

## **Risk-based Authentication - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)**

Market Report | 2025-04-28 | 120 pages | Mordor Intelligence

### **AVAILABLE LICENSES:**

- Single User License \$4750.00
- Team License (1-7 Users) \$5250.00
- Site License \$6500.00
- Corporate License \$8750.00

### **Report description:**

The Risk-based Authentication Market is expected to register a CAGR of 18.8% during the forecast period.

#### Key Highlights

- The COVID-19 pandemic has led to significant growth in fraudulent activities across the globe. According to the Federal Trade Commission, in March 2021, more than 217,000 Americans had filed a coronavirus-related fraud report since January 2020, with losses to Covid-linked fraud totaling USD 382 million. Similarly, the Consumer Financial Bureau fielded 542,300 fraud complaints in 2020, a significant 54% increase compared to 2019.
- Furthermore, according to the Association of Certified Fraud Examiners or ACFE, due to the pandemic, the cyber fraud risk significantly increased from 45% in May 2020 to 47% in August 2020. In addition, it is expected that an increase in cyber fraud risk is expected to reach 60% over the next 12 months.
- Digital channels are becoming imperative as consumers interact with businesses and each other. In the digital world, to accommodate their customers and better manage their organizations, companies are becoming increasingly dependent on a web of systems, both on and off their networks. Such systems assist in managing, storing, and transmitting various information, such as financial accounts, intellectual property, personally identifiable information, transaction records, and others.
- In support of this, various organizations are increasingly adopting automation solutions to enable fast workflow and analyze the work processes to improvise the areas that challenge the company's progress. This has resulted in a massive shift from traditional storage and analytics to cloud-based infrastructure and storage technologies. According to a Flexera 2021 State of the Cloud Report, based on a survey of 750 IT professionals, 92% of the respondents have a multi-cloud strategy, while 82% have a hybrid cloud strategy. About 36% of enterprises reported that their annual spend exceeded USD 12 million, and 83% said that cloud spend exceeds USD 1.2 million per year.

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

## Risk-Based Authentication Market Trends

### Banking and Financial Services Hold the Major Share

- Traditional banks have been turning to new and strategically focused agile institutions. The diverse challenges related to the ever-changing complex regulations, intense competition, and demanding customers have resulted in an alignment toward digital transformation.
- Consumer propensity toward banks that offer services with digitalization is increasing. According to a study by Lightico, in March 2020, around 82% of customers were concerned about visiting their branch in person, and 63% mentioned that they are willing to try the digital application. Thus, these shifts are expected to be long-lasting.
- With the growing popularity of digital banking and remote banking via call centers, the requirement for new and convenient ways to authenticate customer identity has been generated. Mobile and e-banking channels are increasingly used every day to transfer and perform transactions, which opens doors to cybercriminals trying to compromise a user's account to extract money. The low-security level of traditional PINs due to customers forgetting their passcodes or being hacked due to phishing and other cybercrimes has led to the rise of more sophisticated authentication mechanisms, like risk-based authentication systems, in the industry.
- Several organizations and governing bodies, such as the Federal Financial Institutions Examination Council (FFIEC), New York State Department of Financial Services (NYDFS), and the Cybersecurity Regulation and National Association of Insurance Commissioners (NAIC), mandated the use of multi-factor authentication (MFA) to protect access to sensitive data for financial institutions, insurers, banks, and many other organizations.
- Data breaches lead to an exponential rise in costs and loss of valuable customer information. According to Identity Theft Resource Center, the number of data breaches in the United States increased from 784 in 2015 to 1,001 in 2020.
- Moreover, the BFSI sector is experiencing an increase in cloud workloads, where a significant amount of data is moved to the cloud. Furthermore, the rising integration of the third party, such as mobile wallets, coupled with complex security infrastructure where many vendors are deployed around the ecosystem, is creating a significant security challenge in the sector.

### North American Expected to Hold Major Share

- The North American region led the market with the United States as the most prominent contributor to the region's market. The businesses in the region are increasingly dependent on computer networks and electronic data to conduct their regular operations. An increasing pool of personal and financial information is also transferred and stored online.
- This is because of the populous nature of the region in terms of organizational data, compared to other regions. Moreover, the United States currently accounts for the largest share in the adoption of cloud technologies and analytics and is expected to show the same trend in 2020.
- The substantial increase in the number of data breaches across various industries boosts companies to adopt robust authentication methods. For instance, according to the White House Council of Economic Advisers, the US economy faces losses of approximately USD 57 billion to USD 109 billion per annum, due to cyber-attacks.
- According to a statistic presented by Experian PLC, 31% of the data breach victims claimed the theft of their identity, like e-mail ids, passwords, credit/debit card numbers, etc. Also, Risk-based Security, an American firm, reported that 2020 has seen over 3,932 data breaches. When compared to 2019, the number of publicly reported breach events decreased by 48%, however, several records exposed exceeded 37 billion. These facts indicate the growing need for the adoption of a risk-based authentication solution in the country.
- Also, the governments in the region have been encouraging the usage of various authentication techniques. For instance, in

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

April 2020, the US government gave federal agencies the flexibility to use alternative authentication forms to fulfill service gaps and achieve their goals. Agencies can make a risk determination and issue an alternate credential or authenticator for PIV eligible personnel. This is anticipated to augment the demand for the adoption of the market studied.

## Risk-Based Authentication Industry Overview

The intensity of competitive rivalry is high as players engage in strategic investments in the form of innovation, mergers and acquisitions, and expansions. Such investments help the companies in further penetrating the market and gain a better market share. There is a presence of major companies in the market which have strong brand identity creating rivalry for gaining higher share. However, the industry is growing rapidly at a CAGR of 18.8%, which provides further room for the growth of players operating in the market.

### Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

### **Table of Contents:**

#### 1 INTRODUCTION

- 1.1 Study Assumptions and Market Definition
- 1.2 Scope of the Study

#### 2 RESEARCH METHODOLOGY

#### 3 EXECUTIVE SUMMARY

#### 4 MARKET INSIGHTS

- 4.1 Market Overview
- 4.2 Industry Attractiveness - Porter's Five Forces Analysis
- 4.3 Technology Snapshot
- 4.4 Assessment of Impact of COVID-19 on the market
- 4.5 Market Drivers
  - 4.5.1 Growing Data Breaches and Cyber Attacks across Key End-user Verticals
  - 4.5.2 Adoption of BYOD Trends in Enterprises
- 4.6 Market Restraints
  - 4.6.1 Growing Pressure to Update Risk Scores in line With Evolving Cyber-security Threats

#### 5 Market SEGMENTATION

- 5.1 By Offering
  - 5.1.1 Solution
  - 5.1.2 Service
- 5.2 By Deployment
  - 5.2.1 On-premise
  - 5.2.2 Cloud
- 5.3 By End-user Vertical
  - 5.3.1 Banking and Financial Services (BFSI)

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

- 5.3.2 Retail
- 5.3.3 IT and Telecommunication
- 5.3.4 Government
- 5.3.5 Healthcare
- 5.3.6 Other End-user Verticals
- 5.4 By Geography
  - 5.4.1 North America
  - 5.4.2 Europe
  - 5.4.3 Asia Pacific
  - 5.4.4 Latin America
  - 5.4.5 Middle East and Africa

## 6 COMPETITIVE LANDSCAPE

- 6.1 Company Profiles
  - 6.1.1 RSA Security LLC
  - 6.1.2 IBM Corporation
  - 6.1.3 Broadcom Inc. (CA Technologies Inc.)
  - 6.1.4 Micro Focus International plc (NetIQ)
  - 6.1.5 Okta Inc.
  - 6.1.6 SecureAuth Corporation
  - 6.1.7 Thales Group (Gemalto N.V.)
  - 6.1.8 Equifax Inc.
  - 6.1.9 Oracle Corporation
  - 6.1.10 HID Global Corporation (Assa Abloy AB)
  - 6.1.11 Financial Software Systems Inc.

## 7 INVESTMENT ANALYSIS

## 8 FUTURE OF THE MARKET

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: [support@scotts-international.com](mailto:support@scotts-international.com)

[www.scotts-international.com](http://www.scotts-international.com)

**Risk-based Authentication - Market Share Analysis, Industry Trends & Statistics,  
Growth Forecasts (2025 - 2030)**

Market Report | 2025-04-28 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:

- Print this form
- Complete the relevant blank fields and sign
- Send as a scanned email to support@scott's-international.com

**ORDER FORM:**

Select license	License	Price
	Single User License	\$4750.00
	Team License (1-7 Users)	\$5250.00
	Site License	\$6500.00
	Corporate License	\$8750.00
		VAT
		Total

\*Please circle the relevant license option. For any questions please contact support@scott's-international.com or 0048 603 394 346.

\*\* VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*	<input type="text"/>	Phone*	<input type="text"/>
First Name*	<input type="text"/>	Last Name*	<input type="text"/>
Job title*	<input type="text"/>		
Company Name*	<input type="text"/>	EU Vat / Tax ID / NIP number*	<input type="text"/>
Address*	<input type="text"/>	City*	<input type="text"/>
Zip Code*	<input type="text"/>	Country*	<input type="text"/>
		Date	<input type="text" value="2026-03-05"/>
		Signature	

**Scotts International. EU Vat number: PL 6772247784**

tel. 0048 603 394 346 e-mail: support@scott's-international.com

www.scott's-international.com

