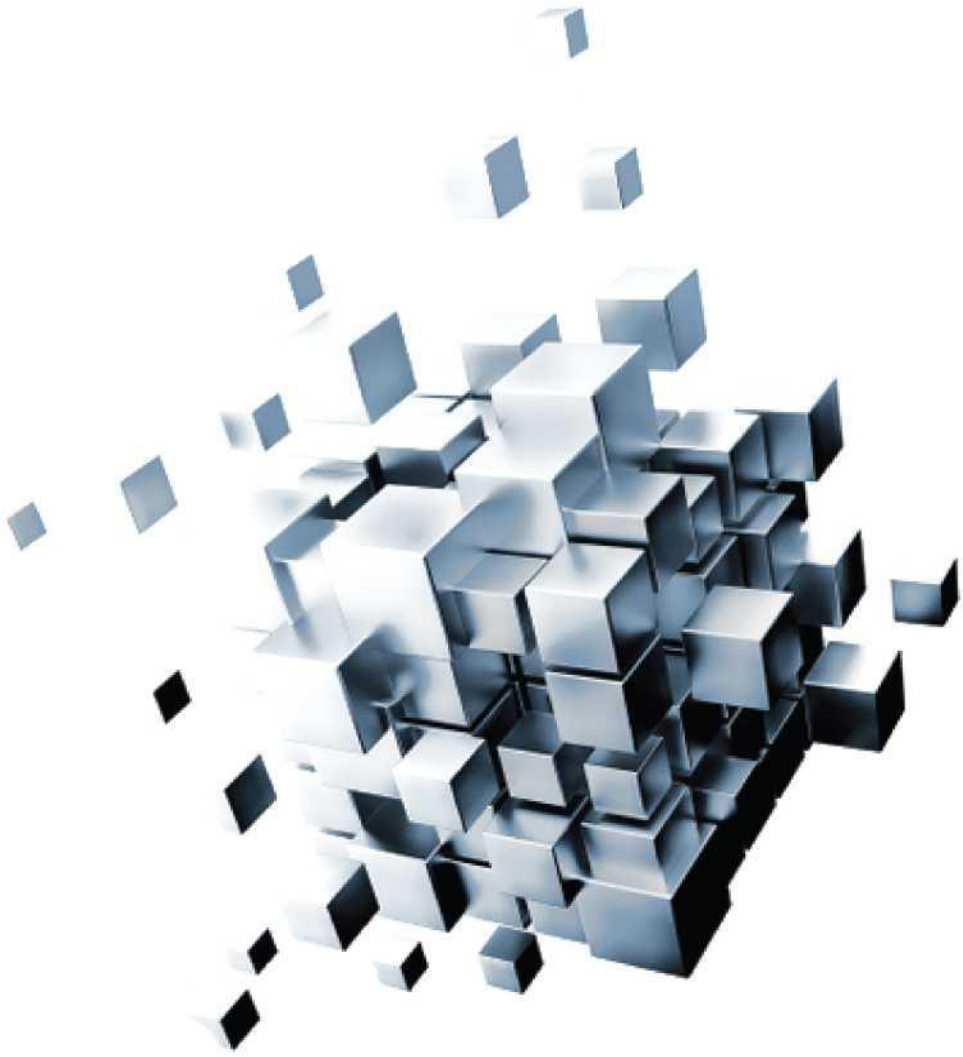
Sicherheit und Risikomanagement

SPARK Matrix™: In-App-Schutz 2022

Markteinblicke, Wettbewerbsbeurteilung und Anbieter-Rankings

April 2022



INHALTSVERZEICHNIS

Exekutiver Überblick

Dieser Forschungsdienst umfasst eine detaillierte Analyse der globalen Marktdynamik des In-App-Schutzes, der wichtigsten Trends, der Anbieterlandschaft und der Wettbewerbspositionierung. Die Studie bietet eine Wettbewerbsanalyse und ein Ranking der führenden Anbieter von In-App-Schutz in Form der SPARK Matrix™. Diese Studie liefert strategische Informationen für Technologieanbieter, um den Markt besser zu verstehen und ihre Wachstumsstrategien zu unterstützen, und für Anwender, um die Fähigkeiten verschiedener Anbieter, die Wettbewerbsdifferenzierung und ihre Marktposition zu bewerten.

Wichtige Forschungsergebnisse

Im Folgenden sind die wichtigsten Forschungsergebnisse aufgeführt:

Technologie-Trends

Die Anbieter von Angeboten für In-App-Schutz stärken weiterhin ihr Wertversprechen, indem sie erheblich in die Verbesserung von Funktionen wie Prävention, Erkennung, Anti-Bot, Clickjacking, Selbstschutz von Runtime-Anwendungen, Multifaktor-Authentifizierung, Risikoanalyse und mehr investieren. Führende Anbieter von In-App-Schutz erweitern ihre Lösungen ständig um KI-ML, um durch die Analyse des Anwendungsverhaltens und die Automatisierung des Erkennungs- und Behebungsprozesses einen robusten Schutz vor Cyber-Bedrohungen zu bieten.

Wichtige Markttreiber und Trends:

Im Folgenden werden die wichtigsten Markttreiber gemäß der strategischen Forschung von Quadrant Knowledge Solutions zum In-App-Schutz aufgeführt:

- Die Lösungen für den In-App-Schutz entwickeln sich weiter und werden immer robuster, um die immer ausgefeilteren Cyber-Bedrohungen zu bekämpfen. Die Anbieter investieren in die Erhöhung der Kundenzahl, die geografische Präsenz, die Präsenz in verschiedenen Branchen, die Ausweitung der Unterstützung von Anwendungsfällen und das Hinzufügen neuer Funktionen zum Schutz öffentlicher und interner Webanwendungen vor verschiedenen Angriffen wie Bot-Attacken, Injektionen, Anwendungsebenen und Denial-of-Service (DoS).

- Viele führende Anbieter von In-App-Schutz konzentrieren sich darauf, integrierte Lösungen anzubieten, einschließlich WAF, Bot-Management-Funktionen, API-Sicherheit, L7 DDoS usw., um ein ganzheitliches Portfolio für die Anwendungssicherheit bereitzustellen. Die Anbieter konzentrieren sich auch darauf, ihre Anwendungssicherheitsfunktionen zu verbessern, indem sie Anwendungen und API-Bedrohungen kontinuierlich überwachen, um neue Fälle zu behandeln, Bedrohungsforschung zu neuen Angriffsvektoren und -tools zu betreiben und anwendbare Abwehrmaßnahmen für einen umfassenden Anwendungsschutz zu entwickeln. Die Anbieter von Produkten für In-App-Schutz konzentrieren sich weiterhin auf die Bereitstellung branchenspezifischer Funktionen und planen, IOT-spezifische Anwendungsfälle abzudecken.

• Die durch die COVID-19-Pandemie verursachten Geschäftsunterbrechungen, die Zunahme der Telearbeit und die erhöhten Risiken, die sich aus Faktoren wie der beispiellosen Zunahme von ungesicherten BYOD-, WYOD- und IoT-Geräten in Unternehmen ergeben, sowie der Druck, die immer strengeren und komplexeren globalen Vorschriften, einschließlich der Datenschutznormen, einzuhalten, führen zu erheblichen Investitionen in In-App-Schutz-Lösungen. Unternehmen konzentrieren sich darauf, spezialisierte Sicherheitslösungen für wachsende Webanwendungen wie mobile Anwendungen und Internet of Things (IoT)-Anwendungen anzubieten, und Kunden konzentrieren sich auf die Einführung einer robusten Lösung, um sich vor verschiedenen Angriffen zu schützen und ihre Anwendungen zu sichern.

• Weitere Markttreiber für das Wachstum des In-App-Schutz-Marktes umfassen kontinuierliche Investitionen in digitale Transformationsprojekte und die damit einhergehende verstärkte Nutzung von Cloud- und hybriden Infrastrukturen, der verstärkte Einsatz von mobilen Geräten und Remote-Arbeit.

• Da sich die Bedrohungen ständig weiterentwickeln und immer ausgefeilter werden, setzen die Anbieter immer mehr fortschrittliche Funktionen wie Code-Verschleierung, White-Boxing-Techniken, Multi-Faktor-Authentifizierung, RASP (Runtime Application Self-Protection) und Risikoanalyse ein.

• Viele Anbieter von In-App-Schutz konzentrieren sich auf die Bereitstellung neuer Präventionsmethoden für Anwendungen durch Sicherheit auf Code-Ebene. Anbieter implementieren automatisierte Schutzmaßnahmen für verdächtige Aktivitäten, wie das Abschalten von Anwendungen, Sandboxing für Benutzer oder die Selbstreparatur von Code, und bringen Bedrohungsakteure durch Verschleierung des Quellcodes, Einfügen von Honeypots und Implementierung irreführender Codemuster aus dem Konzept.

• Unternehmen suchen nach Anbietern, die ihre Wünsche und Bedürfnisse verstehen und in Produkte und Dienstleistungen umsetzen, deren Roadmap und Vision auf die Erfüllung der Kundenbedürfnisse ausgerichtet sind und die umfassende Funktionen zum Schutz öffentlicher und interner Anwendungen vor verschiedenen Angriffen bieten. Außerdem suchen sie nach Anbietern, die robuste Funktionen bieten, verschiedene Anwendungsfälle unterstützen und in verschiedenen Branchen vertreten sind.

Wettbewerbsdynamik und Trends:

- Diese Studie beinhaltet eine Analyse der wichtigsten Anbieter, darunter Approov, Build38, Digital.ai, F5, Guardsquare, IBM, Imperva, Jscrambler, KOBIL GmbH, Lookout, OneSpan, PerimeterX, PreEmptive, Promon, Source Defense, Trustonic, Verimatrix und Zimperium.

- OneSpan, Zimperium, Lookout, Verimatrix, Imperva, Trustonic, GuardSquare und Approov sind die Top-Performer auf dem globalen Markt für In-App-Schutz und wurden in der SPARK-Matrix-Analyse des Marktes für In-App-Schutz 2022 als Top-Technologieführer positioniert.

Marktdefinition und Überblick

Quadrant Knowledge Solutions definiert In-App-Schutz als:

„In-App-Schutz ist ein fortschrittlicher Satz von Anwendungssicherheits-Tools, die zum Schutz, zur Erkennung, Analyse und Behebung von bekannten und unbekannten fortschrittlichen Cyber-Bedrohungen während des gesamten Anwendungslebenszyklus entwickelt wurden. Die Tools bieten Schutz in Echtzeit für hochwertige Anwendungen, die in einer ungesicherten Umgebung laufen, gegen Bedrohungen wie Repackaging, Malware, Script-Injektion, Cryptojacking und SMS-Snatching. Außerdem verhindern die Tools, dass bösartige Skripte oder Tools auf die APIs zugreifen können."

Die zunehmende Nutzung mobiler Geräte bietet Cyber-Kriminellen neue Ziele: mobile Anwendungen und Umgebungen. Da bei mobilen Anwendungen davon ausgegangen wird, dass diejenigen, die direkt auf die Anwendung zugreifen, legitime Nutzer sind, haben Cyber-Kriminelle Zugang zu mehreren Angriffsvektoren. Die COVID-19-Pandemie und die anschließende Zunahme der Nutzung ungesicherter Geräte durch Fernmitarbeiter haben das Risiko weiter erhöht. Da mobile Geräte für verschiedene kritische Aufgaben wie z. B. Bankgeschäfte verwendet werden, hat die Notwendigkeit, eine Technologie für den In-App-Schutz zu gewährleisten, stark an Bedeutung gewonnen. Die Technologie für den In-App-Schutz spielt eine wichtige Rolle beim Schutz dieser Anwendungen vor verschiedenen Arten von Cyber-Bedrohungen. Es gibt verschiedene Bedrohungen, die auf die Umgebung mobiler Anwendungen abzielen und ein ernsthaftes Risiko für die Sicherheitslage des Unternehmens darstellen können. Zu diesen Anwendungsschwachstellen gehören SQL-Injektion, Cross-Site-Scripting (XSS), fehlerhafte Zugriffskontrolle, Pufferüberlauf-Angriffe, Cross-Site-Request-Forgery (CSRF) und Malware wie Screen Scrapping.

Eine Lösung für den In-App-Schutz schützt die Anwendungen und sensiblen Daten von Anwendern beim Zugriff von nicht verwalteten Geräten, ohne dass zusätzliche Software oder Plug-ins erforderlich sind. Während herkömmliche In-App-Lösungen in der Regel eine Erkennung bieten, sind die wichtigsten Komponenten die Auswertung und die Berichterstattung. Die Lösung sollte in der Lage sein, Bedrohungen in Echtzeit zu erkennen, zu bewerten und zu melden. Sie sollte auch Verschleierungs- und Verschlüsselungsfunktionen enthalten, um die Assets der App vor Reverse-Engineering-Versuchen zu schützen, wenn sie nicht in Gebrauch ist. Aufgrund des Anstiegs immer ausgefeilterer Cyber-Bedrohungen verbessern die Anbieter von Lösungen für den In-App-Schutz ständig ihre bestehenden Funktionen und integrieren neue Funktionen und Sicherheitsrichtlinien in ihre Lösungen, um ihren Nutzern eine robustere und ganzheitliche Lösung zur Sicherung ihrer Anwendungen zu bieten.

Nachfolgend sind die wichtigsten Funktionen von Lösungen für den In-App-Schutz aufgeführt:

- **Anwendungshärtung:** Anwendungshärtung schützt Anwendungen vor Reverse Engineering und Tempering, sichert Apps, Repacking und mehr, indem Codeverschleierung, White-Box-Kryptografie und andere Techniken eingesetzt werden. Die Anwendungshärtung umfasst aktive und passive Härtung, um die Verwendung von Debuggern zu erkennen und darauf zu reagieren, indem das Verhalten der Anwendung geändert und die Anwendung auf der Grundlage statischer Analysen widerstandsfähiger gegen Angriffe gemacht wird.

- **Anti-Temperierung:** Anti-Temperierung überwacht das Verhalten von Web- und Mobilanwendungen und deckt das gesamte Laufzeitrisiko und Angriffsspektrum in Echtzeit ab. Mit Anti-Temperierung können Benutzer ihr geistiges Eigentum schützen und Anwendungen vor der Erstellung einer falschen Version, Verunstaltung, Änderung der Logik und dem Einfügen von Workflows bewahren. Außerdem warnt es Anwendungen, wenn Risiken erkannt werden, und schützt vor Versuchen, mobile Apps neu zu verpacken und zu verändern.

- **RASP (Run-time Application Self Protection):** RSAP analysiert kontinuierlich das Verhalten von Web- oder Nicht-Web-Anwendungen und den Kontext des Verhaltens, um bösartige Eingaben oder Verhaltensweisen ohne menschliches Zutun zu erkennen und davor zu schützen. RASP ermöglicht die Integration von Sicherheit in ein laufendes Programm, unabhängig davon, wo es sich befindet, fängt alle Aufrufe von der Anwendung an ein System ab und validiert Datenanforderungen sofort innerhalb der Anwendung. RASP funktioniert ohne Auswirkungen auf das Design der Anwendung, da es auf dem Server läuft, auf dem die Anwendung ausgeführt wird.

- **Risikobewertung:** Der In-App-Schutz analysiert und identifiziert potenzielle Bedrohungsakteure und sensible Daten in Anwendungen, kartiert die Angriffsfläche, scannt und behebt Schwachstellen, ermittelt die Schwachstellen in AppSec-Prozessen und entwirft eine Sicherheits-Roadmap zum Schutz vor Anwendungsangriffen in Echtzeit.

- **Unterstützung der Authentifizierung:** Der In-App-Schutz ermöglicht die automatische Authentifizierung eines Benutzers, wenn dieser auf privilegierte Daten und Anwendungen zugreifen möchte. Der In-App-Schutz verwendet

Multi-Faktor-Authentifizierungsverfahren (MFA) und erhöht die Sicherheit, indem er riskante Passwortverwaltungspraktiken eliminiert. MFA verwendet verschiedene Berechtigungsnachweise wie Passwörter, Nachrichten, digitale Zugangskarten und biometrische Verifizierung zur Authentifizierung von Benutzern. Des Weiteren hilft MFA, risikoreiche Anmeldungen zu erkennen und darauf zu reagieren und Passwörter einfach zurückzusetzen. Es bietet verbesserte Sicherheit und kontrolliert den Zugang zu Ressourcen, indem es riskante Benutzer automatisch in Echtzeit sperrt.

Notwendigkeit der Absicherung von Apps in der „Mobile-First"-Umgebung

Der beispiellose Anstieg der Nutzung mobiler Geräte, der durch verschiedene Faktoren wie technologische Fortschritte, freundliche Geschäftsentscheidungen und einfache Bedienung angetrieben wird, führt dazu, dass Unternehmen einen Mobile-First-Ansatz verfolgen. Unternehmen nehmen mobile Anwendungen schnell an, da sie die internen Abläufe und die Kundenerfahrung durch eine anpassbare Benutzeroberfläche verbessern, Zahlungen über digitale Geldbörsen erleichtern und vieles mehr. Mit dem Umstieg von Webanwendungen auf mobile Anwendungen vergrößern moderne Unternehmen allerdings ihre Angriffsfläche. Zu den mobilen Bedrohungen, mit denen moderne Unternehmen konfrontiert sind, gehören Repackaging, Malware, Script-Injektion, Cryptojacking, SMS-Grabbing und vieles mehr. Darüber hinaus bieten die Kultur der Telearbeit, die zunehmende Verbreitung von Bring Your Own Device (BYOD), der Trend zum Online-Shopping und die unterschiedlichen Sicherheitsniveaus der verschiedenen Softwareumgebungen Bedrohungsakteuren die Möglichkeit, über ungesicherte Mobilgeräte auf sensible Informationen zuzugreifen.

In solchen risikoreichen Umgebungen ist ein integrierter Satz von Anwendungssicherheitsfunktionen erforderlich. Daher setzen Unternehmen zunehmend Tools für den In-App-Schutz ein, um diese wichtigen Anwendungen in nicht vertrauenswürdigen Umgebungen auszuführen. Tools für den In-App-Schutz bieten Funktionen wie Code-Verschleierung, White Boxing-Techniken, Multi-Faktor-Authentifizierung, Runtime Application Self-Protection (RASP) und Risikoanalysen, um Unternehmen bei der Bewältigung dieser Herausforderungen zu unterstützen. Darüber hinaus können Anwendungsentwickler zwar einige Sicherheitsfunktionen integrieren, aber sie bieten keine Sicherheit auf hohem Niveau. Die meisten Entwickler von Mobilgeräten suchen nach Anbietern, die hohe Sicherheit bieten können, ohne ihre Bereitstellungsinitiativen zu stören. Diese Anbieter stellen Entwicklern Tools für den In-App-Schutz zur Verfügung, mit denen sie hochgradige Sicherheit in ihre mobilen Anwendungen integrieren können.

Die API-Wirtschaft steigert den Bedarf an Tools für den In-App-Schutz

Um die wachsende Zahl von Zielgruppen über digitale Plattformen zu erreichen, konzentrieren sich Unternehmen auf die Bereitstellung eines integrierten API-Frameworks mit Plattformen wie SOAP, REST, GraphQL, gRPC und anderen. Außerdem ermöglicht eine effektive API den Unternehmen, ihre Marketingstrategien zu beschleunigen, um ein neueres und breiteres Publikum zu erreichen.

Darüber hinaus bieten die APIs ein hohes Maß an Anpassungsfähigkeit. So kann sie an eine Vielzahl von Vorschriften angepasst werden und gleichzeitig die organisatorische Interoperabilität gewährleisten. Diese Faktoren treiben Unternehmen aller Größenordnungen dazu, auf APIs umzusteigen. Unternehmen benötigen jedoch einen integrierten Satz von Anwendungssicherheitsfunktionen sowie eine mühelose Bereitstellung ihrer APIs, die von Tools für den In-App-Schutz genutzt werden können. Mit Tools für den In-App-Schutz können Entwickler hochgradige Sicherheitsmaßnahmen in ihre APIs integrieren, wie z. B. die Implementierung starker Authentifizierungstechniken in Verbindung mit einer begrenzten Zugriffsrate, um zu verhindern, dass Hacker Daten von API-Servern abgreifen.

Lösungen für den In-App-Schutz erfüllen die wachsenden Anforderungen des dynamischen regulatorischen Umfelds

Bei der Auswahl/Übernahme von Lösungen für den In-App-Schutz achten Unternehmen auf die Einhaltung gesetzlicher Vorschriften wie PCI-DSS, HIPAA, NIS, GDPR, FISMA und ISO 27001, da diese Vorschriften Unternehmen dabei helfen, die Sicherheit zu verbessern und Informationsdiebstahl oder -missbrauch sowie die daraus resultierenden Strafen und negative Publicity zu verhindern. Die globalen Vorschriften werden immer komplexer, und die Unternehmen müssen sich auf die Schaffung einer starken Sicherheitsinfrastruktur und die Umsetzung von Erfolgsmodellen konzentrieren. Gemäß der EU-DSGVO muss das Unternehmen sicherstellen, dass Unternehmensdaten rechtmäßig erhoben werden, und diese Daten überwachen und vor Missbrauch und Ausbeutung schützen. Andernfalls droht eine Strafe. Daher müssen Unternehmen über alle sensiblen Daten und den Zugang zu ihnen Rechenschaft ablegen. Anwendungen enthalten und verarbeiten persönlich identifizierbare Informationen (PII) und sensible Daten wie z.B. Anmeldeinformationen der Benutzer, die von anfälligen mobilen Geräten aus abgegriffen werden können. Der In-App-

Schutz hilft Unternehmen, die strengen globalen Compliance-Standards zu erfüllen, um Sicherheitsverletzungen zu vermeiden und die Einhaltung globaler Vorschriften zu stärken.

Verstärkte Nutzung von Cloud-basierten Ressourcen und Anwendungen

Unternehmen setzen Cloud-basierte Ressourcen und Anwendungen ein, um kostengünstig zu sein, die Informationssicherheit zu verbessern, die Betriebseffizienz zu steigern und wettbewerbsfähig zu bleiben Die zunehmende Nutzung von Cloud-basierten Anwendungen und Diensten gefährdet in vielen Fällen die Sicherheit. Die Abhängigkeit von Cloud-basierten Plattformen von Drittanbietern stellt die Sicherheitsteams vor mehrere Herausforderungen, da sie sich auf die Sicherheitskontrollen und die Ausfallsicherheit eines Drittanbieter-Tools verlassen müssen. Lösungen für den In-App-Schutz unterstützen Unternehmen bei der Absicherung von On-Premise- und Cloud-basierten Anwendungen und Ressourcen gegen Cyber-Bedrohungen. Die Lösung für den In-App-Schutz hilft Unternehmen, sich einen Überblick über das Verhalten und die Aktivitäten von Anwendungen zu verschaffen und Anomalien aufzudecken, falls diese vorhanden sind.

COVID-19 Konsequenzen für die zunehmende Verbreitung von Tools für den In-App-Schutz

Die COVID-19-Pandemie hat Unternehmen dazu veranlasst, ihre Belegschaft durch die verstärkte Einführung von Heimarbeit und BYOD-Optionen (Bring Your Own Device) digital umzugestalten. Dies hat zwar den Fortbestand und sogar das Wachstum der Unternehmen gesichert, aber auch die Herausforderung mit sich gebracht, dass die Zahl der Bedrohungen durch Anwendungen zunimmt. Die Telearbeitskräfte sind schwer zu überwachen und zu managen. Und da ein Großteil der Mitarbeiter von zu Hause und von ihren eigenen ungesicherten Geräten aus arbeitet, werden ihre Aktivitäten und ihr Verhalten nicht mehr überwacht. Darüber hinaus ist ein massiver Anstieg der Nutzung zahlreicher Anwendungen für verschiedene Aktivitäten durch die von zu Hause aus arbeitenden Menschen zu verzeichnen. Die COVID-19-Pandemie hat dazu geführt, dass Unternehmen zunehmend den Nutzen einer Lösung für den In-App-Schutz erkennen. Da herkömmliche Technologien für die Verwaltung persönlicher Geräte und privater Netzwerke unzureichend sind, setzen Unternehmen auf Lösungen für den In-App-Schutz, um sich vor den Gefahren verschiedener Arten von Bedrohungen für hochwertige Anwendungen zu schützen.

Wettbewerbslandschaft und -analyse

Quadrant Knowledge Solutions hat eine eingehende Analyse der wichtigsten Anbieter von Produkten für den In-App-Schutz durchgeführt und dabei deren Produkte, Marktpräsenz und Wertversprechen bewertet. Die Bewertung basiert auf Primärforschung mit Experteninterviews, der Analyse von Anwendungsfällen und der internen Analyse des gesamten WAF-Marktes von Quadrant. Diese Studie umfasst Analysen der wichtigsten Anbieter, darunter Approov, Build38, Digital.ai, F5, Guardsquare, IBM, Imperva, Jscrambler, KOBIL GmbH, Lookout, OneSpan, PerimeterX, PreEmptive, Promon, Source Defense, Trustonic, Verimatrix und Zimperium.

OneSpan, Zimperium, Lookout, Verimatrix, Imperva, Trustonic, GuardSquare und Approov werden in der SPARK Matrix „In-App-Schutz 2022“ als globale Technologieführer identifiziert. Diese Unternehmen bieten eine hochentwickelte und umfassende Technologieplattform zum Schutz, zur Erkennung, Analyse und Beseitigung bekannter und unbekannter fortschrittlicher Cyber-Bedrohungen über den gesamten Lebenszyklus von Anwendungen. Die Plattform bietet Schutz in Echtzeit für hochwertige Anwendungen vor verschiedenen Bedrohungen wie Repackaging, Malware, Skript-Injektion, Cryptojacking, SMS-Snatching und Weiteren, sowie vor Bedrohungen durch eine unsichere Umgebung.

OneSpan bietet In-App-Schutz durch sein Produkt Mobile Application Shielding, das starke, nativ integrierte App-Sicherheit und Laufzeitschutz bietet. Es bietet Overlay-Erkennung, Jailbreak- und Root-Erkennung, Anti-Code-Injection, Anti-Keylogging, Anti-Repacking-Schutz, Debugger-Schutz, Verschleierung und weitere Funktionen zur Sicherung von Anwendungen. Darüber hinaus schützt das Produkt für den In-App-Schutz von OneSpan Apps vor Zero-Day-Angriffen, führt Apps sicher aus und bietet integrierten Schutz vor fremder Code-Injektion.

Zimperium schützt mobile Geräte und Anwendungen in Echtzeit und auf der Grundlage von maschinellem Lernen vor Bedrohungen, die auf Android, iOS und Chrome OS abzielen. Zimperium bietet eine Reihe von Modulen, darunter MAPS Mobile Application Protection Suite, zScan Application Security Testing, zKeyBox Cryptographic Key Protection, zShield Application Shielding und zDefend Runtime Application Self Protection, um mobile Anwendungen vor verschiedenen Arten von Bedrohungen zu schützen. Zimperium ermöglicht es Unternehmen, sich vor der Gefährdung privilegierter Daten und Infrastrukturen, vor Betrug und vor behördlichen Strafen zu schützen. Darüber hinaus bieten die Zimperium-Produkte verschiedene Funktionen wie App-Scanning, App-Shielding, Laufzeitschutz, Threat Management Dashboard und den Schutz sensibler kryptografischer Schlüssel in einer Plattform zur Erkennung und zum Schutz vor fortschrittlichen Bedrohungen.

Lookout bietet kontinuierliche Sicherheit für Anwendungen in Echtzeit und eine fortschrittliche Erkennung von mobilen Bedrohungen durch Lookout Embedded AppDefense. Lookout Embedded AppDefense ermöglicht es Anwendern, den Zustand mobiler Geräte in Echtzeit zu verfolgen - mit minimalem Programmieraufwand für das Lookout SDK - und liefert wichtige Informationen zur Beseitigung von Bedrohungen im Vorfeld. Lookout arbeitet mit Promon zusammen, um robuste Lösungen für den In-App-Schutz anzubieten, die statischen und Laufzeitschutz, Anti-Tempering von Apps und Schutz vor App-Reverse Engineering bieten.

Verimatrix bietet mit seinem Produkt App Shield einen automatisierten und intelligenten In-App-Schutz, der das Risiko menschlicher Fehler ausschließt. Verimatrix App Shield bietet automatische Anti-Tamper-Technologie, Umgebungsprüfungen und Code-Verschleierungsfunktionen, die Anwendungen vor bekannten und unbekannten Bedrohungen schützen. Darüber hinaus ermöglicht das Produkt Unternehmen, ihre Anwendungen vor Bedrohungen wie Reverse Engineering, Repackaging, dynamischer Modifikation, Man-in-the-Middle-Angriffen, Emulatoren und Debuggern sowie Jailbroken mit Root-Funktion zu schützen.

Trustonic bietet Sicherheitslösungen für intelligente Geräte und Anwendungen mit einem einzigartigen Ansatz, der die sicherheitskritischen Teile des Programms isoliert und sich auf deren Absicherung konzentriert. Trustonic verwendet eine vertrauenswürdige Ausführungsumgebung (Trusted Execution Environment, TEE), um den wichtigen Code auf Geräten mit erstklassiger Softwaresicherheit und Whitebox-Kryptografie auszuführen.

Die Anwendungssicherheit von Imperva bietet eine umfassende Reihe von Lösungen zum Schutz aller Arten von Anwendungen und APIs vor Cyber-Bedrohungen. Darüber hinaus ermöglicht die Lösung Unternehmen den Schutz von APIs vor den neuesten automatisierten Angriffen, wie z. B. Cloud WAF, erweiterter Bot-Schutz, Account-Takeover, Clientseitiger-Schutz, Laufzeitschutz und DDoS-Schutz.

GuardSquare bietet mit seinen Lösungen DexGuard, iXGuard, ThreatCast und ProGuard Sicherheit für iOS- und Android-Anwendungen. Die Lösungen bieten mehrere Ebenen der Codehärtung und des Selbstschutzes von Laufzeitanwendungen mit Echtzeittransparenz für iOS- und Android-Anwendungen, um verwertbare Erkenntnisse zu gewinnen. Guardsquare bietet auch ProGuard an, einen Open-Source-Shrinker für Java-Bytecode, der zur Verbesserung und Optimierung von Anwendungscode verwendet werden kann.

Approov ist ein aufstrebender Marktführer auf dem Gebiet des In-App-Schutzes. Approov bietet API Threat Protection Software an, um eine sichere Umgebung für APIs und Unternehmen zu schaffen. Approov blockiert den API-Zugriff von einem nicht autorisierten

Skript oder Tool ohne Fehlalarme, schützt Anwendungen vor Man-in-the-Middle-Angriffen durch dynamisches Zertifikats-Pinning und verhindert, dass gestohlene Geheimnisse von Skripten oder Tools für den Zugriff auf APIs verwendet werden. Approov verhindert, dass Schwachstellen in APIs zur Laufzeit ausgenutzt werden können, im Gegensatz zu SAST- oder DAST-Lösungen, die sich darauf konzentrieren, Entwicklern zu helfen, Schwachstellen vor der Bereitstellung zu beseitigen. Darüber hinaus bietet es Schutz vor Angriffen wie Kontoübernahme, gefälschte Kontoerstellung, Denial-of-Service, Kreditbetrug, App-Impersonation, Man-in-the-Middle, API-Sicherheitsverletzung und Scraping.

F5, Digital.ai, PerimeterX, IBM und die KOBIL GmbH gehören zu den wichtigsten Herausforderern. Diese Unternehmen verfügen über umfassende technologische Fähigkeiten und gewinnen auf dem globalen Markt für In-App-Schutz erheblich an Zugkraft. Diese Unternehmen sind sich der kommenden Markttrends bewusst und haben eine umfassende Roadmap aufgestellt, um künftige Wachstumschancen zu nutzen. Zu den anderen wichtigen Anbietern, die in der SPARK-Matrix 2022 erfasst sind, gehören Promon, Jscrambler, PreEmptive, Source Defense und Build38.

Alle in der SPARK-Matrix 2022 für In-App-Schutz erfassten Anbieter verbessern ihre Fähigkeiten zur Sicherung, Erkennung, Analyse und Behebung bekannter und unbekannter fortschrittlicher Cyber-Bedrohungen während des gesamten Anwendungslebenszyklus. Außerdem helfen sie Unternehmen, ihre Partnerschaftskanäle zu erweitern und verschiedene Anwendungsfälle zu unterstützen. Die Anbieter sind ständig bestrebt, die In-App-Schutzlösungen zu verbessern und die Unterstützung für einfache Bereitstellungsoptionen zu erweitern. Die Anbieter erweitern ihre Angebote ständig, um Verschleierungs- und Verschlüsselungstechniken mit Selbstschutz für Runtime-Anwendungen, Risikoanalysen, Anti-Tempering-Techniken, Multifaktor-Authentifizierung, biometrische Authentifizierung, Anti-Keylogging, Anti-Screen-Scraping, Whitebox-Kryptografie, Root / Jailbreak-Erkennung und weitere Funktionen zu bieten, die eine bessere Abschirmung von Anwendungen ermöglichen, um den Quellcode vor Repacking App-Cloning und Reverse Engineering zu schützen. Während herkömmliche Lösungen für den In-App-Schutz in der Regel eine Erkennung bieten, konzentrieren sich die Anbieter jetzt mehr auf die wichtigsten Komponenten, nämlich die Auswertung und Berichterstattung, um einen umfassenden Einblick in die Bedrohungslandschaft zu erhalten und Anwendungen vor Zero-Day-Angriffen zu schützen. Darüber hinaus konzentrieren sich die Anbieter auf die Vergrößerung ihres Kundenstamms, ihre geografische Präsenz, verschiedene Branchen und die Ausweitung der Unterstützung von Anwendungsfällen. Weiter versuchen sie auch, die Unterstützung für mehrere Bereitstellungsoptionen zu erweitern.

Wichtige Wettbewerbsfaktoren und technologische Unterscheidungsmerkmale

Die meisten führenden Anbieter von In-App-Schutz bieten Standardfunktionen wie Anwendungshärtung, Anti-Tempering, Selbstschutz von Anwendungen zur Laufzeit, Risikoanalyse und Authentifizierungsunterstützung. Die Flexibilität des Einsatzes kann jedoch bei den Angeboten der verschiedenen Anbieter unterschiedlich sein. Aufgrund des zunehmenden Wettbewerbs versuchen die Anbieter verstärkt ihre technologischen Fähigkeiten und ihr allgemeines Wertangebot zu verbessern, um wettbewerbsfähig zu bleiben. Einige der wichtigsten Wettbewerbsfaktoren und Unterscheidungsmerkmale für die Bewertung von Anbietern von In-App-Schutz sind wie folgt:

- **Die Möglichkeit der Ausgereiftheit der Technologie:** Unternehmen sollten eine umfassende Bewertung verschiedener Anbieter von In-App-Schutz durchführen, bevor sie eine Kaufentscheidung treffen. Die Benutzer sollten eine gewichtete Analyse durchführen, die auf den spezifischen Anforderungen ihres Unternehmens in Bezug auf die Überwachung, Filterung und Blockierung von bösartigem Datenverkehr basiert und gleichzeitig Schutz vor ausgeklügelten Cyber-Angriffen bietet. Die Anforderungen eines Unternehmens an den In-App-Schutz können je nach Branche, Schwachstellenmanagement für Anwendungen, Compliance-Anforderungen, gemeinsam verwalteten Diensten, Kundenerfahrung, Anwendungsfällen und Endbenutzergröße unterschiedlich sein. Unternehmen sollten Lösungen für den In-App-Schutz evaluieren, die Ende-zu-Ende-Funktionen zum Schutz ihrer mobilen Anwendungen während ihres gesamten Lebenszyklus bieten. Die Lösungen für den In-App-Schutz sollten alle Arten von Anwendungen, einschließlich mobiler Anwendungen, einseitiger Webanwendungen, Software und verbundener Geräte, bei der proaktiven Abwehr aller Arten von mobilen Bedrohungen unterstützen. Die Lösung sollte es den Anwendungen ermöglichen, sich gegen eine Vielzahl mobiler Bedrohungen wie Repackaging, Malware, Skript-Injektion, Kryptojacking, SMS-Grabbing und andere zu wehren. Außerdem sollte die Lösung Anwendungen in die Lage versetzen, sich vor verschiedenen fortschrittlichen Bedrohungen wie Malware, Code-Injektion, Screen Scrapping, Anwendungsklonen und Reverse Engineering zu schützen. Unternehmen können Lösungen für den In-App-Schutz evaluieren, die eine breite Palette von Authentifizierungsoptionen wie Verhaltensbiometrie, OTPs, Gesichtserkennung,

Fingerabdruckauthentifizierung, elektronische Signaturen und mehr bieten. Sie sollte eine ausgefeilte Technologie zur Abschirmung mobiler Anwendungen und eine mehrkanalige Authentifizierung über das mobile Gerät bieten. Benutzer sollten auch Lösungen für den In-App-Schutz für Funktionen wie Anti-Bot, Clickjacking, Laufzeitanwendungs-Selbstschutz und Anti-Tempering bewerten.

- **Reifegrad von KI und ML:** Die Fähigkeit von Anbietern von Lösungen für den In-App-Schutz, eingebettete KI- und maschinelle Lernfunktionen bereitzustellen, kann sehr unterschiedlich sein. Durch den Einsatz von KI und ML können Anbieter automatisch auf Angriffe reagieren und diese entschärfen sowie Angriffe verhindern, bevor sie Schaden anrichten. Anbieter setzen KI/ML-Technologie ein, um fortschrittliche Netzwerkanalysen, Benutzeranalysen und Bedrohungsdaten zu ermöglichen, um die Prozesse zur Eindämmung von Bedrohungen zu automatisieren und die Wirksamkeit des Anwendungsschutzes zu verbessern. Anwender sollten sich nach Anbietern umsehen, die KI/ML zur Erkennung von Bedrohungsmustern, zur umfassenden Risikoanalyse und zur Reaktion auf Bedrohungen in Echtzeit anbieten und so die Anwendungen der Anwender sichern.

- **Kompetenz und Fachwissen des Anbieters:** Unternehmen sollten eine umfassende Bewertung zahlreicher Lösungen und Anbieter für den In-App-Schutz durchführen, bevor sie eine endgültige Entscheidung treffen. Unternehmen sollten das Fachwissen und die Fachkenntnisse der Anbieter bewerten, um ihre speziellen Sicherheitsprobleme, Anwendungsfälle, Branchen- und regionsspezifischen Anforderungen zu verstehen. Die Benutzer sollten auf Anwenderfreundlichkeit, ein umfassendes Angebot, die Flexibilität der Software zur Anpassung an ständige Marktveränderungen und gesetzliche Vorschriften, die Minimierung der Gesamtbetriebskosten und Transparenz achten. Es wird auch empfohlen, Anbieter in Betracht zu ziehen, die erweiterte Funktionen wie die Prüfung von Anwendungen und Client-Umgebungen, dynamisches Zertifikats-Pinning für die Analyse von Traffic-Mustern die Erkennung von Bedrohungen und die Behebung von Problemen anbieten. Weiter sollten Nutzer auch nach Anbietern Ausschau halten, die fortschrittliche Funktionen wie automatisierte und intelligenzgesteuerte Lösungen für den In-App-Schutz zur Minimierung menschlicher Fehler, Echtzeit-Überwachung von Anwendungen und andere anbieten. Weiter empfiehlt es sich, nach einer Lösung zu suchen, die bereits erfolgreich in großem Maßstab eingesetzt wurde, und die vorhandenen Fallstudien zu diesen Einsätzen sorgfältig analysieren. Dies sollte die Grundlage für die Ausarbeitung bewährter

Verfahren für den Einsatz von Lösungen für den In-App-Schutz bilden.

- **Integration und Interoperabilität:** Die nahtlose Integration und Interoperabilität mit den bestehenden Technologien der Anbieter gehören zu den entscheidenden Faktoren, die sich auf die Technologieeinführung und die Erfahrungen der Nutzer auswirken. Eine Plattform für den In-App-Schutz sollte eine vollautomatische Integration mit den CI/CD-Tools des Anwenders für die Anwendungsentwicklung bieten, um einen umfassenden Schutz der Anwendungen während des gesamten Lebenszyklus zu gewährleisten. Benutzer sollten nach Anbietern Ausschau halten, die eine Integration mit Backend-Sicherheitsplattformen anbieten, einschließlich wichtiger API-Gateways, Cloud-nativer API-Gateways, WAF und anderer ergänzender Lösungen sowie mit Frameworks für die Entwicklung mobiler Anwendungen und Backends. Die Anbieter sollten auch eine einfache Integration mit Android- und iOS-Plattformen sowie plattformübergreifenden Entwicklungsumgebungen bieten und gemeinsame Autorisierungstechniken bereitstellen, die sowohl für die Web- als auch für die mobilen API-Kanäle verwendet werden können, um den rechtmäßigen Zugriff zu validieren.

- **Skalierbarkeit und Verfügbarkeit:** Die Anbieter von In-App-Schutz müssen auch bei hohem Datenaufkommen Schutz bieten, um eine Verfügbarkeit rund um die Uhr zu gewährleisten. Das Produkt für den In-App-Schutz muss in der Lage sein, jede beliebige Anwendung zu schützen, und muss API-Sicherheit und die Sicherheit von serverlosen Anwendungen unterstützen. Das Produkt sollte außerdem mit dem Unternehmen mitwachsen, um kontinuierlichen Schutz vor einer Vielzahl von Bedrohungen zu bieten. Benutzer sollten sich nach Anbietern von In-App-Schutz umsehen, die in der Vergangenheit bereits erfolgreich in großem Umfang eingesetzt wurden, und die vorhandenen Fallstudien zu diesen Einsätzen sorgfältig analysieren. Dies sollte die Grundlage für die Ausarbeitung von Best Practices für die Verwaltung von Einrichtungen für den In-App-Schutz bilden.

- **Technologie-Vision & Roadmap:** Die Benutzer müssen den geeigneten Technologiepartner entsprechend ihren spezifischen Anwendungsfällen, dem Risiko und der Roadmap für die digitale Transformation auswählen. Die Anbieter von In-App-Schutz verbessern und erneuern ständig ihr technologisches Leistungsversprechen über die traditionellen Erkennungsfunktionen hinaus, indem sie ML-basierte Lösungen für False Positives, dynamisches Zertifikats-Pinning und Laufzeitschutz vor API-Schwachstellen implementieren, die darüber hinaus Schutz vor Verschlüsselung, Repackaging von Anwendungen,

Reverse Engineering, Cryptojacking, Malware und Skript-Injektion bieten und Funktionen wie Anwendungshärtung, API-Schutz und vieles mehr. Unternehmen sollten die vorhandenen technologischen Fähigkeiten des Anbieters zusammen mit seiner technologischen Vision und Roadmap sorgfältig bewerten, um die Gesamtzufriedenheit und die Kundenerfahrung für den langfristigen Erfolg zu verbessern.

- **Umfassende Abdeckung von Anwendungsfällen:** Benutzer sollten eine gewichtete Analyse der verschiedenen Parameter durchführen, die für ihre Branchenbedürfnisse erforderlich sind, und nach breit gefächerten Anwendungsfällen Ausschau halten, die Credential Stuffing-Angriffe blockieren, API-Missbrauch durch Bots und Skripte blockieren, Man-in-the-Middle-Angriffe blockieren, App-Impersonation und Denial-of-Service-Angriffe verhindern. Darüber hinaus wird Nutzern mit einer oder mehreren spezifischen Anforderungen empfohlen, Lösungen für den In-App-Schutz unter Berücksichtigung folgender Aspekte zu bewerten die differenzierenden Strategien der Anbieter, zu denen die Skalierung des Netzwerks, die Zeit bis zum Schutz und die flexiblen Bereitstellungsoptionen, einschließlich öffentlicher, privater und hybrider Clouds, gehören können. Die Nutzer müssen Anbieter sorgfältig prüfen, die Transparenz und Berichterstattung für verschiedene Schichten der Sicherheitsinfrastruktur bieten.

SPARK Matrix™: Strategische Leistungsbewertung und Ranking

Die SPARK-Matrix von Quadrant Knowledge Solutions liefert eine Momentaufnahme der Marktpositionierung der wichtigsten Marktteilnehmer. Die SPARK-Matrix bietet eine visuelle Darstellung der Marktteilnehmer und liefert strategische Erkenntnisse darüber, wie jeder Anbieter im Vergleich zu seinen Konkurrenten abschneidet, und zwar in Bezug auf verschiedene Leistungsparameter, die auf der Kategorie der Technologie-Exzellenz und der Kundenwirkung basieren. Die Analyse der Wettbewerbslandschaft von Quadrant ist ein nützlicher Planungsleitfaden für strategische Entscheidungen, z. B. bei der Suche nach M&A-Perspektiven, Partnerschaften, geografischer Expansion, Portfolioerweiterung usw.

Jeder Marktteilnehmer wird im Hinblick auf mehrere Parameter der Technologie-Exzellenz und der Kundenwirkung analysiert. Für jeden der Parameter (siehe Diagramme) wird jedem Anbieter ein Index von 1 (niedrigster Wert) bis 10 (höchster Wert) zugewiesen. Diese Bewertungen werden jedem Marktteilnehmer auf der Grundlage der Forschungsergebnisse zugewiesen. Auf der Grundlage der Bewertungen der einzelnen Teilnehmer werden die X- und Y-Koordinatenwerte berechnet. Diese Koordinaten werden schließlich zur Erstellung der SPARK-Matrix verwendet.

Technologie-Exzellenz	Gewichtung
Ausgereiftheit der Technologie	20 %
Strategie zur Differenzierung im Wettbewerb	20 %
Anwendungsvielfalt	15 %
Skalierbarkeit	15 %
Integration und Interoperabilität	15 %
Vision und Roadmap	15 %

Kundenwirkung	Gewichtung
Produktstrategie und Leistung	20 %
Marktpräsenz	20 %
Nachgewiesene Aufzeichnung	15 %
Einfacher Einsatz und Nutzung	15 %
Hervorragender Kundenservice	15 %
Einzigartiges Wertversprechen	15 %

Kriterien für die Bewertung: Technologie-Exzellenz

- **Anwendungsvielfalt:** Die Fähigkeit, den Einsatz des Produkts für eine Reihe von vertikalen Branchen und/oder mehrere Anwendungsfälle zu demonstrieren.

- **Skalierbarkeit:** Die Fähigkeit nachzuweisen, dass die Lösung eine Skalierbarkeit auf Unternehmensebene unterstützt, zusammen mit Kundenbeispielen.

- **Integration und Interoperabilität:** Die Fähigkeit, eine Produkt- und Technologieplattform anzubieten, die die Integration mit mehreren Best-of-Breed Technologien, bietet vorgefertigte, sofort einsetzbare Integrationen sowie offene API-Unterstützung und -Dienste.

- **Vision und Roadmap:** Bewertung der Produktstrategie und der Roadmap des Anbieters mit einer Analyse der wichtigsten geplanten Verbesserungen, um überlegene Produkte/Technologie anzubieten und die Kundenerfahrung zu verbessern.

Bewertungskriterien: Kundenwirkung

- **Produktstrategie und Leistung:** Bewertung mehrerer Aspekte der Produktstrategie und -leistung im Hinblick auf Produktverfügbarkeit, Preis-/Leistungsverhältnis, hervorragende GTM-Strategie und andere produktspezifische Parameter.

- **Marktpräsenz:** Die Fähigkeit, Einnahmen, Kundenstamm und Marktwachstum zusammen mit einer Präsenz in verschiedenen geografischen Regionen und vertikalen Branchen nachzuweisen.

- **Nachgewiesene Aufzeichnung:** Bewertung des bestehenden Kundenstamms aus dem SMB-, Mid- market- und Großunternehmenssegment, Wachstumsrate und Analyse der Kundenfallstudien.

- **Einfacher Einsatz und Nutzung:** Die Fähigkeit, den Kunden eine überragende Erfahrung bei der Bereitstellung zu bieten, die eine flexible Bereitstellung unterstützt, oder eine überragende Erfahrung bei Kauf, Implementierung und Nutzung nachzuweisen. Darüber hinaus werden die Produkte der Anbieter daraufhin analysiert, ob sie eine anwenderfreundliche Benutzeroberfläche und ein angenehmes Nutzungserlebnis bieten.

- **Hervorragender Kundenservice:** Die Fähigkeit, die Fähigkeit von Anbietern nachzuweisen, eine Reihe von professionellen Dienstleistungen in den Bereichen Beratung, Schulung und Support anzubieten. Darüber hinaus wird auch die Strategie des Unternehmens in Bezug auf Dienstleistungspartner oder die Fähigkeit zur Systemintegration in verschiedenen geografischen Regionen berücksichtigt.

- **Einzigartiges Wertversprechen:** Die Fähigkeit, einzigartige Unterscheidungsmerkmale aufzuzeigen, die durch aktuelle Branchentrends, Branchenkonvergenz, technologische Innovationen und andere Faktoren bedingt sind.

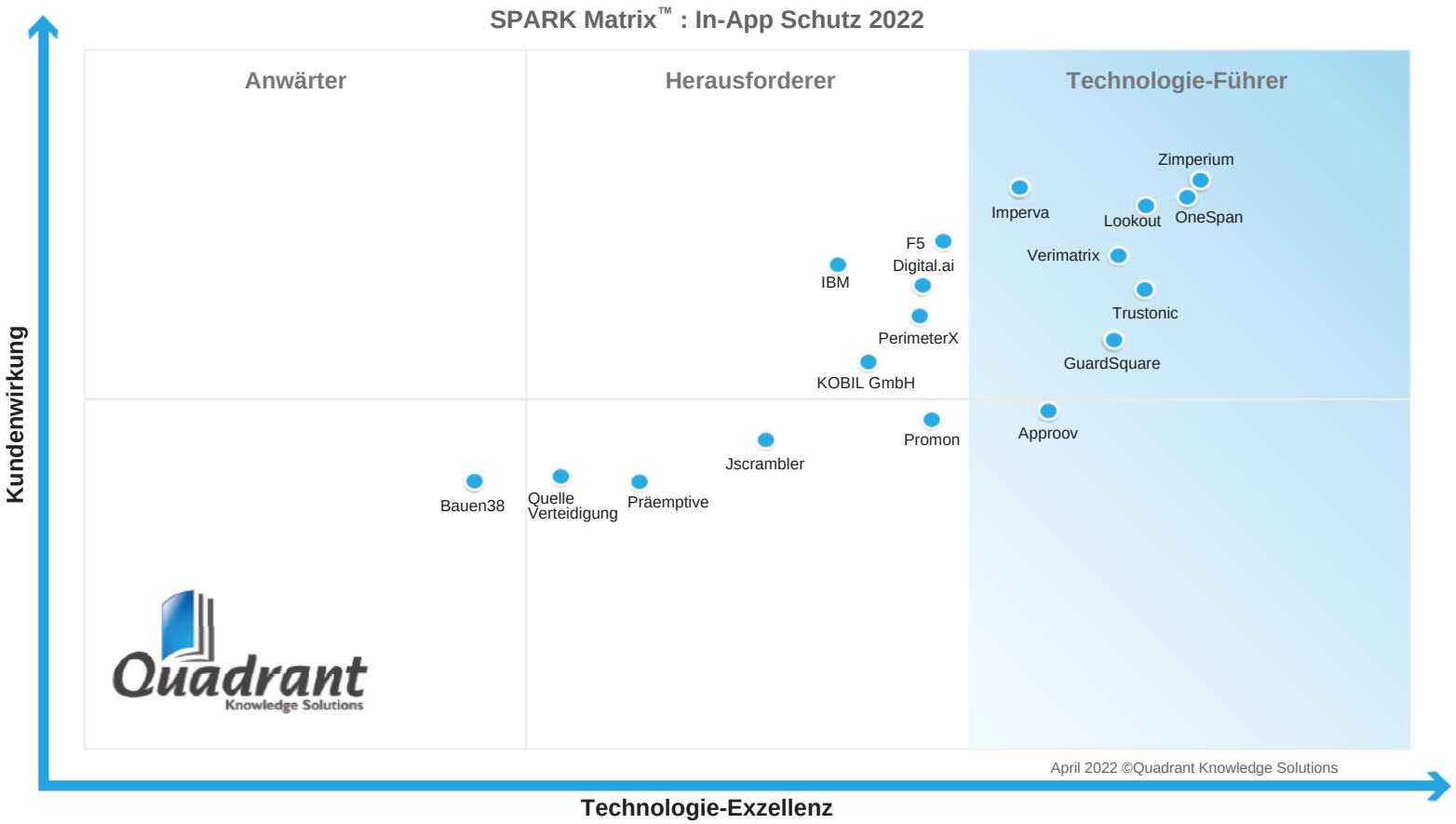
SPARK Matrix™: In-App-Schutz 2022

Strategische Leistungsbewertung und Ranking

Abbildung: 2022 SPARK Matrix™

(Strategische Leistungsbewertung und Ranking)

Markt für In-App-Schutz



Anbieterprofil

Nachfolgend finden Sie die Profile der führenden Anbieter von In-App-Schutz, die weltweit tätig sind. Die folgenden Anbieterprofile wurden auf der Grundlage von Informationen verfasst, die von den Führungskräften des Anbieters im Rahmen des Forschungsprozesses zur Verfügung gestellt wurden, sowie auf der Grundlage öffentlich zugänglicher Informationen. Das Quadrant-Forschungsteam hat sich bei der Erstellung des Profils auch auf die Website des Unternehmens, Whitepapers, Blogs und andere Quellen bezogen. Ein detailliertes Anbieterprofil und eine Analyse aller Anbieter, zusammen mit verschiedenen Wettbewerbsszenarien, sind als kundenspezifische Forschungsergebnisse für unsere Kunden erhältlich. Den Benutzern wird empfohlen, direkt mit den jeweiligen Anbietern in Kontakt zu treten, um ein umfassenderes Verständnis ihrer technischen Möglichkeiten zu erlangen. Anwendern wird empfohlen, Quadrant Knowledge Solutions zu konsultieren, bevor sie Kaufentscheidungen in Bezug auf Technologien für den In-App-Schutz und die Auswahl von Anbietern auf der Grundlage der in diesem Forschungsdienst enthaltenen Forschungsergebnisse treffen.

Zimperium

URL: www.zimperium.com

Zimperium wurde 2010 gegründet und hat seinen Hauptsitz in Dallas, Texas, USA. Das Unternehmen ist ein führender Anbieter von mobilen Sicherheitslösungen, die mobile Geräte und Anwendungen vor komplexen mobilen Bedrohungen schützen. Das Unternehmen bietet Echtzeit-, geräte- und maschinenlernbasierten Schutz für mobile Geräte und Anwendungen vor Bedrohungen wie Geräte-, Netzwerk-, Phishing- und bösartigen App-Angriffen auf Android-, iOS- und Chromebook-Betriebssysteme, mobile Endgeräte und Apps. Zimperium bietet seine Lösungen für den In-App-Schutz für mobile Geräte über seine Produkte an, darunter Mobile Application Protection Suite (MAPS), ZScan, ZKeyBox, ZShield und ZDefend.

Zimperium MAPS ermöglicht es Unternehmen, Compliance-Risiken bereits in der Entwicklungsphase von Apps zu erkennen und Apps während der Nutzung zu überwachen und vor Angriffen zu schützen. Zimperium MAPS bietet Unterfunktionen zum Schutz des Lebenszyklus von mobilen Anwendungen wie zScan, zKeyBox, zShield und zDefend. Zimperium zScan ermöglicht Entwicklern die Suche und Behebung von Compliance-, Datenschutz- und Sicherheitsproblemen in der Entwicklungsphase. Zimperium zKeyBox sichert kryptographische Schlüssel und verhindert, dass sie entdeckt, extrahiert oder manipuliert werden. Zimperium zShield schützt Anwendungen vor Reverse Engineering, Code-Manipulation, Datenschutz, Extraktion von Assets, Extraktion von API-Schlüsseln und Malware-Injektion mit Hilfe von Verschleierungs- und Anti-Manipulationsfunktionen. Zimperium bietet das SDK zDefend zur Erkennung und zum Schutz vor Geräte-, Netzwerk-, Phishing- und Malware-Angriffen.

Zimperium zScan unterstützt Entwickler bei der automatischen Identifizierung von Datenschutz-, Sicherheits- und Compliance-Problemen während des Entwicklungsprozesses, bevor die Anwendungen für die Öffentlichkeit freigegeben werden. zScans Binäranalyse erkennt Schwachstellen im Programm, die ein Angreifer ausnutzen könnte. Darüber hinaus dokumentiert zScan Risiken innerhalb mobiler Apps wie hardwarespezifische Nutzung, unsichere API-Aufrufe und den Umgang mit sensiblen Daten, ermöglicht das Scannen von Apps direkt aus der Build-Pipeline oder den manuellen Upload in die Verwaltungskonsole und ermöglicht es Compliance- und Sicherheitsteams, Richtlinien zu definieren und anzupassen, um sicherzustellen, dass nur die zutreffenden Ergebnisse geöffnet werden. Darüber hinaus erkennt die zScan-Funktion „Build Compare“ sofort, ob die Risiken in jeder nachfolgenden Version steigen oder fallen. Unternehmen können Versionsvergleiche nutzen, um den Fortschritt bei der Einhaltung von Vorschriften zu verfolgen und robustere mobile Anwendungen zu erstellen.

Zimperium zKeyBox verwendet White-Box-Kryptografie, um Schlüssel, Geheimnisse und standardmäßige oder benutzerdefinierte kryptografische Algorithmen auf jeder Plattform innerhalb der mobilen Anwendung zu schützen. zKeyBox stellt sicher, dass die Schlüssel niemals offengelegt werden und die Ausführungslogik nicht zurückverfolgt werden kann. zKeyBox modifiziert und verbirgt kryptografische Algorithmen, ohne die Schlüssel zu gefährden, selbst wenn das Gerät kompromittiert wurde. Darüber hinaus ist Zimperium nicht auf die von der zugrundeliegenden Plattform bereitgestellte Hardware angewiesen, um die Einhaltung gesetzlicher Vorschriften zu unterstützen. Zimperium bietet eine hervorragende Leistung auf einer Vielzahl von Architekturen und verfügt über umfassende kryptografische Erfahrung, um die Benutzer in jeder Phase der Anwendungsimplementierung zu unterstützen.

Zimperium zShield schützt den Quellcode, das geistige Eigentum (IP) und die Daten innerhalb der Anwendung vor Bedrohungen, indem es die Anwendung durch leistungsstarke Verschleierungs- und Anti-Manipulations-Funktionen abhärtet und schützt. zShield bietet Schutz vor Reverse Engineering, Advanced Obfuscation, Anti-Debugging, Binary Packing und Diversification. Darüber hinaus bietet zShield Anti-Tempering-Funktionen, einschließlich Integritätsprüfung, Anti-Methoden-Swizzling, Funktionsaufrufer-Verifizierung, Jailbreak-/Root-Erkennung, Cross-Checking von gemeinsam genutzten Bibliotheken, Mach-O-Binärsignatur-Verifizierung, Google Play-Lizenzierungsschutz und anpassbare Verteidigungsmaßnahmen.

Zimperium's zDefend verhindert die Ausnutzung auf dem Gerät, unterstützt Unternehmen bei der Erlangung von Laufzeit-Transparenz von Bedrohungen und ermöglicht es mobilen Anwendungen, sich gegen mobile Bedrohungen in Echtzeit zu verteidigen. Die patentierte, auf maschinellem Lernen basierende Mobile Threat Defense Engine z9 von Zimperium wird in zDefend eingesetzt. Als Software Development Kit kann die Lösung leicht in jede iOS- oder Android-Anwendung (SDK) integriert werden. Darüber hinaus unterstützt zDefend den umfassenden Schutz von Geräten durch dynamische Reaktion auf Bedrohungen, Transparenz von Bedrohungen, Integration von Sicherheits-Ökosystemen wie SIEM, SOAR und Incident Response sowie flexible Bereitstellungsmodelle und einfache Implementierung.

Analystenperspektive

Es folgt eine Analyse der Fähigkeiten von Zimpreium auf dem globalen Markt für In-App-Schutz:

- Zimperium bietet Module wie die Mobile Application Protection Suite (MAPS), Zscan, ZKeyBox, ZShield und ZDefend, die vor verschiedenen Arten von

Anwendungsbedrohungen schützen. Zimperium MAPS bietet Ende-zu-Ende-Schutz für mobile Anwendungen, von der Entwicklung bis zur Bereitstellung.

MAPS bietet außerdem App-Scanning, App-Shielding, Laufzeitschutz und den Schutz sensibler kryptografischer Schlüssel in einer einzigen Plattform. Das integrierte Dashboard für das Bedrohungsmanagement von MAPS ermöglicht einen Echtzeit-Überblick über die Bedrohungen und die Fähigkeit, auf entdeckte Bedrohungen und Angriffe zu reagieren.

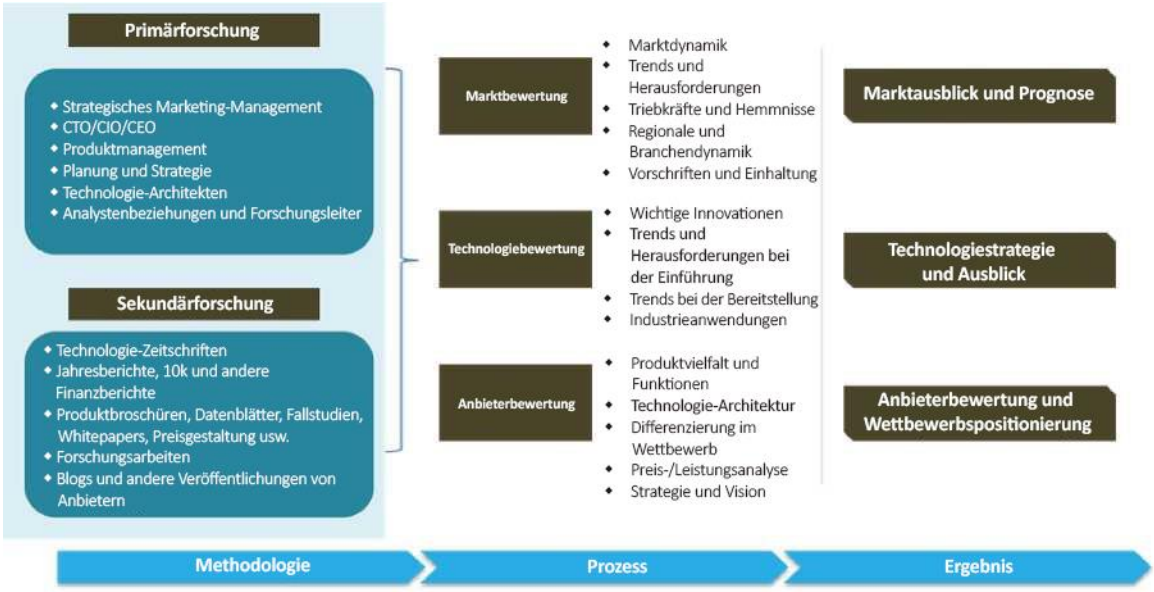
- Was die geografische Präsenz anbelangt, so ist Zimperium in den USA und Europa stark vertreten, gefolgt von anderen EMEA- und APAC-Regionen. Das Unternehmen ist zwar in einer Vielzahl von Branchen vertreten, doch zu den wichtigsten gehören Banken und Finanzdienstleistungen, Behörden und öffentlicher Sektor, IT und Telekommunikation, Fertigung, Gesundheitswesen und Biowissenschaften, Einzelhandel, E-Commerce und Versicherungen. Aus Sicht der Anwendungsfälle unterstützt Zimperium Zero Trust, mobiles EDR, mobilen Phishing-Schutz, mobile DevSecOps und Compliance.

- Zu den wichtigsten Herausforderungen von Zimperium gehört der wachsende Wettbewerb durch neue Anbieter mit innovativen Technologieangeboten. Diesen Anbietern gelingt es, eine starke Marktposition zu erlangen und die Marktdurchdringung bei kleinen bis mittleren Unternehmen zu erhöhen. Sie gehören zu den Hauptzielen für Fusionen und Übernahmen. Mit seinen umfassenden funktionalen Fähigkeiten, der überzeugenden technologischen Differenzierung und dem soliden Kundenwertangebot ist Zimperium jedoch gut positioniert, um seinen Marktanteil im mittleren bis großen Unternehmenssegment zu halten und auszubauen.

- Im Rahmen seiner Technologie-Roadmap investiert Zimperium in die Verbesserung seiner Fähigkeiten, die Sicherung seiner Position als Plattform für den Schutz mobiler Apps, die Erhöhung der Kundenzahl, die geografische Präsenz, verschiedene Branchen und die Ausweitung der Unterstützung von Anwendungsfällen.

Forschungsmethodologien

Quadrant Knowledge Solutions verwendet einen umfassenden Ansatz, um die globalen Marktaussichten für verschiedene Technologien zu erforschen. Der Forschungsansatz von Quadrant bietet unseren Analysten den effektivsten Rahmen zur Identifizierung von Markt- und Technologietrends und hilft bei der Formulierung sinnvoller Wachstumsstrategien für unsere Kunden. Alle Abschnitte unseres Forschungsberichts werden mit einer beträchtlichen Menge an Zeit und Überlegung vorbereitet, bevor wir zum nächsten Schritt übergehen. Nachfolgend finden Sie eine kurze Beschreibung der wichtigsten Abschnitte unserer Forschungsmethoden.



Sekundärforschung

Im Folgenden werden die wichtigsten Informationsquellen für die Durchführung von Sekundärforschung genannt:

Die interne Datenbank von Quadrant

Quadrant Knowledge Solutions unterhält eine firmeneigene Datenbank auf verschiedenen Technologiemärkten. Diese Datenbank bietet unserem Analysten eine angemessene Grundlage, um das Forschungsprojekt in Gang zu bringen. Diese Datenbank enthält Informationen aus den folgenden Quellen:

- Jahresberichte und andere Finanzberichte
- Teilnehmerlisten der Industrie

- Veröffentlichte Sekundärdaten über Unternehmen und ihre Produkte
- Datenbank mit Marktgrößen und Prognosedaten für verschiedene Marktsegmente
- Wichtige Markt- und Technologietrends

Literaturrecherche

Quadrant Knowledge Solutions nutzt mehrere abonnierte Zeitschriften und andere Publikationen, die eine breite Palette von Themen im Zusammenhang mit der Technologieforschung abdecken. Wir nutzen auch die umfangreiche Bibliothek von Verzeichnissen und Zeitschriften zu verschiedenen Technologiebereichen. Unsere Analysten verwenden Blogbeiträge, Whitepapers, Fallstudien und andere Literatur, die von großen Technologieanbietern, Online-Experten und Branchenzeitschriften veröffentlicht werden.

Beiträge von Teilnehmern aus der Industrie

Die Quadrant-Analysten sammeln relevante Dokumente wie Whitepaper, Broschüren, Fallstudien, Preislisten, Datenblätter und andere Berichte von allen wichtigen Branchenteilnehmern.

Primärforschung

Die Analysten von Quadrant verwenden einen zweistufigen Prozess für die Durchführung von Primärforschung, der uns dabei hilft, aussagekräftige und möglichst genaue Marktinformationen zu erfassen. Im Folgenden wird der zweistufige Prozess unserer Primärforschung beschrieben:

Schätzung des Marktes: Auf der Grundlage des Top-down- und Bottom-up-Ansatzes analysiert unser Analyst alle Branchenteilnehmer, um ihr Geschäft auf dem Technologiemarkt für verschiedene Marktsegmente zu schätzen. Wir holen auch Informationen und Nachweise über die Geschäftsentwicklung unserer Kunden im Rahmen unserer Primärforschungsinterviews oder durch einen detaillierten Marktfragebogen ein. Das Quadrant-Forschungsteam führt eine detaillierte Analyse der von den Branchenteilnehmern abgegebenen Kommentare und Beiträge durch.

Kundeninterview: Das Analystenteam von Quadrant führt ein ausführliches Telefoninterview mit allen wichtigen Branchenteilnehmern, um deren Ansichten über die aktuelle und zukünftige Marktdynamik zu erfahren. Unsere Analysten erhalten auch Erfahrungen aus erster Hand mit der Produktdemo des Anbieters, um die technologischen

Fähigkeiten, die Benutzererfahrung, die Produktmerkmale und andere Aspekte zu verstehen. Auf der Grundlage der Anforderungen befragen die Quadrant-Analysten mehrere Personen von jedem Marktteilnehmer, um die Richtigkeit der bereitgestellten Informationen zu überprüfen. Wir engagieren in der Regel mit dem Personal des Kunden in einer der folgenden Funktionen:

- Strategisches Marketing-Management
- Produktmanagement
- Produktplanung
- Planung und Strategie

Feedback von Vertriebspartnern und Endverbrauchern

Das Quadrant-Forschungsteam recherchiert bei verschiedenen Vertriebskanalpartnern, einschließlich Distributoren, Systemintegratoren und Beratern, um die detaillierte Perspektive des Marktes zu verstehen. Unsere Analysten holen auch das Feedback von Endbenutzern aus verschiedenen Branchen und Regionen ein, um die wichtigsten Probleme, Technologietrends und Anbieterkapazitäten auf dem Technologiemarkt zu verstehen.

Datenanalyse: Marktprognose und Wettbewerbsanalyse

Das Analystenteam von Quadrant sammelt alle notwendigen Informationen aus der Sekundär- und Primärforschung in einer Computerdatenbank. Diese Datenbanken werden anschließend analysiert, verifiziert und auf vielfältige Weise miteinander verglichen, um ein genaues Bild des Gesamtmarktes und seiner Segmente zu erhalten. Nach der Analyse aller Marktdaten, Branchentrends, Markttrends, Technologietrends und Schlüsselthemen erstellen wir vorläufige Marktprognosen. Diese vorläufige Marktprognose wird anhand verschiedener Marktszenarien, Wirtschaftsszenarien, Branchentrends und wirtschaftlicher Dynamik getestet. Schließlich kommt das Analystenteam zu einem möglichst genauen Prognoseszenario für den Gesamtmarkt und seine Segmente.

Zusätzlich zu den Marktprognosen führt unser Team eine detaillierte Überprüfung der Branchenteilnehmer durch, um eine Analyse der Wettbewerbslandschaft und der Marktpositionierung sowohl für den Gesamtmarkt als auch für verschiedene Marktsegmente zu erstellen.

SPARK-Matrix:
Strategische Leistungsbewertung und Ranking

Die SPARK-Matrix von Quadrant Knowledge Solutions liefert eine Momentaufnahme der Marktpositionierung der wichtigsten Marktteilnehmer. Die SPARK-Matrix bietet eine visuelle Darstellung der Marktteilnehmer und liefert strategische Erkenntnisse darüber, wie jeder Anbieter im Vergleich zu seinen Konkurrenten rangiert, und zwar in Bezug auf verschiedene Leistungsparameter, die auf der Kategorie der Technologie-Exzellenz und der Kundenwirkung basieren.

Erstellung des Abschlussberichts

Nach der Fertigstellung der Marktanalyse und der Prognosen erstellt unser Analyst die notwendigen Grafiken, Diagramme und Tabellen, um weitere Einblicke zu erhalten und den endgültigen Forschungsbericht vorzubereiten. Unser abschließender Forschungsbericht enthält Informationen wie Marktprognosen, Wettbewerbsanalysen, wichtige Markt- und Technologietrends, Markttreiber, Anbieterprofile und vieles mehr.

Kundenbetreuung

Für Informationen über gedruckte oder elektronische Nachdrucke wenden Sie sich bitte an die Kundenbetreuung unter rmehar@quadrant-solutions.com | www.quadrant-solutions.com