

Identity Governance and Administration

Nitish Deshpande
August 6, 2024



LEADERSHIP
COMPASS
2024

This Leadership Compass Identity Governance and Administration (IGA) provides an overview of the IGA market and a compass to help you find a solution that best meets your needs. It examines solutions that provide both identity lifecycle management and access governance capabilities. Solutions have been assessed based on certain defined required core capabilities that can support organizations in activities such as provisioning, management of entitlements, configuration and enforcement of policies, access certifications, access reviews and user self-service among other. It provides an assessment of the capabilities of these solutions to meet the needs of all organizations to monitor, assess, and manage these risks.

Contents

Executive Summary	4
Key Findings	6
Market Analysis	6
Market Size and Segmentation	9
Delivery Models	10
Required Capabilities	10
Leadership	14
Overall Leadership	14
Product Leadership	15
Innovation Leadership	18
Market Leadership	21
Products and Vendors at a Glance	24
Product/Vendor evaluation	28
Spider graphs	28
BAAR Technologies Inc – BAAR-IGA	30
Bravura – Bravura Security Fabric	33
Broadcom – Symantec IGA	36
Clear Skye – Clear Skye IGA	39
CoffeeBean Technology – CoffeeBean IGA	42
EmpowerID – EmpowerID IAM Suite	45
E-TRUST – HORACIUS IAM	48
Evidian – Evidian IGA for On-Premises solution, Evidian IDAAS Governance with Analytics capabilities	51
Evolveum – MidPoint	54
IBM – IBM Security Verify	57

Identity Plus – Cross Identity	60
ManageEngine – AD360	63
Microsoft – Microsoft Entra ID Governance	66
N8 Identity Inc – TheAccessHub	69
Netwrix – Netwrix Usercube	72
Nexis – NEXIS 4	75
Omada – Omada Identity Cloud, Omada Identity	78
One Identity – One Identity Manager and Identity Manager on Demand	81
OpenText – NetIQ IGA Suite	84
Oracle – Oracle Identity Governance Suite and Access Governance	87
Ping Identity – Ping Identity Governance	90
RSA – RSA Governance & Lifecycle, RSA Governance & Lifecycle Cloud	93
SailPoint – SailPoint Identity Security Platform	96
SAP – SAP Access Governance Solutions	99
Saviynt – Saviynt Identity Cloud	102
Soffid IAM – Soffid IAM	105
Systancia – Systancia Identity and cyberelements.io	108
Tools4ever – HelloID	111
Tuebora – Tuebora IAM Platform	114
ZertID – ZertID	117
Vendors to Watch	120
Avatier	120
Fisher International	120
Elimity	120
iC Consult/ Service Layers	120
Identity Automation	121
Imprivata	121
Kapstone	121
Memory	121
Monokee	122
Okta	122
Pathlock	122
Pirean	122

Simeio.....	123
Tenfold.....	123
TrustBuilder	123
WALLIX	124

Executive Summary

Identity Governance and Administration refers to the increasingly integrated Identity Lifecycle Management and Access Governance markets.

Identity Governance and Administration (IGA) products support the consolidation and synchronization of identity information across multiple repositories and systems of record such as Human Resources/Human Capital Management and other systems in an organization's IT environment. This ensures the user accounts in these connected systems are up to date. The identity information including user accounts, associated access entitlements and other identity attributes is collected from across the connected source systems for correlation and management of individual identities and pushed to the connected target systems, including information about user groups as well as roles and assigned entitlements through a centralized administration console, with a backchannel for gathering information for Access Governance purposes.

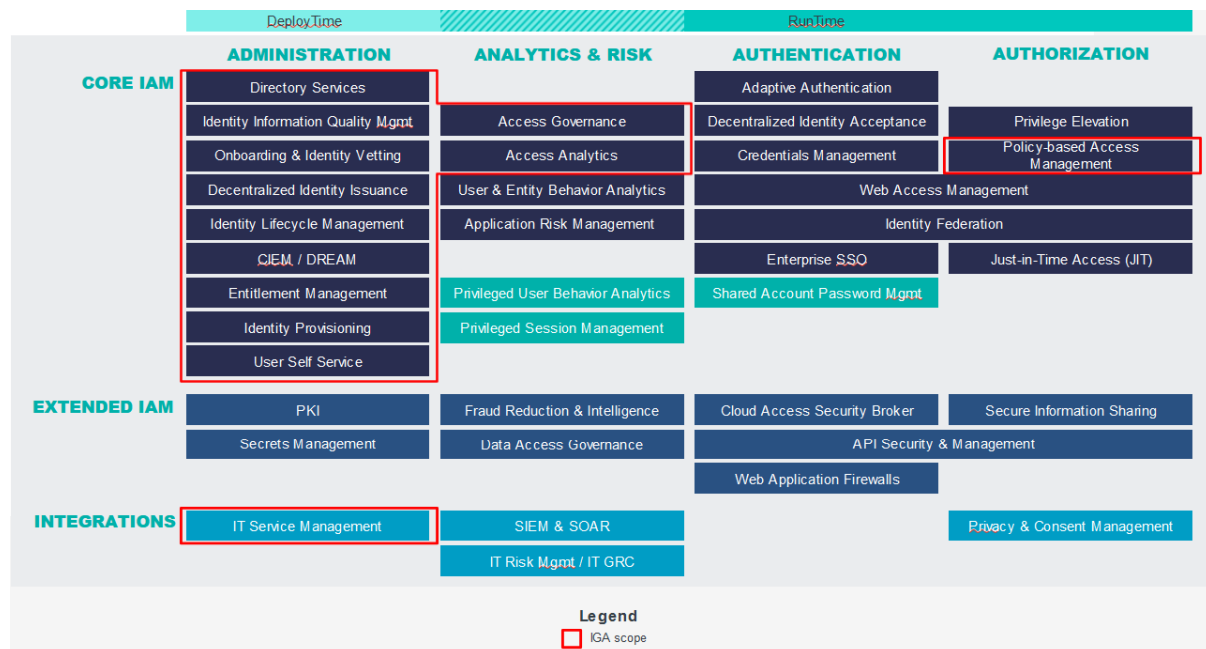


Figure 1: KuppingerCole Reference Architecture highlighting IGA related capabilities

Identity Governance & Administration (IGA) being one of the core disciplines within Identity & Access Management (IAM). It serves three main capability areas, which are:

- User Access Provisioning (UAP)
- Identity Lifecycle Management (ILM)
- Identity and Access Governance (IAG)

User Access Provisioning (UAP) deals with the management and assignment of permissions and access to users across the designated systems and applications in an IT infrastructure of the organization. UAP supports various activities such as creation, modification, and deletion of user accounts. Provisioning and deprovisioning of access can be done automatically based on the roles. This area is responsible for pushing out the changes from the IGA solution to the target systems.

Identity Lifecycle Management (ILM) handles the end-to-end process for human and non-human identities from their creation to deletion. This process is responsible for implementing workflows and management of entitlement process for Joiner, Mover, Leaver (JML) activities.

Identity and Access Governance (IAG) is the element responsible for ensuring user accounts have the right level of access based on their roles and permissions. IAG follows enforcement of policies and access governance principles to avoid any Segregation of Duties (SoD) violations and unauthorized access. This area supports access reviews, analytics, anomaly and outlier detection, and role management.

User Access Provisioning and Identity Lifecycle Management are integrated to provide a seamless approach to managing identities whereas Identity and Access Governance ensures the right policies are enforced to ensure compliance with regulatory requirements.

This approach can also be found in the market with vendors specializing in particularly IAG capabilities. These vendors are targeting the niche market where organizations are looking at having only access governance features in a solution and not the full IGA package, or (more rarely) only UAP and ILM.

Thus these vendors can be classified as either comprehensive IGA vendors, as provisioning-focused, or as governance-focused. The vast majority of the vendors today offer combined capabilities to qualify as IGA vendors, while only a few, especially the new entrants, provide Access Governance or reporting capabilities to cater to specific needs of the organizations, mainly small and medium sized. This KuppingerCole Leadership Compass provides an overview of the IGA market with notable vendors and their products in the market. The vendors in this report offer a range of deployment options varying from on-premises (including the ability to host these by the customer itself or a Managed Services) or IDaaS, with IDaaS being either multi-tenant or single-tenant.

The top drivers for acquiring IGA solutions remain enhancing security, regulatory compliance, risk management, improved user experience, and operational efficiency by leveraging latest AI and machine learning technologies. In this year's report, we have seen vendors invest heavily in automating certain capabilities and using AI and machine learning for recommendation-based features. The IGA market was already mature but with these new

advancements, we have a new perspective on how vendors are managing identities, risks, analytics, and provisioning.

Typical buyers for IGA products are spread across various industry verticals. This trend can be seen mainly in sectors which require a high level of compliance with regulatory authorities. Finance, healthcare, manufacturing and industrial companies, technology firms, and government institutions are some of the main sectors seeking IGA products. The organizations deploying IGA solutions commonly range from mid-market to very large organizations. IGA products deliver strong capabilities in providing a centralized view of who has access, who provided the access, and who has access for how long. Companies in healthcare, finance and government sector which have critical data and strict regulatory compliance requirements rely on IGA solutions for governing identities and managing their life cycle. The IGA market has a global footprint and is not limited to a specific region.

This Leadership Compass with its focus on comprehensive IGA offerings will be followed by a Leadership Compass on Access Governance which will evaluate vendors based on core access governance capabilities. In addition, there is the Leadership Compass on Identity Fabrics, covering comprehensive IAM solutions spanning IGA, Access Management, and other capabilities.

With this series of Leadership Compasses and accompanying Buyers' Compasses, we aim to provide CISOs and security leaders responsible for IAM the most practical and relevant information that they need to evaluate technology vendors based on the specific use-case requirements, whether these are IGA-driven, provisioning focused, governance focused, focused on comprehensive IAM suites such as Identity Fabrics or a combination of these.

Key Findings

- This Leadership Compass evaluates 30 IGA product vendors, with about one fifth being new in the analysis, compared to the previous edition.
- The IGA market is growing, and although maturing it continues to evolve by leveraging AI and machine learning for various capabilities.
- The level of identity and access intelligence has become a key differentiator between IGA product solutions.
- Automation is still the key trend in IGA to reduce management workload by automating tasks, providing recommendations, and improving operational efficiency.
- IGA is essential to business as a strategic approach to ensure overall IT security and achieve regulatory compliance.
- Leading IGA vendors are increasingly focusing on supporting interoperability with other products and services through the provision of secure APIs.
- The Overall Leaders are Saviynt, EmpowerID, SailPoint, IBM, Ping Identity, Broadcom, Oracle, One Identity, Identity Plus, OpenText, RSA, Omada, SAP, Netwrix, BAAR-IGA, CoffeeBean Technology, ZertID, Microsoft.

Market Analysis

The IGA market continues to grow, and although at a mature technical stage, it continues to evolve in the areas of intelligence and automation. Today, there still are some organizations either looking at replacements of UAP and ILM or IAG, but most are opting for a comprehensive IGA solution that simplifies deployment and operations and to tackle risks originating from inefficient access governance features.

Identity Lifecycle Management remains a core IAM requirement, but Identity and Access Governance (IAG) is equally important to be compliant with regulatory frameworks and the need for enforcing the least privilege principle for mitigating access-related risks due to over entitlements across the IT infrastructure. IGA can provide powerful reporting and convenient dashboarding as well as advanced capabilities that build on AI and/or machine learning techniques enabling pattern recognition to deliver valuable intelligence for process optimization, role design, automated reviews, and anomaly detection. Current IGA solutions are made up of established and emerging capabilities. They are as follows:

Established capabilities: This category relates to the capabilities which are mature and present in the IGA solutions from a long time. Some of the major established capabilities but not limited to are as follows:

- **Identity Provisioning:** This area involves providing and revoking user accounts with right access and permissions based on their roles and responsibilities. This process is automated via defined processes and predefined policies and based on connectors to target systems or via manual fulfilment that is controlled via service tickets or other means, either directly or via integration to ITSM solutions.
- **Identity Lifecycle Management:** This deals with the overall management of identities from their creation to deletion. It is where user-centric workflows for managing identities are defined and processes such as JML reside. Tasks related to onboarding, offboarding, and updating the identity information based on change of roles and responsibilities are supported in this area. Identification, monitoring and if required deletion of inactive and orphaned accounts is also a crucial aspect of lifecycle management to avoid unauthorized access risks.
- **Access and Review support:** Regular review of access rights to mitigate access risks is a critical part of the IGA solution. Further capabilities such as Segregation of Duties (SoD) management and access risk analysis, based on detailed logs for audit trails, and role management contributes to ensuring the identities are compliant with various regulatory compliance requirements.

Emerging capabilities: We evaluate the innovation leadership category based around some these but not limited to these capabilities. Vendors are investing to enhance operational efficiency and security requirements. Some of the emerging capabilities in IGA solutions are:

- **Integration of AI and Machine Learning:** IGA vendors are using AI and Machine Learning for tasks such as user behavioral analytics, access recommendations, access reviews and SoD policy violations. Integrating these new technologies has resulted in increasing the overall operational efficiency by replacing manual access reviews and being proactive for identification of access risks.

- **Workflow and Automation:** In general, vendors are also focusing on automating administrative tasks to reduce workload.

IGA solutions can be deployed through various models. At KuppingerCole Analysts, we look at IGA solutions regardless of the deployment model, but flexible deployment models are rated more positively. Some of the deployment models provided by IGA vendors are:

- **Identity-as-a-Service (IDaaS):** This includes vendors who support hosting and management of the IGA solutions on either private cloud or public cloud. This is a preferred approach for organizations aiming at scalability and rapid deployment. However, organizations in finance and healthcare sector running on legacy on-premises systems are still hesitant to move to cloud solutions citing security issues.
- **On-premises:** This is the traditional model and the preferred approach for organizations wanting full control over the IT infrastructure. This model also allows the organizations to implement a high number of customizations. On-premises deployment is mainly preferred by organizations facing strict regulatory requirements.
- **Hybrid deployments:** This model allows the IGA solutions to be deployed in a hybrid model to leverage the best of cloud and on-premises deployment models. This approach offers flexibility by distributing deployment of capabilities on cloud and on-premises. Most commonly, hybrid deployments are used when IDaaS is preferred but security requirements or complex integration of target systems demand some components running on-premises.

One of the adoption patterns we have observed in the market is a managed service supporting ILM, and Access Governance is run by and within the organization itself to retain absolute control over governance functions. There are several other adoption patterns witnessed in the market such as:

- Customers' immediate requirements are limited to either ILM or IAG but do not demand a comprehensive IGA solution. This scenario is not observed frequently.
- Modernization and moving from low-end approach such as Microsoft Active Directory-based propagation of accounts and users to comprehensive and mature IGA solution.
- Another aspect of modernization is whether a capable UAP or ILM tool is already in place and IAG capabilities are added to complete the IGA requirements.
- In most other cases where there is a need for UAP, ILM and IAG, IGA products are preferred.

It is important that organizations scope their IGA requirements well before starting to evaluate products that differ in the strength of functionalities.

Based on these adoption trends, changing customer priorities, and deployment patterns, we decided to center on Identity Governance and Administration holistically in this leadership compass to help security leaders identify relevant IAM market segments and subsequently shortlist the most appropriate technology vendors based on their immediate IAM priorities. In this Identity Governance and Administration Leadership Compass, the primary focus is on the vendors that offer both Identity Lifecycle Management and Access Governance

capabilities, either as a common product or separate but integrable product components to deliver capabilities across the IGA spectrum.

Market Size and Segmentation

KuppingerCole research predicts that the Compound Annual Grow Rate (CAGR) of the Identity Government Administration Market Segment will be 19.6%, lifting the market volume to 5.75 billion US dollars by 2026. For comparison, Privileged Access Management (PAM) has a CAGR of 17.7%, Customer Identity Access Management (CIAM) has a CAGR of 19.9% and the Policy Based Access Management has a CAGR of 30.6%.

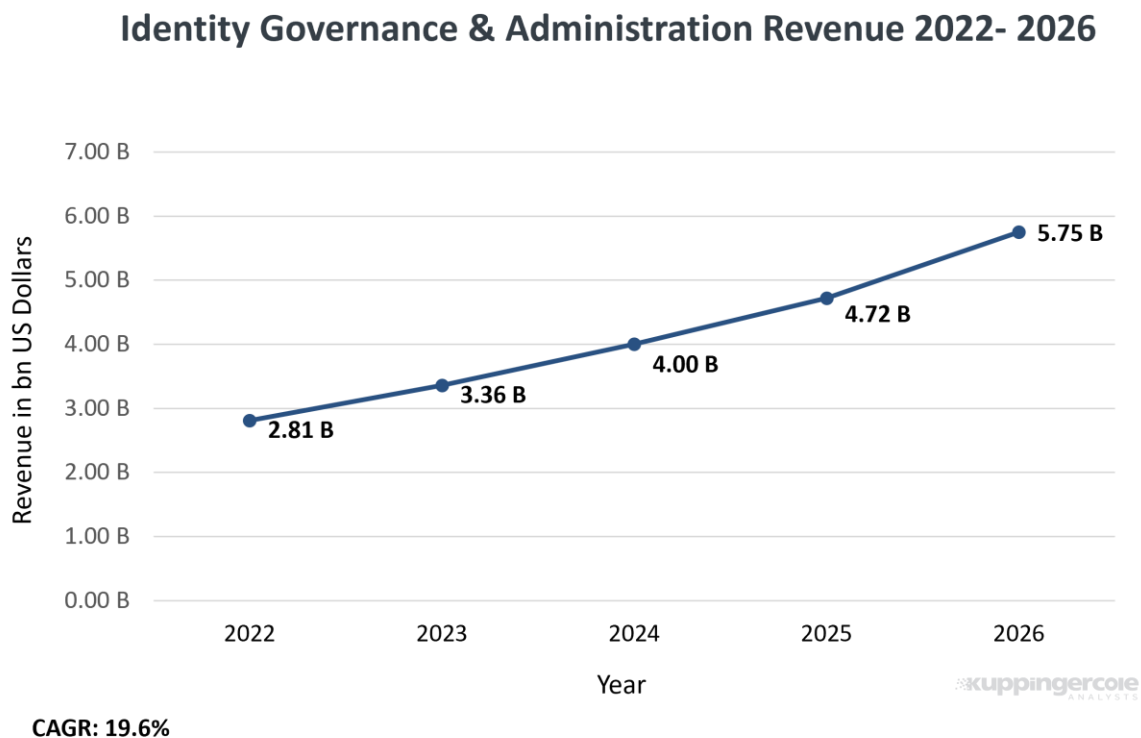


Figure 2: IGA Market Size (Source: KuppingerCole Analysts)

Over the past years, IGA solutions commonly have shifted from a traditional on-premises deployment model to IDaaS deployments. However, many organizations still prefer on-premises or hybrid deployments, for two reasons:

- **Sensitivity of data:** Data held in IGA systems is sensitive from both the privacy and security perspective, which causes some organizations to prefer deployments in their own data centers or at least in segregated tenants.
- **Connectivity to legacy on-premises applications and services:** Connecting IGA solutions to on-premises applications and services, especially when requiring specialized connectors using proprietary APIs, is perceived as being easier in on-premises or hybrid deployments.

On the other hand, most customers expects IDaaS support and the ability to migrate to a pure IDaaS deployments even when they initially opt for a different deployment model.

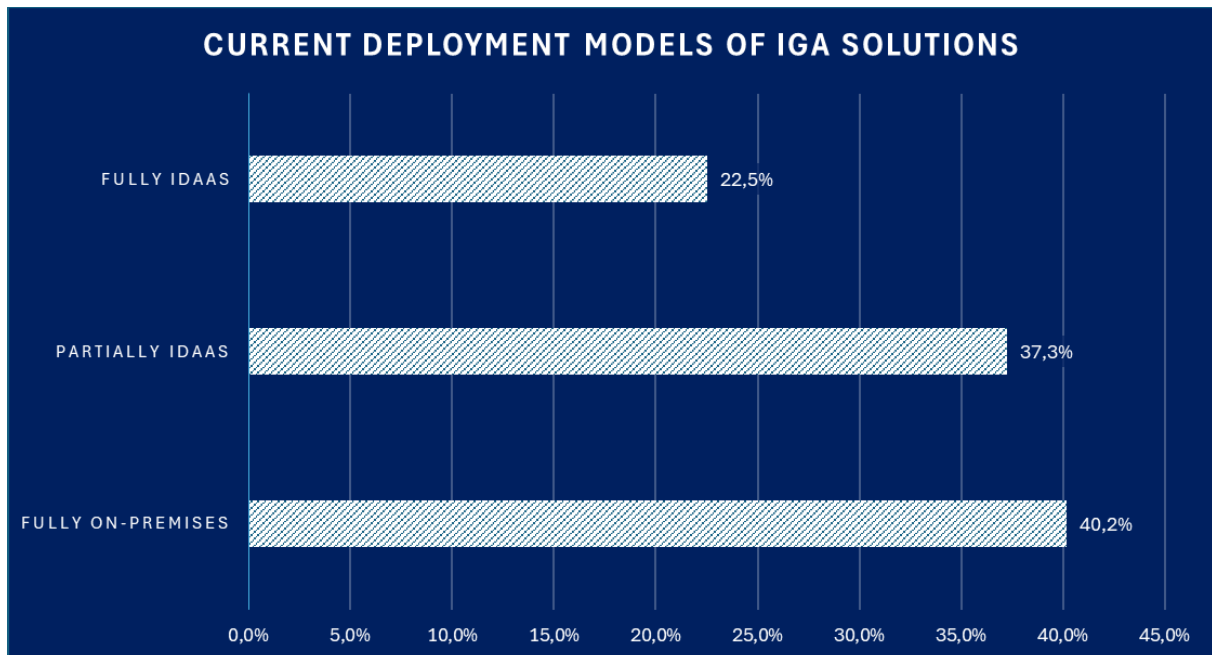


Figure 3: Most current IGA deployments are still on-premises or hybrid, with the share of IDaaS deployments growing (Source: KuppingerCole Analysts).

In the past year, the share of full IDaaS deployments grew from 11.4% to 22.5%, while the share of partial IDaaS deployments saw an increase from 25.7% to 37.3%. This validates the trend towards IDaaS deployments also for IGA, for both replacement and initial deployments of IGA as for modernization of IGA deployments with shifting on-premises solutions of a vendor to IDaaS. KuppingerCole expects more than 80% of the IGA deployments by 2025 to be IDaaS deployments, either multi-tenant or single tenant.

Aside of the deployment trend, we expect seeing more fundamental changes in the way IGA is done, with supporting JIT (Just-in-Time) provisioning and policy-based, dynamic access controls becoming the norm. This will help organizations in overcoming many of today's challenges in IGA that arise due to the complexity of role management and recertification.

Delivery Models

This Leadership Compass is focused on products that are offered in on-premises deployable form, either at the customer's site or deployed and offered as a managed service by a IAM Service Provider or as an IDaaS IGA offering, both multi-tenant or single-tenant.

Required Capabilities

During our evaluation of IGA vendors for the purpose of representation in this Leadership Compass, we look at several evaluation criteria including but not limited to the following groups of capabilities:

- Target System Connectivity
- Workflow Management
- Access Request
- Access Review
- Access Risk Management
- Access Intelligence
- User Interface and Mobile Support
- API support

Each of the above group of capabilities requires one or more of the functions listed below to satisfy the criteria:

- Baseline connectivity to target systems and to Identity Lifecycle Management systems
- Cloud connectors, adding Access Governance support for common cloud services
- Customization of mapping rules between central identities and the accounts per target system
- Centralized identity repository
- Workflow support for request and approval processes
- Workflow support for role lifecycle management
- Tools that support graphical creation and customization of workflows and policies
- Flexible role management with support for role governance
- Support for risk-aware, event-based access review certifications and targeted access review requests
- Support for SoD policies and continuous SoD controls monitoring
- Strong and flexible delegation capabilities
- Access Intelligence capabilities
- Flexible customization of the UI to the specific demand of the customer organization
- Business-friendly user interface

In addition to the above functionalities, we also consider the depth of product's technical specifications for the purpose of evaluation in this Leadership Compass. These product specifications primarily include the following and have a different weightage in our evaluation based on their importance in an IGA solution:

- **Connectivity:** The ability to connect to a wide variety of source and target systems including on-premises systems and applications and SaaS services via direct connections. This includes using standards such as SCIM. It should not only support proprietary APIs where standards are not supported but also deep integrations supporting complex entitlement models such as frequently found in LoB (Line of Business solutions). Integration with other ILM and IGA solutions from other vendors should be supported. Integration to ITSM (IT Service Management) tools for manual assignment of entitlements and the generation and tracking of service tickets is also taken into consideration. We also expect IGA solutions to support automated reconciliation of changes found in target systems and to not only read data from

target systems for IAG purposes, but also to trigger fulfilment of changes back to the target systems.

- **Heritage of connectors:** Having connectors as OEM components or provided by partners is not recommended and considered a risk for ongoing support and available expertise at the vendor.
- **SCIM support:** Support for SCIM (System for Cross-domain Identity Management) is preferred over traditional SPML (Service Provisioning Markup Language) for federated as well as on-premises provisioning. SCIM only is not perceived as being sufficient for connectivity to target systems, with several target systems such as some LoB applications having complex multi-tier entitlement models that can't be sufficiently managed via SCIM.
- **Deployment models:** Supporting multiple delivery options such as on-premises deployments, MSP services, and IDaaS deployments gives the customer a broader choice.
- **Tenant models in IDaaS:** Both single-tenant and multi-tenant deployments have advantages and disadvantages. For single-tenant deployments, a high degree of automation is required to ensure proper and timely propagation of patches. Also, customization models must be designed to ensure that custom changes are not impacted by updates and patches in IDaaS deployments.
- **Customization:** Systems that require little or no coding and that support scripting or, if programming is required, SDKs or support for a range of programming languages, are preferred. We also look for transport mechanisms between IT environments (e.g., development, test, and production), and the ability of keeping customizations unchanged after upgrades. For IDaaS, a limited control of tenants about the timing of updates is preferred.
- **Authentication mechanisms:** We expect IGA products to support basic authentication methods but by default use multi-factor authentication methods to limit the risk of fraud in using and administering these systems. Secure but simplified access for business users takes precedence.
- **Internal security model:** All systems are required to have a sufficiently strong and fine-grained internal security architecture.
- **High availability:** We expect on-premises IGA products and MSP deployments to provide built-in high-availability options or support for third-party HA components where required. For IDaaS, we expect a high service level.
- **Ease of deployment:** Complexity of product architecture and its relative burden on time to deploy as well as configuration and integration of basic services such as authentication, single sign-on, failover and disaster recovery should be minimal.
- **Shopping cart paradigm:** These approaches are popular for simplifying the access request management process by using shopping cart paradigms familiar to the users. Lately, there is an increasing trend towards integration to ITSM/ Service Desk solutions such as ServiceNow for access requests.
- **Out-of-the-box workflows / processes:** IGA solutions should provide a set of standard processes for common IGA use cases such as onboarding users, automated policy-based provision of access entitlements, manual access requests and approvals, mover and relocation, role modeling and management, standard and

emergency leave processes, temporary absence, and other common processes, to support rapid deployment of the solutions.

- **Workflow management:** Workflow capabilities that support customization and creation of workflows using a low code/ no code approach, preferably a drag and drop graphical interface that is easy to use and supports out-of-the-box templates.
- **Standards:** Support for industry standards for direct provisioning including well-known protocols like LDAP, JDBC, above-mentioned SCIM, file transfers of CSV files via HTTP, Telnet, SSH, FTP etc., and others.
- **Analytical capabilities:** Analysis of identity and entitlement data to support capabilities like role management, access requests and policy management. Advanced analytical capabilities beyond reporting, using standard BI (Business Intelligence) technology or other advanced approaches, such as deep machine learning for automated reviews, are becoming increasingly important.
- **Role and risk models:** Especially for the governance part of IGA products, what is becoming increasingly important is the quality and flexibility of role and risk models. These models not only need to be relevant but also need to have a strong conceptual background with sufficient flexibility to adapt to the customer's risk management priorities. It is important that organizations do not spend a lot of effort in adapting their business processes to match the templates offered by the tool, rather have a tool that offers sufficient flexibility to adapt to their IGA requirements.
- **Data governance:** Support for Data Governance and/or integration with Data Governance solutions, i.e., the ability to ensure access to data assets is controlled (roles, policies) and assist organizations with data compliance regulations.
- **Role/SoD concept and access and review support:** Should be able to analyze enterprise as well as application roles for inherent Segregation of Duty (SoD) risks and continuously monitor for new SoD risks being introduced and offer remediation measures. Further capabilities include the ability to perform access request, access certifications, and access approval or rejection.

All these technical specifications are subsequently evaluated for scoring each vendor in this Leadership Compass. We also look at specific Unique Selling Propositions (USPs) and innovative features of products in the overall evaluation which distinguish them from other solutions available in the market.

Leadership

Selecting a vendor of a product or service must not be based only on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identify vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer. To better understand the fundamental principles this report is based on, please refer to [KuppingerCole's Research Methodology](#).

Based on our rating, we created various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

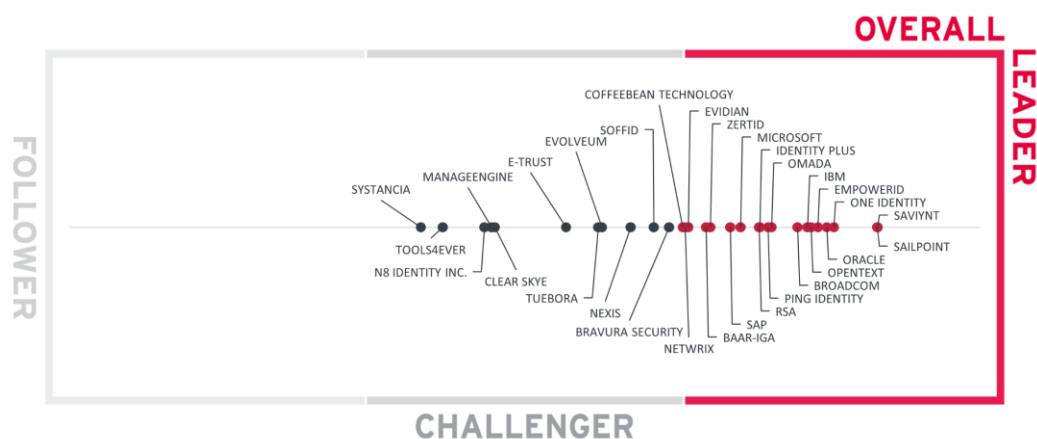


Figure 4: Overall Leadership in the IGA Market

The Overall Leadership chart is linear, with Leaders on the right, Challengers in the center, and Followers appearing on the left. The rating provides a consolidated view of all-around functionality, market presence, and financial security.

However, these vendors may differ significantly from each other in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and their products to get a comprehensive understanding of the players in this market and which of your use cases they support best.

Saviynt and SailPoint are scoring best in Overall Leadership. One Identity, Oracle, Broadcom, EmpowerID, OpenText, and IBM are closely following them. This group of vendors is made up of well-established players and have maintained their position as one of

the leaders because of their breadth and depth of proven as well as emerging capabilities. We strongly recommend further, detailed analysis of the information provided in this document for choosing the vendors that are the best fit for your requirements.

Ping Identity, RSA, Identity Plus, Omada, Microsoft, and SAP are also positioned in the Leaders segment. These vendors also have strong IGA capabilities. Netwrix and Evidian make up the remaining of the vendors in the Leaders segment while BAAR-IGA and ZertID are the new entrants in this segment due to their ability to provide a combination of established capabilities and strong innovative capabilities leveraging artificial intelligence and machine learning capabilities. We recommend referencing to the vendor specific chapters in this report to understand more about their specific strengths and challenges.

Overall Leaders are (in alphabetical order):

- BAAR-IGA
- Broadcom
- CoffeeBean Technology
- EmpowerID
- Evidian
- IBM
- Identity Plus
- Microsoft
- Netwrix
- Omada
- One Identity
- OpenText
- Oracle
- Ping Identity
- RSA
- SailPoint
- SAP
- Saviynt
- ZertID

Product Leadership

Product leadership is the first specific category examined below. This view is mainly based on the presence and completeness of required features as defined in the required capabilities section above. The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.



Figure 5: Product Leadership in the IGA market

IGA products have achieved a level of maturity with almost every established player providing the required breadth and depth of IGA capabilities. In this 2024 edition of the Leadership Compass on IGA, Saviynt and SailPoint take the joint top position in the Product Leadership category. OpenText, Oracle, EmpowerID, Broadcom, IBM, and One Identity are closely following the joint leaders. Omada, Identity Plus, RSA, BAAR-IGA, are also taking strong positions in the Leadership section. Soffid, Bravura, Netwrix, ZertID, and Microsoft are close to the dividing line between leaders and challengers. These solutions are the most complete in terms of functionality, internal product security, deployment options, interoperability, usability, and integrations available.

CoffeeBean Technology, Evidian, Nexis, and E-Trust are at the top of the challenger section. Tuebora, Evolveum are right behind the top challengers. Clear Skye, Systancia, N8 Identity, ManageEngine and Tools4ever are also placed well in the challenger segment, with that chart demonstrating the overall high maturity of the IGA market.

We recommend referencing to the vendor specific chapters in this report to understand more about their specific strengths and challenges.

Product Leaders (in alphabetical order):

- BAAR-IGA
- Bravura Security
- Broadcom
- EmpowerID
- IBM
- Identity Plus
- Microsoft
- Netwrix
- Omada
- One Identity
- OpenText
- Oracle
- Ping Identity
- RSA
- SailPoint
- SAP
- Saviynt
- Soffid
- ZertID

Leadership does not automatically mean that these vendors are the best fit for a specific customer requirement. A thorough evaluation of these requirements and a mapping to the product features by the company's products will be necessary.

Innovation Leadership

Next, we examine innovation in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

This view is mainly based on the evaluation of innovative features, services, and/or technical approaches as defined in the Required Capabilities section. The vertical axis shows the degree of innovation plotted against the combined/overall strength on the horizontal axis. The Innovation Leadership Chart is rectangular and divided into thirds. Innovation Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

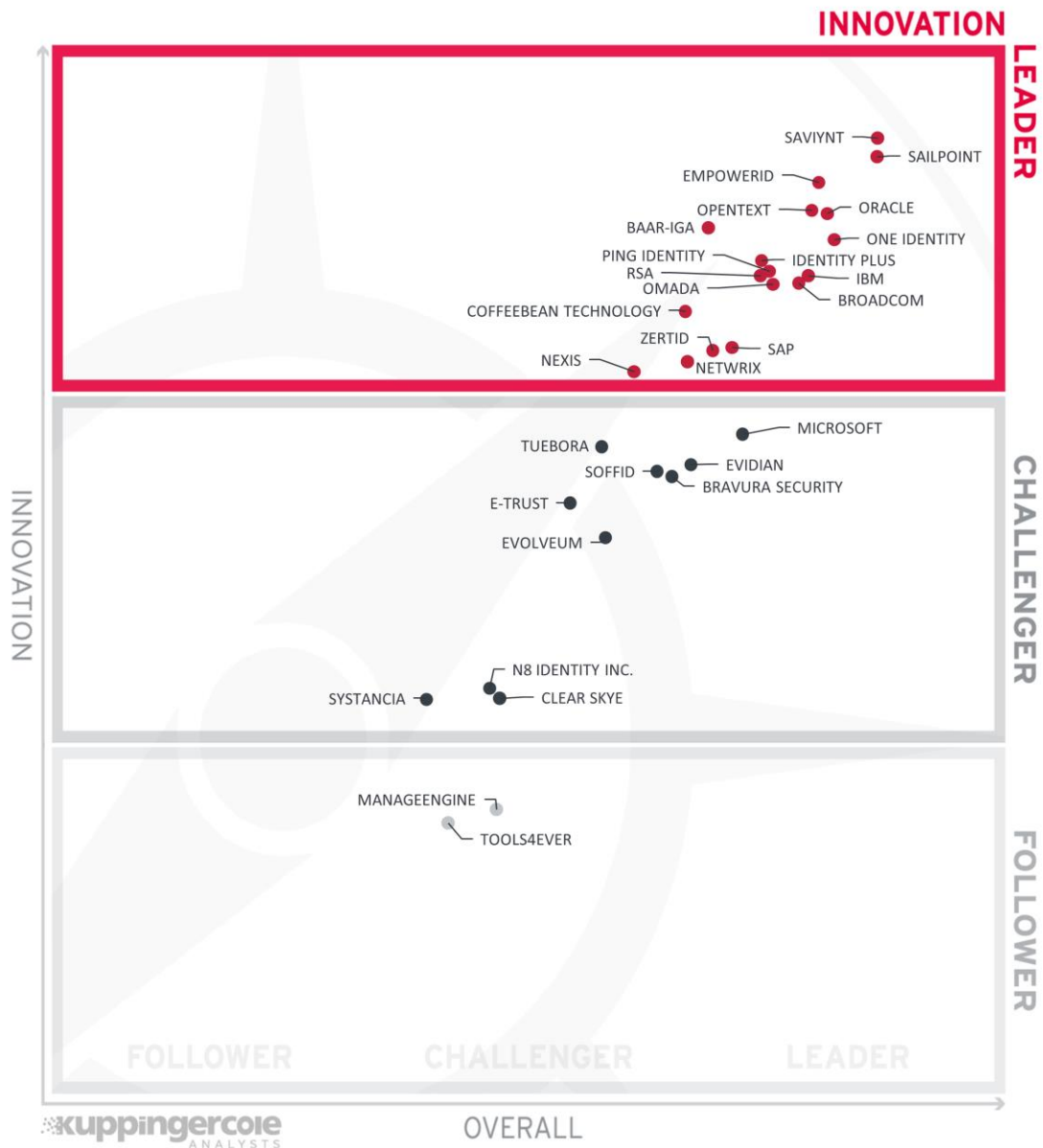


Figure 6: Innovation Leadership in the IGA Market

Innovation Leaders are those vendors that are delivering cutting-edge products, not only in response to customers' requests but also because they are driving the technical changes in the market by anticipating what will be needed in the months and years ahead. There is a correlation between the Overall, Product, and Innovation Leaders, which demonstrates that leadership requires feature-rich products that are looking over the horizon to bring advancements to help their customers.

Saviynt scores best in the innovation leadership category because of their heavy investment in the emerging capabilities of IGA solution. SailPoint, Oracle, OpenText, and EmpowerID very closely follow Saviynt in this category. One Identity, and BAAR-IGA are also in the

upper section of the leaders due to their depth of innovative capabilities. Ping Identity, Identity Plus, RSA, Omada, IBM, Broadcom, and CoffeeBean Technology are placed in the middle of the leader segment. Netwrix, Nexis, SAP, and ZertID are just above the dividing line between leaders and challengers. The vendors in the Leader segment have showcased innovative approaches for established capabilities and are continuously investing in modern technologies for advanced capabilities.

Microsoft, Tuebora, Soffid, Evidian, E-TRUST, Evolveum, and Bravura Security complete the top section of the Challenger segment. These vendors have shown some innovative features, frequently related to the use of Generative AI, and Microsoft with their integration of Privileged Identity Management. The remaining vendors in this category also have interesting features in the roadmap, which may increase their positioning in the future. ManageEngine and Tools4ever make the final Follower segment.

Innovation Leaders (in alphabetical order):

- BAAR-IGA
- Broadcom
- CoffeeBean Technology
- EmpowerID
- IBM
- Identity Plus
- Netwrix
- Nexis
- Omada
- One Identity
- OpenText
- Oracle
- Ping Identity
- RSA
- SailPoint
- SAP
- Saviynt
- ZertID

Leadership does not automatically mean that these vendors are the best fit for a specific customer requirement. A thorough evaluation of these requirements and a mapping of the product features by the company's products will be necessary.

Market Leadership

Finally, we analyze Market Leadership. This is an amalgamation of the number of customers, the number of transactions evaluated, the ratio between customers and managed identities/devices, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and the financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

In this chart, the vertical axis shows the market strength plotted against the combined/overall strength on the horizontal axis. The Market Leadership Chart is rectangular and divided into thirds. Market Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

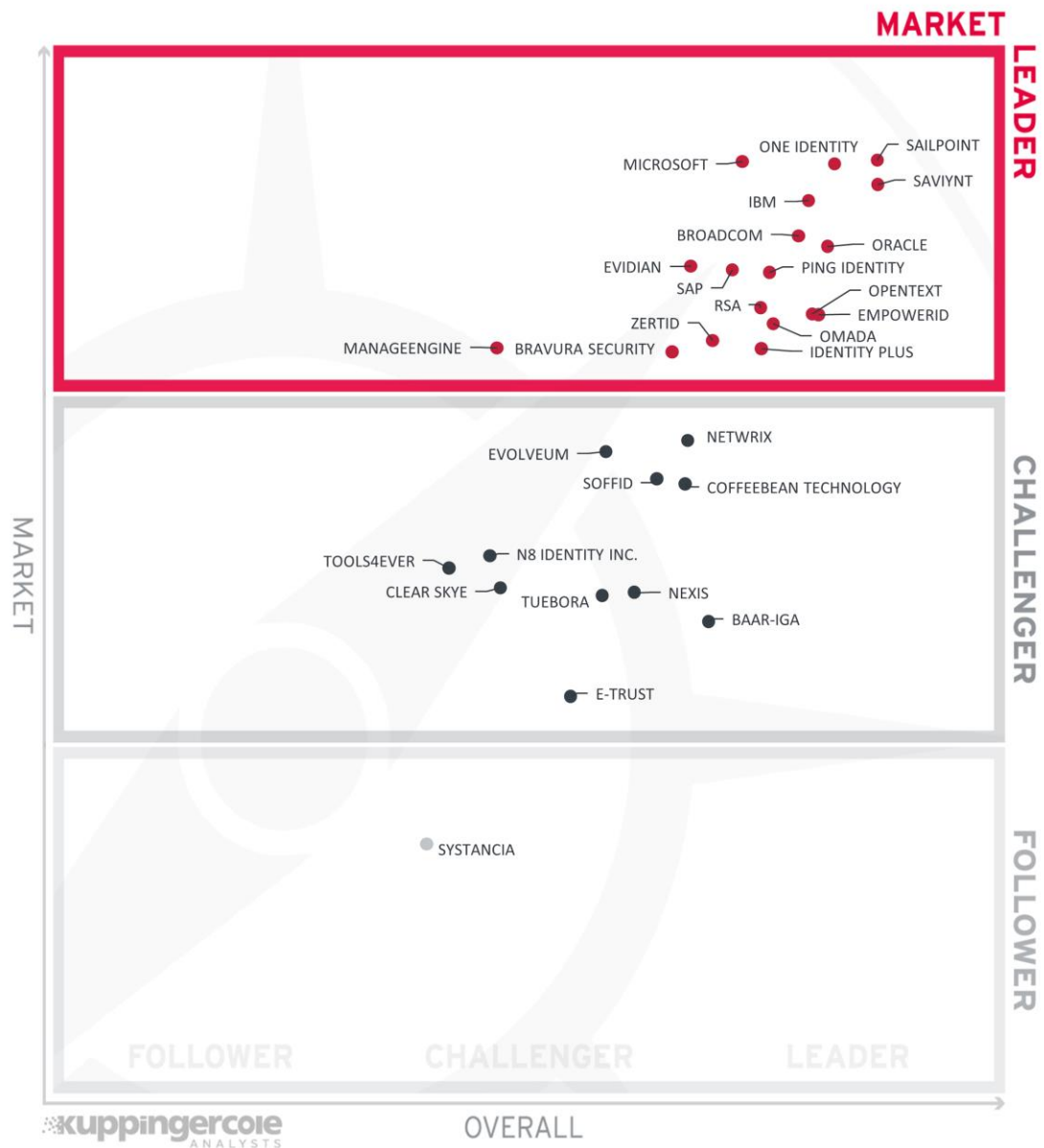


Figure 7: Market Leaders in the IGA Market

The Market Leaders category of the 2024 Leadership Compass IGA consists of global companies and other established IGA vendors. SailPoint is the overall leader in this category closely followed by One Identity, Microsoft and Saviynt. IBM, Broadcom, and Oracle complete the upper section of the Leaders segment. These vendors have solid to excellent financial strength, a significant number of customers, and a strong global partner ecosystem. Evidian, Ping Identity, SAP are placed in the middle of the Leaders segment. ManageEngine, Bravura Security, Omada, Identity Plus, RSA, Open Text, and EmpowerID complete the Leaders segment.

Netwrix, Evolveum, CoffeeBean Technology, and Soffid are placed in the upper section of the Challenger segment. Tools4ever, N8 Identity, Clear Sky, Tuebora, Nexis, BAAR-IGA, and E-Trust complete the Challenger segment. These vendors are currently working to address the gaps in the specific areas we evaluate for Market Leadership of IGA products, including the number of customers, average size of deployments, effectiveness of their partner ecosystem, among others.

Market Leaders (in alphabetical order):

- Bravura Security
- Broadcom
- EmpowerID
- Evidian
- IBM
- Identity Plus
- ManageEngine
- Microsoft
- Omada
- One Identity
- OpenText
- Oracle
- Ping Identity
- RSA
- SailPoint
- SAP
- Saviynt
- ZertID

Leadership does not automatically mean that these vendors are the best fit for a specific customer requirement. A thorough evaluation of these requirements and a mapping of the product features by the company's products will be necessary.

Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this Leadership Compass. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1. Since some vendors may have multiple products, these are listed according to the vendor's name

Vendor	Security	Functionality	Deployment	Interoperability	Usability
BAAR-IGA	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
Bravura Security	Positive	Positive	Positive	Strong Positive	Strong Positive
Broadcom	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Clear Skye	Positive	Neutral	Neutral	Positive	Strong Positive
CoffeeBean Technology	Positive	Positive	Strong Positive	Positive	Strong Positive
EmpowerID	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
E-TRUST	Positive	Strong Positive	Neutral	Positive	Strong Positive
Evidian	Positive	Positive	Positive	Positive	Strong Positive
Evolveum	Neutral	Positive	Positive	Positive	Positive
IBM	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Identity Plus	Strong Positive	Strong Positive	Strong Positive	Positive	Strong Positive
ManageEngine	Neutral	Neutral	Neutral	Neutral	Positive
Microsoft	Strong Positive	Positive	Positive	Positive	Strong Positive
N8 Identity	Neutral	Positive	Neutral	Neutral	Positive
Netwrix	Positive	Strong Positive	Strong Positive	Positive	Strong Positive
Nexis	Positive	Strong Positive	Positive	Positive	Strong Positive
Omada	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
One Identity	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
OpenText	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Oracle	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive

Ping Identity	Positive	Strong Positive	Positive	Positive	Strong Positive
RSA	Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
SailPoint	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
SAP	Positive	Strong Positive	Positive	Positive	Strong Positive
Saviynt	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Soffid	Strong Positive	Strong Positive	Positive	Positive	Strong Positive
Systancia	Neutral	Positive	Positive	Positive	Strong Positive
Tools4ever	Neutral	Neutral	Neutral	Neutral	Strong Positive
Tuebora	Positive	Positive	Positive	Positive	Positive
ZertID	Strong Positive	Strong Positive	Positive	Positive	Strong Positive

Table 1: Comparative Overview of the Ratings for the Product Capabilities

In addition, we provide in Table 2 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
BAAR-IGA	Strong Positive	Weak	Neutral	Neutral
Bravura Security	Positive	Positive	Positive	Strong Positive
Broadcom	Positive	Positive	Positive	Strong Positive
Clear Skye	Neutral	Neutral	Neutral	Neutral
CoffeeBean Technology	Strong Positive	Neutral	Positive	Positive
EmpowerID	Strong Positive	Positive	Positive	Positive
E-TRUST	Positive	Weak	Neutral	Weak
Evidian	Positive	Positive	Positive	Strong Positive
Evolveum	Neutral	Neutral	Neutral	Strong Positive
IBM	Positive	Strong Positive	Strong Positive	Strong Positive
Identity Plus	Strong Positive	Neutral	Neutral	Positive
ManageEngine	Weak	Positive	Neutral	Strong Positive
Microsoft	Positive	Strong Positive	Strong Positive	Strong Positive
N8 Identity	Neutral	Neutral	Neutral	Positive
Netwrix	Positive	Neutral	Positive	Positive
Nexis	Positive	Neutral	Neutral	Neutral
Omada	Positive	Positive	Positive	Positive
One Identity	Strong Positive	Strong Positive	Positive	Strong Positive
OpenText	Strong Positive	Positive	Positive	Positive
Oracle	Strong Positive	Positive	Strong Positive	Positive
Ping Identity	Strong Positive	Positive	Positive	Strong Positive
RSA	Strong Positive	Positive	Positive	Positive
SailPoint	Strong Positive	Strong Positive	Strong Positive	Strong Positive
SAP	Positive	Positive	Strong Positive	Positive
Saviynt	Strong Positive	Positive	Positive	Strong Positive
Soffid	Positive	Neutral	Neutral	Positive
Systancia	Neutral	Weak	Neutral	Weak
Tools4ever	Weak	Neutral	Positive	Neutral
Tuebora	Positive	Weak	Neutral	Neutral

ZertID	Positive	Neutral	Neutral	Strong Positive
--------	----------	---------	---------	-----------------

Table 2: Comparative Overview of the Ratings for Vendors

Product/Vendor evaluation

This section contains a quick rating for every product/service we have included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For this market segment, we look at the following categories:

Identity Lifecycle Management: This refers to the ability to provision and manage identities, access entitlements, and other identity-related information in the target systems over its lifecycle. Other capabilities are considered, including the ability to access identity stores, data modelling and mapping, as well as the ability to manage different identity types.

Target System Support: The number of connectors and the breadth of target systems that the solution can connect to, including, e.g., directory services, business applications, mainframe systems, etc. Connector breadth also looks at support for standard cloud services. Connector depth further examines customization capabilities for connectors through connector toolkits and standards as examples and the connectors' abilities, especially when it comes to connecting to complex target systems such as SAP environments or mainframes.

Self-Service & Mobile Support: User self-service interfaces and support for secure mobile access to selected IGA capabilities. Other capabilities include authenticator options, delegation of tasks and password reset.

Access & Review Support: Integrated Access Governance capabilities that support activities such as the review and disposition of user access requests, certification definition and campaigns, and access remediation. Also looked at is Segregation of Duty (SoD) controls to identify, track, report, and mitigate SoD policy violations as part of integrated risk management capabilities, as well as role management and policy management capabilities.

Identity & Access Intelligence: IGA intelligence that provides business-related insights supporting effective decision making and potentially enhancing governance. Advanced capabilities such as use of AI and/or machine learning techniques that enable pattern recognition for process optimization, role mining, role design, automated reviews, and anomaly detection are considered. Other capabilities can include the use of user access information from authentication and authorization events used for analyzing user access behavior patterns and detecting anomalous access.

Workflow & Automation: Advanced workflow capabilities, including graphical workflow configuration, and the extent to which common IGA tasks can be automated.

Centralized Governance Visibility: This is the extent to which the identities and their access under governance control can be viewed in a consolidated or single-pane view, such

as in a dashboard format. Centralized access to reports and auditing support is typically also provided.

Architecture & Hybrid Environment: This category represents the combination of architecture and hybrid environment support. In architecture, we look at the type of architecture and focus on modern, modular architectures based on microservices. This also affects deployment, given that container-based deployments provide good flexibility. Also evaluated is the solution's ability to support a hybrid environment for customers that anticipate or are currently taking an intermediate step towards migrating from on-premises to the cloud.

BAAR Technologies Inc – BAAR-IGA

BAAR Technologies is a digital transformation company headquartered in Ontario, Canada. It was founded in 2018 to help organizations with digital transformation initiatives, such as digital security through a scalable workflow architecture and an easy-to-build low-code/no-code platform for rapid deployment. Their primary focus is to provide integration with any type of system, rapid onboarding of new clients with minimal coding, and policy monitoring.

BAAR-IGA follows a low-code workflow system which allows for custom integrations on the fly. This ensures any target directory integration can be done. An individual BAAR universal directory is also available. Based on customer requirements, customers can also use their universal directory. BAAR-IGA supports setting up 26 custom attributes out-of-the-box from the user interface during the configuration phase. BAAR-IGA supports management of identities by way of a rule table that can be managed from the user interface. The solution supports creation of any identity type in this table and a set of rules can be associated with the identity.

The full platform is built on a low-code infrastructure automation platform called BAAR (Business Automation, AI, and Robotics). New workflows can be created using the drag and drop features and can interact with any type of IT environment. Existing default workflows can be modified for each client if needed. The configuration setup is flexible. BAAR-IGA has an editor where any workflow can be built and tested.

BAAR-IGA has a modern user interface with configurable dashboard that provides insights into user access to applications, access violations and user journey. The backend supports user identity creation for on-premises customers where the full version is deployed at the customer while for SaaS deployments, the solution is deployed via a docker container. There is a front end available where BAAR-IGA acts as an identity provider that supports SSO and MFA for authentication. The front-end user interface is built using React.JS/Node.JS.

BAAR-IGA supports a wide range of deployment models ranging from complete on-premises deployment, private cloud, hybrid, and complete SaaS deployment. For SaaS, each customer has a docker for BAAR deployed on Kubernetes. Interaction between the front end and BAAR and its various components is conducted by REST API's. Other APIs supported by BAAR-IGA are SCIM, LDAP, SQL, OAuth and SAML. The solution's SDK support is limited to Python where only 30 percent of the capabilities of the solution are available. BAAR-IGA supports Python scripts that can be used for all kinds of customization.

BAAR-IGA's user and admin self-service is provided based on levels of access of user accounts. The solution supports all major authenticators while passwordless access is currently provided through their own authenticator application. The solution has a shopping cart-based approach for selecting and requesting access. BAAR-IGA allows for requesting privileged access via prebuilt workflow templates for approval process. The workflow requires an input of a valid business reason to be initiated. A different ID is set up for the user with the appropriate privileged access which can be made timebound during approval. The solution provides support for delegated access workflows through customization.

BAAR-IGA supports integration with SIEM solutions through Syslog. The solution has a custom reporting engine for creating custom reports and dashboards. For auditing purposes, all types of reports and report formats are supported. The reporting engine allows the creation of reports on the fly, based on SOC/SOX finding of customers. The solution has

limited support for out-of-the-box reports for major compliance frameworks. The major compliance frameworks currently supported by BAAR-IGA are NIST SP 800-53 and SOX.

BAAR-IGA monitors access based on RBAC but supports other access principles such as ABAC, PBAC, CBAC, among others. The solution supports creation of all policies using low code customizable workflows. This is governed by the role designation matrix. The role designation matrix can be configured from the user interface. The role designation matrix has primary and secondary access for users. Primary access is a list of applications/entitlements that the user will be provisioned access in an automated manner during onboarding. Secondary access is a list of applications/entitlements where a user is not provided access in an automated manner, but if a user requests access using the self-serve feature, no additional approvals are needed. BAAR-IGA supports all types of attributes for creating flexible entitlement models.

BAAR-IGA uses AI and machine learning for workflow capabilities. AI is used for conversion of structured data into unstructured data, finding anomalies in user access patterns, and role modelling for finding users with similar entitlement models. The solution's workflows are built in native RPA engine and each workflow can have a separate AI model built into it for intelligent processing of data.

BAAR-IGA can be provided as a unified IGA and IAM platform or individual components based on customer requirements. Their current customer base is limited to India and North America with plans in place to expand to Europe after establishing partnerships. BAAR is supporting customers that mainly use legacy applications and systems in the finance sector due to their product's ability to integrate with legacy systems. They are focused on the mid-market segment while the enterprise segment is limited to using only certain components of their solution. Their roadmap includes adding capabilities around role mining, PAM, analytics engine, and around certain features leveraging AI.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive



Table 3: BAAR-IGA's Rating

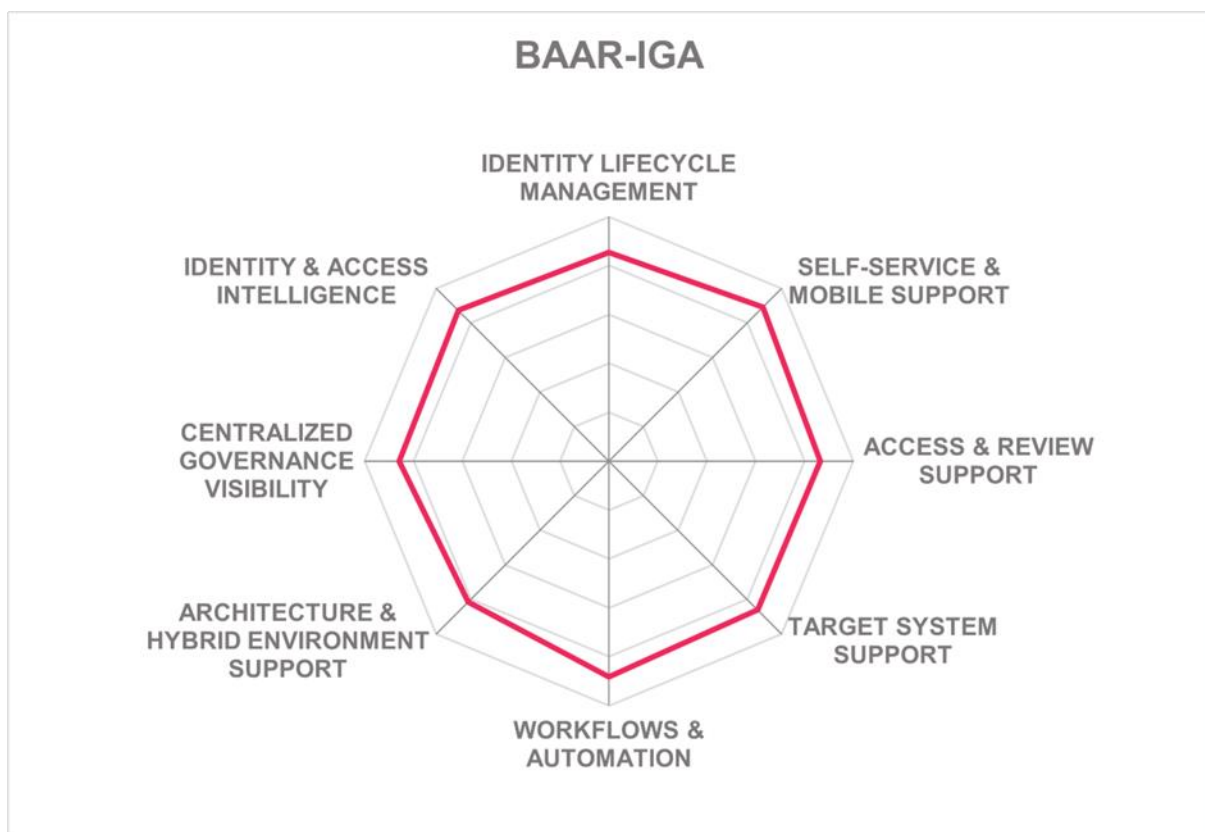
Strengths

- Low code workflow architecture
- Native RPA engine where workflows can be built with individual AI models
- Supports wide range of APIs including SCIM, LDAP, SQL, OAuth and SAML
- Wide range of connectors for on-premises and SaaS systems are available. Custom connectors can also be built from the user interface itself
- Low code policies which can be easily customized based on client's environment
- All types of reports and report formats are supported for auditing purposes
- Modern and user-friendly user interface

Challenges

- SDK support is limited to Python
- Current customer base is mainly in India and North America but plans in place for expansion into Europe
- Out-of-the-box reports for major compliance frameworks is limited but additional reports can be built using requirements
- Supply chain risk management for B2B partner onboarding is missing but planned for 2025

Leader in



Bravura – Bravura Security Fabric

Bravura Security is a cybersecurity specialist company headquartered in Alberta, Canada. Founded in 1982, Bravura, previously known as Hitachi ID, is now fully owned by Constellation Software. The Bravura Security Fabric supports identity lifecycle management automation, access governance, workflows, self-service identity, multi factor authentication, privileged access automation, decentralized credentials, and analytics.

The Bravura Security Fabric consists of multiple components (Privilege, Identity, Pass, Safe, OneAuth, and Cloud) for identity provisioning, authentication privilege access management and compliance. Bravura Identity is the IAM and IGA solution that focuses on provisioning, deprovisioning, transfers, certification, and other related IGA capabilities. It can provide these capabilities across all identity types. The overall Bravura Security Fabric is implemented as a multi-service solution whereas the individual components are implemented as microservices.

Bravura Security supports all major deployment and delivery models including docker containerization. Virtual machines are utilized for core service hosting on EC2 platform. Bravura Security provides a single tenant solution. Bravura Security uses a multi-region architecture which supports hyper scaling. All the functionalities of the solution are exposed via SOAP, REST and GraphQL APIs. Their primary support for SDKs is limited to Python but they also provide scripted integrations for .NET and Java.

Bravura Security Fabric supports all known identity repositories with the possibility to integrate with legacy solutions. Bravura has a rich out-of-the-box native connector library for both on-premises and SaaS systems. They also support universal connectors which can be leveraged for connecting to legacy or custom systems. The mainframe connector is bidirectional that operates in server or client/ server mode. Bravura supports all major authenticators for user and admin self-service. Passwordless authentication is supported via the Bravura OneAuth product. The solution supports secure sharing of credentials, as well as onboarding for privileged and Just-In-Time (JIT) identities.

Bravura Security has a modern and user-friendly user interface. The end user dashboard is informative with all relevant statistics displayed to understand the identity journey. The common platform provides consistent UIs, database, connectors, and API throughout the other components in the Bravura Security Fabric. The solution supports all IGA related reports and report types. Out-of-the-box reports for major compliance frameworks are also supported for HIPAA, GDPR, FERPA, FISMA, SOX, among others.

As part of Bravura Cloud and the new capabilities through GraphQL API, Bravura are introducing AI and machine learning based identity analytics. These functionalities are currently being used for risk classification of user accounts and groups at scale. Their separation of duties engine is built in and can check for toxic combinations for groups and roles. It is also very flexible at the same time to allow for exceptions.

Bravura Security is focused on enterprise businesses with majority of presence in the North American market. The roadmap features include compliance to NIST rules, passkey support for Bravura Safe, policy and role-based provisioning in Bravura Cloud, introduction to containerized version of their core capabilities and SCIM related integrations.

Security	Positive
-----------------	----------

Functionality	Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive



Table 4: Bravura Security Fabric's Rating

Strengths

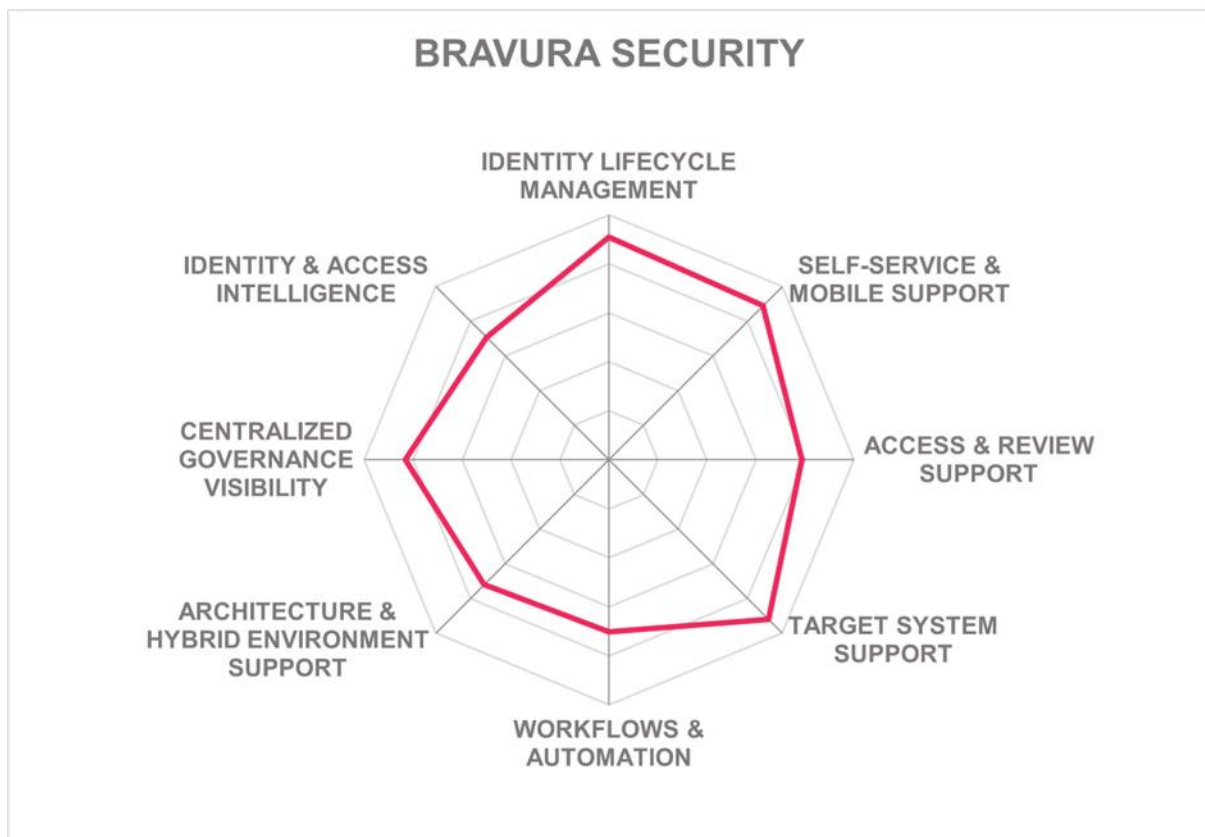
- Product deployment options include on-premises, public and private cloud, and hybrid deployment
- Supports all major capabilities related to identity lifecycle management
- All known connectors supported for on-premises and SaaS systems
- Role and SoD management uses an inbuilt engine
- Unified platform offers services for various capabilities
- UI is modern and user friendly
- Reporting capabilities support all major compliance framework requirements

Challenges

- SCIM initiated lifecycle automation is not yet supported but in roadmap
- Limited presence outside North American market
- Zero Code/ Low code is missing but planned in roadmap
- Quick approval processes missing

Leader in





Broadcom – Symantec IGA

Based in America, Broadcom is a manufacturer of semiconductor and infrastructure software products. It acquired CA Technologies in late 2018 and acquired the Symantec Enterprise business in late 2019. The former CA Security business is now part of the Symantec Enterprise Division of Broadcom. Broadcom's Symantec Enterprise portfolio includes Symantec Identity Governance and Administration (IGA), which consists of Identity Manager, Identity Governance, and the Identity Portal.

Broadcom's identity services leverage a microservices architecture capable of deploying independent business services that can leverage a common set of IAM capabilities, including policies, a risk engine, AI/ML, among others. The solution is built with an API first approach such that majority of the functionality is exposed and invoked via APIs. SOAP, REST, SCIM, SCIM 2.0 and LDAP are the supported protocols. Additionally, the solution architecture accommodates extensibility via loosely coupled interfaces including REST API, Webhooks, event streaming, and pub/sub integrations.

Symantec IGA is still delivered as a virtual appliance. Broadcom suggests this approach separates the complexity of deploying and managing underlying infrastructure. The solution architecture is designed to be modular and various services and components can be scaled as required. The product is designed to meet all the standard requirements for Load Balancing, Failovers, and Disaster Recovery. Other delivery options supported by the solution include software deployed to server and managed services. The solution also supports container-based delivery for Docker and RedHat. Others include Kubernetes, Google GKE, Amazon EKS, Azure EKS and OpenShift. The solution is still missing SaaS delivery. Future deliveries of Symantec IGA will integrate with microservices architecture that has already been released. The solution can be deployed on-premises, public or private cloud, hybrid, as well as offered as a license or subscription based. Symantec IGA supports wide range of SDKs including Android, iOS, Java, C/C++, .NET, JavaScript, and AngularJS programming languages.

Broadcom's products are fully capable of operating in silos, offer a strong line-up of IGA capabilities, including user access certification, SoD, entitlement clean-up, role discovery, automated workflows and policy management, access certification. Broadcom also offers an access risk analyzer and simulator that can estimate a user's risk score based on the change in the context of an access request along with SoD check at shopping cart. Symantec IGA's UI is modern and user-friendly, making it productive for users, given its helpful context advice tools. A customizable form for creating identities based on the requirements is provided. Users can view the certification campaign history via the consultation feature.

Symantec IGA is also highly customizable and configurable with limited to no coding required. The solution offers strong capabilities related to scaling. The identity portfolio and microservices-based security platform adds a level of customization and capabilities that extends from IGA to incorporating authentication use cases, a risk engine and BYO reporting technologies. The policy Xpress engine enables administrators to configure custom business logic without writing any custom code. Symantec provides an entitlement catalogue and shopping cart approach to usability. Symantec's support for out-of-the-box provisioning/de-provisioning for on-premises and SaaS applications extends to wide range of industry standard connectors. Customized connectors can also be developed based on requirements.

Broadcom has a global presence in the medium to enterprise market segment. They have a large set of global integration partners. Their roadmap for this product includes enhanced user interface, AI and machine learning driven attribute management, enhanced auditing interface, intelligence/risk-based provisioning and deprovisioning as well as adaptive role analysis and recommendations leveraging AI/ML.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive



Table 5: Broadcom Symantec's rating

Strengths

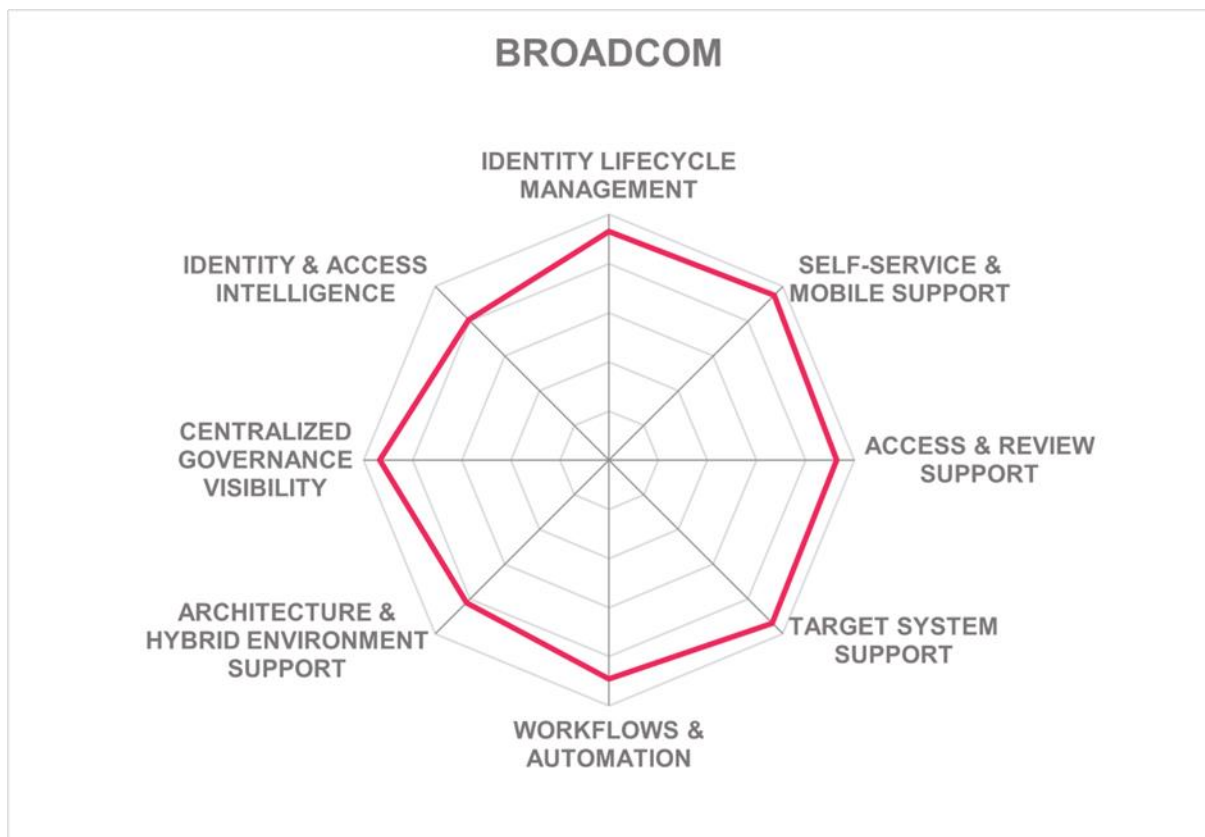
- Customizable and configurable platform with limited to no coding required
- Solutions supports high level of scalability
- Good capabilities for identity lifecycle management
- Large set of major connectors for on-premises and SaaS systems supported
- Solutions supports all known access principles for policy management
- AI and machine learning supported for facilitating workflows
- Strong UI for Mobile
- Solutions can integrate with open source and other third-party reporting solutions through a standards-based, modular architecture
- Global presence with large number of customers and integration partners

Challenges

- Limited product delivery options
- Out-of-the-box reports for some major compliance frameworks is missing
- Customizations cannot be done in separate microservices
- Some features around AI are missing but planned in roadmap

Leader in





Clear Skye – Clear Skye IGA

Clear Skye is a small privately-owned company headquartered in the San Francisco Bay area. Founded in 2016, the Clear Skye IGA solution is built on and exists solely within ServiceNow. Customers install the application directly from the ServiceNow application store. Clear Skye IGA capabilities include Identity Lifecycle, Entitlement Management, Access Requests, Audit, Policy Management, Certifications (access reviews), Identity Analytics, and Workflows.

Clear Skye IGA is built on ServiceNow, which provides the underlying infrastructure such as the database, compute, networking, monitoring, encryption, etc. and the foundational services for the product such as MID Server, workflow, business rules, Flow Designer, IntegrationHub, Reporting, Service Catalogue, Now Mobile, and APIs. Clear Skye has all its data and workflow on the ServiceNow platform to help in improving user experience, reducing training costs and reducing overall costs for the system

Clear Skye IGA's access policies can be configured to leverage any data within the ServiceNow instance, including the CMDB, GRC and SecOps solutions. In addition, all ServiceNow applications can use Clear Skye's identity data. Clear Skye IGA utilizes the customer's Now Platform database for managing accounts, access entitlements, and any other identity related information. Clear Skye supports attribute mapping from source to target with each connector having defined capabilities. The solution supports SCIM and SCIMv2 for identity provisioning and deprovisioning. Clear Skye offers a moderate number of out-of-the-box provisioning connectors for on-premises systems but supports a wide range of connectors for SaaS systems. Clear Skye can generate additional connectors using the ServiceNow Integration Hub's connectivity framework. Since Clear Skye is a ServiceNow solution, out-of-the-box integration to other ITSM tools is missing.

Clear Skye IGA is delivered as a native ServiceNow as-a-service or can take advantage of ServiceNow's on-premises offering. ServiceNow customers benefit from the re-use of their existing ServiceNow investment such that Clear Skye IGA uses a customers' existing ServiceNow infrastructure with no additional components to procure or license. The solution also supports license-based and subscription-based deployment. For on-premises systems, the ServiceNow MID server is used. This is a standard Now platform component that is also available as a Docker container as of the San Diego platform release. Some services, such as reporting, database services, and security model are shared services on the Now Platform.

The product's functionalities are exposed via REST APIs. Most of the functionalities of the solution are available via JavaScript SDK. Being on the Now Platform, the solution takes advantage of the native SDK which is exposed as JavaScript. Clear Skye supports bidirectional integration with connectors that populate the IGA Identity Warehouse as well as provisioning of access to target systems.

Clear Skye IGA uses the standard ServiceNow Service Portal as the interface to request access whereas an end user portal focuses on IGA for workers and supervisors. For requesting items, standard ServiceNow experience is available via the ServiceNow catalogue. Clear Skye has strong access request functionality through its use of the ServiceNow Service Portal. It uses a good model for SoD checks and peer group analysis before forwarding the request to the system. Clear Skye IGA has a good user self-service model and uses a shopping cart paradigm. The user interface supports visual workflows to see access request status. Clear Skye has good access review capabilities, with many

access review templates provided out-of-the-box and the ability to define additional access review capabilities. Users can perform access reviews directly in the ServiceNow Service Portal.

Clear Skye IGA's user interface has improved significantly over the last couple of years. The user interface is modern and friendly. For auditing purposes, Clear Skye has good analytics graphs and a strong reporting tool. The analytics technology uses a no-code approach. It has a strong workflow configuration engine as it uses ServiceNow's low code flow as a strategic workflow modelling tool. The product has a mature workflow designer model and customization of rules, flows and correlations is available.

Clear Skye IGA helps organizations that require lower barrier of entry IGA products or where existing IGA solutions are manual process intensive. The software benefits customers interested in leveraging their existing ServiceNow investment. Clear Skye mainly supports enterprise customers with considerable support given to mid-market and medium-sized businesses. The market presence is almost equal in North America and EMEA, with growth being shown in APAC. Clear Skye has a good partner ecosystem across the globe, which includes Accenture, Ernst & Young, KPMG, and other companies. Their roadmap includes features around separation of duties, enhanced identity analytics and improved dashboarding and monitoring of user journey.

Security	Positive
Functionality	Neutral
Deployment	Neutral
Interoperability	Positive
Usability	Strong Positive



Table 6: Clear Skye's Rating

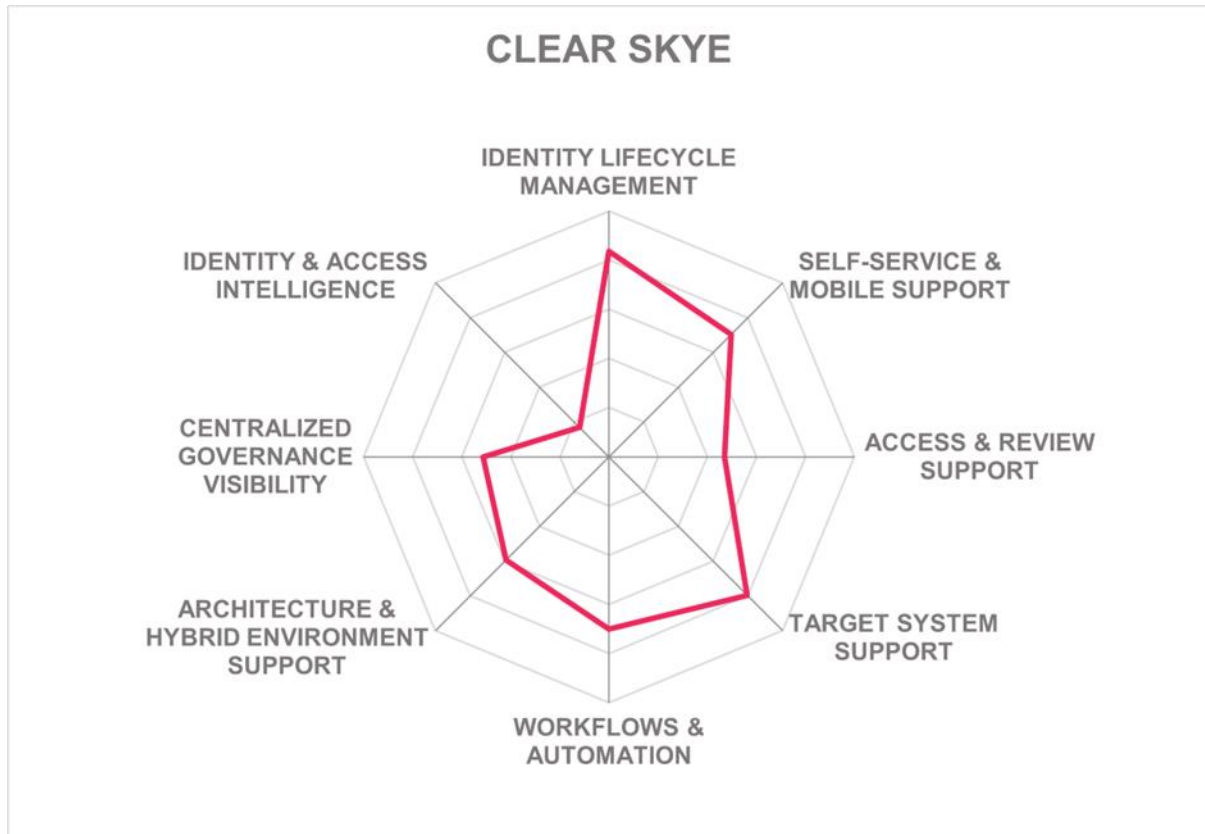
Strengths

- Delivered as a scoped application specifically designed for cloud native ServiceNow deployment
- Covers full breadth and depth of features around identity lifecycle management
- Strong list of connectors for SaaS target systems
- Modern and user-friendly UI
- Can onboard policies directly from the ServiceNow portal
- Capabilities around access request is easy and similar to requesting items from ServiceNow catalogue
- Workflow engine is the ServiceNow workflow engine

Challenges

- Does not cover separation of duties for toxic combinations
- Role mining is missing
- Does not have AI/ ML related capabilities but planned in roadmap

- Does not cover out-of-the-box reports for major compliance frameworks
- As a pure ServiceNow cloud native solution, sometimes disadvantageous
- SDK support is limited to JavaScript



CoffeeBean Technology – CoffeeBean IGA

CoffeeBean Technology is a cloud-native security company headquartered in California, USA. It was founded in 2008 with the mission of providing secure access to applications. The CoffeeBean IGA platform has comprehensive capabilities for major IGA functionalities such as access requests, access reviews, user self-service and target system support.

CoffeeBean's microservices based multi tenancy cloud platform is made of different layers. The first layer is made up of user interfaces having administration and end user portals for authentication, registration, and self-services. The second layer is composed of standard protocols APIs for integration and automation. The third layer is related to core services which includes implementation of business/domain logic. The last layer is used for storage of data.

The CoffeeBean Identity Platform provides an IGA solution that is easily deployable and integrates with any system for provisioning and de-provisioning. The solution also supports the ability to customize provisioning workflows to align with the organization's specific onboarding processes. The solution supports policy-based provisioning based on attributes such as user roles and departments.

CoffeeBean IGA platform has a dedicated module for lifecycle management. The solution supports mapping of policies and business requirements between directories, system, and applications through its dashboard. They provide a low code approach to create different types of workflows and integration within the platform.

The CoffeeBean solution offers a variety of connectors to different SaaS systems, and creating new connectors is possible using the available set of APIs and documentation designed to facilitate such solutions. CoffeeBean has all its functionalities available via APIs such as SOAP, REST, SCIM, LDAP and SQL.

CoffeeBean IGA is predominantly a SaaS solution that supports deployment on a public cloud, featuring subscription-based and on-premises agents and connectors to integrate with specific systems. The platform can also be deployed in private cloud or hybrid cloud depending on the requirement of the customer. They can also deliver the solution using a virtual appliance and containerized deployment (Docker). A managed service option is also available through partnerships with the providers solution an additional layer of services integrated into the platform.

CoffeeBean's user interface is modern and interactive. The admin dashboard and end user dashboard have some user interface differences but can be customized. The user interface supports role creation and group segregation. CoffeeBean provides the user interface in English and Portuguese languages. They have well a defined the access review and access request interface for quick decision making. They support most of the authenticators for user and admin self-service including passwordless authentication. The solution supports creation of policies using a low code workflow design. The new workflow interface supports ready to use policies that can be created, managed, and edited directly within the platform. The ready to use policies support in creation and testing of different types of workflows.

CoffeeBean's adaptive authentication solution employs machine learning for anomaly detection and user behavior pattern analysis. This feature is integrated into their IGA and workflow platform and further enhances the governance capabilities. Further use cases for AI and machine learning include AI analysis within access certification for access review. AI analyzes access patterns, user behavior and risk factors to identify access outliers and

potential risks. This analysis is then presented in the self-service portal in the form of risk scores when doing access reviews. AI also uses this analysis to automatically revoke access for potential high-risk users. These risk scores can be customized using the workflows.

CoffeeBean is focused predominantly on the Latin American market, especially Brazil. They provide provisioning connectors specially to Brazilian solutions, both on-premises and SaaS, which are commonly utilized in Brazil and South America. This includes popular platforms such as RD Station, TOTVS, and Senior Systems. They are also expanding to North America and the EMEA region. Their main customer base is medium to enterprise level organizations. Their roadmap includes enhancing low code workflow, incorporating AI and machine learning for various use cases such as role mining.

Security	Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Strong Positive



Table 7: CoffeeBean IGA's Rating

Strengths

- Comprehensive solution for IGA, IAM, MFA, CIAM, and adaptive authentication
- Inbuilt automation engine which supports system integration through APIs
- UI is modern and interactive
- All the functionalities of the solution are available via APIs such as SOAP, REST, SCIM, LDAP and SQL
- Supports a low code workflow platform that supports variety of out-of-the-box templates
- AI and machine learning leveraged for various use cases such as adaptive authentication and access certifications
- SoD policy supports managing different types of conflicts at various stages of the user's lifecycle
- Access governance features such as access reviews, access requests are handled very quickly

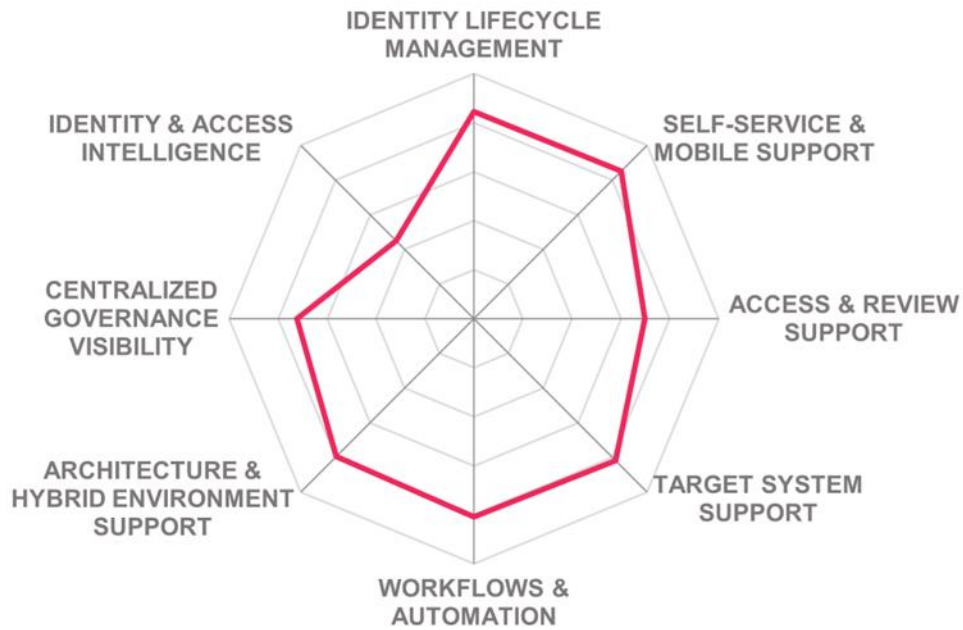
Challenges

- Container based platform support is limited to Docker and Kubernetes
- Presence is limited outside Latin America
- Policy editing, testing and authorization tool is missing

Leader in



COFFEEBEAN TECHNOLOGY



EmpowerID – EmpowerID IAM Suite

EmpowerID is an identity management and cloud security company headquartered in Dublin, Ohio, USA. Founded in 2005, EmpowerID provides multiple products in a suite and offers EmpowerID IAM Suite as its IGA product. It includes identity lifecycle management, group management, risk management, password management, role mining, access recertification, policy-based access control (PBAC), Azure RBAC management, Azure identity management and SharePoint online access management.

EmpowerID has a microservices-based architecture. The core components such as identity governance, access management, privileged access management are structured as microservices to allow independent and easy scalability. EmpowerID leverages Docker containers for packaging and deploying its microservices. EmpowerID employs Azure Kubernetes Service to orchestrate its microservices for automating deployment, scaling and timely patch updates.

EmpowerID has a SCIM microservice connector template allowing to quickly develop a SCIM compliant connector without knowing EmpowerID's API or SCIM. New features from the latest release are a Java based version of EmpowerID's SCIM microservice connector framework. They also have a SCIM Virtual Directory Server. They support a wide range of connectors to SaaS and on-premises systems. SCIM and SCIM 2.0 is supported for identity provisioning.

EmpowerID provides strong role governance features that support role design and SoD compliance. The solution has a fine-grained real-time access control policy engine. The policy engine employs big data approach to recalculate all hierarchy's inheritance and resultant access every 10 minutes. This allows the solution to have powerful policies and modelling to be employed to define access while still allowing an instantaneous answer for real-time decision. The solution has a new business request engine which performs risk and SoD checks for all new access requests. Risk-based analysis of identities, role mining, recertification recommendations, and various outlier detections are also provided in the solution through its intelligence capability. EmpowerID offers a no code workflow engine.

EmpowerID can be deployed on-premises, public cloud, private cloud, and hybrid. On-premises deployment includes Docker, Red Hat, Rancher Labs, Pivotal and SUSE container-based platforms. The solution can also be delivered as a managed service, software deployed to the server, or SaaS. EmpowerID's functionalities are exposed via SOAP, REST, SCIM, SQL, OAuth, SAML and LDAP APIs. They have a workflow studio IDE that supports creating APIs. The APIs need to be published and run on EmpowerID or Azure as App Services or Functions. The solution supports all the functionalities via java, .NET, and JavaScript SDKs. EmpowerID also provides iOS and Android mobile applications where the source is shared with customers via SDKs.

EmpowerID offers a solution with strong IGA and access management capabilities. EmpowerID customers primarily reside in North America and the EMEA regions targeting mid-market to enterprise-sized organizations. Their partner ecosystem is relatively small, with a majority from Europe. Their roadmap includes an enhanced user interface, automating complex requests using LLM, real time risk mitigation and contextual decision making, among others. EmpowerID is a preferred choice for organizations looking for a comprehensive IGA solution with integrated access management features.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive



Table 8: EmpowerID IAM Suite's Rating

Strengths

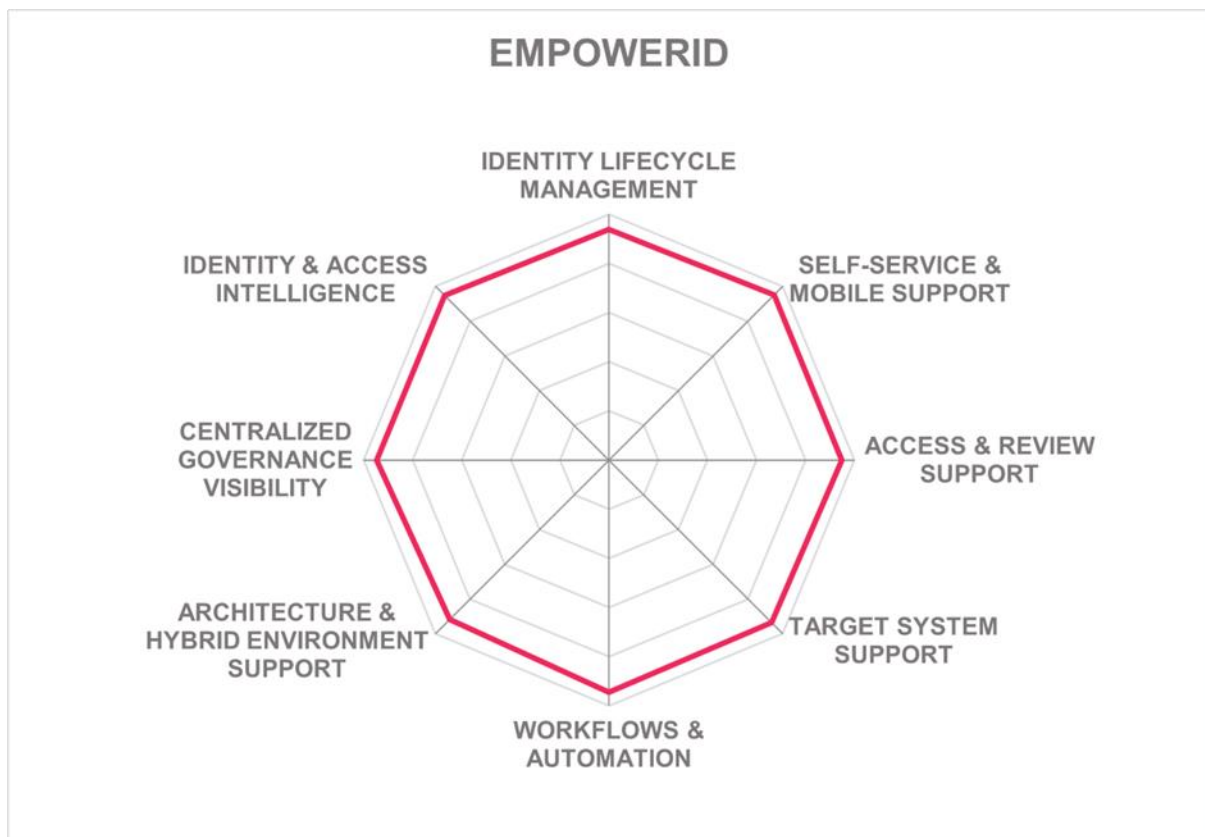
- Supports a wide range of connectors for on-premises and SaaS systems
- User experience in ServiceNow is embedded with all EmpowerID functionalities. Can embed many workflows in ServiceNow using native ServiceNow UI
- User interface is modern, graphical and user friendly
- Workflow engine is no code and uses a drag and drop approach
- Real time risk analysis is provided through the risk analytics functionality
- API functionality is very strong

Challenges

- Relatively weak partner ecosystem
- Support for some SDKs in missing
- Anomaly and identity outlier detection is missing

Leader in





E-TRUST – HORACIUS IAM

E-TRUST is an identity security and access management company headquartered in Brazil. E-TRUST was founded in 1999 with an initial focus on information security. Later in 2006, E-TRUST launched their Identity Access & Governance product HORACIUS. HORACIUS provides user provisioning and access governance capabilities that include access request, recertification, account mapping, and role & SoD management, with more advanced features such as workflows and identity analytics.

HORACIUS IAM system runs within an operating system instance, typically a virtual machine (VM), having strong coupling between its components. The main components of the system are a HORACIUS application which can be accessed by system admins via web browser includes workflows, business rules, policies, self-service portal. People Base Synchronizer is the other component which is responsible for connecting identity bases and synchronizing registration data to HORACIUS. Other components of the system include a scheduler, queue processor and an event processor. All these components except the HORACIUS application are processes of the operating system and the communication between these components and the application is done via databases.

HORACIUS IAM supports identity provisioning and access governance. SCIM is supported for identity provisioning and deprovisioning. They support creating custom connectors using a low code approach. HORACIUS' connectors are flexible and can manage distinct types of data such as attributes, roles, transactions, and variable attributes. They support a wide range of out-of-the-box connectors to SaaS and on-premises systems.

The solution is capable of handling automated user provisioning, separation of duties, shopping cart-based approach for access requests, access reviews and attestations, orphan account monitoring, or employee and third-party contract termination use cases, as well as providing auto-discovery capabilities to identify accounts, groups, group memberships.

HORACIUS has a dual-portal system for self-service where each portal can be configured with authentication methods tailored to the user's role or access level. One portal can be designed for internal use, and another optimized for external publishing. This dual-portal setup allows for distinct menus to be enabled on each portal.

HORACIUS provides out-of-the-box integration to ITSM tools for ServiceNow, Atlassian Jira ServiceDesk, GLPI and any other that supports REST connector. The solution supports out-of-the-box workflows that include registration, orphan account management, account request and review, and SoD, etc. are given. The solution's access governance capabilities includes role discovery, recommendations, risk scoring, anomaly, and outlier detection. HORACIUS has an orphan account reconciliation feature which identifies and manages accounts that are no longer associated with active users or employees.

HORACIUS IAM has a good customizable user interface for the end user. The home page is defined with good tile graphs for admin and manager. The solution supports customization of business rules efficiently. The reporting user interface has a slightly outdated appearance, however, detailed reporting of access rights for auditing is available. The solution has good authentication options for user self-service and admin access which supports biometrics, MFA, and FIDO.

E-TRUST offers all major deployment models for HORACIUS IAM. It can be delivered as-a-service, container (Docker, Redhat, Almalinux), as a managed service or can be deployed as software to the server. The solutions supports full multitenancy using Amazon Web

Service (AWS) for cloud delivery. Most of the functions of the solution are exposed via SOAP, REST, SCIM APIs while only limited functionalities are supported via CLI. The solution's SDK support is limited to Java, PHP, and MS PowerShell. A developer portal is missing in the solution for documentation and training purposes.

E-TRUST customers are primarily medium to mid-market mainly in Brazil. Their roadmap includes the introduction of intuitive wizards to simplify the integration process for AWS and GCP IAM connectors. E-TRUST is a good fit for organizations with access governance requirements to satisfy the most common identity lifecycle administration use-cases with customer-focused in the Latin American region.

Security	Positive
Functionality	Strong Positive
Deployment	Neutral
Interoperability	Positive
Usability	Strong Positive



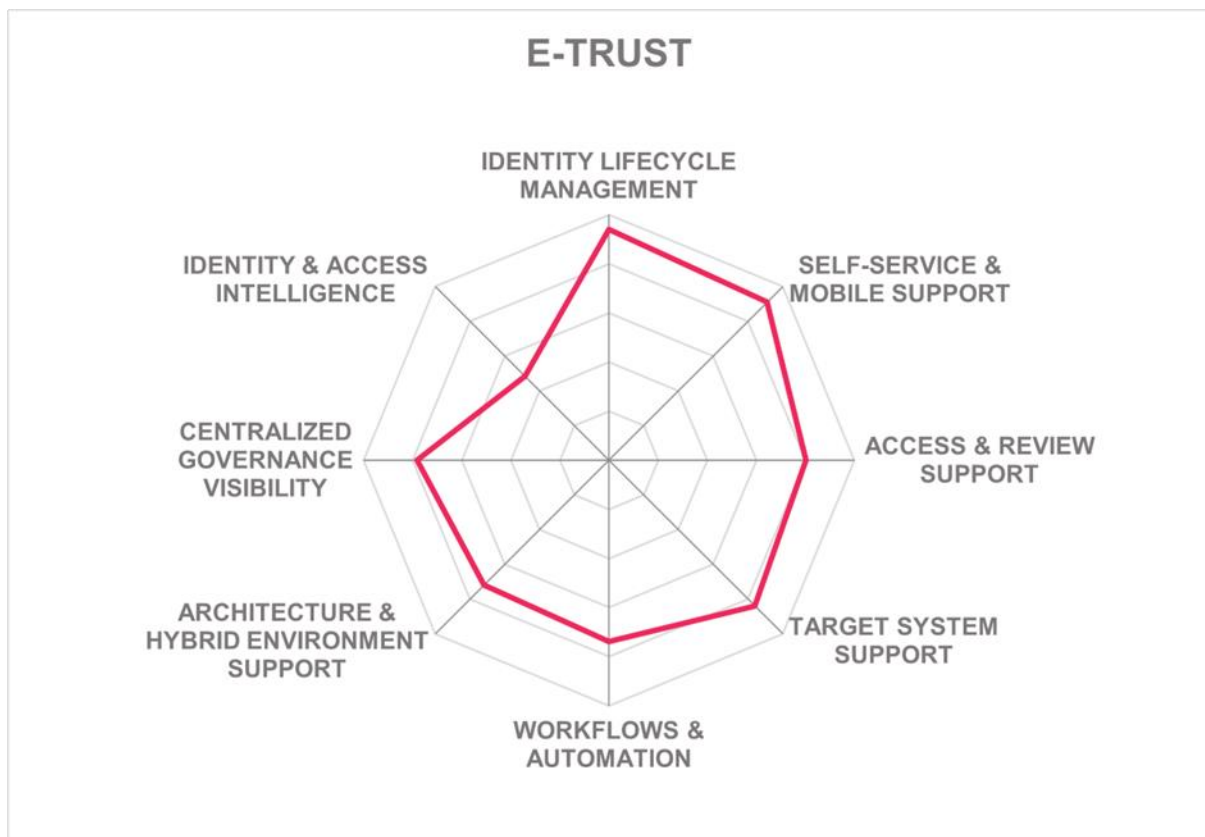
Table 9: HORACIUS IAM's Rating

Strengths

- Covers all major areas related to identity lifecycle management capabilities
- Strong presence in the Latin American market especially in Brazil
- Supports all known platforms and programming languages for delivering SDKs
- Admin's user interface can define all known access policies
- Wide range of out-of-the-box workflow templates are provided
- Anomaly and outlier detection are available using AI and machine learning
- Solution supports all major types of deployment and delivery options

Challenges

- Limited presence outside Brazil
- Does not have experience with creating reports for major compliance frameworks such as FERPA, FISMA, FIPS 200, CCPA, NERC CIP, PCD DSS and CIS
- Support for AI and machine learning for risk analysis and facilitating workflows is missing



Evidian – Evidian IGA for On-Premises solution, Evidian IDAAS Governance with Analytics capabilities

Evidian is an established IAM business with headquarters in France with customers in the finance services, manufacturing, retail, transport, telecom, media, utilities, and public health sectors. Evidian is a dedicated division for the digital security service line of Eviden at Atos. Both Evidian Identity Governance and Administration (IGA) and its option Evidian Analytics are evaluated together as its overall IGA solution in this Leadership Compass.

Evidian offers multiple products in a suite. Evidian Identity Governance and Administration (IGA), offers basic Access Governance in addition to strong on-premises identity lifecycle management capabilities.

Evidian IGA supports automated provisioning and deprovisioning in real time. This applies to capabilities around joiner, mover, leaver, recertification campaigns, orphan accounts, and access request workflows. The solution supports SPML and SCIM for identity provisioning.

Evidian IGA supports a wide range of out-of-the-box connectors for on-premises systems while connector support for SaaS systems lacks breadth of options. The solution delivers a customizable connector for systems without an out-of-the-box connector. The customizable connector is based on the development of a dedicated web service, which implements the custom part of the connector to fit it to the specific target system. Evidian suggests any programming language such as Java, C, PHP, C# that can enable the use of SOAP/WSDL may be used to develop this connector. The solution supports out-of-the-box integration to ITSM tools such as ServiceNow, JIRA and EasyVista. Evidian suggests support for additional ITSM tools can be expanded using the provided SDK.

Evidian Analytics is a new option answering the increasing requirements of advanced Access Governance. It is based on Kubernetes Cloud Infrastructure and OpenSearch Stack, giving Evidian the ability to provide good analytics dashboard capabilities, audit analyses, data history, and data access control.

Evidian IGA supports all major deployment models. The solution is delivered as a SaaS, container (Docker), container orchestration system, managed service or as a software deployed to the server. The solution can also be installed on a virtual machine. Most of the functionalities of the solution are exposed via SOAP, REST, SCIM, OAuth, SAML and LDAP APIs. Evidian provides information around identities, policies, organizations, and audit through APIs. Evidian provides support for SDKs such as Java, .Net, JavaScript while Android and iOS integration is available using open source OIDC SDKs like AppAuth and Nimbus.

Evidian has a modern user interface with customizable dashboards and pre-configured applications. Evidian IGA has invested in AI in IAM functionalities and is using generative AI for separation of duties, insights about security policy, analytics and reporting features and other administrative tasks. They are investing heavily on decentralized identity and its integration in IDaaS. Evidian IGA supports all major authenticators for user and admin self-service with support for all third party passwordless authentication providers.

Evidian IGA has a dynamic and flexible policy model for managing access policies. The security model is based on the implementation of the RBAC model. PBAC is used to define internal rights of the users in the solution. The solution supports definition of risk level of scores for recertifications. Evidian IGA's reporting and analytics has a modern layout with

the possibility to edit filters when defining parameters. The analytics feature supports the creation and modification of dashboards, modification of visualizations, generate reports from various sources and have a cross domain-based dashboard for better IAM data correlation.

Evidian's customers and their partner ecosystem are primarily focused in the EMEA region serving mid-market to enterprise-sized organizations. They have a significant number of customers in North America and APAC region especially in Japan and Singapore. Their roadmap for the next 12 months releasing updated versions of the Evidian Analytics, Evidian IGA and Evidian IDaaS Governance. Other roadmap features are contract management, self-sovereign identity, PAM integration, role mining, verifiable credentials and focused on using generative AI and machine learning for prescriptive IAM. With a regional but strong partner ecosystem across Europe, ATOS acquisition is likely to help Evidian gain access to large customers and enter new geographies.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive



Table 10: Evidian's Rating

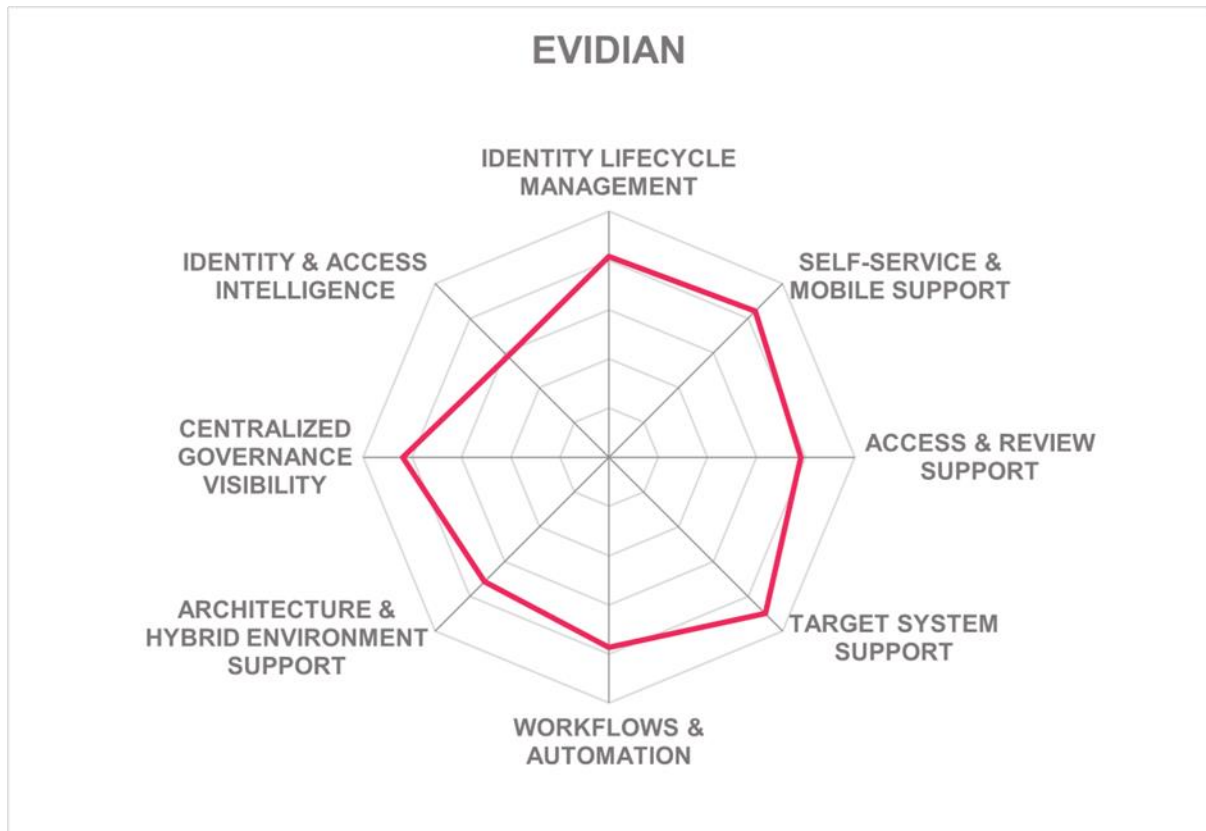
Strengths

- Supports wide range of connectors for on-premises systems
- Analytics capabilities are comprehensive and cover out-of-the-box reports for all major compliance frameworks
- API support supports wide range of industry standard protocols such as SOAP, REST, SCIM, LDAP, SAML and OAuth
- User and admin self-service includes support for all major authentication protocols including passwordless authentication
- UI is modern and user friendly with drag and drop customizable feature for dashboard management
- Intelligence capabilities powered using AI support wide range of functions for security, administration, and analytics

Challenges

- Limited presence and partner ecosystem in USA, only present in EMEA and APAC (mainly Japan)
- Does not cover out-of-the-box integrations to some ITSM tools
- SDK support is limited to Java, JavaScript, and .NET

Leader in



Evolveum – MidPoint

Evolveum is an Open Source IAM vendor based in Slovakia. Founded in 2011, Evolveum's midPoint product is provided as an open source but needs a subscription for professional services. MidPoint being an open-source complete IGA suite is one of its major differentiation factors.

MidPoint's open-source IGA platform is Java based. It is a consistent software system with a well-defined architecture that has been in function for more than a decade now. It can be used in microservice, multiservice, service-oriented, distributed or any other architectural solution.

MidPoint supports SCIM for identity provisioning and deprovisioning. Just-in-time provisioning is also supported by the solution. It supports connectivity to bespoke systems through different options such as by using the midPoint REST API, by creating custom connector, by accessing midPoint DB or by extending the midPoint source code. The solution has limited support for out-of-the-box integration to ITSM tools but can be integrated by creating a necessary connector.

MidPoint supports a good number of out-of-the-box provisioning connectors for on-premises systems, however only a few out-of-the-box connectors to SaaS systems are available. Attribute mapping between connected systems can be scripted using Groovy, JavaScript (ECMAScript), and Python programming languages. MidPoint uses flexible policy-driven mechanism for processes such as access approvals, access certifications, and SoD. For example, the approval engine will compute the approval process for access approval by policy rules which are applied to roles.

Due to its open-source nature, midPoint is offered as a product with no license fees and support subscriptions are available for product support and development. MidPoint's features for access governance include a centralized role management that consists of role discovery support. MidPoint has added role mining in the midPoint 4.8 release in October 2023 that can help with simplifying Role Based Access Control (RBAC) by suggesting new candidates for business roles based on the existing data. In addition to other governance features, midPoint supports role lifecycle management and data protection. They provide policies for RBAC and organizational structure that can be used for SoD use cases. Evolveum leverages a strong skillset around computational engineering to continuously develop and improve the advanced IGA features. Recent examples are role mining, simulations, user experience, and self-service support.

MidPoint offers a unique simulation feature, which has various benefits. It not only aids in predictive analysis but also plays a crucial role in data cleanup and integrity maintenance. Evolveum suggests it can assist in identifying issues with HR data efficiently, providing support thorough cleaning of HR data and/or application inventories, and reducing the overall risk of data corruption. The usefulness of these simulations is notable, as they are available for a wide array of objects, including users, applications, and roles. To further enhance analysis of simulation results, object marking is employed to categorize different issues related to data quality. This function prevents inadvertent damage and generate valuable insights for creating informative dashboards. Additionally, the inclusion of a role mining feature adds to the system's comprehensive capabilities, making it a robust solution for Identity Governance and Administration.

Evolveum has designed midPoint as a universal product which supports deployment in the cloud, on-premises or in a hybrid model. MidPoint is also available in the form of container images and as a standalone Java application. Another option allows a more customizable open-source style using Apache Maven as a build system allowing for customization. The solution also supports private cloud deployment. Almost all of midPoint's functionality is exposed via different APIs such as REST, SQL and SCIM. Their SDK support is currently limited to Java and Python programming languages. Evolveum provides plugin for their intelligent platform midPoint Studio which can help systems integrators.

MidPoint has a good user interface with functional and configurable dashboards and widgets. Role request is available through a shopping cart approach and the solution displays the status of the access request. There is a workflow in place for approval of requests and the solution also supports bulk approval. Reporting capabilities are available based on native report mechanism, although the solution is missing support for major compliance frameworks out-of-the-box reports. Noticeably, midPoint is missing more advanced identity and access intelligence capabilities, however they are included in the product roadmap. Role catalogue model is on par with shopping cart paradigm in terms of execution. Updated user interface is a strong improvement from the previous version and the solution now focuses on low code approach for end users.

Evolveum customers are primarily focused in the EMEA region with North America coming in as the second most important region. Evolveum's customer deployments include medium to enterprise companies and universities. MidPoint provides good on-premises DevOps options and hopes to move towards a hybrid or a full cloud environment in the future. Overall Evolveum midPoint continues to improve and may be of interest to organizations looking for a complete IGA suite. Evolveum has plans to further enhance and work on identity analytics, role mining, outlier detection, risk management and a next gen user self-service support.

Security	Neutral
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive



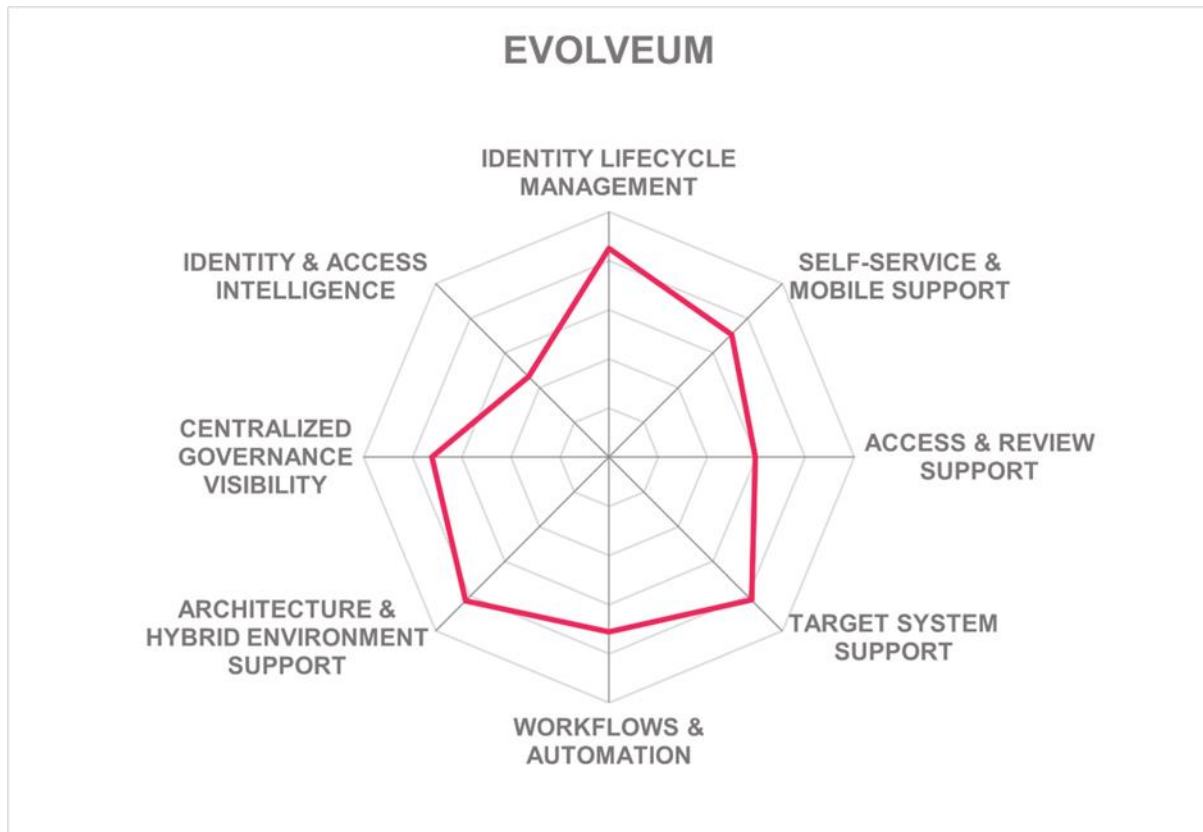
Table 11: MidPoint's Rating

Strengths

- Open-source solution provided at no (license) cost
- Simulation features provides forecast in terms of ability to see the expected outcome in a controlled environment
- Good use of AI/ML for role mining
- Object marking helps to prevent damage, make analysis through configurable dashboard
- MidPoint supports flexible authentication
- Possibility to modify connectors via coding
- Open access is provided with unlimited testing before adoption of the solution

Challenges

- Limited but growing partner ecosystem outside EMEA
- Limited number of major compliance frameworks for reporting supported
- Integration to third party ITSM solution is not available out-of-the-box but can be created through request
- SDK support is limited to Java and Python



IBM – IBM Security Verify

Founded in 1911, IBM, through its IBM Security Verify product, remains one of the largest global IGA vendors for large-sized complex IGA deployment. IBM Security Verify is available as a SaaS solution with IAM capabilities, including single sign-on, MFA, adaptive access control, identity lifecycle management and governance and access governance, and identity analytics capabilities for workforce and consumers. IBM Security Verify Governance and IBM Security Verify SaaS are IBM's current IGA solutions.

IBM Security Verify SaaS is a cloud solution based on microservices and supports multitenancy. The Identity Manager component of Verify Governance is modernized to run in Kubernetes and RedHat OpenShift based container platform while other components are in the process of getting modernized. Verify Dedicated is a fully managed single-tenant deployment for large enterprise. It can be deployed in any region of choice, with high performance scale to guarantee 1000 Transaction Per Second (TPS), and it is priced at a per instance level including infrastructure, operations, and application services management.

IBM Security Verify supports all known major deployment models. The solution can be delivered as-a-service, container based (RedHat OpenShift, Kubernetes), software deployed to the server or as a virtual appliance. IBM also supports managed service using Verify Governance which is provided by IBM Security services. The solution has more than 70 percent of its functionalities available via SOAP, REST, SCIM, SQL, OAuth, SAML and LDAP APIs. They offer SDK support for various programming languages such as for Android, iOS, Java, JavaScript, .NET, and Python.

IBM Security Verify supports SCIM for identity provisioning and deprovisioning as well as API based provisioning adapters across on-premise, cloud and SaaS applications. The solution's out-of-the-box integration support for ITSM tools is limited to ServiceNow. Verify Service Desk is a ServiceNow plugin published in ServiceNow store. It supports access request, access certification, password management and manual fulfilment tickets management. Security Verify supports wide range of out-of-the-box provisioning connectors to both on-premises, SaaS and Cloud infrastructure systems. A custom adapter framework allows customers to build integration to any bespoke systems. The solution's identity lifecycle management covers all aspects from onboarding to off boarding and uses AI and machine learning to analyze parameters of user and requested access.

IBM Security Verify has a modern and user-friendly web browser-based interface. The solution supports passwordless login through QR code for end user, admin, or manager personas. The dashboard provides a tile-based view of all the applications assigned to the user. IBM Security Verify's application management dashboard is even more refined and provides a well-defined layout for application configuration and onboarding including attribute mapping, and single sign on wizard configuration. The solution provides end users and admin with a wide range of authenticator options for access including FIDO2, and FIDO2 U2F. They offer access request and access review by a risk level which is shown in terms of entitlements. The solution also has configurable out-of-the-box policies based on best practices for the analytics model.

IBM Security Verify also provides identity analytics capabilities responsible for providing activity and entitlement data from variety of sources that shows 360 degrees of access and associated risks and will further leverage generative AI to establish identity risk patterns and report unidentified risk patterns. The solution will also introduce Generative AI to automate IGA controls and clean up entitlement mess by recommending enforcement actions. The

recommended actions are generated using AI with details such as risks scores for each task. The reporting model for threats is also supported on this platform.

IBM currently serves customers mainly in the North American region with growing number of customers in APAC and EMEA regions. Their customers are mainly from the finance, insurance, and the public sector. IBM Security Verify Governance continues to move its long line of mature IGA solutions in a positive direction with some significant updates related to leveraging AI. Their roadmap includes creating a unified platform across on-premises, SaaS, and hosted deployments. Other roadmap features include integration of identity fabric use cases, ITDR integration use cases, application integration flexibility aimed at supporting flexible UI and enabling DevOps automation. Overall, the solution is competitive and an interesting solution in the IGA market for enterprise customers. IBM also benefits from its own strong professional services and excellent partner ecosystem, plus easy integration within the overall IBM Security product portfolio.

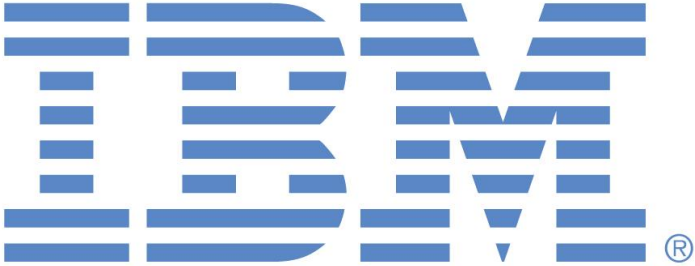
Security	Strong Positive	
Functionality	Strong Positive	
Deployment	Strong Positive	
Interoperability	Strong Positive	
Usability	Strong Positive	

Table 12: IBM Security Verify's Rating

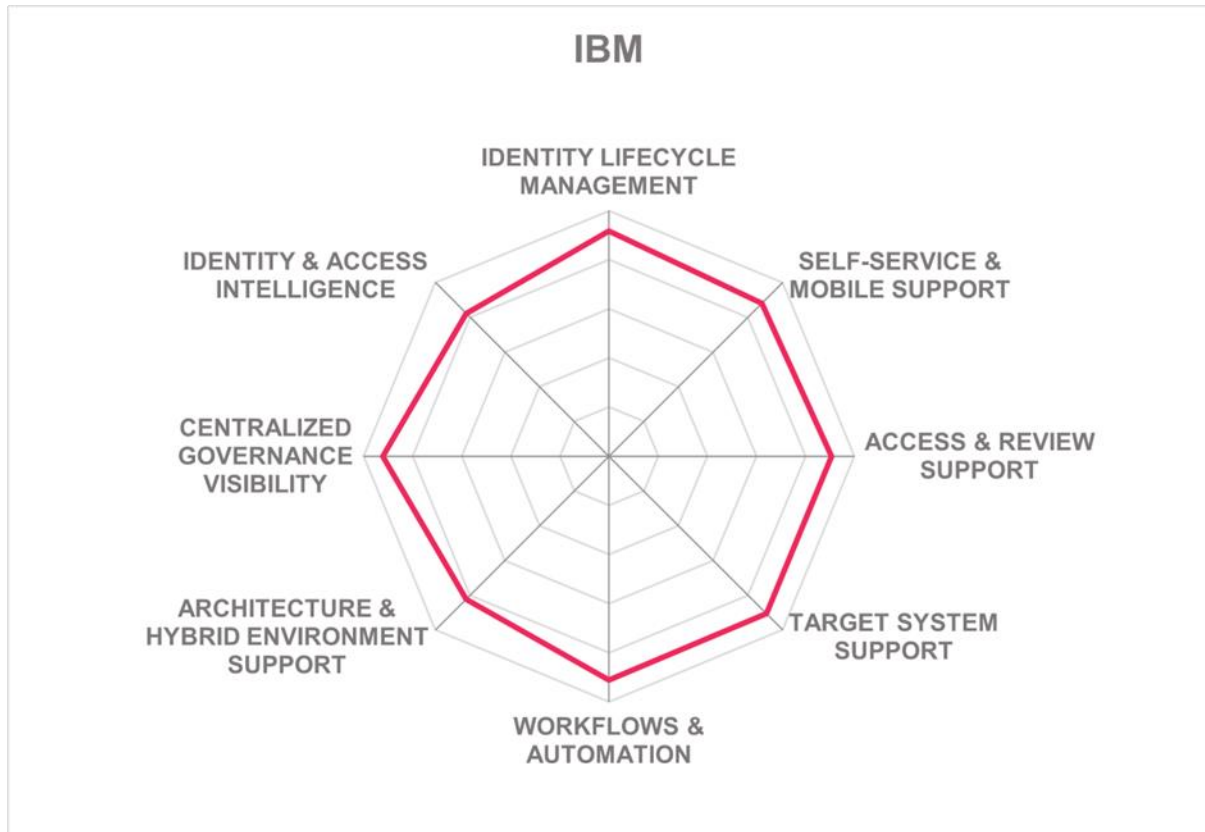
Strengths

- Broad set of connectors supported for both on-premises and SaaS deployments
- User interface is modern and user friendly
- Cloud solution based on microservices and supports multitenancy
- Provides support to all major API protocols such as SOAP, REST, SCIM, LDAP, SQL, OAuth, SAML
- Uses AI for user entitlement risk insights, recommendations, and remediations
- Risk model for access requests, threats is well defined
- Strong partner ecosystem and professional services
- Access request workflow supports many varieties of request contexts with out-of-the-box templates
- Global presence with 24/7 support depending upon incident severity

Challenges

- Does not support out-of-the-box reports for major compliance frameworks
- Presence outside North America is less than half of overall client based, but growing
- Some advanced intelligence capabilities leveraging AI are missing

Leader in



Identity Plus – Cross Identity

Identity Plus, formerly known as Ilantus Technologies, is headquartered in Illinois, USA. It was founded in 2000. Cross Identity is Identity Plus's converged IAM solution which supports Data Access Governance (DAG), Cloud Governance for Infrastructure as a Service (IaaS), and Privileged Access Governance (PAG). Cross identity offers a comprehensive identity governance solution that is designed to manage a wide range of identity types within an organization.

Cross Identity is a cloud-based SaaS identity governance solution. The solution has a collection of loosely coupled, independently deployable microservices. Each microservice is focused on a specific business capability and communicates with other services through well-defined APIs. Cross Identity employs a multitenant architecture where it supports the same version in cloud as well as on-premises deployments.

Cross Identity supports SCIM protocol for identity provisioning and deprovisioning. Automated provisioning is also supported for access management through predefined rules. Cross Identity use SCIM to integrate with a wide range of applications that also support the SCIM standard, streamlining the process of managing user accounts and access rights. It supports out of the integration through APIs to third party ITSM tools such as ServiceNow, Cherwell, Atlassian JIRA ServiceDesk and Remedy. The solution supports a wide variety of connectors for SaaS and on-premises systems.

Cross Identity provides a self-service access request management user interface as part of its identity governance and administration solutions. It has several user-friendly features such as self-service portal, flexible access request and approval workflows, self-service password reset and account unlock features, access review and certification capabilities, role-based access requests, policy violation notifications, and support for mobile access. The solution also supports delegated administration. Cross Identity has a comprehensive capability for reporting. It supports reports for all major compliance frameworks and also has its own analytics module for supporting access intelligence features.

Identity Plus has an established customer base in North America, EMEA, APAC and Latin America. It is mainly focused on the mid-market segment for its IGA solution and supports customers from most of the industry verticals. They have an extensive roadmap for Cross Identity which is focused on automated role mining, natural language processing for access requests, behavioral biometrics, and automated policy enforcement.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Strong Positive

CROSS IDENTITY
I A M C O N V E R G E D

Table 13: Cross Identity's Rating

Strengths

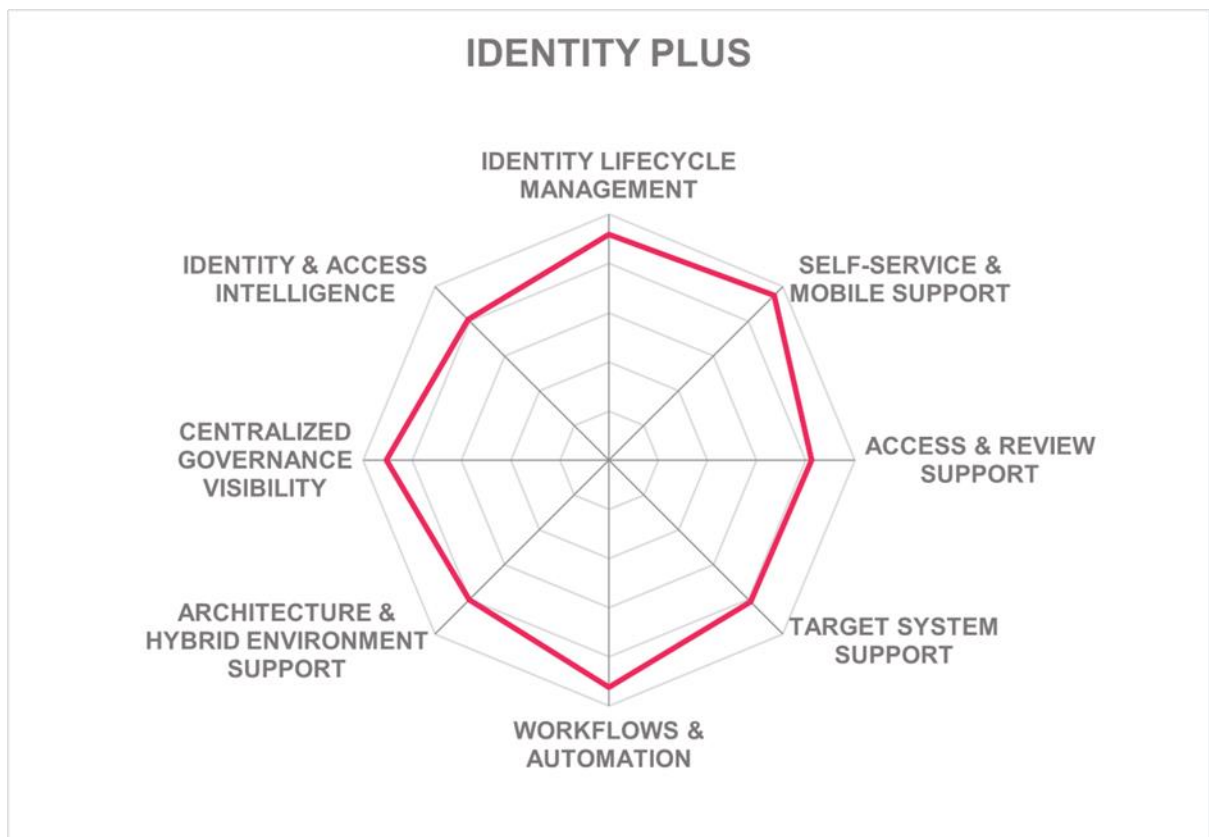
- Identity governance solution offers extensive features for managing and controlling access rights
- Provides an inbuilt identity analytics to support access intelligence
- Automated campaigns for access reviews
- Policy management offers extensive features related to ABAC and RBAC
- Reporting capabilities are impressive with support provided for out-of-the-box reports for major compliance frameworks
- API support includes protocols for SOAP, REST, SCIM, LDAP
- Multiple deployment and delivery options
- Supports all major connectors for on-premises and SaaS systems

Challenges

- Customer base is currently focused on mid-market segment but growing in enterprise segment
- Policy testing tool is not available out-of-the-box
- Functionalities cannot be exposed via CLI

Leader in





ManageEngine – AD360

ManageEngine is an entity of Zoho Corporation headquartered in Texas, USA. It was founded in 2002 and has grown into a large organization with offices in North America, EMEA and APAC. Identity 360 is ManageEngine's SaaS deployment product and AD360 is their on-premises deployment product for IGA. Both the products are focused on providing capabilities related to identity orchestration and integration, risk assessment, template-based provisioning and deprovisioning, and real time security event monitoring logs. In this report we evaluate both the products.

The AD360 architecture consists of modules for a web client, an application server, and the database. SCIM is supported for identity provisioning and deprovisioning. The solution supports out-of-the-box integration for various ITSM tools such as ServiceNow, Atlassian Jira ServiceDesk, ManageEngine ServiceDesk Plus among others. They support a limited number of out-of-the-box provisioning connectors for on-premises and SaaS systems, however other connectors can be customized based on requirement.

AD360 has features that identify potential risks and provide remediation measures such as identity risk assessment, and access governance feature such as access certificate campaigns that verifies and reviews the access rights granted to individuals. Most of the functionalities of the solution are available via REST, SCIM, LDAP, OAuth and SAML APIs. Their SDK support is limited to Android and iOS programming languages.

AD360 has a self-service portal that supports various capabilities such as access request, and an interface to view the status of requests. The solution has strong support for various authenticators for user and admin self-service however support for FIDO is missing. The solution offers delegated administration through delegated workflows. AD360's offline MFA is one of its unique features. Identity risk assessment feature in ADManager Plus provides a comprehensive view of the threat landscape to identify the plausible loopholes, evaluate them, and offers insights on the harm that they might cause and how to proactively get rid of them and secure the network.

ManageEngine has an established customer base in North American with growing presence in EMEA, APAC, and Latin America. Their roadmap includes SoD controls, role-based access control, user behavioral analytics adoption for conditional access, REST API support, and leveraging machine learning for various access support features.

Security	Neutral
Functionality	Neutral
Deployment	Neutral
Interoperability	Neutral
Usability	Positive

ManageEngine 

Table 14: AD360's rating

Strengths

- Supports majority of features related to identity life cycle management

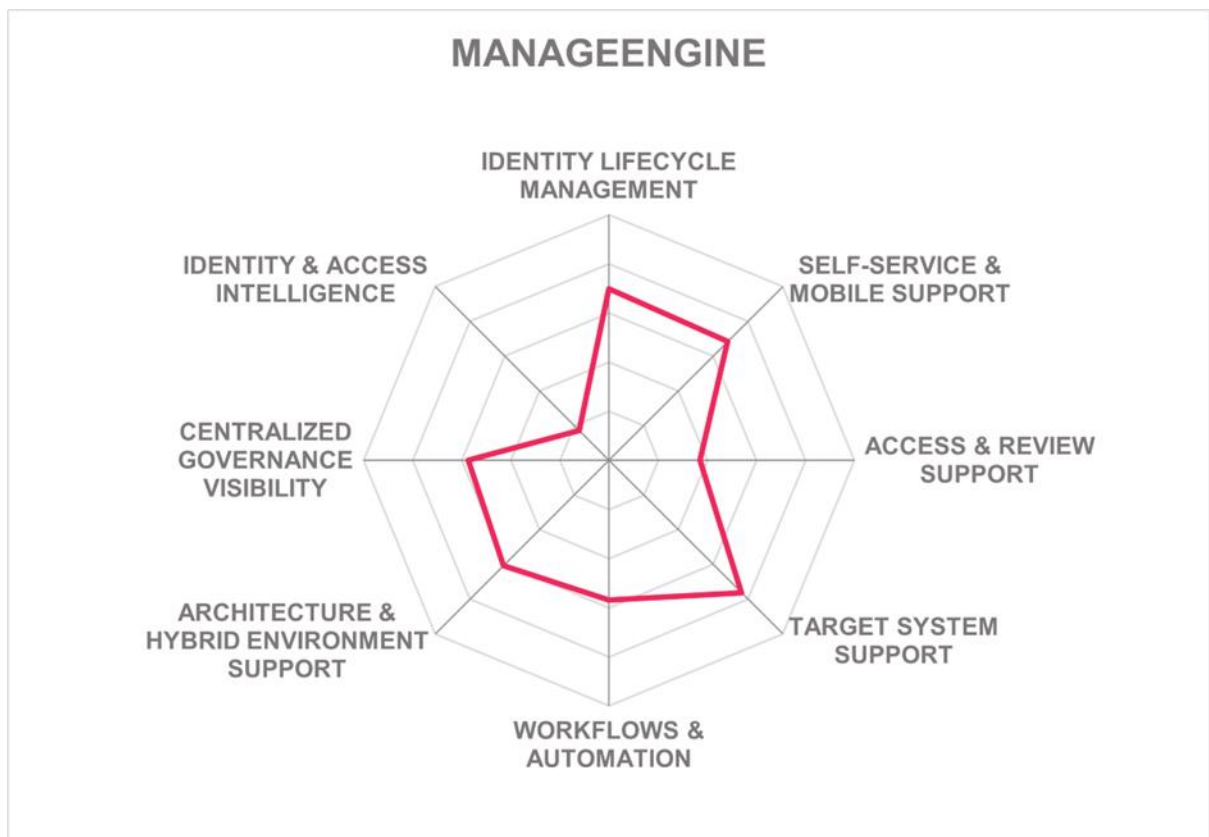
- Deployment is supported for various models such as cloud, on-premises, hybrid
- All the functionalities of the solution are available via APIs
- Supports wide variety of authenticators including passwordless
- Reporting capabilities support all formats, types and out of the reports for most of the major compliance frameworks
- User access monitoring is supported for risk assessment
- Supports wide variety of out-of-the-box templates for workflows

Challenges

- Limited coverage of access intelligence capabilities
- Separation of duties for toxic combinations is when requesting access is missing but it is in roadmap
- Container based platform deployment is not supported
- Solution lacks no code/ low code approach
- Event based micro-certification is not supported

Leader in





Microsoft – Microsoft Entra ID Governance

Founded in 1975, Microsoft has its headquarters in Redmond, Washington, USA. Microsoft Entra ID Governance is Microsoft's IDaaS solution for IGA use cases which covers these capabilities for all types of applications. Entra ID Governance can also be managed by Managed Service Providers (MSPs) for their customers.

Microsoft Entra ID Governance is a multitenant IDaaS solution, with optional agents which a customer can deploy in their data center or private cloud environment to extend the reach of Entra ID Governance to private network-hosted applications. When connecting to an on-premises Active Directory or to an on-premises application during workflow and request processing, a lightweight agent would be needed for synchronization. A Windows Server installed with Microsoft Identity Manager and/or Entra ID Connect would be required for more advanced on-premises scenarios not yet supported with the lightweight agent.

Most of the functionalities of the solution are exposed via REST and SCIM APIs. The solution supports a wide range of SDKs including Android, Java, .NET, JavaScript, Powershell and Python. A developer portal is available for documentation and tutorials for helping with development, integration, configuration, and deployment.

Microsoft Entra ID Governance supports automated workflows for identity lifecycle management of users and guests. However, it lacks CI/CD support when creating custom workflows. Lifecycle workflows orchestrate employee joiner, mover, leaver process with low-code and no-code workflow design. Entitlement management supports review and granting of access through defined policies. Automatic assignment of access is also conducted with Segregation of Duties (SoD) checks.

SCIM is widely supported for identity provisioning. Microsoft provides a guide on how to setup a connection between the Microsoft data model and the SCIM data model as well as for solutions such as LDAP directories and Microsoft Active Directory not having a SCIM interface. There is also support for automated provisioning and deprovisioning into Microsoft SharePoint Online sites, Microsoft Active Directory, and Microsoft Entra ID as well as Microsoft Teams. Onboarding and offboarding of user accounts can be triggered automatically based on detected changes in the incoming data from identity sources such as HR/ HCM systems. The solution currently lacks automated reconciliation support that allows analyzing and comparing changes in target systems and Microsoft Entra ID Governance. This is a roadmap feature. Microsoft supports a good range of out-of-the-box connectors for SaaS systems. Support of connectors to on-premises systems is limited, especially for target systems requiring integration via proprietary APIs instead of standards such as LDAP, ODBC, or SCIM. The solution has a new feature dedicated to additional HR services related to HR ISV ecosystem. This feature supports integration with Microsoft Entra ID Governance through the HR inbound provisioning API.

Entra ID Governance's support for out-of-the-box integration to ITSM tools for automated creation of support tickets in manual fulfilment is limited to ServiceNow. There are policies in place for Privileged Identity Management (PIM) capability, which is rarely found in IGA solutions. PIM also supports Just-In-Time (JIT) provisioning of critical access entitlements.

Entra ID Governance supports self-service guest user provisioning and assignment of entitlements based on user attributes and defined lifecycle policies, thus reducing the effort for managing temporary users and their entitlements. However, support for some other

capabilities such as delegated administration for groups of users is currently missing. The solution also supports a good set of authenticators for user self-service and admin access.

Microsoft Entra ID Governance supports access certification as single-stage or multi-stage access certification. This is done at the level of SaaS applications, cloud group memberships, Teams, Teams shared channels, and Microsoft Azure role assignments. For other applications such as on-premises applications or for entitlement-to-role assignments, certification is not supported. Microsoft Entra ID Governance provides access packages which can integrate application-specific entitlements and also assignments to other Microsoft applications. This helps to simplify the entitlement management.

Entra ID Governance's user interface is API driven, modern, and well-structured with tiles and functions available on the configurable dashboard. Entra ID Governance supports provisioning analysis and policies for user activity monitoring. The solution is leveraging machine learning for recommending access rights based on comparison of employees or other similar attributes. Machine learning based recommendations are also provided for access reviews.

Microsoft Entra ID Governance is available in regions across the globe and supported by a global partner ecosystem. The roadmap includes improving review and management of user's accesses and access reviews for multicloud resources as well as reconciliation. The recently announced Microsoft and SAP partnership will result in deeper integration between Entra ID governance and SAP solutions such as SAP Cloud IAG and SAP BTP.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive



Microsoft

Table 15: Microsoft Entra ID Governance's Rating

Strengths

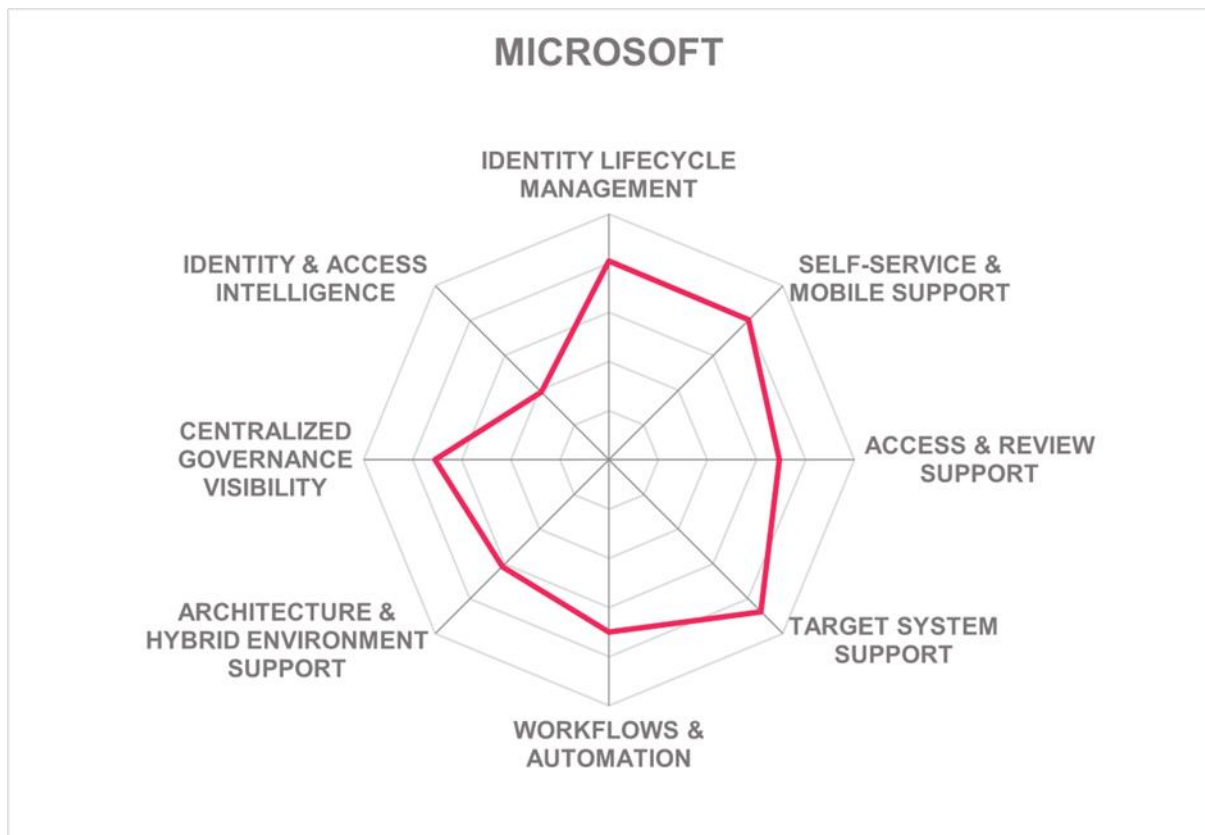
- Graph API framework offers flexibility to manage access across all environments
- User Interface is modern and user friendly
- Supports a wide range of connectors for SaaS systems via SCIM, further integration supported via LDAP and to SQL databases
- Deep integration into the Microsoft Office 365 environment including Teams and SharePoint Online
- Focus on lean IGA with rapid deployment and efficient usage, potentially reducing IGA workloads in organizations
- User lifecycle management of external users is quick and efficient with very few levels of approvals and thus B2B use cases
- Strong set of APIs and good workflow support based on Microsoft Logic Apps
- Machine learning is leveraged for access requests and access review functions

- Microsoft's Security Stack covers more than 40 security categories which helps customers to deploy a single suite instead of combining products from several vendors
- Privileged access supports just in time provisioning
- Global presence provides a strong partner ecosystem

Challenges

- Lack of automated reconciliation from connected target systems
- Does not cover out-of-the-box reports for major compliance frameworks
- Limited connectivity to legacy on-premises applications requiring integration via proprietary APIs
- Baseline role model, no support for hierarchical roles, and limited SoD (Segregations of Duties) support

Leader in



N8 Identity Inc – TheAccessHub

N8 Identity is an identity governance company headquartered in Ontario, Canada. It was founded in 2000 and has been focused on creating autonomous identity governance through AI driven identity solutions. TheAccessHub is their IGA solution, focused on identity learning fabric, leveraging AI and machine learning for recommendations, intelligence, and overall lifecycle of identity.

TheAccessHub is built in the cloud utilizing a modern, API-based microservices architecture. For connection to on-premises systems, it is deployed as a single VM instance, utilizing an on-premises Access Gateway virtual appliance deployed in the customer's data center. TheAccessHub is largely platform agnostic and was designed to easily be implemented in a variety of scenarios. Container based platform is supported for Ubuntu Linux Container single page application, typically deployed in Microsoft Azure in N8 Identity's tenant. The primary technology supporting TheAccessHub consists of Kong API Gateway, Postgres Database, Angular Web App and Java Backend.

TheAccessHub leverages an AI centric model for access recommendations after evaluating user's access based on peer analysis and alignment with compliance rules and policies. The built-in AI and machine learning assesses all access and entitlements held by all users in the system. Users' business activity drives additional or unique access requests, which the AI and machine learning consumes and utilizes to update recommendations and peer analysis views.

TheAccessHub's microservices architectures allows deployment of its modules such access request management, certifications, authentication, provisioning, workflows, and analytics to be deployed individually or as a whole. The solution supports a wide range of out-of-the-box provisioning connectors for SaaS systems as well as on-premises using a gateway that allows for read/write of user accounts and permissions. Overall, more than one hundred connectors are provided out-of-the-box through its TheAccessHub application marketplace. Workflows are supported for automated provisioning and deprovisioning. These workflows are configurable in the UI of the solution.

TheAccessHub supports only cloud delivery for public clouds. It also supports managed services which can be customized based on the requirements of the customer. These managed services are offered as part of its subscription deployment model and includes dedicated N8 professionals for various IGA related services such as identity life cycle management, and certifications. The solution supports less than half of its capabilities via APIs such as REST. Support for other API protocols as well as capabilities exposed via CLIs is currently limited. TheAccessHub utilizes a responsive UI that is fully HTML 5 and leverages APIs thus no SDK is required for mobile support as it is already built in the solution.

TheAccessHub has a similar user interface for admins and end users. It does not support any authentication formats but can integrate with any Identity Provider (IDP) for providing SSO capability. Multifactor, passwordless authentication, FIDO among others is supported as best practice by configuration within the customer's existing Single Sign-On provider. TheAccessHub contains a built-in, out-of-the-box reporting dashboard as the landing page at login. The dashboard presents details of activity and processes in chart format and is customized to their role in TheAccessHub. These charts are segmented into key categories including status of access certification campaigns, data synchronization, risk analytics reporting, and SoD Policy violations.

N8 has significantly improved the solution over the last few years. The latest releases are focused on improving data load, ability to create and maintain hierarchy from external authoritative sources, and real time authorization. This capability allows TheAccessHub to act as the authoritative source (AKA PIP) for an application's most complex fine-grained authorization as entitlements can be retrieved and passed at login by the IDP or queried via a "GetEntitlements" or "IsAuthorized" API. They are predominantly focused on the mid-market segment with most of their customers based in North America. Their roadmap includes issuance and validation of verifiable credentials for front line workers and enhancing integration with Microsoft for leveraging Azure marketplace for near real time provisioning of instances.

Security	Neutral
Functionality	Positive
Deployment	Neutral
Interoperability	Neutral
Usability	Positive

N8IDENTITY

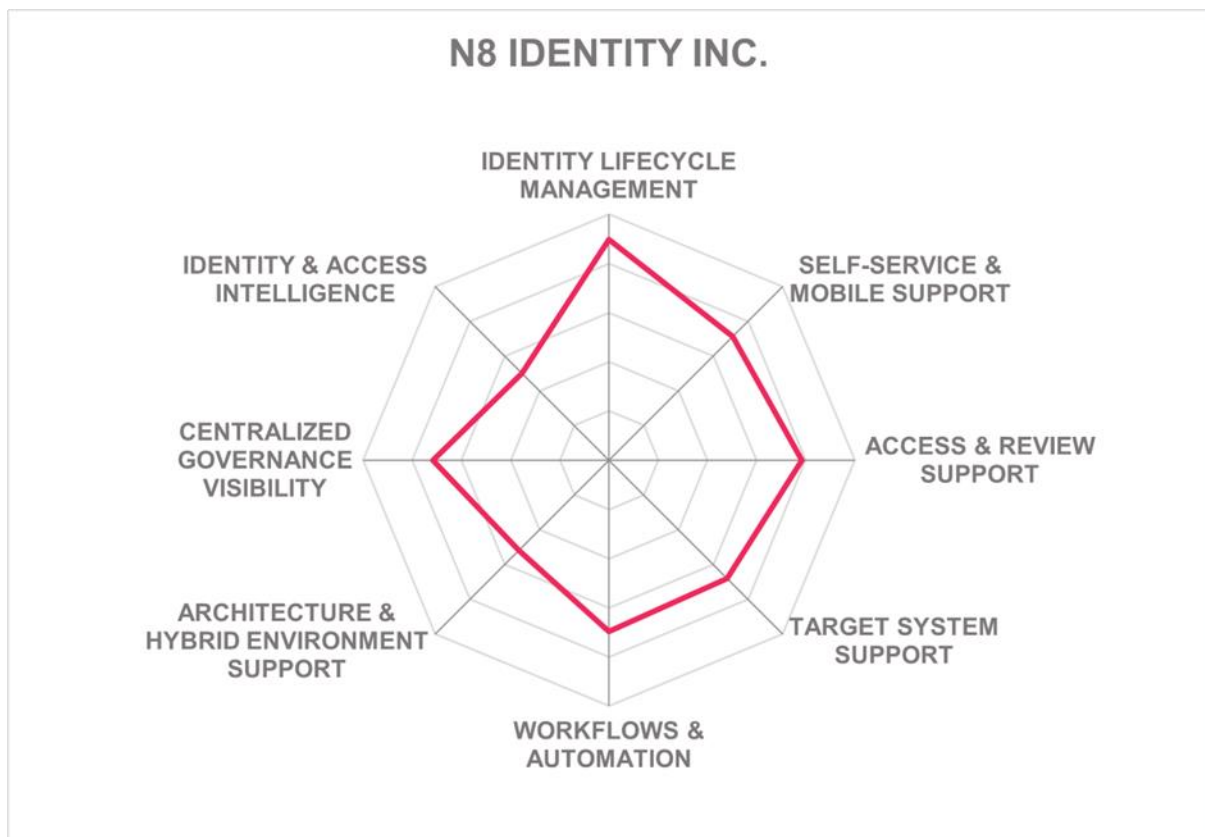
Table 16: TheAccessHub's Rating

Strengths

- Fully microservices based architecture that also supports individual deployment of IGA models
- Dedicated AI and machine learning model for various capabilities such as recommendations
- Built in reporting dashboard is graphical and customizable
- Drag and drop workflow editor is supported in the user interface
- Supports an extensive list of connectors for SaaS systems
- Out-of-the-box integration to third party applications such as ITSM tools is supported
- Multiple user identities can be defined including third party vendors
- Supports a variety of governance use cases

Challenges

- Intelligence features are currently limited to peer group analysis and recommendations
- Depends on third party or customer's SSO provider for providing authenticator services for end user
- Less than half of the capabilities of the solution are available via APIs



Netwrix – Netwrix Usercube

Usercube is a French software company founded in 2009 and acquired by Netwrix in August 2022. Now, Netwrix Usercube is an IAM solution based on the Microsoft Azure PaaS technology platform with capabilities solely dedicated to IGA. Netwrix, with its portfolio of Data, Identity, and Infrastructure security solutions, will develop an integrated security solution with Netwrix Usercube.

Netwrix Usercube deploys a microservices architecture where the microservices represent IGA tasks such as synchronization, identity provisioning, risk detection, access certifications and computing permissions from identity data. Usercube IGA uses a zero code UI and XML based configuration. The architecture provides all extension capabilities in configuration mode. All coding, if necessary, can be done outside of the solution and integrated by using the Usercube REST APIs or CLI. Usercube IGA's complete set of capabilities are available via APIs and CLIs.

The solution supports a wide range of out-of-the-box provisioning connectors for SaaS and on-premises systems. Netwrix Usercube's generic connector interface can be leverage for generating non-out-of-the-box connectors. Netwrix Usercube's generic ITSM connectors allow for quicker integration with ITSM tools such as Service Now, EasyVista, Matrix 42, Jira, and Zendesk. The solution provides generic ITSM connectors to speed up the integration with any ITSM. Netwrix Usercube also provides a fast and easy PowerShell scripting connector to synchronize or provision any identity with any target system.

Netwrix Usercube is offered as a single software available for SaaS and as a subscription based on-premises delivery on all major deployment models. Usercube IGA also supports other deployment options such as Docker container and Kubernetes. For cloud deployment, full multitenancy is supported. They offers SDKs for all major programming languages. Any custom application with any programming language can be integrated via REST API or CLI tools.

Netwrix Usercube has a modern and user-friendly interface with a dynamic and configurable dashboard. It supports configurable attributes along with user activity monitoring. The solution provides risk-based SoD violations before giving access, delegating access or certification. The solution uses machine learning and automation for managing roles, role reconciliation, certification campaigns and error rate management.

Netwrix Usercube supports a wide range of authenticators including passwordless authentication for user self-service and admin access. Usercube is an OpenID client and will trust the enterprise IDP for authentication. Netwrix Usercube role engine computes who is entitled to which access and automatically grants entitlements. The solution also has a flexible multidimensional policy model that leverages role parameters, as well as the real time simulation mechanism.

Netwrix Usercube's customer base is primarily mid-market to enterprise organizations. Their current customer base is centered in the EMEA region with majority of the clients from France. Their planned updates include launching an application owner dashboard, profile delegation, entitlement centered delegation, certification campaigns based on outliers, risks and remediations. Overall Netwrix Usercube is emerging as a strong alternative due to its well-balanced set of IGA capabilities, as well as making good use of identity and access intelligence.

Security	Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Strong Positive

netwrix

Table 17: Netwrix Usercube's Rating

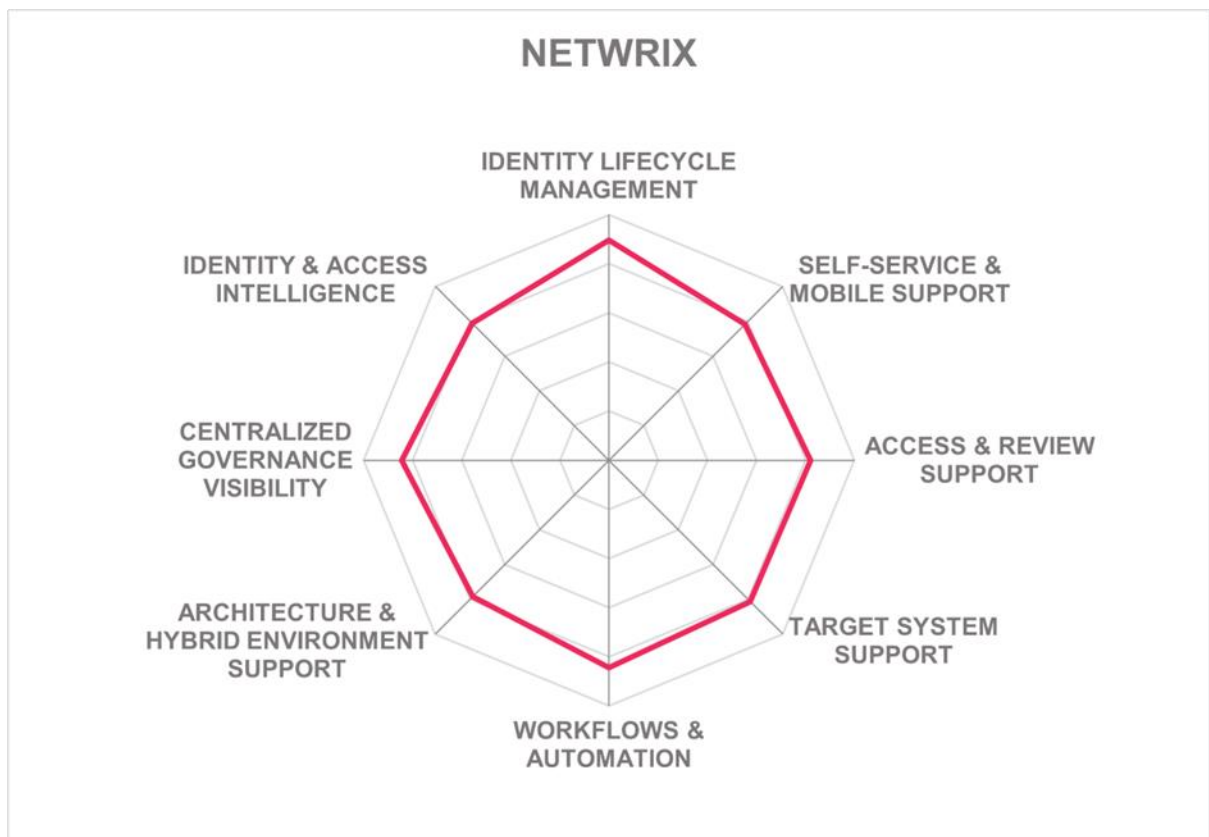
Strengths

- Microservices-based architecture also supports multi-instance deployment
- Wide range of out-of-the-box provisioning connectors supported for on-premises and SaaS systems
- Identity lifecycle management and the data model is flexible and allows wide options for customizations based on the lifecycle's needs
- Flexible multidimensional policy model allowing real time simulation mechanism
- Supports wide range of out-of-the-box workflow templates
- Simulation engine enables to see the impact of a role model change
- Machine learning is leveraged for updating role catalogs
- Partner ecosystem is very strong across the globe

Challenges

- Does not provide out-of-the-box reports for major compliance frameworks
- Presence is limited to EMEA region
- Quick approval processes are missing





Nexis – NEXIS 4

Based in Regensburg, Germany, Nexis first solution was NEXIS Controle. First released in 2014, the solution builds upon a plug-and-play approach to access governance and role lifecycle management as its core focus. Since then, Nexis has made some significant improvements to the core products, now called NEXIS 4. The NEXIS 4 feature set includes access governance, analytics and modeling engine, a fully configurable UI, workflows, policy management, as well as other interesting integration options. NEXIS 4 is primarily an IAG solution for risk and entitlement analyses and remodeling.

NEXIS 4 is a comprehensive solution for access privilege scans, risk analysis, visual remodeling of entitlement structures, and access governance processes. The technical architecture of the solution consists of three layers and a typical web-based client/server architecture. The data storage layer is comprised of a PostgreSQL database cluster with one database for administrative tasks and separate databases for each project that handle the connection to various source systems. On top of that, a web-based application is running in any java-based application server, with Tomcat being the recommended ecosystem.

NEXIS 4 supports all major deployment models with its focus mainly shifting towards cloud. It can be delivered as SaaS (e.g., on Azure, AWS), hardware or appliance, managed service or container based (e.g., Docker, Kubernetes). The solution supports partial multi-tenancy where the analytical interface for working with data is multitenant whereas the logging, reporting and configuration in the admin interface is single tenant. The solution supports exposure of sixty-five percent of its functionalities via SOAP, REST, SCIM, OAuth and SAML APIs. A Java API and a JavaScript API is also supported. Their SDK support is available for sixty five percent of the capabilities via Java. A developer portal is a new addition to help with development, integration, configuration, and deployment.

NEXIS 4 supports a modest number of out-of-the-box connectors to on-premises systems and SaaS systems. Being an IAG solution for risk and entitlement analyses and remodeling, they do not provide target system provisioning capabilities on purpose. For smaller customers, NEXIS 4 on demand can provision directly to the target systems, but only on an individual basis. The solution can support custom connectors using plugins that are based on a comprehensive API and are written in Java. Integrations with third-party ITSM tools such as Remedy, Cherwell, BMC Helix, Atlassian Jira ServiceDesk and ServiceNow is supported by the solution. These ITSM tools can either be connected via an email interface or through generic REST API connector.

NEXIS 4 supports SoD checks, risk intelligence and simulating models for anomaly of entitlement structures, role outlier detection and role optimization simulations as well as real time SoD violation checks. An additional dedicated SoD check for handling SAP Auth Profiles or Auth objects is also available. NEXIS 4 has an automated risk classification of entities and assignments. These automated analyses can be turned on or off and configured according to best practices for each analysis project, depending on the customer's needs.

NEXIS 4 provides a user-friendly and fully configurable interface design that supports 150+ corporate identity settings and a WYSIWYG UI component editor. The role mining and data modelling matrix of NEXIS 4 is advanced and mature. The matrix also works as the main source for developing and approaching the role mining generation. Rule based roles can also be easily generated through correlating with attribute values of relevant users. The workflow editor of NEXIS 4 uses a no code graphical approach which can be easily

configured. The dashboards are customizable and fully compatible with existing IAM solutions.

NEXIS has a limited global presence with its focus mainly in the EMEA region with a relatively limited partner ecosystem. Their customers are mainly in the finance, insurance, and manufacturing verticals. Their roadmap includes deploying assistive AI for recertification, and role management. Further planned updates include improved visualization, context-based workflows, visualization of pre-defined and custom KPIs, reconciliation engine, among others.

Security	Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive



Table 18: NEXIS 4's Rating

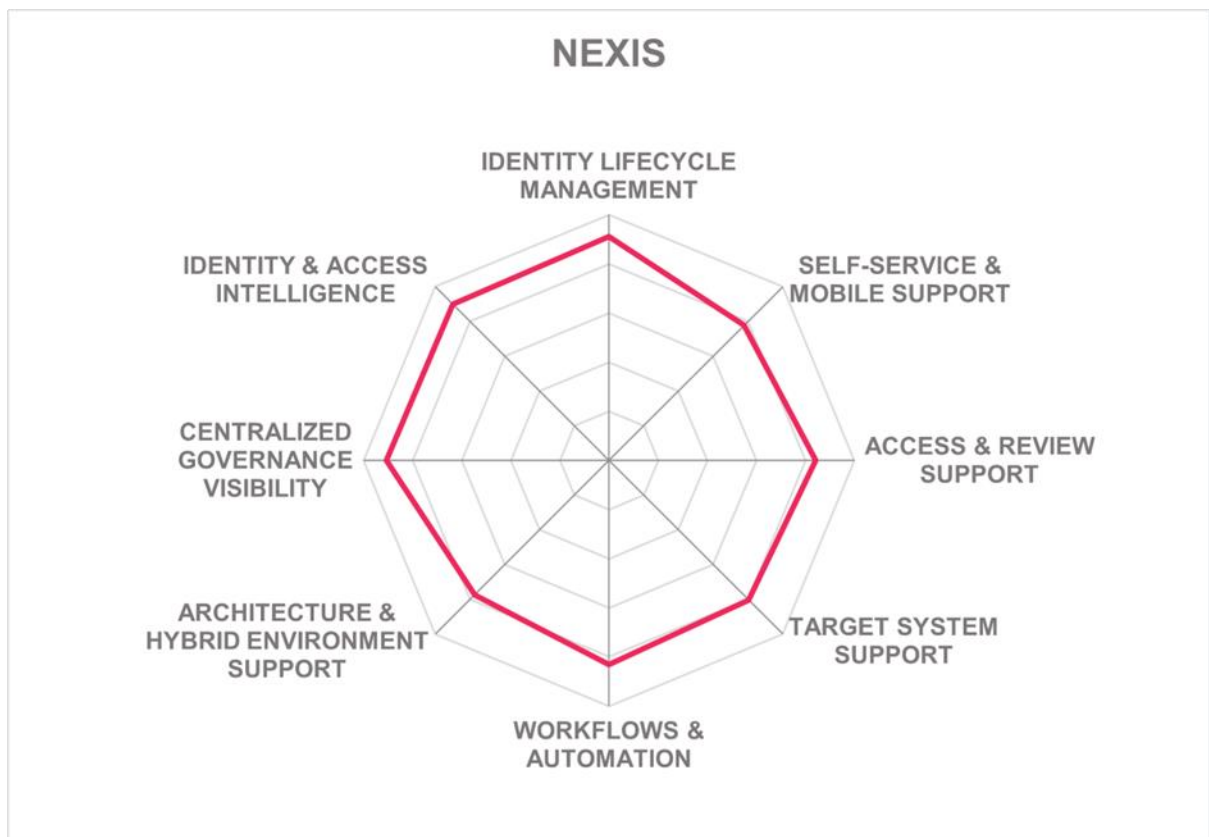
Strengths

- Role mining and data modelling matrix is very advanced and mature for SoD management
- Strong identity and access analytics and modeling capabilities
- Follows a zero-code approach throughout the solution
- Policies support all known access principles
- Supports all deployment and delivery models
- Solution offers more than 185 standard workflow templates
- Supports the majority of access governance use-cases

Challenges

- Presence outside EMEA is missing
- Partner ecosystem is moderate
- Does not support out-of-the-box reports for major compliance frameworks





Omada – Omada Identity Cloud, Omada Identity

Omada, headquartered in Denmark, counts among the established providers of solutions for IGA. Founded in 2000, Omada provides Omada Identity as an on-premises solution and Omada Identity Cloud for customers wanting a cloud-native SaaS solution. Both solutions deliver a full range of IGA functionalities with feature parity between the delivery models. The accelerator package allows customers to be operational within 12 weeks. Omada components include an enterprise server portal and services for provisioning, data warehouse, and role and policy engine.

Omada has released its next generation of Omada Identity Cloud service with a completely cloud-native platform. This platform is the basis for delivering all future features to Omada's customers. This update modernizes data ingestion with focus on real-time data processing and streaming data. The platform is multitenant compute and uses zero-trust architecture which is fully based on exposed APIs. The integration capabilities of this platform allow consumption of the data in both ways.

Omada Identity Cloud Platform supports a wide range of out-of-the-box and configurable connectors for SaaS systems but support for certain legacy on-premises systems is limited. Omada provides a connector community for peers to share, generate and install connectivity packages that are easy to deploy. Omada exposes capabilities via SOAP, REST, SQL, OData and GraphQL APIs. These APIs are used for integration with third-party tools, integration with data in the solution, and managing the cloud platform by itself.

Omada has a customer portal called the Omada Hub which provides documentation, tutorials, videos and a forum for questions and answers. Omada supports JavaScript and .NET programming languages directly and all other modern programming languages can easily be supported by this language support. SCIM is supported for identity provisioning including support for SCIM 2.0. Omada's Identity lifecycle management allows moving of identities as per context, association or roles including review of access right. The solution supports access review for all identities including external identities.

Omada has a GraphQL API for calling business logic which can be used for integration with third-party portals, example being ServiceNow store application provided by Omada for access requests. With the introduction of this GraphQL API, it is now possible to support chatbot interfaces. Customers can integrate with Omada to perform access requests via GraphQL APIs through third-party applications, such as chatbots. AI analysis of user access management data is supported by the solution. Omada's enhanced role mining uses machine learning to provide role suggestions. Omada has also introduced an AI assistant that will help users at decision points using natural language processing. This will include analysis of user access management data.

Omada's peer access analysis and peer recommendations provide rule-based automation to recommend access and highlight outliers. The role mining engine supports role analytics and role discovery. The solution uses advanced machine learning algorithms for role discovery. The current version of the solutions uses PowerBI as the client. Machine learning algorithms also allow the user to see how resources are related to roles and identify patterns.

Omada also provides bottom-up role discovery where if a user has all the characteristics of a role, then the role is implicitly assigned. The solution uses AI for recommending access requests based on peers via a thorough analysis. The solution supports continuous

validation of access policies, closed-loop reconciliation, automatic case management and context modeling.

Omada Identity's UI is modern and user-friendly with good features for user self-service, including the Omada Identity Cloud Management Portal. The portal enables SaaS customers to fully manage the back end of the solution including performing upgrades, creating, and editing environments, and more, without requiring assistance from Omada support. The solution supports a wide range of authenticators including passwordless authentication for users and admins. Omada offers good UI for self-service for access request, delegate access from tablets and mobile phones.

Omada is focused on enterprise-sector customers in North America and EMEA. Their 2024 roadmap includes a new reporting platform that provides Identity analytics that powers enhanced dashboards and role discovery, both delivered in regular update intervals in the cloud, a collaborative role discovery tool for managers and other leaders for creating roles for their populations is also planned in the roadmap.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive



Table 19: Omada's Rating

Strengths

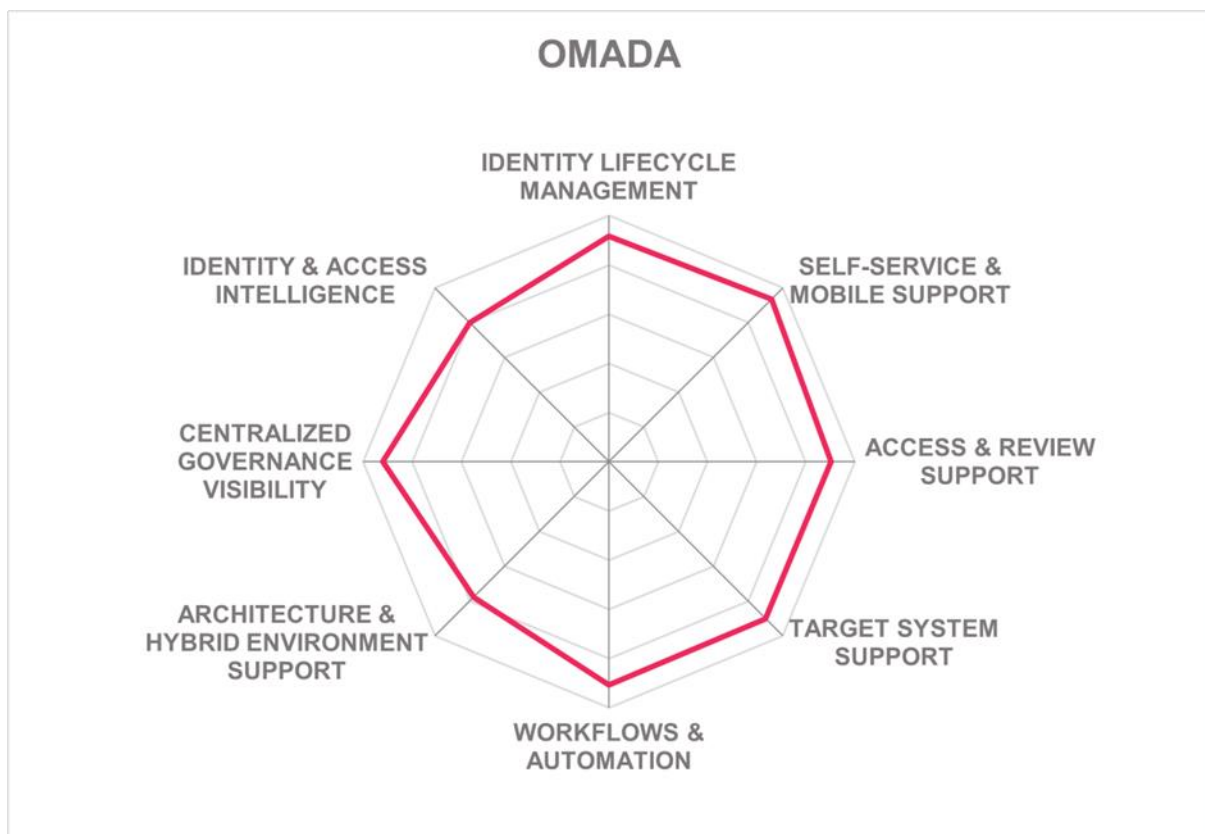
- New cloud native, multitenant and zero trust architecture-based horizons platform delivers all IGA related capabilities
- Unique configurable connector community
- Supports all capabilities related to identity lifecycle management including transfer of identity
- AI and machine learning implemented for various tasks such as role discovery, access recommendations, analysis of access management data
- Interactive AI assistant designed for product documentation, capable of responding with product details in the user's chosen language
- Omada compliance workbench provides unified view of compliance state of all access rights across all systems
- Reporting model uses advanced analytics
- Supports all deployment models

Challenges

- Limited presence outside EMEA and North American market
- Container based platform support is currently available for Docker only

- Out-of-the-box connectors for some legacy on-premises systems are missing, but overall good support for common on-premises systems

Leader in



One Identity – One Identity Manager and Identity Manager on Demand

Founded in 2016, One Identity operates as an independent entity of Quest Software. Based in California, One Identity provides an identity-centric security strategy with a broad and integrated portfolio of identity management solutions developed with a cloud-first strategy. One Identity's Identity Manager provides a single platform for governance and includes identity lifecycle, access request, access certification, auditing, privileged access governance, reporting, and data governance.

One Identity Manager's microservices-based architecture follows a three-tier approach where the database layer conducts main tasks around managing data and calculating inheritance along hierarchical structure such as departments, costs centers, location, or business roles. An object layer which forms the core of One Identity Manager enables oriented access to database layer and the presentation layer which comprises of front end that is used for input and output of data. The architecture model is flexible and supports cloud governance, data access governance, application governance, privileged governance and identities and entitlements.

One Identity Manager supports SCIM for identity provisioning and accelerating application onboarding. Configurable provisioning and deprovisioning workflows are provided which can be either event driven or schedule drive. The solution's support for out-of-the-box integration to ITSM tools is limited to ServiceNow. The connectors to ITSM can consume data and grab ServiceNow catalogue which is the product's unique capability. The integration to other ITSM tools is available based on customer requirements.

One Identity Manager supports a good variety of out-of-the-box provisioning connectors to on-premises systems. Configurable policies for governing automated provisioning are supported along with Just-In-Time provisioning. The solution uses a strong AI for risk score system, peer group analysis, entitlement right sizing and future capabilities will include AI support for recertification requests, access requests. The risk dashboard is interactive and can show role and entitlement sprawl.

One Identity Manager supports on-premises, public and private cloud, and hybrid deployment. License based and subscription-based deployment are also supported by the solution. The solution is delivered as a service, container (Docker), managed service or as software deployed to the server. It can be delivered in hardware or virtual appliance by using a partner from their ecosystem. The solution has all its functionalities exposed via REST, SCIM, .NET and Posh APIs. Their SDK support is limited to .NET and JavaScript programming languages. They have a developer portal for publishing samples and examples, with a repository on GitHub also available.

One Identity Manager's web portal has a modern user interface with a graphical representation of an identity and the associated roles, access, risks, and recommendations. Access control is driven via RBAC policies. Additionally, all access request management capabilities are available via mobile devices. The solution offers support for a good number of authenticators for user self-service and administration including passwordless authentication. One Identity Manager provides real time risk awareness to users when making access requests and approval.

One Identity Manager leverages AI and machine learning for informing governance policy decisions. The solution uses analytics, access frequency and user location to determine access rights and entitlements. AI and machine learning is also being used to recommend

removal of unused entitlements to reduce vulnerabilities. The solution also supports automated role discovery using machine learning.

One Identity is a privately held company with a large customer base predominantly in the EMEA region, followed by North America and expansion into the APAC and Latin America regions. It also maintains a good partner ecosystem proportionally in the same areas. Overall, One Identity continues to enhance the product's functional capabilities, establishing itself amongst the leaders in the market. One Identity remains a recommendation from us for evaluation in product selections.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive



Table 20: One Identity Manager's Rating

Strengths

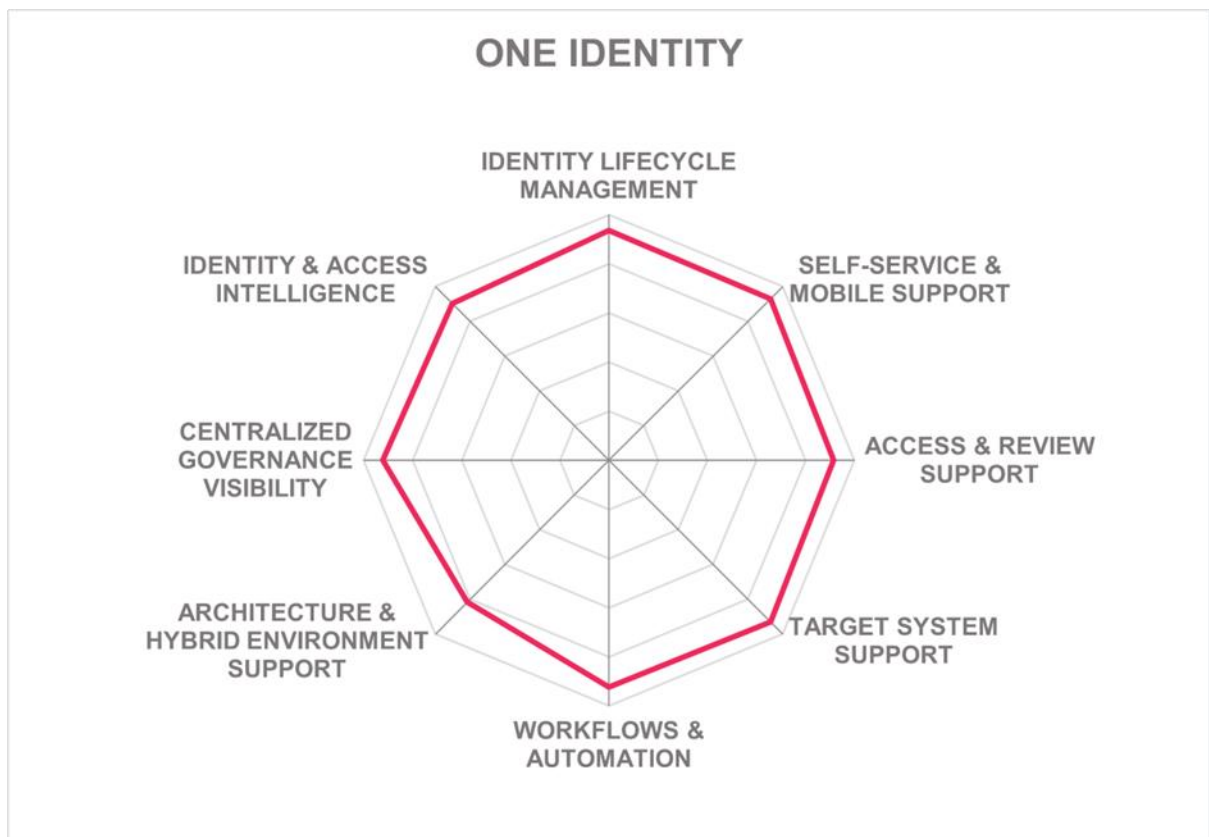
- Supports all major capabilities related to identity lifecycle management
- All major deployment models are supported
- Leverages AI and machine learning for role discovery, access recommendations
- Supports wide variety of out-of-the-box connectors for on-premises
- Strong support for analytics supported via machine learning
- Good features for workflow automations
- Access review and certifications features is well defined and incorporates risk scores
- All the functionalities of the solution are exposed via APIs
- Advanced access intelligence features

Challenges

- SDK support is limited to .NET and JavaScript
- Out-of-the-box integration to ITSM tools needs customizations
- Auditing reports are not categorized out-of-the-box into the specific major compliance framework categories

Leader in





OpenText – NetIQ IGA Suite

OpenText NetIQ IGA Suite previously known as Micro Focus offers an Identity and Access Management Platform as a set of solutions that includes Identity Governance and Administration, Access Management, Advanced Authentication, Data Security, Privileged Access Management and Security Information and Event Management. Founded in 1991 and headquartered in Ontario, Canada, OpenText acquired Microfocus in 2022. The NetIQ IGA Suite is aimed primarily at identity provisioning, lifecycle management, and identity governance for access governance, identity intelligence, and identity tracking to deliver a wide range of IGA capabilities.

The NetIQ IGA solution is a loosely coupled and integrated set of services and optional components that can be deployed both on-premises and as SaaS. NetIQ IGA is a combination of microservice and multiservice implementation, where individual products from identity, access and governance are combined into a platform.

The NetIQ solution supports an event-driven, bi-directional provisioning model which allows organizations to process identity lifecycle events as they happen. SCIM is supported for identity provisioning and deprovisioning. The solution's flexible approach for workflow and policy management, based on the designer tool, is still widely unmatched in the industry. It allows for efficient and easy management of complex environments. The solution supports continuous certification to assure continuous authorization.

NetIQ IGA can integrate via REST API or via email with Atlassian JIRA, TOPdesk, EasyVista, and Cherwell. Their support for other ITSM systems can be integrated via REST and SCIM. NetIQ IGA supports a wide variety of out-of-the-box provisioning connectors for on-premises and SaaS systems. NetIQ also delivers an out-of-the-box REST, SCIM and SOAP integration module that can provide an easy connection for any application without the need for specific coding.

Integrated role mining, adaptive access certification, and risk-based analytics are distinct and improved governance features of NetIQ IGA. Unsupervised machine learning is built-in and supports access management, risk and business roles and is provided through integration with the NetIQ Risk Service. Flexible configurations are provided for roles, groups, policies, access reviews, access requests and approvals. User activity monitoring is also supported by integrating access management data with SIEM information and this integration also works towards training unsupervised machine learning.

NetIQ IGA Suite has a user-friendly interface which uses analytics to compare identities when preparing roles. NetIQ also offers a wide range of IGA related reporting capabilities, including support for major compliance frameworks. The solution can leverage the advanced analytics capabilities provided by Vertica. Vertica is OpenText's unified analytics platform. Including Vertica in the solution allows NetIQ to bring advanced analytics, machine learning and AI to IGA without requiring a huge investment from customers. NetIQ also can combine identity, identity lifecycle, compliance, business context, security, and activity data from their IGA solution with data from other IAM and security products from their portfolio. The graphical representation of the reporting dashboard has been updated and now appears more modern compared to the previous version's outdated visuals.

OpenText supports on-premises, public or private cloud, and SaaS and Hybrid SaaS or Cloud deployment models. The solution can also be deployed to the server, container orchestration systems or container-based platforms (Docker, Red Hat, Rancher Labs,

Pivotal, Mesosphere, SUSE). They also support delivery as a managed service through their vast partner ecosystem. NetIQ IGA supports full multitenancy. All the functionalities of the solution are exposed via REST, SOAP, SCIM, OAuth, SAML, and LDAP APIs as well as managed using CLI. They offer SDKs for wide variety of programming languages including NetIQ Multi-Factor Authentication solution application, iOS, and Android. A developer documentation and samples are provided through a community portal.

OpenText is predominantly focused on mid- to enterprise-level organizations. NetIQ IGA continues to advance using AI and machine learning for autonomous governance and advanced analytics capabilities, policy management, automated access reviews, integration modules with SAP Hana and flexible audit and compliance dashboards. Overall, OpenText NetIQ IGA Suite provides a comprehensive IGA package in the IGA market space with its broad, mature, and evolving functionality with a good partner ecosystem on a global scale.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive



Table 21: NetIQ IGA Suite's Rating

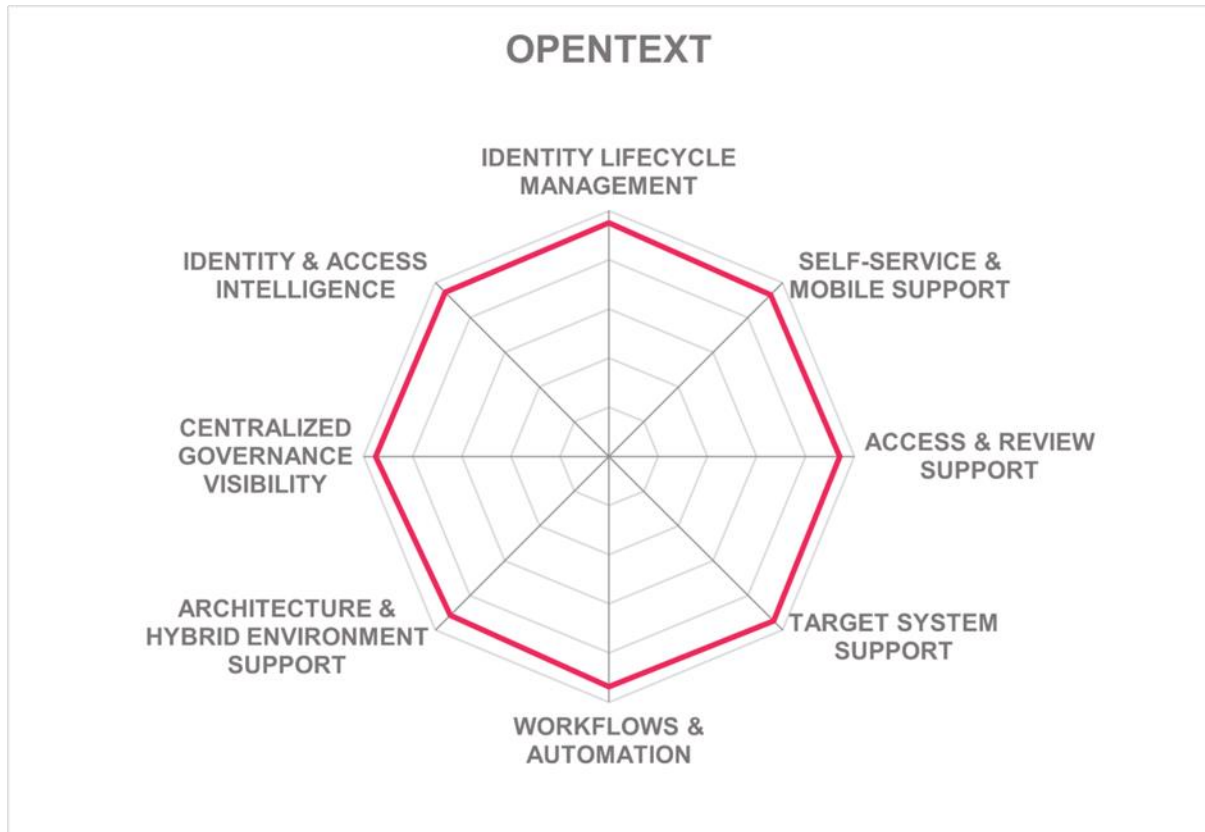
Strengths

- Combination of microservices and multiservice no-code/ low code architecture provides flexibility, scalability, and easy integration with existing services
- All the functionalities of the solution are exposed via APIs
- Machine learning based analytics support in highlighting baselines, anomalies, and risks
- Access governance supports real time decision making
- Supports all capabilities related to identity lifecycle management
- Connector network support for on-premises and SaaS systems is extensive
- Analytics model is advanced and supports out-of-the-box reports for all major compliance frameworks

Challenges

- Quick approval processes are missing
- UI is still lacking a more modern appearance

Leader in



Oracle – Oracle Identity Governance Suite and Access Governance

Oracle Identity Governance (OIG) Suite is the on-premises solution within Oracle's IAM portfolio. Oracle Identity Governance is Oracle's primary IGA solution that includes Oracle Identity Manager. Several IGA and, particularly, access governance capabilities have been significantly improved over the years, especially the integration of modules and the ease of its deployment. Oracle remains a preferred vendor for organizations with a substantial investment in Oracle Fusion Middleware and requires high flexibility for customizations to accommodate complex business processes.

Oracle Identity Governance is a J2EE application which provides identity administration, application management, identity certification and segregation of duties capabilities whereas Oracle Identity Governance has API/Services based architecture. The workflow components of OIG are managed by a separate service-oriented architecture while the core governance functionality is managed by the OIG service.

Oracle Identity Governance supports complete lifecycle management for all users including partners. When partners are expired, automatic access policies trigger to remove the partners access of data. OIG supports SCIM for identity provisioning and deprovisioning. Oracle supports an impressive list of out-of-the-box provisioning connectors for SaaS and on-premises systems. Oracle also supports developing custom connectors to integrate with non-standard/bespoke systems. The Oracle connector suite includes a flat file connector that can be leveraged for offline integration with non-standard systems. Oracle provides out-of-the-box ITSM integration for ServiceNow, Remedy, and BMC Helix ITSM. For Cherwell, Atlassian JIRA Service Desk, TOPdesk and EasyVista, out-of-the-box integrations is not given, however, customers/partners can extend the functionality and integrate these systems.

Oracle provides several deployment options on physical, virtual, private, or public clouds. This flexibility makes it easy for customers to have a scalable solution on heterogeneous clouds. They support delivery of on-premises deployments as a virtual appliance, container-based, software deployed to a server, as well as a managed service through Oracle advanced customer services and Oracle partners.

Oracle Access Governance is offered as a cloud-native service. However, microservices of Oracle Identity Governance Suite such as identity role intelligence and reporting can be rearranged or packed into containers by the customer. OIG's functionalities are fully available via APIs such as SOAP, SCIM, LDAP or REST. LDAP is supported with integration with LDAP directories through LDAP connectors. The solution supports SDKs for selected programming languages such as C/C++, .NET, Java, and JavaScript is given. Their support for Android, iOS, Python, Ruby, and Go can be provided by leveraging REST APIs.

Oracle Identity Governance offers certification for policies that enables business owners to right-size access privileges to enforce the principle of least privilege getting provided by the policies. Oracle Identity Governance Suite has enhanced and modern UI. Risk based access certification is supported by the solution. It supports a wide variety of authenticators for end users and administrator. All the self-service functionalities of OIG related to access request management are available on mobile devices. OIG supports REST APIs for self-service which can be integrated with chatbots and messaging platforms. The solution leverages AI and machine learning for providing recommendations for access reviews and approvals.

OIG offers good analytics for access review campaigns, which can be exported as CSV. It leverages Oracle Business Intelligence/Oracle Analytics Server/Oracle Integrations Cloud for reporting and Oracle Enterprise Manager/Oracle Management Cloud for monitoring and dashboarding. The analytics are AI and machine learning driven. Their user self-service support has a good interface with a customizable landing page. The solution uses a shopping cart paradigm and SoD violation checks are performed at the checkout page. Access request has recommendations feature which uses analytics to suggest access based on entitlement or attribute of the user.

Overall, Oracle Identity Governance Suite continues to innovate and introduce new features. It counts among the leading IGA products in the market. It provides a broad set of features focused on identity provisioning, access governance, and intelligence, as well as good support for enterprise-level architectures, including external workflow systems. They plan monthly release cycles to their Access Governance platform with the latest features. OIG makes an excellent choice for large IGA implementations requiring scalability and flexibility to support complex IAM scenarios.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive



Table 22: Oracle Identity Governance's Rating

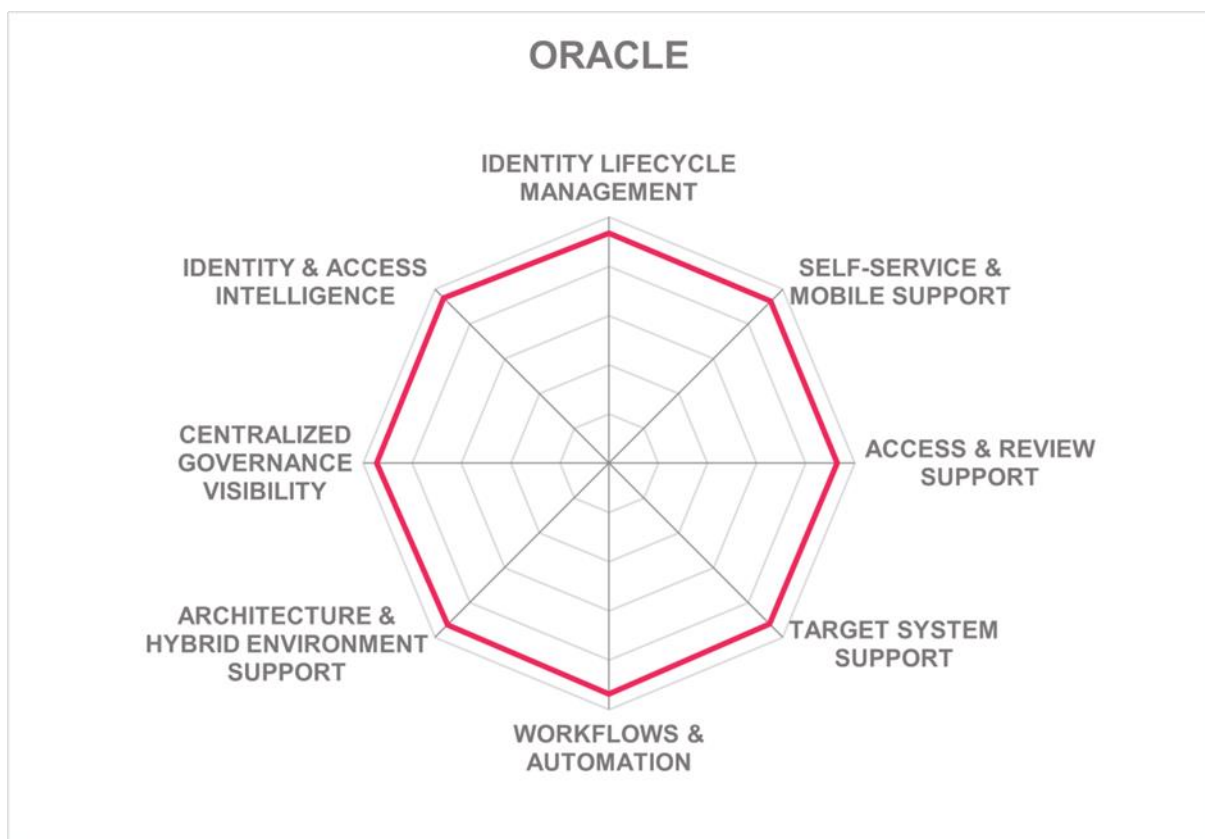
Strengths

- Supports all capabilities related identity and life cycle management of all types of identities
- Supports wide variety of authenticators for user and admin self-service
- Automated access reviews and granting of entitlements
- Reporting and dashboarding tool is mature, advanced and supports all types of out-of-the-box reports for all major compliance frameworks
- Supports all major out-of-the-box provisioning connectors for SaaS and on-premises systems
- Code less workflow engine is easy to use and supports multistage approval workflows
- Powerful access governance capabilities that go through various compliance workflows
- Modern and user-friendly user interface

Challenges

- Support for some major SDKs is missing but can be provided through leveraging their REST API
- Oracle database is required

- Lacks a go-to market approach for acquiring new customers and main customers are Oracle enterprise customers



Ping Identity – Ping Identity Governance

Founded in 2002, Ping Identity is a long-time supplier of authentication and identity and access management solutions. The company is headquartered in Denver, Colorado in the USA, and maintains a global presence through their partner network. Ping Identity Governance is a comprehensive end-to-end workforce identity platform that can address all types of identities, vertical with multitenant, dedicated tenant, or software options for SMB, enterprise, and large enterprise customers.

Ping Identity Governance is implemented as a multiservice architecture. It is delivered as a cloud service with tenant isolation and regional data sovereignty. It includes components like identity management, remote connector server, and reporting engine that can also be deployed on-premises for customers who want to leverage a hybrid architecture or keep some components of the service close to the applications and existing infrastructure.

Ping supports SCIM for identity provisioning along with automated and just in time provisioning. Its governance capabilities have purposefully been built as cloud native to match the increasing demand for governance of workforce related stakeholders. They also support entitlements natively within the platform for all known target systems without the need for any customization. Their solution also supports out-of-the-box integration to third party ITSM tools such as ServiceNow, Atlassian Jira ServiceDesk, and Remedy. The solution supports a no code approach and can also be connected to bespoke systems.

Ping offers both a SaaS service as well as software options for Identity Governance that can be combined to be delivered through managed services. It also supports other flexible deployments such as optional on-premises components for customers who want fine grained control on legacy applications that are still running in their own data centers and hybrid environments. The solution can also be deployed in any public or private cloud and is available as Docker images and Kubernetes orchestrations. All the functionalities of the solution are available via APIs such as SOAP, REST, SCIM, and OAuth. Ping Identity Governance provides REST APIs which can be invoked in a variety of languages SDKs including but not limited to Java, JavaScript, Python.

Ping Identity Governance has a modern user interface with comprehensive actions for admins and end users available in a dedicated portal for access requests and access reviews. The solution supports visualization of customizable end-to-end workflows of granting entitlements with mentioned risks at each level. These workflows can be integrated with the solution's AI and machine learning capabilities to bypass approvals based on the confidence scores generated.

The reporting dashboard provides a view of access at enterprise scale with detailed information. The reporting interface also allows drill down functionality to view access of each user and make decisions related to revoking access based on risk score. The analytics are all driven by AI and machine learning. Ping also has an orchestration engine that provides enhanced user experience based on roles and profiles.

With the acquisition of Ping Identity and ForgeRock by Thoma Bravo and the recent merger of the two companies, two strong, established vendors in the IAM field are joining forces. Ping is a strong candidate for enterprise level organizations. It has a global partner ecosystem and supports customers in North America, EMEA, APAC and a few customers from Latin America. Their roadmap for the next six months is focused on integrating Ping's on-premises and multitenant cloud software with Identity Governance. They also plan to

invest in AI and machine learning based certifications campaigns for regular access reviews, deeper integration with SAP GRC for SoD use cases, and deeper integration with ServiceNow.

Security	Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive

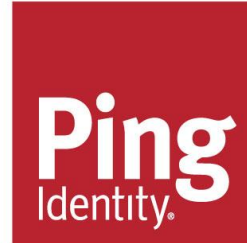


Table 23: Ping Identity Governance's Rating

Strengths

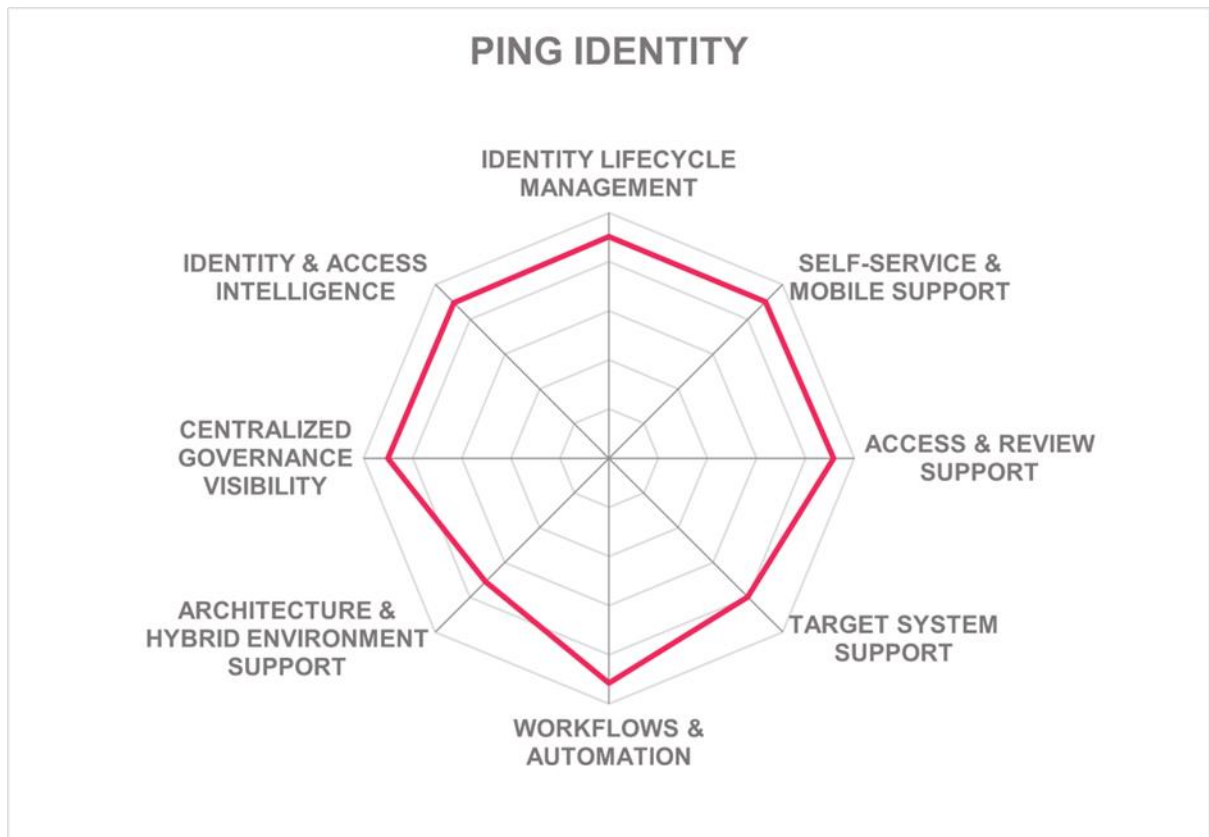
- Supports all capabilities related to access governance, identity lifecycle management, and access management
- Analytics are real time, driven by AI and machine learning
- Orchestration engine provides an enhanced user experience
- Dedicated user interface for policy manager allows creation, editing and management of policies
- Supports extensive list of authenticators for user and admin self-service
- Workflows allow bypass of approvals based on confidence scores generated via AI and machine learning
- Extensive list of out-of-the-box provisioning connectors for SaaS and on-premises systems
- Global presence with extensive partner ecosystem

Challenges

- Does not support out-of-the-box reports for major compliance frameworks
- Access request through chatbots is not available
- Support for integration to some ITSM tools is missing

Leader in





RSA – RSA Governance & Lifecycle, RSA Governance & Lifecycle Cloud

RSA Security, headquartered in Massachusetts, USA, offers a complete identity solution through the RSA Unified Identity Platform. This platform includes capabilities for Access, Authentication, SSO, Identity Governance, and Lifecycle Management. RSA Governance & Lifecycle is its IGA product, delivering both Identity Lifecycle Management and Access Governance capabilities.

The RSA Governance & Lifecycle solution operates with business logic running in an application server, with an Oracle database for data storage and processing. It gathers data through various collectors (using a variety of technologies) to compile identity, account, and entitlement information. Access changes are managed via Access Fulfilment Express (AFX), running on an Enterprise Service Bus (ESB). AFX executes changes in applications and external systems through a set of connectors.

The latest release of RSA Governance & Lifecycle introduces new advanced dashboards with 23 pre-configured dashboards templates that utilize data from a risk engine. The risk engine is configurable and provides risk insights for various identity related parameters. Additionally, the advanced dashboards incorporate an innovative way to include gamification as part of the access reviews.

RSA Governance & Lifecycle offers core IGA capabilities, including automated access certifications, compliance audit reporting and analytics, SoD policy enforcement, rules and policy management, role management and mining, and data access governance. The solution supports various identity and account types, advanced scripting capabilities, automated access discovery, automated provisioning of birth rights, and a continuous risk-based approach to access assurance, including governance for entire identity lifecycle management.

The solution supports SCIM 2.0 for identity provisioning and deprovisioning. Governance & Lifecycle has policies in place for bulk importing of identities and bulk approval or rejections based on SoD violations. The solution supports a set of web service APIs for out-of-the-box integration with multiple ITSM tools such as ServiceNow, Cherwell, BMC Helix ITSM, TOPdesk, and Jira. The solution also supports a wide range of out-of-the-box connectors to both on-premises systems along with an open web services connector framework to easily connect to other SaaS or web-based systems.

RSA Governance & Lifecycle has a modern and user-friendly interface with configurable dashboards providing a consistent experience for users, admins, and third-party identities. The UI adapts the functionalities based on the roles. The capabilities for both identity and access intelligence are visible through basic dashboard graphics and more extensive dashboards available on the RSA Community.

The solution supports a wide variety of authenticator options for self-service and administration access including passwordless authentication, Yubico FIDO tokens and Feitian FIDO security keys. RSA Governance & Lifecycle also includes out-of-the-box reports for major compliance frameworks such as GDPR, HIPAA, FERPA, among others. Access requests in the solution are reviewed using risk analytics. These access request are prioritized based on their urgency and importance. Additionally, the solution also provides dashboard for identifying orphan accounts and policies for alerting privileged access.

RSA Security maintains a substantial global customer base in mid- to enterprise-level organizations. RSA's dominance in the GRC and authentication markets has helped cross-selling and up-selling of RSA Governance & Lifecycle for IGA. Further, RSA Governance & Lifecycle adopts a risk-based approach to Access Governance making it a good choice for organizations with existing RSA deployments. The product meets primary IGA requirements for identity task automation, access governance, and identity & access intelligence while avoiding extensive customizations.

Security	Positive	
Functionality	Strong Positive	
Deployment	Strong Positive	
Interoperability	Strong Positive	
Usability	Strong Positive	

Table 24: RSA SecurID's Rating

Strengths

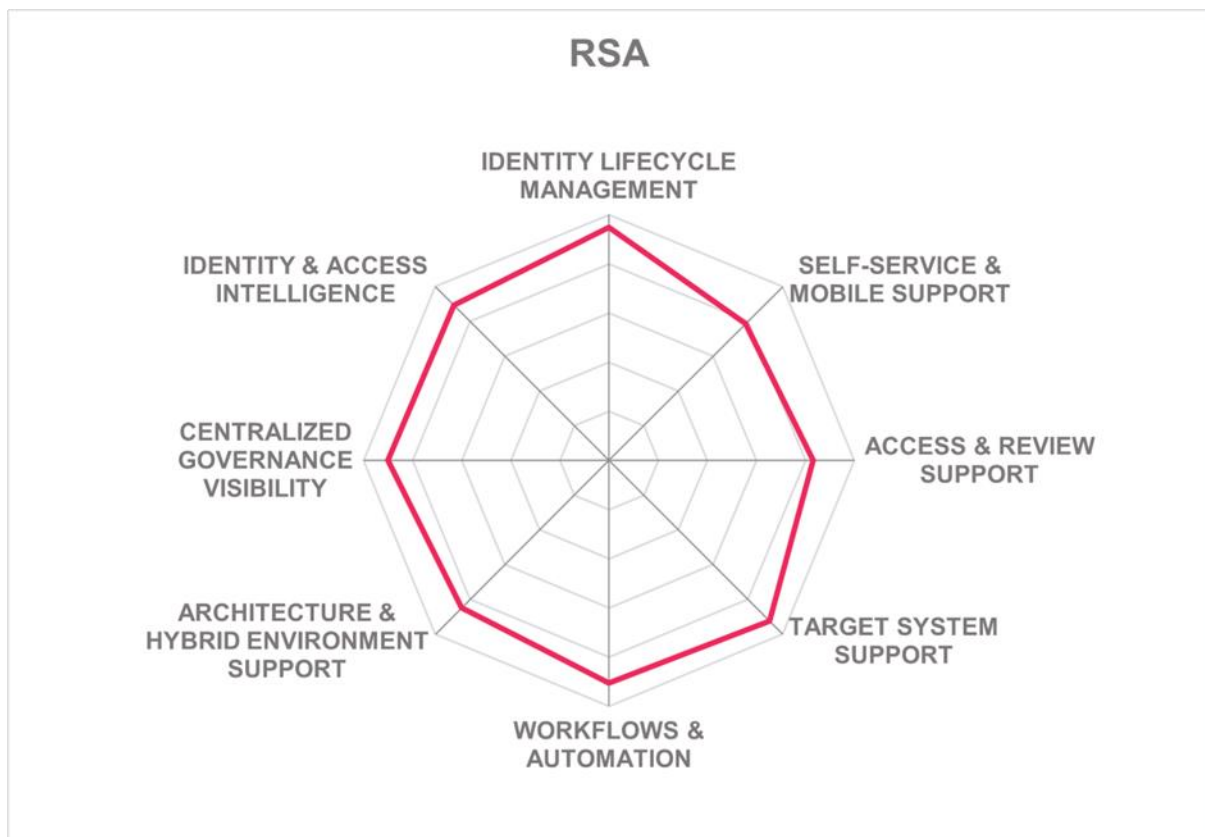
- Supports all capabilities related to identity lifecycle management
- New advanced dashboard is configurable and provides wide range of information for reporting
- Risk engine is analytics driven access for better insights into access governance
- Supports all known deployment models
- API support covers various protocols such as SOAP, REST, SCIM, LDAP and SQL
- RSA has a global partner ecosystem
- Advanced identity and access intelligence capabilities supported
- Supports wide variety of authenticators for user and admin self service

Challenges

- Multitenancy is not supported by the solution
- Support for SDKs is limited to Java and JavaScript programming languages
- Container based platform support is limited to Docker and Kubernetes

Leader in





SailPoint – SailPoint Identity Security Platform

Founded in 2005, SailPoint started as a vendor specialized in access governance and made heavy investments in identity provisioning capabilities over the years. Based in Austin, Texas, SailPoint offers two options to enterprises – a multi-tenant SaaS offering, SailPoint Identity Security Cloud and an on-premises offering, SailPoint IdentityIQ.

SailPoint Identity IQ is custom built to address requirements of enterprises wishing to maintain their identity program on-premises or in their own managed cloud environment. The platform has several modules such as Compliance Manager focused on policy adherence and review of access, Lifecycle Manager for provisioning and access requests, and File Access Manager, which is fine-grained governance over file storage platforms, amongst other capabilities depending on the customers' requirements.

SailPoint Identity Security Cloud is built on a multi-tenant cloud architecture where all components are deployed as microservices. Customers wanting to connect to on-premises systems can leverage their managed virtual appliance as a connection between SailPoint's SaaS product and the on-premises systems. SailPoint Identity Security Cloud is based on their Atlas platform. The platform provides unique insights driven by identity context, access activity intelligence, and embedded AI technology to run identity security programs at a global scale. From workflows for automation, policies for control, and a seamless connectivity fabric to consistent APIs and a comprehensive data layer, Atlas delivers a unified approach to manage and secure identities and data.

SailPoint's workflow engine is built on low-code/no-code principles. The builder allows for drag and drop capabilities to better visualize the data and logic flows. The workflow engine can consume any type of trigger, internal or external, to kick off a recertification. The solution supports mapping of SOD policies from SAP GRC to form a coherent SOD policy across the enterprise and has a dedicated mapping UI for attribute mapping.

The solution supports SCIM for identity provisioning and de-provisioning. SailPoint Identity Security Platform supports a wide variety of core governance capabilities such as access certification, SoD, access request, provisioning, and password management. The solution supports out-of-the-box integration with ITSM tools includes ServiceNow, BMC Helix ITSM, Cherwell, Zendesk, TOPdesk, Remedy, and Atlassian JIRA Service Desk. SailPoint supports wide range of out-of-the-box provisioning connectors for SaaS and on-premises systems.

SailPoint is leveraging AI and machine learning for accelerating onboarding of applications, access insights with Generative AI entitlement descriptions, access recommendations, and least-privilege based roles with role insights and discovery. Their AI driven access modelling capability surfaces recommended roles and allows users the ability to refine the role and scope prior to activating the role for use. SailPoint also offers AI-powered outlier detection and remediation. The solution will analyze activity and access data to monitor changes in the access model and flag any anomalous identities for recertification. SailPoint's event driven orchestration is built on low-code/ no-code principles. The builder allows for drag and drop capabilities to better visualize the data and logic flows. The workflow engine can consume any type of trigger, internal or external, to kick off a recertification. The solution supports mapping of SOD policies from SAP GRC to form a coherent SOD policy across the enterprise and has a dedicated mapping UI for attribute mapping.

SailPoint Identity Security Platform supports public and private cloud deployment. They also supports on-premises deployment of the solution. Along with SaaS, the solution can be delivered as a container (Docker, terraform), as a managed service or can be deployed as a software to the server. Managed Services deployment options are available from SailPoint Partners. All product functionality is exposed via SOAP, SCIM, SQL, OAuth, and REST APIs, as well as most of the functionality being accessible via CLI. They support SDKs for limited programming languages such as Java, Angular and jQuery with most of the functionalities of the solution supported.

SailPoint has a modern and user-friendly UI that supports access request tracking with grate details and a workflow configurator. The solution supports a wide variety of authenticator options for user self-service and admin access. The dashboard for access certification is configurable and there is a graphical UI for displaying user's current access to applications. Provisioning of access and pre-defining of entitlements is dynamically driven by birth rights, roles. Access review and certifications in the solution is AI and machine learning driven. SailPoint's Cloud Infrastructure Entitlement Management supports dynamic visibility while making access reviews of the user on given clouds. The reporting and auditing features of the solution are based on detailed timeline logs. There are event triggers in place to initiate workflow operations which are customizable and configurable.

SailPoint has been a leading vendor in the IGA market. SailPoint has built excellent support for identity and role lifecycle management as part of the IGA solution, with an increased focus on leveraging AI and machine learning. SailPoint's early recognition of Access Governance requirements in heavily regulated industries such as banking combined with strong marketing messaging and execution has led it to be one of the most evaluated IGA vendors for mid-market to enterprise sized organizations. Their roadmap includes various features around automation for application onboarding, generation of access policies, privileged process, and introduction of PAM.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive



Table 25: SailPoint Identity IQ's Rating

Strengths

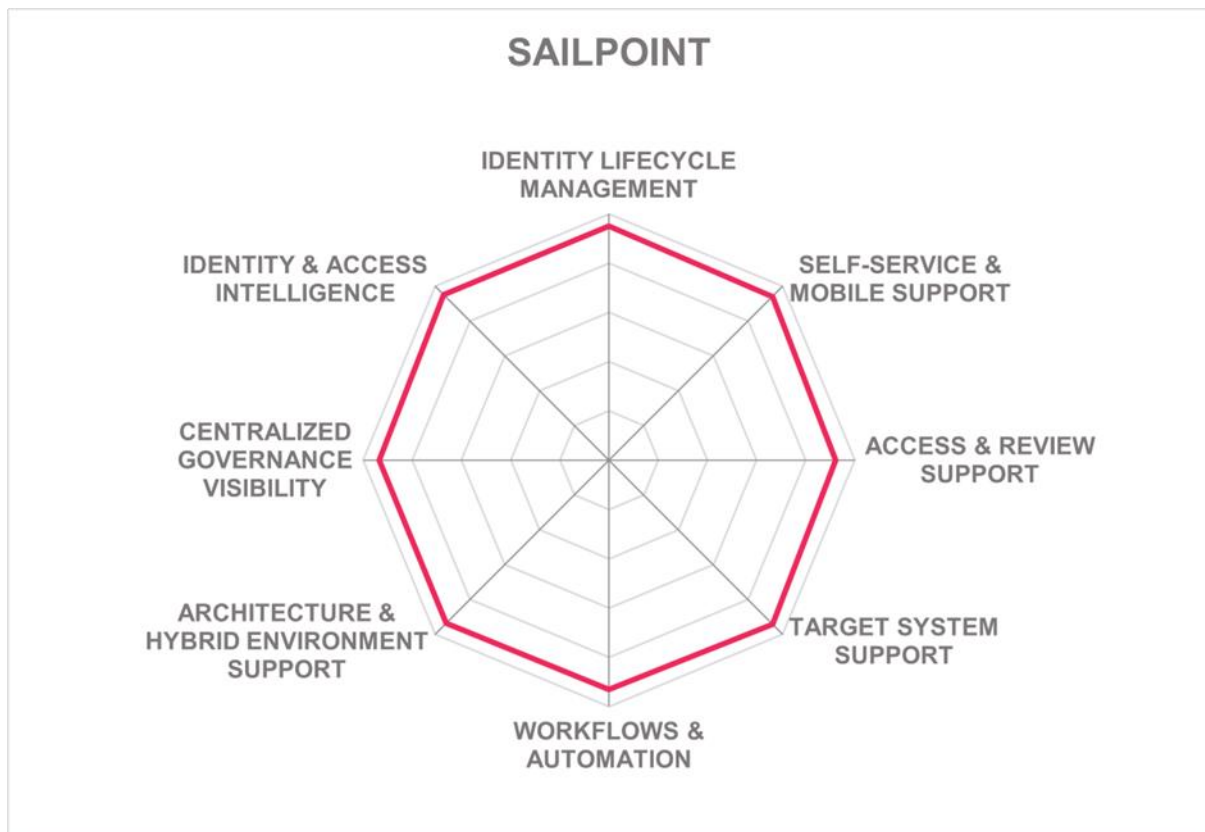
- Leverages AI and machine learning for various tasks such as automated application onboarding, access insights, access request recommendations, access reviews, certification recommendations, and access modelling
- SailPoint has an extensive global partner ecosystem for delivering the solution
- Covers all capabilities related to identity life cycle management
- Dynamic and fine-grained access controls for all enterprise identities
- Workflow engine is fully customizable and supports wide range of functions for identity life cycle management and access governance

- Supports wide variety of out-of-the-box provisioning connectors for both on-premises and SaaS systems
- Multi-tenant SaaS architecture supports automatic upgrades

Challenges

- SoD policy violation not available after addition of each item to shopping cart but is available for the final shopping cart
- Support for SDKs is limited to very few programming languages
- Solution does not support control of privilege elevation and session monitoring

Leader in



SAP – SAP Access Governance Solutions

SAP has an established IAM portfolio. Along with CIAM capabilities from the acquisition of Gigya a few years back, it shows their continued commitment to grow and compete in the mid to enterprise market. SAP offers SAP Access Control and SAP Identity Access Governance products as part of its IGA solution. Both of which are well-integrated with other SAP solutions such as SAP Business Suite to provide excellent Access Governance capabilities for SAP and a few other ERP applications.

SAP Identity Access Governance supports a good set of identity repositories including AD/Azure, LDAP, SAP HR, SAP IDM, SuccessFactors, as well as any SCIM supported repository natively with IGA solutions. SAP IDM is available for synchronization with any supported identity repositories. The solution supports all types of identities, however specific features are not implemented for certain identities. Bulk processing and provisioning of identities is also supported by the solution. SAP IDM and IAG support integrations across most SAP cloud and on-premises applications.

SAP does not support out-of-the-box integration to majority of the third-party ITSM tools, although a workflow interface is provided to extend capabilities. Additionally, Aquera enables integrated ITSM to Access Request in SAP Identity Access Governance. The solution supports most of the out-of-the-box provisioning connectors for SaaS systems, but noticeably there is less breadth of options for connecting to on-premises systems. The solution supports SCIM and SPML for target system connectivity.

Automated provisioning is supported by the solution and policy in place for RBAC when onboarding new users. The solution has Just-In-Time (JIT) provisioning in place with transaction definitions. Solution uses machine learning for flagging malicious transactions/anomalies and allows a user to review the actions. They provide user access monitoring, and the risk scoring is built in the solution for remediation and analysis. Policy testing is a roadmap feature. Other features supported by the solution are access certification, role affirmation combined with automated controls monitoring, UI masking and logging, and centralized authorization management for hybrid landscapes.

For SAP Identity Access Governance, the UI and dashboards are modern and customizable. The solution supports access-request and access review with a possibility of choosing between a one-step or two-step approval process. The solution offers SoD or assignment rules that are integrated with the workflow and can be used to customize the routing or approval process. Business role definitions are automated with a strong UI for role visualization. The solution supports limited authenticator options to both user and admin portals by SAP Cloud Identity authentication.

The solution uses SAP Business AI various intelligence features. It supports matching and learning capabilities connected to anomaly detection. AI is also leveraged for access governance, automated policy administration, mitigating controls management, checking SoD risk violations and for monitoring PAM sessions.

SAP Access Control is on-premises or in the cloud via Private Cloud Extended (PCE) option, with SAP Identity Access Governance as their fully multitenant cloud solution. SAP IAG is a multitenant SaaS solution whereas Access Control, IDM, Enterprise SSO are offered as private cloud editions and deployed like containerized solutions. Less than half of the product's functionality is exposed via REST, SOAP, SCIM, LDAP, SQL APIs. SAP does not provide support for SDKs however they have interfaces that can execute programmatic

functions via ABAP and MSMP exits. SAP Access Control is based on ABAP and is highly flexible and can be extensively customized.

SAP maintains a significant customer base in North America and the EMEA regions, with comparatively lesser presence in APAC and Latin America. SAP is equally focused on the mid-market and enterprise level organizations. Overall, SAP provides a well-rounded set of IGA features. SAP Identity Management remains a contender in the IGA market and a preferred vendor for organizations with significant investments in SAP software.

Security	Positive	
Functionality	Strong Positive	
Deployment	Positive	
Interoperability	Positive	
Usability	Strong Positive	

Table 26: SAP's Rating

Strengths

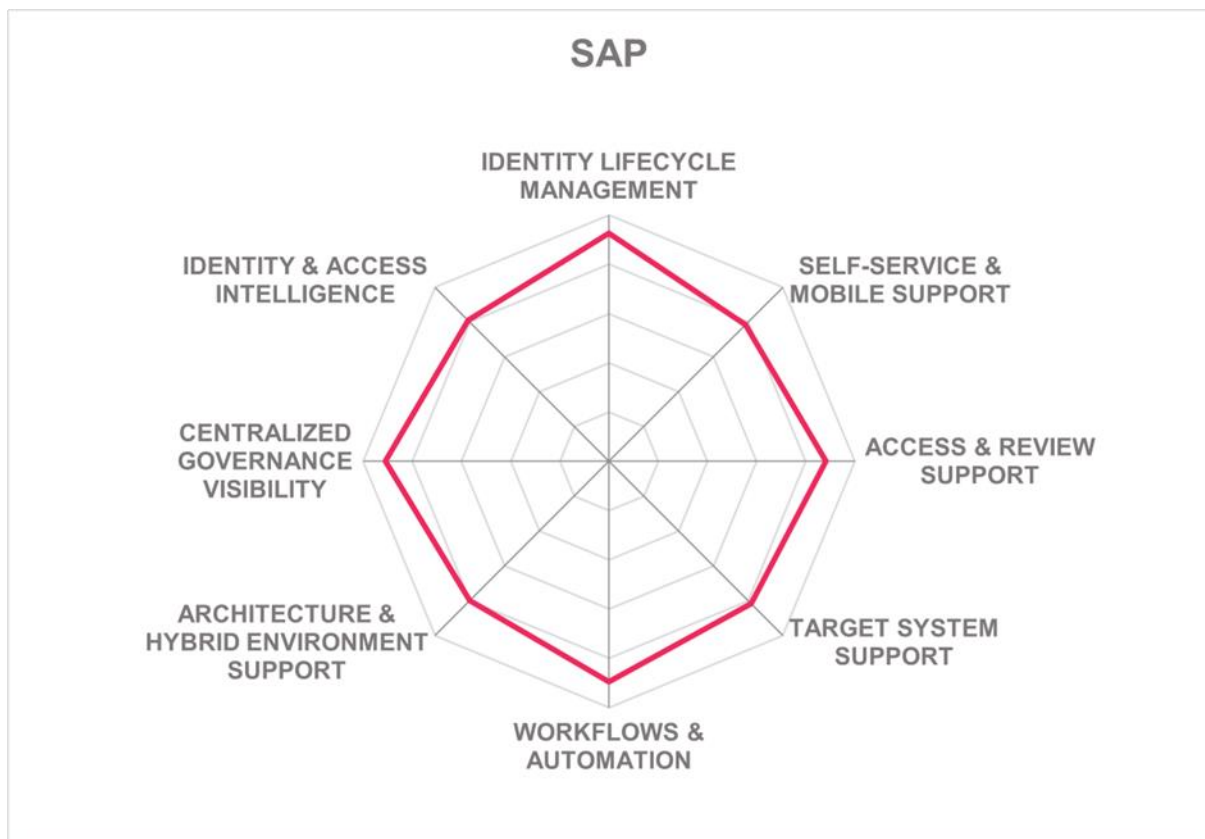
- Risk engine supports analysis and remediation
- Leverages AI and machine learning for access governance
- Policies support all known access principles
- Workflow capabilities are highly flexible and customizable that allow fine grained control
- Supports all capabilities for identity and lifecycle management
- Modern and user-friendly UI
- Integrated SoD analysis for provisioning, certification, and role management
- Strong global partner ecosystem

Challenges

- SDK support for major programming languages is missing
- Policy testing and simulation tool not available but planned in roadmap
- Quick approval processes are missing but planned in roadmap
- Delivery options are limited

Leader in





Saviynt – Saviynt Identity Cloud

Founded in 2010 and based in California (US), Saviynt offers a platform - Enterprise Identity Cloud (EIC), made of five different Identity Governance products. Its four core products are Identity and Administration (IGA), Privilege Access Management (PAM), Application Access Governance (AAG), and External Identity and Risk Management. The converged platform consists of a common admin console and data pane for identity governance, application GRC, and privileged access management capabilities underpinned by intelligence and risk exchange. Saviynt offers a strong lineup of IGA, including PAM, application access governance, External Identity & Risk Management, and data access governance through its Identity Cloud platform. Saviynt also offers ID Risk Exchange and the Saviynt Exchange products to their portfolio, a collaborative platform with their customers to exchange insights.

Saviynt Identity Cloud Platform is a cloud-based solution. Saviynt Identity Cloud's multitenant microservices architecture with shared control plane and isolated data planes provides scalability and at the same time offers the highest level of security. It is built on a containerized model to automatically scale up and down based on the usage of a microservice. Microservices are developed using Spring Boot, Node.js, and Grails to achieve better performance, scale, and agility.

Saviynt Identity Cloud supports SCIM for identity provisioning and deprovisioning. Saviynt integrates with ITSM tools such as ServiceNow, Remedy, Boomi, etc. for manual fulfilment of requests originated from Saviynt. Saviynt also provides extensibility using which any ITSM tool can be integrated through some customization via API. Saviynt Identity Cloud supports a very impressive list of out-of-the-box provisioning connectors for both on-premises and SaaS systems from its rich set of connector options such as prepackaged application connectors, generic connectors, RPA based connectors and connectors available through Saviynt community exchange portal.

Saviynt supports wide range of deployment models and can be delivered as-a-Service and in a container-based platform (Docker, Redhat, Unix/Linux, Windows systems). It can also be deployed as software to the server, as a managed service and virtual appliance. Saviynt has also added a built-in Identity RPA Bot that can deploy on-premises for a hybrid deployment. It can be used for rapid onboarding and convert disconnected applications to connected applications for automated reconciliation, provisioning, and account management. Most of the functionalities of the solution are exposed via SOAP, REST, SCIM, SQL, and LDAP APIs. Their SDK support is available only for Java and JavaScript however, REST based APIs can consume most of the programming languages.

Saviynt Identity Cloud has a web-based policy designer (no-code UI) lets you set and enforce policies for numerous scenarios with centralized management. AI and machine learning-based policy mining and out-of-the-box policy can support admins jumpstart policy set up process. The flexible policy and analytical control framework allow triggering of recertification for any kind of data and events. Saviynt Identity Cloud automatically identifies and creates AI and machine learning models rather than needing admins to configure/tune these models. Generative AI is being leveraged for converting text into SQL and a chatbot to help customers. The solution also supports duplicate identity management which is an automated process to compare and select attributes.

Saviynt Identity Cloud has a modern and user-friendly UI dashboard that can be customized from a simplified view for line managers to more detailed views for analysts and application

owners displaying different aspects of access, activity, and vulnerability risk. The role mining approach employs statistical algorithms to find the most optimal roles and recommends candidate roles. It also shows the applicable members and associated risk details. The solution has an inbuilt hybrid SoD analysis model for discovering entitlements and suggesting roles. The solution's access request/ approval capability is comprehensive with zero code approach for workflow configuration.

Saviynt is focused on enterprise and mid-market organizations primarily in North America with expansions into EMEA and APAC regions. Saviynt's roadmap features for the Identity Cloud includes next generation UI framework, AI capabilities, managing complex ecosystems and enhancing machine identity management. Saviynt is one of the leaders in this leadership compass for its mature and constantly innovating IGA solution.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive



Table 27: Saviynt EIC's Rating

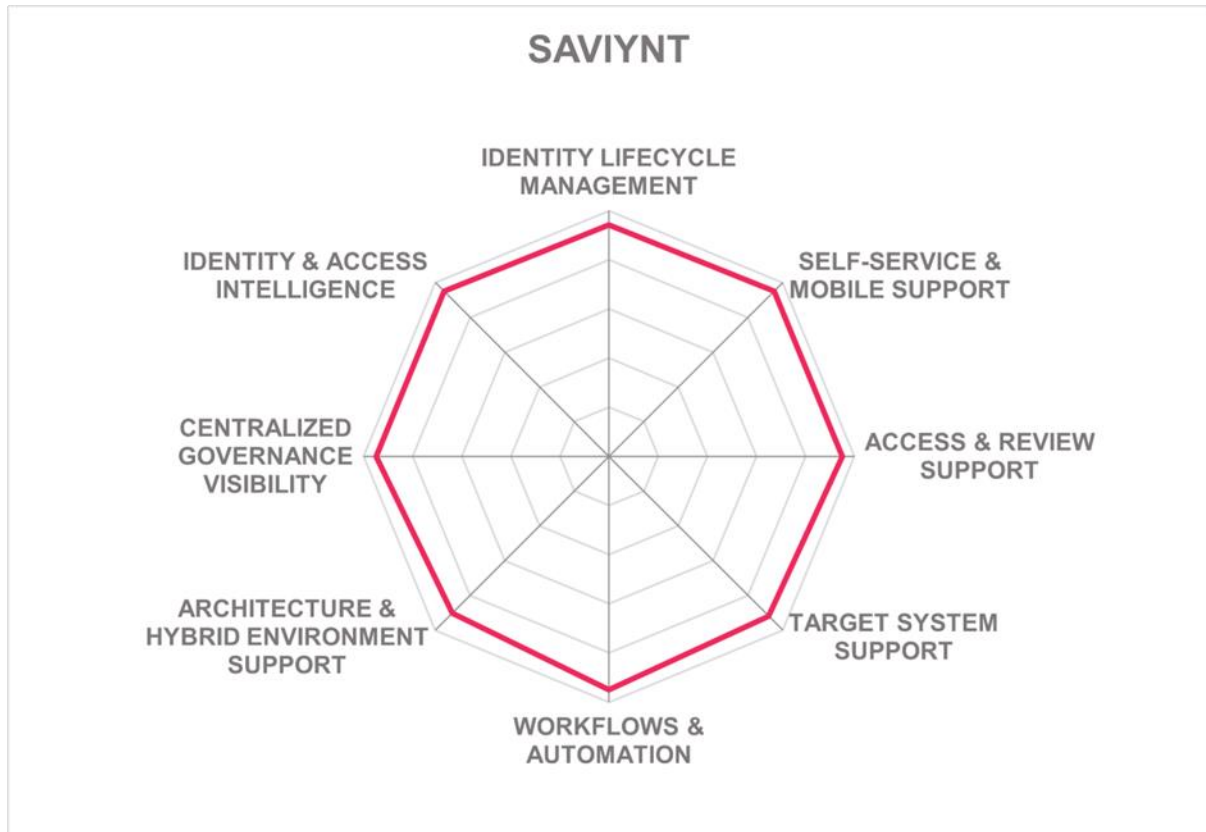
Strengths

- Automatically identifies and creates AI and machine learning models rather than needing admins to configure/tune these models
- Dedicated tool for persona-based activity monitoring
- Rich set of connectors provided through its establish options
- Supports out-of-the-box reports for all major compliance frameworks
- Extensive list of authenticators supported for admin and user self service
- Access certifications driven by AI and machine learning
- Supports out-of-the-box integrations to majority of the third-party tools
- Global partner ecosystem that allows it to support customers from all verticals

Challenges

- Breadth of container-based platforms supported is low
- Limited programming languages supported for SDKs but provides REST based APIs that can be consumed by any programming language
- Functionalities not exposed via CLIs
- Limited but growing presence outside North American market

Leader in



Soffid IAM – Soffid IAM

Based in Spain and established in 2013, Soffid IAM provides a converged IAM Platform that brings Access Management (AM), Single Sign-On (SSO), Identity Governance (IGA), Identity Risk & Compliance (IRC) and Privileged Account Management (PAM) in one comprehensive platform. Soffid offers a subscription service to an enterprise edition of the software product. Technical support service is provided by them only to the enterprise edition. Consulting and deployment services are also available through Soffid services. Soffid offers IGA related provisioning, access governance, and SSO capabilities of its Soffid IAM solution for this on-premises Leadership Compass report.

Soffid IAM has a microservices-based architecture that uses a secure jump server. This allows users to connect to any systems and recordings which are stored securely in the recording storage platform. The solution has a dedicated engine for all provisioning tasks. Enterprise SSO is also provided as a part of the legacy application connection.

Soffid IAM supports on-premises deployment and full multitenancy for private and public cloud deployments. Their other options for delivery include a- a-service, hardware appliance, server deployment, managed services, and container-based platforms (Docker, Rancher Labs, and Red Hat). Soffid releases regular patch updates which can be deployed automatically. Soffid states solution's complete functionalities are exposed via REST, SCIM, SQL, SAML, OAuth, and LDAP APIs. The API support is bidirectional that allows better communication and flexibility between Soffid and other systems. Their SDK support is limited to Java and JavaScript programming languages.

Soffid supports creation, configuration, and real time enforcement of policies. Automated compliance checks are also supported. The solution has a business process manager that supports out-of-the-box workflow templates. The workflow configurator has a drag and drop interface and supports full customization with end-to-end visibility. Access governance capabilities such as role management, SoD management, role mining access control policies are supported by the solution. Soffid uses automation for role mining by identifying profiles based on current roles. Soffid IAM has tools in place to automatically detect inactive accounts and clean up redundant roles.

Soffid IAM supports a wide range of out-of-the-box provisioning connectors for on-premises systems whereas SaaS systems have limited connectors. The solution uses a smart engine to fetch and post information from target systems. Soffid's connectors support two-way integration where any connector can act as an authoritative identity source. Some connectors can support real time updates for identity management. The solutions out-of-the-box integration support to ITSM includes ServiceNow, Cherwell, BMC Helix, TOPdesk, EasyVista, and Atlassian JIRA service desk.

Soffid IAM has an engaging web UI with a tile design dashboard that can be customized. The solution's admin console is web based and supports any web browser including mobile devices. It also supports legacy web applications. The solution supports easy attribute mapping but also supports an online editor for complex scripts. Soffid IAM has a useful dashboard which displays information such as status of requests, analytics, authentication, and risk analysis matrix to compare the risk level before providing access. The solution supports a wide range of authenticator options including approval or rejection of permissions via email or OTP for user and admin self-service. Soffid also has its own authentication application called Soffid Authenticator. They support passwordless authentication for mobile applications, smart card, FIDO token and a digital certificate.

Soffid IAM currently focuses on mid-market organizations but also serves enterprise organizations with customers primarily in Europe, North America, and Latin America. Soffid's partner ecosystem is growing and located in the customer's geographic locations. Soffid offers an alternative open-source solution to organizations with a reasonably well-balanced set of IAM and IGA capabilities.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive



Table 28: Soffid IAM's Rating

Strengths

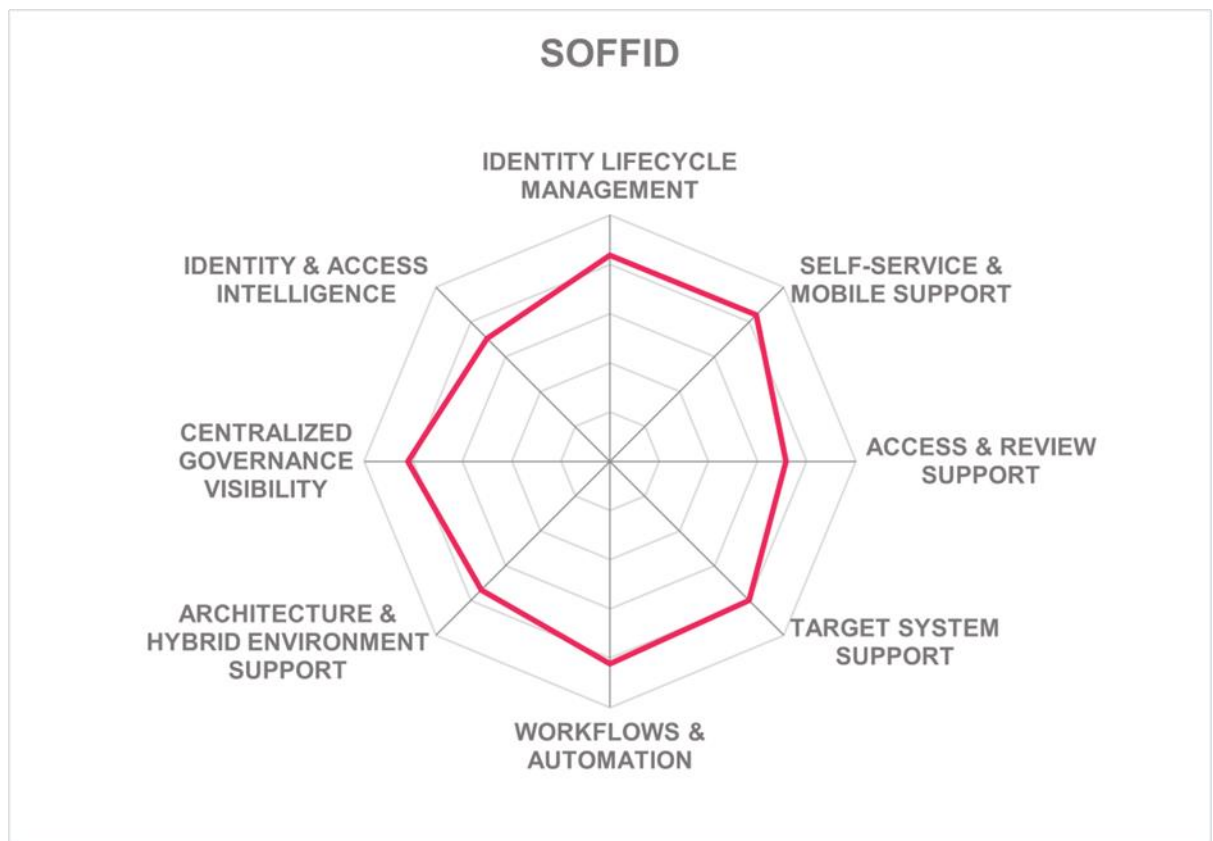
- Supports all major authenticators for user and admin self service
- Workflow engine uses a no code/ low code approach and provides customization through drag and drop interface
- API support includes all major protocols such as SCIM, LDAP, SQL, REST
- SoD and role management is compliant with ISO 27001
- Supports all policies related to identity life cycle management such as onboarding, provisioning, offboarding, change management and automated workflows
- Connector support includes extensive out-of-the-box provisioning connectors for on-premises systems
- Reporting dashboard provides real time insights

Challenges

- No support for out-of-the-box reports for major compliance frameworks
- Out-of-the-box provisioning connectors for SaaS systems lack breadth of options
- Market presence is currently focused on Europe but growing in Latin America, Africa, and Middle East

Leader in





Systancia – Systancia Identity and cyberelements.io

Based in France, Systancia offers an Access Management platform that includes multiple products within a suite to secure end user's digital workspace. Founded in 1998, Systancia's platform includes remote, privileged, virtual access, and IAM capabilities. Systancia Identity provides basic IGA capabilities, focusing on Identity Lifecycle Management, automated provisioning, user self-service, and workflows.

Systancia has a microservices based architecture that includes web applications for managing authentication, identity repository, database for all identity related information. A REST API is provided based on SCIM protocol to manage connectors execution and IGA capabilities. Systancia has an integration engine that communicates information upstream of repository into source application and downstream provisioning of various systems. The provisioning tool integrated into the solution allows the transcription of this data into the various application repositories that require it.

Systancia has centralized user lifecycle management for all types of identities. It also allows synchronization in multiple authoritative sources. The solution has a self-service portal that provides a view of access entitlements. Their SoD management is carried out through prioritization of access rights. Systancia uses SCIM for automated provisioning and deprovisioning of access. Systancia supports entitlements modeling that uses various access principles such as ABAC, RBAC and OrBAC. The UI for entitlement modeling is modern and user friendly.

Systancia supports a moderate number of out-of-the-box provisioning connectors to on-premises and SaaS systems but has a connector builder that can provide integration to any system. The configurable provisioning engine supports configuration of any connector if the target application supports SCIM or has Web APIs. The solution supports a limited number of programming languages for SDKs such as C/C++ and .NET. All the functionalities of the solution are available via APIs such as SOAP, REST, SCIM, SAML, OAuth, SQL, and LDAP.

Systancia Identity is the customer managed software product, sold as a license or as a subscription, including in a customer managed cloud infrastructure. It can be deployed as a SaaS solution within the Systancia SaaS Access Platform, or in a dedicated cloud instance. Systancia can also be delivered as virtual appliances, managed service or as a software deployed to server. The container enablement of the product is still missing but is currently on the roadmap. The product supports all major deployment models. When running the solution-as-a-service, both the Systancia Identity and Systancia Identity Provisioning servers must be installed on-premises. A hybrid cloud SaaS model only requires Systancia Identity Provisioning on-premise to connect to the cloud service.

Systancia has a new interface since 2024. The dashboard for access request and the overall self-service portal has been improved but still has scope for improvement. It has good user self-service and access request management features. The solution supports configuration of workflows to manage validation steps. Systancia Identity has limitations related to authentication methods supported for user and admin self-service. However it can support federated authentication via third party IDP supporting SAML or OIDC. Auditing and reporting can be generated using existing advanced features of Systancia Identity. Personalization of audits and reports is also provided by the solution.

Systancia has plans to converge all their cyber products including integrating IGA in their zero trust SaaS platform cyberelements.io from 2024. Cyberelements.io is Systancia's brand

for cyber solution. Systancia is focused on mid-market and medium level organizations. Their presence is currently limited to EMEA with growth taking place in APAC, North America, and Latin America. Their roadmap for 2024 includes improvement in the UI, extension of API, improvement of connector experience, and integration with cyberelements.io.

Security	Neutral
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive



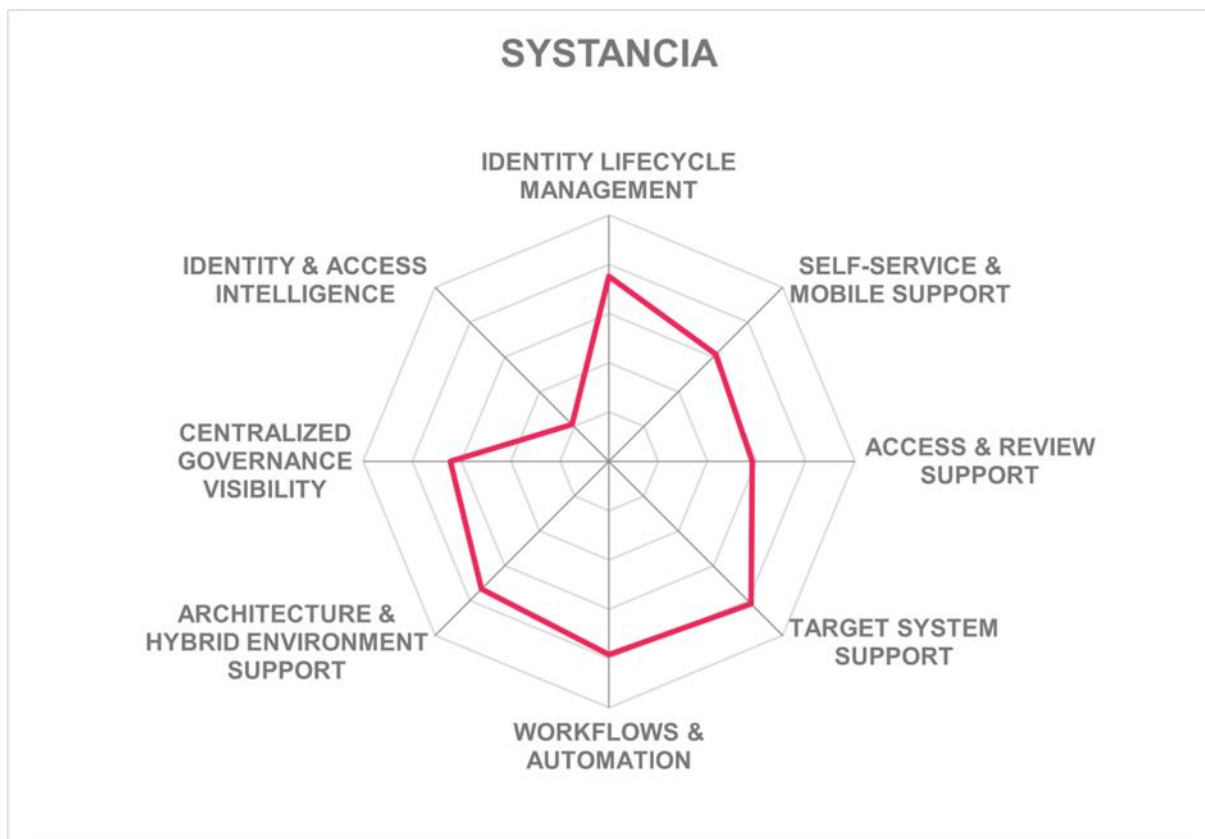
Table 29: Systancia Identity's Rating

Strengths

- Supports all known access principles
- Entitlement policy module has an impressive interface
- Reporting dashboard is customizable and can be adapted according to the authorization and profile of the connected user
- Delegation of rights can be done quickly through workflow or directly from user self-service portal
- All the functionalities of the solution are available via major APIs
- Supports flexible deployment models
- Provides a provisioning engine for building configuring connectors to connect to any system
- Workflow module is provided to configure workflow processes

Challenges

- Intelligence capabilities are limited
- Solution does not support container-based deployment
- Limited presence outside EMEA
- Does not support out-of-the-box reports for major compliance frameworks
- UI is still lacking polished appearance, but enhancements planned in 2024 roadmap



Tools4ever – HelloID

Tools4ever is a Dutch software company which began in the SMB market segment but has grown its portfolio to serve the IAM requirements of larger organizations. Founded in 1999, HelloID is a completely cloud-based with three integrated modules for provisioning, automation, and access management.

HelloID offers a scalable multitenant SaaS solution with segregated and encrypted databases. The user interface and APIs restrict access to only the data for which the customer portal is authorized. Its provisioning and governance modules are built as microservices while other modules such as identity provider, single sign on, access management are in the process of transitioning.

HelloID supports SCIM, REST, JSON, SOAP, XML, and others for identity provisioning and deprovisioning. The solution supports out-of-the-box integration to moderate number of ITSM tools such as ServiceNow, JIRA, TOPdesk, Ultimo, Fresh Service, and SolarWinds. It supports integration to these ITSM tickets via email or APIs. HelloID supports more than 180 out-of-the-box provisioning connectors for SaaS and on-premises however support for some major connectors is missing. Tools4ever can also build custom connectors based on requirements. Customers can also build custom connectors via PowerShell. Tools4ever provides free training and certification to customers for this task. Tools4ever focuses on supporting in creating these custom connectors without any additional cost which then benefits their whole HelloID community.

HelloID is offered as a SaaS only solution with deployment on MS Azure and Google cloud. It is a complete cloud-based platform with on-premises agent provided for management of on-premises accounts and for connections to local databases or filesystems if required. Most of the functionalities of the solution are exposed via REST, OAuth, SAML, OIDC, and SCIM APIs. HelloID has a portal for admins and developers for accessing documentation, tutorials, and examples to assist in integration, development, configuration, and deployments.

HelloID offers a wide variety of templates that can be easily configured and manage complex requests using a custom UI. The overall UI of HelloID is modern and has a configurable dashboard based on the RBAC/ ABAC model. HelloID leverages its partnership with the Elastic ELK Stack to enhance analytics and reporting functionalities. The user self-service access request is well defined and has a transparent workflow. HelloID supports a wide range of authenticator options for user self-service and admin access. The platform does not support passwordless authentication. However it can be engineered to integrate with third party passwordless authentication solutions.

Tools4ever is an established company with prominent presence in the North American and EMEA market. They are mainly focused on mid-market businesses, but they also support enterprise level customers. It is a dominant market leader in the Netherlands. Their roadmap includes adding features around role mining and enhancing SoD. Features around reconciliation and enhancing certification are currently under Beta testing and will be made available from the start of next year.

Security	Neutral
Functionality	Neutral
Deployment	Neutral
Interoperability	Neutral
Usability	Strong Positive



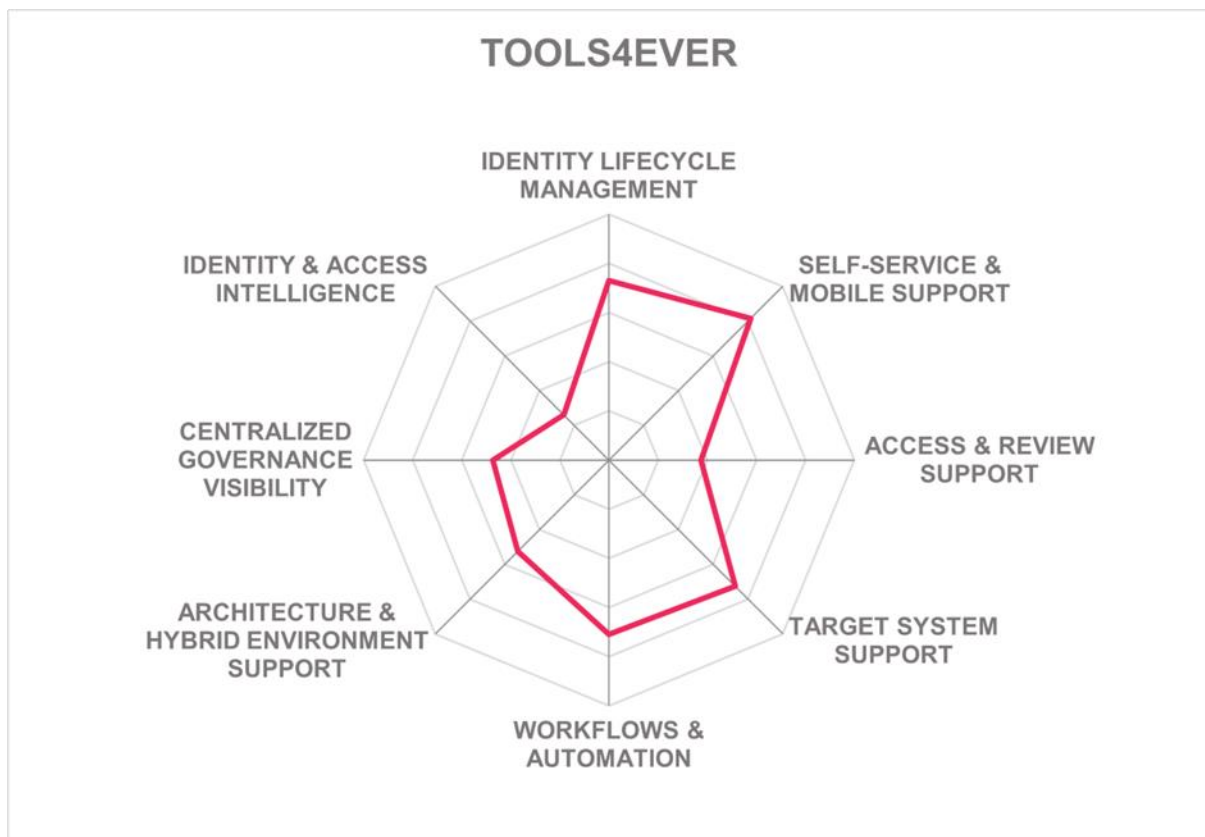
Table 40: Hello ID's Rating

Strengths

- Majority of the functionalities are available via APIs
- Developer portal is comprehensive
- Supports out-of-the-box reports for all major compliance frameworks
- Enhanced reporting capabilities due to its partnership with Elastic
- Policy management has a non-technical user interface and supports various access principles
- Workflows are flexible and configurable through the UI
- Policies support various access principles such as ABAC, RBAC, PBAC

Challenges

- Does not cover some of the access governance features such as SoD management but planned in roadmap
- Recertification campaigns supported only for optional entitlements but planned in 2024 to extend this to cover business rules
- Capabilities around access intelligence are missing
- Deployment options limited to SaaS solutions



Tuebora – Tuebora IAM Platform

Based in San Francisco, California, Tuebora provides a self-driven identity and access management platform. Founded in 2010, Tuebora's identity governance platform is self-driven and operates fully on-cloud. It relies on AI and machine learning for identity analytics and access governance. Tuebora's platform supports policy driven IGA and can be deployed rapidly.

Tuebora is a cloud native IGA solution and has a complete microservices based architecture. The product supports all major deployment models and can be delivered either as a SaaS or as a container based (Docker, EKS Kubernetes) platform. On-premise and private cloud deployment is supported via a virtual appliance while hybrid deployment requires SCIM gateway component on-premise for connectivity with on-premises IT systems to support provisioning and collection. Tuebora uses AWS for cloud hosting and can support individual deployment of identity lifecycle management components without the need for investing in the whole platform.

Tuebora supports an extensive list of out-of-the-box connectors for SaaS systems but does not support a wide variety of connectors for on-premises systems. They have a SCIM designer tool which can be used to develop custom connectors. Almost every capability of the solution is available via REST and SCIM APIs. Tuebora does not provide support for SDKs as it relies on REST APIs for exposing any functionality. A dedicated developer portal hosted on Zendesk is available for customers to access documentation, configuration articles and videos.

Tuebora has worked extensively in creating a policy driven platform. The policy mining dashboard is informative and provides data analytics, reporting dashboard and ability to create custom policies. Tuebora has also leveraged generative AI and natural language models for various use cases such as supporting administrators, application owners and end users for implementation of complex workflows, approve and reject access requests, monitoring of application usage, self service operations such as password reset and an assistant chatbot interface for answering queries. Additionally, the natural language user interaction model is also available for supporting access reviews, access requests and identity provisioning.

Tuebora has a decent and user-friendly UI with SCIM connectors for every application. The solutions supports limited authenticator for user and admin authentication. The reporting dashboard is graphical and supports out-of-the-box reports for some of the major compliance frameworks. A graphical workflow editor is currently not available but planned in roadmap.

Tuebora combines identity provisioning and access governance with its machine learning and identity analytics platform to detect access risks based on real-time tracking of provisioning and user access behavior. It further has its own extensions to address those gaps. Tuebora has further strong intelligence features such as the ability to create workflows using natural language. It supports sandbox-based onboarding of applications with data analysis, cleansing of data and review of configuration.

Tuebora is currently equally focused on mid-market to enterprise level organizations. Their customer base is primarily located in North America with growth expected in EMEA and APAC regions with customers. Their roadmap for the rest of 2024 includes enhancements to reporting services, supporting their SMB solution with more out-of-the-box capabilities and

integrations, improved entitlement modeling, and enhancing the assistant AI driven chatbot interface.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Tuebora

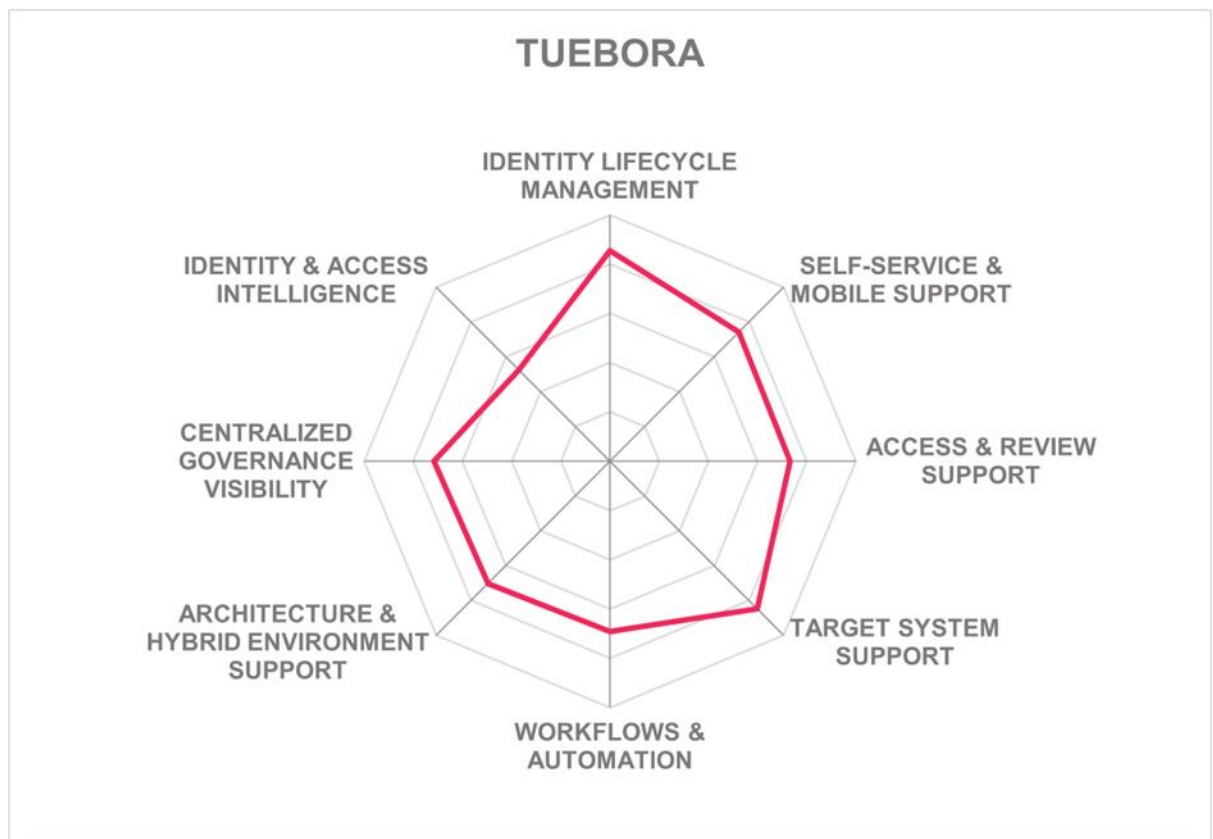
Table 51: Tuebora's Rating

Strengths

- Platform leverages intelligence capabilities for policy mining and configuration
- Ask Tuebora, its GenAI tool simplifies and automates various IAM tasks such as designing complex workflows, onboarding of applications, and managing access requests
- Access governance features cover majority of the use cases such as access reviews, tracking of unused accounts, behavior pattern monitoring, and overall visibility
- Supports all capabilities related to identity life cycle management
- Supports most of the access principles
- Reporting capabilities are extensive with support provided for most of the major compliance frameworks
- Almost all capabilities of the solution are available via APIs
- Supports wide variety of out-of-the-box provisioning connectors for SaaS systems
- Dedicated workspace model interface for development, testing and configuration of new capabilities

Challenges

- Workflow editor does not have a graphical interface but planned in roadmap
- Limited solution delivery options
- Support for out-of-the-box connectors for on-premises systems is limited



ZertID – ZertID

Founded in 2021 and a spin-off of Sysintegra, ZertID was available on the ServiceNow App Store from 2020. ZertID is an IGA solution that is built on top of the ServiceNow platform with rapid implementation ability. The ZertID solution is a combination of three modules for supporting identity life cycle management, IGA, and privileged access management. The product integrates neatly with ServiceNow features such as the CMDB and Security Incident handling.

ZertID has a multitenancy architecture which supports scalability. ZertID can rapidly integrate with any system that supports REST or SOAP API, ability to integrate via XML or CSV, OR supports connection via database. The solution supports real time role and attribute-based access controls. All areas of IGA, including provisioning of connectors to target systems, are supported with major capabilities in user lifecycle management, identity provisioning, and access governance. Its reconciliation engine autonomously identifies access deviations and initiates automatic tasks, such as executing a runbook by itself for resolving anomalies or prompting administrators to act.

SCIM is supported for identity provisioning and deprovisioning. Native integration with ServiceNow is standard, however connectors are available for out-of-the-box integration to other ITSM systems. The solution further inherits the pre-built target system connectors from the ServiceNow integration Hub. They provide support for rapid implementation of new connectors based on the requirements. The solution uses access intelligence for identification of orphaned accounts and then mitigating access related risks. Their access intelligence features also provide recommendations for access based on reference identity selected by the users.

ZertID has a flexible persona-based UI with adaptation to ServiceNow portal design. By utilizing capabilities such as the data management, workflows of ServiceNow, and with full user interface integration into the ServiceNow portal, it is a lean and efficient solution for IGA. ZertID can create custom UAR campaign types just using configuration. Their SoD policies and ABAC rules also do not require any coding. They can leverage the ServiceNow Standard Reporting and Performance Analytics tool for a powerful analytic engine. This capability provides a drag and drops reporting interface for most types of reports.

Cloud deployment of ZertID on ServiceNow is the preferred choice. The solution also supports on-premise deployment for the early few customers who started with on-premises ServiceNow infrastructure. This does not apply to the new customers and the vast majority who run ServiceNow from the cloud. The platform does not provide support for integrating with existing IGA solutions out-of-the-box. The solution can also be delivered as a managed service or deployed as software to the server. However, deployment to server depends on customers having on-premises ServiceNow agreement. The majority of the solution's functionality is available via SOAP, REST, SCIM and LDAP APIs.

ZertID primarily supports mid-market to enterprise level businesses focused on the APAC region with growth planned in North America and EMEA. Their roadmap includes enhancing the use of AI for risk and behavioral analytics and creating more prebuilt libraries for relevant use cases.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive



Table 62: ZertID's Rating

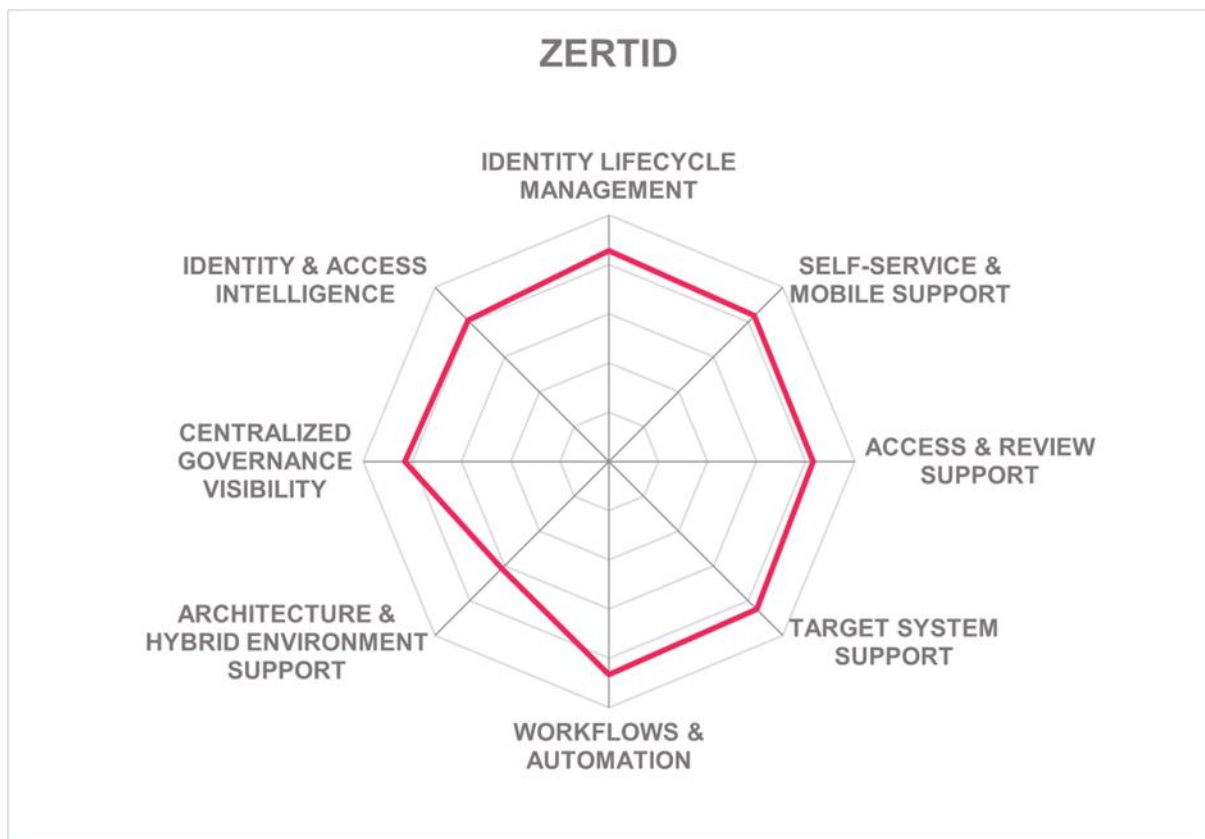
Strengths

- Persona based UI is adaptive and natively integrated into the ServiceNow portal
- Powerful GenAI capabilities that are natively integrated using Now Assist
- Reporting interface is low code/ no code
- Good set of connectors for common requirements of mid-market and medium-sized organizations
- Provides built in capability to simulate the SOD rules prior to saving to production
- Easy deployment on top of ServiceNow
- Majority of the functionality available via API

Challenges

- Limited global partner network
- Variety of connectors is limited due to relying on ServiceNow integration hub but can build custom connectors based on requirements in around 10 business days
- Dedicated ZertID developer portal is missing





Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other companies in the market that readers should be aware of. These vendors did not participate in the rating for various reasons, but nevertheless offer a significant contribution to the market space.

Avatier

Based in California (US), Avatier is one of the few IGA vendors that continues to exhibit innovative changes to adapt to evolving market demands in the recent past. From focusing primarily on providing intelligent user interfaces while lacking the underlying depth of capabilities, Avatier has evolved into a vendor offering comprehensive IGA capabilities with its Identity-as-a-Container platform creating unique market differentiation. Avatier's Identity Anywhere provides a fully containerized IGA platform primarily to solve deployment and scalability issues of traditional IGA.

Why worth watching: Organizations across the industry verticals seeking a solution to traditional IGA deployment challenges should consider Avatier's Identity Anywhere.

Fisher International

Fischer International is a US-based vendor that started early in delivering IDaaS solutions. Their products are also available on-premises and cover both Access Management and IGA. With their overall capabilities and experience in delivering IDaaS, they are specifically attractive to mid-market organizations in North America.

Why worth watching: Proven IDaaS solution covering Access Management and IGA.

Elimity

Founded in 2017, Elimity is a data analytics company headquartered in Mechelen, Belgium. Elimity Insights is their IGA solution. Their focus is on identity analytics and lightweight governance through those analytics. Elimity Insights focuses on fast visibility in the current users and permissions throughout an organization, with access reviews, monitoring, change requests and ITSM integration on top.

Why worth watching: Elimity has a specific and robust offering for those companies that have a strong need for governance but cannot or do not want to go for a full IGA deployment.

iC Consult/ Service Layers

German system integrator iC Consult with their Service Layers division is delivering an integrated solution for Access Management and IGA that builds on the products of Ping Identity, ForgeRock, and One Identity, and extends these towards an integrated solution with

consistent user experience and APIs. They have specific expertise in supporting manufacturing companies in global roll-out and operations.

Why worth watching: Delivery of an integrated solution that builds on mature products and adds a consistent API layer plus flexible, container-based deployment.

Identity Automation

Identity Automation is an US-based provider of an integrated IAM solution covering both Access Management and IGA requirements. Their focus is on higher education, but they also serve other market segments.

Why worth watching: Elim Provider of a solution for IAM that is well-suited for higher education and mid-market companies, following a platform approach.

Imprivata

Imprivata is a digital identity company focused on critical sector industries such as healthcare, and is headquartered in Massachusetts, USA. It was founded in 2002 with the mission to protect solutions that protect critical data and applications. Imprivata's IGA solution is a converged platform that supports various IGA related capabilities such as SSO, MFA, PAM, access reviews, role requests, identity life cycle management and access governance.

Why worth watching: Imprivata has a very dedicated solution for the healthcare sector.

Kapstone

Founded in 2013 with headquarters on the east coast in the northeastern US, Kapstone released its Access Review product with Day Zero Application Onboarding and Attestation in 2016 and introduced Kapstone's Provisioning Gateway and Intelligent Identity products the following year. More recently, Kapstone added both Autonomous IGA and Cloud Governance to its product portfolio. Today Kapstone's Autonomous IGA provides an innovative platform that focuses on three key capabilities - Automation, Intelligence, and Modularity.

Beyond core IGA capabilities, Kapstone Autonomous IGA gives some more advanced features that include service discovery, delegated administration, intelligent identity, application discovery and IGA application on-boarding, role discovery and automated access policies, IDaaS configuration management and analytics, as well as AWS, OCI governance. Kapstone also provides services to map IAM controls to such things as the NIST or HIPPA requirements as well as assessing an organization's security posture.

Why worth watching: Kapstone's autonomous, intelligent, and flexible modular product architecture are some of its key differentiators in the IGA market.

Memory

Memory is a spin-off from Accenture and delivers an integrated solution that supports most areas of IAM, specifically IGA and Access Management. Memory is based in France, as most of the current customers using Memory are. They have some very large installations of Memory deployed.

Why worth watching: Modern architecture, proven scalability and support for complex use cases including supporting machine identities in the IoT (Internet of Things) field.

Monokee

Founded in 2017 and based in Italy, Monokee has a platform that combines IAM capabilities with low code/ no code approach for identity orchestration. Their solution uses a graphical workflow editor and supports majority of the out-of-the-box workflow templates. Their access management platform supports real time monitoring of access requests, flexible authentication, and centralized management of access across multiple platforms through a unified interface.

Why worth watching: The visual identity orchestrator platform can be deployed rapidly and has a user-friendly interface.

Okta

Based in San Francisco, California (US), Okta's cloud identity platform is targeted at the workforce and customer identity management. Okta's acquisitions of Auth0 (CIAM, developers) and atSpoke (IGA) broadened Okta's portfolio in 2021. Okta has, over the past years, grown to one of the leading providers of IDaaS (Identity as a Service) solutions. The Okta Identity Cloud has emerged beyond a service for providing SSO (Single Sign-On) to SaaS services towards an increasingly comprehensive platform covering different types of identities such as workforce and customers and providing capabilities beyond the Access Management features.

Why worth watching: Strengths in various areas of IAM

Pathlock

Founded as Greenlight Technologies and providing the well-known Greenlight GRC connectors extending SAP Access Control, Pathlock has acquired Appspan, Security Weaver, CSI Tools, and SAST Solutions in 2022, delivering both a SaaS-based and an on-premises solutions for application GRC, supporting SAP and a wide range of other LoB solutions. The Pathlock platform is a comprehensive, powerful platform for managing access control and access risk in SAP and other LoB applications, provided as a SaaS service. Based on the integration of capabilities that Pathlock has acquired, it delivers an extensive set of features and market-leading breadth in platform support.

Why worth watching: Fine grained SoD controls and provisioning includes support for simulation of changes.

Pirean

Founded in 2002, Pirean is a medium-sized company with offices in London and Sydney. Their company provides a Consumer and Workforce IDaaS platform with a focus on simplifying how IAM capabilities are delivered for their customers enterprise web and mobile applications.

Beyond Pirean's access management and adaptive authentication, IGA capabilities are given to allow the management of application access entitlements with their lifecycle policies and rules, as well as access certification, SOX, and SoD compliance and innovative user request features.

Why worth watching: With Pirean's focus on high assurance use case and its expanding capabilities into the IGA space, Pirean will be an interesting vendor to watch in the IGA market.

Simeio

Founded in 2007 and based in Atlanta, Georgia (US), Simeio Solutions observed significant growth when shifting from its IAM system integration business into a full-fledged IDaaS service provider over the past few years. Simeio IGA managed services includes orchestration platforms. The platform provides a simple and efficient solution for application on boarding to various IAM technologies from IGA to Access Management and PAM from one Simeio IO Platform.

Why worth watching: Simeio offers good innovation capabilities in RPA and bots and good IGA capabilities as part of the Simeio IGA Managed Services solution which should be considered by organizations primarily in the North American and EMEA regions.

Tenfold

Tenfold, the solution provided by Tenfold Security, is an IGA solution targeted at the mid-market and medium-sized businesses. It delivers a comprehensive set of capabilities for managing user accounts and entitlements across target systems from a central platform, with a high degree of automation.

Why worth watching: Tenfold is a well thought out and feature-rich IGA solution for mid-market and medium-sized organizations.

TrustBuilder

TrustBuilder is a company that is headquartered in Belgium, with a large French subsidiary with offices in Italy, Spain, and the U.S. These are the result of the merger of TrustBuilder and French inWebo. The company focuses on delivering a strong solution for providing consumer and workforce access. The TrustBuilder.io. suite of products supports baseline lifecycle management, primarily targeted at customer and consumer use cases. It also supports policy-based authorization and API security use cases.

Why worth watching: Policy-based and contextual authorization of access

WALLIX

Having started as a PAM vendor, WALLIX has added Access Management and IGA capabilities through acquisitions. These have been integrated into the WALLIX One platform. With the growing and integrated portfolio, WALLIX is moving into the role of a provider of a wide set of essential capabilities for Identity Fabrics.

Why worth watching: Broadening portfolio of IAM capabilities with PAM features standing out.

Related Research

[Leadership Compass: Access Governance](#)
[Leadership Compass: Access Management](#)
[Leadership Compass: Access Controls tools for SAP Environments](#)
[Leadership Compass: Access Control Tools for Multi-vendor LoB Environments](#)
[Leadership Compass: API Security and Management](#)
[Leadership Compass: Customer Identity and Access Management \(CIAM\)](#)
[Leadership Compass: Data Governance](#)
[Leadership Compass: Passwordless Authentication](#)
[Leadership Compass: IDaaS Access Management](#)
[Leadership Compass: Identity Fabrics](#)
[Leadership Compass: Identity API Platforms](#)
[Leadership Compass: Policy Based Access Management](#)
[Executive View Hitachi ID Bravura Security Fabric](#)
[Executive View Hitachi ID Bravura Privilege](#)
[Executive View Cloudentity Authorization Control Plane](#)
[Executive View CyberArk Privilege Cloud](#)
[Executive View IBM Security Verify for CIAM](#)
[Executive View Microsoft Entra Permissions Management](#)
[Executive View One Identity Manager on Demand](#)
[Executive View PingOne Authorize](#)
[Executive View Simeio Identity Orchestrator](#)
[Executive View Atos DirX Access](#)
[Executive View Atos Evidian IDaaS](#)
[Executive View Eviden DirX Audit](#)
[Executive View Eviden DirX Directory](#)
[Executive View Eviden DirX Identity](#)
[Executive View Authlete API Authorization](#)
[Executive View PlainID Policy Manager](#)
[Executive View SailPoint Non-Employee Risk Management](#)
[Executive View SailPoint Identity Security Cloud](#)
[Executive View Saviynt Cloud PAM](#)
[Executive View Saviynt Enterprise Identity Cloud](#)
[Executive View Saviynt Application Access Governance](#)
[Executive View WALLIX Bastion](#)
[Executive View WSO2 Asgardeo](#)

Copyright

©2024 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing in-depth analysis, positions presented in this document will be subject to refinement or even major changes. KuppingerCole refuses all warranties as to the completeness, accuracy, and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole does not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators, and software manufacturers in meeting both tactical and strategic challenges and making better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.