

Identity & Access Management (IAM) Market Forecasts to 2032 – Global Analysis By Component (Solutions and Services), Deployment Mode, Authentication Type, Organization Size, User Type, End User and By Geography

<https://marketpublishers.com/r/I85E44DC6FFDEN.html>

Date: December 2025

Pages: 200

Price: US\$ 4,150.00 (Single User License)

ID: I85E44DC6FFDEN

Abstracts

According to Statistics MRC, the Global Identity & Access Management (IAM) Market is accounted for \$23.97 billion in 2025 and is expected to reach \$62.23 billion by 2032 growing at a CAGR of 14.6% during the forecast period. Identity & Access Management (IAM) refers to a structured system of tools, rules, and procedures designed to verify users and regulate their access to organizational resources. It helps businesses manage digital identities, validate user authentication, and assign appropriate access rights. IAM strengthens security measures, maintains regulatory compliance, minimizes exposure to threats, and streamlines operations through automated account handling, continuous access oversight, and unified governance across all platforms.

According to ForgeRock, 80.0% of IT decision-makers have adopted, expanded, or plan to adopt cloud-based solutions. Thus, the rising adoption of cloud-based solutions by SMEs drives segment growth.

Market Dynamics:

Driver:

Adoption of cloud and hybrid infrastructures

As businesses expand digital services, they require IAM systems that seamlessly authenticate users across public, private, and on-premise environments. Hybrid setups

allow enterprises to retain sensitive data internally while leveraging the scalability of cloud identity platforms. The rise of SaaS adoption is pushing companies to adopt centralized access management frameworks. Modern IAM tools equipped with automation and AI are becoming essential to managing complex, distributed IT ecosystems. As a result, adoption of cloud-enabled IAM platforms continues to accelerate across industries.

Restraint:

Lack of skilled cybersecurity professionals

Complex architectures involving multi-cloud, privileged access, and identity lifecycle management require deep technical expertise. Many organizations face delays in rollout and increased dependency on external service providers because of this talent gap. Misconfigurations in IAM implementations often arise from insufficient knowledge of security policies and standards. The constant evolution of identity threats demands continuous upskilling, which many enterprises cannot maintain internally. This lack of skilled professionals remains a significant obstacle to scaling IAM capabilities effectively.

Opportunity:

Shift to zero trust architecture (ZTA)

Zero trust frameworks rely heavily on continuous authentication, identity verification, and contextual access controls. Enterprises adopting ZTA require advanced IAM tools to enforce strict access governance and micro-segmentation. Increased remote work and distributed networks are accelerating the demand for ZTA-aligned identity solutions. Regulatory pressures are further motivating organizations to implement identity-centric security frameworks. As ZTA becomes a mainstream security model, IAM vendors are well positioned to expand their offerings and market reach.

Threat:

Data privacy and consent hurdles

Laws such as GDPR, HIPAA, and national data protection acts require careful handling of identity data. Failure to secure sensitive user information can result in severe financial penalties and reputational damage. Cross-border data transfers add

complexity to IAM operations in multinational enterprises. Consent-based access controls demand transparent data practices and continuous user communication. These regulatory and privacy constraints pose significant risks for IAM vendors and adopters alike.

Covid-19 Impact:

The pandemic accelerated the adoption of IAM solutions as remote work increased the need for secure digital access. Organizations rapidly adopted cloud identity services to support remote authentication and multi-factor verification. Businesses also recognized gaps in access governance as employees accessed sensitive systems from various locations. IAM providers introduced scalable solutions to meet the surge in digital identity workloads. The shift toward hybrid work models has made strong identity management a permanent priority.

The hybrid segment is expected to be the largest during the forecast period

The hybrid segment is expected to account for the largest market share during the forecast period, as organizations balance flexibility, security, and control. Enterprises prefer hybrid IAM models to maintain sensitive identity data on-premises while using cloud platforms for scalability. This approach helps businesses meet compliance requirements without sacrificing operational efficiency. Hybrid IAM also enables seamless integration with legacy applications that cannot be fully migrated to the cloud. Advancements in API-based identity orchestration are making hybrid deployments more efficient.

The healthcare segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the healthcare segment is predicted to witness the highest growth rate, due to heightened security and compliance requirements. Hospitals and providers must protect sensitive patient records while enabling secure access for clinicians and administrators. The rise of telehealth services has further increased the need for robust identity verification systems. Healthcare organizations are integrating MFA, biometric authentication, and privileged access tools to reduce breach risks. Growing cybersecurity incidents targeting medical systems are pushing institutions to upgrade identity infrastructures.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, due to strong technological maturity and widespread cybersecurity adoption. The presence of major IAM vendors in the U.S. continues to strengthen regional market leadership. Enterprises in regulated sectors such as finance and healthcare lead the demand for advanced identity solutions. Federal and state-level cybersecurity mandates further accelerate IAM deployment. Widespread adoption of cloud and hybrid infrastructures contributes to growing identity management needs.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, owing to rapid digital acceleration across emerging economies. Growing investments in cloud services, e-governance, and cybersecurity are boosting IAM adoption. Enterprises in sectors like BFSI, healthcare, and retail are upgrading identity infrastructures at a fast pace. Regional governments are promoting data protection laws that necessitate stronger identity governance solutions. Expanding mobile and internet penetration is increasing demand for secure user authentication.

Key players in the market

Some of the key players in Identity & Access Management (IAM) Market include Microsoft, Okta, Inc., Ping Identity, CyberArk, SailPoint, ForgeRock, IBM Corp, Oracle Corp, Google LLC, Amazon Web, BeyondTrust, One Identity, Thales Group, RSA Secur, and HID Global.

Key Developments:

In November 2025, IBM and the University of Dayton announced an agreement for the joint research and development of next-generation semiconductor technologies and materials. The collaboration aims to advance critical technologies for the age of AI including AI hardware, advanced packaging, and photonics.

In October 2025, Oracle announced collaboration with Microsoft to develop an integration blueprint to help manufacturers improve supply chain efficiency and responsiveness. The blueprint will enable organizations using Oracle Fusion Cloud Supply Chain & Manufacturing (SCM) to improve data-driven decision making and automate key supply chain processes by capturing live insights from factory equipment and sensors through Azure IoT Operations and Microsoft Fabric.

Components Covered:

Solutions

Services

Deployment Modes Covered:

On-Premises

Cloud (SaaS / IDaaS)

Hybrid

Authentication Types Covered:

Password-Based Authentication

Multi-Factor Authentication (MFA)

Adaptive / Risk-Based Authentication

Passwordless Authentication

Biometrics

Blockchain / Decentralized Identity

Organization Sizes Covered:

Large Enterprises

Small & Medium Enterprises (SMEs)

User Types Covered:

Workforce IAM

Customer IAM (CIAM)

B2B / Partner IAM

Machine Identities / IoT IAM

End Users Covered:

BFSI

IT & Telecom

Manufacturing

Government & Public Sector

Education

Healthcare

Energy & Utilities

Retail & E-commerce

Regions Covered:

North America

US

Canada

Mexico

Europe

Germany

UK

Italy

France

Spain

Rest of Europe

Asia Pacific

Japan

China

India

Australia

New Zealand

South Korea

Rest of Asia Pacific

South America

Argentina

Brazil

Chile

Rest of South America

Middle East & Africa

Saudi Arabia

UAE

Qatar

South Africa

Rest of Middle East & Africa

What our report offers:

- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2024, 2025, 2026, 2028, and 2032
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market estimations
- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

Contents

1 EXECUTIVE SUMMARY

2 PREFACE

- 2.1 Abstract
- 2.2 Stake Holders
- 2.3 Research Scope
- 2.4 Research Methodology
 - 2.4.1 Data Mining
 - 2.4.2 Data Analysis
 - 2.4.3 Data Validation
 - 2.4.4 Research Approach
- 2.5 Research Sources
 - 2.5.1 Primary Research Sources
 - 2.5.2 Secondary Research Sources
 - 2.5.3 Assumptions

3 MARKET TREND ANALYSIS

- 3.1 Introduction
- 3.2 Drivers
- 3.3 Restraints
- 3.4 Opportunities
- 3.5 Threats
- 3.6 End User Analysis
- 3.7 Emerging Markets
- 3.8 Impact of Covid-19

4 PORTERS FIVE FORCE ANALYSIS

- 4.1 Bargaining power of suppliers
- 4.2 Bargaining power of buyers
- 4.3 Threat of substitutes
- 4.4 Threat of new entrants
- 4.5 Competitive rivalry

5 GLOBAL IDENTITY & ACCESS MANAGEMENT (IAM) MARKET, BY COMPONENT

5.1 Introduction

5.2 Solutions

5.2.1 Identity Governance & Administration (IGA)

5.2.2 Identity Analytics & Fraud Detection

5.2.3 Access Management / Single Sign-On (SSO)

5.2.4 Passwordless Authentication & Biometrics

5.2.5 Multi-Factor Authentication (MFA)

5.2.6 Identity Federation (OAuth, SAML, OIDC)

5.2.7 Privileged Access Management (PAM)

5.2.8 Directory Services

5.2.9 Customer Identity & Access Management (CIAM)

5.3 Services

5.3.1 Professional Services

5.3.2 Implementation & Integration

5.3.3 Managed Services

5.3.4 Support & Maintenance

6 GLOBAL IDENTITY & ACCESS MANAGEMENT (IAM) MARKET, BY DEPLOYMENT MODE

6.1 Introduction

6.2 On-Premises

6.3 Cloud (SaaS / IDaaS)

6.4 Hybrid

7 GLOBAL IDENTITY & ACCESS MANAGEMENT (IAM) MARKET, BY AUTHENTICATION TYPE

7.1 Introduction

7.2 Password-Based Authentication

7.3 Multi-Factor Authentication (MFA)

7.4 Adaptive / Risk-Based Authentication

7.5 Passwordless Authentication

7.6 Biometrics

7.7 Blockchain / Decentralized Identity

8 GLOBAL IDENTITY & ACCESS MANAGEMENT (IAM) MARKET, BY ORGANIZATION SIZE

- 8.1 Introduction
- 8.2 Large Enterprises
- 8.3 Small & Medium Enterprises (SMEs)

9 GLOBAL IDENTITY & ACCESS MANAGEMENT (IAM) MARKET, BY USER TYPE

- 9.1 Introduction
- 9.2 Workforce IAM
- 9.3 Customer IAM (CIAM)
- 9.4 B2B / Partner IAM
- 9.5 Machine Identities / IoT IAM

10 GLOBAL IDENTITY & ACCESS MANAGEMENT (IAM) MARKET, BY END USER

- 10.1 Introduction
- 10.2 BFSI
- 10.3 IT & Telecom
- 10.4 Manufacturing
- 10.5 Government & Public Sector
- 10.6 Education
- 10.7 Healthcare
- 10.8 Energy & Utilities
- 10.9 Retail & E-commerce

11 GLOBAL IDENTITY & ACCESS MANAGEMENT (IAM) MARKET, BY GEOGRAPHY

- 11.1 Introduction
- 11.2 North America
 - 11.2.1 US
 - 11.2.2 Canada
 - 11.2.3 Mexico
- 11.3 Europe
 - 11.3.1 Germany
 - 11.3.2 UK
 - 11.3.3 Italy
 - 11.3.4 France
 - 11.3.5 Spain

- 11.3.6 Rest of Europe
- 11.4 Asia Pacific
 - 11.4.1 Japan
 - 11.4.2 China
 - 11.4.3 India
 - 11.4.4 Australia
 - 11.4.5 New Zealand
 - 11.4.6 South Korea
 - 11.4.7 Rest of Asia Pacific
- 11.5 South America
 - 11.5.1 Argentina
 - 11.5.2 Brazil
 - 11.5.3 Chile
 - 11.5.4 Rest of South America
- 11.6 Middle East & Africa
 - 11.6.1 Saudi Arabia
 - 11.6.2 UAE
 - 11.6.3 Qatar
 - 11.6.4 South Africa
 - 11.6.5 Rest of Middle East & Africa

12 KEY DEVELOPMENTS

- 12.1 Agreements, Partnerships, Collaborations and Joint Ventures
- 12.2 Acquisitions & Mergers
- 12.3 New Product Launch
- 12.4 Expansions
- 12.5 Other Key Strategies

13 COMPANY PROFILING

- 13.1 Microsoft Corporation
- 13.2 Okta, Inc.
- 13.3 Ping Identity Corporation
- 13.4 CyberArk Software Ltd.
- 13.5 SailPoint Technologies
- 13.6 ForgeRock, Inc.
- 13.7 IBM Corporation
- 13.8 Oracle Corporation

- 13.9 Google LLC
- 13.10 Amazon Web Services (AWS)
- 13.11 BeyondTrust
- 13.12 One Identity
- 13.13 Thales Group
- 13.14 RSA Security
- 13.15 HID Global

List Of Tables

LIST OF TABLES

Table 1 Global Identity & Access Management (IAM) Market Outlook, By Region (2024-2032) (\$MN)

Table 2 Global Identity & Access Management (IAM) Market Outlook, By Component (2024-2032) (\$MN)

Table 3 Global Identity & Access Management (IAM) Market Outlook, By Solutions (2024-2032) (\$MN)

Table 4 Global Identity & Access Management (IAM) Market Outlook, By Identity Governance & Administration (IGA) (2024-2032) (\$MN)

Table 5 Global Identity & Access Management (IAM) Market Outlook, By Identity Analytics & Fraud Detection (2024-2032) (\$MN)

Table 6 Global Identity & Access Management (IAM) Market Outlook, By Access Management / Single Sign-On (SSO) (2024-2032) (\$MN)

Table 7 Global Identity & Access Management (IAM) Market Outlook, By Passwordless Authentication & Biometrics (2024-2032) (\$MN)

Table 8 Global Identity & Access Management (IAM) Market Outlook, By Multi-Factor Authentication (MFA) (2024-2032) (\$MN)

Table 9 Global Identity & Access Management (IAM) Market Outlook, By Identity Federation (OAuth, SAML, OIDC) (2024-2032) (\$MN)

Table 10 Global Identity & Access Management (IAM) Market Outlook, By Privileged Access Management (PAM) (2024-2032) (\$MN)

Table 11 Global Identity & Access Management (IAM) Market Outlook, By Directory Services (2024-2032) (\$MN)

Table 12 Global Identity & Access Management (IAM) Market Outlook, By Customer Identity & Access Management (CIAM) (2024-2032) (\$MN)

Table 13 Global Identity & Access Management (IAM) Market Outlook, By Services (2024-2032) (\$MN)

Table 14 Global Identity & Access Management (IAM) Market Outlook, By Professional Services (2024-2032) (\$MN)

Table 15 Global Identity & Access Management (IAM) Market Outlook, By Implementation & Integration (2024-2032) (\$MN)

Table 16 Global Identity & Access Management (IAM) Market Outlook, By Managed Services (2024-2032) (\$MN)

Table 17 Global Identity & Access Management (IAM) Market Outlook, By Support & Maintenance (2024-2032) (\$MN)

Table 18 Global Identity & Access Management (IAM) Market Outlook, By Deployment

Mode (2024-2032) (\$MN)

Table 19 Global Identity & Access Management (IAM) Market Outlook, By On-Premises (2024-2032) (\$MN)

Table 20 Global Identity & Access Management (IAM) Market Outlook, By Cloud (SaaS / IDaaS) (2024-2032) (\$MN)

Table 21 Global Identity & Access Management (IAM) Market Outlook, By Hybrid (2024-2032) (\$MN)

Table 22 Global Identity & Access Management (IAM) Market Outlook, By Authentication Type (2024-2032) (\$MN)

Table 23 Global Identity & Access Management (IAM) Market Outlook, By Password-Based Authentication (2024-2032) (\$MN)

Table 24 Global Identity & Access Management (IAM) Market Outlook, By Multi-Factor Authentication (MFA) (2024-2032) (\$MN)

Table 25 Global Identity & Access Management (IAM) Market Outlook, By Adaptive / Risk-Based Authentication (2024-2032) (\$MN)

Table 26 Global Identity & Access Management (IAM) Market Outlook, By Passwordless Authentication (2024-2032) (\$MN)

Table 27 Global Identity & Access Management (IAM) Market Outlook, By Biometrics (2024-2032) (\$MN)

Table 28 Global Identity & Access Management (IAM) Market Outlook, By Blockchain / Decentralized Identity (2024-2032) (\$MN)

Table 29 Global Identity & Access Management (IAM) Market Outlook, By Organization Size (2024-2032) (\$MN)

Table 30 Global Identity & Access Management (IAM) Market Outlook, By Large Enterprises (2024-2032) (\$MN)

Table 31 Global Identity & Access Management (IAM) Market Outlook, By Small & Medium Enterprises (SMEs) (2024-2032) (\$MN)

Table 32 Global Identity & Access Management (IAM) Market Outlook, By User Type (2024-2032) (\$MN)

Table 33 Global Identity & Access Management (IAM) Market Outlook, By Workforce IAM (2024-2032) (\$MN)

Table 34 Global Identity & Access Management (IAM) Market Outlook, By Customer IAM (CIAM) (2024-2032) (\$MN)

Table 35 Global Identity & Access Management (IAM) Market Outlook, By B2B / Partner IAM (2024-2032) (\$MN)

Table 36 Global Identity & Access Management (IAM) Market Outlook, By Machine Identities / IoT IAM (2024-2032) (\$MN)

Table 37 Global Identity & Access Management (IAM) Market Outlook, By End User (2024-2032) (\$MN)

Table 38 Global Identity & Access Management (IAM) Market Outlook, By BFSI (2024-2032) (\$MN)

Table 39 Global Identity & Access Management (IAM) Market Outlook, By IT & Telecom (2024-2032) (\$MN)

Table 40 Global Identity & Access Management (IAM) Market Outlook, By Manufacturing (2024-2032) (\$MN)

Table 41 Global Identity & Access Management (IAM) Market Outlook, By Government & Public Sector (2024-2032) (\$MN)

Table 42 Global Identity & Access Management (IAM) Market Outlook, By Education (2024-2032) (\$MN)

Table 43 Global Identity & Access Management (IAM) Market Outlook, By Healthcare (2024-2032) (\$MN)

Table 44 Global Identity & Access Management (IAM) Market Outlook, By Energy & Utilities (2024-2032) (\$MN)

Table 45 Global Identity & Access Management (IAM) Market Outlook, By Retail & E-commerce (2024-2032) (\$MN)

Note: Tables for North America, Europe, APAC, South America, and Middle East & Africa Regions are also represented in the same manner as above.

I would like to order

Product name: Identity & Access Management (IAM) Market Forecasts to 2032 – Global Analysis By Component (Solutions and Services), Deployment Mode, Authentication Type, Organization Size, User Type, End User and By Geography

Product link: <https://marketpublishers.com/r/l85E44DC6FFDEN.html>

Price: US\$ 4,150.00 (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/l85E44DC6FFDEN.html>