KuppingerCole Analysts

IAM System Integrators - EU

Nitish Deshpande

December 14, 2023

LEADERSHIP COMPASS 2023

This Leadership Compass evaluates and provides insight into the capabilities of IAM system integrators serving customers in the European region. We examine market segments, provider service functionality, relative market share, and innovative approaches to providing IAM system integration services. The report provides valuable insights into the top solution providers as well as other vendors to watch in the IAM system integration space.

Contents

Figures

Introduction / Executive Summary

Identity and access management (IAM) is a core component of the enterprise IT infrastructure and central to protecting digital corporate assets. By enabling enterprises to manage and govern identities and the assets they are authorized to access, IAM can ensure that the right entities — including people, applications/workloads, and devices — can access the right resources at the right time, while preventing unauthorized access, a leading cause of data breaches.

Protecting digital assets, the systems, and applications in an IT environment of growing complexity and of a hybrid nature while facing ever-increasing attacks involve several actions organizations must take. Protecting against internal and external attackers requires a well-thought-out understanding of risks and countermeasures. Among the core elements of every infrastructure, we find IAM. IAM done right ensures that identities, their user accounts and passwords, and their access entitlements are well-managed. IAM thus reduces the attack surface by helping organizations moving towards the “least privilege” principle. IAM provides the tools to automate processes around managing users and access entitlements, but also for regularly reviewing these and identifying, e.g., excessive entitlements.

IAM system integrators specialize in providing identity and access management integration services to companies. System integrators play a key role in unifying various aspects of the IT infrastructure of an organization. Integrators provide a seamless framework for all IAM technologies to operate and fulfil organization’s demands. There are various operations which can be fulfilled by these integrators. Some of the typical functions are assessment, analysis, consultation, design, customization, implementation, training, regulatory and quality assurance, maintenance and support, scalability, and project management. Integrators will assess the existing infrastructure and identify the gaps, opportunities, and requirements before beginning IAM transformation journey.

Most of the integrators in the market have a reference architecture and maturity matrix to help clients determine the required modules of IAM technology. Integrators use this information from assessment for architecture design and review the integration plan by involving key stakeholders. Various factors such as change management are also taken into consideration. System integrators are equipped to tackle specific requirements from customers to customize the architecture design. Customizations could be related to accommodating regulatory requirements before migration for certain applications.

The next major step is to implement the design and provide integration services to customer solutions. System integrators can connect and deploy IAM systems across various databases, application platforms, and operating systems. Integration to third party ITSM solutions and SIEM integrations can also be provided based on requirements. Most of the integration projects involves a team consisting of client employees. Integrators train the client-side employees with necessary operational and maintenance knowledge. In most cases, a dedicated team of IAM professionals from integrators is involved from start to finish phase of the project. Integrators with large workforce deploy a flexible approach to completing projects. The IAM professionals are rotated based on different phases, however certain consultants and developers remain constant.

Another aspect of IAM projects is the maintenance and ongoing support. Certain integrators have a dedicated Managed Services Support team to help clients with new application onboarding, troubleshooting, and rolling out updates. Organizations are looking for system integrators which can support in scaling the operations in the future. Integrators in the market right now can meet this demand by designing scalable solutions.

Most organizations operate in a hybrid environment with a combination of legacy systems and apps that coexist with cloud services. Enabling easy, consistent access to applications is business-critical no matter where those applications are hosted. A unified IAM platform can make your workforce more efficient and productive, with single sign-on (SSO) and other tools that work across on-prem and multi-cloud environments. For your customers, it can create frictionless, targeted experiences that lead to greater satisfaction and loyalty. Integrators can meet this requirement by providing integrations to legacy and SaaS solutions.

Organizations are under intense pressure to differentiate themselves by delivering new digital initiatives and innovative services without disruption. At the same time, they must protect their digital assets, systems, and data, while maintaining regulatory compliance, all in an increasingly complex IT environment amid a sophisticated threat landscape. System Integrators can provide advanced services around authentication for providing additional security. Most of the system integrators in the market can provide support for all major authentication methods. Auditing and forensic capabilities are also being supported by system integrators to provide security incident analysis.

An integrated IAM platform can help organizations modernize IT and achieve their goals for workforce productivity, customer satisfaction, stronger security, greater agility, and faster innovation.

Highlights

- The IAM system integrator market is very mature and has capabilities in supporting all major IAM technologies
- System integrators can provide strong capabilities for meeting regulatory requirements
- Assessment matrices provided by system integrators for understanding customers' requirements are fine-grained
- Most of the vendors in this report have strong capabilities for advanced services such as updating authentication methods for passwordless and risk-based, and support for regulatory compliance., etc.
- Many vendors in this report have limited presence outside their founding country
- Innovation capabilities of vendors is limited due to the requirement of the maturity of services
- Most of the vendors have many professionals who are certified on vendor products

- Most vendors provide integration services for legacy on-premises as well as IDaaS and SaaS

Market Segment

IAM (Identity and Access Management) System Integrators are companies that provide support in consulting, implementing, and/or managing services or operations of IAM technologies for businesses. These services can range from planning and designing to implementing and operating various IAM technologies based on the customer's requirements. The IAM technologies include a range of solutions including full IAM suites, CIAM, identity lifecycle management, identity proofing integrations, Fraud Reduction Intelligence Platforms (FRIP), access management, access governance, privileged access management, authentication services, and data governance, among others. An IAM system integrator is also responsible for ensuring security and efficiency when providing solutions to manage the complex IAM landscape of an organization.

IAM solutions have reached maturity but are limited in evolution by existing technologies. Organizations are seeking these solutions for protection against cyber threats and compliance with constantly evolving regulatory requirements such as GDPR, CCPA, HIPAA, FISMA, etc. Furthermore, the experience and qualifications of the resources of an IAM system integrator are crucial for completing projects within the given time frame and budget.

In this Leadership Compass, the primary focus is on the vendors that specialize in providing system integration services for IAM technologies in Europe. Thus, this Leadership Compass analyzes the types of integration services offered by each participant, including, but not limited to:

- IAM technologies and products/services supported.
- Operating systems and cloud environments supported.
- Directory services supported.
- Types of integration provided.
- Types of customizations and development provided.
- Engagement methods
- Projects and contracts
- Auditing and reporting
- Resource management

Delivery Models

Delivery models should include the ability of vendors to provide options for types of engagement either purely for strategic consulting, professional services, implementation and integration or managed services support. Ultimately, selecting a suitable IAM system integrator delivery model will depend on the customer requirements and use cases.

Required Capabilities

This Leadership Compass analyses the IAM system integrator vendor's ability to provide:

- Breadth of IAM technologies supported
- Training and certification of their personnel on IAM vendor products and services
- Types, methods, and duration of engagements supported by vendors
- Ability of vendors to carry out end-to-end projects as well as take over existing projects
- API coding and integration to third party solutions
- Overall professional services support
- Auditing and reporting capabilities

Evaluation Criteria

Key Capabilities:

- IAM technologies covered
- Operating systems
- Directory services
- Integration and/or synchronization to directory services
- Solution customization, including custom development
- Application integration, including legacy apps and SaaS
- Auditing, reporting & dashboarding
- Support for inbound and outbound federation
- Areas of IAM served (e.g., IGA, Access Management, PAM, CIAM, etc.)
- Locations served: office locations and regions served
- Breakdown of engagements based on duration, region, industry specialties for customers, types of engagements
- Staffing capabilities
    - Number of certified professionals
    - Project and budget handling capabilities
- Roadmap
- Competitive positioning/Unique Selling Propositions

Additional innovative capabilities

- Standards support
- Policy authoring and management
- ITSM Integration (e.g., ServiceNow)
- Mobile support
- Authentication methods
- Developer support and training

Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help to 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.

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

- Service Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

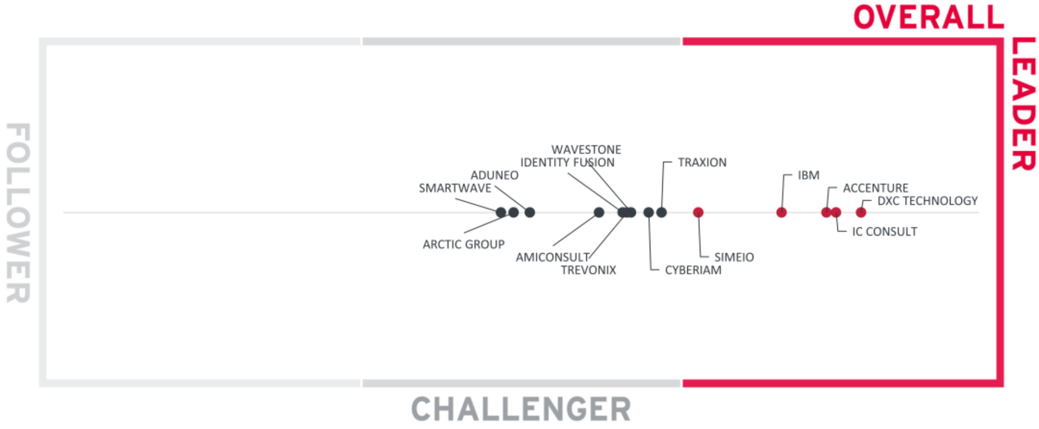


Figure 1: Overall Leadership rating (graphic does not contain a y-axis, vendors to the right score stronger).

Overall Leaders are (in alphabetical order):

- Accenture
- DXC Technology
- IBM
- iC Consult
- Simeio

Service Leadership

Service Leadership is the first specific category examined below. This view is based on the analysis of service features and the overall capabilities of the various services.

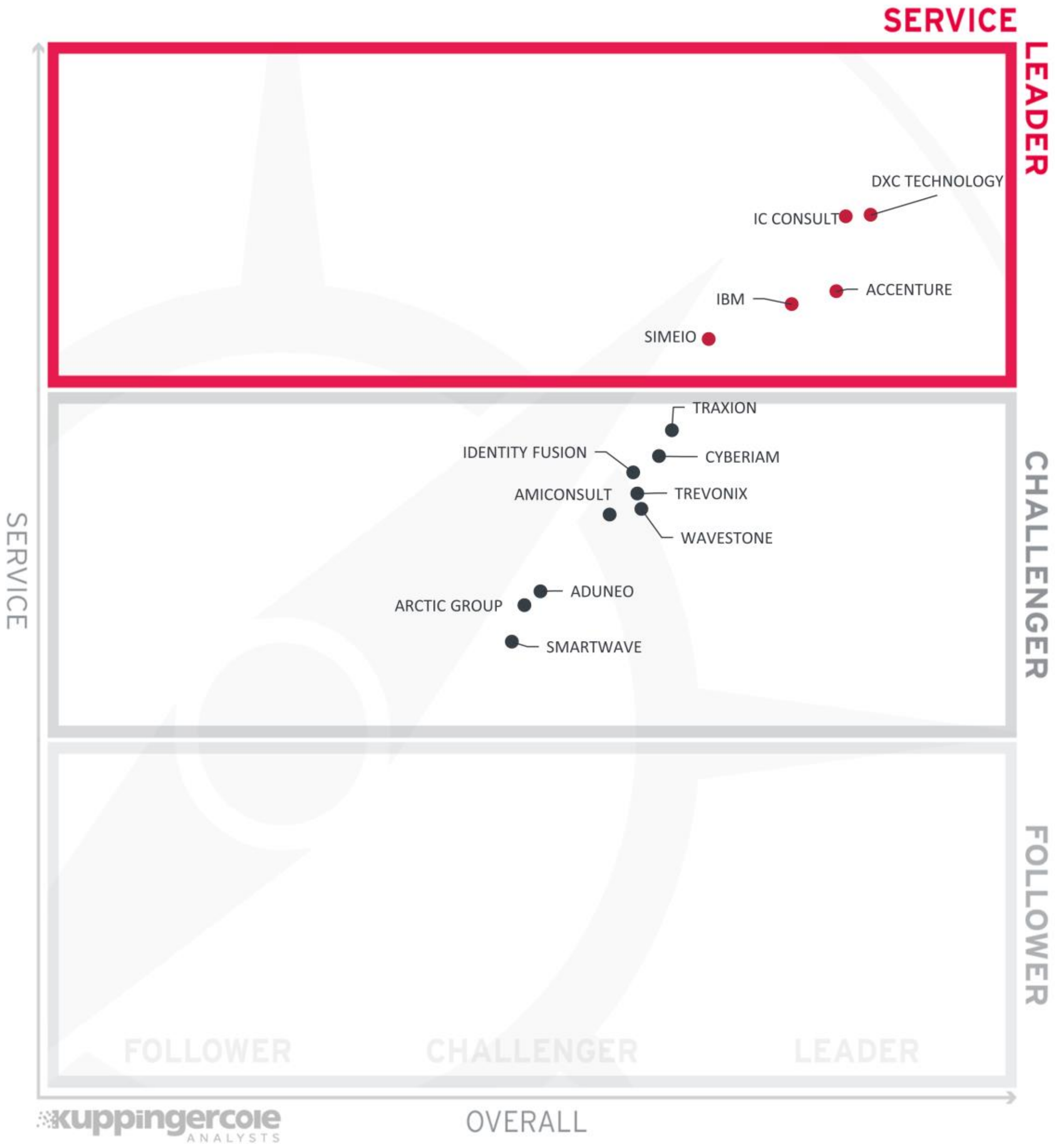


Figure 2: Service Leadership

Product Leadership, or in this case **Service Leadership**, is where we examine the functional strength and completeness of services.

Product Leaders (in alphabetical order):

- Accenture
- DXC Technology
- IBM
- iC Consult
- Simeio

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. Innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other innovative features, while maintaining compatibility with previous versions.

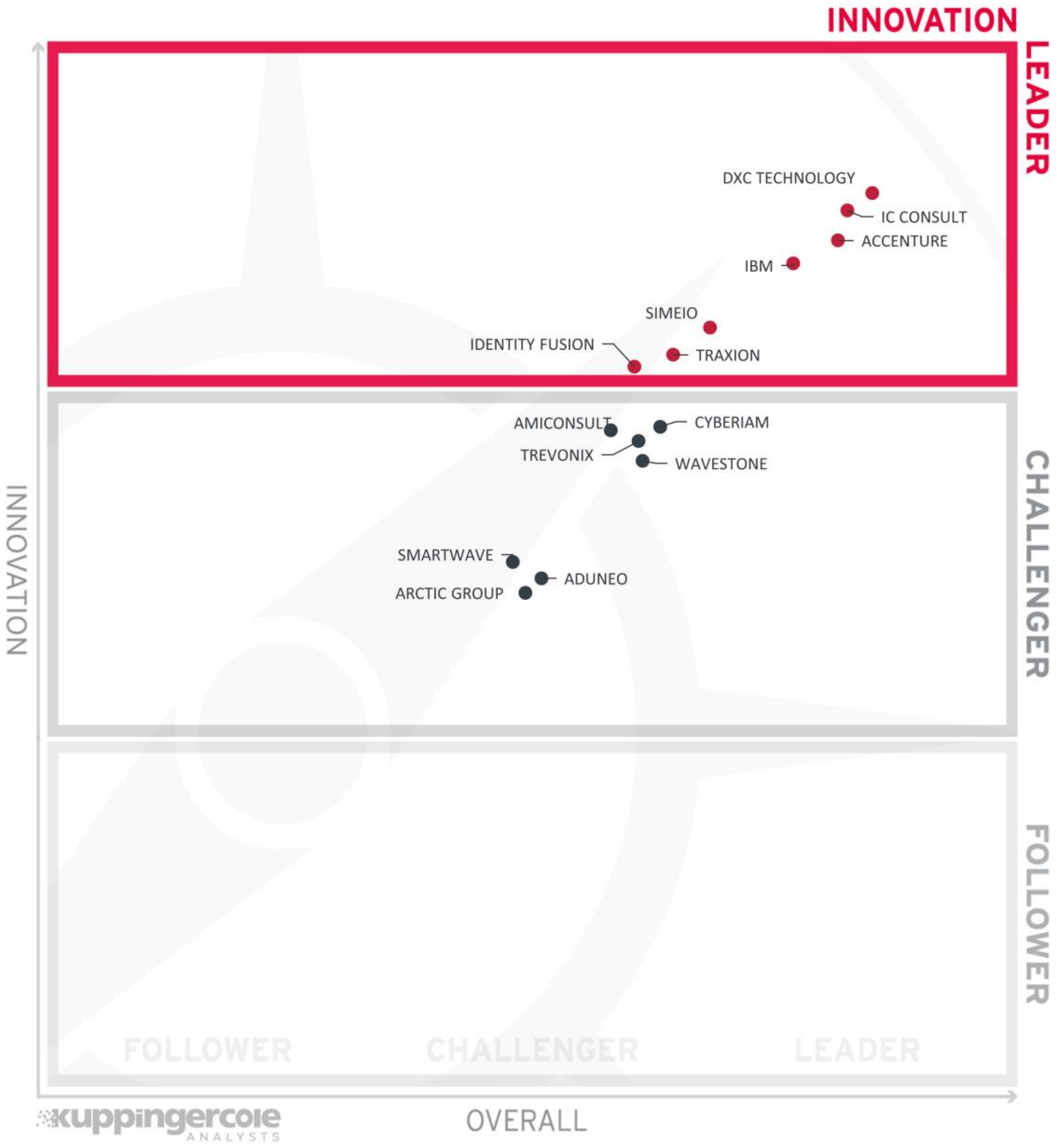


Figure 3: Innovation Leadership

Innovation Leaders (in alphabetical order):

- Accenture
- DXC Technology
- IBM
- iC Consult
- Identity Fusion
- Simeio
- Traxion

Market Leadership

Lastly, we analyze **Market** Leadership. This is an amalgamation of the number of customers, ratio between customers and services utilized, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies. Market Leadership, for the purposes of this report, requires companies to provide services across the European region.

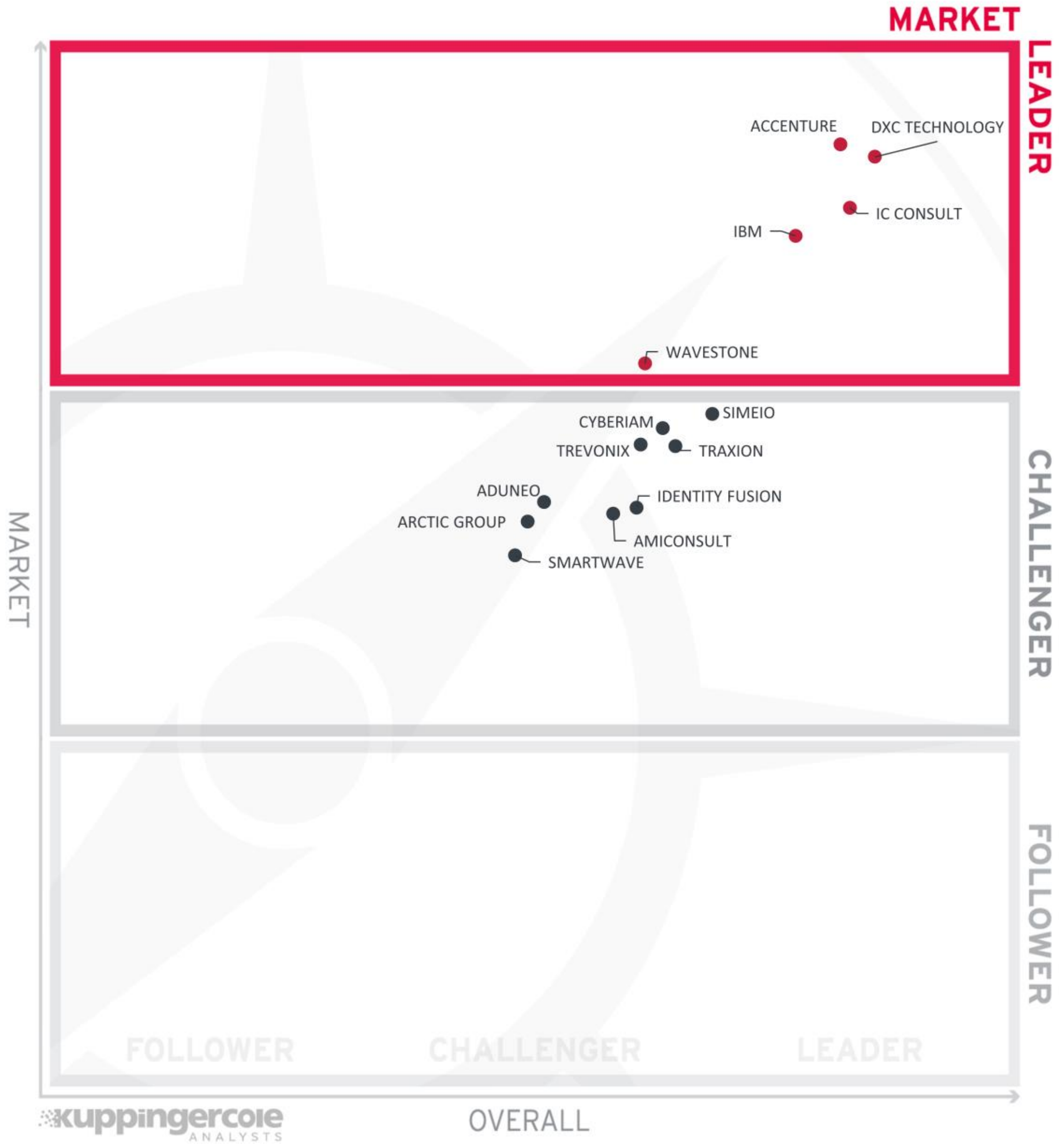


Figure 4: Market Leadership

Market Leaders (in alphabetical order):

- Accenture
- DXC Technology
- IBM
- iC Consult
- Wavestone

Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a solution leader, but for a vendor that is delivering solutions that are both feature-rich and continuously improved. This would be indicated by a strong position in both the Solution Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

The Market/Service Matrix

The first of these correlated views contrasts Service Leadership and Market Leadership.

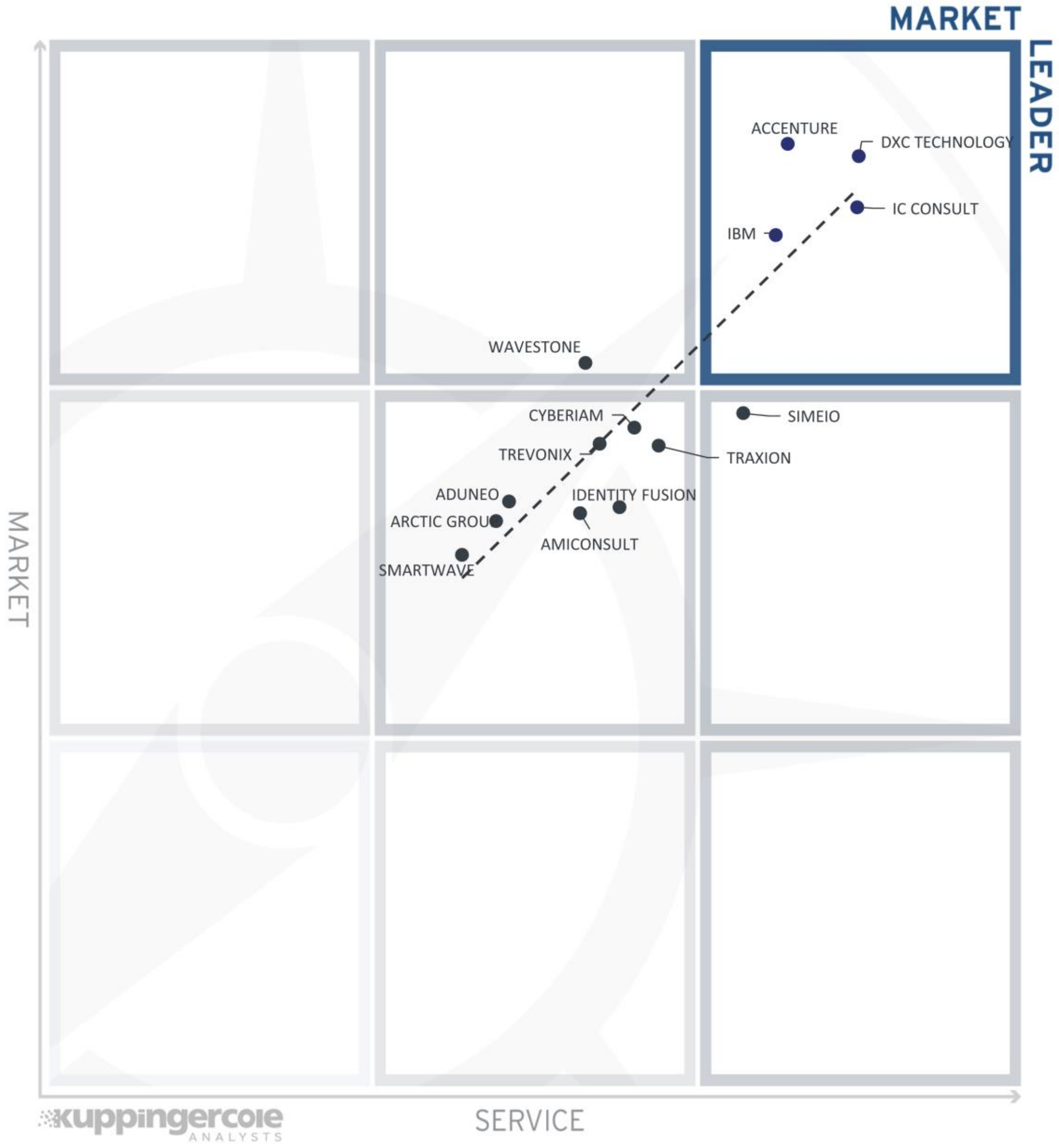


Figure 5: The Market / Service analysis, indicating the relative market strength compared to service rating

Vendors below the line have a scope for improving their market position according to their service maturity. Vendors above the line have strong capabilities when comparing Market Leadership and Service Leadership.

All the vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

The Service/Innovation Matrix

This view shows how Service Leadership and Innovation Leadership are correlated. It is not surprising that there is a fairly good correlation between the two views with a few exceptions. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

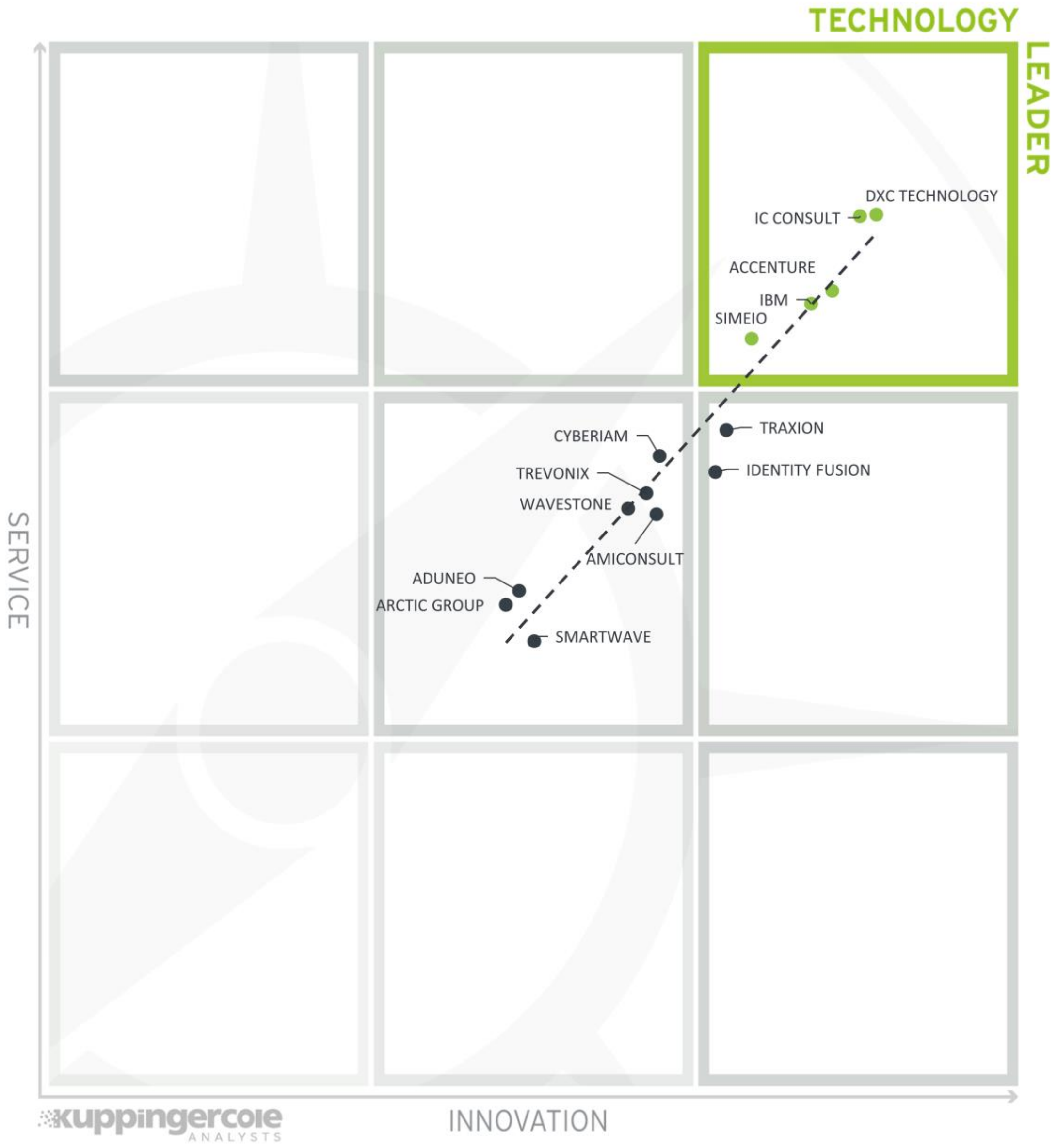


Figure 6: The Innovation / Service rating, relating innovative strength to the current product capabilities

Vendors below the line are more innovative, vendors above the line are, compared to the current Solution Leadership positioning, less innovative.

The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

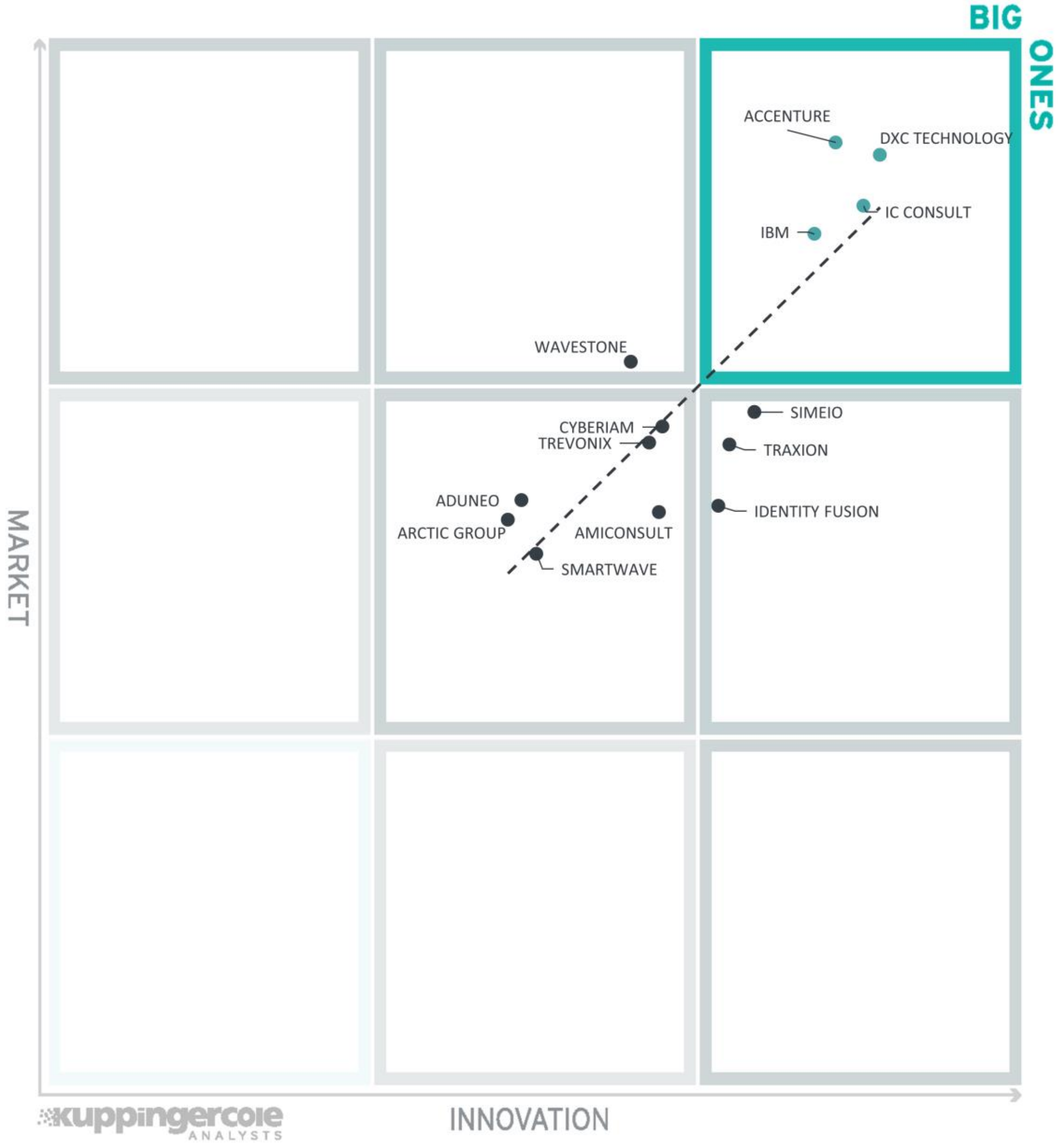


Figure 7: The Innovation / Market matrix, relating innovation to market presence

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate though having less market share, and thus the biggest potential for improving their market position.

Services and Vendors at a Glance

This section provides an overview of the various vendors we have analyzed within this KuppingerCole Leadership Compass on IAM System Integrators. Aside from the rating overview, we provide additional comparisons that put Solution 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 complete regional presence and large customer base yet.

Vendor	Security	Functionality	Service Delivery	Integrations	Serviceability
Accenture	Strong Positive	Strong positive	Strong Positive	Positive	Strong Positive
Aduneo	Positive	Neutral	Weak	Neutral	Positive
amiconsult	Positive	Neutral	Neutral	Strong Positive	Neutral
Arctic Group AB	Strong Positive	Neutral	Weak	Neutral	Neutral
CyberIAM	Strong Positive	Positive	Neutral	Positive	Positive
DXC Technology	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
IBM	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
iC Consult	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Identity Fusion	Strong Positive	Neutral	Neutral	Strong Positive	Neutral
Simeio	Strong Positive	Positive	Neutral	Strong Positive	Positive
SmartWave	Positive	Neutral	Weak	Neutral	Neutral
Traxion	Strong Positive	Positive	Neutral	Strong Positive	Positive
Trevonix	Strong Positive	Positive	Neutral	Neutral	Positive
Wavestone	Strong Positive	Positive	Neutral	Positive	Neutral

Table 1: Comparative overview of the ratings for the service capabilities

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 services, these are listed according to the vendor’s name.

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
Accenture	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Aduneo	Positive	Neutral	Neutral	Weak
amiconsult	Positive	Neutral	Neutral	Weak
Arctic Group AB	Neutral	Neutral	Positive	Weak
CyberIAM	Positive	Neutral	Neutral	Neutral
DXC Technology	Strong Positive	Positive	Strong Positive	Strong Positive
IBM	Strong Positive	Strong Positive	Strong Positive	Positive
iC Consult	Strong Positive	Positive	Strong Positive	Strong Positive
Identity Fusion	Strong Positive	Neutral	Neutral	Weak
Simeio	Positive	Neutral	Neutral	Neutral
SmartWave SA	Positive	Weak	Neutral	Weak
Traxion	Positive	Neutral	Positive	Neutral
Trevonix	Positive	Neutral	Neutral	Neutral
Wavestone	Positive	Neutral	Positive	Neutral

Table 2: Comparative overview of the ratings for vendors

Service/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 Services 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 the LC IAM System Integrators EU, we look at the following seven categories:

- Resource Management: System integrator resource management involves capabilities around how the vendors are proactively working towards providing certifications and training to their IAM professionals. Other capabilities include the ability of IAM professionals to do other tasks and the defined roles of each professional.
- Engagements: Engagements looks at the capabilities of system integrators around establishing relationships with customers over a period of time. Other factors include types and methods of engagements supported by the vendors.
- Project Management: IAM projects are typically complex and need extensive management to help customers in their transformation journey. This category reflects the numbers of project managers (poor, moderate or good strength in numbers), their certification, and experience for each service provider.
- IAM Technologies Breadth: This category represents the major IAM technologies and products such as IGA, PAM, CIAM, etc., that can be delivered by each system integrator.
- API and Integrations: This category considers the experience and capabilities of system integration vendors to provide support for various types of third-party integrations with customer’s solutions as well as the ability of their IAM professionals to code to APIs.
- Auditing and Reporting: System integrators may also provide services such as auditing and forensic capabilities for security incident analysis, reports for compliance frameworks for auditing purposes. This category rates the types and formats of reports that can be developed.
- Professional Services Support: Other advanced services such as authentication methods supported, ability to create and maintain authentication and access control policies, and the ability to provide support services either remotely or on site.

Accenture

Founded in 1989 with its headquarters in Dublin, Ireland, Accenture is a multinational professional services firm that provides consulting, technology, and outsourcing services to businesses and organizations around the world. Accenture has its offices and operations in more than fifty countries. It is one of the largest consultancies globally with strong operations across the entire EU region. Accenture provides integration services in all major industries with a significant share in the finance, health and public services, products and communications, media, and technology industries. Major areas of IAM technology supported by Accenture include IGA, PAM, CIAM, and Access Management, including business consultancy for related business processes, role design, and change management. Other areas of IAM technology supported by Accenture include endpoint security, CASB, API security and management, decentralized identity, verifiable credentials, FRIP, and others.

Accenture has experience with OSes such as Windows, Solaris, RHEL, SUSE and can deliver services on all major platforms by leveraging expertise from its infrastructure services team. Accenture has experience with deploying and maintaining IAM systems on application platforms such as Microsoft, Apache Tomcat, Red Hat JBoss, Oracle WebLogic, IBM WebSphere, and NGINX. Accenture’s dedicated IAM team also supports most databases for deploying and maintaining IAM technologies. They are also experienced with directories such as Microsoft Active Directory, Microsoft Azure AD, and LDAP directory servers. Okta Workforce Identity and AWS Directory Service are also supported. They can support IAM components on IaaS installation for AWS, Microsoft Azure, Alibaba, Google Cloud Platform, Oracle Cloud, and IBM Cloud. Accenture’s support for ITSM integrations is limited to ServiceNow and Atlassian Jira ServiceDesk. They can provide integration with other major ITSM tools by different Accenture service teams.

Accenture’s partnership ecosystem and platform expertise includes all the major vendors. SailPoint, CyberArk, Ping Identity, Saviynt, and Microsoft are some of Accenture’s top-rated delivery and collaboration partners. Accenture invests in training and certification of its own IAM practitioners. Other vendors in the partnership ecosystem include SAP, Oracle, IBM, Okta, and One Identity, among others.

Accenture supports engagements related to RFI, RFP, and architecture review. They also offer strategic consulting, design, implementation, customization, application integration, maintenance, and managed services support. Accenture is focused on providing long-term engagements. Accenture teams are experienced to tackle various engagement methods including but not limited to providing full service with support and subscription, lead consultant with a dedicated team, project manager, defined backups and performing custom development for customers. Accenture has 3,000 certified IAM professionals and developers available for supporting the IAM transformation journey. These professionals are experienced in coding APIs such as SOAP, REST, SCIM, LDAP, Java, and AWS SQS. All major IDEs and SDKs are supported.

There are 3,500 certified project managers in Accenture responsible for 75 percent of the projects being completed on time or undertime and within the allocated budget. Projects that go over time and budget are related to scope changes and external factors. Because of the complexity of many IAM projects, budget contingency is included. Contracts are offered based on the requirements and options range from fixed price to billed hours and ongoing subscriptions. Managed service provider (MSP) contracts are also provided which includes licenses, infrastructure, and labor costs.

Advanced services include support for all major authentication methods including FIDO U2F and FIDO 2.0 authenticators. Auditing and forensic capabilities are available to provide security incident analysis. Reports for all major compliance frameworks are available and can be customized if needed. Furthermore, all IGA report types are available. Accenture teams are also experienced in creating and maintaining policies related to access control, authentication, data access governance (DAG), Governance Risk Compliance (GRC), and Identity Threat Detection and Response (ITDR).

Accenture provides 24x7 support in all major languages. These services are part of their standard solution. Accenture's ability to provide end-to-end services using a global and local approach is one of its strong differentiators. Accenture has an equal footprint in all regions of Europe and focuses on supporting enterprise organizations.

Security	Strong Positive
Functionality	Strong Positive
Service Delivery	Strong Positive
Integrations	Positive
Serviceability	Strong Positive

Table 3: Accenture's rating

Strengths

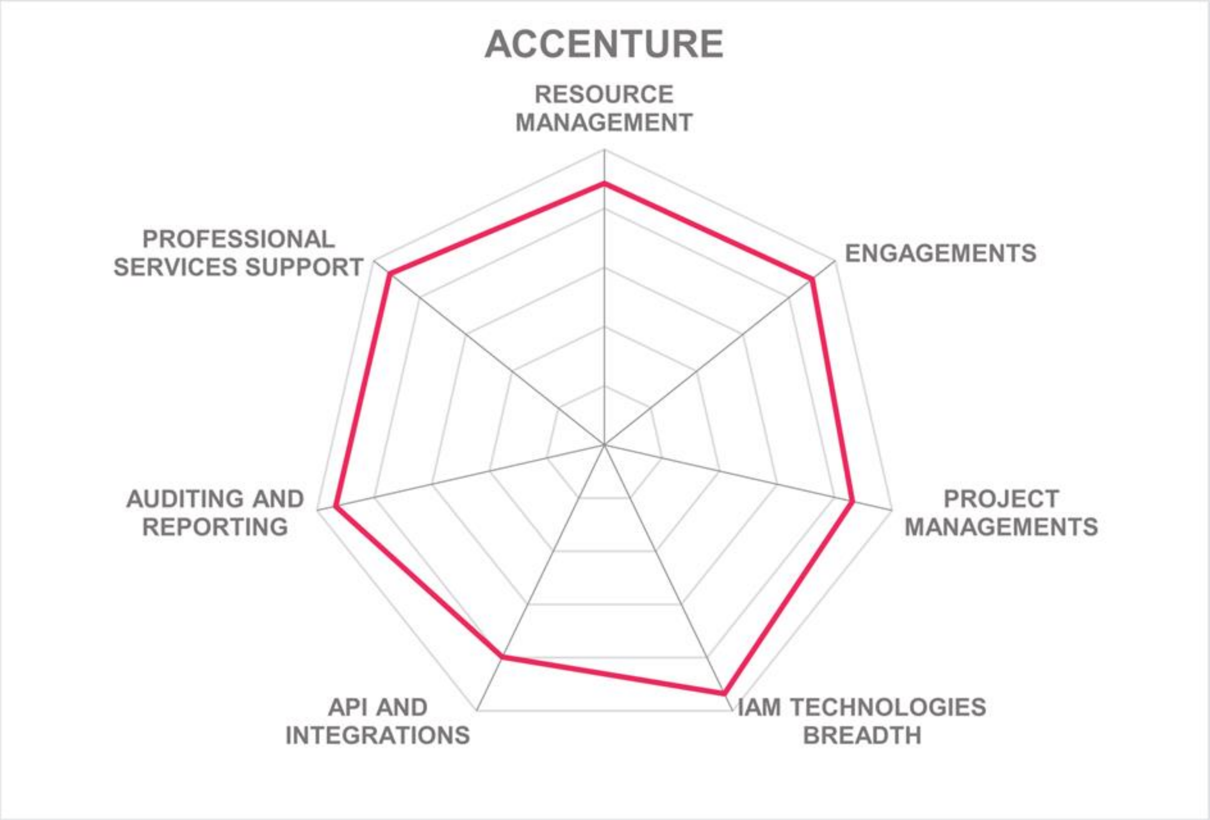
- Breadth of IAM technologies covered
- Global, regional, and local approach to providing services
- Fine-grained IAM transformation journey
- Responsive and step by step approach to project management
- Excellent support for all types of engagements
- Professional services support in all European locations and in all major languages

Challenges

- Mainly long-term engagements are supported
- Support for medium and mid-market organizations is comparatively low
- Moderate but growing partner ecosystem

Leader in

OVERALL LEADER · SERVICE LEADER · INNOVATION LEADER · MARKET LEADER



Aduneo

Aduneo is a French system integrator with their headquarters and operations currently limited to France. Founded in 2001, Aduneo focuses on providing integrations to the banking/ insurance, public healthcare, and energy/ transportation sectors. Major areas of IAM technologies supported by Aduneo are IGA, Access Management, PAM, CIAM and identity federation. Aduneo also considers identities beyond security and address other fields such as identities for the digital workplace, white and yellow pages, and identity information for applications. Other major areas of IAM technology are also supported, however support for decentralized identity, endpoint security, CASB, and FRIP are missing.

Aduneo has experience with operating systems such as Windows, Ubuntu, CentOS, Debian and RHEL. Support for AIX, Solaris and SUSE systems is missing. For deploying and maintaining IAM systems, Aduneo has experience on application platforms such as Microsoft, Apache Tomcat, Redhat JBoss and NGIX. They also support legacy technologies such as Oracle WebLogic and IBM WebSphere. Aduneo has experience with all major databases except IBM DB2. Aduneo supports all major directory services including Okta, Ping, and ForgeRock. For IAM on IaaS installation, Aduneo has experience with Amazon AWS, Google Cloud Platform, IBM cloud, OUTSCALE, NuBo, OVH and Microsoft Azure. Support for Alibaba, Oracle Cloud and Digital Ocean is missing. Aduneo can integrate customer solutions with third party ITSM tools such as ServiceNow and Atlassian JIRA ServiceDesk.

Aduneo's partner ecosystem includes Ping Identity, Microsoft, Okta, Oracle, Saviynt, Yubico, One Identity, Evidian, Sharelock and others. Aduneo Campus is an initiative which partners with ForgeRock as an official French speaking training center which also integrates as an open source. The training center is equipped to train managers, CEO, CISO's and others.

Aduneo is experienced in engagements related to RFI, RFP, and architecture review. It also offers an end-to-end process including consulting, identity and access integration, application development, deployment using automation, and technical support. Managed services support is missing. Most of the IAM engagements are focused on longer duration while Access Management engagements can vary from few days to few years, based on requirements. Aduneo's team is experienced in providing full service including ongoing subscription, defined backups, and integrators working with customer developers. Engagements methods where customers provide their project managers and a lead consultant with a team are also possible. Over sixty-five consultants, developers, and integrators from Aduneo's team are certified by product vendors. Aduneo IAM professionals are also experienced in coding APIs. They can code for SOAP, REST, SCIM, LDAP, JSON, and GraphQL. Other API protocols supported are XML-RPC, Webhooks, RADIUS, and TCP Socket API. They support IDE and SDKs such as Python, Java, .NET, and JavaScript. Major SDKs such as Android, iOS and C/C++ are missing.

Aduneo's project managers have an average experience of over 10 years each. These project managers are instrumental in the timely completion of projects; however, due to delays caused by clients and other external factors, only 50 percent of projects have been completed on time or undertime. On the positive side, 90 percent of projects have been completed within the allocated budget under budget. Aduneo supports these projects by offering varying contract types such as fixed price including software and labor and ongoing subscriptions. Contracts billed based on hours are not provided.

Other advanced services such as authentication methods provided include all conventional types, however support for biometric authentication is missing. FIDO U2F and FIDO 2.0 authenticators are also supported such as WebAuthn, YubiKey and Winkeo. Auditing and forensic capabilities are missing. However, the team has experience developing with all major IGA and AG related reports. Support for major compliance frameworks is limited to GDPR and PCI-DSS. Aduneo's team can also support in creating and maintaining policies related to access control, authentication, and GRC. Support for DAG and ITDR is missing.

Aduneo is based in France and currently focused on customers in French speaking countries such as Belgium, France, Luxembourg, and Switzerland. It can provide support in French and English. Support is provided 24x7 using the ticketing platform while their hotline can also be accessed for requesting support during working hours. Aduneo provides professional services in French speaking countries of Europe. Mid-market industries in the finance (banking/ insurance) sector and public sector are their focus but Aduneo can also provide services to enterprise level organizations.

Security	Positive
Functionality	Neutral
Service Delivery	Weak
Integrations	Neutral
Serviceability	Positive

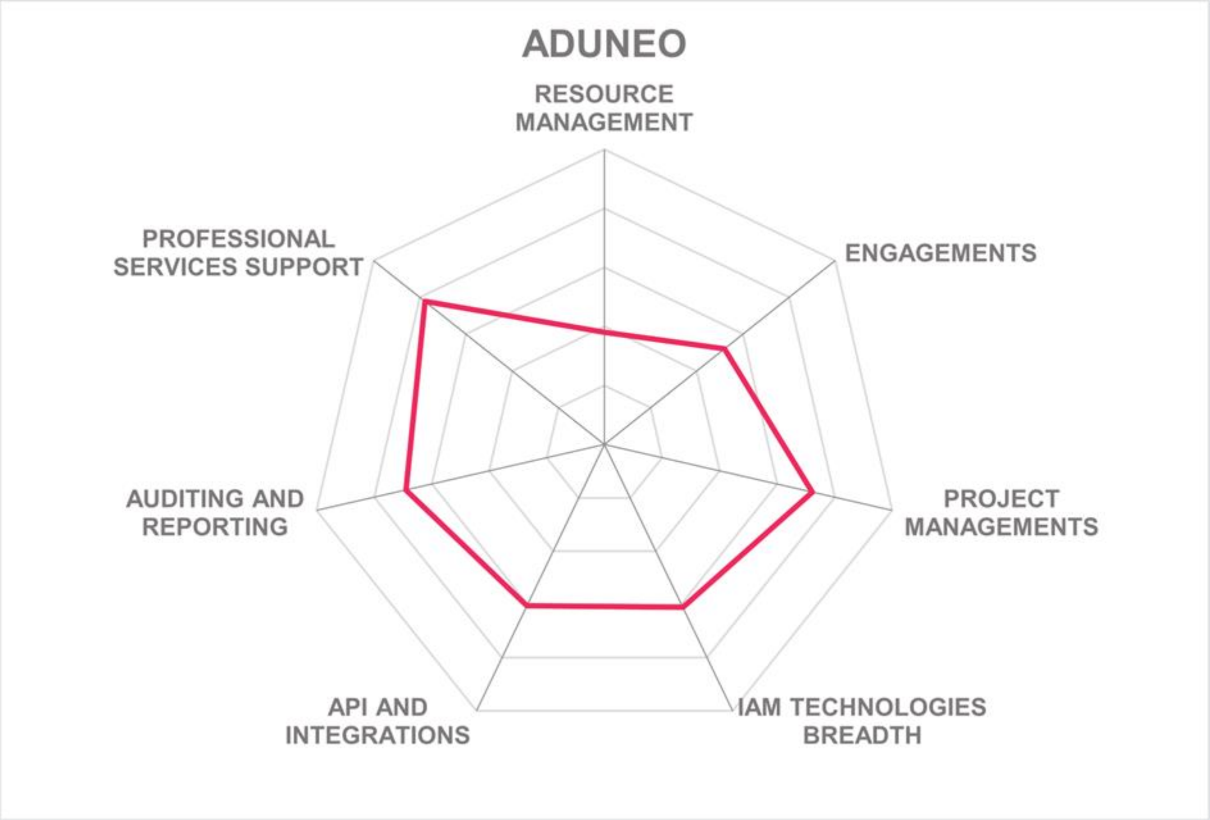
Table 4: Aduneo's rating

Strengths

- Good project lifecycle management
- Excellent support in French speaking regions and works as a training center for French speaking people of ForgeRock
- Moderate but growing partner ecosystem
- Vendor showing strong signs of growth and innovation for the next years
- Wide variety of engagement types and methods supported

Challenges

- Operations are currently limited to French speaking countries but there plans to expand in North Africa in 2024
- Supports majority of databases, OSes, and platforms but some are missing
- Support for reports of major compliance frameworks is limited


ADUNEO
RESOURCE MANAGEMENT
ENGAGEMENTS
PROJECT MANAGEMENTS
IAM TECHNOLOGIES BREADTH
API AND INTEGRATIONS
AUDITING AND REPORTING
PROFESSIONAL SERVICES SUPPORT

amiconsult

Founded in 2003 with its headquarters in Karlsruhe, Germany, amiconsult is an IT consulting company that specializes in workforce and customer identity and access management and SAP technology. With headquarters in Germany, amiconsult mainly focuses on serving customers in the DACH and the Benelux regions. Their main industrial focus is manufacturing, but they have significant customers in the retail, finance, healthcare, and hospitality sectors. amiconsult covers all major IAM technology areas. Support for other areas of IAM technology such as Web Access Management (WAM), API security, decentralized identity, and non-human access management among others is available. FRIP, DLP, endpoint security, and CASB support is missing.

amiconsult has experience in deploying and maintaining IAM systems on operating systems such as Windows, Ubuntu, Debian, RHEL, CentOS SUSE Linux however experience for Solaris, and AIX operating systems is missing. amiconsult has experience with application platforms such as Microsoft, Apache Tomcat and NGINX. Support for Oracle WebLogic, IBM WebSphere and Red Hat JBoss is missing. amiconsult is experienced with all major databases except IBM DB2. Similarly, the amiconsult team is experienced in supporting all major directory services including Google Workspace and Microsoft Azure. IaaS installation on IAM components is supported for Amazon AWS, Google Cloud Platform, Microsoft Azure and STACKIT. They do not work with Alibaba, Oracle Cloud, IBM Cloud, and Digital Ocean. amiconsult can integrate customer's solutions with all major third party ITSM solutions including SAP solution manager. The ability to integrate IAM solutions with SIEM solutions is also available.

amiconsult has a moderate partner ecosystem. Okta, Omada, SailPoint, Saviynt, Microsoft, Ping Identity, cidaas, One Identity and SAP are its product partners. amiconsult is a silver partner of Ping Identity and SAP and advanced partner of STARFACE.

amiconsult supports all types of engagements including RFI, RFP, architecture review, design, implementation, and Managed service support. Support for coding, customization, maintenance, and strategic consulting is also provided. amiconsult prefers long-term engagements with its customers who are either repeat or long-term, with contracts lasting for more than one year. amiconsult has fifteen consultants and integrators which are certified by product vendors. These consultants are also well experienced in coding to all major APIs including SOAP, REST, OData, SCIM, LDAP, and GraphQL. All types of SDKs and IDEs are supported.

amiconsult has fifteen project managers, each has an average of 5 years' experience and have multiple certifications such as PSM, PSO and Prince2. amiconsult states that they have completed all projects within the given time and given budget and with no record of failed projects. Projects and contracts are completed based on billed hours and ongoing subscriptions.

Advanced services provided by amiconsult include support for user self-service for many types of authentication mechanisms including FIDO 2.0 and Windows Hello. SAML, OAuth2, OIDC and JWT are also supported. Support for developing or customizing reports for major compliance frameworks is limited to GDPR and SOX. All IGA report types are also available. amiconsult also has experience creating and maintaining all major types of policies; however, support for ITDR related policies is on the roadmap.

amiconsult can provide support in English and German languages. They do not provide 24x7 support, but remote service is available. Remote service includes consulting to clients around the topics of assessing client needs, designing tailor-made IAM solutions, remotely implementing solutions, providing training and ongoing support for maintenance. amiconsult is currently focused on providing services to the medium market level organizations and enterprises.

Security	Positive
Functionality	Neutral
Service Delivery	Neutral
Integrations	Strong Positive
Serviceability	Neutral

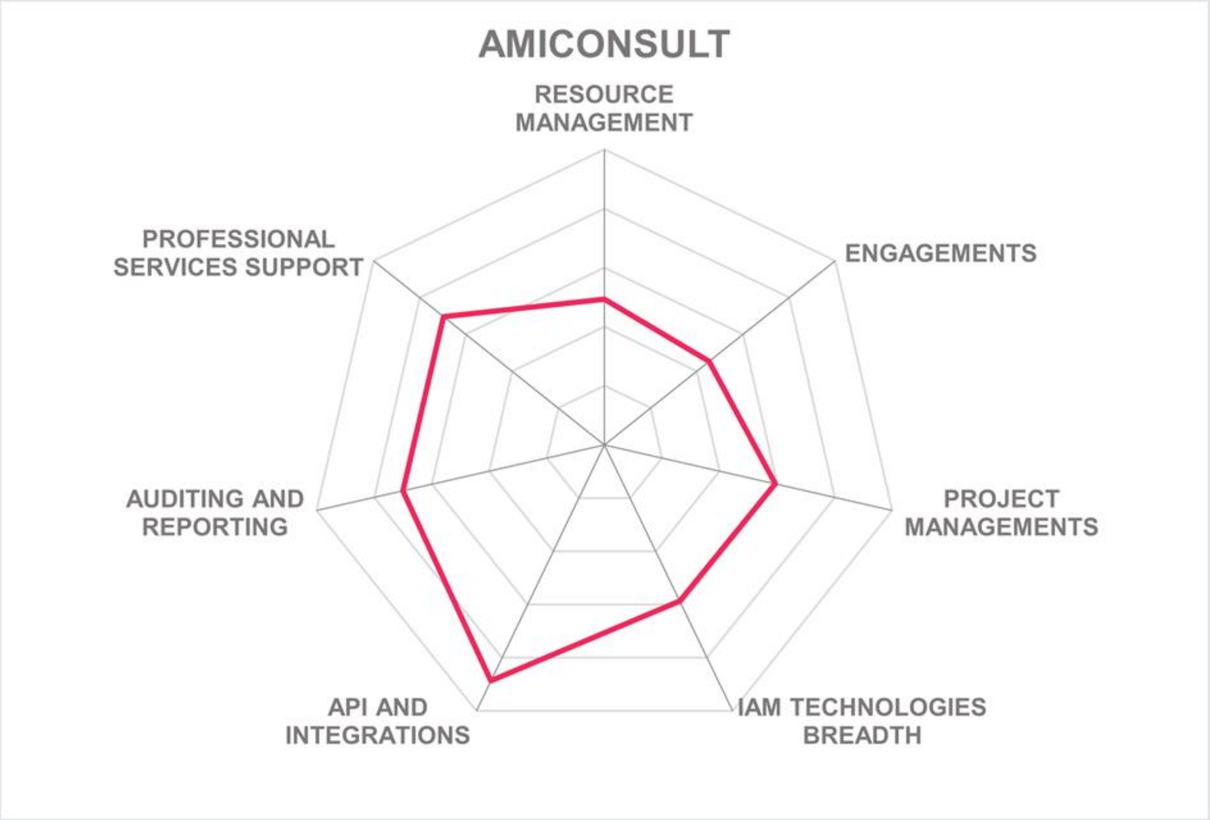
Table 5: amiconsult’s rating

Strengths

- Breadth of IAM technologies supported
- Coding for all mainstream APIs is available
- Strong support for other services such as policy management, SDK support
- Ability to fulfil projects on time and on budget with no failed projects
- Professional services support
- Excellent support for integrating with third party ITSM solutions and SIEM solutions

Challenges

- Focus is currently limited to DACH region customers
- Moderate but growing partner ecosystem
- Reports for major compliance frameworks are limited


AMICONSULT
RESOURCE MANAGEMENT
ENGAGEMENTS
PROJECT MANAGEMENTS
IAM TECHNOLOGIES BREADTH
API AND INTEGRATIONS
AUDITING AND REPORTING
PROFESSIONAL SERVICES SUPPORT

Arctic Group AB

Founded in 1996, Arctic Group AB is an IAM system integrator with their headquarters in Norrbotten, Sweden with focus on cybersecurity IAM. Arctic Group also provides services for application development and management, fraud management, and migration to customers mainly in the Nordic region with limited presence also in the UK and Ireland markets. Finance, telecommunications, aerospace & defence, government, and retail are the key industrial sectors to which Arctic Group provides its services. All major areas of IAM technology including IGA, PAM, and CIAM are supported by Arctic Group. Support for other areas of IAM such as Web Access Management (WAM), API security, MFA, ITDR Access governance, and endpoint security is also available.

Arctic Group has experience with all major operating systems for deploying and maintaining IAM systems. Arctic Group can deploy and maintain IAM systems on all major application platforms including Apache Tomcat, red Hat, JBoss and Oracle WebLogic. Support for IBM WebSphere and NGINX is not available. Arctic Group's experience with databases is limited to Microsoft SQL Server, Oracle Database, and MySQL. Arctic Group is experienced in supporting Microsoft Azure directory, Azure AD, and LDAP directory servers. Support for IAM on IaaS installation is not provided and ITSM integration support is limited to ServiceNow and Atlassian Jira ServiceDesk. Integrating IAM solutions with SIEM solutions is also supported such as Syslog and APIs.

Arctic Group has a strong partner ecosystem. Being a gold partner of Atlassian, Arctic Group has expertise with JIRA and Confluence. CyberArk, One Identity, Ping Identity, RSA, Omada and SailPoint are other major partners in their ecosystem. Arctic Group is also a part of the Allurity Group which allows it to leverage knowledge from other companies in the group for any additional requirements.

Arctic Group supports all types of engagements including end-to-end processes, RFI, RFP and architecture review. Most of these engagements are aimed at establishing long-term or recurring relationships with customers. They are experienced in tackling various engagement methods from providing full service including support with subscriptions, custom development for customers, and having integrators collaborate with customer developers. Defined backups and a team consisting of lead consultant is also available. Arctic Group has fifteen certified consultants and five certified developers to fulfil the engagement requirements. A dedicated developer team is available which is experienced in coding APIs across different protocols such as SOAP, REST, SCIM and LDAP. Support for AWS SQS, AMQP, Google Pub/Sub, and Socket API protocols is not available. The team is also experienced in supporting IDEs and SDKs such as Java, C/C++, .NET, Python, Ruby, and JavaScript. They do not support development using Android and iOS SDKs.

Arctic Group has ten project managers with an average experience of 10 years. This allows 90 percent of the projects to be completed on time or earlier and 80 percent of projects to be completed within allotted budget or under budget. Projects and budget run over only due to scope changes during the project. The contracts offered can be tailored based on requirements, but the standard approach of billed hours or fixed price is supported.

Support for advanced services such as authentication all major authentication methods. Arctic Group supports FIDO U2F and FIDO 2.0 authenticators by working closely with Yubico and RSA. Support for SAML, OAuth2, OIDC and JWT authenticators is also provided. Auditing and forensic capabilities are included in the IGA projects. Compliance framework support is limited to GDPR. All IGA related reports are available except delegated access, SoD, key risk indicators, rehires and users with emergency access. Arctic Group can support creating and maintaining policies related to access control and authentication. Support for policies related to DAG, GRC, and ITDR is missing.

Arctic Group can provide support in English, Norwegian, and Swedish languages. Various levels of support are available, with 24x7 support being the highest possible option. Arctic Labs is a unique proposition from Arctic Group where existing customers can pre-test new features through collaboration. They have a dedicated developer team which works independently from engagements on creating tailor made features and does not rely on IAM integrations. Roadmap includes integrating cybersecurity products outside IAM area and developing more in the ITDR area. Arctic Group is also working on AI/ML capabilities in each product. Arctic Group focuses on providing integration services to enterprise customers but also has a significant share in the mid-market segment.

Security	Strong Positive
Functionality	Neutral
Service Delivery	Weak
Integrations	Neutral
Serviceability	Neutral

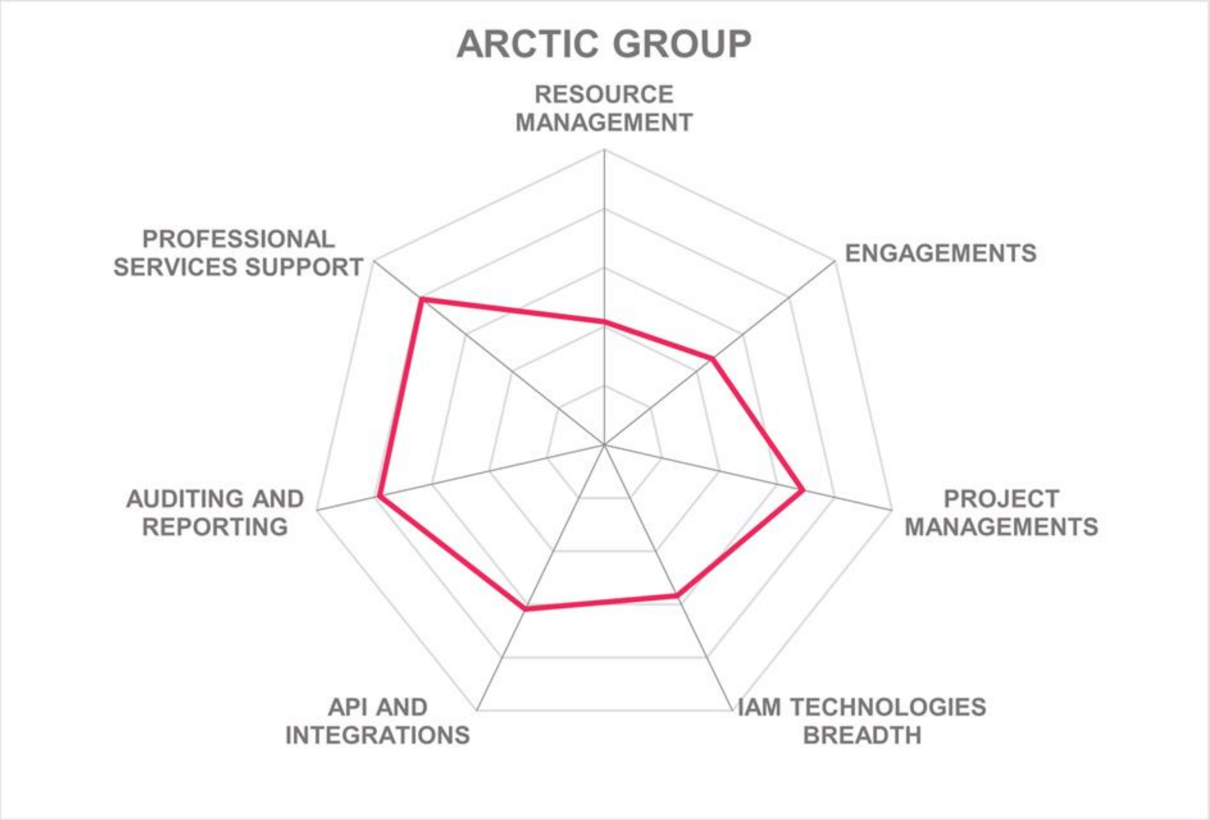
Table 6: Arctic Group’s rating

Strengths

- 24x7 support for all professional services is available
- Auditing and reporting capabilities
- High success rate of projects
- All engagement methods and types supported
- Advanced services such as authentication
- Support for all major operating systems for deploying and maintaining IAM systems

Challenges

- Reports for major compliance frameworks are limited to GDPR
- Good partner ecosystem but still a few major vendors are missing
- Support for integration with third party ITSM solutions is weak


ARCTIC GROUP
RESOURCE MANAGEMENT
ENGAGEMENTS
PROJECT MANAGEMENTS
IAM TECHNOLOGIES BREADTH
API AND INTEGRATIONS
AUDITING AND REPORTING
PROFESSIONAL SERVICES SUPPORT

CyberIAM

Founded in 2017, CyberIAM has its headquarters Cheshire, UK but with a strong presence across the world. CyberIAM specializes in managed cybersecurity solutions in addition to identity, access, and privileged management solutions. Their portfolio ranges from advisory to professional services and support services. CyberIAM provides services to finance, retail, public sector, healthcare, and telecommunications sectors. CyberIAM can support all major IAM technologies as well as other areas of IAM technology such as IDaaS, API security, MFA, Access Governance and ITDR. They do not support FRIP, DLP, Web Access Management, CASB, and Web Application Firewalls.

CyberIAM is experienced with all major operating systems for maintaining and deploying IAM systems; however, support for applications platforms is limited to Microsoft, Apache Tomcat and Red Hat JBoss. They do not support Oracle WebLogic, IBM WebSphere, or NGINX. CyberIAM has deployed and maintained IAM systems on all major databases. Directory services support is provided for Microsoft Azure Directory, Microsoft Azure AD, LDAP, Ping Directory, and Oracle Directory. CyberIAM supports IaaS installation of IAM components for Amazon AWS, Google Cloud Platform and Microsoft Azure. They do not support Alibaba, Oracle Cloud, IBM Cloud and Digital Ocean. CyberIAM supports integrating customer solutions with third-party ITSM solutions for ServiceNow, Atlassian Jira ServiceDesk, BMC Helix and Cherwell. They also support Zendesk and HubSpot for ITSM integration. CyberIAM can also integrate IAM solutions with SIEM solutions such as Splunk.

CyberIAM has a strong partner ecosystem. CyberArk, SailPoint, BeyondTrust, Microsoft, Ping Identity, Saviynt and Okta are its partners for delivering IGA, PAM, CIAM and SSO solutions. Strivacity, Softcat, Ultima, boxxe and Orange Cyberdefense are its other partners. CyberIAM provides maturity assessment including RFP and roadmap before moving to selecting one of its product partners.

CyberIAM has capabilities around supporting all major types of engagements including providing expert services and maturity assessments. They support creating strategic short- and long-term roadmaps for integration fulfilment. CyberIAM team is experienced in providing full service including ongoing support with subscription, defined backups, and end-to-end service of a project. Their support types range from maturity assessment to implementation and managed services. CyberIAM has forty-six certified consultants and forty-nine certified developers to fulfil integration projects. Their integration team is experienced in coding APIs such as REST, SCIM, SOAP, LDAP, RADIUS and JSON-RPC and XML RPC. They do not support GraphQL, AWS SQS, or Google Pub/Sub. CyberIAM provides IDEs and SDK support for Java, C/C++, Python, .NET, Ruby, and JavaScript. They do not support Android and iOS SDKs.

CyberIAM’s team consists of project managers with an average experience of 15 years. Their project managers are certified in Agile PM, Prince2, PMP and Scrum Master. These project managers are instrumental in CyberIAM having a 95 percent success of finishing projects within allotted time and 96 percent success of finishing projects on-budget. CyberIAM offers contract types ranging from fixed price including software and labor costs to billed hours and ongoing subscriptions, depending on project requirement.

CyberIAM's advanced services includes providing support for all major authentication methods including FIDO U2F and FIDO 2.0. SAML, Oath2, OIDC and JWT federation are also supported. Their support for major compliance framework reports is limited to FIPS 200, NERC CIP, NIST SP 800-53, ISO27001 and TSR. They do not support reports for GDPR, FERPA, FISMA and HIPAA. CyberIAM supports all major IGA and AG related reports. They provide policy management for access control, authentication, data access governance, GRC, and ITDR.

CyberIAM can provide 24x7 support services in English, German, French, Spanish, Russian, Finnish, and Dutch. Other languages such as Hindi, Portuguese, Tamil, and Afrikaans are also supported. CyberIAM with its global presence and strong partnerships with leading product vendors, provides its services mainly to the mid-market and enterprise level organizations.

Security	Strong Positive
Functionality	Positive
Service Delivery	Neutral
Integrations	Positive
Serviceability	Positive

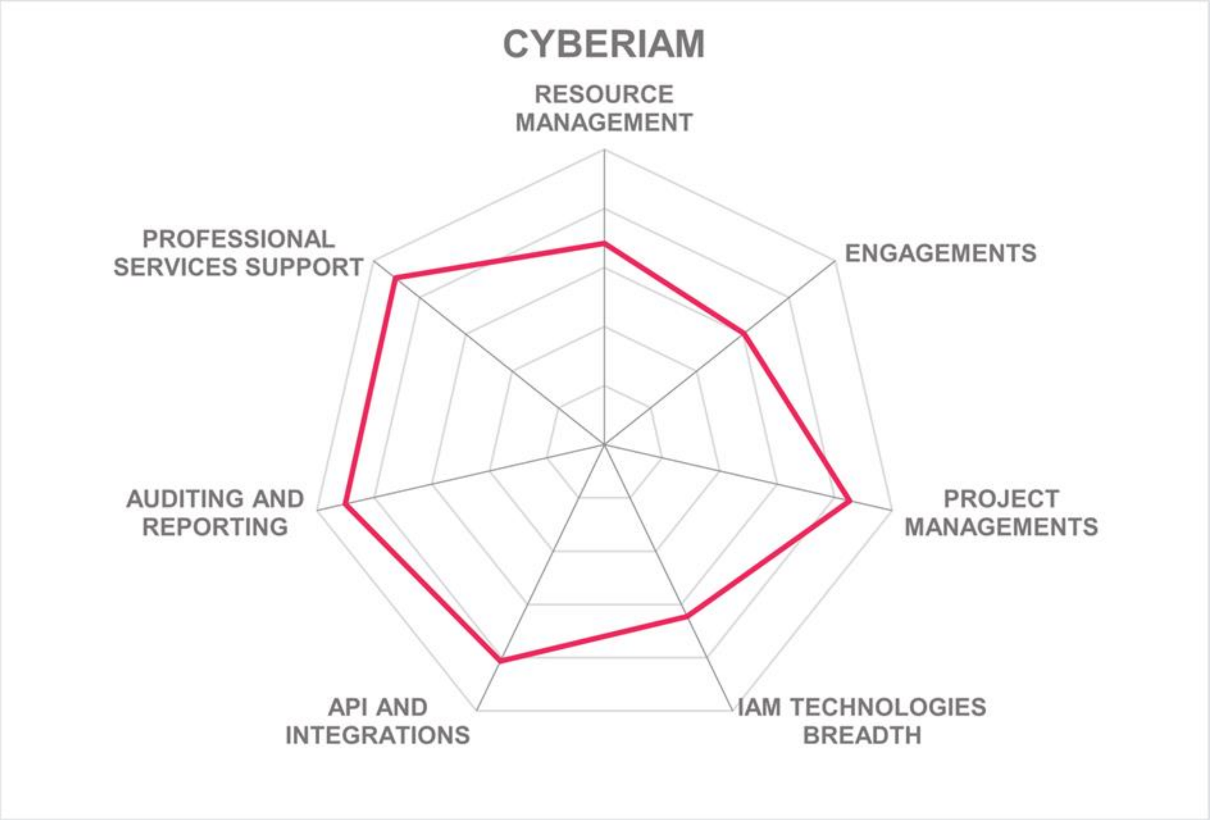
Table 7: CyberIAM's rating

Strengths

- Professional service support
- IAM technologies covered are moderate but major technologies such as IGA, PAM, CIAM are supported
- Project management capabilities with detailed activity plans
- Auditing and reporting capabilities
- Consultant and developer certification is proactively supported
- Breadth of services offering

Challenges

- Current focus is mainly on the UK region but growing to other parts of Europe
- Supports majority of APIs and integration to third parties but still a few are missing
- Cost overrun guarantees for projects not provided


CYBERIAM
RESOURCE MANAGEMENT
ENGAGEMENTS
PROJECT MANAGEMENTS
IAM TECHNOLOGIES BREADTH
API AND INTEGRATIONS
AUDITING AND REPORTING
PROFESSIONAL SERVICES SUPPORT

DXC Technology

Founded in 2017 with headquarters in Virginia, USA, DXC Technology has a global presence providing IT security services. DXC has a significant presence in the European market with most operations in the DACH region, UK, Benelux, and Southern Europe. DXC also has an emerging presence in the Nordics and Eastern European countries. DXC operates across ten verticals with many customers from the finance and manufacturing sectors. DXC supports all major IAM technology areas. They support both on premise and cloud deployments. DXC covers all other areas of IAM technology including FRIP, DLP, CASB, Endpoint Security, RPA, AI/ML, Machine Identity Management, and Decentralized identities.

DXC Technology has experience operating all major operating systems for deploying and maintaining IAM systems. DXC Digital Identity uses Midrange, Wintel teams and cloud platform services for installing and operating products on majority of operating systems. They support deployments for application platforms like Microsoft, Apache Tomcat, Oracle WebLogic, and IBM WebSphere. DXC has its platform and application teams to support client's request for any other specific platform and OS DXC can work will all major databases for operating IAM systems. DXC's experience with directories includes Microsoft, LDAP and Oracle, ForgeRock, NetIQ, IBM, and open-source LDAP products. They support installation of IaaS or IAM components for Microsoft Azure, Alibaba, Amazon AWS, and Google Cloud Platform. They do not support IaaS installation of IAM components on Oracle Cloud, and IBM Cloud. DXC supports integration of customer solutions to ITSM solutions for ServiceNow, BMC Helix, and ManageEngine ServiceDesk Plus. They can support other ITSM solutions based on client requirements. DXC supports SIEM integration implementing a customer connector from IGA tool into client's chosen SIEM tool.

DXC Technology has a very strong partner ecosystem. Microsoft, ForgeRock, SailPoint, Okta, Thales, CyberArk, Oracle, and IBM are some of its major partners for but not limited to access management, IGA, PAM and zero trust solutions. DXC has 3,500+ certified security professionals.

DXC supports an end-to-end approach for identity management. They support engagements methods such as RFI, RFP, strategy, implementation, managed services, testing, decommissioning, and customization. DXC operates short-term projects to long-term support and recurring support. DXC can also support taking over existing projects and fulfilling them according to the requirements. Application development and operational services are also available. DXC uses its global presence and regional approach for projects. DXC's IAM professionals are most, but not all, are certified in various products such as CyberArk Defender, SC-300 Microsoft modules, Thales STA Professional, and SailPoint IdentityIQ Professional. Their IAM professionals are also certified in multiple other vendor certifications. DXC's developers and consultants are experienced in coding APIs such as SOAP, REST, SCIM, Webhooks, LDAP, RADIUS and JSON-RPC. They do not support GraphQL, gRPC, AWS SQS, and UDP/TCP Socket. DXC supports all major IDEs and SDKs.

DXC has fifty project managers with 15 years of experience running large programs. Junior project managers are also available to support senior managers with basic administrative tasks. Eighty percent of DXC's projects are completed on time and on budget. DXC supports agile contracts, fixed price for labor only, fixed price including software and labor, billed hours, and subscription models for support.

DXC's advanced services include support for all major authentication methods. Authentication for decentralized identities and verified credentials is also supported. DXC works with Yubico and Thales for FIDO U2F and FIDO 2.0 authenticators. They also support SAML, OAuth2, OIDC, and JWT federation. DXC supports reports for all major compliance frameworks except FERPA. ITAR and other state privacy laws are also followed by DXC. They also support all IGA report types. The DXC digital identity team does not define KPIs and KRIs, but their security team is able to jump in and assist in this process. Identity team also provides support for generating data to feed to SIEM or corporate risk register tools. DXC also supports creation and maintenance of policies related to access control, authentication, GRC, ITDR, and DAG.

DXC provides 24x7 support in most of the global languages. Customers can select between on demand help, 9 to 5 support, or full 24x7 services. DXC also provides remote support for engagements not following the 24x7 model. DXC roadmap includes investing in CIAM, CIEM, zero trust, and passwordless authentication, among others. DXC, with its global presence and regional approach, is supporting mostly enterprise level organizations and significant customers from mid-market segment.

Security	Strong Positive
Functionality	Strong Positive
Service Delivery	Strong Positive
Integrations	Strong Positive
Serviceability	Strong Positive

Table 8: DXC Technology's rating

Strengths

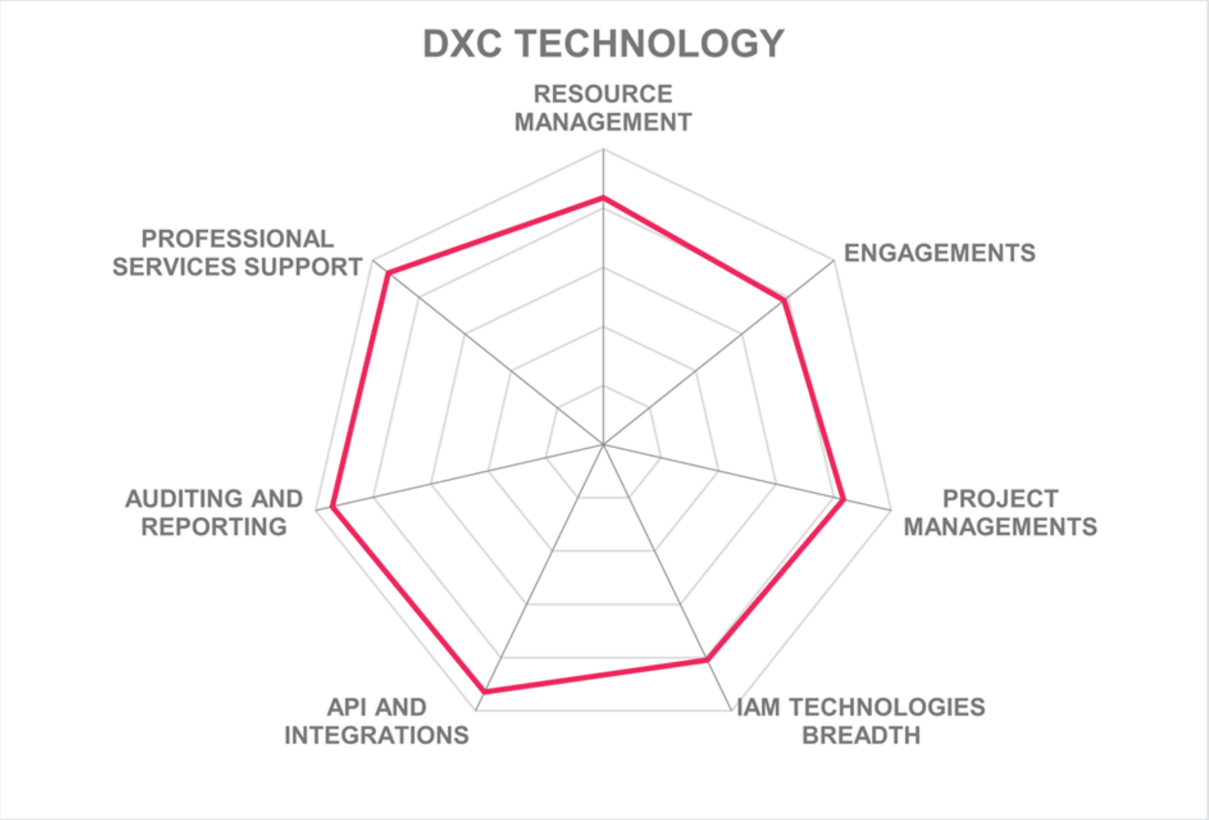
- Global Partner ecosystem
- Detailed methodology for IAM strategy, implementation, and managed services
- Professional service support
- Global presence can be leveraged for delivering projects locally
- All engagement methods, types, and duration supported
- Support for audit and compliance framework reports
- Strong workforce with latest certifications

Challenges

- IaaS installation of IAM components is limited
- Support for API coding is missing some protocols

- DXC’s Digital Identity team does not normally define KPIs and KRIs for customers but DXC’s security team is able to assist in this process

Leader in OVERALL LEADER SERVICE LEADER INNOVATION LEADER MARKET LEADER



IBM

Founded in 1911, IBM has its headquarters in New York, USA. IBM is a major player in the market with its strong global presence. IBM provides its integrations services mainly to customers in the UK, DACH, Benelux, and Southern Europe. They also provide services in the Nordics, eastern Europe, and Middle East. IBM supports all major IAM technology areas. IBM also supports emerging technologies such as self-sovereign ID, decentralized ID, CIEM, secrets management, and digital wallets. They also support other areas of IAM technology including Web Access Management, non-human access management, and containerized workload access.

IBM has experience with all major OSes for installing and maintaining IAM systems. They have experience deploying and operating IAM components on mainframe and various cloud platforms. IBM has experience of deployment across all major application platforms covering both COTS services and bespoke custom-built solutions. They provide support for all major databases. IBM is experienced in supporting all major directory services including IBM security directory server, Oracle DSS, Oracle virtual Directory, and Radiant Logic Virtual Directory. They support IaaS installation of IAM components for Alibaba, Amazon Web Services, Google Cloud, Microsoft Azure, Oracle Cloud, and IBM Cloud. IBM supports ITSM integration with customer solutions for most of the ITSM solutions including ServiceNow, BMC Helix, Cherwell, Atlassian JIRA, and TOPdesk. SIEM integration is available for Splunk, and the support depends on the product implementation.

IBM has a very strong IAM partner ecosystem. All leading vendors in the market are IBM partners for delivering end-to-end IAM services for a variety of IAM solutions. IBM uses its global shared services with local service providers for delivering IAM integrations. SailPoint, Okta, Saviynt, Oracle, RSA, ForgeRock, CyberArk, One Identity, Microsoft, and Broadcom are some of its major partners.

IBM supports all major types of engagements from architecture review, design, implementation, testing, MSP support, ongoing maintenance, and strategic consulting. Typical duration of engagement lengths varies from 9 months to long-term and recurring support. IBM does not perform short-term engagements under 9 months. The majority of their IAM consultants and developers are certified and are experienced in integrating and exposing services via APIs such as SOAP, REST, SCIM, LDAP, RADIUS, GraphQL, and AWS SQS. IBM also provides support for all mainstream IDEs and SDKs.

IBM has more than fifty project managers with an average experience of 10 years. All project managers have industry standard certifications. These project managers are instrumental in having a 90 percent success rate in completing projects on time and on budget. IBM offers contract types such as fixed price, billed hours, and ongoing subscriptions to milestone-based payments to provide financial commitments for successful delivery.

IBM supports all mainstream authentication methods. They also support voice-based authentication, hard- and soft- token based HOTP and TOTP. IBM Verify access management platform supports FIDO U2F and 2.0 authenticators. Yubico, Feitian technologies, HID Global, and SoloKeys are examples of FIDO authenticators supported by

IBM. Other advanced services include support for creating reports for major compliance frameworks for auditing purposes. IBM is experienced with all IGA and AG related reports. Additional support is available for orphaned accounts and accounts which need to be deprovisioned. IBM has a dedicated team to create and maintain policies for access control, authentication, GRC, ITDR, and DAG.

IBM provides 24x7 support in all major languages except Russian. Remote service is also available from regional delivery centres. IBM focuses mainly on enterprise level customers having more than 10,000 employees. They also support mid-market organizations. IBM's roadmap includes incorporating generative AI, leveraging integration with IBM X-force cybersecurity monitoring and detection tools. With its global presence, IBM establishes itself as one of the leaders of IAM system integrations.

Security	Strong Positive
Functionality	Strong Positive
Service Delivery	Positive
Integrations	Strong Positive
Serviceability	Strong Positive

Table 9: IBM's rating

Strengths

- Partner ecosystem is very strong with many products operated by certified professionals
- Auditing and reporting capabilities satisfy all major requirements
- Maturity assessment model for IGA, PAM, and access management
- IAM service offering portfolio for workforce IAM and CIAM
- 24x7 support for professional services in almost all regions of Europe and in all major languages
- All other IAM technologies supported for integration

Challenges

- Short-term engagements are usually not encouraged
- Lack of focus on mid-market and medium market segment
- Support for third party ITSM solutions is limited

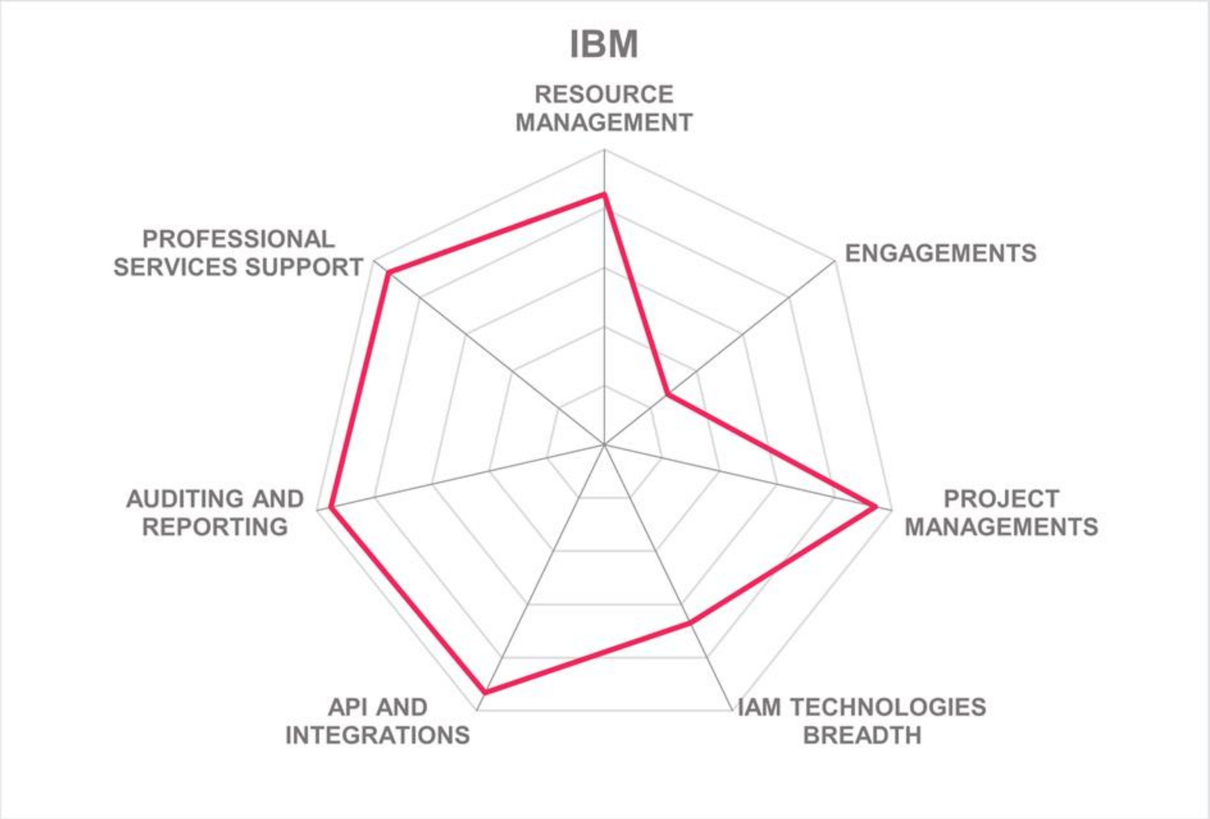
Leader in

OVERALL LEADER

SERVICE LEADER

INNOVATION LEADER

MARKET LEADER



iC Consult

Founded in 1997, globally acting 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, One Identity, SailPoint and extends these towards an integrated solution with consistent user experience and APIs. Headquartered in Munich, Germany, iC Consult has offices across Europe, USA, Canada, India, and China. Most of its customers are from the manufacturing sector with a significant number of customers from finance, insurance, retail, and healthcare. iC Consult covers IGA, PAM, CIAM, and Access Management and all other areas of IAM technology such as ITDR, and Identity First Security.

iC Consult has experience with all mainstream operating systems for deploying and maintaining IAM systems including support for HP-UX OS. iC Consult's experience with application platforms expands beyond all mainstream platforms like Microsoft, Oracle WebLogic, and IBM WebSphere to other platforms like Payara, Glassfish, and WSO2 MSF4J. iC Consult has experience with databases such as Microsoft SQL Server, Oracle, IBM DB2, MongoDB, PostgreSQL and MariaDB for deploying IAM systems. They also support Aurora-DB, DynamoDB, and Neo4J. iC Consult's experience with directory services includes Microsoft Azure Directory, Entra ID, LDAP, Neo4J, and Apache Cassandra. iC Consult is experienced with IAM on IaaS installation within Alibaba, Amazon AWS, Google Cloud, Oracle Cloud, HP Cloud, Rackspace Cloud, Digital Ocean, and Microsoft Azure. They can support integration of customer solutions with third party solutions for all major ITSM solutions. iC Consult can provide integration to any solution if APIs or mail interface is provided. They can also integrate IAM solutions with SIEM solutions.

iC Consult has a strong partner ecosystem with experience in installing and support IAM products using their certified IAM professionals. One Identity, Saviynt, SailPoint, Okta, Ping Identity, Delinea, Oracle, Microsoft, Omada, ForgeRock, EmpowerID, CyberArk, and Broadcom are some of its leading partners for delivering IAM products.

iC Consult supports end-to-end engagements including MSP support, strategic consulting, ongoing maintenance, and customization. iC Consult also resells SaaS, software licenses, and subscriptions. iC Consult mainly supports long-term engagements but can support short-term initial assessment engagements. They support various types of engagement methods including ongoing support with subscription, defined backups, integrators with custom developers and lead consultant with a dedicated team. iC Consult has five hundred certified consultants and developers with experience in all major IAM technologies and coding all major APIs. They do not support IDEs and SDKs for iOS and Android but are experienced with Java, C/C++, .NET, Python, Ruby, and JavaScript.

iC Consult has 117 project managers with an average experience of more than 10 years. Their project managers are certified with industry standard certifications such as PRINCE2, Scrum Master, and SAFe. Most of the projects are completed on time and on budget with exceptions for overruns related to a change of scope. They offer all types of contract variations including fixed price, billed hours, and ongoing subscriptions. They also provide SLA based service fees.

iC Consult Advanced services includes support for all major authentication methods including support for Smartcards and X.509 certificates. They also support all recognized FIDO 2.0 certified authenticators and passkeys. Other types of authenticator support include SAML, OAuth2, OIDC and JWT. iC Consult also supports auditing and forensic capabilities to aid security incident analysis. iC Consult is experienced in developing and customizing reports for major compliance frameworks for FISMA, GDPR, HIPAA, CCPA, NERC CIP, SOX, and PCI DSS. Their team supports all IGA and AG related report types. iC Consult is experienced in creating and maintaining policies for access control, authentication, DAG, GRC and ITDR.

iC Consult provides 24x7 support in English, German, French, Bulgarian, Spanish, and Chinese languages. With a very strong partner eco system and a good strength in certified IAM professionals, iC Consult is one of the leaders when it comes to serving enterprise level customers. Significant support to mid-market segment customers is also available.

Security	Strong Positive
Functionality	Strong Positive
Service Delivery	Strong Positive
Integrations	Strong Positive
Serviceability	Strong Positive

Table 10: iC Consult's rating

Strengths

- Excellent professional service support
- All IAM technologies supported
- IAM Managed Service
- Methodology for end-to-end projects has many detailed milestones
- Most of IAM professionals are certified and working on training and development programs for upcoming IAM engineers
- Partner ecosystem
- Dedicated branch for managed services support for on premises and SaaS

Challenges

- Customers are mainly enterprise level
- Customer in other regions of Europe except DACH is limited but growing in Spain, France, Belgium, and Bulgaria
- Reports for some major compliance frameworks are missing

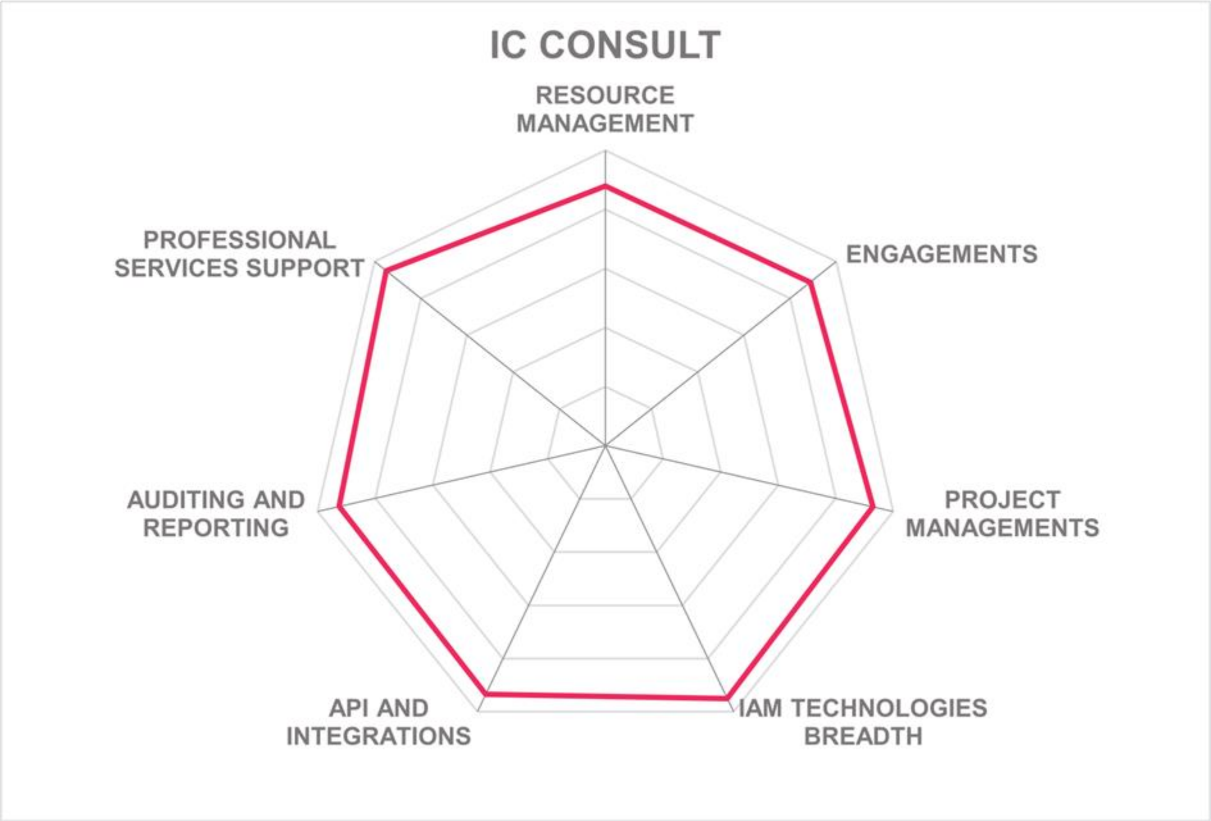
Leader in

OVERALL LEADER

SERVICE LEADER

INNOVATION LEADER

MARKET LEADER



Identity Fusion

Founded in 2013 with headquarters in Tampa, Florida, USA, Identity Fusion has expanded its operations into Europe through its office in London, UK. Main focus areas of Identity Fusion are identity lifecycle management, access control, identity governance, auditing, and reporting, APIs, and service mesh, identity stores and interfaces. Their support for these professional services includes all regions of Europe with most of its clients in the automotive, finance, manufacturing, and technology services. They also support organizations from finance, manufacturing, automotive, and education sectors. Identity Fusion supports all major areas of IAM technologies including PAM. They are mainly focused on identity proofing, verifiable credentials, self-sovereign identity, and identity wallets. They also cover other areas of IAM technologies such as IDaaS, API security, MFA, Risk based authentication and authorization, access governance, and credential and secret management. They do not support DLP, FRIP, CASB, remote user access, and web application firewalls.

Identity Fusion has experience with OSes such as Windows, Ubuntu, Solaris, CentOS, AIX, Amazon Linux, SUSE, Solaris, Debian and RHEL. Identity Fusion’s experience with application platforms includes all mainstream platforms for maintaining and deploying IAM systems. Their support for databases extends to Microsoft SQL server, Oracle Database, PostgreSQL, MySQL, and IBM DB2. LDAP, X.500, and all major user repositories are supported. Identity Fusion’s experience with IaaS Installation of IAM components is limited to Google Cloud platform and Amazon AWS. They do not support Microsoft Azure, Oracle Cloud, or IBM Cloud. They help customers integrate IAM with ITSM solutions such as ServiceNow, Atlassian Jira, BMC Helix, IBM Control Desk, Broadcom, and OpenText Service Management Automation. Identity Fusion teams also have experience in integrating customer solutions with SIEM solutions.

Identity Fusion started with a moderate partner ecosystem in 2020 but now has grown to include major vendors in its ecosystem. Identity Fusion deploys IAM solutions by ForgeRock, Microsoft, Oracle, Ping Identity, OneWelcome, One Login, Okta, ID DataWeb, iProov, Twilio, DUO and Thales. Identity Fusion also partners with integrators such as Accenture, DXC Technology, Capgemini, KPMG, and PwC. Integration to SaaS and legacy applications are supported by Identity Fusion.

Identity Fusion’s engagement support includes all major types from end-to-end processes to individual modules. Their engagement lengths include short-term, long-term, and recurring, depending upon the type of feature implementation. Identity Fusion has fifty certified developers and consultants that are experienced in coding all mainstream APIs. Identity Fusion’s IDE and SDK experience includes iOS, Java, Python, Ruby, and JavaScript. They do not support Android, C/C++, and .NET SDKs.

Identity Fusion has a moderate number of certified project managers with an average experience of five years. Their project managers are certified in industry standard certifications such as Scrum Master, SAFe, and PMP. More than 90 percent of their projects are completed on time and 90 percent of the projects are completed within the allotted budget. They offer contract types from billed hours, fixed price, ongoing subscriptions to block of hours.

Identity Fusion also provides advanced services such as supporting all major types of authentication methods. They also support other authenticators such as AuthFX Authentication broker. FIDO U2F and FIDO 2.0 authenticators such as SIWE (Sign in with Ethereum) and AuthFX with YubiKey are also supported. Identity Fusion also assists with auditing and report creation. Reports for all major compliance frameworks except NERC CIP are supported. They are experienced with all IGA and AG related report types. Identity Fusion's IAM team is also able to support creating and maintaining policies around access control, GRC, ITDR, DAG, and authentication.

Identity Fusion's language support for professional services is limited to English. However, 24x7 support is available based on pre-defined contracts. Remote service is also available for all types of professional services. Identity Fusion provides a dedicated team for each engagement with a well-defined structure of the team and project implementation methodology. With a strong roadmap and global implementations, Identity Fusion is a strong choice for enterprise and mid-market level organizations.

Security	Strong Positive
Functionality	Neutral
Service Delivery	Neutral
Integrations	Strong Positive
Serviceability	Neutral

Table 11: Identity Fusion's rating

Strengths

- Detailed breakdown of capabilities of each major IAM technology
- Step-by-step service offerings for end-to-end project
- Engagements with customers from all industrial sectors
- Detailed project implementation methodology
- Experienced with all major databases, directory services, and application platforms for deploying IAM systems
- Supports reports for major compliance frameworks

Challenges

- Moderate partner ecosystem but many new partner relationships are on the roadmap
- Number of customers is comparatively low
- Support for third party ITSM solutions is limited

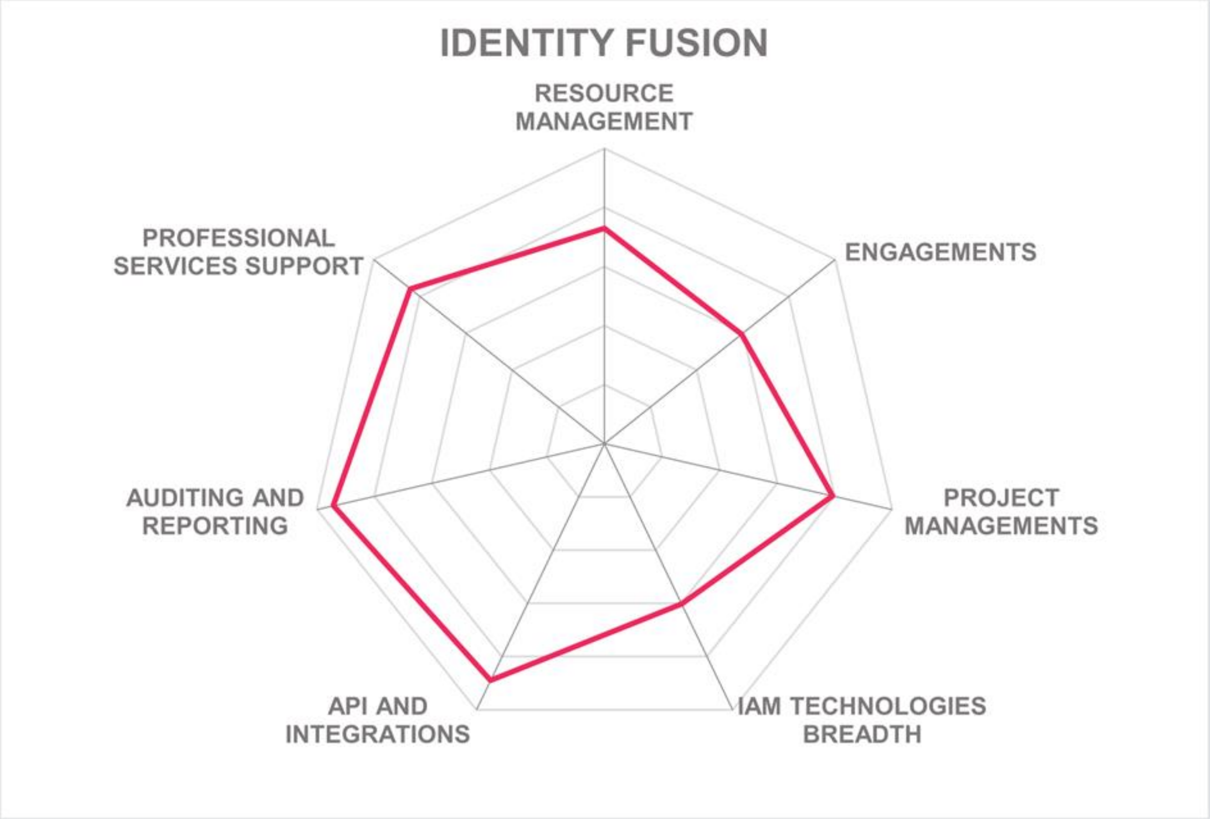
Leader in

OVERALL LEADER

SERVICE LEADER

INNOVATION LEADER

MARKET LEADER



Simeio

Founded in 2007 and based in Atlanta, Georgia (US), Simeio Solutions started as an IAM systems integrator before shifting business into a full-fledged IDaaS service provider over the past few years. Simeio is a privately held company operating from UK for its European business. They have majority of their customers based currently in the UK region. Simeio focuses mainly on clients from the finance, insurance, oil and gas, as well as the manufacturing sectors. Simeio also has clients from other sectors such as retail, healthcare, hospitality, and the public sector. Simeio supports integration for all major IAM technologies such as IGA, CIEM, CIAM, PAM, access management, API management, MFA, authentication, authorization, and web application firewalls amongst others. They do not cover FRIP and network access controls integration.

Simeio has experience with the most common OSes such as CentOS, Windows, Solaris and RHEL. They do not support Ubuntu, Debian, AIX, and SUSE. Simeio’s experience with application platforms includes all mainstream platforms except NGINX. Simeio supports integration with Microsoft SQL server, Oracle database, MySQL, MongoDB, and Maria DB. Simeio is experienced with all major directory services. Support for IaaS installation of IAM components is limited to Amazon AWS, Google Cloud, and Microsoft Azure. Simeio supports all major ITSM solutions for integrating with customer solutions. They also support SIEM integration.

Simeio has a very strong partner ecosystem. Simeio works with IAM solutions by Broadcom, Cisco, CyberArk, Delinea, ForgeRock, HashiCorp, IBM, Microsoft, Okta, One Identity, One Login, Oracle, Ping Identity, RSA, SAP, Saviynt, SailPoint and Thales. Other vendors which are also part of its partner ecosystem are WALLIX, XAYONE, WSO2, Exostar and Beyond Trust.

Simeio supports all engagement types and provides end-to-end processes for transforming IAM deployments. Simeio can also take over existing projects delayed due to other vendors and fulfil the deployments. Simeio support both short-term and long-term engagements. They also support recurring engagements which last for multiple years. Simeio has 70 percent of its consultants and developers certified by product vendors. They support coding of APIs for moderate number of mainstream API protocols such as REST, JSON-RPC, SCIM, LDAP, Webhooks, Java, and UDP/TCP Socket API protocols. They support IDE and SDK types for Android, iOS, Java, C+/C++, .NET, python, JavaScript, Go, and Ruby.

Simeio has fifty project managers with an average experience of 10 years. This helps to achieve 98 percent of projects completed on time and on budget. Simeio provides projects with multiple types of contracts depending on requirements. Simeio also provides cost overrun guarantees.

Simeio supports advanced services such as support for all major authentication methods including support for FIDO, SAML, OAuth, JWT and OIDC federations. Simeio provides auditing and forensic capabilities for security incident analysis. They can create reports for IGA, AG, and all major compliance frameworks. Simeio also supports policy management for access controls, authentication, GRC, ITDR, and DAG.

Simeio provides 24x7 support services in English, Spanish, German, and French languages. Simeio has employees based around the world and provides 24x7 services through its four identity intelligence centres. Simeio places itself as a strong contender for organizations in the mid-market segment with a growing portfolio of enterprise and medium level organizations.

Security	Strong Positive
Functionality	Positive
Service Delivery	Neutral
Integrations	Strong Positive
Serviceability	Positive

Table 12: Simeio's rating

Strengths

- Expertise in providing services to mid-market segment
- Expertise in all IAM technologies
- Hosting services are also provided
- Large partner ecosystem
- Dedicated team for developing and maintaining policies
- Auditing and reporting capabilities
- Support for all third-party integrations with customer solutions
- Fast track implementation timeline
- 24x7 support for professional services

Challenges

- Enterprise level customers are very limited
- Focus is only on UK market in the EMEA region
- Professional services support is not available in all parts of Europe

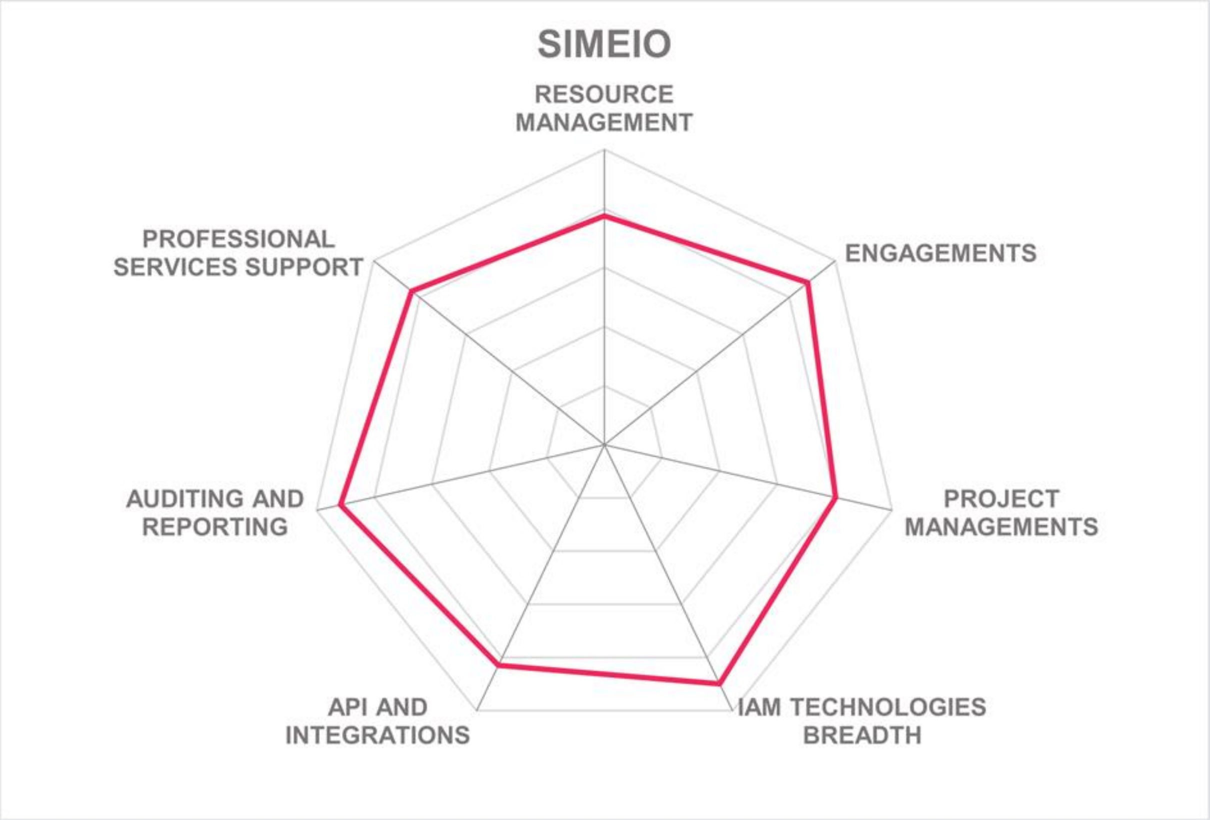
Leader in

OVERALL LEADER

SERVICE LEADER

INNOVATION LEADER

MARKET LEADER


SIMEIO
RESOURCE MANAGEMENT
ENGAGEMENTS
PROJECT MANAGEMENTS
IAM TECHNOLOGIES BREADTH
API AND INTEGRATIONS
AUDITING AND REPORTING
PROFESSIONAL SERVICES SUPPORT

SmartWave SA

Founded in 2001, SmartWave is a Swiss software solutions integrator with its headquarters based in Geneva, Switzerland. SmartWave focuses on customers primarily in the French-speaking Switzerland region but participates also to key projects in other Switzerland regions. SmartWave works with customers from all kinds of industries including finance, manufacturing, healthcare, pharmaceutical, government, insurance, big organizations as well as oil and gas. SmartWave is leveraging API Management, Low Code, Cloud & DevOps and IAM along with strong capabilities in all major types of IAM technologies such as IGA, PAM, and CIAM as well as other areas of IAM technologies including multi-factor authentication (MFA), Digital Signature, API Management, Application Security, Decentralized Identity, and Web Application Firewalls.

SmartWave is experienced with all major operating systems such as Microsoft, Ubuntu, Solaris, SUSE as well as Alpine for containers. SmartWave's experience with application platforms is limited to Microsoft, Apache Tomcat, Red Hat JBoss, Oracle WebLogic, embedded Quarkus, and embedded Jetty. SmartWave has experience with a moderate number of databases such as Microsoft SQL server, Oracle database, PostgreSQL and MariaDB. They support all major directories. OneLogin LDAP service is also supported. SmartWave supports IaaS installation of IAM components for Amazon AWS and Microsoft Azure. SmartWave can also integrate customer solutions with third party ITSM solutions such as ServiceNow, Atlassian JIRA, Ivanti service manager, and EasyVista. They do not support integrating IAM solutions with SIEM solutions.

SmartWave has a moderately strong partner ecosystem among product vendors. Its major partners include ForgeRock, OneLogin, One Identity, RedHat, and WSO2. Other partners from its ecosystem are Microsoft, Saviynt, Keycloak, Netwrix, FreeIPA, LemonLDAP, Radiant Logic, Optimal IdM, HashiCorp, Swisscom, SwissSign and HID Global.

SmartWave supports all engagement types including audit, assessments, end-to-end processes from architecture design, implementation, migration, maintenance, customization, and application integration. SmartWave does not provide MSP support. Their majority of engagement lengths are recurring, but short-term engagements are also accepted. SmartWave has twelve certified consultants and developers a majority of which have extensive experience with coding to all mainstream APIs and API management platforms. SmartWave's supports development for Android, iOS, Java, C+/C++, .NET, and Python. They also support PowerShell, groovy, and bash.

SmartWave supports all engagement types including audit, assessments, end-to-end processes from architecture design, implementation, migration, maintenance, customization, and application integration. SmartWave does not provide MSP support. Their majority of engagement lengths are recurring, but short-term engagements are also accepted. SmartWave has twelve certified consultants and developers a majority of which have extensive experience with coding to all mainstream APIs and API management platforms. SmartWave's supports development for Android, iOS, Java, C+/C++, .NET, and Python. They also support PowerShell, groovy, and bash.

SmartWave has project managers with an average experience of over 10 years. Their project managers are certified in PRINCE2 and Hermes. Sixty-five percent of their projects are completed on time and on budget. Contract types offered for IAM projects consist of fixed price and billed hours to meet their clients' requirements and can resell solutions licenses providing them a partnership relationship.

SmartWave provides advanced services including authentication supported for all major authenticators. In addition, they support Matrix cards and X509 certificates. SmartWave is experienced with FIDO authenticators such as YubiKey, Apple passkey, and phone biometrics. SmartWave does not provide auditing capabilities and support for compliance framework reporting is limited to GDPR. They support most of the IGA and AG related reports but support for KRIs, "users with emergency access," rehires, and attestation related reports are not given. SmartWave's team is experienced in creating and maintaining policies related to access control, authentication, and GRC. They do not support DAG and ITDR.

SmartWave provides professional support services in only English and French languages. 24x7 support is missing but remote services are available via ticket-based, remote control, phone, or email. Their strategy includes both on-premises implementation projects as well and cloud implementation projects and SaaS solutions deployment depending on clients' specifications and constraints. Their roadmap includes passwordless only for on-premises systems, electronic signature of identity proofing and migrating applications from on-premises to other systems. SmartWave currently focuses on mid-market level organizations. With a good number of projects delivered every year and a short duration for building and running applications, SmartWave is a promising company to keep an eye on.

Security	Positive
Functionality	Neutral
Service Delivery	Weak
Integrations	Neutral
Serviceability	Neutral

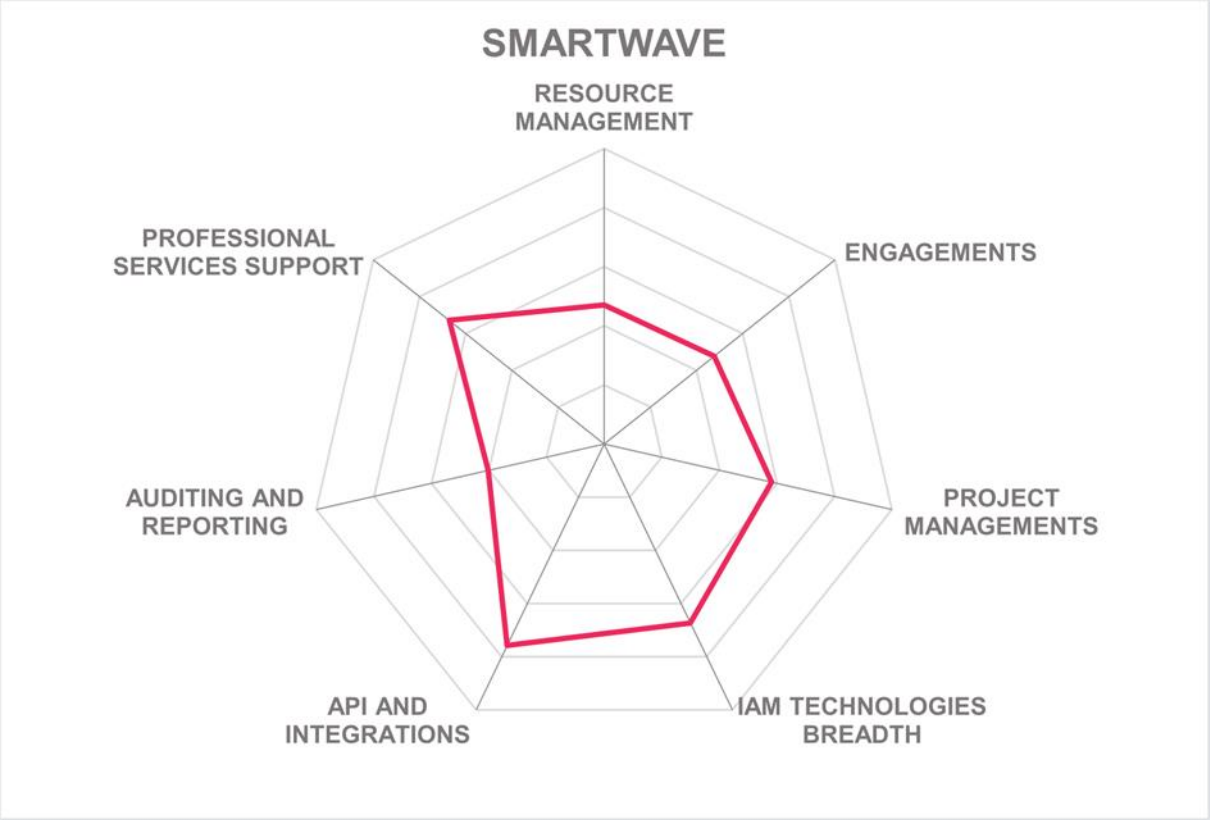
Table 13: SmartWave SA's rating

Strengths

- Support for all major API types
- Covers all major IAM technologies
- Experienced in all major operating systems and application platforms for deploying and maintaining IAM systems
- Full stack support for end-to-end projects
- Covers all types of engagements
- Proximity to Swiss companies

Challenges

- Lack of presence in other regions of Europe except Switzerland
- 24x7 support services not available
- Relatively moderate but growing partner ecosystem
- Weak auditing and reporting capabilities



Traxion

Based in Benelux and founded in 2000, Traxion is a part of a Swiss IT Security (SITS) group which is owned by Triton group fund V. Traxion supports organizations from manufacturing, utilities, finance, chemical, government, education as well as travel and hospitality sectors. Other sectors in which Traxion has customers are retail, insurance, and health care as well as aerospace and defence. Traxion currently has experience of working in Benelux, UK, Nordics and the DACH regions of Europe. Traxion provides support for all major IAM technologies such as IGA, AM, PAM as well as including enterprise key management and certificate lifecycle management. Traxion themselves do not support ITDR, CASB, FRIP, or web application firewalls although this is covered by sister companies in the SITS-group.

Traxion has experience with OSes such as Windows, Ubuntu, SUSE, RHEL and Debian. They do not support AIX, CentOS, and Solaris. Traxion’s experience with application platforms includes all major platforms except Oracle WebLogic and IBM WebSphere. Traxion has experience with deploying and maintaining databases such as Microsoft SQL server, Oracle database, IBM DB2, MySQL, Mongo DB, and MariaDB. They are experienced with all directory services including LDAP directory services. Traxion’s support for IaaS installation of IAM components is limited to Amazon AWS, Google Cloud, and Microsoft Azure. Traxion uses its application onboarding service to integrate customer solutions with any third-party ITSM solution with an interface. They also support SIEM integration using Syslog, customer connectors, and agents.

Traxion’s certified product vendor partner ecosystem includes Thales, Saviynt, SailPoint, Omada, Okta, Ping Identity, Microsoft, CyberArk, Delinea, and Keyfactor. Entrust, Beyond Trust, Nexus, and RSA complete its partner ecosystem. Traxion uses their own maturity matrix for analysing customer IAM maturity when approaching projects. They have a dedicated department for doing legacy application integrations in the various IAM services delivered.

Traxion provides support for all mainstream engagement types. They support role mining, role-based access controls, business advisory and product selections. Traxion have both long-term and short-term engagements. Their 150 certified consultants and developers are experienced in coding to all major API protocols. Traxion provides IDE and SDK support for Java, C+/C++, .NET, PowerShell, JavaScript, and Python. They do not support Android and iOS SDKs.

Traxion uses service owners and product owners instead of project managers to fulfil deliveries. Their product managers have an average experience of more than 10 years and are certified as scrum masters and agile certified product owners. They report that all their projects are completed within the allocated budget and around 80 percent of projects are completed on time. Most of the projects undertaken are long-running projects. Traxion offers contract types ranging from fixed price and time and material offers, to managed service offerings and subscription models.

Traxion supported other services including support for all major authentication methods including FIDO 2.0 authenticators. They support auditing capabilities for major compliance frameworks such as GDPR, HIPAA, SOX, PCI-DSS, NIST SP 800-53, NIS2, ISO 27001, SURF, BIO, and NEN 5710. Traxion supports most of the IGA and AG related reports Traxion teams also have experience in customizing dashboards of identities and access events.

Traxion provides 24x7 services as a part of managed IAM services in English, German, French, and Dutch. Roadmap includes providing managed security solutions and services.

Security	Strong Positive
Functionality	Positive
Service Delivery	Neutral
Integrations	Strong Positive
Serviceability	Positive

Table 14: Traxion's rating

Strengths

- Decent support for all IAM technologies
- Capabilities for integrating with third-party solutions
- Support for coding all mainstream API protocols
- Equal focus on mid-market and enterprise level customers
- 24x7 support for professional services is available
- Support for all auditing and reporting criteria
- Experience in creating and maintaining policies

Challenges

- Focused mainly on the Benelux region
- Moderate sized partner ecosystem
- Experience in supporting some application platforms for deploying and maintaining IAM systems is missing

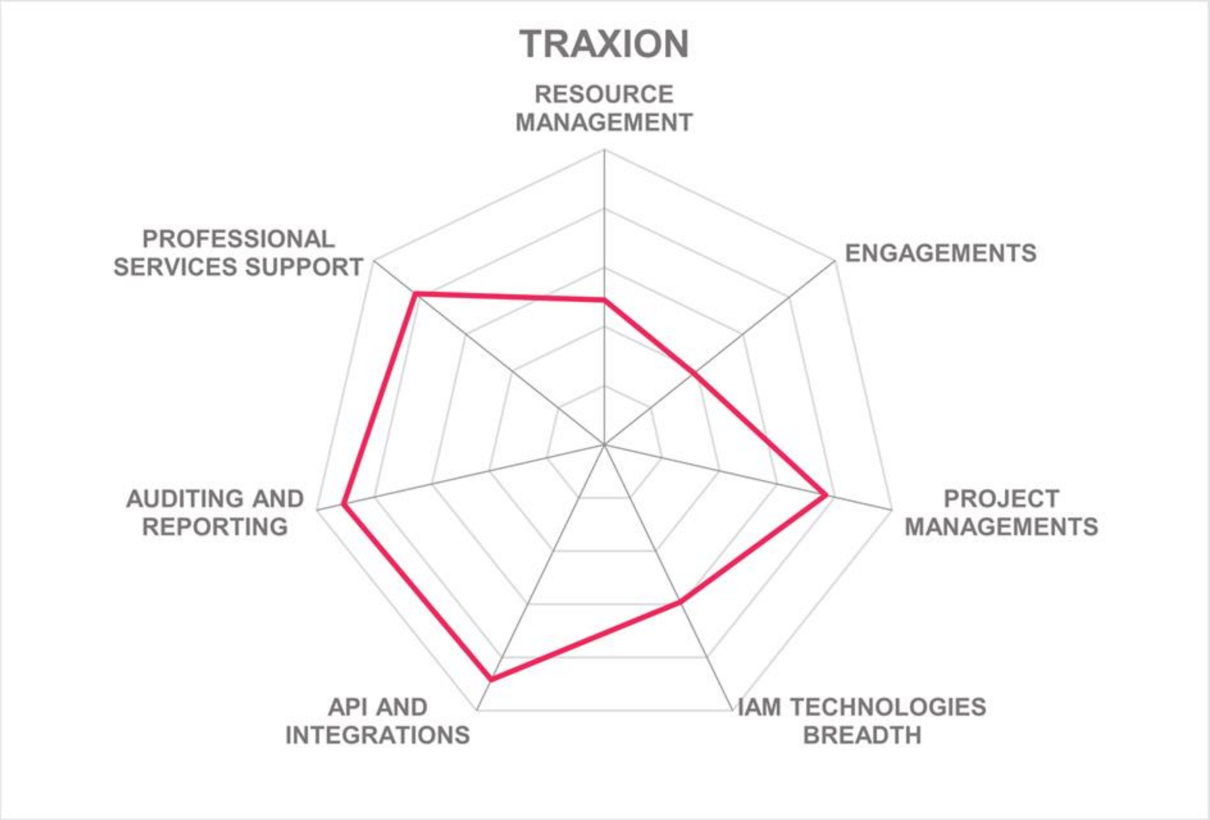
Leader in

OVERALL LEADER

SERVICE LEADER

INNOVATION LEADER

MARKET LEADER


TRAXION
RESOURCE MANAGEMENT
ENGAGEMENTS
PROJECT MANAGEMENTS
IAM TECHNOLOGIES BREADTH
API AND INTEGRATIONS
AUDITING AND REPORTING
PROFESSIONAL SERVICES SUPPORT

Trevonix

Founded in 2019 with headquarters in London, England, Trevonix is an identity and access management company focusing on delivering mainly access management projects. With the merger and acquisition with Identity Methods in early 2023, Trevonix has further reinforced its offerings and filled gaps which were earlier missing. Trevonix has experience of delivering projects to customers mainly in the UK, DACH and Nordics region. Around half of Trevonix customers are based in the finance sector, with the rest being made up of retail, manufacturing, healthcare, utilities, and pharmaceuticals. Trevonix specializes in integrating access management solutions but can also support other areas of IAM technologies such as CIAM, IGA, PAM, web access management, API security, MFA, endpoint security, remote user access, among others. They do not support web application firewalls, DLP and network access controls integration.

Trevonix is experienced with all major operating systems, databases, application platforms and directory services for deploying and maintaining IAM systems. Trevonix supports IaaS installation of IAM components for Amazon AWS, Google Cloud, Microsoft Azure, Oracle Cloud, and IBM Cloud. Trevonix's support for ITSM integration with customers solutions includes ServiceNow, Atlassian JIRA, Ivanti Service Manager, ManageEngine ServiceDesk Plus, OpenText, and Alemba Service Manager. They are experienced in providing integration with SIEM solutions for Splunk integration using Syslog API and custom data format.

Trevonix has a strong vendor partner ecosystem. They are delivery partners of Saviynt and ForgeRock and are an advanced delivery partner of Ping Identity. Trevonix is a gold delivery partner of Okta. Trevonix is also a product certified partner of One Login/ One Identity, CyberRes by OpenText, Transmit Security, Microsoft, Keyless, IDEE, and Cloudentity. Other partners in its ecosystem include Beyond Identity, Beyond Trust, CyberArk, IBM, HYPR, RSA, SailPoint, Thales, WSO2, and Senhasegura.

Trevonix supports multiple engagement types. Their core focus is providing services around consulting, professional services, managed services, and program delivery. They provide ad-hoc support, OWASP coverage, customization, and RFI and RFP projects. Trevonix's main share of engagements is focused on the UK's finance sector. The main type of engagement supported is professional services. Their typical length of engagements ranges from short-term to long-term and recurring. Trevonix has forty certified developers and consultants all with experience in coding all mainstream APIs. They support all IDEs and SDKs.

Trevonix has project managers certified in PRINCE2, PMP, SCM, SAFE and Scrum with an average experience of 10 years. Most of their projects are completed on time and over 90 percent of projects are completed on budget. Trevonix can complete end-to-end projects within 6 to 12 months based on requirements. They offer contract types based on fixed price, billed hours, and ongoing subscriptions. Trevonix also provides cost overrun guarantees.

Trevonix supports advanced services for authentication and compliance reporting. They support all major methods of authentication including FIDO 2.0 such as Yubico YubiKey 5. Trevonix also supports SAML, OAuth2, JWT, and OIDC authentication and federation. Trevonix supports auditing and forensic capabilities for security incident analysis. Their support for developing and customizing reports for major compliance frameworks is available for HIPAA, NERC-CIP, NIST SP 800-53, GDPR, PCI-DSS, and SOX. Trevonix supports development of many IGA report types and support for creating policies is available for access controls, DAG, ITDR, GRC and authentication.

Trevonix is experienced in providing services to medium level organizations. Forty percent of their engagements are aimed at enterprise level organizations with a further equal split between medium and mid-market companies. Professional services support is only available in English and German language and 24x7 support is now available. Trevonix follows a low code / no code approach for implementation and can provide remote services through its locations in UK and India. Their plan is to expand their customer base in Western Europe, Middle East, APAC, and North America by 2024. The roadmap includes plans to increase focus on IGA and PAM offerings and their US entity to create a global offering. Trevonix places itself as a promising vendor in the IAM integrator space focused on medium level organizations but aims to accommodate enterprise organizations in the future.

Security	Strong Positive
Functionality	Positive
Service Delivery	Neutral
Integrations	Neutral
Serviceability	Positive

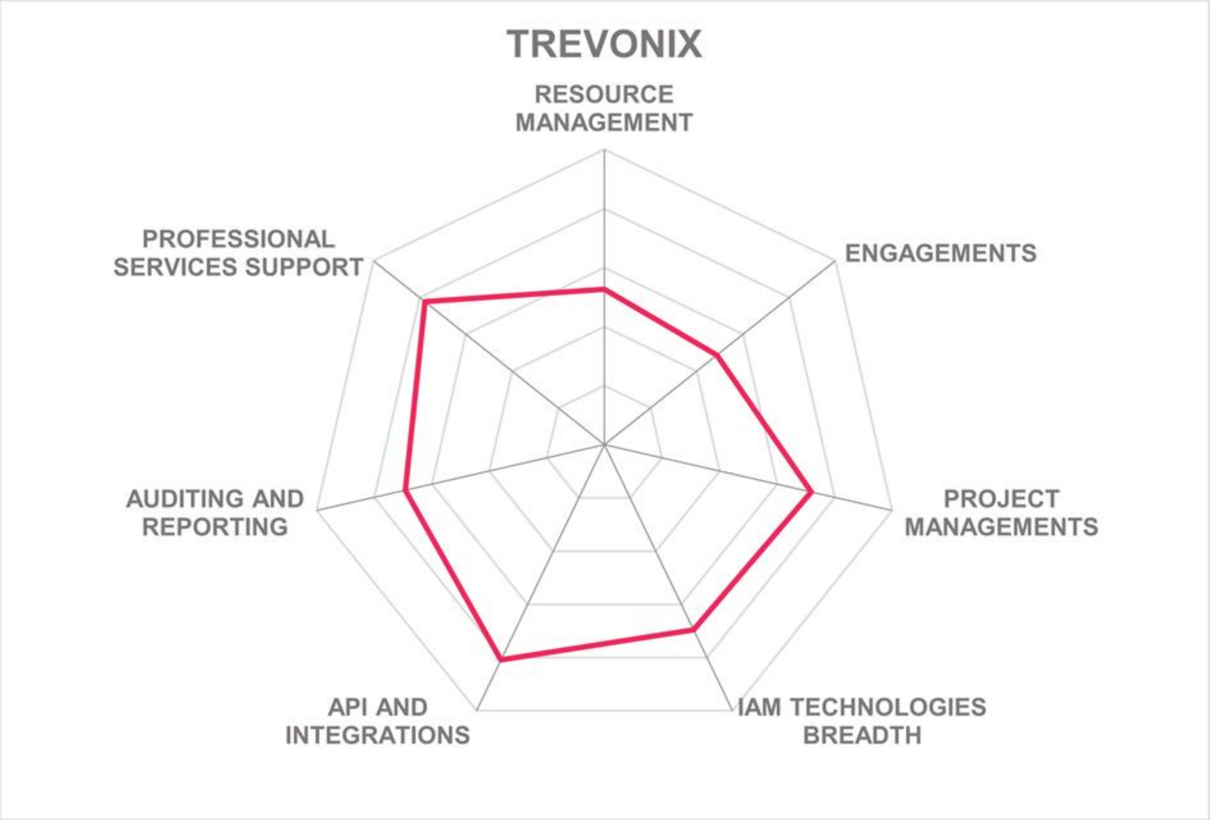
Table 15: Trevonix's rating

Strengths

- Support for access management deployments
- Very quick implementation of end-to-end projects
- Experience with all major OSes, databases, application platforms, and databases for deploying and maintaining IAM systems
- Support for coding all major API protocols
- Good partner ecosystem
- All engagement methods and types supported

Challenges

- Support for integration with third party ITSM solutions is limited but growing
- Support for major compliance frameworks reports is still missing for some protocols
- Presence outside UK is limited


TREVONIX
RESOURCE MANAGEMENT
ENGAGEMENTS
PROJECT MANAGEMENTS
IAM TECHNOLOGIES BREADTH
API AND INTEGRATIONS
AUDITING AND REPORTING
PROFESSIONAL SERVICES SUPPORT

Wavestone

Wavestone is a French management consulting company with its headquarters near Paris, France. Founded in 1990, Wavestone has business across nine countries. They have around 75 percent of their customers based in France while the remaining are in UK, DACH, and Benelux. Wavestone is focused on organizations in the finance sector, but also has customers in retail, manufacturing, energy, and utilities, public sector, as well as travel and hospitality. Wavestone supports end-to-end projects for all areas of IAM with focus on IGA, CIAM, and access management. Their support for projects related to PAM are limited to design and implementation. Wavestone covers other areas of IAM technologies including CIEM, MFA, CASB, DLP, endpoint security, WAM, API security and management and decentralized identity. Wavestone is also involved in sovereign identity projects.

Wavestone is experienced with all mainstream OSes for deploying and maintaining IAM systems. They support all available application platforms except IBM WebSphere. Wavestone prioritizes protocols which are currently in production and not outdated. Wavestone is experienced with databases including Oracle database, Microsoft SQL server, MySQL, PostgreSQL, and Maria DB. Wavestone is experienced with all major directory services. They support IaaS installation of IAM components only for Amazon AWS and Microsoft Azure. Wavestone's support for integration of customer solutions with ITSM solutions is available only for ServiceNow, EasyVista, and GLPI. They support integration with SIEM solutions through a different project where consultation and integration are provided.

Wavestone maintains technical partnerships with product vendors. Their main vendor partners are SailPoint, Saviynt, SAP, Ping Identity, Okta, One Identity, Microsoft, ForgeRock, EmpowerID, and Transmit Security. Wavestone has product certified IAM professionals and a dedicated IAM team for each project to conduct the end-to-end processes. Wavestone can also take over incomplete projects and deliver after maturity assessments.

Wavestone has expertise in providing engagements for IGA and access management. They support end-to-end engagements including deployment and implementation. Architecture review, design, and strategic consulting have a majority share in overall engagements supported. They do not provide MSP support and ongoing maintenance, but they do help customers upgrade and evolve their solutions as needed. Other types of engagements supported are governance, Target Operating Model, and optimization. They support both short-term and long-term engagements; however, most of their engagements are between 3 to 6 months. RFP and RFI engagements are also available depending on client requirements. Wavestone has twenty certified consultants. Their developers are experienced in coding REST, SOAP, SCIM, LDAP, and Java APIs. These IAM professionals can also support IDEs and SDK for Android, iOS, Java, C+/C++, .NET, Python, and JavaScript.

Wavestone has fifty project managers at its cybersecurity division in France with an average experience of more than 15 years, however it is unknown how many of these professionals are certified. Eighty percent of projects are completed on time and on budget. They provide contracts such as time and materials and fixed price for labor.

Wavestone also provides advanced services around role mining, rule mining, and strong self-service support using all major authenticators. They support other authenticators and federation standards including smartcards, JWT, OAuth2, SAML, and OIDC. Wavestone also supports capabilities for compliance, auditing, reporting, and security incident analysis. They have a dedicated team for penetration testing and auditing capabilities for the identity topic. Their support for reports for major compliance frameworks is limited to GDPR, PCI-DSS, SOX, and NIST SP 800-53. Other frameworks supported are DORA for recertification purposes and PSD2 and JSOX. The Wavestone team is experienced in creating and maintaining policies around access controls, authentication, DAG, and GRC.

Wavestone supports professional services in English and French languages in Europe. Remote service is available but 24x7 support are not available. Wavestone focuses on providing support to enterprise level customers, however they do have several mid-market customers. Their roadmap includes collaborating with European consulting firm Q_PERIOR with a view to expanding business in Europe, especially France, DACH, and UK regions. Wavestone with its expertise in various domains is a strong candidate for enterprise level organization’s integration requirements.

Security	Strong Positive
Functionality	Positive
Service Delivery	Neutral
Integrations	Positive
Serviceability	Neutral

Table 16: Wavestone’s rating

Strengths

- Support for all IAM technologies
- Expertise in all industries and domains
- Three step process for implementing end-to-end projects
- Expertise in IGA deployments
- Partner ecosystem
- Well defined IAM assessment framework
- Support for advanced services such as authentication methods
- All IGA and AG related reports can be developed
- Impartial towards software vendor recommendations as they do not form business partnerships with them
- Support for innovative AI features

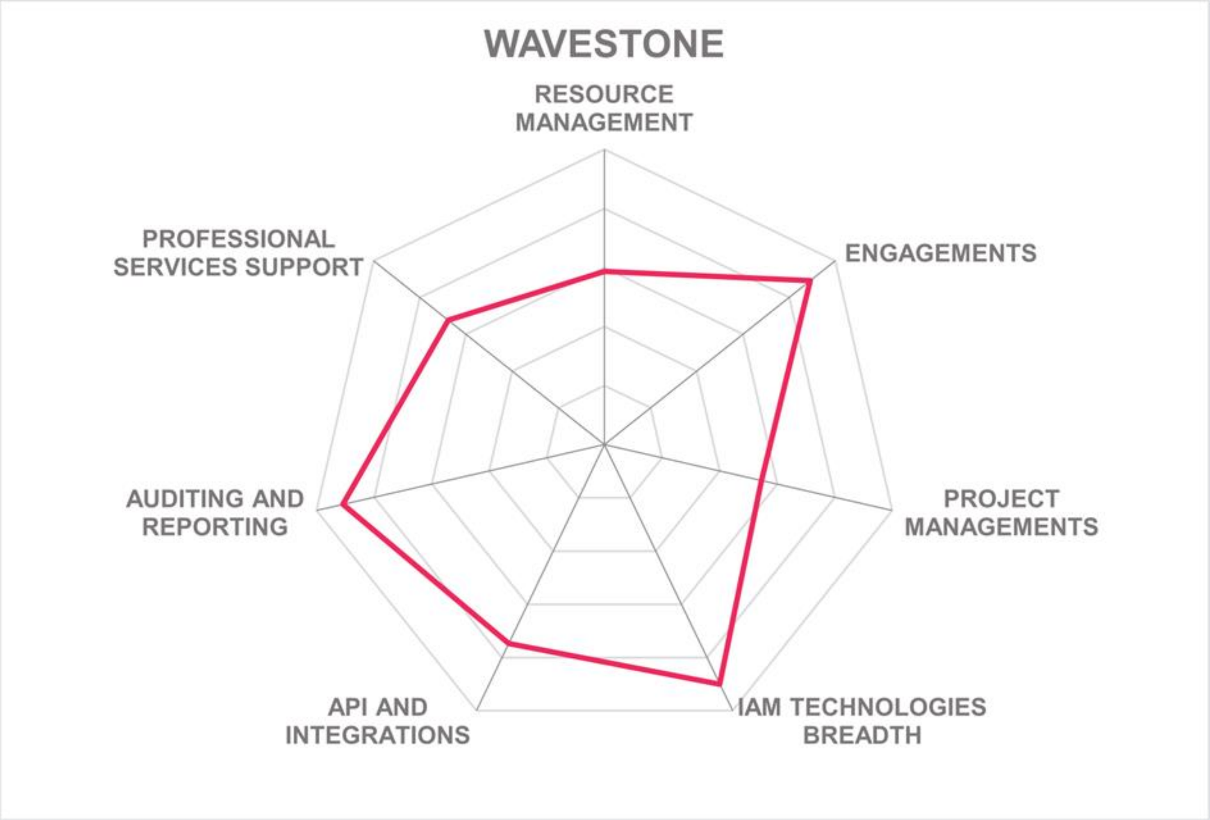
Challenges

- Focus on mid-market and medium level organizations missing
- Small presence outside Southern Europe

- Limited support for integration to third party solutions

Leader in

OVERALL LEADER SERVICE LEADER INNOVATION LEADER MARKET LEADER



Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other vendors in the market that readers should be aware of. These vendors do not fully fit the market definition but offer a significant contribution to the market space. This may be for their supportive capabilities to the solutions reviewed in this document, for their unique methods of addressing the challenges of this segment or may be a fast-growing startup that may be a strong competitor in the future.

Atos

Atos is one of the largest IT consultancies and has with the DirX portfolio and the Evidian products as own product offerings. DirX, under the Atos brand, provides a comprehensive set of IAM capabilities targeted at complex, large-scale environments.

Why worth watching: Atos DirX solutions are proven in their support for complex, large-scale environments and cover both IGA and Access Management capabilities.

Bechtle

Bechtle is a leading European IT reseller and IT service provider, headquartered in Germany and being present in various European countries. Amongst other areas, Bechtle offers IAM system integration and Managed Security Services.

Why worth watching: Large IAM Service Provider with strong regional presence, focused on medium-sized and mid-market organizations.

CGI

CGI is a global IT and Business Consulting and System Integration provider, covering a wide range of areas, including cybersecurity, with IAM being a part of their portfolio.

Why worth watching: Global IT and Business consultancy which can be of interest when IAM / Digital Identity is a central element in transformational projects.

Cognizant

Cognizant is a global company providing business and technology services. They have expertise in cloud deployments, ERP implementations and deep industry practices. Cognizant has more than fifty delivery centers around the world.

Why worth watching: Cognizant has a global presence and can delivery IAM projects using regional, local, and global approach.

Computacenter

Computacenter is a UK-based IT services company covering a wide range of different areas, including IAM. Their IAM practice is established and holds partnerships with a range of IAM and IDaaS providers.

Why worth watching: Experienced and proven IAM practice as part of a large IT services company.

Deloitte

Deloitte is a multinational professional services network known for providing a wide range of services, including audit, tax, consulting, and advisory services to clients across various industries. Deloitte helps to optimize clients'' IT infrastructure, implementing enterprise solutions, and navigating digital transformations.

Why worth watching: Deloitte is a strong candidate for enterprise level organizations for providing system integration capabilities.

Devoteam

Devoteam is a French IT service provider being active in many countries in Europe, Middle East, and Africa. They are partner of various IAM software and IDaaS providers and have a proven IAM practice in several countries.

Why worth watching: Experienced IAM system integrator with presence in many countries in EMEA.

Ernst & Young (EY)

EY has a strong expertise in audit, tax, consulting, and advisory services. They provide full support for strategy, roadmap, vendor selection and project management. Solution architecture and design is also provided.

Why worth watching: EY has a global presence and places itself as a system integrator of choice for companies of enterprise level volume.

Xalient

Xalient has acquired Grabowsky just ahead of publication of this Leadership Compass. Grabowsky operates strongly in the Benelux region. They have strong relationships with leading technology partners for delivering IAM solutions.

Why worth watching: Xalient will now be a strong player in the Benelux region with the acquisition of Grabowsky with vast experience and expertise in providing digital identity strategies.

HCL Technologies

HCL Technologies counts amongst the largest IT service providers globally, with operations in most countries across the globe. They are partner of several IAM specialists such as BeyondTrust, CyberArk, IBM, Saviynt, and SailPoint.

Why wort watching: Experienced provider of IAM services with several established partnerships, able to act on global scale.

ID North

As a part of the Allurity group, ID North operates in the Nordics region. ID North is experienced to tackle all kind of engagements such as consulting, implementation, managed services and technical support. They also support outsourcing identity security and solutions to handle authentication, access control and identity monitoring.

Why worth watching: ID North supports integration services with well-defined service packages depending on business needs.

Infosys

Infosys has its own Microsoft Cloud Business Unit offering that provides an integrated approach across infrastructure, application, and data on the cloud.

Why worth watching: Infosys is a good recommendation for enterprises looking for an end-to-end engagement on Azure.

Intragen

Intragen was founded in 2006 and has its headquarters in London, England. Intragen focuses on delivering IAM solutions, business consultancy, auditing, infrastructure, and security. They cover major areas of IAM technology such as IGA, PAM, CIAM, access management, identity federation, and full IAM suites.

Why worth watching: Intragen places itself as a good candidate for mid-market level organizations for delivering IAM services.

IPG

IPG support IAM integration services from design to implementation. They have experience in undertaking projects related to identity governance, identity management, provisioning, and access management.

Why worth watching: IPG has experience of over 20 years managing more than one thousand projects with a strong partner ecosystem.

ITConcepts

Experienced IT service provider and system integrator with a strong IAM focus. Strong experience with a range of products and services. Established partnerships with several companies, including One Identity.

Why worth watching: Experienced IAM system integrator with focus on Germany, Switzerland, and a partnership in the U.S.

KOGIT

KOGIT operates as an independent consulting firm specializing in intelligent analysis, reporting and audit. They partner vendors include major product vendors.

Why worth watching: KOGIT has strong partner relationships and a Europe-wide network.

KPMG

KPMG has strong extensive expertise in audit, tax, and advisory services. KPMG focuses on designing and implementing solutions for an end-to-end process.

Why worth watching: KPMG has a global presence and expertise in industry insights to meet tailor made requirements of customers.

Nixu Corporation

Nixu is a cybersecurity services specialist headquartered in Finland. They have offices in Finland, the Netherlands, Sweden, and Denmark, and are positioned as a provider of leading-edge innovation in IAM.

Why worth watching: Innovative solutions for digital identities as part of digital services, various established partnerships.

Optiv

Global provider of IAM and cybersecurity services. Deliver both system integration and managed services across the full range of cybersecurity and IAM. Various technology partnerships. European presence, but stronger focus on the U.S. market.

Why worth watching: Experienced service provider with presence in major regions across the globe, specialized on cybersecurity and IAM.

Protiviti

Global IT consultancy, covering all major areas of IT. Their cybersecurity practice also includes Digital Identity services for IAM. They have a range of partnerships with established vendors of IAM software and IDaaS services.

Why worth watching: Global IT consultancy with experience in a wide range of topics, including IAM, capable of service digital identity needs in digital transformation projects.

PwC

Founded in 1998 with headquarters in London, England, Price Waterhouse Coopers (PwC) is one of the leading consulting and advisory firms with a global presence. PwC can execute strategies for diversifying from pure services to include a combination of products, platforms, tech-enabled and managed services.

Why worth watching: With its global presence and regional approach, PwC is a strong candidate and integrator of choice for enterprise level organizations.

SECURIX

SECURIX is a Swiss IAM system integrator with focus of its business activities on the integration and operation of software and cloud solutions. Their offering focuses on the areas of IGA, PAM CIAM and SIEM. They also provided managed services for maintaining integrated systems.

Why worth watching: SECURIX has a strong presence and expertise in the DACH region with expertise in managed services.

Swiss IT Security Group

Swiss-based IT Security service provider and system integrator with operations in various countries, after having acquired several other companies. Proven IAM services with several partnerships.

Why worth watching: Experienced provider of IAM system integration services in different regions and for different products and services.

TIMETOACT Group

DACH / GSA focused provider of IT services, including a strong IAM practice, but also covering a range of other areas. Strong presence in both Germany and Switzerland with experienced teams in the field of IAM.

Why worth watching: Experienced IAM system integrator, but part of a larger group that can add other types of services beyond IAM.

Wipro

Wipro counts amongst the largest IT services companies globally, with operations in many countries, including various European countries. They cover the full range of IT services, including IAM.

Why worth watching: Global IT services provider, also supporting IAM services and operations.

Methodology

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report does not provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e., a complete assessment.

Types of Leadership

We look at four types of leaders:

- Service Leaders: Service Leaders identify the leading-edge services in the particular market. These services deliver most of the capabilities we expect from integrators in that market segment. They are mature.
- Market Leaders: Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack of global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- Innovation Leaders: Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- Overall Leaders: Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas, but they become Overall Leaders by being above average in all areas.

For every area, we distinguish between three levels of products:

- Leaders: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- Challengers: This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- Followers: This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and extensive experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

Service rating

KuppingerCole Analysts AG as an analyst company regularly evaluates products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of services requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Service Delivery
- Integrations
- Serviceability

Security is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and the way the vendor deals with them.

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

Service Delivery is measured by how easy or difficult it is to deploy, deliver and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Integrations refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product/ service to support programmatic access through a well-documented and secure set of APIs.

Serviceability is a measure of how easy the product / service is to use and to administer. We look for services that are logically and intuitive as well as a high degree of consistency across projects across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, integrations, and serviceability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Integrations, and Serviceability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly, and ineffective IT infrastructure.

Vendor rating

We also rate vendors on the following characteristics:

- Innovativeness
- Market position
- Financial strength
- Ecosystem

Innovativeness is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors because innovative vendors are more likely to remain leading-edge. Vendors must support technical standardization initiatives. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active. Therefore, being weak in one segment does not lead to a very low overall rating. This factor considers the vendor's presence in major markets.

Financial strength even while KuppingerCole does not consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

Rating scale for services and vendors

For vendors and service feature areas, we use a separate rating with five different levels, beyond the Leadership rating in the various categories. These levels are

Strong positive

Outstanding support for the subject area, e.g. product functionality, or outstanding position of the company for financial stability.

Positive

Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

Neutral

Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren’t met, while others are well served. For Market Position, it could indicate a regional-only presence.

Weak

Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.

Critical

Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is European coverage, including vendors which are only active in regional markets of Europe.

However, there might be vendors which do not appear in a Leadership Compass document due to various reasons:

- Limited market visibility: There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- Declined to participate: Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.
- Lack of information supply: Products of vendors which don’t provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- Borderline classification: Some products might have only a small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is providing a comprehensive view of the services in a market segment. KuppingerCole will provide regular updates on their Leadership Compass documents.

We provide a quick overview about vendors not covered and their offerings in chapter Vendors to Watch. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

Related Research

Leadership Compass: CIAM Platforms

Leadership Compass: Access Governance

Leadership Compass: Privileged Access Management

Leadership Compass: IGA (Identity Governance& Administration)

Leadership Compass: Access Management

Leadership Compass: Passwordless Authentication

Leadership Compass: Managed Detection and Response

Leadership Compass: Providers of Verified Identity

Market Compass: Security Operations Center as a Service (SOCaaS)

Copyright

©2023 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 deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim 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 do 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.