Gartner Research

Market Guide for Identity Governance and Administration

David Collinson, Henrique Teixeira, Kevin Kampman, Rebecca Archambault, Brian Guthrie

4 July 2022

Gartner

Market Guide for Identity Governance and Administration

Published 4 July 2022 - ID G00741319 - 18 min read

By Analyst(s): David Collinson, Henrique Teixeira, Kevin Kampman, Rebecca Archambault, Brian Guthrie

Initiatives: Identity and Access Management and Fraud Detection

Security and risk management leaders should use this Market Guide as an aid to anticipating future trends, features and integration capabilities in the IGA market. This will help them make better procurement decisions in light of the typical five-to-eight-year life span of IGA tools.

Additional Perspectives

- Summary Translation + Localization: Market Guide for Identity Governance and Administration
  (22 September 2022)

Overview

Key Findings

- The identity governance and administration (IGA) market continues to mature, having shifted focus from providing services from the cloud to managing other cloud assets and integrating additional capabilities into its core tools.
- Security and risk management (SRM) leaders face an assessment challenge. On the one hand, they must assess IGA products against short-term requirements, such as cloud entitlement governance. On the other, they must, at the same time, assess these products' long-term ability to participate in an underpinning identity fabric in which insights from identity and access management (IAM) tools are shared reciprocally with insights from adjacent tools.
- The operational overheads associated with various IGA solutions differ. It is important to look beyond the purely technical capabilities of these solutions and evaluate how (and how easily) they can be deployed, integrated and operated within an existing environment.
- The number of machine identities (for devices, workloads and robots) is surging, particularly with the adoption of DevOps and the requirement to deliver in a fast-paced culture. Many organizations lack tools to manage the life cycle of these new types of identity, so they are looking for IGA offerings to fill the gap.

Recommendations

SRM leaders responsible for IAM and fraud detection should:

- Evaluate IGA vendors not just for their traditional administrative capabilities but also for their ability to meet upcoming cloud-related needs and their plans for solutions that work within an identity fabric. This will enable more complete security coverage and support more insightful artificial intelligence (AI) and machine learning (ML) decisions across the IAM landscape as tools take information from, and share insights with, more than just proprietary, siloed data pools.
- Include ease of deployment and operation in any assessment. It is important to examine SaaS and platform solutions, as well as estimates of the cost of using professional services or managed service providers for differing solutions.
- Treat machine identities as distinct identity types that must be managed and governed similarly to human identities, but with more attention paid to ownership, automation, discovery and improved relations with developers.

- Identify key use cases early in any review process to quickly eliminate from consideration any IGA tool that cannot meet their organization's needs. The chosen tool must support all their use cases.

Strategic Planning Assumption

By 2025, over 40% of organizations will be using identity governance and administration (IGA) analytics and insights from IGA tools as part of a wider identity fabric to reduce security risks across their identity and access management estate.

Market Definition

IGA provides administrative control of digital identities and access rights across multiple systems for multiple user types — members of the workforce, partners and machines. IGA tools aggregate, correlate and orchestrate disparate identity and access rights data distributed throughout an organization's IT ecosystem.

Purpose: IGA's purpose is to manage the complex array of access rights (for roles and group memberships, for example) and identity repositories within organizations, both on-premises and in the cloud. In this way, it ensures appropriate access to resources across highly connected IT environments.

Capabilities: Mandatory capabilities for a complete IGA suite to meet a typical organization's needs are:

- Identity life cycle management
- Entitlement management
- Support for access requests
- Workflow orchestration
- Access certification (also called "attestation")
- Provisioning via automated connectors and service tickets
- Analytics and reporting

Tools that provide only four, five or six of these capabilities to a level that supports typical organizational needs may be referred to as "light" IGA tools.

Optional IGA capabilities include:

- Policy and role management
- Password management
- Segregation of duty

Delivery models:

- Software
- Virtual appliance
- Cloud-hosted
- SaaS
- As a part of a broader platform, such as an IT service management (ITSM) platform

User type: IT leaders with responsibility for IAM

Market Description

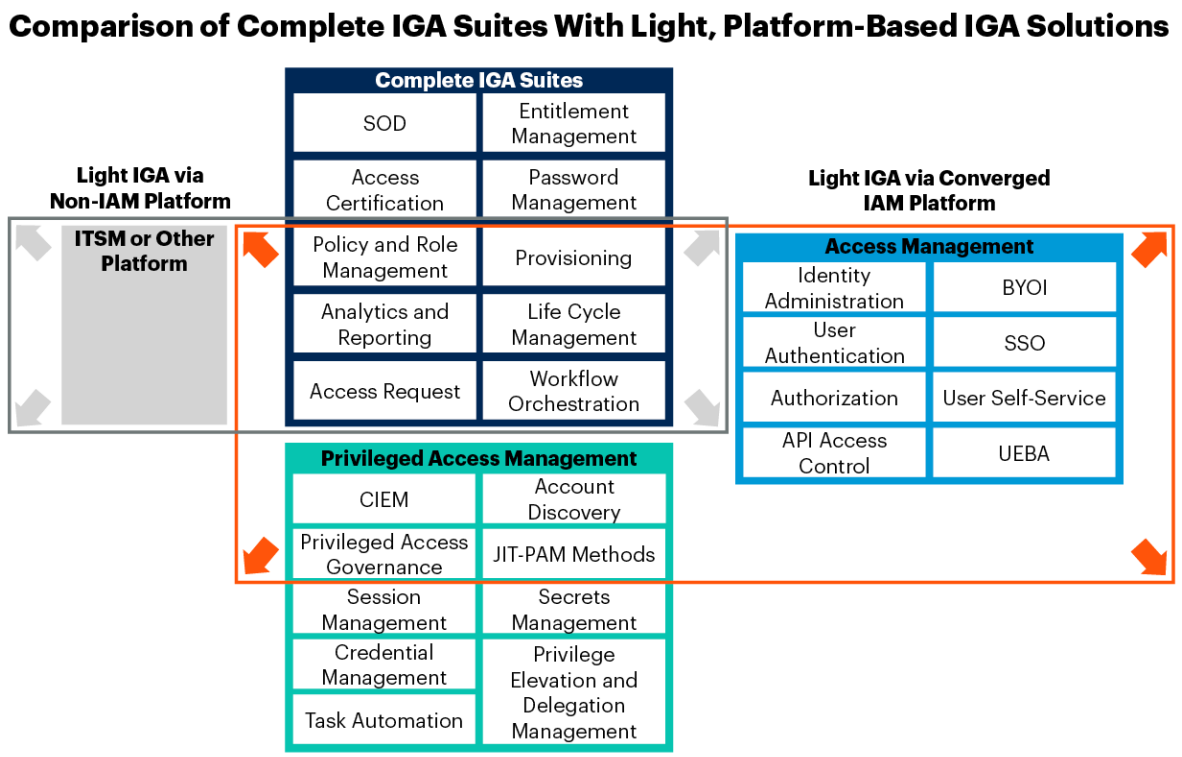
Vendors of complete IGA suites offer the full range of capabilities needed to manage and maintain IGA at a level expected of typical organizations.

There are also vendors that provide “lighter” subsets of these capabilities via platform-based solutions, in conjunction with adjacent tools and technology.

Converged IAM platforms (CIPs) are the most common platform-based solutions, but some organizations use adjacent non-IAM platforms (most notably from ServiceNow) that offer IGA capabilities either directly or via third-party add-on applications.

Figure 1 compares the most common categories of IGA offering.

Figure 1: Comparison of Complete IGA Suites With Light, Platform-Based IGA Solutions



API = application programming interface; BYOI = bring your own identity; CIEM = cloud infrastructure entitlement management; IAM = identity and access management; IGA = identity access and administration; ITSM = IT service management; JIT-PAM = just-

In addition, there are a significant number of vendors of specialized tools. Examples are:

- Segregation of duty (SOD) vendors, such as Pathlock and SafePaas.
- Vendors with Microsoft (Active Directory Domain Services)-specific tools, such as Imanami and ManageEngine.
- Vendors with capabilities especially suited to mergers or management of multiple identity repositories or identity types, such as Radiant Logic and SecZetta.

Most IGA vendors are based in the U.S. or Europe, in line with the markets they predominantly serve. But there are vendors in all regions of the world, often with a user base concentrated around their home region. This can be an important consideration, as deployment and ongoing management of IGA solutions challenges many organizations — even when a solution is SaaS-based. Access to local professional services with experience of particular tools and of local or regional regulations, customs and ways of working is a key consideration.

Market Direction

Organizations continue to move their computing to the cloud. To do so, they are increasing the number of cloud-hosted applications they use and often using multiple cloud infrastructure vendors. Additionally, the growth of DevOps, containerization and automation is generating a significant number of machine identities (workloads and devices), to the extent that nonhuman identities now outnumber humans in many organizations.

At the same time that cloud use and the number of machine identities is expanding, many organizations are looking to simplify and consolidate their tools. Specifically, they want to avoid having multiple point solutions and overlapping technologies. This is increasing the need for an identity fabric that uses common identity services which support distributed working patterns.

IGA vendors are responding in different ways by providing solutions that help to meet both the need to consolidate tools and the requirement for an identity fabric, but not necessarily at the same time.

Most of the complete IGA suite vendors have relatively stable offerings that can fulfill typical organizational needs. Their offerings include the capabilities listed earlier, to a level that organizations without specialized requirements will find meets most of their use-case requirements.

All the main IGA suite vendors have SaaS deployment options, which are increasingly recommended by them in preference to their software-based solutions, even for large, complex organizations. For many such organizations, a complete IGA suite is the obvious starting point, as all such suites have deep capabilities that support complex needs, with no risk of missing key functionality. Furthermore, in addition to offering core capabilities, suite vendors are striving to improve their support for nonhuman identities by introducing dedicated identity types, delivering more insightful analytics through ML, and providing tighter control of cloud-based applications and environments. These vendors' evolution is focused on specific product differentiators such as mobile apps, consumer capabilities, or close integration with specific adjacent technologies like privileged access management (PAM) and ITSM.

More revolutionary changes in the IGA market are occurring within its various platform solutions. Particularly notable is the proliferation of new IGA applications based on the popular ServiceNow platform.

Gartner expects to see additional entrants into the platform sector as vendors seek to enter this growing market through acquisitions, partnerships or product development. In parallel, existing vendors offering light IGA capabilities as part of a platform will continue to enhance their capabilities to get closer to those of a suite.

The capability gap between suites and light IGA offerings is, however, unlikely to fully close. It will probably remain fairly significant, with suites typically offering much stronger management of contract workers and third-party access, deeper connectors, and flexible workflow and policy-based access controls. For larger, or more regulated organizations, it may be a "deal breaker" if light IGA offerings are not sufficiently capable.

SRM leaders should follow the advice in Gartner's Buyer's Guide for Identity Governance and Administration. It will help them define and assess their requirements against different offerings in order to select a product that offers all the functionality required for their use cases.

Although platform-based tools have technical deficiencies, they have attractions in terms of cost, ease of deployment and ongoing management of fewer solutions. The ability to use an existing platform to provide IGA capabilities reduces the overall IT overhead within an organization.

The challenge for IAM leaders is to assess the capabilities and deployment and management implications of available solutions against the needs of their organization both now and for the lifetime of an IGA tool — often five to eight years.

Market Analysis

Cloud and Cloud Entitlement Management

The relentless drive to the cloud continues as organizations adopt cloud services to increase their flexibility and agility, as well as to reduce upfront investment and ongoing service costs. For them to realize these benefits without running high security risks, robust governance and transparency of consumption are required across a range of cloud service providers.

IGA tools — traditionally deployed on-premises — have to support this move by using proprietary connectors to popular SaaS applications and, more usefully, converging on standards-based connectors. This requirement has accelerated the trend for management of off-premises systems and data.

More recent developments include cloud-native security controls that analyze entitlements. They use AI and ML to identify and recommend the removal of risky or unnecessary entitlements.

IGA tools themselves are more often offered and purchased on a SaaS basis than with traditional licensing arrangements for on-premises deployment, with perpetual licensing having been removed from some offerings over the past 12 months. As SaaS IGA offerings are being promoted, it is important to dig below any marketing in order to assess their true cloud credentials and ability to manage other cloud-based assets.

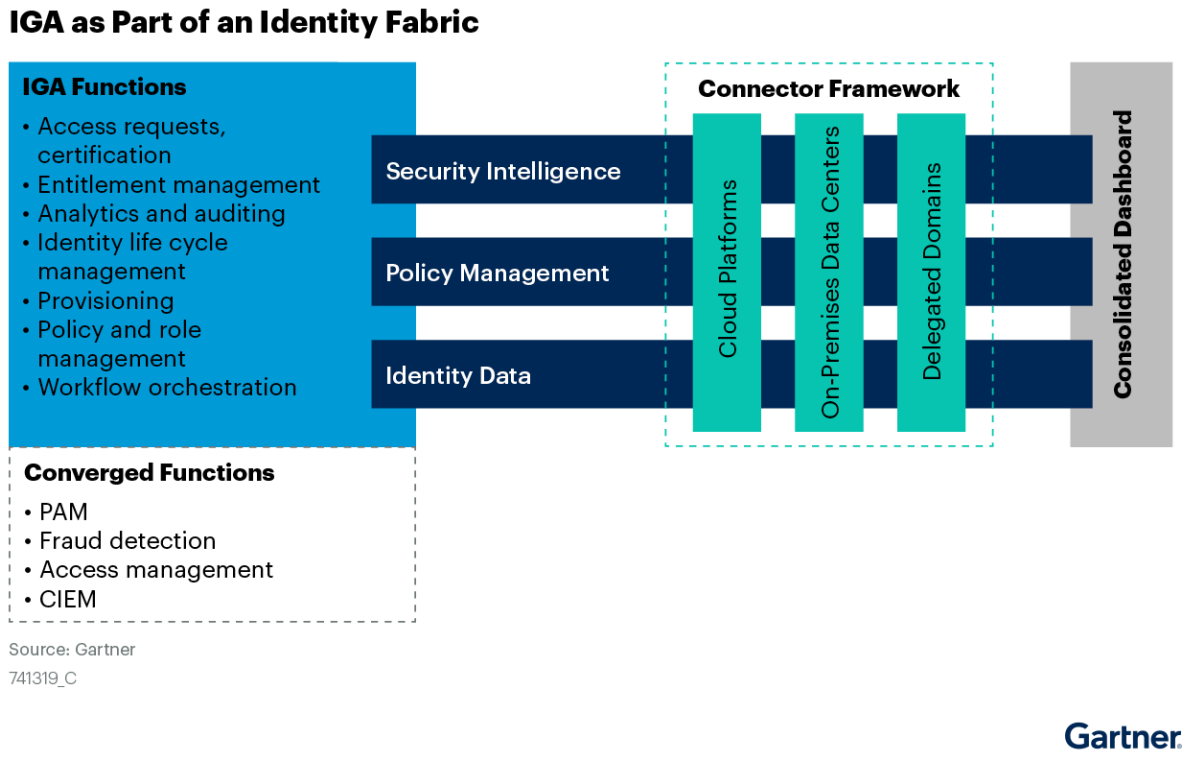
IGA That Supports an Identity Fabric

There is an increasing need for security tools and services to be more composable, and to interoperate better in terms of the exchange of identity-first security insights. IGA capabilities are evolving to play a wider part in the overall identity fabric (see Figure 2). They are also evolving to participate in cybersecurity mesh architecture (see The Future of Security Architecture: Cybersecurity Mesh Architecture (CSMA)).

We expect IGA functions to be more composable as part of a cybersecurity mesh by 2025. It is likely, for example, that they will help guide managers through access certification reviews by taking data and inputs from external sources, as well as from their own internal data. We also expect access management solutions to query IGA (and other) systems for insights when they see atypical scenarios, and thus give a fuller picture of how much risk may be involved in authenticating a user. Insular vendors that are not planning for this future will struggle to catch up and participate when needed.

The ability to participate fully in an identity fabric will act as a value multiplier, compared with insular IGA offerings that fail to play a full part.

Figure 2: IGA as Part of an Identity Fabric



CIEM = cloud infrastructure entitlement management; PAM = privileged access management

Analytics and ML capabilities continue to evolve within IGA tools. Typically, these capabilities can support all areas of governance by performing a range of tasks — from identifying likely groups of individuals in support of role-based access control (RBAC) to helping managers make good decisions and identify entitlement outliers during access certification campaigns. But although intelligence engines are helping to move IGA tools toward a semiautonomous future, to really add value to decision making they will need to accept input from external sources and systems. Similarly, to be highly valuable within a security context, they will need to help make decisions and constructed insights available to other, related systems in support of a wider security mesh.

Rather than assess IGA capabilities solely against current needs, it is important, given the longevity of IGA solutions, to plan mainly for likely requirements in 2030. That involves seeking vendors that understand and address the wider, changing needs of the security market. This market is shifting to IAM solutions that connect devices and applications using modern APIs and other means. SRM leaders should favor standards-based solutions that link solutions, applications and other devices. Specifically for IGA, this means looking for use of the System for Cross-Domain Identity Management (SCIM) and API access to insights, risk decisions and data that can support other security tools as part of an identity fabric. It also means favoring IGA vendors that have plans to incorporate external inputs into their analytics decision-making processes.

Light, Platform-Based IGA

Platform-based IGA developments are being driven by uptake of ServiceNow's platform and the proliferation of IGA applications available from its application store. This buoyant growth in alternatives to IGA suites likely stems from the alternatives' lower cost, coupled with the realization that many organizations do not use even 90% of the features available to them in suites. In fact, it is not uncommon to hear organizations admit to using closer to 30%.

It is in this context that vendors of CIPs and non-IAM-platform-based "light" solutions are looking to quickly include more functionality in order to offer all the core capabilities that organizations actually use, rather than strive for feature-parity with IGA suite vendors.

One of the advantages of platform-based solutions is ease of deployment, given that they are typically IGA feature "add-ons" to tools that organizations already have. Gartner clients indicate that deploying an IGA suite can often take more than a year, and this typically does not include full onboarding of all applications and capabilities. Platform-based solutions, such as those based on ServiceNow's platform, can often be especially attractive if the organization has already deployed the platform solution for support staff and if end users are already familiar with it, as this greatly reduces support costs and deployment times — albeit for a product much less capable than a complete IGA suite. In the same way, CIP solutions tempt organizations with a single product that can span multiple functional areas within the field of IAM, often in line with an organizational goal of minimizing vendors or overlapping capabilities.

The platform market is set to keep growing, and it is likely that non-ITSM platforms will also gain IGA capabilities. Salesforce offers limited application-provisioning capabilities for contract workers, but these may expand. HR platform vendors may similarly look to offer additional functionality in their products. IGA commoditization will expand in less sophisticated offerings. More sophisticated suites will focus on the more complex opportunities that promise to deliver higher value but also pose greater risks associated with data, relationship and organizational challenges.

SRM leaders must not only assess the capabilities of different IGA offerings, but also take account of any trade-offs in terms of deployment, training, and ongoing support and maintenance. When pricing is added to the mix, a complete IGA suite will not necessarily be the most suitable choice for every organization. Conversely, a failure to fully understand all requirements can leave an organization exposed to residual risks if its chosen tool lacks capabilities that are required but overlooked during the assessment period.

Machine Identity Management

Growth in the number of machine identities is significant, and often leads organizations to require multiple tools and processes. Service and system account identities are increasingly being joined by workload, robotic, Internet of Things and other machine identities, resulting in a complex array of identities and associated entitlements. This increases an organization's risk exposure, due to the volume of identities and a lack of common governance.

Some IGA vendors have a specific category of identity to govern these machine accounts, but it is important to look behind the marketing to see how their tools actually work. Features may include the ability to assign owners, link to applications and systems, or "tag" privileged machine identities for management within PAM systems. The different account types and the varying governance capabilities of IGA tools make it important to begin by auditing, categorizing and governing this area to ensure use cases are captured, risks are addressed and the number of tools is minimized.

SRM leaders should establish a machine identity strategy, including cross-functional teams, that gathers requirements, provides leadership, defines ownership, and details the full range of use cases.

Once this strategy has been established and high-level policies and standards are in place, they should look for IGA tools that can perform the following tasks on a continuous basis:

- Discovery.
- Automated life cycle management.
- Reporting on what identities and credentials exist, and where and how they are used.

Tools that provide control over machine identities are converging, but they still differ in terms of interfaces, integrations, credential support, and discovery-, latency- and automation-related capabilities. Expect this market to continue to evolve as relationships between human and nonhuman identities become increasingly complex.

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.

Market Introduction

We consider the vendors in Table 1 representative of the broad IGA market because their products are marketed and sold specifically to serve it. They offer products in the two categories previously identified: complete IGA suites and light, platform-based IGA solutions.

Table 1: Representative Vendors in the Identity Governance and Administration Market

(Enlarged table in Appendix)

Vendor	Product Name	Product Category	Headquarters
Atos	Evidian Identity Governance and Administration	Complete IGA suite	Bezons, France
Bamboo Cloud	Cloud IAM Platform	Light, platform-based IGA solution (part of a converged IAM platform)	Shenzhen, China
Broadcom	Symantec IGA	Complete IGA suite	California, U.S.
Clear Skye	Clear Skye IGA	Light, platform-based IGA solution (part of a non-IAM platform)	California, U.S.
E-TRUST	HORACIUS Identity & Governance	Complete IGA suite	Sao Paulo, Brazil
EmpowerID	Identity Lifecycle and Administration	Complete IGA suite	Ohio, U.S.
Evolveum	midPoint	Complete IGA suite	Bratislava, Slovakia
Fálaina	Fálaina IGA	Complete IGA suite	Singapore
ForgeRock	ForgeRock Identity Governance	Complete IGA suite	California, U.S.
Hitachi ID Systems	Hitachi ID Bravura Security Fabric	Complete IGA suite	Alberta, Canada
IBM	IBM Security Verify Governance	Complete IGA suite	New York, U.S.
Identity Automation	RapidIdentity Identity and Access Management	Complete IGA suite	Texas, U.S.
Ilantus	Compact Identity	Light, platform-based IGA solution (part of a converged IAM platform)	Illinois, U.S.
Imprivata	Imprivata Identity Governance	Complete IGA suite	Massachusetts, U.S.
Iteris	CAP2AM	Complete IGA suite	Sao Paulo, Brazil
Micro Focus	NetIQ Identity Governance and Administration	Complete IGA suite	Newbury, U.K.
Microsoft	Azure Active Directory (Azure AD) Identity Governance	Light, platform-based IGA solution (part of a converged IAM platform)	Washington, U.S.
N8 Identity	TheAccessHub	Complete IGA suite	Ontario, Canada
Okta	Okta Identity Governance	Light, platform-based IGA solution (part of a converged IAM platform)	California, U.S.
Omada	Omada Identity Cloud	Complete IGA suite	Copenhagen, Denmark
One Identity	Identity Governance and Administration	Complete IGA suite	California, U.S.
Oracle	Oracle Identity Governance	Complete IGA suite	Texas, U.S.
Paraview Software	Unified Identity Management Platform	Light, platform-based IGA solution (part of a converged IAM platform)	Shanghai, China
SailPoint	SailPoint IdentityNow, SailPoint IdentityIQ	Complete IGA suite	Texas, U.S.
SAP	SAP Identity Management	Complete IGA suite	Walldorf, Germany
Saviynt	Saviynt Enterprise Identity Cloud	Complete IGA suite	California, U.S.
SecurEnds	SecurEnds	Complete IGA suite	Georgia, U.S.
Soffid	Identity Governance Administration	Light, platform-based IGA solution (part of a converged IAM platform)	Palma, Spain
Sysintegra	ZertID	Light, platform-based IGA solution (part of a non-IAM platform)	Melbourne, Australia
Tuebora	Tuebora (IAM Platform)	Complete IGA suite	California, U.S.
USERCUBE	Usercube IGA	Complete IGA suite	Marseille, France

Source: Gartner (July 2022)

Market Recommendations

SRM leaders should:

- Work with stakeholders to define requirements and build use cases early in the process, to help distinguish between critical needs and desirable features. This distinction will inform discussions about which type of IGA tool is more suitable — a complete IGA suite or a light IGA platform-based solution.

- Identify the type and depth of IGA functionality required. Apply rigor and methodology to separate critical and urgent needs from merely desirable features or future wishes. For example, use risk-based and cost-benefit analysis to identify the most important capabilities.
- Build for 2030, not just for today — ensure planning encompasses features and capabilities that support a wider identity fabric. Look for tools that are outward-facing and able to share security data with other systems openly, rather than tools from vendors that only use internal data or that lock clients into proprietary connectivity.
- Don't discount CIPs or ITSM-based solutions, if your needs are modest. Although lighter in terms of capabilities, they can be cheaper to purchase, deploy and operate, and they can reduce the number of tools and vendors used by an organization.
- Solicit input from other teams (Cloud, PKI, I&O, DevOps, IAM) to form a community of practice, or form a Machine Identity Working Group, to ensure that IGA tools support the rapid growth of, and the relationships between, different types of nonhuman identity.

Note 1
Representative Vendor Selection

The vendors included in this Market Guide were selected to represent examples of providers of products that fall into the category of (1) complete IGA suite or (2) light, platform-based IGA solution (that is, a solution based on a converged IAM platform or forming part of a non-IAM platform). Their products are typically sold in ways that accord with these categories, and they are typically bought and used for the purpose of administering and governing identities. Additionally, the listed vendors have achieved some degree of visibility and traction in this market.

Document Revision History

Market Guide for Identity Governance and Administration - 7 December 2020

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

IAM Leaders' Guide to Identity Governance and Administration

Buyer's Guide for Identity Governance and Administration

Gartner’s Identity Governance and Administration Deployment Planning Model Maximizes Value and Minimizes Risk

Managing Machine Identities, Secrets, Keys and Certificates

Is Light IGA Right for Your IAM Needs?

Table 1: Representative Vendors in the Identity Governance and Administration Market

Vendor	Product Name	Product Category	Headquarters
Atos	Evidian Identity Governance and Administration	Complete IGA suite	Bezons, France
Bamboo Cloud	Cloud IAM Platform	Light, platform-based IGA solution (part of a converged IAM platform)	Shenzhen, China
Broadcom	Symantec IGA	Complete IGA suite	California, U.S.
Clear Skye	Clear Skye IGA	Light, platform-based IGA solution (part of a non-IAM platform)	California, U.S.
E-TRUST	HORACIUS Identity & Governance	Complete IGA suite	Sao Paulo, Brazil
EmpowerID	Identity Lifecycle and Administration	Complete IGA suite	Ohio, U.S.
Evolveum	midPoint	Complete IGA suite	Bratislava, Slovakia
Fálaina	Fálaina IGA	Complete IGA suite	Singapore
ForgeRock	ForgeRock Identity Governance	Complete IGA suite	California, U.S.
Hitachi ID Systems	Hitachi ID Bravura Security Fabric	Complete IGA suite	Alberta, Canada
IBM	IBM Security Verify Governance	Complete IGA suite	New York, U.S.
Identity Automation	RapidIdentity Identity and Access Management	Complete IGA suite	Texas, U.S.

Ilantus	Compact Identity	Light, platform-based IGA solution (part of a converged IAM platform)	Illinois, U.S.
Imprivata	Imprivata Identity Governance	Complete IGA suite	Massachusetts, U.S.
Iteris	CAP2AM	Complete IGA suite	Sao Paulo, Brazil
Micro Focus	NetIQ Identity Governance and Administration	Complete IGA suite	Newbury, U.K.
Microsoft	Azure Active Directory (Azure AD) Identity Governance	Light, platform-based IGA solution (part of a converged IAM platform)	Washington, U.S.
N8 Identity	TheAccessHub	Complete IGA suite	Ontario, Canada
Okta	Okta Identity Governance	Light, platform-based IGA solution (part of a converged IAM platform)	California, U.S.
Omada	Omada Identity Cloud	Complete IGA suite	Copenhagen, Denmark
One Identity	Identity Governance and Administration	Complete IGA suite	California, U.S.
Oracle	Oracle Identity Governance	Complete IGA suite	Texas, U.S.
Paraview Software	Unified Identity Management Platform	Light, platform-based IGA solution (part of a converged IAM platform)	Shanghai, China
SailPoint	SailPoint IdentityNow, SailPoint IdentityIQ	Complete IGA suite	Texas, U.S.
SAP	SAP Identity Management	Complete IGA suite	Walldorf, Germany
Saviynt	Saviynt Enterprise Identity Cloud	Complete IGA suite	California, U.S.

SecurEnds	SecurEnds	Complete IGA suite	Georgia, U.S.
Soffid	Identity Governance Administration	Light, platform-based IGA solution (part of a converged IAM platform)	Palma, Spain
Sysintegra	ZertID	Light, platform-based IGA solution (part of a non-IAM platform)	Melbourne, Australia
Tuebora	Tuebora (IAM Platform)	Complete IGA suite	California, U.S.
USERCUBE	Usercube IGA	Complete IGA suite	Marseille, France

Source: Gartner (July 2022)

Gartner Identity & Access Management Summit

March 20 – 22, 2023 | Grapevine, TX
gartner.com/us/iam

Experience Gartner research live

Join Gartner experts and your peers at Gartner Identity & Access Management Summit 2023, March 20 – 22, in Grapevine, TX, to share valuable insights on adopting an identity-first security mindset, putting identity-based controls at the heart of your organization's protection architecture and expanding capabilities around threat detection and response.

Learn more at **gartner.com/us/iam**

Gartner®