

SIEM Buyers Guide

Software Provider and Product Assessment



EXECUTIVE
SUMMARY

***ISG** Research



SIEM

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 defines Security Information and Event Management (SIEM) as the backbone of an enterprise's security operations (SecOps), delivering a comprehensive approach for collecting, aggregating and analyzing security data from multiple sources. By continuously aggregating logs and security events from various network devices, servers, endpoints and applications,

“

By continuously aggregating logs and security events from various network devices, servers, endpoints and applications, SIEM platforms provide real-time visibility into security incidents and anomalies.

SIEM platforms provide real-time visibility into security incidents and anomalies. This capability is critical for identifying potential threats and breaches across the IT estate, allowing enterprises to respond swiftly and effectively.

SIEM software employs sophisticated analytics, including correlation rules, machine learning (ML) and threat intelligence feeds, enabling security teams to detect patterns of malicious behavior. The platform's centralized nature facilitates detailed reporting, dashboard visualization and alerts, empowering security personnel with actionable insights. SIEM is not only vital for threat detection but also helps in forensic investigations, providing a historical view of security events for understanding and remediating incidents.

Moreover, SIEM plays a crucial role in maintaining compliance with regulations such as GDPR and HIPAA by providing necessary audit trails and security controls. As enterprises face increasingly complex

security challenges, an effective SIEM implementation enhances their ability to manage risks proactively. By encompassing incident detection, response and compliance reporting, SIEM



platforms are essential for any enterprise looking to strengthen its cybersecurity framework and mitigate the impacts of security incidents.

ISG asserts that through 2027, 7 in 10 enterprises will address increasingly sophisticated cyber threats, improve security posture and reduce threat response times using SIEM software to gain real-time visibility across the entire IT infrastructure.

Security strategies incorporating SIEM play a crucial role in bolstering an enterprise's security posture by providing comprehensive visibility into security events across the IT environment. By aggregating and analyzing data logs from diverse sources, SIEM enables enterprises to identify potential threats in real time, allowing for immediate response and mitigation. This proactive threat detection is essential for minimizing vulnerabilities and enhancing the overall security framework of the enterprise.

Cybersecurity
Market Assertion

Through 2027, 7 in 10 enterprises will address increasingly sophisticated cyber threats, improve security posture and reduce threat response times using SIEM software to gain real-time visibility across the entire IT infrastructure.

Jeff Orr
Director of Research, Technology Research

ISG Research

SIEM not only facilitates incident detection and response but also supports regulatory compliance by delivering compliance-reporting capabilities. Enterprises can demonstrate adherence to industry standards by leveraging the audit trails and reports generated by SIEM systems. Moreover, the centralized nature of SIEM improves collaboration among security teams, as they can access real-time data and insights for informed decision-making. This degree of awareness also enables security personnel to focus on high-priority threats rather than being overwhelmed by false alarms.

In aligning security practices with business objectives, SIEM fosters resilience against cyber threats and enhances the enterprise's reputation. By reducing response times and improving incident management efficiency, enterprises can continue their operations with minimal disruption, ensuring business continuity. Ultimately, SIEM serves as a foundational element for a robust cybersecurity strategy, helping enterprises safeguard their assets while supporting their long-term business goals.

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 boost the capabilities of security personnel by offering enhanced threat detection, automated incident response and anomaly identification using SIEM systems. AI algorithms can process vast amounts of security data to identify patterns and correlations that may signify a cyber threat, effectively reducing alert fatigue for security teams. By utilizing natural language processing (NLP), GenAI can automate the investigation of security alerts, generating detailed narratives and remediation recommendations for potential incidents. Furthermore, ML models can continuously learn from historical incidents, improving detection accuracy over time. By empowering security personnel with actionable insights and streamlining incident response workflows, GenAI can enhance overall efficiency and effectiveness in managing SecOps.

Looking ahead, the potential integration of agentic AI functionalities into SIEM software could further revolutionize cybersecurity management by enabling systems to not only analyze data



The potential integration of agentic AI functionalities into SIEM software could further revolutionize cybersecurity management by enabling systems to not only analyze data but also autonomously take actions in response to threats.

but also autonomously take actions in response to threats. In this future scenario, agentic AI could dynamically adjust network security measures, implement automatic responses to detected vulnerabilities and even initiate investigations without human intervention. This would allow enterprises to proactively manage threats, shifting the role of security personnel from reactively addressing incidents to strategically overseeing intelligent systems, thereby enhancing organizational resilience against evolving cyber threats.

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 IAM, EDR and Data Recovery software.

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.



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 SIEM evaluates products based on a variety of capabilities including compliance functionality, compliance reporting, dashboard visualization, data privacy, GenAI and ML, incident response, log management, observability, SIEM deployment models, SOAR support, threat detection, threat intelligence communities, user behavior analytics, and the opportunity to evolve use of the SIEM software over time as a managed service. 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 SIEM: Devo Technology, Elastic, Exabeam, Fortinet, Fortra, Google Cloud, ManageEngine, Microsoft, NetWitness, OpenText, Rapid7, Securonix, SolarWinds, Splunk and Sumo Logic.



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



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.

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.

The ISG Buyers Guide™ for SIEM 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 SIEM 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 SIEM 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 SIEM 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 SIEM 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 SIEM 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

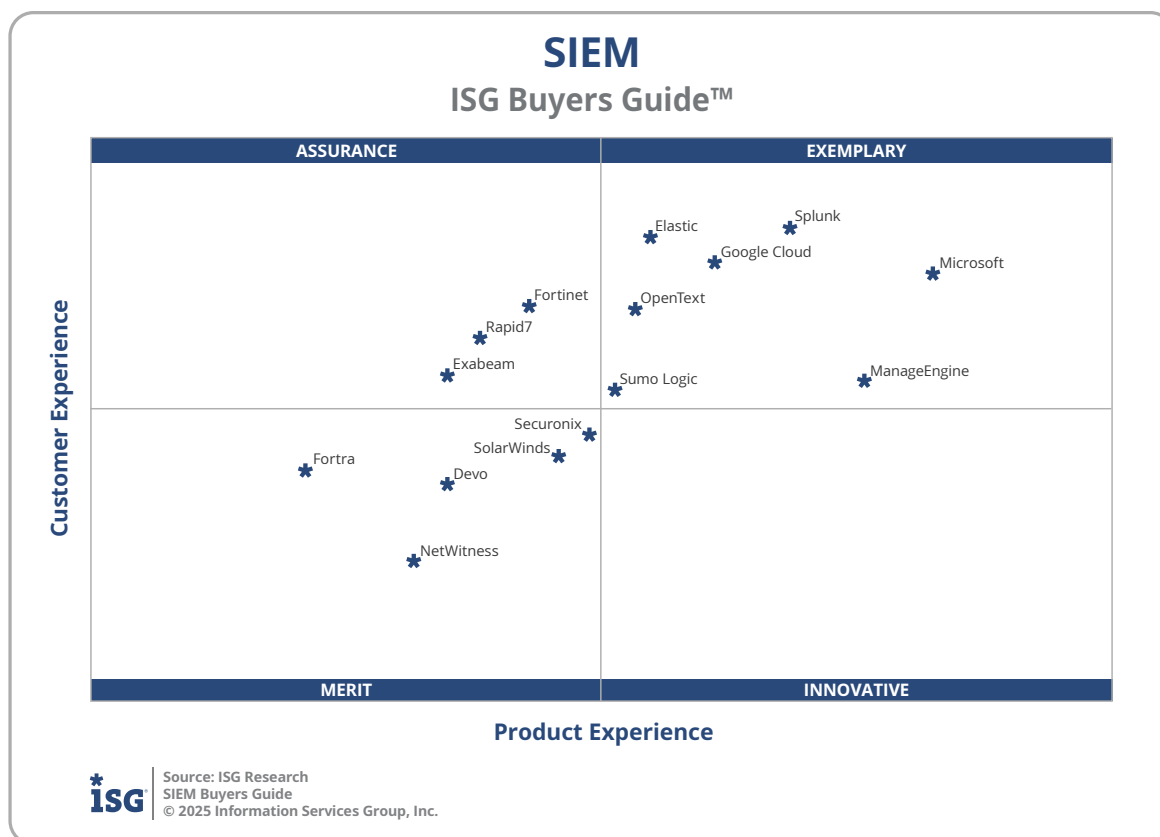
The research finds Microsoft atop the list, followed by Splunk and ManageEngine. Companies that place in the top three of a category earn the designation of Leader. Microsoft has done so in six categories; Splunk in five; ManageEngine in four; Google Cloud in three; Elastic in two; and Securonix in one 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.

SIEM Overall			
Providers	Grade	Performance	
Microsoft	B+	Leader	73.5%
Splunk	B+	Leader	71.3%
ManageEngine	B+	Leader	69.6%
Google Cloud	B		67.7%
Elastic	B		67.4%
OpenText	B		64.1%
Sumo Logic	B-		61.1%
SolarWinds	B-		60.8%
Fortinet	B-		60.0%
Securonix	B-		58.2%
Rapid7	B-		57.7%
Exabeam	B-		56.6%
Devo	C++		53.6%
NetWitness	C++		52.4%
Fortra	C++		50.8%

 Source: ISG Research
SIEM Buyers Guide
© 2025 Information Services Group, Inc.

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: Elastic, Google Cloud, ManageEngine, Microsoft, OpenText, Splunk and Sumo Logic.

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. No providers were rated Innovative in this Buyers Guide.

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: Exabeam, Fortinet and Rapid7.

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: Devo Technology, Fortra, NetWitness, Securonix and SolarWinds.



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 SIEM, 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.

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: Adaptability (8%), Capability (45%), Manageability (9%), Reliability (9%) and Usability (9%). This weighting impacted the resulting overall ratings in this research. Microsoft, ManageEngine and Splunk were designated Product Experience Leaders.

SIEM Product Experience

Providers	Grade	Performance
Microsoft	B+	Leader 57.4%
ManageEngine	B+	Leader 55.6%
Splunk	B	Leader 53.4%
Google Cloud	B	51.2%
Elastic	B-	49.3%
OpenText	B-	48.9%
Sumo Logic	B-	48.2%
Securonix	B-	47.4%
SolarWinds	B-	46.6%
Fortinet	B-	45.9%
Rapid7	C++	44.3%
Devo	C++	43.3%
Exabeam	C++	43.3%
NetWitness	C++	42.3%
Fortra	C+	39.1%



Source: ISG Research
SIEM Buyers Guide
© 2025 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 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 Splunk, Elastic and Google Cloud. These category Leaders best communicate commitment and dedication to customer needs.

SIEM Customer Experience			
Providers	Grade	Performance	
Splunk	B++	Leader	15.8%
Elastic	B++	Leader	15.6%
Google Cloud	B++	Leader	15.2%
Microsoft	B+		15.0%
Fortinet	B+		14.4%
OpenText	B+		14.3%
Rapid7	B+		13.8%
Exabeam	B		13.1%
ManageEngine	B		13.0%
Sumo Logic	B		12.9%
Securonix	B-		12.1%
SolarWinds	B-		11.7%
Fortra	B-		11.4%
Devo	C++		11.2%
NetWitness	C+		9.8%

 Source: ISG Research
SIEM Buyers Guide
© 2025 Information Services Group, Inc.

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 SIEM 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 SIEM 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
Devo Technology	Devo Security Operations	Platform 8.16.3	May 2025
Elastic	Elastic Security	9.0.3	May 2025
Exabeam	New-Scale SIEM	June Release	June 2025
Fortinet	FortiSIEM	7.3.2	May 2025
Fortra	Event Manager	6.9	April 2024
Google Cloud	Google Security Operations SIEM	June 04 Release	June 2025
ManageEngine	Log360	Build 5555	June 2025
Microsoft	Microsoft Sentinel	June Update	June 2025
NetWitness	NetWitness Cloud SIEM	12.5	January 2025
OpenText	OpenText Enterprise Security Manager	7.8	August 2024
Rapid7	InsightIDR	20250131	January 2025
Securonix	Next-Gen SIEM	6.4 May R1 2025	May 2025
SolarWinds	SolarWinds Security Event Manager	2025.2	April 2025
Splunk	Splunk Enterprise Security	8.1.0	June 2025
Sumo Logic	Sumo Logic Cloud SIEM	12.0	June 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 offering SIEM functionality as part of a larger software platform, instead of a standalone application, were not included in this evaluation.

Provider	Product	Revenues > \$100 Million	100+ Employees	Standalone Application
Coralogix	Snowbit SIEM	No	Yes	Yes
DNIF	Hypercloud	No	No	Yes
Gurukul	Gurukul Next-Gen SIEM	No	Yes	Yes
Huawei	SecMaster	Yes	Yes	No
LogPoint	LogPoint SIEM	No	Yes	Yes
Logz.io	Logz.io SIEM	No	Yes	Yes
OSSEC	Atomic OSSEC	No	No	Yes
Palo Alto Networks	Cortex XSIAM	Yes	Yes	No
QAX	QAX SIEM	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.