Market Guide for Mobile Threat Defense Solutions

Published: 22 August 2017 **ID:** G00314969

Analyst(s): Dionisio Zumerle, John Girard

The signs are clear that mobile threats can no longer be ignored. Security and risk management leaders must familiarize themselves with mobile threat defense solutions and plan to gradually integrate them to mitigate mobile risks.

Key Findings

- The mobile threat defense (MTD) market is growing in terms of adoption, and has started to attract some attention from endpoint protection platform (EPP) players and other related markets as it does so.
- There is still a lot of confusion and uncertainty from end users regarding which risks MTD addresses and how urgent or useful MTD can be.
- MTD solutions address device-, network- and application-level threats on iOS and Android platforms by employing crowdsourced threat intelligence and behavioral anomaly detection.
- Mobile app reputation solutions used to perform app vetting are converging with MTD in a single solution.

Recommendations

Security and risk management leaders responsible for mobile security must:

- Introduce MTD solutions gradually depending on industry, applicable regulations, sensitivity of data on mobile devices, use cases and organizational risk appetite. Policy enforcement will not suffice indefinitely as a security intervention.
- Adopt MTD solutions sooner in high-security verticals, with large Android device fleets, or in regulated verticals, such as finance and healthcare.
- Integrate the MTD solution with the enterprise mobility management (EMM) tool. Network traffic proxying deployment options should be selected only where bring your own device (BYOD) is not an important factor, and where strict device management is applied.

Strategic Planning Assumptions

By 2019, mobile malware will amount to one-third of total malware reported in standard tests, up from 7.5% today.

By 2020, 30% of organizations will have MTD in place, an increase from less than 10% in 2017.

Market Definition

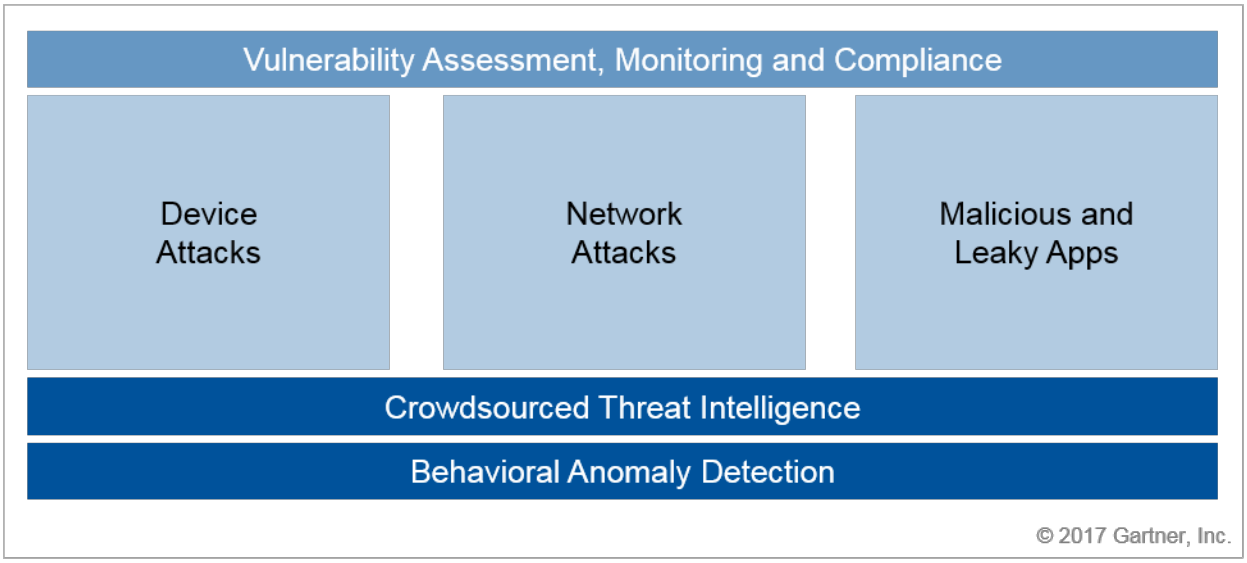
The MTD solution market is made up of solutions that protect organizations from threats on mobile platforms. iOS and Android are the main focus, with some solutions also supporting Windows 10 Mobile.

MTD solutions protect at the device, network and application level:

- On the **device** level, MTD tools monitor system parameters, configuration, firmware and libraries to identify suspicious or malicious activity. Device-level attack detection includes detection of modification of system libraries, system configuration and advanced ways to detect privilege escalation (such as jailbreak or rooting). MTD solutions also check OS versions and security patching to ensure that devices are not prone to major vulnerabilities.
- On the **network** level**,** MTD tools monitor network traffic and disable suspicious connections to and from mobile devices. Techniques include checks for invalid or spoofed certificates and Secure Sockets Layer (SSL) stripping. A variety of other customized man in the middle (MITM) detection techniques are applied. For example, the MTD solution can check for bidding down attacks from the network, where the encryption algorithm negotiated is intentionally weak.
- On the **application** level, MTD tools identify "leaky" apps (meaning apps that can put enterprise data at risk) and malicious apps, through reputation scanning and code analysis. Techniques include signature-based anti-malware filtering, code emulation or simulation, reverse engineering, and static and dynamic app security testing. Mobile app reputation solutions (MARS) have merged with MTD solutions.

MTD solutions provide protection in three phases by preventing, detecting and remediating attacks (see Figure 1). They should employ crowdsourced threat intelligence and behavioral anomaly detection to identify indicators of compromise, and counter threats. By serving a large fleet of devices, MTD solutions can identify what behavior is normal and flag behavior that is not. Also, enterprises can obtain information on current attack trends.

Figure 1. Functionality and Capabilities of MTD Solutions



Source: Gartner (August 2017)

MTD solutions are typically composed of an on-device agent in the form of an app; a server component, which is usually cloud-based; as well as an administrative console that enables enterprises to monitor, report and audit. The console provides identification and categorization of devices (including vulnerability assessment), suggests mitigating measures and prioritizes intervention on vulnerable devices.

Market Direction

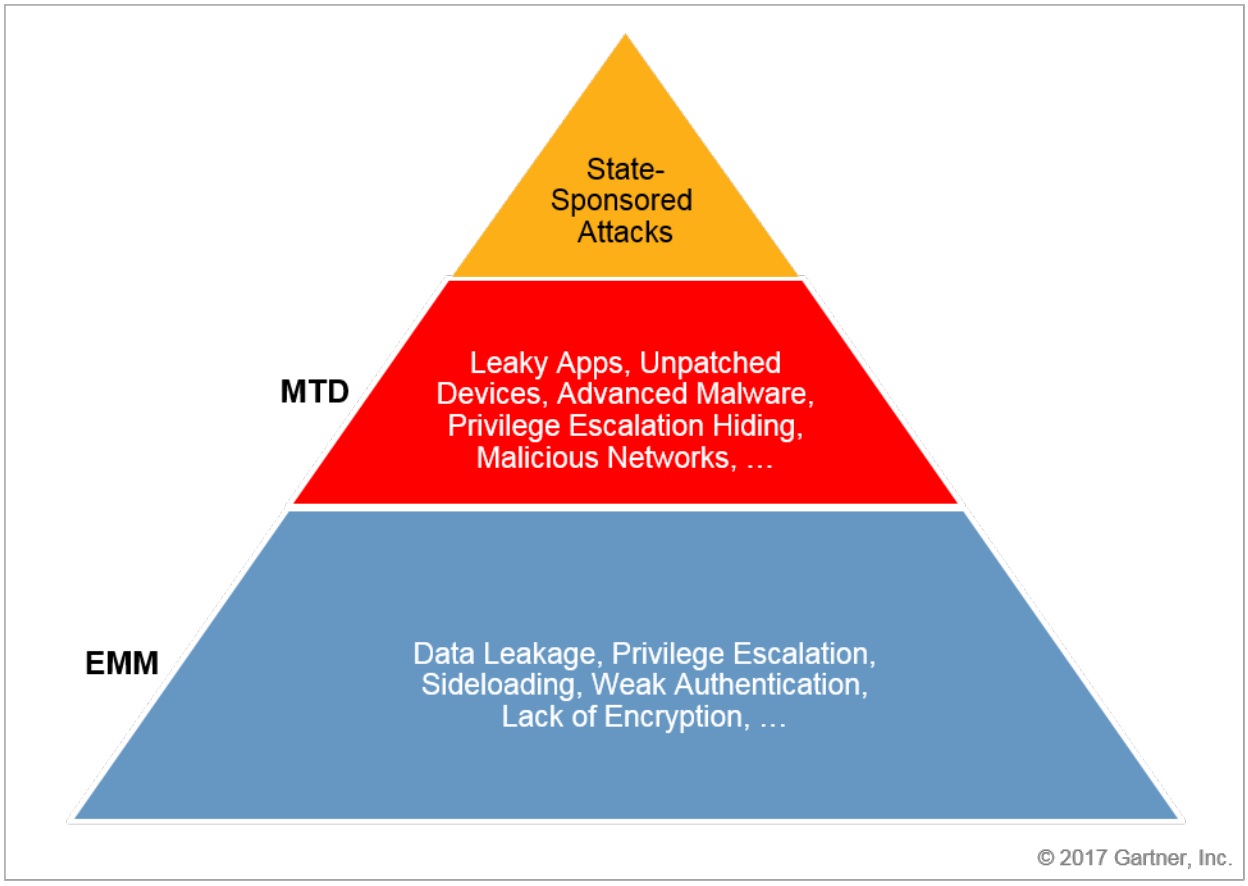
Several signs indicate that mobile malware is growing in importance:

- Mobile malware has grown more than 100% year over year in 2016, representing approximately 7.5% of all malware (Windows malware represents approximately 67% of all malware).[1]
- The high-severity vulnerabilities (CVSS 7-10) registered for Android have increased from 77 in 2015 to 335 in 2016.[2]
- In March 2017, for the first time more Android than Windows simultaneous internet connections were observed,[3] while mobile represents 45% of the total transactions.[4]

Although our examples mention Android prevalently, threats also affect, to a lesser extent, iOS devices.[5] Enterprise concern about threats that EMM tools do not counter drives the MTD market and adoption. These are typically malicious threats (for example, eavesdropping over untrusted wireless networks) or data leakage risks that elude EMM controls (such as spyware apps). Less frequently, the driver is that enterprises also want to avoid endpoint management and support, but want to ensure that the endpoints that access their network can be trusted. In some cases,

regulatory requirements, security audits or a specific internal incident spark MTD enterprise initiatives. As MTD solutions mature, security departments become the main buying center, rather than mobility or IT operations, to provide visibility and actionable intelligence. Figure 2 highlights the main needs and requirements addressed by MTD and EMM. Enterprises that have reasons to believe they require protection from state-sponsored attacks should not mistake MTD for an antidote to those attacks and recognize the difficulty and high costs involved in countering those type of threats. "Market Guide for Secure Mobile Communications" illustrates some purpose-built mobile devices that could be used for those very specific cases.

Figure 2. Mobile Security Threats Addressed by EMM and MTD



Source: Gartner (August 2017)

Gartner estimates the market to amount to less than $100 million at the conclusion of 2016, with most vendors being small and privately held, and at their second or third round of funding. For 2017, Gartner estimates 100% growth year over year. More general market growth potential is considerable if MTD follows the footsteps of its endpoint management counterpart, EMM. Notwithstanding the rapid growth, most enterprises have been slow to adopt MTD solutions because:

- Mobile platforms have been designed without any backward compatibility obligations, putting in place lessons learned from nearly three decades of endpoint security for PCs. Security

mechanisms such as application sandboxing, app store curation and limiting user permission privileges have delivered stronger security than for PCs.

- The lack of highly visible and successful mobile attacks against enterprises has not encouraged organizations to go beyond EMM to protect their mobile devices. Enterprises tend to underestimate the residual risk that can come from malicious threats, privileging approaches that can minimize data leakage.

Although the market is just starting to grow and it might be too small for larger endpoint protection vendors to play in, we have experienced the first signs of consolidation.[6, 7] Even so, we are not seeing actual MTD integration with EPP solutions yet. This could be the case in the long term as mobile and PC platforms evolve and converge, but currently MTD solutions operate in a manner that is distinct from the way EPP solutions do.

Market Analysis

Many of the solutions in this market come from new, small and innovative companies. The malware detection techniques used by MTD are still maturing, and the mobile platforms they have to run on are also rapidly evolving. In addition, the same mechanisms that harden mobile platforms against attacks reduce visibility for MTD and, therefore, their efficacy. Apple and Google are imbuing their mobile platforms with security functionality that may suffice for consumer needs, but not for enterprises. Enterprises need mobile platforms to open up more MTD capabilities.

MTD solutions come in four main architectural implementations, shown in Figure 3:

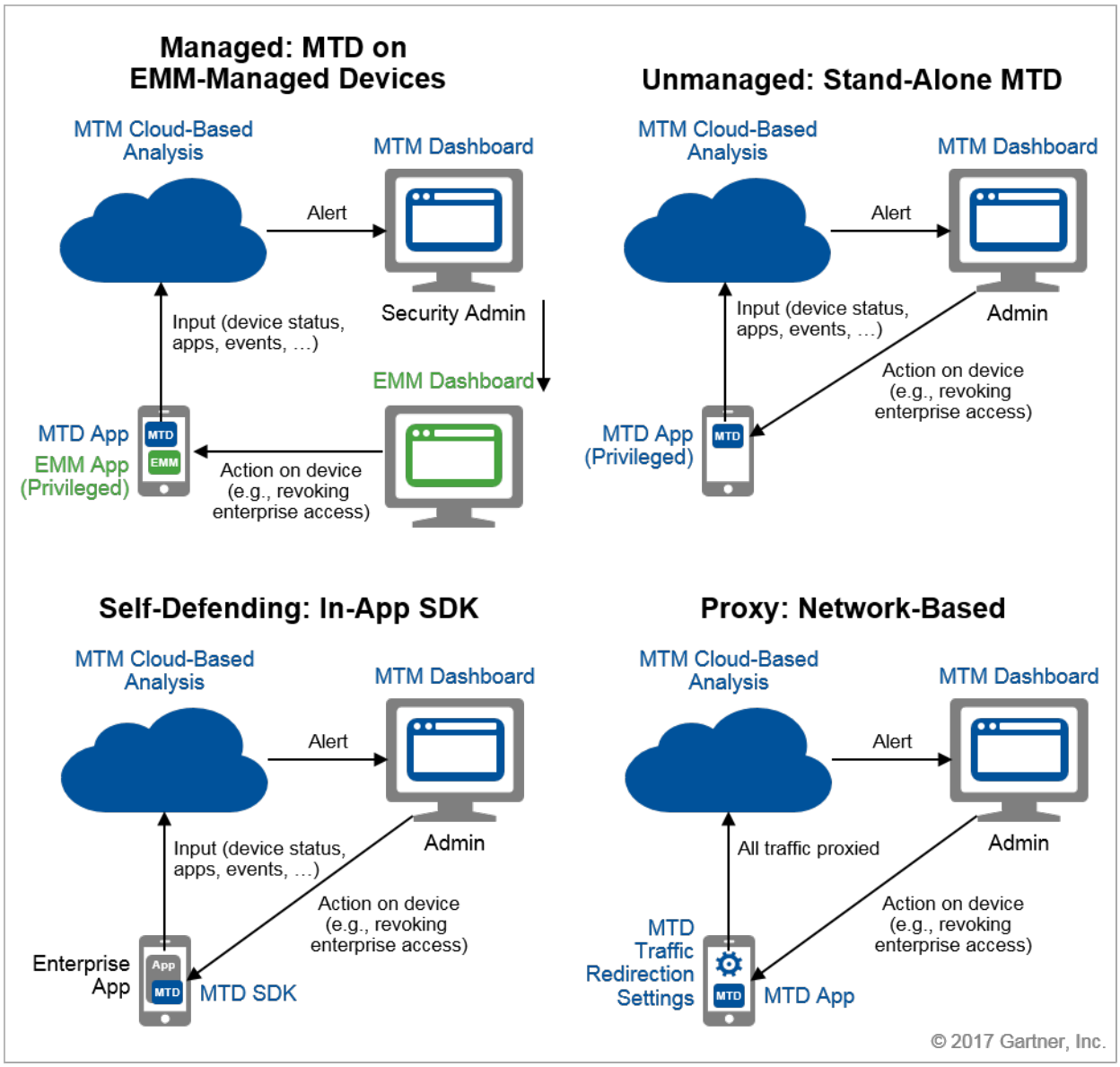
- The most common option is **MTD integrated with EMM on managed devices.** In this configuration, MTD leverages EMM to obtain information about the device, to perform disciplinary actions on the device or to be provisioned on the device. EMM is privileged in the sense that it has an MDM profile on the device, which allows it to take actions, such as performing a remote wipe. The MTD app on the device collects information that it sends to the cloud-based engine to identify attacks and update the defense engine. When an attack or an indicator of compromise is identified, the engine sends an alert to the MTD dashboard, which notifies the EMM dashboard. Action is then taken on the device depending on the organizational policies.
- MTD can also be deployed on **unmanaged devices**. In this setup, everything works similarly, but indicators of compromise cannot trigger as important remediating actions as in the previous case. With some variations and exceptions, this option would operate as follows:

  The MTD app can be privileged instead of the EMM one. While running an MDM profile for MTD solutions is rare, and would revert to a managed approach, the MTD app can be distributed as an enterprise app, rather than installed from the commercial app store, to allow a few more privileges to the app.

For example, an MTD solution can set up a VPN that selectively (for corporate apps) or collectively redirects traffic back to the device, to avoid allowing a compromised device to access corporate resources.[8]

- MTD solutions also start to come in the form of an **SDK** to embed into an app. This can serve to protect consumer-facing apps, or employee- and contractor-facing apps over unmanaged setups. The functionality is similar to the previous case, but the remediation options will focus on actions to be taken in the app itself, rather than on the device. For example, the app may decide to abort operation if it identifies the presence of malware on the device. Some MTD vendors are partnering with app shielding vendors to provide broader functionality, or extending their functionality to encompass app shielding (see "Market Guide for Application Shielding").
- The last option looks at implementations that observe and analyze **network** traffic. In this case, the MTD solution redirects the traffic to and from the device to the analysis engine. There, it can analyze the traffic, filter malware and provide SWG-like functionality, such as domain blacklisting. On the one side, this option adds much more visibility than an app on a device can have. On the other side, the privacy implications for users having all of their traffic constantly monitored will appeal to organizations without large BYOD programs. Enterprises that will find this approach more suitable have iOS-supervised devices and higher security requirements.

Figure 3. MTD Deployment Options



Source: Gartner (August 2017)

MTD vendors are also starting to partner with carriers, both to offer managed mobility services to enterprises as well as to offer consumer solutions (freemiums or as parts of carrier bundles). The latter ones are important not only to grow revenue, but also to increase the crowdsourced-based threat intelligence used.

Representative Vendors

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.

In this section, we provide a list and description of representative vendors in the MTD space. This research does not rank the threat defense performance or granularity of functionality of these products. We have observed a common baseline of functionality that all MTD vendors offer in 2017. The functions include:

- Device-level configuration vulnerabilities: The solution can identify device configurations and settings that can expose the device or make the device vulnerable to attacks. An example might be the device being set in developer mode, or being jailbroken.
- Malicious apps: The solution allows malicious apps to be identified and blocked or blacklisted.
- Network attacks: The solution can identify, block, prevent or remediate network attacks. Examples of attack techniques to be detected are SSL stripping, malicious iOS profile, rogue access Wi-Fi point and badly reputed IP addresses.
- OS version and vulnerability assessment: The solution can identify devices that are running outdated or vulnerable OS versions among the enterprise device fleet. Ideally, it can prioritize them by severity, as well as send alerts.
- Behavioral anomaly detection: The solution can identify, block, prevent or remediate attacks by observing unusual behavior for which it does not have a malicious signature.
- Crowdsourced threat intelligence: The solution collects, aggregates and analyzes threat intelligence from the device it protects. This intelligence is used to identify attack trends and patterns, which it then uses to improve the MTD solution.

Beyond the fundamentals that make the basis for MTD and that the representative vendors in this research all support, Table 1 provides a summary of additional capabilities of the representative MTD vendors discussed.

The situation is that depicted at the time of writing; however, MTD is a space under rapid evolution. We are aware of a number of feature additions and product integrations that are either under testing or scheduled to be added within the next few months.

Table 1. OS Support, Integration Options, Deployment Options and Additional Functionality Support for MTD Solutions (All Solutions Support Core MTD Functionality)

Vendor	OS Support	OS and Kernel-Level Attacks	Leaky Apps	Cellular Network Attacks	URL Filtering	Secure Transport Enforcement	EMM/MAM Integration	SIEM Integration	Deployment Method (app, SDK, proxy)	On-Premises Option
Appthority — Mobile Threat Protection	iOS, Android	No	Yes	No	No	No	AirWatch, MobileIron, Citrix	Splunk, API	App	Yes
Better Mobile Security — Mobile Threat Defense	iOS, Android, Windows 10 Mobile	Yes	Yes (lightweight DLP capabilities)	False base station	Yes	VPN	AirWatch, MobileIron, Citrix, Microsoft	Splunk, Hewlett Packard Enterprise ArcSight, IBM QRadar, LogRhythm, API, syslog	App, SDK	Yes
Check Point — SandBlast Mobile	iOS, Android	Yes	Yes	Yes (via Vaulto)	No	VPN	AirWatch, MobileIron, IBM, Microsoft, Citrix, BlackBerry	Splunk, QRadar, ArcSight, Check Point Smart Event, syslog	App, SDK	Yes
Cyber adAPT — skwiid	iOS, Android, Windows 10 Mobile	No	Yes	No	Yes	VPN	AirWatch, IBM, Microsoft, MobileIron	Splunk, REST API, syslog	Proxy	Yes
Kaymera Adaptive Mobile Threat Defense	iOS, Android	Yes	Yes	False base station	Yes	VPN	AirWatch, MobileIron	Syslog	App	Yes

Vendor	OS Support	OS and Kernel-Level Attacks	Leaky Apps	Cellular Network Attacks	URL Filtering	Secure Transport Enforcement	EMM/MAM Integration	SIEM Integration	Deployment Method (app, SDK, proxy)	On-Premises Option
Lookout — Mobile Endpoint Security	iOS, Android	Yes	Yes	False base station	Yes (Android)	Blackholing	AirWatch, BlackBerry, MobileIron, Microsoft, IBM	Splunk, ArcSight, QRadar, API	App, SDK	No
Pradeo — Mobile Threat Defense	iOS, Android, Windows 10 Mobile	No	Yes	No	Yes (Via Pradeo browser)	Via Pradeo browser	AirWatch, BlackBerry, Microsoft, MobileIron, IBM, SOTI	Splunk, QRadar, ArcSight, syslog	App, SDK	Yes
Proofpoint — Mobile Defense	iOS, Android	No	Yes	No	Yes (SMS, iMessage and email URL protection)	No	AirWatch, MobileIron, IBM, API	Syslog	App, Proxy	No
Symantec-Skycure — Enterprise Mobile Threat Defense	iOS, Android	Yes	Yes	No	Yes	VPN and blackholing	AirWatch, BlackBerry, Citrix, MobileIron, IBM, Microsoft	ArcSight, QRadar, LogRhythm, RSA, Splunk, McAfee, Fortinet, API, syslog/CEF	App, SDK	No
Wandera — Threat Defense	iOS, Android, Windows 10 Mobile	Yes	Yes	False base station	Yes	VPN	AirWatch, BlackBerry, Cisco, Citrix, IBM, Jamf, Microsoft, MobileIron, SAP Afaria, SimpleMDM	Splunk, RSA Security Analytics, ArcSight QRadar, syslog/CEF	App, Proxy	Yes

Vendor	OS Support	OS and Kernel-Level Attacks	Leaky Apps	Cellular Network Attacks	URL Filtering	Secure Transport Enforcement	EMM/MAM Integration	SIEM Integration	Deployment Method (app, SDK, proxy)	On-Premises Option
Zimperium — zIPS	iOS, Android, Windows 10 Mobile	Yes	Yes	False base station	No	VPN	AirWatch, BlackBerry, Matrix42, MobileIron, Microsoft, Citrix, SAP Fiori	Splunk, ArcSight, syslog	App, SDK	Yes

Table legend:
OS support: Operating systems that the MTD solution supports (out of iOS, Android, Windows 10 Mobile).
OS and kernel-level attacks: The solution has functionality that can allow it to identify, block, prevent or remediate OS or kernel-level attacks.
Leaky apps: The solution has functionality that allows it to block, blacklist or identify apps that, while not necessarily malicious, can or do perform actions or request permissions that are in conflict with enterprise policies and could lead to data leakage.
Cellular network attacks: The solution is able to detect threats deriving from cellular network vulnerabilities such as the ones in the SS7 protocol or the false base station (aka Stingray) attack (see Note 1).
URL filtering: The solution can block malicious URLs or internet domains based on policy.
Secure transport enforcement: The solution can provide transport security during an attack (for example, by activating its own or a third-party VPN when it identifies a network or other related threat). Blackholing suggests that the solution can instead block traffic from the device toward the enterprise to protect the enterprise from a compromised device.
EMM/MAM integration: EMM/MAM solutions that the MTD solution functionally integrates with, availability of an API for integration with further products.
SIEM integration: SIEM solutions that the MTD functionally integrates with. Additionally or alternatively, availability of an API for further integrations, or support of syslog or CEF formats.
Deployment method (app, SDK, proxy): As described in Figure 3. App suggests that the solution can be deployed stand-alone or integrated with EMM.
On-premises option: The solution can be deployed on-premises in the enterprise.

Source: Gartner (August 2017)

Appthority

www.appthority.com/solution/overview/

Appthority provides MTD by protecting against leaky and malicious apps, mobile device compromise, and active network threats. Compliance management is enforced directly on the user device using an optional agent, as well as through integration with EMM. Malicious and risky app behaviors are detected through static analysis of the binary code and dynamic behavioral analysis via code emulation or execution. Appthority looks for risk indicators of compromise among policies enforced on the device, potentially malicious network addresses and app-accessible back-end databases for exposed vulnerabilities. Appthority integrates with Google's Android enterprise, and provides a SIEM connector to enable SIEM integration and reporting following a publish-subscribe pattern. Appthority provides on-premises integration/connectivity with EMM systems leveraging an EMM connector as a virtual appliance to be deployed inside the customer's network.

Better Mobile Security

https://better.mobi/mobile-threat-defense

Better Mobile Security provides continuous on-device monitoring of mobile threats with detection, prevention and remediation capabilities. Better Mobile Security addresses network and device threats, including monitoring for OS and kernel-level attacks. On the application level, Better Mobile Security performs checks for malicious signatures, source origin and permissions; conducts static and dynamic analysis; and leverages artificial intelligence models to detect and protect against a wide range of known and unknown app threats. Remediation can take place via integration with EMM, and integration with SIEM is also possible. Better Mobile Security has an integration in place for Office 365, and provides a separate SDK for unmanaged devices as well as lightweight DLP capabilities for mobile devices. Better Mobile Security also integrates with ServiceNow for IT service management.

Check Point

www.checkpoint.com/products/sandblast-mobile/

Check Point's SandBlast Mobile uses technology from the Lacoon Mobile Security acquisition, as well as Check Point technology, such as ThreatCloud, and provides MTD for iOS and Android devices. SandBlast Mobile employs app scanning, SMS anti-phishing and cross-platform attack protection, combined with network and device anomaly detection. Some of the analysis takes place on the device and some of it occurs in the cloud. In the cloud, the app goes through a series of engines including advanced static code flow analysis, dynamic sandboxing (emulation) and machine learning. If a device is suspected of being under attack, SandBlast Mobile can force communications into a closed/quarantined tunnel as well as guide the user to remove the threats from their device. SandBlast Mobile integrates with Vaulto to protect from mobile network attacks such as SS7 vulnerabilities and IMSI catchers. SandBlast Mobile also provides a scalable cloud-based management portal, an on-premises option and an MSSP managed platform, and integrates with major EMM and SIEM tools.

Cyber adAPT

www.cyberadapt.com/skwiid/skwiid-mobile/

Cyber adAPT's skwiid is a network-based platform approach to MTD. In its default configuration, skwiid provides agentless EMM capabilities that feature zero footprint online management of mobile devices, and it can also coexist with other EMM solutions, such as MobileIron and VMware AirWatch. Using a continuous VPN connection built for mobile, skwiid monitors all mobile traffic to network and cloud services, and it will identify anomalies and malicious attacks in these connections. A local agent version is available for deeper analysis and offline protection. Cyber adAPT has modified its original end-user management platform to service unattended Internet of Things (IoT) devices, starting with security cameras.

Kaymera

www.kaymera.com/mobile-threat-defense/

Kaymera provides MTD by identifying attack patterns, indicators of compromise and behavioral anomalies on the network, app and device level. In addition, Kaymera Adaptive MTD takes into account the context in which devices are being used. Kaymera assigns a risk profile to the user (for example, based on seniority or the sensitivity of the data residing on the device). Kaymera AMTD also integrates with EMM solutions to provide remediation. To promote users following best practices, the solution also provides an individual score for each device that increases with best practices followed.

Lookout

lookout.com/products/mobile-endpoint-security

Lookout detects iOS and Android threats and attacks across the app (including malicious, sideloaded and leaky ones), network and device. Lookout's detection uses global crowdsources, including app binaries, OS fingerprints and network connections, and periodic code samples from monitored devices. Administrators can set customizable app, network and device policies, while alerts and advice are also given to the user of the device. Lookout provides a blackholing solution that inhibits the device from contacting and infecting the enterprise network in case of device compromise. Lookout interfaces with EMM tools to facilitate remediation and can also be deployed inside Android Enterprise and Samsung Knox containers. While Lookout does not provide an on-premises option, it provides certain privacy controls to protect information.

Pradeo

www.pradeo.com/en-US/mobile-threat-protection

Pradeo 360° Mobile Threat Protection is an MTD solution that provides application scanning to detect and qualify behavior and vulnerabilities, as well as identification of device and network anomalies. Pradeo's solution is based on a crowdsourced engine that leverages machine learning and combines static, dynamic and behavioral analysis. On the network side, the solution analyzes

network configuration and parameters to prevent attacks. On the device side, Pradeo analyzes the device configuration and settings to identify anomalies. Pradeo 360° Mobile Threat Protection can integrate with EMM suites to ensure that devices comply with security policies. In addition, the solution offers a secure browser and a secure email client.

Proofpoint

www.proofpoint.com/us/products/mobile-defense

Proofpoint Mobile Defense originates from the acquisition of Marble Security in July 2015. The solution operates by simply leveraging an existing MDM on the device, or with an optional on-device Proofpoint app. The integration with MDM allows the detection of app-level threats, while the Proofpoint app adds protection against zero-day attacks, risky Wi-Fi networks and malicious URLs delivered via text or email message. The Proofpoint app also makes it possible to see which apps are compliant or noncompliant based on enterprise policy. The Proofpoint Mobile Defense service can be configured to address different privacy requirements, including anonymizing or removing any app information collection. Proofpoint Mobile Defense integrates via an API with EMM solutions.

Symantec-Skycure

www.skycure.com/mobile-threat-defense/

In July 2017, Symantec acquired Skycure. Skycure leverages crowdsourced threat intelligence, in addition to both device- and server-based analysis, to proactively protect enterprise mobile devices from malware, network threats and vulnerability exploits. Skycure provides predictive malware detection techniques, as well as static and dynamic analysis, crowd-based anomaly detection, and analyses based on signatures, app behavior, structure and permissions. Network threat defense includes a built-in VPN that protects the device, while maintaining network connectivity during an attack. A corporate resource protection feature blocks communication with specific valuable resources (mail servers, file shares and other business systems) during a network attack, while allowing noncritical connections. Skycure provides risk assessments and integrates with major EMM and SIEM products.

Wandera

wandera.com/solutions/threat-defense

Wandera combines network-based traffic monitoring and filtering with on-device threat detection for iOS, Android and Windows 10 Mobile. Wandera uses its MI:RIAM engine to identify misconfigurations, network and device behavioral anomalies, malicious or suspicious network connections, as well as suspicious apps. MI:RIAM is cloud-based and combines machine-learning as well as threat intelligence from various sources, including the devices that Wandera protects. Some capabilities such as device anomaly checks require an on-device agent. In addition to the classical MTD functions and URL filtering, Wandera can provide URL and domain policy enforcement to blacklist, for example, a specific VOD domain when roaming over 4G, but still allow it over Wi-Fi. The solution provides a privacy-preserving mode for those organizations that wish to use the proxy and still protect end-user usage details.

Zimperium

www.zimperium.com/zips-mobile-ips

Zimperium offers zIPS, an MTD solution that operates on the device. zIPS crowdsources and analyzes device configuration and parameters in the cloud, and then updates its engine, z9, on the device. Zimperium identifies malicious apps, tackles network threats and device threats, and includes checks for OS and kernel-level attacks. zIPS also partners with Mi3 to provide app scanning for leaky apps. zIPS provides comprehensive dashboard functionality. Zimperium also offers an SDK, called zIAP, which integrates with SAP Fiori. Zimperium has an integration with major EMMs, as well as the possibility to integrate with SIEM tools that support syslog format. The vendor also partners with a number of carriers to provide MTD as part of mobility services, as well as for consumer applications.

Other Vendors

A number of other vendors have solutions that are relevant to this technology space. Gartner can discuss further vendors in client inquiry, including Asavie, BlackBerry, Corrata, Deep Instinct, IBM, Kaspersky Labs, NowSecure, Opswat, Palo Alto Networks, Sophos, Vaulto, Webroot and Zscaler. FireEye's MTP, which was on last year's list of representative vendors, has been discontinued.

Market Recommendations

Before investing in any MTD solution, security leaders should be sure to have a security baseline in place for mobile devices, possibly enforced via their EMM solution, including:

- Maintaining minimum OS and device standards in place and disallowing enterprise access to unpatched or older devices
- Forbidding app sideloading, and only allowing the official app stores and the enterprise one
- Prohibiting jailbreak/rooting
- Enforcing a complex enough passcode (six character alphanumeric at a minimum) and/or fingerprint-/iris-based authentication, enforcing encryption, as well as having a retry limit
- Enforcing a remote wipe procedure, as well as a periodic encrypted backup

Gartner advises organizations to gradually introduce MTD solutions based on their industry, applicable regulations, sensitivity of data on mobile devices, use cases (for example, frequent international travel in high-concern countries) and organizational risk appetite. Security leaders should recognize that the policy enforcement that organizations apply will not suffice indefinitely as a security intervention. Organizations in high-security verticals, those with large Android device fleets or those in regulated verticals such as finance and healthcare should plan to adopt MTD solutions sooner rather than later. MTD can also be used as a starting point for bring-your-own security negotiation when legal issues or user complaints are a barrier to EMM.

Security leaders should strive to select a solution that integrates with their incumbent EMM tool. The network-based deployment option is more suitable where BYOD is not an important factor, and where strict device management is applied.

Security leaders should shortlist solutions based on their needs, focusing on understanding the core MTD capabilities. The functionality analyzed in Table 1 will provide further understanding of the completeness of a solution. "Comparison of Mobile Threat Defense Solutions" provides an evaluation of MTD solutions against specific threats, and also illustrates a sample methodology to evaluate solutions. Completeness of product will be as important, if not more, than efficacy of the response. Security leaders should realize MTD tools, especially on iOS, have limited visibility on the system and background processes. OS features such as app sandboxing that protect mobile devices from attacks, are the same that inhibit security solutions from fully monitoring what occurs on the device.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"When and How to Go Beyond EMM to Ensure Secure Enterprise Mobility"

"Comparison of Mobile Threat Defense Solutions"

"Comparing Approaches to Mobile Security Strategies"

"Critical Capabilities for High-Security Mobility Management"

"Compare EMM Security Ecosystems to Make a Strategic Selection"

"Market Guide for Secure Mobile Communications"

"Hype Cycle for Mobile Security, 2017"

Evidence

[1] AV-Test Security Report 2015/2016.

[2] Information-technology Promotion Agency, Japan, "Vulnerability Countermeasure Information Database JVN iPedia Registration Status (2016 fourth quarter [Oct.-Dec.])."

[3] "Android Overtakes Windows for First Time," StatCounter GlobalStats.

[4] "Cybercrime Report Q1 2017," ThreatMetrix.

[5] "Malware for iOS," The iPhone Wiki.

[6] "Symantec to Acquire Skycure, Providing Customers With Comprehensive Mobile Threat Defense Across iOS, Android and Windows," Symantec.

[7] "Check Point Aiming to Make Headway in Mobile Security by Buying Lacoon," Tech Times.

[8] "Actions Speak Louder Than Words: Why Automated Mobile Threat Prevention Is the Key to Mobile Threat Defense," Skycure.

Note 1 False Base Station Attack

The false base station attack (also known as Stingray) is a network attack that affects and leverages the cellular connection of a device. Similarly to a rogue access point attack for Wi-Fi, a false base station pretends to be a legitimate cellular base station, in order to allure connections from one or more cellular devices. Under certain circumstances, a false base station can act as a "man in the middle," intercepting traffic, and can at a minimum obtain a permanent identifier of the cellular device, called IMSI. A false base station is also called an IMSI catcher for this reason.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp