Quadrant Knowledge Solutions

Security and Risk Management

SPARK Matrix™: Mobile Threat Management (MTM), Q4,2023

Market Insights, Competitive Evaluation, and Vendor Rankings

October, 2023

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 Mobile Threat Management (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 policies such as BYOD have led to improved employee mobility, the introduction of diverse endpoints with varying security postures has increased the work of Security teams, as the mobile endpoints are vulnerable to attacks and data breaches as they are open to unknown applications and networks. In the case of BYOD, the devices are even more vulnerable when employees use the same device for both private and organizational purposes. Hence, to secure corporate data, organizations are increasingly opting for securing mobile endpoints through Mobile Threat Management (MTM) solutions.

The Mobile Threat Management (MTM) solutions are designed to monitor all the devices and activities, such as the installation of new applications as well as networks accessed by the devices and manage and restrict the devices from accessing non-secure applications and networks. An MTM solution protects mobile devices from device, application, and network-based threats. The solution evaluates OS versions, system settings, firmware, and device configurations on mobile devices for risk hunting. MTM solutions continuously scan for unusual, unsanctioned, and suspicious user activities of users and perform behavioral analysis of devices. Furthermore, MTM solutions scan for unusual behavior in network traffic and unauthorized access to the network. The solution can also detect counterfeit and invalid certificates as well as security actions required to prevent Man-in-the-Middle attacks. An MTM solution identifies malware and grayware in the applications through reverse engineering and analyzing source code.

Quadrant Knowledge Solutions defines Mobile Threat Management (MTM) software as “a solution that detects and analyzes mobile threats and remediates with appropriate measures to protect the mobile devices of an organization against known and unknown threats that arise at the device, application, and network level.” An MTM solution uses Threat Intelligence and Behavioral Analytics capabilities to identify the threat when a device is compromised.

Following are the key capabilities of an MTM solution:

- **Comprehensive mobile endpoint protection:** A Mobile Threat Management Solution monitors, manages, and provides security for all the mobile endpoints of the organization irrespective of its

configuration (includes iOS, Android). The solution provides protection from application-based threats (malware, rootkits, spyware), network-based threats (man-in-the-middle, spoofing), and device-based threats (jailbroken/rooted devices, risky device configurations). The solution utilizes machine learning and behavior-based detection to identify emerging threats with high precision and decline access. The solution also scans applications, monitors mobile device risks, protects devices operating under the BYOD policy to increase employee productivity, and secures organizational and employee data with its built-in privacy controls. The solution protects enterprise infrastructure and corporate data by providing access only to trusted devices and offers real-time visibility into incidents, enabling self-remediation.

- **Anti-phishing & content security:** A mobile threat management solution leverages an AI-based detection engine and metadata analysis to help detect and block access to unsafe websites, malicious links, and other risky, harmful, or inappropriate content across corporate and personal devices. 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 detection:** A mobile threat management solution allows users to monitor OS versions, security update versions, system parameters, device configurations, firmware, and system libraries to detect security misconfigurations, device vulnerabilities, as well as suspicious and malicious activities. Additionally, the solution helps organizations counter endpoint threats arising from malicious or risky applications, identifies malware, and triggers compliance actions. In addition, an MTM solution automatically blocks compromised iOS and Android devices with features like out-of-the-box jailbreak and rooting detection and provides real-time threat insights and analytics to enrolled devices and their operating systems.

- **Application-based detection:** 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 detection:** 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 and customizes device policy and compliance rules to restrict access to vulnerable networks automatically.

- **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. The solution leverages tools to automatically monitor, identify, remediate, mitigate, and classify vulnerabilities before their likely misuse. 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 primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall Mobile Threat Management (MTM) market. This study includes an analysis of key vendors, including Better Mobile Security, BlackBerry, Broadcom, Check Point, Corrata, Cybereason, ESET, IBM, Ivanti, Jamf, Kaspersky, Lookout, McAfee, Palo Alto Networks, Pradeo, Samoby, Sentinel One, Sophos, TEHTRIS, and Zimperium.

Check Point, Corrata, Cybereason, Ivanti, Jamf, Kaspersky, Lookout, and, Pradeo and Zimperium 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 companies' MTM offerings also help organizations effectively implement BYOD, remote working, and other initiatives.

Check Point's Harmony Endpoint provides MTM capabilities 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 enhances the MTM solution by receiving 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.

Corrata is identified as the emerging leader in the SPARK Matrix™ for 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, as per the company, 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.

Cybereason offers Cybereason Mobile, which leverages correlated attack intelligence to protect mobile devices proactively from ransomware and other malware, exploits, fileless and in-memory assaults, and malware. The 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.

Ivanti Neurons for 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, the product pushes local compliance actions that detect and eliminate both known and zero-day mobile attacks on-device, regardless of whether the device is connected to the internet 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.

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.

Kaspersky offers a Secure Mobility Management solution that leverages threat management and protection as well as security policies to enhance the security of third-party enterprise mobile management (EMM) solutions. The solution provides comprehensive capabilities like anti-malware, web control, anti-phishing, application control, rooting and jailbreak detection, third-party EMM integration, anti-theft, mobile device management (MDM), and a self-service portal to prevent, detect, and mitigate attacks in real-time. The key features of the solution include device lifecycle management of Android, iOS, iPadOS, and Windows devices, a corporate app catalog, agent-based threat protection, certificates and VPN management, and response to compliance violations.

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 suite also includes Lookout Security Graph, which 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 surveillance ware campaigns.

Pradeo offers an artificial intelligence, machine learning based MTM solution titled Mobile Threat Defense that stops data loss and enhances compliance while adhering to 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, the solution includes app analysis technology for detecting zero-day threats and data processing, as well as the most advanced and extensive security information available.

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

Broadcom, IBM, Palo Alto Networks, BlackBerry, ESET, Sophos, McAfee, Sentinel One, Better Mobile Security, TEHTRIS, and Samoby 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 2023 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 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, good customer experience, 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.

Threat intelligence & research: Organizations should look for vendors offering a Mobile Threat Management solution that is equipped with a threat intelligence capability that enables collection, analysis, and alerting regarding potential and existing mobile security threats. The solution should monitor various sources and provide real-time and timely updates about vulnerabilities, malware, phishing attacks, and other risks that could impact mobile devices. Vendors should offer an in-depth analysis of threats, including their potential impact, attack methods, recommended mitigation strategies, and actionable steps to enhance security posture. They should also provide periodic reports and updates to help their clients stay informed about the evolving threat landscape.

End user privacy: Organizations should look for vendors who offer Mobile Threat Management solutions with capabilities to prevent privacy violations in the process of securing corporate data. Vendors should provide tools that allow users to control app permissions, giving them the ability to choose what data an app can access. Vendors should utilize containerization techniques that isolate corporate apps and data from personal apps and data. This ensures that corporate information is stored securely within a separate container, reducing the risk of data leakage.

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.

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.

Vendor's Strategy & 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. 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

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 making, such as finding M&A prospects, partnership, geographical expansion, portfolio expansion, and similar others.

Each market participant is 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	Customer Impact	Weightage
Customer data and lifecycle management	15%	Product Strategy & Performance	20%
Customer Targeting and Segmentation	12%	Market Presence	20%
Real-time Personalization and Optimization	13%	Proven Record	15%
Data and Channel Integration	20%	Ease of deployment & Use	15%
Centralized Campaign Management and Execution	10%	Customer Service Excellence	15%
Analytics	10%	Unique Value Proposition	15%
Event Triggering	5%		
Competition Differentiation	5%		
Vision & Roadmap	10%		

Evaluation Criteria: Technology Excellence

- **Threat Detection and Response:** The ability to identify and assess the threat and to create responses that are accurate and appropriate to the identified threat and the capability of the response to make a resilient device.

- **Threat Intelligence and coverage:** The ability to gather information related to different cyber threats and correlate to them by understanding patterns and relationships to understand the exact threat to the device.

- **Device based protection:** The ability to monitor device configurations, security updates and detect device vulnerabilities.

- **Application based protection:** The ability to monitor and review all the applications running on the device, data associated, devices that have access to the app, possibilities for data leak and to remove the apps that are identified as threats.

- **Network based protection:** The ability to secure the device from suspicious networks or links and to protect the device from network-based cyber-attacks.

- **AI/ML Integration:** The extent to which the solution is automated in terms of threat detection, troubleshooting, and resolving.

- **Integration and interoperability:** The integration of MTM with endpoint management platforms such as MDM, EMM, or UEM to manage and monitor the devices from a single console.

- **Vision and Roadmap:** Key planned enhancements to offer superior product/technology.

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.

- **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.

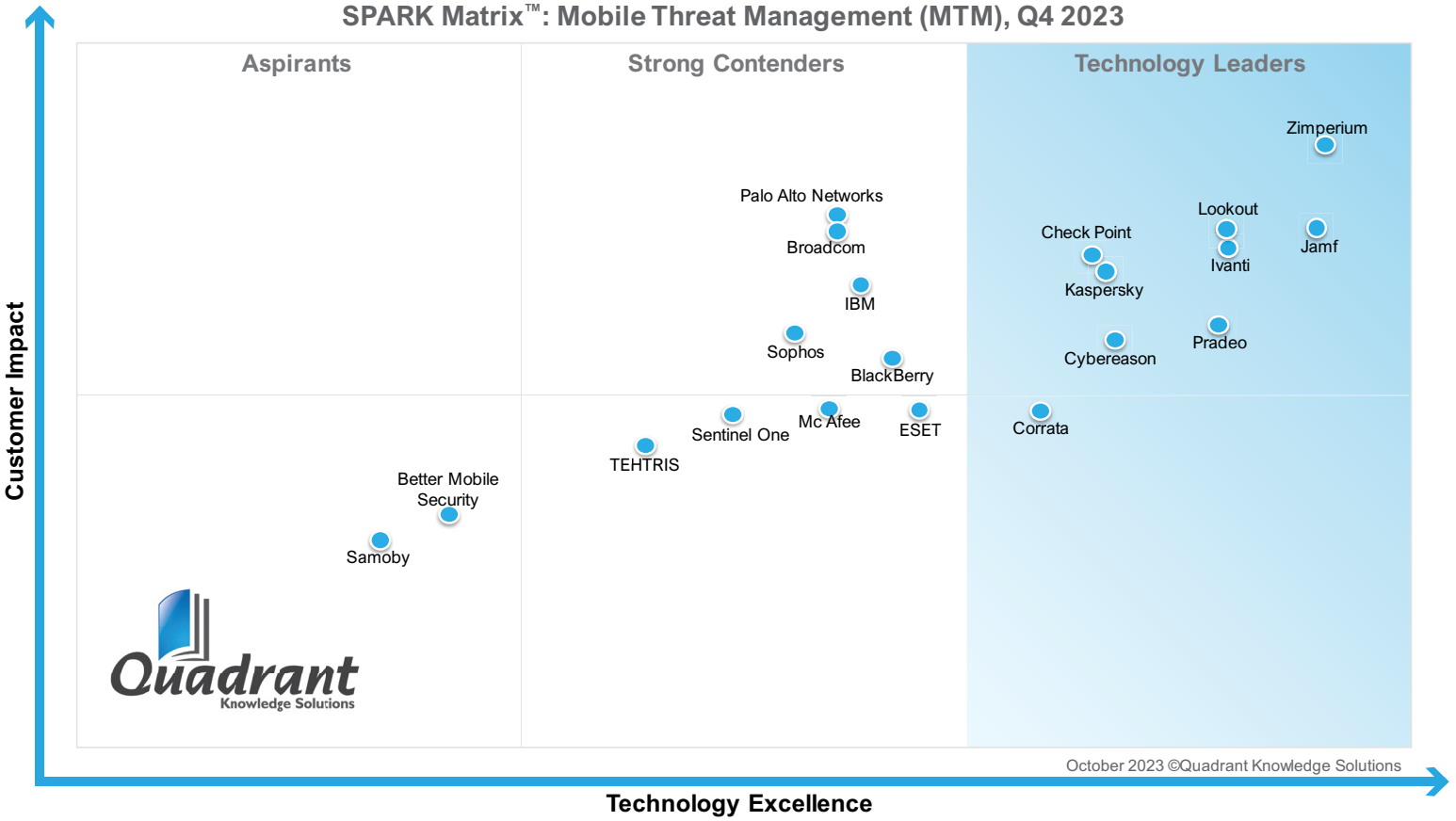
- **Unique Value Proposition:** The ability to demonstrate unique differentiators driven by ongoing industry trends, industry convergence, technology innovation, and such others.

- **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.

SPARK Matrix™: Mobile Threat Management (MTM), Q4 2023

Strategic Performance Assessment and Ranking

Figure: 2023 SPARK Matrix™
Strategic Performance Assessment and Ranking)
Mobile Threat Management (MTM) Market



Vendor Profiles

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: https://www.zimperium.com/

Company Introduction

Founded in 2010 and headquartered in Dallas, TX, Zimperium is a mobile and application security provider. The company provides Machine Learning based protection for Android as well as iOS devices, and Chromebooks against known and unknown threats.

Product Introduction

Zimperium offers Mobile Threat Management (MTM) through its solution Zimperium MTD. Zimperium MTD, formerly known as zIPS, provides comprehensive mobile security for enterprises, and is designed to protect corporate-owned and BYO devices from advanced threats without compromising employee privacy. It enables SMS filtering, Safari Content Filtering, Network Filtering and Browser Extension Filtering. The features of Zimperium MTD include z9, z3A, MAPS, zScan, zShield, zKeyBox, and zDefend.

Technology perspective

Following is the analysis of Zimperium's capabilities in the Mobile Threat Management (MTM) market:

- Zimperium MTD supports on-premises or cloud deployment (AWS, Azure, Oracle and Google) and provides visibility into the risks and vulnerabilities regarding mobile devices and detects device, application, phishing and network-based threats and allows. Zimperium has an unmatched forensic data and it's threat intelligence capability analyzes the threats and triggers the appropriate remediation techniques. Zimperium MTD supports zero-touch deployment. This ability ensures that the solution can be deployed and activated on the mobile endpoints and on-device detection is enabled, ensuring that all the devices are protected even when they are not connected over the network. It also offers integrations with multiple MDMs

at an instance, granular group policies and RBAC, thus providing enterprise grade management capabilities. The solution supports an enhanced mobile ecosystem with enterprise integrations, including SIEM, IAM, XDR, DevOps workflows, ticketing systems, GitHub action, and fraud systems.

- Zimperium's z9 engine uses Machine Learning to detect device, application, and network-based attacks and phishing attacks against mobile devices. z9 detects known and unknown threats by analyzing the behavioral deviations in mobile devices, such as OS statistics and system parameters, malicious applications, anomalous network traffic, and advanced phishing attacks. z9 provides mobile forensics, reducing the threat assessment time and the remediation time.

- Zimperium's Advanced App Analysis (z3A) is a cloud-based mobile risk assessment platform that is designed to analyze and assess the privacy and security of the applications installed on mobile devices. The z3A engine correlates data concerned with the application from the statistics, detects security and privacy risks, runs various tests and validations, and identifies the potential risks before the threat arises. z3A also provides executive, technical, and dev-based reports for every version of different applications.

- Zimperium's Mobile Application Protection Suite (MAPS) is a comprehensive mobile DevSecOps solution that protects mobile applications throughout their lifecycle from development to deployment. MAPS also includes zScan, zShield, zKeyBox, as well as zDefend and utilizes the zConsole for managing all the connected mobile devices and for reporting.

- zScan enables automated discovery of privacy, security, and compliance issues during the deployment process, even before the app is released. zScan can fit directly into the application and the devices without implementing new codes or logging onto other consoles. zScan performs static and dynamic analysis, lists the findings, documents the risks, such as insecure API calls and sensitive data handling, triggers app scanning, and enables compliance and security teams to define and customize policies.

- zKeyBox protects cryptographic keys using white-box cryptography, an approach to hide keys used in general-purpose software implementation, and makes sure that the keys cannot be discovered, extracted, or manipulated. The algorithm executes directly on the encoded keys, ensuring they are

never exposed in the memory. This ensures the keys are kept safe even on compromised, jailbroken, and rooted devices.

- zDefend is an SDK that enables Zimperium MTD to determine if the mobile device is compromised, is facing any network attacks, or has onboarded malicious apps and can take actions on the device even without network connectivity. Zdefend's Runtime Application Self-Protection (RASP) capabilities allow continuous monitoring, protection, and threat modeling within the mobile DevSecOps life cycle.

- One of the key differentiators of Zimperium MTD is that the solution can be used as a stand-alone solution or can be integrated with Mobile Device Management or Enterprise Mobility Management solutions. Once the solution is integrated with other MDM/EMM solutions, Zimperium MTD sends alerts or prompts to the MDM/EMM console whenever a threat is detected, and the MDM/EMM solution triggers the remediation accordingly

Market perspective

- From a geographical presence perspective, Zimperium has a strong presence in North America, Europe, the Middle East, and Africa, followed by Asia Pacific, and is planning to expand its presence. From an industrial vertical perspective, Zimperium focuses on BFSI, Government & Public sector, Manufacturing, Telecommunication, Entertainment & Media, Healthcare, Retail, Transportation, and Food & Beverages.

- From a use case perspective, Zimperium supports Zero Trust, Mobile DevSecOps, Mobile phishing protection, Mobile EDR, and compliance.

Roadmap

As a part of the technology roadmap, Zimperium is planning to expand its on-device detection and the Mobile-First Security Platform with new integrations, new OEMs, new detections, new synergistic workflows, etc. Zimperium is investing in expanding its geographical presence, industrial verticals, and use case support.

Check Point

URL: https://www.checkpoint.com/

Company Introduction

Founded in 1993 and headquartered in Tel Aviv-Yafo, Israel, Check Point is a provider of cloud-based cybersecurity solutions that protect organizational IT systems from cyberattacks in real time and improve the organization's security posture.

Product Introduction

Check Point offers Mobile Threat Management through the Harmony Mobile Solution, which offers comprehensive security to endpoints from sophisticated cyberthreats and stops malware downloaded from the internet or email attachments before it reaches the endpoint. The solution protects endpoints and mitigates the risk of security breaches and information compromise.

Technology perspective

Following is the analysis of Check Point's capabilities in the Mobile Threat Management (MTM) market:

- Harmony Mobile offers comprehensive mobile security by protecting mobile devices from application-based, network-based, and device-based threats. The solution can be integrated and deployed with the existing mobile environment without interrupting the user experience or privacy. The solution offers various capabilities, such as prevention of malicious apps, file downloads, phishing apps, Man-in-The-Middle attacks, and the detection of jailbreaks.

- Harmony Mobile can integrate with MDM/UEM and supports device ownership programs like BYOD. The solution facilitates zero-touch on-device deployment and protects both corporate and private data by offering comprehensive threat prevention. The product's cloud-based intuitive console facilitates device management, offers administrators an application vetting service, and grants access to an analysis report via its dashboard.

- Harmony Mobile provides application and file protection and supports offline application scanning to detect and block malicious apps and files. Harmony Mobile uses a cloud-based Behavioral Risk Engine that leverages Machine Learning, AI, Sandboxing, Static Code flow analysis, anomaly detection, and app reputation techniques to determine malicious and corrupt apps. Harmony mobile integrates with Check Point ThreatCloud to assess the application to detect cyber threats before they are stored in device storage.

- Harmony Mobile provides on-device network protection that covers a range of network security capabilities and blocks infected devices from accessing corporate applications and data. It blocks known and unknown zero-day phishing sites as well as sites using SSL. The capability uses dynamic security intelligence technology to facilitate safe browsing and URL filtering by blocking malicious sites. It also provides Wi-Fi security and prevents MiTM attacks and DNS spoofing.

- One of the differentiating features of Check Point Harmony Mobile is its ability to automatically create forensic reports for thorough insights into compromised assets, attack flow, and correlation with the MITRE ATT&CK Framework. The Forensics functionality automatically tracks and logs endpoint activities, such as changed system registry entries, launched processes, affected files, and network activity, and produces a thorough forensic report. System administrators and incident response teams can efficiently prioritize and stop attacks with the help of robust attack diagnostics and visibility. The threat hunting capability helps users to set queries or use predefined queries to identify and drill down suspicious incidents and take manual remediation actions.

Market perspective

- From a geographical presence perspective, Corrata has a strong presence in Europe, the Middle East, and Africa, followed by North America. From an industrial vertical perspective, Corrata's primary verticals include manufacturing, healthcare, Government and Public sector, financial services, transportation & media, food & beverages, retail, e-commerce, and telecommunication.

- From a use case perspective, Corrata's primary use cases include anti-phishing, malware detection, conditional access, web filtering, Wi-Fi protection, and vulnerability management.

Corrata

URL: https://corrata.com/

Company Introduction

Founded in 2014 and headquartered in Dublin, Ireland, Corrata is a provider of mobile endpoint security for iOS and Android devices and Chromebooks. Corrata's Mobile endpoint security solutions allow organizations to protect their endpoints from cyber threats such as malware, phishing, and communications interception.

Product Introduction

Corrata offers Mobile Threat Management through its Mobile Security solution. The portfolio offers capabilities such as device vulnerability detection, anti-phishing protection, advanced threat detection and response, vulnerability detection, network communication protection, content filtering, device quarantine, robust web filtering, and cloud app control that protect employee devices such as smartphones and tablets without compromising on their privacy. It can be deployed on a standalone basis or integrated with the IT stack, including MDM, EPP, SSO, IAM, SIEM, and CASB.

Technology perspective

Following is the analysis of Corrata's capabilities in the Mobile Threat Management (MTM) market:

- Corrata offers on-device mobile security to protect devices from attacks. The capability also provides real-time visibility and control over device traffic and blocks unsanctioned cloud apps. Corrata offers an enterprise-grade firewall, which, as per the company, provides unparalleled visibility and control over network traffic. The firewall also helps identify advanced malware via AI-assisted network traffic analysis and device status. Corrata's ability to operate on-device and never routing traffic helps prevent latency, performance, and privacy issues. Additionally, it provides a comprehensive feature set for both iOS and Android devices. Corrata's advanced threat detection and response

identifies, prevents, and blocks advanced malware, phishing sites, and other zero-day attacks that happen through any channel, including SMS, emails, and social media.

- Corrata provides anti-phishing protection by detecting threats through its threat intelligence capability and blocking unsafe websites and other risky, harmful, or inappropriate content. Corrata's Network traffic inspection examines DNS requests, IP addresses, port numbers, and Server Name Indicators to identify the source channel of phishing. Corrata's AI-assisted Smart Policy Protection component identifies and quarantines previously unseen sites as well as compromised devices, prevents them from communicating with other devices, and uses metadata analysis to categorize such devices as risky.

- Corrata provides Anti-Malware protection by detecting and blocking access to risky and illegal sites. All the installed apps are scanned on a regular basis to identify malware, harmful applications, and anomalous behavior. Access to rarely used ports is also monitored for evidence of risky content. Corrata augments virus detection techniques by using patented network traffic inspection technology to detect, command, and control traffic and block traffic to known command and control sites as well as the IP addresses of servers linked with threat groups. Various response actions, such as device wipe, device quarantine, user notification, and malware removal, are enabled if malware is detected on any endpoints.

- Corrata offers advanced network protection for mobile communication by monitoring the quality and integrity of Transport Layer Security (TLS), rather than ensuring the security of network infrastructures such as cell towers and Wi-Fi hotspots. The applications and websites' encryption quality are continuously monitored, and the traffic to poorly encrypted websites is blocked. This measure helps prevent attacks like eavesdropping and sensitive communication interception. Additionally, Cert Pinning is used to avoid MiTM attacks against sensitive traffic.

- Corrata's device vulnerability management facilitates automated monitoring and remediation of device vulnerabilities. Continuous monitoring of the key security indicators on the device enables an assessment of the device's vulnerability, and a security score is created based on a combination of operating system status, device configuration, and malware status. Devices with low scores are isolated and are denied access to business applications

and corporate data until the devices are updated, and the misconfigurations are corrected. The Corrata App alerts the user if misconfigurations are detected and provides an interface to remediate the issues.

- End user privacy is a differentiating feature of Corrata's Mobile Security solution. Corrata minimizes the use of sensitive information. It does not keep track of any application's internet usage, browser history, or location history. It does not require permission to access files, directories, or messages being received and becomes reliable for users to install on personal phones as well.

- Another differentiator of Corrata's mobile security solution is its provision of multiple-layer protection to the devices with the use of vulnerability management techniques, quarantining, AitM protection, Encrypted DNS filtering, IP and Port blocking, and an Anti-virus layer. The solution is deployed on-device and does not access private information on the device. Corrata performs deep packet inspection at three layers by inspecting Server Name Indicators, inspects and blocks IP addresses and port numbers, and mandates the use of TLS and certs to avoid MiTM attacks.

Market perspective

- From a geographical presence perspective, Corrata has a strong presence in Europe, the Middle East, and Africa, followed by North America.

- From an industrial vertical perspective, Corrata's primary verticals include manufacturing, healthcare, Government and Public sector, financial services, transportation & media, food & beverages, retail, e-commerce, and telecommunication.

- From a use case perspective, Corrata's primary use cases include anti-phishing, malware detection, conditional access, web filtering, Wi-Fi protection, and vulnerability management.

Roadmap

Corrata has structured a proper roadmap or milestones for the next three years. The company plans to align with the evolving security architectures such as Zero Trust and SSE. Corrata also plans to implement the detection of IOCs in encrypted traffic and integration with XDR. Corrata also plans to expand its business in the Asia-Pacific region.

Cybereason

URL: https://www.cybereason.com/

Company Introduction

Founded in 2012 and headquartered in Boston, MA, Cybereason is the provider of security products and solutions to protect various types of endpoints, including computers, mobile devices, servers, and cloud-based assets, from various types of cyber threats. It has implemented predictive prevention, detection and response, gains attack intelligence through which attack related decisions are made.

Product Introduction

Cybereason Mobile Threat Defense platform provides application, network, operating system, and device-level visibility to detect, prevent, and remediate attacks. The platform offers autonomous threat prevention against operating system vulnerabilities, malware, harmful apps, and unusual network connections. Additionally, Cybereason Mobile Defense maps cross-platform correlations to the MITRE ATT&CK for Mobile Framework to detect malicious activities on endpoints and to streamline incident response.

Technology perspective

Following is the analysis of Cybereason's capabilities in the Mobile Threat Management (MTM) market:

- The Cybereason Mobile Threat Defense platform leverages correlated attack intelligence to protect mobile devices from threats like ransomware, exploits, fileless and in-memory assaults, and malware. The solution provides interoperability with UEM technology partners and offers a user-friendly interface, which enables automated, or one-click threat remediation before they turn into breaches. The platform offers visibility across all attack vectors and auto-remediates with on-device protection. It can detect, investigate, hunt, and remediate threats across traditional and modern mobile endpoints.

- Cybereason Mobile Defense offers behavior-based protection to identify suspicious activities, including the use of malicious mobile apps, unusual

network connections, and operating system flaws. The platform protects mobile devices immediately without any rules, signatures, or human analysis on any device, anywhere, and at any time.

- Cybereason Mobile Threat Defense solution leverages privacy-by-design and protects remote employees' privacy on corporate-owned and BYO devices. The solution also facilitates deep forensics and enhanced search capabilities to enable threat hunting. Cybereason Mobile Threat Defense solution enables maintenance of a mobile ecosystem with enterprise integrations across SIEMS, IAM, XDR, DevOps workflows, ticketing systems, GitHub actions, and fraud systems.

- Cybereason Mobile Threat Defense uses an open XDR approach to analyze the cloud, data across endpoints, workspace, as well as networks and identify the unknown and missed threats. The solution leverages malicious operation - MalOp to identify cross-device attacks and uses cross-platform compromise context throughout all phases of the attack lifecycle. Security analysts can connect and communicate with malicious activities across a variety of endpoints with the help of MalOp's complete alignment with the MITRE ATT&CK for Mobile framework. Furthermore, it reduces false positives and streamlines incident response to defend against user or enterprise-focused threats.

- Cybereason Mobile Threat Defense understands the whole range of mobile risks and threats, which enables security teams to prevent and address cutting-edge threats overlooked by traditional endpoint control mechanisms. Additionally, the solution provides extensive context across the operating system, memory, as well as CPU and identifies unusual behaviors to discover all impacted endpoints, users, and attacker communications more accurately.

- Cybereason Mobile secures mobile devices in a non-intrusive, effective manner that doesn't interfere with user experience, performance, or privacy. Additionally, the Cybereason Nocturnus Team regularly assesses new Indicators of Compromise (IOCs) and key Indicators of Behavior (IOBs) derived from throughout the whole network, as well as other evolving mobile attack techniques.

Market perspective

- From a geographical presence perspective, Cybereason has a strong presence in North America, EMEA, and APAC. From an industrial vertical perspective, Cybereason's primary verticals include Financial Services, Healthcare, and Advanced Manufacturing.

- From a use case perspective, Cybereason's primary use cases include comprehensive ransomware and malware detection and prevention, EDR, XDR, threat hunting and mitigation for traditional and mobile endpoints.

Roadmap

As a part of the technology roadmap, Cybereason will continue to invest across MTM, EDR, and XDR by offering advanced threat detection and improving automated response capabilities. Cybereason also plans for new partnerships and integrations. Cybereason strategizes to grow stronger across North America, the Middle East, and APAC regions.

Ivanti

URL: https://www.ivanti.com/

Company Introduction

Founded in 1985 and headquartered in South Jordan, UT, Ivanti is a provider of IT security, IT service management, IT asset management, unified endpoint management, identity management, and supply chain management solutions. Ivanti's automation platform combines the capabilities of UEM, zero trust security, and enterprise service management to provide a secure and self-service solution.

Product Introduction

Ivanti provides mobile threat management through its Ivanti Neurons for Mobile Threat Defense solution, which protects corporate and mobile-owned devices from various types of threats. The solution enables organizations to monitor, manage, and secure devices against device, network, and application-level attacks, as well as avoid mobile phishing attacks.

Technology perspective

Following is the analysis of the Ivanti's capabilities in the global Mobile Threat Management Management (MTM) market:

- Ivanti Neurons for Mobile Threat Defense is a cloud-based solution for protecting mobile devices against mobile threats and preventing application, network, and device-based threats. The solution uses Machine-Learning algorithms and provides complete visibility into the devices to monitor, manage, and secure the devices against cyberattacks.

- Ivanti Neurons for Mobile Threat Defense's capabilities allow on-device detection and remediation, which uses ML-based protection against phishing attacks even when the devices are offline. It enables organizations to balance security and privacy as well as drive and maintain user adoption. Additionally, Ivanti's MTD uses a proactive remediation approach with the help of policy-based compliance actions that prevent attacks from occurring, isolate infected

devices from the network, get rid of harmful programs along with related content, and stop zero-day attacks.

- Ivanti Neurons for MTD integrates with organizational UEMs for device management, and the administration is performed completely through the cloud administration console. No local server or connectors are needed to deploy and manage. No user action is required to deploy and activate Ivanti Neurons for MTD. Compliance policies can be enforced to prevent the users from disabling or removing MTD from the device.

- Ivanti Neurons for MTD's threat intelligence capability identifies phishing threats and blocks phishing and other malicious links. It detects and remediates phishing threats across emails, texts, SMS, instant messaging, and social media. When malicious URLs are identified, they are blocked, and users are immediately notified of the same.

- Ivanti Neurons for MTD provides continuous visibility into the devices and evaluates them to prepare in-depth reports. It maintains granular control over the devices by closely monitoring the applications by filtering them based on the location, SMS reading, as well as screen recording, and looking for any violation of compliance policies. This capability determines the number of devices with risky apps, proactively leverages app usage policies to allow safe apps, and blocks risky apps based on risk scoring, app behavior, and network credibility. Dashboards and reports are maintained to gain visibility over the history of the devices, applications, network, and threats to assess and remediate when threats arise. Remediation techniques include blocking access to corporate resources, quarantining devices to protect corporate data, and wiping the contaminated device.

- The key differentiators of Ivanti Neurons for Mobile Threat Defense include the use of 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 score, explanation of risks and implications. Additionally, Ivanti MTD pushes a local compliance action that detects and eliminates both known and zero-day mobile attacks on-device, even if the device is not connected to a Wi-Fi or cellular network. Another differentiating feature is that 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.

Market perspective

- From a geographical presence perspective, Ivanti has a strong presence in North America, particularly the US, followed by Europe and Asia Pacific. From an industrial vertical perspective, Ivanti's primary verticals include healthcare, education, logistics, public sector, and retail.

- From a use case perspective, Ivanti supports discovery and visibility, compliance management, patch management, application control, privilege management, secure remote access, and full system reset.

Jamf

URL: https://www.jamf.com/

Company Introduction

Founded in 2002 and headquartered in Minneapolis, MN, Jamf develops IT and security software for organizations to manage and secure modern Apple devices. Jamf offers solutions for macOS, iOS, iPadOS, tvOS, Android, and Windows. All iOS and iPadOS solutions developed by Jamf utilize native Apple frameworks, are immediately usable after contracting, and have real-time policy controls. Jamf offers zero-touch deployment solutions that may be installed and enabled without requiring end-user interaction. Jamf's endpoint protection is tamper-resistant with restrictions that limit functionality in the event of termination or tampering with the endpoint agent.

Product Introduction

Jamf offers Mobile Threat Management (MTM) through its product Jamf Protect. Jamf Protect provides enhanced endpoint security by increasing visibility, prevention, controls, and remediation capabilities. It supports same-day upgradation of Apple software and hardware updates and provides real-time threat detection, prevention, monitoring, alerts, and remediation.

Technology perspective

Following is the analysis of Jamf's capabilities in the Mobile Threat Management (MTM) market:

- Jamf Protect detects malicious links and applications in real-time by securing the endpoints and the company data. Jamf Protect uses behavioral analytics to identify suspicious and malicious activities and supports customized analytics for the unique needs of organizations. It also uses the MITRE ATT&CK framework through which core analytics are mapped.

- Jamf Protect monitors all the removable devices or peripherals connected to an endpoint and helps prevent attacks and data loss. It leverages a Machine

Learning and Threat Intelligence engine titled MI: RIAM to identify and prevent zero-day phishing attacks. Jamf Protect's in-network protection feature prevents network-based attacks, blocks threats like ransomware as well as crypto jacking and blocks access to malicious links and sites.

- Jamf Protect provides security for devices and ensures the privacy of user data by employing encryption to safeguard user and personal information, mitigating risks of data loss and phishing threats. It extends its protection to both company-owned and Bring Your Own (BYO) devices, securing both corporate and personal data.

- The policy actions and threat mitigation measures can be carried out promptly, and the service can constantly run without affecting the device's battery life or performance. For instance, when a newly installed app is to be scanned, the service can use signals from deep integration with device management to decide the next appropriate action. The in-line network elements can then compel the app to wake up and begin the required on-device operations.

- Jamf Protect provides in-network sensors that enable real-time phishing detection and protection by intercepting and scanning Internet requests for malicious domains and URLs before connecting. It also offers control points that may be set up as an on-device content filter, a sanitized DNS service, or a full in-line proxy. Flexibility allows customers to find the right balance between monitoring and privacy protections while also ensuring that the device is protected, even when fully disconnected from the network.

- Jamf Protect monitors endpoint activities like device health and compliance regularly and alerts the user in case of any delayed updates, compliance deviations, or device risks.

- One of the primary differentiators of Jamf Protect is direct policy enforcement without the need for a UEM. Jamf maintains deep technical integrations with its own device management solutions. 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.

Market perspective

- From a geographical presence perspective, Jamf has a strong presence in North America, Europe, Asia Pacific, Canada, the Middle East & Africa, and is expanding its presence in Latin America.

- From an industrial vertical perspective, Jamf has a presence across multiple verticals, including banking & financial services, healthcare & life sciences, retail & eCommerce, education, manufacturing, transportation, and professional services.

- From the use case perspective, Jamf's primary use cases include supporting secure device configurations, extended MDM, preventing phishing attacks and malicious applications, managing risky applications, app vetting workflows, protecting devices from infrastructure attacks, preventing misuse of misplaced devices as well as sensitive data leakage, and consistent access control.

Kaspersky

URL: https://www.kaspersky.co.in/

Company Introduction

Founded in 1997 and headquartered in Altstadt, Zurich, Kaspersky Lab is a global provider of cutting-edge cybersecurity solutions, products, technologies, cloud services, and global threat intelligence that secures business, critical infrastructure, government, and consumers from sophisticated and emerging digital threats.

Product Introduction

Kaspersky offers Mobile Threat Management through its Secure Mobility Management solution. The solution offers threat management and protection, security policies, and enhances the security of third-party enterprise mobile management (EMM) solutions. The solution provides comprehensive capabilities like anti-malware, web control, anti-phishing, application control, rooting and jailbreak detection, third-party EMM integration, anti-theft, mobile device management (MDM), and a self-service portal to prevent, detect, and mitigate attacks in real-time. The key features of the solution include device lifecycle management of Android, iOS, iPadOS and Windows devices, a corporate app catalog, agent-based threat protection, certificates and VPN management, and response to compliance violations.

Technology perspective

Following is the analysis of Kaspersky's capabilities in the Mobile Threat Management (MTM) market:

- Kaspersky Secure Mobility Management is an integrated, AI-based, multi-layered solution for protecting and managing all corporate and personal mobile endpoints used for corporate purposes. The solution includes anti-malware, anti-spam, web, application, and device controls, as well as anti-theft features to control all activities from a single management panel and improve administration tasks. Additionally, it provides centralized management, enterprise security mobility, a single management console, and support to

third-party enterprise mobility management solutions to secure devices from threats in real-time.

- Kaspersky Secure Mobility Management provides security throughout the lifecycle of COBO (Corporate-Owned, Business Only), COPE (Corporate Owned, Personally Enabled), and BYO (Bring Your Own) devices. When a new device is enrolled to the organization's network, the capability ensures that certificates are uploaded, device agent that protects and manages the devices is deployed, corporate security policies are deployed, and business-related applications are installed and configured. Once the device deployment and configuration are done, the device activities are monitored for security events, and incident event response is triggered for events that could impact regulatory compliance.

- Kaspersky Secure Mobility Management blocks access to malicious websites and protects data from phishing attacks using anti-phishing technologies. It can integrate with EMM platforms offered by other vendors to manage and monitor the mobile endpoints. It protects both employee and corporate data on the mobile device.

- Kaspersky Secure Mobility Management includes cloud-assisted threat detection and analysis-based powerful anti-malware to protect organizations from known, unknown, and advanced threats in real-time and provide enhanced protection by integrating on-demand and scheduled scans with automatic updates. Kaspersky Mobile Security's Web Control and Anti-Phishing capability allows users to securely access mobile browsers on Android devices. The capability allows administrators to easily block access to sites breaching corporate usage policies and automatically protect data from phishing attacks in real-time.

- Kaspersky Security for Mobile Application Control provides information about installed software, allows administrators to enforce installation of specific applications, and create and control blocklists as well as whitelists by integrating with Kaspersky Security Network. Additionally, it provides compliance control to enable administrators to block non-compliant device access and automatically implement anti-theft features.

- Kaspersky's key differentiator is its internal threat research capacity, demonstrated by its discovery of the initial mobile malware Cabir and its recent identification of a complex mobile-focused APT (Advance Persistent Threat) operation named Operation Triangulation.

Market perspective

- From a geographical presence perspective, Kaspersky has a strong presence in EMEA, JAPAC, and the Americas. From an industrial vertical perspective, Kaspersky focuses on professional services, agriculture, energy & utilities, Govt & public sector, manufacturing, retail, BFSI, telecommunication, transportation, travel, hospitality, and recreation.

- From a use case perspective, Kaspersky's primary use cases include malware protection, phishing protection, device lifecycle management, and data security enforcement.

Roadmap

As a part of its technology roadmap, Kaspersky plans to expand its MTM capabilities as a full-fledged element of the XDR, with advanced telemetry and response options. Kaspersky also plans to enhance its cross-product functions to provide better multi-level infrastructure-wide security with automated prevention and advanced detection and response capabilities.

Pradeo

URL: https://www.pradeo.com/

Company Introduction

Founded in 2010 and headquartered in Paris, France, Pradeo is a provider of mobile security solutions provider. The Pradeo solution secures organizations' mobile environments with mobile endpoint threat detection and response to end-to-end application security. The company has recently acquired a web application security editor to extend its portfolio to adjacent markets..

Product Introduction

Pradeo Security Mobile Threat Defense allows organizations to secure corporate-owned and personal mobiles against data breaches through mobile devices. The solution automatically detects and mitigates known and sophisticated threats in real-time and enables organizations to prevent data exfiltration, theft, and fraud. It allows organizations to control devices' system integrity by detecting OS vulnerabilities, root/jailbreak exploitation, system takeover, abnormal battery consumption, and such others to mitigate privilege escalation and takeover.

Technology perspective

Following is the analysis of Pradeo's capabilities in the Mobile Threat Management (MTM) market:

- Pradeo leverages Artificial Intelligence to prevent 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 to detect zero-day threats and data processing.

- Pradeo MTD offers comprehensive insights into the operations of mobile devices by conducting thorough analyses that help in the proactive prevention of zero-day threats and maintaining seamless security. The solution ensures

compliance with data privacy regulations across all devices, securing both corporate and personal data while also allowing organizations the flexibility to customize security policies according to their most valued information assets.

- Pradeo MTD provides security to mobile devices at application, network, and device levels. Pradeo's mobile application scanning capability monitors all the applications on the devices for any vulnerabilities and anomalous behavior to detect and prevent zero-day attacks. It also minimizes false positives, enabling accurate threat detection and proactive blocking of malicious applications to prevent application-related cyberattacks.

- Pradeo MTD screens the network configuration and parameters and suggests the network's reliability to prevent network-related attacks such as Man-in-the-middle attacks, session hijacking, and pharming. Pradeo MTD also monitors device integrity in all aspects to identify jailbroken or rooted devices and device vulnerabilities to prevent attacks.

- The key differentiators of Pradeo MTD include its ability to provide in-depth visibility over mobile applications activities, such as data manipulation and exfiltration performed by applications that are not necessarily malicious but still represent a critical privacy threat. The solution also provides a mobile application vetting tool that combines multidimensional behavioral analysis and vulnerability detection capabilities to enable security teams to test mobile applications' compliance and remediate problematic behavior easily.

Market perspective

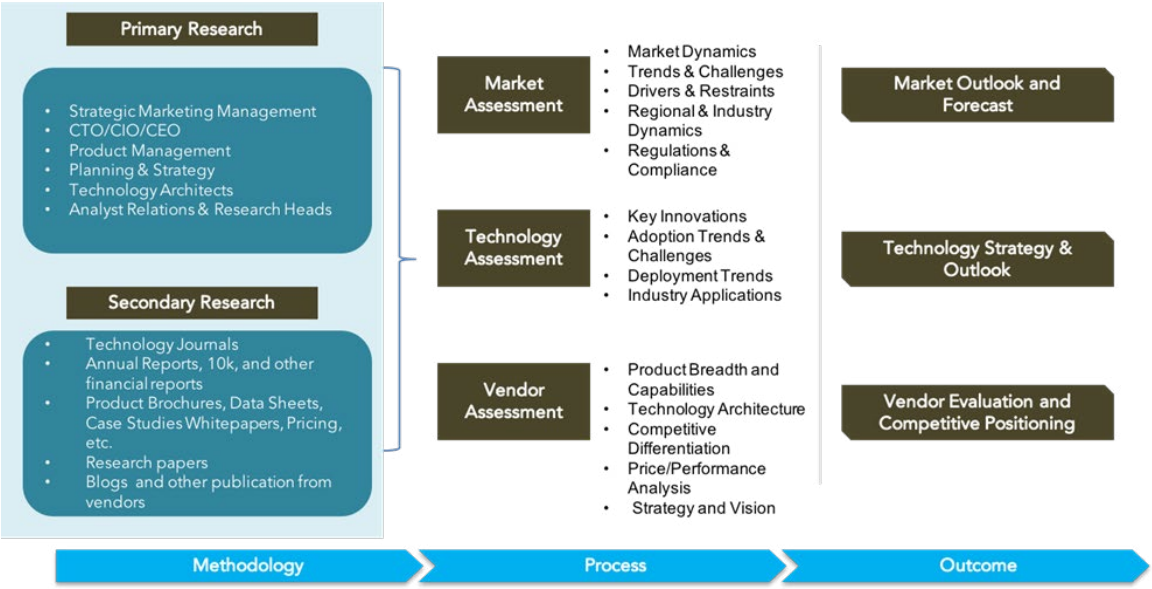
- From a geographical presence perspective, Pradeo has a strong presence in Europe and the US. It is expanding its presence in the Asia Pacific, Canada, the Middle East & Africa, and Latin America.

- From an industrial vertical perspective, Pradeo's primary verticals include banking & financial services, govt & public sectors, healthcare & life sciences, energy & utilities, retail & eCommerce, education, and manufacturing.

- From a use case perspective, Pradeo's primary use cases include anti-phishing, telework protect BYOD and professional devices, protecting unmanaged devices, protection against data leakage from mobile apps, compliance with regulations, and mobile apps security.

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 the 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

ajinkya@quadrant-solutions.com | www.quadrant-solutions.com