Lookout

MTD vs MDM

Mobile Threat Defense | Mobile Device Management

Lookout helps the Defense Industrial Base (DIB) sector comply with the Cybersecurity Maturity Model Certification (CMMC) by protecting FCI and CUI from mobile cyber threats.

Organizations increasingly adopt Mobile Threat Defense (MTD) to augment or replace existing mobile device management (MDM) solutions

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]

Below is a summary of how MTD and MDM address the relevant cybersecurity requirements of Cybersecurity Maturity Model Certification

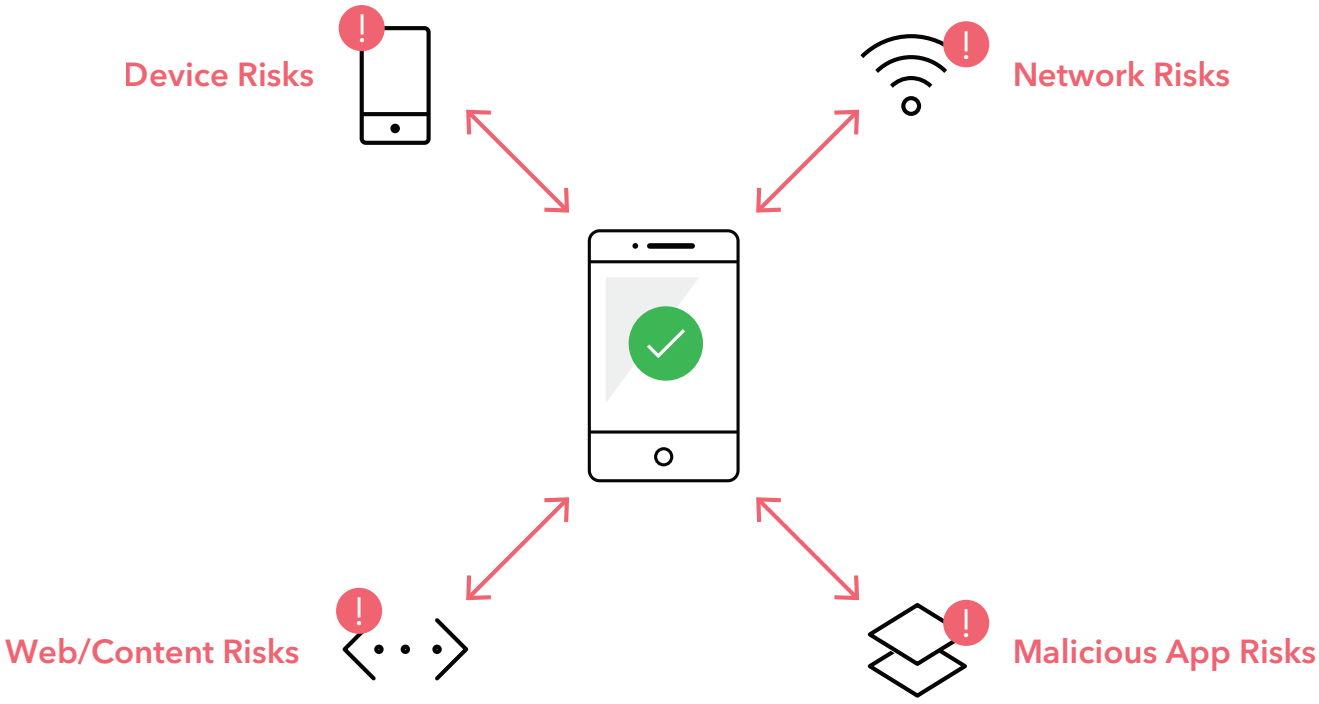
CMMC Requirement	MTD	MDM
C002 Control internal system access *AC.3.020 Level 3 (L3) Control connection of mobile devices.* • *NIST SP 800-171 Rev 1 3.1.18* • *CIS Controls v7.1 13.6, 16.7* • *NIST CSF v1.1 PR.AC-3, PR.AC-6* • *CERT RMM v1.2 TM:SG2.SP2* • *NIST SP 800-53 Rev 4 AC-19* • *UK NCSC Cyber Essentials*	PARTIAL SOLUTION On a continuous basis, Lookout can provide risk status of mobile devices and block the connection to an organization's resources based on that status.	MEETS REQUIREMENT Can provide policies that control the connection of mobile devices to the network.
C014 Perform configuration and change management *CM.5.074 Level 5 (L5) Verify the integrity and correctness of security critical or essential software as defined by the organization (e.g. roots of trust, formal verification, or cryptographic signatures).* • *CMMC modification of Draft NIST SP 800-171B 3.14.1e* • *CIS Controls v7.1 2.10 NIST CSF v1.1 PR.DS-6, PR.DS-8, PR.IP-2* • *NIST CSF v1.1 PR.AC-3, PR.AC-6* • *CERT RMM v1.2 TM:SG2.SP2* • *NIST SP 800-53 Rev 4 SI-7(6), SI-7(9), SI-7(10), SA-17*	MEETS REQUIREMENT Lookout Vulnerability Management detects and provides visibility into risky and vulnerable endpoints, including risky device configurations and vulnerabilities in the operating system.	PARTIAL SOLUTION Limited to verifying that mobile devices are running the latest version of the operating system.
C017 Detect and report events *IR.2.093 Level 2 (L2) Detect and report events.* • *CIS Controls v7.1 19.4* • *NIST CSF v1.1 DE.CM-1, DE.CM-2, DE.CM-3, RS.CO-2* • *CERT RMM v1.2 IMC:SG2.SP1* • *NIST SP 800-53 Rev 4 IR-6*	MEETS REQUIREMENT Lookout detects and protects against app, device and network threats on mobile devices. Prevents compromise of data resulting from risks on such devices.	NO SOLUTION Cannot detect cybersecurity events.
C031 Identify and evaluate risk *RM.4.150 Level 4 (L4) Employ threat intelligence to inform the development of the system and security architecture, selection of security solutions, monitoring, threat hunting, and response and recovery activities.* • *Draft NIST SP 800-171B 3.11.1e* • *NIST CSF v1.1 ID.RA-2, ID.RA-3*	MEETS REQUIREMENT With a sensor network of over 180 million mobile devices and 100 million apps, Lookout applies machine learning and predictive analytics to actively monitor and respond to threats in real-time.	NO SOLUTION Has no native threat intelligence capabilities. (MDM can, however, initiate policies based on threat intelligence provided by an MTD)

Below is a summary of how MTD and MDM address the relevant cybersecurity requirements of Cybersecurity Maturity Model Certification

CMMC Requirement	MTD	MDM
C037 Implement threat monitoring *SA.4.171 Level 4 (L4) Establish and maintain a cyber threat hunting capability to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls.* • *Draft NIST SP 800-171B 3.11.2e* • *NIST CSF v1.1 DE.CM-1 through DE.CM-8* • *NIST SP 800-53 Rev 4 PM-16*	MEETS REQUIREMENT Lookout artificial intelligence identifies known mobile app vulnerabilities, zero-day threats, and emerging phishing sites.	NO SOLUTION Cannot detect cybersecurity events.
C038 Define security requirements for systems and communications *SC.3.182 Level 3 (L3) Prevent unauthorized and unintended information transfer via shared system resources.* • *NIST SP 800-171 Rev 1 3.13.4* • *NIST SP 800-53 Rev 4 SC-4*	PARTIAL SOLUTION Lookout identifies "leaky" and vulnerable apps that can unintentionally leak information to other shared systems.	PARTIAL SOLUTION MDM has no visibility 'leaky' applications or system vulnerabilities that unintentionally leak data. MDM can, however, lock-down access to specific applications and set data controls to restrict unauthorized information transfer.
C039 Control communications at system boundaries *SC.4.199 Level 4 (L4) Utilize threat intelligence to proactively block DNS requests from reaching malicious domains.* • *CMMC*	MEETS REQUIREMENT Detects and protects against phishing attacks by proactively blocking DNS requests in real-time across email, text messages, messaging apps, social media, or any other app attempting to access malicious websites.	PARTIAL SOLUTION Cannot detect malicious websites in real-time at the time access is attempted. However, MDM can be used to set restrictions on access to specific websites that have been predetermined to be malicious.
C039 Control communications at system boundaries *SC.4.229 Level 4 (L4) Utilize a URL categorization service and implement techniques to enforce URL filtering of websites that are not approved by the organization.* • *CMMC* • *CIS Controls v7.1 7.4*	MEETS REQUIREMENT By categorizing URLs as offensive content, Lookout enables system administrators to apply policies to restrict user access to offensive websites.	MEETS REQUIREMENT Can enforce policies to restrict access to predetermined websites that are not approved by the organization.

MTD protects the Defense Industrial Base (DIB) sector from mobile cybersecurity events

MDM provide no detection or protection against mobile cybersecurity threats. Rather, it is a 'management' tool that can apply policies and procedures for the administration and governance of mobile devices and applications used within an organization. To safeguard CUI and FCI against mobile cybersecurity attacks, MTD is required to detect mobile threats, notify of incidents, and block access to the entity's resources. Integrating an MTD with an existing MDM, however, is a sound strategy and will enable MDM 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