Quadrant Knowledge Solutions

Security & Risk Management

SPARK Matrix™: In-App Protection, 2022

Market Insights, Competitive Evaluation, and Vendor Rankings

April 2022

TABLE OF CONTENTS

Executive Overview

This research service includes a detailed analysis of the 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 MatrixTM. 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.

Key Research Findings

Following are the key research findings:

Technology Trends

The vendors of In-App Protection offerings continue to strengthen their value proposition by significantly investing in enhancing capabilities such as prevention, detection, anti-bot, clickjacking, runtime application self-protection, multifactor authentication, risk analysis, and more. Leading In-App Protection vendors are constantly augmenting their solution capabilities with AI ML to offer a robust protection from cyberthreats by analyzing application behavior and automating detection and remediation process.

Key Market Drivers and Trends:

The following are the key market drivers as per Quadrant Knowledge Solutions' In-App Protection strategic research:

- In-App Protection solutions are evolving and becoming more robust to combat the ever-increasing sophistication of cyber threats. The vendors are investing in increasing the number of customers, geographical presence, presence in different industry verticals, expanding use case support, and adding new capabilities to secure public and internal web applications from different attacks like bot attacks, injections, application-layer, and denial of service (DoS).

- Many leading In-App Protection providers are focusing on offering integrated solutions, including WAF, bot management capabilities, API security, L7 DDoS, etc., for providing a holistic application security portfolio. The vendors are also focusing on enhancing their Application Security capabilities by continually monitoring apps and API threats to handle new cases, conducting threat research on new attack vectors and tools, and developing applicable defenses for comprehensive application protection. Vendors of In-App protection products continue to focus on delivering industry-specific capabilities and plan to cover IOT-specific use cases.

- The COVID-19 pandemic-induced disrupted business scenarios, growth in remote working, and increased risk arising out of factors such as an

unprecedented rise in unsecured BYOD, WYOD, and IoT devices across enterprises, and the pressure to comply with ever-stringent and the growing complexities of the global regulatory environment, including data privacy norms is driving significant investment in In-App Protection solutions. Organizations are focusing on offering specialized security solutions for growing web application use cases such as mobile applications, Internet of Things (IoT) applications, and customers are focusing on adopting a robust solution to secure themselves from different attacks and secure their applications.

- Other market drivers for In-App Protection market growth include continued investment in digital transformation projects and the consequently increased adoption of cloud and hybrid infrastructures, increased use of mobile devices and remote working.

- With the continuous evolution and increasing sophistication of threats, vendors are rapidly adopting advanced capabilities such as code obfuscation, white-boxing 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. Vendors are implementing automated defenses for suspicious activities, which include app shutdown, user sandboxing, or code self-repair and derail threat actors by obfuscating source code, inserting honeypots, and implementing deceptive code patterns.

- Organizations are looking for vendors who understand their wants and needs and translate them into products and services, whose roadmap and vision are focused on fulfilling customer needs, and who offer comprehensive capabilities to protect public and internal applications from various attacks. Additionally, they are looking for vendors providing robust features, supporting diverse use cases, and having a presence in different industry verticals.

Competition Dynamics & Trends:

- This study includes an analysis of key vendors, including Approov, Build38, Digital.ai, F5, Guardsquare, IBM, Imperva, Jscrambler, KOBIL GmbH, Lookout,

OneSpan, PerimeterX, PreEmptive, Promon, Source Defense, Trustonic, Verimatrix, and Zimperium.

• OneSpan, Zimperium, Lookout, Verimatrix, Imperva, Trustonic, GuardSquare, and Approov are the top performers in the global In-App protection market and have been positioned as the top technology leaders in the 2022 SPARK Matrix analysis of the In-App protection market.

Market Definition and Overview

Quadrant Knowledge Solutions define In-App Protection as:

"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 repackaging, malware, script injection, cryptojacking, SMS snatching. Additionally, the tools block malicious scripts or tools from accessing the APIs."

The rise in mobile device usage has provided cybercriminals with new targets: mobile apps and environments. As mobile apps work assuming that those directly accessing the app are legitimate users, cybercriminals have access to multiple attack vectors. The COVID-19 pandemic and the subsequent rise in usage of unsecured devices by remote workers have further added to the risk. As mobile devices are being used to perform various critical tasks such as banking, the need to ensure in-app protection technology has gained prominence. The in-app protection technology plays a major role in protecting these applications from various kind of cyber threats. There are various threats targeting the mobile application environment which can cause a serious risk to the organization security posture. Some of these application vulnerabilities includes SQL injection, cross site scripting (XSS), broken access control, buffer overflow attacks, cross-site request forgery (CSRF), and malwares like screen scrapping.

An In-App Protection solution protects users' applications and sensitive data when accessed from unmanaged devices without the need for extra software or plug-ins. While traditional in-app solutions generally provide detection, the most important components are evaluation and reporting. The solution should be able to detect, evaluate, and report threats in real-time. It should also include obfuscation and encryption features to shield the app's assets from reverse engineering attempts when it is not in use. Owing to the rise of increasingly sophisticated cyberthreats, the In-App Protection solution providers are constantly improving their existing capabilities and incorporating new capabilities and security policies into their solution to provide with a more robust and holistic solution for their users for securing their applications.

Following are the key capabilities of In-App Protection solutions:

- **Application Hardening:** Application hardening protects applications from reverse engineering and tempering, secures apps, repacking, and more by leveraging code obfuscation, white-box 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-Tempering:** Anti-tampering monitors web and mobile application behavior and covers the overall runtime risk and attack spectrum in real-time. Anti-tempering 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 against attempts to repackage and alter mobile apps.

- **RASP (Run-time Application Self Protection):** RSAP continuously analyses 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 works without impacting app design by operating on the server where the app is operating.

- **Risk Assessment:** In-App Protection analyses and identifies potential threat actors and sensitive data in applications, map the attack surface, scan, and remediate vulnerabilities, determine AppSec process pain points, and strategize 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.

Need to safeguard apps in the 'mobile-first' environment

The unprecedented rise in mobile device usage, driven by various factors, including technological advancements, friendly business decisions, and ease of use, is witnessing enterprises adopting a mobile-first approach. Enterprises are rapidly adopting mobile applications due to benefits such as enhancement in internal operations and customer experience through customizable user interface, ease of payments through digital wallets, and much more. However, as modern businesses move from web applications to mobile apps, they are increasing their attack surface. Some of the mobile threats faced by modern enterprises include repackaging, malware, script injection, cryptojacking, SMS grabbing, and more. Additionally, remote work culture, increased adoption of Bring Your Own Device (BYOD), online shopping trends, and varying levels of security offered by various software environments serve as entry points for threat actors to access sensitive information through unsecured mobile devices.

In such high-risk environments, there is a need for an integrated set of application security capabilities. Therefore, organizations are increasingly adopting in-app protection tools to run these critical applications in untrusted environments. In-App protection tools provide capabilities, including code obfuscation, white-boxing techniques, multi-factor authentication, runtime application self-protection (RASP), and risk analytics to help organizations overcome these challenges. Moreover, while application developers can integrate some security capabilities, they do not provide high-level security. Most mobile developers look for vendors who can provide high-end security without disrupting their deployment initiatives. These vendors share in-app protection tools with developers to integrate high-level security in their mobile applications.

API economy driving need for in-app protection tools

To reach the growing number of audiences over digital platforms, enterprises are focussing on providing an integrated API framework with platforms like SOAP, REST, GraphQL, gRPC, and more. Also, an effective API enables enterprises to accelerate their marketing strategies to reach out to a newer and wider audience.

In addition, the APIs offer a high level of adaptiveness. Thus, it can be adapted to comply with a host of regulations while ensuring organizational interoperability. These factors are driving enterprises of all sizes to shift towards APIs. However, enterprises do need an integrated set of application security capabilities along with effortless deployment of their APIs, which can be leveraged by In-App protection tools. In-app protection tools allow developers to integrate high-level security measures, such as implementing strong authentication techniques paired with limited rate of access, in their APIs to prevent hackers from harvesting data from API servers.

In-App Protection solution address the growing demands of dynamic regulatory environment

While selecting/adopting In-App Protection solutions, enterprises look for regulatory compliances such as PCI-DSS, HIPAA, NIS, GDPR, FISMA, ISO 27001, as these regulations help organizations upgrade security and prevent information theft or misuse and the consequent penalties and negative publicity. Global regulations are becoming more complex, and enterprises must focus on creating strong security infrastructure and implementing the best practices. According to the EU's GDPR, the enterprise must ensure that enterprise data is gathered legally and monitor and protect this data from misuse and exploitation. Failure to do so would result in a penalty therefore, organizations are required to account for all sensitive data and the access granted to it. Applications contain and process personally identifiable information (PII) and sensitive data like credentials of the users, which can be phished from vulnerable mobile devices. In-App protection helps organizations to meet the stringent global compliance standards to avoid and prevent security breaches and strengthen compliances with global regulations.

Increased Adoption of Cloud-Based Resources and Applications

Enterprises adopt cloud-based resources and applications to be cost-effective, improve information security, upgrade operation efficiency, and be competitive. The increased usage of cloud-based applications and services many times jeopardizes security. The reliance on cloud-based third-party platforms presents

multiple issues for security operations teams since they are obliged to rely on a third-party tool's security controls and resilience. In-App Protection solutions support organizations in securing on-prem and cloud-based applications and resources against cyber threats. The In-App protection solution helps enterprises gain an overview of the behavior and activities of applications and reveals anomalies if present.

COVID-19 consequences driving rising adoption of In-App Protection tools

The COVID-19 pandemic has influenced enterprises to digitally transform their workforce through increased adoption of work-from-home and BYOD (Bring Your Own Device) options. While this has ensured sustenance and even growth for the enterprises, it has brought the challenges of increased application threat incidents. The remote workforce is difficult to monitor and manage. And since a majority of the employees are working from home and from their own unsecured devices, their activities and behavior are no longer being supervised. Furthermore, there is a massive increase in the usage of numerous applications for various activities by the home-bound crowd. Hence, driven by the COVID-19 pandemic, enterprises increasingly understand the benefit of an in-app protection solution. As traditional technologies are insufficient in managing personal devices and private networks, organizations are adopting in-app protection solutions to safeguard themselves from the perils of different types of threats to high-value applications.

Competitive Landscape and Analysis

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

OneSpan, Zimperium, Lookout, Verimatrix, Imperva, Trustonic, GuardSquare, and Approov are identified as global technology leaders in the SPARK Matrix: In-App Protection, 2022. These companies provide a sophisticated and comprehensive technology platform to protect, detect, analyze, and remediate against known and unknown advanced cyber threats throughout the application lifecycle. The platform offers real-time protection for high-value applications against various threats, including repackaging, malware, script injection, cryptojacking, SMS snatching, and others and insecure environment related threats.

OneSpan offers In-App Protection through its product Mobile Application Shielding which provides strong, natively integrated app security and runtime protection. OneSpan Mobile Application Shielding provides overlay detection, jailbreak & root detection, anti-code injection, anti-keylogging, anti-repacking protection, debugger protection, obfuscation, and such other capabilities to secure applications. Additionally, OneSpan's In-App protection product protects apps from zero-day attacks, runs apps securely, and provides integrated protection from foreign code injection.

Zimperium provides real-time, on-device, and machine learning-based protection to mobile devices and applications from threats targeting Android, iOS, and Chrome OSs. Zimperium offers a range of modules, including MAPS Mobile Application Protection Suite, zScan Application Security Testing, zKeyBox Cryptographic Key Protection, zShield Application Shielding, and zDefend Runtime Application Self-Protection to protect mobile applications from various types of threats. Zimperium allows organizations to secure against privileged data and infrastructure exposure, frauds, and regulatory penalties. Additionally, the Zimperium products offer various capabilities, including app scanning, app shielding, runtime protection, threat

management dashboard, and the protection of sensitive cryptographic keys in one platform to detect and protect from advanced threats.

Lookout provides continuous and real-time security for applications along with advanced mobile threat detection through its Lookout Embedded AppDefense. Lookout Embedded AppDefense allows users to track mobile device health in real-time with its minimum coding for Lookout SDK and provides critical information to remediate advance threats. Lookout partners with Promon to provide robust In-App protection solutions that provide static and runtime protection, anti-tempering of apps, and protection from app reverse engineering.

Verimatrix offers automated and intelligence-driven in-app protection through its App Shield product to eliminate the risk of human error. Verimatrix App Shield provides automated anti-tamper technology, environmental checks, and code obfuscation capabilities that protect applications from known and unknown threats. Additionally, the product allows organizations to secure their apps from threats such as reverse engineering, repackaging, dynamic modification, man-in-the-middle attacks, emulators & debuggers, and rooted jailbroken.

Trustonic offers security solutions to smart devices and applications with a unique approach that isolates the security-critical sections of the program and focuses on securing them. Trustonic utilizes Trusted Execution Environment (TEE) to run the important code on devices with world-class software security and Whitebox cryptography.

Imperva's application security provides a comprehensive set of solutions to protect all kinds of applications and APIs from cyber threats. Additionally, the solution protects allows organizations to secure APIs from the latest automated attacks such as cloud WAF, advanced bot protection, account takeover, client-side protection, runtime protection, and DDoS protection.

GuardSquare provides security for both iOS and Android applications through its DexGuard, iXGuard, ThreatCast, and ProGuard solutions. The solutions offer multiple layers of code hardening and runtime application self-protection with real-time visibility iOS and android applications to gain actionable insights. Guardsquare also offers ProGuard, an open source shrinker for Java bytecode that may be used to improve and optimize application code.

Approov is an emerging leader in the In-App Protection market. Approov offers API Threat Protection Software to create a secure environment for APIs and businesses. Approov blocks API access from an unauthorized script or tool with zero false positives, protects apps from Man-in-the-Middle attacks via dynamic certificate pinning and prevents stolen secrets from being used by scripts or tools to access APIs. Approov prevents vulnerabilities in APIs from being exploited at runtime, unlike SAST or DAST solutions, which focus on helping developers eliminate vulnerabilities before deployment. Additionally, it offers protection against attacks such as account takeover, fake account creation, denial of service, credit fraud, app impersonation, man-in-the-middle, API security breach, and scraping.

F5, Digital.ai, PerimeterX, IBM, and KOBIL GmbH have been positioned amongst the primary challengers. These companies provide comprehensive technology 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 2022 SPARK Matrix include Promon, Jscrambler, PreEmptive, Source Defense, and Build38.

All the vendors captured in the 2022 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, they help organizations expand their partnership channels and support diverse use cases. Vendors are consistently looking to enhance 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-tempering techniques, multifactor authentication, biometric authentication, anti-keylogging, anti-screen scraping, Whitebox cryptography, jailbreak/root detection, and more capabilities enabling 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, which are 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

A majority of the leading In-App Protection vendors may provide off-the-shelf capabilities, including Application hardening, anti-tempering, run-time application self-protection, risk analysis, and authentication support. However, the flexibility of deployment 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 competitive factors and differentiators for the evaluation of In-App Protection vendors are as follows:

- **The Sophistication of Technology Capability:** 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 should evaluate In-App protection solutions that offer end-to-end capabilities to protect their mobile apps throughout their entire life cycle. The In-App protection solutions should help all types of apps, including mobile apps, single-page web apps, software, and connected devices, to proactively defend against all types of mobile threats. The solution should enable apps to develop resilience against a variety of mobile threats such as repackaging, malware, script injection, cryptojacking, SMS grabbing, and others. Besides, the solution should enable applications to protect themselves against various advanced threats such as malware, code injection, screen scrapping, application cloning, and reverse engineering. Enterprises may evaluate in-App protection solutions that provide a wide range of authentication options such as behavioral biometrics, OTPs, facial recognition, fingerprint authentication, e-signatures, and more. It should offer sophisticated 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-tempering.

- **Maturity of AI and ML:** In-App protection solution vendors' capability to provide embedded AI and machine learning capabilities may differ significantly. By leveraging AI and ML, vendors can automatically respond to and mitigate attacks, and prevent attacks before they cause any damage. Vendors are using AI/ML technology to enable advanced network analytics, user analytics, and threat intelligence to automate the mitigation processes and improve the effectiveness of application protection. Users should look at vendors offering AI/ML for detecting threats patterns, comprehensive risk analysis, and responding to threats in real-time and thus securing users' applications.

- **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 evaluate vendors' expertise and domain knowledge in understanding their unique security problems, use cases, industry, and region-specific requirements. Users should look for ease of use, comprehensiveness of offering, software's flexibility to adapt with constant market changes and regulatory requirements, minimizing total cost of ownership, and transparency. Users are also advised to consider the vendors providing advanced capabilities like application attestation, client environment attestation, dynamic certificate pinning for analysis of traffic patterns, threat detection, and remediation. Uses should also look for vendors providing advanced functionalities like automated and intelligence-driven in-app protection solutions to minimize human error, real-time monitoring of applications, and others. Users should also look for a solution with a history of successful large-scale deployments and carefully analyze the existing case studies of those deployments. This should form the basis to prepare the best practice for in-app protection solution deployments.

- **Integration and Interoperability:** Seamless integration and interoperability with vendors' existing technologies are amongst the crucial factors impacting technology deployment and ownership experience. An In-App Protection platform should offer fully automated integration with the user's application development CI/CD tools to provide comprehensive protection to applications throughout the application lifecycle. Users should look for 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. Vendors should also provide simple integration with Android and iOS platforms, as well as cross-platform development environments, and provide common authorization techniques to be used for both the web and mobile API channels to validate 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 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 to prepare best practices for managing the In-App protection deployments.

- **Technology Vision & 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 application, reverse engineering, cryptojacking, malware, script injection and offer capabilities such as application hardening, API protection, and more. 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

- **Comprehensive Use Case Coverage:** Users should employ weighted analysis of the various parameters required for their industry needs and look for broad range use cases, blocks credential stuffing attacks, blocks API abuse by bots and scripts, blocks man-in-the-middle attacks, prevents app impersonation, and prevents denial of service attacks. Moreover, users with one or more specific requirements are advised to evaluate In-App protection solutions by considering

vendors' differentiating strategies that may include network scale, time to protection, and flexible deployment options, including public, private, and hybrid cloud. Users must carefully examine vendors that provide 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 makings, such as finding M&A prospects, partnership, geographical expansion, portfolio expansion, and 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

- **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.

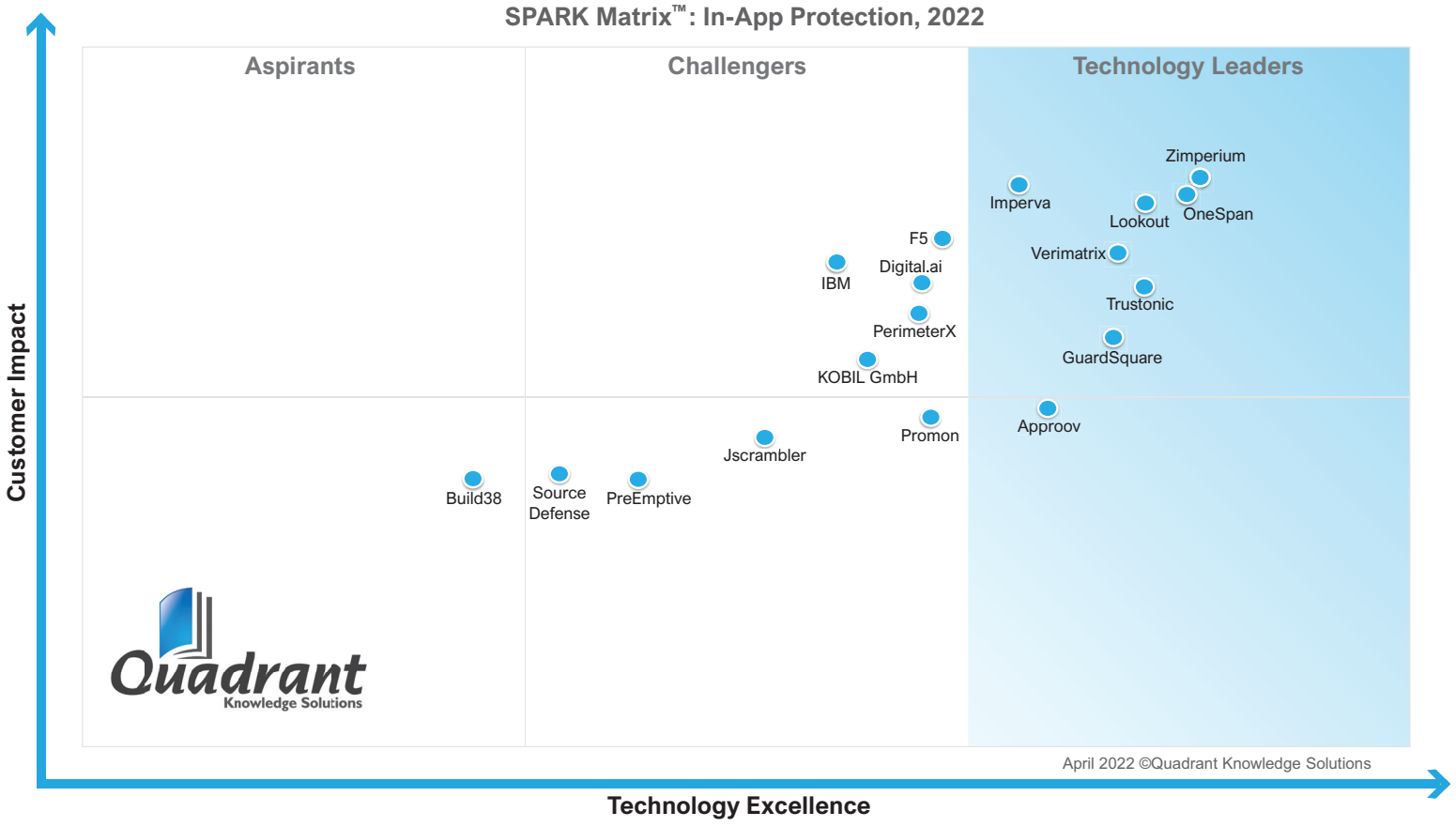
- **Customer Service Excellence:** The ability to demonstrate vendors capability to provide a range of professional services from consulting, training, and support. Additionally, the company's service partner strategy or system integration capability across geographical regions is also considered.

- **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, 2022

Strategic Performance Assessment and Ranking

Figure: 2022 SPARK Matrix™
(Strategic Performance Assessment and Ranking)
In-App Protection Market



Vendors Profile

Following are the profiles of the leading In-App Protection 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, along with publicly available information. 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 directly speak to respective vendors for a more comprehensive understanding of their technical 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: www.zimperium.com

Founded in 2010 and headquartered in Dallas, TX, USA, Zimperium is a leading provider of mobile security solutions that protect mobile devices and applications from sophisticated mobile threats. The company provides real-time, on-device, and machine learning-based protection to mobile devices and applications from threats such as 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 its products, including Mobile Application Protection Suite (MAPS), ZScan, ZKeyBox, ZShield, and ZDefend.

Zimperium MAPS enables organizations to identify compliance risks during the app development phase and monitor and protect apps from attacks while in use. Zimperium MAPS offers sub-features to protect mobile app life cycle such as zScan, zKeyBox, zShield, and zDefend. Zimperium zScan enables developers to search and fix compliances, privacy, and security issues in the development phase. Zimperium zKeyBox secures cryptographic keys and prevents them from being detected, extracted, or manipulated. Zimperium zShield protects apps from reverse engineering, code tampering, privacy, extracting assets, extracting API keys, and malware injection with the help of obfuscation and anti-tampering functionality. Zimperium provides SDK zDefend to detect and protect against device, network, phishing, and malware attacks.

Zimperium zScan assists developers in automatically identifying privacy, security, and compliance concerns during the development process before the apps are released to the public. zScan's binary analysis detects vulnerabilities in the program that an attacker could exploit. Furthermore, zScan documents risks within mobile apps such as hardware-specific usage, insecure API calls, and sensitive data handling, allows apps to be scanned directly from the build pipeline or manually uploaded to the administrative console as desired and enables compliance and security teams to define and customize policies to ensure only the applicable findings are opened. Furthermore, zScan's "Build Compare" feature instantly identifies whether risks are trending up or down in each succeeding version. Organizations can use version comparisons to track compliance progress and create more robust mobile apps.

Zimperium zKeyBox uses white-box cryptography to safeguard keys, secrets, and standard or custom cryptographic algorithms on any platform within the mobile application. zKeyBox ensures that keys are never exposed, and the execution logic is untraceable. zKeyBox also modifies and obscures cryptographic algorithms without compromising keys even if the device has been compromised. Furthermore, Zimperium does not rely on hardware provided by the underlying platform to support regulatory compliance, provides great performance on a wide range of architecture, and a deep cryptographic experience to help the users through every stage of their application implementation.

Zimperium zShield protects the source code, intellectual property (IP), and data within the application from threat actors by hardening and protecting the app utilizing powerful obfuscation and anti-tampering capability. zShield guards against reverse engineering, Advanced Obfuscation, Anti-Debugging, Binary Packing, and Diversification. Additionally, zShield offers anti- tempering features, including Integrity Checking, Anti-Method Swizzling, Function Caller Verification, Jailbreak / Rooting Detection, Shared Library Cross-Checking, Mach-O Binary Signature Verification, Google Play Licensing Protection, and Customizable defense actions.

Zimperium's zDefend prevents on-device exploitation, assists enterprises in gaining runtime threat visibility, and allows mobile apps to defend themselves against mobile threats in real-time. Zimperium's patented machine-learning-based Mobile Threat Defense engine z9 is used in zDefend. As a software development kit, the solution may be easily integrated into any iOS or Android application (SDK). Furthermore, zDefend aids in comprehensive device protection by providing dynamic threat response, threat visibility, security ecosystem integrations such as SIEM, SOAR, and incident response, as well as flexible deployment models and simple implementation.

Analyst Perspective

Following is the analysis of Zimpreium's capabilities in the global In-App Protection market:

- Zimperium offers modules such as Mobile Application Protection Suite (MAPS), Zscan, ZKeyBox, ZShield, and ZDefend that protect from various types of application threats. Zimperium MAPS provides end-to-end protection for mobile apps, from development to deployment.

MAPS also offers app scanning, app shielding, runtime protection, and the protection of sensitive cryptographic keys 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.

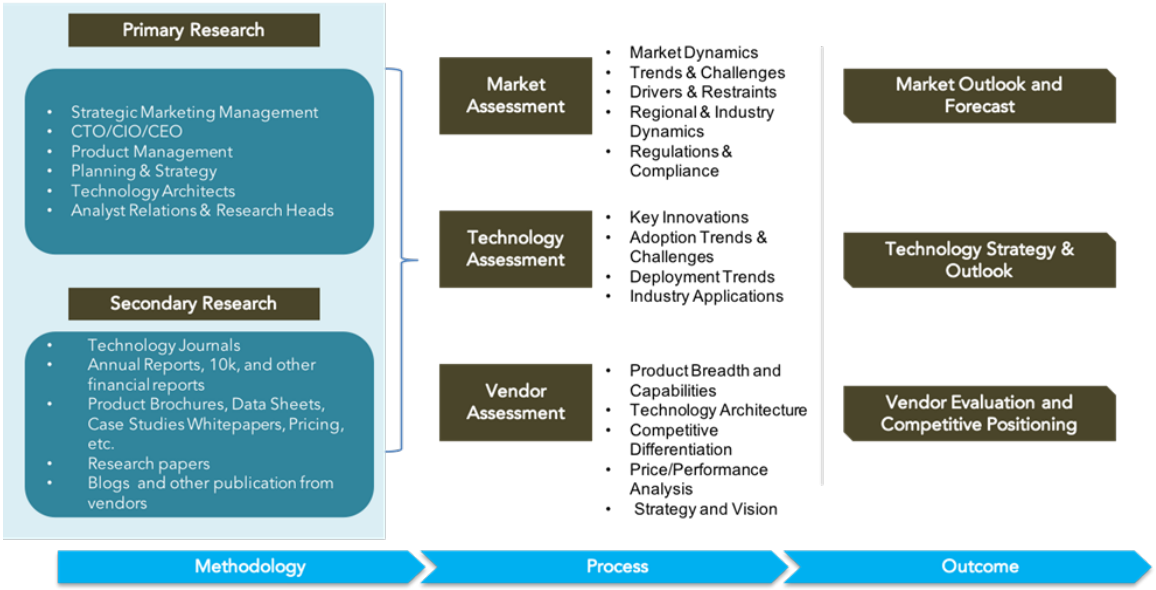
- Concerning geographical presence, Zimperium has a strong presence in the US and Europe, followed by other EMEA and APAC regions. From an industry vertical perspective, while the company has a presence across a wide variety of industries, its primary verticals include banking and financial services,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

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

- As part of its technology roadmap, Zimperium is investing in improving its capabilities, securing its position as the mobile app protection platform, increasing the number of customers, geographical presence, different industry verticals, and expanding use case support.

Research Methodologies

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