+357 96 030922
info@marketpublishers.com

Multi-factor Authentication - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2024 - 2029)

https://marketpublishers.com/r/MF593EFA66ACEN.html
Date: July 2024
Pages: 157
Price: US$ 4,750.00 (Single User License)
ID: MF593EFA66ACEN

Abstracts

The Multi-factor Authentication Market size is estimated at USD 18.12 billion in 2024, and is expected to reach USD 38.90 billion by 2029, growing at a CAGR of 16.5% during the forecast period (2024-2029).

With the increasing frequency and sophistication of cyber threats, including phishing attacks and data breaches, organizations are pressured to implement strong security measures such as multi-factor authentication to protect confidential information and prevent unauthorized access. Strict data protection legislation and compliance standards, including the General Data Protection Regulation, Health Insurance Portability and Accountability Act, and PCI Security Standards, drive MFA adoption.

•To drive demand for multi-factor authentication solutions, regulatory compliance is crucial. Governments and industry regulators worldwide, such as the General Data Protection Regulation, HIPAA, or PCI DSS, have set strict security standards to protect sensitive data. Organizations increasingly rely on MFA as a reliable means of enhancing authentication security to comply with these requirements. The failure to comply with these regulations may lead to significant sanctions and possible judicial consequences, making the implementation of MFA a key element in risk mitigation for companies.

•The rising instances of cyber-attacks in various end-user industries, including BFSI, Healthcare, and IT & Telecom, supported by their increasing usage of the internet to have digitalized operational processes, are fueling the demand for multi-factor authentications (MFA) solutions in the market due to their application in adding a layer of protection to the users' access control, endpoint systems or company's data, which

+357 96 030922
info@marketpublishers.com

effectively helps prevent stolen passwords, malware, phishing, and ransomware attacks, driving the growth of the market.

•The emergence of industrial automation and the usage of cloud-based software for automating business functionalities in enterprises are raising the number of IIoTs and the usage of computers in any business environment. This can raise the risk of cyber-attacks and unethical access to the company's business operations and data, fueling the demand for MFA solutions due to their application in providing secure access and authentications before using the devices of the enterprises, which is expected to drive the market's growth during the forecast period.

•One of the biggest challenges for MFA is the increase in management complexity for administrators and end users. In most cases, MFA is complex and not user-friendly as it requires additional steps for end users. As organizations undergo digital transformation, there are challenges associated with complexities in implementing and using multi-factor authentication. Legacy infrastructure, characterized by outdated hardware, software, and protocols, poses limitations to implementing modern cybersecurity measures. Combining these outdated systems with modern technology frequently results in an environment that makes it more challenging to implement and maintain strong cybersecurity frameworks.

•Defense spending in many countries worldwide is increasing due to the strategies to strengthen their geopolitical positions at a global scale, which is driving the demand for cybersecurity solutions as, in the trend of digitalization, cyber wars are becoming more prevalent. Furthermore, the number of cyber-attacks has increased to weaken national security, which shows the importance of adopting cybersecurity solutions in private and government organizations, which could accelerate the demand for MFA in the future.

Multi-factor Authentication Market Trends

Healthcare Sector to be the Fastest Growing End User

The MFA market in the healthcare sector is evolving rapidly, with healthcare organizations increasingly seeking to protect patient data, ensure compliance, and protect against a rapidly changing threat landscape. In the past few years, the growing use of advanced technologies such as AI, ML, and IoT in healthcare has enlarged the attack surface for cybercriminals. In response, healthcare organizations globally are analyzed to increase their investments in cybersecurity to prevent and mitigate cyberattacks, thus driving the market's growth.

+357 96 030922
info@marketpublishers.com

The healthcare sector has become a target of significant interest among cybercriminals due to its generation of valuable data from electronic health records (HER), electronic medical records (EMRs), wearable devices, a range of sensors, IoT platforms, etc. Market vendors are indulging in partnership activities to foster cybersecurity in the healthcare sector, thus significantly expanding the market's growth.

According to the World Economic Forum, in 2023, for the 13th year in a row, the healthcare industry reported the most expensive data breaches, at an average cost of USD 10.93 million, which is almost double that of the financial sector, which came second with an average cost of USD 5.9 million. To maintain the integrity, confidentiality, and availability of patient information, it is necessary to protect such digital assets.

Asia-Pacific is analyzed to hold a significant share of the market. For instance, in April 2024, to make it easier for beneficiaries of the Central Government Health Scheme to access healthcare services, the Union Ministry of Health launched the myCGHS iOS app. Developed by NIC Himachal Pradesh and the NIC Health Team, the app enables appointment booking and accessing health records, lab reports, medicine history, and reimbursement claim status. Two-factor authentication and MPIN are part of the security measures. The launch is a milestone in digital healthcare and will enhance CGHS services. It is available on the App Store and Google Play at no charge. The Union Health Minister emphasized the commitment of the Government to leverage technology to make healthcare accessible.

Overall, the growing adoption of advanced technologies in the healthcare sector, with further growth in connected devices, will require these end-user industries to strengthen their cybersecurity landscape.

North America Holds Significant Market Share

The United States is at the epicenter of cybercrime due to the growing penetration of digital technologies in end-user industries compared to other countries. Businesses in the US face a higher volume of cyberattacks, which incur costly consequences. Cybersecurity has become an increasingly important area of focus in the United States, owing to the rising number of cyber threats and attacks that organizations and individuals face.

+357 96 030922
info@marketpublishers.com

As per the Identity Theft Resource Center (ITRC) report published in February 2024, in 2023, the United States recorded 3,205 data breaches, which is a 78% increase in 2022 and a 72% increase since 2021. Such high-profile data breaches and cybersecurity incidents have raised awareness among businesses and consumers about the importance of implementing robust security measures to safeguard personal and sensitive information. Hence, companies are increasingly adopting multi-factor authentication solutions to help organizations mitigate the risk of account takeover and identity-related fraud.

The increasing frequency of cyber-attacks drives the adoption of multi-factor authentication solutions in the United States. Many organizations in the region are adopting and investing in cybersecurity solutions owing to the growing regulatory requirement and many industries subject to regulations such as GDPR, HIPPA, and PCI DSS. This requires organizations to implement cybersecurity solutions and increase their investments in multi-factor authentication solutions.

As online threats and cyberattacks increase in Canada, the Canadian Government has recognized the importance of safeguarding citizens' and immigrants' sensitive information and personal data. Hence, in July 2023, the Canadian Government made multi-factor authentication mandatory for users accessing immigration, refugees, and citizenship services through GCKey. The new policy applies to individuals creating a new account using GCKey and those signing into their existing accounts. Such adoptions are driving the demand for MFA solutions.

In addition, Canada's demand for data security solutions is continuously growing. Canada has stringent data protection regulations, including the Personal Information Protection and Electronic Documents Act (PIPEDA). Organizations must implement robust data security measures such as MFA solutions to ensure compliance with these regulations, driving the demand for data security solutions. As organizations undergo digital transformation, there is a greater reliance on digital data. Protecting sensitive information throughout its lifecycle, from creation to storage and transmission, becomes a critical aspect of digital initiatives.

Therefore, the increasing number of cybercrimes and data and security breaches in Canada fuel the adoption of multi-factor authentication, which is expected to increase for securing digital identities, owing to the increasing number of identity theft cases across the industries, supporting the market’s growth.

+357 96 030922
info@marketpublishers.com

Multi-factor Authentication Industry Overview

The multi-factor authentication market is fragmented due to the presence of both global players and small and medium-sized enterprises. Some of the major players in the market are Yubico AB, Giesecke+Devrient GmbH, Thetis, GoTrustid Inc., and Thales. Players in the market are adopting strategies such as partnerships and acquisitions to enhance their product offerings and gain sustainable competitive advantage.

•In February 2024, Giesecke+Devrient expanded its digital portfolio in the financial platforms business by increasing its stake in the software company Netcetera to broaden its product portfolio in the areas of digital payment and digital banking, which would create an opportunity for the company to offer MFA-based solutions to the financial industries in the market, which would support the growth of the company’s market presence in the future.

•In November 2023 - Okta Inc. partnered with Trio, a Mobile Device Management (MDM) solution, enabling Trio to provide a comprehensive solution for managing and securing devices in workplaces of any size, which would fuel the growth of the company's market presence in the MFA market supported by the company's strategic focus on developing solutions in the identity access management solutions in the market.

Additional Benefits:

The market estimate (ME) sheet in Excel format

3 months of analyst support

+357 96 030922
info@marketpublishers.com

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 Analysis of Macro Eeconomic Scenarios
4.3 Insights on the Regulatory Landscape Related to Cyber Security

5 MARKET DYNAMICS

5.1 Market Drivers
  5.1.1 Rising Cybercrime, Digital Disruption, and Increased Compliance Demands
  5.1.2 Rising Adoption of Interconnected Devices
  5.1.3 Increased Instances of Identity Theft and Fraud
5.2 Market Challenges
  5.2.1 Lack of Technical Expertise
  5.2.2 Complexities in Implementing and Using Multi-factor Authentication
5.3 Market Opportunities
  5.3.1 Standards/Specifications for Authentication Solutions (ACE, FBA, FIDO, etc.)
  5.3.2 Pricing Analysis for MFA Tools (Hardware and Software)

6 MARKET SEGMENTATION

6.1 By Offering Type
  6.1.1 Hardware
    6.1.1.1 Token
    6.1.1.2 Biometric Devices
    6.1.1.3 Other Devices
  6.1.2 Software
    6.1.2.1 Authenticator Solutions

+357 96 030922
info@marketpublishers.com

6.1.2.2 Mobile Apps
6.1.3 Services
6.2 By Authentication Type
6.2.1 Two-factor Authentication
6.2.2 Three-factor Authentication
6.2.3 Four-factor Authentication
6.2.4 Other Types of Authentication
6.3 By End-user Industry
6.3.1 Banking and Financial Institutions
6.3.2 Cryptocurrency
6.3.3 Technology-based Companies (SaaS & IT Service Vendors)
6.3.4 Government - Federal, State, and Local Entities (Including System Integrators)
6.3.5 Healthcare and Pharmaceutical
6.3.6 Retail and E-commerce
6.3.7 Process-based Applications - Energy and Manufacturing
6.3.8 Other End-user Verticals - Education, Immigration, Etc.
6.4 By Geography***
6.4.1 North America
6.4.1.1 United States
6.4.1.2 Canada
6.4.2 Europe
6.4.2.1 United Kingdom
6.4.2.2 Germany
6.4.2.3 France
6.4.3 Asia-Pacific
6.4.3.1 China
6.4.3.2 India
6.4.3.3 Japan
6.4.3.4 Australia and New Zealand
6.4.4 Latin America
6.4.5 Middle East and Africa

7 COMPETITIVE LANDSCAPE

7.1 Vendor Positioning Analysis
7.2 Company Profiles*
7.2.1 Yubico AB
7.2.2 Giesecke+Devrient GmbH
7.2.3 Thetis

+357 96 030922
info@marketpublishers.com

7.2.4 GoTrustid Inc.
7.2.5 Thales
7.2.6 Duo (Cisco Systems Inc.)
7.2.7 RSA SECURITY LLC
7.2.8 Okta Inc.
7.2.9 Google LLC (ALPHABET INC.)
7.2.10 Ping Identity Corporation
7.2.11 ManageEngine (Zoho Corporation Pvt. Ltd)
7.2.12 Microsoft Corporation
7.2.13 Telesign Corporation (Proximus Group)

8 FUTURE OUTLOOK OF THE MARKET

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Multi-factor Authentication - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2024 - 2029)

Product link: https://marketpublishers.com/r/MF593EFA66ACEN.html

Price: US$ 4,750.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:
info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/MF593EFA66ACEN.html