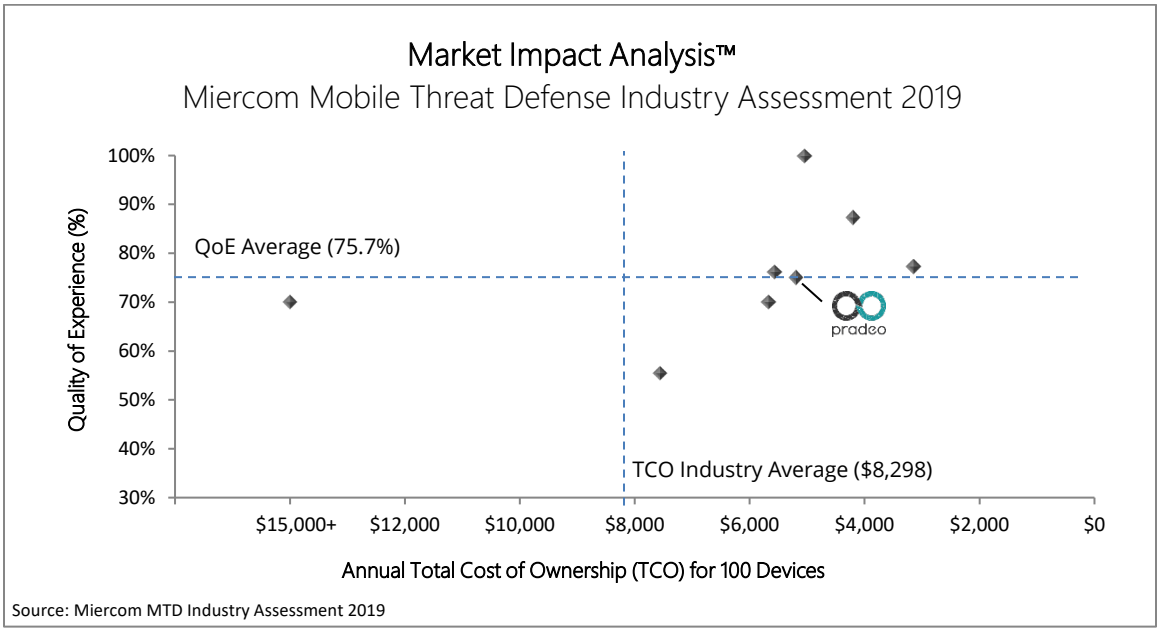
Mobile Threat Defense

Pradeo Mobile Threat Defense uses patented artificial intelligence engine for identifying application behaviors and mobile activity that can put the enterprise at risk. Combined with real-time analysis, zero-day protection and minimal use of resources, Pradeo security scans for behavior and vulnerabilities comparable to leading MTD solutions. Threat defenses include: signature-less scanning; static, dynamic and behavioral-based analysis; false positive detection; application blocking; vulnerability detection; and automated remediation. Pradeo security also protects networks and devices against Man-in-the-Middle attacks, access control and secure connections. By monitoring device integrity, Pradeo can detect operating system vulnerabilities, device rooting and exploitation as well as abnormal resource usage. Across all threat vectors, Pradeo integrates with MDM and EMM solutions to auto-update blacklists, update device statuses and track policy compliance.

For more information, visit: https://www.pradeo.com/en-US/mobile-threat-protection.



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

- Supports zero-day protection against malicious applications, device vulnerabilities and false positive malware
- Identifies rooted devices
- Supports Man-in-the-Middle detection
- Provides policy management and auto-remediation
- Supports MDM, EMM and SIEM integration

Features Not Verified

The following are features were not observed during testing:

- Detection of unknown, persistent and sideloaded categories of malware
- Behavioral detection of sensitive information collection, app permission and file system access
- Detection of unsecure network traffic, cloud service, command and control communication
- Prevention of dynamic code downloads
- Detection of known and zero-day phishing sites, malicious URLs and app privacy
- URL filtering
- Prevention of Man-in-the-Middle attacks
- Detection of malicious profiles, enterprise developer certificates and unsecure device settings
- Ease of client installation, user action and intuitiveness
- Support of policy compliance, conditional access and reporting

Analysis

Recommended Buy: Average Quality but Low Cost

Pradeo Mobile Threat Defense achieved a QoE score of 75 percent – a solid average for MTD solutions, coupled with its very affordable cost makes this solution a good value purchase decision.

We did not receive a response from Pradeo to participate in this MTD industry study. Our results are based off our own observations with publicly available resources and feedback from customers currently using this product. Pradeo is recommended to resubmit their current product for evaluation and receive feedback from Miercom engineers and prove unverified features to increase their QoE score.

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.