IDC MarketScape

IDC MarketScape: Worldwide Cyber-Recovery 2023 Vendor Assessment

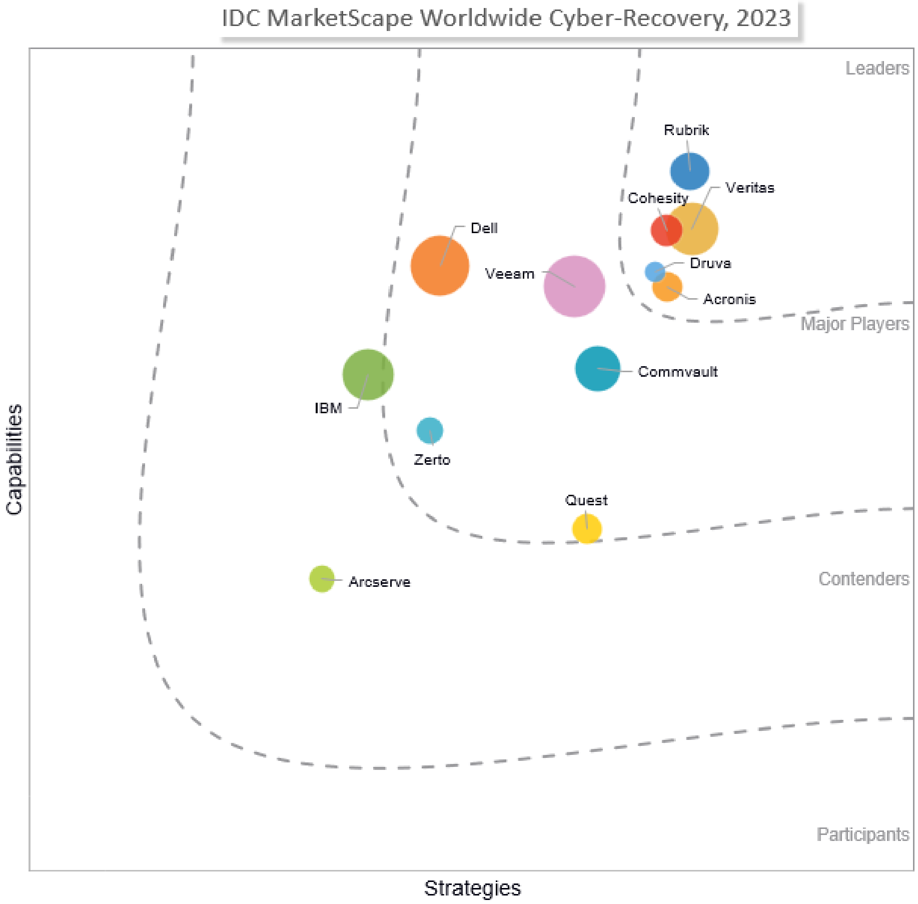
Phil Goodwin Johnny Yu Greg Macatee

THIS IDC MARKETSCAPE EXCERPT FEATURES COHESITY

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Cyber-Recovery Vendor Assessment



Source: IDC, 2023

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

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: IDC MarketScape: Worldwide Cyber-Recovery 2023 Vendor Assessment (Doc # US49787923). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

Cyberattack is front and center among the biggest threats faced by organizations worldwide. Cyberattackers spare no organization regardless of size, industry, geography, or political boundary. Unfortunately, there is no end in sight for cybercrime because it is simply too profitable for the perpetrators. For victims, the consequences can include lost revenue, permanently lost customers, lost employee productivity, regulatory fines, and unrecoverable data, not to mention the ransom cost itself. Perhaps worse, some organizations face shareholder lawsuits and class action lawsuits in the wake of the attack.

In the early days of ransomware attacks, organizations relied on data backup images to recover. As attackers became more sophisticated and comprehensive and attacks began with wiping out the backup images, IT teams began declaring disaster responses to cyberevents. However, there are important differences between disaster recoveries (DRs) and cyber-recoveries. Table 1 makes the comparison. Table 1 does not attempt to capture every step of either process, but rather to illustrate that DR efforts alone are likely to yield poor results for cyberevents.

TABLE 1

Disaster Response Versus Cyber-Response

High-Level DR Process	High-Level CR Process
Declare a disaster	Detect the attack
Provision recovery environment	Physically isolate the attack from further spread; shut down systems as needed
Restore data, if needed, from the last recovery point	Conduct forensic analysis: ▪ Determine attack type ▪ Determine when the attack began ▪ Identify all systems affected
Restart compute services in the prescribed order	Establish isolated sandbox: ▪ Restore data to sandbox ▪ Scan data and systems for malware ▪ Scan backups for malware ▪ Determine last clean point in time, which may vary by file system or database

TABLE 1

Disaster Response Versus Cyber-Response

High-Level DR Process	High-Level CR Process
	▪ Validate recovery
Initiate application failover	Provision recovery environment: ▪ May require bare metal
Run integrity checks (i.e., restart databases and roll logs forward as needed)	Push recovery environment to production
Validate recovery with users	Validate recovery
Resume operations	Resume operations
Fail back when appropriate	

Source: IDC, 2023

IDC uses the U.S. National Institute of Standards and Technology (NIST) framework for cyber-resilience. This framework includes five "pillars": identify, protect, detect, respond, and recover (for more information, go to **www.nist.gov/cyberframework/**). Fundamentally, these pillars fall into two categories: proactive defense and reactive recovery. To be truly cyber-resilient, organizations need "both," but unfortunately no single vendor can supply everything. Traditional data protection tends to focus on the "respond and recover" pillars, with data security focusing on the identify, protect, and detect pillars. However, many vendors — whether rooted in data protection or data security — are moving to offer capabilities across all five pillars, at least for some specific capabilities.

IT leaders acknowledge no one can prevent cyberattack with absolute certainty. In fact, most agree that an attacker is going to get inside their systems sooner or later. Moreover, our research shows data exfiltration ransom events occur about 50% more often than data encryption ransom events. This is because organizations are getting better at recovering encrypted data, but there is no recovery from data exfiltration; organizational leaders decide to either pay the ransom or not. However, even though there is no recovery from exfiltration, cyber-recovery vendors can offer important capabilities to reduce the impact, such as strong data encryption and immutability.

We believe cyber-resilient organizations will begin by locking down on three principles:

- **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. Without this, they are again relying on criminals to do the honorable thing after receiving the ransom.

- **Rapid recovery with minimal data loss:** Downtime is the friend of attackers and the enemy of victims. The prospect of a long recovery may drive the organization to pay the ransom, even if it has clean, recoverable data. Being able to detect the attack, quarantine it, assess the damage, and resume operations quickly mitigates any damage.

Because of the unique requirements for cyber-response (CR), IT organizations are moving quickly to implement cyber-response systems and vendors are responding to user and market needs just as quickly with rapidly evolving solutions. This dynamic market is good for IT consumers as it offers high differentiation, robust competition, and an opportunity to find a solution that closely fits the organization's needs. This IDC MarketScape evaluates what we believe are the 12 most prominent cyber-recovery vendors. Each vendor has unique capabilities and applicable "sweet spot" scenarios. This evaluation is intended to help IT buyers differentiate between the different vendors to select the right one for their situation.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Cyber-recovery is not a capability unto itself, but rather a combination of capabilities. In broad terms, cyber-recovery starts with fundamental data protection and builds upon DR. Thus it is not a product per se, but rather an integrated set of capabilities for the specific purpose of responding to ransomware. While backup/recovery (B/R) can claim to help with ransomware recovery, B/R alone is not nearly enough as discussed previously. Thus we were not interested in evaluating B/R vendors but rather vendors with purpose-built cyber-recovery capabilities.

To be worthy of consideration for this IDC MarketScape, vendors must be able to ensure data survival, data integrity, and rapid recovery as described previously. Functionality such as immutability, encryption, and strong air-gapped data are table stakes. We believe that each of the vendors considered in this document cross this threshold. We are confident that any of these solutions, when properly configured and managed, can facilitate complete data recovery in the event of a ransomware attack.

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 B/R).
- 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 CR.
- The solution must be able to address at least the Respond and Recover pillars of the NIST cyber-recovery framework 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 SMB to large-scale enterprises.

- The core solution must have been in general market availability on January 1, 2022, with all features under consideration in general availability as of May 30, 2023. 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

All of the vendors in this analysis support on-premises, hybrid cloud, and multicloud environments. However, some do so from a predominantly on-premises perspective, others from a predominantly cloud perspective, and others with a blend of both. All of them are quite viable, so 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.
- **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 PROFILES

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 2023 IDC MarketScape for worldwide cyber-recovery.

Cohesity is one of the newer companies in the data protection marketplace. So, while it has strong capabilities in core data protection, the company has been able to pivot quickly and effectively into cyber-resilience. Cohesity's cyber-recovery portfolio includes Data Protect (on premises and as a service), SiteContinuity (on premises and as a service), DataHawk, and FortKnox, all supported on the Cohesity Data Cloud platform. Cohesity has been selected as a key partner by AWS for its data protection/cybercapabilities and more recently by IBM for inclusion in IBM's Storage Defender product line. (IBM is identified as a Contender in this 2023 IDC MarketScape for worldwide cyber-recovery.)

From its inception, Cohesity's architecture has been designed for extensibility. This extensibility is not only for third-party connections but also for the user experience. Cohesity develops and manages the core of its solution but is not shy about utilizing and adopting third-party technology from companies such as Tenable, zScaler, BigID, and Qualys. The Cohesity architecture not only facilitated relatively rapid development for inclusion of these partner functions but did so in such a seamless way that it is transparent to the user.

Cohesity has also created its Data Security Alliance, which includes companies such as CrowdStrike, Mandiant, Palo Alto Networks, and Netskope, including the four companies mentioned previously. This alliance gives the company the ability to participate in the greater ecosystem of cybersecurity vendors and to adopt, partner, leverage, or interface with critical functionality. It also gives customers of the alliance members assurance that Cohesity will support and interface with them. This includes SIEM, SOAR, EDR/XDR, ITSM, DLP, and data security posture management (DSPM).

Cohesity's product portfolio is designed to assist customers in cyberpreparedness, including vulnerability scanning, early detection, incident response, and forensic analysis to orchestrated recovery. It also has machine learning (ML)-based anomaly detection that analyzes backup data to compute the odds of an anomaly and identify novel or emergent trends.

Cohesity takes cyberpreparedness and recovery beyond just technology with its Cohesity Cyber Emergency Response Team (CERT). This team is available to assist customers in rapidly responding to active cyberattacks for securing the Cohesity cluster, forensic analysis, data restoration, and cluster recovery.

Strengths

- Broad-ranging cybersecurity and recovery capabilities without forgetting the fundamentals of backup/recovery and disaster recovery
- Well-integrated user interface that is intuitive to use and seamlessly incorporates third-party IP
- Strong "upstream" ecosystem development and IP leverage via the Data Security Alliance
- Strong "downstream" ecosystem of relationships, including AWS and IBM
- Zero trust concepts extensively embedded in the solution

Challenges

As the cyber-recovery/security market rapidly evolves, new capabilities and functions are being constantly introduced. Cohesity is working hard to stay at the forefront, but not every idea is a good idea. Cohesity must choose judiciously what opportunities to pursue and ensure focus on those that offer real value to customers. Similarly, the partnership game is not one of numbers. While it will be tempting for Cohesity to add as many logos as possible to its Data Security Alliance (a list of 22 vendors at the time this document was written), the company should focus only on those that result in true added value.

Consider Cohesity When

Cohesity will be considered primarily by medium- to large-scale enterprises, although smaller enterprises might also find its cloud offering appealing. Customers that already use products from members of the Data Security Alliance may find adding Cohesity to be simpler in some cases. It will be considered by those organizations looking for a broad, very capable product and have the IT staff to support and manage it.

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 replication and protection software revenue according to IDC 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 replication and protection (DR&P) software:** DR&P remains a core market tracked by IDC. DR&P 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

- *Implementing Zero Trust in Data Protection* (IDC #US50225723, March 2023)
- *IDC Market Framework: Data Resilience* (IDC #US49800322, October 2022)
- *Cyber-Recovery: Why DR Is Not Enough for Data Trust* (IDC #US49743422, October 2022)

Synopsis

This IDC study examines the 12 most prominent cyber-recovery vendors on a worldwide basis. Each has its unique market position, and this evaluation is intended to help IT buyers identify short-list candidates for the buyer's specific scenario as a first step in the buying process or developing a proof of concept. Differentiating between cyber-recovery solutions is a challenge for IT buyers because the vendor capabilities vary so widely. Yet the decision is crucial. Choosing the wrong solution can lead to poor cyberevent outcomes and cost time, money, and reputation.

"Cyber-recovery is the cornerstone of cyber-resilience," said Phil Goodwin, research vice president, Infrastructure Systems, Platforms, and Technologies Group, IDC. "Without the ability to recover data accurately and rapidly, organizations may be forced to pay a ransom to avoid data loss and serious business consequences. Choosing the right cyber-recovery vendor is a crucial step in any cyberpreparedness planning. Matching organizational requirements with vendor capabilities ensures the best possible outcome, and this IDC MarketScape for worldwide cyber-recovery is intended to help IT buyers in that effort."

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

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, and web conference and conference event proceedings. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/about/worldwideoffices. Please contact IDC report sales at +1.508.988.7988 or www.idc.com/?modal=contact_repsales for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights.