Magic Quadrant for Enterprise Backup and Recovery Software Solutions

Published 19 July 2021 - ID G00733940 - 40 min read

By Analyst(s): Santhosh Rao, Nik Simpson, Michael Hoeck, Jerry Rozeman

Initiatives: Data Center Infrastructure

The move toward public cloud, heightened concerns over ransomware along with complexities associated with backup and data management are forcing I&O leaders to rearchitect their backup infrastructure and explore alternative solutions. This research provides analyses of backup and recovery vendors.

This Magic Quadrant is related to other research:

View All Magic Quadrants and Critical Capabilities

Market Definition/Description

Gartner's view of the enterprise backup and recovery software solution market is focused on transformational technologies or approaches delivering on the future needs of end users. It is not focused on the market as it is today. Gartner defines the market as follows: Backup and recovery software solutions are designed to capture a point-in-time copy (backup) of an enterprise workload and write the data out to a secondary storage device for the purpose of recovering this data in case of loss.

The core capabilities of a backup and recovery solution include:

- Back up and recover operating systems, files, databases and applications in the on-premises data center.
- Create a copy of the backup in the same physical location as the production environment for the purpose of quick operational recovery.
- Assign multiple backup and retention policies that align with the organization's recovery objectives.
- Report success and failure of backup/recovery tasks.

Additional capabilities that can be provided by the solution are:

- Create a second backup copy of on-premises backup data in the public cloud/secondary data center.
- Tier backup data to the public cloud.
- Protect public cloud IaaS, PaaS and SaaS workloads.
- Protect remote sites.

The solution can be offered as an appliance, as software only or as a vendor-managed service offering.

Magic Quadrant

Figure 1: Magic Quadrant for Enterprise Backup and Recovery Software Solutions

Source: Gartner (July 2021)

Vendor Strengths and Cautions

Acronis

Acronis is a Visionary in this Magic Quadrant. It leads with the Acronis Cyber Protect Cloud platform, a cloud-based backup and security service targeted at the midmarket segment, primarily delivered by service providers through 30 data centers spread across all major geographies. The vendor also offers Acronis Cyber Protect, a software solution that can be deployed on-premises that provides an integrated backup and security solution for physical servers, on-premises VMs, and cloud instances and endpoints. In 2020, Acronis introduced several security features on both its on-premises and backup as a service (BaaS) platforms that improved malware detection and provided safe recovery of backup copies.

Strengths

- **Differentiated cybersecurity capabilities** — Acronis' ransomware protection capabilities, such as its ability to actively scan for security threats and verify the authenticity and recoverability of backup copies, strongly complement its backup capabilities.
- **BaaS** — The Acronis Cyber Protect Cloud platform provides a comprehensive BaaS offering. The service is available in all major geographies through the vendor's cloud data centers and via partnerships with public cloud providers.
- **Edge environments and endpoint protection** — Acronis offers a strong and differentiated data protection solution for remote sites/edge locations and endpoints.

Cautions

- **Weak database support** — Acronis' backup and recovery capabilities for databases such as Oracle Database, Microsoft SQL, SAP HANA and NoSQL are not comprehensive.
- **Limited enterprise data center presence** — Most of Acronis' enterprise clients use its solution to protect edge environments and endpoints. Acronis' product and sales strategy has limited focus on enterprise data center backup.
- **Limited public cloud support** — Acronis trails the competition in its ability to provide data protection capabilities for public cloud IaaS and SaaS workloads.

Arcserve

Arcserve did not respond to requests for supplemental information. Gartner's analysis is therefore based on other credible sources, including Gartner client inquiries, Gartner Peer Insights, press releases from Arcserve and technical documentation available on Arcserve's website.

Arcserve is a Challenger in this Magic Quadrant. Arcserve's backup portfolio includes Arcserve Unified Data Protection (UDP), Arcserve Backup, Arcserve Appliances, Arcserve UDP Cloud Direct, Arcserve UDP Cloud Hybrid Secured by Sophos and Arcserve Cloud Backup for Office 365. Arcserve's operations are geographically diversified, and most of its clients are in the midmarket segment. During the evaluation period, Arcserve released UDP 8.0, which includes support for immutable cloud storage backups, integration with Oracle RMAN, support for Nutanix AHV backup and Microsoft Teams backup. It also announced Arcserve X series Appliances, an integrated backup, disaster recovery (DR) and security solution. In March 2021, the vendor merged with StorageCraft, which further expanded its product portfolio to include scale-out storage and provide additional data protection capabilities such as SaaS backup.

Strengths

- **Breadth of platform support** — Arcserve UDP addresses the data protection requirements of a broad range of operating systems, hypervisors and databases.
- **Anti-malware capabilities** — Arcserve partners with Sophos to offer appliances with built-in malware detection capabilities. Data can be recovered either to an on-premises target or Arcserve UDP Cloud.
- **Low acquisition cost** — Arcserve offers one the lowest socket-based license prices among all vendors evaluated in the market in 2020.

Cautions

- **Cloud-native data protection** — Arcserve UDP does not integrate with public cloud snapshot APIs provided by Amazon Elastic Compute Cloud (EC2), Microsoft Azure VMs or Google Compute Engine (GCE). It also does not support backup of PaaS environments such as Amazon Web Services (AWS) Amazon Relational Database Service (RDS) or Azure SQL.
- **Tape support** — Arcserve customers that require tape support must separately install Arcserve Backup alongside Arcserve UDP.

- **Limited integration with storage array snapshots** — Arcserve UDP integrates with hardware snapshot APIs from a limited number of primary storage array vendors.

Cohesity

Cohesity is a Leader in this Magic Quadrant. Its backup product portfolio mainly consists of DataProtect, which is a service that runs on Cohesity Helios, a SaaS-based data management platform. Cohesity's operations are mainly focused in North America and Western Europe, and its clients tend to be in the upper midmarket and enterprise segments. The vendor released two major software updates in the last 12 months — 6.5.1 and 6.6; new key features include support for instant restore of Oracle Databases; DR for VMware; Microsoft Office 365 SharePoint Online, Teams and Groups backup; AWS Amazon RDS and Aurora database backup; and multiple enhancements to Azure VM backup and tiering. In October 2020, Cohesity announced its BaaS offering under its Data Management as a Service (DMaaS) portfolio that uses the Cohesity Helios platform, DataProtect service and AWS infrastructure to protect and manage hybrid environments.

Strengths

- **Operational simplicity** — Gartner Peer Insights customer reviews and Gartner client inquiries indicate that the DataProtect service is simple to use and easy to manage at scale.
- **Ecosystem support** — The Cohesity marketplace enables ISVs to integrate with the Cohesity platform and offers a broad range of additional data reuse capabilities, such as data masking, cyber vulnerabilities scanning in the backup snapshots and mainframe backup.
- **Unified management** — Cohesity customers can leverage Helios, a SaaS-based platform that facilitates centralized management of multiple Cohesity environments. It also provides DR orchestration, ransomware detection, capacity management, issue root cause analysis and case management, as well as global search capabilities.

Cautions

- **Higher operational costs for public cloud application backup** — Cohesity requires a three-node VM cluster to be deployed in the public cloud to support granular protection and recovery of instances hosted in public cloud IaaS. This increases the total cost of ownership of running the backup infrastructure in the public cloud.

- **Code quality** — The Cohesity DataProtect service was released with a relatively high number of known issues and issues reported by customers, indicating a need for improvement in the quality assurance testing process.
- **Limited presence in emerging markets** — Cohesity has a limited direct presence and a relatively small number of channel partners in emerging markets, requiring customers to ensure that they work with a credible partner and rely on local references when selecting Cohesity.

Commvault

Commvault is a Leader in this Magic Quadrant. Its backup/recovery portfolio mainly comprises Commvault Complete Data Protection, Commvault HyperScale X and Commvault Metallic. Commvault's operations are geographically diversified, and its clients tend to be in the large enterprise segment. During the evaluation period, the vendor continued to strengthen and expand its cloud-native data protection capabilities for Commvault Complete Data Protection, focusing mainly on AWS, Microsoft Azure and Google Cloud Platform. It also announced two HyperScale X appliances — HS2300 and HS4300 — with increased capacity and performance. Commvault also rolled out key features to its Metallic SaaS platform — backup for SAP HANA, Oracle, Salesforce, files and Kubernetes. The Commvault Metallic service was also made available in EMEA and the Asia/Pacific region.

Strengths

- **Deployment flexibility** — Commvault's customers can select one or a combination of software-only, appliance or SaaS solutions based on the organization's requirements. All three environments can be managed through Commvault Command Center or Metallic, thus providing a unified management experience.
- **Cloud-native protection** — Commvault Complete Data Protection combined with Commvault Metallic protects all major public cloud IaaS, PaaS and SaaS workloads, offering a comprehensive multicloud data protection solution. Commvault was able to provide several customer references that protect over 1,000 virtual instances and manage petabyte-plus storage in AWS and Microsoft Azure.
- **Data protection as a service** — An aggressive feature release cadence and rapid geographic expansion ensure that Commvault Metallic is well-positioned to address customers that are transitioning to an as-a-service model in hybrid infrastructure environments.

Cautions

- **Release cadence and code quality** — Commvault's frequent feature releases for its Commvault Complete Data Protection platform has resulted in a relatively high number of issues and hotfixes, indicating an inadequate prerelease quality assurance testing process.
- **High acquisition and maintenance costs** — Commvault's large enterprise customers and prospects report that Commvault Backup & Recovery is offered at higher price points when compared to the competition. Commvault's customers also express concern regarding high maintenance costs.
- **Commvault HyperScale X and Red Hat** — The HyperScale X appliance is built on the Red Hat operating system, thus creating an external dependency for providing OS updates and important patches.

Dell Technologies

Dell Technologies is a Leader in this Magic Quadrant. Its backup and recovery software portfolio mainly consists of the Dell EMC Data Protection Suite, composed of Avamar, NetWorker and PowerProtect Data Manager. Its appliance portfolio is composed of the PowerProtect DP series (integrated appliances) and PowerProtect DD Series (target-based appliances). Dell Technologies' operations are geographically diversified, and its clients span the midmarket and enterprise segments of the market. In the last 12 months, the vendor made four major software updates to PowerProtect Data Manager. These updates include support for application-consistent backups in Kubernetes, including VMware Tanzu Kubernetes, SAP HANA backup; guest workload support for AWS, Azure and Google Cloud Platform; and improvements to Oracle Database and VMware backup, including protection of VMware Cloud Foundation infrastructure. In August 2020, Dell Technologies discontinued Dell EMC PowerProtect X400 in an effort to consolidate its appliance portfolio.

Strengths

- **Anti-ransomware solutions** — The Dell EMC PowerProtect Cyber Recovery solution offers comprehensive ransomware detection and recovery capabilities both on-premises and in the public cloud. The solution supports an immutable and air-gapped architecture, and meets Sheltered Harbor recommendations.
- **VMware relationship** — The Dell EMC Data Protection Suite provides deep integration with VMware by integrating with vSphere APIs for backup and offering plug-ins for vRealize Suite automation, DR to cloud and support for VMware Tanzu Kubernetes environments.

- **Solution selling** — Enterprise customers usually purchase the Data Protection Suite as part of a larger solution that often includes servers, storage and system management software, thus simplifying vendor management and providing a one-stop-shop experience. The Data Protection Suite also provides deep integration with storage products in the portfolio.

Cautions

- **Dependency on third-party vendors** — Dell Technologies depends on OEM technology for protecting Nutanix AHV VMs and OpenStack environments, as well as for granular search and restore for Microsoft Exchange, SharePoint and SQL Server.
- **Public cloud product complexity** — With multiple products addressing cloud-native data protection requirements — PowerProtect Data Manager, PowerProtect Cloud Snapshot Manager, Avamar Virtual Edition, NetWorker Virtual Edition and PowerProtect DD Virtual Edition — Dell Technologies creates the same level of complexity and overlap associated with its on-premises solutions in the public cloud.
- **Change management** — PowerProtect Data Manager's focus on new feature support implies that large enterprises with a broad application set will continue to implement multiple tools from Dell Technologies or other vendors, as part of their backup infrastructure.

Druva

Druva is a Visionary and a new entrant in this Magic Quadrant. The Druva Cloud Platform is a BaaS-based offering that leverages AWS infrastructure for storing and managing backup data. The platform consists of three products: Phoenix for server backup, inSync for SaaS applications and endpoint backup, and CloudRanger for cloud-native backup and DR. Druva's operations are geographically diversified, with clients tending to be in the midmarket and enterprise segment, and mainly using the platform to protect distributed environments, endpoints, cloud-native services and SaaS applications. Capabilities delivered in the last year include a ransomware recovery service, integrated backup and archiving for network-attached storage (NAS) data, Azure Active Directory integration, and enhancements for Oracle and Microsoft SQL Server backup. Druva acquired sfApex in November 2020 to improve its Salesforce data protection capabilities.

Strengths

- **SaaS delivery model** — The Druva Cloud Platform is offered as a SaaS-based platform, and therefore simplifies management, minimizes operational overhead and allows customers to benefit from the pay-as-you-go pricing model.

- **Data management** — The metadata pipeline and repository provide for differentiated search and analytics capabilities that enable use cases such as e-discovery, ransomware detection and recovery, and storage optimization.
- **SaaS application data protection** — Druva backs up and securely stores a broad range of SaaS applications, including all major Microsoft Office 365 offerings, Google Workspace, Salesforce and Slack.

Cautions

- **Limited enterprise data center presence** — Druva has limited references for protecting large enterprise data center environments.
- **Limited public cloud breadth** — Support for non-AWS public cloud IaaS environments such as Microsoft Azure and Google Cloud Platform is largely a work in progress.
- **Local backup copy** — Druva offers limited support for storing local backup copies when protecting on-premises data center environments. Phoenix CloudCache, a software appliance used to store local copies, has limited scalability and resilience, and stores backups for retention periods of up to 30 days only.

IBM

IBM is a Challenger in this Magic Quadrant. Its Spectrum Protect portfolio consists of Spectrum Protect, Spectrum Protect Plus, Spectrum Protect Snapshot and Spectrum Copy Data Management. Together, they address data protection and reuse requirements for a broad range of applications. IBM's operations are geographically diversified, and its clients tend to be in the large enterprise segment of the market. In the past year, the vendor released two updates for Spectrum Protect and Spectrum Protect Plus. Key feature announcements included Spectrum Protect Plus availability in the AWS marketplace, enhancements to Kubernetes backup and support for Google Cloud object storage as a backup target.

Strengths

- **Container backup** — IBM Spectrum Protect Plus offers a comprehensive solution for container backup. It provides automated discovery of container environments and protects persistent volume claims (PVCs) and metadata (etcd) for OpenShift and Kubernetes managed containers.

- **Backup immutability** — Spectrum Protect Plus stores the primary backup data as immutable snapshots on its disk storage repositories (vSnap). Backup copies can also be transferred to WORM-supported media such as IBM Cloud Object Storage (COS) or tape for air-gapped protection.
- **Simplified deployment experience** — All Spectrum Protect Plus components are packaged into a single OVA file that can be used to deploy the backup software as a virtual appliance in VMware and Hyper-V environments. IBM Blueprints provides prevalidated reference architectures and sizing guidelines that further simplify the deployment experience.

Cautions

- **Cloud-native data protection** — The Spectrum Protect suite does not integrate with Azure-native snapshot APIs. Backup of Google Cloud Platform environments, DBaaS offerings such as AWS RDS and Azure Managed SQL, and SaaS workloads such as Microsoft Office 365 SharePoint Online, Microsoft Teams, Google Workspace and Salesforce is not supported.
- **Dependency on third-party vendors** — IBM depends on third-party vendors to address backup requirements for Microsoft SharePoint, Microsoft 365 Exchange Online, some NoSQL databases, Nutanix AHV VMs, OpenStack environments, hardware snapshot management and bare-metal recovery of operating systems.
- **Postsales support experience** — The Spectrum Protect suite trails market leaders in its ability to provide proactive issue discovery through AI and automated incident management and response.

Micro Focus

Micro Focus is a Niche Player and a new entrant in this Magic Quadrant. It leads with Data Protector, a platform that primarily protects workloads in physical and virtual environments. Data Protector is offered in two editions — the Express edition, mainly for virtual environments, and the Premium edition, positioned for virtual and physical environments, and integration with cloud environments. The vendor's operations are geographically diversified, and its clients tend to be mainly in the midmarket segment. Key capabilities announced last year were support for Microsoft 365 Exchange Online, improved Hyper-V backup by integrating with change block tracking capability and integration with Hewlett Packard Enterprise (HPE) Primera storage array snapshots.

Strengths

- **Pricing** — Data Protector Express edition offers one of the lowest price-per-socket licensing among the vendors evaluated in this research.
- **Ecosystem integration** — Data Protector integrates with the hardware snapshot capabilities of a number of primary storage array vendors, and supports a broad range of purpose-built deduplication appliance target vendors.
- **Product localization** — Data Protector is localized in four languages, thus addressing country-specific language preferences.

Cautions

- **Widening capability gap** — Micro Focus trails the competition in its ability to provide data protection capabilities for public cloud IaaS, SaaS and hyperconverged infrastructure (HCI). It lacks critical anti-ransomware functionality such as detection of anomalous conditions, isolated recovery orchestration and integration with third-party malware scanners.
- **User Interface** — Data Protector provides a legacy non-web-based UI that significantly trails the competition in user experience.
- **Partner enablement** — Customers sourcing Data Protector through partners must ensure that they select a credible partner with adequate deployment and support experience with Data Protector. Micro Focus' partner enablement for Data Protector, post its acquisition of HPE's software business, remains a work in progress.

Rubrik

Rubrik is a Leader in this Magic Quadrant. Its product portfolio mainly consists of Rubrik Cloud Data Management (RCDM), its core backup software platform; Polaris, a SaaS-based platform that provides centralized visibility and management, and leverages metadata to provide ransomware assessment, recovery and data classification; and Mosaic, for protection of NoSQL workloads. Rubrik's operations are geographically diverse, and its clients are mainly in the large enterprise segment of the market. In the last 12 months, it had two major releases of RCDM that added backup support for AWS RDS, Microsoft Office 365 OneDrive, SAP HANA on Google Cloud Platform and VMware Cloud on AWS. These releases also focused on improving backup and recovery performance of Oracle, SQL Server and VMware environments. In December 2020, Rubrik acquired Igneous, a vendor that specializes in scale-out NAS data management for cloud-based archival and recovery.

Strengths

- **Centralized monitoring and management** — The Polaris SaaS platform provides centralized visibility of multiple Rubrik cluster deployments located either on-premises or in the cloud, protection of IaaS instances, SaaS applications, and integrated security and workflow management.
- **Operational simplicity and automation** — Gartner Peer Insights customer reviews and Gartner client inquiries indicate that Rubrik offers an intuitive UI that is easy to operate and scales well. The platform offers a comprehensive set of APIs for policy management that can be integrated with third-party orchestration tools to automate complex workflows.
- **Database support** — RCDM supports granular and comprehensive support for all major relational databases and NoSQL databases. Instant recovery of Microsoft SQL Server and Oracle Database, and a change block tracking (CBT) driver for SQL databases are key capabilities that help reduce backup recovery time objective (RTO) and recovery point objective (RPO).

Cautions

- **SaaS backup application support** — Rubrik does not support backup of Salesforce and Google Workspace environments.
- **Public cloud costs** — RCDM requires a four-node VM cluster to be deployed in the public cloud to support granular protection and recovery of applications and databases hosted in public cloud IaaS. This increases the compute costs of running the backup infrastructure in the public cloud for non-cloud-native workloads.
- **Emerging markets** — Rubrik has a limited direct presence in emerging geographies when compared to other market leaders, requiring customers to ensure that they work with a credible partner and rely on local references.

Unitrends

Unitrends is a Niche Player in this Magic Quadrant. Its backup portfolio consists of the Unitrends Backup Software, Recovery Series Backup Appliance and Spanning Backup for SaaS application backup. The vendor's operations are geographically diverse, and its customers tend to be in the midmarket segment. In the last 12 months, Unitrends announced the Recovery Series Gen 9 appliances with improved capacity and performance. It also released UniView, a platform that offers central management of multiple Recovery Series appliances and SaaS applications, and has continued to improve security and analytics capabilities on its software platform.

Strengths

- **Integrated cloud storage for archival and DR** — Unitrends offers unlimited retention of backup data with no egress charges, and optional DR through its Unitrends Cloud data centers, at significantly lower costs when compared to public cloud providers.
- **SaaS backup** — Unitrends supports the data protection requirements of all major SaaS applications that support third-party backup, including Microsoft 365, Google Workspace and Salesforce through Spanning.
- **Appliance portfolio** — Recovery Series Gen 9 is offered in 15 different configurations, addressing a broad range of backup capacity and performance requirements. Appliances are sold as an annual subscription and include all software functionality, optional support for Unitrends Cloud and free hardware replacement every four years.

Cautions

- **Scalability** — The Unitrends Recovery Series Backup Appliance lacks a clustered file system and therefore offers limited scalability and may not suit enterprises with backup requirements of more than 100TB.
- **Public cloud backup** — Unitrends does not integrate with snapshot APIs provided by AWS EC2, Azure VMs or GCE.
- **Database support** — Unitrends does not support backup of Oracle RAC Database instances, and offers limited capabilities for backing up SAP HANA and NoSQL databases such as MongoDB and Cassandra. It does not back up DBaaS instances such as AWS RDS or Azure SQL Managed Instance.

Veeam

Veeam is a Leader in this Magic Quadrant. It leads with the Veeam Availability Suite (VAS), which is composed of Veeam Backup & Replication and Veeam ONE for backup monitoring and analytics. Backup for public cloud environments and DR orchestration is enabled through add-on products. Veeam's operations are geographically diversified, and its clients tend to be in the enterprise and midmarket segments. In the last 12 months, it announced new tools for Azure and Google Cloud Platform backup, an immutable backup repository option for Linux-based backup targets, and plug-ins for Oracle RMAN backup in AIX environments and SAP on Oracle. Veeam also significantly expanded its AWS backup capabilities by introducing support for AWS RDS, application-consistent EC2 backup, cross-region DR on AWS, change-block tracking with EBS volumes and support for AWS Outposts. In October 2020, Veeam acquired Kasten, thereby expanding its product portfolio to include container backup support.

Strengths

- **Instant recovery** — Veeam provides instant recovery of Hyper-V, VMware VMs and NAS environments, as well as automated instant recovery of Microsoft SQL Server and Oracle Databases, thus significantly reducing the recovery time of these workloads.
- **Cloud cost transparency** — Veeam provides administrators with a granular view of estimated cloud backup costs of various components when creating a backup policy for protecting AWS and Microsoft Azure instances. This helps users readjust backup policies, if required, and provides predictable pricing.
- **Technical support** — Veeam's customers express a high level of satisfaction with its technical support. This is augmented by the Veeam Intelligent Diagnostics feature that detects configuration and performance issues, and provides an option for automatic remediation via Veeam ONE.

Cautions

- **Deployment complexity** — Some customers report that large-scale Veeam deployments are complex to manage because the deployments typically include several components, including multiple backup servers, proxy servers, mount servers, agents and backup repositories.
- **Data reduction** — Veeam lacks global deduplication, thus increasing reliance on third-party deduplication appliances to reduce storage costs.

- **Automated tiering for cloud-native backup** — The vendor does not support automated tiering of AWS and Azure VM backup copies from hot cloud object storage tiers to low-cost storage tiers such as AWS Glacier or Microsoft Azure Archive Storage. This increases the storage costs of backups that require a longer retention period.

Veritas Technologies

Veritas Technologies is a Leader in this Magic Quadrant. Its backup product portfolio mainly consists of NetBackup, NetBackup Appliances and Backup Exec. Veritas' operations are geographically diversified, and its clients tend to be mainly in the large enterprise segment, with some presence in the midmarket. Veritas announced two major updates to NetBackup — 8.3 and 9.0. These updates include support for Azure Archive tiering, Azure Stack, AWS Outposts, VMware on AWS, VMware on Azure, and improvements for backup of Oracle, Microsoft SQL Server and NAS. Veritas also announced NetBackup Flex Scale, an integrated scale-out appliance reference architecture based on NetBackup 9.0. In January 2021, Veritas acquired HubStor, which specializes in protection of SaaS applications.

Strengths

- **Broad ecosystem support** — NetBackup supports a broad range of operating systems, hypervisors and public clouds, and integrates with all major primary storage array vendors.
- **Automation** — NetBackup 9.0 provides over 500 APIs that help automate deployment and policy management of large Veritas backup infrastructure deployments.
- **Backup to cloud** — NetBackup supports several public cloud storage targets. Media Server Deduplication Pool (MSDP) cloud servers deployed on-premises deduplicate backup data before sending it to the cloud storage target, thus reducing storage and bandwidth costs significantly. Backup data can be sent to multiple cloud storage targets from the same media storage pool.

Cautions

- **Integrated scanning** — Malware and security scanning in an isolated recovery environment, using third-party security engines, requires API integration or scripting.
- **Technical support** — Some Veritas' customers indicate that technical support quality and response time are substandard.

- **Complex appliance portfolio** — Customers evaluating Veritas' appliances must thoroughly understand the architecture differences and benefits of NetBackup Flex Scale, NetBackup Flex and NetBackup Appliances, as all three products have identical software attributes.

Zerto

Zerto is a Niche Player and a new entrant in this Magic Quadrant. The Zerto platform is a converged backup and DR solution aimed at protecting workloads both on-premises and in the cloud. Zerto's operations are geographically diversified, and its clients tend to be mainly in the enterprise segment, with some presence in the midmarket. During the evaluation period, it announced two major version updates to the Zerto platform — 8.0 and 8.5. These platform updates include support for VSS-based backup for Windows, support for AWS and Microsoft Azure as long-term retention targets, instant file recovery, and improvements in backup performance and capacity monitoring.

Strengths

- **Converged backup and DR solution** — Zerto provides a single platform that combines backup and DR functionality, thus simplifying data protection architectures. Its CDP-based architecture allows for very low RPOs.
- **Operational simplicity** — Gartner Peer Insights customer reviews and Gartner client inquiries indicate that Zerto offers an intuitive UI that facilitates ease of use.
- **Cross-platform recovery** — The Zerto platform supports recovery of VMware or Hyper-V VMs on AWS or Microsoft Azure, thus providing multiple options for recovery.

Cautions

- **Credibility as a backup provider** — Given its nontraditional architecture, Zerto is not viewed as a direct buying alternative to traditional backup vendors. Customers selecting Zerto must thoroughly understand its architecture and infrastructure requirements, and ensure that backup capabilities such as application consistency, granular recovery and retention period requirements are addressed.
- **Anti-ransomware capabilities** — Zerto offers no support for malware detection, relies on third-party storage repositories for providing backup immutability, and trails the competition on identification of clean backup copies and providing an isolated recovery environment. Due to architectural limitations, Zerto does not support air-gapping capabilities.

- **Public cloud backup** — Zerto does not support backup of AWS EC2 instances into the same availability zone. Backup of Microsoft Azure instances requires customers to install two Zerto Cloud appliances in the same region, thus increasing management complexity.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

- Druva
- Micro Focus
- Zerto

Dropped

- Actifio

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that analysts believe are necessary for inclusion in this research.

Gartner analysts have assessed that the vendor can effectively compete in the enterprise backup and recovery software solution market.

Gartner has determined that the vendor is a significant player in the market, due to market presence, competitive visibility and/or technology innovation.

The vendor must meet at least one of the following revenue criteria:

- Revenue must be derived solely from its backup and recovery product portfolio. This revenue should not include revenue generated from implementation services or managed services.

- The vendor must have generated revenue of greater than $50 million (GAAP) from the sale of product licenses and maintenance over the last four quarters (as of 1 March 2021).

or

- The vendor must have generated subscription revenue of greater than $25 million (GAAP) over the last four quarters (as of 1 March 2021).

or

- The vendor must have generated a revenue of greater than $25 million (GAAP) from the sale of product licenses and maintenance over the last four quarters (as of 1 March 2021) combined with a growth rate of 20% or greater from the prior four quarters.

The vendor's qualifying backup and recovery solutions must be sold and marketed primarily to upper-end midmarket and large enterprise organizations. Gartner defines the upper-end midmarket as being 500 to 999 employees, and the large enterprise as being 1,000 employees or greater.

The vendor must employ at least 100 full-time employees in engineering, sales and marketing functions combined.

The vendor's qualifying backup and recovery solution must focus on protecting enterprise environments running in the data center. The data center can be either a traditional one or a colocation facility. Protection of cloud-based IaaS, PaaS and SaaS workloads and remote sites is seen as an extension to these core capabilities.

The vendor must have at least one backup and recovery solution commercially available for use by enterprises for three calendar years prior to 1 March 2021 (it must have been commercially available at least as early as March 2018).

New products or updates to existing products that were released in the last 12 months must have been generally available on or before 31 March 2021 to be considered for evaluation.

The vendor must serve an installed base of at least 1,000 customers within the market, as defined in the Market Definition/Description section. In addition, at least 250 of the 1,000 customers must have deployed the backup solution for a minimum of 100 physical servers or 100 virtual servers in a single deployment site or cloud region. This excludes endpoint backups.

The vendor must actively sell and support its backup and recovery products under its own brand name in at least two of the following major regions: North America, Europe or the Asia/Pacific region. At least 20% of total revenue and existing customer count must originate from outside of its major region.

The vendor solution must support backup and granular restores of data in at least the following environments:

- Hypervisor: VMware and Hyper-V via integration with backup frameworks provided by these hypervisors
- Applications: Microsoft Exchange and Microsoft SharePoint, or support Microsoft Office 365 backup
- Operating Systems: Windows, Linux
- Databases: Database-consistent copies of Oracle and Microsoft SQL Servers

Product may be sold either as a software-only offering or as an integrated backup storage appliance (backup application plus backup storage in a single integrated offering).

The following exclusion criteria apply:

- Vendors offering products or solutions with software that is sourced entirely from a third-party ISV.
- Products that serve only as a target or destination for backup, but do not actually perform the backup and restore management function. Examples include purpose-built deduplication appliances, SAN, NAS or object storage.
- Vendors that back up directly to the public cloud without storing a local copy on-premises.
- Vendors with a main source of product revenue (more than 75% of total revenue) that comes from data center hosts and managed service providers.

- Products or solutions that are designed and mainly positioned as solutions for backing up endpoints such as laptops, desktops and mobile devices.
- Products or solutions that are designed and positioned as solutions to back up remote offices, edge locations and lower midmarket/SMB environments.
- Products or solutions designed for homogeneous environments, such as tools designed to back up only Microsoft Hyper-V or VMware, or Red Hat or containers.
- Products or solutions designed to back up specific storage or hyperconverged system vendors.
- Products that serve only as replication and DR tools.
- Products that serve primarily for managing snapshot and replication capabilities of storage arrays.
- Products that are positioned mainly for copy data management.
- Products that are mainly continuous data protection solutions.

Evaluation Criteria

Ability to Execute

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	Low
Customer Experience	High
Operations	NotRated

Source: Gartner (July 2021)

Completeness of Vision

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Medium

Source: Gartner (July 2021)

Quadrant Descriptions

Leaders

Leaders have the highest combined measures of Ability to Execute and Completeness of Vision. They have the most comprehensive and scalable product portfolios. They have a proven track record of established market presence and financial performance. For vision, they are perceived in the industry as thought leaders and intellectual property (IP) creators, and have well-articulated plans for enhancing recovery capabilities, improving ease of deployment and administration, and increasing their scalability and product breadth. For vendors to have long-term success, they must aim to support data protection requirements of hybrid IT. A cornerstone for Leaders is the ability to articulate how new requirements will be addressed as part of their vision for recovery management.

As a group, Leaders can be expected to be considered as part of most new purchase proposals and to have high success rates in winning new business. This does not mean, however, that a large market share alone is a primary indicator of a Leader. Leaders are strategic vendors, well-positioned for the future having established success in meeting the needs of upper-midsize and large data centers.

Challengers

Challengers can execute today, but may have a more limited vision than Leaders, or have yet to fully produce or market their vision. They have capable products and can perform well for many enterprises. These vendors have the financial and market resources and the capabilities to potentially become Leaders. Yet, the important question is whether they understand the market trends and market requirements to succeed tomorrow, and whether they can sustain their momentum by executing at a high level over time.

A Challenger may have a robust backup portfolio, but not yet been able to fully leverage its opportunities or does not have the same ability as Leaders to influence end-user expectations and/or be considered for substantially more or broader deployments. Challengers may not aggressively compete outside their existing account base and focus mainly on retention. These vendors may not devote enough development resources to delivering products with broad industry appeal and differentiated features in a timely manner, or may not effectively market their capabilities and/or fully exploit enough field resources to result in a greater market presence.

Visionaries

Visionaries are forward-thinking, advancing their portfolio capabilities ahead, or well ahead, of the market, but their overall execution has not propelled them into being Challengers or possibly Leaders. (Often, this is due to limited sales and marketing, or elongated time to initially install and configure, but is sometimes due to scalability or breadth of functionality and/or platform support.) These vendors are predominantly differentiated by product innovation and perceived customer benefits. However, because some are relatively new to the market, they have not yet achieved solution completeness or sustained broad sales, and marketing and mind share success, nor demonstrated the continued successful large-enterprise deployments required to give them the higher visibility of Leaders.

Some vendors move out of the Visionaries quadrant and into the Niche Players quadrant because their technology is no longer visionary (the competition caught up to them). In some cases, they have not been able to establish a market presence that justifies moving to the Challengers or Leaders quadrants, or even remaining in the Visionaries quadrant.

Niche Players

It is important to note that Gartner does not recommend eliminating Niche Players from customer evaluations. Niche Players are specifically and consciously focused on a subsegment of the overall market, or they offer relatively broad capabilities without very large-enterprise scale or the overall success of competitors in other quadrants. In several cases, Niche Players are very strong in the upper-midsize-enterprise segment, and they also opportunistically sell to large enterprises, but with offerings and overall services that, at present, are not as complete as other vendors focused on the large-enterprise market.

Niche Players may focus on specific geographies, vertical markets, or a focused backup deployment or use-case service; or they may simply have modest horizons and/or lower overall capabilities compared with competitors. Other Niche Players are too new to the market or have fallen behind, and, although worth watching, have yet to fully develop complete functionality or to consistently demonstrate an expansive vision or the Ability to Execute.

Context

Infrastructure and operations (I&O) leaders tasked with backup operations must redesign the backup infrastructure to include the following aspects of technology, operations and consumption:

- Invest in backup solutions that address data protection requirements in the data center, public cloud and edge environments. Favor solutions that offer a single pane of glass to manage these distributed environments.
- Choose backup solutions that provide a comprehensive solution for ransomware detection and recovery from ransomware attacks.
- Understand thoroughly the level of resilience provided on the primary backup copy and the need to invest in additional backup copies to ensure backup resilience.
- Choose products that offer a secure and granular recovery testing experience.
- Align the backup architecture with your organization's operational recovery needs. Optimize backup storage usage by using disk-based backup appliances or SAN storage for operational recovery, and either tape or object storage for long-term retention.
- Thoroughly understand the long-term total cost of ownership of moving from perpetual licensing to subscription-based licensing models. For subscriptions, understand the cost implications of annualized payments versus upfront payments, and of exiting the subscription before the term is complete.
- Understand the long-term cost implications of various pricing models offered by vendors — VM-based, socket-based, node-based, front-end TB, back-end TB and agent-based. Invest in the right model based on the application and infrastructure roadmap of the organization.
- Select vendors that support tiering of backup copies to the public cloud to save on on-premises storage costs. Choose solutions that support recovery of applications from backup copies in the public cloud to address test/development or DR use cases.
- Select vendors that are able to augment the value of backup data by making it available to address compliance requirements, support analytics, reuse backup data for test/dev and provide add-on capabilities such as DR.

Market Overview

The enterprise backup and recovery software market underwent significant transformation in the past two years. Backup vendors evaluated in this Magic Quadrant mainly focused on the following areas:

- **Centralized management:** As enterprises move toward a hybrid IT model, and workloads are distributed across the data center, public cloud and the edge, protecting these workloads, irrespective of location, is critical. Leading backup vendors are addressing this by offering a management platform that can be deployed either in the main data center or as a service hosted in the public cloud.

- **Ransomware resilience, detection and remediation:** The recent increase in the number of ransomware attacks has resulted in vendors taking concrete steps toward providing ransomware detection and remediation as well as a resilient backup infrastructure. While most vendors support the creation of immutable second copies of backup through write once, read many (WORM)-enabled storage, others such as IBM and Rubrik aim to make the primary backup repository more resilient by supporting immutable snapshots. Leading vendors are building capabilities to detect ransomware attacks by tracking large changes to file system data, and through other means, by partnering with security vendors or by developing these capabilities in-house. Most vendors also aim to simplify the ransomware recovery process through creation of an isolated test environment, and provide a clean backup copy to recover specific files. Such efforts remain largely a work in progress.

- **Support for public cloud IaaS and PaaS backup:** During the evaluation period, leading on-premises backup vendors increased their investment toward building capabilities to protect cloud-native workloads, particularly VMs and applications hosted in AWS, Microsoft Azure and Google Cloud Platform. Some backup vendors are also supporting backup of DBaaS products such as Amazon RDS, Amazon Aurora and Microsoft Azure SQL. While some vendors integrated the backup software with the native snapshot capabilities offered by these cloud providers, most continue to reuse their existing backup software “as is” in the cloud to provide agent-based backup of the applications hosted in the cloud.

- **Support for SaaS-based applications:** In the past two years, I&O leaders have begun to include SaaS applications such as Microsoft Office 365, Google G Suite and Salesforce as a part of their backup strategy. Most vendors evaluated in this research have started delivering Office 365 backup via partners or developing these capabilities in-house. Protecting G Suite and Salesforce remains largely a work in progress.

- **Tiering to the public cloud:** Most vendors evaluated in this Magic Quadrant support tiering backup data to the public cloud. This reduces on-premises backup storage costs. The most commonly supported public cloud storage targets are Amazon Simple Storage Service (Amazon S3) and Azure Blob storage. Backup data in most cases is self-describing, meaning that if the on-premises data and catalog are lost, then an instance of the backup software can be reinstalled in the cloud and data can be restored. Some vendors also integrate with the life cycle policies of cloud providers (for example, data migration from AWS S3 to Glacier, or Azure Blob to Azure Archive Blob storage).

- **Recovery in the public cloud:** Today, leading backup vendors support restoring backup data to servers in the public cloud. An instance of the backup software can be installed in the public cloud, and backup data can be restored to a compute instance in the public cloud. This provides quick operational recovery if the on-premises environment is not available. The backup data can also be used for test/development purposes in the public cloud.

- **NoSQL database backup:** While traditional enterprises continue to run their core business applications on relational database management system (RDMS) databases such as Oracle and Microsoft SQL, Mode 2 projects such as big data usually leverage NoSQL databases such as MongoDB and Cassandra. As these projects begin to scale and deliver tangible value, there is a growing need to protect such environments. Established vendors such as Commvault, Dell Technologies and Veritas Technologies have started addressing these backup requirements by building such capabilities natively into the backup platform. Vendors such as Rubrik and Cohesity have made strategic acquisitions in this space.

- **Instant recovery of databases and virtual machines:** A majority of vendors support instant recovery of VMs by mounting the backed-up VM directly on the production host via NFS. VMs can thus become instantly available, while the actual recovery process can be initiated in the background. Similarly, vendors such as Cohesity and Rubrik offer instant recovery of databases such as Microsoft SQL and Oracle.

- **Container backup:** Leading vendors announced support for container backup either by building these capabilities natively into their existing platform or through acquisitions. While Gartner client inquiries show low interest for container backup, we anticipate that it will increase in adoption over the next two years, as more containers using persistent storage are deployed to support production workloads.

- **Subscription licensing:** Enterprises that are migrating to the public cloud find the subscription-based model a simpler way to procure backup solutions. While subscription-based licensing is not necessarily less expensive compared to perpetual licensing, it is more predictable and easier to manage.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

Document Revision History

Magic Quadrant for Data Center Backup and Recovery Solutions - 20 July 2020

Magic Quadrant for Data Center Backup and Recovery Solutions - 10 October 2019

Magic Quadrant for Data Center Backup and Recovery Solutions - 31 July 2017

Magic Quadrant for Data Center Backup and Recovery Software - 8 June 2016

Magic Quadrant for Enterprise Backup Software and Integrated Appliances - 15 June 2015

Magic Quadrant for Enterprise Backup Software and Integrated Appliances - 16 June 2014

Magic Quadrant for Enterprise Backup/Recovery Software - 5 June 2013

Magic Quadrant for Enterprise Backup/Recovery Software - 11 June 2012

Magic Quadrant for Enterprise Disk-Based Backup/Recovery - 28 January 2011

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

How Markets and Vendors Are Evaluated in Gartner Magic Quadrants

Market Guide for Backup as a Service

Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware

Designing and Implementing a Ransomware Defense Architecture

5 Key Challenges You Must Solve With Your Next Backup Platform

Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware

---

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Product or Service	High
Overall Viability	High
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	Low
Customer Experience	High
Operations	NotRated

Source: Gartner (July 2021)

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Medium

Source: Gartner (July 2021)