

Private/Hybrid Cloud – Data Center Solutions

Resiliency Platforms

A research report comparing vendor strengths,
challenges and competitive differentiators

Executive Summary 03

Provider Positioning 06

Introduction

Definition 10

Scope of Report 11

Provider Classifications 12

Appendix

Methodology & Team 21

Author & Editor Biographies 22

About Our Company & Research 24

Resiliency Platforms 13 – 19

Who Should Read This Section 14

Quadrant 15

Definition & Eligibility Criteria 16

Observations 17

Provider Profile 19

Report Author: Shashank Rajmane

Enterprises are moving away from cloud-first strategies toward a balanced hybrid operating model

This ISG Provider Lens® study evaluates software vendors and platform providers that support enterprise hybrid cloud operations and resiliency strategies, helping buyers assess vendors based on governance, operational maturity, automation, financial accountability and cyber recovery readiness across increasingly distributed IT estates. It presents an independent benchmarking of leading vendors delivering private hybrid cloud and data center (PHCDC) solutions globally. It is designed to help enterprise buyers choose vendors capable of managing complex hybrid cloud environments and enabling resiliency strategies to run business operations without disruptions. This study assesses how effectively vendors align their platforms, operating models and support services to evolving enterprise needs.

Market Context

The global hybrid cloud solutions market is entering a new phase in which enterprises are prioritizing operational control, cyber resilience, sovereign cloud readiness and, most importantly, AI-enabled infrastructure modernization. Enterprises are moving away from *cloud-first* strategies toward more balanced hybrid operating models that combine public cloud, private cloud, colocation, edge and sovereign environments. ISG research indicates that over 80 percent of enterprises are revising their cloud strategies to accommodate AI workloads, operational resilience and governance requirements.

AI is emerging as one of the most significant drivers of infrastructure transformation. Hyperscaler and enterprise investments in AI infrastructure continue to accelerate globally, driving the demand for higher-density compute, GPU-enabled architectures, distributed data platforms and hybrid AI operating models. Sovereign cloud markets are projected to grow rapidly as enterprises and governments seek increased control over data locality and AI governance. Sovereignty has evolved

AIOps is rapidly
evolving from alert
correlation to **agentic**
and **autonomous**
operational
intelligence.



Executive Summary

from a regional compliance concern into a strategic operating principle that influences infrastructure placement, cloud selection, AI deployment and resiliency design. The market is also witnessing a strong convergence between hybrid cloud operations and resiliency platforms. Vendors are embedding FinOps, AIOps, observability, disaster recovery (DR), cyber vaulting and automated recovery orchestration into unified operational control planes. This convergence is shifting the market away from isolated infrastructure tools toward platform-oriented operating models designed to improve governance, automation, operational efficiency and recoverability across complex hybrid environments.

Enterprise Priorities

Enterprise buyers are increasingly prioritizing operational consistency and resilience across highly heterogeneous environments. Hybrid cloud adoption continues to grow because organizations require flexibility in workload placement while maintaining control over data, compliance, performance and cost. As hybrid estates expand, enterprises are shifting their focus from infrastructure provisioning toward

operational governance. Buyers increasingly expect hybrid cloud management platforms (HCMPs) to provide unified observability, topology-aware AIOps, automation, policy enforcement and integrated FinOps capabilities. Platforms are expected to correlate infrastructure, applications, services, costs and workflows into a single operational context rather than function as isolated monitoring or provisioning tools.

AI-driven operations are becoming a key enterprise priority. Organizations are adopting platforms that reduce alert fatigue, accelerate root cause analysis (RCA) and automate remediation workflows. However, enterprises remain cautious about uncontrolled automation and increasingly demand governed AI-assisted operations with explainability, policy controls and human oversight, particularly in large organizations where operational errors can create cascading business impact across distributed environments. Financial accountability is another growing priority. Enterprises are moving beyond basic cloud cost reporting toward integrated FinOps models that combine cost governance,

workload optimization, licensing intelligence, and showback and chargeback across hybrid environments. The emergence of AI workloads and GPU-intensive infrastructure is further increasing the demand for deeper cost transparency and optimization across private cloud, Kubernetes, edge and sovereign cloud environments.

Cyber resilience has also become a board-level requirement. Buyers increasingly expect resiliency platforms to support immutable backups, air-gapped vaulting, threat-aware recovery, cleanroom recovery validation, identity resilience and orchestrated DR. Evaluation criteria for backup platforms now extend beyond recovery speed to include the ability to restore trusted and validated environments after cyber incidents. At the same time, enterprises are becoming more selective about platform consolidation. Many organizations are attempting to reduce operational silos and simplify management layers by favoring vendors that can unify ITSM, AIOps, automation, FinOps and resiliency capabilities into coherent operational frameworks. However, buyers remain cautious

about excessive vendor lock-in, ecosystem dependency and operational complexity.

Vendor Dynamics

Vendors in the hybrid cloud operations market segment are responding by repositioning themselves from infrastructure management or backup vendors into broader platform-oriented operational and resiliency providers. Across the HCMP segment, vendors are strengthening unified control planes that combine observability, automation, orchestration, policy governance and financial management into integrated operational models. Vendors are embedding AI-driven RCA, remediation guidance, topology-aware automation and policy-led workflows into hybrid operations platforms. Increasingly, these platforms are integrating OpenTelemetry, service-centric dependency mapping and AI-assisted runbooks to reduce manual operations overhead and improve mean time to recovery (MTTR). FinOps capabilities are also expanding significantly. Vendors such as are also seen integrating budgeting, anomaly detection, Kubernetes optimization, cloud commitment management and chargeback and showback into operational



Executive Summary

workflows. This expansion reflects enterprise demand for financial governance that extends beyond public cloud into private cloud, SaaS, Kubernetes and AI-driven infrastructure environments.

In the resiliency segment, vendors are increasingly positioning themselves as cyber resilience platforms rather than traditional backup providers. Solutions from vendors are increasingly combining clean recovery validation, cyber vaulting, immutable storage, threat analytics, orchestrated recovery and identity resilience into integrated offerings. Vendors are also expanding cloud-native recovery capabilities through recovery as code, application-aware orchestration and continuous readiness testing. Also, infrastructure-centric providers are tightly aligning operations and resiliency with their infrastructure portfolios. In contrast, software-led vendors are focusing on broader operational abstraction, automation and multi-environment governance. Despite significant innovation, complexity remains a common challenge across the market. Many platforms still depend on strong configuration management database

(CMDB) maturity, accurate discovery, extensive integrations and ecosystem alignment to deliver full value. Enterprises, therefore, continue to evaluate providers on innovation, as well as on operational simplicity, interoperability and long-term architectural flexibility.

Future Outlook

The PHCDC solutions market will continue evolving toward unified operational and resiliency platforms that combine AI-assisted operations, policy-led automation, cyber resilience and financial governance into integrated hybrid operating models. The market is expected to shift further toward *platformized operations* where infrastructure management, observability, FinOps, security and recovery will be increasingly interconnected through shared operational intelligence. Sovereign cloud and sovereign AI will become increasingly important strategic drivers over the next several years. Enterprises will place increased emphasis on data residency, infrastructure control, regional compliance and operational independence when selecting vendors and designing hybrid cloud strategies, particularly in highly regulated

industries and global organizations managing distributed data and AI environments.

AI-enabled operations will also mature rapidly, but enterprises are expected to prioritize governed autonomy over fully autonomous operations. Buyers will increasingly favor vendors that can demonstrate explainable AI, policy-based remediation, operational auditability and controlled automation rather than purely autonomous decision-making. In the resiliency space, cyber recovery validation and identity resilience will become core enterprise requirements rather than premium capabilities. Enterprises will increasingly evaluate providers on their ability to deliver trusted recovery, operational continuity and validated recoverability across hybrid and cloud-native environments.

Ultimately, the PHCDC solutions market is moving toward a future in which operational governance, resilience, financial accountability and sovereignty are inseparable components of enterprise hybrid cloud strategy. Enterprises that align these capabilities through integrated platforms and disciplined operating models

will be better positioned to manage complexity, improve agility and support long-term digital transformation initiatives.

The market is evolving due to increased demand for AI infrastructure, hybrid cloud operational complexity, cyber resilience requirements and sovereign cloud mandates. At the same time, enterprises are seeking to reduce overdependence on hyperscaler-centric architectures. Challenges such as geopolitical concerns, data residency requirements and rising cloud costs are reinforcing demand for hybrid operating models that provide improved control and flexibility.





Provider Positioning

Page 1 of 4

	Hybrid Cloud Operations Platforms (AIOps enabled)	Resiliency Platforms
Abiquo	Contender	Not In
Acronis	Not In	Product Challenger
Arcserve	Not In	Contender
Asigra	Not In	Contender
Axcient	Not In	Product Challenger
BMC Software	Leader	Not In
Broadcom (VMware)	Leader	Leader
Centilytics	Contender	Not In
Cisco	Contender	Not In
CloudBolt Software	Leader	Not In





Provider Positioning

Page 2 of 4

	Hybrid Cloud Operations Platforms (AIOps enabled)	Resiliency Platforms
CloudSphere	Contender	Not In
Cohesity	Not In	Leader
Commvault	Not In	Leader
CoreStack	Rising Star ★	Not In
Datto	Not In	Contender
Dell Technologies	Product Challenger	Leader
Druva	Not In	Product Challenger
Emma	Product Challenger	Not In
Flexera	Leader	Not In
HCLSoftware	Leader	Not In





Provider Positioning

Page 3 of 4

	Hybrid Cloud Operations Platforms (AIOps enabled)	Resiliency Platforms
HPE	Leader	Leader
HYCU	Not In	Product Challenger
IBM	Leader	Product Challenger
ManageEngine	Product Challenger	Not In
N-able	Not In	Contender
NAKIVO	Not In	Product Challenger
NetApp	Not In	Product Challenger
Nutanix	Product Challenger	Not In
OpenText	Contender	Product Challenger
Quest Global	Not In	Contender





Provider Positioning

Page 4 of 4

	Hybrid Cloud Operations Platforms (AIOps enabled)	Resiliency Platforms
Redstor	Not In	Contender
Resolve Systems	Product Challenger	Not In
Rubrik	Not In	Leader
ScienceLogic	Market Challenger	Not In
SEP	Not In	Contender
ServiceNow	Leader	Not In
Unitrends	Not In	Product Challenger
UnityOne AI	Product Challenger	Not In
Veeam	Not In	Leader
Vembu Technologies	Not In	Contender



This study focuses on what ISG perceives as the most critical aspects of **Private/Hybrid Cloud – Data Center Solutions** in 2026.

Simplified Illustration Source: ISG 2026

Hybrid Cloud Operations Platforms (AIOps enabled)

Resiliency Platforms

Definition

The global software platforms market, enabling private and hybrid cloud environments, is expanding as enterprises modernize their digital foundations and pursue control, sovereignty and resilience. ISVs play a key role here, offering platforms with the orchestration, automation and governance capabilities needed to operate distributed private data centers, public clouds and sovereign cloud regions. The demand for sovereign-ready solutions is rising, mainly in Europe but also in regions where national data governance, digital autonomy and jurisdictional control have become a priority.

AI is accelerating this evolution, making AI- and ML-enabled platforms essential for managing complex distributed architectures, dynamic workloads and large-scale data flows. Modern hybrid cloud management, observability and cyber-resilient platforms now rely on AIOps-driven insights, predictive analytics and autonomous remediation for performance, optimized resource consumption and strong security postures. Concurrently, AI is driving a resurgence of edge computing, as organizations prefer data processing near the

sources for low latency, reduced storage costs and to process sensitive information within controlled environments.

Rising energy costs, data center capacity constraints and the growing power demands of AI workloads are making enterprises prioritize sustainability and evaluate ISVs on energy-efficient infrastructure utilization, granular consumption insights and carbon-aware workload placement. ISVs are moving toward productized, platform-based delivery models that enable consistent, scalable operations across environments. This study evaluates software vendors that underpin modern private, hybrid and sovereign cloud ecosystems with the required platforms, automation and resilience.



Scope of the Report

This ISG Provider Lens® quadrant report covers the following two quadrants for solutions: Hybrid Cloud Operations Platforms (AIOps enabled) and Resiliency Platforms.

This ISG Provider Lens® study offers IT decision-makers:

- Transparency on the strengths and weaknesses of relevant vendors
- A differentiated positioning of providers by segments (quadrants)
- Focus on the regional market

Our study serves as an important decision-making basis for positioning, key relationships and GTM considerations. ISG advisors and enterprise clients also use information from these reports to evaluate their current vendor relationships and potential engagements.

Provider Classifications

The provider position reflects the suitability of providers for a defined market segment (quadrant). Without further additions, the position always applies to all company sizes classes and industries. In case the service requirements from enterprise customers differ and the spectrum of providers operating in the local market is sufficiently wide, a further differentiation of the providers by performance is made according to the target group for products and services. In doing so, ISG either considers the industry requirements or the number of employees, as well as the corporate structures of customers and positions providers according to their focus area. As a result, ISG differentiates them, if necessary, into two client target groups that are defined as follows:

- **Midmarket:** Companies with 100 to 4,999 employees or revenues between \$20 million and \$999 million with central headquarters in the respective country, usually privately owned.

- **Large Accounts:** Multinational companies with more than 5,000 employees or revenue above \$1 billion, with activities worldwide and globally distributed decision-making structures.

The ISG Provider Lens® quadrants are created using an evaluation matrix containing four segments (Leader, Product & Market Challenger and Contender), and the providers are positioned accordingly. Each ISG Provider Lens® quadrant may include a service provider(s) which ISG believes has strong potential to move into the Leader quadrant. This type of provider can be classified as a Rising Star.

- **Number of providers in each quadrant:** ISG rates and positions the most relevant providers according to the scope of the report for each quadrant and limits the maximum of providers per quadrant to 25 (exceptions are possible).





Provider Classifications: Quadrant Key

Product Challengers offer a product and service portfolio that reflect excellent service and technology stacks. These providers and vendors deliver an unmatched broad and deep range of capabilities. They show evidence of investing to enhance their market presence and competitive strengths.

Contenders offer services and products meeting the evaluation criteria that qualifies them to be included in the IPL quadrant. These promising service providers or vendors show evidence of rapidly investing in products/ services and follow sensible market approach with a goal of becoming a Product or Market Challenger within 12 to 18 months.

Leaders have a comprehensive product and service offering, a strong market presence and established competitive position. The product portfolios and competitive strategies of Leaders are strongly positioned to win business in the markets covered by the study. The Leaders also represent innovative strength and competitive stability.

Market Challengers have a strong presence in the market and offer a significant edge over other vendors and providers based on competitive strength. Often, Market Challengers are the established and well-known vendors in the regions or vertical markets covered in the study.

★ **Rising Stars** have promising portfolios or the market experience to become a Leader, including the required roadmap and adequate focus on key market trends and customer requirements. Rising Stars also have excellent management and understanding of the local market in the studied region. These vendors and service providers give evidence of significant progress toward their goals in the last 12 months. ISG expects Rising Stars to reach the Leader quadrant within the next 12 to 24 months if they continue their delivery of above-average market impact and strength of innovation.

Not in means the service provider or vendor was not included in this quadrant. Among the possible reasons for this designation: ISG could not obtain enough information to position the company; the company does not provide the relevant service or solution as defined for each quadrant of a study; or the company did not meet the eligibility criteria for the study quadrant. Omission from the quadrant does not imply that the service provider or vendor does not offer or plan to offer this service or solution.





Resiliency Platforms

Who Should Read This Section

This report is valuable for vendors offering **resiliency platforms globally** to understand their market position and for enterprises looking to evaluate these vendors. In this quadrant, ISG highlights the current market positioning of these vendors and examines how each vendor addresses key global challenges.

IT and infrastructure leaders

Should read this report to evaluate resiliency platform vendors that strengthen continuity for private and hybrid data center environments. The comparison highlights capabilities that help design for disruption, reduce downtime and protect critical workloads and data, enabling the alignment of resilience investments with risk appetite, regulatory obligations and availability targets.

Software development and technology leaders

Should read this report to understand how resiliency platforms support application and data recovery across hybrid environments. It helps teams align architecture and engineering practices with recovery requirements, automate resilience testing and runbooks and restore modern application stacks predictably without slowing delivery velocity.

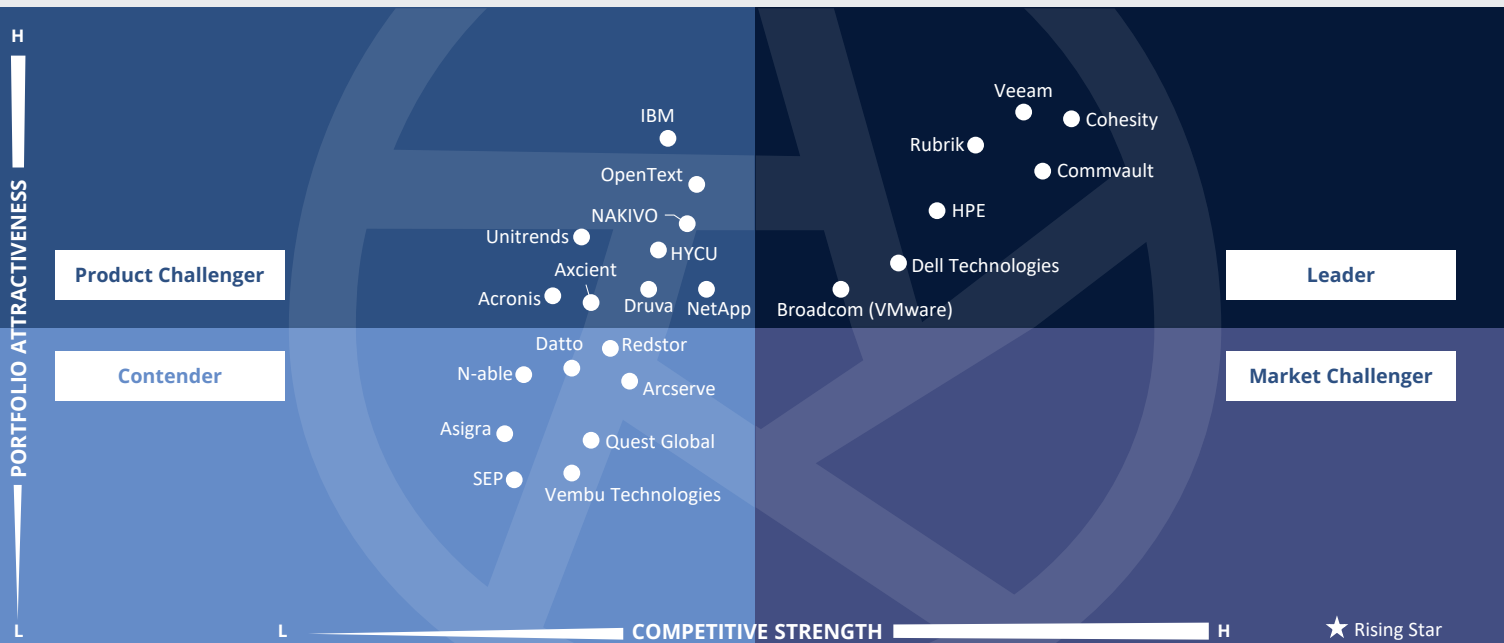
Sourcing, procurement and vendor management

Professionals should read this report to understand the global resiliency platform landscape and how vendors are differentiated based on delivery models, ecosystem fit and support coverage. The insights can enable informed vendor selection and contract negotiation around recovery commitments, service scope and governance, reducing continuity risk while optimizing cost and supplier accountability.



Private/Hybrid Cloud – Data Center Solutions Resiliency Platforms

Global 2026



This quadrant assesses software vendors offering robust resiliency platforms for **backup** and **DR** strategies across on-premises, public, private and **hybrid cloud** environments. These platforms are vital for maintaining **business continuity**.

Shashank Rajmane



Resiliency Platforms

Definition

This quadrant assesses independent solution vendors offering AI-powered resiliency platforms that support backup, disaster recovery (DR) and cyber resilience across on-premises, private, public, hybrid, edge cloud and SaaS environments. These platforms enable enterprises to maintain fault-tolerant operations by protecting data, applications and system states, thus ensuring business continuity during disruptions such as outages, performance degradation, cyber incidents or infrastructure failures. The platforms are delivered either as software licenses or as managed, platform-based services.

AI plays a central role in enhancing the effectiveness of these platforms; modern resiliency platforms use ML and advanced analytics to reduce fault detection time, identify clean and uncompromised recovery points, accelerate incident investigation, and support or automate recovery runbooks under definitive policy guardrails. Their core capabilities include backup and recovery orchestration, system failover, failback and alternate-site operations.

These platforms also support business continuity, DR planning, implementation and continuous testing to validate readiness.

Eligibility Criteria

1. **Provide a unified platform** for backup and DR across on-premises, private, public, hybrid, edge cloud and SaaS environments
2. **Offer real-time monitoring** and visibility into recovery environments and protected assets
3. **Support through reporting and analytics** to track performance metrics, identify trends and ensure compliance
4. **Use AI and ML to detect anomalies or malware** and to validate or recommend clean recovery points
5. **Support manual and automated recovery** of data, applications and system states under defined policy controls
6. **Use AI to accelerate investigation and RCA**, and to recommend protection or recovery policies aligned with recovery point objective/recovery time objective (RPO/RTO) requirements
7. **Enable AI-assisted or automated recovery workflows** with continuous testing under suitable guardrails
8. **Implement best-practice DR procedures**, including solution testing, readiness validation and refresh cycles
9. **Integrate with adjacent platforms**, including infrastructure management, cyber resilience and backup ecosystems
10. **Provide robust failover and failback capabilities** to ensure continuity and controlled restoration



Observations

In the resiliency solutions space, there is a clear shift from a traditional backup-led approach toward an integrated cyber resilience strategy. Most vendors are combining capabilities such as immutable storage, threat detection, clean recovery validation and orchestrated DR into unified offerings. There is a strong emphasis on validated recovery outcomes, with features such as cleanroom recovery, anomaly detection and automated testing becoming standard. This shift reflects enterprises' need to restore data and reestablish trusted, uncompromised environments amid rising ransomware and regulatory pressures.

A common theme is the move to hybrid and cloud-native recovery models. Vendors are increasingly supporting distributed environments through capabilities such as recovery-as-code, continuous data protection, identity-aware recovery and cross-cloud orchestration. This shift indicates a broader transition from infrastructure-centric DR to application- and service-centric resilience. However, it also introduces complexity, as many

platforms require integration across multiple components or rely on ecosystem partners to achieve full coverage.

For enterprise buyers, the resiliency market is evolving into a platform-driven, cyber-focused discipline. Leading solutions now aim to embed resilience into day-to-day operations, governance and security workflows rather than treating it as a standalone function. This approach improves recovery confidence and operational alignment, but also raises the bar for implementation maturity, integration and cost management. Enterprises should, therefore, evaluate vendors on feature depth and their ability to deliver consistent, validated and operationally integrated resilience across complex hybrid cloud estates.

From the 40 companies assessed for this study, 24 qualified for this quadrant, with seven being Leaders.

Broadcom (VMware)

Broadcom (VMware) turns VMware-native resiliency into an integrated VCF operating layer rather than adjacent recovery products. This approach supports enterprises that seek policy-governed resilience within private cloud operations through convergence and monitoring.

COHESITY

Cohesity is assessed as a cyber resilience platform rather than merely a backup provider. Its ability to connect protection, vaulting, investigation and recovery across mixed estates supports integrated resilience without requiring an abrupt platform reset.

Commvault

Commvault positions Unity as a coordinated operating model for resilience that integrates cyber recovery, identity resilience and data security. This model supports enterprises that require recovery, identity restoration and cloud governance.

Dell Technologies

Dell Technologies positions PowerProtect Data Manager as a unified, AI-assisted resiliency layer through its dashboard, assistant and snapshot anomaly detection, advancing beyond vault and storage foundations toward more coordinated enterprise resiliency operations.

Hewlett Packard Enterprise

HPE presents resilience as a broader platform that links workload recovery, storage-native cyber controls, isolated vaulting and partner-led orchestration. This approach enhances its position across operational resilience, clean recovery and demonstrable recoverability.



Resiliency Platforms

Rubrik

Rubrik places identity resilience at the center of its cyber recovery strategy, extending protection from Active Directory and Entra ID to Okta and linking detection with rollback and trusted recovery, addressing a key point of failure in modern resilience.

Veeam

Veeam extends immutable vaulting into a more operational, clean recovery platform by combining Veeam Data Platform v13, a hardened software appliance, deeper SOC and ITSM integrations and broader cross-cloud vaulting to support faster validation and recovery.



Cohesity



"Cohesity offers a flexible resiliency portfolio that supports self-managed, SaaS and isolated vaulting models, suitable for complex enterprises operating across hybrid cloud environments where governance, control and recovery speed are essential."

Shashank Rajmane

Overview

Cohesity is headquartered in California, U.S., and has more than 6,000 employees across 15 countries. Its resiliency portfolio, packaged as the Cohesity Data Cloud, spans DataProtect, NetBackup, FortKnox, RecoveryAgent and the Helios control plane, covering backup, cyber vaulting, threat detection, orchestrated recovery and centralized management across on-premises, cloud, SaaS and hybrid environments. It is also advancing shared management across DataProtect and NetBackup, DirectIO support, broader threat scanning, clean recovery workflows, self-managed vaulting and identity-focused recovery.

Strengths

Unified oversight capabilities: Unified oversight capabilities: Cohesity's Helios unifies DataProtect and NetBackup, providing shared login, reporting, security controls and operational visibility across mixed environments. Using DirectIO and SpanFS, Helios extends the Cohesity modern data platform into NetBackup estates, reducing operational duplication and providing buyers with a clear path to implement common security and recovery practices across diverse environments.

AI-led recovery orchestration: Cohesity's RecoveryAgent extends the resiliency offering from a backup solution to an operational recovery platform. These AI-enabled agents can perform actions such as creating customizable blueprints,

rehearsals, threat-aware steps and provide recovery point guidance. These capabilities create a more repeatable and auditable recovery process for enterprise teams that need strong readiness validation and less manual coordination during disruptions.

Robust recovery controls: Cohesity combines FortKnox vaulting, immutability, quorum and role-based controls, anomaly detection, malware scanning and cleanroom recovery practices in a layered defense model. This combination improves confidence that recovery data remains intact, governable and less likely to reintroduce compromise during a cyber event.

Caution

Cohesity can strengthen its position by standardizing recovery orchestration across its operations. While RecoveryAgent expansion is progressing, buyers with cloud native, SaaS or multi-hypervisor recovery needs should validate maturity based on workloads.





Appendix

The ISG Provider Lens 2026 – Private/Hybrid Cloud – Data Center Solutions study analyzes the relevant software vendors/service providers in the global market, based on a multi-phased research and analysis process, and positions these providers based on the ISG Research methodology.

Study Sponsor:

Heiko Henkes

Lead Author:

Shashank Rajmane

Editor:

Ritu Sharma

Research Analyst:

Yatharth Bharti

Data Analysts:

Sachitha Kamath and Lakshmi Kavya Bandaru

Consultant Advisors:

Anay Nawathe and Rob Brindley

Project Manager:

Manikanta Shankaran

Information Services Group Inc. is solely responsible for the content of this report. Unless otherwise cited, all content, including illustrations, research, conclusions, assertions and positions contained in this report were developed by, and are the sole property of, Information Services Group Inc.

The research and analysis presented in this report includes research from the ISG Provider Lens® program, ongoing ISG Research programs, interviews with ISG advisors, briefings with service providers and analysis of publicly available market information from multiple sources. The data collected for this report represent information that ISG believes to be current as of May 2026 for providers that actively participated and for providers that did not. ISG recognizes that many mergers and acquisitions may have occurred since then, but this report does not reflect these changes.

All revenue references are in U.S. dollars (\$US) unless noted otherwise.

The study was conducted in the following steps:

1. Definition of Private/Hybrid Cloud – Data Center Solutions market
2. Use of questionnaire-based surveys of service providers/vendor across all trend topics
3. Interactive discussions with service providers/vendors on capabilities and use cases
4. Leverage ISG's internal databases and advisor knowledge & experience (wherever applicable)
5. Detailed analysis and evaluation of services and service documentation based on the facts & figures received from providers and other sources.

6. Use of the following key evaluation criteria:

- * Strategy and vision
- * Innovation
- * Brand awareness and presence in the market
- * Sales and partner landscape
- * Breadth and depth of portfolio of services offered
- * Technology advancements



Author and Editor Biographies

Author



Shashank Rajmane
Manager and Principal Analyst

Shashank Rajmane has more than a decade of extensive experience in research and works as a Principal Analyst at ISG. He leads the efforts for ISG Provider Lens® studies — Public Cloud Services & Solutions and Private/Hybrid Cloud & Data Center Outsourcing Services. He also authors the U.S. and Global reports. Apart from these, Shashank has been part of many consulting engagements and helping ISG's enterprise clients with their cloud strategy, along with selecting the right service providers/vendors based on their IT-related buying requirements. He has authored several white papers, thought leadership articles,

briefing notes, blogs and service provider intelligence reports, especially in the next-generation hybrid cloud and infrastructure services domain. Shashank has also delivered several workshops, webinars and podcasts and has been quoted in IT journals.

Research Analyst and Co-Author



Yatharth Bharti
Senior Research Analyst

Yatharth is a Senior Research Analyst at ISG. He is responsible for supporting and co-authoring Provider Lens® studies on Public Cloud and Private Hybrid Cloud Data Centre Solutions and Services. Yatharth supports the Lead Analysts in the research process on multiple regions and authors the global summary report, and focal points. He also collaborates with the Lead Analysts in the process of rating the providers and building insights around the market trends and drivers.

Yatharth has over 7 years of experience with a strong background in research, data analysis, and business analysis. In his previous role, Yatharth oversaw custom research and analysis projects to support businesses in better decision-making. Specializing across various industries with Everest Group, Yatharth provided valuable insights and recommendations and led in-depth analyses of enterprises and their operations to provide tailored insights to the clients.



Author and Editor Biographies

Study Sponsor



Heiko Henkes
Director & Principal Analyst, Global IPL Content Lead

Heiko Henkes serves as Director and Principal Analyst at ISG, overseeing the Global ISG Provider Lens® (IPL) Program for all IT Outsourcing (ITO) studies alongside his pivotal role in the global IPL division as a strategic program manager and thought leader for IPL lead analysts.

Henkes heads Star of Excellence, ISG's global customer experience initiative, steering program design and its integration with IPL and ISG's sourcing practice. His expertise lies in guiding companies through IT-based business model transformations, leveraging his deep understanding of continuous transformation,

IT competencies, sustainable business strategies and change management in a cloud-AI-driven business landscape. Henkes is known for his contributions as a keynote speaker on digital innovation, sharing insights on using technology for business growth and transformation.

IPL Product Owner



Jan Erik Aase
Partner and Global Head – ISG Provider Lens®

Mr. Aase brings extensive experience in the implementation and research of service integration and management of both IT and business processes. With over 35 years of experience, he is highly skilled at analyzing vendor governance trends and methodologies, identifying inefficiencies in current processes, and advising the industry. Jan Erik has experience on all four sides of the sourcing and vendor governance lifecycle - as a client, an industry analyst, a service provider and an advisor.

Now as a research director, principal analyst and global head of ISG Provider Lens®, he is very well positioned to assess and report on the state of the industry and make recommendations for both enterprises and service provider clients.



Provider Lens®

The ISG Provider Lens® Quadrant research series is the only service provider evaluation of its kind to combine empirical, data-driven research and market analysis with the real-world experience and observations of ISG's global advisory team. Enterprises will find a wealth of detailed data and market analysis to help guide their selection of appropriate sourcing partners. ISG advisors use the reports to validate their own market knowledge and make recommendations to ISG's enterprise clients. The research currently covers providers offering their services across multiple geographies globally.

For more information about ISG Provider Lens® research, please visit this [webpage](#).

Research™

ISG Research™ provides subscription research, advisory consulting and executive event services focused on market trends and disruptive technologies driving change in business computing. ISG Research™ delivers guidance that helps businesses accelerate growth and create more value.

ISG offers research specifically about providers to state and local governments (including counties and cities) and higher education institutions. Visit: [Public Sector](#).

For more information about ISG Research™ subscriptions, please email contact@isg-one.com, call +1.203.454.3900, or visit research.isg-one.com.

ISG (Information Services Group) (Nasdaq: III) is a leading 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.

For more information, visit isg-one.com.





JUNE, 2026

REPORT: PRIVATE/HYBRID CLOUD – DATA CENTER SOLUTIONS