Quadrant Knowledge Solutions

Security and Risk Management

SPARK Matrix™: Mobile Threat Management (MTM), Q4 2022

Market Insights, Competitive Evaluation, and Vendor Rankings

November 2022

TABLE OF CONTENTS

Executive Overview

This research service includes a detailed analysis of global Mobile Threat Management (MTM) market dynamics, major trends, vendor landscape, and competitive positioning analysis. The study provides competition analysis and ranking of the leading MTM vendors in the form of SPARK Matrix. This research provides strategic information for technology vendors to better understand the market supporting their growth strategies and for users to evaluate different vendors capabilities, competitive differentiation, and its market position.

Market Dynamics and Overview

While the adoption of mobile devices has improved employee mobility, it has also made the job of the SecOps teams harder by adding another endpoint to be secured, as trends like hybrid work and flexible workspace witness allow workers to access organizational networks via various nonsecure endpoints such as tablets, personal desktops, laptops, smartphones, and other mobile devices. Due to such a heterogeneous device landscape, endpoint management is becoming increasingly difficult for organizations.

Therefore, organizations require advanced modern management, identity, and threat capabilities to protect all their endpoints. Mobile Threat Management (MTM) solutions help in this regard by protecting mobile devices, networks, and mobile applications from sophisticated and dynamic mobile threats. An MTM solution evaluates OS versions, system settings, firmware, and device configurations on mobile devices to look for risks. It also looks for misconfigurations and other vulnerabilities. Additionally, MTM solutions continuously scan for unusual, unsanctioned, and suspicious activities of users that escalate their privileges to get unauthorized access to the network. Furthermore, MTM solutions scan for unusual behavior in network traffic. The solutions can also detect counterfeit and invalid certificates as well as compromised security needed to prevent Man-in-the-Middle attacks. An MTM solution identifies malware and grayware in the applications through reverse engineering and analyzing source code.

An MTM solution also helps organizations seamlessly integrate BYOD policies into their workforce and helps respond to threats before they cause any potential damage. Additionally, an MTM solution provides greater visibility into the critical risks associated with the mobile devices used for organizational purposes and safeguards sensitive organizational data.

Quadrant Knowledge Solutions defines a Mobile threat management (MTM) solution as “an advanced solution that protects, detects, analyzes, and remediates against known and unknown mobile device threats in the organizations.” The solution utilizes different techniques, including machine learning and mobile threat intelligence-based behavioral analysis. It provides real-time reporting and control against malicious activity (attacks) targeting mobile endpoints and applications.

Following are the key capabilities of Mobile Threat Management:

- **Mobile Endpoint Protection:** A mobile threat management solution helps organizations monitor mobile endpoints running on iOS, Android as well as Chrome OS and secure them against app-based threats (malware, rootkits, and spyware). The solution also provides protection from network-based threats (man-in-the-middle attacks) and device-based threats (jailbroken/rooted devices, outdated OS, risky device configurations). A mobile threat management solution also utilizes machine learning and behavior-based detection to identify emerging threats with high precision and decline kernel access. The solution also scans applications, monitors mobile device risks, protects BYOD to increase employee productivity, and secures organizational and employee data with its built-in privacy controls. It protects enterprise infrastructure and corporate data by providing access only to trusted devices and provides real-time visibility into incidents enabling self-remediation.

- **Anti-Phishing and Content Security:** A mobile threat management solution helps organizations detect and block access to unsafe websites, malicious links, and other risky, harmful, or inappropriate content across corporate and personal devices by leveraging an AI-based detection engine and metadata analysis. It also alerts users about risky access in real-time and stops attackers from accessing both personal and corporate data without violating end-user privacy.

- **Threat Detection and Response:** A mobile threat management solution allows organizations to continuously monitor, identify, prevent, and block advanced malware, phishing sites, and zero-day attacks. Additionally, it quickly quarantines compromised devices and provides complete visibility into malicious, unauthorized, or accidental access to sensitive corporate data.

- **Device-based Protection:** A mobile threat management solution allows users to monitor OS versions, security update versions, system parameters, device configuration, firmware, and system libraries to detect security misconfigurations, device vulnerabilities, and suspicious and malicious activities. Additionally, the solution helps organizations overcome endpoint threats from vulnerabilities

to malicious or risky applications, identifies malware and trigger compliance actions, automatically blocks compromised iOS and Android devices with features like out-of-the-box jailbreak and root detection, and provides real-time threat insights and analytics to enrolled devices and their operating systems.

- **Application-based Protection:** A mobile threat management solution utilizes application-based protection, which allows organizations to review the apps installed on users' devices and check external data use, analyze app codes, examine URLs, review security implementations and developers and apps' reputation, detect data leakage and privacy issues, identify grayware and malware, as well as automatically scan enrolled devices to identify and uninstall malicious code and suspicious application.

- **Network-based Protection:** A mobile threat management solution provides protection against network attacks such as Man in the Middle/ SSL stripping on public Wi-Fi by monitoring network traffic and blocking malicious links or connections. It allows devices outside the network perimeter to securely access sensitive data, customizes device policy and compliance rules to automatically restrict access to vulnerable networks.

- **Device Vulnerability Management:** A mobile threat management solution enables the identification of potential vulnerabilities in the devices, network, and software and helps remediate these vulnerabilities. It leverages tools to automatically monitor, identify, remediate, mitigate, and classify vulnerabilities before they are exploited. The solution promotes rapid remediation and offers real-time visibility into devices to reduce the attack surface.

Competitive Landscape and Analysis

Quadrant Knowledge Solutions conducted an in-depth analysis of the major Mobile Threat Management (MTM) vendors by evaluating their products, market presence, and value proposition. The evaluation is based on the primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall Mobile Threat Management market. This study includes an analysis of key vendors, including Better Mobile Security, BlackBerry, Broadcom, Check Point, Corrata, CrowdStrike, Cybereason, Deep Instinct, ESET, IBM, Ivanti, Jamf, Kaspersky, Lookout, Palo Alto Networks, Pradeo, Psafe, Sophos, TEHTRIS, and Zimperium.

Zimperium, Lookout, Jamf, CrowdStrike, Check Point, Deep Instinct, Ivanti, Pradeo, Cybereason, and Corrata are the top performers and technology leaders in the global MTM market. These companies provide a sophisticated and comprehensive technology platform to deploy, manage, and secure corporate resources and applications on a diverse range of endpoints with different configurations, including mobile devices, desktops, laptops, and tablets. The platforms also provide centralized visibility and control over all endpoints deployed within an organizational environment. The MTM technology helps organizations effectively implement BYOD, remote working, and other initiatives.

Zimperium offers modules such as machine learning-based technology (z9), mobile device security (zIPS), mobile application analysis (z3A), and a Mobile Application Protection Suite (MAPS). Zimperium provides protection from identified and unidentified devices, networks, phishing, or any malicious app attacks on-device, complete mobile security solutions for Android, iOS, and Chromebook.

Lookout provides easy-to-use cloud modules for security detection, visibility, response, and remediation. The modules are accumulated into use-case-specific product packages to form and provide the Lookout product suite. The Lookout Security Graph gathers data from nearly 210 million mobile devices worldwide and over 175 million applications to identify emerging threats and continuously support the discovery of new threats such as Pegasus, Hermit, SilkBean, and other surveillanceware campaigns.

Jamf maintains deep technical integrations with its own device management solutions Jamf Pro and Jamf Now, as well as other leading MDM/UEMs. Jamf has co-developed capabilities with all leading UEM solutions, including Microsoft

Endpoint Manager, VMware Workspace ONE, IBM MaaS360, Ivanti/MobileIron Core and Cloud, Citrix, and more to streamline deployments, automate device lifecycle management to reduce administrative overhead, allow admins to remain in the UEM console while benefiting from enhanced contextual data on device risk posture, deployment status, and more from the data feed integrations.

Pradeo offers an artificial intelligence, machine learning-based MTM solution titled Mobile Threat Defense to stop data loss and enhance compliance with data privacy standards. Pradeo Security Mobile Threat Defense provides 360° threat protection, accurate mobile threat detection, automated protection, integration with EMM and UEM solutions, data privacy law compliance, and customizable security policy. Additionally, it includes app analysis technology for detecting zero-day threats and data processing, as well as the most advanced and extensive security information available.

Deep Instinct offers a predictive threat prevention platform to secure endpoints, mobile devices, and networks. It provides multi-layer protection provisioned across three stages, pre-execution that predicts & prevents, on-execution that detects and automatically responds, and post-execution that automatically analyzes and remediates known and unknown threats. Deep Instinct supports deep learning to efficiently detect, scan, and secure devices by preventing malicious applications from running on the devices.

Check Point's Harmony Endpoint provides MTM with a focus on detecting and preventing threats to apps, devices, and networks. It offers high levels of security against mobile phishing and message-based attacks targeting mobile devices. The integration of Harmony Endpoint with Check Point ThreatCloud intelligence helps the MTM solution by offering updates on advanced threats and malicious applications based on the data and telemetry collected from all the devices in the operational threat intelligence platform globally.

Ivanti Mobile Threat Management leverages machine learning algorithms to gain real-time insights into applications on user devices and improve decision-making with the use of detailed information representation on threat assessment scores as well as an explanation of risks and implications. Additionally, Ivanti MTD pushes local compliance actions that detect and eliminate both known and zero-day mobile attacks on-device, regardless the device is connected to a Wi-Fi or cellular network or not. Ivanti MTD provides granular control with a range of administrative features, which include filtering mobile apps with characteristics and receiving notifications for risks associated with newly created apps.

The CrowdStrike Falcon platform offers single lightweight-agent architecture and leverages cloud-scale artificial intelligence (AI) to provide real-time protection and visibility. Falcon Mobile helps organizations gain visibility into Wi-Fi, Bluetooth, and network connections and uncover spoofing and network interference. It enables organizations to detect vulnerable devices, including jailbroken devices and devices with non-compliant configurations and outdated iOS versions.

Cybereason Mobile leverages correlated attack intelligence to protect mobile devices proactively from ransomware and other malware, exploits, fileless and in-memory assaults, and malware. The Cybereason MTM product offers a user-friendly interface, which enables automated, or one-click threat remediation before they turn into breaches. Cybereason Mobile offers robust visibility across all attack vectors as well as auto-remediation and on-device protection. The product can detect, investigate, hunt, and remediate threats across traditional and next-gen mobile endpoints.

Corrata is identified as the emerging leader in the SPARK Matrix™ Mobile Threat Management. Corrata offers on-device mobile security and data control to protect devices from attacks and threats. It also provides visibility and control of all device traffic in real time and blocks unsanctioned cloud apps. Corrata offers an enterprise-grade firewall which it states provides unparalleled visibility, control over network traffic and helps identify advanced malware via AI-assisted network traffic analysis and device status. Corrata helps prevent latency, performance, and privacy issues by operating on-device and never routing traffic. Additionally, it provides a comprehensive feature set for both iOS and Android.

Broadcom, IBM, Palo Alto Networks, BlackBerry, ESET, Sophos, Kaspersky, Better Mobile Security, TEHTRIS, and Psafe have been positioned among the primary challengers. These companies provide comprehensive technology capabilities and are rapidly gaining market traction across industries and geographical regions. All the vendors captured in the 2022 SPARK Matrix™ of Mobile Threat Management vendors are emphasizing improving their capabilities to stop network threats, control data and access, and secure all mobile devices. They are also emphasizing on minimizing the complexity of the security stack and protecting against unauthorized access to sensitive data and digital assets. Additionally, they are emphasizing expanding the partnership channels and supporting diverse use cases. Organizations are consistently looking at enhancing user experience and expanding support for multiple deployment options.

Key Competitive Factors and Technology Differentiators

While a majority of the leading Mobile Threat Management (MTM) vendors may provide off-the-shelf MTM capabilities, seamless integration, comprehensive endpoint management, data and applications management, secure remote access and control, compliance check, patch management, software updating, endpoint security, and analytics & reporting, the flexibility of deployment and increased security posture may differ by different vendors offerings. Driven by increasing competition, vendors are increasingly looking at improving their technology capabilities and overall value proposition to remain competitive. Following are some of the key competitive factors and differentiators for the evaluation of MTM vendors:

The Sophistication of Technology Platform: Users should evaluate an MTM solution that offers comprehensive capabilities, including complete endpoint management, data and application management, secure remote access and control, endpoint compliance evaluation and remediation, patch management, automated software update, endpoint security, and analytics & reporting. Organizations are looking for vendors whose products can support endpoint devices running on a host of operating systems, including Android, iOS, Windows, and such others. They are also looking for other features, including easy integration with other cross-functional security tools to prevent vulnerabilities, easy functionality and management, operability in multi-cloud environments, ability to identify and protect from novel security threats, integration with identity solutions, automated onboarding, and support for mobile devices, and applications. The MTM solution should be able to detect known and zero-day threats as well as and phishing threats across device network, application, on-device without requiring updates or cloud connectivity. The vendor should offer a holistic and robust MTM solution that can fulfill the user's industry-specific and use case-specific requirements. An MTM solution should have robust enterprise capabilities to support the rollout and future-proofing of deployment - support for multiple MDMs, zero-touch activation, BYOD support, group-based policy controls and mapping, customizable RBAC controls, third-party integrations, etc. Additionally, the vendors' customer value proposition may vary in terms of ease of deployment, ease of use, price/performance ratio, support for a broad range of use cases, employee experience, global support, flexible & elastic subscription service, and such others.

Integration & Interoperability: MTM vendors are increasingly integrating their products with identity solutions, endpoint security solutions, and analytics solutions to provide a holistic solution with capabilities apart from endpoint management. An MTM solution should support integration with existing third-party applications. MTM vendors should provide deep integration with device management solutions like MDM/UEM solutions. MTM vendors are also offering advanced security by integrating with various security solutions like XDR, endpoint protection platforms (EDR), Endpoint Protection Platforms, endpoint DLP, and such others to provide best-in-breed endpoint protection and centralized visibility into cross-platform threats. Users should look for vendors offering integration points with device management suites (UEM), identity providers (IDP), and security operations tooling (SIEM, SOAR, and EDR) which fit within existing workflows.

Scalability: An MTM vendor should offer a sophisticated solution that can manage, secure, and monitor all endpoints and applications. The solution should be able to support a wide variety of mobile devices. Due to the wide acceptance of the BYOD policy and the current COVID-19 pandemic, employees are increasingly using their personal devices, leading to a huge rise in mobile devices. Also, organizations are seeing a massive rise in the number of IoT devices. Furthermore, the number of applications that organizations are using is also increasing. Therefore, the users should select a solution that can support the ever-increasing number of endpoints and applications. The platform should offer scalability to cope with the high demand and workload while ensuring the best experience for employees and less burden on IT/admin resources. Users should choose a platform that can help them reduce risk and secure all endpoints. Most of the MTM vendors claim to support large-scale enterprise-class deployment capability. However, the depth of technical functionalities and capabilities for smooth upscaling and downscaling with multiple endpoints may differ from vendor to vendor.

Vendors' Strategy and Roadmap: The vendors' capability to formulate a comprehensive and compelling technology roadmap is a crucial factor for users prior to the adoption of the MTM solution. The vendor should have a firm understanding of the market dynamics to analyze the potential investments of their assets. In order to gain a competitive edge or become a pioneer in the security industry, the vendor should have strong strategic objectives and the ability to identify the trends that can be implemented across their business. Vendors should implement gap analysis to determine priorities and deliver value to their stakeholders. Vendors' roadmap strategy execution should include specific timelines and estimated capital for each project. There should be a specialized team of delegations responsible for the success of the roadmap and growth

strategy. Some of the vendors are enhancing comprehensive threat defense as well as enterprise data policy enforcement and continue to strengthen their core MTD technology and detections, build tighter integrations/ synergies and embed OEM cases in adjacent markets. Furthermore, the vendors are focusing on additional zero-trust integrations and focusing on improving user experience and phishing detection capabilities. Additionally, the vendors' vision to incorporate predictive and advanced analytics in the platform will provoke smart decision-making and anticipate the probability of cyber threats.

Access Management: Users should look for MTM vendors providing management controls, including zero-trust security, that allow admins to customize security policies, device posture, and identity checks. Zero-trust security helps organizations secure their organizational assets against data breaches and modern cyber-attacks by verifying insiders or outsiders through a network perimeter. It helps secure user access to applications and information, irrespective of the location, time, and nature of the device used, by authenticating and authorizing users in real time. The MTM solution should also determine compliance of devices as well as detect abnormal behaviors and other attributes to examine the security risk involved in granting access at the moment of logging in. Users should look for MTM Vendors whose product boosts contextual risk assessment with real-time threat data from an ecosystem of endpoint security solutions. The MTM product should be able to check devices and context in a multitude of ways and act before giving permission to access resources. The MTM solution should be designed with a privacy-first orientation, including having granular privacy controls and not requiring data to be sent to a security cloud for detection. An MTM product should enforce multi-factor authentication and should be able to automatically remediate out-of-compliance endpoints and can also deny access or remotely wipe the data from compromised endpoints.

Support for Non-traditional Devices: Many organizations are moving towards digital transformation by allowing their employees to work remotely and use non-traditional devices such as smartphones, laptops, tablets, etc. The MTM solutions help organizations protect, monitor, and manage all traditional and non-traditional devices centrally. MTM vendors are increasingly adding support for a wide variety of non-traditional devices for digital transformation and enhancing productivity.

SPARK Matrix™: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix™ provides a snapshot of the market positioning of the key market participants. SPARK Matrix provides a visual representation of market participants and provides strategic insights on how each supplier ranks related to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact. Quadrant's Competitive Landscape Analysis is a useful planning guide for strategic decision makings, such as finding M&A prospects, partnership, geographical expansion, portfolio expansion, and similar others.

Each market participants are analyzed against several parameters of Technology Excellence and Customer Impact. In each of the parameters (see charts), an index is assigned to each supplier from 1 (lowest) to 10 (highest). These ratings are designated to each market participant based on the research findings. Based on the individual participant ratings, X and Y coordinate values are calculated. These coordinates are finally used to make SPARK Matrix™.

Technology Excellence	Weightage
Sophistication of Technology	20%
Competitive Differentiation Strategy	20%
Application Diversity	15%
Scalability	15%
Integration & Interoperability	15%
Vision & Roadmap	15%

Customer Impact	Weightage
Product Strategy & Performance	20%
Market Presence	20%
Proven Record	15%
Ease of Deployment & Use	15%
Customer Service Excellence	15%
Unique Value Proposition	15%

Evaluation Criteria: Technology Excellence

- **The sophistication of Technology:** The ability to provide comprehensive functional capabilities and product features, technology innovations, product/platform architecture, and such others.

- **Competitive Differentiation Strategy:** The ability to differentiate from competitors through functional capabilities and/or innovations and/or GTM strategy, customer value proposition, and such others.

- **Application Diversity:** The ability to demonstrate product deployment for a range of industry verticals and/or multiple use cases.

- **Scalability:** The ability to demonstrate that the solution supports enterprise-grade scalability along with customer case examples.

- **Integration & Interoperability:** The ability to offer product and technology platform that supports integration with multiple best-of-breed technologies, provides prebuilt out-of-the-box integrations, and open API support and services.

- **Vision & Roadmap:** Evaluation of the vendor's product strategy and roadmap with the analysis of key planned enhancements to offer superior products/technology and improve the customer ownership experience.

Evaluation Criteria: Customer Impact

- **Product Strategy & Performance:** Evaluation of multiple aspects of product strategy and performance in terms of product availability, price to performance ratio, excellence in GTM strategy, and other product-specific parameters.

- **Market Presence:** The ability to demonstrate revenue, client base, and market growth along with a presence in various geographical regions and industry verticals.

- **Proven Record:** Evaluation of the existing client base from SMB, mid-market and large enterprise segment, growth rate, and analysis of the customer case studies.

- **Ease of Deployment & Use:** The ability to provide superior deployment experience to clients supporting flexible deployment or demonstrate superior purchase, implementation and usage experience. Additionally, vendors' products are analyzed to offer user-friendly UI and ownership experience.

- **Customer Service Excellence:** The ability to demonstrate vendors capability to provide a range of professional services from consulting,

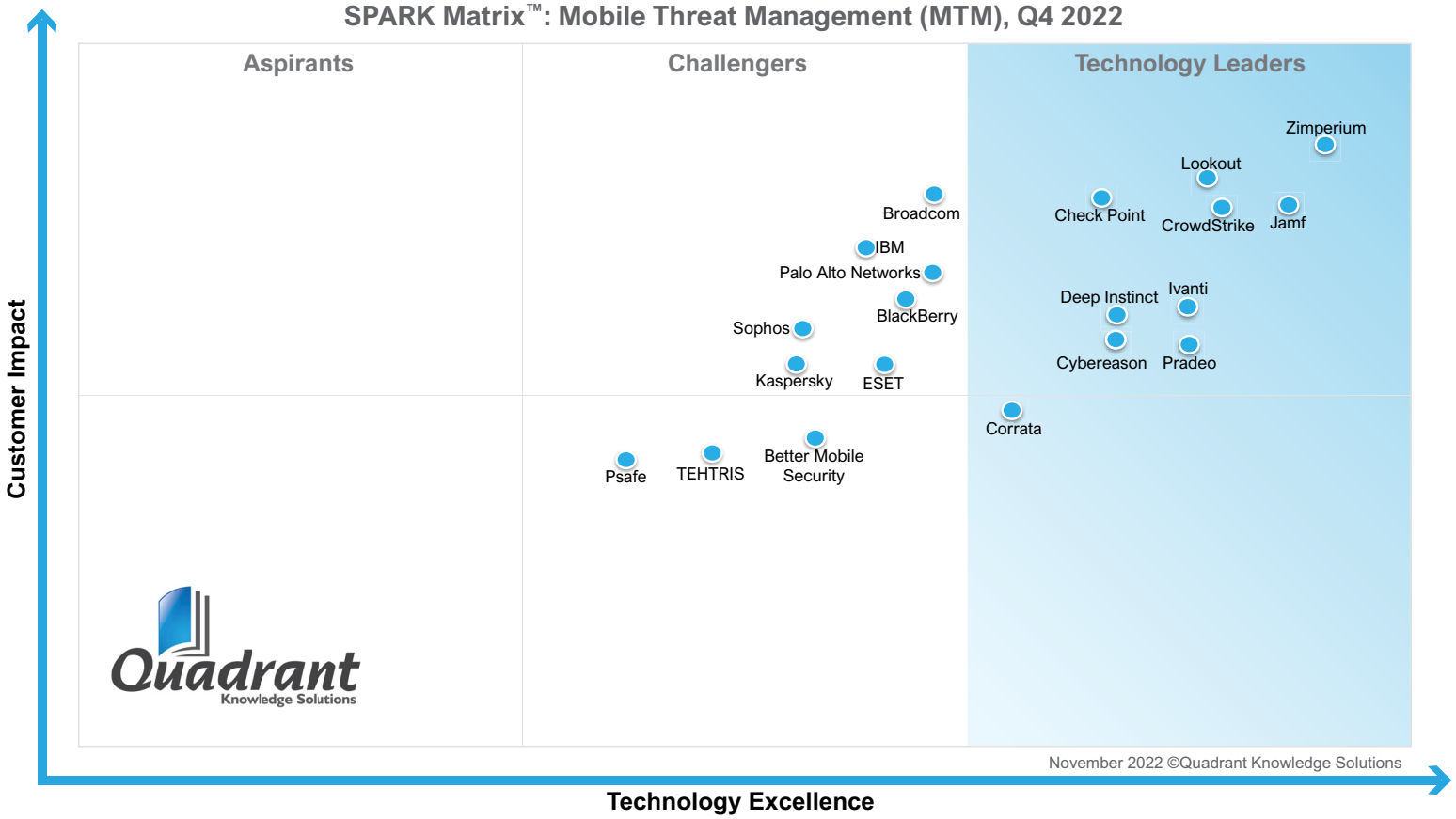
training, and support. Additionally, the company's service partner strategy or system integration capability across geographical regions is also considered.

- **Unique Value Proposition:** The ability to demonstrate unique differentiators driven by ongoing industry trends, industry convergence, technology innovation, and such others.

SPARK Matrix™: Mobile Threat Management (MTM), Q4 2022

Strategic Performance Assessment and Ranking

Figure: 2022 SPARK Matrix™
(Strategic Performance Assessment and Ranking)
Mobile Threat Management Market



Vendor Profile

Following are the profiles of the leading MTM vendors with a global impact. The following vendor profiles are written based on the information provided by the vendor's executives as part of the research process. Quadrant research team has also referred to the company's website, whitepapers, blogs, and other sources for writing the profile. A detailed vendor profile and analysis of all the vendors, along with various competitive scenarios, are available as a custom research deliverable to our clients. Users are advised to directly speak to respective vendors for a more comprehensive understanding of their technology capabilities. Users are advised to consult Quadrant Knowledge Solutions before making any purchase decisions, regarding MTM and vendor selection based on research findings included in this research service.

Zimperium

URL : www.zimperium.com

Established in 2010 and headquartered in Dallas, TX, Zimperium is a leading provider of Mobile Threat Management (MTM) solutions. The company provides real-time, on-device, and machine learning-based protection to mobile devices and applications from threats targeting Android, iOS, and Chromebook devices. The company offers a range of products, including zIPS, z3A, zDefend, and Mobile Application Protection Suite (MAPS), that cover the entire mobile threat management landscape.

Zimperium offers on-device machine learning-based security engine z9, which is specifically focused on mobile devices to help organizations identify, detect and protect against known, zero-day, or new threats targeting iOS, Android, and Chromebook devices in real-time even when not connected to the network. The solution also provides detailed information or analysis about attacks and threats. Zimperium powered by z9, defends against phishing, network, device, and malicious app assaults. On-device performance of Zimperium z9 is effective while posing no latency or privacy risks to users.

Zimperium zIPS provides continuous protection for mobile devices; both managed and BYOD, and the information accessed by them; by leveraging powerful mobile threat research. In addition, it offers on-device mobile security and cloud-hosted administrative dashboards that can be integrated with multiple UEMs and EPPs.

Zimperium cloud-based z3A offers continuous monitoring and analysis of mobile apps, with detailed intelligence, including content, intent, contextual analysis, as well as privacy and security ratings. z3A uses unique and highly analytical engines, including static and dynamic analysis, for assessing the privacy and security risk of iOS and Android applications. Zimperium z3A enables administrators to create highly customized and granular app policies and can be deployed across all users or individuals or new groups, or existing EMM/UEM members.

Zimperium MAPS enables organizations to identify compliance risks during the app development phase and monitor and protect apps from attacks while in use. Zimperium MAPS offers sub-features to protect mobile app life cycle such as zScan, zKeyBox, zShield, and zDefend. Zimperium zScan enables developers to search and fix compliances, privacy, and security issues in the development

phase. Zimperium zKeyBox secures cryptographic keys and prevents them from being detected, extracted, or manipulated. Zimperium zShield protects apps from reverse engineering, code tampering, privacy, extracting assets, extracting API keys, and malware injection with the help of obfuscation and anti-tampering functionality. Zimperium provides SDK zDefend to detect and protect against device, network, phishing, and malware attacks.

MDE's managed threat-hunting service offers proactive threat hunting, prioritization, and additional context and insights to further allow the security operation centers (SOCs) to swiftly and accurately identify and address threats.

Analyst Perspective

Following is the analysis of Zimperium's capabilities in the global Mobile Threat Management market:

- Zimperium, an MTM provider, offers modules such as machine learning-based technology (z9), mobile device security (zIPS), mobile application analysis (z3A), and Mobile Application Protection Suite (MAPS). Zimperium provides protection from identified and unidentified devices, networks, phishing, or any malicious app attacks on-device, complete mobile security solutions for Android, iOS, and Chromebook.

- Zimperium provides solutions that can work with multiple UEMs in a single tenant, including BlackBerry, Citrix, IBM, JAMF, Microsoft, Ivanti, SOTI, and VMware Workspace ONE. Zimperium manages and protects the complete development life cycle, and its solution can be managed on any cloud as well as on-prem.

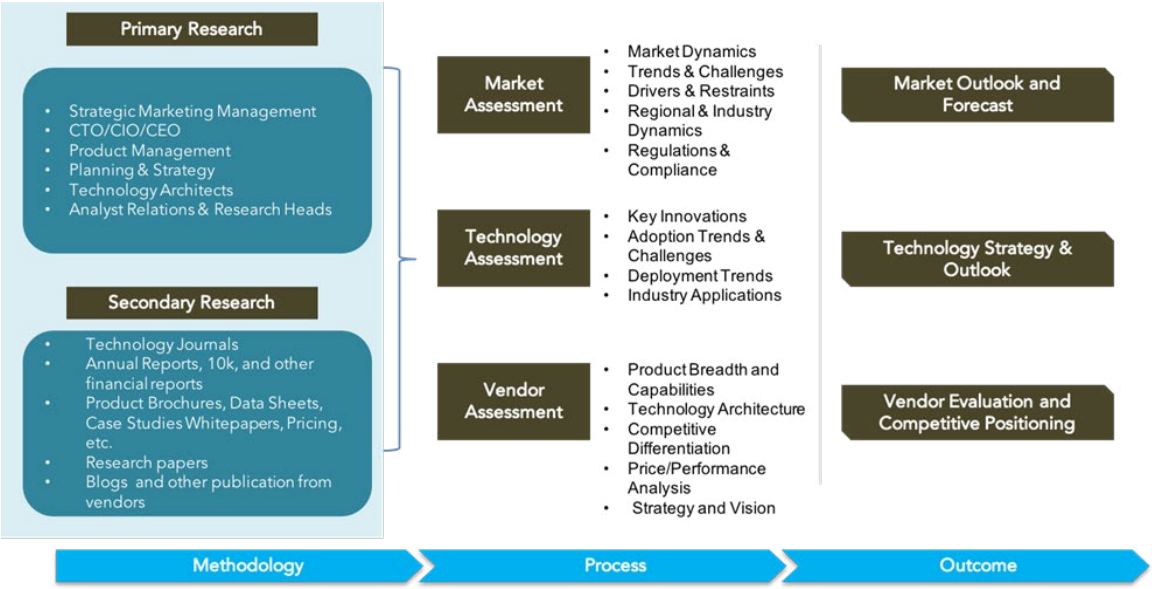
- Concerning geographical presence, Zimperium has a strong presence in the US and Europe, followed by other EMEA and APAC regions. From an industry vertical perspective, while the company has a presence across a wide variety of industries, its primary verticals include banking and financial services, government, and public sector, IT and telecom, manufacturing, healthcare and life sciences, retail, eCommerce, and insurance. From a use case perspective, Zimperium supports zero trust, mobile EDR, mobile phishing protection, mobile DevSecOps, and compliance.

- Zimperium's primary challenges include the growing competition from emerging vendors with innovative technology offerings. These vendors are successful in gaining a strong market position with increased penetration amongst small to mid-market organizations and are amongst the primary targets for mergers and acquisitions. However, with its comprehensive functional capabilities, compelling technology differentiation, and robust customer value proposition, Zimperium, is well-positioned to maintain and grow its market share with continued success amongst mid-market to large enterprise segments.

- As part of its technology roadmap, Zimperium continues to strengthen its core MTD technology and detections, build tighter integrations/ synergies and embed OEM cases in adjacent markets. Furthermore, the company is focusing on additional zero-trust integrations and focusing on improving user experience and phishing detection capabilities. Additionally, the company is investing in improving its MTM capabilities, securing its position as the mobile app protection platform, increasing the number of customers, geographical presence, different industry verticals, and expanding use case support.

Research Methodologies

Quadrant Knowledge Solutions uses a comprehensive approach to conduct global market outlook research for various technologies. Quadrant's research approach provides our analysts with the most effective framework to identify market and technology trends and helps in formulating meaningful growth strategies for our clients. All the sections of our research report are prepared with a considerable amount of time and thought process before moving on to the next step. Following is a brief description of the major sections of our research methodologies.



Secondary Research

Following are the major sources of information for conducting secondary research:

Quadrant's Internal Database

Quadrant Knowledge Solutions maintains a proprietary database in several technology marketplaces. This database provides our analyst with an adequate foundation to kick-start the research project. This database includes information from the following sources:

- Annual reports and other financial reports
- Industry participant lists
- Published secondary data on companies and their products

- Database of market sizes and forecast data for different market segments
- Major market and technology trends

Literature Research

Quadrant Knowledge Solutions leverages on several magazine subscriptions and other publications that cover a wide range of subjects related to technology research. We also use the extensive library of directories and Journals on various technology domains. Our analysts use blog posts, whitepapers, case studies, and other literature published by major technology vendors, online experts, and industry news publications.

Inputs from Industry Participants

Quadrant analysts collect relevant documents such as whitepaper, brochures, case studies, price lists, datasheet, and other reports from all major industry participants.

Primary Research

Quadrant analysts use a two-step process for conducting primary research that helps us in capturing meaningful and most accurate market information. Below is the two-step process of our primary research:

Market Estimation: Based on the top-down and bottom-up approach, our analyst analyses all industry participants to estimate their business in the technology market for various market segments. We also seek information and verification of client business performance as part of our primary research interviews or through a detailed market questionnaire. The Quadrant research team conducts a detailed analysis of the comments and inputs provided by the industry participants.

Client Interview: Quadrant analyst team conducts a detailed telephonic interview of all major industry participants to get their perspectives of the current and future market dynamics. Our analyst also gets their first-hand experience with the vendor's product demo to understand their technology capabilities, user experience, product features, and other aspects. Based on the requirements, Quadrant analysts interview with more than one person from each of the market participants to verify the accuracy of the information provided. We typically engage

with client personnel in one of the following functions:

- Strategic Marketing Management
- Product Management
- Product Planning
- Planning & Strategy

Feedback from Channel Partners and End Users

Quadrant research team researches with various sales channel partners, including distributors, system integrators, and consultants to understand the detailed perspective of the market. Our analysts also get feedback from end-users from multiple industries and geographical regions to understand key issues, technology trends, and supplier capabilities in the technology market.

Data Analysis: Market Forecast & Competition Analysis

Quadrant's analysts' team gathers all the necessary information from secondary research and primary research to a computer database. These databases are then analyzed, verified, and cross-tabulated in numerous ways to get the right picture of the overall market and its segments. After analyzing all the market data, industry trends, market trends, technology trends, and key issues, we prepare preliminary market forecasts. This preliminary market forecast is tested against several market scenarios, economic most accurate forecast scenario for the overall market and its segments.

In addition to market forecasts, our team conducts a detailed review of industry participants to prepare competitive landscape and market positioning analysis for the overall market as well as for various market segments.

SPARK Matrix:
Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix provides a snapshot of the market positioning of the key market participants. SPARK Matrix representation provides a visual representation of market participants and provides strategic insights on how each supplier ranks in comparison to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact.

Final Report Preparation

After finalization of market analysis and forecasts, our analyst prepares necessary graphs, charts, and table to get further insights and preparation of the final research report. Our final research report includes information including market forecast; competitive analysis; major market & technology trends; market drivers; vendor profiles, and such others.

Client Support

For information on hard-copy or electronic reprints, please contact Client Support at
rmehar@quadrant-solutions.com | www.quadrant-solutions.com