SPARK Matrix™

Security & Risk Management

SPARK Matrix™: Risk-Based Authentication (RBA), 2021

Market Insights, Competitive Evaluation, and Vendor Rankings

June 2021

Quadrant Knowledge Solutions

Table of Contents

Executive Overview

This research service includes a detailed analysis of the global Risk-Based Authentication (RBA) solution market dynamics, major trends, vendor landscape, and competitive positioning analysis. The study provides a comprehensive competition analysis and ranking of the leading RBA vendors in the form of the SPARK Matrix. This research provides strategic information for technology vendors to better understand the market supporting their growth strategies and for users to evaluate different vendors' capabilities, competitive differentiation, and market position.

Key Research Findings

Followings are the key research findings:

Technology Trends

RBA vendors continue to strengthen their risk engine by integrating extensively with industry consortium or third-party risk signal providers. Vendors are continuously leveraging artificial intelligence, machine learning, and advanced analytics to offer real-time monitoring and analysis of extensive data feeds, fine-tuning risk models to accommodate new intelligence, and accurate determination of risk scores for users and transactions. Vendors are also ensuring seamless and secure access by using various biometric authentication techniques.

Key Market Drivers Trends:

- The market drivers for the growth in RBA solutions include continued investments in digital transformation projects leading to increased online availability across verticals, increase in remote working, increased use of mobile and personal devices, and pandemic-related increase in online fraud. All these factors are driving the need for secured authentication solutions that offer a seamless customer experience.
- Driven by the growing demand for adaptive authentication solutions, most of the leading IAM vendors are offering RBA capability, either through an in-house risk engine or by integrating with third-party risk service providers. There are also many niche players that are offering industry-specific expertise, such as for e-commerce.
- With disrupted business scenarios, increase in remote working, and rise in online activity and frauds, a robust authentication mechanism is the need of the hour in this time of the Covid-19 pandemic. Critical investments in RBA solutions are postulated to grow, with organizations focusing more on security

and seamless user experience being the new long-term strategy to lock in customers for the long haul.

- The robust value proposition of the RBA solution involves providing a robust risk scoring engine, rule management, authentication mechanism, user self-service, alert and case management, and visualization and reporting. The continuous transformation of RBA solution driven by advanced technologies are driving the market adoption amongst the large enterprises.

Competition Dynamics & Trends:

- This study includes analysis of key vendors, including Accops, Appgate, Broadcom, CoffeeBean Technology, CyberArk, Duo Security (CISCO), ForgeRock, IBM, Kount, LexisNexis Risk Solution, Microsoft, Okta, OneLogin, OneSpan, Ping Identity, RSA, SecureAuth, Silverfort, Swivel Secure, and TransUnion.

- IBM, Kount, Ping Identity, LexisNexis Risk Solution, Okta, Microsoft, Appgate, and OneSpan are the top performers in the global RBA market and have been positioned as the top technology leaders in the 2021 SPARK Matrix analysis of the RBA market. TransUnion has been positioned as emerging technology leaders with their overall technology value proposition.

Market Overview and Technology Trends

Quadrant Knowledge Solutions defines RBA as:

"Risk Based-Authentication (RBA), also known as Adaptive Authentication is a form of a powerful authentication process that utilizes a set of rules to calculate risk scores by considering comprehensive factors such as IP address, browser, physical location, user role, behavior, devices type, day/time, consecutive login failure and such others prior to granting access. The RBA solution offers an aggregate risk score for each user login and enforces flexible authentication based on those risk scores."

RBA solutions eliminate fraud by calculating the risk level for every access request and then deciding the level of authentication needed for each login/ transaction. RBA helps alleviate various types of frauds like ATO fraud, payment fraud, mobile fraud, phishing, and cyber threats like botnet attacks by enforcing authentication according to the level of risk entailed.

Before RBA, static authentication was the most popular and till-date widely used technique. As the name suggests, organizations use the same authentication method for all customers and transactions- using usernames and passwords. Despite being predominantly used, static authentication has many challenges. Users often choose simple passwords as they are easy to remember, thereby increasing the risk of fraud. If they choose a difficult password, it becomes hard to memorize it, and they resort to unsecured methods like writing it down, making it vulnerable to thefts. Both scenarios involve the usage of frail, commonly used, and badly stored usernames and passwords, which makes it easier for cybercriminals to hack and exploit the system.

The effectiveness of the static authentication systems has been further challenged by an unprecedented rise in cyberattacks fueled by the digitalization of businesses, remote working, increased online activity, and increased adoption of BYOD/ WYOD policies. Also, technological advancements are making it possible for cybercriminals to find new and innovative ways to launch high-volume and complex fraud attacks. Therefore, organizations are continuously embracing sophisticated technologies such as RBA for enhanced security to operate smoothly in these challenging environments.

RBA solutions offer a robust authentication mechanism to help determine the risk level and possibility of fraud. It adds an additional layer of security before providing access by assessing the level of risk. The risk assessment is based on various contextual factors like IP address, user behavior and role, device and network details, physical location, geo-velocity (physical distance between consecutive login attempts), day of the week, time of day, consecutive login failures, and so on. For login attempts with a high-risk score, the user is prompted for more authentication steps to confirm and validate its identity. Also, if the risk score is low and the user is behaving in an expected

way, then the system will include fewer steps while authenticating the user. RBA solutions commonly use multi-factor authentication (MFA) to secure the identity of an individual and deter hackers. Instead of simply requesting a username and password, MFA requires an additional verification factor, which diminishes the probability of a cyber-attack. While enforcing stringent authentication for malicious and high-risk users, RBA ensures simplified access for trusted users. By balancing security and user experience, RBA is gaining popularity amongst organizations across a range of verticals.

Following are the key capabilities of an RBA solution:

- **Risk Scoring Engine**- Risk scoring is the most important capability of Risk-Based Authentication (RBA) solutions. Risk scoring is the process of assessing the risk associated with each access request by generating a risk score based on user behavioral patterns and factors like device, location, browsing time, IP address, network type, time of the day, login activity, and such others. Thus, the risk scoring engine utilizes contextual factors related to access attempts or transactions to better estimate the risk involved. Based on the risk score, the system decides the level of authentication needed. For transactions or access requests with a high-risk score, the system prompts additional authentication steps or may block access. On the contrary, a low-risk score indicates trusted users, and the system lowers authentication level to offer seamless access to such users. This extra level of security makes it difficult for hackers and fraudsters to gain any unauthorized access.

- **Rule Management**- Rule management, also known as policy management, facilitates the kind of steps that the RBA solution must take. In rule management, authentication for each of the customer logins is provided based on the risk scores, which could be low, medium, and high. Some RBA solutions have an inbuilt rule in which the software defines certain cut-offs or ranges. Many customers are looking for customizable rule management, where an organization can make their own rules depending on how much risk they can accept depending on customers and situations. Additionally, there can be a combination of both, where the software may have its default rule along with that one can customize the same as per the requirement.

- **Authentication Mechanism (MFA)**- Risk-Based Authentication or Adaptive Authentication solution offers varied levels of authentication based on the risk level. RBA solution vendors offer Multi-Factor Authentication (MFA). MFA is an authentication method that enforces two or more verification steps before granting access to an account or application. It provides additional security from identity theft, data breaches, cyberattacks, etc. MFA involves multiple authentication steps to verify that the user is who he claims to be. To identify

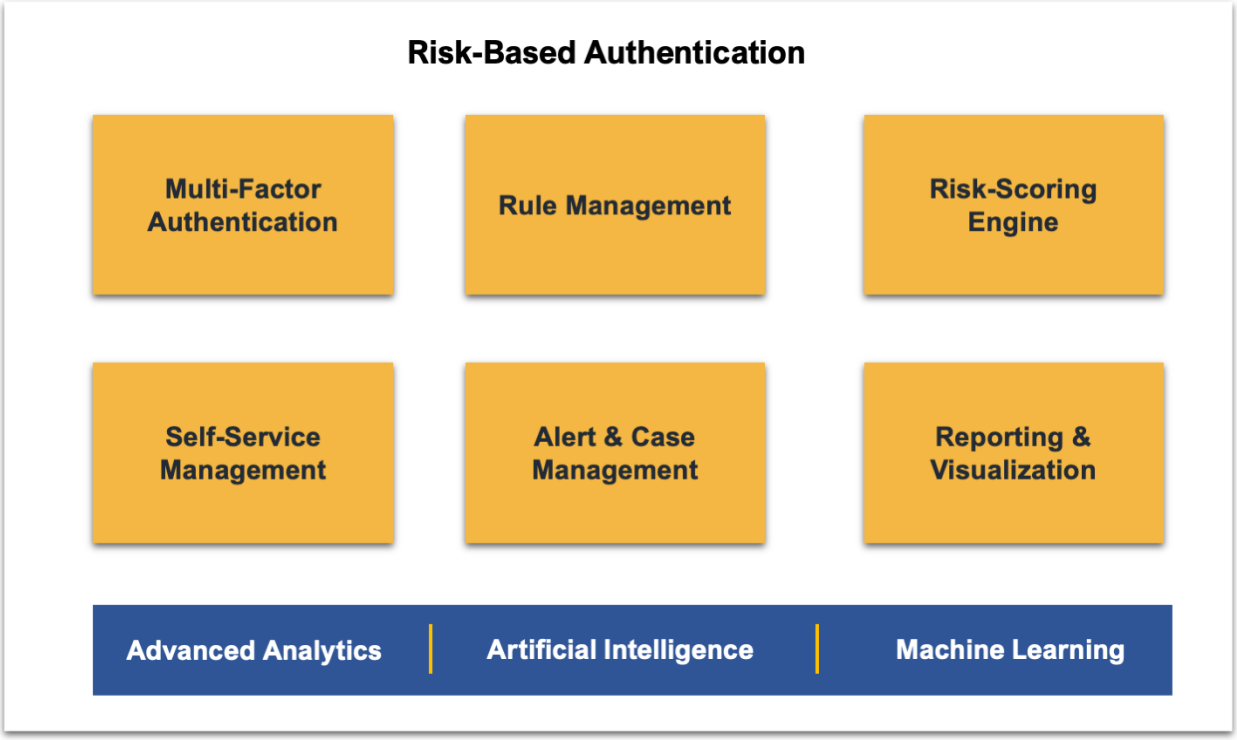
the user, MFA can utilize a combination of username, password, PIN number or an ID, hardware/software token, two-factor authentication (2FA), One-time Password (OTP), Time-based One-Time Password (TOTP), FIDO, biometric authentication, or more. Biometric authentication, including fingerprint recognition, facial recognition, voice recognition, iris recognition, etc., is getting increasingly popular amongst RBA vendors.

- **Self-Service Management**- RBA solutions offer a self-service capability that enables users to perform various actions like user ID and password recovery, password reset, and such others. The capability allows users to self-register if they are new to the platform and manage their devices according to the company's policies. They can introduce a new device for authentication or remove the existing device and set up default devices. The authentication methods can be changed. For instance, users can decide if they would like to receive an OTP through email or SMS.

- **Alert and Case Management**- RBA solutions offer an alert and case management capability that helps manage risk and fraud in real-time. Alerting helps to quickly notify and prevent high-risk login attempts. RBA solution also provides an investigation of suspicious activities. Furthermore, by embracing the RBA solution, the admins can have a holistic view of the attacks, and accordingly, they can design the policies to safeguard the company. With the help of RBA, admin and users can get an email/ message alert when logging is attempted from a different location, different device, or at an unusual time. RBA's case management helps in analyzing and marking activities as genuine or fraud based on the investigation, and then the markings are fed back into the risk engine for enhancing the precision of the risk score of the future activities.

- **Visualization and Reporting**- RBA solutions offer visualization capabilities, including network information, user behavior, system information, and application data, to help users navigate through large datasets. It collects and collates data from different sources and puts it in a single graphical presentation to make it easy to understand and analyze. RBA solutions utilize various visualization techniques like graphs, pie diagrams, etc., to analyze huge data and detect any peculiar activity. Reporting capability in an RBA solution refers to generating reports to get a holistic view relating to risk profiles, fraud patterns, active anomalies, devices with a potential virus, trends, locations, IP addresses, etc. These reports are submitted for internal audits to the higher authorities, commonly known as internal reporting, and are also used for compliance with external norms.

Figure: Key Components of Risk-Based Authentication Solution



Source: Quadrant Knowledge Solutions

Growing Frequency and Sophistication of Evolving Threat Landscape is Driving the Demand for Risk-Based Authentication Solutions

In this digital age, a majority of services, such as shopping, banking, transactions, socializing, and so on, are delivered over the internet. Enterprises are undergoing digital transformation with the aim to reduce cost, increase efficiency and availability, and enhance customer experience. However, in this digital transformation journey, organizations are facing numerous challenges pertaining to security.

Some of the challenges faced by modern enterprises include the adoption of the cloud, a rise in unsecured BYOD/WYOD and IoT devices, increased cyber threats, and frail authentication mechanisms. Modern businesses are favoring cloud-based services over on-premises storage of data and applications, thereby increasing the probability of unauthorized access. In addition, the increased adoption of policies such as Bring Your Own Device (BYOD) and Wear Your Own Device (WYOD) is allowing users to access information/resources through a variety of unsecured devices, including laptops, computers, tablets, smartphones, and wearables, resulting in data and network security challenges for businesses. Furthermore, cybercriminals are using increasingly sophisticated techniques to carry out cyberattacks via means like ransomware, phishing, identity theft, account take over, botnet attacks, and many more. Hackers are exploiting the increased remote working and online shopping trends. In such high-risk environments, traditional static authentication methods relying on weak and easily interceptable passwords are insufficient to provide adequate security.

Therefore, organizations are increasingly adopting Risk-Based Authentication (RBA) solutions, also known as Adaptive Authentication solutions, to overcome all these challenges. Risk-Based Authentication (RBA) solutions help organizations overcome these challenges while ensuring robust security and offering a seamless customer experience. Risk-based authentication is based on a set of rules that use various contextual factors to calculate the risk associated with any user or transaction. Based on the risk score assigned, it determines the level of authentication needed. RBA solutions offer adaptive multi-factor authentication (MFA), which enforces stringent authentication steps for high-risk score users and less stringent authentication to offer a seamless experience for trusted users with the low-risk score. Thus, RBA solutions offer a perfect authentication mechanism for organizations aiming at achieving the right balance between high security and enhanced user experience.

RBA Solutions are Continuously Transforming Driven by Advanced Analytics, AI, ML, and Behavioral Biometrics

To tackle the issue of rising sophistication and volume of cyberattacks, vendors are enhancing their RBA solutions by integrating emerging technologies like AI, ML, advanced analytics, and biometrics. RBA solutions use AI and ML to enable real-time monitoring and analysis of large datasets. Powered by AI & ML, RBA solutions can efficiently monitor a user's behavior to provide precision in regard to profile and login patterns. It tracks any anomaly in the device's location, IP address, login time, and network. Powered by ML, the risk engine calibrates to accommodate any new intelligence or insight. RBA solutions use advanced analytics to accurately determine the risk score for any user or login attempt so that risky users are prompted with stricter authentication while trusted users are offered a seamless login experience. Additionally, a majority of RBA vendors are also opting for biometric authentication, as it ensures paramount security by being unique to every user, cannot be stolen or tampered with, and offers ease of use. As biometric authentication ensures accurate identification and verification of an individual, it is proving critical for preventing online fraud. Thus, RBA solutions are leveraging AI, ML, advanced analytics, and biometrics to ensure robust security and enhanced customer experience.

As the banking and financial sector has been the prime target for cybercriminals, banks and FIs have been the early adopters of RBA solutions. Apart from banking, other industries like retail, gaming, healthcare, and aviation are also increasingly adopting digital transformation. The e-commerce industry is witnessing a boom driven by the ongoing COVID-19 pandemic. Therefore, e-commerce vendors are increasingly demanding robust authentication mechanisms like RBA that offer protection against online frauds like phishing, account take over, chargeback, friendly fraud, and more while ensuring a seamless customer experience. Online gaming is another segment always on the hackers' radar as the segment is monetarily lucrative. RBA not only ensures secured access to online accounts but also removes the risk of anonymity by offering biometric authentication. As healthcare is another prime vector for phishing and malware attacks, healthcare organizations are using RBA systems to secure the sensitive information of patients like personal details, insurance, bank details, medical records, etc. RBA solutions are also being used in the aviation business, which deals with a vast volume of personal data from customers.

Furthermore, due to the COVID-19 pandemic, a majority of the global workforce is working remotely. With the need to ensure secured remote access, organizations are adopting RBA solutions to verify that the user accessing the company's data and resources are genuine employees and customers. With its capability to balance security and customer experience, the demand for RBA solutions will increase in all sectors.

Competitive Landscape and Analysis

Quadrant Knowledge Solutions conducted an in-depth analysis of Risk-based authentication vendors by evaluating their products, market presence, and customer value proposition. The evaluation is based on primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall market. This study includes an analysis of key vendors, including Accops, Appgate, Broadcom, CyberArk, CoffeeBean Technology, Duo Security (Cisco), ForgeRock, IBM, Kount, LexisNexis Risk Solutions, Ping Identity, Microsoft, OneLogin, OneSpan, Okta, RSA, Silverfort, SecureAuth, Swivel Secure, and TransUnion,

IBM, Ping Identity, Kount, LexisNexis Risk Solutions, Okta, Microsoft, Appgate, and OneSpan are the top performers and technology leaders in the global RBA market. These companies provide a sophisticated and comprehensive risk-based authentication technology platform to address a variety of RBA use cases.

IBM Security offers an integrated RBA solution with end-to-end functional capabilities, providing robust authentication, risk management, and cloud-based access management. IBM's RBA solution is incorporated with the risk-intelligence consortium, digital identity risk-engine, and API-based integration for continuous and enhanced risk-authentication.

Kount's RBA solution is powered by patented AI-driven technology, with detailed reporting, comprehensive intelligence, offering seamless payment fraud protection. Kount incorporates a passive biometric analysis tool that monitors behavioral patterns to provide enhanced protection from bots, precise risk detection to users, and guard data against malicious logins.

Ping Identity is a leading IAM vendor with a robust in-house risk engine and configurable authentication policies. It uses UEBA and ML models with AI to analyze risk predictors in real-time for seamless login. The company's risk management with third-party services can be well integrated across their platform to address numerous use cases for RBA & MFA.

LexisNexis® Risk Solutions is well-recognized in the market for its strong RBA capabilities across the entire customer journey to address frauds while offering a seamless customer experience. The company's recent addition of behavioral biometrics capability helps in making improved fraud decisions with robust authentication capabilities. **Okta** with Auth0 offers platforms to manage a broader range of risk-based authentication solutions. The platform is equipped with ML capabilities, API access management for enhanced security, and report generation functionality. **Microsoft** continues to enhance its ML-powered intelligent risk-based authentication solutions and automation for secure and seamless user login.

Appgate is recognized for its RBA capabilities that are driven by powerful MI & robust rules to provide seamless authentication. **OneSpan** is recognized for its risk-analytics solution that leverage the power of AI & ML for threat detection and taking informed decisions for fraud prevention. The solution incorporates a future-proof platform with seamless third-party technology integration. **TransUnion** has significantly enhanced its technology capabilities and continues to focus on RBA modules. The company continues to leverage machine learning for predicting digital transaction outcomes, regardless of known or unknown customer or device.

RSA continues to leverage its strong domain knowledge to offer a comprehensive fraud detection platform that leverages risk-based MFA for enhanced protection. RSA's risk-based authentication feature is coupled with robust ML analysis of multiple risk indicators along with fine-grained policy controls. **CyberArk** is amongst the leading vendors offering next-generation RBA solution capabilities with an AI-driven user behavioral analytics engine that creates in-depth insights in real-time. **Broadcom** provides enhanced RBA capabilities with OOTB features. **ForgeRock**'s platform is harnessed by advanced AI to orchestrate risk journeys and accomplish a Zero Trust or CARTA security model and providing a comprehensive risk-based authentication process. **OneLogin** leverages AI risk-score technology with an enhanced adaptive solution to guard against sophisticated credential-based threats and attacks, offering frictionless SSO. **Duo Security** (Cisco) offers a robust solution that is equipped with robust MFA capabilities. The solution integrates with any application to guard users and devices.

SecureAuth, with its powerful capabilities, continues to leverage AI-driven analytics integrated with granular configurations, SSO, and detailed reporting with seamless user engagement. **CoffeeBean Technology** offers robust risk-based authentication solutions for enhanced adaptive authentication capabilities. The company plans to continue enhancing its integration with new FIDO protocols. **Accops** has strong experience in the RBA space in detecting SSO, includes detailed audit logs for enhanced effectiveness of its multi-factor authentication performance. **Swivel Secure** offer robust RBA platforms that support a wide range of architectural requirements entailing a broad option of authentication factors. They are positioned amongst the emerging challengers. **Silverfort**'s platform is well recognized for its AI-driven risk engine and enhanced adaptive authentication capabilities and is positioned as an aspirant.

Key Competitive Factors and Technology Differentiators

A majority of the leading Risk-Based Authentication (RBA) vendors may provide off-the-shelf RBA capabilities, good customer experience, seamless integration, a robust risk scoring engine, rule management, authentication mechanism (MFA), user self-service, alerting and case management and visualization and reporting. However, the flexibility of deployment and authentication mechanisms 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 RBA vendors are as follows.

- **The Sophistication of Technology Capabilities**: The growing volume, sophistication, and intricacies in online frauds are consistently elevating FIs and businesses' risk exposure. In the past few years, global organizations across geographical regions have observed a surge in fraud attacks, including identity frauds, payment frauds, cybersecurity breaches, and such others, driving the need for a robust RBA solution. Imposters are increasingly using high-end tools to launch sophisticated and complex attacks. A powerful, scalable, and advanced RBA solution is needed to check the rising fraud threats and the surge in the sophistication of such threats and manage the challenges of consistently changing fraud patterns and cyber-attack dynamics. Therefore, users should evaluate an RBA solution that offers comprehensive capabilities, including managing large datasets, a risk-based engine, advanced authentication capabilities like MFA and biometric authentication, real-time fraud detection and interdiction, alert and case management, visualization and reporting, and rule management. Additionally, vendors' customer value proposition may differ in terms of ease of deployment, ease of use, price/performance ratio, support for a broad range of fraud and risk-based use cases, global support service, and such others. Most of the vendors are offering these functionalities and continue to invest heavily in further enhancing their platforms with AI, ML, newer authentication protocols, and risk-based analytics. An advanced RBA solution can provide a superior customer experience and detect malicious login activities in real-time.

- **Technology Vision & Roadmap**: The use of sophisticated technology by hackers is enabling a surge in cybercrimes like account takeovers (ATO), malicious logins, payment frauds, botnet attacks, sophisticated targeted attacks, loyalty fraud, and others. Hence, it is imperative for users to choose the appropriate technology partner as per their specific-use cases, evolving fraud trends, and their digital transformation roadmap. The RBA vendors are constantly enhancing and innovating their technology value proposition in

terms of providing a holistic risk-based authentication solution with comprehensive data integration, customer verification & validation, sophisticated risk engine powered by advanced analytics, AI & ML, custom model development, robust investigation and case management, advanced visualization tools, incorporation of workflow and process automation, and such others. The vendors are also focusing on offering an exceptional digital experience to customers through a seamless RBA authentication process. Organizations should carefully evaluate the vendor's existing technology capabilities along with their technology vision and roadmap to improve overall satisfaction and customer ownership experience for long-term success.

- **Vendor's Expertise and Domain Knowledge**: FIs and organizations should conduct a comprehensive evaluation of numerous RBA solutions and vendors before making a final decision. Organizations should evaluate vendors' expertise and domain knowledge in understanding their unique business problems, use cases, and industry-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. Organizations should look for solutions providing a unified and effective risk analysis tool that swiftly provides appropriate information vital to making the right decisions. Users must watch out for integrated solutions offering comprehensive coverage with a continuous and holistic view of customers and the associated accounts, and the risk factors. FIs should look out for RBA solutions supporting multiple forms of AI and rules-based detection models and should have the potential for third-party data integration. 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 RBA platform deployments.

- **AI, ML, and Advanced Analytics**: AI, ML, and advanced analytics are emerging technologies in the RBA space. Driven by AI, ML, and advanced analytics, an RBA solution provides enhanced analysis of huge datasets, thereby increasing the solution's efficiency. Powered by these emerging technologies, an RBA solution offers continuous monitoring & real-time anomaly detection. Further, the solution helps detect a user habit or deviation which may need more authentication. Advanced analytics gives precise risk detection of all users in each login session. Vendors are increasingly using advanced analytics techniques like predictive analytics, big data analytics, social network analytics, user behavior analytics, graph analytics, NLP, risk-rating models, and others to overcome the challenges in the RBA domain and maximize their solution's overall efficiency and effectiveness. AI-powered

robust customer-risk rating models offer real-time risk scores based on multiple factors, and their enhanced detection capabilities can cut across jurisdictions and businesses.

- **Integration and Interoperability**: Seamless integration and interoperability with vendors' existing technologies are amongst the crucial factors impacting technology deployment & ownership experience. The RBA solution should offer seamless integration and interoperability with multiple fraud analytics solutions, industry consortium, third-party risk signals, IAM solutions, and mobile security applications to ensure smooth operation, information exchange, and flexibility of implementation. The solution should also support integration with third-party device compliance solutions, SIEM solutions, and payment service providers and gateways. Users should evaluate vendors' capability to provide out-of-the-box integration with best-of-breed technologies and custom integration with various fraud detection & enterprise products. Also, users should assess the RBA platform in offering breadth and depth of integration capability specific to their existing tools and 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

- **The sophistication of Technology**: The ability to provide comprehensive functional capabilities and product features, technology innovations, product/platform architecture, and such others
- **Competitive Differentiation Strategy**: The ability to differentiate from competitors through functional capabilities and/or innovations and/or GTM strategy, customer value proposition, and such others.
- **Application Diversity**: The ability to demonstrate product deployment for a range of industry verticals and/or multiple use cases.

- **Scalability**: The ability to demonstrate that the solution supports enterprise-grade scalability along with customer case examples.
- **Integration & Interoperability**: The ability to offer product and technology platforms supporting integration with multiple best-of-breed technologies, providing 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.

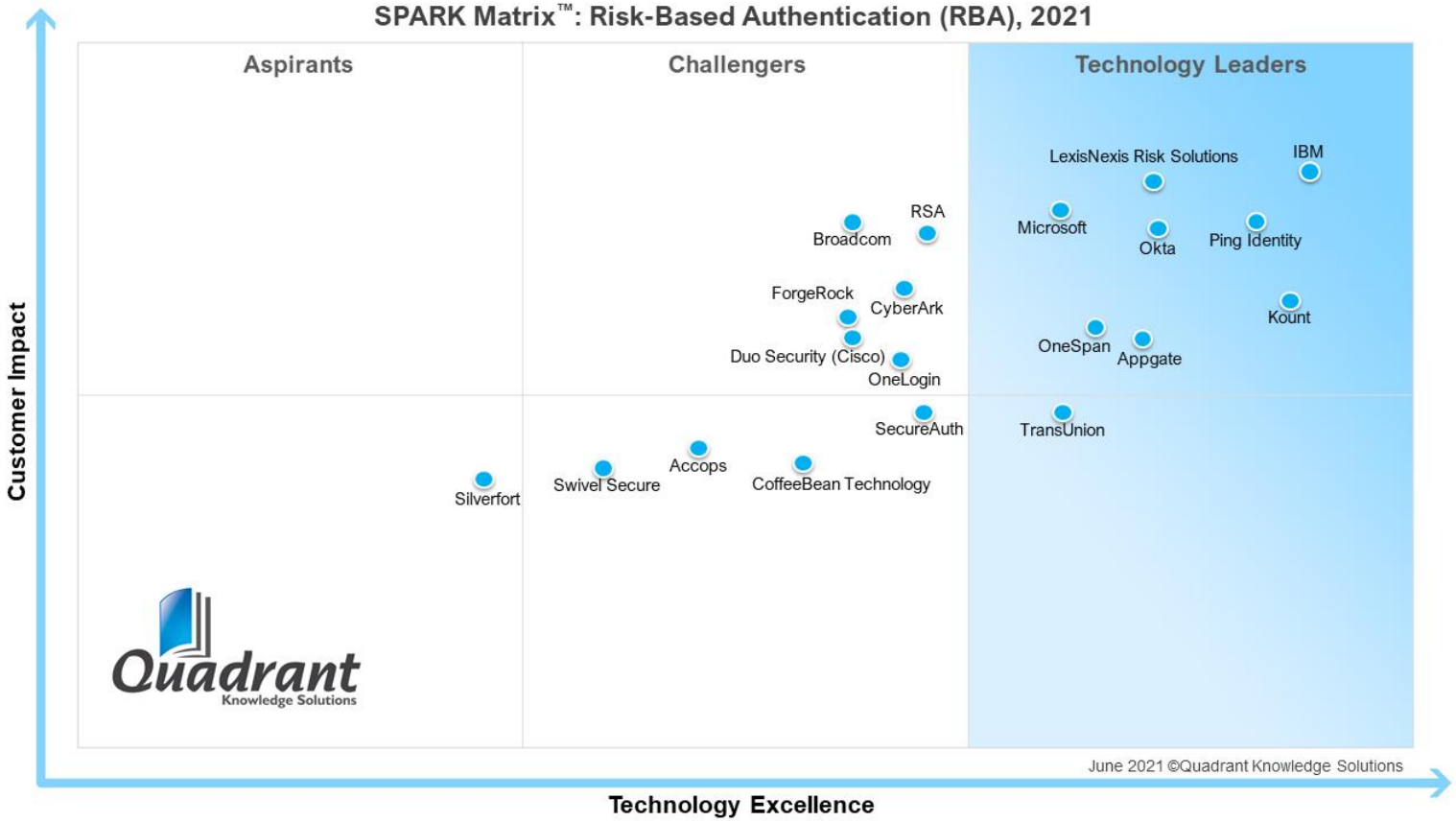
Evaluation Criteria: Customer Impact

- **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 a 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™: Risk-Based Authentication (RBA)

Strategic Performance Assessment and Ranking

Figure: 2021 SPARK Matrix™
(Strategic Performance Assessment and Ranking)
Risk-Based Authentication (RBA) Market



Vendor Profiles

Following are the profiles of the leading RBA 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 RBA technology and vendor selection based on research findings included in this research service.

IBM Security

URL: https://www.ibm.com/

Founded in 1911 and headquartered in Armonk, New York, IBM Security is a leading provider of enterprise security products and services worldwide. IBM Security offers a portfolio of advanced and integrated solutions, including identity & access management, data security, SIEM, SOAR, security services, cloud security, and others. IBM Security offers risk-based authentication through its Trusteer Pinpoint Detect and Verify solutions, enabling the prevention of fraudulent activities and high-risk transactions.

The IBM Security Trusteer Pinpoint Detect solution offers robust features such as digital identity protection and authentication, digital identity trust scoring, device identification & intelligence, global threat intelligence, behavioral biometrics, and visibility and control over the customer journey. The AI and ML-driven solution offers frictionless customer experience and digital identity trust to help in real-time fraud identification without compromising on security. IBM Trusteer Pinpoint Detect is a cloud-based solution offering risk assessments for digital identities to distinguish between malicious users and genuine users. It uses this capability to help safeguard digital channels against ATO's and frauds by detecting malware-infected end-user devices.

The IBM Security Verify solution offers access management and multi-factor authentication to safeguard user access while securely adopting web, mobile, IoT, and cloud technologies. It verifies access to balance usability and security via the use of risk-based access, SSO, integrated access management control, detect federation, and mobile MFA. It helps enforce risk-based access policies that provide minimum friction during authentication when the user is known and provide strong multi-factor authentication if the risk is high. Verify enforces RBA by assessing factors like user data, application data, device information, geolocation, IP address, and such others. The solution offers password-less login to work applications. Thus, the solution eliminates barriers to mobile productivity while ensuring risk-aware authentication. It can be deployed on-premises or in a virtual or hardware appliance containerized with docker.

The IBM Security Risk-Based Authentication solution caters to both workforce and consumers through a single solution. The solution integrates evidence-based fraud protection and user access management in real-time for digital user experience. The solution offers advanced policy authoring for applications, users, groups, and roles and orchestrates policies based on user journey and context. It enforces risk-based access policies across channels depending on the actual risk to the organizations. The solution is built on an intelligence-based cybersecurity platform to mitigate

malware, phishing-driven fraud, eliminate ATO attacks, and alleviate digital channel risk. The solution offers robust features such as device fingerprinting, device compliance, behavioral biometrics, the ability to detect BOT attacks and new user threats, identity life-cycle events, and dashboarding & reporting. Additionally, the solution offers alert and base management capability through in-built integration with IBM SIEM (QRadar) and case management (Resilient) solutions; and API-based integration to enable connection with any IAM systems.

Analyst Perspective

Following is the analysis of IBM Security's capabilities in the RBA market:

- IBM is a leading cloud platform and cognitive solutions provider. The company offers innovative technology products and services to organizations around the globe. IBM Security provides robust risk-based authentication solution that enables secure, frictionless, and risk-aware digital interactions for people, devices, and things across any cloud environment. IBM's RBA inspects a wide range of identity risks, including device data, network connection, passive behavior, anomaly detection, fraud patterns and consortium data, to ensure transparent and evidence-based fraud protection.

- IBM Security RBA solution offers advanced device risk detection and protects users from threats such as malware for ATO, SMS stealers, remote access tools, emulators, repackaged applications, spoofed attributes, rooted devices, and such others. The solution also offers robust device fingerprinting based on a proprietary algorithm, which creates a device ID that can sustain spoofing, SIM swipes, application removal, and such more.

- The company offers advanced behavioral anomaly & behavioral biometrics for the web as well as mobile. The company also provides a risk intelligence consortium comprising numerous confirmed fraudulent devices, cyber-attack methods, risky IP addresses, and high-risk ISPs. In addition, the solution offers a digital identity risk engine that can be used with any IAM solution through API-based integration.

- In terms of geographical perspective, IBM has a strong presence in the USA, followed by Europe and Latin America. The company is also extending its presence in APAC and Canada. IBM supports multiple use cases through robust cloud solution, automated business rules, deep analytical detail, and cost-effective web access. IBM supports multiple use cases user login protection and in-application activity using continuous assessment, SSO login protection, compliance with PSD2, FFIEC, and such others by advanced MFA capabilities, and new account onboarding. The company caters to various industry verticals such as BFSI, retail, healthcare, government,

telecommunication, transport & media, and manufacturing. From the perspective of the challenge, IBM states the policy offering capabilities can be enhanced and making policies in the system more visible to the business.

- From the roadmap perspective, the company is focusing on enhancing its third-party risk signal provider ecosystem and expanding deployment patterns to cater to complex hybrid cloud deployments. The company is also focusing on automating adaptive controls to change in-session entitlements based on risk. In addition, the company plans to further improve the graphical representation & management of access risk policies as per the user journey. The company also plans to enhance policy automation by adding more tools to test, validate, and simulate the impact of policy authoring on the access system.

Kount

URL: https://kount.com/

Kount, an Equifax company, was founded in 2007 and is headquartered in Boise, Idaho, USA. Kount is a leading provider of fraud prevention solutions to merchants and processors across the globe. Kount's solution portfolio, the Identity Trust Platform, includes Kount Command, Kount Control, Dispute and Chargeback Management, and Data on Demand for complete customer journey protection. The platform is built on Kount's Identity Trust Global Network™ and advanced artificial intelligence. Kount' analyses robust network, comprising billions of interactions annually to helps organizations establish identity trust at any point in the customer journey, ultimately delivering personalized experiences.

Kount Control uses a multi-layered approach to account takeover protection through adaptive, multi-factor authentication (MFA), a protection layer, a policy and customization layer, and analytics reporting. The solution keeps bad actors out of customer accounts and allows for seamless login experiences for legitimate customers. Organizations can evaluate the riskiness of login events and provide online experiences that drive desired business outcomes.

Kount Control's protection layer assesses user behavior, device, and network anomalies to identify high-risk login activity from malicious bots, credential stuffing, and brute-force attacks. This assessment helps businesses decide in real-time if it should approve or decline the activity or challenge it with step-up authentication. Step-up authentication is available via Kount's Email multi-factor authentication (MFA) or Equifax's Secure multi-factor authentication (MFA). Kount Control's multi-factor authentication options elevate authentication security to the next level by verifying users via one-time passcodes (OTP) through email or SMS. Kount's Email multi-factor authentication challenges users by sending them a numeric passcode to the email address linked to the customer account. Users can verify their digital identity by retrieving and entering the passcode. The Equifax Secure multi-factor authentication option is for use cases that require a second layer of security or mobile-first support through a user's mobile number and device or SIM card via a dynamic hyperlink delivered via SMS. Additionally, the solution can leverage Equifax offerings, including InstaTouch Pay, InstaTouch ID, and Account Verification.

Kount Control's policy and customization layer helps businesses customize user experiences and minimize friction by detecting and segmenting users based on common characteristics. Businesses can identify users based on datasets comprising analytics such as user type, device specifics, IP risk, geolocation, custom data, and more to apply the appropriate level of friction.

Kount Control's reporting and visualization layer offers multi-dimensional data and real-time reporting for detailed customer insights. Businesses can use these insights to adjust workflows and fraud mitigation policies and further customize customer experiences. This functionality reports failed login attempts, risky IPs, compromised accounts, and inbound anomalies, so businesses can better understand how account takeover attacks affect them.

Kount's Data on Demand solution is powered by the Identity Trust Global Network and enhances a company's customer knowledge with thousands of additional data points. Businesses can review the data on their own or combine it with additional company-collected data for deep analytics on a single platform. Built on Snowflake and hosted by Kount in a private data warehouse, Data on Demand has the performance, scale, and security needed for big data analytics. Kount's Identity Trust Global Network safeguards the entire customer cycle, helps accelerate global expansion, introduces new use cases, enhances customer experiences, expands omnichannel capabilities, and more.

Analyst Perspective

Following is the analysis of Kount's capabilities in the RBA market:

- Kount offers market-leading, cloud-based, risk-based authentication technology to provide real-time access to data elements that provide a complete picture of a customer's digital identity while optimizing business decisions. The company's advanced AI uses supervised and unsupervised machine learning to produce an actionable risk assessment called Omniscore. Using both types of machine learning mean Kount can detect existing and emerging fraud, automate decisions, and minimize manual reviews. Kount's sophisticated technology platform is backed by comprehensive intelligence from the Identity Trust Global Network. In addition, the platform is well-recognized for its industry-leading solutions for protection from payments fraud, new account fraud, and account takeover attacks. The company's superior technology platform is coupled with professional services that offer a strong customer ownership experience, especially to merchant, e-commerce, and payment processing industries.

- Kount offers key differentiating features through its extensive Identity Trust Global Network coupled with unique physical and digital identity data from Equifax. Kount offers numerous integrations with key payment service providers, gateways, and platforms. Kount also provides high customer satisfaction, excellent NPS rates, and outstanding retention. Kount provides comprehensive customer journey protection and establishes the level of trust behind each account creation, login, and payment event to prevent account

takeover, payments fraud, malicious bot activity, and loyalty fraud. After a business approves a transaction, Kount keeps working to prevent chargebacks and fees from friendly fraud through its dispute management solution. Kount also provides a robust offering of professional services, from consulting and policy management to performance guarantee models, to fulfil any use case or customer need. Kount states the biggest challenges for businesses amid the pandemic situation have been automation, the massive availability of compromised data, and the consistent pressure to create seamless customer experiences that do not compromise security.

- From the geographical presence perspective, Kount has a strong presence globally. The company is also expanding its presence in Europe, Latin America, EMEA, and APAC. Kount caters to several industry verticals such as e-commerce, financial institution, public sector, gaming and streaming, health and insurance, and travel, leisure, and entertainment.

- In terms of roadmap, Kount continues to focus and enhance its capabilities with Equifax to offer new products and use cases and improve customer experiences.

Ping Identity

URL: https://www.pingidentity.com/

Founded in 2002 and headquartered in Denver, Colorado, Ping Identity is a leading provider of secured identity solutions for enterprises globally. The company offers the Ping Intelligent Identity™ platform, which provides zero-trust identity-defined security for customers, employees, and partners to help enhance protection and engagement across the global business. The Ping Intelligent Identity™ platform offers RBA capabilities through its cloud based PingOne Risk Management service that leverages machine learning and intelligent, configurable policies to offer secured authentication. PingOne Risk Management evaluates multiple risk signals to verify user identity and detect potential threats.

PingOne Risk Management, powered by ML models and advanced analytics, continuously analyses various contextual user information to identify potential attacks and threats. The risk management service helps to comprehend the risk levels, enables businesses to create intelligence-based, configurable policies which apply precise authentication for resources, and offers a zero-login experience to trusted users. It also includes risk dashboards to view reports on high-risk events and provide detailed insights, including filtering capabilities and the option to inspect monitored user activity. The PingOne Risk Management service integrates with PingFederate, with additional integrations including PingOne, PingID, and PingOne MFA and third-party products using the API. PingOne Risk Management leverages multiple risk predictors such as user & entity behavior analytics, anonymous network detection, IP reputation, and impossible travel to enable intelligent authentication decisioning.

PingOne Risk Management leverages user & entity behavior analytics (UEBA) and ML to understand the predictable behavioral patterns of workforce users within organizations. This functionality enables enterprises to consider several data points along with device type, operating system, browser version, date and time, user location, IP range to determine anomalies as low, medium, or high-risk and prompt the user to provide for the precise authentication. Furthermore, the service enables businesses to fine-tune rule settings to ensure just the right users get access to the organizational resources.

The anonymous network detection functionality enables enterprises to analyze user's IP address data to decide if the address is from any anonymous network and whether to deny access or perform step-authentication. This functionality can also create a whitelist to include an enterprise's VPN networks, assuring that VPN users can access authorized resources. The IP functionality analyses the IP address and data from various intelligent sources for involvement in malicious and anomalous activities and then ask for stronger authentication to verify the user's identity. PingOne Risk

Management's impossible travel feature evaluates users' location data to calculate if time-lapse amidst two login locations is physically possible. If impossible lapse time is calculated, then the user can be prompted for step-up authentication, or access is denied.

Analyst Perspective

Following is the analysis of Ping Identity's capabilities in the RBA market:

- Ping Identity provides industry-leading identity and access management solutions that allow workforces, customers, and partner identities to securely access any services, applications, or APIs from any device. The company offers a unique RBA solution that offers a robust in-house risk engine and the capability to adjust threshold and customize policies in accordance with businesses. PingOne Risk Management, along with third-party risk services, can be integrated across the Ping Identity platform to resolve workforce, customer, and partner use cases for RBA, MFA, and authorization.

- Ping Identity offers the ability to support highly distributed enterprises with complex use cases like non-standard app integration, performance and scale needs, diverse user populations, and more.

- The company provides the ability for large enterprises to consolidate on a single enterprise-grade platform and minimizing the need for numerous MFA, WAM, SSO, directory, and RBA solutions. The company enables large enterprises to move sprawled, legacy IAM investments to SaaS-delivered and cloud-hosted delivery models. The company measures customer satisfaction directly via Net Promoter surveys from all Ping customers and seeks detail and feedback for continuous improvement.

- In terms of geographical presence, the company has a major presence in North America, EMEA, followed by Europe and the APAC. The company supports multiple use cases such as risk assessment of employees, confirming customers' and employees' identities before allowing them access to their accounts to eliminate fraudulent access and compromised credentials. From the challenge perspective, the company launched risk management in 2020 and is in the initial stages of the services. It is mostly relying on the market education that other companies have conducted. Ping also believes the customers are already aware of the importance of RBA as a paradigm. Therefore, the company thinks right now is a good time to enter this market and offer an integrated solution to the entire IAM suite.

- From the roadmap perspective, the company plans to focus on supporting external risk feeds in multiple integration levels which is provided out of the

box by Ping; third-party vendor feeds using direct integration to PingOne or indirect integration via PingFederate adapter; and customer-specific feeds and signals. The company also plans to continue enhancing and enriching the risk models list, including more focus on CIAM risk models, such as device trust, bot detection, credential leakage-related predictors, user-based anomaly detection, and more. Ping Identity continues to expand to full risk-based identity management by adding other use cases relevant to the Ping platform, such as password reset, directory access, account creation, and more. Ping is also focusing on continuous authentication during an ongoing session and prompting the user to authenticate if any anomaly is detected. Furthermore, the company continues to enhance its dashboards and analytics capabilities to assist in security investigation and analyze user behavior and policy hygiene with a consolidated risk view across Ping services, dynamic reports, personalization, and more.

LexisNexis Risk Solutions

URL: https://risk.lexisnexis.com/

Founded in 1997 and headquartered in Georgia, USA, LexisNexis Risk Solutions is a major global provider of risk management solutions for a broad range of industries. The company offers a portfolio of solutions offering innovative technologies, information-based analytics, decision tools, and data services for multiple industries. The LexisNexis Risk ThreatMetrix solution unifies digital identity intelligence and authentication attributes to offer enhanced risk decisioning across the entire customer lifecycle. The solution combines integral components of LexID® Digital and the LexisNexis® Digital Identity Network® to deliver powerful risk decisioning that combines robust digital identity intelligence with relevant transaction insights.

ThreatMetrix's risk-based authentication process offers multi-layered, risk-based authentication, which adapts to every customer by combining their digital & physical identity footprint to create assurance and trust during the customer onboarding and ongoing identity management process. The RBA is powered by a robust engine & workflow which combines customized lines of defense into a consolidated decision engine, which intelligently adapts to scenarios involving higher risk identities. The RBA capability creates four layers of defense: risk assessment, digital & identity assessment, fraud assessment, and identity authentication to enhance fraud & risk decisions. The risk assessment layer helps in knowing the risk prior to knowing the person. It utilizes based on factors like geolocation, VPN & proxies, device ID & attributes, malware & bots, and behavioral analytics to accomplish this task. The identity verification layer helps to know the claimed identity by verifying the collated identity evidence from public records and several credit bureaus. The fraud assessment layer helps to know the risks linked with identity and behavior through deceased screening, behavioral analytics, velocity checks, and email risk. The identity authentication layer helps to know the person who they claim they are by document authentication, OTPs, knowledge-based authentication, and biometrics.

The LexisNexis ThreatMetrix solution offers best-in-class fraud, identity, and authentication services to enable online businesses to determine trusted customers efficiently from potential imposters in real-time seamlessly. This solution unifies digital identity intelligence with physical identity characteristics such as digital identity intelligence, real-time decision analytics combining market-leading behavioral analytics along with clear-box ML and case management. Further, the solution offers smart authentication with various types of MFA, integrating risk-based and strong customer authentication (SCA) strategies to fulfill rising regulatory needs seamlessly. The solution also offers investigation and review, entailing case management, forensics, and reporting capabilities to enhance, route, and resolve high-risk events.

Analyst Perspective

Following is the analysis of LexisNexis's capabilities in the RBA market:

- LexisNexis® Risk Solutions manages the power of data and advanced analytics, to enable insights which help businesses and government entities minimize risk and enhance decisions to help businesses globally. The company provides solutions and decision tools that unify public and industry-specific content with sophisticated technology and analytics to help organizations in evaluating and predicting risk and improving operational efficiency. LexisNexis ThreatMetrix offers strong RBA capabilities that offer multi-layered analysis of identity and transaction across the customer lifecycle to ensure comprehensive fraud prevention while ensuring a frictionless customer experience.

- LexisNexis ThreatMetrix solution has recently added behavioral biometrics capability to enable businesses to detect high-risk scenarios and make enhanced fraud and risk decisions. This capability adds an additional layer of intelligence to its prevailing identity and authentication solution, which reflects as a robust tool in the fight against cyber frauds. The behavioral biometrics capability can help users differentiate humans from non-human traffic like bots, detect good and trusted customer profiles, reliably profile fraudsters, spot session anomalies and create trust relating to genuine customers, making it a key differentiator.

- In terms of geographical presence, the company has a major presence across the globe. The company caters to various industry verticals such as insurance, financial services, healthcare, and government. The company supports multiple use cases with its ThreatMetrix solution to swiftly detect and eliminate rising fraud schemes that entail customer touchpoints.

Okta

URL: https://www.okta.com/

Founded in 2009 and headquartered in California, USA, Okta is a major identity solution provider across the globe. The company provides robust solutions such as workforce identity and customer identity powered through the Okta platform and Auth0 platform for identity use cases. Okta offers flagship products for risk-based authentication solutions such as adaptive SSO, adaptive MFA, risk-scoring engine, and the ThreatInsight tool.

The SSO solution offers a single username and password for accessing all the workplace productivity apps used by the users and enhancing the end-user experiences. This solution helps to easily deploy the cloud and offers frictionless secure user access with a centralized control point. The solution also offers identity store integration and adaptive security policies. The solution empowers end users and simplifies auditing & reporting access to users.

The adaptive MFA solution strengthens the security of the application with contextual step-up authentication using a wide range of second factors. This solution assigns a risk score to every log-in attempt based on contextual cues, like location, device, and IP address. Depending on the risk level, the solution can allow or deny access or hint the user to submit an additional authentication factor to protect against potential breaches. The adaptive MFA secures accounts from credential thefts and MFA frauds with cloud-to-ground protection, proactive security, and integrated security. This solution also secures employees, partners, contractors, and customers with a broad range of MFA factors to enable smart access decisions across all business use cases. The solution offers a strong end-user access experience and ensures compliance with all the regulations.

The RBA solution offers a robust risk scoring engine that decides the probability of anomalous sign-ins. The risk engine assigns a risk level to every Okta sign-in using the models that use contextual information regarding the sign-in along with available information about the users. The admins are enabled to configure a sign-on policy rule to conduct different actions depending on the risk level of the sign-in. The admins can also build a sign-on policy rule, set a risk level, and assign a similar action based on the stated risk levels. New users are initially assigned as high risk, and over time the risk level is lowered to complement and not replace prevailing security tools like bot management, web application firewalls (WAFs), and security compliance. The risk engine comprises system log events offering insights showing how the risk level was decided, including a combination of three factors: anomalous location, anomalous device, and suspected threat, based on ThreatInsight detection.

The ThreatInsight tool evaluates the context of this log-in attempt and analyses the risk. If the user is trying to get access in a low-risk environment, they can just tap an Okta Verify push notification to complete authentication. ThreatInsight consolidates the data across the Okta network to detect and prevent malicious sign-in attempts. The tool also guards against automated bots attempting credential stuffing, and such other cybercrimes.

Analyst Perspective

Following is the analysis of Okta's capabilities in the RBA market:

- Okta harnesses two robust platforms from Okta and Auth0 to manage a wider set of digital identity solutions while ensuring secure access to the users. The company helps guard the identities of the workforce and customers across the world. Okta's platform offers B2B integrations to allow users to easily connect with vendor and partner identities while creating a centralized holistic view for identities & access. The B2B integration provides a seamless connection among customers, vendor, and partner identities. Okta has over 7,000 pre-built integrations with applications and infrastructure providers. In addition, Okta's MFA solution is equipped with factor sequencing and active directory (AD) to ensure enhanced factor chains based on higher risk sign-in activity. The MFA solution can be paired with the ThreatInsight tool for enhanced risk assessment with authentication in three steps.

- The platform offers an access gateway that helps employees to access on-premises applications. This capability enables organizations to uphold investments in the existing in-house web apps while parallelly supporting the new cloud investments. The platform provides API access management which enables organizations to view, manage, and secure API access via a centralized control point. This management also helps to enhance security and development and simplify authorization policies, thus giving more time for the development team. Okta's RBA solution is powered with ML capabilities which strengthen the adaptive MFA and adaptive SSO functionalities. The ML leverages to create a powerful behavioral profile and empowering users to automate security, making it a key differentiator.

- In terms of geographical presence, the company has a presence in the USA, Canada, France, Sweden, Germany, Netherlands, and Australia, followed by Japan and Singapore. The company supports multiple use cases with enhanced MFA and SSO functionalities.

Appgate

URL: https://www.appgate.com/

Founded in 2017 and headquartered in Florida, USA, Appgate is a major provider of cloud & hybrid-ready security, software, and services. The company offers zero trust network access, digital threat protection, risk-based authentication, and threat advisory services. Appgate offers a robust RBA solution that includes capabilities like customizable authentication, transaction monitoring, and risk orchestration.

Appgate s authentication solution offers robust multi-factor authentication through mobile SDKs which enables authentication via push notification, QR-code, biometric facial recognition, and email SMS OTPs. These customizable authentication capabilities offer protection at the user level by adapting to known user behaviors, using context to verify users, approve legitimate transactions and enforce authentication workflows. This capability further helps organizations create customized rules to prompt action, like step-up authentication, based on risk tolerance and enforce authentication methods that work best for the enterprise.

The transaction monitoring and authentication capabilities enable organizations to create customized workflows and seamlessly integrate solutions. Appgate's RBA uses machine-learning powered capabilities equipped with a flexible, rules-based system for robust transactional risk detection. This model eliminates binary decision-making by analyzing additional risk variables and offering sophisticated authentication techniques. The object-oriented drag and drop risk orchestration capability makes it easy to bind authentication & transaction monitoring by enabling enterprises to create a seamless customizable authentication workflow based on risk thresholds.

Appgate's RBA solution offers a layered approach to combat authentication and transactional risk efficiently. The solution enables the integration of systems to orchestrate seamlessly together, offering enhanced protection. This empowers organizations to seamlessly authenticate users, monitors transactions, and implement workflows based on risk tolerance.

Analyst Perspective

Following is the analysis of Appgate's capabilities in the RBA market:

- The RBA solution detects and mitigates device and user behavior anomalies in real-time through device identification and multi-factor authentication. It is driven by robust machine learning and strong rules, offering seamless fraud management with a simplified console. The solution provides frictionless authentication with threat intelligence, agile fraud detection, ease of

integration, trusted device ID, and a drag and drop interface, thus making them the key differentiators.

- From the geographical presence perspective, the company has a major presence in Europe, South America, and Japan. The company supports multiple use cases through effective transaction monitoring & authentication, risk & context-based authentication, and seamless integration.

Microsoft

URL: https://www.microsoft.com/

Founded in September 2009 and headquartered in Redmond, Washington, USA, Microsoft Security is a major provider of intelligent security solutions worldwide. The company provides a comprehensive suite of integrated security solutions, including Identity & Access Management, Threat Protection, Information Protection, and Zero Trust and Cloud Security. The company also offers secure remote work functionality. The Microsoft Identity & Access Management solution offers protection against identity compromise. The solution also offers unified identity & access management, simplified identity governance, secure access to apps, decentralized identity, blockchain, and privacy.

Microsoft offers a comprehensive identity & access management solution with integrated security. This solution enhances Zero Trust defenses to offer secure remote access for working during the ongoing pandemic. The Identity & Access Management solution offers robust capabilities such as SSO, MFA, conditional access, identity protection, Privileged Identity Management (PIM), password-less authentication, and external identities.

The Single sign-on (SSO) capability offers a seamless experience to users while protecting organizations. It achieves this by offering only one set of login credentials to access all the apps, without the need to remember numerous credentials or repeating passwords. This capability offers easy access to the user's software as a service (SaaS) apps, cloud apps, or on-premises apps regardless of location with SSO. The SSO capability equips users with seamless sign-in experiences, enhanced employee productivity, improved security, and accelerated IT efficiency.

Microsoft's Multifactor authentication (MFA) capability safeguards enterprises against data breaches caused by lost or stolen credentials with robust authentication and seamless identity. This capability enables a second protection layer when the user attempts to sign in. Users are challenged with additional factors like fingerprints or OTP when they try to access accounts or apps on any device. The conditional access capability allows enterprises to configure and refine or adjust access policies with contextual factors like users, devices, locations, and real-time risk information to manage the resources a specific user can access, as well as the time and means of their access. This capability implements granular access control with real-time adaptive policies.

The identity protection capability protects organizations by securing their identity infrastructure. This capability automates risk detection and remediation for identity-based risks. Further, this capability helps to track users and sign-in risks, create risk

policies that maintain an equilibrium between security and productivity with minimized response time and desk expenses, and prioritize high-risk users with an easy-to-use interface, risk insights, and recommendations.

The Privileged Identity Management (PIM) functionality helps admin accounts stay secure with limited access to crucial operations. This functionality manages, controls, and tracks access rights to vital resources in organizations. This functionality also helps control least privilege access, utilize just-in-time privileged access, and discover & monitor access. The password-less authentication capability offers password-less authentication with new standards like Web Authentication API (WebAuthN) and Fast Identity Online (FIDO2).

Azure AD External identities is equipped with a set of capabilities that organizations can use to secure and control employees, customers, and partners. This capability provides several ways to interact and share resources or apps with users based externally. In addition, the capability helps enable B2B collaboration, built self-service sign-up flows, scale apps to customers, and seamless experience. Azure AD enterprise identity service offers SSO, MFA, and conditional access to safeguard users from online threats. This capability offers benefits such as secure access to apps regardless of location, frictionless sign-in and security for users, and combined internal and external identity management.

Analyst Perspective

Following is the analysis of Microsoft's capabilities in the RBA market:

- Microsoft Security helps protect organizations and people against cyber threats and risks with ML-powered intelligent security solutions powered with automation, helping users to work securely and seamlessly from anywhere regardless of any platform. Azure AD protects identities with secure, adaptive access, simplifies access with seamless end-user experiences, streamlines control with unified identity management, and ensures compliance with simplified identity governance, thus making it a key differentiator.

- The access management solutions, decentralized identity technology offers digital identity and safeguard privacy with fully secure user experiences. Further benefits organization with mitigating risks, using electronic data verification and enhances transparency & auditability. Also beneficial for developers to build user-centric apps and services and build genuine serverless apps which store data along users.

- The company offers Cloud security that can safeguard any app. Azure Security Center enhances multi-cloud security posture. Azure Defender safeguards hybrid clouds workload with Azure Defender, and Github helps create secure

apps. Azure AD also provides an identity control plane in the cloud to help users safeguard identities with secured adaptive access. It also offers simplified access along with smooth end-user experiences and enhanced control with unified identity management and ensures compliance with easy identity governance.

- In terms of geographical perspective, the company has a strong presence across the globe. The company supports multiple use cases through Microsoft Azure AD.

OneSpan

URL: https://www.onespan.com/

Founded in 1991 and headquartered in Chicago, Illinois, OneSpan offers digital identity and anti-fraud solutions across the globe. OneSpan's Intelligent Adaptive Authentication Solution is powered by Trusted Identity Platform. OneSpan offers risk-based authentication through its Intelligent Adaptive Authentication (IAA) solution and offers unique capabilities such as simplifying complex authentication changes, open & future-proof technology systems, orchestration technology, regulatory compliance, visibility to mobile channel integrity, and operational efficiency.

The IAA solution offers robust features like a unique risk analytics engine that leverages ML for enhanced fraud detection, and customized and pre-configured rulesets focuses to manage compliance requirements faster. The solution provides comprehensive visibility to mobile channel integrity, leveraging user, device, and app data from the mobile device comprising OS version, geolocation, device ID, malware detection, and such more. This visibility provides a precise measure of trust through a risk analytics score. The solution uses an advanced user interface to provide a single point of control for several rules, workflows, and actionable authorizations.

OneSpan's IAA solution reviews and scores hundreds of user actions and behavior with device and transaction data in real-time, helping to decide the right authentication requirements for every single transaction. The solution consolidates data from the user's device, mobile apps, and disparate data sources, the user behavior, transactions details, and key contextual data across all the digital channels. Then the solution analyzes and scores single transactions with the help of an ML-driven risk analytics engine, offering a clear fraud view. The solution then takes the required action on the basis of the risk score. Thus, users performing high-risk transactions will be prompted for a step-up authentication process, while funds will be transferred without an additional security layer when the risk score is low. Lastly, the solution ensures the transaction is completed seamlessly.

OneSpan's MFA capability guards accounts and transactions through numerous authentication factors and also fulfills the requirements for a simple sign-in process. This capability enables robust authentication using a broad range of easy verification options such as software authentication, mobile authenticators, SMS delivery, hardware authentication, smart card readers, biometric authentication, push notification, and Cronto visual transaction technology.

The IAA solution is equipped with a feature-rich, centralized management console that enables the addition of new authentication techniques for larger bank communities in just a few minutes, thereby optimizing on time and money. The solution is built on an

open, cloud-based architecture that enables seamless integration of third-party tools and data, which integrates directly into the platform's risk analytics engine and helps accelerate the accuracy if fraud detection through fraud data. OneSpan's IAA solution includes orchestration technology that streamlines deployment and also offers speed-to-market and deployment benefits to organizations.

Analyst Perspective

Following is the analysis of OneSpan's capabilities in the RBA market:

- OneSpan caters to more than 10,000 customers, a majority of them mainly global banks. The OneSpan Intelligent Adaptive Authentication (IAA) solution is based on an open, cloud-based architecture to enable simple and easy integration with new and prevailing tools and technologies that can be leveraged to enhance fraud detection and user experience. The platform unifies MFA, behavioral analysis, biometrics, risk analytics, and mobile app security technologies with the latest cloud, ML, micro-services, and container technologies. The IAA solution offers profound visibility and security for mobile devices and applications through app shielding, device binding, root detection, device ID, secure storage, obfuscation, and such others. The solution enables comprehensive biometric features comprising fingerprint, face recognition, and FaceID.

- The solution offers a prebuilt and customizable ruleset coupled with supervised and unsupervised ML algorithms to enhance fraud detection in real-time, making it a key differentiator. The solution is equipped with a future-proof platform that enables smooth integration with third-party technology. It also supports MFA authentication and transaction signing. The solution enables an extensive combination of software and hardware authentication technology. Further, it supports risk-based authentication orchestration, enabling appropriate security for every unique user journey. Furthermore, the solution provides consistent transaction monitoring to proactively identify and alleviate fraud across digital channels.

- Concerning geographical presence, the company has a strong presence across the globe. The company supports multiple use cases through robust OneSpan Cloud Authentication, secure automation agreement, risk analytics Mobile Security Suite, e-signature platform, OneSpan Mobile Authenticator Studio, Cronto® technology, and OneSpan Authentication Server.

IBM Security

URL: https://www.ibm.com/

Founded in 1911 and headquartered in Armonk, New York, IBM Security is a leading provider of enterprise security products and services worldwide. IBM Security offers a portfolio of advanced and integrated solutions, including identity & access management, data security, SIEM, SOAR, security services, cloud security, and others. IBM Security offers risk-based authentication through its Trusteer Pinpoint Detect and Verify solutions, enabling the prevention of fraudulent activities and high-risk transactions.

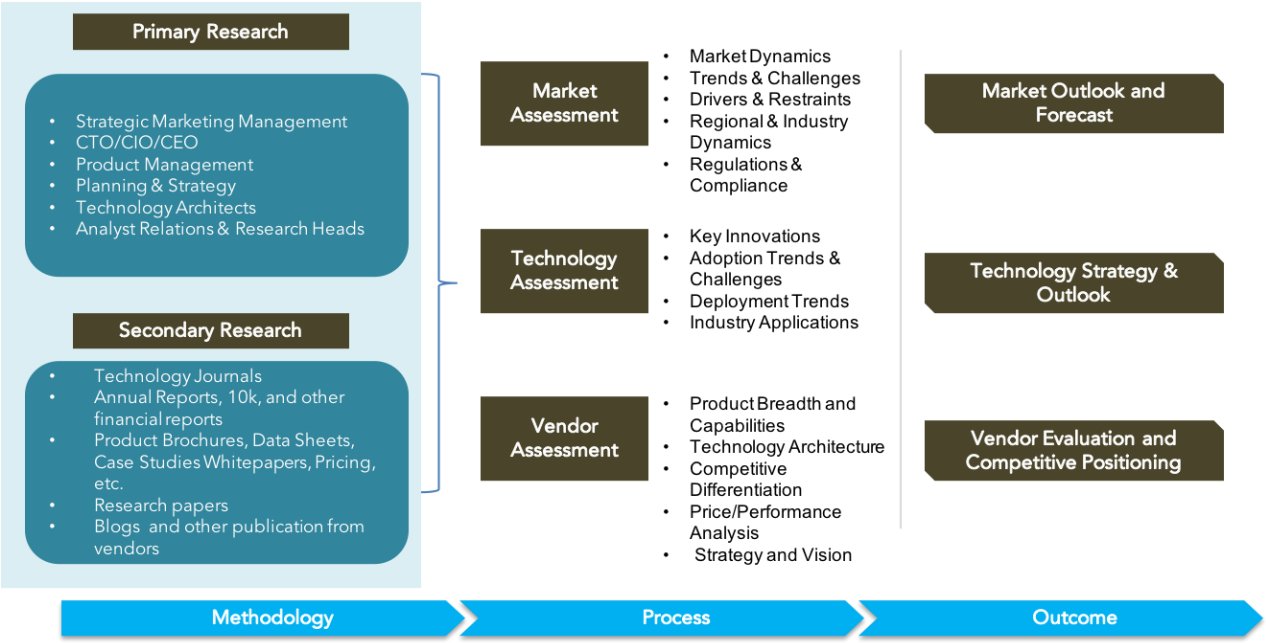
Analyst Perspective

Following is the analysis of IBM Security's capabilities in the RBA market:

- IBM is a leading cloud platform and cognitive solutions provider. The company offers innovative technology products and services to organizations around the globe. IBM Security provides robust risk-based authentication solution that enables secure, frictionless, and risk-aware digital interactions for people, devices, and things across any cloud environment. IBM's RBA inspects a wide range of identity risks, including device data, network connection, passive behavior, anomaly detection, fraud patterns and consortium data, to ensure transparent and evidence-based fraud protection.

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 a 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 whitepapers, 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 research 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.