IDC MarketScape

# IDC MarketScape: Worldwide Cyber-Recovery 2025 Vendor Assessment

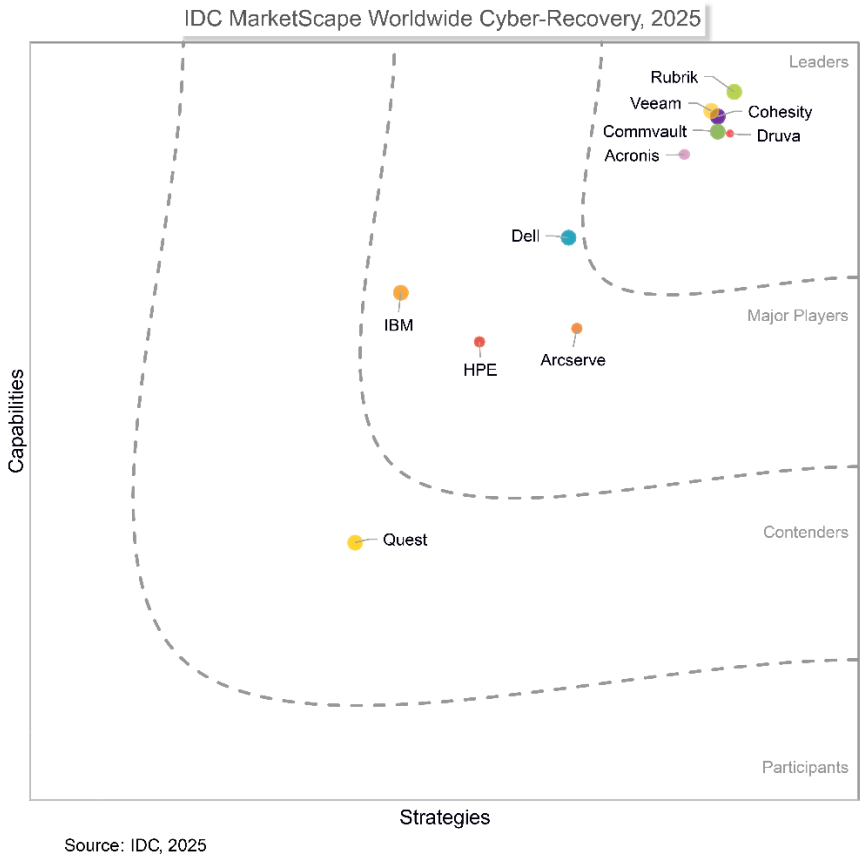
Johnny Yu Phil Goodwin

## THIS EXCERPT FEATURES COHESITY AS A LEADER

## IDC MARKETSCAPE FIGURE

### FIGURE 1

**IDC MarketScape Worldwide Cyber-Recovery Vendor Assessment**




Source: IDC, 2025

October 2025, IDC #US52040125e

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

## ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Cyber-Recovery 2025 Vendor Assessment (Doc # US52040125).

## IDC OPINION

Cyberattacks continue to be one of the biggest threats organizations face. A successful attack can lead to lost revenue, significant downtime, stolen data, regulatory fines, and a host of other consequences. Cybercrime is simply too organized and profitable to be completely stopped, and the ease with which perpetrators can deploy ransomware, combined with the relatively low risk of getting caught, ensures there is never a shortage of malicious actors.

Data protection and disaster recovery (DR) has traditionally been the answer to large-scale data outage events, but recovering from cyberattacks call for more than what traditional DR offers. This is where cyber-recovery comes in. Although data protection is the core component of cyber-recovery, not all data protection vendors offer a cyber-recovery solution. In addition to being able to back up and recover data, cyber-recovery requires capabilities specifically geared toward addressing the following foundational cyber-resilience needs:

- **Absolutely certain data survival:** Without absolutely certain data survival, it is highly likely that the organization will be forced to pay the ransom to get its data back. It is also likely to suffer data loss, as our research shows this to be common among victims. Organizations need to know they can get their data back no matter what.
- **Absolutely certain data integrity.** Similarly to data survival, organizations need to know that the data they recover is accurate data. Recovering data that has been modified or tampered with is as bad as or worse than not being able to recover at all, as much of the value of data lies in its legitimacy, authenticity, and validity.
- **Rapid recovery with minimal data loss.** The prospect of a long recovery may drive organizations to pay the ransom, even if they have clean, recoverable data. Being able to detect the attack early, quarantine it, assess the damage, and resume operations quickly mitigates any damage and prevents organizations from considering paying the ransom in hopes of a faster recovery.

Organizations are recognizing the threat and the importance of investing resources to defend against it. IDC research has found more than one-third of organizations plan to significantly increase their budget for cyber-recovery and resilience compared with last year. Similarly, an IDC survey found security to be one of the top 3 areas organizations say are the least likely to see budgetary setbacks.

To offer guidance to organizations looking to improve their cyberincident outcomes, this IDC MarketScape evaluates what we believe are the 11 most prominent cyber-recovery vendors. It is designed to help readers differentiate between these vendors' solutions and align their capabilities and features with their own organizational needs.

## IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

To narrow the list of participants to those we believe are most significant, we applied the following inclusion criteria:

- The solution must be a suite of software products (i.e., not just standalone backup/recovery).
- The solution must be primarily software, although delivery/integration with appliances is permitted as long as they are less than 50% of the solution price (as a percentage of actual selling price).
- The solution must include tools/modules specifically designed for cyber-recovery.
- The NIST cyber-recovery framework consists of five pillars: identify, detect, protect, respond, and recovery. The solution must be able to address at least the respond and recovery pillars, plus one other pillar.
- Data protection–related software revenue must exceed $100 million.
- The solution must be at least 70% "own IP" (as measured by percentage of actual selling price).
- The solution must be available worldwide (i.e., a presence in North America, EMEA, APAC, or at least 10 different countries) and have ≥20% of revenue outside of North America.
- The solution must address on-premises, multi–public cloud, and hybrid cloud workloads.
- The solution must be able to address small and midsize business (SMB) to large-scale enterprises.
- The core solution must have been in general market availability on January 1, 2024, with all features under consideration in general availability as of March 30, 2025. Features released after that time are considered road map items.

Our goal was to facilitate a head-to-head assessment with enough latitude that each vendor can illustrate its unique value and not box vendors into a one-size-fits-all evaluation.

## ADVICE FOR TECHNOLOGY BUYERS

The vendors in this analysis support on-premises, hybrid cloud, and multicloud environments. However, some do so using a predominantly on-premises deployment methodology and others from a predominantly cloud-based methodology. Others will use a blend of both. Buyers need to consider which architecture fits their environment and strategic direction most closely.

Cyber-recovery vendors differentiate themselves in a number of ways. Very often, these involve trade-offs. Some of the key buying criteria are:

- **Complexity.** The solutions evaluated in this IDC MarketScape range from simple to manage to rather complex. Not surprisingly, the complex solutions may have more capabilities. IT buyers must balance between the desire for simplicity and the need for robust features/functions.
- **Breadth of solution.** Some vendors seek to supply as many capabilities as possible while others focus on specific capabilities where they believe they can excel. No vendor can supply everything, and no company needs everything. IT buyers should focus on what they need or can reasonably expect to need in the future.
- **Service offerings.** Some vendors' solutions may offer services for deployment, onboarding, technical support, day-to-day management, incident response, consultation, and training. Some buyers will want to look closely at what vendors can provide beyond tools and technology to lower their management and administrative burden or bolster their cyber-resilience knowledge and expertise.
- **Price.** While price was not an evaluation criterion in this IDC MarketScape, it certainly is an issue for every buyer. Solutions mentioned in this document will vary greatly by price, and finding that balance between cost and solution capabilities is the goal.
- **Incumbency.** Although this evaluation is conducted as if every reader has a clean slate, we know that's not true. Some IT buyers will forego some minor "nice to haves" to continue operating with an incumbent vendor. Others will insist on what they deem "best of breed," regardless of incumbency. Only the buyer can make that trade-off.

This IDC MarketScape is not intended to be a buyer's guide. We have based the evaluation on criteria that we believe to be most important for cyber-recovery, but our

values and weightings may not match any specific IT buyer's needs. Its best use is as a means to begin solution differentiation and formulate a short list of vendor candidates for further consideration. Again, we believe every vendor in this evaluation could be the perfect solution in some scenarios and less optimal in other scenarios. IT buyers are advised to use this document in the short list formulation to narrow the field and then apply their own due diligence and proof of concept prior to making any selection or purchase.

## VENDOR SUMMARY PROFILE

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

### Cohesity

IDC has identified Cohesity as a Leader in this 2025 IDC MarketScape for worldwide cyber-recovery.

Cohesity, founded in 2013 and headquartered in San Jose, California, started in the data protection market and has since pivoted into cyber-recovery, focusing on enabling organizations to recover quickly and safely from malicious, disruptive events. The centerpiece of its cyber-recovery portfolio is the Cohesity Data Cloud, an integrated platform that combines Cohesity's DataProtect data protection, RecoveryAgent DR and cyber-recovery orchestration offering, DataHawk data security and threat scanning tool, and FortKnox immutable cybervaulting solution.

Cohesity's advanced cyber-recovery capabilities include automated clean room orchestration, AI-guided anomaly detection, threat monitoring and hunting, instant mass recovery, granular data classification, cybervaulting, and a broad portfolio of integrations with leading security vendors through the company's Data Security Alliance. Key integrations span SIEM/SOAR tools (e.g., Splunk, MS Sentinel, and Palo Alto XSOAR), endpoint security (e.g., CrowdStrike and Tenable), DSPM vendors (e.g., BigID and Cyera), identity security (e.g., Semperis and CyberArk), and cloud platforms (e.g., AWS, Azure, and GCP).

The platform's unified Helios interface manages both on-premises and multicloud deployments, enabling centralized oversight for complex environments. Cohesity also expanded its platform in 2024 to include Gaia, a generative AI (GenAI) application that uses retrieval-augmented generation (RAG) technology to get insights and generate answers to user questions about enterprise data under the purview of Cohesity Data Cloud.

Cohesity closed its acquisition of a large portion of Veritas' portfolio at the end of 2024, which included Veritas' flagship NetBackup cyber-recovery solution. Cohesity plans to continue developing and enhancing both its own Data Cloud and NetBackup while integrating the two product lines.

## Strengths

- **AI-assisted recovery orchestration:** Cohesity's RecoveryAgent delivers comprehensive, AI-powered cyber-recovery orchestration. It supports end-to-end workflows that guide users from incident detection through rehearsals, clean room setup, forensic validation, and automated restoration. Blueprints offer customizable, repeatable runbooks, and recovery can be validated non disruptively, reducing operational risk.
- **Advanced threat and anomaly detection:** The platform incorporates multiple layers of threat detection through AI/ML, signature-based scanning, and behavioral analytics for both backup and primary data. Continuous, proactive threat hunting is available, supported by integrations with leading threat intelligence feeds and third-party security platforms. The architecture includes automated quarantine of infected snapshots and robust access controls.
- **Cybervaulting and data immutability:** Cohesity FortKnox provides an air-gapped, immutable copy of critical data stored offsite or on premises, protected with advanced quorum controls and compliance-grade WORM technology. This helps ensure a surviving copy of data for reliable recovery even if primary and backup environments are compromised.
- **Extensive data security ecosystem:** The Data Security Alliance program integrates Cohesity with over 30 leading security, response, and posture management solutions. These integrations can help streamline collaboration between ITOps and SecOps and minimize time to recovery during a cyberincident.

## Challenges

- **Platform complexity following merger:** Integration of Cohesity and Veritas portfolios, while well advanced, brings inherent complexity. Current customers of DataProtect or NetBackup may experience learning curves or transitional workflows as unified operations and interfaces are being fully realized.
- **Licensing and feature segmentation:** Some advanced cyber-recovery capabilities such as DataHawk, curated recovery, and in-depth operational analytics are available only in higher subscription tiers or as add-ons. This may increase evaluation time or total cost for buyers seeking specific advanced features.

## Consider Cohesity When

Cohesity's cyber-recovery offering is suited for large-scale enterprises that can fully benefit from its high degree of automation. Smaller organizations can still benefit from Cohesity's Cloud Services SaaS offering to take advantage of its backup and recovery, DR, threat defense, and data security capabilities. Cohesity is especially compelling for buyers that highly value a robust security ecosystem and require collaborative response capabilities that bridge IT, security, and external partners.

# APPENDIX

## Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed. In this case, because cyber-recovery is a use case for other data protection products, we have used the vendor's data protection software revenue according to IDC's research as the market share.

## IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the

vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

## Market Definition

Cyber-recovery capabilities are built upon data replication and protection software and disaster recovery systems. Our definitions of pertinent market components follow:

- **Data protection software:** Data protection software is focused on protection, restoration, and recovery of data in the event of physical or logical errors. Products within the data protection and recovery market include data protection, continuous data protection (CDP), bare metal restore, backup/recovery software, host-based replication, and array-based replication (inclusive of snapshots, mirror/clones, and remote replication). Data protection software includes revenue from licensed software and online data protection services (aka online backup) licensed in a subscription fashion. This is inclusive of file- and image-level backup software, continuous data protection software, and backup reporting software.
- **Data protection as a service (DPaaS):** DPaaS is an umbrella term that includes backup, archive, disaster recovery, and cyber-recovery as a service. These are cloud-based services fully managed by the service provider. Most DPaaS solutions can address on-premises workloads as well as hybrid and multicloud workloads.
- **Disaster recovery and disaster recovery as a service (DRaaS):** Disaster recovery systems include all of the infrastructure, process management, and services necessary to restart an entire workload either on premises or in public cloud environment. DRaaS differs from on-premises and traditional disaster recovery in that DRaaS is a cloud-based, fully managed service. An organization may declare a disaster response based on datacenter fires or broken water pipes, power loss, and regional events such as train derailments, plane crashes, or terror events as well as earthquakes, floods, tornadoes, and hurricanes.
- **Cyber-recovery and cyber-recovery as a service (CRaaS):** Cyber-recovery builds upon disaster recovery, and CRaaS builds upon DRaaS. Cyber-recovery in both contexts includes all infrastructure, process management, analytics/forensics, and professional services to assist organizations in recovering from malware attacks in general and ransomware specifically. To qualify as a CRaaS service, we believe it must include all of the components of DRaaS (in other words, the ability to reestablish an application workload in its entirety) plus provisioning for a sanitary sandbox, forensic analysis, and curated

recovery. Some vendors may go substantially beyond that with additional data security functions for value-add and differentiation.

## LEARN MORE

## Related Research

- *Data Protection's Importance — IT Initiatives Least Impacted by Economic Factors* (IDC #US53699625, July 2025)
- *Skill Issues When It Comes to Cyber-Response* (IDC #US53152425, February 2025)
- *Cyber-Recovery and Cyber-Resilience to Drive a Significant Increase in the Budget for 2025* (IDC #US52679424, October 2024)

## Synopsis

This IDC study is an evaluation of the 11 most prominent cyber-recovery vendors on a worldwide basis. While it offers details on each vendor's capabilities and offerings, it is not meant to be a buyer guide. Instead, this evaluation is intended to help IT buyers differentiate between cyber-recovery solutions and narrow down candidates that fit their specific needs.

"No single cyber-recovery vendor offers the perfect solution for every organization's cyber-resilience needs," said Johnny Yu, research manager, Infrastructure Software Platform at IDC. "This IDC MarketScape is designed to give IT buyers the knowledge to find the solutions that best match their organizational needs, cyber-resilience skill levels, and infrastructure requirements."

## ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

## Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com