

Identity and Access Management Platforms Buyers Guide

Software Provider and Product Assessment

SOFTWARE
PROVIDER
REPORT

***ISG** Research

Licensed by:





Key Takeaways

Identity and access management has evolved from directory-centric administration into a strategic security control layer for governing access across cloud, hybrid and partner ecosystems. Enterprises increasingly rely on IAM to manage identity lifecycles, enforce least-privilege access and support zero trust security models. AI, adaptive authentication and automation are strengthening IAM's ability to reduce identity-based risk while improving operational efficiency and user experience.

Software Provider Summary

The ISG Buyers Guide™ for Identity and Access Management Platforms evaluates 31 software providers offering products that support identity lifecycle management, authentication, authorization and access governance. The research ranked the top three overall leaders as Microsoft, AWS and Oracle. Providers were classified using weighted performance in Product Experience and Customer Experience for ISG quadrant placement. AWS, CyberArk, Google Cloud, IBM, Keeper Security, ManageEngine, Microsoft, Okta, One Identity, Oracle, SailPoint, SAP and SecureAuth were rated Exemplary, with BeyondTrust, Delinea and Ping Identity rated Innovative. Broadcom, JumpCloud, OpenText and Thales were rated Assurance, and Andromeda Security, Apono, Beyond Identity, Entrust, Eviden, Fortinet, Jisc, Keycloak, ObserveID, RSA and Twine Security and were rated Merit.

Product Experience Insights

Product Experience, representing 80% of the evaluation, focuses on Capability (50%) and Platform (30%), including adaptability, manageability, reliability and usability. Microsoft, AWS and Okta achieved the highest performance as Leaders in this category, supported by access management, authentication, governance and integration capabilities. Leaders demonstrated enterprise-grade platform capabilities across distributed identity, cloud and hybrid operating environments.

Customer Experience Value

Customer Experience, representing 20% of the evaluation, focuses on validation and TCO/ROI. Microsoft, IBM and Oracle were the Leaders in this category, showing strong customer commitment and clear dedication to customer needs. Providers with lower performance often lacked sufficient information to demonstrate customer success, articulate commitment to customer experience or communicate measurable value through TCO/ROI.

Strategic Recommendations

Enterprises should evaluate IAM platforms based on the ability to provide unified identity lifecycle management, strong authentication and consistent access governance across distributed environments. Assessment should prioritize adaptive access controls, multifactor authentication, API and connector integration, auditability and scalability. Organizations should also evaluate AI-enabled risk analysis and lifecycle automation that improve security and operational efficiency while supporting zero trust principles.



Identity and Access Management Platforms

Identity and access management remains central to enterprise cybersecurity as digital operations expand across cloud, hybrid and partner ecosystems. Security leaders must control access to sensitive systems while maintaining operational efficiency and user productivity. ISG Research asserts that by 2028, more than 70% of enterprises will prioritize IAM platforms as a primary control point for reducing identity-based attack risk and improving compliance outcomes.

ISG Research defines Identity and Access Management (IAM) as a framework of policies, processes and software that ensures individuals and systems have appropriate access to enterprise resources at the right time. IAM governs identity lifecycle management, authentication and authorization across environments while enforcing least-privilege principles.

IAM encompasses capabilities such as user provisioning and de-provisioning, single sign-on, multifactor authentication and role-based access control. It also integrates with broader security systems to provide visibility into access activity and support audit and compliance requirements across a diverse population of employees, contractors and third-party users.

The category originated as a directory-centric function focused on managing user accounts within on-premises systems. Early software emphasized authentication and basic access control tied to enterprise directories, with limited integration across applications and environments.

IAM has evolved into a cloud-first, identity-centric security discipline. Current IAM platforms support distributed architectures, application programming interface (API)-driven integration and identity federation across software-as-a-service (SaaS) and hybrid environments. The shift toward zero-trust security models has elevated IAM from an administrative function to a strategic control layer that continuously evaluates identity, context and risk before granting access.

The emergence of non-human identity (NHI) management extends these principles beyond human users to applications, services, workloads, devices and increasingly autonomous AI agents. NHI is complementary to IAM, applying identity governance and access control to identities that operate without direct human interaction while addressing their distinct requirements for discovery, ownership, credential management and lifecycle automation.

Cybersecurity
Market Assertion

By 2028, more than 70% of enterprises will prioritize IAM platforms as a primary control point for reducing identity-based attack risk and improving compliance outcomes.

Jeff Orr
Director of Research, Technology Research

ISG Research

The graphic is a dark blue rectangular box with a light blue border. It contains the title 'Cybersecurity' in large white font, followed by 'Market Assertion' in smaller white font. Below this is a paragraph of white text stating the market assertion. At the bottom right is a circular portrait of Jeff Orr, a man with glasses and a blue shirt. Below the portrait is his name 'Jeff Orr' and title 'Director of Research, Technology Research' in white. At the bottom left is the 'ISG Research' logo in white.



Enterprises require IAM approaches that reduce exposure to identity-based threats while enabling seamless access for users across environments. This includes the ability to manage identities at scale, enforce consistent access policies and maintain visibility into user activity without introducing operational friction.

Security and IT leaders also need IAM capabilities that align with regulatory requirements and support audit readiness. As organizations expand their ecosystems, nonemployees and non-

“

As organizations expand their ecosystems, nonemployees and non-human identities must be governed with the same rigor as workforce users, while accounting for the distinct scale, velocity and lifecycle requirements of machine-driven access.

human identities must be governed with the same rigor as workforce users, while accounting for the distinct scale, velocity and lifecycle requirements of machine-driven access.

Effective IAM software must deliver unified identity lifecycle management through strong authentication and adaptive access controls. This includes support for single sign-on, multifactor authentication and policy-based authorization that incorporates user behavior and contextual signals. Integration through APIs and prebuilt connectors is essential to ensure consistent enforcement across applications and infrastructure.

Successful IAM platforms also provide robust auditing, reporting and governance capabilities to support compliance and risk management. Usability remains a key requirement because self-service features and streamlined workflows reduce administrative overhead while improving the user experience. The ability to operate across hybrid and multicloud environments without fragmentation is now a baseline expectation.

Artificial intelligence is improving IAM operations through automated analysis of user behavior, access

patterns and risk signals. Machine learning models enable adaptive authentication by assessing contextual factors such as location, device and activity to adjust access decisions dynamically. Artificial intelligence-driven automation streamlines provisioning and de-provisioning processes, reducing manual effort and minimizing errors. Security teams benefit from faster detection of anomalous access activity and more precise policy enforcement, strengthening protection while improving operational efficiency.

IAM is distinct from adjacent categories such as endpoint security and threat detection because it focuses on identity as the primary control plane for access rather than controls operating at other layers of the security stack. IAM enables organizations to establish



consistent identity governance, enforce access policies and manage authentication across increasingly distributed environments.

Enterprises should prioritize IAM platforms that align with zero trust principles, integrate with existing security ecosystems and deliver measurable improvements in access control and operational efficiency. Evaluating provider capabilities in scalability, usability and governance will help organizations reduce risk and support evolving digital business requirements.

The 2026 ISG Buyers Guide™ for Identity and Access Management Platforms evaluates software providers across key capability areas, including access management and governance, use of artificial intelligence and machine learning, APIs and application connector integration, auditing and reporting, identity verification, multifactor authentication, role-based access control, self-service functionality, user provisioning and migration to managed service environments. This research assessed the following software providers: Andromeda Security, Apono, AWS, Beyond Identity, BeyondTrust, Broadcom, CyberArk, Delinea, Entrust, Eviden, Fortinet, Google Cloud, IBM, JumpCloud, Keeper Security, Keycloak, ManageEngine, Microsoft, Okta, One Identity, OpenAthens, OpenText, Oracle, Ping Identity, RSA, SailPoint Technologies, SAP, SecureAuth, Thales and Twine Security.



The Findings

The software providers and products evaluated in this research offer product and customer experiences, but not every feature is equally valuable to every enterprise or is needed to support the relevant business processes and use cases. Moreover, having too many product capabilities may be a negative factor for an enterprise if it introduces unnecessary complexity. Nonetheless, you may decide that a more comprehensive set of capabilities is important and meets your enterprise's requirements.

An effective customer relationship with a software provider is vital to the success of any investment. The overall customer experience and the full lifecycle of engagement play a key role in ensuring satisfaction and long-term success. Providers with dedicated customer leadership, such as chief customer officers, tend to invest more deeply in these relationships and prioritize customer outcomes in line with TCO and ROI expectations. It is equally important that this commitment to customer success is evident throughout the provider's website, the buying process and the customer journey.

Overall Scoring of Software Providers Across Categories

The research finds Microsoft atop the list, followed by AWS and Oracle. Providers that place in the top three of a category earn the designation of Leader. Microsoft has done so in five categories; AWS in three; Okta and Oracle in two; and IBM, Ping Identity and SecureAuth in one category.

The quadrant chart below presents ratings for Product Experience and Customer Experience on the x- and y-axes, respectively, to visually classify software providers. Those providers whose Product Experience has above-median weighted performance on the axis, in aggregate across the two product categories, place farther to the right. The performance and weighting for the Customer Experience category determine 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.

IAM Platforms Overall

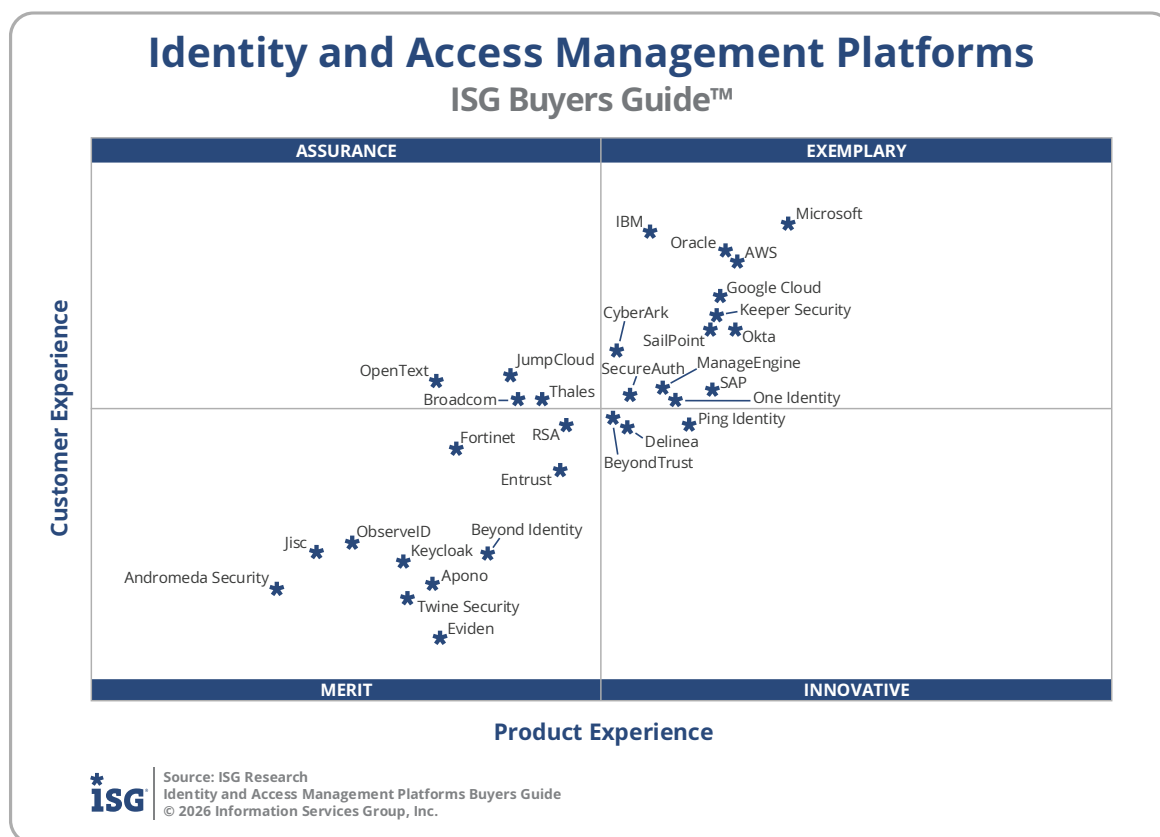
Providers	Grade	Performance
Microsoft	A	Leader 89.6%
AWS	A-	Leader 85.9%
Oracle	A-	Leader 85.4%
Okta	A-	84.5%
Google Cloud	A-	84.2%
Keeper Security	A-	83.6%
SailPoint	A-	83.3%
SAP	A-	81.8%
IBM	A-	81.4%
Ping Identity	B++	80.1%
One Identity	B++	79.5%
ManageEngine	B++	79.0%
SecureAuth	B++	77.3%
CyberArk	B++	77.2%
Delinea	B++	76.4%
BeyondTrust	B++	75.8%
RSA	B+	73.0%
Thales	B+	72.0%
Entrust	B+	71.8%
JumpCloud	B+	70.8%
Broadcom	B+	70.6%
OpenText	B	66.2%
Fortinet	B	66.2%
Beyond Identity	B	65.9%
Apono	B-	62.3%
Eviden	B-	61.3%
Keycloak	B-	61.1%
Twine Security	B-	60.5%
ObserveID	B-	58.4%
Jisc	C++	56.2%
Andromeda Security	C++	53.3%



Source: ISG Research
Identity and Access Management Platforms Buyers Guide
© 2026 Information Services Group, Inc.



The research categorizes and rates software providers into one of four categories: Assurance, Exemplary, Merit or Innovative. Placement represents the software providers' weighted performance in meeting the requirements of Product and Customer Experience.



Exemplary: This rating (upper right) applies to those providers that performed above the median in Product and Customer Experience requirements. The providers rated Exemplary are: AWS, CyberArk, Google Cloud, IBM, Keeper Security, ManageEngine, Microsoft, Okta, One Identity, Oracle, SailPoint, SAP and SecureAuth.

Innovative: This rating (lower right) applies to those that performed above median in Product Experience but not in Customer Experience. The providers rated Innovative are: BeyondTrust, Delinea and Ping Identity.

Assurance: This rating (upper left) applies to those that performed above median in Customer Experience but not in Product Experience. The providers rated Assurance are: Broadcom, JumpCloud, OpenText and Thales.

Merit: This rating (lower left) applies to those that did not surpass the median in Customer or Product Experience. The providers rated Merit are: Andromeda Security, Apono, Beyond Identity, Entrust, Eviden, Fortinet, Jisc, Keycloak, ObserveID, RSA and Twine Security.



We advise enterprises to use this research as a supplement to their own evaluations, recognizing that ratings or rankings are not the sole representation of a provider's value nor do they indicate universal suitability of a set of products.

Product Experience

The process of researching products to address an enterprise's needs should be comprehensive, evaluating specific capabilities and the underlying platform of the product. Our evaluation of the Product Experience examines the lifecycle of onboarding, configuration, operations, usage and maintenance. Too often, provider assessments focus on market execution and future vision rather than the full product.

Product Experience accounted for 80% of the overall rating. The subcategory weighting within Product Experience was 50% for Capability and 30% for Platform. Microsoft, AWS and Okta were designated Product Experience Leaders.

IAM Platforms

Product Experience

Providers	Grade	Performance
Microsoft	A	Leader 71.3%
AWS	A-	Leader 68.4%
Okta	A-	Leader 68.2%
Oracle	A-	67.7%
Google Cloud	A-	67.3%
Keeper Security	A-	67.1%
SailPoint	A-	66.9%
SAP	A-	66.7%
Ping Identity	A-	65.6%
One Identity	B++	64.6%
ManageEngine	B++	63.8%
IBM	B++	63.3%
SecureAuth	B++	62.2%
Delinea	B++	62.0%
CyberArk	B++	61.4%
BeyondTrust	B++	61.1%
RSA	B+	58.5%
Entrust	B+	58.1%
Thales	B+	57.1%
Broadcom	B+	55.7%
JumpCloud	B+	55.3%
Beyond Identity	B	53.8%
Fortinet	B	52.1%
Eviden	B	51.2%
OpenText	B	51.0%
Apono	B	50.8%
Twine Security	B-	49.3%
Keycloak	B-	49.1%
Okta	B-	46.1%
Jisc	C++	44.1%
Andromeda Security	C++	41.9%



Source: ISG Research
Identity and Access Management Platforms Buyers Guide
© 2026 Information Services Group, Inc.



Capability of the Product

The Capability criteria assess products and features across a broad range of IAM capabilities that support access management and governance, use of artificial intelligence and machine learning, APIs and application connector integration, auditing and reporting, identity verification, multifactor authentication, role-based access control, self-service functionality, user provisioning and migration to managed service environments.

This evaluation spans 39 function points across 14 sections and carries a weighting of 50% in the overall rating. Microsoft, Okta and Ping Identity are the Leaders in this category.

The Capability component of our grading provides an evaluation framework for enterprises. Software providers with greater breadth and depth and those that support the full set of requirements for this Buyers Guide fared better.

IAM Platforms Capability

Providers	Grade	Performance
Microsoft	A	Leader 93.5%
Okta	A	Leader 91.4%
Ping Identity	A	Leader 90.7%
Oracle	A	89.7%
AWS	A	87.7%
SailPoint	A	87.7%
Google Cloud	A-	87.3%
Keeper Security	A-	85.4%
IBM	A-	84.9%
SAP	A-	84.9%
Entrust	A-	84.7%
CyberArk	A-	84.6%
ManageEngine	A-	83.1%
One Identity	A-	81.6%
BeyondTrust	A-	81.5%
Delinea	B++	78.7%
RSA	B+	74.4%
Thales	B+	74.3%
JumpCloud	B+	73.9%
SecureAuth	B+	73.3%
Beyond Identity	B+	72.7%
Broadcom	B+	71.5%
Twine Security	B+	71.4%
Eviden	B+	71.4%
Fortinet	B	67.4%
Keycloak	B	66.7%
Apono	B-	61.5%
OpenText	B-	59.4%
ObserveID	C++	53.5%
Andromeda Security	C++	50.7%
Jisc	C+	49.4%



Source: ISG Research
Identity and Access Management Platforms Buyers Guide
© 2026 Information Services Group, Inc.



Platform of the Product

The Platform category in the ISG Buyers Guide™ evaluates the underlying components of a platform and examines how well a software product meets enterprise needs across business and IT. The category examines specific requirements for adaptability, manageability, reliability and usability.

Adaptability measures a product's ability to be configured and integrated into enterprise environments, while manageability focuses on governance, security and compliance. Reliability considers performance and scalability across environments, and usability assesses how intuitive and accessible the product is through design, AI use and ongoing provider investment.

ISG Research evaluated 16 function points in five sections to assess the full scope of platform capabilities. The research weights Platform at 30% of the overall rating. SecureAuth, Microsoft and AWS are the Leaders in this category.

Platform is an essential evaluation category as it indicates the strength and resilience of a software provider's product architecture. A well-designed platform ensures secure and compliant operations, dependable scalability and uptime, and a unified, intuitive experience for a range of usage personas. It also reflects the provider's capacity to support deployment models while maintaining flexibility to meet enterprise demands.

Software providers that performed best in the Platform category have support for the breadth and depth of needs across business and IT, supporting adaptability, manageability, reliability and usability. Providers with lower performance were challenged in one or more of these areas or did not demonstrate a cohesive, enterprise-grade approach.

IAM Platforms Platform

Providers	Grade	Performance
SecureAuth	A-	Leader 85.2%
Microsoft	A-	Leader 82.0%
AWS	A-	Leader 81.6%
Keeper Security	A-	81.5%
SAP	B++	80.9%
One Identity	B++	79.2%
Google Cloud	B++	79.0%
SailPoint	B++	76.7%
Oracle	B++	76.0%
Delinea	B++	75.3%
Okta	B++	75.1%
ManageEngine	B+	74.2%
OpenText	B+	70.9%
RSA	B+	70.9%
IBM	B+	69.4%
BeyondTrust	B	67.8%
Ping Identity	B	67.4%
Apono	B	66.7%
Broadcom	B	66.6%
Thales	B	66.5%
ObserveID	B	64.6%
Jisc	B	64.5%
CyberArk	B	63.6%
Fortinet	B-	61.5%
JumpCloud	B-	61.3%
Beyond Identity	B-	58.1%
Andromeda Security	C++	54.9%
Keycloak	C++	52.7%
Entrust	C++	52.6%
Eviden	C++	51.7%
Twine Security	C+	45.5%



Source: ISG Research
Identity and Access Management Platforms Buyers Guide
© 2026 Information Services Group, Inc.



Customer Experience

The importance of a customer relationship with a software provider is essential to the actual success of the products and technology. The evaluation of the Customer Experience and the entire lifecycle an enterprise has with its software provider is critical to ensuring satisfaction with that provider. The ISG Buyers Guide™ examines a software provider's customer commitment, viability, customer success, sales and onboarding, product roadmap, and partner and support services. The Customer Experience category also examines TCO/ROI and how well a software provider demonstrates the product's overall value, costs and benefits, including the tools and resources available to evaluate these factors.

The research results in Customer Experience account for 20% of the full 100% index, and represent the underlying provider validation and TCO/ROI requirements as they relate to the framework of commitment and value to the software provider-customer relationship.

The software providers that ranked the highest in the Customer Experience category are Microsoft, IBM and Oracle. These category Leaders best communicate commitment and dedication to customer needs.

Software providers that did not perform well in this category did not provide sufficient information to demonstrate success or articulate a commitment to customer experience. Partnering with a software provider requires continuous investment, so a holistic evaluation must include examination of the customer experience by providers.

IAM Platforms Customer Experience

Providers	Grade	Performance
Microsoft	A	Leader 18.3%
IBM	A	Leader 18.1%
Oracle	A	Leader 17.8%
AWS	A	17.6%
Google Cloud	A-	16.9%
Keeper Security	A-	16.5%
SailPoint	A-	16.4%
Okta	A-	16.3%
CyberArk	B++	15.8%
JumpCloud	B++	15.4%
OpenText	B++	15.3%
ManageEngine	B++	15.2%
SAP	B++	15.1%
SecureAuth	B++	15.1%
One Identity	B+	15.0%
Thales	B+	14.9%
Broadcom	B+	14.9%
BeyondTrust	B+	14.7%
RSA	B+	14.5%
Ping Identity	B+	14.5%
Delinea	B+	14.5%
Fortinet	B+	14.1%
Entrust	B	13.7%
Okta	B-	12.3%
Jisc	B-	12.1%
Beyond Identity	B-	12.1%
Keycloak	B-	11.9%
Apono	B-	11.5%
Andromeda Security	B-	11.4%
Twine Security	C++	11.2%
Eviden	C++	10.1%



Source: ISG Research
Identity and Access Management Platforms Buyers Guide
© 2026 Information Services Group, Inc.



Keeper Security

Company and Product Profile

KeeperPAM; released June 2026

"KeeperPAM manages access to servers, web applications, databases, and workloads. The cloud native zero knowledge platform combines enterprise password management, secrets management, connection management, zero trust network access, and remote browser isolation. These capabilities are delivered through a unified interface." – Keeper Security

Summary

Our analysis classified Keeper Security as Exemplary, receiving an overall grade of A- with an 83.0% performance. Keeper Security's best grouped results came in Product Experience with an 83.1% performance and an A- grade. In Customer Experience, Keeper Security also received an A- grade with an 82.7% performance.

Strengths

The KeeperPAM platform demonstrated strengths in Platform and Customer Experience. In Platforms, it performed well in configurability and functionality to manage performance and scalability. Its Customer Experience functionality rated highly for available support for employees or prospects to calculate TCO/ROI.

Challenges

Keeper Security could strengthen its position further with how it demonstrates financial viability through scale and growth and customer durability and diversification. Capabilities could be strengthened with more industry-specific examples of connectors and partner applications for its App Marketplace and publishing updates on a regular cadence.

IAM Platforms		
Keeper Security		
Exemplary Provider		
Category	Performance	Grade
Overall	83.0%	A-
Product	83.1%	A-
Capability	85.4%	A-
Platform	81.5%	A-
Customer	82.7%	A-

 Source: ISG Research
Identity and Access Management Platforms Buyers Guide
© 2026 Information Services Group, Inc.



Software Provider Inclusion

For inclusion in the 2026 ISG Buyers Guide™ for Identity and Access Management Platforms, a software provider must be in good standing financially and ethically, have at least \$100 million in annual or projected revenue verified by independent sources and sell products and provide support in two or more of the following regions: North America, EU, UK and APAC. 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 past 12 months.

IAM software manages user identities and access permissions, ensuring appropriate access, regulatory compliance and enhanced security through advanced authentication and role-based controls.

The research is 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 contain 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 this research, we automatically evaluate that provider for inclusion.

We invited all software providers offering relevant products and meeting the inclusion requirements to participate in the evaluation process at no cost.

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 significantly impact classification and ratings, we recommend additional scrutiny when evaluating those providers.



Products Evaluated

Provider	Product Names	Version	Release Month/Year
Andromeda Security	Andromeda Platform	2026 release	June 2026
Apono	Cloud Privileged Access	2026 release	June 2026
AWS	AWS Identity and Access Management (specific to AWS services)	2026 release	July 2026
Beyond Identity	Secure Access Platform	2.112.1	June 2026
BeyondTrust	BeyondTrust Pathfinder Platform (Insights, Entitle, and Privileged Remote Access products)	2026 release	July 2026
Broadcom	Symantec Privileged Access Manager	4.3.1	May 2026
CyberArk	Privileged Access Manager	15.2	April 2026
Delinea	Identity Lifecycle Management	2026 release	April 2026
Entrust	Entrust Identity as a Service (IDaaS)	5.46.1	June 2026
Eviden	Evidian IAM (SaaS version)	2026 release	April 2026
Fortinet	FortiAuthenticator Cloud	26.2.a	June 2026
Google Cloud	Google Cloud Identity	2026 release	April 2026
IBM	IBM Verify Workforce Identity	2026 release	July 2026
Jisc	OpenAthens	2026 release	June 2026
JumpCloud	JumpCloud Platform	2.147.7	July 2026
Keeper Security	KeeperPAM	2026 release	June 2026
Keycloak	Keycloak IAM	26.6.4	June 2026



Provider	Product Names	Version	Release Month/Year
ManageEngine	Identity 360	2026 release	May 2026
Microsoft	Entra ID	2026 release	June 2026
Okta	Okta Identity Platform	3.7	June 2026
Okta	Workforce Identity	2026.07.2	July 2026
One Identity	OneLogin Workforce Identity	2026 release	June 2026
OpenText	OpenText Access Manager (NetIQ)	CE 26.2 (v5.1.3)	June 2026
Oracle	OCI Identity and Access Management	2026 release	July 2026
Ping Identity	PingOne for Workforce	2026 release	July 2026
RSA	SecurID	8.9	January 2026
SailPoint	Identity Security Cloud	2026 release	March 2026
SAP	SAP Cloud Identity Services (part of Financial Management)	Q2 2026 release	June 2026
SecureAuth	SecureAuth Workforce Identity Management	26.0.0	June 2026
Thales	SafeNet Trusted Access	2026 release	June 2026
Twine Security	Twine Security IAM AI Digital Employee	2026 release	February 2026



Buyers Guide Overview

ISG Research has conducted market research for over two decades across vertical industries, business applications, AI and IT. We have designed the ISG Buyers Guide™ to provide a balanced perspective on software providers and products, rooted in an understanding of business and IT requirements. Utilizing our research methodology and decades of experience,

“

ISG Research has designed the Buyers Guide to provide a balanced perspective on software providers, rooted in an understanding of business and IT requirements.

our Buyers Guide is an effective tool for assessing and selecting software providers and products. The findings of this research provide a comprehensive approach to rating software providers and ranking how each meets specific product and customer experience requirements.

This ISG Buyers Guide™ is the distillation of continuous market and product research. It is an assessment of how well software providers' offerings address enterprises' requirements. The Value Index methodology is structured to support a request for information (RFI) or request for proposal (RFP) process by incorporating all criteria needed to evaluate, select, utilize and maintain relationships with software providers. The ISG Buyers Guide™ evaluates customer experience and product experience across capability and platform criteria.

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. It can ensure the best long-term relationship and value achieved from a resource and financial investment. We believe it is important to take a comprehensive, research-based approach, since the wrong choice of software can raise the total cost of ownership, lower the return on investment and hamper an enterprise's ability to reach its potential. In addition, this approach can reduce the project's development and deployment time and eliminate the risk of relying on opinions or historical biases.

ISG Research believes that an objective review of existing and potential new software providers and products is a critical strategy for the adoption and implementation of enterprise software. An enterprise's review should include an analysis of both what is possible and what is relevant. We urge enterprises to conduct a thorough evaluation, and we offer this ISG Buyers Guide™ as both the results of our in-depth analysis of these providers and as an evaluation methodology.



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 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 and research, in-depth knowledge and governance of provider ecosystems, and the expertise of its 1,500 professionals worldwide working together to help clients maximize the value of their technology investments.

About the Authors



Jeff Orr

Director of Research, IT and Technologies

Jeff Orr leads the research and advisory for the CIO and IT Leader Research Practice at ISG, with a focus on IT modernization and transformation. Jeff's coverage spans AppDev/DevOps and business platforms, cloud computing, cybersecurity, intelligent automation and IT Management across the enterprise.



David Menninger

Executive Director, Software Research and Distinguished Analyst

David Menninger leads the overall team for software research and advisory, supporting IT and expertise in AI software at ISG. With over three decades of experience in enterprise software, Dave's leadership has advanced digital transformation with information and insights for enterprises around the world.