

Licensed for Distribution

**Gartner.** This research note is restricted to the personal use of ().

# Critical Capabilities for Identity Governance and Administration

Published 5 June 2018 - ID G00332371 - 84 min read

By Analysts Brian Iverson, Kevin Kampman, Felix Gaehtgens

---

IGA tools help organizations control access risks by managing user accounts and entitlements in infrastructure systems and applications enterprisewide. Security and risk management leaders responsible for identity and access management 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](#)

## Overview

### Key Findings

- Most identity governance and administration products have matured to provide well-balanced governance and administration functionality that satisfies the requirements of the typical organization with regulatory compliance obligations concerning the management of access risk.
- The transition of IGA to cloud delivery is just beginning; most IGA products continue to be targeted for deployment on-premises, with a primary focus on managing on-premises applications.
- IGA solutions can be difficult to deploy. Gartner estimates that 50% of IGA deployments are in distress — i.e., they have failed to achieve functional, budgetary or timing commitments. IGA deployments that end up in distress often prioritize provisioning during early phases.
- Using IGA tools merely to automate an organization's manual processes for account administration and to manage access risk usually replicates inadequate processes,

while requiring significant assembly and even customization. This increases the cost and time required for deployment and future upgrades.

## Recommendations

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

- Determine which IGA capabilities and application integrations are most valuable to the organization, while assessing the deployment risks associated with these elements.
- Create a roadmap for IGA deployment that prioritizes the high-value, low-risk elements, saving higher-risk elements for later phases — for most organizations, governance-oriented capabilities provide the most value, with less deployment risk than provisioning.
- Treat IGA deployment as a broadly scoped business process re-engineering project, not merely a technology project. IGA should be approached as a platform for adopting best practices and redesigning processes for the management of user access.

## Strategic Planning Assumptions

By 2019, more than 50% of identity governance and administration (IGA) vendors will have significant IGA capabilities available as a service, which is an increase from fewer than 20% in 2017.

By 2020, more than 30% of new IGA deployments will be service-based, which is an increase from fewer than 10% in 2017.

## What You Need to Know

IGA plays a critical role in the administration and control of user access for most organizations with more than 2,500 users and many that have as few as 700 users. IGA is the largest investment that most 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. IGA often consumes more of an IAM program's capital expenditure/operating expenditure (capex/opex) budget than all of the other IAM investments combined. 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.

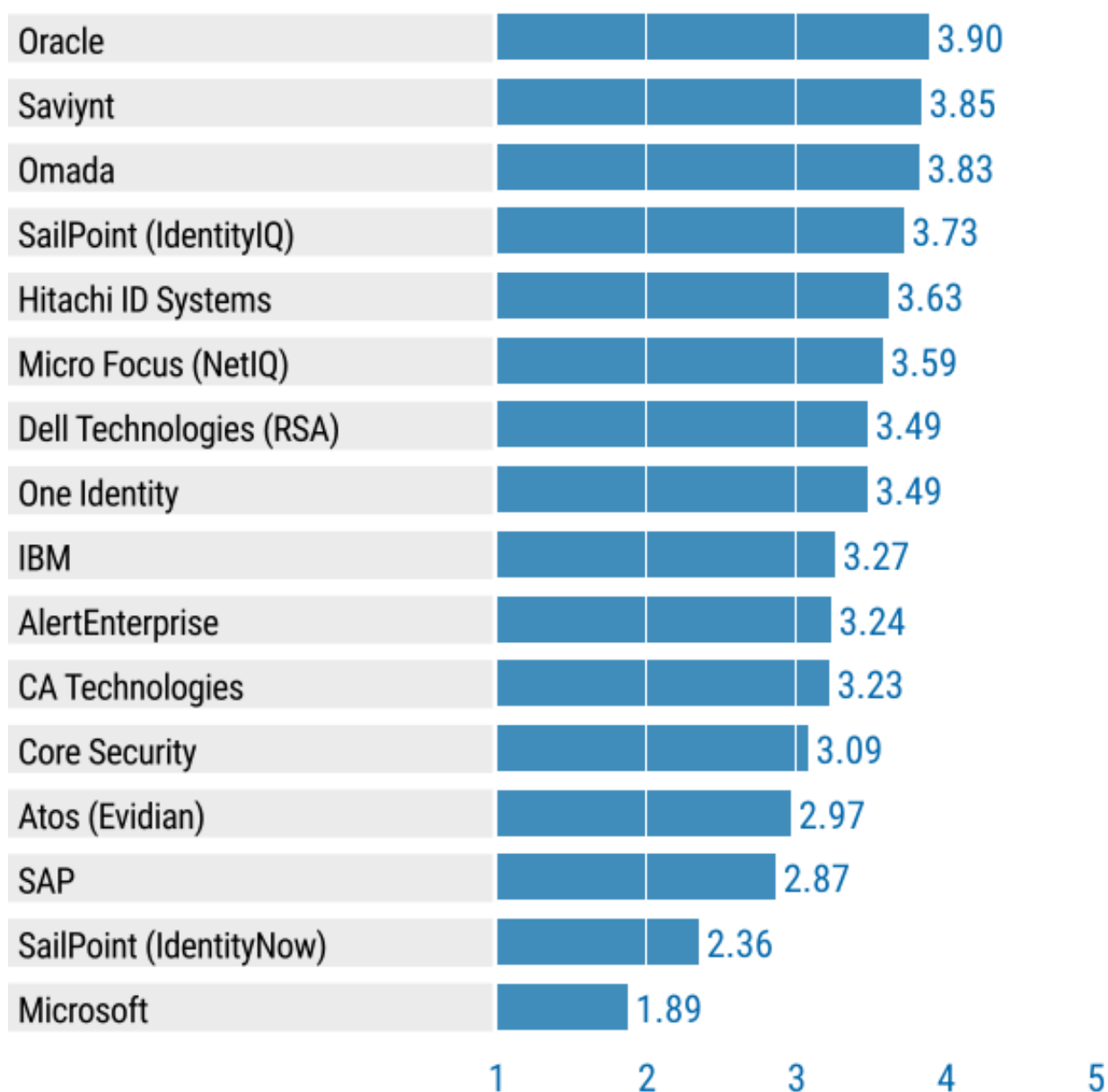
## Analysis

## Critical Capabilities Use-Case Graphics

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

Source: Gartner (June 2018)

### Product or Service Scores for Global Enterprise



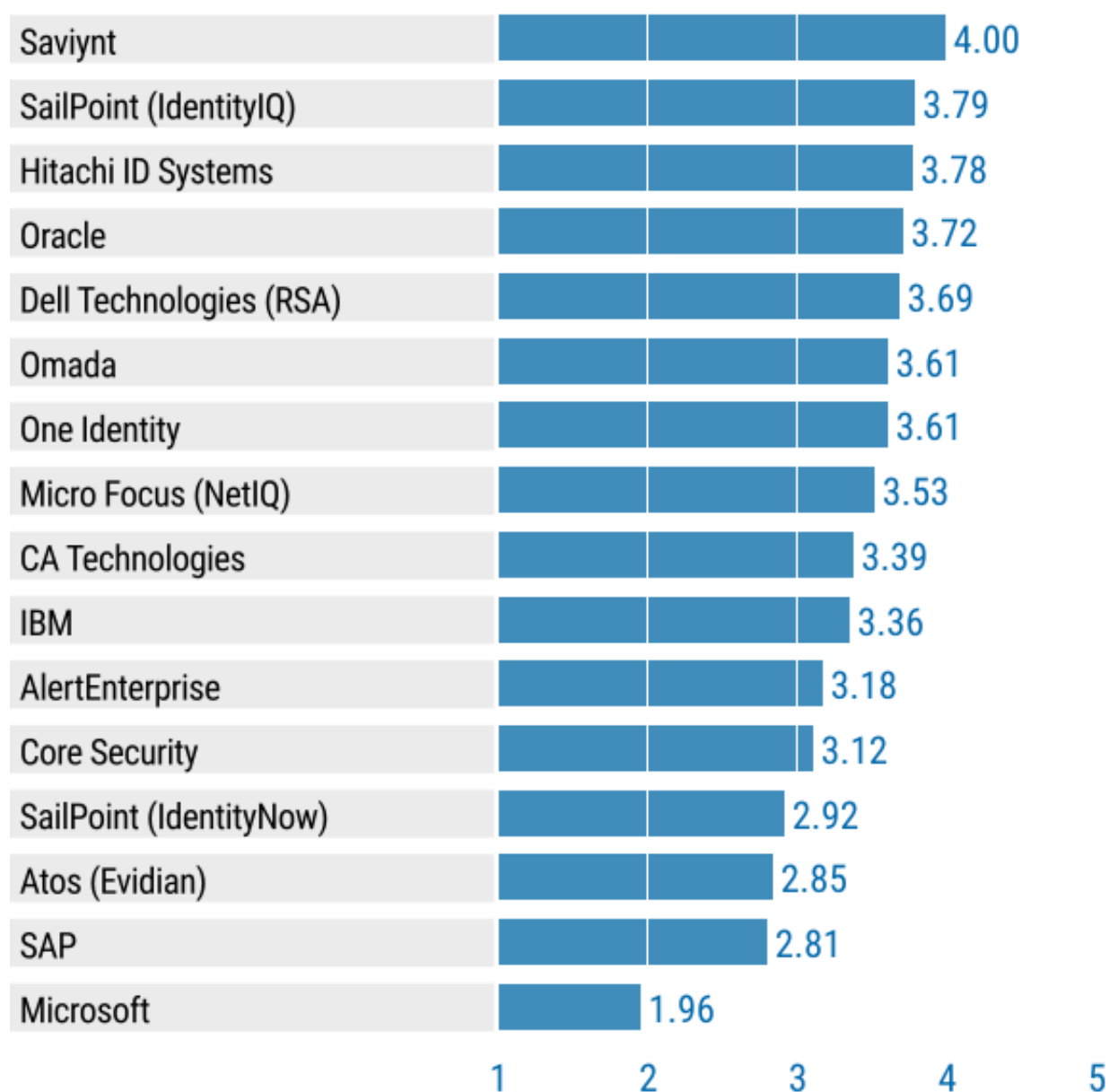
As of June 2018

© Gartner, Inc

Figure 2. Vendors' Product Scores for the Midsize or Large-Enterprise Use Case

Source: Gartner (June 2018)

## Product or Service Scores for Midsize or Large Enterprise



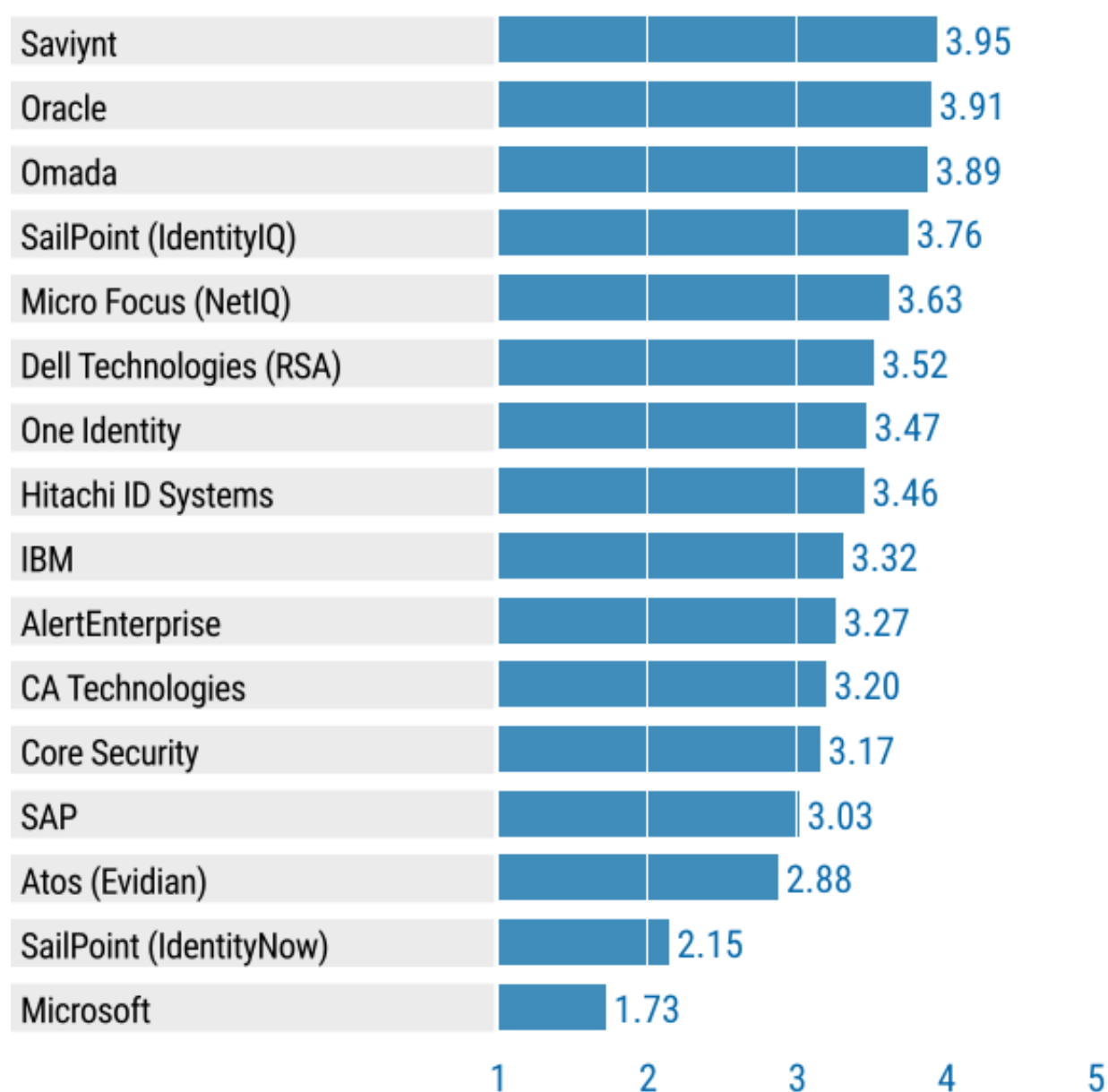
As of June 2018

© Gartner, Inc

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

Source: Gartner (June 2018)

## Product or Service Scores for Governance-Focused



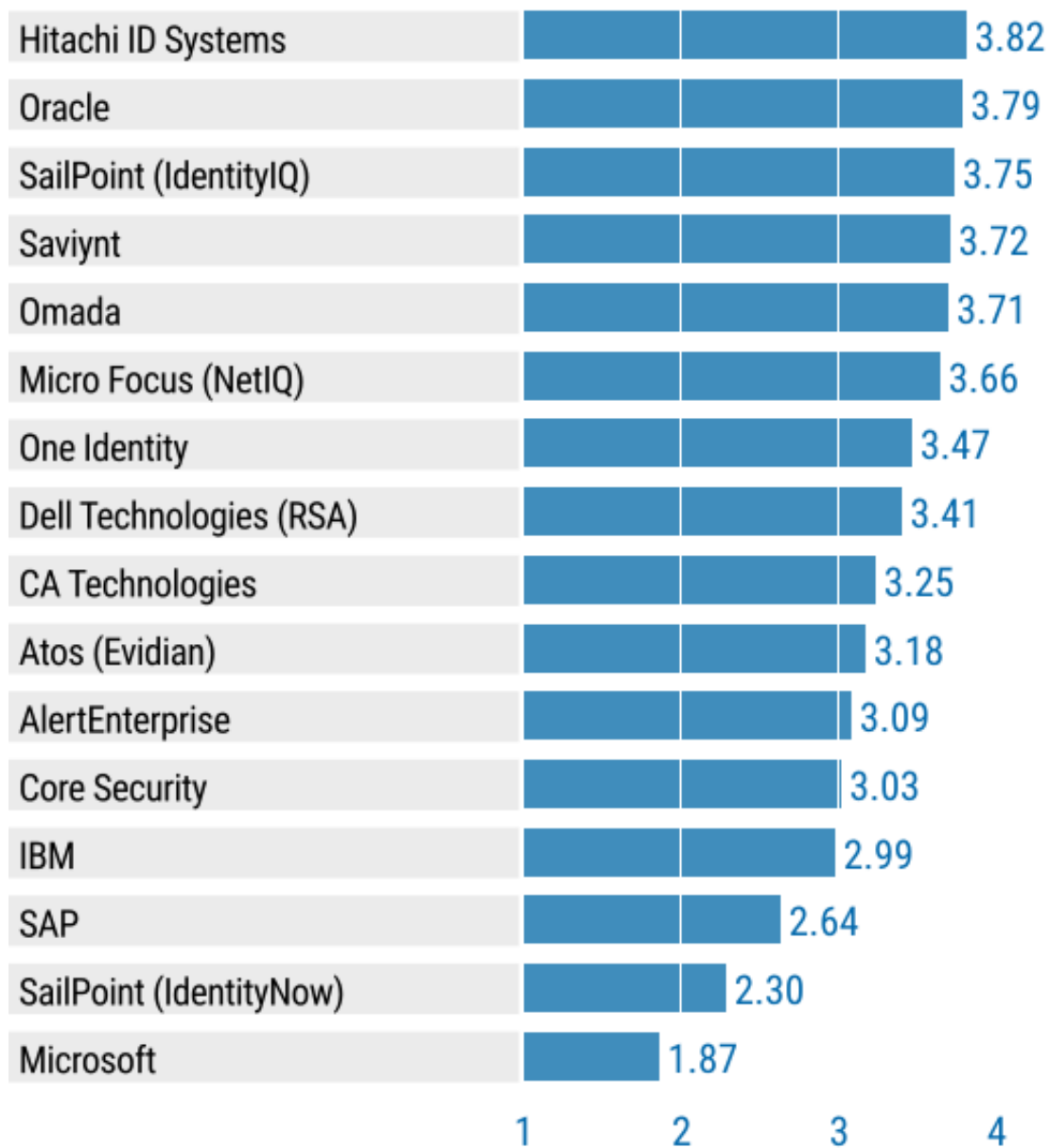
As of June 2018

© Gartner, Inc

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

Source: Gartner (June 2018)

## Product or Service Scores for Automation-Focused



As of June 2018  
Vendors

© Gartner, Inc

### AlertEnterprise

Enterprise Guardian's unified platform for IGA extends to support the management and monitoring of physical security and operational technology, as well as analytics for threats and behavioral risks. The Enterprise Guardian suite is composed of two core modules that can be purchased together or separately:

- Enterprise Guardian Physical Suite

- Enterprise Guardian Logical Suite

AlertEnterprise has focused its attention on highly regulated industries, such as critical infrastructure and natural resources extraction and processing. Enterprise Guardian is an attractive solution for organizations interested in working toward the convergence of logical, physical and operational technology security.

Identity Life Cycle: Basic employee life cycle scenarios, along with anonymous user self-registration, require significant assembly. There have been improvements in support of contractor and business partner scenarios; however, enabling delegated administration requires significant assembly.

Entitlements Management: The entitlements data model is robust and extensible, offering deep insights into applications with complex authorization models. Support for importing entitlements from applications is average, and there is no dashboard for monitoring application onboarding.

Access Requests: The access request interface is functionally complete, but presented in a linear manner that is less intuitive for business user than what is common among leading products. Enterprise Guardian now provides an API that allows requests to be submitted remotely, such as from IT service management (ITSM) tools.

Workflow: Enterprise Guardian provides a ready to run (RTR) workflow, but modification is needed to conform to the four-stage model. The workflow features are flexible, with built-in handling of requests for entitlements with training requirements, as well as support for changing the contents of in-flight requests.

Policy and Role Management: Can operate with two layers of roles (called "enterprise" and "application" roles), although the product's role management framework is not as flexible as has become customary with other products. This is because enterprise roles can be defined as containers for application roles only, making it more difficult to implement a two-layer enterprise role management framework.

Access Certification: Provides a highly functional and flexible set of features for access certification that can support all of the common scenarios, although some workflow configuration is needed. There is only limited support for narrowing certification campaign scopes based on exceptional access or incremental changes.

Fulfillment: Only three connectors — file, database and Active Directory (AD) — are included with the base product. However, numerous connectors are available for purchase, covering all of the most typical IT systems (excluding mainframe), plus connectors for applications — e.g., surveillance, physical access control system (PACS) and security automation — that are not typically supported by IGA tools.

**Auditing:** Provides extensive support for analyzing and mitigating segregation of duties (SOD) risks, with content packs available for business-oriented risk analysis for applications with complex authorization models. An improved case management framework allows for the assignment of audit cases to multiple types of policy violations.

**Reporting and Analytics:** Provides a report builder with a selection of built-in information reports. Although the product provides interesting behavioral analytics, support for core IGA analytics is incomplete, and role mining is rudimentary.

**Ease of Deployment:** The product benefits from running as a unified platform, but gaps in functionality require significant assembly and some customization to overcome. However, there has been modest improvement in features (especially identity life cycle and auditing) to support multiple scenarios that required significant assembly in previous years.

**Scalability and Performance:** The scale and performance of the base platform are bolstered by the incorporation of big data storage for entitlements and history data. However, the application architecture allows only indirect support for isolating workloads by hiding nodes from load balancers.

## **Atos (Evidian)**

Evidian Identity Governance & Administration (IGA) 10 is a converged offering from Atos that replaced two previous product lines: Evidian IAM9 (acquired when Atos purchased Bull in 2014) and DirX IAM Suite. The current version, Evidian IGA 10 Evolution 1, is offered as a base product (made up of Policy Manager, Request Manager, IDSynchronisation and reporting modules) with several optional modules. The optional modules required to fulfill typical IGA requirements include the following:

- Workflow Editor
- Policy Creation Module

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

**Entitlements Management:** A new interactive report for managing user account ownership has been added, and account types are maintained as connection contexts. The schema for entitlements is not extensible, but entitlements (called "permissions" in Evidian's data model) can be assigned to contexts so they can be associated with policies.



**Access Requests:** The access request interface is linear and possesses elements such as a requirement to choose between roles and permissions, which may be confusing for business users.

**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 customization.

**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:** New support for access certification campaigns based on organization chart, although campaigns for applications and certifying the entitlements catalog itself are not supported. Provides excellent support for certifications involving attributes such as expiration dates.

**Fulfillment:** The base set of connectors includes some popular cloud apps, whereas connectors for mainframe and specialized systems are sold separately. Support for multidomain AD environments is below average, but support for fulfillment using service tickets has been improved.

**Auditing:** The product has the ability to 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.

**Reporting and Analytics:** Reporting capabilities are more than adequate, including some useful metrics. Role mining is provided by a separate utility that must be loaded with IGA data.

**Ease of Deployment:** The core product is based on Windows, but compiled Java code is used in place of scripting for several scenarios. The new version has reduced the excessive modularity of previous versions, although some discontinuity (such as separate role mining utility) remains.

**Scalability and Performance:** There is support for high availability at the application and data tiers, including the ability to dedicate modules to separate nodes. The product benefits from performance advantages of native Windows compiled code for several modules.

## CA Technologies

CA Identity Suite is part of a full IAM suite from CA Technologies and fulfills a broad range of IGA requirements. It includes three modules:

- **CA Identity Manager** — A back end for identity life cycle, provisioning and policy-driven administration

- CA Identity Governance — Entitlements management for the support of governance functionality
- CA Identity Portal — A modern user interface (UI) that presents a unified experience for end-user functions, such as access requests, password management and access certification

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

**Identity Life Cycle:** CA's Deployment Xpress feature provides prebuilt use-case templates for all four identity life cycle patterns (see definition of capability). The provided use cases are not yet robust, so some work needs to be done to handle more-complex aspects of common scenario combinations.

**Entitlements Management:** The entitlements data model is flexible, and its interfaces satisfy all key scenarios, but the schema for entitlement metadata is limited to extension through key value pairs. There are gaps in facilities for assisting with the orchestration of application onboarding and maintaining entitlements.

**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 now.

**Workflow:** Deployment Xpress can provide a highly functional approval workflow template that conforms to the standard, four-stage workflow pattern, requiring only a custom participant resolver for manager approval and configuration of escalation policies.

**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 subordinates — require a work-around in which contractors are modeled as entitlements.

**Fulfillment:** A broad collection of connectors is included with the base product, and indirect fulfillment is supported through an ITSM integration framework (with built-in support for multiple ITSM tools). Support for AD provisioning is better than what is available with most products, despite the need to configure endpoints for every domain in a forest.

**Auditing:** There is no central console for defining audit policies — even SOD policy definition is handled inconsistently. The concept of case management to resolve audit issues is not directly supported, so workflow and access certification must be used as alternatives.

**Reporting and Analytics:** Jaspersoft Business Intelligence provides a strong platform for reporting and analytics, and the role mining and related analytics are especially strong, compared with other vendors' capabilities. The Identity Analytics dashboard provides performance information, but effectiveness metrics are missing.

**Ease of Deployment:** The Deployment Xpress facility allows 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.

**Scalability and Performance:** The product has demonstrated high levels of scalability, especially in B2C and governance-to-constituent (G2C) scenarios; however, reliance on data processing in the application tier when using the optional directory server back-end could pose challenges in large-scale deployments.

## Core Security

Core Security Access Assurance Suite (AAS) is an IGA solution composed of multiple products that are often sold individually to customers focused on specific aspects of IGA functionality. The individual products that make up the suite (and are required to provide full IGA functionality) include:

- Core Access
- Core Compliance
- Core Certify
- Core Provisioning
- Core Password
- Visual Identity Suite

AAS is a good choice for organizations that require a balanced approach to provisioning and access governance, with built-in support for behavioral analytics.

**Identity Life Cycle:** Provides adequate support for common employee, contractor and self-registration scenarios (see definition for this capability), including expiration process for nonemployees. Setup of onboarding processes for contractors and delegated administration requires workflow assembly.

**Entitlements Management:** There is a wizard-driven process for onboarding accounts and entitlements, with excellent support for managing the ownership of accounts and

mastering entitlement data. Access Insight provides deep insight into complex authorization models for analytics.

**Access Requests:** Provides an attractive interface for access requests; however, the process is more linear than necessary despite being based on a shopping cart paradigm. Only English is supported out of the box — support for other languages requires translation by Core Security professional services. Some user controls, such as the ability for recipients to cancel requests, are lacking.

**Workflow:** The built-in request workflow conforms to the standard, four-stage request approval pattern, with the final control-owner stage using a mechanism that Core Security calls a microcertification.

**Policy and Role Management:** There is a new Role Designer product included with Visual Identity Suite; however, it is not yet integrated with AAS and does not add a great deal of benefit to core IGA scenarios. Role management in AAS is hampered by policies that are defined separately from roles through a matrix table mechanism, which does not provide a preview of policy changes.

**Access Certification:** Historically, excellent support for access certification has been improved over the last two years with better support for scoping certification campaigns. The display of information and additional details in certification tasks can be controlled easily during campaign setup, but there are limitations on what can be done within certification tasks, such as facilitating changes to attribute values.

**Fulfillment:** Core Security provides a limited set of connectors with the base product; however, there is a large library of connectors available for purchase separately or as part of a bundle. The Core Connector API was released in 2017 to supply customers with more options for integrating with target systems. Complex attribute generation can be challenging, and AD support is average.

**Auditing:** Microcertifications provide a flexible interface for managing audit cases that can be triggered from exceptions to policies beyond SOD and rogue account detection. There are gaps in the ability to specify and evaluate controls over identity integrity.

**Reporting and Analytics:** Access Insight provides a powerful and efficient IAM-specific analytics engine, with an impressive set of built-in metrics. Reporting is built around Microsoft SQL Server Reporting Services (SSRS), and a modest collection of built-in reports is provided.

**Ease of Deployment:** The product is reasonably easy to deploy and configure, especially with regard to configuring nodes for scalability and fault tolerance. When scripting is required, various commodity languages can be used interchangeably, although there are multiple instances in which stored procedures, XSLT scripts and XML files must be manipulated.

**Scalability and Performance:** This product includes few of the standard considerations for scalability, such as clustering and fine-grained control over task execution across nodes. However, the product's performance benefits from the use of native Windows code and leveraging the data tier for some data processing.

## Dell Technologies (RSA)

Massachusetts-based RSA, formerly the Security Division of EMC, is now part of Dell Technologies. RSA Identity Governance and Lifecycle (IG&L) can be delivered as a hardware appliance or as software only, running on-premises or via a SaaS offering. The product is broken down into modules that can be purchased separately:

- RSA Identity Governance — A collection of entitlement data for access reviews and policy enforcement, reporting and analytics
- RSA Identity Lifecycle — User self-service access requests, approvals, password management provisioning
- RSA Business Role Manager — Role mining, modeling and management
- Data Access Governance (DAG) — Governance of access to data resources (e.g., file shares and SharePoint)

The first three modules are required to deliver the full range of IGA capabilities. RSA IG&L is most often selected by organizations with extensive governance requirements looking to provide a business-friendly user experience.

**Identity Life Cycle:** Working with feeds for employees is supported well, especially with the join feature for multiple sources, and there is basic support for handling delegated administration and self-registration. There is no built-in support for the sponsorship-and-expiration pattern that is typically used for contractors and business partners, so forms and workflows must be assembled.

**Entitlements Management:** Good support for essential functionality, with a flexible schema for entitlement metadata, especially the application concept as a way to organize accounts and entitlements while providing application-specific metadata.

**Access Requests:** Although it has not kept pace with the latest user experience developments of competitors, RSA still provides one of the most business-friendly interfaces for access requests, with many options for receiving additional context for entitlements.

**Workflow:** Workflow templates are provided through the RSA Link community, although the default workflow with delegation support may be adequate for most cases with configuration.

**Policy and Role Management:** Excellent support for managing distinctions among role types through the concept of role sets. Despite the native ability to support

expiration dates for entitlement assignments, there is a lack of control over what happens to assignments when expiration occurs.

**Access Certification:** Many types of certification campaigns are well-supported, but campaign types for reviewing supervisor assignments, contractor validity, entitlement metadata and exceptional access are missing. Electronic signatures are supported in the form of a password prompt for the submission of certification tasks.

**Fulfillment:** Exemplary support for manual fulfillment, including multiple, built-in integrations with ITSM tools. A rich set of connectors is available from RSA, all of which are included with the Lifecycle module.

**Auditing:** Provides an auditing framework for SOD conflicts primarily. Other scenarios require custom rules defined in various ways, often using role membership rules to assign roles to users with specific issues. Custom workflows simulating audit cases can be launched based on attribute values that indicate exceptions.

**Reporting and Analytics:** There is an expanded collection of built-in reports and analytics, including excellent role metrics. The Business Role Manager module provides excellent role-mining and affinity analysis features.

**Ease of Deployment:** The availability of software or hardware appliances enhances ease of deployment. The number of scenarios requiring custom workflows is typical of this type of product, but scenarios requiring data handling that were evaluated often relied on SQL queries.

**Scalability and Performance:** The product benefits from an efficient data model that pushes significant processing to the data tier. However, configuration to support scalability and performance can be more complex than for other products.

## Hitachi ID Systems

This IAM suite vendor's primary product is Hitachi ID Identity and Access Management Suite, which is composed of three modules:

- Identity Manager
- Password Manager
- Privileged Access Manager

The products can be purchased separately, with Identity Manager capable of satisfying IGA requirements. All three modules are deployed as a single platform 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 automated fulfillment (provisioning) and policy-based administration.

**Identity Life Cycle:** Integrated reference builds (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, with the unique ability in this market to leverage social identity for anonymous user self-registration.

**Entitlements Management:** Provides the basic entitlements management features expected of IGA tools; however, administrative maintenance of account metadata is not directly supported, so the handling of multiple account types requires a work-around.

**Access Requests:** The interface for access requests has been enhanced and continues to provide users with good control over requests, but the overall experience remains linear and IT-focused. The ability to compare users is limited to reports and the only way to copy access from one user to another is through a "model after" feature.

**Workflow:** The included corporate reference build provides a predefined workflow model, with solid support for the most common workflow needs, requiring only minor configuration to satisfy most scenarios (see definition for this capability). 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 product supports a two-layer role model through a combination of user classes and roles, 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 new features, such as the ability to display entitlement assignment metadata (e.g., expiration dates) in tasks and for reviewers to delegate individual items or partial tasks. Electronic signatures are supported in the form of password prompts for task submission.

**Fulfillment:** Provides a highly flexible fulfillment engine with one of the largest connector libraries in the market. All connectors, including those for complex applications, are available as part of the base product. There is a built-in framework for manual fulfillment with numerous connectors for ITSM tools included.

**Auditing:** The reporting system can detect a broad range of integrity constraint exceptions. These report results can be fed back into the workflow system to generate predefined requests that behave like audit cases to facilitate remediation.

**Reporting and Analytics:** The product provides a generous collection of built-in reports, including some new reports for desirable metrics, but there is no report designer provided; custom reports are written as Python scripts. Analytics are delivered via reports, and the role-mining reports are noninteractive.

**Ease of Deployment:** Identity Express (corporate, B2B and B2C) reference builds 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.

**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.

## **IBM**

IBM Security Identity Governance and Intelligence (IGI) 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.
- **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 cloud applications. The product is a good choice for global organizations with complex processes that require automation along with governance that can be extended (through an integrated business activity model) to applications with complex authorization models. The solution is delivered as a virtual appliance for multiple hypervisors to simplify on-premises or cloud deployment.

**Identity Life Cycle:** Only authoritative source (employee) scenarios are supported adequately. Contractor and delegated administration (business partner) scenarios require 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.

**Entitlements Management:** The entitlements data model supports deep insight into fine-grained entitlements for complex applications (with built-in support for SAP and others) that can be tied to a business activity model. There is also a dashboard for 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 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.

**Workflow:** There is no suitable default workflow to support the standard, four-stage request approval workflow, so assembly 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 now supported directly in workflow configuration.

**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 bind roles 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 definition for this capability), 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.

**Fulfillment:** IGI includes an extensive collection of connectors; 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.

**Reporting and Analytics:** Solid reporting and analytics support 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 are supported only through reports.

**Ease of Deployment:** Virtual appliance form factor greatly simplifies deployment and supports pattern-based deployment of multiple instances; however, configuring the product can be complex, occasionally requiring compiled Java code in situations where other products rely on scripting.

**Scalability and Performance:** Makes good use of clustering for the application and data tiers, although a directory server is still used for the identity repository. Strictly event-driven design for resource-intensive tasks supports the finely tuned allocation of processing to specific nodes.

## **Micro Focus (NetIQ)**

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

- NetIQ Identity Manager
- NetIQ Identity Governance

Micro Focus is continuing its transformation of IGA products that will eventually position Identity Governance as the core of its IGA offering. In the meantime, Identity Manager remains the core, and it's made up of the following modules:

- 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)

**Identity Life Cycle:** Managing the synchronization of identity records with HR systems is accomplished entirely through driver configuration. However, support of other scenarios for contractors, delegated administration (business partners) and self-registration requires significant assembly. There is excellent support for managing identities of robotic process automation (RPA) bots.

**Entitlements Management:** Identity Governance provides an excellent foundation and flexible schema for managing entitlements, with good tools for discovery and enrichment.

**Access Requests:** Identity Manager provides a simple, intuitive and uncluttered single-page interface for creating access requests.

**Workflow:** Identity Manager's highly flexible workflow engine enables the assembly of workflows to accomplish all of the expected scenarios, although non-SOD policy checks must be added to workflow individually. There is even 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.

**Fulfillment:** The Identity Manager driver framework is powerful and highly 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.

**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.

**Reporting and Analytics:** Reporting and analytics have been improved significantly with the addition of integrated role mining, as well as a generous collection of useful metrics.

**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 Manager 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.

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

## **Microsoft**

Microsoft Identity Manager (MIM), formerly known as Forefront Identity Manager (FIM), is included with Microsoft Enterprise Mobility + Security (EMS) suite and as part of Azure AD Premium. The role of MIM in Microsoft's IAM portfolio is transitioning toward that of acting as a bridge between Azure AD services and on-premises applications. MIM still provides basic IGA capabilities (including governance features provided through the B HOLD module), but Microsoft has indicated that future development will add functionality on the Azure AD platform.

**Identity Life Cycle:** There is basic support for employee and contractor identity life cycle scenarios, while delegated administration and self-registration would require customization. These features are on the roadmap for delivery through Azure AD B2B and B2C capabilities. Configuration of supported patterns is more complex than for other products.

**Entitlements Management:** The lack of a robust entitlement data model is a significant area of weakness for MIM. Handling entitlements requires extension of the base schema in the products "metaverse" and entitlement assignments for specific applications are managed as separate multivalued attributes on identities.

**Access Requests:** MIM provides basic access request capabilities for group memberships, which can trigger account creation according to outbound synchronization rules. The access request experience is split between the MIM portal

for on-premises applications and Azure AD portal for cloud applications. There is no user comparison feature, and only requesters can cancel requests after submission.

**Workflow:** MIM uses Windows Workflow Foundation as the workflow engine, which provides the basic tools necessary to configure multistep approval workflows.

Customization is needed to support common approval workflow features, such as delegation and forwarding requests to different approvers.

**Policy and Role Management:** The BHOLD module provides only basic elements needed for role-based and policy-driven administration, with org unit objects behaving similar to business roles and role objects behaving similar to technical roles in a two-layer enterprise role management framework. However, several important features are missing, including flexible policies for role assignment and ability to preview changes to roles and policies.

**Access Certification:** The BHOLD module provides only minimal support for access certifications (called attestations in BHOLD) to be performed for sets of users with access to BHOLD-managed applications. Most access certification scenarios are not supported with BHOLD, although some certification types for privileged access, application access assignments and group memberships are available in Azure AD.

**Fulfillment:** MIM provides basic support for provisioning via built-in management agents that include some flexible connectors. Azure AD extends provisioning to support cloud applications via built-in connectors and SCIM protocol support.

Supporting manual fulfillment requires customization.

**Auditing:** Toxic combinations of permissions can be defined for BHOLD-managed applications only. Support for other types of policies is limited, and there is no case management mechanism available for orchestrating remediation.

**Reporting and Analytics:** MIM and Azure AD provide only minimal reports relating to password management, group management and sign-in activity. Neither MIM nor Azure AD provides report builders, so customers are expected to export data and use System Center Data Warehouse or PowerBI for most reporting.

**Ease of Deployment:** Azure AD is a cloud service, but MIM (along with the BHOLD module) is deployed as on-premises software. Although the depth of MIM's support for IGA use cases is limited, MIM is often more difficult to configure for IGA scenarios than other products — many common IGA scenarios are likely to require customization.

**Scalability and Performance:** MIM components can be installed on separate servers, but other indicators of scalability and performance of IGA tools, such as granular control over task execution or automated handling of archival data, are not present.

**Omada**

Omada's primary product, Omada Identity Suite, originally used Microsoft Forefront Identity Manager (now known as Microsoft Identity Manager) Synchronization Service as its provisioning platform. However, it has been extended significantly to emerge as a stand-alone IGA suite, with its own provisioning services. The product is built around a Base Server that can be extended with several modules that are packaged in three delivery models:

- Essentials Edition — Governance and basic connectivity modules.
- Professional Edition — Builds on the Essentials Edition with Identity Lifecycle (ILM), Access Management (AM), Business Administration modules and Connector Packages.
- Enterprise Edition — Builds on the Professional Edition with deep customization, enhanced workflow and approval automation, extended provisioning, password reset, custom extensions, and APIs and advanced connectors.

The Essentials and Professional Editions of the product are available for on-premises and cloud deployment, whereas the Enterprise Edition is available for on-premises deployment. The Enterprise Edition is required to fulfill the most typical IGA requirements, because the other editions are targeted at customers with the simplest requirements. All modules are deployed as a single platform and deliver a consistent user experience.

**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. Assembly is required for workflows to handle contractor expiration and delegated administration scenarios.

**Entitlements Management:** The Application Onboarding feature has been enhanced to manage all key aspects of importing accounts and enriching accounts from target systems. There is also support for modeling entitlements from applications with complex authorization models.

**Access Request:** Omada provides a free-form, single-page shopping cart approach that supports all access request scenarios, including request templates.

**Workflow:** The unique survey approach 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:** 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:** The survey feature offers full support for all scenarios, including the relatively unique ability to edit attribute values in certification tasks, which is useful for reviews of the entitlements catalog and users or entitlement assignments with expiration dates. Also supports electronic signatures in the form of a password prompt.

**Fulfillment:** Built with a highly extensible connector framework that supports native connectors, as well as the embedded Microsoft Identity Integration Server (MIIS) synchronization engine. A unique classification policy concept can manage the logic required to derive complex attribute values, such as directory containers.

**Auditing:** Multiple types of audit policies are defined via central console, although many policies may require 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.

**Reporting and Analytics:** The product's reporting and analytics features are built around Microsoft SSRS, but the implementation of IGA-specific analytics is incomplete. Role mining has been enhanced to include a workflow-driven process for managing role proposals.

**Ease of Deployment:** The product can be complex, with separate enterprise, database and provisioning server components and requirements for multiple databases. A lot of configuration work occurs at the database level, requiring SQL queries and creation of views. There is support for scripted deployment, and a configuration transport feature supports collaboration and staged deployment.

**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, a Quest Software company, is an IAM-focused brand that offers One Identity Manager as its IGA solution. One Identity Manager is available as a traditional, on-premises solution, as well as a managed service that is bundled with One Identity Cloud Access Manager. One Identity Manager is built on a Microsoft .NET platform. It's a good choice for large enterprises that need a balanced governance and automation solution, especially those organizations that have significant expertise with Microsoft .NET technologies.

**Identity Life Cycle:** Support for employee and self-registration (consumer) scenarios is provided, but contractor and delegated administration scenarios are not supported directly and require setup of form and workflow assets to support a sponsorship-and-expiration pattern. However, there's a built-in organization model that helps with delegated administration.

**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, which may impose more administrative burden than other tools.

**Access Requests:** The shopping cart interface for access requests functions well. A complete set of controls enables users to inspect their own access, compare users, review request history and cancel requests.

**Workflow:** The four-stage policy and approval process is supported by an included template. Overall support for policy checks is good, and there is now a possibility to integrate multifactor 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. Configuration certification of privileged accounts is more complex than for other products. It's now possible to integrate multifactor authentication for submitting certification tasks that require electronic signatures.

**Fulfillment:** There is solid support for automated fulfillment through a good collection of connectors provided with the base product. Connect for Cloud supports fulfillment for more cloud applications than other IGA products; however, support for manual fulfillment requires workflow assembly. There is little support for proxy-based fulfillment across security zones.

**Auditing:** The HelpDesk subsystem can be used to handle audit cases generated from a variety of policy types, but only SOD controls appear to be supported systematically. A company policy module is available to perform arbitrary checks of the integrity of identity data and accounts.

**Reporting and Analytics:** There is a good selection of built-in reports and dashboards, with interesting 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.

**Ease of Deployment:** The product provides a unified platform for IGA, with good support for internal change tracking. Multiple interfaces are involved in various aspects of configuration, including a non-web Windows graphical UI (GUI).

**Scalability and Performance:** Full and thoughtful support for scalability and performance considerations through the product's "JobService" architecture enable flexible workload distribution, although sizing guidelines suggest the product may be CPU-intensive.

## Oracle

Oracle Identity Governance (OIG) delivers a unified platform for full IGA functionality, which can be purchased as a stand-alone product or as part of the Oracle Enterprise Identity Services Suite. Oracle also provides some IGA functionality through Oracle Identity Cloud Service (IDCS), which is primarily focused on supporting Oracle's application portfolio and is intended to augment the on-premises OIG product in hybrid on-premises and cloud IGA scenarios. OIG is especially well-suited to global enterprises with mature and complex processes for access administration and significant requirements for the automation of account management.

**Identity Life Cycle:** Good support for most of the common identity life cycle scenarios (employees, contractors and self-registration), with an organization model to support delegated administration. However, establishing 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.

**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 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. Policy coverage is excellent, and there is built-in support for time-limited workflow approvals as well.



**Access Certification:** Excellent support for almost all certification campaign types, including certification of the entitlements catalog. Electronic signatures are supported for certification task submission.

**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. There is an extensive collection of connectors, but they are licensed separately from the base product.

**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.

**Reporting and Analytics:** Oracle Business Intelligence is included with the product to provide a powerful engine for reporting and analytics. An exhaustive 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, the product requires more compiled Java code than other products, although there is some support for Groovy scripting.

**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 on-premises, governance-oriented IGA solution, which is delivered as the IdentityIQ Governance Platform with two modules:

- SailPoint Compliance Manager
- SailPoint Lifecycle Manager

Provisioning functionality is included as part of Lifecycle Manager, although connectors are included as part of the IdentityIQ Governance Platform. SailPoint also offers an IdentityIQ Password Management module, as well as a variety of IdentityIQ Integration Modules covering mobile device management (MDM), third-party provisioning, service catalog and service desk. SailPoint IdentityIQ is used most often by organizations with significant regulatory obligations requiring a governance-oriented approach to IGA.

**Identity Life Cycle:** Base identity life cycle processes for employees are supported well, but processes for contractors and business partners require more assembly than should be necessary. Self-registration is provided out of the box.

**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 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. Good controls enable users to view and cancel requests by and for them.

**Workflow:** The default workflow for access requests supports the common four-stage approval process with minimal configuration. The most common features (e.g., delegation, escalation and notification) are configurable. 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, but control over how roles are detached when policies no longer apply requires modification of an analysis workflow. Expiration dates for entitlement assignments are not supported well.

**Access Certification:** Excellent support for all access certification campaign scenarios. Electronic signatures for certification tasks are provided as a configuration option.

**Fulfillment:** Comprehensive support for manual and automated fulfillment. There are built-in integration modules for multiple ITSM tools. All of the most desirable connectors are provided as part of the base product. The AD connector can manage multiple domains in a forest as a single application.

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

**Reporting and Analytics:** Out-of-the-box reporting and analytics are strong, with some useful metrics included. The object model requires data export in most cases for reporting, although web services interfaces are available for directly querying system objects, if desired.

**Ease of Deployment:** Benefits from being built as a unified product, but there is underlying complexity related to database and application server dependencies.

Configuration requires BeanShell (Java syntax and object model) scripting, some compiled Java code and direct manipulation of some XML objects.

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 demonstrated the ability to squeeze out sufficient performance and scalability for enterprise needs.

## SailPoint (IdentityNow)

IdentityNow is SailPoint's cloud-based solution for IGA, which is delivered as a multitenant, SaaS solution. IdentityNow's IGA functionality is delivered through the following modules:

- SailPoint IdentityNow for Provisioning
- SailPoint IdentityNow for Access Certification
- SailPoint IdentityNow for Access Request

An IdentityNow for Password Management module is available to cover SSPR and password synchronization. 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.

Identity Life Cycle: IdentityNow can handle only the employee identity life cycle process adequately, although 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: Extensible schema for the entitlements catalog and excellent handling of applications with complex schemas. There is built-in support for account mappings based on a custom taxonomy.

Access Requests: Limited functionality for access requests that allows only self-request for access profiles within applications.

Workflow: The workflow is fixed and limited to one approval level (resource-owner approval). There is no ability to assemble workflows to support the most common workflow features, such as multiple approval steps and delegation, although escalation support and ITSM integration have been improved slightly.

Policy and Role Management: Supports only simple roles that can be defined to contain access profiles.

Access Certification: Only basic user-level (organization chart) access certification is supported, with limited ability to filter entitlements included in such certification campaigns.

Fulfillment: IdentityNow uses the same connector framework as IdentityIQ, so all of the most desirable connectors are provided as part of the base product. However,

there is only basic support for manual and automated fulfillment and a lack of flexibility that requires involvement of SailPoint DevOps or professional services to address some scenarios.

Auditing: There is no support for SOD or other types of audit policies.

Reporting and Analytics: Offers only basic reporting through a set of built-in reports that expanded slightly during the past year. However, there is still no support for creating custom reports in the tool or even using external reporting tools.

Ease of Deployment: IdentityNow was built from the ground up as a multitenant SaaS 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 that is desirable for enterprise deployments.

## SAP

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

- SAP Access Control — A SOD controls monitoring product
- SAP Identity Management
- SAP Cloud Identity Access Governance
- SAP Cloud Identity Provisioning

SAP Access Control is used most often for governance over SAP's business applications, although non-SAP applications are supported as well. SAP Identity Management provides virtual directory capabilities for account management and attribute synchronization in a heterogeneous environment. The SAP Cloud Identity services (Access Governance and Provisioning) are used by customers primarily to assist with managing applications SAP applications hosted in the cloud — these services were not evaluated as part of the Critical Capabilities. 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, as well as basic support for contractor scenarios. There is little support beyond that for business partner or consumer scenarios.

**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 24 languages is built in for the administrative and end-user interfaces.

**Workflow:** Overall workflow support is complete, but configuration requires significant assembly. 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 controls monitoring by adding some enterprise role management and policy-driven assignment of access. However, enterprise role management functionality is not sophisticated and requires significant assembly and occasional customization to support common scenarios.

**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 required to enable electronic signatures for certification tasks.

**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.

**Auditing:** SAP Access Control provides complete support for process-driven SOD and critical access policies with a case management interface available for remediation. The case management concept is not extended to other types of policy violations, and non-SOD policies can be complex to define.

**Reporting and Analytics:** 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 good selection of built-in reports, especially covering risk analytics, but metrics are missing.

**Ease of Deployment:** The reliance on multiple products to support IGA, each with their own deployment considerations, and 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's Security Manager is a full-featured IGA service delivered on a cloud platform that extends the scope of IGA to include functionality usually associated with DAG and SOD controls monitoring products. 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.

**Identity Life Cycle:** All four identity life cycle patterns are well-supported, 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.

**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.

**Workflow:** Superior features more common in SOD controls monitoring than IGA, most notably the ability to change the contents of in-flight requests.

**Policy and Role Management:** Outstanding support for role management bridges the gap between enterprise and application role management with the ability to 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.

**Fulfillment:** Combines support for homegrown and OpenICF connectors, with enhanced extensibility through RPA and Apache Camel integration. A rich selection of additional connectors can be purchased separately as premium editions of the product, although basic IGA functions are supported for premium connectors at no charge.

**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 premium modules. Provides a case management interface that can be used to assign follow-up for the full range of audit events.

**Reporting and Analytics:** The service is driven heavily by analytics, and the built-in analytics include useful advanced metrics. 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).

**Ease of Deployment:** Cloud is the preferred deployment approach, although there are appliance-based deployment options, including AMIs and CloudFormation templates available for deployment in AWS. There is also the possibility for traditional on-premises deployment that sacrifices much of the deployment ease.

**Scalability and Performance:** Thorough approach to supporting scalability and performance, which involves clustering, the ability to dedicate nodes to specific tasks and continuous archiving of historical data.

## Context

IGA software can be complex and expensive, often representing the largest investment for IAM programs, while also presenting the most deployment risk. There are numerous IGA capabilities, and organizations often require features from most of these capabilities to achieve their objectives for exercising and demonstrating control over user access in heterogeneous environments.

Gartner recommends that organizations pursue a governance-first approach when deploying IGA functionality to exploit maximum value from IGA capabilities in a manner that minimizes deployment risk during early project phases (see "IGA Best Practices: Governance First, Automated Provisioning Later"). Automated provisioning is the most difficult, expensive and unpredictable part of IGA deployment projects. Organizations that focus on provisioning too much in the early deployment phases are front-loading their projects with excessive risk and are likely to struggle. IAM leaders must manage expectations for provisioning, based on the recognition that most organizations automate fulfillment for only 15% to 25% of the applications covered by their IGA deployments. Fulfillment for the remaining applications is handled through the generation of service tickets by the IGA tool and by human intervention.

Gartner suggests that organizations adopt more homogeneous processes for access administration to avoid customizations for specific application integrations. Recent

Gartner research has focused on best practices for identity life cycles (see "IGA Best Practices: Establish an Identity Perimeter With Identity Life Cycle Processes"), approval workflows for access requests (see "IGA Best Practices: Standardize Approval Workflows for Access Requests") and enterprise role management (see "IGA Best Practices: Take Control of Enterprise Role Management"). This assists clients with enhancing control over user access and improving the effectiveness of their IGA implementations.

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 101 scenarios drawn from common client needs and process guidance presented in Gartner research. They were asked to explain how their products would be configured 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, 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.
- 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 repositories. Direct fulfillment is called "provisioning," and it connects to account repositories, whereas indirect fulfillment uses a workflow or external system as proxies for completing changes.
- Password Management — Enables SSPR, as well as synchronizes passwords among different account repositories. Password management is a capability of IGA tools, but not a critical capability, because stand-alone password management tools provide better support for this, and modern IGA deployment practices are incompatible with IGA tools for password management.
- 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.
- Reporting and Analytics — Provide a mechanism to report on and deliver deeper insights into the data available to an IGA tool. Role mining is a typical analytics scenario for designing and optimizing role definitions that all IGA tools must support; however, analytics can be applied to numerous other scenarios. For example, analytics can be applied to operational data to evaluate quality of service (QoS) and adherence to SLAs, as well as to identify anomalous usage patterns.

## 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. The processes supporting employee relationships are usually augmented with additional processes for managing nonemployees (e.g., contractors), business partners (e.g., vendors) and customers. 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 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 (e.g., 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 (e.g., 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 ended 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 ended 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** — Allows 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 G2C 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 source 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 consume and even understand 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.

Entitlements management for IGA tools was evaluated using scenarios that covered the following functionalities:

- 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) 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; creating synthetic entitlements; and by extending the schema.
- Integration — Integrating management of entitlements with external tools, such as coordinating account coverage with a privileged access management (PAM) tool.

## Access Requests

This interface enables end users to request access to resources, such as accounts, roles and entitlements, and has a major impact on the user experience. The main goal is to provide a business-friendly access request experience that enables users to request access to a broad range of resources.

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 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 the following criteria:

- Business-friendly access request experience allowing:
  - End users to request access for themselves
  - Managers to request access for subordinates
  - Managers to copy access from one user to multiple users
  - Feedback to requesters about dependencies and potential policy violations prior to request submission
  - Creation of templates for frequent access requests
- Ability of requester and recipient to view request status and change or cancel in-flight requests
- 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 and the most common European languages (French, German and Spanish)

## 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 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 a 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, he or she 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 known as enterprise roles) are often focused on grouping people to represent organizational structures (e.g., relationships, departments, locations and authority levels) to make policy administration more efficient.
- Technical roles — Roles in the resource layer (sometimes known 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 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.

### Access Certification

Access certification is the process of requiring people such as managers and resource owners to certify the access that users have to resources on a periodic basis to ensure that access is still reasonable. Access certification helps with regulatory compliance and cleaning up accumulated access.

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 such as 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 (e.g., expiration dates) in certification tasks

- Support for reviewers to apply electronic signatures to certification tasks, as required by some regulations

## 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 (e.g., AD and other Lightweight Directory Access Protocol [LDAP]) directories; email systems (e.g., 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 15% to 25% of infrastructure systems and business applications covered by their IGA deployments (see "IGA Best Practices: Governance First, Automated Provisioning Later").

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, identity bridges or IAM as a service (IDaaS) tools are emerging as partial solutions to provisioning and deprovisioning for cloud applications as an alternative 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 transition between indirect and direct fulfillment for target systems

## 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

## Reporting and Analytics

Reporting and analytics 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 by built-in reports, custom reports, dashboards for metrics and data modeling.

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.

Increasingly, IGA products are using powerful analytics tools to satisfy reporting requirements and to 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 and statistical methods to generate insights 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.

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.

Analytics are often applied to operational data generated by the IGA tool for the purpose of evaluating QoS and adherence to SLAs. Analytics can also be applied to identity data to evaluate attribute completeness and quality. Finally, analytics can be applied to authentication- or authorization-related log data generated by (and imported from) external systems to evaluate user behavior. This provides input to

governance (e.g., whether access was used, when it was last used and how often it was used during certain time periods) or to identify anomalous usage patterns. 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. The following criteria were used to evaluate the reporting and auditing capability:

- 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-relational database management system (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 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
- The relative balance between configuration and more-involved assembly or customization in covered scenarios, favoring:
  - 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 (e.g., 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 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

Organizations with more than 10,000 employees often have complex processes for managing large numbers of users and entitlements with strict compliance requirements.

The scalability and performance capability is weighted heavily, because the volume of account and entitlement data is often a significant obstacle that must be overcome to succeed with deployment. Fulfillment and policy and role management are 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. Entitlements management and auditing are valued, because these organizations are often subject to multiple stringent regulatory regimes that make compliance a business imperative.

Scalability and performance become even more critical for the largest global enterprises (those with more than 50,000 employees and potentially thousands of applications). It may become a hurdle that must be overcome by products before any other capabilities can be considered.

#### Midsize or Large Enterprise

Organizations with fewer than 10,000 employees often possess simpler environments and require a good balance between provisioning and governance, with low TCO.

Ease of deployment is weighted most heavily because midsize-to-large 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. Access requests and workflows are 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 process frameworks they can adopt, rather than customize.

#### Governance-Focused

IGA deployments 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 — entitlements management, access certification, policy and role management, access requests, workflow, and auditing — are most important for governance-focused deployments. This starts with entitlements management, because the ability to capture and model entitlements management from a broad range of systems is critical to the proper functioning of other governance processes.

Access certification is important because, in many cases, it's required for regulatory compliance, and it provides a way to clean up accumulated access. Policy and role management is important, because it simplifies the environment and standardizes the enforcement of policies. Reporting and analytics are valued, because of their ability to support compliance reporting and provide insight into the effectiveness of controls.

#### 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 integrate with external account repositories. Identity life cycle is important, because HR feeds and nonemployee management 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

Microsoft has been added this year as a result of the vendor starting to build new, cloud-based IGA capabilities.

### Dropped

No vendors were dropped since last year.

## Inclusion Criteria

To qualify for inclusion, vendor organizations must:

- Have booked total revenue of at least \$22 million for IGA products and subscriptions (including maintenance revenue) for 12 consecutive months (fiscal year) between 1 January 2016 and 30 September 2017. Or they must be mentioned as considered vendors for evaluation in 15% of Gartner inquiries in this market between 1 October 2016 and 30 September 2017.
- Sell or support their own IGA product or service developed in-house, rather than offer it as a reseller or third-party provider.
- Have sold their IGA product or service to customers in different vertical industries (vendors who only sell their product within a particular industry or vertical are excluded).

To further qualify for inclusion in the 2018 Critical Capabilities for Identity Governance and Administration, the vendor's IGA product/solution must offer:

- An integrated identity repository that masters 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-user-friendly UIs 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 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 specification and execution of access certification campaigns covering identities and entitlement assignments involving specified actors (e.g., managers and resource/application owners).
- Tools to reconcile data from target systems with IGA data for multiple, targeted technical environments (e.g., Windows, iSeries, UNIX/Linux, multiple applications and SaaS).
- Tools and connectors to automatically propagate changes to target systems (e.g., 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 architectures for the above, including a connector architecture for data collection and fulfillment actions.
- Products must be deployed for use with customer production environments for purposes consistent with objectives of IGA.

## Table 1: Weighting for Critical Capabilities in Use Cases

Enlarge Table

-



<b>Critical Capabilities</b>	<b>Global Enterprise</b>	<b>Midsized or Large Enterprise</b>	<b>Governance-Focused</b>	<b>Adaptive</b>
Identity Life Cycle	8%	8%	5%	15%
Entitlements Management	10%	5%	15%	10%
Access Requests	7%	14%	9%	10%
Workflow	7%	14%	5%	10%
Policy and Role Management	10%	5%	15%	10%
Access Certification	8%	7%	15%	10%
Fulfillment	10%	12%	2%	10%
Auditing	10%	0%	10%	10%
Reporting and Analytics	10%	5%	14%	10%
Ease of Deployment	5%	30%	5%	10%
Scalability and Performance	15%	0%	5%	10%
Total	100%	100%	100%	100%

As of June 2018

Source: Gartner (June 2018)

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 with 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

Enlarge Table

•

Critical Capabilities	AlertEnterprise	Atos (Evidian)	CA Technologies	Core Security
Identity Life Cycle	2.9	4.1	3.1	2.6
Entitlements Management	3.0	2.5	3.2	2.8
Access Requests	3.5	2.7	4.1	2.7
Workflow	3.4	2.8	3.1	3.5
Policy and Role Management	3.4	3.2	2.5	2.8
Access Certification	3.7	2.8	3.5	3.9
Fulfillment	2.7	3.1	3.6	3.3
Auditing	3.2	2.5	2.3	3.0

Critical Capabilities	AlertEnterprise	Atos (Evidian)	CA Technologies	Core Security
Reporting and Analytics	3.0	3.0	3.6	3.9
Ease of Deployment	3.1	2.5	3.3	3.0
Scalability and Performance	3.6	3.2	3.4	2.7

As of June 2018

Source: Gartner (June 2018)

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

Enlarge Table

•

Use Cases	AlertEnterprise	Atos (Evidian)	CA Technologies	Core Security
Global Enterprise	3.24	2.97	3.23	3.09
Midsized or Large Enterprise	3.18	2.85	3.39	3.12

Use Cases	AlertEnterprise	Atos (Evidian)	CA Technologies	Core Security
Governance-Focused	3.27	2.88	3.20	3.17
Automation-Focused	3.09	3.18	3.25	3.03

As of June 2018

Source: Gartner (June 2018)

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 October and November 2017 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.

By Brian Iverson, Kevin Kampman, Felix Gaehtgens



© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. If you are authorized to access this publication, your use of it is subject to the [Gartner Usage Policy](#) posted on gartner.com. 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 and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to

change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "[Guiding Principles on Independence and Objectivity](#)."

- [About](#)
- [Careers](#)
- [Newsroom](#)
- [Policies](#)
- [Site Index](#)
- [IT Glossary](#)
- [Gartner Blog Network](#)
- [Contact](#)
- [Send Feedback](#)



© 2018 Gartner, Inc. and/or its Affiliates. All Rights Reserved.

## Switching to Simplified Site

Your browser version is currently supported by Gartner.com. If you change to the simplified version of the site, some features will no longer be available to you.

[SWITCH](#)

Sort  
Sort  
Sort  
Sort  
Sort  
Sort  
Sort  
Sort  
Sort

