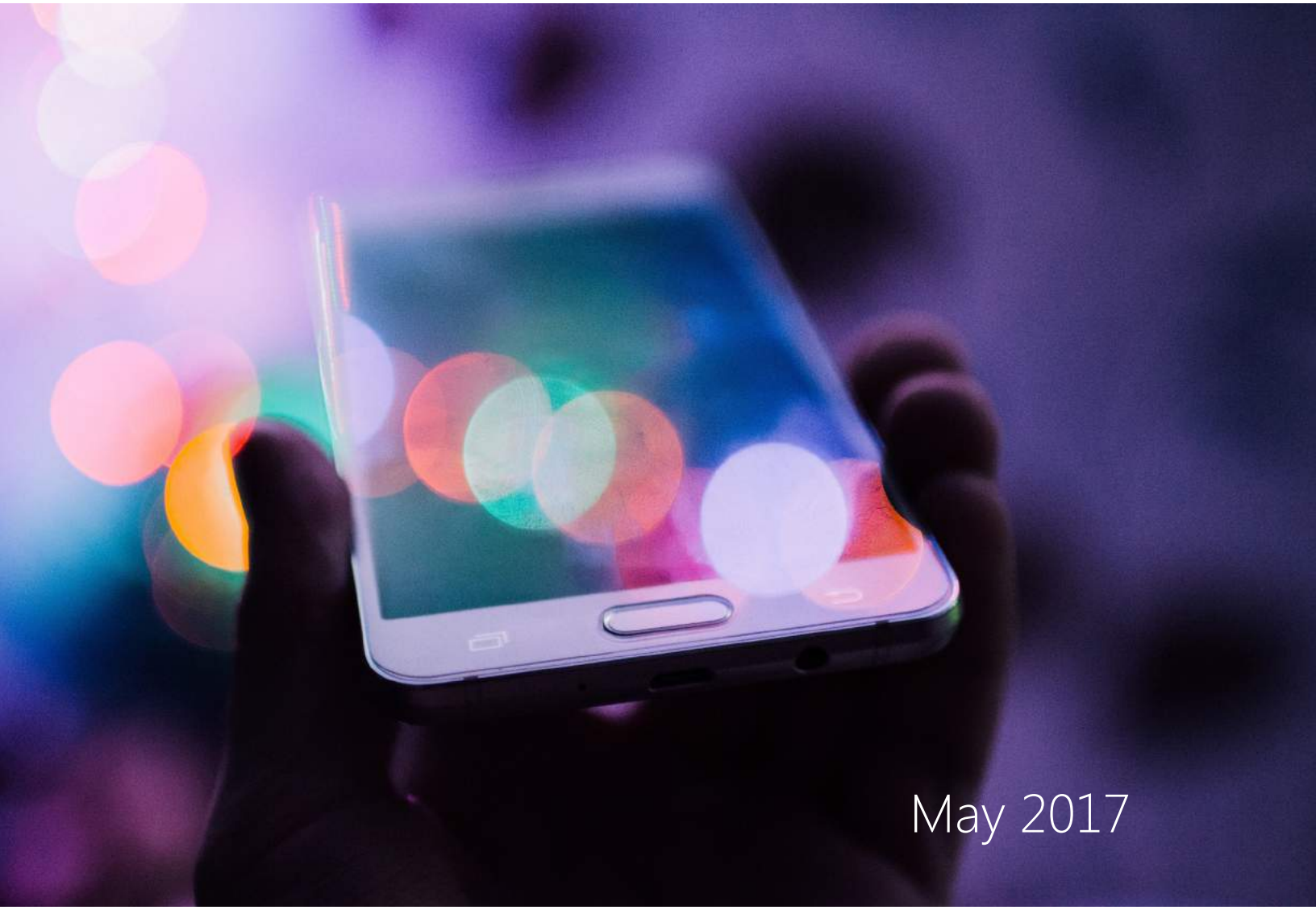
Miercom

Industry Assessment 2017

Mobile Threat Defense (MTD)



Report Excerpt Prepared for: Check Point SOFTWARE TECHNOLOGIES LTD

Contents

Executive Summary

The popularity of mobile devices for conducting enterprise business has surpassed that of desktops and laptops around the world. Consequently, the mobile threat vector has become an increasingly widened attack surface and issue for businesses. Since 2014 the mobile threat landscape has had over five times growth, with more than 2.5 million known mobile malware for devices to date. This high-risk attack vector for enterprises prompts the urgent need and search for reliable defense solutions to protect their network's data and users' mobile endpoints.

Miercom Industry Assessments compare similar products and are continuously updated with results which best reflect current vendor averages in detection efficacy. Every vendor tested is afforded the opportunity, at no charge, to represent themselves in the review.

In late 2016, an assessment was conducted which considered commercially available enterprise-level Mobile Threat Detection (MTD) solutions. This report was prepared for Check Point based on our wholly independent MTD Industry Assessment. The Check Point SandBlast Mobile solution is competitively assessed against similar MTD solutions, with key findings and industry analysis therein.

This report details the leading MTD solutions and how they protect mobile devices against malicious applications, network attacks and device vulnerabilities, as well as provides an index comparison to Check Point SandBlast. During Miercom testing, the Quality of Experience (QoE) and unique features of each MTD solution were also assessed to determine the overall value of each product.

The areas examined, tested and recorded as part of this study included the following:

- Malicious Malware and Applications – targeting both Android and iOS-based mobile devices. This includes both applications and malware that execute on the mobile device, as well as remotely conducted exploits utilizing command and control servers.
- Network Attack Vulnerabilities – testing via multiple Man-in-the-Middle (MiTM) attacking techniques to monitor and extract data from even encrypted communications.
- Mobile Device Vulnerabilities – including root-accessible smartphones and outdated firmware.

Key Findings

- **SandBlast Mobile** could detect and block 100 percent of malicious applications and network attacks, and mitigate all device vulnerabilities, regardless of operating system.
- **SandBlast Mobile** had 33 percent better protection against network attacks than the industry average - most notably against MiTM authentication based threats.
- **SandBlast Mobile** detected 20% more Android and iOS device vulnerabilities than the average MTD solution.
- **All vendors** provide a very clear, user-friendly dashboard with detailed and exportable event logs that enable subsequent, further threat analysis.

Robert Smithers

CEO

Miercom

Introduction

With more smartphones and tablets being accommodated in enterprise networks, the growing implementation of Bring Your Own Device (BYOD) strategies prompt the enterprise network administrator to pay more attention to the mobile-platform threat landscape.

Enterprises already secure their own network and devices, but when employees and clients are sharing information through an increasing number of mobile and BYOD technologies on a corporate network, the security is not always extended. Mobile phone security, in the form of an application alone, is not enough to protect the network and can't be effectively monitored by the enterprise. This presents the need for an MTD solution that can monitor and prevent threats from entering an enterprise network from both BYOD and corporate-assigned mobile devices.

MTD goes beyond Mobile Device Management (MDM) solutions by incorporating device protection with that of remote servers and cloud-based solutions, but it can also work hand-in-hand with the control and policy enforcement of MDM to offer well-rounded defense. Mobile devices themselves open the door for many attacks and exploitable operating system vulnerabilities. Enterprises also need protection against MiTM attacks which are becoming more likely over unsecured WiFi hot spots. MTD is security-focused, ensuring new exploits are detected and prevented.

To address the range of mobile threats we look at malicious applications, network attacks and device vulnerabilities. False positive avoidance efficacy is included in application and network threat security because an MTD solution should protect without being too unrealistic about which activity is allowed and useful for a company. Lastly, we evaluate the ease of use for each solution tested. Security that is too complex to understand and implement does not complement the time and budget constraints of an enterprise's IT department.

Solutions Considered for Review

The MTD Industry Assessment was made known to leading enterprise MTD vendors in the marketplace.

Skycure

Impact of Mobile Threat Growth

The International Data Corporation (IDC), in its *Worldwide Quarterly Mobile Phone Tracker,* reported in November 2016 that annual smartphone global sales would surpass 1 billion units. Of all smartphones shipped this past year, Android remains the top seller, garnering 85 percent market share. From the attacker's point of view, the more devices sold equates to more access points to disrupt a network.

Consequently, money spent on mobile device security and protection has increased to parallel mobile device market trends. Predominantly Android-based device security is purchased because of its greater potential to be compromised.

Organizations do not have the time, resources or budget to handle every single security threat. The need for a solution to both detect and then remediate mobile-device threats is becoming more apparent – and becoming more relevant as mobile device deployment grows.

And leading MTD vendors are gearing up to stay ahead of the curve as the threats are multiplying and morphing. Their collective goal is to produce a solution that can detect, mitigate and prevent threats in real-time. Additionally, administrative control needs to remain simple, with a quick learning curve to accommodate the enterprise's resource constraints.

Enterprise Purchases

Any enterprise that utilizes mobile devices in their network should be interested in protecting their assets. This can range from small businesses to Fortune 500 and Global 5000 companies. The latter have been among the first to purchase and trial and/or deploy the latest and greatest MTD solutions since they have the most at stake. Additionally, organizations with highly sensitive data related to health care, technology and insurance are just as aggressive in evaluating new products. It's not enough to use traditional on-premise protection against attackers; the world of mobile, remote and cloud services exposes the backdoors of the enterprise require attention.

Bottom line: Enterprises need to protect against mobile device threats, network attacks and inherent vulnerabilities using one core solution. MTD offers the best functionality and deployment for detecting and eliminating threat vectors for an enterprise.

Miercom Industry Assessment

Independent of any party, Miercom undertakes a thorough, in-depth competitive analysis of products and services. Tested products and/or services include network equipment, software products, hybrid products and services like Software as a Service (SaaS).

All vendors in a particular space are considered and invited to participate with their product prior to the review, at no charge to them. All vendors are afforded the opportunity to review their results during testing, following testing and prior to information being published.

Industry averages of the data, taken from the average performance or efficacy score in any given area, are maintained by Miercom. These Industry Averages are updated in real-time, as additional products may be tested. Miercom publishes these results at least every six months.

How We Did It

As with most technology areas, Miercom uses a proprietary "Industry Assessment" methodology to evaluate competitive mobile device protection products for their real-world use in enterprise environments. Using hands-on testing, realistic threat environments are produced and applied to provide a fair means of determining the strengths, weaknesses and techniques used by each security solution in responding to malicious activity.

The Miercom Security Test Suite contains unique, custom-crafted attacks and malicious-application samples. High detection efficacy against this blend of samples indicates that the security solution under test delivers robust and granular protection on multiple attack vectors.

MTD solutions are tested against three vectors that attackers use to compromise an enterprise network: malicious applications, network attacks and device vulnerabilities.

Malicious Applications

Third-party applications are not always secure and can expose the device to manipulation. The attacker can retrieve data from the phone or disguise itself as a corporate device while entering a business network.

To test, we first sideloaded safe applications on each phone using Android ADB and iFunbox for iPhones. Then legacy and unknown malicious .APK and .IPA files were sideloaded. Legacy samples should be easier to detect; unknown samples are challenging since some MTD solutions use reputation techniques. The applications flagged as a threat were recorded and notifications regarding these samples were observed.

False positive avoidance was tested to determine if benign applications were suspicious enough to be falsely identified as a threat. Sometimes applications include advertisement software and if the MTD solution is too stringent, it may block the application. It was important to see if the MTD under test would be unrealistically protective in the real world.

Network Attacks

Wireless interception, unsecure configurations and captive portals are the main areas which attackers use to gain access into an enterprise network.

Mobile devices use corporate WiFi to communicate to a business network. Using traffic interception, traffic decryption and fraudulent authentication we tested whether an MTD solution could detect the external monitoring, manipulation and access of a mock user.

VPN and suspicious configurations are other ways that attackers trick a mobile device to reroute communications to remote, malicious Command and Control (C&C) servers. MTD solutions were tested for the detection efficacy of these instances.

Captive portal false positives were non-malicious captive portals seen in places like an airport, a café or campus library. While captive portals can be exploited and used for malicious intent, they are not always harmful. The MTD solution under test should flag only when there is a legitimate threat and avoid the captive portals examined in multiple locations.

Device Vulnerabilities

Operating systems are exploited by attackers, so developers update with software patches to prevent this. If the end user does not implement these updates, the device remains vulnerable.

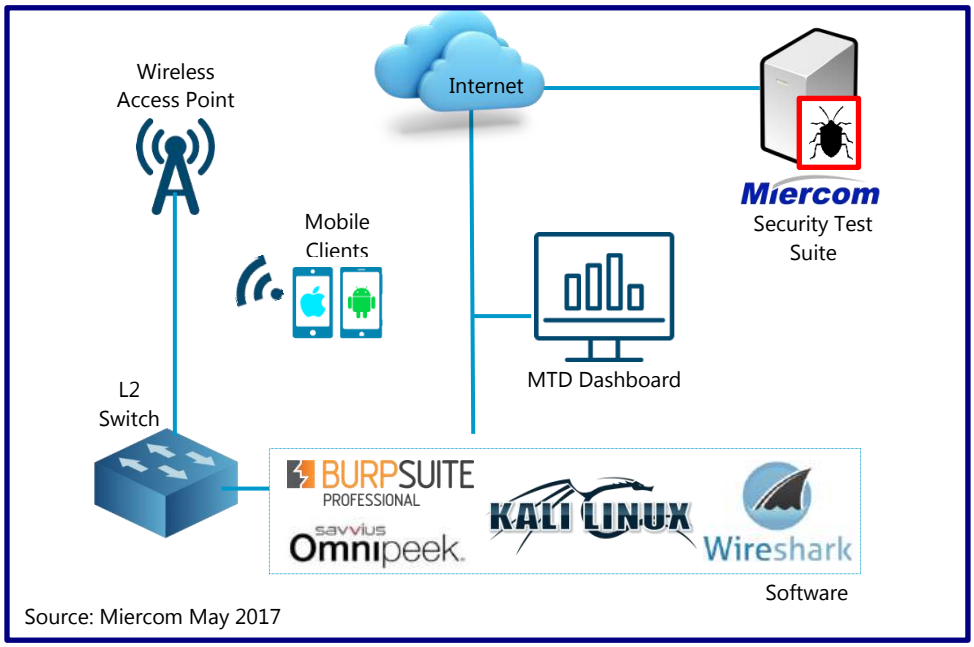
Mobile devices can be rooted or jailbroken to provide more control and customization options, but this leaves direct control for an attacker if the device becomes compromised.

Malicious profiles can be enabled by a user through a link or new application settings, letting an attacker have remote access to the device and network.

These vulnerabilities all have one thing in common: they are preventable by the user. But if the user is unaware, the device and network remain exposed. A useful MTD solution should detect that these vulnerabilities are present and notify the user and network administrator.

During testing, devices were rolled back to outdated operating systems, others were rooted, and some were exposed to a malicious profile. MTD solutions were expected to notify and, if capable, provide remediation steps.

Lab Topology



Mobile devices are loaded with the mobile client component of the MTD solution under test. The client software communicates with the MTD server, which is observed in the test bed on an administrative monitor (after appropriate login credentials are applied).

Several versions of the Android and iOS operating systems were used when analyzing attacks.

Malicious applications were delivered using the Miercom Security Test Suite. Network attacks were executed using Kali Linux and BurpSuite software. Any malicious application samples that are missed by the product being tested are observed and can be captured using network tapping software.

Test Tools

Miercom used a mixture of proprietary tools, custom scripts and leading industry test equipment to create real-world environments and attack scenarios.

Test Tool	Version
Kali Linux	2.0
Burp Suite	1.6
Savvius OmniPeek	10
Wireshark	2.0

Kali Linux is a Linux operating system distribution 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" attacks on encrypted network connections. *SSL Strip* was used for hijacking and monitoring secured HTTPS traffic.

Burp Suite includes the *Burp Proxy* tool which acts as a proxy server to intercept, inspect and modify traffic to and from client and server. This tool was used for "Man-in-the-Middle" attacks for the Network Attack section of this industry assessment.

Savvius OmniPeek 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.

Wireshark creates and analyzes packet captures. It calculates application and network response times, data and network volume statistics for over 1,200 applications.

Client Device	Operating System
Google Pixel XL	Android
HTC One M10	Android
Huawei P9 Plus	Android
Meizu Pro 6 Plus	Android
Samsung Galaxy S5, 7Edge	Android
iPhone 5, 6, 6s, 7	iOS

Malicious Applications

Malicious applications are used for stealing sensitive or personally identifiable information, degrading device performance or using an endpoint in a botnet attack.

In 2016, Check Point discovered the "DressCode" malicious application on GooglePlay. This app was downloaded by up to two million users, externally operated with a C&C server. The infected user enters a BYOD network and gives the attacker access to the organization through the application, exposing private communications and files.

Check Point was also able to identify malware attributed as "Gooligan" which rooted more than 1 million Android devices. Compromised devices had accessible Google accounts, messages, documents, photos, mail and storage. This malware belongs to a family of threats which operate remotely with C&C servers and deeply rooted into the factory reset process and system applications. This persistent malware continues to infect users through third-party app stores, direct message links or adware.

Miercom used the following threats to replicate real-world apps that an attacker would use for carrying out such attacks.

Type	Description
Known	Samples have high reputation and are expected to be 100 percent detectable for the most basic protection
Unknown, Modified	Modified SHA signatures render these samples without a reputation but remain as threatening as known malicious apps
Unknown, Zero-day	Zero-day implies these threats have never been listed or seen by threat intelligence systems, so they are too new to have a reputation
Remote Exploits	Specifically apps that may be reliant on C&C servers to carry out malicious intent
False Positive Avoidance	Seemingly risky apps that pose no threat; adware may look like malware but it is just annoying and may violate stringent policies
iOS	Apple iOS apps that are germane to this platform only

Method

All clients were loaded with a set of applications:

- Adobe Acrobat Reader
- Facebook
- FTPManager Free
- Line
- Microsoft Excel
- My Data Manager
- Pandora
- TeamViewer
- WebMD
- Zedge

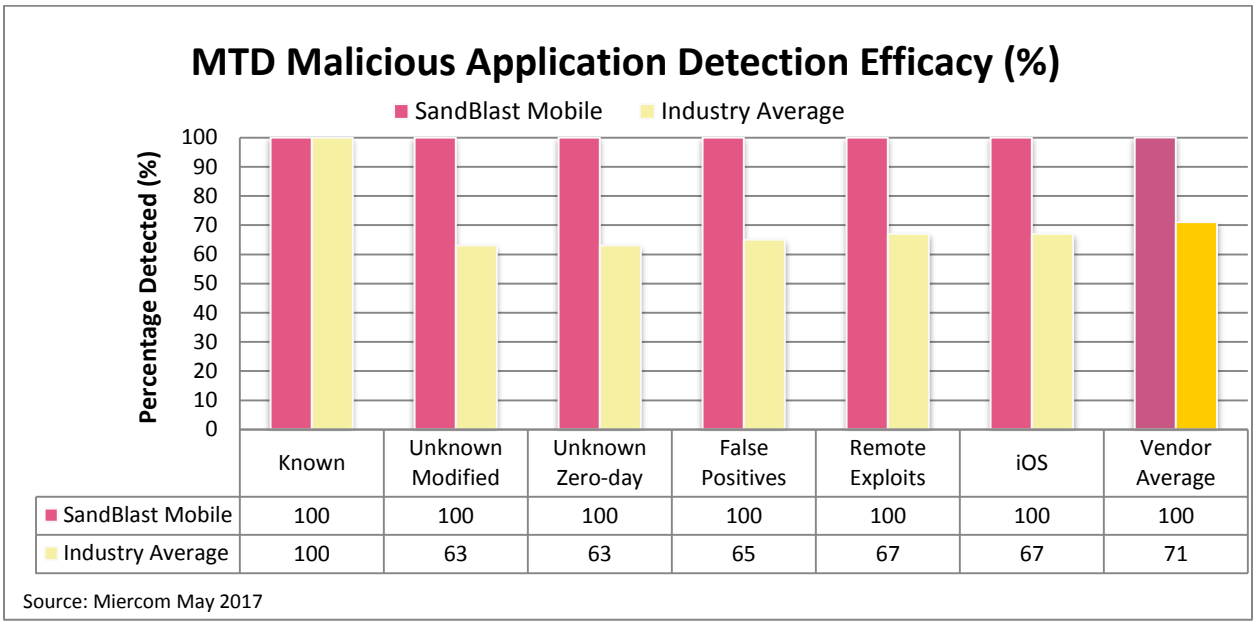
Then the MTD application under test was applied to each client. The clients were rebooted and any necessary credentials were setup to register the clients within the administrative console.

Malicious applications were loaded using Android Debug Bridge (ADB) USB for Android phones and iFunbox for iPhones. A predetermined amount of malicious application samples were delivered to each client using a script. The number of samples detected was recorded and compared to the total samples for an efficacy percentage.

False positives samples are intentionally suspicious, albeit legitimate. The False Positive Avoidance test evaluates how well an MTD solution can both discern between suspicious and malicious samples. A score of 100 percent implies the MTD solution can avoid the unnecessary flagging of clean samples. The purpose of this test is show that while a solution may have high detection percentages, it should be the result of security that is refined and not just overly strict.

Test Results

The results compare MTD solutions with an Industry Average for each category of malicious apps.



	Known	Unknown Modified	Unknown Zero-day	False Positives	Remote Exploits	iOS	Vendor Average
SandBlast Mobile	100	100	100	100	100	100	100
Industry Average	100	63	63	65	67	67	71

Source: Miercom May 2017

The Industry Average for detecting malicious applications stands at 71 percent.

SandBlast Mobile could detect all malicious apps, despite a sample unknown to virus databases, which was quite impressive. SandBlast Mobile leveraged reputation-based analysis, behavioral anomalies and, more importantly, full application emulation – the key to its high application detection rate – to provide the best malware prevention.

Network Attacks

Attacks can be software based, as with malicious apps, or they can be network oriented. Network attacks use the enterprise infrastructure against itself. For example, clients communicating to servers via WiFi are susceptible to an attacker listening in on encrypted traffic. If the attacker can pose as a trusted source, clients will begin sending information to the wrong place. Once access is gained, all sensitive data is at risk within the organization.

A notable MiTM attack is "Superfish," which installed a universal, self-signed Certificate Authority (CA) for spreading ads on encrypted pages. The CA provided each client with the same private key, enabling SSL communication to be tapped, intercepted or modified.

Common attacks, described below, were recreated in tests to mimic unauthorized network access.

Type	Description
SSL Interception	Known as "SSL Bump" is a malicious proxy that routes traffic through the attacker network
SSL Stripping	Attacker obtains connection and rewrites content in plaintext, excluding HTTPS links, exposing encrypted traffic
Man-in-the-Middle (MiTM) Attack	Circumvents mutual authentication by acting as both client and server CA, redirecting the client to a malicious network
Detect VPN	A user downloads an app or configuration profile requesting VPN authorization which would route traffic through the attacker VPN
Suspicious Configuration	Clients may be connected to potential C&C servers, especially on networks with exploitable, default configurations
Captive Portal False Positive Avoidance	Web interfaces used to authenticate users require login credentials to access the local network

Method

Using Kali Linux with SLL Interception and SSL Stripping, attacks were made over wireless connections between the client and the test network server.

SSL Interception, or Bump, created a key and certificate. By installing on the client devices, the attacker had a proxy by which to reroute traffic.

SSL Strip enabled IP forwarding traffic which redirected traffic to go to Port 8080, instead of Port 80. All of the victim's data was rerouted to the attacker.

BurpSuite was used to carry out the MiTM attacks. Custom certificates were made to capture and decrypt traffic traversing from client to server.

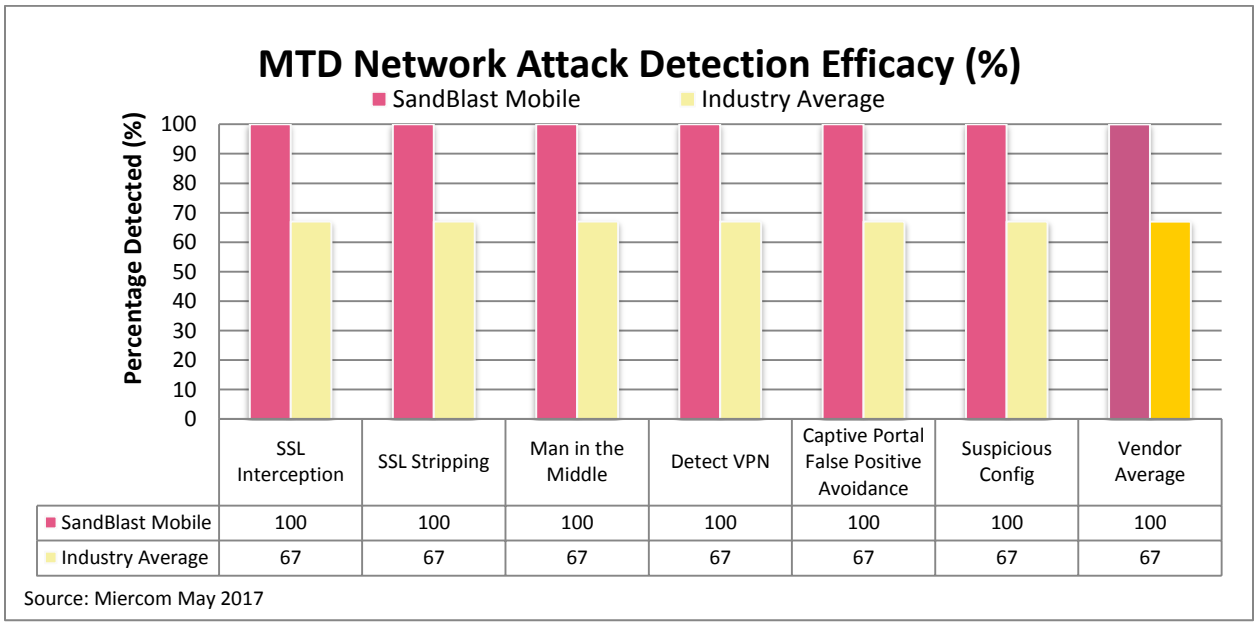
VPN testing was conducted using live network configurations. We "roamed" to multiple locations sampling VPN networks and examined how each vendor's product interacted with the VPN network.

Captive Portal was recreated using the wireless captive portal of a network in a commercial location. The MTD solution under test should be able to alert that a captive portal is being used and identify the network requesting credentials.

While malicious Captive Portal detection was not included at this time of testing, it is worth noting that this proxy interface should be identified as malicious by a vendor when involving suspicious measures such as decryption of traffic or detection of VPN. Public captive portals available in commercial areas should not always be identified as malicious when requesting credentials for network access. Future testing will include emulated malicious captive portals to determine if MTD vendors can discern between legitimate and compromised portals.

Test Results

The below results compare each MTD product to the Industry Average by attack category.



	SSL Interception	SSL Stripping	Man in the Middle	Detect VPN	Captive Portal False Positive Avoidance	Suspicious Config	Vendor Average
SandBlast Mobile	100	100	100	100	100	100	100
Industry Average	67	67	67	67	67	67	67

Source: Miercom May 2017

The Industry Average was poor at 67 percent. SandBlast Mobile was able to detect and block 100 percent of network attack attempts. While the efficacy scores above reflect detection only, it is important to note that some MTD solutions could not block network attacks they were able to detect. Other solutions were unable to either detect or block.

Device Vulnerability

Aside from malicious-software and network-based vectors, attackers gain access by targeting devices that are vulnerable because of modified access, outdated firmware and malicious profile installation. Failure to update to the latest operating system release is a major contributor to several weaknesses which leave devices exposed and susceptible to intercepted secure connections, hijacking, manipulation and data breaches. For an enterprise, it means a network vulnerability.

The tests detailed in the table below were performed on Android and iOS-based smartphones to determine how well the MTD solution could detect these vulnerabilities and prevent these threats from executing.

Type	Description
Android, Rooted Device	Android mobile operating system is modified to have privileged control, or "root access", giving admin permission to the device
Android, Outdated Operating System	Outdated Android operating systems contain vulnerabilities that have been patched by updates and later versions
iOS, Jailbroken Device	iOS mobile firmware is modified to have privileged control by "jailbreaking", giving admin permission to the device
iOS, Outdated Operating System	Outdated iOS firmware contains vulnerabilities that have been patched by updates and later versions
iOS, Malicious Profile	These "mobileconfig" files give permission to configure system settings such as WiFi and VPN, and can access secure connections

Methodology

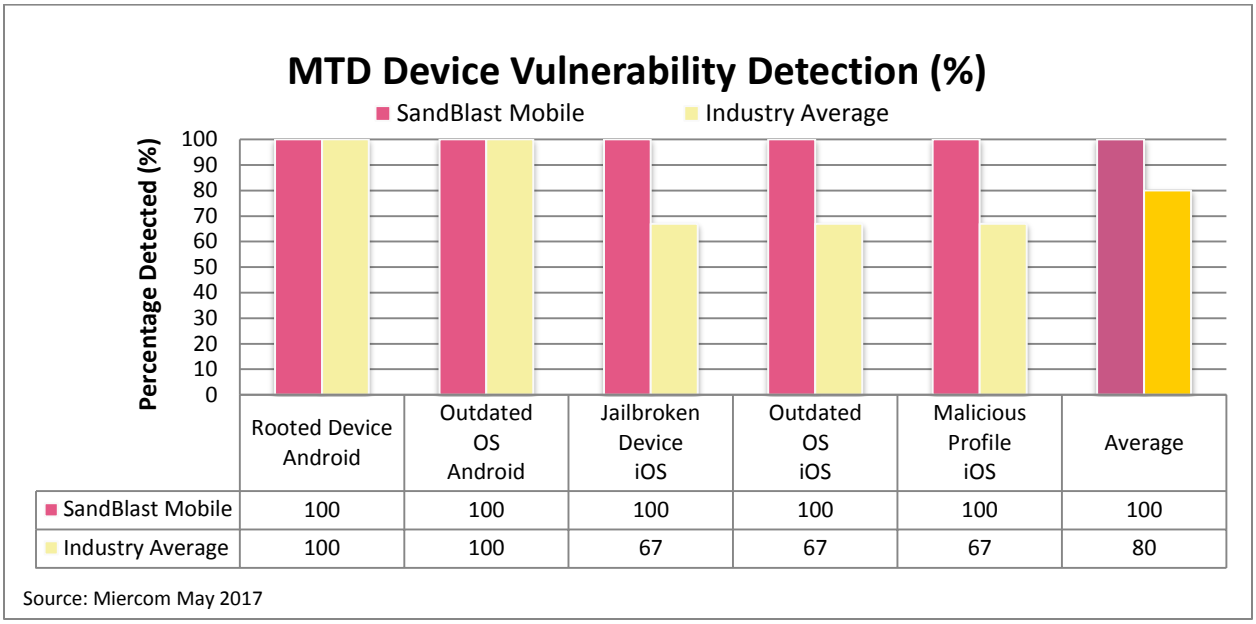
Android and iOS devices were rooted, or jailbroken, to create a root-access vulnerability. The MTD solution was expected to detect that the endpoint left its privileged control open to harmful manipulation.

Android and iOS devices were manually rolled back to an outdated firmware release, left unprotected by recent updates. The MTD solution was expected to identify the obsolete firmware version and notify the user and admin for remediation.

For iOS clients only, a custom malicious profile was installed to remotely access the device. Whether or not the MTD product was able to gain permission to system settings was recorded.

Test Results

The below results compare each MTD solution to the Industry Average for each type of device vulnerability for both Android and iOS operating systems.



	Rooted Device Android	Outdated OS Android	Jailbroken Device iOS	Outdated OS iOS	Malicious Profile iOS	Average
SandBlast Mobile	100	100	100	100	100	100
Industry Average	100	100	67	67	67	80

Source: Miercom May 2017

The Industry Average stands at 80 percent. SandBlast Mobile and other vendors were able to detect root-access devices, outdated firmware and a malicious iOS profile. However, some vendors did not support iOS protection.

Quality of Experience

The administrator and user experiences with the MTD solution distinguish a great product from a good one. SandBlast Mobile and other MTD vendors were assessed for:

- Deployment,
- Usability and
- Remediation experience, using the scale below.

	SandBlast Mobile	Industry Average
Deployment	●	●
Usability	●	●
Remediation	●	●

Deployment

● SandBlast Mobile

DEPLOYMENT RATING: EXCELLENT

Setting up and configuring SandBlast Mobile was easy. Within minutes, the console was connected to the network and vulnerabilities or threats could be observed being detected.

● Industry Average

DEPLOYMENT RATING: VERY GOOD

Some solutions similarly had quick and straightforward setups, while offering helpful and friendly technical support. But some solutions required more detailed instructions, multiple links and application windows which could result in more human error.

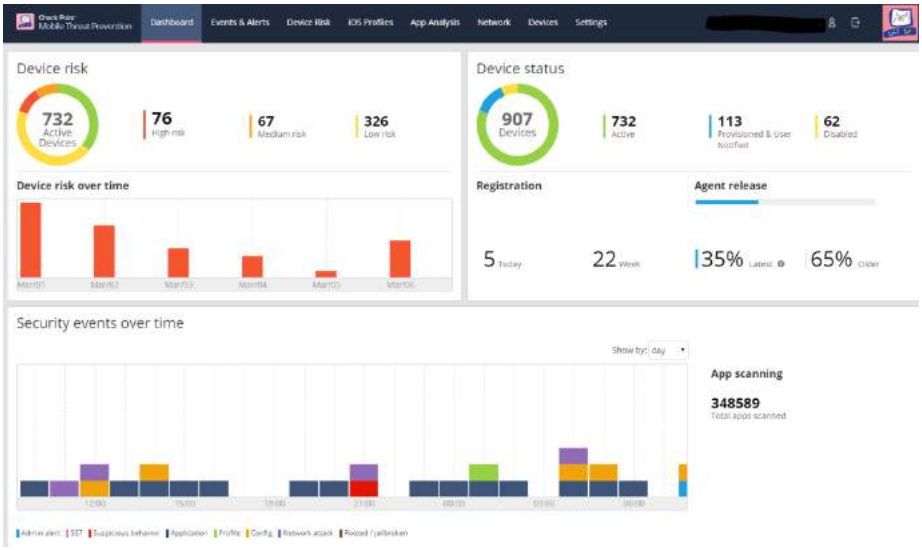
Usability

● SandBlast Mobile

USABILITY RATING: EXCELLENT

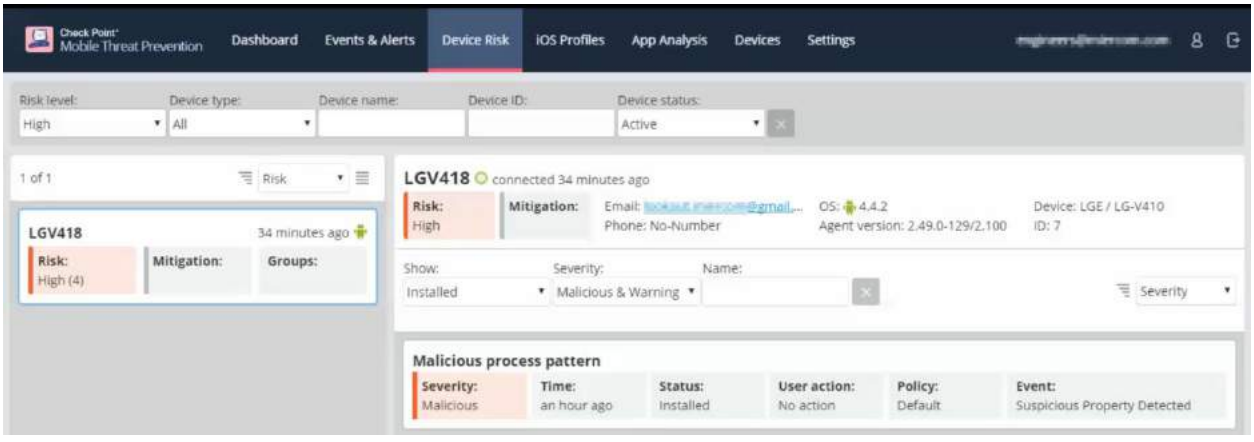
Dashboard monitoring of malware processing and quarantine status was very straightforward. A first-time user could easily navigate and understand the details of threat events and remember how to reproduce details of these threats.

Figure 1: SandBlast Mobile Admin Dashboard



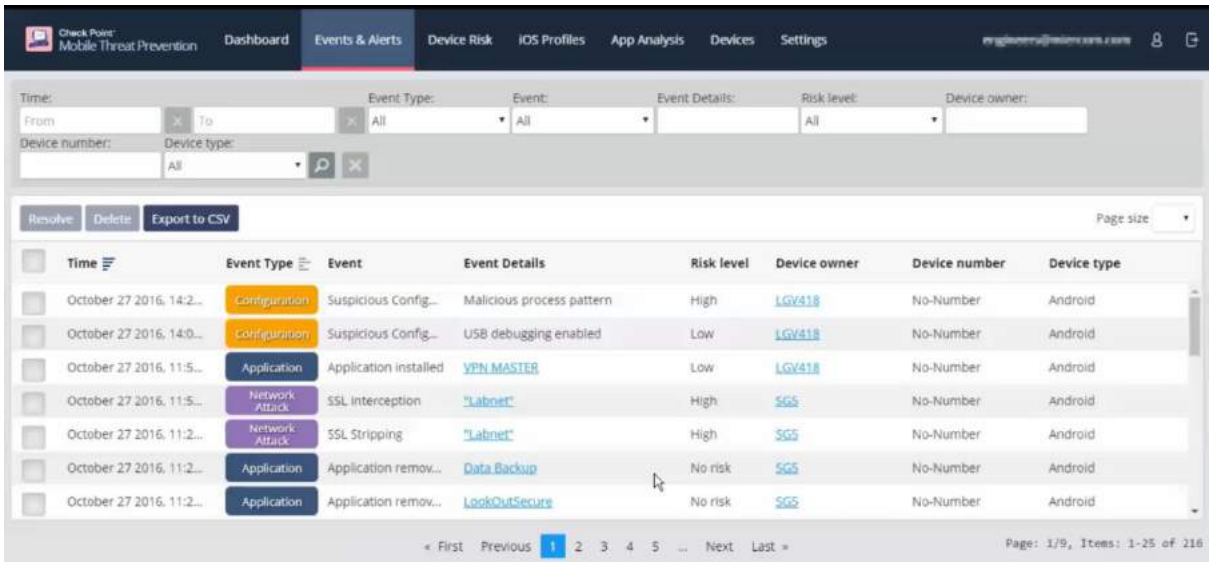
The dashboard is clear and simple. Tabs at the top allow you to view each threat, the risk level and more detailed analysis. The aesthetic is pleasing and not overwhelming. Messages are displayed to both administrator (in console) and the user.

Figure 2: SandBlast Mobile Device Risk Assessment



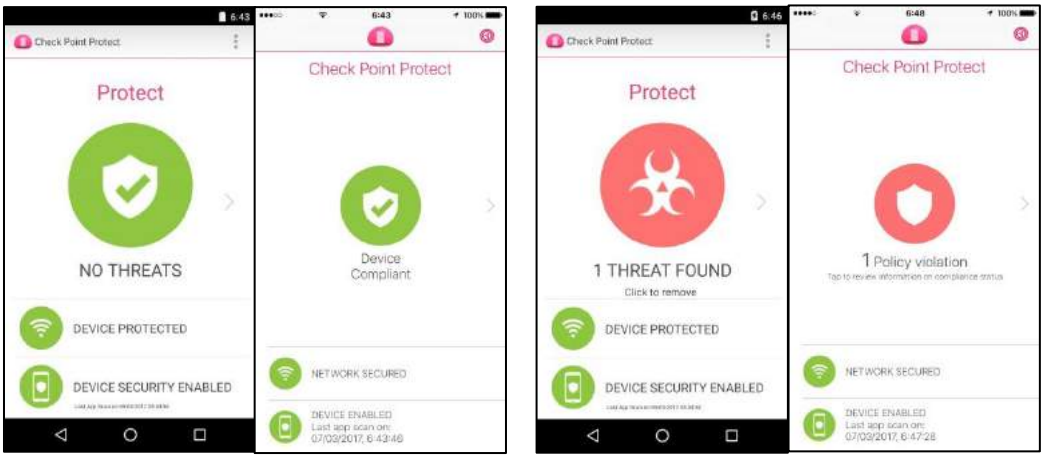
Threats are ranked as low, medium and high risk. The outcome is dependent on the stringency of the policies set for the network.

Figure 3: SandBlast Mobile Threat List



Threats are sortable by timestamp or event type. As in Figure 2, each threat is assigned a risk level. This is a more detailed view of the threat itself, not just the device it affects.

Figure 4: SandBlast Mobile Android and iOS Notifications



Protection against threats is visible through Android and iOS platforms. The notifications are clear and simple.

● Industry Average

USABILITY RATING: VERY GOOD

Other vendors also had aesthetically pleasing interfaces with easy task execution to minimize errors, but one interface had so much detail that it could be overwhelming to a first time user. In general, every interface was simple and helpful for monitoring threats.

Remediation

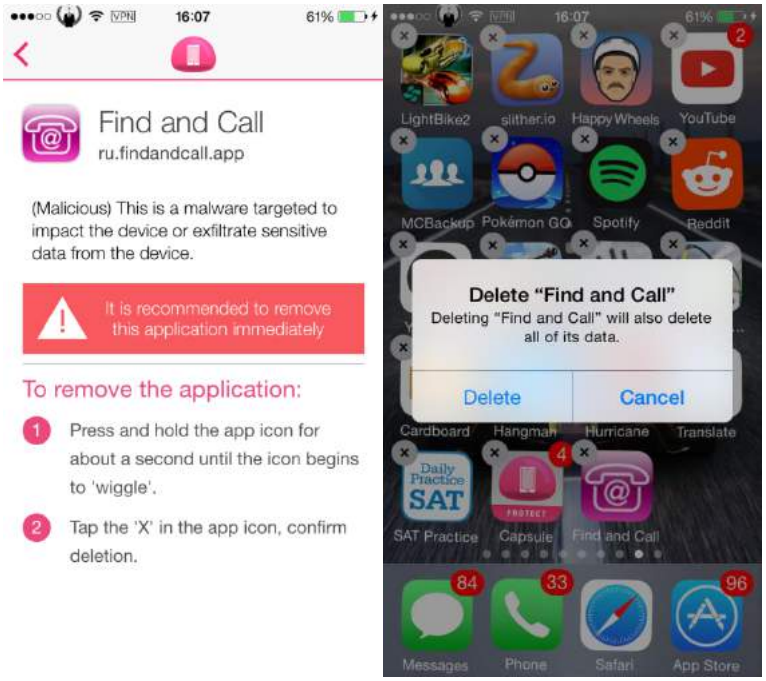
The MTD solution monitors all mobile device activity to identify, block and report threats of compromised devices. Remediation options can be made available for each client and administrator.

- SandBlast Mobile

REMEDIATION RATING: EXCELLENT

The administrator has a full view of the threats that need to be remediated. The end user is also guided through the steps of removing malicious activity or firmware. The steps were clear, easy and took less than a minute to perform. The figure below shows an example of a notification regarding malicious application installation.

Figure 8: SandBlast Mobile Endpoint Malicious App Remediation



The endpoint is notified of the type of application that is being installed. A two-step process is offered to remove it.

- Industry Average

REMEDIATION RATING: GOOD

Some vendors lacked blocking capabilities but still offered informative remediation recommendations. One vendor could alert the administrator of a threat in the console but gave no visibility of the outcome, leaving remediation steps ambiguous and open-ended.

Unique Features

Malicious attackers are always looking to exploit coverage gaps, but SandBlast Mobile offers the following unique features to counteract these threats.

SandBlast Mobile

"Action-based" Detection: SandBlast Mobile detection does not rely exclusively on vulnerability type or reputation. Installations are monitored and threats are categorized into risk-based enterprise policy violations.

Innovative False Positive Detection: Instead of solely examining the signature database, SandBlast Mobile evaluates activity based on two factors – reputation and complexity.

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 Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. 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 weak areas of security or performance. Unless there is active participation or an Ongoing Customer Care plan in state, all exploit samples are proprietary and kept confidential. Samples and specific vulnerabilities are not publicly published for the safety of the vendor, its products and product users.

About Miercom Annual 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.

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 report but errors and/or oversights can occur. The information documented in this report 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.

This report was part of Miercom's continuous Industry Assessment of Mobile Threat Defense products. Each vendor featured is 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 express 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.