Security and Risk Management

SPARK Matrix™: In-App Protection, Q1 2024

Market Insights, Competitive Evaluation, and Vendor Rankings

March, 2024

TABLE OF CONTENTS

Executive Overview

This research service includes a detailed analysis of global In-app protection market dynamics, major trends, vendor landscape, and competitive positioning analysis. The study provides competition analysis and ranking of the leading network operating system 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 their market position.

Market Dynamics and Overview

Quadrant Knowledge Solutions defines In-App Protection as: “a security solution that protects the information assets generated by an enterprise’s business function against vulnerabilities and risks associated throughout an application development lifecycle.” In-app protection vendors consistently seek to understand attackers’ perspectives and devise threat mitigation strategies by constantly innovating their products and services.

With the rise in cloud computing and continued use of mobile devices across different walks of life, mobile application developers are increasingly adopting a user-friendly, web-enabled, and more flexible approach to develop applications that drive the end users to visit hundreds of websites, enter dozens of search terms, upload a batch of photos, or use tap on the phone for payments. Data and information stored in different formats like databases, messages, emails, spreadsheets, and documents can be at risk of misuse, unauthorized access, or destruction. Companies that handle large numbers of applications spread across different data centers and cloud platforms invest in protecting this sensitive information.

Due to the increasing demands for applications across distributed environments with specific expertise and tools for each environment, there is a need for a fast, responsive, frictionless digital experience and employee collaboration platforms. These platforms help organizations focus on enterprise effectiveness, ensure a stable flow of information within/across the enterprise, emphasize organizational learning, and help cultivate leadership to support and drive efficient business functions. As service providers store large amounts of data in electronic form, applications become vulnerable to hackers who steal valuable information using popular techniques such as cloning of the application, code injection, debugging, emulation, external screen sharing, fake execution environment, hooking frameworks for keylogging, malware injection, man-in-the-middle scenarios, native code-hooks, repackaging, rooting/jailbreak, screen-scrapping, system, and user screen shorts.

Due to the versatile nature of mobile applications, developers often take advantage of the device’s size and mobility to develop web-based or native apps for social networking, entertainment, and productivity but often lack an incident response plan to mitigate high risks associated with malware or physical attacks throughout the application development process. Although basic administrative controls such as processes, policies, and plans exist to establish control and restriction over some threat landscapes, a more secure and technical approach may help application developers protect their application components such as JavaScript/ app code, data, intellectual property, or APIs.

The in-app protection market offers products and services to cater to the needs of these problems. They categorize a security threat, determine the cause, preserve any evidence, and get the systems back online so the applications can resume their functions. In-app vendors consider many issues, beginning with a clear understanding of what information assets need protection with strict adherence to regulations and laws of respective geographies. Their solutions are centered on identifying threats in the form of malware and botnets that steal victim's confidential data. Additionally, the vendors also provide vulnerability assessment measures to determine the effectiveness of existing security posture for app development teams and develop innovative ways to present failure analysis data through metric dashboards.

In-app protection or mobile app protection vendors offer solutions with a strong emphasis on technical security controls such as account management, access controls, information flow, and separation of duties, all of which are necessary to protect sensitive data within the applications from the inside out.

The following are the key capabilities provided by an In-app protection solution:

- **Application Hardening:** An In-app protection solution provides prevention capabilities that help the app development team harden the security of the newly developed application before introducing it to the market. This capability prevents attackers from using tampering techniques or reverse engineering and restricts access to the application environment.

- **Application Vulnerability Assessment:** An In-app protection solution provides field-tested best practices for the app development team to assess potential vulnerabilities through rule and policy-based security checks using available tools, patented solutions, and security practices. The assessments are usually conducted based on user engagement or intent to request information and are carried out through defined measures such as scan coverage, time to detection, patching rate, etc.,

- **Application Shielding:** An In-app protection solution helps protect core areas of app development, such as source code, intellectual property (IP), and servers, from potential attacks by immediately shielding the threats using automation, injection, and environmental checks. App shielding is an automated process delivered in separate packages for iOS and Android.

- **Obfuscation:** An In-app protection solution provides code obfuscation capability. This capability obfuscates an application's source code to make it more difficult for attackers to reverse-engineer and extract sensitive information like API keys.

- **Runtime Application Self Protection (RASP):** An In-app protection solution provides Mobile RASP protection in real-time that allows developers to quickly identify and respond to security threats within an application's runtime environment, which also includes detection and blocking of unauthorized access to APIs.

- **Process Integration:** In-app protection solution provides secure, reliable, flexible, and scalable integration options that allow companies to connect their people, data, and applications through a secure advanced transmission process and effectively cover organizations of all sizes.

Competitive Landscape and Analysis

Quadrant Knowledge Solutions conducted an in-depth analysis of major vendors in the In-app protection solution market 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 In-app protection solution market. This study includes an analysis of key vendors such as Appdome, Approov, Build38, Digital.ai, F5, Guardsquare, Jscrambler, OneSpan, Preemptive, Promon, Verimatrix, and Zimperium.

The In-app protection market is segmented based on the application users, engagement levels, frequency of the app usage, session duration, and in-app purchases made by the end users. While most of the vendors from our exclusive sampling have focused on the financial services market, which includes payments, fintech, mobile banking, and digital wallets, few niche vendors cover the market based on user behavior, such as social media and interactive entertainment platforms. We have also included vendors whose products are aimed at customers from the healthcare, manufacturing, high-tech, travel, and hospitality industries.

Zimperium, Verimatrix, Appdome, Promon, Guardsquare, and Build38 have been identified as global technology leaders in the SPARK Matrix^{TM}: In-app protection market, 2023.

Appdome distinguishes itself with a rapid, no-code build system for mobile app defense and threat detection. It integrates with DevOps CI/CD pipelines and offers a Certified Secure™ certificate for build verification. Appdome provides RBAC controls, agentless threat monitoring via ThreatScope™, and attack intelligence reports. It also offers Build2Test automated testing services and an enforcement mechanism to shut down applications, protect user data, and maintain acceptable crash rates in case of incidents such as malware attacks, phishing attacks, and man-in-the-middle attacks.

Approov platform offers comprehensive mobility security by providing trusted device verification for access to APIs and cloud services. It is recognized for its prompt support, user-friendly deployment options, and insightful analytics with over-the-air delivery of updates. In addition, Approov's pricing is transparent and based on the number of active apps. Its unique feature of securely relocating customer secrets upon potential compromise without causing false service disruption alerts strengthens its position in the market.

Build38 distinguishes itself with an active hardening server that provides enhanced security to both on-premises and cloud environments. The platform offers multiple layers of mobile protection, including runtime environment verification, app integrity guarantee, and data protection. With Mobile XDR, Build38 protects applications from fraud and minimizes revenue impact with Mobile XDR (app shielding, monitoring, detection, and response) to provide real-time monitoring and response. The company also offers next-generation RASP with granular detection capabilities and full control over the app lifecycle management.

Digital.ai offers a comprehensive security solution for mobile apps. The solution embeds security in the development process to protect code, keys, and data and prevent reverse engineering and tampering. It also provides visibility into at-risk apps and responds to threats in real-time with Runtime Application Self Protection (RASP), including step-up authentication and altering app features. This ensures robust application security from development to deployment and effective response to threats.

F5 provides a robust solution for app security that reduces risks and prevents threats like app repackaging and malware. It also ensures compliance with privacy, payment, and health standards, including CCPA, GDPR, PCI-DSS, EMVCo SBMP, PSD2, and HIPAA. F5's low-code integration technology enables rapid deployment and scaling.

Guardsquare provides mobile app security features such as code hardening, runtime application self-protection, mobile app security testing, mobile application shielding, and threat monitoring capabilities to resist reverse engineering, tampering, and other threats. Guardsquare DexGuard protects Android apps and SDKs, iXGuard protects iOS apps and SDKs offers, AppSweep finds and fixes security issues within the app's code and dependencies, and Threat cast provides threat monitoring solutions for iOS and Android mobile app security.

Jscrambler JavaScript protection and web monitoring platform offers a comprehensive In-app protection suite that ensures the integrity of source code via application shielding, runtime protection, and code obfuscation. The suite provides complete control over in-app protection and real-time web monitoring capabilities by offering visibility of all website scripts, real-time detection of malicious behavior, and risk assessment using Webpage Script Inventory, Website Threat Monitoring, and Risk Scoring. It also enables control by mitigating risks, blocking malicious behaviors, and protecting data using script behavior management and data fencing. It also offers comprehensive dashboards and custom reporting that offers actionable insights, security posture adjustment, and compliance reports, ensuring revenue safeguarding.

OneSpan's mobile security suite offers an all-in-one developer's toolkit to secure the core components of an application using flexible authentication options and capabilities with a unique single framework that integrates built-in application security. OneSpan offers security features that imbibed strong authentication such as behavioral biometrics, push notification, FIDO, QR code, and Cronto graphical cryptogram.

PreEmptive's DashO offers app shielding and hardening solutions directly infused into .NET, Java, Android, or iOS. Their continuous threat and protection research services keep track of cybersecurity vulnerabilities and mitigation measures up to date to stay ahead of attacks. The platform simplifies app protection, enabling the creation of a protected build for Android, Web, or Java in minutes, irrespective of the build environment. The platform support covers both mature apps facing new risks and unreleased apps.

Promon SHIELD stands out with its developer-friendly integration that ensures timely adoption of security and advanced obfuscation techniques that cover not only CI/CD lifecycles but also post-compilation workflows/procedures with minimal impact on user experience. These capabilities empower developers to focus on core functionalities such as managing software toolchains or writing effective code while Promon safeguards their creations.

Verimatrix XTD platform stands out with its multi-layered protection and AI/ML analysis for Android and iOS, along with support for hybrid development frameworks. It offers flexible deployment options, including a SaaS offering and an on-site toolchain with full automation for CI/CD pipeline integration. Verimatrix's in-house VMX labs provide the latest threat advisories, while its real-time monitoring and control with XTD detection enhance security. Its wide platform support further strengthens its competitive position.

Zimperium offers a mobile-first security platform that provides real-time protection on devices. The platform offers real-time, on-device protection, AI-based threat detection, and a privacy-centric approach. The platform helps organizations adhere to various industry and regional regulations. Zimperium's in-app protection technology is comprehensive, providing real-time threat visibility and protection against advanced cyber threats. Its approach to mitigating internal network breaches is thorough, with protection spanning across devices, networks, applications, and phishing attempts, along with sophisticated mitigation strategies.

Key Competitive Factors and Technology Differentiators

The following are the key competitive factors and differentiators for the evaluation of the network operating system platform and its vendors. While most In-app protection solutions provide all core functionalities, the breadth and depth of functionality may differ depending on different vendor offerings. Some of the key competitive factors and technology differentiators are:

Zero-Code Injection Technology: Users should look for vendors who offer zero-code injection techniques such as signature-based, and anomaly-based detection as well as behavioral analysis to prevent bad actors deploy threats like reverse-engineering.

JSON Web Tokens: Users should look for vendors who provide secure ways to exchange short-lived and one-time authentication information.

Certificate Pinning: Users should look for vendors who provide a certificate pinning feature as a part of an end-to-end security offering that informs the users and developers of a remote host's identity while operating in a hostile environment.

AI/ML Based Monitoring: Users should look for vendors who provide use cases and capabilities to monitor, detect, and prevent code injection attacks using machine learning algorithms that focus on several most common vulnerabilities in JavaScript, and TypeScript.

Bot Defense for Mobile Apps: Users should look for vendors who protect internet applications from malware bots by using native Mobile SDK to collect telemetry from web applications and mobile endpoints.

Integration and Interoperability: Users should look for vendors offering fully automated integration/interoperable capabilities with other cross-functional areas such as CI/CD, API gateway, cloud-native API Gateway, and WAF.

Scalability and Availability: Users should look for vendors who ensure high availability during traffic surges and provide options for businesses to execute large-scale deployments of security features.

Comprehensive Use Case Coverage: Users should look for vendors who have coverage of use cases such as account takeover prevention, credit fraud prevention, and MitM attack prevention and conduct a thorough analysis of costs and benefits offered to them and critically evaluate the feasibility of the solutions offered by the respective vendors.

SPARK Matrix™: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions's SPARK Matrix provides a snapshot of the market positioning of the key market participants. The 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, partnerships, 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 the SPARK Matrix.

Technology Excellence	Weightage
Support for Core-Banking	35%
Ease of Integration	15%
User Experience	15%
Compliance & Reporting	10%
Competition Differentiation Strategy	15%
Vision & Roadmap	10%

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

- **Sophistication of App Security Functionality:** The ability to provide application security features that help protect organizations against cyber-attacks.

- **Ease of Integration:** The ability to couple performance of "best of breed" applications with organizational processes using simple user interfaces that support end-to-end processes.

- **User Experience:** The ability to offer security-related functional requirements along with a user-friendly experience.

- **Compliance & Reporting:** The ability to demonstrate regulatory compliance and reporting standards to ensure applications and systems meet specific requirements. They often cover areas such as access controls, data protection, encryption, incident response, secure coding practices, and vulnerability management.

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

- 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.

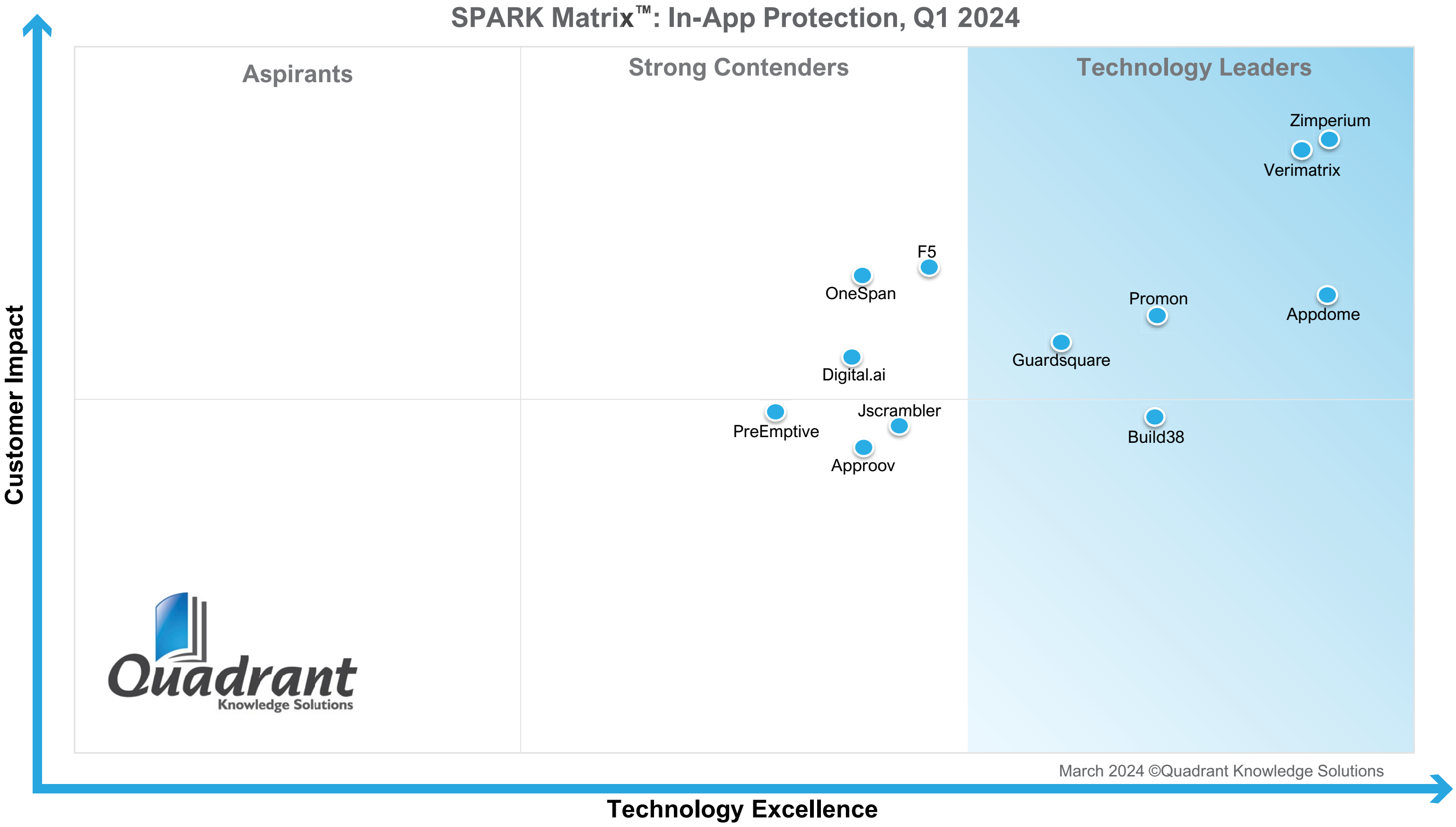
SPARK Matrix™:
In-App Protection

Strategic Performance Assessment and Ranking

Figure: 2024 SPARK Matrix™

(Strategic Performance Assessment and Ranking)

In-App Protection Market



Vendor Profile

Following are the profiles of the leading In-app protection solution vendors with a global impact. The following vendor profiles are written based on the information provided by the vendors' executives as part of the research process. The Quadrant research team has also referred to the company websites, 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 speak directly 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 In-app protection technology 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 provides mobile and application security solutions that provide real-time, on-device, and machine learning-based protection to mobile devices and applications from various types of threats. These threats include device, network, phishing, and malicious app attacks targeting Android, iOS, and Chromebook OSes, mobile endpoints, and apps. Zimperium's Mobile Application Protection Suite (MAPS) provides in-app protection solutions for mobile devices to build compliant, secure, and resilient mobile apps.

Product Introduction:

The company offers a comprehensive suite of in-app protection capabilities through its Mobile Application Protection Suite (MAPS). These capabilities include No-Code App Shielding for safeguarding applications without additional code, Code Obfuscation for securing integral application code, and Data Obfuscation for protecting sensitive data. Runtime Application Self Protection (RASP) ensures security in hostile environments, while Tamper Resistance prevents the bypassing of business logos and repackaging of apps with malware. Threat Reporting & Insights provide valuable information on real threats and attacks. Malware Protection and Phishing Protection shield apps from various cyber threats. Cryptographic Key Protection ensures the safety of cryptographic keys, and Network Protection safeguards apps from unsafe networks.

Technology Perspective:

Following is the analysis of Zimperium's capabilities in the global In-app protection market:

- Zimperium's Mobile Application Suite (MAPS) provides credential protection capabilities such as no-code app shielding and code obfuscation techniques to safeguard sensitive credentials and ensure protection against credential theft and unauthorized access across all industries, particularly in financial services and government sectors.

- Zimperium's Mobile Application Suite (MAPS) provides data confidentiality capabilities through data obfuscation methods to protect sensitive data like payment information, PHI, IP, and PII to ensure data confidentiality and compliance with industry regulations.

- Zimperium's Mobile Application Suite (MAPS)provides runtime security measures to maintain effective security measures in hostile environments through Runtime Application self-protection mechanisms. These capabilities mitigate risks to banking and retail sectors, such as on-device fraud and tampering in financial transactions.

- Zimperium's Mobile Application Suite (MAPS)provides tamper resistance and malware protection capabilities to prevent unauthorized modifications and malware attacks, safeguarding applications from repackaging with malware and ensuring integrity across various sectors like media, retail, and government.

- Zimperium's Mobile Application Suite (MAPS) provides insightful threat reporting capabilities that provide security teams with real-time insights into threats and attacks, enabling proactive responses across diverse sectors like finance, manufacturing, and transportation & and logistics.

- Zimperium's Mobile Application Suite (MAPS) provides anti-phishing capabilities such as Phishing Protection measures to defend against phishing scams, enhancing security in industries like retail and government, where data breaches and network vulnerabilities pose significant risks.

- Zimperium's Mobile Application Suite (MAPS) provides Digital Rights Management (DRM) capability to protect payment information and proprietary content in the retail and media sectors, ensuring secure transactions and intellectual property protection.

- Zimperium's Mobile Application Suite (MAPS) provides cryptographic key protection mechanisms to ensure the security of cryptographic keys, safeguarding sensitive operations and data across all industries, particularly crucial in finance, healthcare, and government applications.

- Zimperium's Mobile Application Suite (MAPS) provides a comprehensive network protection measure to safeguard apps from unsafe networks, preventing eavesdropping on app communication and ensuring secure data transmission across sectors like finance, government, transportation & and logistics.

- Some of the differentiators of Mobile Application Suite (MAPS) include its ability to offer tailored industry solutions to develop in-app protection mechanisms tailored to specified industries like finance, biotech, manufacturing, media, government, retail, and transportation & and logistics to address sector-specific security needs.

- Another differentiator is the ability to apply application shielding to both mobile and desktop applications. It includes traditional, root/jailbreak, debugger, and Instrumentation detections, as well as Malware and Phishing detection.

- Another differentiator is the mobile device attestation feature that allows enterprises to not only verify the user but also trust the device when allowing transactions.

- Another differentiator is the ability to offer application shielding for Android to provide automatic Java to Native translation before applying obfuscation, Runtime, and Tamper resistance protections. This elevates the security posture by removing the difficulty in using traditional Java-based hacking and debugging tools but making reverse engineering more difficult.

- Another differentiator is the cryptographic key protection. zKeybox, is fully configurable for both size and speed considerations and offers a comprehensive range of standard cryptographic ciphers and works across mobile, web, desktop, and embedded platforms.

- Another differentiator is the tamper resistance feature available on all supported platforms, including the Apple-embedded bit code-based applications. This allows customers developing on Apple platforms to leverage Apple's forward-compatible technology with the best-of-breed tamper resistance.

Market Perspective:

- Regarding geographical presence, Zimperium has a presence in North America, EMEA, and JAPAC regions. Regarding industry verticals, the company's primary verticals include payment technology providers, wallets, neo-banks, banking, biotech, manufacturing, media & and entertainment, government, retail, transportation & and logistics.

- The top use cases of Zimperium include Payment Information and Transaction Protection, Credential Theft Prevention, Account Takeover Prevention, Identity Theft Prevention, On-Device Fraud Prevention, IP and Data Protection, and PII Protection

Challenges:

- Primary challenges for Zimperium include increasing technological advancements in In-app protection and the entry of other IT providers in the mobile app security market with a diverse set of products and services. However, Zimperium is well-positioned to expand its share in the global market of In-app protection owing to its comprehensive technology and unique components, where Zimperium has significant capability to deliver end-to-end solutions to monitor and measure enterprises' performance.

Roadmap:

- The company's roadmap outlines several key technological advancements aimed at enhancing its in-app protection solution. These include the integration of Windows ARM architecture support to enable seamless operation on Windows ARM devices and support security across Surface Tablets and Laptops.

- Zimperium also plans to improve compatibility to minimize conflicts within the application environment and to ensure smooth functioning across various components. Additionally, it also ensures a comprehensive security framework to support C++ 20 standards for modern applications. Enhancements may be expected in Secure PIN features, including UI animations and TR-34 key block support, streamlined integration, and enhanced user experience, particularly for Fintech customers.

- To keep up with the evolving threats and continue offering robust security, Zimperium plans to upgrade anti-tampering mechanisms like hooking, anti-jailbreak, and anti-rooting protections to keep pace with evolving threats, ensuring robust security.

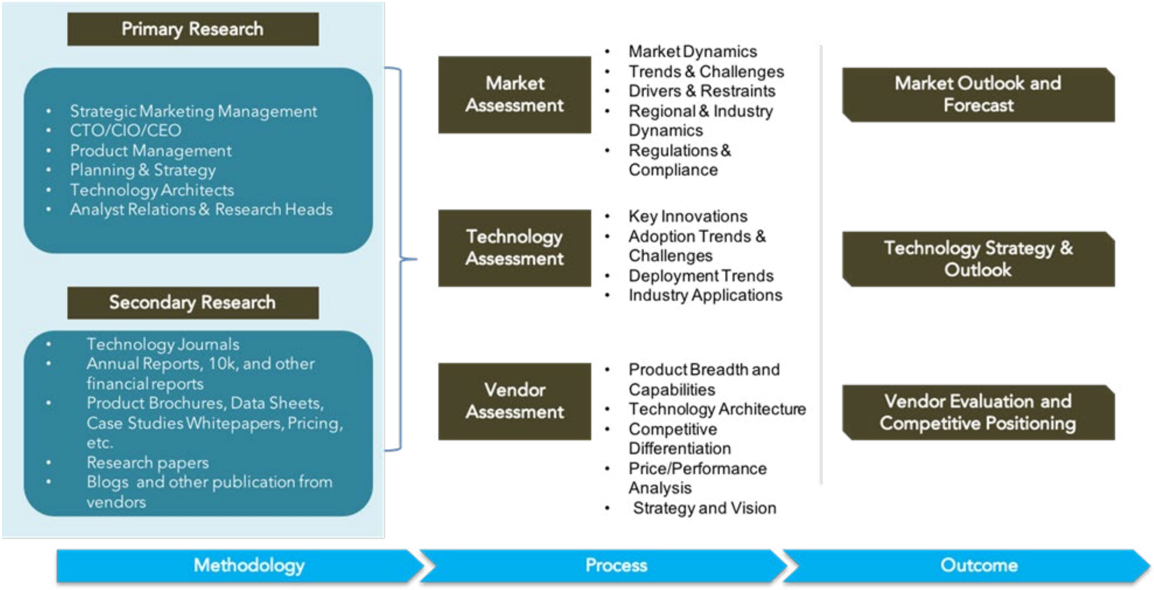
- The company's roadmap also includes integrations with DevOps platforms for seamless security integration, protection of Hybrid Apps, and the launch of MAPS Platform, offering end-to-end application security.

- Zimperium's roadmap also focuses on expanding Zero Touch Protection and simplifying protection processes that align with the commitment to provide features that can be used easily with minimal impact. Tailored Data Security and Advanced Protection capabilities also demonstrate a forward-looking approach to addressing code-lifting attacks.

- Lastly, to meet the security standards quickly and easily, Zimperium continues to work towards enhancing compliance and risk protection features that cater to businesses with market-specific regulatory requirements.

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.


Primary Research
Strategic Marketing Management
CTO/CIO/CEO
Product Management
Planning & Strategy
Technology Architects
Analyst Relations & Research Heads
Secondary Research
Technology Journals
Annual Reports, 10k, and other financial reports
Product Brochures, Data Sheets, Case Studies Whitepapers, Pricing, etc.
Research papers
Blogs and other publication from vendors
Market Assessment
Market Dynamics
Trends & Challenges
Drivers & Restraints
Regional & Industry Dynamics
Regulations & Compliance
Technology Assessment
Key Innovations
Adoption Trends & Challenges
Deployment Trends
Industry Applications
Vendor Assessment
Product Breadth and Capabilities
Technology Architecture
Competitive Differentiation
Price/Performance Analysis
Strategy and Vision
Market Outlook and Forecast
Technology Strategy & Outlook
Vendor Evaluation and Competitive Positioning
Methodology
Process
Outcome

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
- 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 a 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, 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 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