

Critical Capabilities for Identity Governance and Administration

Published 6 November 2019 - ID G00366959 - 98 min read

By Analysts [Henrique Teixeira, David Collinson](#)

Initiatives: [Identity and Access Management and Fraud Detection](#)

IGA tools help organizations control access risks, achieve and maintain compliance, and improve efficiency by managing user accounts and entitlements in infrastructure systems and applications. SRM leaders responsible for IAM should evaluate critical capabilities during IGA tool selection.

This Critical Capabilities is related to other research:

[Magic Quadrant for Identity Governance and Administration](#)

[View All Magic Quadrants and Critical Capabilities](#)

More on This Topic

This is part of an in-depth collection of research. See the collection:

- [IAM Leaders' Guide to Identity Governance and Administration](#)

Overview

Key Findings

- The transition of identity governance and administration (IGA) to cloud delivery is ongoing. The majority of IGA vendors have included some kind of SaaS-delivered capability, with only two out of the 11 vendors evaluated not offering at least a managed services offering. There is a big variation of delivery types offered today, from basic hosted models all the way to cloud-architected IGA solutions.
- Most IGA products have matured to provide well-balanced governance and administration functionality, but identity analytics capabilities still vary among vendors, and few vendors offer advanced analytics capabilities.
- Analytics is most commonly used in the early phases of the IGA deployment during the analysis and design of user and entitlement relationships. More than half of the organizations have already made use of (identity) analytics, with the most common use cases being monitoring (61%), privileged account discovery (58%), access policy analysis (52%) and reporting (52%).
- IGA solutions can be difficult to deploy. Gartner estimates that 50% of IGA deployments are in distress — that is, they have failed to achieve functional, budgetary or timing commitments. The

IGA deployments that most often end up in distress are software-delivered or prioritize provisioning during early phases.

Recommendations

Security and risk management leaders responsible for identity and access management should:

- Implement a SaaS-delivered IGA strategy, either as a replacement of software-delivered implementations or to enhance existing IGA platforms. SaaS-delivered IGA is the preferred delivery method for identity analytics, for supporting SaaS applications as target systems or for adding elastic performance capabilities to adjust computing processing power up and down for high-volume use cases like access requests and password reset.
- Prioritize identity analytics use cases as a way to mitigate risk earlier in the process of adoption of IGA processes. Select IGA tools that can support analytics for both cleanup and continuous governance, on top of more traditional analytics use cases like designing user and entitlements relationships (role mining and engineering).
- Choose solutions that can be delivered at least as a cloud-hosted model, if a cloud-architected SaaS-delivered IGA solution is not feasible due to regulations or other factors. This will reduce the complexity of ongoing operations, break and fix, and the application of critical updates.
- Leverage indirect fulfillment, like ITSM ticketing integration, as a mechanism to further reduce the complexity of developing and maintaining customized provisioning adapters.

Strategic Planning Assumptions

By 2022, SaaS-delivered IGA solutions will augment or replace 75% of existing software-delivered IGA implementations globally, up from 30% today.

Through 2022, IGA implementations that start with cleanup analytics will show twice the return on investment (ROI) as ones that don't.

By 2022, more than 50% of IGA vendors will offer predictive and recommendation engines leveraged by machine learning (ML) and artificial intelligence (AI) analytics, up from less than 15% today.

What You Need to Know

IGA plays a critical role in the administration, monitoring and control of user access for most organizations with more than 2,500 users and many that have as few as 500 users. IGA is typically one of the largest investments identity and access management (IAM) programs make, including the cost of software and professional services, as well as the head count and additional support required to grow and maintain the system.

Deployments of IGA products continue to challenge IAM leaders because they sometimes underestimate the effort and lack skilled staff to implement such products. However, newer approaches for outsourcing IGA capabilities to SaaS-delivered solutions can help balance an IAM program's capital expenditure (capex) or operating expenditure (opex) budget and reduce implementation risk compared to a traditional software-delivered IGA implementation.

Leveraging indirect fulfillment, as explained in the context section of this research, can also significantly reduce the complexity of IGA implementations. Indirect fulfillment techniques may include the integration with ITSM systems for creating tickets or using the IGA tool itself to orchestrate requests to be executed manually. Other indirect mechanisms may leverage SaaS-delivered access management tools as intermediaries for provisioning to SaaS target systems, or by using RPA to automate manual provisioning tasks. At the time of this writing, the vast majority of IGA vendors did not offer support for out-of-the-box integrations with RPA tools. In this case, an RPA strategy would need to be very carefully planned in order to avoid more risks and costs with custom development.

Identity analytics plays a big role in reducing identity risk. Identity analytics is being offered by several vendors to identify dormant accounts and excessive privileges, for example. Analytics are also being offered to provide context and risk-scoring calculations during access requests, approvals and certifications. In 2020, we will start to see more AI-driven predictive identity governance use cases. Predictive governance is the evolution of the current crop of recommendation and context-based identity analytics capabilities and, when it arrives, it will enable IGA tools to anticipate required actions for risk mitigation and perform more autonomous decisions.

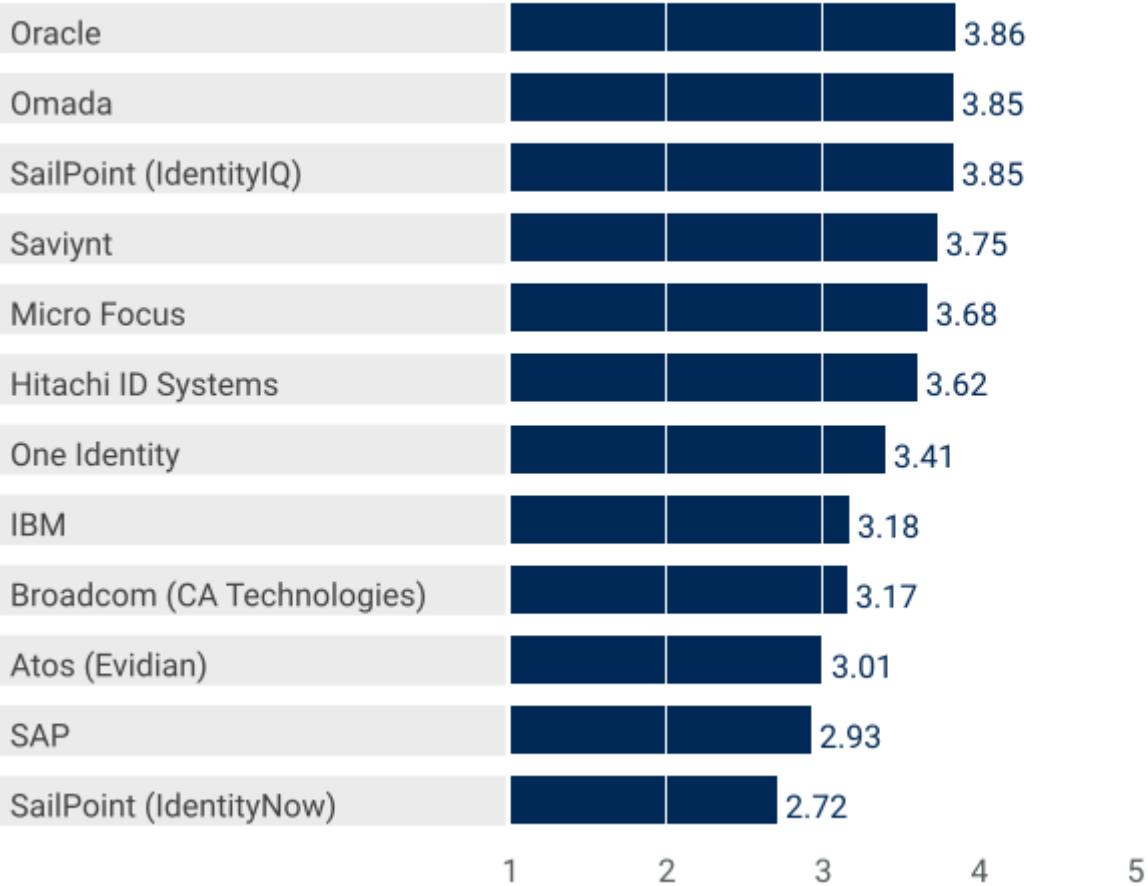
IAM leaders should use this research to gain an understanding of how IGA products can address their needs and to augment their evaluations of vendors' IGA solutions.

Analysis

Critical Capabilities Use-Case Graphics

Figure 1. Vendors' Product Scores for the Global Enterprise Use Case

Product or Service Scores for Global Enterprise



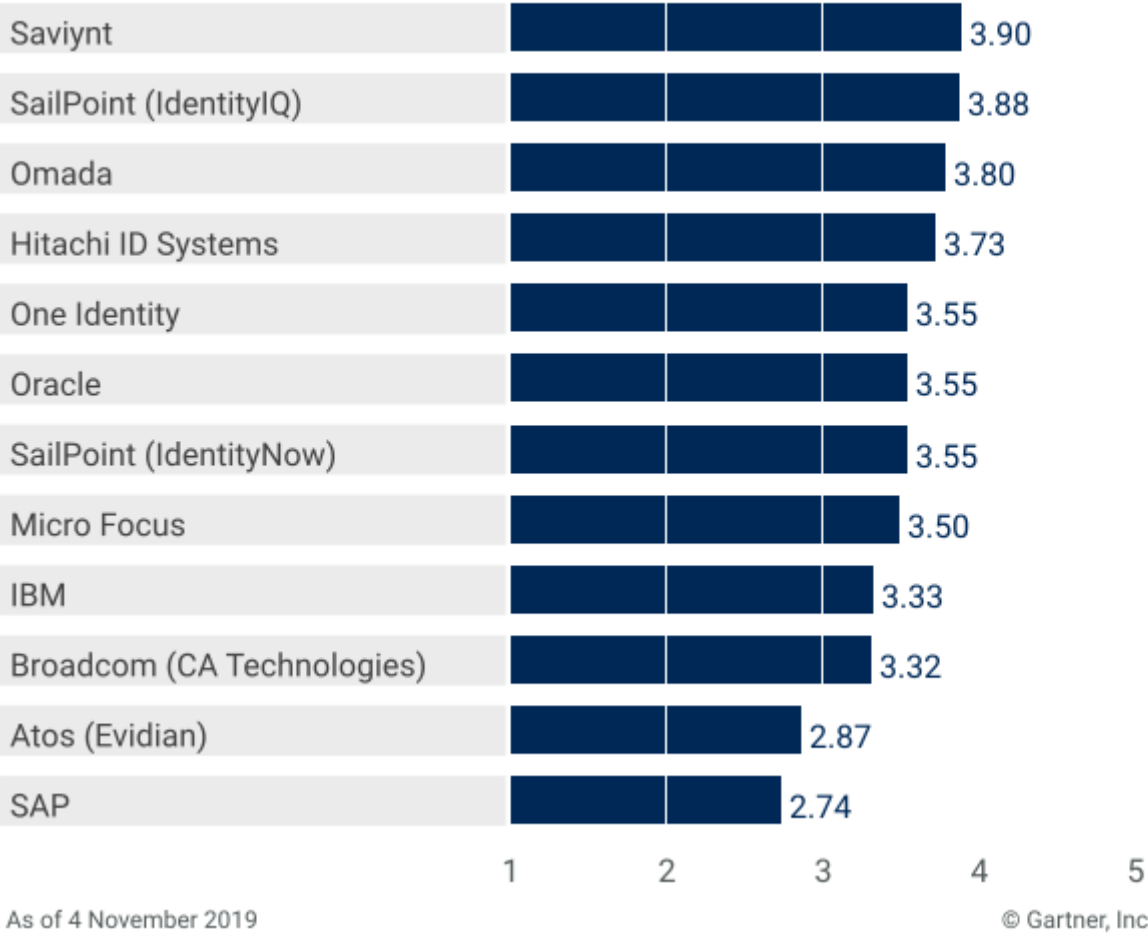
As of 4 November 2019

© Gartner, Inc

Source: Gartner

Figure 2. Vendors’ Product Scores for the Midsize Enterprise Use Case

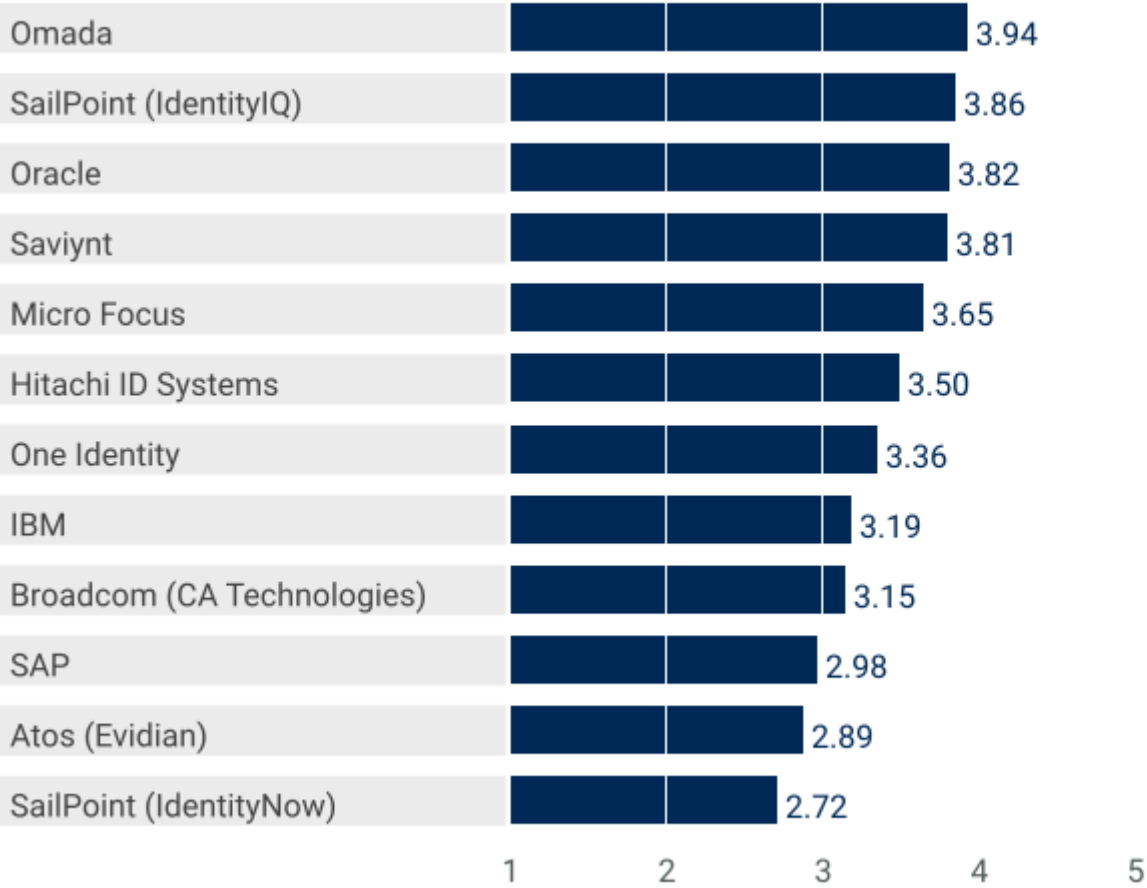
Product or Service Scores for Midsize Enterprise



Source: Gartner

Figure 3. Vendors’ Product Scores for the Governance-Focused Use Case

Product or Service Scores for Governance-Focused



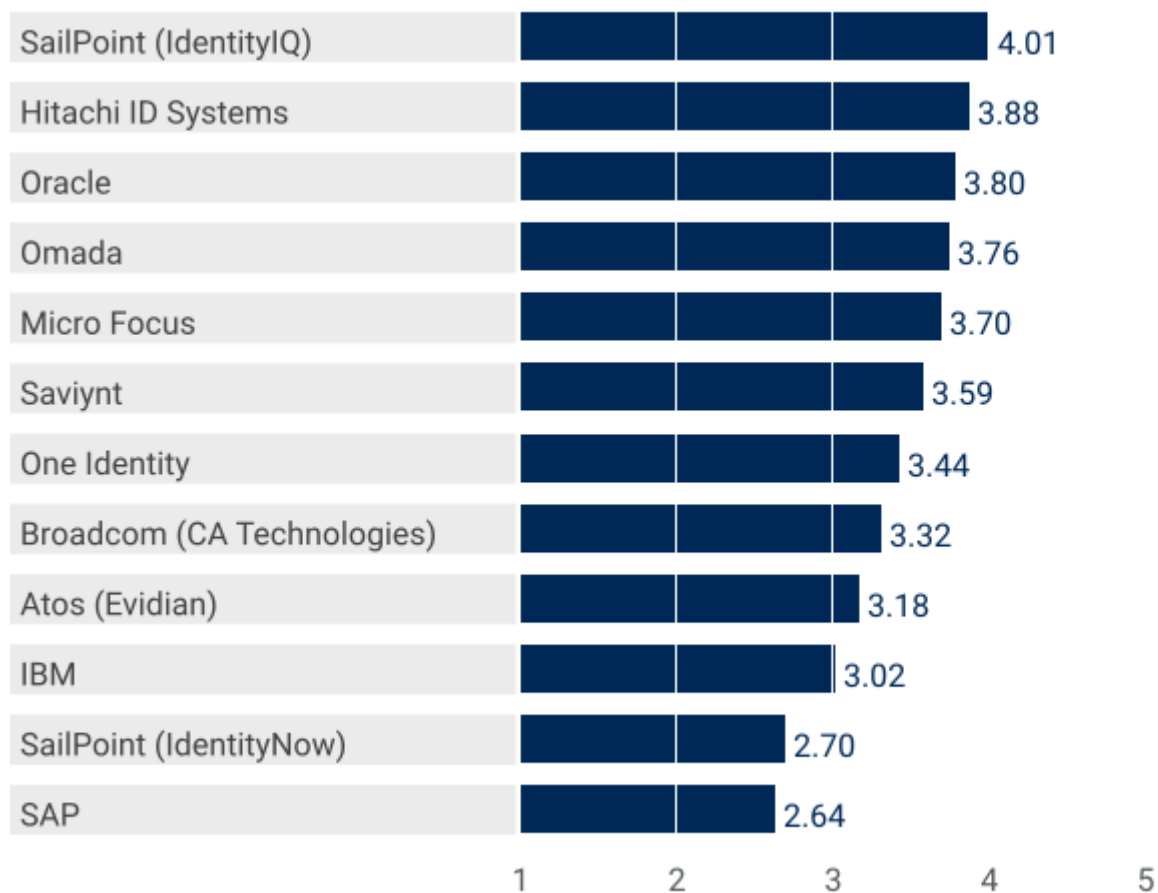
As of 4 November 2019

© Gartner, Inc

Source: Gartner

Figure 4. Vendors’ Product Scores for the Automation-Focused Use Case

Product or Service Scores for Automation-Focused



As of 4 November 2019

© Gartner, Inc

Source: Gartner

Vendors

Atos (Evidian)

Evidian Identity Governance & Administration (IGA) 10 Evolution 2 (evaluated the release from August 2018) is offered as a base product made up of Policy Manager, Request Manager, IDSynchronisation and reporting modules, with several optional modules. The base license allows up to 100 applications. The base connectors included are LDAP, SQL, CSV, UNIX, Lotus Notes, Active Directory, Exchange, Skype, SharePoint, Office 365, G Suite and Salesforce. The optional modules required to fulfill typical IGA requirements include the following:

- Workflow Editor
- Policy Creation Module
- Evidian Analytics and Intelligence
- Authentication Management

The Evidian solution will appeal to clients looking for a tight integration between IGA and access management (AM), which is provided as a separate software solution, especially within the EMEA region.

Identity Life Cycle: Good support for all four identity life cycle patterns, including RPA bots with a flexible organizational model that enables identities to be associated with multiple organizations simultaneously.

Entitlements Management: Entitlements are called “permissions” in Evidian’s data model. The schema for entitlements is not extensible, but permissions can be assigned to contexts so they can be associated with policies. For account correlation, there are no graphical analytic capabilities requiring administrators to rely on reconciliation reports.

Access Requests: The access request interface is linear and can be a little confusing for business users (for example, having to choose between roles and permissions before proceeding). Five languages are supported out of the box.

Workflow: The built-in workflow is highly flexible, offering as many as six levels of approvals. However, the means of controlling the workflow’s behavior can be complex (involving contexts and permissions), and basic features such as the delegation and handling of inactive approvers require configuration. Electronic signatures are not supported for approvals.

Policy and Role Management: There is a flexible role model that distinguishes between different types of roles. Policies to control the assignment of roles (including detachment behavior) are defined separately from the roles themselves.

Access Certification: Access certification campaigns can be based on the organization’s chart, and now, with Evolution 2, Evidian adds the possibility to perform certification campaigns by application/resource. It provides excellent support for certifications involving attributes such as expiration dates. Risk context for certifications can be set in a risk level slider during the campaign definition, but peer group analysis and microcertifications are not supported.

Fulfillment: The base set of connectors is limited, and connectors for mainframe and specialized systems are sold separately. Few SaaS connectors exist. Support for multidomain AD environments is below average, and support for fulfillment using service tickets leverages a generic ITSM connector that can be flexible. However, it is more complex to deploy than an out-of-the-box connector. Integrators need to implement specific ticket creation (and status checking) of the ITSM tool.

Auditing: The product can define SOD conflicts down to the entitlement level; however, there is no case management framework. Other audit policies often require the creation and scheduling of tasks tied to custom workflows.

Identity Analytics and Reporting: Identity analytics capabilities are market average, including some very useful metrics for cleanup. There are improved reconciliation capabilities available that

can be used for generating predefined reports, including dormant accounts. However, there are no peer-group analyses for defining outlier detection metrics.

Ease of Deployment: The core product is based on a software-only install on Windows, and compiled Java code is used in place of scripting for several scenarios. There is no virtual appliance, nor are there SaaS-delivered options, which could reduce the complexity of deployment. The newer versions have reduced the excessive fragmentation of previous versions, although some discontinuity (such as separate role mining and analytics utility) remains.

Scalability and Performance: Unlike other vendors, support for high availability at the application and data tiers requires a paid optional HA module and includes the ability to dedicate modules to separate nodes.

Broadcom (CA Technologies)

Broadcom offers one single IGA product licensed as the Layer 7 Identity Suite 14.3 (released April 2019 and formerly known as CA Identity Suite). Layer 7 Identity Suite is part of a full IAM suite from Broadcom as a result of the CA Technologies acquisition in 2018 and fulfills a broad range of IGA requirements. The suite includes the Identity Portal as a common user interface for two distinct products:

- Layer 7 Identity Manager — A back end for identity life cycle, provisioning and policy-driven administration
- Layer 7 Identity Governance — Entitlements management for the support of governance functionality

Layer 7 Identity Suite is used most often by global enterprises that are focused on provisioning and require maximum flexibility with workflow. The product is also well suited to managing large-scale, external-facing customer identity and access management (CIAM) scenarios.

Identity Life Cycle: Broadcom's Layer 7 Identity Suite Deployment Xpress feature provides prebuilt use-case templates for all four identity life cycle patterns, including RPA bots. Connectors for PeopleSoft and Workday are included, as well as a generic HR integration framework for other types of HCM systems. Contractor expirations are well handled, with scheduled email alerts to notify managers. Detecting flaws in feed files requires modifying a parser for bulk load, involving code creation.

Entitlement Management: The entitlements data model is flexible, and its interfaces satisfy all key scenarios. The schema is extensible, with 100 custom attributes catering for most customer needs via the out-of-the-box schema. Alternatively, customers can use an external identity store for adding more attributes. There are gaps in application onboarding support, such as a missing overall dashboard to measure and track progress. When discovering roles and entitlements of applications, Identity Governance offers a visual representation of these.

Access Requests: The Identity Portal module provides a well-rounded and business-friendly access request process, with an excellent single-page approach and shopping cart. Additional context for access requests, including recommendations, is available to requesters. Thirteen languages are supported out of the box.

Workflow: Deployment Xpress can provide a highly functional approval workflow template that conforms to the standard, four-stage workflow pattern, requiring only a simple configuration for manager approval and configuration of escalation policies. Electronic signatures are not supported out of the box, requiring a custom plug-in to be developed.

Policy and Role Management: Poor back end integration between the Identity Manager and Identity Governance products inhibits the ability to provide a coherent approach that combines administration with entitlements management. There is basic support for a two-layer role model, but policies are evaluated only during synchronization events, and there is no preview of role/policy changes.

Access Certification: Coverage of certification campaign types is relatively complete, including certification of the entitlements catalog, but relationship-oriented certifications (for example, managers certifying relationships with contractors) require a workaround in which contractors are modeled as entitlements. Broadcom has recently moved some of the certification capabilities to be delivered by the Identity Portal interface and reduced the confusion of having to work with three different modules. Automatic actions, like automatically initiating a campaign based on increased risk, can be defined in certification campaigns, but risk calculation and microcertifications would require customizations of the product.

Fulfillment: Broadcom has above-average fulfillment capabilities, and all 40+ provisioning connectors are included in the base product license. It also offers indirect fulfillment abilities through ITSM integrations (CA Service Desk, CA Cloud Service Management, BMC Remedy ITSM and ServiceNow are supported out of the box) or the IGA solution itself to orchestrate requests to be executed manually. Support for AD provisioning is better than most other products offer, despite the need to configure provisioning targets for every domain in a forest.

Auditing: There is no central console for defining audit policies. Even SOD policy definition is handled inconsistently. There is no case management framework to resolve audit issues, so workflow and access certification must be used as alternatives.

Identity Analytics and Reporting: Broadcom has below-average identity analytics capabilities and hasn't improved its analytics capabilities since last year. Risk calculations are done in real time for access requests, but each risk needs to be scored by an administrator. Jaspersoft Business Intelligence provides a strong platform for reporting and analytics. The identity analytics dashboard provides performance information, but effectiveness metrics require either the creation of custom reports or need to be manually extracted via yet another Windows thick client interface called Client Tools.

Ease of Deployment: The Deployment Xpress facility allows DevOps-like, pattern-based deployment in a virtual appliance form factor of all components needed to run the product. Deployment Xpress also provides a way to add functionality through the installation of components needed to fulfill common use cases. Broadcom has also released a Migration Xpress capability to facilitate the migration of existing configurations into the virtual appliance form factor, as well as a virtual appliance option for Azure. No SaaS-delivered IGA option is offered; however, hosted options are provided by third parties.

Scalability and Performance: The product has demonstrated high levels of scalability, especially in B2C and government-to-citizen (G2C) scenarios; however, reliance on data processing in the application tier when using the optional directory server back end can hamper performance in large-scale deployments.

Hitachi ID Systems

Hitachi ID's IGA solution version 11.1.2 (released in May 2019) is composed of two modules:

- Hitachi ID Identity Manager — Manages identity, account and entitlement life cycles, along with all the supporting policies and analytics.
- Hitachi ID Password Manager — Provides self-service management of passwords, PINs, certificates, biometric samples, security question/answer profiles, drive encryption keys and other credentials.

The products can be purchased separately, with Identity Manager capable of satisfying IGA requirements. The two modules can be deployed as a single platform (using a single installer) running on Windows. Hitachi ID Identity and Access Management Suite is most often deployed by organizations that need account and password management, with strong support for direct fulfillment (automated provisioning) and policy-based administration.

Identity Life Cycle: Integrated reference implementations (called Identity Express) are provided for corporate, partner portal and B2C scenarios. There is built-in support for all of the common identity life cycle scenarios, including RPA bots, with the ability to leverage social identity for user self-registration.

Entitlements Management: Provides the basic entitlements management features expected of IGA tools; however, administrative maintenance of account (as opposed to user profile) metadata requires double-targeting account repositories. Dashboards exist for various account and application correlation tasks.

Access Requests: The interface for access requests has been enhanced and continues to provide users with good control over requests, but the overall user experience and interfaces remain IT-focused. There is a user compare feature but no visual representation at the time of requests.

Customers can choose five out of seven core languages at no charge. Additional language packs are chargeable.

Workflow: The included corporate reference implementation provides a predefined workflow model, with solid support for the most common workflow needs, requiring only minor configuration to satisfy most scenarios. A mobile app is available for more convenient approvals. Requirements for electronic signatures on approvals can be satisfied with a password prompt.

Policy and Role Management: The implementation of a multilayer role model requires a combination of user classes and roles in the product, with user classes acting as business roles. There is flexibility in how policies can be applied, due to the openness of the policy model, with plug-in points for scripting that behavior.

Access Certification: In addition to support for all certification campaign types, there are additional features, such as the ability to display and correct entitlement assignment metadata (such as expiration dates) in tasks and for reviewers to delegate individual items or partial tasks. The certification workflow and UI can also be used to (1) build and repair organizational chart data, (2) review and update identity attributes, and (3) onboard new users, rather than only to deactivate identities or deprovision entitlements. Electronic signatures are supported in the form of password prompts for task submission. Hitachi ID supports risk scoring during certification campaigns, but automatic decisions require some scripting. Microcertification campaigns would also require some customization, and a single user certification would have to be configured.

Fulfillment: Has one of the largest collections for fulfillment, with more than 100 adapters, which are all included in the base product license, except one, which is the native z/OS listener. It does offer strong indirect fulfillment abilities through ITSM integration (over 15 ITSM products supported out of the box), or using its own included functionality to orchestrate manual requests.

Auditing: The reporting system can detect identity integrity constraint exceptions, but individual reports for identifying such exceptions are not provided out of the box and need to be configured, with individual controls for each type of violation. These report results can be fed back into the workflow system to generate predefined requests that behave like audit cases to facilitate remediation.

Identity Analytics and Reporting: Hitachi ID has below-average identity analytics capabilities. There is good support for data quality analysis, and it supports the concept of risk scoring. However, identifying outlier types of entitlements or excessive privileges require custom reports to be built by writing SQL SELECT statements and embedding them in Python scripts. The product provides a generous collection of built-in reports, including some new reports for desirable metrics, but there is no report designer provided. Analytics are only delivered via reports, and the role-mining analysis is not interactive.

Ease of Deployment: Identity Express (workforce, B2B and B2C) reference implementations can be selected as part of the installation to provide configurable frameworks for common features that,

in other IGA products, usually require significant assembly or even customization. Hitachi ID offers a single-tenant IaaS-hosted vendor-managed model. This offer may present an easier option than to negotiate a third-party contract for hosting and managing the Hitachi ID software.

Scalability and Performance: The product implements an active-active multimaster replication model that does not require configuration of middleware components. Most data processing has been pushed to the database tier to maximize performance. There is a new continuous reconciliation process that monitors for delta changes and that was introduced to provide a more scalable way to ingest large volumes of data, such as in CIAM scenarios.

IBM

IBM Security Identity Governance and Intelligence (IGI) version 5.2.5 (released February 2019) is made up of three modules:

- **Compliance Module** — Provides access review and certification, including access revocation fulfillment, least privilege policy configuration and validation, SOD configuration and validation, and compliance reporting.
- **Lifecycle Module** — Provides policy-based (context-based) provisioning, request-based provisioning (self-service or manager), applications and user onboarding, audit reporting (history of access), password management, and provisioning connectors. RPA bots are not as well supported as other products, requiring a customer adapter to be built.
- **Analytics Module** — Provides role management, modeling and mining, role life cycle management, access and roles optimization, and risk-based access classification.

IBM sells an Enterprise Edition that includes all of the modules, plus premium connectors for ERP, CRM and SaaS applications.

IBM also offers a separate multitenant SaaS-delivered IAM solution with light IGA capabilities, called IBM Cloud Identity. Clients can complement IBM IGI with IBM Cloud Identity as part of a hybrid IGA deployment model to gain more cloud provisioning capabilities, or they can utilize IBM Cloud Identity stand-alone, in more simplified use cases for managing cloud-only applications. IBM Cloud Identity is still missing basic IGA capabilities (such as Policy and Role Management, Access Requests, and Access Certifications) and a more robust set of cloud-native provisioning adapters for fulfillment. Cloud Identity provisioning targets available at the time of this writing include: Atlassian Apps, Box, Egnyte, Google G Suite and Apps, Microsoft O365 and Apps, PagerDuty, Salesforce, ServiceNow, Slack, and Zendesk.

IBM also released a beta version of an analytics module that also supports continuous compliance through microcertifications called Cloud Identity Analyze (CIA). CIA was not considered in the scoring of IBM due to the module not being generally available at the time of analysis. IBM IGI is a good choice for global organizations with complex processes that require automation along with

governance that can be extended to applications with complex authorization models (through an integrated business activity model). The solution is delivered as a virtual appliance for multiple hypervisors to simplify on-premises or IaaS deployment.

Identity Life Cycle: Only authoritative source (employee) scenarios are supported adequately. A data integration ecosystem is available, leveraging container-based collection of microservices to integrate various sources of data. Contractor and delegated administration (business partner) scenarios require some assembly of forms, workflows and rules. There is no direct support for self-registration, although APIs are available for handling self-registration through a custom web application. Detecting flaws in feed files requires a custom adapter to be built.

Entitlements Management: The schema for the entitlement catalog is very extensible. The entitlements data model supports deep insight into fine-grained entitlements for complex applications (with built-in support for SAP, Guardium, Secret Server and others) that can be tied to a business activity model. It also supports the concept of a nonhuman RPA identity to be managed. There is also a dashboard for visual representation of tracking application onboarding activities.

Access Requests: Overall, the access request interface is business-friendly, with a shopping cart and a tabular view of access request elements. It lacks support for dependencies among entitlements in the interface, the ability to enforce expiration dates for requests and the ability for recipients to cancel requests made on their behalf. A unique ServiceNow app is available for submitting access requests. Sixteen languages are supported out of the box.

Workflow: There is no suitable default workflow to support the standard, four-stage request approval workflow, so assembly through configuration is required. Fortunately, IGI provides a highly flexible workflow engine with good support for notification of multiple types of policy violations at the point of request submission. Escalation is supported directly in workflow configuration. Electronic signature capabilities are not supported out of the box, requiring custom extensions to meet this need.

Policy and Role Management: Provides excellent support for two-layer role models and specialization of role types, but the use of policies as a way to automatically bind roles to users in different layers is limited. Establishing desirable levels of policy enforcement requires work with custom rules and task scheduling.

Access Certification: IGI now provides complete support for all access certification campaign types (see the Critical Capabilities section), including basic certification of the entitlements catalog. There is a lack of flexibility regarding the actions that can be taken to change attribute values, such as expiration dates for users and entitlements. IGI is able to trigger microcertifications based on risk, but campaigns need to be manually defined in order to configure a dataset to include only accesses that match the risk condition.

Fulfillment: IGI includes an extensive collection of connectors (more than 50); however, the configuration of connectors can be labor-intensive. The inclusion of IBM Security Directory

Integrator (ISDI) enables more extensibility for custom application connectors than is generally available in the market.

Auditing: Provides a flexible framework for SOD policy analysis and enforcement. There is no general-purpose auditing framework for controls beyond SOD, and most scenarios require the creation and scheduling of custom tasks that could trigger custom workflows for auditing and data integrity checks.

Identity Analytics and Reporting: IBM released a beta version of an analytics module called Cloud Identity Analyze (CIA), which was not considered in the scoring of IBM, as it was not generally available at the time of analysis. Prior to the upcoming release of CIA, existing identity analytics capabilities in IGI are average. They include access analytics, role mining and optimization, access risk controls, SOD analysis, and outlier detection. Analytics is marred by the lack of built-in metrics. Role mining is comprehensive, with a cost-driven methodology and tunable parameters, but role affinity analytics is supported only through reports. Peer group analysis is not supported in the current version of IGI.

Ease of Deployment: Virtual appliance form factor greatly simplifies deployment and supports pattern-based deployment of multiple instances; however, since configuration options are limited, customization is often required. Implementing the product can be complex, occasionally requiring compiled Java code in situations where other products rely on scripting. Developments in the last year include the launch of a new identity broker and nodeJS framework to simplify the development, deployment and configuration of connectors.

Scalability and Performance: Makes good use of clustering for the application and data tiers. The most recent release of IGI removes the dependency of previous versions on the external LDAP directory for the support of Identity Brokerage target integration, using a more efficient RDBMS approach. Strictly event-driven design for resource-intensive tasks supports the finely tuned allocation of processing to specific nodes.

Micro Focus

Micro Focus approaches the IGA market with a combination of two distinct modules:

- Micro Focus NetIQ Identity Manager 4.7 (released March 2019) — The module is going through a renaming process into Identity Administration, but existing documentation still refers to the module as Identity Manager.
- Micro Focus NetIQ Identity Governance 3.5 (released December 2018) — Adds certifications, role mining and engineering, and analytics capabilities to Identity Manager.

Micro Focus is continuing its transformation of IGA products to eventually unite all of the company's IGA capabilities into a single product offering. Currently, the Identity Manager and

Identity Governance products are combined to deliver the full set of IGA capabilities through the following modules:

- Identity Governance — Support for access certification, role management and analytics
- Identity Vault — The identity repository
- Role-Based Provisioning Module — Support for access requests and workflow
- Reporting Module — Reporting and analytics
- Identity Manager Drivers — Connectors and logic for provisioning
- Self-Service Password Reset (SSPR)

Micro Focus offers a solution that is suited to organizations looking for strong analytics for cleanup capabilities, scalability for management and governance of large volumes of identity data, including B2C identities via its robust CIAM capabilities.

Identity Life Cycle: Managing the synchronization of identity records with HR systems is easily accomplished through driver configuration. There are also robust customer identity life cycle capabilities; however, support of other scenarios for contractors, delegated administration (business partners) and self-registration requires significant assembly through configuration. There is excellent support for managing identities of robotic process automation (RPA) bots.

Entitlements Management: Identity Governance provides a mixed foundation for managing entitlements. The schema is flexible and there are good tools for discovery and enrichment, including automation elements. An “insights” tab to view by application and visual dashboard for application onboarding and account correlation helps management. However, there is no native support for account dependencies or working with PAM-controlled accounts, resulting in configuration needed to support this functionality.

Access Requests: Identity Manager provides a single-page, easy-to-use interface for creating access requests. Fifteen languages are supported out of the box. Functionality added this year includes default, customizable expiration dates. Multiple users can be selected with subordinate view contextualizing decisions. Selecting one user with “ideal” permissions, for example, can be used to copy to one or more other users.

Workflow: All of the common scenarios can be managed within Identity Manager’s workflow engine by configuring the provided templates. There is an ability to configure workflow to support changes to in-flight requests, as well as support for electronic signatures in approvals.

Policy and Role Management: Identity Governance provides support for more two-layer enterprise role management mechanisms than any other product in the market. All scenarios are supported — most notably, the control over how roles can be removed from users when policies no longer apply.

Access Certification: Identity Governance provides robust access certification features with the ability to support all scenarios (see definition of this capability), although review of the entitlements catalog is limited in the ability for reviewers to update entitlement metadata. There is support for risk-based recommendations during campaigns, and the solution also supports automatically triggering microcertifications based on events.

Fulfillment: The Identity Manager driver framework is flexible, with excellent support for AD domains. Internal mapping tables are available to simplify the calculation of complex attribute values, such as for directory container placement. A new data testing and emulation feature was included for improved application onboarding. Micro Focus Identity Manager can also integrate via RESTful APIs with ITSM tools for indirect fulfillment, with out-of-the-box support for BMC Helix ITSM and ServiceNow.

Auditing: Identity Governance provides SOD policy enforcement for entitlements and audit case management. Policies in Identity Manager can be used to check for a broad range of issues and can be configured to create audit cases in Identity Governance for some issues that are detected.

Identity Analytics and Reporting: Micro Focus has above-average identity analytics capabilities. The solution can automate unused/dormant/stale account detection and reviews, and provides an efficient way to define and measure governance KPIs using a feature called Time Series Metrics Automation. Micro Focus also supports composite scoring. The solution allows the calculation of a risk score based on compounding factors, like the number of accounts in the application, the number of approved SOD exceptions and active compliance violations.

Ease of Deployment: Despite requiring two products to provide IGA capabilities, Micro Focus continues to simplify deployment through its microservices architecture and API support. The Designer tool for Identity Administration makes configuring drivers and policies easier than with other products. The application collection section of the Identity Governance UI facilitates more rapid onboarding of applications. At the time of this research, Micro Focus has yet to introduce a SaaS-delivered IGA offering. Hosted options are provided only by third parties.

Scalability and Performance: Numerous components can be installed on separate servers that can support high levels of scalability; however, the use of a directory server for Identity Manager can handicap performance at scale.

Omada

Omada Identity Suite (Gartner evaluated version 14, released October 2018) can still leverage Microsoft Identity Manager Synchronization Service as part of its provisioning platform. However, it has been extended significantly to emerge as a stand-alone IGA suite, with its own provisioning services. Omada released in September 2017 a multitenant cloud-architected SaaS solution, OISaaS. OISaaS runs on Microsoft Azure and is based on the same code base as the OIS, and significantly reduces the complexity of adoption of the Omada IGA platform.

OIS and OISaaS are licensed in two editions:

- **Omada Identity Suite Governance** — Includes features for identity life cycle, focusing on reporting for governance purposes and includes access certification, deprovisioning and reconciliation.
- **Omada Identity Suite Enterprise** — Full IGA feature set, with the same capabilities of the Identity Suite Governance, adding policy and role management, access requests, provisioning to target systems, data modeling, forms and report designer, and workflow editor.

The OISaaS offers one of the most complete IGA products available in a SaaS-delivered approach. It can offer a very good option to large or midsize enterprises and for governance-focused use cases, especially if there is an existing investment on Microsoft's Microsoft Azure infrastructure or Microsoft Identity Manager legacy deployments looking for modernization. OISaaS also offers a unique subscription option to its SaaS customers to allow complete data isolation for its clients.

Identity Life Cycle: There is excellent support for the user-facing elements of all identity life cycle scenarios, as well as built-in organization context for delegated administration. RPA bots are well supported, with supervision relationships handled well. An SDK is offered for importing identity data, and an identity model that allows for the definition of multiple identity sources. Assembly by configuration is still required for workflows to handle contractor expiration and delegated administration scenarios.

Entitlements Management: The application onboarding feature manages all key aspects of importing accounts and enriching accounts from target systems. There is support for modeling entitlements from applications with complex authorization models. There isn't a graphical dashboard for account correlation and application onboarded, but colors and tabulation do help. Strong SAP integration is available for many predefined roles.

Access Request: Omada provides a free-form, single-page shopping cart approach that supports all access request scenarios, including request templates. Seven languages are supported out of the box.

Workflow: The workflow engine is flexible, yet relatively easy to configure, with default support for policy analysis and control-owner stages at the beginning and end of the approval workflow. Electronic signatures are supported in the form of a password prompt.

Policy and Role Management: Support for the two-layer enterprise model is implemented. The policy model overall is reasonably flexible in handling assignment policies for roles and expiration dates for access requests, with some flexibility for handling the removal of accounts and entitlements. There is support for multiple types of roles, but processes for role management are not applied consistently.

Access Certification: There is a survey module that offers full support for all common access certification scenarios, including the relatively unique ability to edit attribute values in certification tasks. This can be useful for reviews of the entitlements catalog and users or entitlement

assignments with expiration dates. Campaigns can include risk scoring for either automating approvals or to define microcertifications based on high-risk entitlements only (campaigns still need to be manually scheduled). Lastly, access certifications also support electronic signatures in the form of a password prompt.

Fulfillment: Built with an extensible connector framework that supports a combination of native connectors, connectors based on standard protocols (REST, OData, SCIM v2, SOAP, LDAP), as well as the tight integration to the Microsoft Identity Manager (MIM) synchronization engine. A unique classification policy concept can manage the logic required to derive complex attribute values, such as directory containers. Developments in the last year include options for indirect fulfillment, which can delegate a request to be fulfilled by an ITSM tool (including a connector for ServiceNow) or for being evaluated by an external system like SAP GRC. Omada also has a partnership with Aquera, an SCIM connectivity gateway provider for IAM platforms. OIS and OISaaS can leverage its SCIM connector to integrate with Aquera's platform, which offers an indirect fulfillment approach via its robotic automation adapter.

Auditing: Multiple types of audit policies are defined via central console, although many policies may require the generation of custom views. A business activity model can support SOD risk analysis for applications with complex authorization models (SAP support is built-in). A robust audit case management framework that can orchestrate remediation activities is provided.

Identity Analytics and Reporting: Omada has above-average identity analytics capabilities. Omada offers an application onboarding feature that automates the process of cleaning up user data. OIS automatically computes risk scores based on multiple factors (for example, if an account has excessive entitlements). The risk scores as well as information of when entitlements were last used are presented in workflows.

Ease of Deployment: The software-delivered product can be complex, with separate enterprise, database and provisioning server components and requirements for multiple databases. The complexity is significantly reduced with OISaaS product, and allows alternative methods for integrating the SaaS-delivered solution with on-premises target systems (via Microsoft Azure ExpressRoute) besides the traditional IPsec VPN tunnels normally used by SaaS-delivered IGA solutions. Omada has also created a strong best practices process framework called IdentityPROCESS+ that can help organizations streamline the deployment of the IGA solution.

Scalability and Performance: The product relies on the scalability and resilience features of the Microsoft SQL Server platform, while providing additional support for archiving data. Sizing guidelines indicate that enterprise deployments may require more hardware than other products in similar-sized environments.

One Identity

One Identity offers One Identity Manager as its IGA solution (Gartner evaluated version 8.1, released March 2019). One Identity Manager is available as a traditional, software-delivered

solution, as well as a managed service. One Identity Manager is built on the Microsoft .NET platform. It's a good choice for medium to large enterprises that need a balanced governance and automation solution, especially those organizations that have significant expertise with Microsoft .NET technologies.

One Identity also offers a separate multitenant, SaaS-delivered and cloud-architected IAM solution with light IGA capabilities called One Identity Starling (OIS). OIS is used to provide complementary functionality to One Identity Manager in a hybrid cloud/on-premises solution. One Identity Starling Connect extends governance and provisioning from on-premises to include connected cloud apps for unified management of cloud applications. Also, One Identity Starling includes modules for identity analytics and risk intelligence, and it can complement Identity Manager or other IGA solutions to provide risk-based analysis on identity, access and usage information.

Identity Life Cycle: Support for employee and self-registration (customer) as well as RPA bot scenarios is provided, with contractor scenarios requiring minor setup. Delegated administration is provided with a built-in organization model to assist a sponsorship-and-expiration pattern.

Entitlements Management: Provides a highly capable synchronization editor interface for modeling and testing the import of accounts and entitlements from applications. Working with entitlements typically requires the curation of service items. There is a wizard and GUI that is used for account correlation.

Access Requests: The shopping cart interface for access requests is well designed. A complete set of controls enables users to inspect their own access, compare users, review request history and cancel requests. The administrative interface supports German and English languages, with the web interface localized for 15 languages to support end users.

Workflow: The four-stage policy and approval process is supported by an included template. Overall support for policy checks is good. Even though electronic signatures are not supported, it's now possible to integrate One Identity Starling Two Factor Authentication for approvals that require electronic signatures.

Policy and Role Management: Provides a rich role framework, with support for numerous types of roles, but simulation mode cannot preview entitlements that may be removed from users as a result of changes to role definitions. Dynamic rules have sufficient flexibility to control the behavior of how users are assigned to, and removed from, roles.

Access Certification: The full range of certification campaign types is supported, including the ability to certify the entitlements catalog. The configuration of certification of privileged accounts is more complex than for other products. Even though electronic signatures are not supported, it's now possible to integrate One Identity Starling Two Factor Authentication for submitting certification tasks that require electronic signatures. One Identity Manager can leverage peer group analysis to establish risk scores during campaigns, which can be used to automate some low-risk approvals (workflows for the campaign still need to be manually configured). Microcertifications

can leverage the peer group analysis-based risk scoring and need to be started either at predetermined times or manually triggered as ad hoc campaigns.

Fulfillment: There is solid support for automated fulfillment through a good collection of connectors provided with the base product. Starling Connect for Cloud supports fulfillment for over 30 SaaS target systems. There is little support for proxy-based fulfillment across security zones. Indirect fulfillment is supported, either via ITSM integration (there is a ServiceNow connector) or via its own internal workflows, which need to be configured for manual provisioning in order to notify designated fulfillment teams.

Auditing: The HelpDesk subsystem can be used to handle audit cases generated from a variety of policy types, but only SOD controls are supported systematically. A company policy module is available to perform arbitrary checks of the integrity of identity data and accounts. One Identity Manager also provides a feature called TimeTrace, which tracks changes to an object that were made up to any point in the past.

Identity Analytics and Reporting: There is a good selection of built-in reports and dashboards, with extensive analytics of data quality and basic support for role mining. There are some built-in performance metrics delivered as dashboards, but nothing for monitoring the effectiveness of governance. For risk scoring, administrators need first to assign a risk value to entitlements. The solution offers out-of-the-box capabilities for identifying duplicate, unused and orphan accounts, and excessive entitlement assignment.

Ease of Deployment: The product provides a unified platform for IGA, with good support for internal change tracking. Docker containers are supported as a delivery method for some of the product's core modules (Job Server, Application Server and Web Server). However, multiple interfaces are involved in various aspects of configuration, including a nonweb Windows-only graphical UI (GUI).

Scalability and Performance: Full and thoughtful support for scalability and performance considerations through the product's "Job Server" architecture enables flexible workload distribution, although sizing guidelines suggest the product may be CPU-intensive and processing happens majorly at the application layer instead of the database layer.

Oracle

Oracle offers its Oracle Identity Governance (OIG) suite as software. The OIG suite 12cPS3 (evaluated release from August 2017) includes three main modules: Oracle Identity Manager, Oracle Identity Analytics and Oracle Privileged Account Manager.

In addition, Oracle also offers a separate multitenant, SaaS-delivered IAM solution with light IGA capabilities called Oracle Identity Cloud Service (IDCS) 18.4.2 (latest release was December 2018). Organizations with very basic IGA needs can use IDCS in lieu of OIG, but it still misses very basic IGA capabilities like Policy and Role Management (only basic roles are available), Workflows and Access Certifications. The SaaS solution is mostly focused on provisioning and reconciliation, and

includes access request with peer-group analysis, with activity and analytics reports. IDCS can also be used in conjunction with OIG as part of a hybrid IGA deployment model to gain more cloud-provisioning capabilities.

OIG is especially well suited to global enterprises with mature and complex processes for access administration and balanced requirements for governance-focused use cases and automation of account management use cases.

Identity Life Cycle: Good support for most of the common identity life cycle scenarios (employees, contractors, self-registration and RPA bots), with an organization model to support delegated administration. However, configuring partner organizations for delegated administration is an administrative task and is not workflow-driven.

Entitlements Management: Excellent support for the management of metadata for entitlements, with deep insight into entitlements for applications with complex authorization models. Provides the ability to maintain a taxonomy of account types that can be used to categorize accounts. Account correlation during application onboarding is aided by a customizable graphical dashboard.

Access Requests: The shopping cart paradigm is well implemented, with a relatively free-form user experience and lots of contextual information provided by the access advisor functionality. User control over requests, such as request history and canceling requests, is excellent. Support for 26 languages is built into the product for administrative and end-user interfaces.

Workflow: Excellent workflow support based on Oracle's SOA BPEL Integration allows all evaluated scenarios to be fulfilled, with good integration of policy analysis via the Identity Audit module. There is built-in support for electronic signatures as part of approvals.

Policy and Role Management: The role design environment is well structured and workflow-driven, and it enables preview of role and policy changes. It includes the concept of categories for roles and several role types that allow for great flexibility in defining two-level role models. Policy coverage is excellent, and there is built-in support for time-limited workflow approvals as well.

Access Certification: Almost all certification campaign types are supported out of the box, including certification of the entitlements catalog (some customization is required for organization chart certifications). Electronic signatures are supported for certification task submission, and both passwords and digital certificates are supported. There is also a new capability for creating campaigns based on filters that can be applied to the identity and entitlements metadata. Risk-based certifications are more complex to configure and would require custom tasks to be built. That would be the case for either creating more automated certification steps for low-risk entitlements or for enabling the concept of microcertifications.

Fulfillment: Provides a robust platform for fulfillment, but implementing connectivity is complex, with a variety of adapters (requiring compiled Java code) and scripted options needed to control

behavior. It offers a set of over 10 direct provisioning connectors as part of the base license, with more than 30 additional options for purchase, for both cloud and on-premises fulfillment, with good capability to connect to ERP systems and model complex multilevel entitlements. Development in the last year includes a revised connector framework that is expected to facilitate application onboarding. IDCS can also be leveraged for extending fulfillment to SaaS applications.

Auditing: The Identity Audit module provides a central console for managing a relatively broad range of audit policies, and there is a good framework for managing audit cases generated from policy exceptions.

Identity Analytics and Reporting: Oracle provides below-average identity analytics capabilities. Oracle leverages OIA for performing all role mining activities, and also requires Oracle BI and OIM for completing other role management activities and generating reports. Oracle Business Intelligence is included with the product to provide a powerful (but generic) engine for reporting and analytics. A good set of foundational reports is provided, along with some metrics. However, many scenarios require the creation of custom reports.

Ease of Deployment: There is good support for pattern- and script-based deployment in complex environments, as well as the Deployment Manager for migrating configuration changes among environments (such as test to production). However, it may require multiple modules to be implemented (OIM, OIA), and the product requires more compiled Java code than other products, although there is some support for Apache Groovy scripting. The IDCS SaaS-delivered approach can be used to simplify some of the deployment tasks of the IGA platform, but it is very limited in comparison with the software-delivered OIG product.

Scalability and Performance: Built with thorough consideration for scalability and performance by driving significant data processing to the data tier. It supports horizontal and vertical scaling of nodes for different types (front and back end) of processing.

SailPoint (IdentityIQ)

IdentityIQ is SailPoint's Software-delivered, governance-oriented IGA solution, which is delivered as the IdentityIQ Governance Platform (version 7.3 released in August 2018 was evaluated) with several modules:

- SailPoint IdentityIQ Compliance Manager
- SailPoint IdentityIQ Lifecycle Manager
- SailPoint IdentityIQ File Access Manager (formerly known as SecurityIQ)
- SailPoint IdentityIQ Password Manager
- SailPoint IdentityIQ AI (formerly known as IdentityAI)

- SailPoint IdentityIQ Advanced Integrations (PAM, Service Catalog, Service Desk, IaaS, SIEM, EMM)

Provisioning functionality is included as part of Lifecycle Manager, and connectors are included as part of the IdentityIQ Governance Platform. SailPoint IdentityIQ is used most often by large organizations with complex environments with significant regulatory obligations requiring a governance-oriented approach to IGA. In 2019, SailPoint released a cloud-hosted, vendor-managed service based on IdentityIQ. In addition, partners of SailPoint also offer cloud-hosted IdentityIQ as a service.

Identity Life Cycle: Base identity life cycle processes for employees and contractors are supported well, including the ability to manage contractors. RPA bots are well supported, with their own identity type. Live feed integration with leading HR tools is present. Self-registration is provided out of the box. A facility is provided to recommend owners for orphaned accounts.

Entitlements Management: Flexible schema for the entitlements catalog and excellent handling of applications with complex schemas, including support for dependencies. There is built-in support for account mappings based on a custom taxonomy and a graphical dashboard for tracking application inventory and onboarding activities.

Access Requests: An overall business-friendly approach to access requests, with a hybrid single-page tabbed interface and a shopping cart paradigm, and risk-based recommendations are provided for request approvals. Good controls enable users to view and cancel requests by and for them. Sixteen languages are supported out of the box.

Workflow: The default workflow for access requests supports the common four-stage approval process with minimal configuration. The most common features (such as delegation, escalation and notification) are configurable. Password-based electronic signatures for workflow approvals are provided as a configuration option.

Policy and Role Management: Provides an excellent design environment for working with multiple types of roles, which is very helpful when defining two-level role models. Role detachment when policies no longer apply is performed through an analysis workflow and then the scheduling of a role propagation task. It has one of the best analytics capabilities for role modeling among all vendors.

Access Certification: Excellent support for all access certification campaign scenarios. Electronic signatures for certification tasks are provided as a configuration option. Risk information can be calculated based on peer group analysis and provided back to approvers. Roadmap items include risk-based autonomous approvals. Ongoing peer group analysis can be used to detect outliers and trigger microcertifications, but campaigns need to be manually defined based on the level of risk threshold violation, for example.

Fulfillment: Comprehensive support for automated fulfillment, with more than 100 connectors. All of the most common connectors are provided as part of the base product. The AD connector can manage multiple domains in a forest as a single application. IdentityIQ also supports robust methods for indirect fulfillment via its own internal case management system, external API integrations or out-of-the-box integration with ServiceNow, HP Service Manager and BMC Helix ITSM.

Auditing: A single console allows the definition of a broad range of policies for auditing various conditions. The identity aggregation process can be configured to evaluate policies every time it is run to generate violations in a manner consistent with a case management pattern.

Identity Analytics and Reporting: Out-of-the-box reporting and analytics are strong, with useful metrics included. The object model requires data export if external BI or reporting tools are to be used, although web services interfaces are available for directly querying system objects. A new governance recommendation engine leveraging ML and peer group analysis is available via the IdentityIQ AI module. It can automatically calculate risk scores for both users and applications. For users, it can be based on roles held by the user, additional (non-role-encapsulated) entitlements, policy violations, and time since last certification. The recommendation engine is available as of March 2019 via APIs, and UI integration is planned for 2Q19.

Ease of Deployment: IdentityIQ benefits from being built as a unified product, but there is an underlying complexity related to database and application server dependencies. Deployment requires BeanShell (Java syntax and object model) scripting, some compiled Java code and direct manipulation of some XML objects. With a new vendor-hosted offering of IdentityIQ, SailPoint simplifies the process of deployment of its software-delivered product, which was already available as a hosted service by third parties.

Scalability and Performance: Despite some architectural drawbacks due to the inefficiency of the data model and the inability to push processing to the data tier, SailPoint has the ability to demonstrate sufficient performance and scalability for enterprise needs.

SailPoint (IdentityNow)

IdentityNow is SailPoint's multitenant, cloud-architected and SaaS-delivered solution with full IGA capabilities. SailPoint doesn't use a discrete version numbering for IdentityNow. Gartner evaluated the release as of April 2019. IdentityNow's IGA functionality is delivered through the following modules:

- IdentityNow for Password Management
- IdentityNow for Access Certification
- IdentityNow for Provisioning
- IdentityNow for Access Request

- IdentityNow for Separation of Duties
- IdentityNow for AI

IdentityNow is targeted at organizations with simple needs for access requests and provisioning and few governance requirements that are concerned primarily with minimizing operational expenses required to support their IAM programs. Back in 2013, IdentityNow was the first (and only) IGA product in the market to be released as a multitenant, cloud-architected and SaaS-delivered solution. It now faces bigger competition from other vendors that offer some limited SaaS-delivered IGA capabilities.

Identity Life Cycle: IdentityNow can handle the employee and RPA bots identity life cycle process adequately. Multiple authoritative sources are supported. Typical process patterns for contractors and business partners are not supported. Self-registration is supported only through API calls.

Entitlements Management: Overall, this area is weak. While the schema is extensible and there is excellent handling of applications with complex schemas, there is minimal support for dependencies among accounts. Entitlement discovery, enrichment and correlation is weak, requiring scheduled jobs and lacking analytics and graphical overviews to aid in correlation. Deeper integration with ERP systems for fine-grained access control in these systems is lacking.

Access Requests: Access requests are available for self and for others, with a drop-down menu to select subordinates. Changing requests is not supported and instead requires cancelation and resubmission. “My team” view allows manager to compare multiple staff. Seventeen languages are supported out of the box.

Workflow: The workflow capabilities are limited. Although escalations are now handled, delegation is on a one-by-one case. Additionally, there is no ability to assemble workflows to support the most common workflow features, such as multiple approval steps, although ITSM integration is available, as are email and mobile approvals. Electronic signatures are not supported.

Policy and Role Management: Support to two-level role models is very basic, only simple roles can be defined to contain access profiles. Included this year was a number of policy management items, such as segregation of duty policies, but role mining capabilities are not present out of the box, instead requiring the purchase of SailPoint’s AI solution for this.

Access Certification: Only basic user-level (organization chart) access certification is supported, with limited ability to filter entitlements included in such certification campaigns. New for this year is risk-based recommendations to approvers, based on peer group analysis. The concept of risk-based continuous microcertifications is not supported. However, smaller scoped certifications can be manually created through the Dynamic Discover Engine (DDE) functionality to certify via search attributes.

Fulfillment: IdentityNow uses the same connector framework as IdentityIQ, so all of the most common connectors are provided as part of the base product. There is a manual work item processing capability for handling indirect (manual) fulfillment, but there is no out-of-the-box integrations with ITSM tools (a generic API-based connector is provided and requires customization).

Auditing: IdentityNow's new Dynamic Discovery Engine IGA search facility improves the way the product handles SOD and audit control points. It now allows the creation of more flexible and granular controls than it was possible in previous versions. It also includes a very basic task management feature, but it is not a full case management system.

Identity Analytics and Reporting: This year, a new dynamic discovery engine was released for IdentityNow that includes more capabilities for entitlements management, leveraging peer group analysis and anomaly detection. Also, predictive recommendations can be obtained via API integrations with the IdentityNow for AI module, in a similar fashion that was implemented with IdentityIQ and its AI module.

Ease of Deployment: IdentityNow was built from the ground up as a multitenant SaaS-delivered application, with deployment, environment migration, operation, updates and patching handled by SailPoint operations.

Scalability and Performance: IdentityNow is built on a microservices architecture. It relies on Amazon Web Services (AWS) elastic scaling to support large volumes of objects and transactions; however, it lacks the flexibility (and customizability) that is desirable for enterprise deployments.

SAP

SAP approaches IGA requirements with a hybrid cloud/on-premises solution set involving three separate products and services:

- **SAP Access Control** — SAP's core IGA product is software-delivered and also available as a virtual appliance or IaaS-hosted solution. Release v12.04 from January 2019 was evaluated as part of this research.
- **SAP Identity Management** — This is a software-delivered product that fulfills basic needs for identity management. It is offered at no charge to SAP clients to manage users within the SAP ERP environment, and can, for a charge, also provision to non-SAP environments. It is required to perform core functionality in the critical capabilities, like HR integrations in identity life cycle, provisioning and identity synchronization.
- **SAP Cloud Identity Access Governance (IAG)** — This is a multitenant, cloud-architected and SaaS-delivered solution with light IGA capabilities focused on managing users in SaaS target applications, but also supports on-premises targets. Quarterly releases are made available on a continuous basis.

SAP BI is included with SAP Access Control for reporting and analytics. Other, more advanced analytics scenarios, including use cases in this Critical Capabilities research, will require SAP Lumira and SAP Cloud IAG.

SAP Access Control is used most often for governance over SAP (and third-party) business applications, instead of more general-purpose IT user administration and provisioning use cases. SAP Identity Management provides virtual directory capabilities for account management and attribute synchronization in a heterogeneous environment. The SAP Cloud IAG is used by customers to assist with managing SAP applications hosted in the cloud. SAP released this year a new feature called SAP IAG bridge, which offers an option to existing SAP Access Control and Identity Management clients to integrate with the Cloud IAG product and onboard cloud-based applications. SAP Identity Management and SAP Access Control are typically deployed by customers with significant investments in SAP software that require deep insight into SAP's business applications.

Identity Life Cycle: SAP Identity Management provides built-in integration with SAP's HR applications, Human Capital Management (HCM) and SuccessFactors, supporting functionality such as appropriate roles being automatically generated based on assignment policies and SoD rules. Overall, life cycle capabilities are weaker than average, with less capability to support contractor and RPA bot scenarios and more configuration or customization required. Detecting flaws in feed files requires scripting against the connectors.

Entitlements Management: SAP Access Control provides a flexible entitlements data model with support for deep insight into applications, with complex authorization models. Support for multiple account types and account correlation is limited.

Access Requests: The interface for requesting access is visually appealing and functional, but it is more sequential than is typical in the market. It is one of the few products that allows an approver to modify an incorrect request. Support for 25 languages is built in for the administrative and end-user interfaces and a newly added risk score is made visible.

Workflow: Overall workflow support is complete and highly flexible, but configuration requires significant assembly when compared to other vendors. Electronic signatures for workflow approvals are supported in the standard solution.

Policy and Role Management: SAP Access Control bridges the gap between IGA and SOD control monitoring by adding enterprise role management and policy-driven assignment of access. It supports the concept of two-level role models, and role governance is well supported. However, some assembly and occasional customization may be required to support a number of common scenarios (for example, those distinguishing between role types or involving contractor management).

Access Certification: SAP Access Control provides a full-featured platform for access certification, but configuration of certification campaigns can be more complex than for other products.

Customization is required to enable electronic signatures for certification tasks. There is support for risk-based recommendations during campaigns; however, there is no support for microcertifications.

Fulfillment: SAP Identity Management provides minimal fulfillment support for infrastructure systems, although SAP Access Control offers excellent support for complex business applications, especially SAP solutions. Manual and service desk fulfillment requires workflow assembly and custom adapters to be created. RPA support for indirect fulfillment is good, and SAP has its own RPA solution.

Auditing: SAP Access Control provides complete support for process-driven SOD and critical access policies with a case management interface available for remediation. SOD controls monitoring allows clients to gain deeper insight into complex business applications than with most other products in the IGA market. The case management concept is not extended to other types of policy violations, and non-SOD policies can be complex to define.

Identity Analytics and Reporting: SAP BusinessObjects BI platform and Lumira are provided for reporting and analytics across SAP Identity Management and SAP Access Control. Role mining is supported in SAP Access Control. There is a very good selection of built-in reports, especially covering risk analytics, but more advanced analytics scenarios may require SAP Lumira and SAP Cloud IAG.

Ease of Deployment: The reliance on multiple products to support IGA, each with its own deployment considerations, and the need for extensive customization to support common scenarios make SAP one of the most difficult IGA toolsets to deploy and configure.

Scalability and Performance: The products are built for scalability and are intended for deployment in global enterprises; however, some considerations for performance at scale are missing, such as built-in archiving of historical data.

Saviynt

Saviynt Security Manager (SSM) is a full-featured IGA service that extends the scope of IGA to include functionality usually associated with PAM, DAG and SOD controls monitoring products. This is offered as a SaaS-delivered, cloud-architected and single-tenant service. SSM's latest release is version 5.4 (Gartner has evaluated version 5.3.1, released March 2019, which was the version available at the time of this analysis). The service is offered as a core module, simply called Saviynt Security Manager, which includes a set of basic, flexible connectors. Additional premium modules provide connectivity and additional functionality for specific types of applications, such as mainframe, ERP, electronic health record (EHR) and cloud storage. Alternatively, Saviynt offers the same solution as a virtual appliance that can be hosted in clients' data centers, using the same code base and capabilities of the SaaS-delivered service.

SSM can be the best option for government and public-sector clients in North America looking for SaaS-delivered capabilities, due to its unique FedRAMP certification, and is also suited to large to

midsize enterprises with strong governance-focused requirements.

Identity Life Cycle: All four identity life cycle patterns are well supported, including RPA bots, with built-in functionality. Detecting flaws in feed files requires the creation of analytics that are executed prior to feed processing.

Entitlements Management: Provides a deep and flexible entitlements data model that supports as many as five levels of hierarchy for entitlements. This is necessary for Saviynt's SOD controls monitoring and DAG functionalities. It also provides a full-featured UI for maintaining application inventory that supports assigning and tracking activities related to application onboarding. A graphical dashboard provides various risks and comparators to aid decision making.

Access Requests: The access request interface is based on a limited shopping cart paradigm. Requesters can only add applications to the cart and then select entitlements within the cart, which can be awkward when creating requests involving multiple systems. It is not easy for subjects of requests to view status, and they cannot cancel requests submitted on their behalf. Sixteen languages are supported out of the box.

Workflow: Superior features more common in SOD controls monitoring than IGA, such as preventive SOD checks. Digital signatures are not supported.

Policy and Role Management: Outstanding support for role management bridges the gap between business and application role management, with excellent support of two-level role models. It can design and transport roles for complex applications with their own role-based access control (RBAC) models. Policies for role assignment (and detachment) are handled separately via provisioning rules.

Access Certification: Offers the most full-featured support for access certification, covering all scenarios, with exemplary support for targeted campaigns that include only exceptional access, changes within a certain period of time or specific types of accounts. Risk-based recommendations are available throughout the product, including certifications, and autonomous approvals are also configurable. Microcertifications can be automatically triggered based on events.

Fulfillment: SSM offers over 30 direct provisioning connectors, with LDAP, AD, UNIX, RACF, Database, SCIM and scripted REST with full functionality, and over 23 additional connectors with basic functionality as part of the base license. The product combines support for user-developed and OpenICF connectors, with extensibility through custom REST web services and Apache Camel middleware integration framework. Optional connectors can be purchased separately, and they are premium editions of the basic connectors that come with the base license. These premium connectors are necessary for performing more advanced governance of accesses in these platforms, like SOD monitoring for example. There is a very robust capability for indirect fulfillment via the access request interface or via ITSM integration.

Auditing: Provides exemplary support for SOD risk analysis with a business-activity-driven framework that maps policies to fine-grained entitlements, as well as content available for multiple complex applications via the optional premium connector modules. Provides a case management interface that can be used to assign follow-up for the full range of audit events.

Identity Analytics and Reporting: Saviynt has above-average identity analytics capabilities. It supports risk scoring at both user and application levels and is computed using a statistical model with static and dynamic inputs. Clients get the flexibility to configure this model and modify on an ongoing basis. Even though there are not a lot of out-of-the-box reports focusing on data cleanup, it has additional good capabilities for outlier detection. Role mining and related affinity analytics provided by the Role Workbench are excellent, even supporting role management for applications with complex authorization models (with suitable premium modules for applications). For this year, there is a new report builder using neural networks for extracting identity intelligence from the user data warehouse. Lastly, there is a compliance feature called ControlExchange with approximately 1,200 controls mapped to various regulations and compliance frameworks that can significantly expedite compliance reporting.

Ease of Deployment: The solution is based on a cloud-architected, IaaS-hosted and vendor-managed service in the cloud, with advanced shared DevOps capabilities for the orchestration of patches and updates. Alternatively, there are appliance-based deployment options, including AMIs and CloudFormation templates available for deployment in AWS. There is also the possibility for traditional software-delivered deployment that sacrifices much of the deployment ease.

Scalability and Performance: Thorough approach to supporting scalability and performance, which involves clustering, big data strategies, the ability to dedicate nodes to specific tasks and continuous archiving of historical data. Also, the SaaS-delivered offering can automatically increase and decrease processing resources based on demand.

Context

IGA software can be complex and expensive, often representing the largest investment for IAM programs, while also presenting the highest risk for deployment. The IGA market has evolved from the combination of different point product markets, including identity provisioning and administration, identity governance, and identity analytics. There are numerous capabilities organizations will require to achieve their objectives for exercising and demonstrating control over user access in heterogeneous environments.

Gartner recommends that organizations prioritize analytics when deploying IGA in order to mitigate critical identity risks earlier in the implementation process (see [“IGA Best Practices: Prioritize Analytics When Adopting IGA”](#)). This prioritization exercise should include the evaluation of IGA tools that can support out-of-the-box identity analytics capabilities.

It is important to separate identity analytics cleanup use cases from continuous governance use cases in order to simplify the decision-making process as to when to use identity analytics.

Cleanup use cases will be the most useful capabilities in the beginning of a new IGA implementation or expansion. It includes using peer group analysis for identifying outlier accounts, dormant, unused accounts, or accounts with excessive privileges (and remediating those findings). Continuous governance use cases will be helpful to sustain and enhance already existing IGA processes. A typical usage of identity analytics for continuous governance includes role mining exercises (see [“IGA Best Practices: Take Control of Enterprise Role Management”](#)) but also can be used for calculating risk to help the decision-making process of approvers when reviewing access requests or certification campaigns. In 2020, the IGA market will start to see more predictive identity governance use cases. However, IGA tools available today are only providing risk-based recommendations (if at all) and are not yet ready to deliver full capacity of performing autonomous actions or making anticipatory predictions.

Besides prioritizing analytics, Gartner also recommends that organizations should be careful when choosing a fulfillment strategy for automated provisioning. Successful IGA deployments will leverage a combination of direct and indirect fulfillment strategies. That means a cost-benefit analysis must be applied, and preference should be given to out-of-the-box provisioning adapters to automate fulfillment to targets with only the highest volume of requests. For the remaining targets, the cost-benefit analysis should take into consideration if there are indirect methods for fulfillment that can be leveraged. For example, this can include

- Using the IGA automated access request and workflow capabilities to open a ticket on an ITSM tool for processing a manual fulfillment.
- Leveraging SaaS-delivered access management tools as a gateway for the IGA platform to provision to cloud applications.
- Leveraging RPA tools for fulfilling the last steps of creating, updating and deleting accounts in target systems.

Lastly, some IGA tools will even simulate help desk capabilities internally, for opening and keeping track of manual tickets for provisioning users into disconnected applications.

Automated provisioning is historically the most difficult, expensive and unpredictable part of IGA deployment projects. Most organizations automate fulfillment for only 15% to 25% of the applications covered by their IGA deployments (see [“IGA Best Practices: Governance First, Automated Provisioning Later”](#)). Organizations that are mostly concerned with process automation should choose IGA solutions with flexible indirect fulfillment capabilities, which is as important as selecting a solution with a vast out-of-the-box provisioning adapter library. Alternatively, third-party connectors are also available for IGA solutions that support the SCIM standard, which the vast majority of solutions do.

The IGA market is mature, and products typically address most of the needs of their customers for customary IGA scenarios. Where products differ is in their approaches to the problems IGA is

intended to address. Some products provide what their vendors consider to be best-practice frameworks for access administration to enable customers to adopt their processes without customization. Other products are designed to be as flexible as possible and to accommodate significant customization.

This research used a tabletop proof of concept (POC) approach to perform product evaluations. This year, vendors were presented with 110 scenarios drawn from common client needs and process guidance presented in Gartner research. They were asked to explain how their products would be configured, or would need to be customized, to address the scenarios and to characterize the user experience when relevant. Vendors were allowed to augment their narratives with representative screenshots to illustrate some aspects of their capabilities.

Product/Service Class Definition

IGA tools manage digital identities and access rights across multiple systems. To accomplish this, IGA tools aggregate and correlate disparate identity and access rights data, which is distributed throughout the IT landscape. This aggregated data serves as the basis for other IGA functions, including identity life cycle management, policy and role management, access requests, access certification, reporting, and fulfillment via automated provisioning and service tickets. IGA tools are delivered as software or as a service and possess the following attributes:

- **Identity Life Cycle** — Maintains digital identities (both human and nonhuman), their relationships with the organization and their attributes during the entire process, from creation to eventual archival.
- **Entitlements Management** — Maintains a link between identities and access rights to be able to tell who has access to what and who is responsible for maintaining an account or access right. This includes curating and maintaining the entitlements catalog, to describe the types of accounts, roles, group memberships and other entitlements.
- **Access Requests** — Enable end users to request access rights across numerous infrastructure systems and business applications through a business-friendly UI.
- **Workflow** — Orchestrates tasks to enable functions, such as access approvals, notifications, escalations and integrations, and other business processes. Most often, this enables managers or resource owners to approve or deny access requests, ideally through context-driven information.
- **Policy and Role Management** — Maintain policies that govern automation of the assignment (and removal) of access rights for users, availability of access rights for requests by different types of end users, approval processes, and dependencies and incompatibilities among access rights. Roles are common vehicles for improving the consistency and efficiency of these policies.

- **Access Certification** — Requires managers and resource stewards to certify, on a periodic basis, the access rights users have been assigned to ensure that access complies with policies.
- **Fulfillment** — Propagates changes initiated by the IGA tool to account for repositories. Direct fulfillment, sometimes referred to as “automated provisioning,” connects to account repositories, whereas indirect fulfillment uses a workflow or external system as proxies for completing changes. Indirect fulfillment (or manual provisioning) will include capabilities to easily integrate with external ITSM tools for opening tickets for manual fulfillment and also for leveraging AM or RPA tools.
- **Auditing** — Evaluates business rules and controls against the current state of identities and access rights, alerting control owners of exceptions (such as invalid identity states or the creation of rogue accounts in managed systems) and supporting timely and orderly remediation.
- **Identity Analytics and Reporting** — Provide a mechanism to evaluate risk based on identity information insights. Role mining is a typical analytics scenario for designing and optimizing role definitions that all IGA tools must support. However, analytics capabilities in IGA tools have evolved to also apply techniques to clean up excessive, outlier or incorrect entitlements and enhance the continuous process of identity governance. This includes risk reporting, smarter microcertification campaigns, contextualized access requests and approvals, and enhanced policy violation detection, among other use cases.

Critical Capabilities Definition

Identity Life Cycle

Identity life cycle processes maintain the identity repository and provide a means to create and maintain identities, as well as manage identity-related attributes. The identity repository is usually provided as an exclusive resource of an IGA tool.

IGA products often rely on authoritative sources for identity information, such as HR systems for employee information or databases for contractors and temporary workers. The processes supporting employee relationships are usually augmented with additional processes for managing nonemployees (such as contractors), business partners (such as vendors), customers and increasingly other software accounts like RPA bots. For cases in which users are unconnected with formal organizational processes, such as an employment life cycle, the closure of the life cycle must be internalized, usually via an expiration process.

IGA products must be able to handle the multiple identity life cycles that are typical in organizations, as well as support orderly transitions among people who may have multiple relationships with the organization at various times or even concurrently. IGA tools may need to work with multiple authoritative sources and master identity information for people not covered by authoritative sources. This requires these tools to provide facilities to support the following four

identity life cycle patterns (see [“IGA Best Practices: Establish an Identity Perimeter With Identity Life Cycle Processes”](#)):

- **Authoritative source** — Relies on a source of people information (such as an HR application) to control the beginning and end of a person’s relationship (such as the employment relationship) with the organization and master some identity attributes.
- **Sponsorship and expiration** — Allows authorized people (such as managers) to sponsor relationships with individuals (such as contractors). Sponsors are responsible for determining when relationships begin and end; however, expiration dates ensure that the relationship can be terminated in the future if the sponsor fails to signal the actual end of the relationship.
- **Delegated administration** — Establishes relationships at the organizational level for business partners, such as vendors and institutional customers, then delegates responsibility for associating people with those organizations to specific individuals. These organizational relationships can constrain the access available to users. As with the sponsorship-and-expiration pattern, expiration dates are often associated with these users to ensure that the relationship can be terminated if an organizational administrator does not follow through on signaling the actual end of the relationship. This is a common pattern for B2B scenarios.
- **Self-registration** — Enables anonymous users to register and be associated with an existing relationship (via a CRM system, for example) or to create a new identity. This is a common pattern for B2C and B2B scenarios.

Entitlements Management

Entitlements management is concerned with maintaining the entitlements repository and providing a means to capture, organize and assign ownership of the accounts and entitlements that determine the access users have from various account repositories throughout the environment.

An entitlement is an abstract data structure that can represent the many forms of permissions that users have in a broad range of infrastructure systems and business applications. IGA products can capture entitlements from a variety of target systems, using the connectors provided for fulfillment; however, doing so is not essential. Often, simpler methods, such as importing entitlements from flat-file extracts, are sufficient (especially in the early stages of IGA deployment). The entitlements repository is kept up to date with the relationships between accounts and entitlements in target systems through reconciliation processes.

IGA products are concerned primarily with entitlements involved with day-to-day administration, typically roles or groups in the target system. However, many business applications have complex, multilevel authorization models that provide their own role-based administration frameworks. Some IGA tools may be able to understand and even manage the different types of entitlements from multiple levels of complex authorization models, typically for specific applications from vendors such as Oracle and SAP.

Entitlements are often defined using IT-oriented cryptic names and lack descriptive metadata on source systems. Hence, there's a need to enrich entitlements in the IGA tool's entitlements catalog to associate friendly names, descriptions, tags and additional metadata that would be more meaningful to business users. Maintaining the entitlements catalog improves the legibility of the access environment across access requests, workflow and access certification capabilities.

This year the following scenarios were introduced to reflect new capabilities of IGA tools:

- Complex data models and identity types — The ability to support complex data models to accommodate software robots and smart devices that require flexibility and extensibility
- Identity analytics for account correlation — The ability to use analytics to visually assist with application onboarding

Additionally, the following functionality was evaluated using existing scenarios:

- Application onboarding — The ability to import accounts and entitlements from applications, the presence of a dashboard to monitor the onboarding and the process of enriching entitlements, as well as the ability to detect the presence of new entitlements awaiting enrichment.
- Account management — Categorizing accounts according to a taxonomy (business user, system, administrative, operational and sponsored accounts) (see [“IGA Best Practices: Focus on Three Planes of Control Over User Access”](#)) and assigning owners to accounts manually or based on account correlation rules.
- Entitlements catalog — Enriching entitlements by assigning friendly names and other metadata to entitlements, using a built-in schema, by creating synthetic entitlements and extending the schema.
- Integration — Integrating management of entitlements with external tools, such as coordinating account coverage with a privileged access management (PAM) tool.
- Password management — Enabling users to self-reset forgotten passwords, synchronizing passwords to and from target systems, and enforcing password constraints.

Access Requests

This capability enables end users to request access to resources, such as accounts, roles and entitlements for themselves (and in some cases for others), and has a major impact on the user experience.

Users select access to request from a catalog that is derived from the set of entitlements managed by the IGA tool. To provide a business-friendly experience, the entitlements data should be enriched (as discussed for the Entitlements Management capability) by administrators and analysts with

metadata to translate IT-oriented and cryptic names into friendly names, descriptions and search keywords.

Modern approaches to access requests commoditize access, eliminating rigidly sequential request flows, and provide users with a familiar paradigm (such as a shopping cart) for making requests. Users should be able to search for access and browse various models of entitlement hierarchies to discover the access they want to request. For example, users should be able to browse their own access and, under certain circumstances, the access of others. Managers should be able to browse the access of subordinates for comparisons and even copy access from one user to another when generating requests.

Users should also be able to review their request status and history. Users should be able to cancel in-flight requests at any time prior to fulfillment. It may even be possible for requesters to modify their requests, usually by allowing a canceled request to be placed back in a shopping cart for modification and resubmission.

The evaluation of the access requests capability focused primarily on the functionality and usability of the web interface for creating and managing access requests according to a number of criteria:

- Business-friendly access request experience allowing:
 - End users to request access for themselves
 - Managers to request access for subordinates
 - Project-specific approval context
 - Managers to copy access from one user to one or many users
 - Feedback to requesters about dependencies and potential policy violations prior to request submission
 - The creation of templates for frequent access requests
- The ability of requester and recipient to view request status and change or cancel in-flight requests
- The ability of end users to inspect their own access and view history of requests made on their behalf
- Support for internationalization and availability of multiple languages for the end-user interface:
 - Tools should support Unicode double-byte (UTF-16) character sets
 - Baseline support is for English, French, German and Spanish

Additionally, a new scenario was added this year to evaluate the use of analytics in support of automation based on risk criteria.

Workflow

Workflows generally coordinate with people and external systems to make decisions in support of policies. Most often, this enables managers and resource owners to approve or deny access requests. Workflow also orchestrates tasks that may not be directly related to access requests.

Workflows for approval processes usually follow a limited number of basic patterns and, without requiring customization, should support:

- Delegation — Approvers allowing others to act on their behalf for approval tasks
- Escalation — Requests forwarded to another approver if there is no response during a given time limit

Gartner recommends that organizations adopt a standard approval workflow driven by metadata for requests and approvals, rather than create separate workflows for applications (see [“IGA Best Practices: Standardize Approval Workflows for Access Requests”](#)). The evaluation of IGA products’ workflow capability is focused on the ability to support a standard workflow that implements it, following a four-stage pattern:

- Policy Analysis — Checking for control exceptions, such as SOD conflicts, dependencies, training requirements, sensitive access and impacts on risk scores in the context of a framework for policy analysis. Adding controls should not require modification of the workflow to perform required policy checks. For example, adding a new SOD risk via a policy console would be evaluated automatically during this stage without requiring workflow modification.
- Manager Approval — Depending on the context of the request, recipients’ direct supervisors or project managers may need to be consulted for approval. A manager approval may be suppressed if the requester fulfills the manager role (directly or through delegation) with respect to the request.
- Resource Approval — Individuals or groups of approvers responsible for resources being requested must provide approvals. Specific approvers should be selected based on metadata associated with entitlements being requested. When groups are specified as approvers, approval by one member of the group is sufficient. A resource approval may be suppressed if the requester (or requester’s manager) has been configured as (or is equivalent to) the resource approver.
- Control Approval — Unresolved control exceptions may require additional approval steps to enable a policy owner to render final judgment and select mitigating controls, if necessary. For example, if an SOD conflict is flagged during policy analysis and the request is approved by the manager and resource approver, the owner of the specific SOD control would be required to pass

final judgment on the request. After that, they would specify the mitigating controls required for that specific risk.

IGA workflows are often used to orchestrate system activities involving multiple integrated systems, so integration scenarios involving ITSM tools and electronic mail were evaluated. IGA tools should also provide a process control console to allow administrators to view the status of in-flight requests and resolve issues. Finally, workflow should provide approvers with the ability to electronically sign their approvals as required by some regulations.

Policy and Role Management

Policies and roles in IGA products work together to enable organizations to improve the efficiency of, and control over, access administration. Roles bring groups of users together with sets of entitlements, whereas policies control the automatic assignment and removal of roles for users.

Organizations usually pursue role management to leverage policies for assigning access to users as an alternative to requiring access requests. These policies also enable users to be removed from roles in an orderly manner when policies no longer apply, as an alternative to relying on access certification to remove access. Roles also improve the legibility of the environment by compressing multiple entitlements into roles with names and descriptions that are more meaningful to business users. Policies can also cover the expiration of request-based access and the handling of accounts no longer assigned to individuals, usually by disabling accounts and removing them after a retention period.

Gartner recommends the use of a two-layer enterprise role management framework to manage roles and policies at an enterprise scale with IGA tools in a heterogeneous environment (see [“IGA Best Practices: Take Control of Enterprise Role Management”](#)). In such an enterprise role management framework, the two layers — people and resources — align with the two logical IGA repositories:

- The people layer is aligned with the identity repository.
- The resource layer is aligned with the entitlements repository.

Although most IGA tools do not enforce strict distinctions between the roles for people and resources, IGA products generally recognize a semantic distinction between business and technical roles:

- Business roles — Roles in the people layer (sometimes referred by some vendors as enterprise roles) are often focused on grouping people to represent organizational structures (such as relationships, departments, locations and authority levels) to make policy administration more efficient.

- Technical roles — Roles in the resource layer (sometimes referred by some vendors as IT, provisioning or application roles) are often focused on grouping cohesive sets of entitlements to make the assignment of access more uniform and efficient.

The evaluation of the policy and role management capability for IGA products is focused on the ability of the tools to operate with a two-layer enterprise role management framework, using scenarios that covered the following functionalities:

- Interface for role and policy definition that supports preview of the impact of proposed changes. For example, show the users that would gain and lose access to a role if a new policy is applied.
- Support for handling expiration dates for request-based access.
- Handling of assignment and detachment policies for roles that offer precise control over how role assignments are handled when users are no longer covered by assignment policies.
- Role governance process to control the design and deployment of roles and associated policies through well-defined role states with support of version control and workflow approvals.
- Handling of accounts during life cycle events, such as disabling certain accounts prior to removal or transferring privileged accounts to different owners (see [“IGA Best Practices: Focus on Three Planes of Control Over User Access”](#)).
- Controlling the visibility of users or entitlements within such actions as delegation or access requests.

Role mining is considered the prototypical analytics scenario for IGA tools because it enables organizations to identify patterns of access among users and create candidate roles out of sets of entitlements to simplify administration. Analytics can also work in the other direction through role affinity analysis, finding users with direct entitlement assignments that are identical (or close) to the entitlements included in role definitions. This enables direct entitlement assignments to be replaced by role assignments. New scenarios were included this year for measuring the capacity of enhanced policy and role management experience, including the following analytics-driven functionalities:

- Ability to choose more than one method for role modeling, like affinity groups based on peer group analysis, risk evaluation and user behavior analytics.
- Ability to evaluate impact (what-if) before publishing policy and roles.
- Continuous monitoring of role assignments and policy effectiveness, alerting when anomalies in entitlements are detected and recommending corrections.

- Ability to leverage actual usage data of entitlements (that is, frequency a protected resource is actually accessed) in order to recommend adding new or removing unnecessary entitlements from roles.
- Continuous monitoring of policy effectiveness. Monitor user entitlements and access for adherence to access policy and alerts if any deviation occurs from the policy (including SOD violations).

Access Certification

Access certification is the process of requiring people (such as managers) to certify the access that users have to resources to ensure that access is still reasonable.

Access certification helps with regulatory compliance and cleaning up accumulated access, and it can be performed on a periodic basis or on a dynamic basis when certain risk thresholds are exceeded for a particular user (microcertifications). There are four types of access certification campaigns:

- Resource-based certification is the most common type of certification campaign. Resource owners (or approvers) review all users who possess certain resources, such as roles, entitlements or accounts.
- Organization chart certification requires managers to review the attributes of, or access assigned to, their subordinates.
- Account certification requires people to review the accounts for which they have been identified as owners to confirm that the accounts are still necessary and have the correct privileges. This type of certification is most often applied to system, operational and sponsored accounts.
- Entitlements catalog certification asks resource owners to review resource definitions (roles or entitlements), associated policies and metadata that are maintained in the entitlements catalog for accuracy.

Within an access certification task, the reviewer is asked to affirm or revoke access for specific users or entitlements. A third option may be to defer or forward specific items in a certification task, which allows a review to deflect the decision to another individual, if the assigned reviewer is unable to arrive at an informed decision. When access is flagged for revocation, a request for removal of access is submitted through the normal fulfillment mechanism for the targeted resource.

Access certification campaigns are created and queued by administrators, who are responsible for defining the scope, timing and other characteristics. These campaigns are generally executed according to a schedule, but they can be initiated on demand or even based on events in the system, such as changes in users' roles or characteristics like attribute values. Access certification

campaigns are usually performed on a snapshot of data that was obtained at a specific time, although some products allow certifications to be performed with real-time data as well.

The access certification capability was evaluated using scenarios that covered the following functionality:

- Support for resource-based certification campaigns, with various options for selecting in-scope entitlements
- Support for organization chart certification campaigns, with various options for selecting in-scope entitlements
- Support for account certification campaigns involving users responsible for administrative, system, operational and sponsored accounts
- Support for entitlements catalog certification campaigns, with the ability to certify and/or update metadata, including policies
- Support for special-purpose certification campaigns, including organizational hierarchy certification, contractor certification and single-user certification after department change
- Flexibility of control over certification campaigns and tasks, including the ability to reassign tasks, forward items with tasks, select columns to display within tasks, determine whether to allow bulk tasks ("select all" items to perform an action) and the ability to update items (such as expiration dates) in certification tasks
- Support for reviewers to apply electronic signatures to certification tasks, as required by some regulations

New scenarios were included this year for measuring the capacity of enhanced access certification experience, including the following analytics-driven functionalities:

- Configuring campaigns for automated certification of accesses of low risk.
- Ability to initiate microcertification campaigns for each user or group of users that are associated with events with a risk score above a certain level.

Fulfillment

Fulfillment is one of the most visible and complex capabilities of an IGA product. It allows changes initiated by the system to be reflected in target systems. Direct fulfillment connects with target systems, whereas indirect fulfillment uses a workflow or external system to complete actions.

Direct fulfillment, often known as provisioning, is efficient, but can be challenging to implement. IGA vendors often provide connectors for target system directories (such as AD and other

Lightweight Directory Access Protocol [LDAP]), email systems (such as Exchange), UNIX/Linux systems, and complex suites of business applications from vendors such as Oracle and SAP. Flexible connectors are usually available for interfacing with relational database management systems (RDBMSs) or other target systems for which specific connectors are not provided. These flexible connectors support well-known protocols, such as HTTP, Telnet, Secure Shell (SSH) or web services. Implementing provisioning is the most costly element of IGA deployments. As a result, most organizations use direct fulfillment for only a subset of business applications covered by their IGA deployments (see the Context section).

Indirect fulfillment is exemplified by the concept of a service desk connector, which allows account management operations for certain target systems to be forwarded to a service desk for fulfillment by technicians. Many IGA products provide a manual fulfillment feature that simulates (with workflow) what would be done by an ITSM tool for cases in which such a tool is unavailable or can't be easily integrated. Indirect fulfillment enables end-to-end IGA deployments to bypass the complexity of direct fulfillment and to scale rapidly. Indirect fulfillment is applicable in other areas as well. For example, RPA for automating the provisioning of unsupported applications or SaaS-delivered IAM tools are emerging as solutions to provisioning and deprovisioning for cloud applications as alternatives to developing unique connectors for every cloud app.

The evaluation of fulfillment focuses on the following criteria:

- Breadth and depth of built-in connectors, especially the availability of flexible connectors
- Ease of configuring indirect fulfillment, either stand-alone or integrated with ITSM tools, as the default mode of fulfillment when target systems are integrated
- The methods for configuring connectors, along with the availability of facilities and support for techniques that simplify complex integration scenarios
- Granular control over provisioning and deprovisioning operations to facilitate the transition between indirect and direct fulfillment for target systems
- Ability to leverage indirect fulfillment, integrated with RPA tools, or SaaS-delivered AM platforms (new for this year)

Auditing

The auditing capability supports the evaluation of business rules and controls that are enforceable through an IGA product. Auditing can be used to monitor the integrity of data maintained and monitor the performance of processes controlled by an IGA product.

Auditing can be thought of as a point-in-time or a continuous activity. The goal is to provide assurance to auditors and other stakeholders that business rules and controls are being enforced and to enable an organization to demonstrate that it has control over the environment. This often

requires periodic testing of controls to identify exceptions and provide for notification or case management to facilitate follow-up and remediation for exceptions.

When a case management framework is supported, identified exceptions would be checked against past cases related to the same exception instance to determine whether the exception has been reviewed previously:

- If the most recent case was closed with something like a “resolved” state, then it would be necessary to create a new case for the exception.
- If the most recent case for the exception was closed with something like a “false positive” or “approved exception” status, then the test results could be ignored for a certain period of time.

When business rules or controls are defined, they should be associated with an owner who would be responsible for investigating and remediating exceptions. Audit evidence is generated when tests are run, and exceptions are reviewed and resolved properly. The intention of auditing is to improve transparency through the operation of controls to make it easier for auditors and other stakeholders to rely on the IGA system to enforce controls.

IGA products have always had support for enforcing SOD controls, usually just as explicit policies that identify toxic combinations of roles. In recent years, more products have added support for defining more robust SOD controls, using increasingly fine-grained entitlements. Multiple IGA products support SOD controls that are defined in terms of business activity models mapped to entitlements in applications with complex authorization models.

The following criteria were used to evaluate the auditing capability:

- Availability of a framework and console for defining audit controls with enough flexibility to cover multiple control types, such as SOD, integrity of identity data and processes, and rogue accounts
- Availability of a case management framework to orchestrate and capture audit data related to the remediation of issues identified by audit policies
- Support for robust, business-activity-driven SOD controls, with content (predefined mappings of controls to entitlements) available for business applications with complex authorization models

Identity Analytics and Reporting

Some IGA tools provide specific analytics and reporting modules and some have embedded identity analytics and risk-based information in other capabilities, like access certification and requests.

The identity analytics and reporting capabilities of IGA tools have evolved to include more powerful risk-based decisions and cleanup capabilities. An increased amount of IGA tools from the current

generation now support deeper and more flexible interactions with available data. Beyond simply providing a report editor for defining custom reports, these analytics tools enable data to be analyzed using multiple perspectives (like peer group analysis) and statistical methods to generate insights and calculate risk from the information. Most often, this involves analyzing identity, entitlements and operational data; however, log data collected from target systems can be incorporated into reporting and analytics.

Reporting is still used 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 facilitated not only by built-in and custom reports, but also dashboards for metrics and data visualization.

The majority of IGA tools usually provide a collection of built-in reports that can be generated by authorized users or as scheduled tasks. The results are usually presented as a webpage, but there are often options for rendering in other formats, such as comma-separated values (CSV), PDF or spreadsheet files. Most of these reports are configurable and are most useful for general information requirements in the early phases of an IGA deployment.

Analytics are essential for computing metrics that are critical to monitoring the effective operation of an IGA tool. Analytics also serve as the mechanism by which many audit controls can be enforced. IGA products should present a reasonably coherent view of their data that can be used for reporting and analytics, even with external business intelligence (BI) tools. This is usually provided by a dedicated reporting database or a set of restricted views or web services interfaces to the data.

Continuous governance use cases leveraging identity analytics were evaluated in previous sections like policy and role management, access requests and certification.

The following new criteria for this year was used to evaluate specific cleanup identity analytics capabilities:

- Discover stale accounts (inactive, disabled, expired, dormant)
- Discover high-risk privileged accounts (root, admin, super users)
- Discover outliers (out of standard, excessive or unusual entitlements within accounts)
- Remediate and clean up discovered inconsistencies

Other identity analytics and reporting capabilities that were evaluated:

- Availability of built-in reports to cover the most common reporting needs, along with the ability to build custom reports delivered through the tool
- Suitability of data for reporting and analytics, including facilities for exporting or reformatting data when non-RDBMS repositories, such as LDAP directories or complex object models, are

used for persistence

- Robust role-mining facility, with the ability to model and generate candidate roles in a design environment
- Availability of predefined analytics to assist with the evaluation of the IGA tool's activities and service levels, including the ability to perform role affinity analysis
- Ability to generate metrics based on complex calculations that are rendered in a manner suitable for display in dashboards

Ease of Deployment

In many cases, deployment is the largest contributor to IGA total cost of ownership (TCO). Just getting the products installed correctly for an environment can be difficult and costly, as is assembly, making configuration changes and applying customizations to suit the product to the organization.

IGA products are complex enough to be beyond the capability of most organizations to deploy on their own. They usually require professional services from a third party or, occasionally, the vendor. Even with assistance from professional services, ease of deployment is a concern because it can have a direct bearing on the speed of deployment and TCO. Professional services can cost between 50% and 300% of licensing costs for a typical software-delivered deployment during the first year. This could depend on the complexity of the tool selected and the ability of the customer to streamline processes to conform to best practices and/or the tool's capabilities. Organizations should factor in the cost for additional professional services to assist with performing upgrades.

The following criteria were used to evaluate the ease-of-deployment capability:

- Complexity of the product itself and its underlying stack, including the supporting software, such as an application server and a database.
- Availability of cloud or appliance deployment form factors. A SaaS-delivered solution can reduce an average of 20% to 60% of the deployment costs of an IGA solution, depending on the use cases. Efforts for architecture and integration and application onboarding should remain equivalent.
- The relative balance between configuration and more involved assembly or customization in covered scenarios, including:
 - Configuration and administrative UI over manipulation of low-level product components.
 - Commodity scripting languages over the need for compiled code.

- Overall product support for configuration and change management, including the ability to migrate configurations between software development life cycle (SDLC) environments (for example, development to test to production) and support for patterned or scripted deployment.
- Ease of configuring enterprise-class services, such as external authentication to the IGA tool's end-user interface — either pass-through authentication to an existing directory or integration with a single sign-on (SSO) tool — and multiple instances for scaling, failover and disaster recovery.

Scalability and Performance

The five dimensions of scalability and performance for IGA tools are the number of identities/attributes; number of target systems, accounts and entitlements; number of connections between users and entitlements; volume of log information collected; and efficiency of the data model.

Reconciliation, reporting, policy calculation and the generation of access certification campaigns can impose a heavy load on an IGA product and, occasionally, other systems. The IGA product should be able to balance the load of reconciliations, reporting and policy calculation, while not affecting the availability of other services, especially the ability of users to request and approve access and perform certification tasks.

There should be clear guidance on how to size an IGA tool deployment for adequate performance under expected loads. Cost is a consideration when judging scalability. If it takes a lot of hardware to achieve acceptable performance at scale, then this would be considered a drawback. Some architectures are more scalable than others due to the efficient use of processing and memory resources.

Use Cases

Global Enterprise

This type of enterprise (with over 10,000 employees) typically has complex processes for managing large numbers of users and entitlements with strict compliance requirements.

Scalability and performance is very important for global enterprises and become even more critical for the largest global enterprises (those with more than 50,000 employees and potentially thousands of applications). In those situations, it may become a hurdle that must be overcome by products before any other capabilities can be considered. Identity analytics and reporting, policy and role management, and workflow are also weighted most heavily because larger organizations deal with very large volumes of accounts, repositories and identity data in general. Robust entitlement controls and efficient enterprise role management become a prerequisite for managing huge volumes of identity data.

Fulfillment, auditing and identity life cycle are also important because large numbers of account repositories often prevent users from obtaining the access they need and from adhering to security requirements without significant automation. These organizations are often subject to multiple stringent regulatory regimes that make compliance, like SOD monitoring, a business imperative.

Midsized Enterprise

Enterprises with less than 1,000 employees possess simpler environments and require a good balance between fulfillment (including provisioning) and governance, with low TCO.

Ease of deployment is weighted most heavily because midsized enterprises may not have the dedicated staff with sufficient skills to support a complex IGA deployment. They need to be up and running with visible functionality quickly.

Identity analytics and reporting is important because it can be used to facilitate the cleanup of unnecessary or dormant entitlements and mitigate risk in a usually staff-constrained environment. Access requests and identity life cycle are also important because process maturity is often lower, so a high proportion of entitlements will be assigned based on requests. Such organizations will be looking for examples of life cycle processes they can adopt, rather than customize.

Governance-Focused

Organizations that focus on governance are concerned primarily with managing and enforcing access policies and demonstrating control over user access.

The elements of what could be considered the governance chain of capabilities — identity analytics and reporting, entitlements management, access certification, policy and role management, access requests, workflow, and auditing — are most important for governance-focused deployments.

Access certification and auditing are very important because, in many cases, it's required for regulatory compliance, and it provides a way to detect and remediate out-of-compliance findings. Identity analytics is also very important because of its ability to support risk mitigation strategies, compliance reporting and provide insight into the effectiveness of controls.

Entitlements management is important because of its ability to capture and model entitlements management from a broad range of systems, which is critical to the proper functioning and optimization of other governance processes.

Policy and role management is important because it simplifies the environment and standardizes the enforcement of policies.

Automation-Focused

Provisioning is the original automation-focused use case for IGA deployments, targeting efficiency and control simultaneously through end-to-end automation.

Fulfillment is weighted most heavily because the effectiveness of automation is determined by the ability to efficiently integrate with external account repositories. Identity life cycle is important because HR feeds and nonemployee management activities initiate the automated processes. Policy and role management is valued for the ability to automatically determine access that users should be assigned.

Vendors Added and Dropped

Added

No vendors were added since last year. Although there are more vendors now providing IGA services, none were able to meet our inclusion criteria, and so none were added.

Dropped

Microsoft met the minimum revenue goals, but was dropped from this Critical Capabilities because it no longer met the technical inclusion criteria after deprecating the BHOLD component of its IGA solution, Microsoft Identity Manager (MIM). BHOLD was required for policy and role management, analytics, and access certification. Microsoft is redeveloping this functionality in its SaaS-delivered IAM offering, Azure Active Directory, which is also available in Enterprise Mobility + Security (EMS). At the time of analysis, some of this functionality (such as access certification) was already generally available, while other functions (such as policy and role management) were available in public preview, but was not yet generally available. Microsoft's strategy is to enhance its IGA capabilities in Azure Active Directory, and Gartner expects Microsoft to eventually meet those technical inclusion criteria for IGA in the near future.

The following vendors fulfill the technical inclusion criteria of the Critical Capabilities but were excluded because they did not meet the minimum revenue goals, specifically the requirement for having added 50 new clients ("net new logos") within the fiscal year:

- AlertEnterprise offers its Enterprise Guardian suite of products. It can extend beyond traditional IAM for logical assets toward areas of physical security and operational technology (OT), including visitor management, physical access control systems (PACSS), badging systems and interfaces, and supervisory control and data acquisition (SCADA) industrial control systems. The platform also includes threat and risk behavioral analytics for risk scoring by combining identity information with user activity feeds. AlertEnterprise does not yet offer IGA as a service.
- Core Security is headquartered in the U.S. and offers the Core Access Assurance Suite (AAS) as software. The solution will have a strong appeal to organizations with a heavy focus on security that are looking for synergies between IGA and real-time security intelligence. The company was acquired by Help Systems in February 2019.
- Dell Technologies (RSA) offers its IGA solution RSA Identity Governance and Lifecycle (IG&L) as software. The solution is also available as a cloud-hosted option called My Access Live. Several partners of RSA also host the solution as a managed service. The solution is a good fit for organizations with heavy governance requirements.

Inclusion Criteria

To qualify for inclusion in the 2019 Magic Quadrant and Critical Capabilities for Identity Governance and Administration, vendors need to:

- For any period of 12 consecutive months (fiscal year) between 1 January 2018 and 30 April 2019 have booked a total revenue of at least \$25 million for IGA products and subscriptions (inclusive of maintenance revenue but excluding professional services revenue) OR revenue of \$20 million for IGA products and subscriptions (inclusive of maintenance revenue but excluding professional services revenue) and a year-over-year growth rate of 10%.
- Have sold to at least 50 net new named IGA accounts (new logos, independent of reimplementations from previous versions of a product) during the same period of 12 consecutive months (fiscal year) between 1 January 2018 and 30 April 2019.
- Have sold and supported their own IGA product or service developed in-house, rather than offered as a reseller or third-party provider.
- Have sold their IGA product or service to clients in different verticals or industries (that is, vendors that only sell their product within a particular industry or vertical are excluded).

In addition, the vendor's IGA product/solution must offer:

- An integrated identity repository that masters (stores) information about people for whom access to managed information systems must be administered, along with the ability to support multiple identity life cycles to manage this information. This includes synchronization with authoritative sources (such as HR systems) as well as administrative workflows.
- Tools for application entitlement discovery, mining, management and enrichment, including the maintenance of an entitlements catalog.
- Functionality to manage the linkage of identities with accounts and entitlements, including the ability to tell who has access to what and who is responsible for maintaining an account or entitlement.
- Tools to manage the end-to-end process of requesting access through business-friendly user interfaces by end users with approval workflows.
- Support for role-based administration across multiple applications, including governance over role engineering and administration as well as integrated role mining and role analytics to allow for the replacement of direct entitlement assignments for users with role assignments.
- Facilities for specifying and enforcing policies, such as those that govern automatic assignment (and removal) of roles and entitlements, visibility of roles and entitlements for selection in access requests, dependencies and incompatibilities between roles and entitlements, and so on.

- Support for the specification and execution of access certification campaigns covering identities and entitlement assignments involving specified actors (such as managers and resource/application owners).
- Tools to reconcile data from target systems with IGA data for multiple targeted technical environments (for example, Windows, IBM i, UNIX/Linux, multiple applications and SaaS).
- Tools and connectors to automatically propagate changes to target systems (direct fulfillment or “provisioning”), as well as indirect fulfillment where changes are made using workflows or external processes (such as service tickets submitted through ITSM tools).
- Analytics and reporting of identities, entitlement assignments and administrative actions.
- Underlying architecture for the above, including connector architecture for data collection and fulfillment actions.
- Products deployed for use with customer production environments for purposes consistent with the objectives of IGA.

Changes in Inclusion Criteria From Last Year

With respect to the 2018 Critical Capabilities inclusion criteria, the following has changed:

- The minimum revenue was raised to focus this research on the segment of the market that is most relevant across Gartner’s clients. This means that a vendor must have more than \$25 million in revenue to be included in this research. Alternatively, a vendor could qualify by having \$20 million revenue, but year-over-year growth of 10% or higher (which is over the average IGA market growth).

We also limited inclusion this year to vendors that closed at least 50 new deals with new clients (net new logos), excluding new deals or upgrades with existing clients.

Table 1: Weighting for Critical Capabilities in Use Cases

Critical Capabilities ↓	Global Enterprise ↓	Midsize Enterprise ↓	Governance-Focused ↓	Automation-Focused ↓
Identity Life Cycle	10%	10%	7%	20%
Entitlements Management	7%	5%	10%	5%
Access Requests	5%	10%	7%	10%

Critical Capabilities ↓	Global Enterprise ↓	Midsize Enterprise ↓	Governance-Focused ↓	Automation-Focused ↓
Workflow	12%	6%	7%	8%
Policy and Role Management	12%	2%	10%	10%
Access Certification	8%	7%	15%	2%
Fulfillment	10%	6%	5%	30%
Auditing	10%	2%	15%	2%
Identity Analytics and Reporting	12%	11%	15%	5%
Ease of Deployment	2%	39%	4%	4%
Scalability and Performance	12%	2%	5%	4%
Total	100%	100%	100%	100%
As of November 2019				

Source: Gartner (November 2019)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighed in terms of its relative importance for specific product/service use cases.

Critical Capabilities Rating

Each of the products/services has been evaluated on the critical capabilities on a scale of 1 to 5; a score of 1 = Poor (most or all defined requirements are not achieved), while 5 = Outstanding (significantly exceeds requirements).

Table 2: Product/Service Rating on Critical Capabilities

Critical Capabilities ↓	Atos (Evidian) ↓	Broadcom (CA Technologies) ↓	Hitachi ID Systems ↓	IBM ↓	Micro Focus ↓
Identity Life Cycle	4.1	3.1	4.4	1.9	3.0
Entitlements Management	2.6	3.2	3.3	3.4	3.6
Access Requests	2.7	4.1	3.7	3.6	3.6
Workflow	2.8	3.1	3.9	3.3	3.8
Policy and Role Management	3.2	2.5	3.0	3.4	4.5
Access Certification	2.6	3.3	3.9	3.7	3.5
Fulfillment	3.1	3.6	4.2	3.1	4.0
Auditing	2.5	2.3	3.1	2.6	3.2
Identity Analytics and Reporting	3.0	3.6	2.8	3.0	4.0
Ease of Deployment	2.6	3.2	3.8	3.7	3.3
Scalability and Performance	3.2	3.4	4.0	3.9	3.4
As of November 2019					

Source: Gartner (November 2019)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use-case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3: Product Score in Use Cases

Use Cases ↓	Atos (Evidian) ↓	Broadcom (CA Technologies) ↓	Hitachi ID Systems ↓	IBM ↓	Micro Focus ↓
Global Enterprise	3.01	3.17	3.62	3.18	3.68
Midsize Enterprise	2.87	3.32	3.73	3.33	3.50
Governance-Focused	2.89	3.15	3.50	3.19	3.65
Automation-Focused	3.18	3.32	3.88	3.02	3.70
As of November 2019					

Source: Gartner (November 2019)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

Evidence

Data for evaluating critical capabilities was collected during July and August 2019 from vendors participating in this research, concurrently with data collection for the [“Magic Quadrant for Identity Governance and Administration.”](#)

Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when

considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor's product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.

Document Revision History

[Critical Capabilities for Identity Governance and Administration - 5 June 2018](#)

[Critical Capabilities for Identity Governance and Administration - 1 May 2017](#)

[Critical Capabilities for Identity Governance and Administration - 15 March 2016](#)

[Critical Capabilities for Identity Governance and Administration - 2 February 2015](#)

Recommended by the Authors

[Magic Quadrant for Identity Governance and Administration](#)

[Definition: Identity Governance and Administration](#)

[IGA Best Practices: Prioritize Analytics When Adopting IGA](#)

[IGA Best Practices: Governance First, Automated Provisioning Later](#)

[IGA Best Practices: Focus on Three Planes of Control Over User Access](#)

[How Products and Services Are Evaluated in Gartner Critical Capabilities](#)

Recommended For You

[Magic Quadrant for Identity Governance and Administration](#)

[Gartner Peer Insights 'Voice of the Customer': Identity Governance and Administration](#)

[Definition: Identity Governance and Administration](#)

[The Identity Governance and Administration Landscape Is Changing](#)

[Tool: Identity Governance and Administration Deployment Prioritization](#)

© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)."

[About Gartner](#) [Careers](#) [Newsroom](#) [Policies](#) [Privacy Policy](#) [Contact Us](#) [Site Index](#) [Help](#) [Get the App](#)

© 2020 Gartner, Inc. and/or its affiliates. All rights reserved.