organization as a factor of authentication.	PARTIAL SOLUTION With MTD input, MDM can enact policies to prevent authentication. MDM can prevent access based on outdated OS and can enforce a passcode on the device.	PARTIAL SOLUTION With input from an MTD, MAM can enact policies to prevent authentication to mam-protected apps. MAM can also prevent access based n out-of-date app versions.
User Privacy *Protection of user privacy and adherence with privacy regulations across various industries.*	MEETS REQUIREMENTS Lookout only requires email address for setup and does not require GPS location. Lookout also provides an advanced privacy mode to suppress additional user information.	NO SOLUTION Many MDM tools let employers monitor all device activity - including personal calls and web traffic - at any given time. No privacy mode is available.	PARTIAL SOLUTION As a stand-alone solution, MAM manages only those applications required by employer and limits use of user's information. Many MAM solutions, however, are deployed with MDM.
Threat Notification *Continuous monitoring for cybersecurity events and notification of these events.*	MEETS REQUIREMENTS Upon detection of a mobile cybersecurity event, Lookout immediately notifies administrator and designated recipients of event.	NO SOLUTION Cannot detect mobile cybersecurity events	NO SOLUTION Cannot detect mobile cybersecurity events

MTD protects organizations from multiple cybersecurity events

MDM and MAM solutions provide no detection or protection against cybersecurity threats and user behaviors. Rather these are 'management' tools that can apply policies and procedures for the administration and governance of mobile devices used within an organization. For protection against mobile cybersecurity attacks, a MTD solution is required so that threats can be detected and blocked to protect the organization. Integrating a MTD with an existing MDM and/or MAM solution, however, is a sound strategy and will enable these management tools to apply policies based on threat information.



To learn more, visit lookout.com

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