G00293658

Market Guide for Mobile Threat Defense Solutions

Published: 28 July 2016

Analyst(s): John Girard, Dionisio Zumerle

It is becoming increasingly important that security leaders look at the anti-malware, mobile threat defense solutions market, the products available and how they should be used. Gradually add MTD systems to the organization to mitigate attacks, emphasizing integration, and avoid long-term contracts.

Key Findings

- Mobile threat defense solutions protect mobile platforms by addressing threats to devices, OSs, networks and apps.
- The techniques used in MTD are advanced and are still maturing, and the mobile platforms they run on are also rapidly evolving. Many of the solutions in this market come from small, new and innovative companies.
- Enterprise mobility management and other configuration control mechanisms already strengthen mobile platforms against attacks. They also make it harder for MTD solutions to have granular visibility and to operate efficiently.
- Companies can also use mobile app reputation solutions to prevent mobile threats.
- Many mobile threats exploit the configurations of unmanaged, jailbroken devices, and these exploits typically do not apply to enterprise-managed, nonjailbroken devices.

Recommendations

- Consider MTD to mitigate attacks that evade app store controls and safe device configuration and profile policies.
- Add MTD in your organization gradually, especially if you do not have security-focused EMM in such verticals as finance, healthcare, government, insurance and utilities.
- Avoid long-term agreements, and pick solutions that will integrate, rather than interfere with, your current or future EMM solutions, if you decide you want to use MTD.

Strategic Planning Assumptions

By 2018, fewer than 15% of organizations will have mobile threat defense (MTD) in place, which is an increase from fewer than 5% today.

By 2018, 80% of organizations with MTD solutions in place will integrate them with their enterprise mobility management (EMM) solutions, which is an increase from the fewer-than-5% current estimate.

Market Definition

The MTD solutions market is made up of products that protect organizations from threats on mobile platforms, including iOS, Android and Windows 10 Mobile. MTD solutions provide security at one or more of these four levels:

- **Device behavioral anomalies —** MTD tools provide behavioral anomaly detection by tracking expected and acceptable use patterns.
- **Vulnerability assessments —** MTD tools inspect devices for configuration weaknesses that will lead to malware execution.
- **Network security —** MTD tools monitor network traffic and disable suspicious connections to and from mobile devices.
- **App scans —** MTD tools identify "leaky" apps (meaning apps that can put enterprise data at risk) and malicious apps, through reputation scanning and code analysis.

MTD architectures vary; however, they typically involve an agent residing on the mobile device, as well as a server component that aggregates findings. MTD solutions use various methods to gather intelligence around mobile threats and attacks. Crowdsourced threat intelligence analysis is a prevalent method, and the server component is often cloud-based. Crowdsourced threat intelligence is often collected in addition to customer devices, from consumers that install a basic version of the app available in consumer app stores.

In addition to the device agent and the server component, an administrative console enables enterprises to report and audit. This console provides identification and categorization, suggests mitigating measures, and prioritizes intervention on vulnerable devices.

MTD tools are stand-alone, but can and should be able to interoperate with EMM tools to obtain information about the device, to perform disciplinary actions on the device, or to be provisioned on the device (see "When and How to Go Beyond EMM to Ensure Secure Enterprise Mobility").

Market Direction

MTD adoption is driven by enterprise concerns about threats that can't be countered with traditional mobile management tools, such as EMM. These are typically malicious threats (such as

eavesdropping over untrusted wireless networks) or data leakage risks that elude EMM controls (such as SMS-grabbing apps).

At this point, this market is modest; most vendors are small and privately held. Enterprises have been slow to adopt MTD solutions for several reasons:

- Mobile platforms have had the advantage of being designed from scratch after having observed and learned from nearly 30 years of personal computing. Hence, the security mechanisms implemented have been stronger from the beginning. App sandboxing, app store distribution and the limitations of user permission privileges are some examples.
- Soon after adopting mobile devices, enterprises realized they can be locked down more successfully than traditional PC devices. A strong mobile device configuration policy can minimize the risks of most of the forms of attack that enterprises have seen "in the wild" so far.
- The lack of highly visible and successful mobile attacks against enterprises, which can be used as a reference, has not encouraged organizations to go beyond EMM to protect their mobile devices. IT leaders must distinguish between real-world, mobile malware threats, and user self-inflicted exploits (which need to be solved by changing user behaviors), or mobile devices that were intentionally made vulnerable through jailbreaking and rooting, but would otherwise be at low risk.
- Companies get into serious trouble, and CIOs stay awake at night, as a result of data breaches that can be largely addressed in the mobile device world by means other than active threat defense. These include improved employee awareness training, better workflow design, secure app development, and the use of data loss prevention and disaster recovery management solutions.

However, basic policy enforcement will not suffice indefinitely. As mobile attack techniques become more practical and realistic (for example, the Stagefright vulnerability exploit, the iOS malicious profile and XcodeGhost), enterprises will be required to more quickly "step up their games" in terms of security.

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 that functionality may not suffice for enterprises.

Enterprises often need more control and visibility as to what happens on their devices, and the ability to correlate those events with events occurring on their infrastructure. Policies and requirements vary and certain app actions that may seem innocuous to a consumer may prove to be policy violations for an enterprise. Enterprises would need mobile platforms to provide more enterprise features and to increasingly open up functionality for preferred MTD vendors in the future.

Market Analysis

MTD solutions play a similar role for iOS and Android devices to that of endpoint protection platforms (EPPs) for traditional PC and Mac devices. Instead of mimicking EPP behavior on a mobile endpoint, efficient MTD solutions use techniques tailored for smaller, more resource-restrained devices. Many of the techniques used by these solutions resemble techniques encountered in advanced threat defense solutions (see "Five Styles of Advanced Threat Defense"). MTD solutions do not focus on prevention alone; they detect attacks and offer remediation steps. MTD solutions operate at the device, network and app levels.

The Device Level

On the device level, MTD tools provide behavioral anomaly detection and vulnerability assessments. Behavioral anomaly detection focuses on identifying unexpected behavior, rather than known malware, and is a step beyond simply reporting jailbreaks or rooting. For example, during an attack, MTD tools might observe an anomalous battery consumption surge, interpret it as the sign of intense activity caused by a malicious actor on the device, and investigate further to identify the attack.

Behavioral anomaly detection should not be completely automatic, and it could be done by the vendor's security operations center (SOC), which has access to device data. Anomaly detection also has its challenges, especially on iOS. The MTD app has limited visibility into configuration parameters and background processes. Synergy or partnerships with the device EMM, or with the mobile platform itself, can help reduce that limitation.

Vulnerability assessment provides a way to identify vulnerabilities for the specific device model and OS versions of the enterprise mobile device fleet. Tools will also provide additional methods to detect device privilege escalations (e.g., jailbreak and rooting) to what the EMM employs, which minimizes evasion possibilities. The purpose is to identify and categorize vulnerable devices, as well as mitigate risks, where possible. Here too, synergy with EMM can help to identify the device model, OS version and other characteristics that can help evaluate the device more precisely.

The Network Level

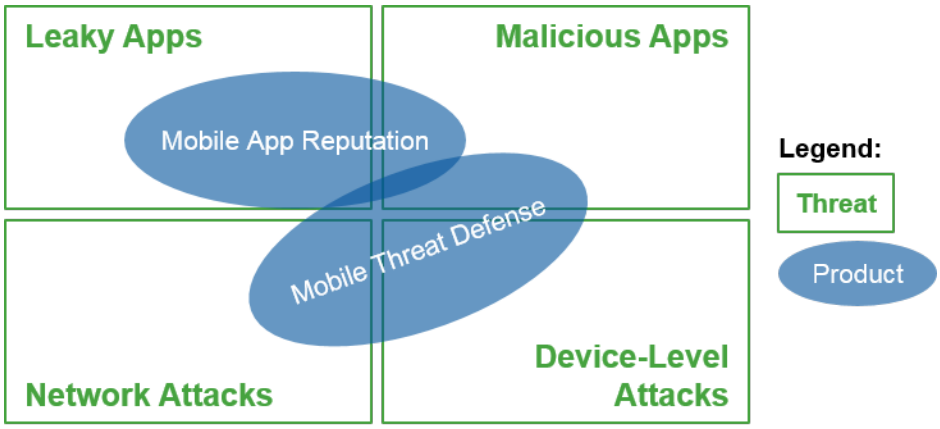
On the network level, MTD tools monitor network traffic and disable suspicious networks from mobile devices. MTD tools employ network intrusion prevention techniques, identify invalid certificates and Secure Sockets Layer (SSL) stripping, and guard against man in the middle (MITM) attacks. In certain instances, when an attack is identified, some MTDs intercept and redirect the connection over a secure tunnel, to avoid eavesdropping. MTD tools also identify rogue Wi-Fi access points that bear misleading service set identifier (SSID) addresses.

The App Level

On the app level, MTD tools' main goal is to identify malicious apps. To do so, MTD solutions apply static and dynamic malware detection techniques. Static techniques include signature-based, anti-malware filtering; reverse engineering; and static app security testing. Many commercial apps are obfuscated and may not easily reveal malicious code during static analysis.

Dynamic techniques include code emulation or remote execution of the app to identify malicious behavior. (A detailed description of many of the techniques used and adapted for a mobile environment, can be found in "Network Sandboxing for Malware Detection.") In this particular app security area, techniques and vendors overlap with the mobile app reputation solution (MARS) offerings. Different from MTD, MARS products focus on identifying leaky apps — i.e., apps that can put enterprise data at risk (see Figure 1). Because of this overlap, this Market Guide includes vendors that represent both categories.

Figure 1. Focus and Overlap of MTD and MARS



Source: Gartner (July 2016)

Not all vendors apply all of the techniques described, and there is a great deal of variety in the specific ways that vendors apply the different techniques, making it hard to compare or contrast them. The techniques are maturing, the vendors are evolving and a standard best method has not been identified.

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.

Although it's still young, this market has already begun to evolve and consolidate, with large and established security vendors entering the market either by acquiring smaller vendors, or by tailoring an existing offer for mobile devices. In addition, certain EMM vendors are partnering with and, in some instances, even acquiring MTD vendors. Gartner has compiled a list of companies that are promoting themselves in the MTD market. They are a mix of small, specialized startups and mainstream vendors.

Table 1. Functional Capabilities of MTD Vendors

Vendor	Behavior Anomaly Detection	Vulnerability Assessment	Network Security	App Scan
Appthority Mobile App Risk Management	√	√		√
Better Mobile Security Mobile Threat Defense	√		√	
BlackBerry DTEK		√[1]	√[2]	
Check Point Mobile Threat Prevention	√	√	√	√
Cyber adAPT Secure Device Management	√[3]	√[3]	√[3]	√[3]
Deep Instinct Mobile APT		√	√	√
FireEye Mobile Threat Prevention				√
IBM Mobile Threat Management	√	√		√
Lookout Mobile Endpoint Security		√	√	√
NowSecure Protect		√	√	√
Opswat Metadefender		√		√
Palo Alto Networks Global Protect			√[3]	√[3]
Pradeo Pradeo Apps Security		√		√
Skycure Enterprise Mobile Threat Defense	√	√	√[3]	√
Wandera Threat Defense	√	√	√	√
Zimperium zIPS	√	√	√	√

Vendor	Behavior Anomaly Detection	Vulnerability Assessment	Network Security	App Scan
Zscaler Zscaler App	√[3]	√[3]	√[3]	

The marked capabilities may not be available on all mobile platforms:
[1] Distribution limited to a monitored container
[2] Virtual private network (VPN) tied to monitored container
[3] Operates on traffic passing through VPN tunnel

Source: Gartner (July 2016)

Appthority

appthority.com/products

Appthority provides iOS and Android with automated and scalable threat defense and app reputation analysis, app security testing, device risk analysis, mobile threat assessment, and compliance management. Malicious and risky app behaviors are detected through static analysis of the binary code and dynamic behavioral analysis via code emulation or execution. The Appthority solution integrates with major EMMs, including AirWatch and MobileIron. Appthority's on-device mobile agents for iOS and Android provide proactive threat detection, expedited device remediation and employee self-remediation options.

BlackBerry

play.google.com/store/apps/details?id=com.blackberry.privacydashboard&hl=en

BlackBerry DTEK concentrates on app management as a threat defense for BlackBerry devices running Android. DTEK assesses the security posture of the device and assigns a rating to it. It also monitors apps and alerts when it identifies privacy-invasive behavior. Trusted app-side loading can be managed on Samsung Knox, and container-compatible apps can be put into custom distributions to the Good Work container.

Better Mobile Security

better.mobi/productsreal-time-threat-prevention-2/real-time-threat-prevention-2

Better Mobile Security combines agent-based, continuous device monitoring and remediation with supervised device updates, remote diagnostics and a holistic app risk analyzer that can be placed in the enterprise app distribution process to assess vulnerabilities before apps are released to mobile users. Remediation can take place via integration with EMM, and integration with security information and event management (SIEM) is also possible.

Check Point

checkpoint.com/products/mobile-threat-prevention

Check Point Mobile Threat Prevention (MTP), which originated from the Lacoon acquisition, provides MTD for iOS and Android devices. MTP employs app scanning, combined with network and device anomaly detection. Some of the analysis takes place on the device and some of it occurs in the cloud. MTP also provides a cloud-based management portal and integrates with major EMM and SIEM tools to provide device visibility.

Cyber adAPT

cyberadapt.com/product/secure-device-management

Cyber adAPT Secure Device Management (SDM) provides an always-on secure IPsec VPN connection for Android, iOS, Windows and OSX devices. Through its VPN, SDM monitors all mobile traffic to network and cloud services, and it will identify anomalies and malicious attacks in these connections. SDM accomplishes these functions with an agentless, certificate-based solution. It can also coexist with EMM solutions, such as MobileIron and AirWatch.

Deep Instinct

deepinstinct.com/#/what-we-do

Deep Instinct scans Android and iOS apps and identifies and blocks threats by employing deep learning. It combines a device agent with an on-premises or cloud-based appliance. Deep Instinct's solution recognizes threats in real time by training on hundreds of millions of samples and can, in this way, recognize and detect attack variants, as well as attacks that have not been seen in the wild before.

FireEye

fireeye.com/products/mobile-threat-protection-mobile-security-products.html

FireEye Mobile Threat Prevention leverages the company's sandboxing solution to scan and identify malicious or privacy-invasive iOS and Android apps. MTP provides a report for each scanned app, highlighting its suspicious or potentially unwanted behavior. FireEye integrates with major EMM suites, including AirWatch and MobileIron.

IBM

ibm.com/software/products/en/maas360-mobile-threat-management

IBM MaaS360 Mobile Threat Management (MTM) leverages anomaly detection from IBM's acquisition of Trusteer. MTM provides malware and privilege escalation detection, as well as app scanning and web content filtering. The solution synergizes with the IBM EMM for remediation. Access to business data and networks can be blocked when app problems are indicated. Device

profile corruption or other suspicious activity will block access to encrypted data and can trigger partial or full system wipes.

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. Customizable threat alerts can be configured to monitor all device apps, and send warnings to the admin console. EMM-based remediation is supported, as well as local alerts and advice given to the end user of the device. Integration with Microsoft and most leading EMM solutions is available. Lookout can also act as an event feed for SIEM systems.

NowSecure

nowsecure.com/protect

NowSecure monitors mobile device system, configuration and network activity, and it reports on suspicious apps, activities, and traffic for iOS and Android. The tool is designed to be noninvasive, so that it will be acceptable in bring-your-own-device scenarios. It provides users with real-time notifications and alerts, and a risk score for the device, as well as identifying countries and organizations that are accessing user data.

Opswat

opswat.com/products/metadefender/endpoint/management

Opswat has been known for many years as the go-to database for validating versions of security programs. The company now offers Metadefender, a cloud-based, self-contained validation system that deploys agents that will fully examine platforms and apps for all popular OSs, including Android, iOS, Linux, OS X and Windows. It can be run stand-alone or be integrated with other EMM, EPP and VPN solutions.

Palo Alto Networks

https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/globalprotect

Palo Alto Networks' GlobalProtect routes mobile device traffic via an always-on VPN through its on-premises or cloud-based, next-generation firewall appliance. The WildFire sandboxing engine is used to scan Android apps, but not iOS. The solution integrates with third-party EMMs, including AirWatch and MobileIron.

Pradeo

https://www.pradeo.com

Pradeo's Apps Security Solution is a secured apps manager that uses Pradeo's behavioral analysis engine, called Trust Revealing, to scan iOS, Android and Windows Mobile apps and regulate mobile app installations, depending on the potential threat level. The product also scans mobile devices and provides a threat analysis report. A secure browser and a secure email client are available.

Skycure

https://www.skycure.com

Skycure's predictive malware detection techniques include static and dynamic analysis, crowd-based anomaly detection, and analyses based on signatures, app behavior, structure, permissions, etc. 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 EMMs.

Wandera

wandera.com/solutions/threat-defense

Wandera monitors devices for misconfigurations and behavioral anomalies, scans for malicious or suspicious network connections, and scans for suspicious apps by means of its cloud-based, machine-learning engine, supplemented with its dynamic app analysis and reputation tests from third-party sources. In addition, Wandera monitors data use to determine reasonable and expected user behavior patterns. Data use has additional value for analyzing efficiency, as well as giving a picture of appropriate versus inappropriate content, hidden data use and fragmentation conditions that can affect regulatory compliance.

Zimperium

https://www.zimperium.com/zips-mobile-ips

Zimperium provides zIPS, an MTD solution that conducts behavioral anomaly detection in real time on the device. zIPS focuses on monitoring the device configuration and parameters, as well as identifying anomalous behavior. zIPS also provides network security and a vulnerability assessment of an enterprise's mobile risk posture, as well as app scanning for iOS and Android apps. Zimperium's offer is integrated with major EMMs, such as AirWatch, BlackBerry (Good Technology), Citrix and MobileIron.

Zscaler

zscaler.com/products/zscaler-app

Zscaler is a secure web gateway (SWG) and cloud access security broker (CASB) that specializes in monitored, mobile VPNs. The Zscaler App and VPN direct internet traffic to a tunnel that's monitored for detection of anomalous behavior of the platform, network connection, app and user. Protection is limited to events that can be detected and managed within the tunnel. The system is

agentless by default; however, a local agent can be added to actively manage authentication and policy enforcement. Protective responses can include displaying warnings to users and redirection to remediation sites.

Market Recommendations

Although mobile malware is not the primary risk for enterprises, security leaders should track the market and gradually integrate their mobile software with threat defense solutions. Typical verticals will be finance, healthcare, government, insurance and utilities. These products may also provide the equivalent of some mobile device management functions among unmanaged consumer devices, and companies may be able to leverage the benefit.

Security leaders that have to settle for less-security-focused EMM solutions, due to usability requirements from their workforces, should look into this market and evaluate whether the promises of these solutions can enhance their mobile endpoint security posture. MTD solutions that are integrated with EMM to provide synergy and easier deployment will have a greater impact.

Security leaders that have decided their endpoints need MTD now should act tactically and not wait for market consolidation. Short-term deals with vendors that can integrate with EMMs will be the more interesting ones.

In 2016, companies should be cautious about giving complete platform control to MTD tools. MTD should be treated as a source of expert opinion on mobile systems' health; however, due to the lack of visibility over mobile platforms, there may be cases in which both EMM and MTD tools ignore security posture issues that become management gaps.

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"

"Network Sandboxing for Malware Detection"

"Five Styles of Advanced Threat Defense"

"Magic Quadrant for Enterprise Mobility Management Suites"

"Critical Capabilities for Enterprise Mobility Management Suites"

"Mobile Device Security: A Comparison of Platforms"

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