Market Guide for Identity Governance and Administration

26 August 2024 - ID G00815279 - 36 min read

By Nathan Harris, Rebecca Archambault, **and 2 more**

The identity governance and administration market remains dynamic with a range of client business drivers, leading to a variety of offered IAM features. This research helps security and risk management leaders responsible for IAM navigate the IGA market and improve decision making.

Overview

Key Findings

- Business drivers and required outcomes vary greatly across organizations and industries, leading to different prioritization of various IGA features for implementation. There is no one best-practice identity governance and administration (IGA) initiative and corresponding feature set.
- There is still substantial innovation and product development in this market, including robust startup activity. Features for enabling visibility and intelligence (including AI-enabled IGA) are improving more rapidly, as are IGA capabilities for machine identities and accounts.
- Many clients still encounter substantial challenges in implementation, especially completing application integration to IGA tools. Native features in IGA tools to support rapid integration and comprehensive visibility are still insufficient for some organizations, leading them to acquire and implement supplemental tooling to assist with integration and visibility.

Recommendations

Security and risk management (SRM) leaders responsible for identity and access management (IAM) should:

- Ensure their IGA solution delivers the best value for their organization by selecting their IGA solution based on support for their required outcomes. They should clearly outline and prioritize their organization’s required outcomes (business drivers) for IGA including the relative priority of security, compliance, business enablement and efficiency/cost-effectiveness.

- Accelerate the realization of business value from their IGA investments by leveraging the visibility (data integration and management) and intelligence (AI/ML-based analytics) capabilities provided by their existing vendor products. They should also prioritize visibility and intelligence features in any IGA technology purchase decision.

- Address speed of integration and/or incomplete visibility shortfalls with their primary IGA vendor by evaluating the capabilities available from supplemental IGA visibility and integration specialist vendors.

Market Definition

This document was revised on 27 August 2024. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Gartner defines identity governance and administration (IGA) as the solution to manage the identity life cycle and govern access across on-premises and cloud environments. To accomplish this, IGA tools aggregate and correlate disparate identity and access rights data, and provide full capability controls over accounts and associated access.

IGA's purpose is to enable organizations to effectively manage identities, accounts and associated entitlements across infrastructure and applications, regardless of hosting strategy. This must be done in a way that meets required outcomes for compliance, security risk management, and business process and IT service delivery enablement:

- **Compliance outcomes:** Ensuring that access/entitlements that are in scope for different regulations and policy requirements are governed in a way that meets these requirements.

- **Security risk management outcomes:** Ensuring that the organization has full visibility into access that exists in their environments, and can identify and effectively control high-risk access, including overpermissioning (least privilege violations).

- **Business process and service delivery enablement outcomes:** Enabling the organization to grant and provision justified access as quickly, efficiently, and with as little friction as possible.

IGA solutions may also fulfill the purpose of unifying and correlating identity data for organizations with multiple person and machine identity authoritative sources. This is done to provide a single view of identity (system of record) for their dependent processes and systems.

Mandatory Features

- Identity life cycle management and identity data integration (including with multiple sources).

- Access request processing and workflow orchestration.

- Access certification (also called attestation or review).

- Provisioning via automated connectors (including some options for apps that don't use System for Cross-Domain Identity Management [SCIM]) and via integration to IT service management (ITSM)/ticketing systems to trigger manual fulfillment flows.
- Policy and role management.
- Auditing, reporting and basic analytics (descriptive and diagnostic analytics), including risk scoring.
- Entitlement management and data integration (e.g., discovery, entitlement catalog management, and entitlement data enrichment, including descriptions, owners and sensitivity ratings).

Common Features

- Segregation of duty (SOD) controls.
- Advanced analytics, including predictive and prescriptive analytics to enable rapid improvements (e.g., policy and rule modeling and recommendations, access approval and certification recommendations, and AI-based assistants).
- Identity registration and profile management for identities or attributes not managed by another authoritative source (commonly nonemployee workforce or business partner populations).
- Identity life cycle management and identity data integration for machine identities (devices, workloads, services, robotic process automation [RPA] bots) and associated accounts.
- Secrets provisioning and reset capability, including self-service password management and key provisioning/update.
- Data access governance, including for structured and unstructured data.
- Out-of-the-box capabilities for or integration with systems that provide cloud infrastructure entitlement management (CIEM).
- Integration with externalized authorization management (EAM) (for shared authorization policy/policy orchestration).
- Support for shared signals, including (but not limited to) continuous access evaluation protocol (CAEP), including the ability to send shared signals and receive and respond to shared signals.

Market Description

The IGA market worldwide grew 14.3% from 2022 to 2023, with forecast 2023 to 2024 growth of 13.9%, as of 1Q24. [1] While historically this market been strongly driven by organizations' needs to support compliance outcomes, increasing realization that IGA solutions are also critical for business enablement and security risk management, including identity-first security, is driving this growth.

Given this, the IGA market is growing more rapidly outside of the heavily regulated sectors that have accounted for most market growth to this point.

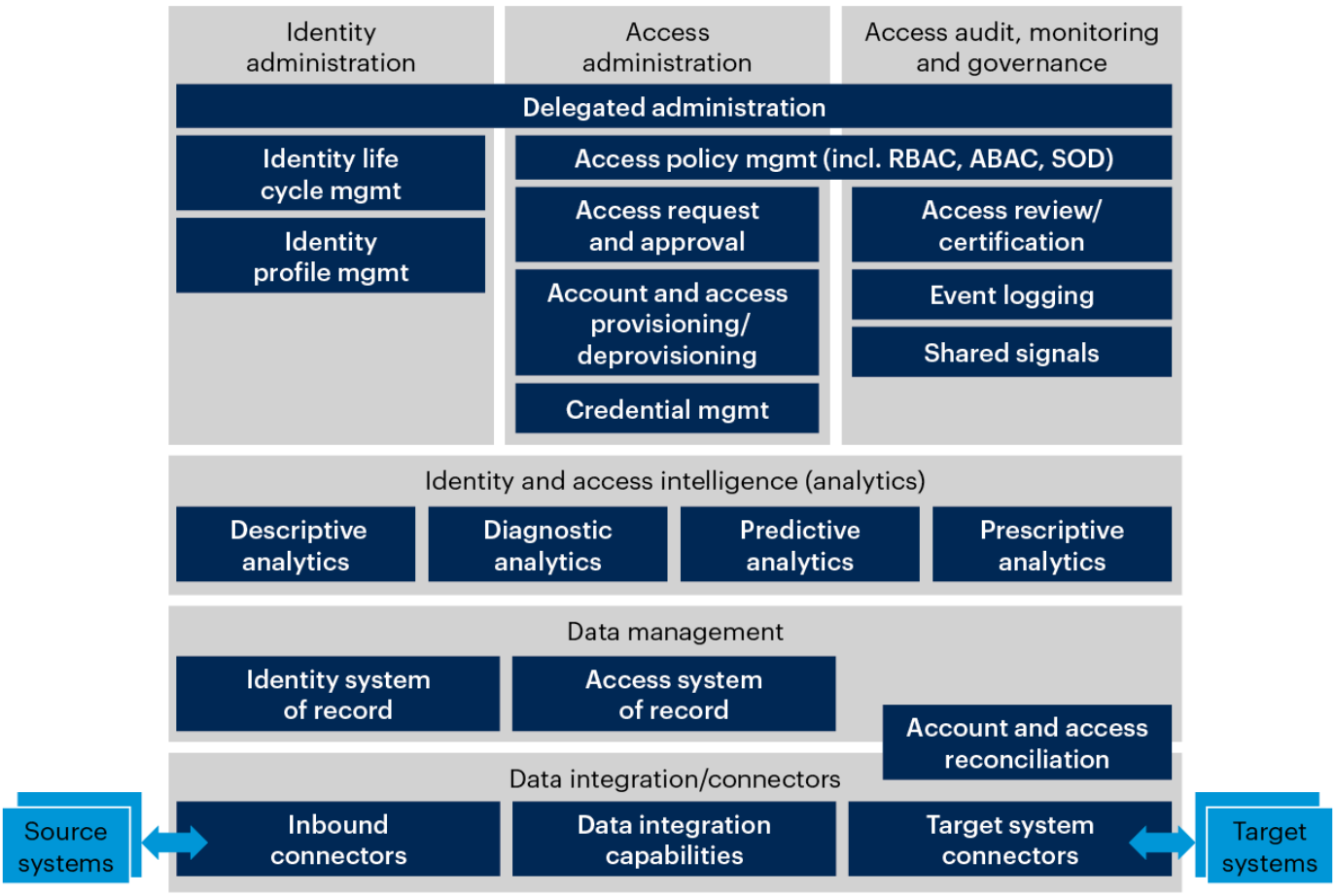
There are a variety of business drivers for IGA solution adoption, along with the features and capabilities needed to fully deliver these outcomes in most client implementations. This variety is driving more IGA technology vendors to include more out-of-the-box (OOTB) features in their IGA tooling. Light IGA products that offer a subset of IGA features are still available in the market and are still appropriate for clients with simpler long-term requirements. However, this research focuses on full-featured IGA vendors/products, which will provide required capabilities for most clients in this market.

Gartner will continue to cover light IGA through dedicated research separate from this Market Guide, such as **Is Light IGA Right for Your IAM Needs?**

To understand how IGA capabilities work together, see Figure 1.

Figure 1: How IGA Capabilities Fit Together

How IGA Capabilities Fit Together



Source: Gartner
815279_C

Gartner

In addition, there are many vendors that offer specialized tools/capabilities in the IGA space that are sometimes beneficial, even for clients who are satisfied with the mandatory features of their existing IGA tool. Most significant are tools with focused capability on identity and access visibility, data management, and accelerated integration of target systems, including but not limited to SCIM gateway products. See additional detail in the Analysis section below.

Market Direction

Given the diversity in this market, there are many factors driving the market direction in 2024. The four most significant drivers we see are the:

- Accelerating shift to SaaS delivery of IGA solutions
- Increasing influence of security and business enablement drivers relative to the compliance driver
- Accelerating capability improvements in support of these drivers/outcomes for:
  - Identity and access visibility

    - Identity and access intelligence
    - IGA capabilities for managing machine identities, accounts and access
- Continued demand for improved speed/ease of integration for target systems including integrating/understanding target system entitlements

Some sectors and regions that have historically been less positive on SaaS adoption are seeing increased uptake of and migration to SaaS IGA tooling. However, some demand for self-hosted options for IGA will remain in some sectors and regions for at least the next few years (the above shift won't completely eliminate the need for self-hosted IGA options in the broader market).

While many organizations have adopted IGA tooling primarily in support of regulatory compliance requirements, an increasing number of client companies are driving IGA adoption and implementation to support security outcomes and business enablement and efficiency outcomes. This impacts this market in two ways:

- The business drivers and critical IGA capabilities to achieve these are highly variable among client organizations. As most organizations mature in their IGA implementations, they often come to realize that achieving all relevant business drivers/outcomes is required.
- This progression further leads to a market state where any vendors that wish to compete in the broader market versus remaining a niche vendor must target full-featured IGA capabilities. Gartner predicts additional evolution of available IGA technologies from light IGA to full-featured IGA in the coming year.

Broader IT trends outside IAM markets will accelerate capability improvements within the IGA market, especially in these three areas:

- Identity and access visibility, including identity and access data management and data integration capabilities.
- Identity and access intelligence, including using AI to resolve challenges with IGA processes. While we don't anticipate that AI-enabled IGA will become a mandatory feature of IGA solutions within the next year, we do see increased demand.
- IGA features for effective management of machine identities and accounts for an increasing number of machine actor types (applications/services, RPA bots, containerized workloads, devices).

Finally, customer implementation challenges continue. It is difficult to rapidly and easily integrate target systems with IGA solutions, and especially target system entitlement management. These ongoing challenges will drive additional innovation for both IGA niche vendors and full-featured IGA

vendors in support of application and access data integration automation. This includes the use of AI-enabled software engineering methods to accelerate target system integration with IGA solutions.

Market Analysis

Multiple Business Outcomes Driving Full-Featured IGA Adoption

The key business drivers/outcomes impacting the IGA market have shifted over time. The initial vendors in the market were focused on access administration automation challenges (business enablement). Due to the inclusion of access governance requirements in various regulations, compliance took over for many years as the highest impact business driver for the IGA market and associated IGA feature development. In recent years, there has been an increased focus on and recognition of achieving strong security risk management outcomes as a critical driver in many client organizations. IAM professionals have formed a view that identity is the core foundation of cybersecurity posture. SRM leaders should adopt identity-first security approaches to their IAM programs and IGA solution selection specifically, positioning their organizations as proactive instead of reactive.

The goal of identity-first security is to shift from a point-in-time configuration to real-time, dynamic enablement, which will include account provisioning and policy orchestration, with the right entitlements and attributes determined dynamically.

Identity-first security requires centralized policies to be extended to decentralized assets. In order to control access to decentralized, distributed digital assets in a consistent manner, IAM leaders must combine centralized IAM controls, policies, data, and programs with decentralized and context-sensitive enforcement. For more information, see **Identity-First Security Maximizes Cybersecurity Effectiveness**.

In addition to compliance and security risk management drivers, the initial primary driver/outcome for the IGA market, business process enablement and efficiency, has never really gone away. And, in fact, there is now increasing recognition by many client organizations that business enablement was likely underprioritized in the industry due to the perceived more urgent needs to address compliance and security gaps.

The net result is that IGA is, and likely always will be, a multibusiness driver market for nearly all clients. The only real distinction between client organizations in different regions and industries is the relative priority of compliance, security and business enablement. Because of this, vendors that wish to maximize their utility across the market cannot just focus on related IGA features for any one, or

even two, of these critical outcomes. They must have sufficient capability to support all of the major business drivers for IGA solutions across industries and regions.

Substantial Innovation in Visibility, Intelligence and Machine Identity

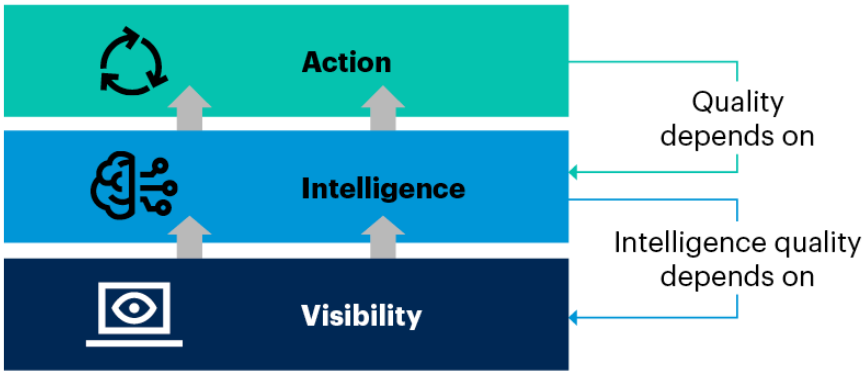
While capability improvements continue for all features in the IGA market, three areas stand out as currently having the highest volume and fastest pace of innovation:

- **Visibility improvements,** including capabilities for more rapid target system integration, improved support for data integration/data management, and enhancements to better support access data relationship visualization
- **Intelligence improvements,** including advanced analytics and all forms of AI application to IGA processes and data, including generative AI (GenAI) capabilities for IGA
- **Machine identity governance and administration support,** including supporting machine-identity-specific datasets, expanding machine IGA support beyond service accounts to other machine actor types moving toward full support for all IGA use cases for all machine actors

The first two of these, visibility and intelligence improvements, were called out as high-value areas for enhancement in related Gartner research. (See **4 Steps to Improve IAM Capabilities Using Data Management Top Practices** and **Identity and Access Intelligence Innovation with Generative AI**.) While these are not IGA-specific, they have particularly strong potential for improving all IGA processes and capabilities (see Figure 2) due to the data-heavy and high-complexity nature of IGA processes. These capabilities also strongly support all of the top business drivers and associated outcomes for IGA implementations. Further, improved IGA visibility and intelligence capabilities are also important enablers of organizational efforts toward improving IAM hygiene (see **Prioritize IAM Hygiene for Robust Identity-First Security**).

Figure 2: The Visibility, Intelligence, Action (VIA) Model

The Visibility, Intelligence, Action (VIA) Model



Source: Gartner
789808_C

Gartner

Strong Visibility

Strong visibility is vital to all intelligence, both human and machine. It is not possible to make up for missing or poor-quality data by applying extra intelligence. Specific areas of visibility innovation and improvement we are seeing include:

- Advancements in identity data merging and synchronization from multiple authoritative sources
- Improvements in schema mapping capabilities, spanning authoritative sources, IGA tooling and target systems
- Advancements in data integration and management for high-volume file-based integrations (for entitlement data for disconnected applications with no direct IGA integration)
- Application of graph databases to enable improved visibility into identity, account, role, group and entitlement interrelationships
- Improvement in various new application integration methods, including AI-augmented software engineering to accelerate application integration to IGA products

Intelligence

For intelligence, there are substantial, ongoing advances in analytics, including AI-based analytics, in support of available IGA processes. These advanced analytics capabilities often include:

- Identification of and recommendations for remediation of overprivileging situations (least privilege violations), which provides high value for security risk management

- Recommendations for additional access that is justified for specific actors and proposed rules (both role-based and attribute-based) to automate this access, which are of high value for business/workforce enablement

See Note 1 for a more complete list of potential top-value access intelligence use cases.

When combined, the capabilities above have substantial value for streamlining and simplifying access review/certification processes, which delivers value for compliance.

While the potential value of these use cases is high, the adoption or implementation of access intelligence enhancements by client organizations remains slower than expected. Contributing factors include:

- Lack of sufficient data/data quality to enable AI/ML-based approaches
- Lack of familiarity with the capabilities among potential adopters
- Concerns related to the risk of using AI/ML for access decisions for high-risk access
- Concerns related to the acceptability of AI-driven approaches to regulators, compliance associates and control oversight teams
- Requirement to add local language models (LLMs), for GenAI specifically, to keep sensitive client access configuration data out of public LLMs

Machine Identity Management

Growth in the number of machine identities is significant, and requirements to effectively manage this population often lead organizations to require multiple tools and processes. The range of service and system account identities are further expanded with the addition of workload, robotic process automation (RPA), devices and other machine identities, resulting in a complex array of identities, accounts, credentials and associated entitlements. This increases an organization's risk exposure and overall management costs, due to the volume of identities and a lack of common management processes/tools.

IAM leaders should plan to implement IGA-based machine identity management capabilities as part of an identity fabric approach to machine

identity management that includes required privileged access management (PAM) and credential/secrets management components.

For a full description of "identity fabric," see Gartner's **Definition: Identity Fabric**, and see Note 2 for suggested typical IGA requirements for IGA for machine identities.

IAM leaders should:

- Clearly identify the high-value use cases and associated capabilities for all of these high innovation areas of IGA.
- Include strong support of the use cases and capabilities as requirements in their IGA solution selection processes or their implementation and enhancement plans for existing IGA solutions (including with their existing IGA technology vendors).

Integration and Visibility Specialists Available to Help Solve Integration Challenges

IGA solution implementation has long been known to have a long tail of application integration. This integration effort is necessary to achieve complete visibility into all access. There is some movement by IGA vendors in this area, but there are also a number of vendors specializing in integration (both data and application integration) and visibility. Some client companies are adopting these integration specialist tools in addition to a primary IGA vendor in order to accelerate target system integration and achieve target visibility coverage.

There are different types of specialist vendors that clients with more complex integration challenges may find value in:

- Identity data integration specialists with capabilities for complex, multiple-source joins, schema translation and protocol translation (example vendors include Aquera and Radiant Logic)
- Rapid target system integration specialists, including SCIM gateway vendors and app integration specialists (example vendors include Aquera, Cerby and Traxion)
- Specialists in file-based integration management for disconnected IGA target applications (Aquera, for example)
- IGA data visibility/visualization specialist vendors that enable modeling of more complex identity, account, role, group and entitlement relationships (example vendors include Elimity, Oleria and Veza)

IAM leaders implementing IGA solutions for more complex and dynamic IT environments should weigh the value of adding an IGA integration and visibility specialist solution to their IGA implementation relative to the acquisition cost. These integration specialist vendors can substantially accelerate integration in highly complex and dynamic IT environments.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Vendor Selection

Gartner estimates that there are at least 55 vendors in the IGA market overall. For the 20 vendors listed in this research, Gartner has verified that they offer a SaaS version of their IGA solution, and sell in multiple regions (i.e., they are not a single-region vendor).

Table 1: Representative Vendors in Identity Governance and Administration

Vendor	IGA Product	Location of Company Headquarters
Atos	Evidian Identity Governance and Administration	Bezons, France
Delinea	Fastpath	California, U.S.
EmpowerID	Identity life cycle and administration	Ohio, U.S.
Fischer International Identity	Identity Access Governance	Florida, U.S.
IBM	IBM Security Verify Governance	New York, U.S.
Imprivata	Imprivata Identity Governance and Administration	Massachusetts, U.S.

ManageEngine	ManageEngine AD360, ManageEngine Identity360	Texas, U.S.
Netwrix	Usercube	Texas, U.S.
Omada	Omada Identity Cloud	Copenhagen, Denmark
One Identity	Identity Governance and Administration	California, U.S.
OpenIAM	OpenIAM Workforce Identity	New York, U.S.
OpenText	NetIQ	Ontario, Canada
Oracle	Oracle Identity Governance	Texas, U.S.
Ping Identity	Identity Governance, Identity Management	Colorado, U.S.
RSA Security	Governance & Lifecycle	Massachusetts, U.S.
SailPoint	Identity Security Cloud, IdentityIQ	Texas, U.S.
Saviynt	Saviynt Identity Cloud	California, U.S.
Soffid	Soffid Identity Governance Administration	Palma de Mallorca, Spain

Tuebora	Tuebora Self-Driven IAM	California, U.S.
Zilla Security	Zilla Identity Security Platform	Massachusetts, U.S.

Source: Gartner (August 2024)

Vendor Profiles

Atos

Atos was formed in 1997 through a merger of two French IT companies. In April 2023, Atos launched Eviden as a subsidiary company. Evidian is the brand for Eviden's IAM offerings, which include IGA, access management, directory services and enterprise single sign-on (ESSO).

Evidian IGA solution is offered in two ways, identity as-a-service (delivered as SaaS) and as a software solution.

Evidian IGA supports common features, including segregation of duty (SOD) controls and advanced analytics (such as predictive and prescriptive analytics to enable rapid improvements — for example, policy and rule modeling and recommendations, access approval and certification recommendations and AI-based assistants). It also supports identity registration and profile management for identities or attributes not managed by another authoritative source (commonly nonemployee workforce or business partner populations). From a machine account perspective, it supports identity life cycle management and identity data integration for machine identities (devices, workloads, services, RPA bots) and associated accounts. Plus it supports secrets provisioning and reset capability, including self-service password management and key provisioning/update and data access governance, including structured data.

Delinea

Delinea has strong brand awareness, specifically in the PAM space, and has recently acquired Fastpath (IGA) and Authomize (identity threat detection and response [ITDR]/cloud infrastructure entitlement management [CIEM]).

Delinea IGA is deployed as SaaS and enables customers to administer and govern accounts and access for interactions between all identities and data including servers, workstations, service accounts and critical business applications.

Delinea's IGA solution supports SOD with OOTB rulesets. Delinea has advanced analytics with an AI-assisted query builder, identity life cycle management for humans and machines, data access

governance (DAG) for both structured and unstructured data, as well as integrations with other identity, access and directory solutions. Delinea has extended its least privilege reach to applications and cloud infrastructure by provisioning user accounts and access rights to applications and data. This expansion provides customers with identity life cycle management and a centralized view of privileges and permissions across both infrastructure and applications.

EmpowerID

EmpowerID was founded in 2005 and offers a single platform including IGA, access management and PAM features.

EmpowerID's IGA solution is delivered as a SaaS or through an on-premises installation. EmpowerID operates as a container and microservices-based solution, which enables the SaaS and on-premises options to offer equal functionality, the only difference being the infrastructure location in which they are deployed.

EmpowerID supports common features including SOD controls (including fine-grained and cross-application SOD), advanced analytics including prescriptive analytics for policy and role modeling, and AI-based recommendations for access approval and certifications. It also supports identity registration, profile management and delegated administration for nonemployee or business partner populations. From a machine account perspective, it supports devices, workloads, services and RPA bots in addition to secrets provisioning and reset capability including self-service password management and key provisioning/update. Its solution also implements DAG and CIEM, as well as integrates with externalized authorization management (EAM).

Fischer International Identity

Fischer International Identity is a privately held company founded in 2005. It offers both on-premises and cloud versions of IGA. Fischer International Identity offers two IGA add-on options: (1) Workflow Studio, a low-code, no-code solution for designing robust data workflows; and (2) Accelerated Identity: an OOTB solution that builds the IGA codebase used for deployment.

Fischer International Identity IGA supports all common features, such as SOD controls and advanced analytics, including predictive and prescriptive analytics to enable rapid improvements (for example, policy and rule modeling and recommendations, access approval and certification recommendations, AI-based assistants). It also provides identity registration and profile management for identities or attributes not managed by another authoritative source (commonly nonemployee workforce or business partner populations). It supports identity life cycle management and identity data integration for machine identities (devices, workloads, services, RPA bots) and associated accounts, secrets provisioning and reset capability, including self-service password management and key provisioning/update. The solution also provides OOTB capabilities for or integration with systems that provide CIEM and integration with EAM (for shared authorization policy/policy orchestration).

IBM

IBM is a large, global IT company that provides both technology and consulting services, as well as its software-delivered identity governance solution, IBM Security Verify Governance (ISVG). This solution has evolved from multiple earlier products known as IBM Security Identity Governance and Intelligence (IGI) and IBM Security Identity Manager (ISIM).

IBM's identity governance solution supports SaaS delivery, software delivery or a hybrid solution. Container-based delivery options are supported on Kubernetes and Red Hat OpenShift.

Its product integrates with the IBM ecosystem and other ERP systems, such as SAP, supporting risk analysis across multiple products and a developer portal for APIs. It provides OOTB integration to ServiceNow and can accommodate other ITSM products via API.

ISVG supports common features, such as analytics using machine learning, which provide adaptive analysis. It also includes entitlements and risk scores, along with external and customized recommendations. ISVG provides SOD risk analysis, and its capabilities also include nonemployee identity registration and profile management, as well as life cycle and data integration for machine identities.

Imprivata

Imprivata acquired Caradigm's identity and access management business in 2017, allowing expansion of its IGA features and functionality. Imprivata sells IAM solutions to any industry and region, but does have a strong sales and marketing focus on companies in the healthcare industry.

Imprivata offers a range of IAM products for access management, privileged access management and IGA. Its IGA product, Imprivata Identity Governance and Administration, is available as SaaS and as deployable software.

Imprivata's IGA solution offers some common features such as advanced analytics, including predictive and prescriptive analytics to enable rapid improvements. It also offers identity registration and profile management for identities or attributes not managed by another authoritative source, identity life cycle management and identity data integration for machine identities (e.g., devices, workloads, services, RPA bots) and associated accounts, and self-service password reset.

ManageEngine

ManageEngine is a division of Zoho Corp., a privately held company focusing on software tools for IT services, operations and security. ManageEngine currently offers more than 60 enterprise IT management products and more than 60 free tools. ManageEngine offers IT management products across domains such as IAM, enterprise service management, unified endpoint management and security, IT operations management, security information and event management, advanced IT analytics, and low-code app development.

ManageEngine offers AD360 as a suite of IAM solutions, which includes IGA and AM capabilities, delivered as software. AD360 also integrates with its software-delivered PAM360 product, providing PAM capabilities. ManageEngine also has a cloud-delivered offering that provides the same features as AD360, called Identity360.

ManageEngine supports common features, including SOD controls, and supports identity registration and profile management for nonemployee or business partner populations. The solution also implements DAG, including structured and unstructured data. From a machine identity perspective, PAM360 supports devices, workloads, services and RPA bots, in addition to secrets provisioning and reset capability for Kubernetes, including self-service password management and key provisioning/update.

Netwrix

Usercube was acquired by Netwrix in August 2022. Its technologies cover IGA as well as Active Directory (AD) security and PAM.

Netwrix Usercube offers a SaaS IGA. The software-delivered version of Netwrix's IGA solution, which is less commonly deployed, is delivered as a .NET application. Netwrix GroupID continues to be offered and is Microsoft-centric, but not SaaS-delivered. The company also provides solutions for data, including discovery, classification and governance, as well as configuration and endpoint management.

Netwrix Usercube supports common features, including identity registration and profile management for nonemployee or business partner populations. From a machine account perspective, it supports devices, workloads, services and RPA, in addition to secret provisioning and reset. The solution also implements DAG features for both structured and unstructured data.

Omada

Omada entered the IGA software market in 2013, releasing Omada Identity Suite (OIS) as a full-featured IGA solution.

Currently, Omada has two full-featured IGA products, Omada Identity Cloud which is a SaaS solution, and Omada Identity, which is its software-delivered solution. The two products have the same codebase, allowing for migration between the two products. Omada provides policy-based configuration as an alternative to writing code.

Omada Identity Cloud supports common features such as SOD controls, advanced analytics (including prescriptive analytics to enable rapid improvements for policy and role modeling), access approval and certification recommendations, and AI-based assistants. It also supports identity registration and profile management for nonemployee or business partner populations. From a machine identity perspective, it supports identity life cycle management and identity data integration

for machine identities (devices, workloads, services and RPA bots) in addition to secrets provisioning and reset capability (including self-service password management and key provisioning/update).

One Identity

One Identity is a Quest Software business that, in 2021, acquired OneLogin, a provider of IAM software offering workforce identity and customer identity solutions.

One Identity's Identity Manager product covers the full IGA suite, PAM and access management (AM) capabilities. One Identity also provides a separate cloud-architected SaaS solution called One Identity Manager On Demand, focusing on identity analytics and cloud application provisioning. One Identity also offers Active Roles, a product that simplifies the management and operation of a customer's Microsoft AD and Entra ID environments.

One Identity Manager supports all of the common features, such as SOD controls, advanced analytics (including prescriptive analytics to enable rapid improvements for policy and role modeling), access approval and certification recommendations, and AI-based assistants. It also supports identity registration and profile management for nonemployee or business partner populations. From a machine identity perspective, it supports devices, workloads, services and RPA bots, in addition to secrets provisioning and reset capability (including self-service password management and key provisioning/update). This solution also implements DAG for unstructured data and supports integration with CIEM as well as integration with EAM and support for CAEP.

OpenIAM

OpenIAM, which has expanded across the U.S., Europe and Asia since its founding in 2008, focuses on a developer-centric solution. OpenIAM provides an open-source IGA platform, allowing businesses and developers to incorporate any customizations needed.

OpenIAM offers an on-premises deployment and an identity as a service (SaaS). Additionally, OpenIAM is free to download.

OpenIAM supports common features such as SOD controls, identity registration and profile management for identities or attributes not managed by another authoritative source (commonly nonemployee workforce or business partner populations). Also, OpenIAM supports identity life cycle management and identity data integration for machine identities (devices, workloads, services, RPA bots) and associated accounts. OpenIAM also supports secrets provisioning and reset capability, including self-service password management and key provisioning/update, and OOTB capabilities for or integration with systems that provide cloud infrastructure entitlement management (CIEM).

OpenText

OpenText is a publicly traded company that announced its acquisition of British software firm Micro Focus in 2022, with which it entered the IGA market.

OpenText IGA is offered via a SaaS solution, either as a single tenant or a multitenant, and is available as an on-premises solution.

OpenText supports some common features such as SOD controls, advanced analytics, access approval and certification recommendations, and identity registration and profile management for nonemployee or business partner populations. From a machine account perspective, it supports devices, workloads, services and RPA bots in addition to secrets provisioning and reset, including self-service password management and key provisioning/update. The following OpenText IGA features are only supported via extensions and customizations, which are CIEM integration, integration with EAM, and support for shared signals including (but not limited to) CAEP.

Oracle

Oracle initially offered identity management tools compatible only with its own software. However, Oracle expanded its IGA capabilities with the acquisition of Thor in 2005 to include systems from other vendors. In addition to IGA products, it also offers a range of cloud business applications, strategic cloud platform services and cloud database management systems, among a wide range of IT products.

Oracle Identity Governance (OIG) Suite supports both on-premises and cloud deployments. Oracle has self-service features via a catalog that suggests initiation of an application onboarding request, and suggests access and provisioning requests based on roles and entitlements.

Oracle supports common features such as SOD, advanced analytics (including policy and rule modeling), and registration and profile management for nonemployees. In addition, it supports secrets provisioning and self-service password management. Oracle Access Governance is a cloud-native IGA service to enable all the standard IGA features, but with a focus on user experience, codeless workflow, insights using AI/ML and integrations with Oracle's applications, non-Oracle workloads, and cloud infrastructure, with OOTB CIEM functionality.

Ping Identity

Ping Identity, a provider of AM solutions, entered the IGA market in August 2023 when it was combined with ForgeRock. The Ping Identity platform includes Ping Identity Governance, a cloud-native IGA suite delivered as a SaaS IAM platform, based on the integration of ForgeRock's identity governance product. Ping Identity also offers several IGA and AM products as software, such as PingIDM (for life cycle management), PingFederate (for federated SSO), and PingAuthorize (for policy-based access control). Ping Identity has rebranded its IGA solution to Ping Identity Governance and its life cycle management solution as PingIDM, which is available both as software and as a cloud-hosted service.

Ping Identity Governance supports common features such as SOD controls, advanced analytics (including prescriptive analytics to enable rapid improvements for policy and role modeling), access approval and certification recommendations, and AI-based assistants. PingIDM also implements DAG

and supports identity registration and profile management for B2B use cases, including nonemployee or business partner populations. From a machine identity perspective, it supports devices, workloads, services and RPA bots, in addition to secrets provisioning and reset, including self-service password management and key provisioning/update.

RSA Security

RSA Security separated from its RSA Conference business in 2022 and spun off several product lines to refocus exclusively on IAM.

RSA offers its Unified Identity Platform, which delivers identity solutions, encompassing AM, user authentication and IGA. Offerings within the platform include Governance & Lifecycle, Risk AI for contextual risk analysis, Mobile Lock for enhanced mobile security, the FIDO-certified RSA Authenticator App for both iOS and Android, and multiple hardware authenticator options. RSA Governance & Lifecycle is the company's IGA offering and is available in both software and SaaS.

The product supports common features such as SoD controls and advanced analytics to enable rapid improvements in policy definition and enforcement, role mining, and risk modeling. Additionally, the solution offers recommendations for access approval and certifications, and AI-based assistants. RSA supports identity registration and profile management for employee, nonemployee and business partner populations. For machine identities, the company supports devices, workloads, services and RPA bots, providing capabilities such as secrets provisioning and reset, self-service password management, and key provisioning/update. The solution also implements DAG, integrates with EAM systems and supports shared signals including CAEP.

SailPoint

SailPoint was acquired by Thoma Bravo in August 2022 and is now privately held.

SailPoint offers two versions of IGA suites: IdentityIQ (on-premises) and Identity Security Cloud (multitenant SaaS-based, formally known as IdentityNow). Identity Security Cloud is built on top of SailPoint's multitenant Atlas SaaS platform. Identity Security Cloud is licensed in three options: Standard, Business and Business Plus.

SailPoint supports all of the common features, such as SOD controls and advanced analytics, including predictive and prescriptive analytics to enable rapid improvements (for example, policy and rule modeling and access approval and certification recommendations, AI-based assistants). It supports identity registration and profile management for identities or attributes not managed by another authoritative source (commonly nonemployee workforce or business partner populations).

SailPoint also supports identity life cycle management and identity data integration for machine identities (devices, workloads, services, RPA bots) and associated accounts. From a machine account perspective, SailPoint supports secrets management and automated secret rotation for the accounts customers use to connect Identity Security Cloud to their applications. Also, SailPoint

supports data access governance for structured and unstructured data, and OOTB capabilities for or integration with systems that provide CIEM and integration with EAM (for shared authorization policy/policy orchestration). Plus SailPoint supports shared signals, such as CAEP, including both the ability to send shared signals and receive and respond to shared signals.

Saviynt

Saviynt provides direct client support and support through a network of partners that offer consulting and integration services.

Saviynt is a cloud-based SaaS solution. Its IGA product is part of a platform, Saviynt Identity Cloud, comprising five products, including IGA, PAM and Application Access Governance (AAG), External Identity & Risk Management as well Machine ID Management. The Saviynt Identity Cloud is delivered as a SaaS solution, tenant data-isolating IGA service. The same solution can be delivered as a virtual appliance for hosting in clients' data centers, third-party managed service provider (MSP) data centers or customer cloud infrastructure.

Saviynt supports all common features, including SOD, advanced analytics using AI (known as "Savi" and used to make peer group recommendations) and ML that supports risk scoring at both user and application levels. Its solution includes policy and role modeling, access approval recommendations and certifications. In addition, Saviynt supports identity registration and profile management for nonemployee or business partner populations (branded as External Identity & Risk Management), as well as machine identities (branded as Machine ID Management) including devices, workloads, services and RPA bots. Secrets provisioning, along with self-service password management, structured and unstructured data support, CIEM, integration with EAM, and CAEP are also supported.

Soffid

Soffid IAM provides a converged IAM platform that brings AM, SSO, IGA, IRC and PAM as an augmented solution.

Soffid Deployment is supported as both SaaS and on-premises for all of its products. It offers identity orchestration across the ecosystem, with consolidated pricing, using a wide range of OOTB connectors.

Soffid's capabilities include identity registration for nonemployees, secrets provisioning and SOD capabilities. In addition, it provides advanced analytics, CIEM capabilities and support for shared signals (CAEP).

Tuebora

Tuebora offers an IGA solution that seeks to apply machine learning to streamline access administration automation in access requests, policy generation and role management. Tuebora has raised a total of $1.28 million in funding, with the latest funding round in March 2019.

Tuebora's IGA solutions include Prescriptive Analytics and Access Control, which provides access management capabilities. Tuebora's solution set is delivered as both software and as SaaS.

Tuebora supports common features such as SOD controls, advanced analytics (including prescriptive analytics to enable rapid improvements for policy and role modeling), access approval and certification recommendations, and AI-based assistants. It also supports identity registration and profile management for nonemployee and business partner populations. From a machine identity perspective, Tuebora supports life cycle management for devices, workloads, services and RPA bots in addition to secrets provisioning and reset (including self-service password management). Its solution implements DAG, CIEM and integration with EAM systems.

Zilla Security

Zilla Security is a privately held company that was founded in 2019.

Zilla Security provides a suite of three security and compliance-focused IGA solutions. Zilla Secure addresses least privilege security and automated remediation; Zilla Compliance provides access certifications, SOD and audit evidence; and Zilla Provisioning implements access requests and identity life cycle management. These are delivered as a SaaS solution that integrates with cloud and on-premises infrastructure and applications.

Zilla Security supports common features such as SOD controls, advanced analytics (including prescriptive analytics to enable rapid improvements for policy and role modeling), and AI-based recommendations to simplify access approval, life cycle management and certifications. From a machine identity perspective, Zilla Security supports life cycle management for service accounts in devices, workloads, services and RPA bots. It does not natively track machine identities that use digital certificates, API keys or secrets, but rather integrates with PAM solutions. In addition, Zilla implements DAG for structured and unstructured data, and provides native CIEM capabilities.

Market Recommendations

Security and risk management leaders should:

- Clearly outline and prioritize their organization's required outcomes (business drivers) for IGA implementation, including the relative priority of security, compliance, business enablement and efficiency/cost-effectiveness:
    - Select IGA solutions based on support for required outcomes, relative to both short-term requirements and strategic long-term requirements. Full IGA solution implementations, including target system integrations, take years, so they need to select an IGA solution that will meet strategic/long-term needs as well.
- Accelerate the realization of business value from IGA investments:

    - Fully leverage the visibility (data integration and management) and intelligence (AI/ML-based analytics) capabilities provided by existing vendor products and prioritize visibility and intelligence features in any IGA technology purchase decision:
    - Carefully evaluate their needs for IGA capabilities for machine actors/identities, and include these use cases in their IGA solution selection process as well.
    - Plan the IGA components of their machine identity management strategy as part of an identity fabric approach that includes integration with required secrets management and PAM capabilities. (Do not assume all machine IAM needs can be met with just one IGA solution.)
- Evaluate supplemental IGA visibility and integration specialist vendors where requirements for speed of integration and/or acceleration of more comprehensive access visibility can't be met with existing IGA technology. This can include SCIM gateway solutions, for example.

Evidence

[1] **Forecast: Information Security and Risk Management, Worldwide, 2022-2028, 1Q24 Update**

Note 1: Potential Top-Value Access Intelligence Use Cases

- Identifying orphan accounts and those with assigned entitlements that haven't been or aren't being used.
- Identifying/assigning risk ratings for entitlements, accounts and identities.
- Identifying privileged access and accounts (discovery).
- Rapidly identifying instances of overpermissioning (least privilege violations) for remediation.
- Providing approve/deny recommendations for access reviewers and approvers.
- Providing suggestions for access requesters/recipients ("it looks like you need/will need this access").
- Role modeling/role engineering for organizations using role-based access control (RBAC) to reduce role structure maintenance costs.
- Rapidly identifying role-based and attribute-based rules for automation (birthright access) to enable organizations to accelerate access administration automation and manual administration reduction (both labor and costs).

Note 2: IGA Requirements for Machine Identities

Differences in data requirements between machine identities and human identities:

- **Ownership:** For machines, ownership means the “responsible human,” not the actor who should be using the identity/account. Human-focused IGA solutions will assume the identity/account owner is the person to whom the identity/account refers (i.e., the only one who should be using that identity/account).
- **Login configuration:** Machine accounts need to be tracked for interactive and noninteractive login, with RPA accounts being enabled for interactive login and most other machine accounts being prevented for use for interactive login. This “attribute” isn’t applicable to human identities at all.

IGA features for machine identity management that align with IGA for humans:

- Correlation/linking of machine accounts to machine identities
- Reconciliation of entitlements for machine accounts relative to access policies set in the IGA system
- Flagging machine identities/accounts as “privileged” for co-management with PAM tooling
- Synchronizing basic machine identity information from appropriate sources (configuration management database [CMDB] systems, for example)

IGA features for machine identity management that differ from IGA for humans:

- Assigning owners and custodians/operators (those authorized to help manage machine accounts and credentials for a given machine actor) for machine identities
- Integrating with credential management systems for automation of machine account credential generation and management
- Managing machine identities associated with the applications and systems that the identities are used for
- Distinguishing different types of machine accounts (interactive/noninteractive, service accounts, RPA bots, devices, workloads, etc.)
- Discovering and centrally governing accounts for workloads issued by platforms such as infrastructure-as-code (IaC) platforms and Kubernetes