

Identity Governance Administration (IGA), 2022

Summary

Omdia view

Identity governance and administration (IGA) is a class of enterprise security technology that manages the lifecycle of an identity within an organization. This starts with the onboarding of a new employee into the corporate identity store and the provisioning of appropriate access rights. It then continues with the changes as a person progresses through the company, gaining promotions or switching to different teams, and ends with the deletion of the identity from the corporate directory and deactivation of their access entitlements when the person leaves the organization.

Catalyst

This report describes the evolution of IGA technology and introduces the key capabilities of a platform in this product category.

As this report chronicles, IGA started life in the early 2000s as a tool for organizations to meet a sudden surge of legal and regulatory requirements. In other words, its initial purpose was compliance. However, as with another technology that came into existence for that purpose, namely security information and event management (SIEM), it has grown into a key enabler of security as well particularly now that the COVID-19 pandemic has turbocharged the digital transformation programs that were already underway, in a more cautious fashion, at most organizations.

There are two dimensions to the problems IGA seeks to address in the current environment. First, there is the atomization of the workforce, a process that was already underway long before the pandemic; it is driven by business process outsourcing (BPO), the increasing ease of mobile computing, and, more broadly, by the changing work-life balance priorities of new generations entering work. In this context, COVID-19 merely accelerated the process, driving millions of knowledge workers around the world to work from home on a full-time basis. While some of them are, of course, returning to the office now, that return is frequently only partial, and flexible work is very much the spirit of the age.

In this environment, there is a shift in priorities to the following:

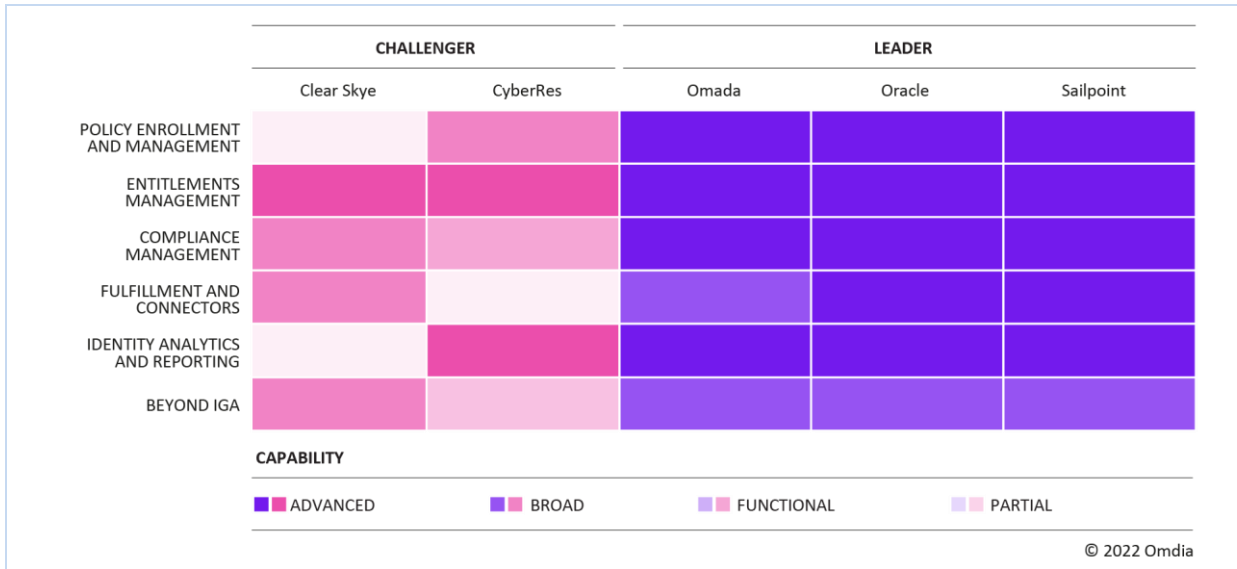
- The ability to bring new employees into the workforce.
- The provision of appropriate hardware, software, and critically the services they require to do their jobs.
- The ability to keep up with the changes in their working practices as they move through the organization is critical.

The second dimension is the cloudification of application infrastructures. Enterprise applications were already moving to the cloud long before the pandemic, to be delivered as a service. However, the impact of the pandemic was to turbocharge that process. Applications for use by employees and

partners now needed to be in the cloud for ease of remote access, while apps for the consumer also rushed to the cloud as online channels became the sole points of interaction with customers for many businesses. While IGA is not primarily designed to address the B2C identity requirement, it does deliver lifecycle management and entitlement control for the identities of developers, whose role became more critical as the pandemic accelerated digital transformation projects.

This backdrop explains the importance Omdia attributes to the cloud, not only as a locus from which to deliver IGA but also as the place where an increasing number of corporate assets now reside, which puts a new level of requirement of entitlements management.

Figure 1: The identity governance administration vendors covered in this report



Source: Omdia

IGA evolved out of IAM because of growing compliance needs

Identity and access management (IAM) technology has a long pedigree in IT with origins back in the second half of the 20th century (particularly the 1960s and 1970s) when computer systems were increasing their presence within organizations, and it became more convenient to catalog employees and their roles and responsibilities in digital form rather than in physical file systems, particularly for large organizations.

LAN and home computing boosted the need for IAM

The importance of such technology only increased as the microcomputer revolution took off in the 1980s. Employees could work not only on a desktop computer sitting on a LAN in the office but also from home on their PCs. Since these “home PCs” were initially desktop machines belonging to the employee, tight controls needed to be enforced on what corporate assets someone could and could not access when working in such a scenario. This period also saw the rise of computer viruses and the antivirus software needed to combat them.

By the 1990s, the laptop revolution was underway enabling employees to take their machines home or on the road, and as internet connectivity became ever more ubiquitous, the idea of “working from anywhere” took off. IAM platforms then had to manage and control identities and their access rights on and off the corporate network.

Furthermore, as business process outsourcing (BPO) took off as part of economic globalization, it was increasingly common for some of those identities to come from other organizations (e.g., partners, suppliers, resellers, and contractors). With that, the concept of identity federation was born, allowing enterprises to share their corporate directories with each other so that employees could work across corporate borders and thus behind the firewall of another company.

Tighter regulations in the 2000s drove the growth of IGA

The new millennium brought a whole host of new challenges and saw technology arising to address them. The Enron, Tyco, and WorldCom scandals of the early 2000s provoked a global legislative response to the wholesale corporate malfeasance it revealed, with the most obvious manifestation

of this reaction being the Sarbanes–Oxley Act (SOX) of 2002. SOX was set up to protect investors from fraudulent accounting activities by corporations.

Suddenly, regulatory compliance gained new teeth, and identity management systems went from being an operational aid to a legal necessity.

It was during the early 2000s that IGA platforms came into being. What had previously been the “front half” of an IAM system such as handling the onboarding of new employers, setting up their access rights, and adjusting them in accordance with role changes became a discipline. Meanwhile, the other half of IAM—handling daily access requests of the identities held on the system—started to be offered in software as a service (SaaS) mode, or to use the parlance gaining currency at the time, it began to move into the cloud; Okta, the market leader in this new identity as a service (IDaaS) sector, was founded in 2009.

The need for IGA arose in response to the stringent new data regulations that were emerging such as SOX as well as the Health Insurance Portability and Accountability Act (HIPAA), passed in 1996 to govern the burgeoning world of health information, its electronic exchange, privacy, and security. SOX, HIPAA, and myriad other regulations like the Payment Card Industry Data Security Standards (PCI DSS) of 2004. These regulations demanded an improvement in data management and transparency.

Market size and growth

In 2022, the IGA market is projected to reach \$6.7bn (or 20.1% of the overall identity, authentication, and access market). The IGA market is projected to have good growth during the forecast period, increasing to \$12.1bn in 2026.

Figure 2: The world market for IGA by revenue (\$m)



© 2022 Omdia

Source: Omdia

Scope of this Market Radar

Omdia has broken down the important capabilities of IGA solutions into seven major categories:

- Identity lifecycle management
- Policy enrollment and management
- Entitlements management
- Compliance management (access certification)
- Fulfillment and connectors
- Identity analytics and reporting
- Beyond IGA

Criteria for scoring IGA vendors

Identity lifecycle management

Identity lifecycle management can be defined as the bedrock for identity governance. In today's flexible and real-time world, there needs to be an updating and modernization of the identity lifecycle management for applications. This needs to be done at scale to be successful and effective. Identity lifecycle management includes capabilities such as user provisioning, identity lifecycle management support, and access requests and approvals.

Policy enrollment and management

Policies are at the heart of identity governance. Policies specify how things should be and what the ideal state of all the systems and data is. Policies can be complicated and can evolve and change over time. This can be a result of changes to regulations and changes in organizational needs as a company grows and evolves. Omdia believes that this makes policy management a challenging thing to do. Policy enrollment and management includes capabilities such as policy management, role management, and role hierarchy.

Entitlements management

Entitlements are also known as authorizations, privileges, access rights, permissions, or rules, and refer to the corporate assets (devices, databases, applications, services, etc.) that an individual employee, partner, or contractor can access and what they are allowed to do on that asset. For example, read only, read and write, upload and download data, copy, forward, and delete. They evolve as a person makes their way through different roles at an organization, and it is the job of entitlements management to handle the moves, adds, and changes (MACs) required to accompany and enable that process. Entitlements management includes capabilities such as traditional entitlements and cloud entitlements.

Compliance management (access certification)

Compliance management has evolved in recent years to consider today's dynamic and remote workforce. Compliance management includes capabilities such as access request and certification, segregation of duties (SoD) and data access governance (DAG).

Fulfillment and connectors

Fulfillment is a capability that deals with the propagation of changes to target systems. Fulfillment creates, modifies, and deletes user accounts. Strictly speaking, this capability fulfills the policy; for example, by creating an account when such an account is mandated by the policy.

Connectors are processes instantiated in software that run on a schedule, extracting data from a source, and writing it into a destination location often filtering and transforming it into a proper format or structure for the purposes of querying and analysis.

Identity analytics and reporting

Identity analytics and reporting is a function to enable the vast amounts of data available to and generated by an IGA tool to be leveraged to enhance governance and provide valuable intelligence. This is complemented by inbuilt reports, custom reports, data modeling, and dashboards for metrics. IGA products are increasingly being used as powerful analytics tools to satisfy reporting requirements and to support deeper and more flexible interactions with available data. These analytics tools allow data to be analyzed using multiple perspectives and statistical methods to generate insights from the information. This involves exploiting identity, entitlements, and operational data. Identity analytics reporting includes capabilities such as customizable and advanced reporting, auditing features, and identity analytics with AI/ML.

Beyond IGA

This criterion scores vendors from two perspectives:

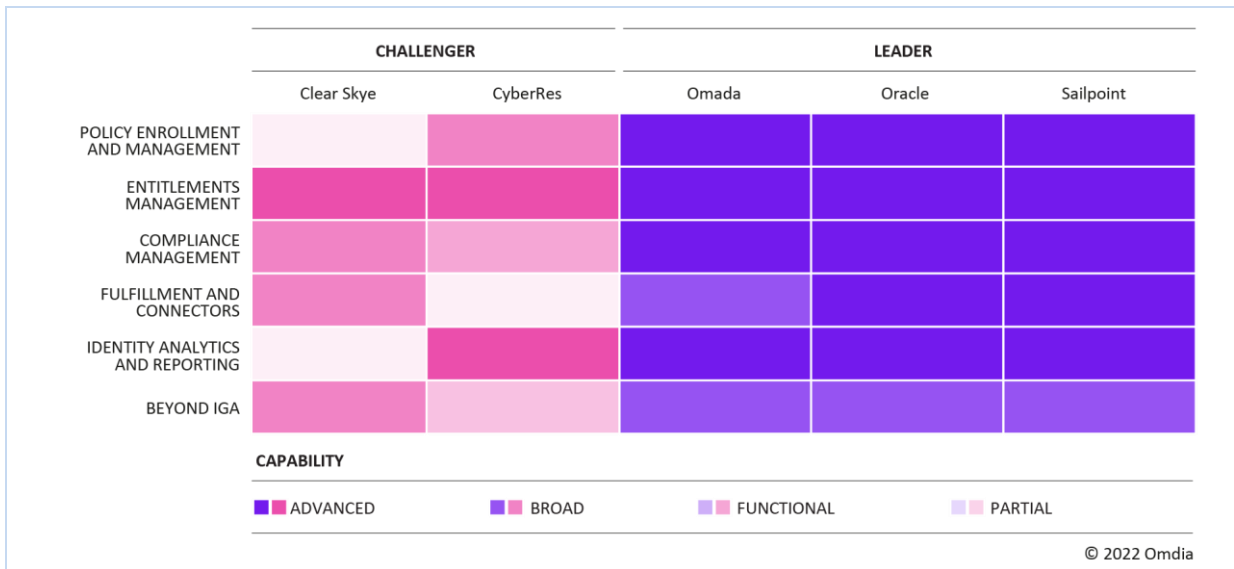
- On the breadth of their existing integrations with other security tools. Examples are PAM, cloud security posture management (CSPM), or endpoint security.
- On the vendor's plans to develop their own technology in contiguous areas of security.

Omdia Market Radars represent a benchmarking exercise that is usually performed on less-mature markets, while sectors that have been in existence and have developed for longer, such as firewalls or identity management platforms, are considered in a different type of report, namely an Omdia Universe.

As such, a Market Radar uses more coarse-grained criteria to provide an early look at how a sector is evolving and who Omdia considers the current frontrunners are. It does not include a facility for weighting the individual criteria. If it did, we would have given extra weight to Beyond IGA because:

- The range of technical capabilities of each platform is fairly standard, and most of the products under consideration meet the majority of these requirements, which means stark differentiation between them is difficult.

Figure 3: The IGA vendors in this report



Source: Omdia

As **Figure 3** shows, we have scored the vendors on a range of criteria resulting in a ranking where we have three Leaders and two Challengers. It is worth noting, however, that the technical differences between the groups were minimal in that any IGA platform must bring a certain set of capabilities to the table, such that one or two of our Challengers were very close to being Leaders. That said, here is our rationale for the rankings.

For Challenger **Clear Skye**, the colors in the heatmap explain what we considered to be its greatest strengths.

CyberRes ranked as a Challenger, although it was close to making it into the Leader category. Omdia liked where the company has come from with its IGA offering and very much appreciated where it is going with its product roadmap.

Omada is ranked as a Leader. This reflects the fact that Omada has a highly scalable IGA solution with a best practices framework that leverages its 20 years’ experience in this space.

Oracle is also a Leader here due to the depth of Oracle’s knowledge in IGA as evidenced by its longevity in this market and the thousands of customers that rely on its technology in this sector. It is also moving towards a more prescriptive stance based on recommendations and/or automated actions, which is in line with the broader trend towards proactive security that Omdia has identified and lionized over the last couple of years.

Sailpoint is a Leader for a couple of reasons. It is the largest vendor in the IGA space in terms of revenue. It also has a comprehensive offering that can be acquired as software for deployment wherever the customer prefers (i.e., on-premises or in a private cloud), or as a service delivered from the cloud.

Where the IGA market is headed

Before we pass to the profiles of individual vendors, a word about where Omdia sees the IGA market going. IGA has needed to evolve and modernize in recent years, and the pandemic has accelerated this process. Traditional IGA products/solutions were built to address user provisioning through complex integration and systematic application of heavily engineered, role-based access control (RBAC) structures. Having a cloud-based IGA product that also offers APIs that can be readily consumed and make connectivity easier to integrate.

IGA vendors need to adapt and evolve their products and services to better fit the current business environment. This involves cloudification of their IGA products and launching new features such as APIs into their portfolios. IGA technology already needs to move into the cloud, an inflection point that should bring with it opportunities for service providers. While large enterprises have traditionally onboarded and managed their employee identities themselves, that activity may have become cumbersome if they grow through M&A, while the B2B aspect can be even more challenging to a global MNC. Service providers that can handle identity federation should scope out business opportunities in this context. Having a cloud-based approach will be critical in enabling IGA to work seamlessly with other services and simplifying the evolution to a future-proof IT security infrastructure.

Vendor analysis

Oracle

Oracle is an established player in the identity governance and administration (IGA) market, which it entered midway through the 2000s such that it has had a comprehensive offering here for many years called Oracle Identity Governance (OIG). Now it is developing a new, cloud-native platform called Oracle Access Governance (OAG) designed to run hybrid with OIG or as a replacement. Oracle will continue to invest in both products. While OIG does both the governance and administration side of IGA, OAG delivers governance from the cloud, while on the administration side (i.e., the identity lifecycle management part) is cloud-delivered by its OCI IAM service.

The management of the identity lifecycle for employees and partners—from the initial provisioning of access rights through the changes required as someone progresses through the organization until deactivation when they leave—is a vital part of the work of IT operations and security. Meanwhile monitoring access patterns, curtailing unnecessary and excessive entitlements, is essential to maintaining optimal security posture.

As IGA evolves beyond RBAC and towards the policy-based (PBAC) and attribute-based (ABAC) approaches, there is an opportunity for providers to help existing customers on that journey, as well as to pick up new ones requiring a more advanced technology platform to meet these emerging requirements.

With its extensive experience, large customer base, and comprehensive technical resources in IGA, Oracle is well placed to ride this evolutionary wave, allowing existing customers to move to its new, cloud-native IGA service at the pace that best suits them and attracting a new clientele that needs to move from legacy providers that have failed to keep up with emerging market trends.

Why put Oracle's IGA on your radar?

The depth of Oracle's knowledge in IGA is evidenced by its longevity in this market and the thousands of customers that rely on its technology in this sector. Now the vendor is developing the next generation of its IGA offering founded on contemporary thinking about how applications should be delivered and the kind of functionality a modern IGA platform should offer.

In particular, it is moving towards a more prescriptive stance based on recommendations and/or automated actions, which is in line with the broader trend towards proactive security that Omdia has identified and lionized over the last couple of years.

IGA is what used to be the front end of an identity and access management (IAM) platform, handling the onboarding of new employees' identities and the provisioning of the appropriate entitlements (rights of access to applications and databases) for them to do their jobs as well as the necessary adjustments when they changed roles and deprovisioning when they left the organization. In other words, the MACs. The other half of IAM, meanwhile, was the access side of the equation, covering features such as multifactor authentication (MFA) and single sign-on (SSO).

Since the turn of the millennium, the IAM market has essentially bifurcated, with the two core capabilities being provisioning and access management. The provisioning added a governance capability and became IGA. Meanwhile, access management morphed into what is now known as the identity as a service (IDaaS) market with the new acronym blurring the lines because it includes identity lifecycle management (LCM), which is also a subset of IGA functionality. Each sector has followed its own trajectory with the IDaaS side moving into the cloud from around 2010 driven by a couple of key changes in the work environment.

There was the cloudification of enterprise applications generally plus the spread of remote working. After all, if someone was requesting access from random location outside the corporate network to apps that were themselves residing in the cloud, why not grant that access from the cloud?

While slower to make that same transition, IGA is now also moving into the cloud, making it easier for admins to access the platform from anywhere and removing the upfront costs of deploying traditional on-premises server software.

Some perceive IDaaS with LCM as good-enough IAM. A significant portion of the SME space probably feels this way, which is why some of the pure-play IDaaS vendors have been so successful there. Larger enterprises, on the other hand, do not get enough IGA functionality from IDaaS services, and typically have several IAM platforms in place (e.g., IGA + IDaaS, and/or AM) to address their typical requirements.

Will IGA and access reunite?

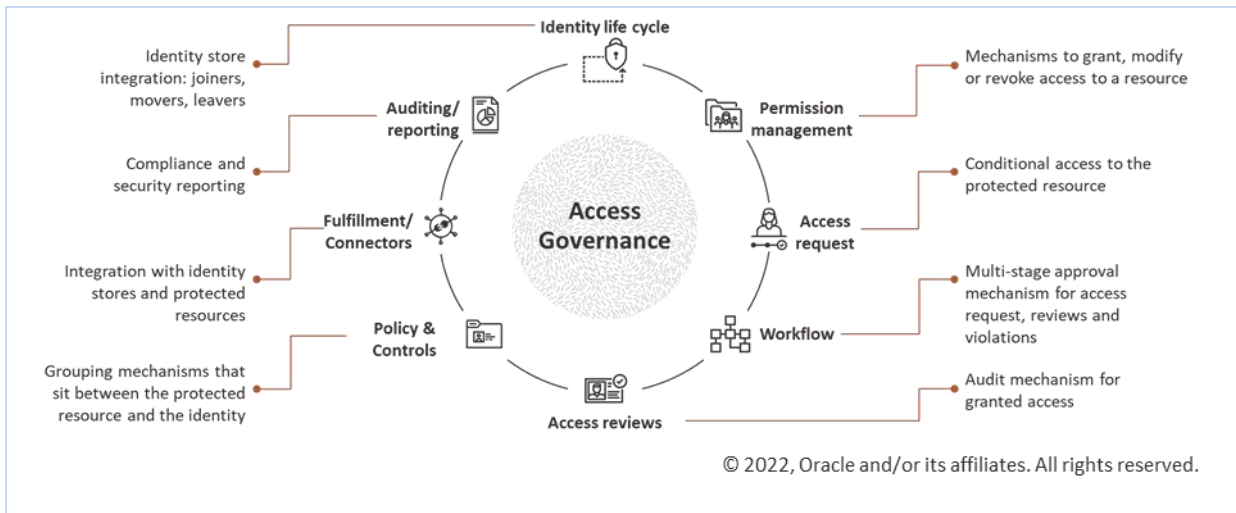
Beyond this evolution in delivery models for both access and now IGA technology, however, there are trends in the market that suggest that in the coming years these two branches of identity management may actually start to converge again.

The entire field of identity is now called to be more responsive and flexible to address the more mutable nature of organizations, applications, and end-user roles and access requirements. The role of IGA has gone from provisioning who has access to what to understanding how access is being used within an organization and dynamically enforcing policies around that usage. And with ideas such as dynamic authorization, relying on ABAC rather than the traditional RBAC approach as a means of achieving the goals of responsiveness and flexibility, there is an argument that IGA and access will need to become one system again.

We are certainly seeing moves in this direction. Okta, the cloud-native market leader in IDaaS, has launched its Okta Identity Governance service this year, while in October 2021, One Identity, a Tier 2 IGA and PAM vendor, acquired OneLogin, a challenger to Okta in the IDaaS market. And in August 2022, Netwrix, which offers both PAM and data access governance (DAG) technology, acquired a smaller IGA player called Usercube, with plans to integrate its technology into both the existing Netwrix offerings in the identity space.

It is no coincidence, therefore, that Oracle's new cloud-native offering is called Oracle Access Governance.

Figure 6: Oracle’s access governance capabilities



Source: Oracle

Product/service overview

Oracle Identity Governance (OIG): Given that it has been in the market for well over a decade, OIG has obviously been Oracle’s flagship offering in the IGA market until now, and as you would expect from such a product it is by now a comprehensive, fully featured, and highly customizable platform with all the bells and whistles of an enterprise IGA system. While it started life in the era when IGA was always on-premises software and is still available in that format, OIG’s delivery modes have evolved such that it can now be acquired as containerized software for deployment in a cloud of the customer’s choosing (public or private, and managed by the customer themselves), or as an Oracle-managed cloud service.

OIG’s core function is, of course, to manage users’ access privileges within enterprise IT resources. Beyond that:

- As enterprise IGA requirements have grown more complex and the costs associated with managing them have increased, the platform has added capabilities such as OIG Self Service, which supports use cases such as access requests to approvals, as well as updates to personal profiles.
- Similarly, application onboarding has been streamlined with an extensive set of connectors available to automate the process and eliminate manual configuration, with features such as schema discovery for flat file and database.
- The allocation of audit and compliance tasks has been simplified.
- Meanwhile Oracle Identity Role Intelligence, which is based on analytics backed by ML has been added for greater understanding and automation to meet the expanding requirement for understanding of access patterns and entitlements to underpin the curtailment of excess permissions, as well as to automate and optimize RBAC.

- Workflows are highly customizable with the use of Oracle's SOA Composite Application Architecture, while for customers with less-sophisticated requirements, a simpler version of this tooling will be made available in the near future.

Oracle Cloud Infrastructure IAM (OCI IAM): OCI IAM, formerly Oracle Identity Cloud Service, was introduced in 2018 as a SaaS-delivered identity service focusing primarily on access management, but also providing identity lifecycle management for applications running on-premises, hosted in the cloud, or delivered as SaaS.

In addition to leveraging IAM standards such as SAML, OpenID Connect, and SCIM, OCI IAM leverages a set of proxies, bridges, and gateways that extend support to virtually any target system. This includes Oracle's widely used suite of business applications (E-Business Suite, Peoplesoft, JD Edwards, etc.) as well as non-Oracle targets such as SAP and Active Directory. OCI IAM serves as the cornerstone of Oracle's SaaS-delivered IAM offerings.

OCI IAM does not, however, natively offer access governance capabilities and traditionally, customers rely on external IGA solutions such as OIG for managing access risk, segregation of duties (SoD) checking, and entitlement reviews.

Oracle Access Governance (OAG): Against this backdrop of a mature, comprehensive product offering in OIG and an IDaaS service in OCI IAM that lacks strong governance capabilities, Oracle is now rolling out OAG, which is a cloud-native service delivering the reach, control, and visibility across an organization's entire environment, from mainframe applications through to SaaS apps and including edge and IoT environments.

While it inevitably currently lacks full feature parity with OIG today, the company has a roadmap for the next few years to achieve that goal:

- OAG's current capabilities are in the areas of governance and compliance, as well as identity intelligence.
- Identity orchestration, i.e. the ability to orchestrate behavior across identity systems via an abstraction layer that apps use to integrate with those systems, without changing the application code or modifying configurations, exists as a framework today. However, Oracle plans broader support for it going forward.
- Access management is delivered by OCI IAM, of course, and is still evolving in its capabilities. At the moment the platform focuses on identity intelligence and access review, but there are plans to support PBAC in addition to PBAC-controlled RBAC within months. There will also be an extensible and customizable attribute library for ABAC further down the road.

Clearly, the first phase for the rollout focuses on integration with OIG, enabling the vendor's thousands of enterprise customers to migrate across to the new platform at a rate that suits them. For this purpose, Oracle compiles a lightweight custom agent that is highly encrypted, managed from the cloud by OAG, and designed to work with the customer's OIG installation. Via this agent, OAG syncs all datastores within an hour then makes event-based updates.

There are also plans to enable the development of agents for third-party IGA systems, enabling OAG to integrate with them and, over time, to potentially replace them altogether.

Company information

Background

While Oracle itself was founded in 1977 as a provider of database technology, the vendor has been in the IGA business since its 2005 acquisition of Thor Technologies, a provider of what at the time was called “secure enterprise provisioning.” Its offering was further strengthened in 2010 when it acquired Sun Microsystems, which brought it an established IAM portfolio that included a significant identity analytics capability.

The Oracle Identity Governance Suite of products had its origins in the Thor acquisition and was then enhanced when Sun’s technology came into the fold. OIG manages user provisioning and deprovisioning and provides actionable identity intelligence that enables remediation of high-risk user entitlements.

Current position

This report comes as Oracle is transitioning both its IGA product offering and customer base from a mature, full-featured product that started life as on-premises software to a new, cloud-native one, with a rapid cadence of new features scheduled for the latter.

The challenge that any vendor with a significant customer base on an existing product faces when planning the introduction of a brand new one that will ultimately replace it is, of course, how best to ease customers from one to the other. If they are heavily invested in OIG, they will have built up considerable in-house expertise on configuring and running it, so any migration to OAG will need to be as seamless as possible. It should ideally be offered in as piecemeal a form as customers may desire, enabling them to swap out their legacy OIG functionality and replace it with the OAG equivalent without the generating the feeling of a second “Big Bang” among those operating the platform or the wider employee base.

Of course, Oracle has extensive experience in managing such migratory processes, and Omdia is confident that the vendor will be able to move the majority of its OIG customers across to OAG in a relatively painless process. It will be interesting to see whether it also manages to attract significant net-new customers to the OAG platform given its forward-thinking approach to many of the core requirements of IGA.

Future plans

OAG introduces a number of new concepts to Oracle’s IGA offering. While OIG already has a cloud-based deployment option, the new platform is cloud native, which means that it is designed and developed from the outset to take advantage of the scalability and flexibility of the cloud.

Beyond that, however, Oracle is also developing OAG with the new tenets of IGA at its core, which include a more flexible approach to access control based ultimately on attributes rather than roles, as well as a more proactive stance on how to improve security posture with an IGA platform, which essentially move identity analytics into the 21st century.

Key facts

Table 2: Data sheet: Oracle

Product/Service name	Oracle Identity Governance Oracle Access Governance OCI IAM	Product classification	IGA
Version number	OIG – 14C	Release dates	2005 June 2022 2018
Industries covered	All	Geographies covered	Global
Relevant company sizes	All	Licensing options	SaaS licensing based on identities under management for OAG and OCI IAM
URL	www.oracle.com	Routes to market	Direct and channel
Company headquarters	Austin, TX (US)	Number of employees	+130,000

Source: Omdia

Appendix

Further reading

[Identity, Authentication, Access Market Tracker – IH22 Database](#) (May 2022)

[Fundamentals of Identity Governance Administration \(IGA\)](#) (March 2022)

[2022 Trends to Watch: Identity, Authentication, Access](#) (November 2021)

Authors

Rik Turner, Principal Analyst, Cybersecurity

Don Tait, Senior Analyst, Cybersecurity

askananalyst@omdia.com

Citation Policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials