

IAM Security Services Market Forecasts to 2032 – Global Analysis By Component (Solutions, Platforms, and Services), Service Type, Deployment Type, Organization Size, End User and By Geography

<https://marketpublishers.com/r/I906CEA2CBF4EN.html>

Date: September 2025

Pages: 200

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

ID: I906CEA2CBF4EN

Abstracts

According to Statistics MRC, the Global IAM Security Services Market is accounted for \$23.48 billion in 2025 and is expected to reach \$67.57 billion by 2032 growing at a CAGR of 16.3% during the forecast period. IAM (Identity and Access Management) Security Services encompass strategies and tools designed to grant appropriate access to authorized individuals at the right time and for valid purposes. They cover authentication, authorization, access management, and identity governance to safeguard data, applications, and systems. By overseeing digital identities and permissions, IAM services strengthen security, support regulatory compliance, mitigate risks, and simplify user access across varied IT infrastructures.

According to ForgeRock, 80.0% of IT decision-makers have adopted, expanded, or plan to adopt cloud-based solutions in 2021.

Market Dynamics:

Driver:

Growing digital transformation and cloud adoption

Growing digital transformation and cloud adoption is significantly accelerating the demand for IAM security services. As enterprises migrate workloads to cloud environments, the need for robust identity governance and access control intensifies. Cloud-native IAM solutions offer scalability, centralized policy enforcement, and

seamless integration across hybrid infrastructures. The proliferation of remote work and BYOD policies further amplifies the need for secure authentication and user provisioning. Additionally, digital-first strategies across sectors from banking to healthcare require advanced IAM frameworks to manage identities. This transformation is driving innovation in zero-trust architectures, federated identity models, and adaptive access technologies.

Restraint:

Complexity of implementation and integration

Organizations often struggle with legacy systems, fragmented identity repositories, and inconsistent access policies. Integrating IAM solutions across diverse platforms—cloud, on-premises, and mobile requires significant technical expertise and time. Misalignment between IT and security teams can lead to configuration errors and compliance gaps. Moreover, customizing IAM frameworks to meet industry-specific regulations adds further complexity. These challenges slow down deployment timelines and increase operational costs, deterring smaller enterprises from full-scale implementation.

Opportunity:

Adoption of AI and machine learning

AI-driven analytics enable real-time anomaly detection, risk-based authentication, and predictive access control. Machine learning models continuously adapt to user behavior, reducing false positives and enhancing threat response. These technologies also automate identity lifecycle management, improving efficiency and reducing human error. As cyber threats grow more sophisticated, AI-powered IAM tools offer proactive defense mechanisms. The convergence of IAM with AI and big data is reshaping identity governance, making it more intelligent, scalable, and resilient.

Threat:

Data privacy and sovereignty concerns

IAM systems handle sensitive user credentials, access logs, and behavioral data, making them prime targets for breaches. Compliance with global regulations like GDPR, CCPA, and India's DPDP Act requires stringent data handling protocols. Cross-border data flows and third-party integrations further complicate privacy management. A single

misconfiguration or breach can lead to reputational damage and legal penalties. These concerns are prompting organizations to adopt localized data storage and privacy-by-design principles, but they also increase implementation complexity.

Covid-19 Impact:

The COVID-19 pandemic accelerated the adoption of IAM security services across industries. With remote work becoming the norm, organizations faced urgent needs for secure access to cloud applications and internal systems. IAM solutions enabled multi-factor authentication, role-based access, and real-time monitoring to support distributed workforces. The crisis also highlighted vulnerabilities in legacy access controls, prompting rapid modernization. Overall, the pandemic served as a catalyst for IAM innovation, driving demand for scalable, cloud-native, and AI-enhanced identity solutions.

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

The solutions segment is expected to account for the largest market share during the forecast period, due to escalating cyber risks, widespread cloud adoption, and the normalization of remote work—all of which necessitate robust, scalable identity management. Core solutions include MFA, identity governance frameworks, and AI/ML-powered access controls. The rise of zero-trust models and password less authentication is transforming traditional security approaches. Compliance requirements such as GDPR and CCPA, along with rapid digitalization in industries like BFSI, healthcare, and IT, are intensifying market growth.

The IT & telecom segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the IT & telecom segment is predicted to witness the highest growth rate, due to its vast digital infrastructure, high data sensitivity, and growing cyber threats. Adoption of technologies like multi-factor authentication (MFA), identity federation, and AI-based access controls is accelerating. Emerging trends such as zero-trust architecture, passwordless authentication, and decentralized identity are reshaping security frameworks. Key developments include cloud-native IAM deployments, integration with 5G networks, and enhanced identity governance to support scalability, compliance, and secure user access across complex ecosystems.

Region with largest share:

During the forecast period, the Asia Pacific region is expected to hold the largest market share, driven by rapid digital transformation, rising cyberattacks, and expanding cloud adoption across sectors. Governments and enterprises are embracing technologies like MFA, single sign-on (SSO), and AI-powered identity analytics. Emerging trends include zero-trust frameworks, biometric authentication, and mobile-first IAM solutions. Key developments involve regulatory initiatives, increased investment in cloud-native IAM platforms, and strategic partnerships to enhance identity governance, scalability, and secure access in hybrid IT environments.

Region with highest CAGR:

Over the forecast period, the North America region is anticipated to exhibit the highest CAGR, due to the escalating threat landscape, characterized by sophisticated cyberattacks and data breaches, compels organizations to prioritize robust security. Stringent regulatory frameworks like HIPAA and CCPA also mandate strong access controls and data protection, accelerating IAM adoption. Furthermore, the widespread shift to cloud-based technologies, remote work, and the growth of non-human identities are creating new security perimeters that require advanced IAM solutions to manage and secure access effectively. The emerging trend of Zero Trust security and the integration of AI and machine learning for adaptive authentication are driving the market.

Key players in the market

Some of the key players in IAM Security Services Market include IBM, Google, Microsoft, Cisco Systems, Oracle, Amazon Web Services, Okta, Dell Technologies, Ping Identity, Hewlett Packard Enterprise (HPE), CyberArk, Thales Group, ForgeRock, Broadcom, and SailPoint Technologies.

Key Developments:

In July 2025, IBM and Elior Group announce their association to create an “agentic AI & Data Factory” to serve Elior Group's innovation, digital transformation, and improved operational performance. This collaboration represents a major step forward in the innovation and digitization of the Elior Group, a world leader in contract catering and services for businesses and local authorities.

In May 2025, Cisco announced a groundbreaking initiative with HUMAIN – Saudi

Arabia's new AI enterprise – to help build the world's most open, scalable, resilient and cost-efficient AI infrastructure. This landmark collaboration will set a new standard for how AI infrastructure is designed, secured and delivered – combining Cisco's global expertise with the Kingdom's bold AI ambitions.

In April 2025, Ping Identity announced its newly redesigned Nexus Partner Program, which includes enhanced offerings, go-to-market opportunities, and benefits for partners of all types. The new program rewards and recognizes partners for their deep knowledge of Ping's solutions, empowering them to deliver the level of expertise, experience, and results that exceed customer expectations.

Components Covered:

Solutions

Platforms

Services

Service Types Covered:

Identity Management as a Service (IDaaS)

Multi-Factor Authentication (MFA)

Access Management as a Service (AMaaS)

Single Sign-On (SSO)

Privileged Access Management (PAM)

Directory-as-a-Service (DaaS)

Deployment Types Covered:

Cloud-Based

On-Premises

Hybrid

Organization Sizes Covered:

Large Enterprises

Small and Medium Enterprises (SMEs)

End Users Covered:

Banking, Financial Services, and Insurance (BFSI)

IT & Telecom

Education

Healthcare

Retail & E-commerce

Manufacturing

Government

Energy

Other End Users

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 IAM SECURITY SERVICES MARKET, BY COMPONENT

- 5.1 Introduction
- 5.2 Solutions
- 5.3 Platforms
- 5.4 Services

6 GLOBAL IAM SECURITY SERVICES MARKET, BY SERVICE TYPE

- 6.1 Introduction
- 6.2 Identity Management as a Service (IDaaS)
- 6.3 Multi-Factor Authentication (MFA)
- 6.4 Access Management as a Service (AMaaS)
- 6.5 Single Sign-On (SSO)
- 6.6 Privileged Access Management (PAM)
- 6.7 Directory-as-a-Service (DaaS)

7 GLOBAL IAM SECURITY SERVICES MARKET, BY DEPLOYMENT TYPE

- 7.1 Introduction
- 7.2 Cloud-Based
- 7.3 On-Premises
- 7.4 Hybrid

8 GLOBAL IAM SECURITY SERVICES MARKET, BY ORGANIZATION SIZE

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

9 GLOBAL IAM SECURITY SERVICES MARKET, BY END USER

- 9.1 Introduction
- 9.2 Banking, Financial Services, and Insurance (BFSI)
- 9.3 IT & Telecom
- 9.4 Education
- 9.5 Healthcare
- 9.6 Retail & E-commerce
- 9.7 Manufacturing
- 9.8 Government

9.9 Energy

9.10 Other End Users

10 GLOBAL IAM SECURITY SERVICES MARKET, BY GEOGRAPHY

10.1 Introduction

10.2 North America

10.2.1 US

10.2.2 Canada

10.2.3 Mexico

10.3 Europe

10.3.1 Germany

10.3.2 UK

10.3.3 Italy

10.3.4 France

10.3.5 Spain

10.3.6 Rest of Europe

10.4 Asia Pacific

10.4.1 Japan

10.4.2 China

10.4.3 India

10.4.4 Australia

10.4.5 New Zealand

10.4.6 South Korea

10.4.7 Rest of Asia Pacific

10.5 South America

10.5.1 Argentina

10.5.2 Brazil

10.5.3 Chile

10.5.4 Rest of South America

10.6 Middle East & Africa

10.6.1 Saudi Arabia

10.6.2 UAE

10.6.3 Qatar

10.6.4 South Africa

10.6.5 Rest of Middle East & Africa

11 KEY DEVELOPMENTS

- 11.1 Agreements, Partnerships, Collaborations and Joint Ventures
- 11.2 Acquisitions & Mergers
- 11.3 New Product Launch
- 11.4 Expansions
- 11.5 Other Key Strategies

12 COMPANY PROFILING

- 12.1 IBM
- 12.2 Google
- 12.3 Microsoft
- 12.4 Cisco Systems
- 12.5 Oracle
- 12.6 Amazon Web Services
- 12.7 Okta
- 12.8 Dell Technologies
- 12.9 Ping Identity
- 12.10 Hewlett Packard Enterprise (HPE)
- 12.11 CyberArk
- 12.12 Thales Group
- 12.13 ForgeRock
- 12.14 Broadcom
- 12.15 SailPoint Technologies

List Of Tables

LIST OF TABLES

Table 1 Global IAM Security Services Market Outlook, By Region (2024-2032) (\$MN)

Table 2 Global IAM Security Services Market Outlook, By Component (2024-2032) (\$MN)

Table 3 Global IAM Security Services Market Outlook, By Solutions (2024-2032) (\$MN)

Table 4 Global IAM Security Services Market Outlook, By Platforms (2024-2032) (\$MN)

Table 5 Global IAM Security Services Market Outlook, By Services (2024-2032) (\$MN)

Table 6 Global IAM Security Services Market Outlook, By Service Type (2024-2032) (\$MN)

Table 7 Global IAM Security Services Market Outlook, By Identity Management as a Service (IDaaS) (2024-2032) (\$MN)

Table 8 Global IAM Security Services Market Outlook, By Multi-Factor Authentication (MFA) (2024-2032) (\$MN)

Table 9 Global IAM Security Services Market Outlook, By Access Management as a Service (AMaaS) (2024-2032) (\$MN)

Table 10 Global IAM Security Services Market Outlook, By Single Sign-On (SSO) (2024-2032) (\$MN)

Table 11 Global IAM Security Services Market Outlook, By Privileged Access Management (PAM) (2024-2032) (\$MN)

Table 12 Global IAM Security Services Market Outlook, By Directory-as-a-Service (DaaS) (2024-2032) (\$MN)

Table 13 Global IAM Security Services Market Outlook, By Deployment Type (2024-2032) (\$MN)

Table 14 Global IAM Security Services Market Outlook, By Cloud-Based (2024-2032) (\$MN)

Table 15 Global IAM Security Services Market Outlook, By On-Premises (2024-2032) (\$MN)

Table 16 Global IAM Security Services Market Outlook, By Hybrid (2024-2032) (\$MN)

Table 17 Global IAM Security Services Market Outlook, By Organization Size (2024-2032) (\$MN)

Table 18 Global IAM Security Services Market Outlook, By Large Enterprises (2024-2032) (\$MN)

Table 19 Global IAM Security Services Market Outlook, By Small and Medium Enterprises (SMEs) (2024-2032) (\$MN)

Table 20 Global IAM Security Services Market Outlook, By End User (2024-2032) (\$MN)

Table 21 Global IAM Security Services Market Outlook, By Banking, Financial Services, and Insurance (BFSI) (2024-2032) (\$MN)

Table 22 Global IAM Security Services Market Outlook, By IT & Telecom (2024-2032) (\$MN)

Table 23 Global IAM Security Services Market Outlook, By Education (2024-2032) (\$MN)

Table 24 Global IAM Security Services Market Outlook, By Healthcare (2024-2032) (\$MN)

Table 25 Global IAM Security Services Market Outlook, By Retail & E-commerce (2024-2032) (\$MN)

Table 26 Global IAM Security Services Market Outlook, By Manufacturing (2024-2032) (\$MN)

Table 27 Global IAM Security Services Market Outlook, By Government (2024-2032) (\$MN)

Table 28 Global IAM Security Services Market Outlook, By Energy (2024-2032) (\$MN)

Table 29 Global IAM Security Services Market Outlook, By Other End Users (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: IAM Security Services Market Forecasts to 2032 – Global Analysis By Component (Solutions, Platforms, and Services), Service Type, Deployment Type, Organization Size, End User and By Geography

Product link: <https://marketpublishers.com/r/I906CEA2CBF4EN.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/I906CEA2CBF4EN.html>