

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.

However, with over 32 million patient records breached in 2019 , the healthcare industry must refine its security strategy to get ahead of hackers.¹

Organizations increasingly adopt MTD



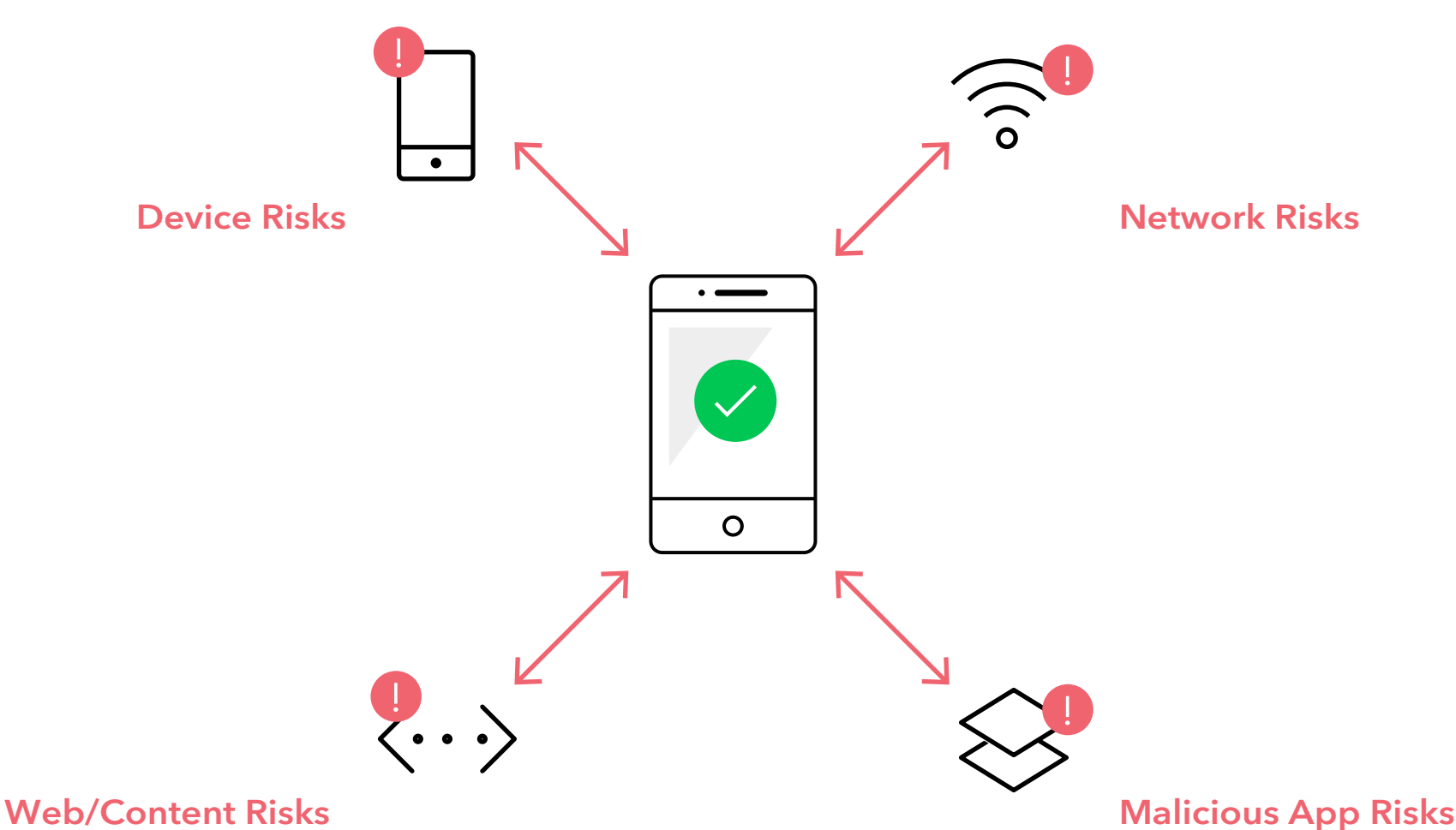
Guidance for Healthcare Organizations

Satisfying regulatory cybersecurity requirements of the Health Insurance Portability and Accountability Act (HIPAA) security rule.

HIPAA Security Rule Requirement	MTD	MDM	MAM
<p>§164.306 (a)(2)</p> <p><i>Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.</i></p>	<div>MEETS REQUIREMENTS</div> <p>Protects against phishing, app-based, network-based, and device-based threats.</p>	<div>NO SOLUTION</div> <p>Cannot detect cybersecurity threats.</p>	<div>NO SOLUTION</div> <p>Cannot detect cybersecurity threats.</p>
<p>§164.308 (a)(1)(i)</p> <p><i>Implement policies and procedures to prevent, detect, contain, and correct security violations.</i></p>	<div>MEETS REQUIREMENTS</div> <p>Can establish policies to prevent, detect, contain and mitigate mobile threats.</p>	<div>PARTIAL SOLUTION</div> <p>Cannot detect mobile threats. Limited to wiping a device to mitigate security risk.</p>	<div>PARTIAL SOLUTION</div> <p>Cannot detect mobile threats. Limited to wiping data from managed apps to mitigate security risk.</p>
<p>§164.308 (a)(1)(ii)(A)</p> <p><i>Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information...</i></p>	<div>MEETS REQUIREMENTS</div> <p>Continuously scans mobile fleet to provide an accurate and thorough assessment of device risk in order to limit access to electronic protected health information.</p>	<div>NO SOLUTION</div> <p>Cannot assess risks and vulnerabilities to electronic protected health information.</p>	<div>NO SOLUTION</div> <p>Cannot assess risks and vulnerabilities to electronic protected health information.</p>
<p>§164.308 (a)(1)(ii)(B)</p> <p><i>Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).</i></p>	<div>MEETS REQUIREMENTS</div> <p>Detects mobile threats, assigns a risk level, and will take action to execute security measures for policy compliance.</p>	<div>PARTIAL SOLUTION</div> <p>Cannot detect threats but can implement device policies to reduce risk (i.e. whitelist/blacklist specific domains, set user permissions, mitigate threat based on MTD input).</p>	<div>PARTIAL SOLUTION</div> <p>Cannot detect threats but can implement application policies to reduce risk (i.e. restrict copy/paste, data loss prevention, set app permissions, mitigate threat based on MTD input)</p>
<p>§164.308(a)(1)(ii)(D)</p> <p><i>Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.</i></p>	<div>PARTIAL SOLUTION</div> <p>Provides security incident tracking and audit logs of access and actions taken within the system, which can be regularly reviewed.</p>	<div>PARTIAL SOLUTION</div> <p>Contains an audit trail of management activities taken on all managed devices, which can regularly be reviewed.</p>	<div>PARTIAL SOLUTION</div> <p>Contains an audit trail of management activities relative to the managed applications, which can be regularly reviewed.</p>
<p>§164.308(a)(4)(ii)(C)</p> <p><i>Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.</i></p>	<div>PARTIAL SOLUTION</div> <p>Provides mobile device risk-level to MDM or IAM solutions to enable real-time enforcement of the entity's access authorization policies.</p>	<div>PARTIAL SOLUTION</div> <p>Can define authorization policies to manage access to mobile devices and corporate resources.</p> <p>Requires MTD input to restrict access to high-risk mobile devices.</p>	<div>PARTIAL SOLUTION</div> <p>Can define authorization policies to manage access to applications on mobile devices.</p> <p>Requires MTD input to restrict access to high-risk mobile devices.</p>
<p>§164.308(a)(5)(ii)(A)</p> <p><i>Protection from malicious software. Procedures for guarding against, detecting, and reporting malicious software.</i></p>	<div>MEETS REQUIREMENTS</div> <p>Protects against malicious mobile software by detecting the risk, and executing procedures to contain, report, and mitigate the threat.</p>	<div>NO SOLUTION</div> <p>Cannot detect malicious software applications.</p>	<div>NO SOLUTION</div> <p>Cannot detect malicious software applications.</p>
<p>§164.308(a)(6)(ii)</p> <p><i>Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents...</i></p>	<div>MEETS REQUIREMENTS</div> <p>Identifies suspected and known mobile security threats and responds based on default or custom policies set by the organization to mitigate the harmful effects of a security incident.</p>	<div>NO SOLUTION</div> <p>Cannot detect mobile security threats.</p>	<div>NO SOLUTION</div> <p>Cannot detect mobile security threats.</p>

MTD protects healthcare organizations from multiple cybersecurity events

MDM and MAM solutions provide no detection or protection against mobile cybersecurity threats. Rather these are ‘management’ tools that can apply policies and procedures for the administration and governance of mobile devices and applications used within an organization. To safeguard protected health information 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 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



1. <https://www.prnewswire.com/news-releases/32-million-breached-patient-records-in-first-half-of-2019-double-total-for-all-of-2018-300894237.html>
2. Zumerle, Dionisio and Girard, John. 2018 Gartner Market Guide for Mobile Threat Defense. IDC. 2018
3. Hochmuth, Phil. 2018 Enterprise Mobility Decision Maker Survey: Software, Management and Security Highlights. IDC. 2018 (MCM = Mobile Content Management)