CHECK POINT SANDBLAST MOBILE

MOBILE THREAT DEFENSE

2019 REPORT

MIERCOM CERTIFIED SECURE

LEARN MORE ABOUT THE TESTED BENEFITS OF CHECK POINT SANDBLAST MOBILE THREAT DEFENSE.

DR190620C

Detailed Lab Report

Find this report on:

https://miercom.com/check-point

CERTIFIED SECURE 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.

TABLE OF CONTENTS

01 | EXECUTIVE SUMMARY	4
02 | INDUSTRY ASSESSMENT™ SUMMARY	6
03 | ABOUT MOBILE THREAT DEFENSE	8
04 | SANDBLAST MOBILE	9
05 | HOW WE DID IT	10
06 | PROTECTIVE FEATURES	12
07 | NETWORK ATTACK PREVENTION	15
08 | DEVICE VULNERABILITY	16
09 | REMEDIATION	17
10 | EASE OF USE	18
11 | ABOUT MIERCOM	19

EXECUTIVE SUMMARY

MOBILE DEVICES ARE A HIGH-RISK FACTOR PROMPTING AN URGENT NEED FOR RELIABLE DEFENSES TO PROTECT CORPORATE DATA.

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. Check Point SandBlast Mobile offers a Mobile Threat Defense (MTD) solution with features to accomplish this and engaged Miercom for independent validation.

Testing consisted of exposing the MTD solution to multiple iterations of attacks, particularly newly found malware. Check Point SandBlast Mobile detected high percentages of our custom-crafted sample set once examined by its included Check Point ThreatCloud Sandbox.

KEY FINDINGS

99% SECURITY

SandBlast Mobile surpassed its competition. The average vendor only scored 63.8% efficacy for MTD features: threat protection, network attack prevention, device vulnerability prevention, remediation tools and ease of use.

A+ ANALYTICS

For threat defense scenarios, SandBlast Mobile scored a **97.2%** efficacy rating. It was able to find advanced malware applications with impeccable accuracy. For behavioral-based attacks, it caught **98.3%** of the attempted breaches.

PERFECT PREVENTION

SandBlast Mobile detected 100% of browsing, privacy invasions, network-based and device-based threats and vulnerabilities. Its combination of refined remediation tools and easily navigated interface made stopping threats effortless.

> *"Based on our observations, we found the Check Point SandBlast Mobile solution to be a superior defense against the latest threat trends and techniques – no matter how advanced or evasive. SandBlast Mobile stands up to its claims and outperforms its competition, earning the Miercom Certified Secure award for its sophisticated mobile defense technology."*
>
> **- ROB SMITHERS, CEO MIERCOM**

Our test results indicate that the SandBlast Mobile solution is an excellent choice for enterprises looking to protect their network against the ever growing world of mobile threats.

We were thoroughly impressed with the security that SandBlast Mobile provided, and further so by its competitive standing in its market space. The average vendor fell short by as much as 39 percent in defensive measures against the multiple attack scenarios and vectors tested.

Since our last testing of SandBlast Mobile, the MTD solution has improved its network-based defense by 33 percent for Man-in-the-Middle (MiTM) detection. In this round of testing, it was also assessed for MiTM prevention, scoring 100 percent efficacy compared to the vendor average of only 50 percent.

Additionally, during subsequent rounds of testing with us, Check Point has been able to make their product better. In the three times we've seen SandBlast Mobile, we find this solution continually improves its ease of use, and its detection efficacy is unparalleled. With this, SandBlast Mobile continues to stay ahead of the curve when compared to its competition.

For 30 use case scenarios, simulated with cutting edge test tools and a realistic corporate network environment, SandBlast Mobile offered 100 percent security against 28 of these tests. Their global and dynamic intelligence feeds allow its defense to keep its finger on the pulse for new threats designed to take down a network. In addition to its paramount attention to detail, the application and dashboard interface was seamless and intuitive – making threat and device visibility simple and useful for quick remediation without affecting work productivity.

Check Point SandBlast Mobile was Miercom verified to have fast, easy security for mobile endpoints, with straightforward visibility and tools, to protect corporate users and sensitive business data. It showed a 99.8 percent quality of experience (compared to the average 78.4 percent) and a first-year cost similar to other MTD products. From this cost-benefit analysis, we found SandBlast Mobile to be an extremely valuable product to enterprises looking for a mobile defense solution.

Rob Smithers, CEO

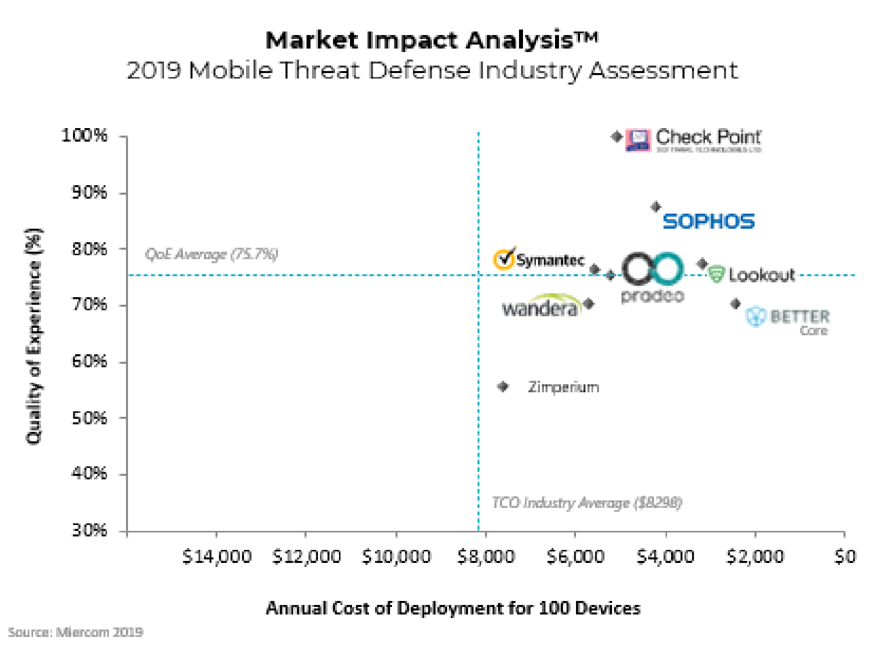
Miercom

Miercom CERTIFIED SECURE™

INDUSTRY ASSESSMENT™ SUMMARY

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 the Check Point SandBlast Mobile solution with respect to similar vendors in its 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.



Source: Miercom 2019

Check Point SandBlast Mobile showed the highest Quality of Experience (QoE) rating of 99.8 percent. Its pricing, at $5040 for 100 devices per year, was less than the average MTD vendor. Check Point SandBlast Mobile offers exceptional value with the best QoE and detection efficacy, as well as very good relative total cost of ownership. From this, we believe SandBlast Mobile to be an excellent and affordable choice for protecting enterprise mobile devices.

Miercom's Market Impact Analysis (MIA) for Mobile Threat Defense of 2019 investigates product value on the basis of quality of functionality and use, as well as the average cost for first-year deployment.

Quality of Experience, also called QoE (vertical axis), summarizes the security efficacy, ease of use, service setup and utilization, support, business practices and legal restrictions involved with the product under test. The percentage is derived from current and past experience, user feedback, product strengths and opportunities to improve.

The Total Cost of Ownership, or TCO (horizontal axis), is the sum of costs calculated per a specified device count for a first-year deployment. This cost is subject to change, based on current discounts or negotiations made between vendor and customer. But this cost is used to best reflect the cost of training and related expenses, product upgrades, support, licensing and legal restrictions.

Please note: Vendors featured in this assessment consist of both active participants in hands-on testing and analysis, and some which were not actively involved but subjectively evaluated. All vendors are afforded to opportunity to participate in our MTD Industry Assessment at no charge.

Miercom tested Check Point SandBlast Mobile against similar MTD solutions using five categories. These tests provide a well-rounded and comparable set of scores that were used in calculating the Industry Average for each test area. Check Point is compared to the Industry Average, per test area, to determine the relevance and novelty of its mobile defense features and capabilities.

The following efficacy ratings look at the protective features offered against malware and other threat-based attacks on mobile endpoints; network attack prevention for attacks using the business network to infiltrate mobile devices; inherent device vulnerabilities that put the network and its endpoints at risk; remediation options for fixing issues before they become costly network problems; and ease of use to evaluate how intuitive the product is for both the end user and network administrator.

Mobile Threat Defense Efficacy Scores 2019

Check Point SandBlast Mobile vs Industry Average

Test Category	Check Point SandBlast Mobile	Industry Average
Protective Features	99	64
Network Attack Prevention	100	75
Device Vulnerability	100	90
Remediation	100	70
Ease of Use	100	93
Average	**99.8**	**78.4**

Source: Miercom 2019

**The Industry Average is calculated based on efficacy ratings of actively participating vendors of the MTD Industry Assessment only.*

Check Point SandBlast Mobile achieved a detection and functionality efficacy rating of 99.8 percent, outperforming the average vendor by over 21 percent. It had perfect defense against network attacks and device vulnerabilities, and near perfect protection against malicious file transfers and manipulation. Remediation was straightforward, and immediately effective, with a dashboard that was easy to use and intuitive to navigate.

ABOUT MOBILE THREAT DEFENSE

> *According to a WhiteHat Security study, 85% of mobile applications violate security standards. While web and mobile applications offer advanced user experiences, businesses with traditional applications and systems fail to provide support for this transition to evolving mobile technology. Nearly 70% of applications, according to this 2018 study, showed inherited vulnerabilities from third-party libraries and open source software.*

Mobile devices are at the forefront of communication, but they bring new threats that most businesses are not capable to handle. Challenges range from flaws in mobile application software, encrypted communications, browsing capabilities and visibility of end user devices.

Without an MTD system in place to monitor, detect and remediate these issues, the network and its users are susceptible to data theft, unauthorized access and devasting breaches that cost businesses productivity and overhead.

To combat the mobile threat landscape is the Mobile Threat Defense solution – a product deployable on employees' corporate and personal mobile devices, protecting the corporate network. Such protection includes actionable insight and step-by-step removal of threats and vulnerabilities before, during and after an attack. These attacks are inevitable, but they are not impossible to overcome with the right security measures in place.

MOBILE THREAT DEFENSE NECESSITIES

✓ **DETECTION**

Advanced analysis finds mobile threats attempting to enter the network before they become a problem.

✓ **PREVENTION**

If an attacker unleashes a payload, it can be prevented from infecting the device and spreading to the network.

✓ **VISIBILITY & ACTION**

Thorough attention to mobile devices and knowledgeable actions against threats are paramount to protection.

✓ **EASY IMPLEMENTATION**

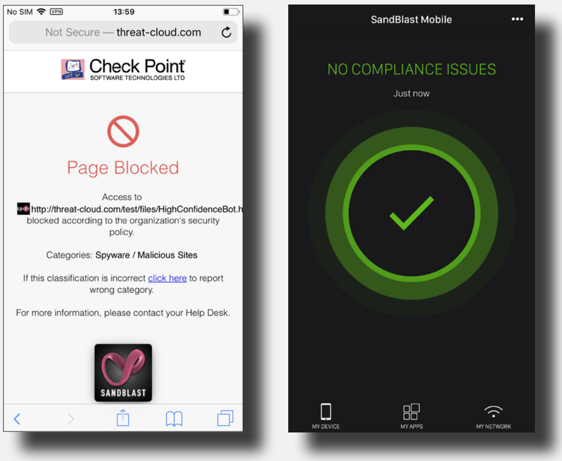
Being secure isn't enough if the process is confusing. Being able to get mobile protection should be fast, easy and intuitive.

SANDBLAST MOBILE

Check Point SandBlast Mobile offers a mobile threat defense solution that includes all the necessary protection and more. Its security includes complete threat detection and mitigation with top-rate efficacy and prevention against sensitive data extraction. With its simple deployment, devices are given robust protection against the latest threats for multiple attack vectors.

SANDBLAST MOBILE HELPS BUSINESSES REDUCE RISK & IMPROVE PRODUCTIVITY BY STOPPING THREATS IN THEIR TRACKS.

SandBlast Mobile examines all mobile applications in a virtual, cloud-based environment as well as examines any suspicious network behavior. Device vulnerabilities are also assessed to determine if they pose a risk to sensitive information and privacy. Both Android and iOS smartphones and tablets are scanned before they are allowed on the network and then constantly checked to maintain that access.



Not Secure — threat-cloud.com

Page Blocked

Access to http://threat-cloud.com/test/files/HighConfidenceBot.h blocked according to the organization's security policy.

Categories: Spyware / Malicious Sites

If this classification is incorrect click here to report wrong category.

For more information, please contact your Help Desk.

NO COMPLIANCE ISSUES

Just now

Threats are stopped on the device and immediately disconnected from the network, alerting both user and network of the violation.

CENTRALIZED THREAT INTELLIGENCE

SandBlast Mobile uses a cloud-based dashboard to view and manage devices and infections with real-time surveillance. Check Point's ThreatCloud dynamic security intelligence is constantly updated with the latest threat trends on a daily basis using feeds from more than 100,000 security gateways and 100 million endpoints across the globe.

UNIQUE FEATURES:

- ANTI-PHISHING
- SAFE BROWSING
- CONDITIONAL ACCESS
- ANTI-BOT
- URL FILTERING
- WI-FI NETWORK SECURITY
- EASY DEPLOYMENT

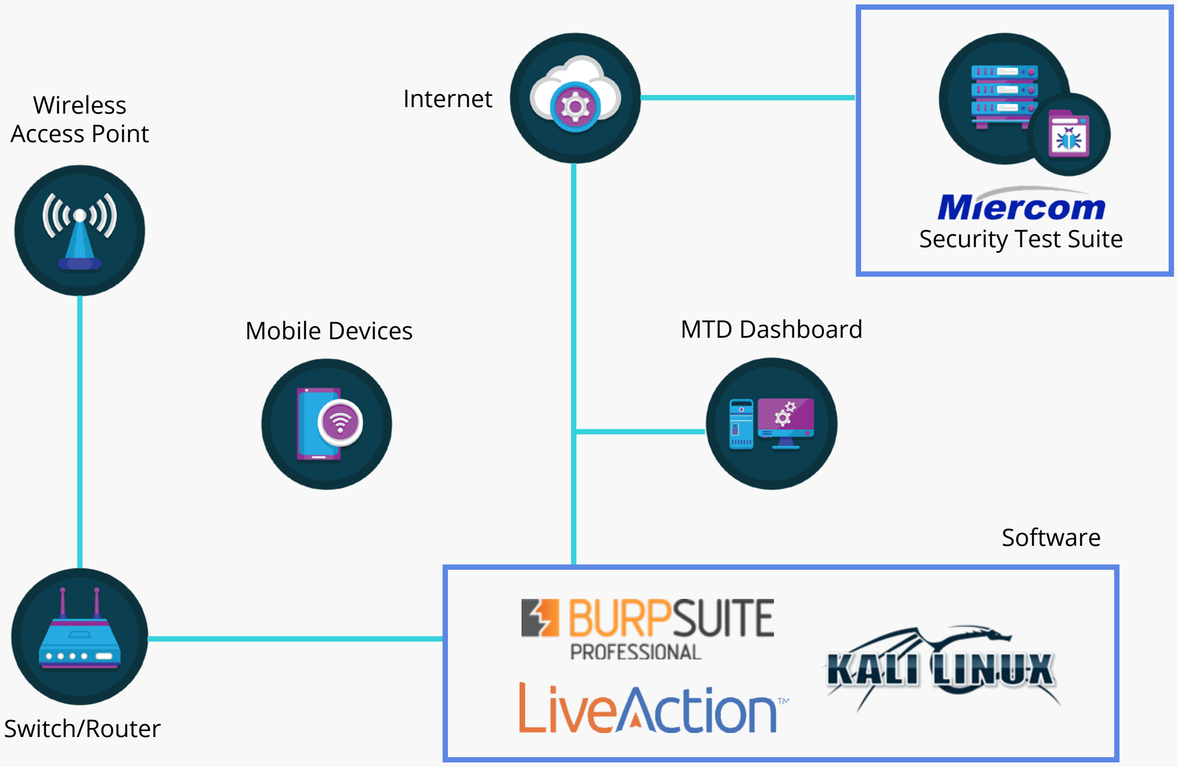
HOW WE DID IT

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.



Source: Miercom July 2019

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.

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*
- *Zedge*

The MTD solution under test was applied to each client. The clients were rebooted, and any necessary credentials were set up to register the clients within the administrative console.

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

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

Using a detailed methodology and test tools, we applied multiple common and advanced mobile-based breach scenarios to the test network environment. From these tests we found the following results for each MTD solution and compared to infer the benefit of the Check Point SandBlast Mobile defense solution.

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.

IT IS NOT A MATTER OF IF, BUT WHEN.

ATTACKERS USE MULTIPLE VECTORS TO BREACH A NETWORK.

MTD SOLUTIONS SHOULD BE READY FOR EVERY CASE.

Using four main categories of threats, we tested Check Point SandBlast Mobile and competing solutions for the security efficacy of protective features. Results are detailed with percentages of samples blocked, as well as insight as to how Check Point SandBlast Mobile compares. From this, we validated the claimed protective features offered.

THREAT DEFENSE

We first took a look at malware applications – some known, some signatureless, and others installed unconventionally. We further looked at advanced samples that defined the robust and granular capabilities of the global intelligence and techniques of the MTD solution under test.

Threat Type	Check Point SandBlast Mobile	Industry Average
Malware Download Prevention	100	48
Known Malware Detection	100	81.9
Zero-Day Malware Detection	83.3	56.8
False Positive Malware Detection	100	63.4
Persistent Malware Detection	100	46.1
Sideloaded Malware Detection	100	100
Average	**97.2**	**66.0**

Source: Miercom July 2019

Check Point SandBlast Mobile proved 31 percent more effective at preventing mobile malware on both Android and iOS operating systems than the average score for all MTD vendors. SandBlast Mobile was able to detect 100 percent of malware download samples, known malware, false positive malware and sideloaded malware. In terms of prevention, SandBlast Mobile blocked 100 percent of persistent malware – specialized, evasive malware that is hard to remove. The most threatening malware was the set of zero-day malware; these samples have modified SHA signatures, rendering them undetectable to legacy signature-based scanning technology. SandBlast Mobile detected over 83 percent of the in-the-wild malware, an impressive feat that outperformed the average vendor which could only identify a little over half of these threats. Initial scores were lower, but upon retesting – after the Check Point ThreatCloud Sandbox examined these samples – SandBlast Mobile was able to detect most, if not all, the threats attempted. This shows that as more threats are observed with Check Point's global cloud intelligence, the more sophisticated all SandBlast Mobile detection becomes – in real-time.

BEHAVIORAL DETECTION

Not all malicious activity is easy to detect. Some threats using evasive exploit techniques require comparison to a normal, baseline activity to determine if they are out of the norm. Behavioral detection of anomalies effectively mitigates evasive malicious threats – for constant, but intelligent, surveillance of access, information collection, services and code injection.

Scenario	Check Point SandBlast Mobile	Industry Average
Sensitive Information Collection	100	50
Sensitive Application Permission	100	62
Sensitive File System Access	100	40
Unsecure Network Traffic	90	94
Cloud Services	100	74
Data Exfiltration	100	50
Command & Control Communication	100	50
Dynamic Code Download	100	50
Average	**98.3**	**58.8**

Source: Miercom July 2019

Check Point SandBlast Mobile was over 39 percent more secure than the average vendor against use cases where behavioral detection was employed. SandBlast mobile could detect 50 percent more samples than the average vendor for: sensitive information collection, data exfiltration, command and control communication and dynamic code downloads.

SAFE BROWSING

Not all websites are equal. Attackers depend on human nature to guide users towards malicious sites based on social engineering.

Threat Type	Check Point SandBlast Mobile	Industry Average
Known Phishing Sites	100	73.3
Zero-Day Phishing Sites	100	60
Malicious URLs	100	50
URL Filtering	100	62.5
Average	**100**	**61.4**

Source: Miercom July 2019

Check Point SandBlast Mobile detected 100 percent of browser-based exploits - 38.6 percent higher than its competitors.

PRIVACY

Private user and corporate data should stay exactly that - confidential. MTD solutions were tested for their ability to prevent applications collecting sensitive information, or at least more than necessary.

Threat Type	Check Point SandBlast Mobile	Industry Average
Application Privacy	100	100
Average	**100**	**100**

Source: Miercom July 2019

Check Point SandBlast Mobile was up to the industry standard, ensuring 100 percent privacy against application information gathering.

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.

MTD solutions should detect and prevent MiTM activity before it puts the network at risk.

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

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.

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.

Threat Type	Check Point SandBlast Mobile	Industry Average
Man-in-the-Middle Detection	100	100
Man-in-the-Middle Prevention	100	50
Average	**100**	**75**

Source: Miercom July 2019

Check Point SandBlast Mobile was able to both detect and prevent all instances of MiTM attack attempts via mobile devices – an efficacy 25 percent higher than the average MTD vendor.

DEVICE VULNERABILITY

MTD solutions were tested for their ability to detect and prevent device vulnerabilities that put the network at risk for a breach. 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.

SANDBLAST MOBILE HAS 100 PERCENT PROTECTION AGAINST CONNECTED VULNERABLE DEVICES.

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.

Threat Type	Check Point SandBlast Mobile	Industry Average
Rooted Device Detection	100	100
Malicious Profile Prevention	100	60
Enterprise Developer Certificate	100	100
Unsecure Device Settings	100	100
Average	**100**	**90**

Source: Miercom July 2019

Check Point SandBlast Mobile had 100 percent efficacy against all vulnerability scenarios - 10 percent higher than the average vendor. Despite their hardened operating system, iOS devices were susceptible to malicious configuration profiles. The average vendor could only protect 60 percent of the time against this particular vulnerability; Check Point was able to prevent all instances of attempted profile installations.

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.

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

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.

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.

Remediation Features	Check Point SandBlast Mobile	Industry Average
Policy Compliance	100	90
Conditional Access	100	55
Reporting	100	65
Average	**100**	**70**

Source: Miercom July 2019

Check Point SandBlast Mobile offered the best remediation tools for isolating infections, visualize threats and export detailed status reports. The average vendor had 30 percent less effective corrective actions.

EASE OF USE

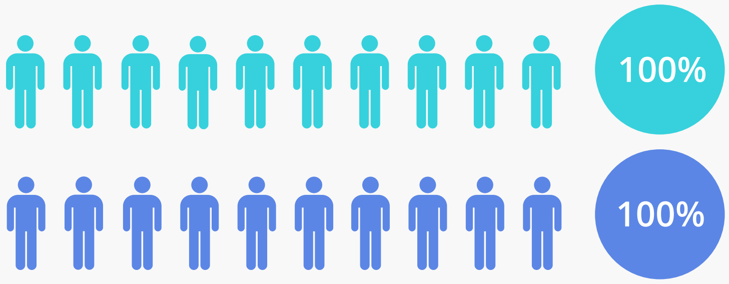
Usability is underrated and sometimes overlooked. But despite accurate detection and prevention, a front-end that is hard to use or deploy will result in downtime and frustrated users. This can be a make-or-break aspect when deciding between two similarly effective MTD solutions.

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.

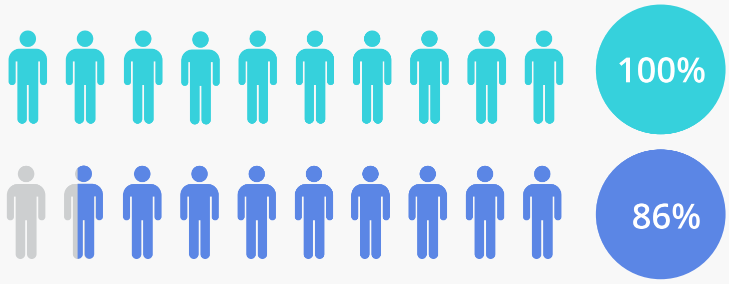
USER ACTION

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

Check Point SandBlast Mobile has a perfect score for its easy client installation, matching the Industry Average vendor. Simply download the client application, enter credentials, and your device is protected.



USER ACTION

Check Point SandBlast Mobile is impressively straightforward in all actions taken during test case scenarios in previous sections. The average vendor was only 86 percent effective of having a clear interface and instruction before, during and after a breach.

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.

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.

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.

FOR MORE INFO

CONTACT US

reviews@miercom.com

Miercom

elevating testing standards.