Check Point
SOFTWARE TECHNOLOGIES LTD

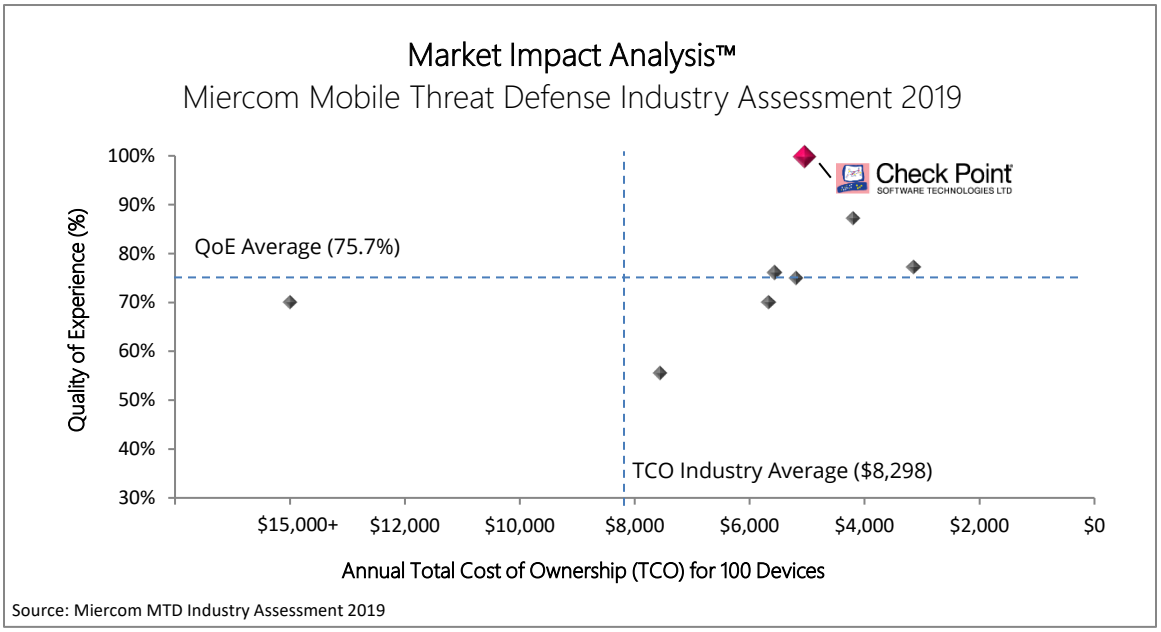
SandBlast Mobile

Check Point SandBlast Mobile offers a lightweight mobile threat defense application for iOS and Android to gather data and analyze threats in an enterprise environment by monitoring operating systems, applications and network connections. Its simple deployment gives devices top-rate detection efficacy and prevention against malicious behavior.

SandBlast Mobile examines all mobile applications both on-device and virtually, performing resource-intensive analysis is performed in the cloud to minimize impact on device performance and battery life while maintaining the end user experience. Mobile devices continuously checked for authorized access and privacy.

Users can view and manage devices or infections with a cloud-based dashboard with real-time surveillance. Check Point's ThreatCloud dynamic security intelligence is updated daily with the latest threat trends using feeds from more than 100,000 security gateways and 100 million global endpoints.

For more information, visit: https://www.checkpoint.com/products/mobile-security/.



Source: Miercom MTD Industry Assessment 2019

Using collected data from our observations, comparative test reports and other sources, we formed the Market Impact Analysis™ map of current enterprise MTD products. This visual evaluation presents the relationship between product quality and value over the course of one year. Quality of Experience (QoE) is measured using the average rates of detection and prevention efficacy, as well as scored ease of use and remediation action options. Total Cost of Ownership (TCO) factors in the costs of installation, management and maintenance into product purchase price for 100 licensed users.

The graph shows a quick view of product effectiveness relative to projected total costs, allowing enterprises to make better informed purchasing decisions and providing insight to vendors as to where their product is in the competitive landscape.

Key Strengths

- 100% detection of known malware, false positive malware and sideloaded malware
- 100% prevention of malware downloads and persistent malware attempts
- 100% detection of sensitive information collection, app permission and file system access
- 90% unsecure network traffic detection
- 100% detection of cloud services and command & control communications
- 100% prevention of data exfiltration and dynamic code downloads
- 100% detection of known & zero-day phishing sites and malicious URLs
- 100% URL filtering
- 100% application privacy detection
- 100% Man-in-the-Middle attack detection and prevention
- 100% rooted device detection
- 100% malicious profile prevention
- 100% detection of enterprise developer certificates and unsecured device settings
- Easy client installation
- High value MTD product when compared to similar products

Features Not Verified

Check Point actively participated in our MTD Industry Assessment study. By giving Miercom engineers full access to product and support, SandBlast Mobile was subjected to every test case scenario.

Analysis

Recommended Buy: High Quality, High Value.

Check Point showed 99 percent security: 97.2 percent efficacy against malware; 98.3 percent efficacy for behavioral-based attacks; and 100 percent detection of browsing and privacy scenarios. Pairing its high-level security with its top-notch remediation and ease of use, we found this product was a simple but granular solution at an affordable annual cost for mobile protection.

For a detailed report of our findings, see our Miercom report: https://miercom.com/2019-mtd-check-point-sandblast-mobile.

For a full overview of the SandBlast Mobile architecture, visit: https://community.checkpoint.com/t5/SandBlast-Mobile/SandBlast-Mobile-Architecture-Overview/td-p/40322

About Miercom MTD Testing

Each product that was tested independently in the Miercom Industry Assessment was evaluated using sets of malware, network attacks and device vulnerabilities in a controlled environment. To test MTD features, the smartphones and tablets were removed from all Internet connections and threat samples were introduced via USB drive. The mobile security program was directed to scan for threats and, upon completion, the results were recorded as a percentage detected and/or blocked from the total samples sent. Any and all anomalies which may have occurred during testing were noted as well. All software used to conduct these threats were obtained on the Internet, Google Play Store and/or Apple AppStore.

Every vendor is afforded the opportunity to represent their product in our Industry Assessment product reviews, free of charge. Any vendor included in our studies has had opportunity to review results before publishing and has opportunity to resubmit a product for test review if they do not agree with the results.

Some vendors opted to not actively participate in our study. Regardless, Miercom reserves the option to review products through open source means, through customer deployments and feedback, or by using data from previous product reviews.

Miercom is an editorial publishing company and reserves the right to publish and print editorial opinion on vendor products. We never agree to overly restrictive EULAs or other legalese of unconscionable terms that suppress free speech or limit the comparing and contrasting of products or services which impede customers from making informed purchasing decisions.