Lookout

MDM vs MAM vs MTD

Mobile Device Management | Mobile App Management | Mobile Threat Defense

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

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]

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%]

Guidance for Financial Services

Satisfying Regulatory Cybersecurity Requirements of the New York Department of Financial Services (NYDFS) regulation 23 NYCRR 500

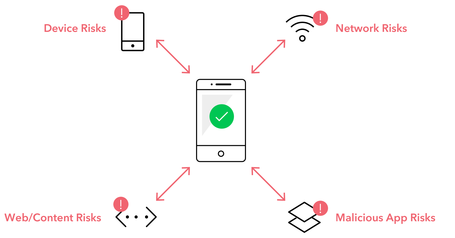
Below is a summary of how MDM, MAM, and MTD address the relevant cybersecurity requirements prescribed by NYDFS 23 NYCRR 500.

NYDFS Requirement	MTD	MDM	MAM
Cybersecurity Program (500.02) *Identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems...*	MEETS REQUIRMENTS MTD provides visibility into the spectrum of mobile risk including phishing, app-based, network-based, and device-based threats	NO SOLUTION No internal or external mobile threat assessment capability	NO SOLUTION No internal or external mobile threat assessment capability
Cybersecurity Program (500.02) *Use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information...*	PARTIAL SOLUTION MTD effectively detects mobile phishing, app-based, network-based, and device-based threats and initiates actions based on default or custom policies. (can build targeted policies based on the threat status)	PARTIAL SOLUTION Supports policies to restrict use of device Can leverage containers to prevent data leakage Can remotely wipe data from devices	PARTIAL SOLUTION Supports policies to restrict use of application Can leverage containers to prevent data leakage Can remotely wipe data from devices
Cybersecurity Program (500.02) *Detect Cybersecurity Events*	MEETS REQUIRMENTS Lookout artificial intelligence identifies known mobile app vulnerabilities, zero-day threats, and emerging phishing sites	NO SOLUTION Cannot detect cybersecurity events	NO SOLUTION Cannot detect cybersecurity events
Cybersecurity Program (500.02) *Respond to identified or detected Cybersecurity Events to mitigate any negative effects.*	MEETS REQUIRMENTS Lookout detects mobile threats, assigns a risk level, and will take action based on a default system policy or custom policy set by the organization	PARTIAL SOLUTION Cannot detect mobile cybersecurity events (can mitigate based on MTD input)	PARTIAL SOLUTION Cannot detect mobile cybersecurity events (can mitigate based on MTD input)
Penetration Testing and Vulnerability Assessments (500.05) *Bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.*	MEETS REQUIRMENTS Scans mobile fleet to assess and report on mobile vulnerabilities	NO SOLUTION Limited to identifying outdated OS versions	NO SOLUTION Limited to identifying outdated OS versions
Audit Trail: (500.06) *Include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.*	MEETS REQUIRMENTS Lookout provides a threat event history to show actions taken within the system including threat remediation activity	PARTIAL SOLUTION Audit trail available for management activities taken on the device	PARTIAL SOLUTION Audit trail available for management activities relative to the managed applications
Risk Assessment (500.09) *The Covered Entity's Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored...*	MEETS REQUIRMENTS On a continuous basis, Lookout can provide risk status of mobile devices	PARTIAL SOLUTION Cannot detect mobile cybersecurity events in real-time as threats evolve However, MDM can be used to set restrictions on the use of specific apps that have been deemed vulnerable	PARTIAL SOLUTION Cannot detect mobile cybersecurity events in real-time as threats evolve MAM can only manage use of apps that have enrolled in MAM. No other device-level management is available
Notices to Superintendent (500.17) *Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred...*	MEETS REQUIRMENTS 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

For the NYDFS regulation, visit https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

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