Multifactor Authentication (MFA) - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 159 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 Multifactor Authentication Market size is estimated at USD 21.11 billion in 2025, and is expected to reach USD 45.30 billion by 2030, at a CAGR of 16.5% during the forecast period (2025-2030).

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, are driving 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, IT, and telecom, supported by their increasing usage of the internet to have digitalized operational processes, are fueling the demand for multi-factor authentication (MFA) solutions in the market. MFA adds a layer of protection to the user's access control, endpoint systems, or company data, which effectively helps prevent stolen passwords, malware, phishing, and ransomware attacks.

Multi-factor authentication (MFA) has been significantly used to enhance security measures in the Industrial Internet of Things (IIoT). It helps integrate two or more authentication factors such as biometrics, possession, one-time passwords (OTP), timestamps, challenges, and passwords, which can be used for the secure access of IIOT users, network administrators, and maintenance personnel, driving the demand for NFA solution in the market in line with the growth of IIOT worldwide.

Technology is only one of the components of MFA. Effective data security primarily requires the best practices of MFA, including detailed policies and procedures for handling and storing critical data and dealing with security violations. An effective MFA also depends upon the IT staff's knowledge of data security requirements and end-user awareness of data security practices.

Furthermore, the Israel-Palestine issue has also prompted an increase in cyber attacks. For instance, various hacktivist groups have targeted critical infrastructure, government agencies, and organizations in both Israel and Palestine. DDoS attacks, defacements, and data breaches are also included in these attacks. As other countries take a stand on the war, the conflict has spread beyond the immediate region, affecting several other countries. Therefore, the growing geopolitical concerns are expected to cause several cyber threats, indicating an upward trend in adopting and implementing cybersecurity strategies and solutions during the forecast period.

Multifactor Authentication (MFA) Market Trends

Two-factor Authentication Type to Witness Major Growth

- There has been a growing demand for two-factor authentication globally as it adds a layer of authentication, typically requiring something the user knows, such as a password or an OTP. This multi-tiered approach significantly reduces the vulnerability to phishing attempts and credential stuffing, thereby providing strong security to digital assets.
- Additionally, the growing number of data breaches and cyber-attacks has underscored the inadequacy of reliance solely on passwords. The compromised credentials of one platform often serve as the keys to unlocking multiple accounts, leading to reduced breaches with far-reaching repercussions. Due to this, most companies are integrating two-factor authentication into their authentication frameworks. With this, organizations can eliminate unauthorized access even during password compromises, driving the demand for two-factor authentication.
- Furthermore, as the demand grows, most companies have started implementing two-factor authentication systems to provide more security to their users, driving the market's growth. For instance, in April 2024, the Pension Fund Regulatory and Development Authority (PFRDA) of India announced that the organization planned to revamp its current login process for the National Pension System (NPS) to enhance its security system. The organization has implemented a two-factor Aadhaar authentication and made the new security mandatory for all password-based users logging into the Central Recordkeeping Agency system of the NPS.
- Furthermore, the growing cloud-based services and the advent of Internet of Things (IoT) devices have expanded the cyber threats exponentially. As of March 2023, GSMA reported that the Internet of Things (IoT) connections across the world in enterprises are increasing significantly, and these connections would reach 44 billion by 2030, raising the risk of data breaches. Due to this, cloud service providers and enterprises have started implementing two-factor authentication, which can authenticate users and devices across disparate platforms and environments.

North America Holds the Largest Market Share

- The United States faces a sophisticated and evolving cyber threat landscape. It 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 United States face a higher volume of cyber-attacks, which incur costly consequences. Cybersecurity has become an increasingly important area of focus in the country, owing to the rising number of cyber threats and attacks that organizations and individuals face.

- Additionally, as per the Identity Theft Resource Center (ITRC) report published in February 2024, in 2023, the United States recorded 3,205 data breaches, a 78% increase from 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 cybersecurity market in Canada is evolving with the increasing digitalization trends in the private and public sectors. For instance, the country's energy sector is witnessing a transformation driven by digital technologies such as cloud, AI, IoT, and quantum computing. As the industry evolves, the country's cybersecurity demand is growing.
- The shift toward cloud deployment of security solutions to minimize the total cost of ownership is anticipated to offer multi-factor authentication solution providers the opportunity to develop solutions to suit customer demands in the country.

Multifactor Authentication (MFA) Market 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.

- February 2024 - Giesecke+Devrient bolstered its digital portfolio in financial platforms by increasing its stake in software firm Netcetera. This move aims to enhance Giesecke+Devrient's offerings in digital payments and banking, paving the way for the company to introduce MFA-based solutions to the financial sector, thereby strengthening its market presence.
- November 2023 - Okta Inc. teamed up with Trio, a mobile device management (MDM) provider. This collaboration empowers Trio to deliver a holistic solution for device management and security across workplaces of all sizes. This partnership is poised to amplify Okta's footprint in the MFA market, aligning with its strategic emphasis on identity access management solutions.

Additional Benefits:

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

Table of Contents:

SCOTTS
INTERNATIONAL

Multifactor Authentication (MFA) - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 159 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@scotts-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@scotts-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*

Phone*

First Name*

Last Name*

Job title*

Company Name*

EU Vat / Tax ID / NIP number*

Address*

City*

Zip Code*

Country*

Date 2026-03-05

Signature