Miercom

Mobile Threat Defense (MTD)

Industry Assessment

IA190910B

www.miercom.com

INDUSTRY ASSESSMENT MIERCOM REPORT

Miercom reports are published after thorough testing by our engineers of claimed features and functionality. To validate your Mobile Threat Defense solution, contact sales@miercom.com.

Miercom

elevating testing standards

Miercom

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Business tasks and communications are made easier with the help of mobile devices, allowing employees to work on the go. But the mobile industry is accelerating at a pace that businesses did not anticipate – leaving many devices open to attack.

In the best case, an infected network will significantly reduce productivity and drive maintenance costs upward. But in the worst case, the network and its users may experience severe data breaches that can cause an outright halt to business operations. Even further, stolen information could entail expensive, and thorough, technical and legal investigations to resolve.

The best way to protect against mobile attacks? A defensive solution that stops threats before they are even seen.

In 2019, we tested Mobile Threat Defense (MTD) solutions – exposing them to multiple attack iterations, particularly newly found malware and behaviorially anomalistic scenarios. Our results were used to analyze the MTD industry for defense efficacy, the most potent threats, and which winning attributes of an MTD solution all vendors should have.

MTD solutions should live up to their claims, making a worthy network investment. This report shows the true capabilities of MTD solutions on the market today.

01 MARKET ANALYSIS

First we look at the overall quality of experience and cost for investing in the average MTD solution. Our Market Impact Analysis™ chart indicates where vendor's products land with respect to this average cost-benefit.

02 VENDOR ANALYSIS

Next we discuss each tested MTD vendor product individually, noting its Market Impact Analysis™ value, competitive differentiators and defense strengths.

KEY FINDINGS

63.8% SECURITY FEATURES

The average MTD solution is exactly that. Average. We feel most products are not adequate for handling malware, behavioral detection and safe browsing – resulting in data loss and poor productivity.

75% MITM ATTACK PROTECTION

While every tested vendor could detect Man-in-the-Middle (MiTM) attacks, only half of them could prevent them. This prevention is a crucial feature given the frequency of these attacks.

90% VULNERABILITY DEFENSE

Most vendors had perfect protection for rooted devices, developer certificates and unsecure device settings. However, the average MTD solution only had 60 percent malicious profile prevention.

70% EFFECTIVE REMEDIATION

Most vendors were able to employ policy compliance during network violations. But when it came to conditional access and reporting, the average MTD solution only scored as high as 65 percent.

93% EASE OF DEPLOYMENT & USE

Client installation of each MTD solution scored 100 percent. When it came to user action, the average vendor offers 86 percent of the same interface and action features as the best MTD solution.

This report reviews each vendor for strengths that contributed to features we find ideal in a valuable MTD solution. Vendors that chose to actively participate in this round of testing showed us unique capabilities that put them ahead of its competition. One vendor, who had previously tested with Miercom, saw an improvement in MiTM attack detection by 33 percent - proving that Miercom engineers can greatly aid in the product development that keeps them ahead of the curve.

Using 30 use case scenarios, simulated with cutting edge test tools and a realistic corporate network environment, we gained insight on the global, dynamic intelligence of vendors that keep their finger on the pulse for new threats. Our results, as well as cost analysis for an annual subscription and related expenses, were used to provide a summary of product values in our MIA™ chart.

Based on our observations, we found the average MTD solution has many opportunities for improvement. Some vendors showed excellent efficacy against even the most potent of attacks, with impressive dashboards and remediation tools. Our intention going forward is to have more vendors actively participate in product testing to help better develop their MTD solution for realistic scenarios that put networks at risk – hardening the industry of mobile security and keeping enterprises informed of the best products for their network.

Rob Smithers, CEO
Miercom

MARKET IMPACT ANALYSIS™
2019
MOBILE THREAT DEFENSE

After analyzing each MTD solution for its features, functionality and cost-benefit value, we created a visual map of how each vendor's product impacts the market. The following chart details the annual cost-benefit of MTD solutions in the industry.

Why this is important: Using this tool, customers can easily infer the value offered by employing these solutions to enhance BYOD and network security in the corporate network and/or the personal mobile devices that connect to the corporate network.

Two factors make up the Market Impact Analysis™ map: Quality of Experience (QoE) and Total Cost of Ownership (TCO). This report investigates product value on the basis of quality of functionality and use, as well as the average cost for annual deployment of 100 devices.

QOE

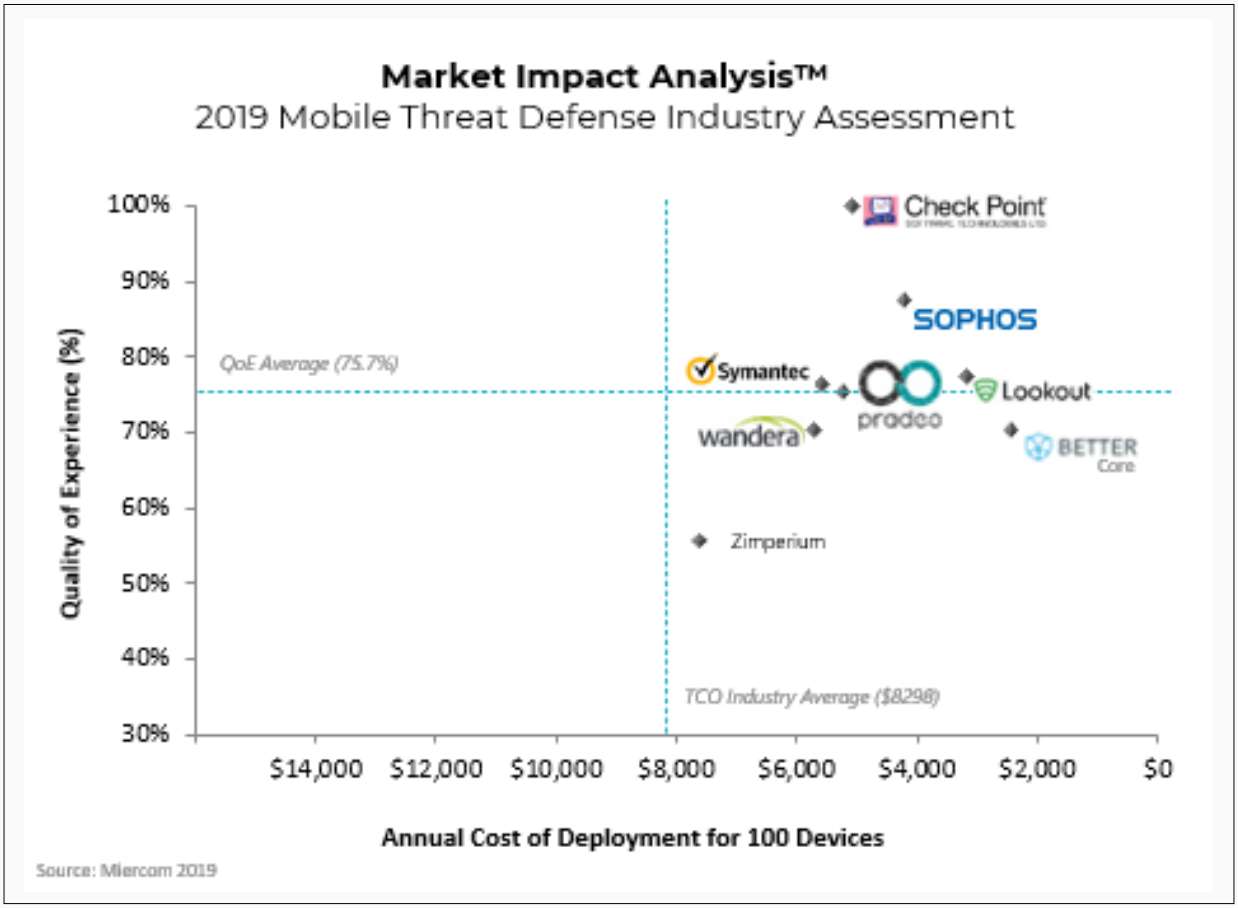
QUALITY OF EXPERIENCE

The vertical axis of the MIA™ map summarizes security efficacy, ease of use, service setup and utilization, support, business practices and legal restrictions involved. The percentage is derived from current and past experience, open source information, user feedback, product strengths and oppotrunities to improve.

TCO

TOTAL COST OF OWNERSHIP

The horizontal axis of the MIA™ map summarizes annual deployment costs per 100 devices. While subject to change, it is based on current discounts or negotiations made between vendor and customer. It also best reflects the cost of training and related expenses, product upgrades, support, licensing and legal restrictions.



VARYING QUALITY AND COST

The quality of experience for MTD products varied from around 55 to 99 percent, but at a range of affordable costs ranging from about $3000 to $7500 per year. One vendor remained an outlier, with a very costly solution with only average quality. For a majority of vendors/products tested, higher cost did not yield better detection efficacy or QoE.

HOW CAN THE INDUSTRY IMPROVE?

Miercom uses test data to allow vendors and customers to have a transparent visual of the direction in mobile security. We so far find that there is still much yet to be addressed – detection efficacy, remediation, ease of use. This report is a living document and vendors are invited to prove capabilities that may impact their score. Prior to testing, all vendors are offered the opportunity to participate in this industry wide study, at no charge. Vendors that choose to actively participate or facilitate our evaluation show transparency which earns them a higher quality of experience. We assume vendors which are less open about their feature set fail to prove their advertised capabilities, scoring a default 70 percent efficacy in respective areas of testing. Proven features raise the QoE score to the current value assigned in the MIA™ map.

MOBILE SECURITY FACT SHEET

Running a mobile threat defense seems logical for protecting against such risks and consequences. But not every MTD solution approaches these threats in the same ways, making it difficult to discern which will help an enterprise more. Our report analyzes the prevalent attack vectors, which ones are mostly detected or prevented, and which ones still need to be addressed.

Just like MTD defenses, attacks are unique and don't always use a single point of entry. There are multiple stages of attacks that mobile security has the chance to defend against. For example, a victim can lose privacy when clicking a malicious link that exploits their device's software, or the network's security flaws, to gain root access. From here, an attacker can install a malicious application or monitor the user's activity.

What's important for MTD solutions is to have a well-rounded insight and set of tools to find and stop these threats from putting the device and network at risk. Below are some quick facts about the mobile security landscape we see today.

- "The average total cost of a data breach: 3.92 million USD." – *IBM Security*
- "25,000 new malware apps [are] detected on corporate devices each month." – *Wandera*
- "71% [of Americans] worry about the hacking of personal data, 67% about identity theft." – *Gallup*
- "89% of the global workforce is mobile and mostly composed of BYOD devices." – *Pradeo*
- "...the rise in Android threats by almost 4,000 variants per day [indicates] a severe risk that manifests in the form of data loss, privacy concerns, theft, and fraud." – *Symantec*
- "By 2020, 30% of organizations will have MTD in place, an increase from less than 10% in 2018." – *Gartner*
- "...Spectre and Meltdown vulnerabilities...allow attackers to view application data in memory on the chipset...in everything from mobile phones to server hardware." - *Cisco*
- "With 2 billion users forecasted by 2020, mobile banking logins are becoming more significant than web logins." – *Pradeo*

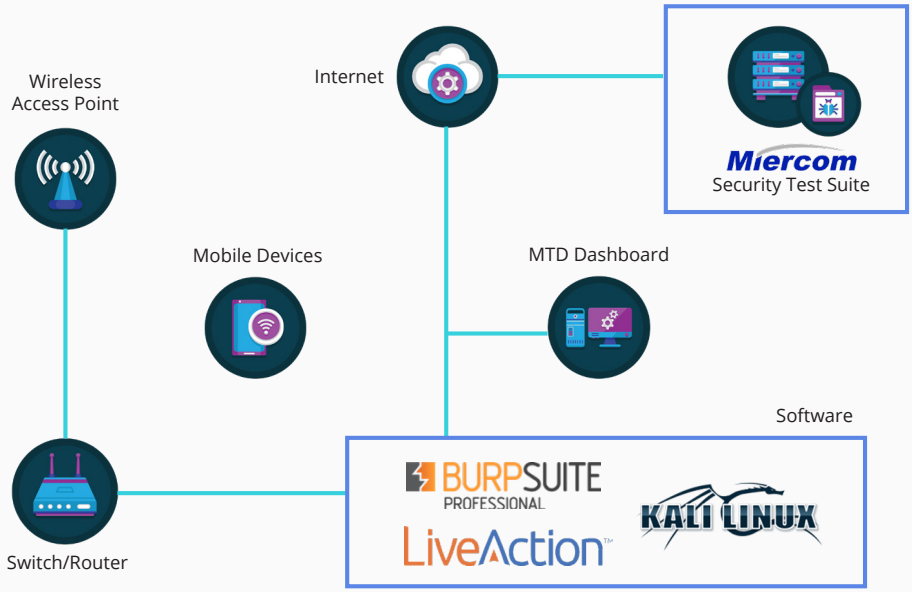
HOW WE DID IT

THE LATEST THREATS.

A REALISTIC ENVIRONMENT.

Miercom uses a proprietary Industry Assessment methodology to evaluate competitive MTD solutions for their real-world enterprise functionality and quality of experience. With hands-on testing, these environments are reproduced to evaluate for strengths, weaknesses, techniques and unique functionality for each security solution in response to malicious activity. The Miercom Security Test Suite contains a proprietary process, including the use of custom-crafted attacks and malicious applications to test security efficacy. This blend of samples provides a strong metric for testing vendors for robust, granular defenses against multiple breach methods.

Mobile devices have the client component of the MTD solution applied and enabled to communicate with the MTD server during attacks. The MTD server is monitored via dashboard after appropriate login credentials are entered. Using several versions of both Android and iOS operating systems, attacks are delivered using the Miercom Security Test Suite – including the malware database, Kali Linux, and BurpSuite software. Missed samples are observed and captured using the LiveAction Omnipeek network tapping software.



Source: Miercom July 2019

TEST TOOLS

KALI LINUX

The Linux operating system is used in offensive security testing with a comprehensive set of tools. Two tools used during testing were SSL Split and SSL Strip. SSL Split created Man-in-the-middle (MiTM) attacks on encrypted network connections. SSL Strip was used for hijacking and monitoring secured HTTPS traffic.

BURP SUITE

This suite includes the Burp Proxy tool which acts as a proxy server to intercept, inspect and modify traffic to, and from, the client and server. This tool was used for MiTM attacks for the Network Attack Prevention section of this MTD assessment.

LIVEACTION OMNIPEEK

This tool captures network traffic and creates packet files for replay. Statistics can help monitor changes in real-time. By baselining normal activity, changes can be observed to analyze problem areas in the network. For more information, visit: https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/.

METHOD

Mobile devices were loaded with a set of applications, including: *Adobe Acrobat Reader; Facebook; FTPManager Free; Line; Microsoft Excel; My Data Manager; Pandora; TeamViewer; WebMD; and Zedge.*

The MTD solution under test was applied to each client. Clients were rebooted and registered for the admin console.

Malicious applications were loaded using the Android Debug Bridge (ADB) USB for Android devices and iFunbox for iOS devices. A script delivered a predetermined amount of malicious samples d to each client. The number of samples detected were recorded as a percentage of the total samples sent to form an efficacy score.

False positive samples were intentionally suspicious, but safe. False positive detection shows how well the MTD solution can discern between legitimate and malicious samples. A score of 100 percent implies the MTD solution can avoid the unnecessary flagging of clean samples. What we derive from this data is that while a solution may have high detection efficacy, it should be equally aware of applications behavior and not just alerting because of an overly stringent interpretation of events.

TEST RESULTS

PROTECTIVE FEATURES

Corporate networks are filled with employees using their own personal devices. And while businesses seem protected on the network front, the mobile devices are left unwatched. Each device comes with its own downloaded applications, verified or third-party, as well as browsing capabilities and access to personal or business data.

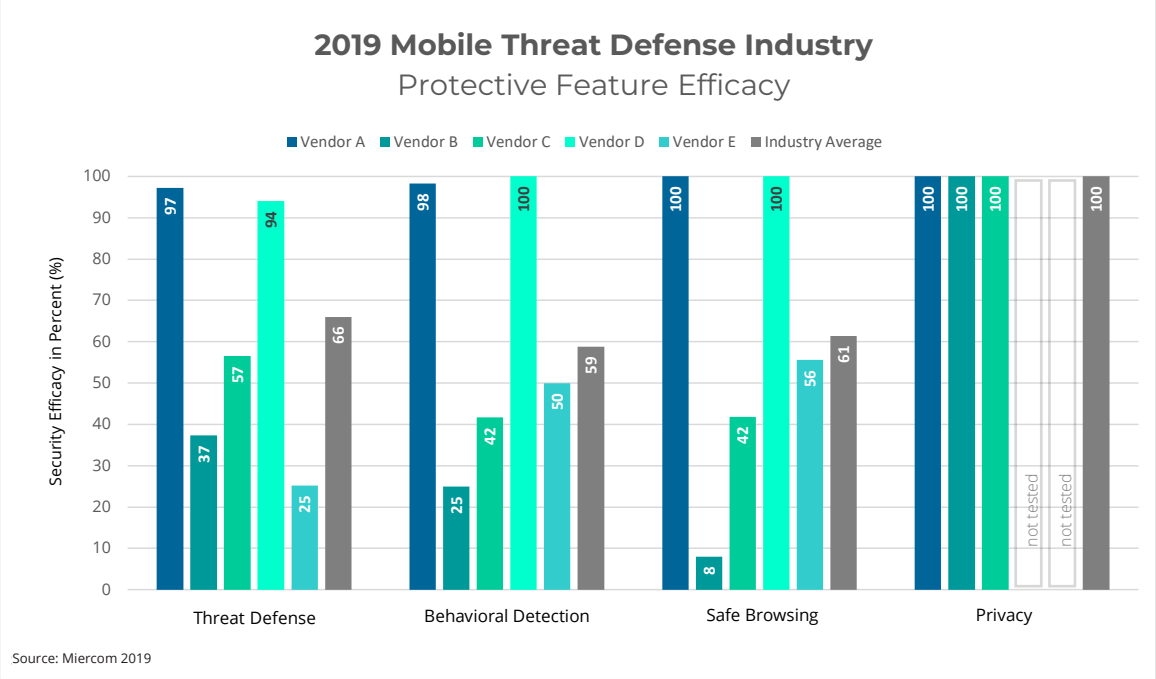
Attackers see all these mobile features as points of entry into user devices as well as its connected network. MTD solutions are installed on each device and managed by the network to counter any threat that may utilize these vectors. Being able to detect malicious applications, stop connections to malicious servers, and protect the privacy of users and network are the core functions of a basic MTD solution.

THREAT DEFENSE
Malware can be legacy, unknown, persistent or sideloaded. Detection accuracy matters.

BEHAVIORAL DETECTION
Not every file is trackable. Signatureless threats require intelligent behavioral analysis to prevent.

SAFE BROWSING
Leveraging human error, attackers use phishing and other browser-based exploits to gain access.

PRIVACY
Hacked devices put their data in unknown hands. A data leak means the user and network are at risk.



Source: Miercom 2019

Vendors were able to secure against threats, malicious behavior, browsing and privacy scenarios at the efficacies shown above. The average vendor (in grey) showed no more than 66 percent efficacy for each main category except privacy. The most easily detected threat was known malware and the least reliable feature was malware download prevention. Vendors varied in their security, but one vendor consistently scored 97 percent or higher in every category. (Note: "Not Tested" indicates the vendor's feature was not available for evaluation at time of testing.)

NETWORK ATTACK PREVENTION

By implementing Man-in-the-Middle (MiTM) attacks using Kali Linux SSL Bump and SSL Stripping exploits, we tested the ability of MTD solutions to detect and prevent these attacks.

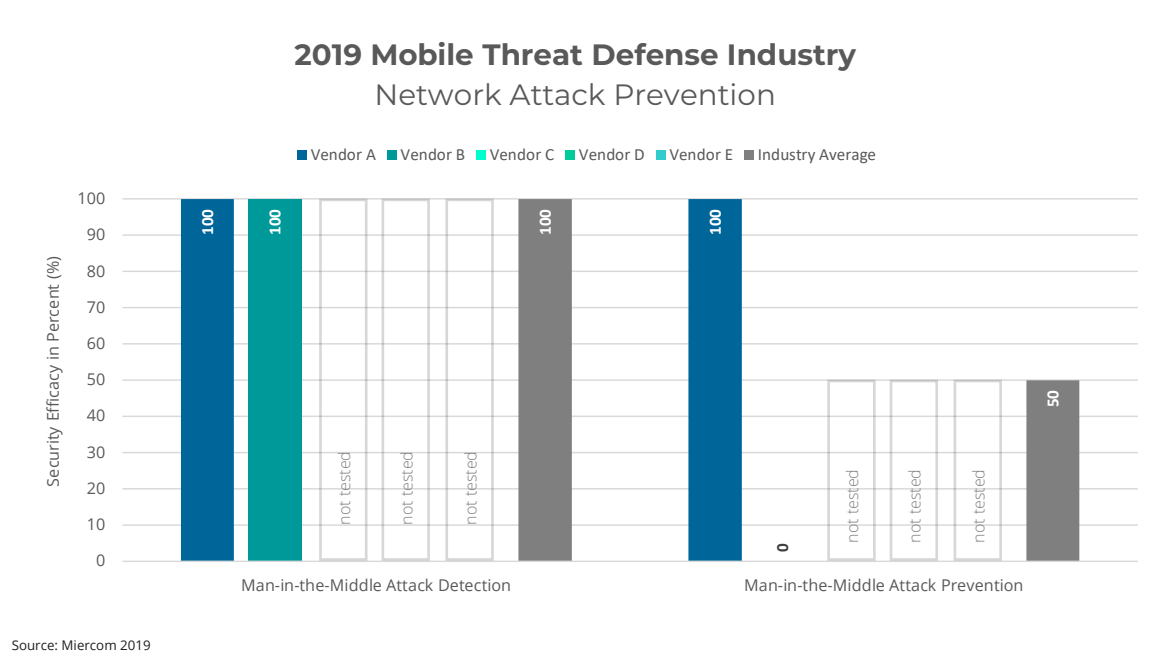
MiTM attackers pose as legitimate connections and servers to reroute wireless communications. The unsuspecting user's communication becomes compromised, allowing attackers to gain access to credentials, personal information and network permissions. A popular type of MiTM attack is SSL hijacking which we analyzed during testing.

JUST BECAUSE YOU ARE USING SECURE SOCKET LAYER (SSL), DOES NOT MEAN YOU ARE CONNECTED TO A SECURE SERVER.

Using an external device, we recreated MiTM attack scenarios using the following two methods:

SSL INTERCEPTION
A malicious proxy that routes traffic through an attacker network.

SSL STRIPPING
An attack obtains connection and rewrites content in plaintext (excluding HTTPS links) to expose encrypted traffic.



Source: Miercom 2019

Two of the five vendors in this study were observed having network attack prevention capabilities. These two vendors detected all MiTM attempts, but only one of these vendors was able to also stop all MiTM attacks. The other vendor was unable to block any. Three vendors have yet to be tested for this feature, as their demo versions did not allow a preview of this functionality. They are invited to submit their product at any time to prove this capability. To date, the average vendor can detect MiTM attacks with 100 percent eficacy but only bock with 50 percent efficacy. (Note: "Not Tested" indicates the vendor's feature was not available for evaluation at time of testing.)

DEVICE VULNERABILITY

MTD solutions were tested for their ability to detect and prevent device vulnerabilities that put the network at risk for a breach. Outdated software patches, rooted devices, and unsecure settings all have one thing in common – they are preventable. But if the user is unaware, the device remains exposed to attacks. An MTD solution should detect vulnerabilities to harden devices and help corporate networks avoid intercepted connections, hijacking, manipulation and data breaches. Vulnerabilities tested include the categories below:

ROOTED DEVICE

Rootkits allow users to customize their Android devices, but they also give attackers an opportunity to gain operating system access. MTD solutions should detect root access based on unexpected system behavior.

MALICIOUS PROFILE

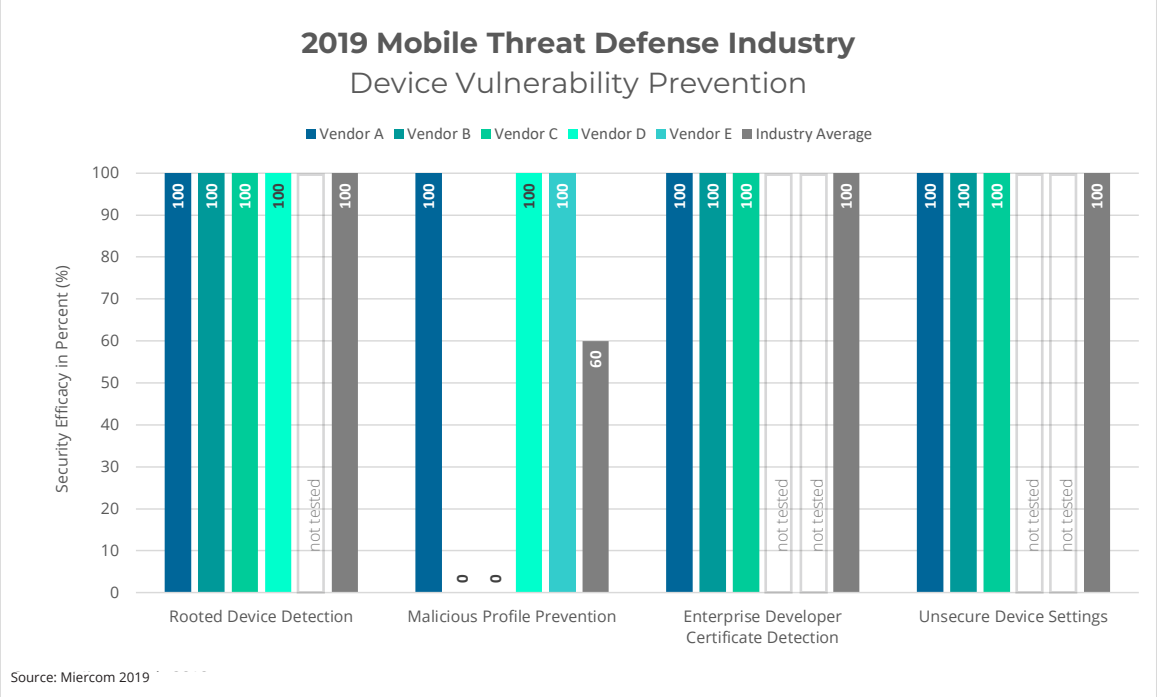
iOS is a reputably hardened operating system but can still be directly accessed and manipulated using malicious configuration profiles. MTD solutions should prevent any control of an iOS device.

DEVELOPER CERTIFICATE

iOS application developers receive certificates before their work is verified for the AppStore. Illegitimate sources use certificates to distribute malware that should be scanned for intent.

UNSECURED SETTINGS

Default configurations can be vulnerable for exploitation. For example, outdated firmware and enabled Bluetooth services can allow attackers to enter the network. An MTD should routinely check settings.



Source: Miercom 2019

Of the four vendors tested for rooted device detection, all were able to find this vulnerabiliity with 100 percent efficacy. Malicious profile prevention was tested for all vendors – three vendors showed 100 percent efficacy while the other two could not detect any samples. The enterprise developer certificate was tested on three vendors, who found this vulnerability with 100 percent efficacy. Last we looked at unsecure device settings on three vendors. Of these vendors, all were capable of identifying settings that put the device and network at risk. The average vendor is excellent at device vulnerability prevention but could improve on malicious profile prevention. (Note: "Not Tested" indicates the vendor's feature was not available for evaluation at time of testing.)

REMEDIATION

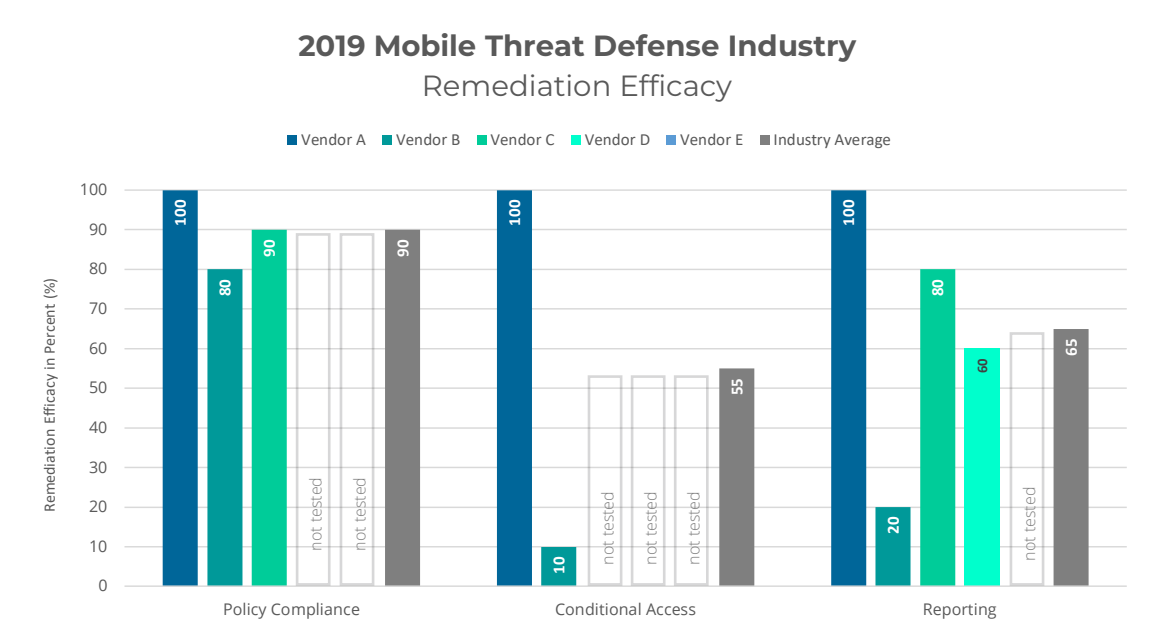
MTD solutions should be able to take control after a breach. Whether it's to quarantine devices or gain actionable insight, the mobile defense product should have the latest features to help ensure threats are contained and remediated. Networks should always have visibility of violated policies, unauthorized access, and device statuses. Quarantined devices should have details displayed, with instructions on what to do next. Reporting is crucial for administrative knowledge of the what, where and when of mobile activity.

POST-ATTACK ACTIONS MAKE THE DIFFERENCE. HAVING SOLID REMEDIATION ENSURES THREATS ARE ISOLATED AND REMOVED.

POLICY COMPLIANCE Policies segment networks and reduce attack surfaces. MTD solutions should extend policy compliance to isolate and alert infected devices.

CONDITIONAL ACCESS Corporate networks should provision access to ensure private data and business-only applications remain in the hands of authorized users.

REPORTING Reporting tools help users and administrators have a clear indication of threats in real-time. They should be intuitive and detailed for remediation.



Source: Miercom 2019

The average vendor had 90 percent efficacy when it came to policy compliance which ensures infected devices do not affect the rest of the network. Conditional access was tested on only two vendors. One vendor was able to perfectly provision access, while the other could only perform this task 10 percent of the time. Reporting was an area to be improved; the average vendor only had a 65 percent rating in this category and one vendor was as low as 36.7 percent. (Note: "Not Tested" indicates the vendor's feature was not available for evaluation at time of testing.)

EASE OF USE

Usability is underrated and sometimes overlooked. But despite accurate detection and prevention, a front-end that is hard to use or deploy will result in downtime and frustrated users. This can be a make-or-break aspect when deciding between two similarly effective MTD solutions.

CLIENT INSTALLATION

Deployment of the MTD solution should be simple. Client installation of the solution on mobile devices should be intuitive, clear and effective immediately.

USER ACTION

Before, during and after threats enter the network, MTD operations, from both the client and administrative end, should be quick and easy to use.

CLIENT INSTALLATION

The average vendor has a perfect score for its easy client installation. Simply download the client application, enter credentials, and your device is protected.

USER ACTION

During test case scenarios in previous sections, the average vendor was 86 percent effective in all actions taken. This includes features like a clear interface and proper instruction before, during and after a breach.

CONCLUSIONS

From our test data and analysis, we conclude the following:

- **Most vendors need to improve their detection and prevention abilities – especially zero-day malware, false positive detection and persistent malware prevention.**
- **Many vendors lack adequate behavioral detection; the majority of vendors provide only basic protection of unsecured network traffic. There needs to be more of an emphasis on sensitive data collection, system file access, cloud services, data exfiltration, command and control communication and dynamic code downloads.**
- **More than half of the vendors tested have poor internal browser protection. The biggest threat is malicious URLs, but phishing and filtering are still in need of at least 40 percent improvement.**
- **MTD users are at least guaranteed privacy - all vendors tested scored 100 percent. Man-in-the-Middle attacks are detectable, but some vendors struggle in prevention when blocking connections to malicious sites.**
- **Device vulnerabilities are well-covered by MTD solutions, with one exception – malicious Apple iOS profiles that most vendors could not detect.**
- **In terms of remediation, policy compliance was offered but not necessarily conditional access and strong reporting.**
- **Every vendor has fairly straightforward client installation process, but some vendors could benefit from improving their dashboard and user actions.**
- **Huge disparity regarding value amongst vendor products in that the cost does not necessarily correlate to a better protection solution.**

VENDOR ANALYSIS

In this section, we look at individual vendors with commentary on the feature set we have observed and their current value as seen in our lab. The order of vendors is alphabetical and does not correlate to the randomized order of results in the previous sections.

- **Better** Mobile Threat Defense
  https://miercom.com/better-mobile-threat-defense-mtd-industry-assessment-product-profile
- **Check Point** SandBlast Mobile
  https://miercom.com/check-point-sandblast-mobile-mtd-industry-assessment-product-profile/
- **Lookout** Mobile Endpoint Security
  https://miercom.com/lookout-mobile-endpoint-security-mtd-industry-assessment-product-profile/
- **Pradeo** Mobile Threat Defense
  https://miercom.com/pradeo-mobile-threat-defense-mtd-industry-assessment-product-profile
- **Sophos** Sophos Mobile
  https://miercom.com/sophos-mobile-mtd-industry-assessment-product-profile/
- **Symantec** Endpoint Protection Mobile
  https://miercom.com/symantec-endpoint-protection-mobile-mtd-industry-assessment-product-profile/
- **Wandera** Mobile Threat Defense
  https://miercom.com/wandera-mobile-threat-defense-mtd-industry-assessment-product-profile
- **Zimperium** zIPS Enterprise-grade Mobile Security
  https://miercom.com/zimperium-zips-enterprise-grade-mobile-security-mtd-industry-assessment-product-profile/

Suggest a product for review

Contact reviews@miercom.com to be evaluated today.

ABOUT MIERCOM

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed. Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Green, Certified Interoperable and Certified Secure. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

ABOUT DISCOVERED EXPLOITS

Miercom is under no obligation to provide notification or samples to any vendor with vulnerabilities discovered during testing. Active participation is afforded to each vendor before, during and after testing to work with Miercom to rectify any weaknesses found in security or performance. Unless there is active participation or an Ongoing Customer Care plan in place, all exploit samples are proprietary and kept confidential. Samples and specific vulnerabilities are kept confidential for the safety of the vendor, its products and product users.

ABOUT MIERCOM INDUSTRY ASSESSMENT

Our Industry Assessment consists of comparative observations of products on the market which is published with results and recommendations. Every vendor is afforded the opportunity to represent themselves in the review. If a vendor does not actively participate, Miercom may elect to acquire the product(s) for testing. Industry Assessments are updated regularly to best reflect the current averages and comparative measurements. Any product tested by Miercom is eligible to be included in its industry assessment.

CUSTOMER USE AND EVALUATION

We encourage customers to do their own product trials, as tests are based on the average environment and do not reflect every possible deployment scenario. We offer consulting services and engineering assistance for any customer who wishes to perform an on-site evaluation.

USE OF THIS REPORT

Every effort was made to ensure the accuracy of the data contained in this document, but errors and/or oversights can occur. The information documented may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

When conducting this Industry Assessment of Mobile Threat Defense products, Miercom approached multiple vendors in this market. Each vendor featured was allowed to participate before, during and after testing. Results published may be refuted, retested and republished should a featured vendor choose to participate.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether expressed or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.