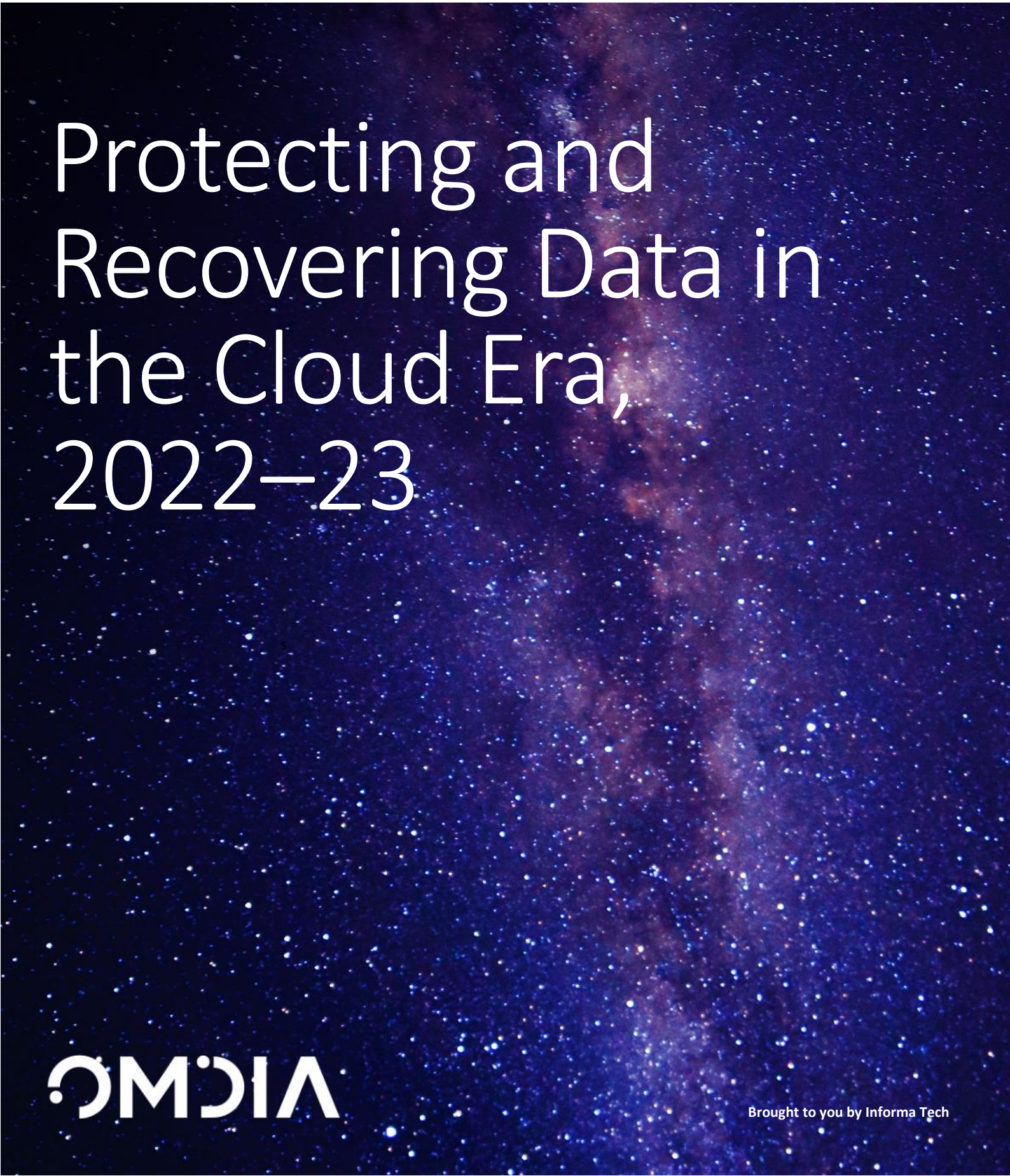
OMDIA

UNIVERSE

Publication date
14 February 2023

Authors
Dennis Hahn
Principal Analyst, Data Center Storage and Data Management
Roy Illsley, Chief Analyst, Cloud and Data Center

Protecting and Recovering Data in the Cloud Era, 2022–23



OMDIA

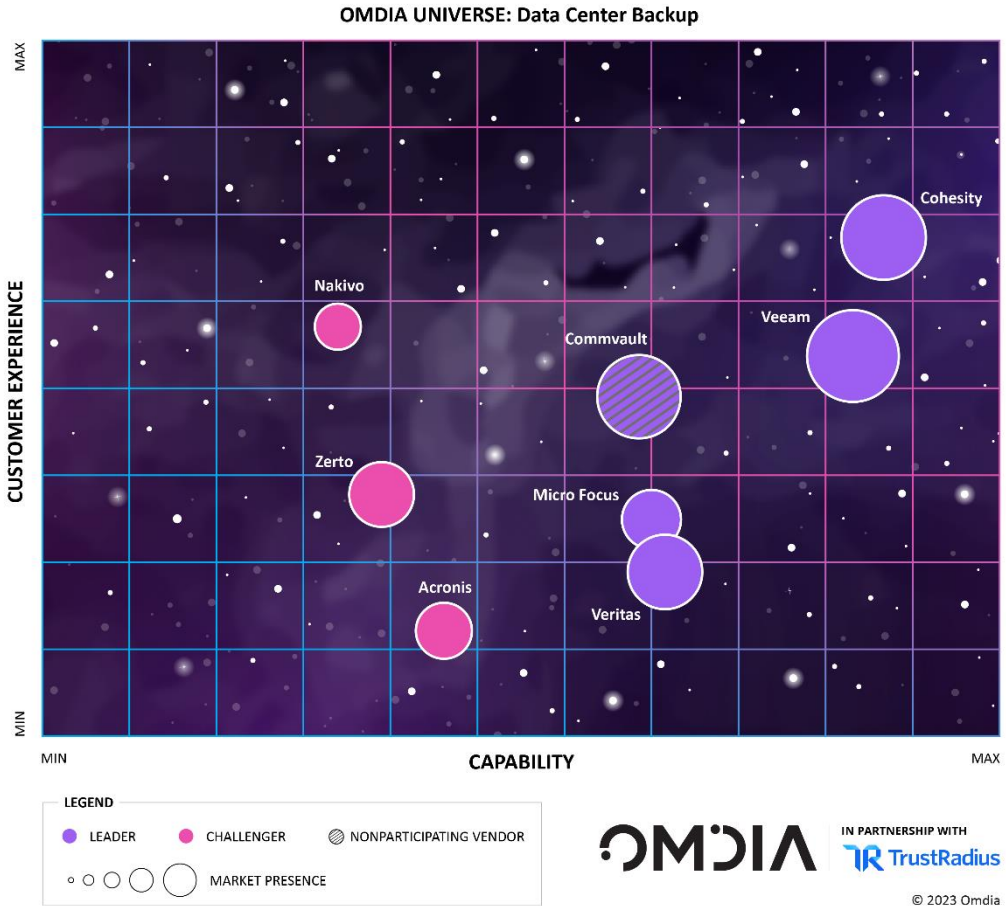
Brought to you by Informa Tech

Summary

Catalyst

Data protection technologies have gained greater prominence, as the need for backups has never been greater. Today, backup technologies concentrate on protecting data from operator error and ransomware attacks. Data and infrastructure recovery is the focus—whether the data resides in the public cloud, on-premises, or in hybrid data centers. **Figure 1** shows the results of Omdia's vendor assessments for those covered in this Universe report on the backup and recovery market. Note that Micro Focus was recently acquired by OpenText.

Figure 1: The Omdia Universe for protecting and recovering data in the cloud era



Source: Omdia

All vendors included in the report were approached to provide input to this study. The vendors that do not appear either declined to participate or did not complete the response questionnaire in time before publication. Any nonparticipant vendor evaluations that were still included were based on publicly available information, analyst insights, and feedback from their customer base sourced directly via TrustRadius and Informa Tech audiences.

Omdia view

Data has become how businesses operate, compete, and thrive in this new data economy. Therefore, organizational data must be protected under all conditions, no matter where it resides—on-premises, in remote locations, in the various types of clouds, in cloud native infrastructure, or as part of a multicloud environment. It used to be that only critical data needed backup protection, but with today's reliance on data, all data now needs to be protected to some degree. Shifting business requirements have required legacy backup software to change from merely making duplicated copies of data and doing media management to much, much more. Modern backups now overlap many data protection solutions, as they are geared toward protecting data anywhere it lives. If data is lost, these backups aim to recover it quickly and with good operational continuity. The leading backup vendors have demonstrated a clear understanding of what their solutions must offer customers. Most of the vendors analyzed in this report have the major backup features checked off to one degree or another. The difference in their offerings is in the details of how they have carried out those features, with varying degrees of simplicity, flexibility, and offering completeness. Some vendor offerings also include functionality that goes beyond backup into the broader data management area, which might be the deciding factor behind a few user purchases.

In the last couple of years, vendors have focused on making recoverable copies of data, no matter where it resides, to some service-level agreement (SLA)-driven recovery point objective (RPO) and recovery time objective (RTO) depending on the criticality of the data being protected. At the same time, the need to bring back data in the case of a ransomware attack has emerged as a reason to reconsider data protection strategies. The ransomware protection need has really driven backup and recovery to become more of a single concept around continuous data protection (CDP) without any data loss. Companies can no longer afford to lose even little bits of data if this data was important enough to protect in the first place. Overlaying all these requirements increases the need to simplify the deployment and management of data protection.

Omdia expects further evolution will be driven by what new business-related problems the vendor solutions can solve and how well they resonate with the customers. For example, the need to provide solutions for problems of data sovereignty, environmental sustainability, and archive analytics is at the forefront of the next wave in functionality. All vendors have their own roadmaps. Understanding not only the features they require but also the direction these companies are headed toward will provide clarity and help end users choose the product that meets their needs.

Key messages

- Cohesity was the overall leader (see **Figure 1**); it recorded leading scores in 4 out of the 11 product categories and was above average in all.
- Veeam was a close second overall; it was less than 1 percentage point behind the overall leader. The company recorded leading scores in 5 out of the 11 product categories and was above average in all.
- Commvault, Micro Focus (acquired by OpenText), and Veritas were also classified as leaders because they scored a total capability score of over 68%, did not have any low category scores, and only recorded four category product capability scores below the average.
- Acronis, Nakivo, and Zerto were classified as challengers because they all scored less than 68% in terms of total capabilities and had numerous low category scores.

Analyzing the data center backup universe

Market definition

The backup market has evolved from providing legacy on-premises data protection for critical applications to providing comprehensive data protection for all data vulnerable to loss. This report is guided by Omdia's vision of what a backup solution should currently deliver, as well as those areas that extend and differentiate a vendor's offering. The primary role of backup is to protect all data. Backup and recovery software must be flexible enough to protect the data in the many different places data resides and deliver on the SLAs that protected data needs around backup frequency and recovery. Such software needs to absolutely guarantee data recovery in the face of ransomware attacks. With the shortage of data center personnel, backup technologies must be simple to deploy and operate by a variety of skilled data center personnel. And while protecting data is the primary task, assisting IT operations in improving data management is a secondary consideration.

Product capability subcategories

For the most part, the vendor offerings covered in this report checked all the major data protection boxes and would make a fine product choice. What Omdia has tried to do in its analysis is to suggest that for a particular set of use case needs, a certain vendor might have the better offering because of implementation details. The current market reality is that backup technologies are and have been quickly evolving, so there are often different approaches to each of Omdia's eight product capability subcategories, each with its own strengths and weaknesses. The subcategories are described in the following sections.

Copy capabilities

The starting point for backup is its capability to flexibly make copies of the data it protects and send those copies to a variety of backup repositories. A backup software tool needs to provide a distributed set of multiple copies across different locations and media. Following the 3-2-1 rule for backup (three copies of the data, two different local devices, and one offsite) makes sure that there will be local and remote copies to ensure data recoverability. All tools need to support the ability to make copies offsite to a cloud repository and support the appropriate transmission controls and change tracking to provide a great usage experience. It is important for copy capabilities to support a spectrum of copy SLAs, especially in the frequency of backups.

Omdia believes that the best backup applications support the flexibility to copy, snapshot, replicate, and provide CDP copies as the use case warrants. And while the ultimate goal of any data protection scheme is recovery, copy capabilities serve as the all-important underpinning for any data recovery.

Recovery capabilities

The role of backup is to have a secure copy of the data, and recovery is about how to get backup copies back when the operations organization needs them. In the case of complete site failure or ransomware attack, the speed and sequence of recovery can be very important to organizations. Support for near-instant recovery is a must for most critical applications these days. Great backup tools provide for the universal recovery of data from any location to another. As locations change, infrastructure may change also, so physical-to-virtual (P2V) and virtual-to-cloud (V2C) conversions many be required. In the event of a disaster, it is unknown what location(s) might be available to accept any recovery data. Any recovery needs to be 100% assured, which means it needs to be integrity checked and tested. Many of the covered vendors support automated recovery testing and complete logging of the results on an ongoing basis.

In Omdia's opinion, not enough effort typically gets put into ensuring recovery is well-planned and periodically tested. Self-service recovery portals are also not demanded enough by data center operators, as they can be convenient for users and have the bonus of not involving the backup team. This is especially true in the era of hybrid cloud, where backup copies can serve as data migration and placement approaches.

Operational management

From an operational perspective, overall operational backup simplicity has become a must-have. Simplicity allows non-specialists to operate backups; it also allows for the task of backups to be completed quickly and efficiently. Simplicity helps deal with the labor shortage and keeps operating costs down. Backup tools need to operate in a variety of software environments, as one approach for backup work no longer works for all. Modern expectations are that backups and restores can be accomplished for virtual machines (VMs), platform as a service (PaaS), software as a service (SaaS), Docker, K8s, and hyper-converged environments. This can create a lot of complexity, so automation is very important to deliver a simple-to-use solution. Another thing that can lead to better operational efficiency is the use of tools that support a single consolidated view for monitoring the backup environment.

Omdia sees the extent of workflow automations as an interesting measure of simplicity and operational cost savings within backup offerings. When evaluating the various offerings, it is clear that backup vendors have attempted to evolve the customer experience toward greater operational simplicity.

Reporting management

The task of backups is really made up of various processes being kicked off (usually) based on a schedule and running processes to copy completion. In an ideal world, all these processes would not have to be monitored and logged, but this is a naive and dangerous view. Arguably, the root cause for the inability to restore data often comes down to bad copies and incomplete copy processes. This is why comprehensive real-time reporting with alerting is so important.

Backup reporting also meets several other strategic needs, like validating compliance, audit logging, and identifying when changes need to occur in the environment. Metering and cost controls have recently emerged as an important reporting capability with the inclusion of public cloud resources into backup processes. Reporting appears to be the first place artificial intelligence/machine learning (AI/ML) technologies are being applied to backups. Using advanced analytics, backup and recovery times can be estimated, and misconfigurations can be identified.

In the future, Omdia expects the data being collected for reporting will be fed into analytics to improve automation, detect anomalies, and correct misconfigurations. Often, operators of large backup installations can easily get swamped with too much information; analytics appears to be well-positioned to easily help in that area of reporting. In the future, AI will also provide better user help, support, and even training to dashboard operators. As data and storage infrastructure has become more distributed, Omdia has seen more vendor efforts put into centralized reporting and management from a single user portal. This centralization can provide an enterprise with much better visibility into the state of an organization's data protection and a place to develop to deliver analytics-derived insights.

Deployment coverage

A key characteristic of any backup solution is that it must be platform agnostic and operate in all environments. While an enterprise business may choose different data protection solutions based on the benefits it delivers within a certain environment, Omdia does expect all backup solutions to be capable of working across all the different environments. When considering data located in on-premises bare metal, on-premises virtualized, and remote locations, the various types of clouds, cloud native infrastructure, and multicloud environments, it becomes obvious why this flexibility to run almost anywhere is important. It is also important that a deployment can support a myriad of different application workloads.

An increasingly popular way to access backup technology is as-a-service (backup as a service, BaaS), which protects data on-premises but can be controlled and managed from a cloud portal. By using BaaS, organizations can lower backup costs, control risk, and side-step the complexities of self-deployment. Backup appliances are another deployment option. The appliance technique of deployment provides for a turnkey implementation but at a greater level of lock-in. Omdia does not prescribe the architecture of a backup solution, but we do look at how flexibly a backup offering can be deployed into multiple scenarios. A flexible architecture provides the best coverage and should help to eliminate lock-in concerns while still providing the benefit of deployment simplicity.

Product integrations

There are several important data repository, application protection, and API management integrations to consider in support of backing up applications. Backup repository choice is one of the more important backup architecture and usage decisions that can be made. In the past, duplication appliances have been very popular, but deduplication has largely become a commodity. Modern choices for backup data retention are cloud storage, on-premises object/file storage, and software-defined repositories on storage servers. The strategy used for backup data retention dictates the cost, scalability, and performance of the data copies and restores.

Often, there are also data tiering options to consider that help in managing long-term retention costs, like cloud archive, active archive, and tape. Extended capabilities such as tagging, searchable namespace, and versioning of the data repository can be part of the bigger IT picture. Most backups are supported by server setup information for migration and work with an application to create consistent snapshots of the data, where the app is directed to flush buffers and prepare for backup. Depending on application coverage, these client-side integrations can be very important.

Omdia perceives that most integration relies on backup APIs to direct activity and obtain environment information. Maintaining a robust and stable API set is very important to workflow automation and third-party software interaction. Major enterprises often have umbrella monitoring dashboards and alerting to connect other applications into. Integrations with ancillary applications that support problem ticketing, like ServiceNow, and cloud cost tracking can be important third-party capabilities for augmenting and extending functionality.

Hybrid cloud

According to best practice, backup copies of data should be placed both locally and remotely to diversify against data loss. They should be placed locally for the fastest network restores and offsite (remote) to protect against catastrophic failures. Public cloud companies have made compelling arguments around the cost savings gained by using cloud as a data center's recovery site and the extra resiliency that using cloud storage can provide. To be able to recover in the cloud, the backup offering should support at least Amazon Web Services (AWS), Azure, or Google Cloud Platform (GCP) as remote repositories from which data can be recovered to cloud-located compute instances. Great hybrid backup offerings should also support non-hyperscaler online storage-only clouds like Backblaze, Wasabi, etc. These are likely to deliver lower storage costs but are less convenient to restore from, as data typically needs to get copied back to on-premises compute infrastructure and not within the cloud. To make data copies between such a diverse set of applications and repositories, the backup software should work based on predetermined SLAs to control and set up these workflows. Operating at this level allows administrators to manage the big picture and let the software manage the details. Environment policies and roles are also important since they are the backbone of automation and the way the cloud operates. Many of the covered offerings could be used not only in backup scenarios, but also as data mobility tools, enabling data to be moved between locations with ease.

Omdia expects multicloud initiatives in the future to accelerate into cloud native and SaaS (e.g., Microsoft 365) domains, where backup workflows can easily be destabilized by (for instance) Kubernetes with its very agile approach to operations. Other key features quickly being added to backup offerings for serving cloud better are the tracking of storage consumption and accounting for cloud costs, with the goal of minimizing them.

Data security & ransomware

Beyond protecting data against accidental loss, backup is now taking on an important role in securing data from theft and malicious activity. The first line of defense in securing data is networking and access controls, but the industry has quickly recognized that an essential fallback when frontend protections enviably fail is to possess recent, ransomware-clean, versioned data copies. To effectively thwart ransomware, backups need to be comprehensive in stored data coverage and immutable. Comprehensive protection of all enterprise data has become especially important as data environments have become more distributed with multicloud, remote workers, and Internet of Things (IoT) data collection. Repository data should always be encrypted with well-thought-out key management to protect against theft and the threat of exposing company information for ransom. And all data and control access must be passworded with strong multi-factor authentication (MFA) to keep malicious actors from turning off and neutralizing backups. Automatically generated compliance and audit reports are often the key to ensuring proper resiliency from system intrusion gaps and misconfigurations within environments. Similar reporting is also important to actively monitor the state of upgrades and patches to avoid incidents.

Omdia is currently seeing some vendors extending beyond protected backups into scanning data to detect attacks, assisting with automated recoveries and creating sandboxes separated from production to check data for viruses. Another emerging area around compliance includes the vendors taking on data sovereignty concerns by providing capabilities to ensure backup processes and data retention comply with relevant data privacy, origination tracking, and security laws from the different countries. It is important to note that with the increase in sophisticated cyberattacks Omdia saw last year, it is now a must-have requirement that at least one copy of backed-up data must be stored in immutable storage that cannot be altered by ransomware.

Market dynamics

The backup market is a relatively old market that has continued to evolve to take on the new challenges of cloud computing, SaaS protection, remote workers, ransomware, etc. At one time, best practice backup was sending copies to an on-premises duplication appliance, and before that, shipping stacks of tape copies to an offsite physical media vaulting company. The backup capabilities and software features to appropriately address the broad idea of data protection are substantial and have grown over time, making analysis and decision-making as to what product is best for a particular data center user and usage scenario difficult. Note that it is outside the scope of this report to cover the many backup vendors targeting and designing for the protection of small businesses, home offices, and personal devices.

Table 1: Vendor rankings in the data center backup universe

Vendor	Product(s) evaluated
Leaders	
Cohesity	DataProtect, DataProtect-as-a-Service, FortKnox
Veeam	Veeam Backup & Replication, Veeam Availability Suite
Micro Focus	Data protector, Data Protector for Cloud
Commvault	Complete Data Protection, HyperScale X, Metallic
Veritas	NetBackup, NetBackup Appliances (Backup Exec)
Challengers	
Nakivo	Backup & Replication
Zerto	Zerto 9.7, Zerto for Kubernetes, Zerto In-Cloud, Zerto Backup for SaaS, HPE GreenLake for Backup and Recovery
Acronis	Acronis Cyber Protect, Cyber Protect Cloud, Acronis Detection and Response

Source: Omdia

Market leaders

The Universe leaders largely include those vendors that have expanded their solutions into all areas of data protection. Their offerings are likely to be made up of a core product, and they often add on capabilities and subproducts (not always listed below) for comprehensive solution coverage.

The market leaders all scored above 93% for solution breadth and greater than 68% for total capability (see **Figure 1**), so Omdia considered 68% to be the threshold capability score that divided the leaders from the challengers. The common trait the leaders shared was a comprehensive solution that has no significant gaps in their capabilities to protect data. It comes as no surprise that the scores between the leaders accounted for all the category-leading scores. However, some of the challengers were equally as good in specific categories. The value of the leaders is they can accommodate any specific requirement a customer may expect from data protection, but they may not be the best in that specific category. In essence, the leaders are very good all-rounders and provide a breadth of coverage with a good degree of depth.

Market challengers

The challengers have demonstrated strength in one or two of the management areas or a less comprehensive set of capabilities across all areas. It is likely they are trying to grow their capabilities as their users and the market dictate. The market challengers all scored above 70% for solution breadth and greater than 50% for total capability. They all had at least two categories where they performed below the average, but these were not always within the same categories. The market challengers represent slightly lower all-around ability than the leaders. While they may have some strengths that are equal to or better than the leaders, the challengers have some categories where they either do not provide solutions or are still evolving. The market challengers can provide some greater depth in one or more specific areas but lack the comprehensive breadth of the leaders.

Market prospects

For this Universe, Omdia could not identify any companies in the prospects category. While we believe there are some prospects that could have been covered, like those specializing in Kubernetes (K8s) backup, the goal of this report is to help data center enterprise vendors assess offerings for broad data center coverage and all their data protection needs.

Market outlook

According to Omdia's *Software Market Forecasts: Infrastructure, 2021–26* report, the backup market was worth $10,934m in 2022, and it is growing (2021–26 CAGR of 7%). This market is forecast to be worth $14.4bn globally by 2026; however, its adoption is not uniform across all market verticals. Retail (2019–24 CAGR of 8.0%) and healthcare (2019–24 CAGR of 7.7%) represent the leading verticals, while education (2019–24 CAGR of 6.1%) and utilities (2019–24 CAGR of 4.9%) are the markets with the slowest adoption. It is notable that in 2019, professional services was in the bottom category (slowest adoption), but in 2022 it jumped up to fourth highest (2019–24 CAGR of 7.2%) as a reflection of the changing landscape and the increasing use of advanced backup technologies. Omdia believes that the variation in adoption rates highlights those industry verticals that are undergoing digital transformation and therefore have a growing reliance on data and its protection in their businesses.

Vendor analysis

Cohesity (Omdia recommendation: Leader)

Product(s): DataProtect, DataProtect-as-a-Service, and FortKnox

Cohesity should appear on your shortlist if your organization is looking for a modernized data protection approach that scores high in all areas and really does well in core backup and recovery and monitoring and reporting hybrid data protection capabilities.

Overview

Cohesity is classified as a leader in this Omdia Universe. The company scored a total capability score of 78%, which positioned it as having the top score, followed very closely by Veeam, which scored only 1 percentage point lower. When summing up the detailed product subcategory scoring, Cohesity took top honors in solution breadth (99%), strategy & roadmap (85%), and solution capability (66%) (see **Figure 3**). The company's entrance into the data protection market with a modern set of solutions certainly helped it take these top spots.

Cohesity DataProtect is a backup and recovery software solution that can be consumed as a service (BaaS) or deployed in the customer's self-managed environment on physical and virtual appliances. The company's extensible platform and Helios control plane make the offering easier to install and operate. Cohesity's strategies include an early focus on security and backup protection from ransomware. It does a good job supporting recovery orchestration and a slew of features to provide for fast and efficient recoveries.

In terms of customer experience, Cohesity's customers gave it the highest recommendation score of the group at 93%, driven by high product and vendor experience scores. If reviewing customers had concerns, it was in the contract terms & pricing area. Cohesity's customers indicated a very strong score for its professional services and strength in customer support.

Figure 3: Omdia Universe ratings – Cohesity

Source: Omdia

Strengths

Cohesity achieved the top scores in four of Omdia's eight product capability subcategories. It also received the highest recommendation score, indicating that it delivers on the required customer experience beyond the mere technology.

Cohesity achieved a top subcategory score of 61% (15 percentage points over average) in the security & ransomware coverage subcategory. The company came out on top largely because its solution can protect the data from attack, detect an attack early, and recover rapidly from an attack using automated management approaches. The success of Cohesity's offering hinges on its ability to

control the storage repository to create an immutable backup architecture that ensures a recently stored data version can be recovered, even if network-level protections fail. Immutability means that safely stored backup data cannot be encrypted, modified, or deleted. To detect data being attacked by ransomware, data change rates are continually monitored. Helios also uses ML-based algorithms to detect these abnormal file use patterns and create actionable alerts and recommend a clean point-in-time snapshot to recover. Backups are the last line of defense after ransomware slips by a data center's perimeter and networking defenses, so it is important to be able to identify uninfected recovery points and recover quickly. Cohesity's instant mass recovery solutions scan and find clean copies to check their status and then allow a near-instant mounting of the data to reduce downtime.

Securing the backup infrastructure is very important in stopping unauthorized changes to data and backup configuration. Cohesity uses granular role-based access controls (RBAC) in its overall management. This ensures administrators can do their jobs while also making sure each administrator is not granted more control than needed. MFA is also used, along with a variety of Active Directory integrations. In support of immutability, DataLock applies a time-bound WORM policy, ensuring backup copies cannot be deleted by ransomware. Going even a step further, quorums of more than one backup administrator can be required to apply critical configuration changes.

Cohesity received a top subcategory score of 61% (9 percentage points over average) in operational management. Omdia was impressed by the approach Cohesity engineers have taken with the development of the company's product. The DataProtect product offering considers people, processes, and platforms, which results in a unified and highly automated data protection user experience. Prior to this offering consolidation, most data protection infrastructure was deployed as a distributed system of backup servers, agents, proxies, and media servers that data center administrators had to closely monitor to keep running.

Cohesity jumped into the data protection market about eight years ago with a converged platform that eliminated the disjointed complexity resulting from many of the traditional data protection solutions of the time. Recovery is made easier because DataProtect maps each incremental backup to an incremental snapshot. This data store mapping enables a very large number of efficiently stored snapshots and good recovery granularity. Cohesity is known for often providing the storage repository as an appliance to the market. Most recovery capabilities today are guided by data recovery SLAs. The more controlled appliance approach has allowed Cohesity to score well on operational management capabilities. Gaining visibility and control over these data copies is paramount to providing near-instant recoveries, individual file restores, and automating the process of recovery.

Cohesity received the top subcategory score of 66% (6 percentage points over average) in reporting management by collecting an impressive range of metrics based on the end-to-end workflows being monitored. Omdia liked the Cohesity Helios all-in-one management and reporting, which can be used on-premises or as a Cohesity-hosted service. End-to-end monitoring requires copy engines, connectivity, security, and the storage repository to be tracked across many different types of compute infrastructure, including on-premises VM, bare metal, and cloud computing infrastructures, which Helios seems to do well. Understanding the data protection setup and then monitoring it is key to operational efficiency and agility. With Helios, a user can get an overall view of their data

protection jobs and data stores as well as analyze status at the granular level using powerful filtering options. In support of recovery, Cohesity applies an indexing engine to provide recovery options. Good reporting requires strong visibility and control over stored data copies. With Helios, users can schedule, filter, and download reports that (for instance) might be used to status how the tiering storage layer is using lower cost media and cloud archive storage.

Limitations

The foundation of Cohesity's solution is its creation of a robust storage repository solution, which drives it toward an appliance-focused go-to-market. As Omdia has already mentioned, this approach has many advantages, but it also tends to lock users into a Cohesity storing infrastructure. The company does make its storage repository more open by allowing other backup vendor software to work with it, though some of the functionality will likely be lost. Users were also concerned about Cohesity's inflexible pricing, which can become quite complex and will possibly be too expensive for mid-market buyers.

Companies that are primarily seeking comprehensive hybrid data protection offerings for on-premises, cloud, and edge environments (including BaaS as an option) should strongly consider Cohesity offerings. Users from SMBs who are looking for low cost cloud-first protection or BaaS offerings and have limited on-premises needs might consider other options.

Appendix

Methodology

Omdia Universe

The process of writing a Universe is time-consuming and multifaceted:

- Omdia analysts perform an in-depth review of the market using our market forecasting data and ICT Enterprise Insights survey data.
- Omdia creates a matrix of capabilities, attributes, and features that we consider to be important now and in the next 12–18 months for the market.
- Vendors are interviewed and provide in-depth briefings on their current solutions and future plans.
- Analysts supplement these briefings with other information obtained from industry events and user conferences.
- Analysts derive insights on the customer experience with each solution via reviews and ratings on TrustRadius, augmented by direct Omdia customer rating surveys.
- The Universe is peer-reviewed by other Omdia analysts before being proofread by a team of dedicated editors.

Inclusion criteria

There are many vendors in the backup market that offer solutions to customers of all sizes. However, inclusion in this Universe is based on the vendor's ability to offer data center-level solutions specifically for addressing the eight major aspects of backup and data protection discussed in the ***Product capability subcategories*** section of this report. All the vendors have had a chance to review and verify the accuracy of the information. As is typical with these projects, some vendors are unable to meet the strict deadlines for the return of submissions, so Omdia did the best we could to represent their products.

The criteria for inclusion of a vendor in the *Omdia Universe: Protecting and Recovering Data in the Cloud Era, 2022–23* are as follows:

- The vendor must be a global vendor with customers in three regions: Asia & Oceania; Europe, the Middle East, and Africa (EMEA); and North America.
- The vendor backup offering must operate at a data center enterprise level of functionality and provide some level of recovery in response to a ransomware attack.
- The vendors must offer protection for at least on-premises and cloud data, and then store it on a variety of backup media—on-premises, cloud, and tape.
- The vendor must have at least 250 customers, and they must be a mix of midsize enterprises (1,000–4,999 employees) and large enterprises (5,000-plus employees).

Omdia ratings

- **Market leader:** This category represents the leading solutions that Omdia believes are worthy of a place on most technology selection shortlists. The vendor has established a commanding market position with a product that is widely accepted as best of breed.
- **Market challenger:** The vendors in this category have a good market positioning and are selling and marketing the product well. The products offer competitive functionality and a good price-performance proposition and should be considered as part of the technology selection.
- **Market prospect:** The solutions in this category provide often provide strong niche functionality needed but often lack comprehensive needs coverage or suffer from a low customer satisfaction rating. None of the companies covered in this Universe were identified as prospects.

The scoring for the Universe is performed by a number of independent analysts against a common maturity model, and the average score for each subcategory and dimension is calculated. The overall position is based on the weighted average score, where each subcategory in a dimension is allocated. Omdia's eight product capability subcategories, each with its own strengths and weaknesses, are listed in the ***Product capability subcategories*** section. It is important to note the scoring of these subcategories has not been normalized to the highest receiving 100%. For example, a 60% in one subcategory may be the highest score, while an 80% might be the top score in another. Care should be taken compare scores across subcategories, as both 60% and 80% would be top scores, and 80% is not necessarily a better score than 60%.

Further reading

Software Market Forecast: Infrastructure, 2021–26 (September 2022)

Reviews of backup vendor offerings on TrustRadius

Authors

Dennis Hahn, Principal Analyst, Data Center Storage and Data Management

Roy Illsley, Chief Analyst, Cloud and Data Center

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com