Identity and Access Management Buyers Guide

Software Provider and Product Assessment

EXECUTIVE SUMMARY

ISG Research

Identity and Access Management

Chief Information Officers (CIOs), Chief Information Security Officers (CISOs) and Information Security (InfoSec) leaders face an ever-evolving cyber threat reality. As businesses rely more on digital infrastructures, the urgency to protect sensitive data and ensure operational integrity grows. A strategic approach that blends innovation with effective management of security technologies is essential. Utilizing advanced cybersecurity software tools is crucial for countering emerging threats and fortifying defenses against diverse cyber risks. Enterprises must grasp the capabilities and intricacies of these tools to safeguard valuable assets, enhance compliance and reduce security breaches. Data breaches can inflict significant financial and reputational damage, making proactive measures and incident response protocols vital for effective defense and recovery. This Buyers Guide offers insights to help enterprise security leaders make informed decisions on selecting and deploying critical cybersecurity technologies, ultimately improving their security posture and fostering a safer digital environment.

ISG Research defines Identity and Access Management (IAM) as a comprehensive approach aimed at ensuring that the right individuals have the appropriate access to technology resources at the right time. IAM strategies play a pivotal role in the cybersecurity framework of an enterprise by managing user identities and access permissions across IT environments. They facilitate user provisioning, which includes the creation, management and deletion of user accounts and roles, ensuring users have the least privilege necessary for their job functions. IAM approaches often incorporate advanced authentication methods, such as single sign-on (SSO) and multi-factor authentication (MFA), significantly reducing the risk of unauthorized access.

> **IAM is indispensable for safeguarding resources, protecting sensitive data and promoting a secure, efficient operational environment.**

In addition to providing secure access, IAM tools support regulatory compliance by maintaining detailed logs of user activities, which are essential for audits and investigations. They also enable enterprises to implement role-based access control (RBAC), ensuring policies align with business needs while mitigating security risks. Furthermore, IAM approaches often integrate with other security technologies like Security Information and Event Management (SIEM) systems, enhancing overall enterprise security posture by providing contextual understanding during potential security incidents. For enterprises managing a diverse user base—including employees, contractors and third-party providers—effective IAM is crucial. In summary, IAM is indispensable for safeguarding resources, protecting sensitive data and promoting a secure, efficient operational environment. ISG asserts that by 2027, over two-thirds of enterprises will

have adopted identity and access management platforms to protect enterprises' intellectual assets and resources.

IAM is integral to enhancing an enterprise's security posture by ensuring that only authorized individuals have access to critical resources. By implementing robust IAM practices, enterprises can mitigate risks associated with unauthorized access and potential data breaches. IAM approaches streamline user provisioning and de-provisioning, enabling enterprises to efficiently manage user identities throughout their lifecycle. This process not only improves security but also enhances operational efficiency by reducing the administrative overhead associated with access management.

Furthermore, IAM supports compliance with regulatory obligations, such as GDPR and HIPAA, by providing detailed audit trails and reporting capabilities. By effectively managing access control through role-based access management, enterprises can limit exposure of sensitive data by enforcing the principle of least privilege. This alignment with business objectives fosters trust among customers and stakeholders, as they can be assured that their data is protected. Additionally, IAM approaches enhance user experience through self-service features, allowing employees to perform tasks like password resets without involving IT, thereby improving productivity. Overall, a robust IAM approach fortifies the enterprise's security framework while supporting the broader business goals of trust, efficiency and compliance.

Generative AI (GenAI) is transforming enterprise cybersecurity software by automating complex processes and enhancing decision-making. By leveraging GenAI, enterprises can streamline threat detection, optimize resource allocation and proactively identify vulnerabilities, leading to improved operational performance. Additionally, GenAI enables teams to extract valuable insights from extensive data, fostering informed strategic planning and collaboration. As enterprises navigate digital transformation, integrating cybersecurity software with GenAI capabilities becomes crucial for maintaining a competitive edge and enhancing organizational resilience.

GenAI can significantly enhance the productivity and efficiency of security personnel within IAM by automating routine tasks, enhancing security policy management and improving user experience. AI models can analyze user behavior to enable dynamic access control policies that adapt in real time, reducing manual overhead. Automated provisioning and de-provisioning of user accounts can streamline the onboarding and offboarding processes, minimizing errors and enhancing compliance. Additionally, GenAI can streamline user authentication processes through intelligent risk assessment, leading to more reliable and

user-friendly MFA methods. By automating alerts for suspicious access patterns and providing comprehensive insights into user access trends, GenAI allows security teams to focus on higher-priority tasks, thus increasing overall operational efficiency.

In the future, the integration of agentic AI functionalities into IAM systems could improve identity security by enabling fully autonomous management of access controls and user identities. In this envisioned scenario, agentic AI could not only monitor user behavior and access patterns but also proactively adjust permissions and access rights based on emerging threats or changes in user roles without human intervention. It could facilitate real-time policy adjustments and implement context-aware access control measures that adapt as situations evolve, thereby enhancing both security and usability. Furthermore, in cases of detected anomalies, agentic AI could autonomously escalate or restrict access as needed while initiating investigations into potential security breaches. This forward-looking integration would allow enterprises to maintain robust identity security in a seamless and adaptive manner, significantly reducing their risk exposure.

In the future, the integration of agentic AI functionalities into IAM systems could improve identity security by enabling fully autonomous management of access controls and user identities.

CIOs and security leaders should approach cybersecurity software incorporating GenAI, large language models (LLMs) and future agentic AI capabilities with enthusiasm and caution. While these technologies offer significant benefits, they also come with unique challenges and prerequisites. A holistic evaluation must include technical aspects and business, ethical and strategic considerations. Other areas of focus include risk awareness, critical infrastructure, organizational readiness, governance and compliance, and a long-term perspective on the sustainability and scalability of AI approaches.

Our Cybersecurity Buyers Guide research is designed to provide a comprehensive view of a software provider's capability to enhance the effectiveness, performance and governance of cybersecurity measures within an enterprise. Separate Buyers Guide research reports are available for SIEM, EDR and Data Recovery software.

ISG believes a methodical approach is essential to maximize competitiveness. It is critical to select the right software provider and product to improve the performance of your enterprise's people, process, information and technology components.

The insights gained from understanding current cybersecurity software providers are invaluable for enterprise CIOs, CISOs and VPs of InfoSec who aim to align their technology investments with organizational goals, enhance security workflows and cultivate a culture of

resilience. By investing in the right cybersecurity tools, these leaders can unlock new avenues for protection and transformation, positioning their enterprises to thrive.

The ISG Buyers Guide™ for Identity and Access Management evaluates products based on a variety of capabilities, including access management and governance, the use of GenAI and machine learning (ML), APIs and application connector integration, auditing and reporting, identity verification, MFA, RBAC, self-service functionality, user provisioning and the ability to migrate the enterprise to a managed service provider using the existing IAM product. To be included in this Buyers Guide, software providers must meet or exceed the inclusion criteria and have commercially available products.

This research evaluates the following software providers that offer products addressing key elements of IAM: BeyondTrust, Broadcom, CyberArk, Delinea, Entrust, Eviden, Fortinet, Fortra, Google Cloud, IBM, JumpCloud, ManageEngine, Microsoft, Okta, OpenText, Oracle, Ping Identity, RSA, SailPoint and Thales.

Buyers Guide Overview

For over two decades, ISG Research has conducted market research in a spectrum of areas across business applications, tools and technologies. We have designed the Buyers Guide to provide a balanced perspective of software providers and products that is rooted in an understanding of the business requirements in any enterprise. Utilization of our research methodology and decades of experience enables our Buyers Guide to be an effective method to assess and select software providers and products. The findings of this research undertaking contribute to our comprehensive approach to rating software providers in a manner that is based on the assessments completed by an enterprise.

> **ISG Research has designed the Buyers Guide to provide a balanced perspective of software providers and products that is rooted in an understanding of business requirements in any enterprise.**

The ISG Buyers Guide™ for Identity and Access Management is the distillation of over a year of market and product research efforts. It is an assessment of how well software providers' offerings address enterprises' requirements for IAM software. The index is structured to support a request for information (RFI) that could be used in the request for proposal (RFP) process by incorporating all criteria needed to evaluate, select, utilize and maintain relationships with software providers. An effective product and customer experience with a provider can ensure the best long-term relationship and value achieved from a resource and financial investment.

In this Buyers Guide, ISG Research evaluates the software in seven key categories that are weighted to reflect buyers' needs based on our expertise and research. Five are product-experience related: Adaptability, Capability, Manageability, Reliability, and Usability. In addition, we consider two customer-experience categories: Validation, and Total Cost of Ownership/Return on Investment (TCO/ROI). To assess functionality, one of the components of Capability, we applied the ISG Research Value Index methodology and blueprint, which links the personas and processes for IAM to an enterprise's requirements.

The structure of the research reflects our understanding that the effective evaluation of software providers and products involves far more than just examining product features, potential revenue or customers generated from a provider's marketing and sales efforts. We believe it is important to take a comprehensive, research-based approach, since making the wrong choice of IAM technology can raise the total cost of ownership, lower the return on investment and hamper an enterprise's ability to reach its full performance potential. In addition, this approach can reduce the project's development and deployment time and

eliminate the risk of relying on a short list of software providers that does not represent a best fit for your enterprise.

ISG Research believes that an objective review of software providers and products is a critical business strategy for the adoption and implementation of IAM software and applications. An enterprise's review should include a thorough analysis of both what is possible and what is relevant. We urge enterprises to do a thorough job of evaluating IAM systems and tools and offer this Buyers Guide as both the results of our in-depth analysis of these providers and as an evaluation methodology.

How To Use This Buyers Guide

Evaluating Software Providers: The Process

We recommend using the Buyers Guide to assess and evaluate new or existing software providers for your enterprise. The market research can be used as an evaluation framework to establish a formal request for information from providers on products and customer experience and will shorten the cycle time when creating an RFI. The steps listed below provide a process that can facilitate best possible outcomes.

1. Define the business case and goals.
   Define the mission and business case for investment and the expected outcomes from your organizational and technological efforts.
2. Specify the business needs.
   Defining the business requirements helps identify what specific capabilities are required with respect to people, processes, information and technology.
3. Assess the required roles and responsibilities.
   Identify the individuals required for success at every level of the enterprise from executives to frontline workers and determine the needs of each.
4. Outline the project's critical path.
   What needs to be done, in what order and who will do it? This outline should make clear the prior dependencies at each step of the project plan.
5. Ascertain the technology approach.
   Determine the business and technology approach that most closely aligns to your enterprise's requirements.
6. Establish software provider evaluation criteria.
   Utilize the product experience: Adaptability, Capability, Manageability, Reliability and Usability, and the customer experience in TCO/ROI and Validation.
7. Evaluate and select the technology properly.
   Weight the categories in the technology evaluation criteria to reflect your enterprise's priorities to determine the short list of software providers and products.
8. Establish the business initiative team to start the project.
   Identify who will lead the project and the members of the team needed to plan and execute it with timelines, priorities and resources.

The Findings

All of the products we evaluated are feature-rich, but not all the capabilities offered by a software provider are equally valuable to types of workers or support everything needed to manage products on a continuous basis. Moreover, the existence of too many capabilities may be a negative factor for an enterprise if it introduces unnecessary complexity. Nonetheless, you may decide that a larger number of features in the product is a plus, especially if some of them match your enterprise's established practices or support an initiative that is driving the purchase of new software.

Factors beyond features and functions or software provider assessments may become a deciding factor. For example, an enterprise may face budget constraints such that the TCO evaluation can tip the balance to one provider or another. This is where the Value Index methodology and the appropriate category weighting can be applied to determine the best fit of software providers and products to your specific needs.

Overall Scoring of Software Providers Across Categories

The research finds Microsoft atop the list, followed by IBM and Oracle. Companies that place in the top three of a category earn the designation of Leader. IBM has done so in seven categories; Microsoft in five categories; ManageEngine in three categories; Okta and Oracle in two categories; and Delinea and Google Cloud in one category.

The overall representation of the research below places the rating of the Product Experience and Customer Experience on the *x* and *y* axes, respectively, to provide a visual representation and classification of the software providers. Those providers whose Product Experience have a higher weighted performance to the axis in aggregate of the five product categories place farther to the right, while the performance and weighting for the two Customer Experience categories determines placement on the vertical axis. In short, software providers that place closer to the upper-right on this chart performed better than those closer to the lower-left.

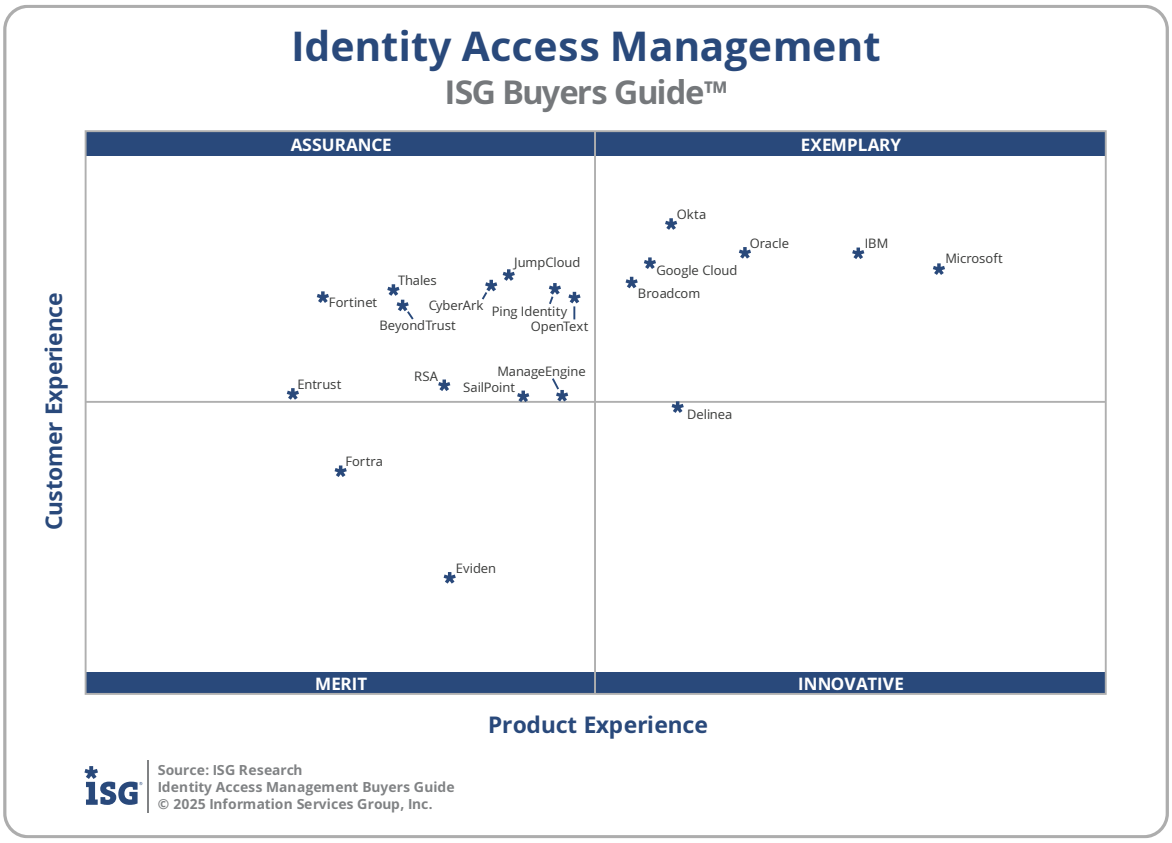
Identity Access Management

Overall

Providers	Grade	Performance
Microsoft	B++	Leader 75.3%
IBM	B+	Leader 73.5%
Oracle	B+	Leader 69.1%
Okta	B	67.6%
Google Cloud	B	66.8%
Broadcom	B	66.0%
Delinea	B	63.6%
OpenText	B	63.1%
ManageEngine	B	63.0%
Ping Identity	B-	62.5%
JumpCloud	B-	59.9%
CyberArk	B-	58.8%
SailPoint	B-	57.8%
BeyondTrust	B-	57.5%
Thales	B-	56.6%
RSA	C++	55.9%
Fortinet	C++	54.7%
Eviden	C++	52.1%
Entrust	C++	51.3%
Fortra	C++	51.0%

Source: ISG Research
Identity Access Management Buyers Guide

The research places software providers into one of four overall categories: Assurance, Exemplary, Merit or Innovative. This representation classifies providers' overall weighted performance.



Exemplary: The categorization and placement of software providers in Exemplary (upper right) represent those that performed the best in meeting the overall Product and Customer Experience requirements. The providers rated Exemplary are: Broadcom, Google Cloud, IBM, Microsoft, Okta and Oracle.

Innovative: The categorization and placement of software providers in Innovative (lower right) represent those that performed the best in meeting the overall Product Experience requirements but did not achieve the highest levels of requirements in Customer Experience. The provider rated Innovative is: Delinea.

Assurance: The categorization and placement of software providers in Assurance (upper left) represent those that achieved the highest levels in the overall Customer Experience requirements but did not achieve the highest levels of Product Experience. The providers rated Assurance are: BeyondTrust, CyberArk, Entrust, Fortinet, JumpCloud, ManageEngine, OpenText, Ping Identity, RSA, SailPoint and Thales.

Merit: The categorization of software providers in Merit (lower left) represents those that did not reach the rating of Assurance, Exemplary or Innovative ratings in Customer or Product Experience or surpass the threshold for the other three categories. The providers rated Merit are: Eviden and Fortra.

We warn that close provider placement proximity should not be taken to imply that the packages evaluated are functionally identical or equally well suited for use by every enterprise or for a specific process. Although there is a high degree of commonality in how enterprises handle IAM, there are many idiosyncrasies and differences in how they do these functions that can make one software provider's offering a better fit than another's for a particular enterprise's needs.

We advise enterprises to assess and evaluate software providers based on organizational requirements and use this research as a supplement to internal evaluation of a provider and products.

Product Experience

The process of researching products to address an enterprise's needs should be comprehensive. Our Value Index methodology examines Product Experience and how it aligns with an enterprise's lifecycle of onboarding, configuration, operations, usage and maintenance. Too often, software providers are not evaluated for the entirety of the product; instead, they are evaluated on market execution and vision of the future, which are flawed since they do not represent an enterprise's requirements but how the provider operates. As more software providers orient to a complete product experience, evaluations will be more robust.

Identity Access Management
Product Experience

Providers	Grade	Performance
Microsoft	B+	*Leader* 59.9%
IBM	B+	*Leader* 57.1%
Oracle	B	*Leader* 52.5%
Delinea	B	51.0%
Okta	B	50.9%
Google Cloud	B-	49.9%
Broadcom	B-	49.2%
OpenText	B-	47.5%
ManageEngine	B-	47.3%
Ping Identity	B-	47.0%
SailPoint	B-	46.0%
JumpCloud	B-	45.2%
CyberArk	C++	44.6%
RSA	C++	43.0%
Eviden	C++	43.0%
BeyondTrust	C++	41.2%
Thales	C++	40.9%
Fortra	C+	39.3%
Fortinet	C+	38.7%
Entrust	C+	37.3%

Source: ISG Research
Identity Access Management Buyers Guide

The research results in Product Experience are ranked at 80%, or four-fifths, of the overall rating using the specific underlying weighted category performance. Importance was placed on the categories as follows: Usability (9%), Capability (45%), Reliability (9%), Adaptability (8%) and Manageability (9%). This weighting impacted the resulting overall ratings in this research. Microsoft, IBM and Oracle were designated Product Experience Leaders.

Customer Experience

The importance of a customer relationship with a software provider is essential to the actual success of the products and technology. The advancement of the Customer Experience and the entire lifecycle an enterprise has with its software provider is critical for ensuring satisfaction in working with that provider. Technology providers that have chief customer officers are more likely to have greater investments in the customer relationship and focus more on their success. These leaders also need to take responsibility for ensuring this commitment is made abundantly clear on the website and in the buying process and customer journey.

The research results in Customer Experience are ranked at 20%, or one-fifth, using the specific underlying weighted category performance as it relates to the framework of commitment and value to the software provider-customer relationship. The two evaluation categories are Validation (10%) and TCO/ROI (10%), which are weighted to represent their importance to the overall research.

The software providers that evaluated the highest overall in the aggregated and weighted Customer Experience categories are Okta, Oracle and IBM. These category Leaders best communicate commitment and dedication to customer needs.

Identity Access Management
Customer Experience

Providers	Grade	Performance
Okta	B++	*Leader* 16.1%
Oracle	B++	*Leader* 15.4%
IBM	B++	*Leader* 15.3%
Google Cloud	B++	15.2%
Microsoft	B+	15.0%
JumpCloud	B+	14.8%
Broadcom	B+	14.8%
Ping Identity	B+	14.6%
CyberArk	B+	14.6%
Thales	B+	14.5%
Fortinet	B+	14.4%
OpenText	B+	14.3%
BeyondTrust	B+	14.1%
RSA	B	12.9%
Entrust	B	12.7%
ManageEngine	B	12.6%
SailPoint	B	12.6%
Delinea	B	12.5%
Fortra	B-	11.4%
Eviden	C+	9.6%

Source: ISG Research
Identity Access Management Buyers Guide

Software providers that did not perform well in this category were unable to provide sufficient customer case studies to demonstrate success or articulate their commitment to customer experience and an enterprise's journey. The selection of a software provider means a continuous investment by the enterprise, so a holistic evaluation must include examination of how they support their customer experience.

Appendix: Software Provider Inclusion

For inclusion in the ISG Buyers Guide™ for Identity and Access Management in 2025, a software provider must be in good standing financially and ethically, have at least $100 million in annual or projected revenue verified using independent sources, sell products and provide support on at least two continents, and have at least 100 employees. The principal source of the relevant business unit's revenue must be software-related, and there must have been at least one major software release in the last 18 months.

The research is designed to be independent of the specifics of software provider packaging and pricing. To represent the real-world environment in which businesses operate, we include providers that offer suites or packages of products that may include relevant individual modules or applications. If a software provider is actively marketing, selling and developing a product for the general market and it is reflected on the provider's website that the product is within the scope of the research, that provider is automatically evaluated for inclusion.

All software providers that offer relevant IAM products and meet the inclusion requirements were invited to participate in the evaluation process at no cost to them.

Software providers that meet our inclusion criteria but did not completely participate in our Buyers Guide were assessed solely on publicly available information. As this could have a significant impact on classification and ratings, we recommend additional scrutiny when evaluating those providers.

Products Evaluated

Provider	Product Names	Version	Release Month/Year
BeyondTrust	Pathfinder Platform	25.03	March 2025
Broadcom	Symantec Privileged Access Manager	4.2.2	April 2025
CyberArk	Privileged Access Manager	14.4	June 2025
Delinea	Identity Lifecycle Management	Spring (Q2) 2025	June 2025
Entrust	Identity as a Service (IDaaS)	5.41	May 2025
Eviden	Evidian IAM	N/A	June 2025
Fortinet	FortiAuthenticator Cloud	25.2.a	May 2025
Fortra	Access Assurance Suite	N/A	June 2025
Google Cloud	Google Cloud Identity	2024	September 2024
IBM	IBM Verify Workforce Identity	N/A	June 2025
JumpCloud	JumpCloud Platform	February	February 2025
ManageEngine	Identity360	2025	May 2025
Microsoft	Microsoft Entra ID	February	February 2025
Okta	Workforce Identity, Auth0	2025.06.0, 202508	June 2025, February 2025
OpenText	OpenText Access Manager (NetIQ)	5.1	April 2024
Oracle	OCI Identity and Access Management	14c (14.1.2.1.0)	March 2025
Ping Identity	PingOne for Workforce	2025	May 2025
RSA	SecurID	8.8	May 2025

SailPoint	IdentityIQ, Identity Security Cloud	2025.2.0, IQService-Feb-2025	May 2025, February 2025
Thales	SafeNet Trusted Access	2025	May 2025

Providers of Promise

We did not include software providers that, as a result of our research and analysis, did not satisfy the criteria for inclusion in this Buyers Guide. These are listed below as "Providers of Promise." Products that are exclusively available as part of a software platform and not sold to enterprises as standalone products are not included in this evaluation.

Provider	Product	Revenue > $100 Million	100+ Employees	Standalone Product
Andromeda Security, Inc.	Andromeda Platform	No	No	Yes
Apono	Cloud Privileged Access	No	No	Yes
AWS	AWS Identity and Access Management	Yes	Yes	No
Beyond Identity	Secure Access Platform	No	Yes	Yes
Keeper Security	KeeperPAM	No	Yes	Yes
Keycloak	Keycloak IAM	No	No	Yes
Mimoto	Mimoto	No	No	Yes
One Identity	OneLogin Workforce Identity	No	Yes	Yes
OpenAthens	OpenAthens	No	No	Yes
SAP	SAP Cloud Identity Services	Yes	Yes	No
SecureAuth	SecureAuth Workforce Identity Management	No	Yes	Yes
Twine Security	Twine Security IAM AI Digital Employee	No	No	Yes

About ISG Software Research and Advisory

ISG Software Research and Advisory provides market research and coverage of the technology industry, informing enterprises, software and service providers, and investment firms. The ISG Buyers Guides provide insight on software categories and providers that can be used in the RFI/RFP process to assess, evaluate and select software providers.

About ISG Research

ISG Research provides subscription research, advisory, consulting and executive event services focused on market trends and disruptive technologies. ISG Research delivers guidance that helps businesses accelerate growth and create more value. For further information about ISG Research subscriptions, please visit research.isg-one.com.

About ISG

ISG (Nasdaq: III) is a global AI-centered technology research and advisory firm. A trusted partner to more than 900 clients, including 75 of the world's top 100 enterprises, ISG is a long-time leader in technology and business services sourcing that is now at the forefront of leveraging AI to help organizations achieve operational excellence and faster growth. The firm, founded in 2006, is known for its proprietary market data, in-depth knowledge of provider ecosystems, and the expertise of its 1,600 professionals worldwide working together to help clients maximize the value of their technology investments.