

# IAM Systems Integrators North America: Go Big or Boutique?

Nitish Deshpande

May 28, 2024



LEADERSHIP  
COMPASS  
2024

The IAM Systems Integrators North America Leadership Compass provides insight into the capabilities of IAM systems integrators serving customers in the North American region. This report also provides analysis of the top solutions providers in the IAM systems integration space as well as vendors to watch. In this report, we examine the market segmentation, provider service functionality, relative market shares, and innovative approaches to providing IAM system integration services.

## Contents

Contents .....	2
Figures .....	3
Introduction / Executive Summary.....	5
Highlights .....	6
Market Segmentation.....	7
Delivery Models .....	9
Required Capabilities.....	9
Leadership.....	10
Overall Leadership.....	10
Service Leadership .....	11
Innovation Leadership .....	12
Market Leadership .....	14
Services and Vendors at a Glance.....	15
Service/Vendor evaluation .....	17
Spider graphs .....	17
Accenture.....	18
Avancer.....	21
Clango .....	24
DXC Technology.....	27
GAVS Technologies (GAVS).....	31
IAMConcepts .....	34
IBM .....	37
iC Consult .....	40
Identity Fusion .....	43
KeyData .....	46
Optiv .....	49
Simeio.....	53

Wipro .....	56
Vendors to Watch.....	59
Atos.....	59
CGI .....	59
Cognizant.....	59
Computacenter .....	59
Computer Integrated Services .....	59
Deloitte.....	60
Ernst & Young (EY) .....	60
HCL Technologies .....	60
Idenhaus .....	60
Infosys .....	60
IPG.....	61
KPMG .....	61
Protiviti.....	61
PwC .....	61
Uberether.....	61
Xalient.....	62
Related Research.....	62
Copyright.....	62

## Figures

Figure 1: Overall Leadership.....	11
Figure 2: Service Leadership.....	12
Figure 3: Innovation Leadership.....	13
Figure 4: Market Leadership.....	15
Figure 5: Accenture capabilities evaluation.....	20
Figure 6: Avancer capabilities evaluation .....	23
Figure 7: Clango capabilities evaluation.....	26
Figure 8: DXC Technology capabilities evaluation .....	30
Figure 9: GAVS capabilities evaluation.....	33
Figure 10: IAMConcepts capabilities evaluation.....	36
Figure 11: IBM capabilities evaluation.....	39

Figure 12: iC Consult capabilities evaluation .....	42
Figure 13: Identity Fusion capabilities evaluation .....	45
Figure 14: KeyData capabilities evaluation.....	48
Figure 15: Optiv Leadership.....	52
Figure 16: Simeio Leadership.....	55
Figure 17: Wipro Leadership.....	58

## 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. To better understand the fundamental principles this report is based on, please refer to [KuppingerCole's Research Methodology](#).

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 move towards the “least privilege” principle. IAM provides the tools to automate processes around managing users and access entitlements and also for regularly reviewing these and identifying excessive entitlements.

IAM systems integrators specialize in providing identity and access management integration services to companies. Systems 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 that can be fulfilled by these integrators. Some of the typical functions are assessment, analysis, consultation, design, customization, implementation, and training, as well as regulatory and quality assurance, maintenance and support, scalability, and project management. Integrators assess the existing infrastructure and identify the gaps, opportunities, and requirements before organizations begin the IAM transformation journey.

Most of the integrators in the market provide 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. Systems 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. Systems integrators connect and deploy IAM systems across various databases, application platforms, and operating systems. Integration to third-party IT Service Management (ITSM) and Security Information and Event Management (SIEM) solutions can also be provided based on each organization's 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 that support them in scaling their operations. Integrators in the market can meet this demand by helping to design scalable solutions.

Most organizations operate in a hybrid environment with a combination of legacy systems and applications 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 organization's 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, such solutions can create frictionless, targeted experiences that lead to greater satisfaction and loyalty. Integrators can meet this requirement by providing integrations to legacy and Software-as-a-Service (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 legacy digital assets, systems, and data, while maintaining regulatory compliance, all in an increasingly complex IT environment amid a sophisticated threat landscape. Systems Integrators can provide advanced services around authentication for providing additional security. Most of the systems 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 market for IAM systems integrators is mature and can support a wide range of IAM technologies effectively.

- Systems integrators have robust capabilities to ensure compliance with regulatory standards.
- Systems integrators offer detailed assessment matrices to comprehend customers' needs thoroughly.
- The majority of vendors featured in this report excel in advanced services such as upgrading authentication methods to passwordless access and implementing risk-based measures, alongside aiding regulatory compliance.
- Several vendors included in this report are focused on supporting clients in USA with a few exceptions from Canadian vendors that are focused on Canada.
- Most of the vendors have achieved innovation maturity due to limitations of the requirements of the services.

- Most of the vendors have a considerable number of IAM professionals certified in major product vendors.
- Most vendors offer integration services to both legacy systems and Identity-as-a-Service (IDaaS) and SaaS solutions.
- North American IAM Systems Integrators market is made up of boutique and big firms with each having their own strengths and challenges

## Market Segmentation

Identity and Access Management (IAM) systems 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, Customer Identity and Access Management (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 systems 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 systems 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 North America. As such, 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:
  - **Full service:** includes ongoing support with subscription, meaning integrators take control of the full deployment with subscription-based approach for providing support and maintenance
  - **Lead Consultant with team:** Systems integrator provides a lead consultant along with a dedicated/ flexible team for the entire engagement duration
  - **Customer providing project manager:** The client provides project manager to coordinate with consultants and developers from the systems integrator team

- **Integrators work with customer developers:** Systems integrators fulfil deployments by using the developers from the customer while providing a framework and methodology
- Projects and contracts
- Auditing and reporting
- Resource management

In this Leadership Compass, we review a mix of boutique firms and established players. The established players have vast resources and tend to leverage their global footprint to deliver projects in the North American market. These vendors support all known service offerings and IAM technologies along with a vast network of strong partnership with leading technology vendors. These firms are also investing heavily in AI, cloud services, and future market trends. They can accommodate a large number of engagements and requests due to a higher number of workforces. They can help transform large organizations with their industry knowledge and experts.

However, large firms come with their own set of challenges. Generally, the larger the firm, the slower they are in getting started with the engagements. By way of analogy, it takes a temperature of at least 100 million degrees Celsius to get a Tokamak to start a nuclear fusion. That is about what it takes for the big firms to notice your engagement requirements. Large service firms often also have a one-size-fits-all approach tailored to enterprises in specific verticals, which may not align with organizations looking for more specialized approach. Pricing proposals of big firms can also be multiple times greater than offers from a boutique vendor due to the larger firms' tendency to overstaff projects and include multiple management levels in the project scope.

Boutique firms, on the other hand, are focused on specialized offerings as per their capacity. They have limited resources but are agile for that same reason. These firms can be very quick off the line to understand the project scope and provide initial support. Most of these boutique firms are a collaborative venture of experienced professionals who previously held major positions at big 4 and other top firms. They only employ specialists who provide a proactive culture and create a collaborative environment for their clients. Due to their specialized approach, boutique firms can also be more value for money compared to big players.

Despite having these advantages over big firms, the boutique firms have their own set of challenges. Taking on a complex and vast number of engagements can be a challenge due to lower number of specialists available. These firms do not have additional talent available on the bench to address any immediate new additions in the project scope. This also translates to having limitations in providing 24x7 professional services support to their clients. The big firms can provide any type of requested support in any time zone due to their global footprint.

However, there are certain vendors in this report that have limited resources compared to big firms, but they are successfully managing millions of identities and supporting most of the major IAM technologies. In general, North American vendors are focused mainly on USA but there are few specialists from Canada which are worth exploring based on your requirements.



## 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 systems integrator delivery model will depend on the customer requirements and use cases.

## Required Capabilities

This Leadership Compass analyzes the IAM systems 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 conduct 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

Key Capabilities:

- Breadth of IAM technologies covered
- Operating systems supported
- Directory services supported
- Integration and/or synchronization to directory services
- Solution customization, including custom development
- Application integration, including legacy apps and SaaS
- Auditing, reporting, and dashboarding
- Support for inbound and outbound federation
- Areas of IAM served (such as 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
- Competitive positioning/Unique Selling Propositions

Additional innovative capabilities

- Standards support
- Policy authoring and management expertise
- IT Service Management integration such as ServiceNow, BMC Cherwell, Atlassian Jira ServiceDesk
- Mobile application and SDK support
- Support for deploying modern, passwordless 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. To better understand the fundamental principles this report is based on, please refer to [KuppingerCole's Research Methodology](#).

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

- Service Leadership
- Innovation Leadership
- Market Leadership

## Overall Leadership

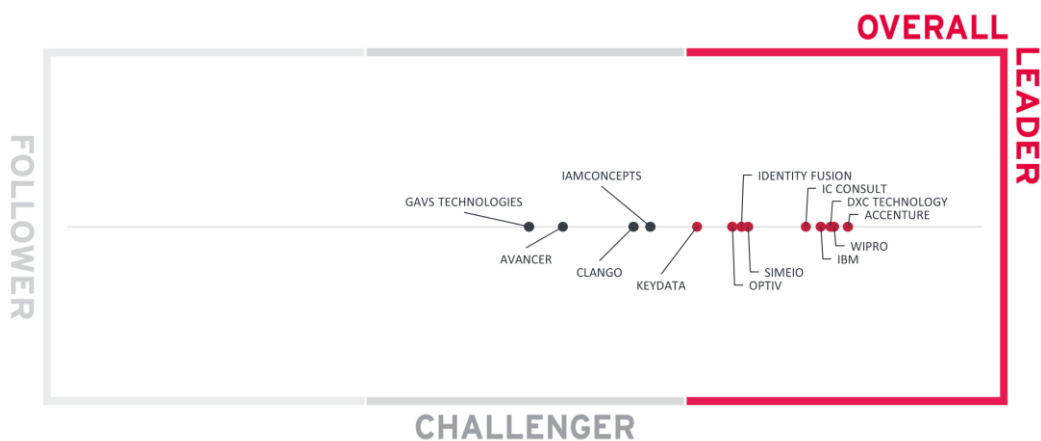


Figure 1: Overall Leadership

Overall Leaders are (in alphabetical order):

- Accenture
- DXC Technology
- IBM
- iC Consult
- Identity Fusion
- KeyData
- Optiv
- Simeio
- Wipro

## Service Leadership

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

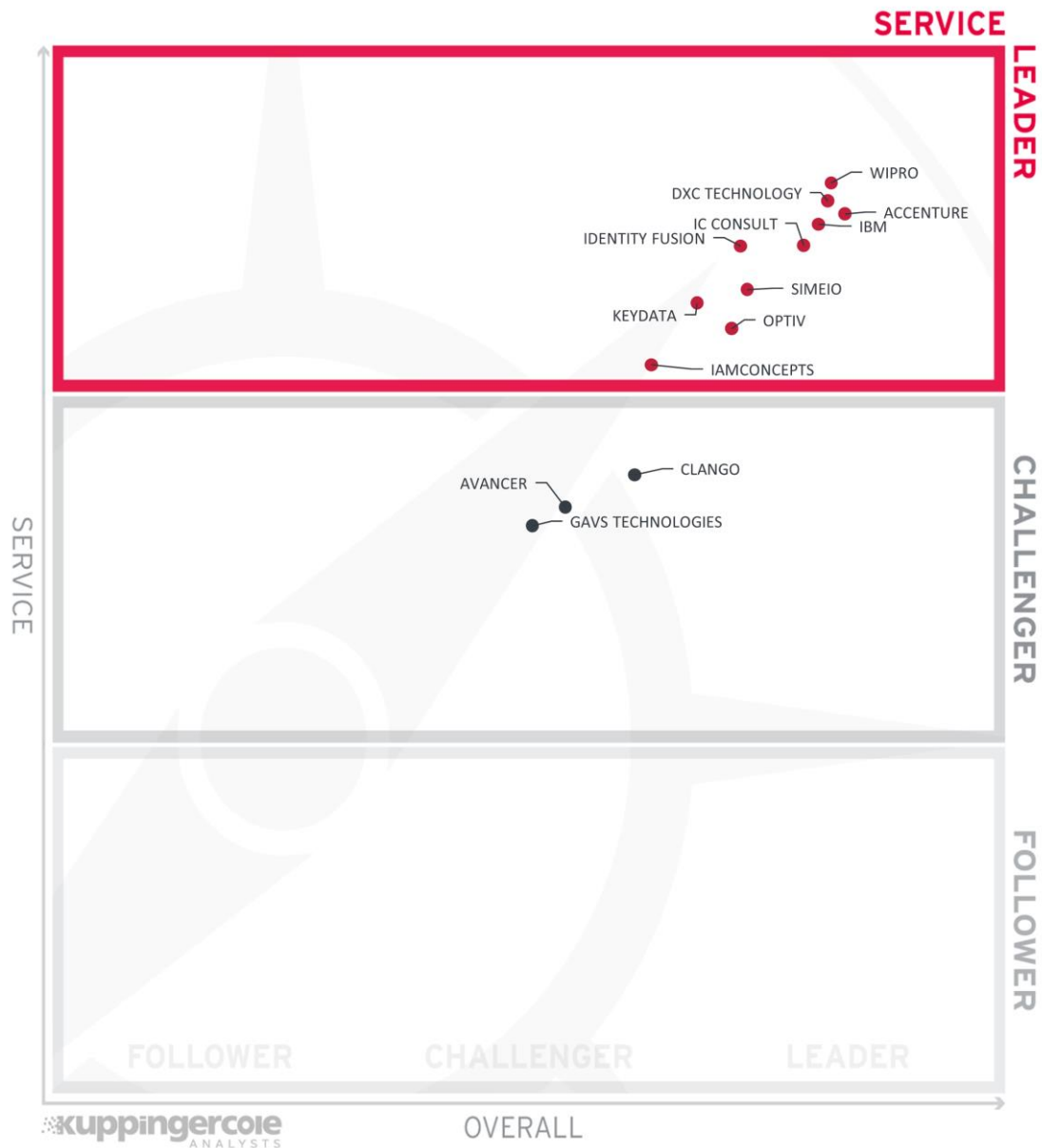


Figure 2: Service Leadership

**Service Leadership** is where we examine the functional strength and completeness of services.

Service Leaders (in alphabetical order):

- Accenture

- DXC Technology
- IAMConcepts
- IBM
- iC Consult
- Identity Fusion
- KeyData
- Optiv
- Simeio
- Wipro

## 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 cutting-edge services, while maintaining compatibility with previous versions.

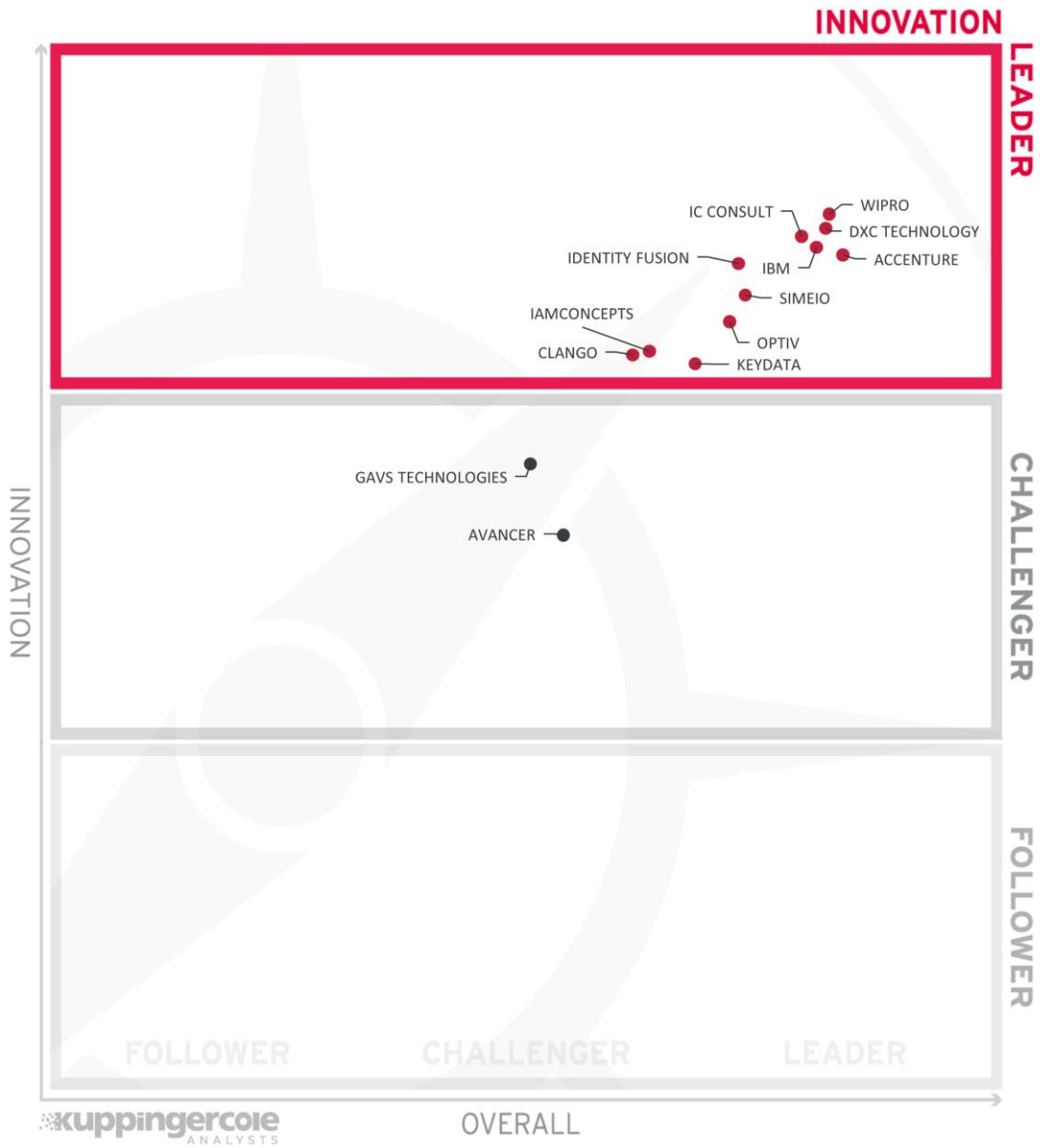


Figure 3: Innovation leadership

Innovation Leaders (in alphabetical order):

- Accenture
- Clango
- DXC Technology
- IAMConcepts
- IBM
- iC Consult
- Identity Fusion
- KeyData

- Optiv
- Simeio
- Wipro

## Market Leadership

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

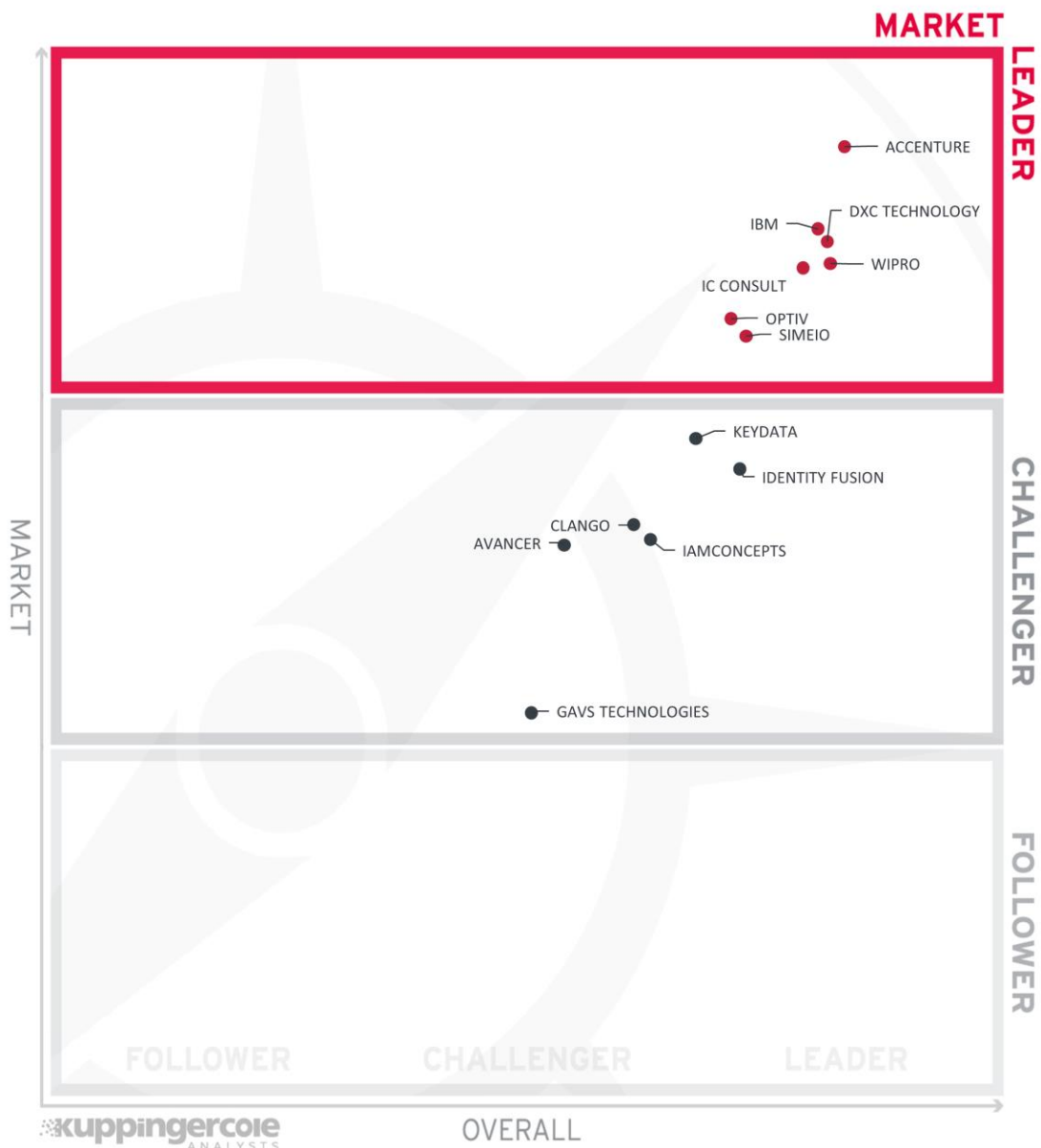


Figure 4: Market Leadership

Market Leaders (in alphabetical order):

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

## 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 Systems 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
Avancer	Strong Positive	Positive	Neutral	Positive	Neutral
Clango	Strong Positive	Positive	Neutral	Strong Positive	Neutral
DXC Technology	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Gavs Technologies	Strong Positive	Neutral	Weak	Strong Positive	Neutral
IAMConcepts	Strong Positive	Positive	Positive	Strong Positive	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	Strong Positive	Strong Positive	Strong Positive	Strong Positive
KeyData	Strong Positive	Positive	Positive	Strong Positive	Positive
Optiv	Strong Positive	Positive	Positive	Positive	Positive
Simeio	Strong Positive	Strong Positive	Positive	Strong Positive	Positive
Wipro	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive

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 products, 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
Avancer	Positive	Neutral	Neutral	Neutral
Clango	Strong Positive	Positive	Positive	Neutral
DXC Technology	Strong Positive	Positive	Strong Positive	Strong Positive
Gavs Technologies	Strong Positive	Weak	Neutral	Weak
IAMConcepts	Strong Positive	Neutral	Positive	Neutral
IBM	Strong Positive	Strong Positive	Strong Positive	Strong Positive
iC Consult	Strong Positive	Positive	Strong Positive	Strong Positive
Identity Fusion	Strong Positive	Positive	Neutral	Neutral
KeyData	Strong Positive	Positive	Positive	Positive
Optiv	Strong Positive	Positive	Strong Positive	Positive
Simeio	Strong Positive	Positive	Positive	Positive
Wipro	Strong Positive	Positive	Strong Positive	Strong Positive

Table 2: Comparative overview of the ratings for vendors



## Service/Vendor evaluation

This section contains a rating for each integrator we've evaluated in this Leadership Compass. For many of these integrators there are additional reports available on KuppingerCole website (see the end of this report for available further research).

### 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 Systems Integrators North America, we look at the following seven categories:

**Resource Management:** Systems integrator resource management involves how integrators proactively provide certification courses and training classes to their IAM professionals. Other capabilities include the ability of IAM professionals to perform tasks outside of their defined roles.

**Engagements:** Engagements looks at the capabilities of systems integrators around establishing relationships with customers over a period of time. Other factors include types and methods of engagements supported by the vendors, and number and size of engagements performed by vendors over the course of three years.

**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 systems integrator.

**API and Integrations:** This category considers the experience and capabilities of system integration vendors to provide support for several types of third-party integrations with customers' solutions as well as the ability of their IAM professionals to code to APIs.

**Auditing and Reporting:** Systems 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 50 countries. It is one of the largest consultancies globally with strong operations across the North American 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, and 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 (AD), Microsoft Entra ID, and LDAP directory servers. Okta Workforce Identity and AWS Directory Service are also supported. Accenture can support projects for deploying IAM on cloud services including 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, Saviynt, Okta, 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, Ping Identity, Oracle, IBM, 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 and establishing long term relationships with its clients. Accenture teams are experienced at tackling 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 over 3,000 dedicated 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 globally at Accenture responsible for a reported 75 percent of the projects completed on time or undertime and within the allocated budget.

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 2.0 authenticators. Auditing and forensic capabilities are available to provide security incident analysis. Reports for all major compliance framework reports 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 throughout the year for 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 focuses majority of its North American operations in USA with growing operations in Canada and Mexico. They are focused on supporting enterprise and mid-market level organizations.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Service Delivery</b>	Strong Positive
<b>Integrations</b>	Positive
<b>Serviceability</b>	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 North American locations and in all major languages

### Challenges

- Mainly long-term engagements are supported
- Support for medium and mid-market organizations is comparatively low
- Focused partner ecosystem
- Tendency to overstaff projects

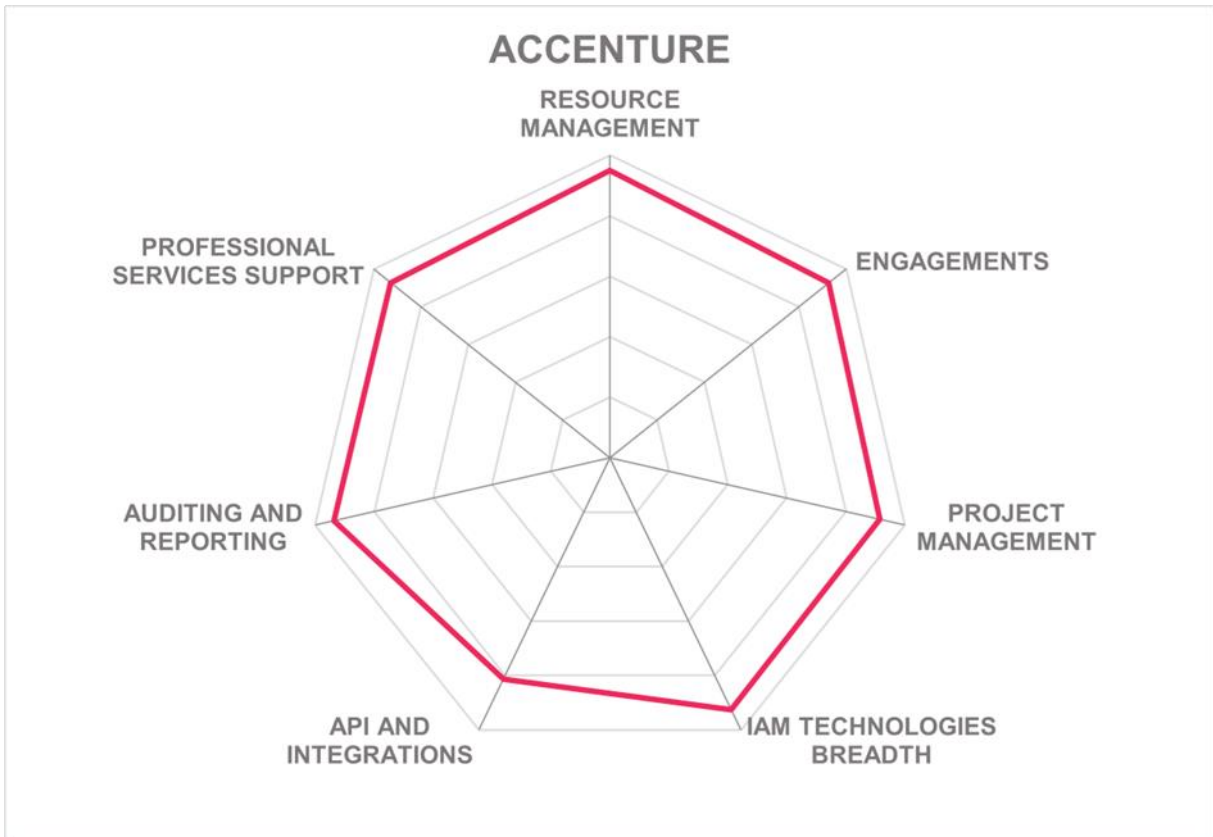


Figure 5: Accenture capabilities evaluation

## Avancer

Avancer is a cyber security consulting firm with their headquarters in New Jersey, USA. Founded in 2004, Avancer began providing integration services to healthcare sector but has now expanded to finance, insurance, manufacturing, and public sector organizations. Avancer supports all major areas of IAM technologies such as IGA, Access Management, PAM, CIAM and identity federation. They are also focused on providing support for application security and application onboarding. Avancer supports other major areas of IAM technology such as MFA, Access Governance, IDaaS, Web Access Management (WAM) and others to name a few. However, support for decentralized identity, CASB, Web Application Firewalls, and FRIP are missing.

Avancer's partner ecosystem includes SailPoint, Saviynt, Microsoft, One Identity, SecZetta, Oracle, Ping Identity, CyberArk, Beyond Trust, SecureAuth, and others. Avancer has strategic partnerships with vendors based on domains such as Identity Management, MFA, SSO, PAM, and Password Management.

Avancer has experience with operating systems such as Windows, Ubuntu, CentOS, Debian, Solaris, SUSE and RHEL. Support for AIX is missing. Avancer has experience deploying and maintaining IAM systems on application platforms such as Microsoft, Apache Tomcat, RedHat JBoss, Oracle WebLogic, IBM WebSphere, and NGINX. Avancer has experience with databases such as Microsoft SQL server, Oracle, MySQL, PostgreSQL, and Amazon RDS. They do not support IBM DB2, MongoDB, or MariaDB. Avancer supports all major directory services including ODSEE, OUD and Unbound. For IAM on IaaS installation, Avancer is experienced with Amazon AWS, Google Cloud Platform, Oracle Cloud and Microsoft Azure. Support for Alibaba, IBM Cloud, and Digital Ocean is missing. Avancer can integrate customer solutions with third-party ITSM tools such as ServiceNow, Cherwell, Ivanti Service Manager, ManageEngine ServiceDesk Plus, OpenText Service Management Automation, Broadcom, Freshworks, Sunview Software, and Atlassian JIRA ServiceDesk. Avancer has trained professionals to integrate third-party intelligence solution such as Palo Alto Cortex and CrowdStrike Falcon platform. Avancer also has experience in configuring IAM to SIEM connections by generating logs in a syslog format and directing them to a specified location.

Avancer is experienced in engagements related to assessment, advisory, implementation, integrations, managed support, RFI, and RFP. They also support customization, coding, application integration, and strategic consulting. Avancer supports engagement durations of all lengths with average duration for their end-to-end process taking 6-8 months. Avancer is experienced in providing support for various engagements methods such as full service including ongoing subscription, defined backups, and integrators working with customer developers. Avancer has nearly 92 consultants, developers, and integrators that are certified by product vendors. These professionals are also experienced in coding mainstream APIs. They can code for SOAP, REST, SCIM, LDAP, JSON, and GraphQL. Other API protocols supported are XML-RPC, Webhooks, Java, AWS SQS, and TCP Socket API. They support IDE and SDKs such as Python, Java, C/C++, .NET, and JavaScript. However, support for major SDKs such as Android and iOS are missing.

Avancer’s project managers have an average experience of over 10 years each with 75 percent of these managers being certified. Their project managers are responsible for 95 percent of projects being completed on time or undertime. 95 percent of the projects have also been completed within the allocated budget. Avancer offers various project contract types such as fixed price including software and labor and ongoing subscriptions. Contracts which are billed based on hours are also provided.

Avancer supports other advanced services such as all major authentication methods, however support for mobile biometric authentication and FIDO 2.0 are missing. Federation protocols supported are SAML, OIDC, OAuth2, and JWT are supported. Auditing and forensic capabilities are supported by identifying given areas in the logs to aid in security analysis depending on the solution. Avancer has experience developing with all major IGA and AG related reports. They also provide support for most major compliance frameworks reports. Avancer’s team can also support in creating and maintaining policies related to access control, authentication, and GRC. Support for ITDR is not yet present.

Avancer is currently focused on customers only in the USA. However, they can provide 18x7 support in English language to customers in USA and Canada. Avancer provides remote support by managed services to their customers from USA or India locations. Mid-market industries in the finance and health care sector are their focus, but Avancer is equipped to also provide services to enterprise level organizations.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Positive
<b>Service Delivery</b>	Neutral
<b>Integrations</b>	Positive
<b>Serviceability</b>	Neutral



Table 4: Avancer’s rating

**Strengths**

- Internally built Identity Bridge product used for orchestration of managed services
- Wide variety of engagement types and methods supported
- Support for majority of mainstream APIs supported
- High success rate of projects
- Supports all engagement durations
- Uses agile methodologies and scalable factory frameworks for faster onboarding of applications
- Supports majority of the report types for major compliance frameworks
- Project management

**Challenges**

- 24x7 support is missing but 18x7 support is available

- Partner ecosystem is focused but growing
- Number of engagements supported is limited

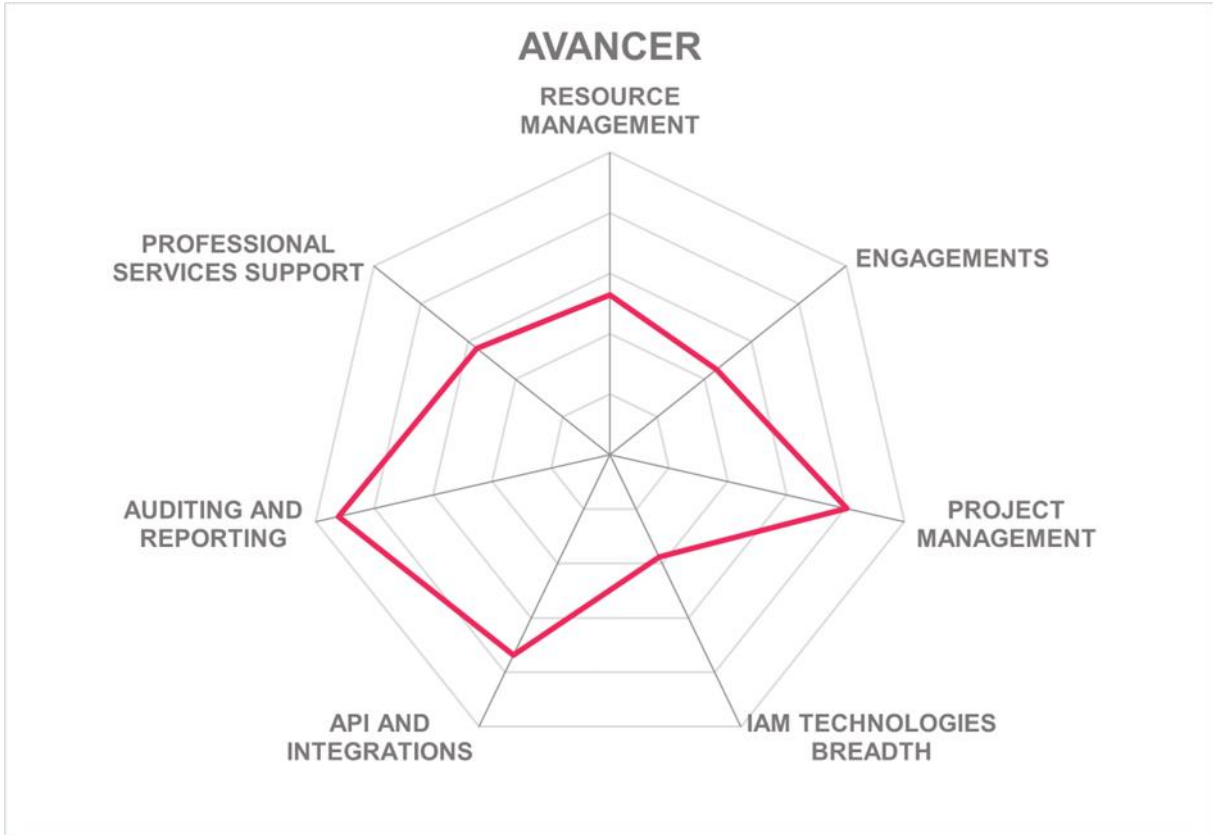


Figure 6: Avancer capabilities evaluation

## Clango

Founded in 1993 with headquarters in Virginia, USA, Clango specializes in providing identity security consultancy and engineering services to mitigate risks and reinforce defenses around core identity management business processes. Clango has customers in all industrial sectors including healthcare, finance, insurance, government, retail, and utilities. They also have a significant customer base in the manufacturing and pharmaceutical sectors. Clango has experience in supporting all major areas of IAM technologies such as IGA, PAM, Access Management, CIAM, data access governance and identity federation. Clango also supports other major areas of IAM technology such as Web Access Management (WAM), IDaaS, MFA, CASB, FRIP, risk-based authentication, SSPR, among others.

Clango has experience with operating systems such as CentOS, Windows, SUSE, Debian, RHEL, Solaris, and Ubuntu. Support for AIX is missing. They are experienced in application platforms such as Microsoft, Apache Tomcat, RedHat JBoss, Oracle WebLogic, IBM WebSphere, and NGINX. Clango is also experienced in deploying on one-off platforms. They have experience with databases such as MariaDB, Microsoft SQL server, Oracle, MySQL, PostgreSQL, IBM DB2, and MongoDB.

Clango supports all major directory services such as Microsoft Azure Directory, Azure AD, LDAP directory services, Okta, and virtual directories. They provide support for IaaS installation of IAM components for Google Cloud Platform, Oracle Cloud, Amazon AWS, and Microsoft Azure. They do not provide support for Alibaba, IBM Cloud, or Digital Ocean. Clango has experience of integrating customer solutions with third-party ITSM tools such as ServiceNow, Atlassian JIRA ServiceDesk, BMC Helix, and ManageEngine ServiceDesk Plus. Clango's developer team can support integration to other solutions as long as standard protocols are mentioned. They support various integration methods such as ETL, database level integration, or API integration depending on the requirements of target SIEM platform.

Clango partner ecosystem includes CyberArk, Delinea, ForgeRock, Omada, IBM, Microsoft, Okta/Auth0, Oracle, RSA, SailPoint, and SAP. Other partners include BeyondTrust, EmpowerID, Cisco, and ManageEngine.

Clango is experienced in various types of engagements such as RFI, RFP, design, implementation, integrations, maintenance, consulting, managed services, and customization. Clango supports both short-term and long-term engagement durations. They are experienced in engagement methods such as defined backups, full service including ongoing subscription, lead consultant with team, integrators working with customer developers, and customer providing project manager. Clango has over 100 consultants, developers, and integrators certified on at least one IAM vendor's certification program. Their team is experienced in coding all APIs such as AWS SQS, SOAP, REST, SCIM, LDAP, JSON, GraphQL, Webhooks, Java, NetIQ IDM drivers, and UDP/TCP Socket API. They provide support for the majority of the IDE and SDKs such as iOS, C/C++, Android, Java, Python, .NET, and JavaScript. They do not support Ruby and Go SDKs.

Clango has eight project managers with average experience of more than ten years. These project managers are certified in PMP, CSM, and ITIL. They are responsible for delivering a reported 80 percent of the projects on time and within allotted budget. Clango reports that



delays in project timelines are associated with scope changes from stakeholders. Clango supports all types of contracts for delivering projects such as fixed price for labor only, billed hours, and ongoing subscriptions.

Other advanced services supported by Clango include experience with all major authentication methods except FIDO 2.0, and passkeys. They support federation protocols such as SAML, OIDC, and OAuth2. They are experienced in helping customers set up auditing and forensic capabilities for security incident analysis. Clango’s team has experience in developing the most commonly requested types of reports. They have a strong knowledge of compliance requirements thus they are experienced in developing all major IGA and AG related reports. They provide customers with KPI recommendations and help in developing reports based on those indicators. Clango provides support for all major compliance frameworks reports such as GDPR, FERPA, HIPAA, CCPA, PCI-DSS, NERC CIP, and SOX. They also aid customers in creating and maintaining policies for access control, authentication, ITDR, DAG, and GRC.

Clango has customers spread across the North American region with majority of them being in USA. They provide 24x7 support in English to their customers as part of the standard service. Clango also provides remote support. Their main focus is on enterprise level organizations, but they are also capable of handling mid-market and medium size organizations. Their overall reputation in the market appears to be strong since they report that most of their clients are long-term. Clango’s roadmap includes investing in IAM advisory services, enhancing their partner ecosystem, developing managed services, and focusing on automation and orchestration features. They plan to introduce unified dashboards and add more components to tackle current integration problems.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Positive	
<b>Service Delivery</b>	Neutral	
<b>Integrations</b>	Strong Positive	
<b>Serviceability</b>	Neutral	

Table 5: Clango’s rating

**Strengths**

- All IAM technologies supported
- Experienced in coding all mainstream API protocols
- Support for all forms of authenticators available
- All engagement methods and types supported
- Project managers are certified in PMP, ITIL, and CSM
- Supports report design for all major compliance frameworks
- Support for all major operating systems for deploying and maintaining IAM systems

**Challenges**

- Partner ecosystem is good but still a few major vendors are missing
- 24x7 services are not part of the standard services
- 24x7 support is available but not part of standard service offering

Leader in

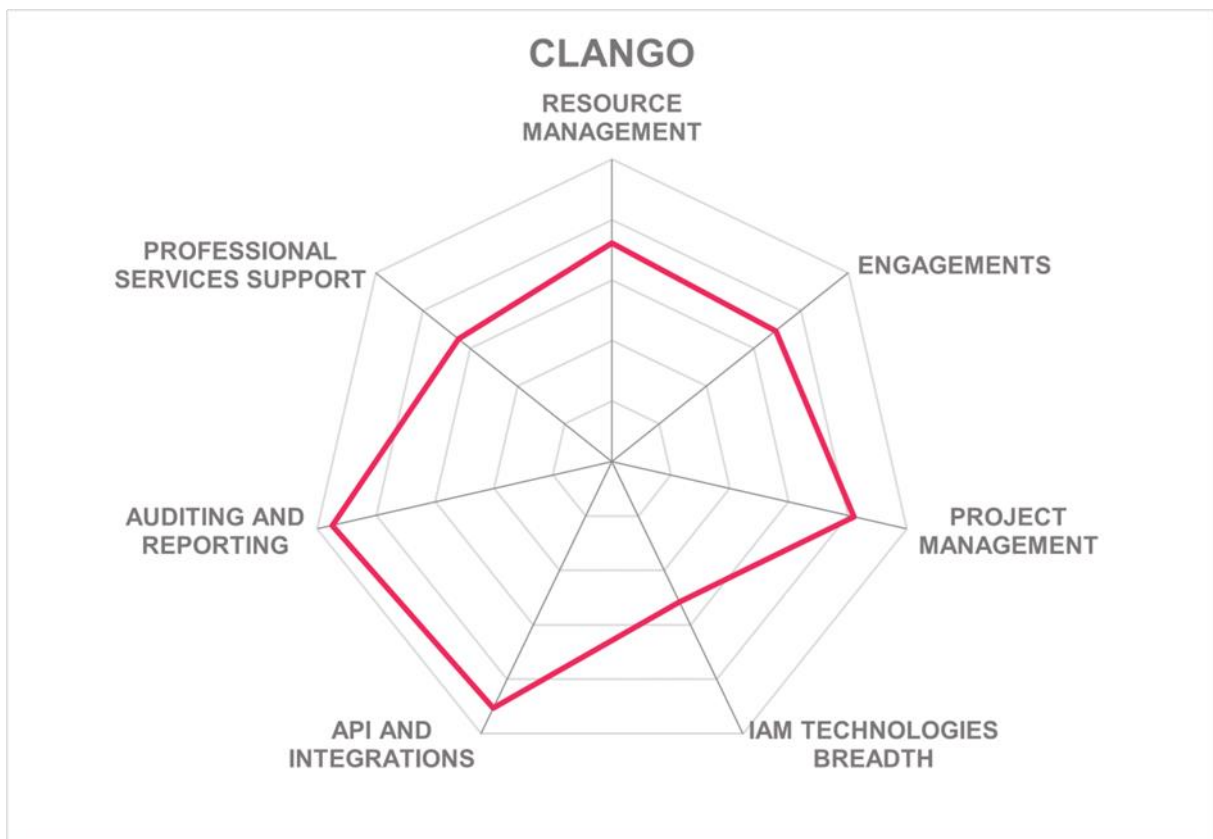


Figure 7: Clango capabilities evaluation

## DXC Technology

Founded in 2017 with headquarters in Virginia, USA, [DXC Technology](#) has a global presence providing IT security services. DXC has offices across North America including USA, Canada, Mexico, and Bermuda. They also have customers in Latin America. DXC operates across 10 verticals with many customers from the finance and manufacturing sectors. DXC supports all major IAM technology areas. They support both on-premises 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 with all major operating systems for deploying and maintaining IAM systems. DXC Digital Identity uses Midrange, Wintel teams, and cloud platform services for installing and maintaining products on majority of operating systems. They support deployments for application platforms like Microsoft, Apache Tomcat, Oracle WebLogic, and IBM WebSphere. DXC's platform and application teams support client requests for any other specific platform and OS. DXC can work with all major databases required for IAM systems.

DXC's experience with directories includes Microsoft, Oracle, Ping Identity (ForgeRock), NetIQ, IBM, and open-source LDAP products. They support provisioning and configuring of IaaS and IAM components for Microsoft Azure, Alibaba, Amazon AWS, and Google Cloud Platform. They do not support IaaS installation of IAM components on Oracle Cloud, Digital Ocean, and IBM Cloud. DXC supports integration of customer solutions to ITSM solutions such as ServiceNow, BMC Helix, and ManageEngine ServiceDesk Plus. They can support other ITSM solutions if requested. DXC supports SIEM integration. The IGA tool gathers log files and the DXC cyber transformation and operations team can build custom connectors for their chosen SIEM platforms.

DXC Technology has a very strong partner ecosystem. Microsoft, Ping Identity (including 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 more than 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 runs short-term and long-term projects and can provide 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 certified in various products such as CyberArk Defender, Microsoft SC-300 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 or AWS SQS. DXC supports all major IDEs and SDKs.

DXC has 50 project managers with 15 years of experience running large programs. Junior project managers are also available to support senior managers with basic administrative

tasks. 80 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 2.0 authenticators. They also support SAML, OAuth2, OIDC, and JWT federation protocols. DXC supports reports for all major compliance frameworks except FERPA. 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 advisory team is able to jump in and assist in this process. Their Identity team also provides support for configuring SIEM feeds or export to 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 many languages. Customers can select between on demand help, 9x5 support, or full 24x7 services. DXC also provides remote support for engagements not following the 24x7 model. They have also worked with their customers on other internal requests by operationalizing and supporting those services. Their reputation in the market is good because of their experience and services. 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.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Strong Positive	
<b>Service Delivery</b>	Strong Positive	
<b>Integrations</b>	Strong Positive	
<b>Serviceability</b>	Strong Positive	

Table 7: 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**

- Deployment of IAM components to IaaS 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

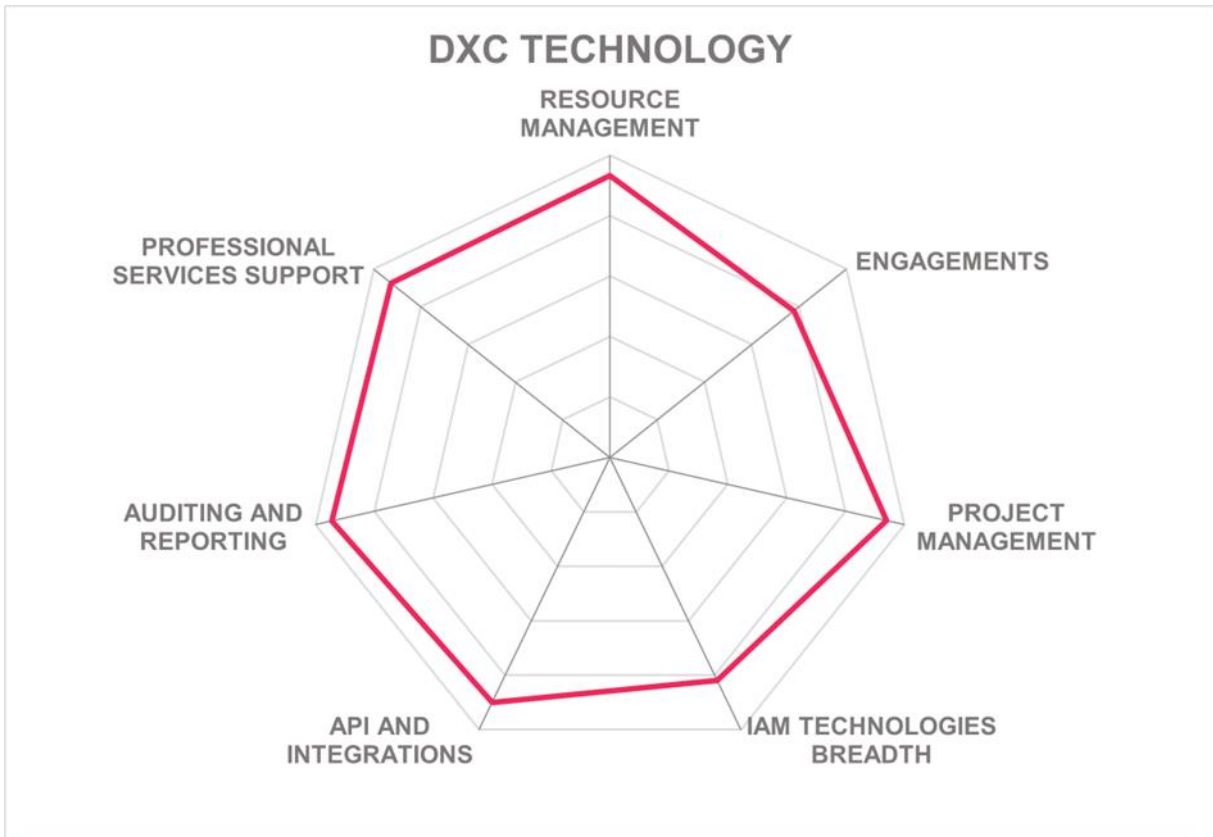


Figure 8: DXC Technology capabilities evaluation

## GAVS Technologies (GAVS)

Founded in 2003 with headquarters in New Jersey, USA, GAVS Technologies is an IT services and solution provider specializing in AI-led digital transformation initiatives and infrastructure managed services, cloud migration, and cybersecurity. GAVS has a global presence in India and Middle East, but their focus in the North American market is limited mainly to USA. GAVS specializes in supporting customers mainly from the healthcare sector. They also support customers from finance, manufacturing, communications, telecom, and utilities sector. GAVS supports all major IAM technology areas such as IGA, PAM, CIAM, Access Management, and Identity Federation. They also cover all other areas of IAM technology including WAM, IDaaS, MFA, Endpoint Security, FRIP, DLP, CASB, RPA, AI/ML, machine identity management, and decentralized identities.

GAVS has experience with operating systems such as CentOS, Windows, SUSE, Debian, RHEL, AIX and Ubuntu. They are experienced in application platforms such as Microsoft, Apache Tomcat, RedHat JBoss, Oracle WebLogic, IBM WebSphere, and NGINX. They have experience deploying and maintaining IAM systems on databases such as MariaDB, Microsoft SQL server, Oracle database, MySQL, PostgreSQL, IBM DB2 and MongoDB. GAVS supports all major directory services such as Microsoft Azure Directory, Azure AD, and LDAP directory services. They are experienced in providing support for IaaS installation of IAM components for Google Cloud Platform, IBM Cloud, Amazon AWS, and Microsoft Azure. They do not provide support for Alibaba, Oracle Cloud and Digital Ocean. GAVS is experienced in integrating customer solutions with third-party ITSM tools such as ServiceNow, Atlassian JIRA ServiceDesk, IBM Control Desk, ManageEngine ServiceDesk Plus and Freshworks. They can also customize solutions to have integration with third-party solutions such as IBM's QRadar and OneLogin. They can integrate solutions with third-party analytics and intelligences solutions such as ZIF. GAVS can also integrate IAM solutions with SIEM solutions.

GAVS partner ecosystem includes ISVs and OEMs such as Saviynt, IBM, SailPoint, Ping Identity (including ForgeRock), CyberArk, Okta, Microsoft, One Identity, Beyond Trust, Arcon, and VMWare Workspace One. Other partners include RSA, Cisco, Lenovo, EY, Kyndryl, and NTT.

GAVS is experienced in various types of engagements including end-to-end processes such as design, implementation, integrations, maintenance, consulting, managed services, customization, RFI, and RFP. They have a defined deployment framework which covers all IAM services. GAVS supports mainly long-term engagement durations; and support for short term durations lasting between 3 to 6 months is not available. They are experienced in engagement methods such as defined backups, full service including ongoing subscription, lead consultant with team, integrators working with customer developers, and customer providing project manager. GAVS has more than 15 consultants, developers, and integrators that are certified by product vendors. These certified IAM professionals are experienced in coding APIs such as SOAP, REST, SCIM, GraphQL, Webhooks, RADIUS, Java, AWS SQS, and AMQP. They provide support for IDE and SDKs such as iOS, C/C++, Android, Java, Python, .NET, Ruby, Go, and JavaScript.

GAVS has more than 10 project managers with average experience of more than 12 years. They are responsible for delivering a reported 90 percent of the projects on time and in allotted budget. They support all types of contracts for delivering projects such as fixed price, billed hours, and ongoing subscriptions.

Advanced services supported by GAVS include support for all major authentication methods including FIDO2 2.0. They also support other authentication and authorization mechanisms such as CAEP SAML, OIDC, and OAuth2. They support auditing and forensic capabilities for security incident analysis. They are also experienced in developing all major types of reports, IGA and AG related reports and all known report formats. GAVS provides support for majority of the major compliance frameworks reports such as GDPR, FERPA, HIPAA, CCPA, PCI-DSS, and SOX. Their team is also experienced at creating and maintaining policies for access control, authentication, ITDR, DAG, and GRC.

GAVS can provide 24x7 support services (in English) in USA, Canada, and Mexico. These services are part of the standard services that do not incur any additional costs. They also provide remote support. Their roadmap includes investing in secured digital banking, AI-driven IAM workflow automation, improved CIAM implementations, platform consolidation for Microsoft, Okta, Onedidentity, SailPoint and IBM. GAVS is currently focused on supporting mid-market customers, but they also have significant customers in the enterprise level organizations.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Neutral	
<b>Service Delivery</b>	Weak	
<b>Integrations</b>	Strong Positive	
<b>Serviceability</b>	Neutral	

Table 8: GAVS's rating

### Strengths

Supports majority of IAM technologies

- Critical operating systems, application platforms and directory services supported
- Supports all IDEs and SDKs
- Auditing, compliance, and reporting capabilities
- Supports most major authenticators including FIDO 2.0
- 24x7 support is available as part of standard service offering
- Project management capacity

### Challenges

- Current focus in North America is mainly on USA but growing in Canada and Mexico
- Support for few of the API protocols is missing
- Support for third-party ITSM solutions is limited



- No cost overrun guarantees for projects not provided
- Partner ecosystem is limited

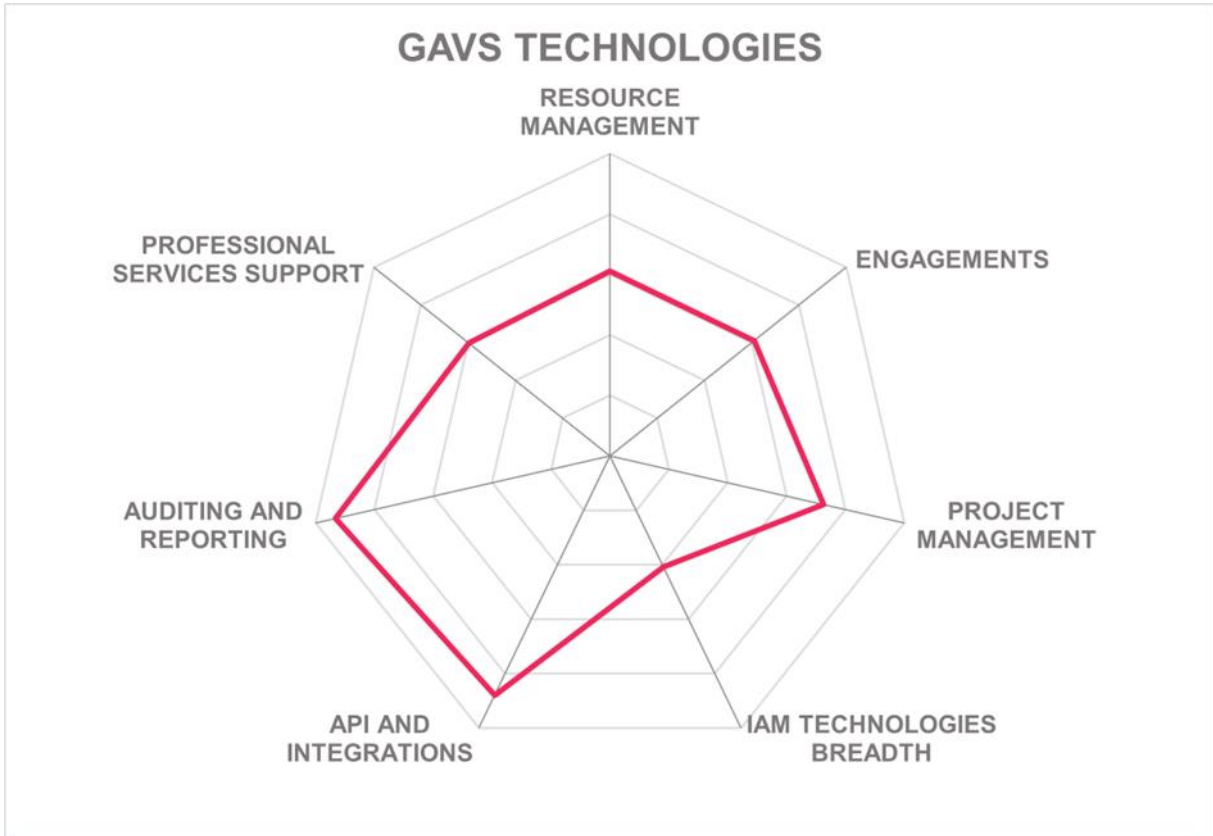


Figure 9: GAVS capabilities evaluation

## IAMConcepts

Founded in 2013 with headquarters in Toronto, Canada, IAMConcepts is a cybersecurity consulting firm focused on delivering enterprise identity and access management solutions. They specialize in IAM consulting, solution implementation, and solution management. They also specialize in managed services. IAMConcepts is mainly focused on Canada, but they also provide services to customers in USA, Mexico, and Europe. Their customers are equally spread out across all industry sectors including finance, healthcare, government, retail, insurance, and others. IAMConcepts supports major IAM technology areas such as IGA, PAM, CIAM, Access Management and Identity Federation. IGA and PAM are their main areas but demand for CIAM is growing. They also provide full support for other areas of IAM technology such as credential and secret management, vendor access management, WAM, IDaaS, MFA, Endpoint Security, FRIP, DLP, CASB, and decentralized identities, among others.

IAMConcepts has divided its partner ecosystem into service partners and technical partners. Other certified partners from their ecosystem include CyberArk, Delinea, Ping Identity (including ForgeRock), IBM, SailPoint and Saviynt. BeyondTrust, Broadcom, Entrust, Microsoft, Oracle, and Transmit Security are the other partners in their vendor ecosystem. Their main partners are IBM, Saviynt, SailPoint, Okta, Ping Identity, and CyberArk.

IAMConcepts has experience with operating systems such as CentOS, Windows, Debian, RHEL, AIX, Solaris, and Ubuntu. Support for SUSE is missing. They are experienced in all major application platforms such as Microsoft, Apache Tomcat, RedHat JBoss, Oracle WebLogic, IBM WebSphere, and NGINX. They have experience deploying and maintaining databases for IAM systems such as Microsoft SQL server, Oracle database, MySQL, PostgreSQL, IBM DB2, and MongoDB. Support for MariaDB is missing. IAM Concepts supports all major directory services including Microsoft Azure Directory, Azure AD, and LDAP directory services. Their staff can support IaaS installation of IAM components for Google Cloud Platform, Oracle Cloud, IBM Cloud, Amazon AWS, and Microsoft Azure. They do not provide support for Alibaba and Digital Ocean. IAM Concepts can integrate customer solutions with third-party ITSM tools such as TOPdesk, Hornbill, ServiceNow, Atlassian JIRA ServiceDesk, IBM Control Desk, ManageEngine ServiceDesk Plus, and Freshworks. They are experienced in customizing solutions to integrate with third-party analytics/ intelligence or user behavior analysis solutions. They can also integrate IAM solutions with SIEM solutions.

IAMConcepts is experienced in various types of engagements such as RFI, RFP, end-to-end processes such as design, implementation, integrations, maintenance, consulting, managed services, and customization. They support both short-term and long-term engagement durations. Their team is experienced in engagement methods such as defined backups, full service including ongoing subscription, lead consultant with team, integrators working with customer developers and customer providing project manager. IAMConcepts has 70 consultants, developers, and integrators that are certified by product vendors. Their IAM professionals are experienced in coding APIs such as SOAP, REST, SCIM, GraphQL, RADIUS, Java, AWS SQS and UCD/TCP Socket API. Support for gRPC, Webhooks and AMQP is missing. They also provide support for all IDE and SDKs such as iOS, C/C++, Android, Java, Python, .NET, Ruby, Go, and JavaScript.

IAMConcepts has project managers with an average experience of more than five years and IAM senior managers with an average of more than 13 years of experience in supporting clients in US, Canada, and Europe. They state that they deliver all their projects on time and within allotted budget. They support all types of contracts for delivering projects such as fixed price, billed hours, and ongoing subscriptions.

IAMConcepts also provides advanced services such as support for all major authentication methods including FIDO 2.0. They are also experienced in supporting federation protocols such as JWT, SAML, OIDC, and OAuth2. They can aid auditing and forensic capabilities for security incident analysis. They are also experienced in developing major types of IGA and AG related reports and all known report formats. They are experienced in providing support for majority of the major compliance frameworks reports such as GDPR, FERPA, HIPAA, CCPA, PCI-DSS, and SOX. Their team can create and maintain policies for access control, authentication, ITDR, DAG, and GRC.

IAMConcepts provides 24x7 support services in English and French language to their North American customers. The 24x7 services are part of the standard services. They also offer remote managed services support. They have a strong reputation in the market for providing long-term engagements. IAM Concepts' roadmap includes expanding their business in the US and focusing on mid-market segment for their MSSP platform. IAM Concepts is currently focused on supporting enterprise level organizations.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Positive	
<b>Service Delivery</b>	Positive	
<b>Integrations</b>	Strong Positive	
<b>Serviceability</b>	Positive	

Table 9: IAM Concept's rating

### Strengths

- Majority of API protocols supported
- Supports integration with all known ITSM solutions
- All major authenticators supported
- Engagement durations of all lengths supported
- Supports all major IDEs and SDKs
- Agile and responsive project management methodology
- Supports reports for almost all major compliance frameworks

### Challenges

- Limited focus on mid-market and medium level organizations but planned in roadmap
- Cost overrun guarantees are not provided
- Partner ecosystem size is moderate

Leader in

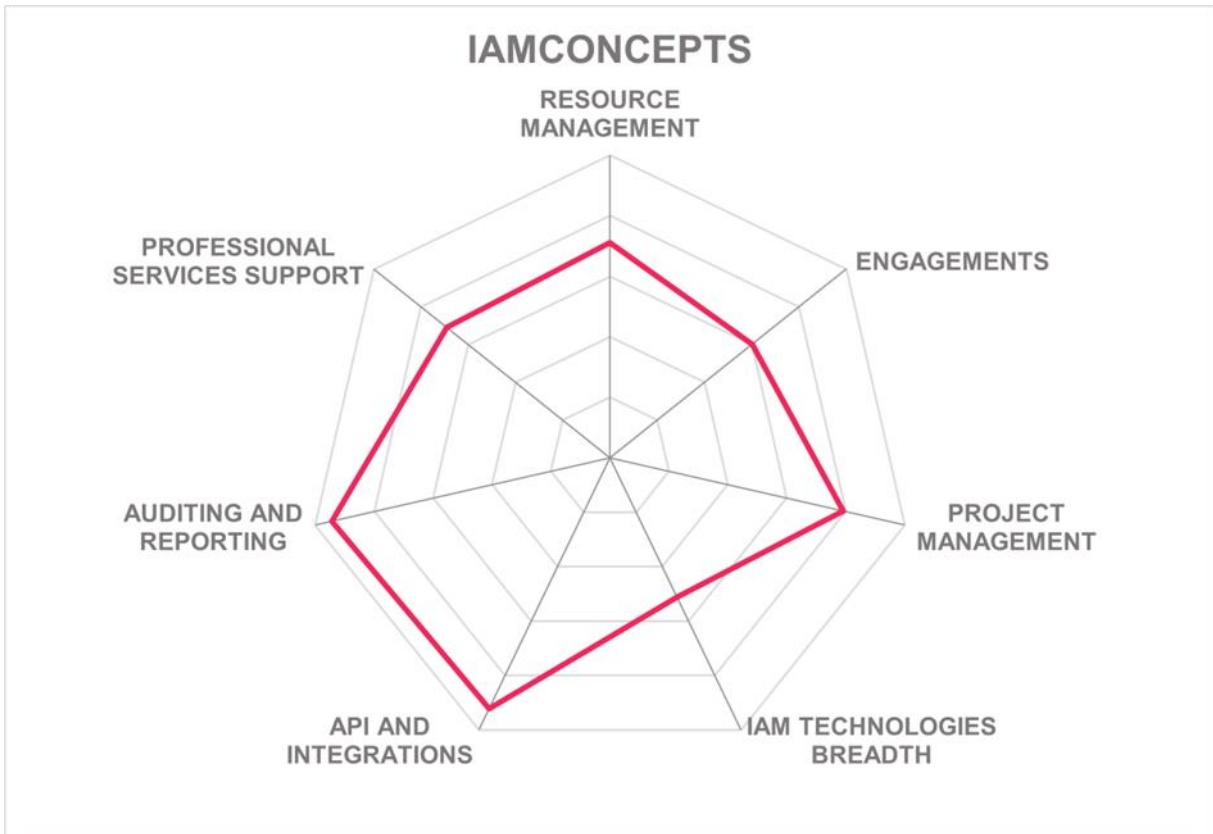


Figure 10: IAMConcepts capabilities evaluation

## 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 has an almost equal share of customers in the USA and Canada. They also provide professional services support in Mexico. 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 with 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 Microsoft EntraID/ Active Directory (AD), 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, Delinea, 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 six months to long-term and recurring support. 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 50 project managers with an average experience of ten years. All project managers have industry standard certifications. These project managers are instrumental in having a reported 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, and hard- and soft- token based HOTP and TOTP. IBM Verify access management platform supports FIDO U2F and 2.0 authenticators such as Yubico, Feitian technologies, HID Global, and SoloKeys. 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 finding 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. Remote service is also available from regional delivery centers. They provide 24x7 support as a part of their standard services to support mission critical IAM systems. Another option of 16x5 support for supporting critical incidents on IAM systems which are less sensitive is also available. They also provide remote services at their regional delivery centers. 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 and 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.

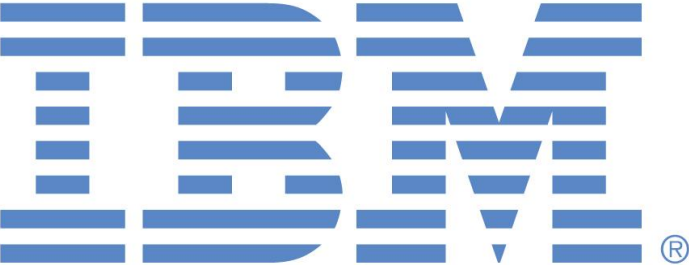
<b>Security</b>	Strong Positive	
<b>Functionality</b>	Strong Positive	
<b>Service Delivery</b>	Positive	
<b>Integrations</b>	Strong Positive	
<b>Serviceability</b>	Strong Positive	

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, CIAM, and Access Management
- IAM service offering portfolio for workforce IAM and CIAM
- 24x7 support for professional services in almost all regions of North America
- 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

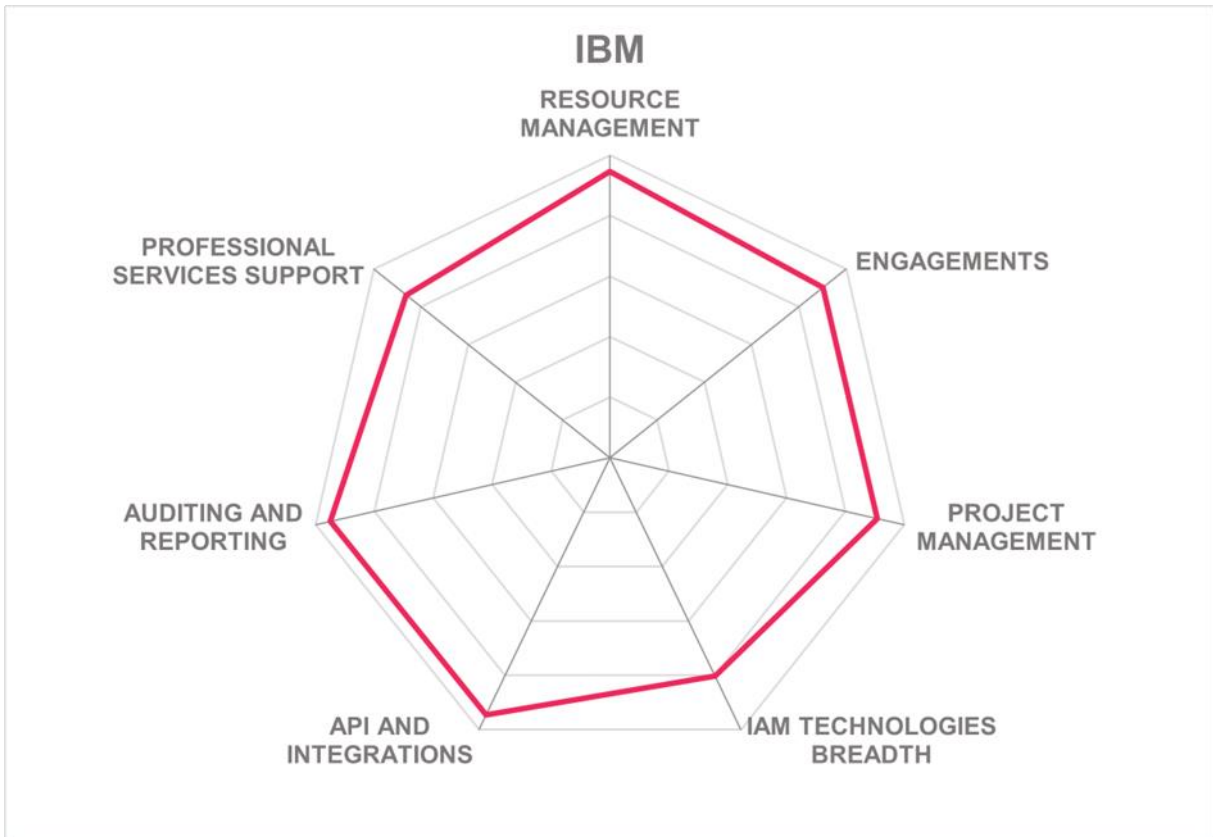


Figure 11: IBM capabilities evaluation

## iC Consult

Founded in 1997, iC Consult has transformed into a global systems integrator through recent acquisitions. Their Service Layers division delivers an integrated solution for Access Management and IGA. This division builds on the products of Ping Identity, ForgeRock, One Identity, and 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. Currently, the company's primary focus in North America is on the US. Most of their customers are in the manufacturing sector with a significant number in the following industries, automotive, 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 supporting 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 has collaborated with vendors such as Okta and Oracle to identify potential for improvements within their products and innovate solutions to address these gaps. Additionally, iC Consult partners with vendors to assist in implementing complex solutions for their customers.

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 500 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 around 120 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. The majority of the projects are completed on time and



on budget with exceptions for overruns related to change of scopes. 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. iC Consult supports federation protocols such as 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, French, and Spanish. iC Consult provides 24x7 support along with remote support. They have helped customers in making successful IGA deployments. A surveyed customer stated that they go above and beyond the scope of engagements. With a very strong partner ecosystem and an impressive number of 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.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Strong Positive	
<b>Service Delivery</b>	Strong Positive	
<b>Integrations</b>	Strong Positive	
<b>Serviceability</b>	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
- Reports for some major compliance frameworks are missing
- Focus on Canada is limited but growing

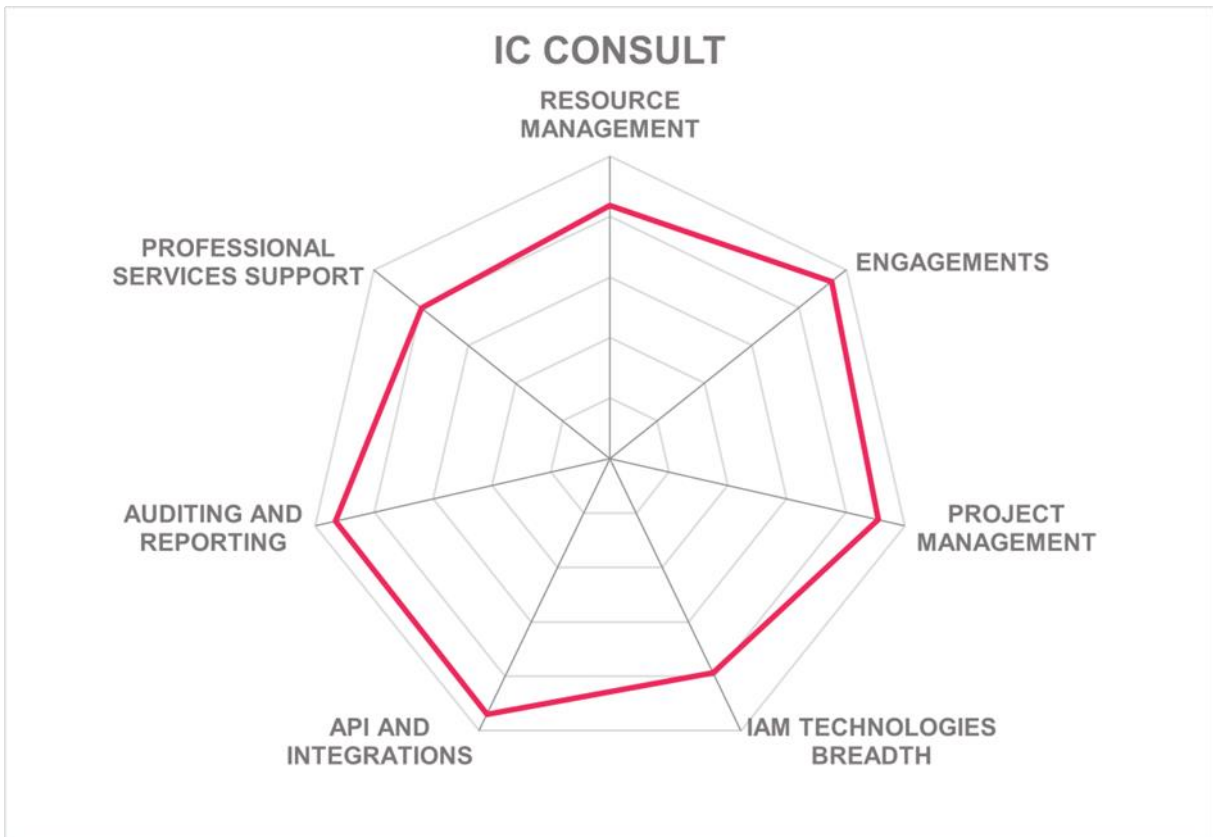


Figure 12: iC Consult capabilities evaluation

## Identity Fusion

Founded in 2013 with headquarters in Tampa, Florida, USA, Identity Fusion focuses on identity lifecycle management, access control, IGA, auditing, and reporting, APIs, and service mesh, identity stores, and interfaces. The majority of its clients are in the healthcare, automotive, finance, manufacturing, and technology services. Identity Fusion supports all major areas of IAM technologies. They are also 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.

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 available for Microsoft Azure, Google Cloud platform and Amazon AWS. They do not support Oracle Cloud, or IBM Cloud. They help customers integrate customer solutions 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 Ping Identity (including ForgeRock), Microsoft, Oracle, OneWelcome, OneLogin, Okta, ID DataWeb, iProov, Twillio, DUO, and Thales. Identity Fusion also partners with integrators such as Accenture, DXC Technology, Capgemini, KPMG, and PwC. Integration with SaaS and legacy applications is supported by Identity Fusion.

Identity Fusion's engagement support includes all major types from end-to-end processes to individual engagements like coding, customization, consulting, implementation, among others. Their engagement lengths include short-term, long-term, and recurring, depending upon the type of feature implementation. Identity Fusion has 50 certified developers and consultants that are experienced in coding all mainstream APIs. Identity Fusion's IDE and SDK experience includes iOS, Android, Java, Python, Ruby, and JavaScript. They do not support 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 integration with AuthFX Authentication broker. 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 are supported. They are experienced with all IGA and AG related report types. Identity Fusion’s IAM team can craft and manage policies around access control, GRC, ITDR, DAG, and authentication.

Identity Fusion’s language support for professional services is available in English language however 24x7 support is not part of standard services. 24x7 support can be provided 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 good roadmap and global implementations, Identity Fusion is a strong choice for enterprise and mid-market level organizations.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Service Delivery</b>	Strong Positive
<b>Integrations</b>	Strong Positive
<b>Serviceability</b>	Strong Positive



Table 12: Identity Fusion’s rating

### Strengths

- Detailed breakdown of capabilities with defined modules and sub-offerings for each major IAM technology
- Step-by-step service offerings for end-to-end projects
- 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

- 24x7 support is not part of standard services
- Number of customers is comparatively low
- Support for third-party ITSM solutions is limited

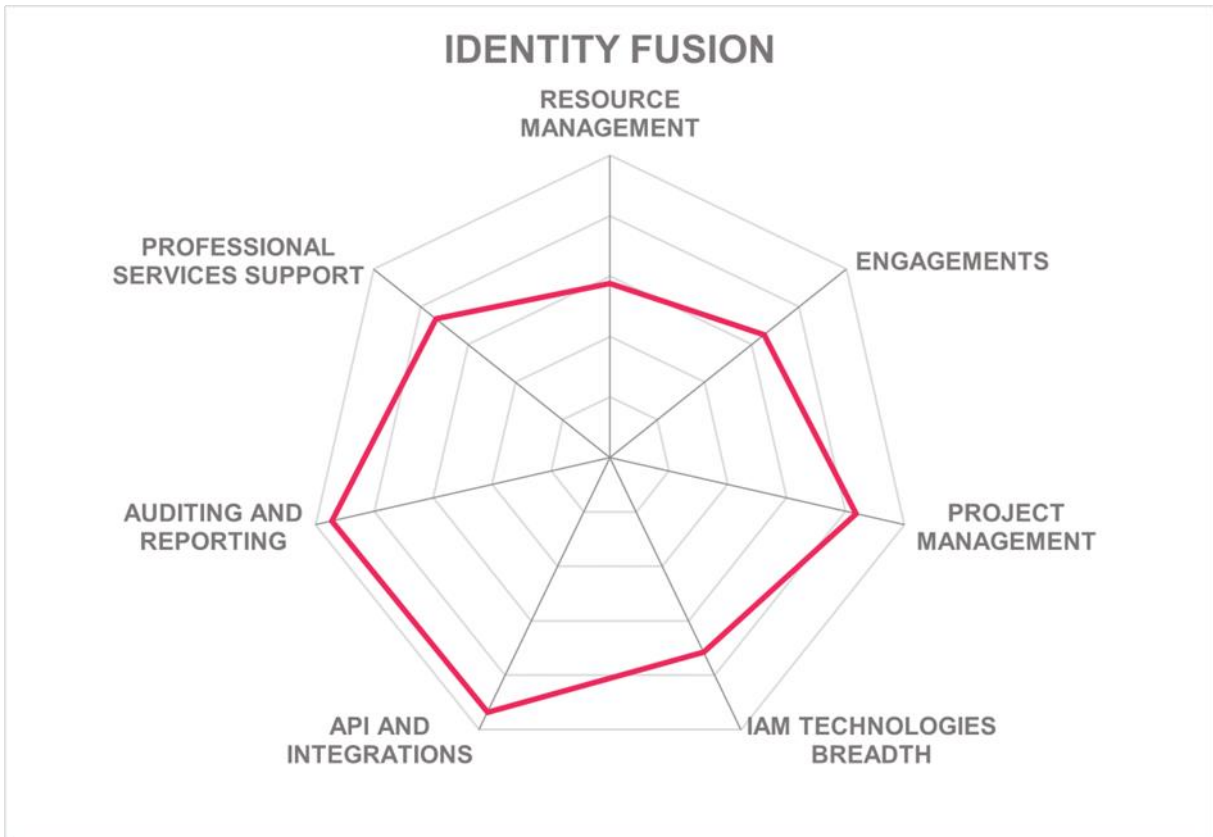


Figure 13: Identity Fusion capabilities evaluation

## KeyData

Founded in 2005, KeyData is a Canadian firm that specializes in providing identity security focused system integration, offering the full spectrum of professional services. With their headquarters in Toronto, Canada, KeyData has most of their North American customers in Canada. KeyData mainly supports companies in the finance and public sector. They also have customers in the education, agriculture, healthcare, utilities, transportation, and telecom sectors. KeyData supports all major areas of IAM technologies such as PAM, CIAM, CIEM, ITDR, and Cloud Security Management. They also cover other areas of IAM technologies such as WAM, IDaaS, API security, MFA, risk-based authentication, and authorization, CASB, WAF, access governance, and credential and secret management, among others.

KeyData has experience with most of the major OSES such as Windows, Ubuntu, Solaris, CentOS, Debian and RHEL. Support for AIX and SUSE is not available. They have experience with all major application platforms such as Microsoft, Apache Tomcat, RedHat JBoss, Oracle WebLogic, and IBM WebSphere. They have deployed and maintained IAM systems on databases such as Microsoft SQL server, Oracle Database, PostgreSQL, MySQL, and IBM DB2. Their experienced SMEs support all variations of directory services including Azure AD, Microsoft Active Directory, and directories to local solution providers such as ForgeRock's local OpenLDAP directory.

KeyData has experience with IaaS installation of IAM components on Amazon AWS, Google Cloud platform, Microsoft Azure, and Oracle Cloud. They do not support Alibaba, Digital Ocean, and IBM Cloud. They can integrate customer solutions with majority of the third-party ITSM solutions such as ServiceNow, Atlassian Jira, BMC Helix, IBM Control Desk, Broadcom, and OpenText Service Management Automation. Depending on the solution, KeyData can fulfil ITSM integrations using OOTB connectors or through custom integration services. They can also integrate customer solutions with SIEM solutions through syslog.

KeyData's partner ecosystem includes product vendors such as SailPoint, CyberArk, Okta, Microsoft, Saviynt, BeyondTrust, Ping Identity, ForgeRock, CrowdStrike, SentinelOne, Wix, and Venafi. They have highest number of Okta certified professionals in Canada. They are also SailPoint's top delivery partner in Canada. KeyData has a strategic partnership with CrowdStrike for supporting ITDR deployments.

KeyData supports all types of engagements and specialize in providing end-to-end services including assessments, training, road mapping, and vendor selection. KeyData's implementation methodology is focused on rapid delivery hence their typical engagement length is between 6-9 months. Their managed services agreements are for three years on average. KeyData has 135 certified developers and consultants. Their client-facing consultants are certified by product vendor on the technical side. These engineers are experienced in coding most of the mainstream APIs such as SOAP, REST, SCIM, LDAP, RADIUS, GraphQL, Webhooks, Java and UDP/TCP Socket API. They also support IDEs and SDKs such as Java, C/C++, .NET, Python, and JavaScript. They do not support iOS, Android, Ruby, and Go SDKs.

KeyData has ten certified project managers with an average experience of ten years. These project managers are certified in CISSP and PMP. KeyData has completed 95 percent of

their projects on time and 95 percent of the projects are completed within the specified budget. They offer contract types from billed hours, fixed price, ongoing subscriptions, staff augmentation, and managed services.

KeyData provides advanced services such as supporting all major types of authentication methods like FIDO 2.0 authenticators. They also support auditing and forensic capabilities to aid security incident analysis. Their identity security SMEs are trained on identifying the available solution logs and analyzing SIEM events to assist in auditing and forensics. They support all types and formats of reports except HTML and XML for auditing and report creation. They are also experienced in developing reports for all major compliance frameworks such as FERPA, FISMA, GDPR, and HIPAA, among others. Their team is also involved in helping clients become CMMC compliant. Their team is experienced in creating and maintaining policies around access control, GRC, ITDR, DAG, and authentication.

KeyData has 24x7 managed service support in English and French languages. Their basic support model includes all required ITIL processes with 8x5 support. Their advanced model includes 24x7 support; the premium model includes 24x7 support, a dedicated account representative, and vulnerability management and disaster recovery support. They also provide remote support with their resources located in Canada and India. KeyData has expertise in all regulatory frameworks and a strong roadmap that includes automated cloud migration, generative AI, enhanced multi-cloud security, and expanding their business in USA. They have a large and diverse client base across businesses of all sizes.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Positive	
<b>Service Delivery</b>	Positive	
<b>Integrations</b>	Strong Positive	
<b>Serviceability</b>	Positive	

Table 13: KeyData's rating

### Strengths

- Strong presence in Canadian market
- 24x7 professional services support available as part of standard services
- Partner ecosystem is very extensive
- Detailed differentiation of their services and offerings
- Experienced with integration for legacy and SaaS applications
- Defined roadmap showing innovation capabilities
- Supports reports for major compliance frameworks

### Challenges

- Support for some IDEs and SDKs is not available
- Cost overrun guarantees not provided
- Focus is only on the Canadian market but expansion to USA on the roadmap

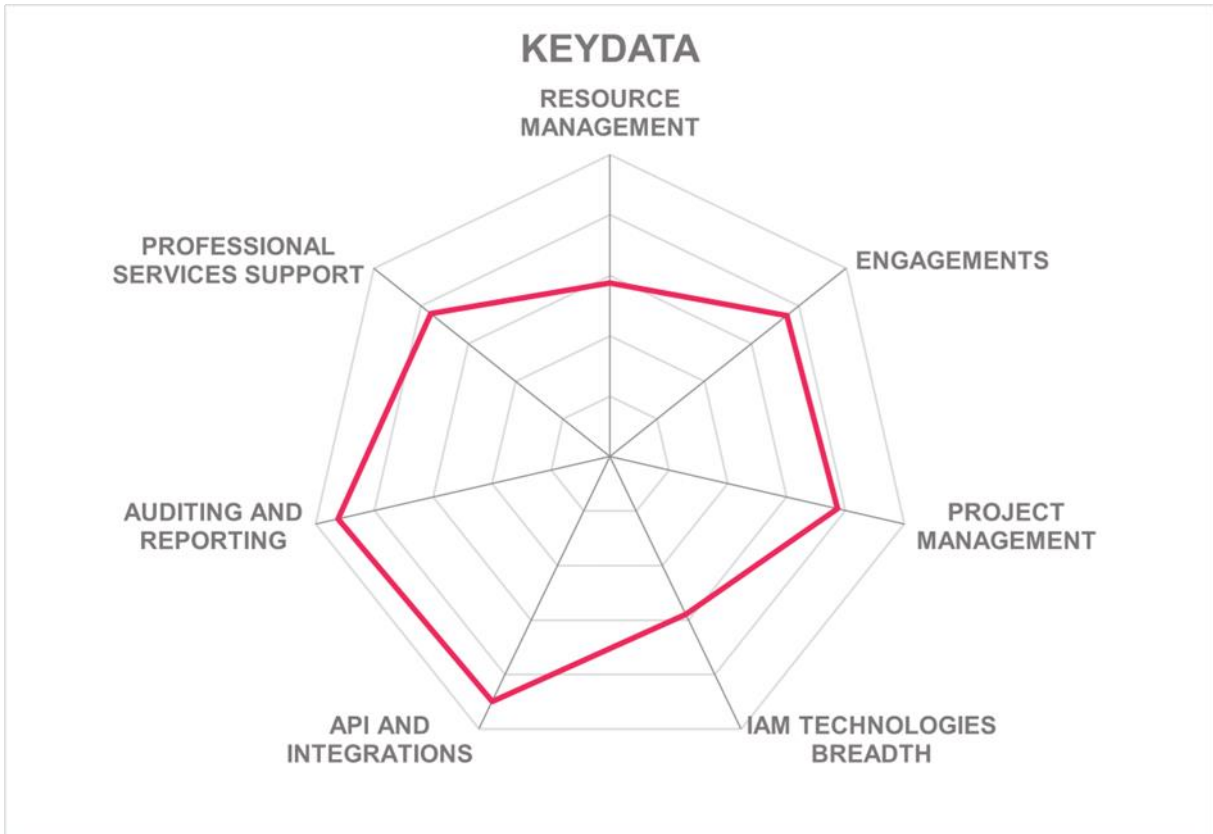


Figure 14: KeyData capabilities evaluation



## Optiv

Founded in 2015 as a result of the Accuvant-FishNet merger with headquarters in Colorado, USA, Optiv delivers strategic and technical security advisory to large number of North American customers. Their major focus is on workforce and consumer Access Management, advisory services IGA, and PAM. Most of their North American customers are in the US. Their top industry verticals are finance, insurance, healthcare, and manufacturing. They also do extensive work in the public sector and recently acquired ClearShark to further bolster sales in that vertical. Optiv is experienced in supporting business challenges across all major IAM domain areas such as workforce identity, IGA, PAM, CIAM, Access Management and Identity Federation. They also cover all other areas of IAM technology including FRIP, DLP, CASB, RPA, WAM, IDaaS, MFA, AI/ML, Machine Identity Management, and decentralized identities, among others.

Optiv has a very mature partner ecosystem which includes certifications in Palo Alto, Microsoft, Zscaler, Amazon, CyberArk, BeyondTrust, Okta, Ping Identity, SailPoint, Saviynt, RSA and IBM, among others. They developed their own migration tool for CyberArk. They also support proprietary automation use cases for Readibots, SailPoint automated regression testing with Selenium; Ping DaVinci Self Service Application Integration, and JIT Passwordless access; and Okta deployment via Terraform as part of their identity management engagements. Their partners for providing secure continuous authentication are Ping, Okta, Transmit, OLOID (it is a Physical Access Control Solution [PACS]), HYPR, Beyond Identity, CrowdStrike, and Zscaler. Their partner vendors for Digital ID Proofing are Ping, Okta, Transmit, 1Kosmos, ID DataWeb, and Jumio to prevent account take over (ATO) and fraudulent activity.

Optiv has experience with all major operating systems such as Ubuntu, AIX, Solaris, CentOS, Windows, SUSE, Debian, RHEL, AIX, and AS400. They are experienced in deploying and maintaining IAM systems on application platforms such as Microsoft, Apache Tomcat, RedHat JBoss, Oracle WebLogic, IBM WebSphere, and NGINX. They have experience deploying and maintaining IAM systems on databases such as MySQL, PostgreSQL, IBM DB2, MariaDB, Microsoft SQL server, Oracle database, and MongoDB. Optiv supports all major directory services such as Microsoft Azure Directory, Azure AD, and LDAP directory services. Optiv can support IaaS installation of IAM components for Alibaba, Oracle Cloud, Google Cloud Platform, IBM Cloud, Amazon AWS, and Microsoft Azure. As long as the vendor of the solution will fully support the implementation, Optiv can support IaaS installation. Optiv is experienced in integrating customer solutions with third-party ITSM tools such as ServiceNow, Atlassian JIRA ServiceDesk, Cherwell, BMC Remedy, and Ivanti Service Manager. Optiv can also integrate IAM solutions with SIEM solutions using syslog and JSON.

Optiv is experienced in many types of engagements including end-to-end support, and discrete services such as design, implementation, integrations, maintenance, consulting, managed services, customization, RFI, and RFP. They can also provide ongoing identity SME support to customers for identity leadership or technical roles. They have a defined framework which outlines strategies, capabilities, and key dependencies for all identity projects. In addition, Optiv boasts a dedicated organizational change management (OCM) team, which compiles business use cases and organizes and coordinates top-down support

to assist in completion of complex initiatives. Optiv also provides a full suite of cyber services spanning advisory, deployment, and managed services. They support short-term and long-term engagement durations. They are experienced in various engagement methods such as defined backups, full service including ongoing subscription, lead consultant with team, integrators working with customer developers, and customer providing project manager. Optiv has hundreds of vendor product certified consultants, developers, and integrators. Optiv's team is experienced in coding APIs such as SOAP, REST, JSON, XML, SCIM, LDAP, RADIUS, and Java. They provide support for limited IDE and SDKs such as Java, .NET, and JavaScript.

Optiv has more than 50 project and program managers with an average experience of more than six years. The majority of their project managers are certified in PMP, SAFe4, and Scrum. These project managers are responsible for delivering 90 percent of the projects on time and within allotted budget. The reasons cited for having a few projects go overtime and budget is related to scope changes from the customer. They support all types of contracts for delivering projects such as fixed price, billed hours, and ongoing subscriptions. They also have SLAs for their managed services offering. Cost overrun guarantees are also provided with fixed fee contracts.

Optiv supports other advanced services such as deploying all major authentication methods including FIDO 2.0. They also support other federation protocols such as JWT, SAML, OIDC, and OAuth2. They can provide auditing and forensic capabilities for security incident analysis. Optiv has extensive capabilities in DFIR. They also provide comprehensive remediation capabilities across all domains including identity. Optiv are also experienced in developing all major types of reports, including IGA and AG related reports and in all report formats. Optiv also provides support for creating reports for all major compliance frameworks such as GDPR, FERPA, FISMA, NERC CIP, HIPAA, CCPA, PCI-DSS, and SOX. They have capabilities in developing strategies, conducting risk assessments, and reporting across all standard and custom frameworks. Their team can customize identity-related dashboards across all products and establish full-featured KPI tracking. Their team can author and maintain policies for access control, authentication, ITDR, DAG, and GRC. They also have other practices focused specifically on data security, data privacy, and SecOps.

Optiv provides managed identity services with 24X7 support for specific vendor solutions. In addition, Optiv has a large business in providing authorized support for a wide variety of cyber vendors. These services are part of the standard services and do not incur any additional costs. They also provide remote support. Optiv is currently focused on supporting mid-market customers, but they also have significant customers in the enterprise level organizations.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Positive	
<b>Service Delivery</b>	Positive	
<b>Integrations</b>	Positive	
<b>Serviceability</b>	Positive	

Table 14: Optiv's rating

**Strengths**

- Partner ecosystem is very extensive
- Breadth of IAM technologies supported is good
- Identity modernization framework
- All engagements duration lengths supported
- Auditing and reporting capabilities
- Good pricing model

**Challenges**

- Support for ITSM solutions is limited
- Support for some API protocols is missing
- Experience with IDEs and SDKs is limited
- Focus is currently limited to mid-market level organizations

Leader in



OVERALL  
LEADER



SERVICE  
LEADER



INNOVATION  
LEADER



MARKET  
LEADER

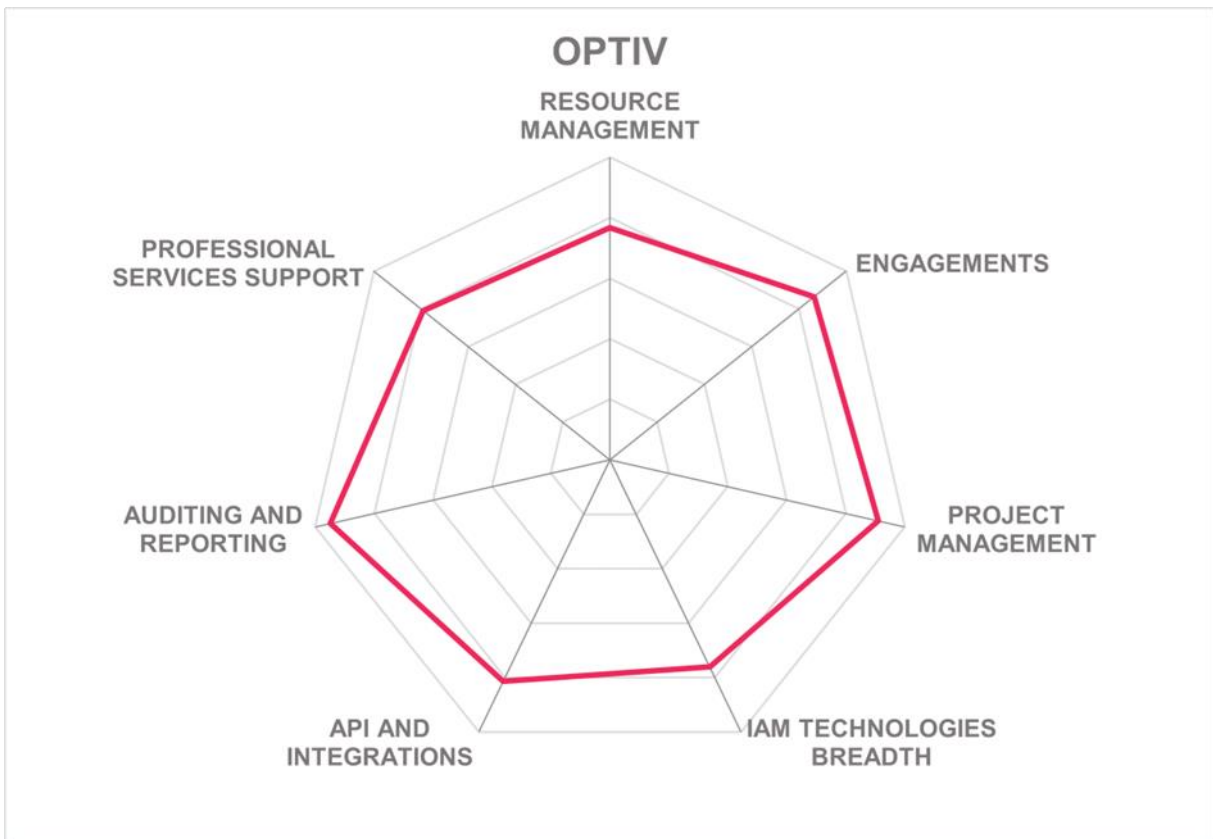


Figure 15: Optiv capabilities evaluation

## 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. They have majority of their North American customers in USA with an almost equal spread across the country. 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 among 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, Ubuntu, and Debian. 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 1Kosmos, Attivo Network, Broadcom, Cisco, Cloudentity, CyberArk, Delinea, F5, IDEE, Ping Identity (including ForgeRock), Saviynt, and SailPoint.

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' failures 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 a 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 SDKs, types for Android, iOS, Java, C+/C++, .NET, python, JavaScript, Go, and Ruby.

Simeio has 50 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, and French languages. Simeio has employees based around the world and provides 24x7 services through its four identity

intelligence centers. Simeio places itself as a strong contender for organizations in the mid-market segment with a growing portfolio of enterprise and medium level organizations.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Strong Positive	
<b>Service Delivery</b>	Positive	
<b>Integrations</b>	Strong Positive	
<b>Serviceability</b>	Positive	

Table 15: Simeio's rating

### Strengths

- Expertise in providing services to mid-market segment
- Expertise in all IAM technologies
- Hosting services are also provided
- 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 limited
- Support for major API protocols available but still some major protocols are missing
- Partner ecosystem is missing some major vendors



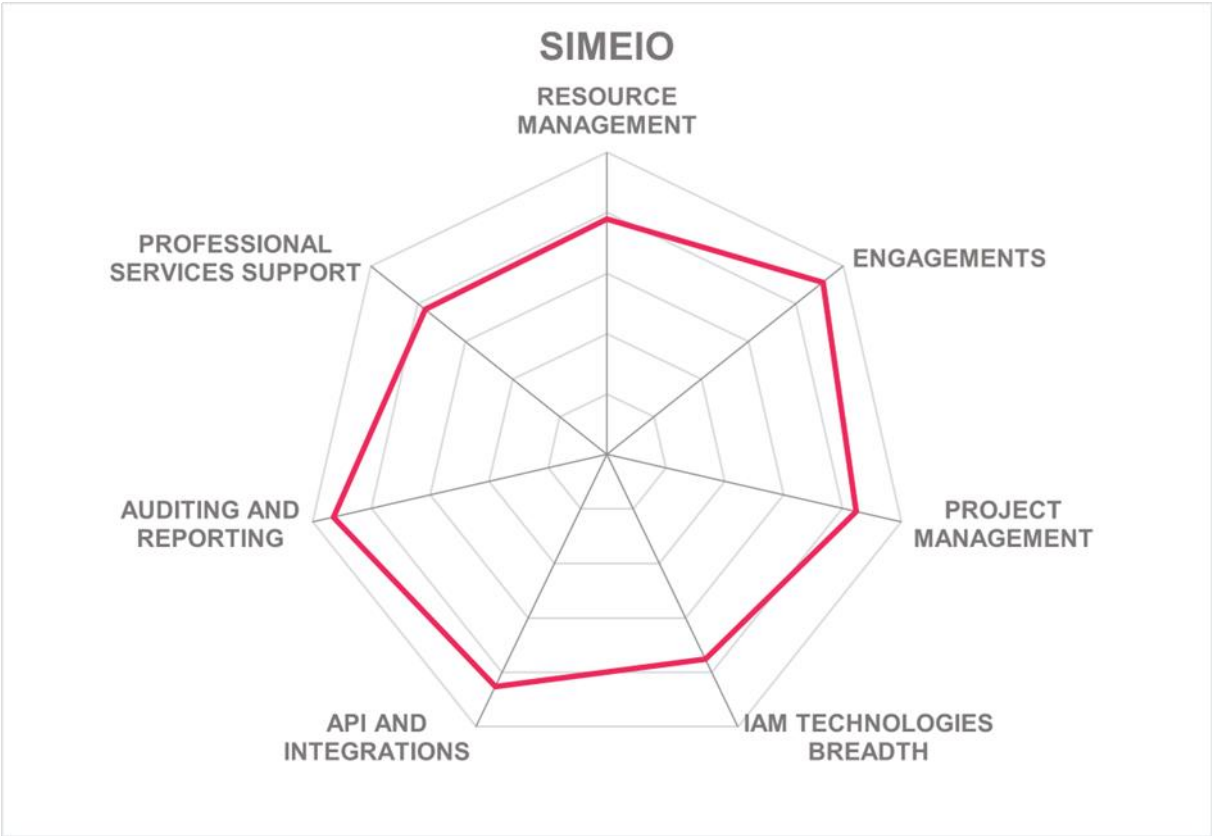


Figure 16: Simeio capabilities evaluation

## Wipro

Founded in 1945 with headquarters in Bangalore, India, Wipro is a global technology and consulting firm focused providing solutions for cybersecurity, cloud and infrastructure security, data and OT security, and digital identity. They have their offices across 66 countries but focus mainly on providing professional services in USA in the North American region. Most of their clients are in the finance, retail, healthcare, utilities, and manufacturing sectors. Wipro supports all major areas of IAM technologies with main focus on IGA, PAM, and CIAM. They also support identity federation, identity proofing, and access management, among others. Other areas of IAM technologies are also covered such as access governance, and credential and secret management, IDaaS, API security, MFA, risk-based authentication, and authorization, DLP, FRIP, CASB, remote user access, and web application firewalls.

Wipro has experience with OSes such as Windows, Ubuntu, Solaris, CentOS, AIX, Amazon Linux, SUSE, Solaris, Debian and RHEL. They are experienced with all mainstream applications platforms including Apache HTTP server, Sun Java system web server, and F5 for maintaining and deploying IAM systems. Their support for databases extends to Oracle RAC, Microsoft SQL server, Oracle Database, PostgreSQL, MySQL, and IBM DB2. They support deployment of IAM systems on directories such as Microsoft Azure Directory, Azure AD, LDAP directory services, Oracle Internet Directory, Apache Directory, OpenDJ, NetIQ Directory, and Oracle Unified Directory. Wipro is experienced with IaaS Installation of IAM components is available for Microsoft Azure, Google Cloud platform, Oracle Cloud, and Amazon AWS. Wipro can integrate customers solutions with all mainstream ITSM solutions. They are also experienced in integrating customer solutions with any third-party exposed SIEM solutions using REST or SOAP APIs.

Wipro has an extensive partner ecosystem of vendors such as Checkpoint, Cisco, CyberArk, Delinea, F5, ForgeRock, HashiCorp, IBM, Microsoft, Nexus, Okta, OpenText, Palo Alto, RSA, SailPoint, Saviynt, SAP, and Thales, among others.

Wipro supports various types of engagement methods such as maturity assessment, strategy and roadmap consulting, implementation, customization, managed services, IAM automation, M&A consulting, zero trust identity consulting. They are experienced in tackling engagement lengths ranging from a few months to recurring and long-term durations. Wipro has invested heavily by having more than 2300 developers and consultants certified in vendor products such as SailPoint, Saviynt, CyberArk, Microsoft, Okta, and SAP. They are all experienced in coding mainstream APIs such as SCIM, SOAP, REST, JSON, and LDAP, among others. They also are experienced with all mainstream IDEs and SDKs such as iOS, Android, Java, Python, Ruby, and JavaScript.

Wipro has many certified project managers with an average experience of more than ten years. Their project managers are certified in vendor products such as SailPoint Identity IQ, Saviynt IGA professional, Microsoft, and CyberArk. Wipro has completed 98 percent of their projects on time and 90 percent of the projects completed within the allotted budget. They offer various contract types such as billed hours, fixed price, ongoing subscriptions, and fixed capacity. They also provide cost overrun guarantees.



Wipro can also support other advanced services such as supporting all major types of authentication methods including FIDO 2.0. They also have a FIDO Coacher working in their team. Wipro’s team assists with auditing and report creation for all types and formats of reports. Reports for all major compliance frameworks are supported. They are also experienced with all IGA and AG related report types. Wipro has an identity management platform, called IMC, which provides a single pane of glass that brings all IAM technologies deployed in the enterprise, ITSM tools, automation utilities, and reports under one interface using advanced API and integration methods. It is a platform targeted at IAM administrators, application owners, and governance teams. Wipro’s IAM team is also able to support creating and maintaining policies around access control, GRC, ITDR, DAG, and authentication.

Wipro can provide professional services support in all major languages. They offer 24x7 services in three different support options based on capacity. Remote service is also available for all types of professional services based on pre-defined contracts. Their roadmap for 2024 includes focus on enhancing their CIAM, IGA, PAM, and passwordless/MFA offering. Their customers are mainly from mid-market to enterprise level organizations.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Strong Positive	
<b>Service Delivery</b>	Strong Positive	
<b>Integrations</b>	Strong Positive	
<b>Serviceability</b>	Strong Positive	

Table 17: Wipro’s rating

### Strengths

- Experience with all major OSES, application platforms, and directory services for deploying and maintaining IAM systems
- Support for coding all major API protocols
- Detailed 24x7 professional services support
- Auditing and reporting capabilities
- Extensive global partner ecosystem with over 2300 professionals certified in product vendors
- All engagement methods and types supported
- Detailed identity security services catalogue
- Global presence for delivering projects in any region

### Challenges

- Support for some database types is missing
- Support for some IaaS installation platforms is missing

Leader in

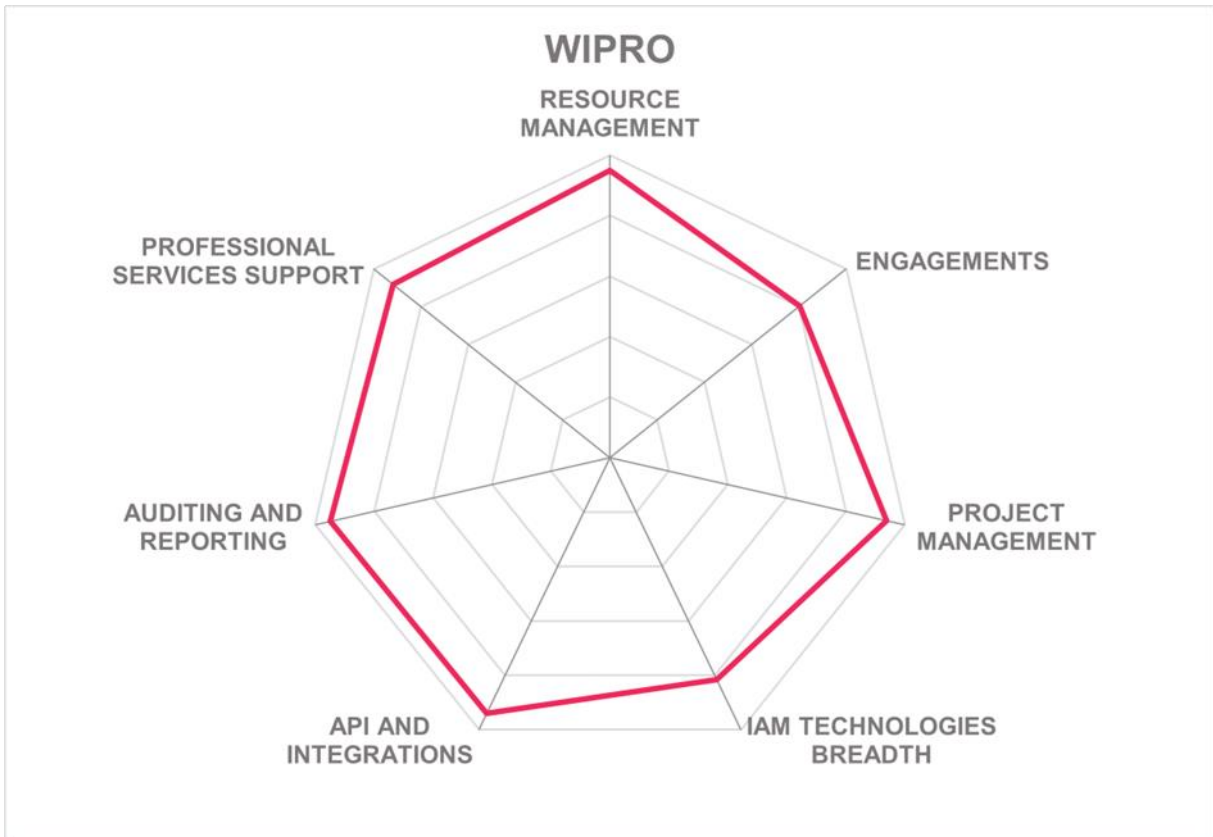


Figure 17: Wipro capabilities evaluation

## 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 strong.

### Atos

Atos is one of the largest IT consultancies and has the DirX portfolio and the Evidian products as own product solutions. 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.

### 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 deliver 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.

### Computer Integrated Services

Founded in 1995 with headquarters in Texas, USA, Computer Integrated Services (CIS) specializes in identity and access management, managed services, cloud migrations, and cyber security services. CIS provides integration services mainly to healthcare sector but also supports manufacturing, government, utilities, finance, and insurance organizations.

Why worth watching: Strong commitment to delivering projects with detailed scope

## 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.

## 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 systems integrator of choice for companies of enterprise level volume.

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

## Idenhaus

Founded in 2014, Idenhaus has its headquarters in Atlanta, USA. Idenhaus specializes in providing consulting services in the areas of strategy, analysis, requirements, and design of IAM solutions. They have an almost equal share of customers in the USA and Canada. They also provide professional services support in Mexico. Idenhaus helps organizations with all major IAM technology areas such as IGA, PAM, CIAM, and Identity Federation.

Why worth watching: Partner ecosystem for delivering IAM technologies includes various vendors, and it is focused on mid-market to enterprise level customers

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.

## 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.

## 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.

## 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.

## Uberether

Uberether was founded in 2010 and have their headquarters in Virginia, USA. They focus on identity, security, and automation. They also provide tenant platform security and managed services. They specialize in the ICAM domain with their orchestrated human/non-human

ICAM solution. Their customer base is currently limited to USA in the North American region. The majority of their clients are in the public sector and aerospace and defense industry with their customers being involved in very high-level national defense operations with millions of identities.

Why worth watching: Expertise in supporting organizations in the defense and military sectors

## Xalient

Founded in 2015 with headquarters in Leeds, England, Xalient has also expanded its operations to North America. Xalient focuses its service solutions on providing managed services and professional services including consulting, deployment and advisory. They support customers in USA, Canada, and Mexico in North America. They have clients spread across all industries, including manufacturing, retail, finance, and healthcare. Xalient supports IAM technologies such as IGA, PAM, CIAM, IAM advisory services, and identity federation.

Why worth watching: Experience with all major OSes, databases, application platforms, and databases for deploying and maintaining IAM systems.

## 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

©2024 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing 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](mailto:clients@kuppingercole.com).