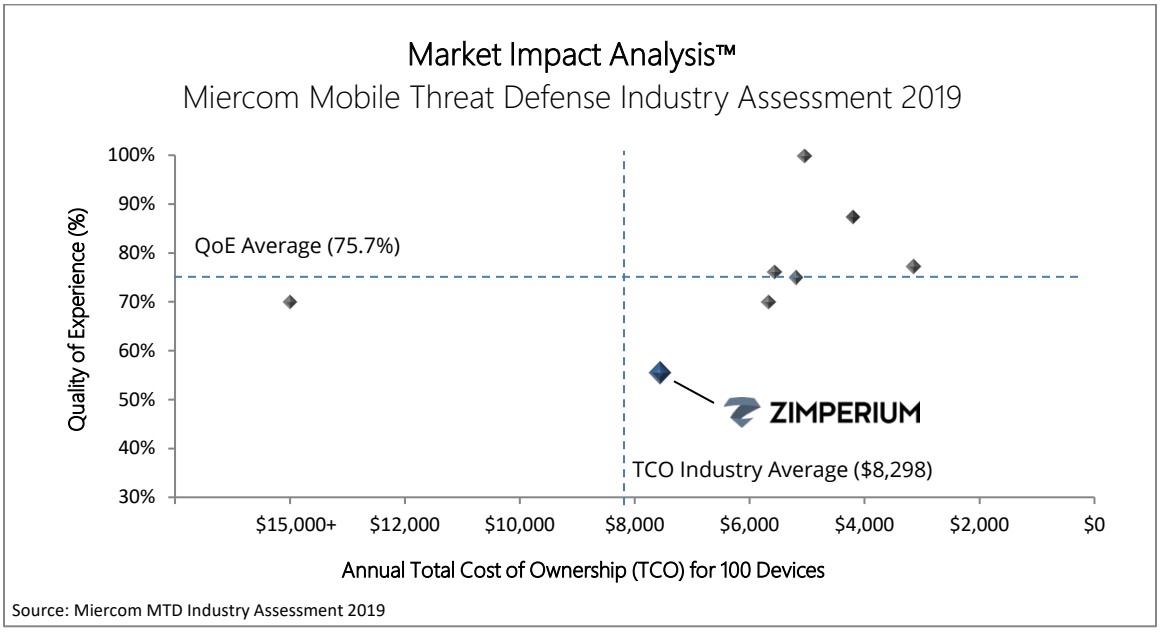
ZIMPERIUM

zIPS Enterprise-grade Mobile Security

Zimperium's zIPS mobile security is an on-device, stand-alone application that provides endpoint antivirus protection for mobile devices and data against threats of a BYOD corporate network. It is part of the Zimperium's four key solutions: zIAP, an SDK that protects mobile applications; zConsole, a management and reporting console for policy and integration control; and z3A, a reporting and analytics tool for security and privacy protection. Zimperium security is further enhanced using is machine learning core engine, z9, to detect zero-day exploits in real-time on device or in the cloud. Together, the Zimperium mobile security solution can protect against mobile application attacks and risks, network threats, privilege abuse and advanced exploits resulting from device vulnerabilities and social engineering.

For more information, visit: https://zimperium.com.



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% sideloaded malware detection
- 80% detection of sensitive application permission and unsecure network traffic
- 100% application privacy detection
- 100% Man-in-the-Middle attack detection
- 100% detection of rooted devices, enterprise developer certificates and unsecured device settings
- Effective policy compliance for remediation
- Easy client installation

Suggested Recommendations

- Improve threat defenses, specifically: detection of known malware, unknown malware, false positive malware; and prevention of malware downloads and persistent malware attempts
- Expand behavioral detection for sensitive information collection, sensitive file system access, cloud services; and prevention of data exfiltration and dynamic code downloads
- Strengthen known phishing site detection and add capability to detect zero-day phishing sites, malicious URLs and perform URL filtering
- Include ability to prevent Man-in-the-Middle attacks and malicious profiles

Analysis

Affordable Solution but Poor Quality

Zimperium zIPS has a QoE score of 55.5 percent, 23 percent below the average of other products in the industry. This score reflects its ability to detect malware, network threats and device vulnerabilities, while providing appropriate and easy to use interfaces for immediate visibility, control and remediation. While it is an affordable option, Zimperium lacks an impressive defense that will protect most of the enterprise BYOD network.

Since choosing to not to actively participate in this MTD industry study, Zimperium is highly recommended to submit their current product for full evaluation. This allows for access to all available features for engineering feedback to improve the listed recommendations.

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.