Identity and Access Management
Market Guide

Volume 1, 2025

TABLE OF CONTENTS

VENDOR DIRECTORY

METHODOLOGY

To produce a comprehensive and reliable analysis of the Identity and Access Management vendor ecosystem for 2025, ISMG employed a proprietary, AI-driven methodology that combined automation, structured data modeling, and editorial oversight. To enhance the credibility and accuracy of our 2025 Identity and Access Management Market Guide, we've integrated advanced AI techniques and benchmarks focused on mitigating hallucinations in large language models (LLMs). This approach ensures that our vendor profiles are grounded in factual information, aligning with the latest industry standards for AI reliability.

- **AI-Powered Vendor Intelligence**
  At the core of our methodology is ISMG's Apollo AI workflow engine, which processes and synthesizes extensive vendor information from publicly available sources. This includes product descriptions, media mentions, analyst reports, press releases, and SEC filings. The data is normalized to maintain consistency across vendors, regardless of company size or language used in public messaging.

- **Structured Profile Generation and Hallucination Mitigation**
  Each vendor's dataset is processed through Apollo AI, a proprietary framework designed to minimize hallucinations. To maintain the highest standard of factual accuracy in AI-generated outputs, our Anti-Hallucination Architecture integrates a multilayered system of safeguards and validation mechanisms:

  1. **Sophisticated Verification Systems**
     At the core of the architecture lies an advanced verification engine that continuously cross-checks generated content against reliable and pre-validated data sources. This ensures that outputs remain aligned with established facts and domain-specific knowledge.

  2. **Continuous Data Validation**
     Rather than relying solely on pre-generation checks, the system employs ongoing validation processes throughout the inference pipeline. This proactive approach identifies and corrects inconsistencies in real time, minimizing the risk of hallucinated or misleading content.

3. Post-Processing Verification Filters

Even after generation, outputs undergo rigorous filtering using post-processing verification layers. These filters apply rule-based and ML-driven checks to catch residual errors or unsupported claims, further bolstering trustworthiness.

4. Grounding in Validated Data Only

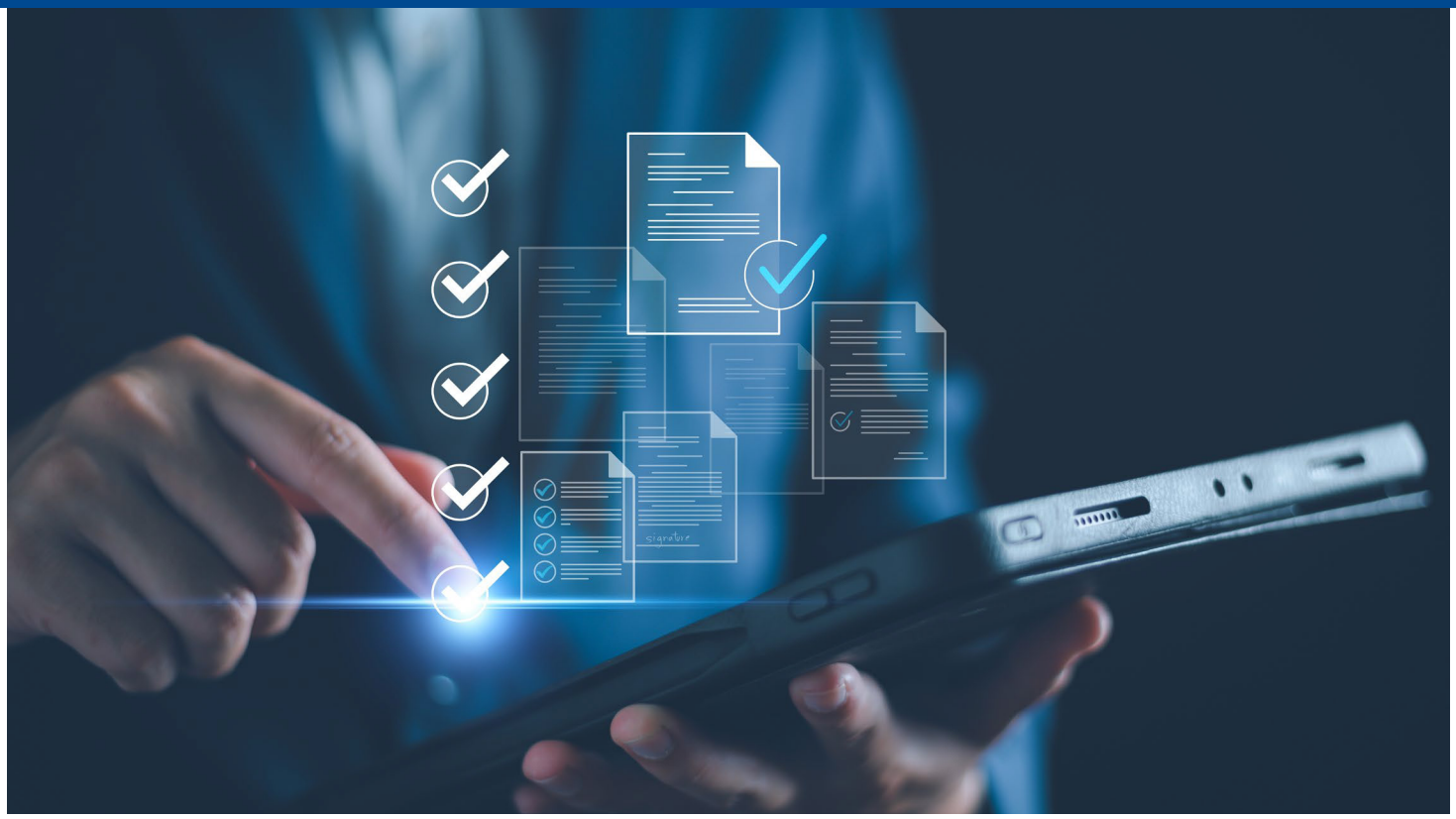
All outputs are firmly grounded in verified data repositories. The architecture prohibits the inclusion of unvalidated or speculative information, ensuring that every response is both accurate and contextually relevant.

- **Summarization for Print and Web**

  To maintain readability in the print version of the guide, long-form vendor profiles are summarized while preserving key insights.

- **Scope and Update Timeline**

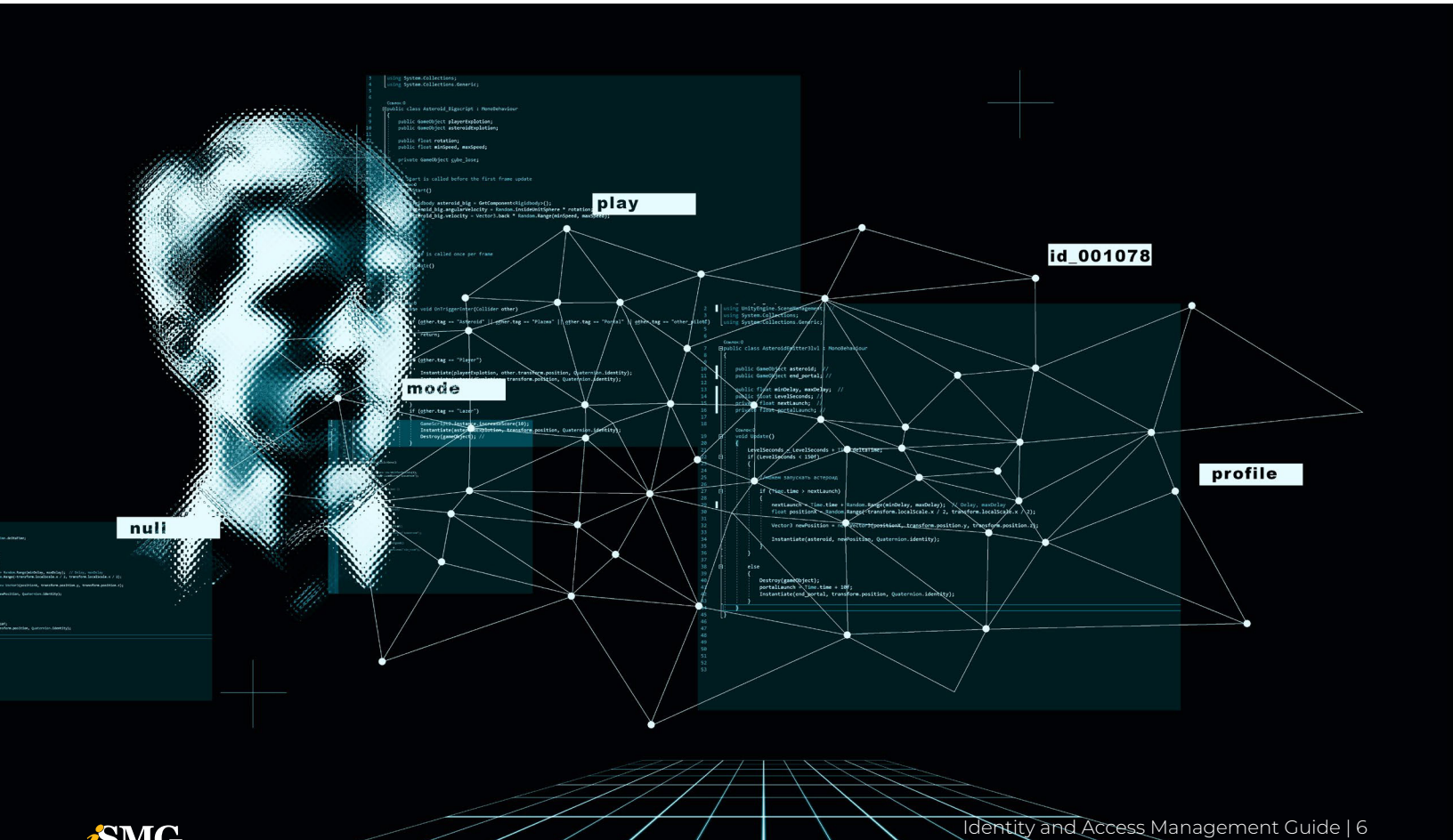
  This guide reflects the state of the Identity and Access Management market as of February 1, 2025. Vendors included are relevant to core IAM categories such as IGA, PAM, CIAM, Access Management and SSO, and Decentralized Identity.



THE IDENTITY AND ACCESS MANAGEMENT VENDOR MARKET IN 2025:
A COMPREHENSIVE ANALYSIS

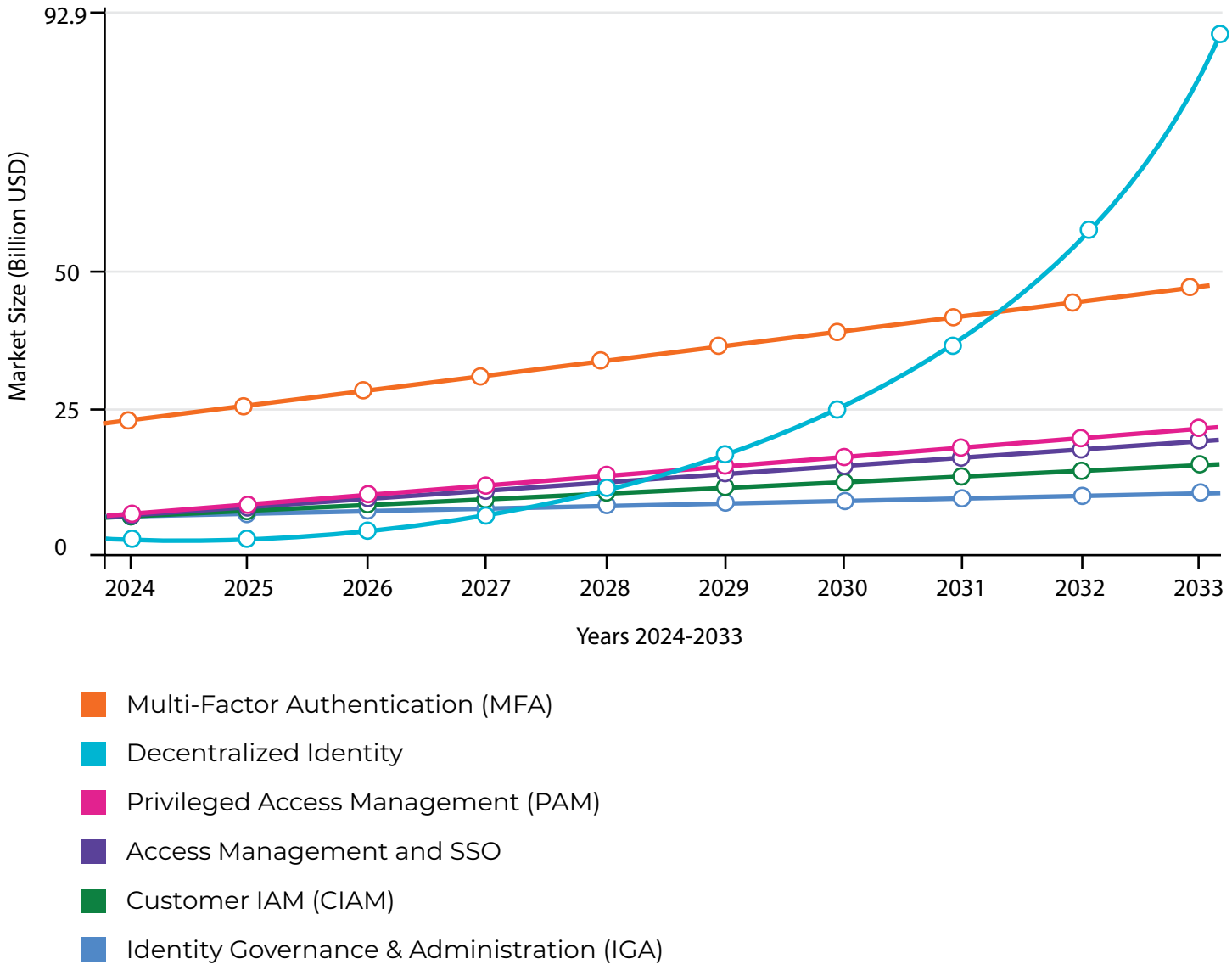
Introduction to the Identity and Access Management (IAM) Market in 2025

Identity and Access Management (IAM) has evolved from a niche security solution to a foundational pillar of modern cybersecurity and business enablement. As organizations navigate a complex web of cloud services, remote work, digital transformation and escalating cyberthreats, IAM emerges as the linchpin that governs who can access what - and under what circumstances. The 2025 IAM market reflects this critical role, characterized by robust growth, technological innovation and the convergence of identity with broader security strategies.



IAM Market Projected Growth (2024-2033)

This timeline shows the projected growth of each IAM market segment over time, based on current CAGR estimates. Note that growth rates will likely fluctuate over time, particularly for emerging segments like Decentralized Identity.

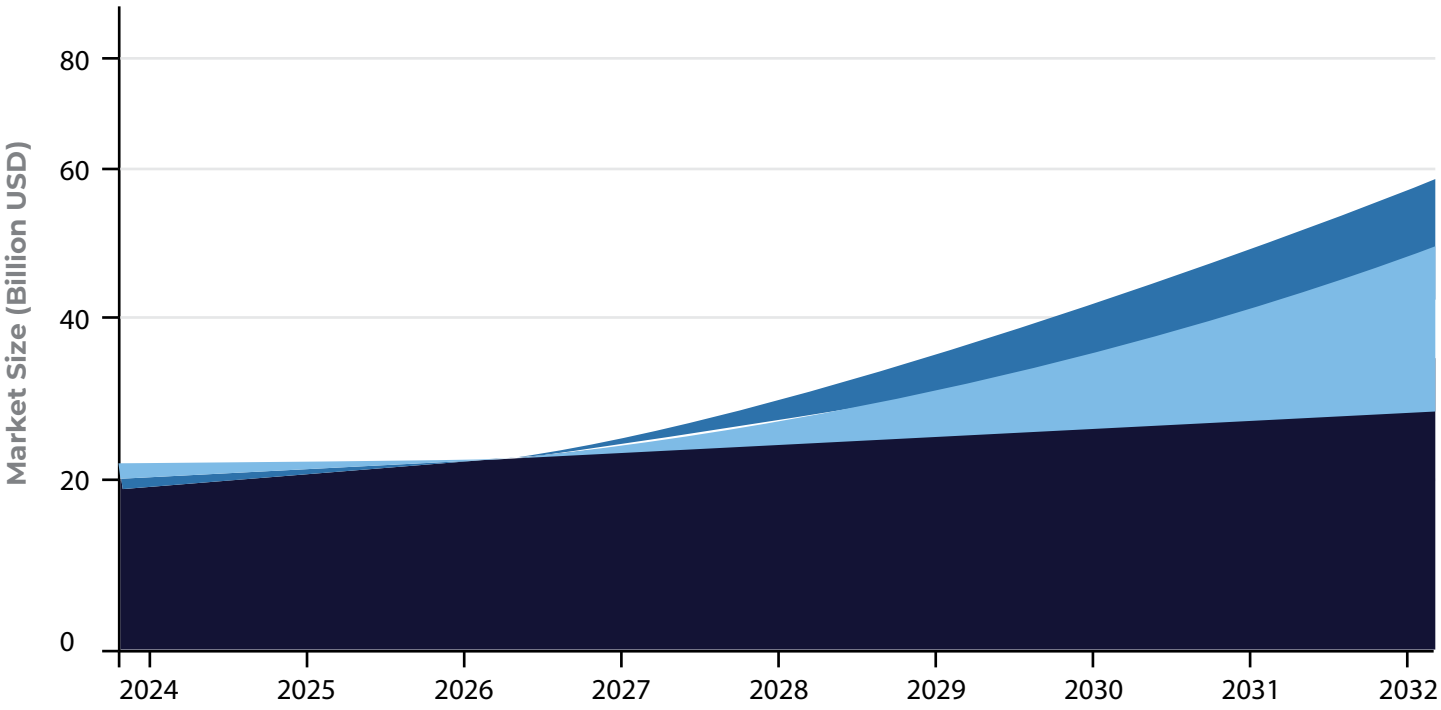


Market Size and Forecast

The global IAM market is expected to surpass $24 billion by 2025, with some forecasts offering even steeper projections. MarketsandMarkets estimates growth from $22.9 billion in 2024 to $34.3 billion by 2029 at a CAGR of 8.4%[1]. Fortune Business Insights projects the market to reach $61.7 billion by 2032, growing at a CAGR of 15.3%[2]. This growth is driven by the adoption of cloud services, regulatory demands, digital identity expansion and increasing credential-based threats.

IAM Market Size Projections (2024-2032)

Chart View | Table View | Line Chart | Area Chart



- MarketsandMarkets (8.4% CAGR)
- Identity Management Institute (13% CAGR)
- Fortune Business Insights (15.3% CAGR)

Key Insights:

- Fortune Business Insights has the most aggressive projection with 15.3% CAGR, reaching $61.7B by 2032
- MarketsandMarkets offers the most conservative outlook with 8.4% CAGR
- Identity Management Institute's projection (13% CAGR) falls between the other two
- By 2029, projections range from $34.3B (MarketsandMarkets) to approximately $48.8B (Fortune Business Insights)

Data sources: Identity Management Institute, MarketsandMarkets, Fortune Business Insights

Note: Projections are based on reported CAGR values and may not reflect all market variables.

IAM Market Size Projections (2024-2032) - Table View

Chart View | Table View

Year	Identity Management Institute (13% CAGR)	MarketsandMarkets (8.4% CAGR)	Fortune Business Insights (15.3% CAGR)
2024	$21.2B	$22.9B	$19.8B
2025	$24.0B	$24.8B	$22.8B
2026	$27.1B	$26.9B	$26.3B
2027	$30.6B	$29.2B	$30.3B
2028	$34.6B	$31.6B	$34.9B
2029	$39.1B	$34.3B	$40.3B
2030	$44.2B	$37.2B	$46.4B
2031	$50.0B	$40.3B	$53.5B
2032	$56.5B	$43.7B	$61.7B

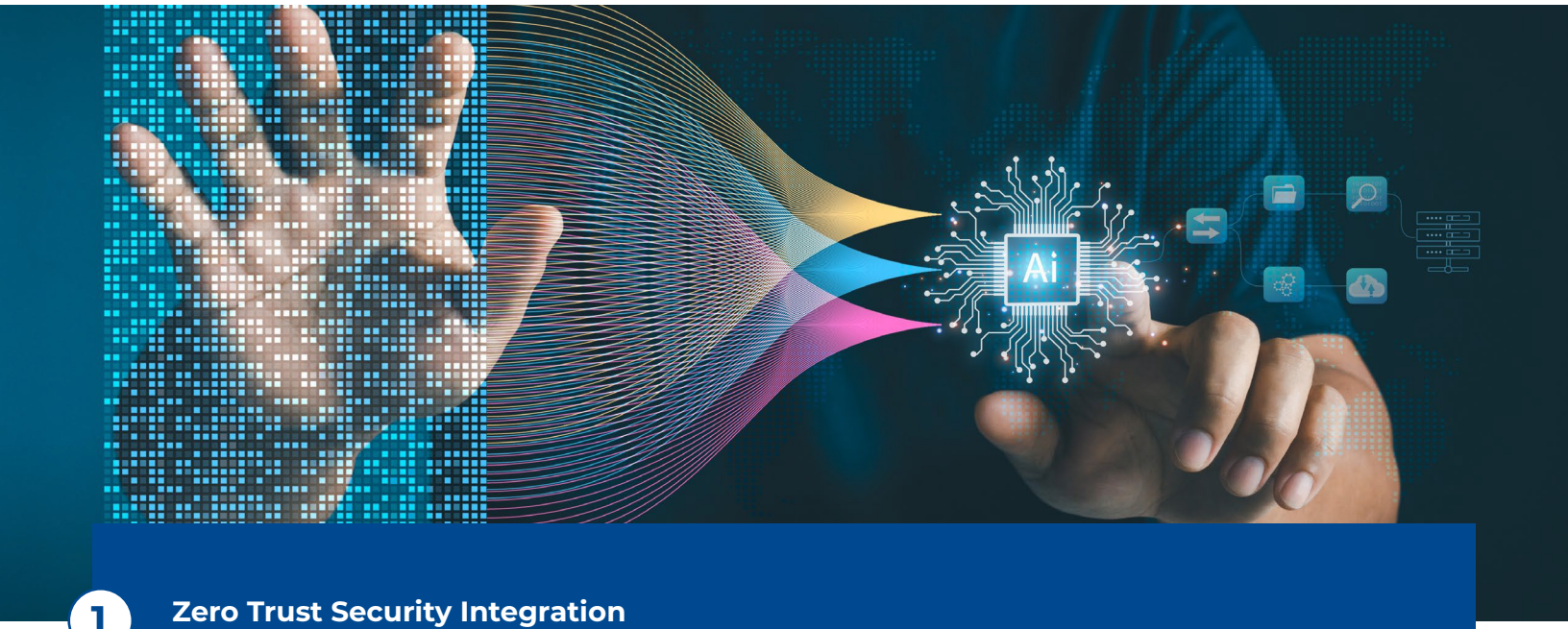
Key Insights:

- Fortune Business Insights has the most aggressive projection with 15.3% CAGR, reaching $61.7B by 2032
- MarketsandMarkets offers the most conservative outlook with 8.4% CAGR
- Identity Management Institute's projection (13% CAGR) falls between the other two
- By 2029, projections range from $34.3B (MarketsandMarkets) to approximately $48.8B (Fortune Business Insights)

Data sources: Identity Management Institute, MarketsandMarkets, Fortune Business Insights

Note: Projections are based on reported CAGR values and may not reflect all market variables.

KEY TECHNOLOGIES DRIVING **IAM IN 2025**



1 **Zero Trust Security Integration**

IAM is central to zero trust security, which treats identity as the new perimeter. 81% of organizations report at least partial implementation of zero-trust frameworks[3]. IAM systems now verify user/device identities continuously, apply least-privilege access and perform real-time risk assessments. Core technologies include conditional access, session management and continuous authentication.

2 **Artificial Intelligence (AI) and Machine Learning (ML)**

AI and ML technologies enable intelligent access decisions, behavioral anomaly detection and life cycle automation. AI-driven IAM can recommend access policies, automate onboarding and identify risky behaviors[4]. Intelligent agents and chat-based interfaces are emerging in access request workflows, enhancing efficiency and experience.

3 **Passwordless Authentication and Advanced Multifactor Authentication (MFA)**

Passwordless methods - passkeys, FIDO2 and biometrics - are gaining traction. Over 1 billion users have enabled at least one passkey, with 69% of consumers recognizing them as more secure and convenient. MFA is now a baseline control, projected to grow from $10.3 billion in 2025 to $32.8 billion by 2035, at a CAGR of 12.4%[5].

4

Identity Fabric and Unified Platforms

Identity fabric architectures unify IAM across cloud and on-premises environments. They integrate single sign-on (SSO), governance, directories and analytics in a service mesh. Gartner and vendors such as Condatis highlight identity fabric as foundational to secure access[6], simplifying deployments and reducing silos in hybrid IT.

5

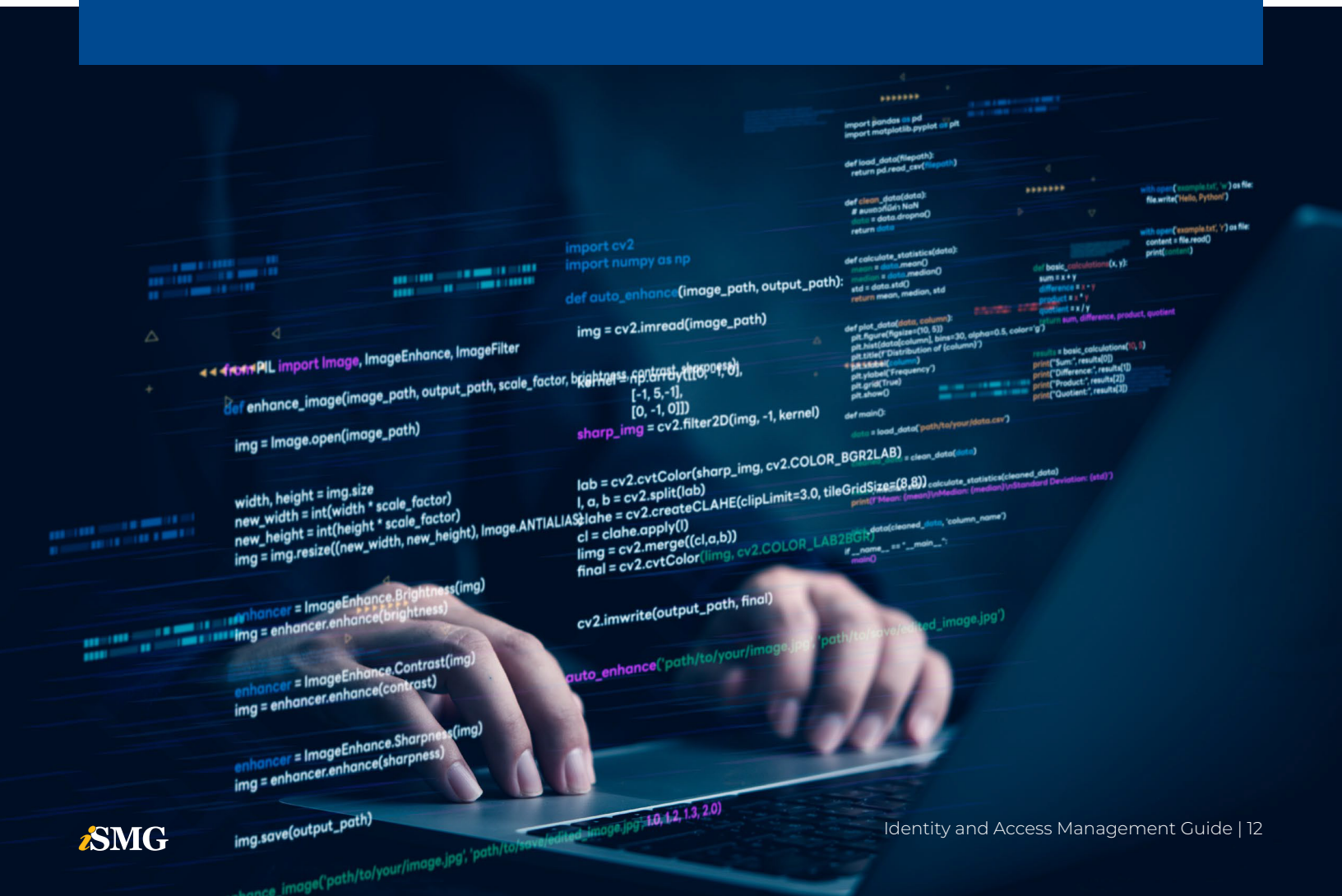
Cloud IAM and Identity as a Service (IDaaS)

Cloud-delivered IAM (IDaaS) is growing rapidly. The market is expected to reach $63.65 billion by 2033, growing at a CAGR of 24.7%[7]. Platforms such as Microsoft Entra and Okta lead with scalable, low-maintenance solutions across workforce and consumer identity use cases.

6

Convergence with EDR and ITDR

IAM is converging with Endpoint Detection and Response (EDR) and Identity Threat Detection and Response (ITDR). By correlating identity data with device telemetry, companies such as Microsoft and CrowdStrike enable risk-based access decisions and real-time threat prevention aligned with zero trust policies.



KEY IAM MARKET **SEGMENTS**

IAM in 2025 comprises several interconnected submarkets.

- **Identity Governance and Administration (IGA):** Managing identity lifecycles, role-based access, and compliance reporting. The IGA software market is forecasted to grow to $5.8 billion by 2027.
- **Privileged Access Management (PAM):** Securing administrative accounts, session monitoring, and JIT privilege elevation. PAM is expected to reach $5.2 billion by 2025.
- **Customer IAM (CIAM):** Managing millions of external user identities with a focus on scalability, privacy, and user experience. The CIAM market is growing at ~13% annually, driven by digital transformation and privacy regulations.
- **Access Management and SSO:** Federated identity, SSO, and risk-based authentication. The access management market grew 17.6% in 2023, with strong growth expected through 2027.
- **Multi-Factor Authentication (MFA):** A market projected to reach nearly $20 billion by 2025, with an emphasis on phishing-resistant and passwordless methods.
- **Decentralized Identity:** An emerging segment using blockchain and verifiable credentials to give users more control over their identities. Forecasts predict a growth from $1.15 billion in 2024 to potentially $89.6 billion by 2033, although this segment is still in early stages.

Identity and Access Management (IAM) Market Segments

Identity Governance & Administration (IGA) CAGR

Managing identity lifecycles, role-based access, and compliance reporting.

+8.8% CAGR

2024 Market Size	2025 Projected
$4.5B	$5.8B

Privileged Access Management (PAM) CAGR

Securing administrative accounts, session monitoring, and JIT privilege elevation.

+30% CAGR

2024 Market Size	2025 Projected
$4.8B	$5.6B

Customer IAM (CIAM) CAGR

Managing millions of external user identities with focus on scalability, privacy, and user experience.

+13% CAGR

2024 Market Size	2025 Projected

Access Management and SSO CAGR

Federated identity, SSO, and risk-based authentication.

+17.6% CAGR

2024 Market Size	2025 Projected
$4.8B	$5.6B

Multi-Factor Authentication (MFA) CAGR

A market with emphasis on phishing-resistant and passwordless methods.

+21.2% CAGR

2024 Market Size	2025 Projected
$16.5B	$20B

Decentralized Identity

An emerging segment using blockchain and verifiable credentials to give users more control over their identities.

+8.8% CAGR

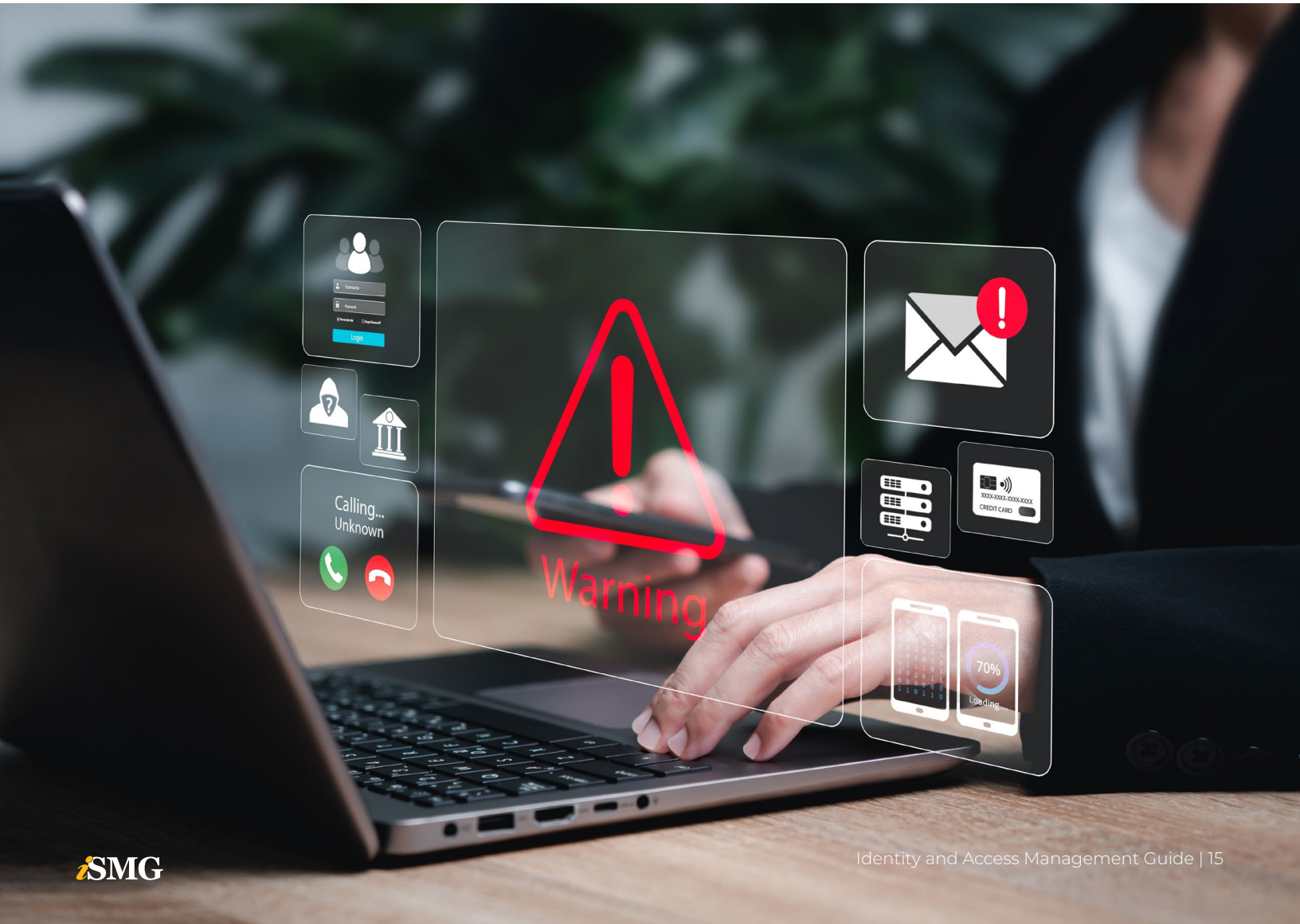
2024 Market Size	2025 Projected
$4.5B	$5.8B

Data sources: Industry forecasts and market analysis reports.

Note: Projections are based on reported growth rates and may not reflect all market variables. Decentralized Identity in particular has a wide range of potential outcomes.

MARKET DYNAMICS AND **CHALLENGES**

The IAM market's growth is driven by regulatory compliance - such as GDPR, SOX and PCI DSS - digital transformation and increasing cyberthreats. But implementation remains complex. Integrating modern IAM with legacy systems, managing identity sprawl and balancing security with user experience are top challenges. Many organizations are adopting identity brokers and phased modernization strategies to ease integration, while managed IAM services are emerging to address skills gaps and operational complexity. Identity-related attacks such as phishing, credential stuffing and MFA bypass remain persistent threats, underscoring the need for advanced threat detection and risk-based IAM capabilities. IAM is no longer just an access control tool; it's a dynamic security platform that blends authentication, governance, analytics and risk management to protect the modern enterprise.



CONCLUSION

The IAM market in 2025 is defined by dynamic growth, technological innovation and a strategic shift toward identity as a cornerstone of enterprise security. As organizations adopt zero trust architectures, embrace AI-driven security automation and move toward cloud-native solutions, IAM stands at the forefront of these transformations. Vendors and customers alike must navigate a complex landscape of technologies, regulations and threats, but those who succeed in building resilient, user-friendly and secure identity ecosystems will be well-positioned to thrive in the digital era.

Footnotes & Sources

1. MarketsandMarkets. Identity and Access Management Market Forecast. https://www.marketsandmarkets.com/Market-Reports/identity-access-management-iam-market-1168.html

2. Fortune Business Insights. IAM Market Size, Share & Growth Report 2024-2032. https://www.fortunebusinessinsights.com/industry-reports/identity-and-access management-market-100373

3. Gitnux. Zero Trust Adoption Statistics 2025. https://gitnux.org/zero-trust-statistics/

4. Identity Management Institute. IAM Market Report 2025. https://identitymanagementinstitute.org/iam-market-report-2025/

5. Future Market Insights. Multi-Factor Authentication (MFA) Market Forecast 2025-2035. https://www.futuremarketinsights.com/reports/multi-factor-authentication-market

6. Condatis. Gartner Predicts 2024: Identity Fabric as Security Foundation. https://condatis.com/gartner-predicts-2024/

7. Market Data Forecast. Identity-as-a-Service (IDaaS) Market Forecast. https://www.marketdataforecast.com/market-reports/idaas-market

IAM VENDOR PROFILES

1Kosmos

OVERVIEW

1Kosmos provides secure identity proofing and passwordless authentication using biometrics and blockchain via its BlockID platform.

CORE CAPABILITIES

- Biometric identity verification with liveness detection;
- Passwordless login via biometrics, devices and FIDO2;
- Blockchain-backed credential storage;
- Digital identity wallet for user-managed credentials;
- Standards-based integration (SAML, OAuth and OpenID)

IDEAL USE CASES / INTEGRATIONS

1Kosmos is ideal for regulated industries needing strong identity assurance. It integrates with enterprise IAM systems and citizen service platforms.

UNIQUE DIFFERENTIATORS

1Kosmos combines blockchain with biometric authentication for secure, privacy-centric identity management. It supports NIST, ISO, SOC 2 and GDPR compliance.

1Password

OVERVIEW

1Password offers enterprise-grade password and identity management with user-friendly tools to secure credentials, devices and application access across teams.

CORE CAPABILITIES

- Enterprise password vault with secure sharing;
- Extended Access Management (XAM) for full identity visibility;
- SSO and System for Cross-Domain Identity Management (SCIM) provisioning support;
- Device trust for access control by device compliance;
- Application insights for shadow IT detection;
- Passkey support for passwordless authentication.

IDEAL USE CASES / INTEGRATIONS

1Password is ideal for enterprises securing remote/hybrid workforces. It integrates with identity providers (IdPs), SCIM and device management tools.

UNIQUE DIFFERENTIATORS

1Password combines credential management with device and app intelligence. It has a strong focus on usability, passkey adoption and securing unmanaged identities.

Auth0

OVERVIEW

Auth0 provides a flexible identity platform for authentication and authorization, enabling secure access for apps and APIs across any environment.

CORE CAPABILITIES

- Authentication with username/ password, social and enterprise logins;
- SSO across apps;
- MFA;
- Customizable universal login;
- Role-based user management and permissions;
- Extensibility via rules, actions and hooks;
- Built-in threat detection and IP throttling.

IDEAL USE CASES / INTEGRATIONS

Auth0 is ideal for developers securing modern apps and APIs. It integrates with IdPs, corporate directories and custom workflows.

UNIQUE DIFFERENTIATORS

Auth0 is highly extensible with low-code customization options and provides a strong support for enterprise federation and passwordless experiences.

Avatier

OVERVIEW

Avatier delivers flexible, containerized IAM solutions that streamline user life cycle management, access governance and compliance across hybrid environments.

CORE CAPABILITIES

- Cloud-independent IAM with Docker-based deployment;
- Automated provisioning and deprovisioning;
- Access governance with policy enforcement and audit reporting;
- Self-service password management;
- SSO across applications;
- Apollo AI assistant for IT and compliance automation;
- 80+ prebuilt application and system connectors.

IDEAL USE CASES / INTEGRATIONS

Avatier is ideal for enterprises managing hybrid or multi-cloud environments. It integrates with legacy and modern systems across IT, HR and compliance workflows.

UNIQUE DIFFERENTIATORS

Avatier's platform is the first IAM platform built on container technology. It combines AI-driven automation with self-service tools to reduce IT overhead and enhance compliance.

Amazon Web Services (AWS)

OVERVIEW

AWS provides scalable cloud services with robust IAM to enforce least-privilege access across AWS environments.

CORE CAPABILITIES

- Fine-grained access control via IAM policies;
- Role-based access without long-term credentials;
- Centralized SSO via the IAM Identity Center;
- Attribute-Based Access Control (ABAC)
- IAM Access Analyzer for permissions auditing;
- MFA for enhanced security.

IDEAL USE CASES / INTEGRATIONS

AWS is ideal for organizations securing AWS environments across accounts and teams. It integrates with IdPs, applications and AWS-native services.

UNIQUE DIFFERENTIATORS

IAM is deeply embedded in AWS services. It offers dynamic, attribute-driven access control and automated analysis to minimize overprivileged access.

Axiad

OVERVIEW

Axiad provides enterprisewide passwordless authentication and credential management, helping organizations secure human and machine identities across hybrid environments.

CORE CAPABILITIES

- Unified credential life cycle management (FIDO, public key infrastructure, or PKI, and smart cards);
- Identity risk visibility and automated remediation;
- Phishing-resistant MFA at scale;
- Credential issuance and revocation services;
- Integrations with IdPs, PAM and PKI systems.

IDEAL USE CASES / INTEGRATIONS

Axiad is ideal for enterprises needing passwordless access, regulatory compliance or identity risk management. It integrates with IAM tools, IdPs and compliance frameworks such as CMMC 2.0 and CJIS.

UNIQUE DIFFERENTIATORS

Axiad bridges gaps left by legacy IAM, delivering a zero trust-aligned platform without requiring system overhauls.

Beyond Identity

OVERVIEW

Beyond Identity provides passwordless IAM, enabling secure access based on user and device trust while eliminating identity-based threats.

CORE CAPABILITIES

- Passwordless authentication with device-bound passkeys;
- Real-time device trust and posture enforcement;
- Phishing-resistant MFA;
- Secure SSO with identity provider integration;
- Access360 for SSO risk analysis and policy hardening;
- Integrations with EDR, zero trust network access (ZTNA), security information and event management (SIEM) and mobile device management (MDM) tools.

IDEAL USE CASES / INTEGRATIONS

Beyond Identity is ideal for organizations securing workforce and bring your own device access, enhancing customer authentication flows or ensuring compliance. It integrates with IdPs, EDR, ZTNA, SIEM and MDM platforms.

UNIQUE DIFFERENTIATORS

Beyond Identity eliminates passwords entirely and enforces continuous, risk-based access without compromising user experience. It is aligned with zero trust principles.

BeyondTrust

OVERVIEW

BeyondTrust secures identities and access with market-leading PAM and ITDR solutions for hybrid environments. It is trusted by 20,000+ customers, including 75 of the Fortune 100.

CORE CAPABILITIES

- PAM with password management, session monitoring and least privilege;
- Secure credential vaulting and rotation via Password Safe;
- VPN-less, secure remote access with full session control;
- Endpoint privilege and application control across operating systems;
- Identity analytics and threat detection;
- Centralized policy and reporting via BeyondInsight.

IDEAL USE CASES / INTEGRATIONS

BeyondTrust is perfect for large enterprises securing remote access, enforcing least privilege and meeting compliance. It integrates across IT and OT environments.

UNIQUE DIFFERENTIATORS

BeyondTrust combines PAM, remote access and endpoint control under a unified platform with real-time identity threat insights.

BIO-key International

OVERVIEW

BIO-key delivers IAM with a focus on biometric, passwordless authentication. It is known for Identity-Bound Biometrics (IBB), serving sectors from government to education.

CORE CAPABILITIES

- PortalGuard® IDaaS with SSO, MFA, self-service password reset and biometric login;
- Proprietary IBB tech linking biometrics to identity;
- MobileAuth™ for palm/face scan authentication;
- WEB-key® for large-scale biometric life cycle management;
- Biometric hardware (including fingerprint scanners and FIDO keys).

IDEAL USE CASES / INTEGRATIONS

BIO-key is ideal for secure workforce and customer authentication, shared workstation environments, and remote access security.

UNIQUE DIFFERENTIATORS

BIO-key's IBB eliminates reliance on devices or passwords, offering unmatched biometric precision and flexibility.

Bitwarden

OVERVIEW

Bitwarden provides open-source password and identity security for individuals and organizations worldwide, emphasizing transparency and scalability.

CORE CAPABILITIES

- Password manager with end-to-end encryption and two-factor authentication;
- Secrets manager for DevOps and CI/CD credentials;
- Tools for passkeys and passwordless login;
- Authenticator for time-based one-time passwords (TOTPs);
- SCIM and directory integrations;
- On-premises hosting option.

IDEAL USE CASES / INTEGRATIONS

Bitwarden is best suited for credential and secret management, passwordless rollouts and secure remote teams.

UNIQUE DIFFERENTIATORS

Being open-source and flexible, Bitwarden balances enterprise-grade security with developer-friendly tools.

Broadcom

OVERVIEW

Broadcom offers IAM solutions through its Symantec and CA Technologies portfolios, focusing on identity governance, access control and PAM.

CORE CAPABILITIES

- Symantec Identity Security Suite for IAM and PAM;
- CA Identity Manager for automated provisioning;
- SiteMinder for SSO and access policy enforcement;
- PAM for privileged session control;
- Identity governance for access reviews and reporting;
- Risk-based access via adaptive authentication.

IDEAL USE CASES / INTEGRATIONS

Broadcom is ideal for enterprises needing scalable identity governance across hybrid infrastructures.

UNIQUE DIFFERENTIATORS

Broadcom provides deep integration across its infrastructure tools with strong compliance and risk management support.

Cisco Systems

OVERVIEW

Cisco extends its networking expertise into IAM, offering secure access, identity visibility and zero trust enforcement across endpoints and the cloud.

CORE CAPABILITIES

- Cisco Duo for MFA, SSO and adaptive access;
- Identity Services Engine for network access control (NAC);
- Cisco Identity Intelligence for AI-powered identity risk monitoring;
- Cisco Secure Access for security service edge (SSE) and ZTNA.

IDEAL USE CASES / INTEGRATIONS

Cisco is perfect for enterprises implementing zero trust, managing privileged access and securing hybrid workforces.

UNIQUE DIFFERENTIATORS

Cisco provides identity and network security with AI-driven insights, NAC and SSE integration in one ecosystem.

Clear Skye

OVERVIEW

Clear Skye delivers IGA built natively on ServiceNow, simplifying identity workflows through native integration.

CORE CAPABILITIES

- Clear Skye IGA for life cycle, access and separation of duties (SoD) management;
- Identity life cycle automation via ServiceNow attributes;
- Streamlined access request and review processes;
- SoD enforcement within ServiceNow workflows;
- Pre-built connectors for popular platforms (such as Active Directory (AD), Okta and AWS).

IDEAL USE CASES / INTEGRATIONS

Clear Skye is ideal for ServiceNow-driven enterprises aiming to simplify IGA, reduce risk and automate compliance.

UNIQUE DIFFERENTIATORS

Native ServiceNow build allows identity governance to operate within existing IT service management and governance, risk and compliance workflows - no additional UI or training needed.

CyberArk

OVERVIEW

CyberArk provides comprehensive identity security solutions focused on human and machine identity protection. Known for its leadership in PAM, CyberArk serves 10,000+ customers globally, including over half of the Fortune 500.

CORE CAPABILITIES

- PAM with credential vaulting, session isolation and analytics;
- CyberArk Identity for SSO, adaptive MFA and life cycle management;
- Endpoint Privilege Manager for least privilege and credential protection;
- Secrets management for DevOps and automation tools;
- Identity compliance with access reviews and policy enforcement;
- Secure Web Sessions for monitoring and recording user activity;
- CORA AI™ for identity threat detection and risk automation.

IDEAL USE CASES / INTEGRATIONS

CyberArk is ideal for enterprises managing complex hybrid/cloud access, securing privileged accounts and enforcing least privilege policies.

UNIQUE DIFFERENTIATORS

CyberArk provides AI-powered CORA engine, deep PAM heritage and full-stack identity security in a single unified platform.

Delinea

Delinea

OVERVIEW

Delinea delivers identity security and PAM solutions across cloud and hybrid environments. With more than 10,000 customers, it emphasizes JIT access and threat-aware controls.

CORE CAPABILITIES

- Cloud-native Delinea Platform with adaptive access controls;
- Secret Server for credential vaulting and session auditing;
- Identity life cycle management with joiner-mover-leaver automation;
- Privilege Control for Servers and Cloud Entitlements;
- Privileged Remote Access without VPN;
- Real-time Identity Threat Protection and visualization;
- Credential Manager for secure, shared access.

IDEAL USE CASES / INTEGRATIONS

Delinea is best for enterprises needing scalable PAM with seamless cloud integrations and strong identity threat detection.

UNIQUE DIFFERENTIATORS

Delinea offers deep visibility into identity pathways and real-time threat mitigation with 99.995% SLA-backed uptime.

EmpowerID

OVERVIEW

EmpowerID unifies IGA, PAM and access management into a single platform with extensive customization. It is designed for complex enterprise environments.

CORE CAPABILITIES

- Identity life cycle management with RBAC and ABAC;
- SSO and MFA with protocol flexibility;
- PAM with just-in-time access and credential vaulting;
- Identity governance and compliant access delivery;
- Partner Identity Management and external directory integration;
- Visual Workflow Studio for low-code process automation;
- Agentic AI for smart identity decisions.

IDEAL USE CASES / INTEGRATIONS

EmpowerID is ideal for organizations seeking tailored identity solutions with governance and external partner access support.

UNIQUE DIFFERENTIATORS

EmpowerID provides end-to-end identity orchestration with business-aligned access policies and AI-powered workflows.

Entrust

OVERVIEW

Entrust secures identities with IAM and credential issuance solutions, supporting zero trust and adaptive authentication. It is trusted by enterprises and governments worldwide.

CORE CAPABILITIES

- Entrust IDaaS for cloud IAM with adaptive authentication;
- Identity Enterprise for high-assurance, on-premises MFA;
- Identity Essentials for Windows VPN MFA;
- Broad MFA options and passwordless methods;
- SSO across protocols and environments;
- Digital onboarding and smart credential issuance;
- CIAM with low-code orchestration.

IDEAL USE CASES / INTEGRATIONS

Entrust is ideal for regulated industries requiring high-assurance authentication and credential management.

UNIQUE DIFFERENTIATORS

Entrust combines digital ID proofing, orchestration and credential issuance with strong compliance support.

Fischer Identity

OVERVIEW

Fischer Identity offers a no-code, cloud-native IAM and IGA platform hosted on AWS, managing 15M+ identities globally across critical sectors.

CORE CAPABILITIES

- Life cycle management with RBAC, ABAC and PBAC;
- SSO and MFA with adaptive and passwordless options;
- Full-featured IGA with auditing and certifications;
- Self-service password management;
- Accelerated Identity™ for rapid deployment;
- Managed Identity Services (MIS)
- 100+ native connectors for seamless integration.

IDEAL USE CASES / INTEGRATIONS

Fischer Identity is best for education, healthcare and finance organizations needing fast deployment and cloud-native IAM.

UNIQUE DIFFERENTIATORS

Fischer Identity provides a no-code platform with rapid 60-day deployments and managed service options.

Frontegg

OVERVIEW

Frontegg is a low-code CIAM platform built for B2B SaaS applications. It simplifies the integration of authentication, authorization, and user management while prioritizing Zero Trust security and compliance.

CORE CAPABILITIES

- MFA, passwordless login, SSO, and social logins
- Role-based access control (RBAC) and user hierarchy support
- AI-powered anomaly detection (bot activity, session risk)
- Centralized security dashboard and insights
- Compliance with ISO 27001, SOC 2, HIPAA, GDPR, PCI DSS
- Cloud-native, multi-tenant Kubernetes architecture

IDEAL USE CASES / INTEGRATIONS

Ideal for SaaS apps and enterprises needing secure identity management, fast user onboarding, and built-in compliance. Integrates with SAML, OpenID, and major IdPs.

UNIQUE DIFFERENTIATORS

Frontegg combines robust security features, a developer-friendly admin portal, and out-of-the-box compliance, accelerating identity implementation for modern SaaS platforms.

FusionAuth

OVERVIEW

FusionAuth is an API-first IAM platform built for developers. It offers customizable, standards-based authentication for modern applications at scale.

CORE CAPABILITIES

- SSO, MFA, passwordless and biometric login;
- Flexible user and role management;
- Cloud, on-premises or hybrid deployment;
- Customizable UIs and workflows via APIs and webhooks;
- Advanced security features and compliance support;
- High performance for large-scale authentication demands.

IDEAL USE CASES / INTEGRATIONS

FusionAuth is ideal for development teams building secure authentication into web and mobile apps with fine-grained control.

UNIQUE DIFFERENTIATORS

FusionAuth provides developer-centric IAM with flexible deployment and deep extensibility via API/webhook-first design.

Gluu

OVERVIEW

Gluu is an open-source IAM platform built for customization and scale. It supports modern protocols and cloud-native architectures

CORE CAPABILITIES

- SSO, MFA and access management via Gluu Server;
- Gluu Flex for Kubernetes-native IAM;
- Gluu Solo for simplified cloud-hosted deployment;
- oxAuth and oxTrust for protocol and admin functions;
- Casa for user self-service MFA;
- Passport for social logins;
- Agama Lab for low-code authentication flow design.

IDEAL USE CASES / INTEGRATIONS

Gluu is ideal for organizations seeking open-source, standards-based IAM with full admin control.

UNIQUE DIFFERENTIATORS

Gluu provides a Kubernetes-ready IAM stack with rich customization through Agama Lab and full protocol support.

Google Cloud

OVERVIEW

Google Cloud offers a robust cloud-native IAM framework, enabling fine-grained access control, centralized user management and secure integrations with external identity providers.

CORE CAPABILITIES

- Fine-grained IAM with centralized visibility and control;
- Cloud Identity and Workforce Identity Federation;
- Workload Identity Federation for non-human identity access;
- Context-aware access with attribute-based policies;
- ML-powered Recommender for access optimization;
- Comprehensive audit logging for compliance.

IDEAL USE CASES / INTEGRATIONS

Google Cloud is best suited for enterprises managing multi-cloud or hybrid environments with strict compliance needs. It integrates natively with the Google Cloud Platform and supports AD, Entra ID and other IdPs.

UNIQUE DIFFERENTIATORS

Google's attribute-based and agentless access controls, combined with real-time ML recommendations and unified policy management, provide exceptional scalability and insight.

HID Global

OVERVIEW

HID Global delivers comprehensive physical and digital identity solutions, including identity life cycle, biometric authentication and credential management for complex enterprise environments.

CORE CAPABILITIES

- Physical identity and access management via HID SAFE™;
- Cloud-based MFA and federation (HID® Authentication Service);
- Biometric and token-based MFA (HID DigitalPersona®);
- AI-powered ID verification (HID IDV Service);
- iPaaS integrations for physical and digital identity convergence;
- Visitor IAM.

IDEAL USE CASES / INTEGRATIONS

HID Global is ideal for security-sensitive industries such as government, healthcare and finance. It integrates with SSO, IdPs and physical security systems.

UNIQUE DIFFERENTIATORS

HID Global combines physical and logical access, backed by scalable, standards-based identity orchestration and robust biometric options.

HYPR Corp

OVERVIEW

HYPR specializes in passwordless authentication and identity assurance, delivering phishing-resistant access controls powered by biometrics and adaptive risk signals

CORE CAPABILITIES

- Passwordless MFA (FIDO2-certified);
- Adaptive risk engine for contextual authentication;
- Identity verification during onboarding (HYPR Affirm);
- Unified management via HYPR Control Center;
- Mobile biometric app for cross-platform authentication.

IDEAL USE CASES / INTEGRATIONS

HYPR is best for organizations eliminating credential-based risks and deploying phishing-resistant MFA. It is compatible with major IdPs and platforms.

UNIQUE DIFFERENTIATORS

HYPR eliminates passwords entirely and strengthens identity integrity with native device biometrics and continuous risk scoring.

IBM Corporation

OVERVIEW

IBM offers a scalable, AI-enhanced IAM suite for hybrid and multi-cloud environments, combining governance, authentication and CIAM features under one platform.

CORE CAPABILITIES

- AI-powered access via IBM Security Verify;
- Fine-grained cloud IAM for IBM Cloud;
- Identity governance and life cycle automation;
- Legacy and modern app integration (IBM Security Verify Gateway);
- CIAM with progressive profiling and adaptive access;
- Federated SSO and MFA.

IDEAL USE CASES / INTEGRATIONS

IBM is ideal for complex enterprises needing broad IAM functionality across cloud and on-premises, with integrations across IBM, Okta, Entra ID, Ping and more.

UNIQUE DIFFERENTIATORS

IBM's unified IAM suite with AI-driven recommendations and low-code legacy integration boosts flexibility and modernization.

ID.me

OVERVIEW

ID.me is a digital identity network offering IAL2-compliant verification and omnichannel identity services for secure access across public and private sectors.

CORE CAPABILITIES

- NIST IAL2-compliant ID verification;
- Digital wallet for secure credential reuse;
- Multi-channel MFA (SMS, email and app);
- Credential brokering to major IdPs;
- Centralized access policy enforcement;
- Online, in-person and call center verification.

IDEAL USE CASES / INTEGRATIONS

ID.me is designed for sectors with high-assurance identity requirements - such as government, healthcare and education. It integrates with Okta, ForgeRock and other platforms.

UNIQUE DIFFERENTIATORS

ID.me provides flexible verification across channels and a consumer-friendly digital wallet for trusted identity reuse.

Identity Automation

Identity Automation
a Jamf company

OVERVIEW

Identity Automation, now part of Jamf, delivers RapidIdentity - an IAM platform optimized for education and healthcare - with strong life cycle, SSO and threat detection capabilities.

CORE CAPABILITIES

- End-to-end identity life cycle management;
- Access governance with policy enforcement;
- SSO and MFA for secure, user-friendly access;
- Identity data synchronization across systems;
- Real-time threat detection and automated response.

IDEAL USE CASES / INTEGRATIONS

Identity Automation is tailored for K-12, higher education and healthcare settings with complex access needs. It integrates with Jamf and existing IT ecosystems.

UNIQUE DIFFERENTIATORS

Identity Automation combines IAM and device management, which is purpose-built for user-heavy, compliance-focused sectors such as education and healthcare.

IdRamp

OVERVIEW

IdRamp is a decentralized identity orchestration platform that simplifies IAM using blockchain and self-sovereign identity. It enables zero trust architecture, passwordless access and user-controlled privacy with vendor-agnostic integration.

CORE CAPABILITIES

- Identity verification via biometrics, document authentication and liveness detection;
- Blockchain-based decentralized identity management;
- Passwordless authentication using verifiable credentials;
- Modular orchestration layer for identity services;
- Seamless integration with IAM tools (such as Microsoft Entra Verified ID, Ping and Oracle).

IDEAL USE CASES / INTEGRATIONS

IdRamp is suitable for enterprises adopting decentralized or passwordless identity models. It easily integrates with existing IAM platforms and supports rapid deployment via zero-code workflows.

UNIQUE DIFFERENTIATORS

IdRamp's use of decentralized tech and zero-code orchestration enables scalable, user-centric IAM without disrupting existing infrastructures.

Incode Technologies

OVERVIEW

Incode provides an AI-driven, automated identity platform focused on fraud prevention and seamless user experiences across industries such as finance, gaming and healthcare.

CORE CAPABILITIES

- Biometric authentication and liveness detection;
- Document and OCR-based ID verification;
- Compliance with know your customer, anti-money laundering and know your business regulations;
- Reusable digital identities via Incode Network and Incode ID;
- Fraud detection and risk scoring.

IDEAL USE CASES / INTEGRATIONS

Incode is ideal for high-assurance industries requiring fast, secure onboarding. It supports seamless integrations in sectors such as banking, retail, healthcare and government.

UNIQUE DIFFERENTIATORS

Incode's reusable identity network and selfie-based onboarding create frictionless, high-trust identity experiences across platforms.

IndyKite

OVERVIEW

IndyKite offers graph-based, identity-centric data solutions that embed context, governance and AI into IAM processes for secure, personalized experiences.

CORE CAPABILITIES

- Identity Knowledge Graph for relationship modeling;
- Knowledge-based access control;
- AI Control Suite for secure AI data governance;
- ContX IQ for real-time, contextual data queries.

IDEAL USE CASES / INTEGRATIONS

IndyKite is ideal for enterprises embedding security into AI workflows, externalizing access control or delivering personalized user experiences.

UNIQUE DIFFERENTIATORS

IndyKite brings real-time, graph-based intelligence and context into IAM, unlocking powerful access decisions and AI trust layers.

JumpCloud

OVERVIEW

JumpCloud is a cloud-native directory platform unifying IAM, device management and zero trust controls for modern hybrid and remote-first organizations.

CORE CAPABILITIES

- Cloud directory with identity and policy control;
- SSO, MFA and conditional access policies;
- LDAP/RADIUS for legacy system support;
- Device management for Windows, macOS and Linux;
- AWS IAM Identity Center integration.

IDEAL USE CASES / INTEGRATIONS

JumpCloud is ideal for organizations seeking centralized identity and endpoint control. It integrates with cloud, on-premises apps and hybrid infrastructure.

UNIQUE DIFFERENTIATORS

JumpCloud merges identity, access and device management in one platform, enabling simplified zero trust across distributed environments.

Keeper Security

OVERVIEW

Keeper Security delivers zero-knowledge IAM tools including PAM, secrets management and password security, optimized for secure remote and DevOps access.

CORE CAPABILITIES

- KeeperPAM® for just-in-time privileged access;
- Enterprise password vault with RBAC and auditing;
- Secrets Manager integrated with CI/CD pipelines;
- Browser-based remote access via Keeper Connection Manager;
- Keeper SSO Connect® and SIEM-ready alerting.

IDEAL USE CASES / INTEGRATIONS

Keeper Security is best suited for organizations enforcing zero trust, DevOps security and PAM. It integrates with IdPs, infrastructure and development tools.

UNIQUE DIFFERENTIATORS

Keeper Security offers agentless remote access, end-to-end secrets life cycle control and cloud-native PAM - all under zero-knowledge encryption.

Keyfactor

KEYFACTOR

OVERVIEW

Keyfactor secures machine identities and digital trust through scalable PKI, certificate life cycle automation and IoT identity management.

CORE CAPABILITIES

- Keyfactor Command for certificate life cycle automation;
- EJBCA Enterprise for scalable PKI;
- SignServer for code/document signing;
- IoT identity platform for embedded device trust;
- Cloud-hosted PKI as a service (PKIaaS).

IDEAL USE CASES / INTEGRATIONS

Keyfactor is ideal for hybrid enterprises managing machine identity sprawl, IoT device security and post-quantum cryptography readiness.

UNIQUE DIFFERENTIATORS

Keyfactor offers unified, cloud-first machine identity management across IT, OT and IoT environments - with deep PKI expertise and automation.

LastPass

OVERVIEW

LastPass delivers cloud-based password management, SSO and adaptive MFA under a zero-knowledge model for small- and medium-sized businesses and enterprises.

CORE CAPABILITIES

- Centralized password vaults and sharing policies;
- SSO for 1,200+ pre-integrated applications;
- Adaptive MFA with contextual risk factors;
- Directory integration with Entra ID, Okta and Google;
- Admin dashboard with analytics and compliance tools.

IDEAL USE CASES / INTEGRATIONS

LastPass is ideal for remote and hybrid workforces needing credential security and automated IAM. It integrates easily with enterprise IdPs

UNIQUE DIFFERENTIATORS

LastPass combines ease of use and security with zero-knowledge encryption, providing scalable IAM for businesses of all sizes.

LoginRadius

OVERVIEW

LoginRadius is a cloud-native CIAM platform that helps organizations manage and authenticate customer identities while delivering secure, privacy-first digital experiences at scale.

CORE CAPABILITIES

- Traditional, passwordless and social login authentication;
- Risk-based and adaptive MFA (TOTP, SMS and email);
- GDPR/CCPA-compliant user registration and consent tools;
- Partner IAM with custom access controls;
- Centralized identity data store with encryption and audit logging;
- Developer APIs, SDKs and pre-built UI components;
- High availability and global scalability.

IDEAL USE CASES / INTEGRATIONS

LoginRadius' platform is designed for B2C and B2B enterprises in retail, finance, healthcare, media and SaaS sectors requiring secure, scalable and compliant CIAM.

UNIQUE DIFFERENTIATORS

LoginRadius blends privacy-by-design compliance with developer-friendly CIAM tooling and global uptime guarantees.

Microsoft Entra

OVERVIEW

Microsoft Entra is a comprehensive IAM suite offering identity governance, access management and security tools for users, workloads and external identities across multi-cloud and hybrid environments.

CORE CAPABILITIES

- Entra ID (formerly Azure AD): SSO, MFA and identity protection;
- Life cycle automation with ID Governance;
- Risk-based access enforcement via ID Protection;
- Entra External ID for B2B/B2C user access;
- Workload ID for app and service identities;
- Permissions Management across AWS, Azure and GCP;
- Decentralized digital credentials via Verified ID;
- Entra Connect for hybrid AD synchronization;

IDEAL USE CASES / INTEGRATIONS

Microsoft Entra is ideal for enterprises with hybrid/multi-cloud infrastructure, needing secure workforce and customer identity management.

UNIQUE DIFFERENTIATORS

Microsoft Entra offers a tightly integrated identity suite spanning user, workload and decentralized identity - unified within a trusted cloud ecosystem.

Netwrix

OVERVIEW

Netwrix delivers IAM, data security and privileged access governance solutions to help enterprises reduce risk, enforce compliance and streamline identity operations.

CORE CAPABILITIES

- Identity Manager for automated provisioning and deprovisioning;
- Directory Manager for delegated AD/ Entra ID tasks;
- Privilege Secure for JIT access, session recording and vaulting;
- Password Policy Enforcer to strengthen AD credential rules;
- Access Analyzer for visibility and remediation of excessive permissions;
- 1Secure for cloud-based auditing and monitoring.

IDEAL USE CASES / INTEGRATIONS

Netwrix is well-suited for regulated industries managing AD-centric IAM, PAM and access compliance.

UNIQUE DIFFERENTIATORS

Netwrix combines identity governance, privileged access and delegated AD admin tools in one policy-driven platform.

Okta

OVERVIEW

Okta offers an independent, cloud-based IAM platform for workforce and customer identity, supporting secure access to applications, infrastructure and APIs.

CORE CAPABILITIES

- SSO for workforce and external users;
- Adaptive MFA with behavior/context-based policies;
- Universal Directory for centralized identity management;
- Life cycle automation for provisioning across apps;
- API Access Management for tokenized resource control;
- Advanced Server Access for infrastructure protection;
- Auth0-powered customer identity solutions.

IDEAL USE CASES / INTEGRATIONS

Okta is ideal for cloud-native organizations, CIAM-heavy businesses and hybrid IT environments. It supports broad app and IdP integrations.

UNIQUE DIFFERENTIATORS

Okta's identity-first architecture, vendor neutrality and developer-centric CIAM toolkit (Auth0) drive its enterprise appeal.

Omada Identity

OVERVIEW

Omada Identity Cloud provides intelligent IGA to manage the highest level of Identity workflow complexity. Ideal for organizations that need a scalable SaaS solution to support their security, compliance, and efficiency goals that can be deployed in 90 days.

CORE CAPABILITIES

- Identity lifecycle management (joiner, mover, leaver automation)
- Access requests, approvals, and provisioning with SoD enforcement
- Role lifecycle management and governance
- Policy-based access control
- Compliance dashboards, audit trails, and reporting
- AI-powered assistant to accelerate access decisions and streamline governance tasks
- Pre-built deployment accelerators (Cloud Accelerator Package)

IDEAL USE CASES / INTEGRATIONS

Omada is ideal for mid-to-large enterprises needing to scale IGA across hybrid or multi-cloud environments. Omada's configurable connectivity framework simplifies integration with systems and applications.

UNIQUE DIFFERENTIATORS

Combines process frameworks (IdentityPROCESS+, IdentityPROJECT+) with AI-powered support. Offers both SaaS and on-prem flexibility with fast deployment options.

One Identity

OVERVIEW

One Identity provides a modular IAM platform - One Identity Fabric - that integrates identity governance, access, privileged access and AD management into a unified framework.

CORE CAPABILITIES

- Identity Manager for identity life cycle and compliance;
- OneLogin for SSO, MFA and cloud access management;
- Safeguard for privileged access and session monitoring;
- Active Roles for automated AD/Entra ID management;
- Fabric integration for centralized policy and control.

IDEAL USE CASES / INTEGRATIONS

One Identity is built for enterprises unifying IAM components or modernizing legacy identity systems across hybrid environments.

UNIQUE DIFFERENTIATORS

One Identity's holistic fabric model enables flexible, modular IAM strategies, blending governance, PAM and access under a single architecture.

OneLogin

OVERVIEW

OneLogin, a One Identity company, delivers a unified cloud IAM platform for workforce, partner and customer identities, enabling secure access, adaptive authentication and life cycle automation across hybrid environments.

CORE CAPABILITIES

- SSO with 6,000+ pre-integrated applications;
- SmartFactor Authentication with machine learning-based risk analysis;
- Unified Cloud Directory integrating AD, LDAP, Workday and Google;
- Automated provisioning/ deprovisioning workflows;
- Context-aware adaptive authentication;
- Cloud-based privileged access management;
- CIAM with social login, branding and scale.

IDEAL USE CASES / INTEGRATIONS

OneLogin is ideal for enterprises needing flexible identity access for workforce and customers, integrated with major directories and business apps.

UNIQUE DIFFERENTIATORS

OneLogin combines adaptive security, PAM and CIAM in a single platform, powered by Vigilance AI for intelligent risk-based access control.

OneSpan

OVERVIEW

OneSpan specializes in identity verification, authentication and transaction security for high-assurance industries such as banking and healthcare.

CORE CAPABILITIES

- API-based MFA and adaptive authentication suite;
- Cloud and on-premises authentication servers (OTP, FIDO and OATH);
- Secure mobile app SDKs with biometric authentication and threat detection;
- AI-powered identity verification using documents and biometrics;
- Hardware tokens (Digipass®) for high-security environments.

IDEAL USE CASES / INTEGRATIONS

OneSpan is suited for financial institutions and regulated sectors requiring transaction integrity, fraud prevention and customer onboarding.

UNIQUE DIFFERENTIATORS

OneSpan combines advanced risk analytics, biometric ID verification and secure hardware options for end-to-end trust.

OpenText

OVERVIEW

OpenText offers a comprehensive IAM suite - through its NetIQ heritage - spanning identity life cycle, access control, governance and privileged access for hybrid and multi-cloud enterprises.

CORE CAPABILITIES

- Identity Manager for life cycle automation;
- Access Manager for SSO across web apps;
- Identity Governance for reviews and compliance;
- Advanced Authentication with biometrics and risk-based authentication;
- Privileged Access Manager with session control;
- Data Access Governance for unstructured data;
- Core Identity Foundation for cloud-native IAM.

IDEAL USE CASES / INTEGRATIONS

OpenText is built for enterprises managing complex, multi-directory and hybrid environments with governance and compliance mandates.

UNIQUE DIFFERENTIATORS

OpenText unifies structured/unstructured identity control across internal and third-party ecosystems with enterprise-grade auditability.

Optimal IdM

OVERVIEW

Optimal IdM offers customizable IAM solutions across cloud, on-premises and hybrid models, backed by 24/7 support and high-availability guarantees.

CORE CAPABILITIES

- OptimalCloud: SSO, MFA and delegated admin for 11K+ applications;
- Virtual Identity Server (VIS): LDAP virtual directory for real-time data integration;
- IGA with workflow automation and auditing;
- CIAM with self-registration, security policies and branding;
- Managed IAM services.

IDEAL USE CASES / INTEGRATIONS

Optimal IdM is ideal for organizations requiring tailored IAM setups, strong customer identity control and managed IAM deployment support.

UNIQUE DIFFERENTIATORS

Optimal IdM is ideal for organizations requiring tailored IAM setups, strong customer identity control and managed IAM deployment support.

Oracle

OVERVIEW

Oracle delivers a full-stack IAM suite supporting hybrid, on-premises and cloud-native deployments, optimized for high-scale enterprise access and compliance.

CORE CAPABILITIES

- Oracle Cloud Infrastructure IAM: SSO, MFA, adaptive authentication and life cycle management;
- Oracle Identity Governance with RBAC and certifications;
- Oracle Access Management for federated and risk-based control;
- Oracle Unified Directory for scalable identity data storage;
- Access Governance analytics for policy and access reviews.

IDEAL USE CASES / INTEGRATIONS

Oracle is best suited for large enterprises across public, education and manufacturing sectors requiring scalable and compliant access control.

UNIQUE DIFFERENTIATORS

Oracle's integration of governance, directory services and modern IAM supports secure digital transformation at global scale.

Ping Identity

OVERVIEW

Ping Identity delivers a modular IAM platform supporting CIAM, workforce access, zero trust and hybrid cloud architecture with a strong emphasis on orchestration and real-time decisions.

CORE CAPABILITIES

- PingOne Advanced Identity Cloud for CIAM and workforce;
- PingFederate for SAML, OAuth and OpenID SSO;
- PingID for context-aware MFA;
- PingAccess for app/API access control;
- PingDirectory for identity data storage;
- PingAuthorize for ABAC policies;
- PingOne DaVinci for no-code identity workflow orchestration.

IDEAL USE CASES / INTEGRATIONS

Ping Identity is ideal for complex identity use cases requiring federated access, dynamic policy enforcement and seamless integration across hybrid systems.

UNIQUE DIFFERENTIATORS

Ping Identity is known for its orchestration (PingOne DaVinci), depth of protocol support and enterprise-ready policy management.

Radiant Logic

OVERVIEW

Radiant Logic unifies identity data across hybrid IT environments, enhancing IAM and IGA with centralized and virtualized identity views.

CORE CAPABILITIES

- RadiantOne Identity Data Platform for global identity unification;
- Identity Data Management and correlation;
- Real-time identity synchronization;
- Identity analytics for governance and anomaly detection;
- Identity observability and monitoring tools;
- AI-enhanced IAM insights.

IDEAL USE CASES / INTEGRATIONS

Radiant Logic is ideal for enterprises undergoing mergers and acquisitions or hybrid cloud transitions or for building zero trust architectures needing consistent identity foundations.

UNIQUE DIFFERENTIATORS

Radiant Logic virtualizes identity data from multiple sources, powering more accurate access decisions across IAM/IGA tools.

RSA Security

OVERVIEW

RSA Security delivers integrated IAM solutions through its Unified Identity Platform, enabling secure access, governance and risk-based authentication for hybrid enterprises.

CORE CAPABILITIES

- Unified Identity Platform with governance and authentication;
- ID Plus cloud-native IAM with MFA, SSO and passwordless login;
- SecurID tokens, biometrics and mobile authentication;
- Governance and life cycle tools for IGA and access certifications.

IDEAL USE CASES / INTEGRATIONS

RSA Security is a trusted partner for government and finance sectors, providing solutions for zero trust, regulatory compliance and hybrid IAM transitions.

UNIQUE DIFFERENTIATORS

RSA Security blends legacy strength with modern cloud IAM, offering a balance of deep security controls and flexible deployment models.

SailPoint

OVERVIEW

SailPoint delivers unified, identity-first security, that manages and protects access for human and digital identities enabling enterprises to reduce risk, ensure compliance, and drive secure growth.

CORE CAPABILITIES

- SailPoint Identity Security Cloud -lifecycle management, compliance management, access modeling, analytics
- Advanced capabilities for protecting third-parties, machines, sensitive data, cloud entitlements, and more
- SailPoint Atlas: unified, intelligent, cloud-native platform providing common services that power Identity Security Cloud
- Robust data model to manage and analyze identity and context to optimize access
- AI/ML to automate identity processes, detect anomalies, recommend access
- Out-of-the-box integrations with thousands of apps—e.g. SAP, ServiceNow, Workday, AWS, & Microsoft

IDEAL USE CASES / INTEGRATIONS

SailPoint is ideal for global enterprises seeking to unify identity security across humans and machines with scalability, AI-powered automation, and deep integration across hybrid and multi-cloud environments.

UNIQUE DIFFERENTIATORS

SailPoint leads in identity-first security and AI innovations that offer unmatched depth in data and access governance; coverage across all digital identities; and extensibility across IT ecosystems.

Salesforce

OVERVIEW

Salesforce provides integrated IAM services for internal and external users, enabling SSO, MFA and customer authentication within the Salesforce ecosystem and beyond.

CORE CAPABILITIES

- Salesforce Identity for SSO, MFA and social login;
- CIAM with self-registration, branding and passwordless options;
- Identity Connect for AD synchronization and SCIM provisioning;
- Embedded Login and Headless Identity for branded authentication flows;
- Support for OAuth 2.0 and OpenID Connect.

IDEAL USE CASES / INTEGRATIONS

Salesforce is ideal for enterprises managing portals and customer apps within Salesforce, requiring secure, seamless access and user life cycle control.

UNIQUE DIFFERENTIATORS

Salesforce Identity unites IAM with CRM data and UX, allowing secure, consistent experiences across apps, portals and clouds.

Saviynt

OVERVIEW

Saviynt offers a converged, cloud-native identity platform - Enterprise Identity Cloud (EIC) - that unifies IGA, PAM, application governance and posture management across hybrid and multi-cloud environments.

CORE CAPABILITIES

- Integrated IGA, PAM, identity security posture management and Application Access Governance in EIC;
- AI-driven risk scoring via Saviynt Intelligence;
- Agentless PAM with JIT access and credential-less authentication;
- Continuous identity risk monitoring (ISPM);
- Fine-grained entitlement visibility and SoD enforcement.

IDEAL USE CASES / INTEGRATIONS

Saviynt is ideal for organizations modernizing legacy identity tools, managing hybrid/multi-cloud access and enforcing zero trust.

UNIQUE DIFFERENTIATORS

Saviynt's all-in-one platform and AI-driven insights streamline complex identity governance at scale.

SecureAuth

OVERVIEW

SecureAuth delivers adaptive IAM for hybrid and cloud environments, focusing on passwordless access, behavioral biometrics and seamless user experience.

CORE CAPABILITIES

- Adaptive SSO and MFA with behavior analytics;
- Arculix platform for passwordless continuous authentication;
- CIAM with customizable workflows and branding;
- Fine-grained authorization based on contextual data;
- Delegated partner IAM for third-party access control.

IDEAL USE CASES / INTEGRATIONS

SecureAuth is ideal for organizations implementing zero trust, securing customer portals and modernizing IAM.

UNIQUE DIFFERENTIATORS

SecureAuth combines risk-based and behavioral authentication with delegated external IAM in a flexible, scalable platform.

SecZetta

OVERVIEW

SecZetta, now part of SailPoint, specializes in third-party identity life cycle and risk management, enhancing extended workforce governance.

CORE CAPABILITIES

- Workflow-based life cycle management for non-employees;
- Identity proofing and centralization;
- Delegated administration for external managers;
- Risk scoring for access control decisions.

IDEAL USE CASES / INTEGRATIONS

SecZetta is ideal for organizations managing contractors, vendors and partners with temporary access.

UNIQUE DIFFERENTIATORS

SecZetta is purpose-built for governing non-employee identities with configurable risk and life cycle tools.

Semperis

OVERVIEW

Semperis protects identity infrastructure, focusing on hybrid AD threat detection, response and disaster recovery.

CORE CAPABILITIES

- Directory Services Protector for real-time AD/Entra monitoring;
- AD Forest Recovery for malware-free rollback;
- ML-based Identity Runtime Protection;
- Delegation Manager for granular AD access;
- Purple Knight vulnerability assessment tool.

IDEAL USE CASES / INTEGRATIONS

Semperis is tailored for enterprises securing AD environments from ransomware, insider threats and misconfigurations.

UNIQUE DIFFERENTIATORS

Semperis enables real-time AD resilience with rollback and runtime attack protection.

Simeio

OVERVIEW

Simeio offers end-to-end IAM services - advisory, implementation and managed services - backed by its proprietary Identity Orchestrator platform.

CORE CAPABILITIES

- Identity Orchestrator for cross-platform orchestration;
- Managed IAM for provisioning, certification and governance;
- PAM, SSO and MFA services;
- IAM advisory, roadmapping and professional integration.

IDEAL USE CASES / INTEGRATIONS

Simeio is ideal for enterprises seeking IAM outsourcing or multi-vendor orchestration under a single interface.

UNIQUE DIFFERENTIATORS

Simeio delivers vendor-agnostic IAM management through deep services and platform orchestration.

Strata Identity

OVERVIEW

Strata Identity decouples identity from applications through its Maverics Identity Orchestration Platform, enabling unified policies across hybrid/multi-cloud IdPs.

CORE CAPABILITIES

- No-code orchestration of identity flows and IdPs;
- Identity Continuity for automatic IdP failover;
- Service Extensions for custom logic;
- Pre-built orchestration recipes for legacy apps and migrations.

IDEAL USE CASES / INTEGRATIONS

Strata Identity is ideal for IdP transitions, legacy IAM modernization and distributed identity unification.

UNIQUE DIFFERENTIATORS

Strata Identity enables identity translation across systems, modernizing access without app rewrites.

Thales

OVERVIEW

Thales offers a modular IAM suite for workforce, B2C and B2B use cases with a focus on compliance, adaptive access and identity verification.

CORE CAPABILITIES

- OneWelcome identity platform for SSO, MFA and orchestration;
- SafeNet Trusted Access (IDaaS with policy-based access);
- Identity & Access Core for authentication and storage;
- Adaptive risk-based access;
- Biometric identity proofing

IDEAL USE CASES / INTEGRATIONS

Thales is ideal for multinational organizations needing robust IAM with regulatory alignment across sectors.

UNIQUE DIFFERENTIATORS

Thales blends strong IAM with digital identity verification and modular deployment across CIAM, workforces and B2B needs.

Transmit Security

OVERVIEW

Transmit Security is a CIAM-first platform delivering passwordless, orchestrated identity experiences with integrated fraud prevention.

CORE CAPABILITIES

- Mosaic CIAM for B2C/B2B registration, authentication and life cycle management;
- Drag-and-drop Identity Orchestration workflows;
- Passwordless and biometric authentication (passkeys and magic links);
- Document/biometric-based identity verification;
- Real-time fraud analytics and response.

IDEAL USE CASES / INTEGRATIONS

Transmit Security is ideal for digital-first organizations focused on secure and frictionless customer onboarding and access.

UNIQUE DIFFERENTIATORS

Transmit Security combines no-code orchestration with strong fraud and identity verification for seamless and secure customer experience.

Trusona

OVERVIEW

Trusona delivers app-less, passwordless authentication using QR-based login, identity binding and anti-replay protection.

CORE CAPABILITIES

- Authentication Cloud with proxy-based passwordless access;
- Trusonafication for identity-device binding;
- Identity proofing via government ID verification;
- Anti-Replay (TruAR) tech for session uniqueness;
- APIs/SDKs for easy web and mobile integration.

IDEAL USE CASES / INTEGRATIONS

Trusona is ideal for B2C and enterprise use cases needing frictionless, phishing-resistant authentication.

UNIQUE DIFFERENTIATORS

Trusona enables secure, app-free sign-ins with patented identity binding and replay attack prevention.

Varonis

OVERVIEW

Varonis secures enterprise data through access governance, threat detection and data-centric identity protections.

CORE CAPABILITIES

- Unified Data Security Platform across cloud and on-premises environments;
- DatAdvantage for access visibility and behavior analytics;
- DataPrivilege for user-managed entitlement reviews;
- Identity threat detection and response (ITDR);
- AD and Entra monitoring for misconfig and abuse;
- IAM integration for enforcing least privilege.

IDEAL USE CASES / INTEGRATIONS

Varonis is ideal for data-rich organizations needing access governance, insider threat monitoring and compliance automation.

UNIQUE DIFFERENTIATORS

Varonis brings deep data context into IAM, enabling identity-driven security for unstructured data.

Venafi

OVERVIEW

Venafi specializes in machine identity management, automating the life cycle of digital certificates and cryptographic keys.

CORE CAPABILITIES

- Trust Protection Platform for cert/key orchestration;
- TLS Protect for automated cert life cycle;
- SSH Protect for key governance and audit;
- CodeSign Protect for secured signing workflows;
- Identity-based access and role control.

IDEAL USE CASES / INTEGRATIONS

Venafi provides solutions for securing machine-to-machine trust in modern DevOps, cloud-native and PKI-heavy environments.

UNIQUE DIFFERENTIATORS

Venafi, now part of CyberArk, uniquely centralizes and automates machine identity life cycle at enterprise scale.

About ISMG

IInformation Security Media Group (ISMG) is the world's largest media organization devoted solely to cybersecurity, information technology, artificial intelligence and operational technology. Each of its 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment, OT security, AI and fraud. Its annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800)944-0401 · sales@ismg.io

ISMG

BANK INFO SECURITY · CAREERS INFO SECURITY · GOV INFO SECURITY · HEALTHCARE INFO SECURITY

CU Just for Credit Unions INFO SECURITY · Data Breach Prevention. Response. Notification. TODAY · infoRisk TODAY · AIToday.io · CIO.inc

CyberEd.io · CyberEdBoard · DeviceSecurity.io · FraudToday.io · PaymentSecurity.io

CYBER THEORY · GREYHEAD AN ISMG COMPANY · Xtra mile LIFECYCLE MARKETING · QG MEDIA