Market Guide for Mobile Threat Defense

Published 29 March 2021 - ID G00736793 - 24 min read

By Dionisio Zumerle, Rob Smith

Mobile threat defense products counter malicious threats to iOS and Android devices. Security and risk management leaders who need to strengthen their mobile security posture should adopt MTD products to improve their overall security hygiene.

Overview

Key Findings

- Mobile threat defense (MTD) products aim to prevent and detect enterprise threats, such as malware, on iOS and Android devices. To do so, MTD products use a variety of techniques, including machine learning and behavioral analysis. Offerings come from a variety of vendors, including endpoint protection platform (EPP) vendors and stand-alone MTD providers.
- Gartner still sees large-scale MTD adoption centered on regulated and high-security sectors. Among mainstream organizations, MTD product adoption is largely limited to organizations that want to improve their overall security hygiene or provide device posture information for “bring your own device” (BYOD) equipment, rather than those aiming to counter malicious mobile threats.
- Enterprises that derive value from MTD do so by implementing security hygiene using proactive measures, such as app vetting and device vulnerability management, rather than the ability to detect and counter advanced attacks.
- Emerging use cases envisage MTD as a component of zero-trust network access (ZTNA) architecture and of an extended detection and response (XDR) system for detection and response, which can serve as a pilot for unified endpoint security. This is in addition to the use of MTD for mobile phishing protection.

Recommendations

To address mobile risks, security and IT leaders responsible for the security of iOS and Android endpoints should:

- Prioritize MTD adoption in high-security and regulated sectors and in organizations with large or fragmented Android device fleets.
- Establish a security baseline for mobile devices before investing in MTD products, and use these products' app vetting and device vulnerability management features to demonstrate immediate benefits, rather than expect them to counter advanced malicious threats or uncover major breaches.
- Integrate MTD with incumbent unified endpoint management (UEM) tools. They should favor the app-based option and leave proxy-based deployment for corporate-owned business-only (COBO) scenarios.
- Use MTD products to protect enterprise infrastructure where BYOD policies are in operation and for other use cases in which devices must stay unmanaged. Emphasize strategic vendor fit over product differentiation, unless they address high-security contexts and situations with specific mobile security needs.

Strategic Planning Assumption

By 2025, more than half of organizations in regulated industries will have a security solution for both iOS and Android devices.

Market Definition

The mobile threat defense (MTD) market relates to products that protect organizations from threats on iOS and Android devices. MTD products protect at the device, network and application levels and focus on countering malicious actions.

Market Description

MTD products not only prevent attacks, but also detect and remediate them. MTD focuses on identifying and thwarting malicious threats, rather than relying on device management configuration to protect against simple user mistakes.

MTD products offer protections beyond the device and app restrictions that UEM tools offer. These additional protections include:

- At the device level, the ability to assess posture, such as OS version, security updates, system parameters, device configuration, firmware and system libraries, in order to identify security misconfigurations, device vulnerabilities, and suspicious or malicious activity. For example, MTD tools can check for modification of system libraries and configurations, as well as for privilege escalation, such as a jailbreak or rooting.

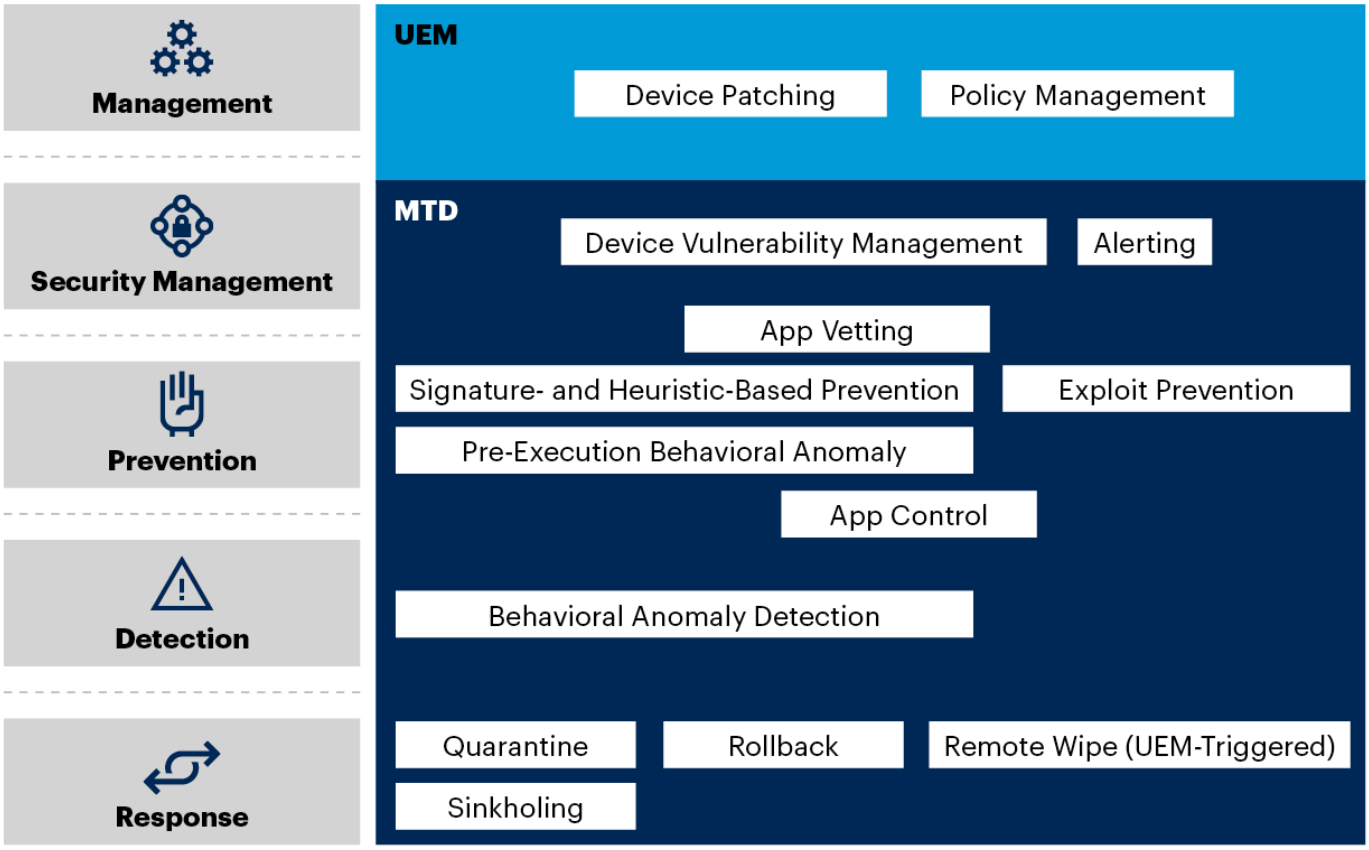
- At the network level, the ability to monitor wireless and cellular network traffic for unsanctioned, suspicious or malicious behavior. MTD tools can detect man-in-the-middle attacks by checking for invalid certificates, for stripping of Transport Layer Security (TLS), and for “bidding down” attacks. For example, an MTD tool could detect a malicious URL or a malicious wireless network that deliberately negotiates to use a weak encryption algorithm with a mobile device.

- At the application level, the ability to identify grayware (see Note 1) and malware. Techniques used include signature- and heuristics-based malware scanning, code emulation and simulation, sandboxing, application reverse engineering, and static and dynamic app security scanning.

To work, mobile malware must circumvent controls built into mobile OSs, such as those for app store curation and native mobile OS hardening. MTD therefore tends to focus on preventing and detecting anomalous behavior by collecting and analyzing indicators of compromise, as well as expected behavior. To do so, MTD products gather threat intelligence from the devices they support, as well as from external sources, and use an analysis engine that resides in the cloud, on-premises or on an MTD app installed on the devices. Figure 1 illustrates MTD functionality, and how it relates to UEM tools.

Figure 1: Mobile Threat Defense Functionality Compared With That of Unified Endpoint Management

Comparison of Mobile Threat Defense and Unified Endpoint Management Functionality



Source: Gartner
736793_C

Gartner

MTD products typically include an on-device agent in the form of an app (see Note 2), and provide an administrative console that enables enterprises to monitor, report and audit. The console provides identification and categorization of the riskiness of devices, suggests mitigating measures, integrates with UEM tools, and enables the administrators using the console to prioritize intervention on vulnerable devices.

Market Direction

The MTD market is relatively small, compared with other endpoint security markets such as the EPP market, but it continues to grow, predominantly in regulated and high-security sectors. Gartner estimates that the MTD market reached $350 million in 2020.

The perception of enterprise risk from malicious threats against mobile devices continues to evolve. Every year, we encounter a number of impactful and highly visible successful mobile attacks. [1,2,3] Only a small portion are truly against enterprises and business users. [4] Many of the most impactful attacks continue to be targeted, with a particular geopolitical and individual focus, rather than an enterprise orientation. [5]

Even though attacks against mobile devices are not rare, we do not have evidence of a major enterprise breach that can be directly attributed to an attack against a mobile device. It is difficult to determine whether this is because of the lesser visibility of the underlying functions and components of iOS and Android, compared with Windows, Linux or macOS, or because attacks simply focus on traditional OSs.

We are, however, seeing a modest increase in demand for mobile forensic services from Gartner clients. Some of this increase is due to recent mobile security incidents that cannot be fully explained with existing mobile security capabilities.

> **We expect slow but steady growth in MTD adoption as mobile security maturity grows across enterprises, rather than an abrupt surge in adoption following a spectacular mobile breach.**

As adoption grows, we do see evidence of blocked attacks against mobile devices — phishing attacks, for example. [6] For the most part, however, what MTD can visibly demonstrate is an improvement in security hygiene (see the section on app vetting in Use Cases section below, for example). It can be seen as the next logical step for an organization that is ready to strengthen its mobile security.

Although the MTD market is still relatively small, we have seen large deployments of MTD products, especially in regulated industries. The products are mature enough for adoption for enterprises of any size. As mobile security maturity grows within an organization, security departments become the buyers, rather than mobility or IT operations teams. Security teams see MTD as a way to obtain visibility into the mobile fleet, without having direct access to mobile device management (MDM) or UEM tools.

Many EPP vendors offer MTD products, either as homegrown solutions or as solutions resulting from an acquisition or partnership. Although some EPP mobile security modules lack the richness of features of some stand-alone MTD products, the ability to manage the security of mobile devices through the same EPP dashboard and to perform investigations cross-platform appeals to organizations. In the long term, we see most organizations using an EPP or unified endpoint security

(UES) product to cover all their endpoint security needs, including mobile (see the section on ZTNA in the Use Cases section; for more details on UES, see also Innovation Insight for Unified Endpoint Security).

Market Analysis

Deployment Options

There are four deployment options for MTD solutions (see also Figure 2):

- **MTD integrated with UEM.** In this deployment option a UEM tool facilitates MTD enrollment. It also provides information that the MTD product collects and sends to its analysis engine, which can identify threats and raise alerts. At the MTD product's indication, the UEM tool performs remedial actions on the device, such as a remote wipe. Most MTD vendors offer this approach.

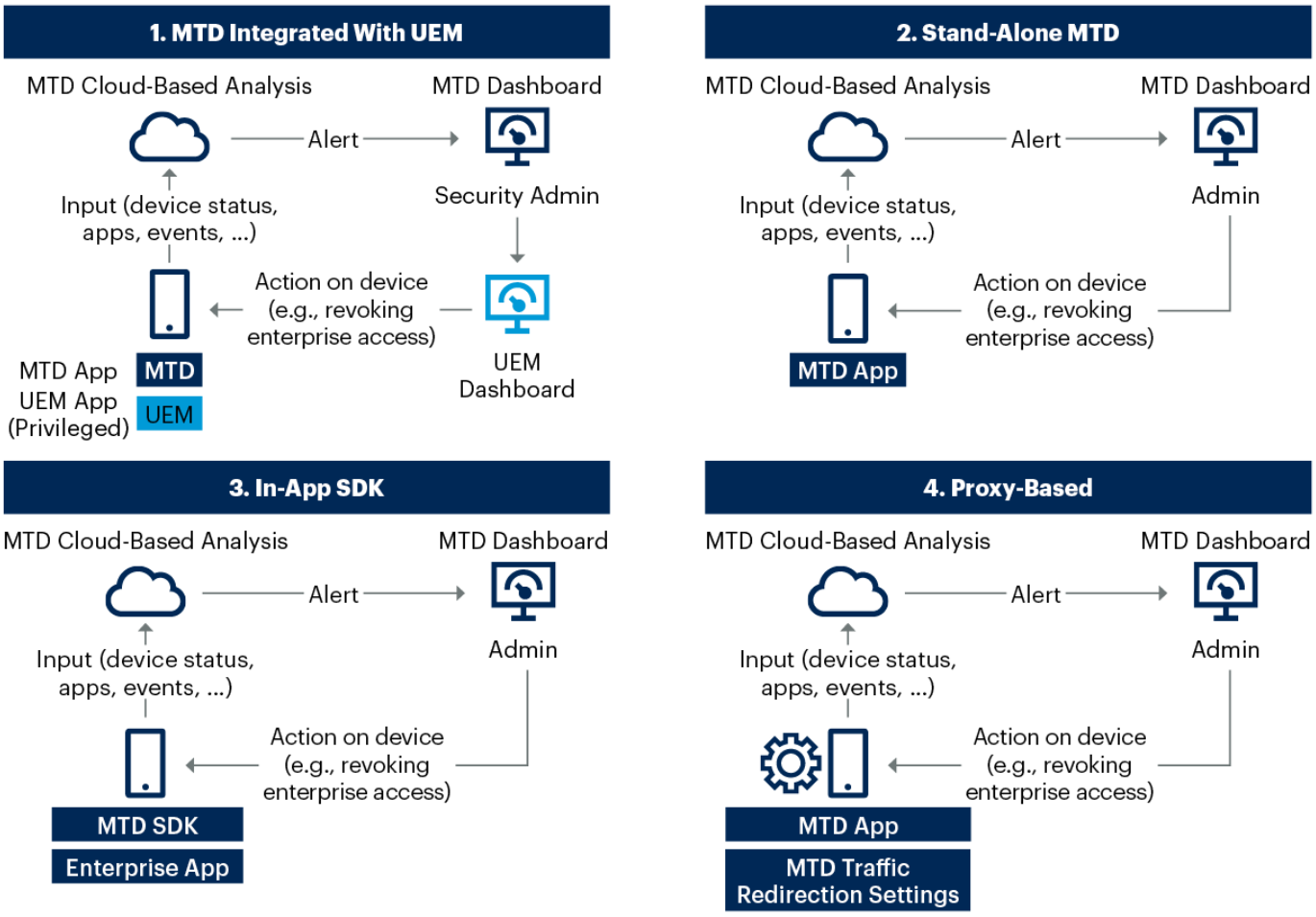
- **Stand-alone MTD app installed on devices.** Typically, these devices are unmanaged. This deployment option is encountered where device management is not possible because of user experience or privacy considerations. It is becoming more popular as options such as Microsoft's MAM-WE (see Note 3) provide the ability to run enterprise apps on an unenrolled device (for more information, see the passage about ZTNA in the Use Cases section). An unmanaged device provides limited information and remediation options to the MTD app that runs on it (for example, the list of apps used on an iOS device is not accessible). Some of these technical limitations also apply to BYOD deployment modes such as iOS User Enrollment [7] and Android Enterprise profile owner. [8] All MTD vendors offer this approach.

- **SDK version that can be embedded in a homegrown app.** The goal here is to provide protection for the enterprise apps that host an SDK, rather than for the device itself. For example, the app may decide to abort an operation if it identifies the presence of malware on a device. This method is mostly used to protect consumer-facing apps, rather than employee-facing apps. MTD vendors increasingly partner with app-shielding vendors to offer more comprehensive solutions that offer anti-malware functionality. [9] Examples of vendors that support this deployment option are BETTER, Lookout and Zimperium.

- **Proxy-based MTD solution that diverts and inspects all network traffic.** The MTD solution redirects traffic passing to and from the device to an analysis engine. There it analyzes the traffic, filters malware and provides functionality often found in secure web gateways (see Magic Quadrant for Secure Web Gateways), such as domain block listing and content filtering. This approach requires an efficient way to redirect traffic to avoid battery drain. It allows for more visibility, but the privacy implications of constant traffic monitoring confine it to COBO scenarios, especially as iOS has introduced a native way to inspect network traffic directly on devices. [10] Vendors that offer this approach as an option include Wandera and Corrata.

Figure 2: MTD Deployment Options

MTD Deployment Options



Source: Gartner
736793_C

Gartner

Use Cases

Organizations usually look for an **all-round mobile security tool** that tackles malicious threats. Sometimes this need is driven by compliance, especially in regulated industries such as financial services. In those cases, the ability to scan for malicious apps and perform device vulnerability management are the two main features that end users look for.

App vetting is the analysis of apps to identify not just malicious ones but also, more importantly, those that conflict with organizational requirements. [11] It is easy to quickly be overwhelmed by the number of apps to be scanned. MTD solutions (and mobile app security testing solutions) provide a way to define acceptable app behavior and create lists of blocked and allowed apps. Given recent concerns about the privacy policies of specific apps, app vetting has gained greater prominence as a use case. [12,13]

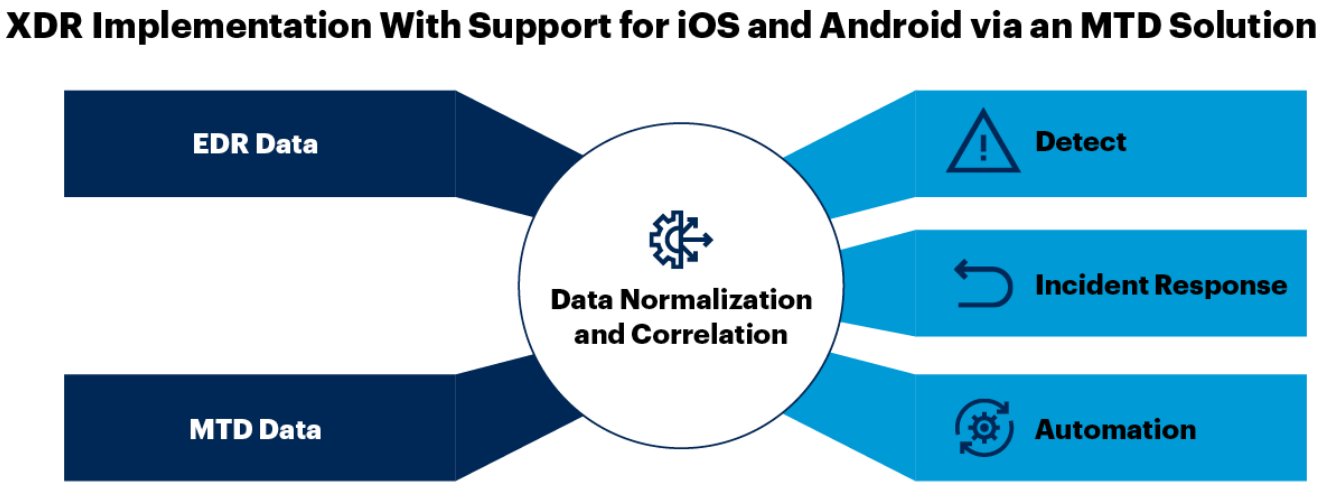
Some organizations use MTD solutions not only to vet third-party apps, but also to act as lightweight mobile app security testing solutions for their mobile apps (see Avoid Mobile Application Security Pitfalls).

Mobile phishing has recently emerged as an important use case. There are numerous channels to reach mobile devices that do not have phishing protection. [14,15] Additionally, the screens of mobile devices are small, the presentation of information tends to leave out details to enhance the user experience, and mobile devices are the preferred platforms for consuming notifications. [16] This makes mobile devices a threat vector to initiate attacks such as account takeovers.

Driven by evidence that mobile phishing attempts are successful, [17,18] either as the main attacks, [19,20] or as parts of a larger attack, [21] MTD solutions have developed protections against malicious URLs sent via email, text, social media, instant messaging and other apps. Implementations vary, and some MTD solutions can block a URL, whereas some others alert the user about the threat. Some MTD solutions can identify only known malicious URLs, while others can dynamically recognize unknown phishing links.

A new use case sees MTD used as part of a UES or an **XDR** system. We are increasingly observing endpoint security vendors that offer endpoint detection and response (EDR) extend support to iOS and Android, either on their own or in partnership with vendors of MTD solutions. Adding visibility for mobile devices, UES and XDR solutions can improve detection and identify lateral movement (see Figure 3). As mobile devices do not provide kernel-level access, mobile EDR visibility is limited, compared with what is available for Windows 10 devices, but we expect mobile devices to gradually accommodate the need for visibility, in a similar fashion to what we have observed for Apple macOS. [22] The UES framework (see Innovation Insight for Unified Endpoint Security) takes XDR and the following use case of ZTNA and provides cross-platform support for both.

Figure 3: XDR Implementation With Support for iOS and Android via an MTD Solution



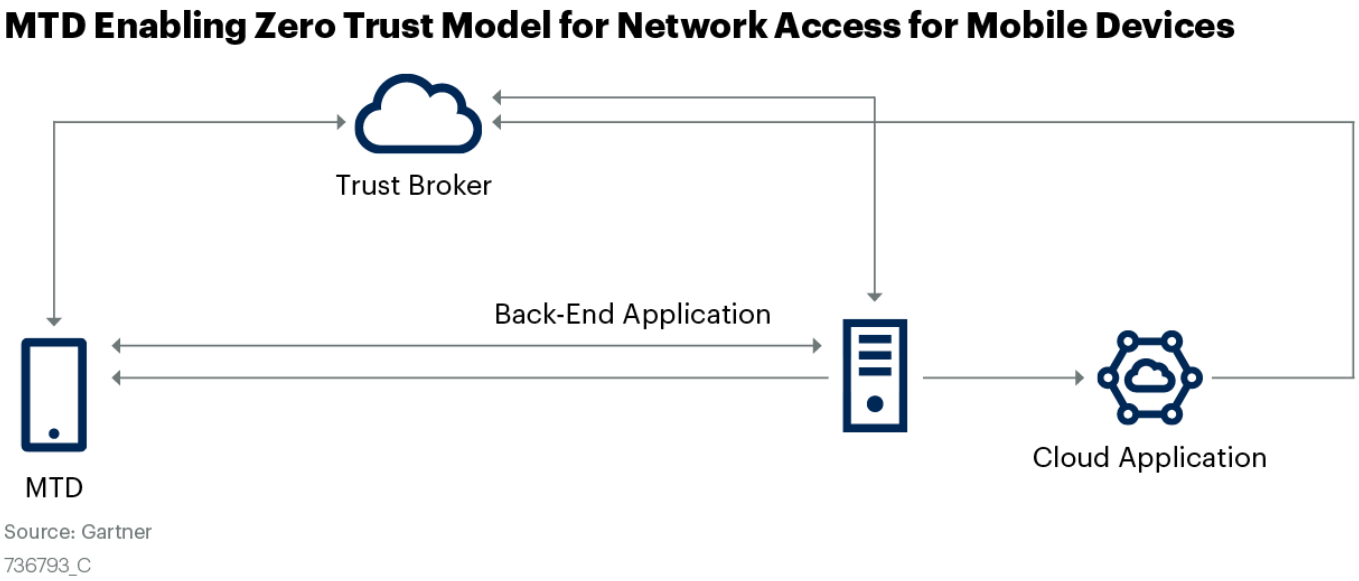
Source: Gartner
736793 C

Gartner

MTD is emerging as a component that enables implementation of ZTNA for iOS and Android devices. As Figure 4 highlights, MTD can provide an assessment of a device to a ZTNA trust broker (see Market Guide for Zero Trust Network Access), which can decide whether to allow access to a specific enterprise application. When a device requests enterprise access, the ZTNA trust broker queries the endpoint's MTD. It can require installation of MTD when it is missing, in order to complete access, and the return of device posture information or a security score when MTD is present. Based on this information, the ZTNA system can require additional authentication or grant partial, full or no access.

MTD can enable ZTNA on unmanaged iOS and Android devices, making it suitable for BYOD and work-from-home scenarios. This can be on a per-application basis, so that, when a user launches an application on a device, the application allows access only when MTD is running on the device. MAM-WE [23] is Microsoft's implementation of this option, where organizations deploy Outlook and other Microsoft applications on unmanaged devices. [24] Using Microsoft's Conditional Access [25] and MTD, an organization can enable an unmanaged device to access Outlook securely, or deny access if a device is compromised, without affecting personal usage of the device, [26] but MTD solutions also support broader alternatives. [27]

Figure 4: MTD Enabling a Zero-Trust Model for Network Access for Mobile Devices



Gartner

Representative Vendors

Market Introduction

In this section, we provide a list of representative vendors in the MTD market (see Notes 4 and 5). MTD functionality typically covers:

- **Device-level configuration vulnerabilities:** The MTD solution can identify device configurations and settings that may expose a device or make a device vulnerable to attack. These may include, for example, the device being in developer mode, the device being rooted or jailbroken, or the OS version being outdated.
- **Malicious apps:** The MTD solution allows malicious apps to be identified and blocked or block-listed.
- **Network attacks:** The MTD solution can identify, block, prevent or remediate network attacks. Examples of attacks to be detected are SSL stripping, malicious iOS profiles, malicious URLs, rogue access Wi-Fi points and badly reputed IP addresses.

Most MTD vendors support both iOS and Android, and most products integrate out of the box with those of the Leaders in Magic Quadrant for Unified Endpoint Management.

Some MTD vendors provide additional functionality, including:

- **Device vulnerability management:** The product shows the vulnerabilities for the device fleet, based on model, OS version, carrier version and security patch level, and provides prioritization.
- **App vetting:** The product can block or identify apps that can perform actions or request permissions that are in conflict with enterprise policies and could lead to data leakage. These are not necessarily malicious apps. The enterprise administrator can customize the policies.
- **Anti-mobile phishing:** The product can identify or block malicious URLs.
- **Device attack protection:** The product can identify, block, prevent or remediate OS-level attacks.
- **Risk score:** The solution can process information and assign a security score for use as the basis of a decision to deny or grant access to a specific app.
- **Content filtering:** The product can put specific domains on a block list or disallow connection through specific access channels, such as cellular and Wi-Fi.
- **Cellular network attack protection:** The product can detect threats deriving from cellular network vulnerabilities, such as those in the SS7 protocol or the false base station attack (also known as Stingray, see Note 6).
- **Secure transport enforcement:** The product can provide transport security during an attack, either activating its own or a third-party VPN, or by performing sinkholing.

To help potential customers identify which MTD offering best addresses their needs, we have grouped vendors into categories (see Tables 1 through 4). Vendors' offerings are listed in the table or tables that best describe their focus. Vendors offer functionality with varying degrees of efficacy and granularity. This report does not rank MTD vendors or products.

Table 1: Vendors That Offer All-Round Mobile Threat Defense Capabilities

Vendor	*Product Name*
BETTER	Mobile Threat Defense
Check Point Software Technologies	SandBlast Mobile
Lookout	Mobile Endpoint Security
Pradeo	Mobile Threat Defense
Wandera	Threat Defense
Zimperium	zIPS

Source: Gartner (March 2021)

Table 2: Vendors That Offer Network-Focused Mobile Security Capabilities

Vendor	*Product Name*
Akamai	Asavie SD Mobile
Corrata	Security and Control
Cisco	Security Connector
Palo Alto Networks	GlobalProtect
Wandera	Threat Defense

Vendor	Product Name

Source: Gartner (March 2021)

Table 3: Vendors That Offer Mobile Security Capabilities as Part of an EPP or UES Offering

Vendor	Product Name
BlackBerry	Protect for Mobile, Persona for Mobile
Check Point Software Technologies	SandBlast Mobile
CrowdStrike	Falcon for Mobile
Cybereason	Mobile
Deep Instinct	D-Client
Kaspersky (see Note 7)	Security for Mobile
McAfee	MVISION Mobile
Microsoft	Defender
Sophos	Intercept X for Mobile
Symantec	Endpoint Protection Mobile
TEHTRIS	Mobile Threat Defense

Source: Gartner (March 2021)

Table 4: Vendors That Offer Mobile Security Capabilities as Part of a UEM Offering

Vendor	Product Name
BlackBerry	Protect for Mobile, Persona for Mobile
IBM	Mobile Threat Management
MobileIron	Threat Defense

Source: Gartner (March 2021)

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Recommendations

Before investing in an MTD solution, security and risk management leaders should ensure they have a security baseline in place for their mobile devices (see Note 8). The most obvious way to enforce such a baseline is via a UEM solution. Usage of an MTD solution on top should aim not only to address advanced malicious threats, but also to improve enterprise security hygiene.

Organizations should prioritize the introduction of MTD on the basis of industry, applicable regulations, the sensitivity of data on mobile devices, use cases (for example, frequent international travel in high-concern countries) and organizational risk appetite.

Organizations that should plan to adopt MTD solutions sooner rather than later are:

- Those in high-security sectors.
- Those with large and fragmented Android device fleets (although we must point out that Google has recently made major improvements to the security and consistency of Android devices [28,29,30]).
- Those in regulated sectors such as finance and healthcare.

Security and risk management leaders looking for immediate, visible value to justify an MTD investment should use the app-vetting and device vulnerability management features. These two features enable them to demonstrate quickly how MTD reduces application risk and device risk.

Security and risk management leaders should integrate their chosen MTD solution with their incumbent UEM tool. They should favor app-based deployment, leaving proxy-based deployment

options for COBO use cases.

MTD deployment can be used as a first step toward a UES strategy (see Innovation Insight for Unified Endpoint Security), where modern endpoint management is used to manage devices (see Adopt Continuous Endpoint Engineering and Modern Management to Ensure Digital Workplace Success).

Where devices must stay unmanaged, such as in certain BYOD use cases, security and risk management leaders should use MTD to protect enterprise infrastructure.

Security and risk management leaders can use the list of MTD capabilities and features in the Market Introduction section to compile an MTD vendor shortlist. Apart from in certain high-security contexts and situations with specific mobile security needs, product differentiation is less important than strategic vendor fit. Additionally, we see no value in adopting antivirus solutions that do not provide behavioral anomaly prevention and detection, as the underlying mobile platforms already perform signature-based scans to look for malware.

Evidence

[1] New Wroba Campaign Is Latest Sign of Growing Mobile Threats, Dark Reading.

Fakespy Masquerades as Postal Service Apps Around the World, IT Security Guru.

SourMint: Malicious Code, Ad Fraud, and Data Leak in iOS, snyk.

Malicious Optimizers Hosted on Google Play Amassed 470,000 Downloads, Security Week.

Android App Infects Millions of Devices With a Single Update, Dark Reading.

[2] Project Zero: Introducing the In-the-Wild Series, Project Zero.

[3] Attackers Continue to Nibble at Apple's iOS Security, Dark Reading.

[4] You've Got (0-click) Mail!, ZecOps.

[5] Hiding in Plain Sight: PhantomLance Walks Into a Market, Secure List.

Operation Poisoned News: Hong Kong Users Targeted With Mobile Malware via Local News Links TrendLabs Security Intelligence Blog, Trend Micro.

Iran 'Hides Spyware in Wallpaper, Restaurant and Games Apps', BBC.

[6] Mobile Phishing, Microsoft.

[7] iOS 13 Will Dramatically Improve MDM for BYOD. Hello User Enrollment!, TechTarget.

[8] 9 Mobile Threats That Breach Android Enterprise's Containers Security, Pradeo.

[9] Lookout App Defense Penetrates Global Markets With New Customers and Strategic Partnerships, Helping Customers Prevent Data Compromise in Mobile Apps, Lookout.

Better Together: Guardsquare Partners With Zimperium to Provide Customers With Comprehensive Mobile App Protection, Guardsquare.

Create a Zero Trust strategy for Your Mobile Workers, Lookout.

[10] NetworkExtension, Apple Developer.

[11] Vetting the Security of Mobile Applications, NIST.

[12] What's Going on With TikTok, Insider.

[13] WhatsApp Issues Clarification Over New Privacy Policy; Says It's for Business Accounts, Republic World.

[14] Phishers Serve Fake Login Pages via Google Translate, SecurityWeek.

[15] Attackers Add a New Spin to Old Scams, Dark Reading.

[16] Mobile Is Now the Preferred Platform for Reading Email With More Than Half of All Email Opens, Return Path.

[17] Phishing Campaign Targeting Verizon Mobile Users, Dark Reading.

[18] Lookout Mobile Phishing Encounter Rates for EMEA 3Q19.

[19] BEC Goes Mobile as Cybercriminals Turn to SMS, Agari.

[20] 2019 Mobile Threat Landscape Report, CrowdStrike.

[21] Stealing Corporate Funds Still Top Goal of Messaging Attacks, Dark Reading.

[22] EndpointSecurity, Apple Developer.

[23] Add Mobile Threat Defense Apps to Unenrolled Devices, Microsoft.

[24] Tutorial: Protect Exchange Online Email on Unmanaged Devices, Microsoft.

[25] Mobile Threat Defense Integration With Intune, Microsoft.

Learn About Conditional Access and Intune, Microsoft.

[26] Microsoft Intune Brings Mobile Threat Defense to Unenrolled BYO Devices, Microsoft.

[27] Wandera Private Access Is a Zero Trust Network Access Solution, Wandera.

[28] Google Play Protect — App Defense Alliance, Google.

[29] Accelerating Android Updates, Android Developers.

[30] Devices, Android.

Mobile Phishing Report 2018, Wandera.

You've Got (0-click) Mail!, ZecOps.

A Spyware Vendor Seemingly Made a Fake WhatsApp to Hack Targets, Data Protection News.

Note 1: Grayware

Grayware apps are not necessarily malicious, but can conflict with enterprise policies or even put enterprise data at risk. Grayware includes "leakware" — apps that can lead to data leakage. An example of grayware or leakware is an app that has permission to access the contact list of a device, and that collects this information and sends it to an advertiser.

Note 2: MTD App

Depending on the vendor and the options it provides, an MTD app can be distributed as an enterprise app or downloaded and installed directly from a commercial app store. Enterprise app onboarding might be more laborious if done manually without the aid of a mobile app management or UEM tool, but offers greater customization and access privileges. It can also provide better visibility and enforce more corrective actions on the device.

Note 3: MAM-WE

MAM-WE stands for Mobile Application Management — Without Enrollment. It is a particular way of provisioning devices with enterprise data without installing a management profile, but only an application profile.

Note 4: Representative Vendor Selection

This Market Guide identifies vendors that provide mobile security functionality, with a focus on those that can provide at least some MTD features. Gartner estimates that more than 25 vendors provide some degree of MTD functionality within the broader mobile security market.

Note 5: Gartner's Initial Market Coverage

This Market Guide provides Gartner's initial coverage of the market and focuses on the market definition, rationale for the market and market dynamics.

Note 6: False Base Station Attacks

A false base station attack (also known as a Stingray attack) is a network attack that exploits the cellular connection of a device. Similar to a rogue Wi-Fi access point, a false base station pretends to be a legitimate cellular base station to attract connections from one or more cellular devices. Under certain circumstances, a false base station can act as a "man in the middle," intercepting traffic. At minimum, it can obtain the permanent international mobile subscriber identity (IMSI) identifier of a cellular device. A false base station is therefore also called an "IMSI catcher."

Note 7: Kaspersky

In September 2017, the U.S. government ordered all federal agencies to remove Kaspersky's software from their systems. Several media reports, citing unnamed intelligence sources, made additional claims. Gartner is unaware of any evidence brought forward in this matter. Kaspersky launched its Global Transparency Initiative (GTI), established data centers in Switzerland to relocate customer data processing functions, and launched transparency centers in Switzerland and Spain to allow external review of its internal processes and its products' source code. The company has undergone a SOC 2 Type 1 audit by a Big 4 firm and obtained ISO/IEC 27001:2013 certification, and increased bug bounty awards up to $100,000 for security researchers. Kaspersky is continuing to migrate North America and Europe customers and plans to open additional transparency centers in Kuala Lumpur, Malaysia, and São Paulo, Brazil. Gartner clients who work directly with U.S. federal agencies should consider this information in their vendor selection and continue to monitor this situation for updates.

Note 8: Baseline

A security baseline for mobile devices should include measures to:

- Maintain minimum OS and device standards, and disallow enterprise access to unpatched devices, as well as to devices that do not receive patches in a timely manner. (Typically, this limits the device list to recent iOS and Android Enterprise Recommended devices, but Gartner maintains a more granular analysis of the list of minimum versions in Mobile OSs and Device Security: A Comparison of Platforms.)
- Forbid app sideloading (see Note 9), and only allow downloads from official app stores and the enterprise store.
- Prohibit jailbreaking and rooting of devices, as well as unlocked bootloaders.
- Enforce a complex passcode (at least six-character alphanumeric, with the option to use biometric-based authentication) and impose encryption, as well as a passcode retry limit.
- Establish a remote wipe procedure in case of loss or prolonged inactivity, and conduct periodic encrypted backups.

Note 9: Sideloading

In the context of mobile apps, sideloading refers to the practice of a user installing an app on a mobile device without downloading it from an app store. Rather, the user installs the app from another device, such as a macOS or Windows laptop. This practice creates security issues, as it bypasses the app store curation mechanism and can introduce malware to the device.