WHITEPAPER

Why integration of Mobile Threat Defense (MTD) solutions with EMM makes sense?

By 42Gears Team

Table of Contents

Introduction

As businesses are adopting sophisticated mobile devices, operating systems, apps, and networks, they all are becoming vulnerable to different security threats such as malware, phishing, network attacks and man-in-the-middle attacks that are hard to detect and prevent.

With an increase in the adoption of sophisticated technology, enhanced work arenas and incorporation of new forms of endpoints such as IoT and Wearables, the amount of associated security threats has increased exponentially. More than 1.5 million new incidents of mobile malware have been detected by McAfee Labs in the first quarter of the year 2017- for a total of more than 16 million mobile malware incidents.

According to Gartner's Market Guide for Mobile Threat Defense Solutions, by 2019, mobile malware will amount to one-third of total malware reported in standard tests, up sharply from 7.5% of malware today.

The constantly evolving threat landscape is providing an opportunity for Mobile Threat Defense (MTD) solutions to invade into digital business ecosystems to secure them from cyber risks. Businesses are left with no choice but to adopt MTD solutions and ensure a Mobile Threat Defense strategy is in place. According to Gartner, by 2020, 30% of organizations will have MTD in place.[1]

Mobile threats that can impact businesses

Pegasus Spyware

Pegasus, an enterprise class spyware was introduced recently to target mobile devices such as iPads, iPhones and Android smartphones used by employees. It was considered the most powerful attack that allowed hackers to stealthily spy on victims, collect information from voice communications, messaging, contact lists, email, GPS, passwords and camera. These days' employees are using their own mobile devices for work and if their devices come under the Pegasus attack, it can endanger corporate data.

Mobile Malware

A large number of mobile devices can be turned into botnets by a new malware which is controlled by the attackers. The first malware Viking Horde was made to target Android devices. It could convert rooted or non-rooted devices to botnets that used proxy IP addresses and disguise ad clicks and generate revenue for attackers. Many such kinds of botnets have been created so far, including the Hummingbad, which infected over 10 million Android operating systems in recent years.[2]

Malware as Adware

Attackers are also gaining access to the internal networks of companies through SMS phishing on mobile devices. It is basically sending out a link to download a malicious app through SMS, which allows hackers to control the users' phone, steal credentials and access internal network. This ad and click fraud in mobile devices is a growing concern for organizations. The worst part is that these adware can easily spread as a spyware to the entire botnet, which allows attackers to keep an eye on millions of devices.

Removed or Dead Apps

Multiple outdated apps are removed by security teams of Google or Apple stores without any notice or reason, but if these apps are still exist on employees devices, these unknown apps can leak out the company's sensitive data to third parties through malware.

Why do we need MTD solutions?

For years, corporate leaders have been embracing the value offered by mobile devices without realizing the devastating effects of not securing data transferred through these devices. Enterprises have implemented BYOD, which allow employees to access corporate resources from their own devices. Now, in lack of proper security tools and strategies, they have failed in thwarting the employees to gain access to company's data and resources from their own devices. There is a need for organizations to deploy essential Mobile Threat Prevention (MTP) solutions to protect business from these cyber threats.

Three levels MTD protection

The MTD market is offering solutions for different platforms such as Android, iOS and partly for Windows as well. According to Gartner, MTD solutions are providing security at three levels, i.e. Device level, Network level, and Application level.3

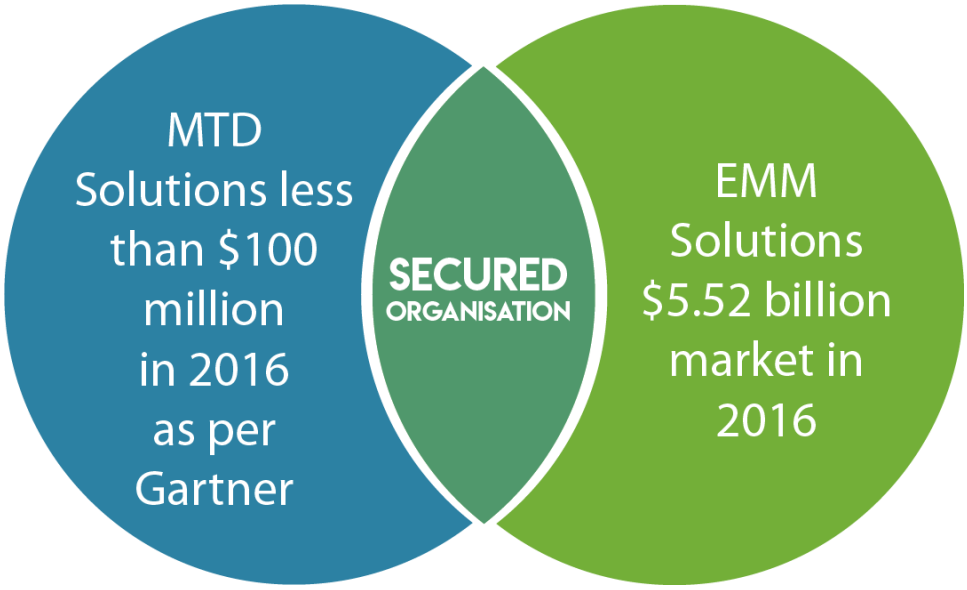
Device level: MTD tools track system parameters, configuration, firmware and libraries to detect malicious activity. These solutions protect devices against security vulnerabilities by checking OS versions and security patches from time to time. Additionally, they inspect devices for configuration weaknesses which can lead to malware execution.

Network level: MTD tools keep track of network traffic and disable the connections from mobile devices if it is suspicious. MTD tools protect the organizational network by using various techniques like man-in-the-middle detection, checks for invalid or spoofed certificates and Secure Sockets Layer (SSL) stripping.

Application level: MTD tools safeguard enterprise data from malicious apps through reputation scanning and code analysis. To identify and prevent leaky apps, MTD uses techniques such as signature-based anti-malware filtering, code emulation or simulation, reverse engineering, static and dynamic app security testing.

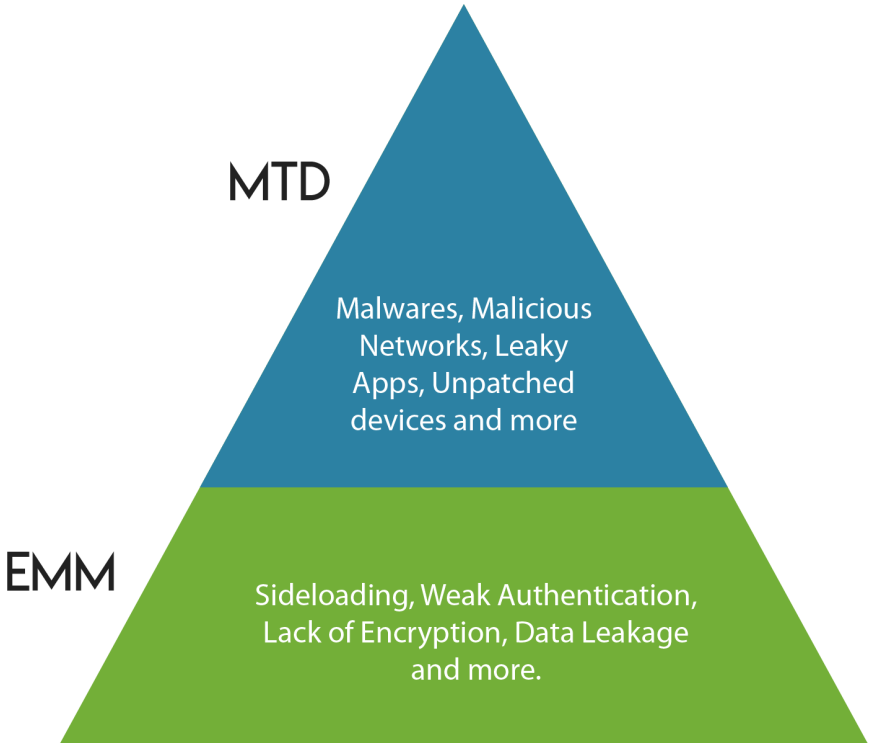
MTD solutions not only identify and prevent malicious activities, but also take remedial actions in order to protect enterprise data. Many solutions work in tandem with MTD solutions such as Mobile App Reputation Solutions (MARS) to protect against leaky apps. Also, using behavioral anomaly detection, enterprises can identify compromise indicators and obtain information on current attack trends.

EMM and MTD integration



Enterprise Mobility Management (EMM) platforms help organizations manage and control devices and applications in a more secure and compliant environment. As EMM has evolved to UEM, it now allows enterprises to manage multiple devices, platforms and endpoints.

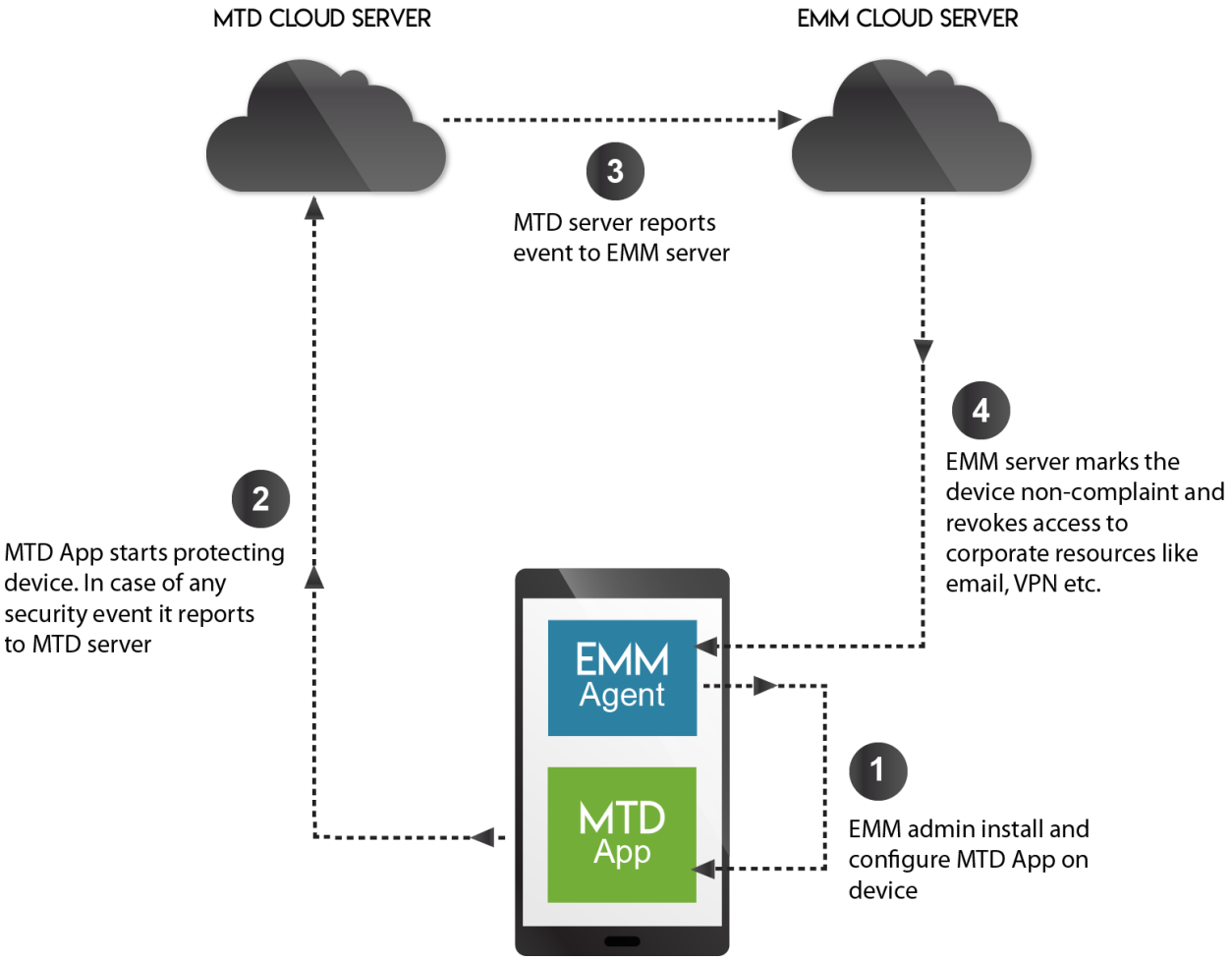
Mobile malware and other vulnerabilities are on the rise, giving rise to Mobile Threat Protection solutions that have started invading enterprise ecosystems and complement EMM or UEM solutions. Even though EMM or UEM solutions provide security to mobile devices, it can be enhanced by the integration of MTD solutions. EMM can address security threats such as data leakage, privilege escalation sideloading, weak authentication and lack of encryption. However, there are many threats that EMM can't control such as **leaky apps, unpatched devices, advance malware, malicious networks and privilege escalation hiding** which MTD solutions can control very well.



Source: Gartner (August 2017)

How EMM and MTD works in tandem

As EMM obtains device information, MTD/ MTP leverages that information to perform disciplinary actions on the device or to provision the device. EMM contains MDM profile on the devices which allows admin to take actions like wipe data or device remotely. An EMM agent has to install and configure MTD on devices. MTD app can then start protecting devices against security threats. If any malicious events are noticed by MTD, it can be reported to MTD server, which in turn, will report it to the EMM server. The EMM server can then mark the device a non-compliant and revoke access to corporate resources like email, VPN, etc.



Factors to be considered before choosing an MTD solution

There is no single MTD solution that can perfectly fit all organizations. Organizations must take into account their unique nature of business before deciding which solution would work best. Before choosing a MTD solution, organization must explore these parameters:

- Industry type
- OS used by the organization
- Applicable regulations
- BYOD or COPE or the blend of BYOD and COPE
- Kind of access employees have on their devices

- The EMM solution used by the organization

There are many MTD solution vendors available in the market. Businesses should choose whatever suits as per the organizational need.

MTD Vendors comparative analysis

Vendors	OS support	OS level attacks	Leaky apps	Cellular network attacks	URL filtering	EMM integration	Deployment method
Checkpoint	iOS, Android	Yes	Yes	Yes	No	Yes	App, SDK
Lookout	iOS, Android	Yes	Yes	No	Yes	Yes	App, SDK
Pradeo	iOS, Android, Windows 10 mobile	No	Yes	No	Yes	Yes	App, SDK
Symantec	iOS, Android	Yes	Yes	No	Yes	Yes	App, SDK
Wandera	iOS, Android,	Yes	Yes	No	Yes	Yes	App, Proxy

	Windows 10 mobile						
Zimperium	iOS, Android, Windows 10 mobile	Yes	Yes	No	No	Yes	App, SDK

Source: Gartner (August, 2017)

Mobile management and protection are inextricably linked. EMM and MTD solution integration will offer a seamless mobile management solution with high grade security to organizations. Introducing an MTD solution depends on the industry type, sensitivity of data on mobile devices and organization's risk management capability. Industries such as finance and healthcare will adopt MTD soon as they come under high regulated verticals. Industries deploying large number of Android devices also come under high-security verticals and are recommended to adopt the MTD as soon as possible.

42Gears' EMM solution has integrated with a few MTD vendors to offer a seamless mobile management solution with high-grade mobile security.

Read more to know how 42Gears MTD feature detect malware threat and secures mobile devices.

References

1. https://www.gartner.com/doc/3393617/market-guide-mobile-threat-defense

2. https://www.csoonline.com/article/2157785/data-protection/five-new-threats-to-your-mobile-security.html

3. https://www.gartner.com/doc/3393617/market-guide-mobile-threat-defense