Quadrant Knowledge Solutions

Security and Risk Management

SPARK Matrix™: In-App Protection, 2023

Market Insights, Competitive Evaluation, and Vendor Rankings

May, 2023

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 In-App Protection 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 market position.

Market Dynamics and Overview

Quadrant Knowledge Solutions define an In-App Protection as:

"*An In-App Protection is an advanced set of application security tools designed to protect, detect, analyze, and remediate against known and unknown advanced cyber threats throughout the application lifecycle.*" The tools provide real-time protection for high-value applications running in an unsecured environment against threats such as reverse engineering, repackaging, malware, script injection, cryptojacking, and SMS snatching. Additionally, the tools provide features like RASP (Runtime Application Self-Protection) for real-time monitoring and prevention of application-layer attacks and blocks malicious scripts or tools from accessing the APIs.

The increased usage of mobile devices has created new opportunities for cybercriminals to target mobile apps and environments. Mobile apps often assume that their users are legitimate, providing cybercriminals with multiple avenues of attack. As mobile devices are now being used for critical tasks like banking, there is a growing need to ensure in-app protection technology is in place. In-app protection technology is critical for safeguarding these applications against various cyber threats targeting the mobile application environment, such as SQL injection, cross-site scripting (XSS), broken access control, buffer overflow attacks, cross-site request forgery (CSRF), and malwares like screen scraping.

The In-App Protection solution is also necessary to protect users' applications and sensitive data when accessed from unmanaged devices. Traditional in-app solutions provide detection, but the most critical components are evaluation and reporting. An effective solution should be able to detect, evaluate, and report threats in real-time. It should also include obfuscation and encryption features to protect the app's assets from reverse engineering attempts. In response to increasingly sophisticated cyber threats, In-App Protection solution providers are continuously improving their solutions' existing capabilities and incorporating new security policies into their solutions to offer users a more comprehensive and robust approach to securing their applications. With the continuous evolution and increasing sophistication of threats, vendors are rapidly adopting advanced capabilities such as code obfuscation, whiteboxing techniques, multi-factor authentication, runtime application self-protection (RASP), and risk analytics.

Many In-App Protection providers are focusing on providing new prevention methods for applications through code-level security and implementing automated defenses for suspicious activities, which include app shutdown, code self-repair and thwarting threat actors by obfuscating source code, inserting honeypots, and implementing deceptive code patterns.

Following are the key capabilities of an In-App Protection solution:

- **Application Hardening:** Application hardening protects applications from reverse engineering and tampering, secures apps, repacking, and more by leveraging code obfuscation, whitebox cryptography, and other techniques. Application hardening includes active hardening and passive hardening to detect and respond to the use of debuggers by altering the application's behavior and making the application more resistant to attacks based on static analysis.

- **Anti-Tampering Techniques:** Anti-tampering monitors web and mobile application behavior and covers the overall runtime risk and attack spectrum in real-time. Anti-tampering allows users to secure intellectual property and protect applications from creating a false version, defacing, changing logic, and inserting workflows. Additionally, it alerts applications when risks are detected and secures them against attempts to repackage and alter.

- **Code Obfuscation:** Code obfuscation transforms the source code, including variables and functions, by using encryption or compression to obscure the code, inserting dummy code or control statements, and adding unnecessary complexity to the source code while still maintaining its functionality. It protects apps against malicious attacks such as reverse engineering and software piracy by making it more difficult for attackers to understand the code and find vulnerabilities.

- **Runtime Application Self Protection (RASP):** RASP continuously analyzes web or non-web app behavior and context of behavior to detect and protect from malicious input or behavior without any human involvement. RASP allows integration of security into a running program, regardless of where its location, intercepts all calls from the app to a system, and validates data requests immediately within the app. RASP directly works within the application without impacting application design.

- **Risk Assessment:** In-App Protection tool analyses and identifies potential threat actors and sensitive data in applications, maps the attack surface, scans, and remediates vulnerabilities, determines AppSec process pain points, and strategizes the security roadmap to protect against application attacks in real-time.

- **Authentication Support:** In-App Protection enables automatic authentication of a user when they request to access privileged data and applications. In-App Protection uses multi-factor authentication (MFA) techniques and enhances security by eliminating risky password management practices. MFA uses various credentials such as passwords, messages, digital access cards, and biometric verification to authenticate users. It helps to detect and respond to high-risk logins and easily reset passwords. It provides enhanced security and controls access to resources by automatically blocking risky users in real-time.

Competitive Landscape and Analysis

Quadrant Knowledge Solutions conducted an in-depth analysis of the major vendors of In-App protection 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 market. This study includes an analysis of key vendors, including AppDome, Approov, Build38, Digital.ai, F5, Guardsquare, Imperva, Jscrambler, KOBIL, Lookout, OneSpan, PreEmptive, Promon, Verimatrix, and Zimperium.

The In-App Protection market is fragmented with players of varied sizes. Most of these players focus on mobile security, while a few offers in-app protection as part of their larger cybersecurity portfolio. Regarding geographical distribution, a majority of the players in this study are located in Europe, while the others are based out of North America.

OneSpan, Zimperium, Lookout, Verimatrix, GuardSquare, Build38, and Approov have been identified as global technology leaders in the SPARK Matrix: In-App Protection, 2023. These companies provide a sophisticated and comprehensive technology platform to protect, detect, analyze, and remediate known and unknown advanced cyber threats throughout the application lifecycle. The platforms offered by these companies provide real-time protection to high-value applications against various threats, including repackaging, malware, script injection, crypto-jacking, SMS snatching, and insecure environment-related threats.

F5, Digital.ai, Imperva, AppDome, and KOBIL have been positioned as the primary challengers. These companies provide comprehensive technology as well as capabilities and are gaining significant market traction in the global In-App Protection market. These companies are also mindful of the upcoming market trends and have outlined a comprehensive roadmap to tap into future growth opportunities. The other key vendors captured in the 2023 SPARK Matrix™ include Promon, Jscrambler, and PreEmptive.

Zimperium absorbed the Application Protection business from Trustonic in 2022. The Trustonic TAP solution and service were already being provided through a collaboration with Zimperium. As a result of this move, mobile application developers and existing TAP users can now utilize Zimperium's software-only security solutions for mobile application security testing, application protection, cryptographic key protection, data security, device attestation, and monitoring.

The advent of 5G and PSD2 regulation is accelerating the market adoption of In-App Protection tools. With more sensitive data being processed and increasingly rigorous regulatory and privacy constraints, mobile app developers and organizations seek to protect their apps against security threats. In-App Protection, offered as a Security-Service or Cloud-Based Mobile App Shielding, is becoming more common as organizations seek to reduce the cost and complexity associated with on-prem solutions. Cloud-based shielding provides scalability and flexibility, making it easier to manage and deploy app shielding solutions.

A shift can be observed in the balance of security investment from a "shift left" (vulnerability eradication efforts) model to a "shield right" (runtime and in-app protection) model and a shift from server-side RASP to mobile RASP as well. Additionally, In-App Protection tools are increasingly being integrated with DevSecOps workflows to provide continuous application security throughout the development and deployment process.

Moreover, vendors are entering into technology partnerships to provide end-to-end security solutions. This type of collaboration provides a more comprehensive security solution for organizations that prefer maintaining relationships with fewer vendors.

All the vendors captured in the 2023 SPARK Matrix™ of In-App Protection are enhancing their capabilities to secure, detect, analyze, and remediate against known and unknown advanced cyber threats throughout the application lifecycle. Additionally, the vendors are helping organizations expand their partnership channels and support diverse use cases. Vendors are consistently looking to enhance their In-App Protection solutions and expand support for easy deployment options. Vendors continue to enhance their offerings to provide obfuscation and encryption techniques with runtime application self-protection, risk analysis, anti-tampering techniques, multifactor authentication, biometric authentication, anti-keylogging, anti-screen scraping, Whitebox cryptography, jailbreak/root detection, and more capabilities to enable better application shielding to protect the source code from repackaging, app cloning, and reverse engineering. While traditional in-app protection solutions generally provide detection, vendors are now focusing more on the most important components: evaluation and reporting, to get comprehensive visibility into the threat landscape to protect applications from zero-day attacks. Additionally, the vendors are focusing on increasing their customer base, geographical presence, different industry verticals, and expanding use case support. Vendors are also looking at expanding support for multiple deployment options.

Key Competitive Factors and Technology Differentiators

The following are the key competitive factors and differentiators for the evaluation of In-App Protection solutions and vendors. While most In-App Protection solutions may provide all the core functionalities, the breadth and depth of functionalities 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. Some of the key differentiators include:

- **Sophistication of Technology:** Enterprises are advised to conduct a comprehensive evaluation of different In-App protection vendors before making a purchase decision. Users should employ a weighted analysis based on their specific enterprise's needs in terms of monitoring, filtering, and blocking malicious traffic while protecting against sophisticated cyberattacks. An enterprise's In-App protection requirements may differ based on the industry vertical, application vulnerability management, compliance requirements, co-managed services, customer experience, use cases, and end-user size. Enterprises ought to assess In-App protection solutions that provide end-to-end functionalities, ensuring the safeguarding of mobile applications throughout their entire life cycle. These In-App protection solutions must have the capacity to safeguard all types of applications, including mobile apps, single-page web apps, software, and connected devices, proactively defending against a broad spectrum of mobile threats. The solution should empower applications to develop resilience against various mobile threats like repackaging, malware, script injection, cryptojacking, SMS grabbing, and others. Additionally, the solution should offer protection against advanced threats, such as malware, code injection, screen scrapping, application cloning, and reverse engineering. Businesses can consider In-App protection solutions that provide various authentication options, including behavioral biometrics, OTPs, facial recognition, fingerprint authentication, e-signatures, and others. It should also include advanced mobile app shielding technology and multi-channel authentication via the mobile device. Users should also evaluate In-App protection solutions for capabilities such as anti-bot, clickjacking, runtime application self-protection, and anti-tampering.

- **Maturity of AI and ML:** In-App protection solution vendors' capability to provide embedded AI and machine learning capabilities may differ significantly. Vendors utilize AI and ML to automatically respond to and prevent attacks, effectively mitigating any potential harm. By integrating AI/ML technology, vendors can enhance network analytics, user analytics, and threat intelligence, streamlining the mitigation processes and improving the overall effectiveness of application protection. Users are recommended to consider vendors that offer AI/ML for identifying threat patterns, conducting a comprehensive risk analysis, and responding to threats in real-time, thereby providing optimal security for their applications.

- **Vendors Strategy and Roadmap:** Users must choose the appropriate technology partner as per their specific-use cases, risk exposure, and digital transformation roadmap. The In-App Protection vendors are constantly enhancing and innovating their technology value proposition beyond traditional detection capabilities by implementing ML-based solutions for false positives, dynamic certificate pinning, run-time protection from API vulnerabilities, which further help provide protection from encryption, repacking of applications, reverse engineering, cryptojacking, malware, script injection and offer capabilities such as application hardening, API protection, and more. Vendors are focusing on providing low code/no code integrations, threat insight, end-to-end API security, and post-coding solutions. Enterprises should carefully evaluate the vendor's existing technology capabilities along with their technology vision and roadmap to improve overall satisfaction and customer ownership experience for long-term success.

- **Vendor's Expertise and Domain Knowledge:** Organizations should conduct a comprehensive evaluation of numerous In-App Protection solutions and vendors before making a final decision. Organizations should assess vendors' proficiency and expertise in comprehending their specific security challenges, industry, region-specific requirements, and use cases. Users ought to prioritize vendors offering ease of use, comprehensive offerings, software adaptability to market fluctuations and regulatory requirements, cost-effectiveness, and transparency. Additionally, users are recommended to consider vendors providing advanced capabilities, such as application attestation, client environment attestation, dynamic certificate pinning for traffic pattern analysis, threat detection, and remediation. Furthermore, users should search for vendors providing automated and intelligence-driven in-app protection solutions, real-time monitoring of applications, and other advanced

functionalities to minimize human errors. It is advisable to choose a solution that has a history of successful large-scale deployments and analyze existing case studies to prepare the best practices for in-app protection solution deployments.

- **Integration and Interoperability:** Seamless integration and interoperability with vendors' existing technologies are among the crucial factors impacting technology deployment and ownership experience. An In-App Protection solution must offer fully automated integration with the user's application development CI/CD tools to ensure comprehensive protection throughout the application lifecycle. Users should consider vendors providing integration with backend security platforms, including key API gateway, cloud-native API Gateway, WAF, and other complementary solutions, as well as with mobile app and backend development frameworks. Additionally, vendors should facilitate easy integration with and iOS platforms, cross-platform development environments, and provide common authorization techniques applicable for both web and mobile API channels to authenticate lawful access.

- **Scalability and Availability:** The In-App Protection vendors must provide protection even during traffic surges to ensure 24×7 availability. The in-app protection product must be capable of protecting any application and must support API security and the security of serverless applications. The product should also scale with the business to provide continuous protection against a bevy of threats. Users should look for In-App protection vendors with a history of successful large-scale deployments and carefully analyze the existing case studies of those deployments. This should form the basis for preparing best practices for managing the In-App protection deployments.

- **Comprehensive Use Case Coverage:** Users are recommended to perform a weighted analysis of various parameters pertinent to their industry requirements and seek a wide range of use cases. Key considerations should include the ability to block credential stuffing attacks, API abuse by bots and scripts, man-in-the-middle attacks, prevent app impersonation, IoT attacks, and denial of service attacks. Additionally, users with specific requirements should evaluate In-App protection solutions and consider vendors' differentiating strategies, such as network scale, time to protection, and flexible deployment options, including public, private, and hybrid cloud. Users must also look for vendors that offer visibility and reporting for various layers of security infrastructure

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, 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 SPARK Matrix™.

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

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

Evaluation Criteria: Technology Excellence

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

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

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

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

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

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

Evaluation Criteria: Customer Impact

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

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

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

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

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

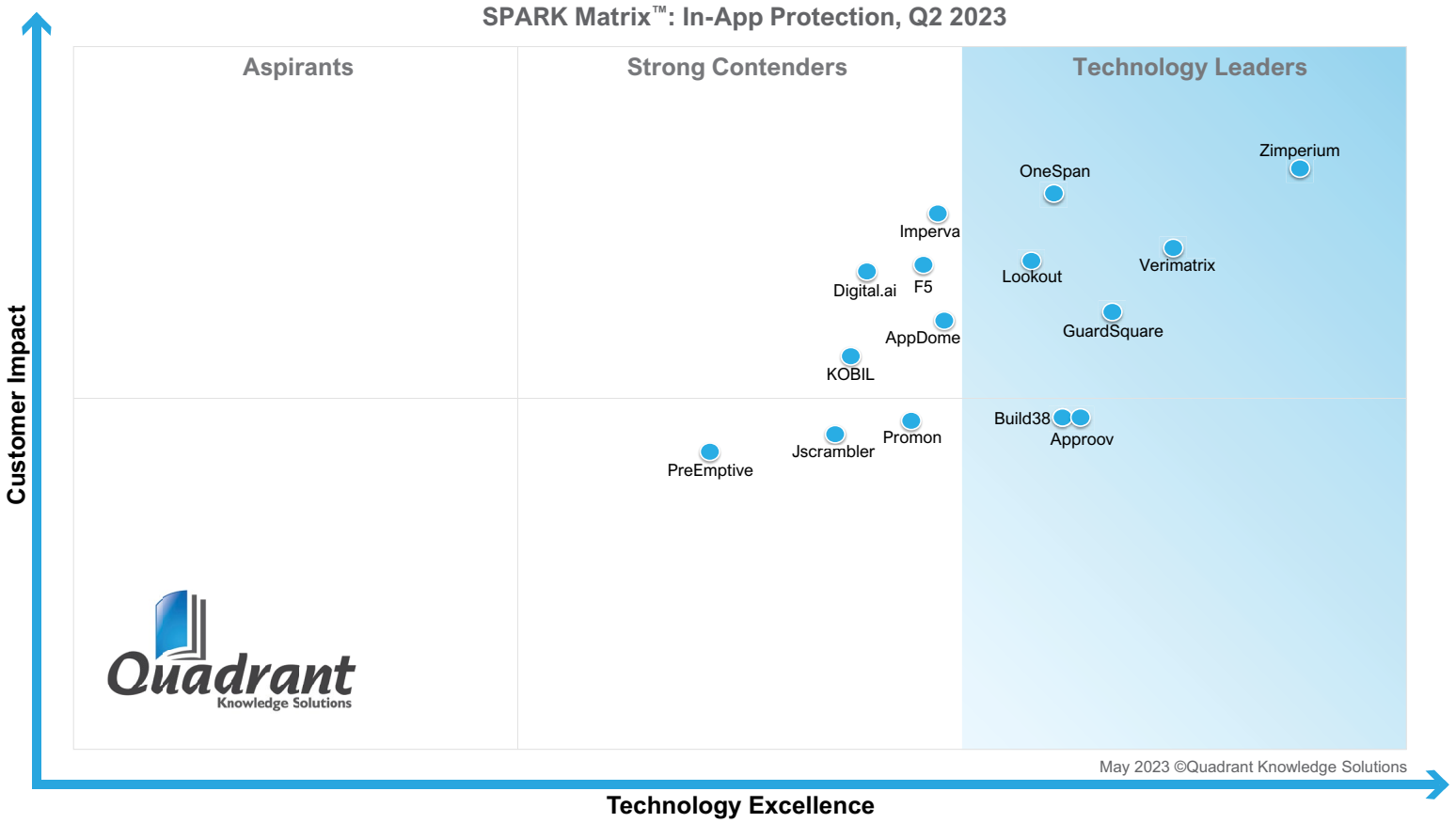
training, and support. Additionally, the company's service partner strategy or system integration capability across geographical regions is also considered.

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

SPARK Matrix™: In-App Protection

Strategic Performance Assessment and Ranking

Figure: 2023 SPARK Matrix™
(Strategic Performance Assessment and Ranking)
In-App Protection Market



Vendor Profiles

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 vendor's executives as part of the research process. The 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 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 solution and vendor selection based on research findings included in this research service.

Zimperium

URL: http://www.zimperium.com

Founded in 2010 and headquartered in Dallas, TX, Zimperium is a leading provider of mobile and application security solutions. The company provides real-time, on-device, and machine learning-based protection to mobile devices and applications from various threats, including device, network, phishing, and malicious app attacks targeting Android, iOS, and Chromebook OSes, mobile endpoints, and apps. Zimperium provides its in-app protection solutions for mobile devices through various products, including Mobile Application Protection Suite (MAPS), zScan, zKeyBox, zShield, and zDefend.

As a part of Zimperium's Mobile-First Security Platform™, the only platform offering autonomous and complete coverage for all endpoints and apps, Zimperium MAPS provides end-to-end protection for mobile apps. MAPS offers No-Code App Shielding, Code Obfuscation, Data Obfuscation, Runtime Application Self Protection, Tamper Resistance, Threat Reporting & Insights, Malware Protection, Phishing Protection, Cryptographic Key Protection, and Network Protection in one platform. The integrated threat management dashboard provided by MAPS enables real-time threat visibility as well as the capacity to respond to emerging threats and attacks discovered.

Analyst Perspective

Following is the analysis of Zimperium capabilities in the global In-App Protection market:

- Zimperium MAPS is a mobile application protection software that offers several sub-features to protect the entire mobile app lifecycle. These sub-features include zScan, zKeyBox, zShield, and zDefend. zScan assists developers in identifying security, privacy, and compliance issues during the development phase to allow developers to address them before the application is released to the public. zKeyBox offers protection to cryptographic keys and algorithms, ensuring that they remain secure. zShield provides protection against reverse engineering, code tampering, privacy, API key extraction, and malware injection. Lastly, zDefend protects mobile apps against on-device exploitation and provides real-time defense against mobile threats.

- Zimperium's zScan performs binary analysis to identify exploitable vulnerabilities. It also documents mobile app risks, such as hardware-specific usage and insecure API calls, and allows apps to be scanned directly from the build pipeline or manually uploaded to the administrative console. It also allows the compliance and security teams to customize policies to ensure that only applicable findings are opened. Additionally, zScan's "Build Compare" feature helps organizations track compliance progress and create more robust mobile apps.

- zKeyBox's whitebox cryptography protects keys and cryptographic algorithms on any platform within the mobile application. zKeyBox obscures cryptographic algorithms without compromising keys and ensures that the execution logic is untraceable. zKeyBox provides high performance on a wide range of architectures and a deep cryptographic experience to assist users throughout their application implementation.

- zShield provides protection against reverse engineering, advanced obfuscation, anti-debugging, binary packing, and diversification. It also offers anti-tampering features such as integrity checking, anti-method swizzling, function caller verification, and jailbreak/rooting detection. Organizations can customize the defense actions to meet their specific needs.

- zDefend provides comprehensive device protection from on-device exploitation, assists enterprises in gaining runtime threat visibility, and allows mobile apps to defend themselves against mobile threats in real time. ZDefend can integrate with SIEM, SOAR, and incident response, allowing enterprises to gain runtime threat visibility. It provides dynamic threat response, flexible deployment models, and simple implementation.

- Zimperium application shielding is a security feature that can be implemented on both mobile and desktop applications. The feature includes various types of detections such as root/jailbreak, debugger, and instrumentation-based detections, as well as malware and phishing detection. The feature automatically translates Java to native before applying obfuscation, runtime, and tamper resistance protections when applied to Android applications. This translation

enhances security by preventing the use of traditional Java-based hacking and debugging tools, making it harder for hackers to reverse engineer the code.

- Zimperium also provides Mobile Device Attestation capabilities, which adds value to fraud and identity use cases by allowing enterprises to verify the user and ensure they can trust the device when conducting transactions. The cryptographic key protection is fully configurable for size and speed and includes a comprehensive offering of standard Cryptographic ciphers. Furthermore, zShield tamper resistance is available on supported platforms. It leverages Apple's forward-compatible technology to provide robust tamper resistance.

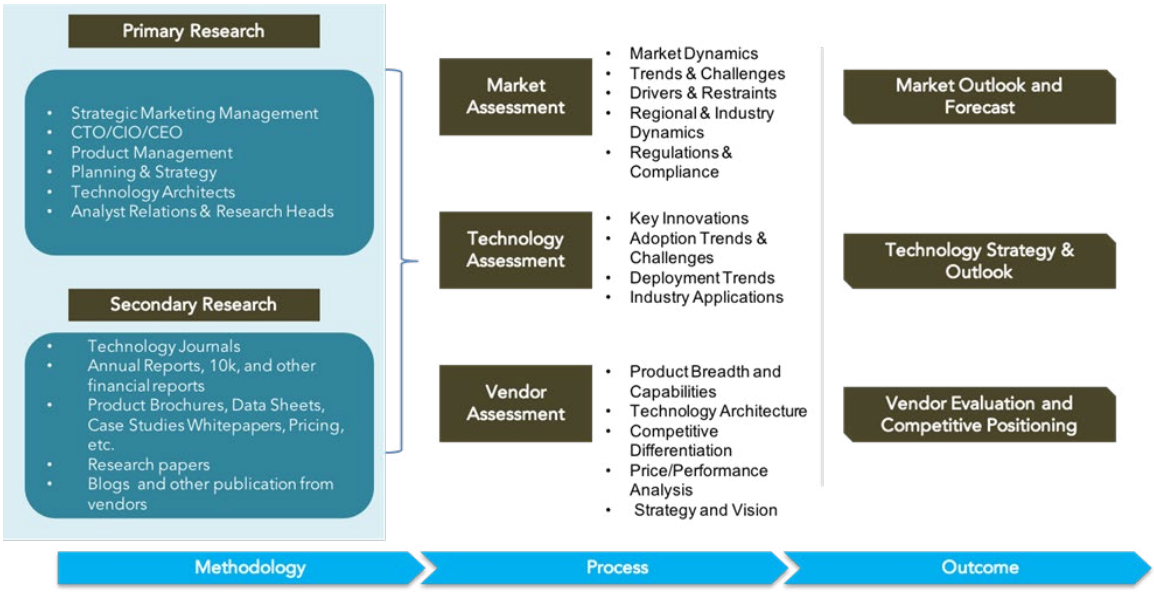
- Concerning geographical presence, Zimperium has a strong presence in North America, particularly the US, and Europe, as well as the EMEA and APAC regions. From an industry vertical perspective, the company's primary verticals include banking and financial services, government and public sector, IT and telecom, manufacturing, healthcare and life sciences, retail, eCommerce, and insurance. From a use case perspective, Zimperium offers sensitive data protection, anti-piracy, citizen safety applications, fraud prevention, secure payments, digital identity verification, and IP protection.

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

- As part of its technology roadmap, Zimperium is investing in modularizing its SDKs to provide them with the flexibility to fit onto modern OS and IoT platforms, the addition of low code/no code platform to reduce integration challenges and cost across customer segments, and threat insights and actionability during development and post-release for developers and security teams.

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