Magic Quadrant for Enterprise Backup and Recovery Software Solutions

7 August 2023 - ID G00776884 - 43 min read

By Michael Hoeck, Nik Simpson, **and 2 more**

As enterprises expand their use of hybrid and multicloud environments and SaaS applications, while managing the adaptive threat of ransomware attacks, I&O leaders must continually assess their backup and recovery capabilities. This research provides analyses of backup and recovery vendors.

Market Definition/Description

Gartner defines enterprise backup and recovery software solutions as vendor-developed solutions that capture a point-in-time copy (backup) of enterprise workloads in on-premises, hybrid, multicloud and SaaS environments. These solutions write the data to a secondary storage target for the purpose of recovering this data in case of loss. They can be offered as software-only, hardware or virtualized appliance, or as a SaaS-based, backup as a service (BaaS).

Protecting and recovering business application data irrespective of the underlying infrastructure type and location is now more critical than ever before. As enterprises move toward more complex environments that include mass amounts of data, enterprise backup and recovery software solutions are expected to protect these workloads, whether they reside in on-premises, hybrid, multicloud or SaaS environments.

Enterprise backup and recovery software solutions are vital to an organization's ability to recover data following events that cause data to become inaccessible. Whether the event is accidental, malicious or environmental, organizations utilize these solutions to effectively recover and restore access to the affected data.

Solutions must offer effective capabilities to simplify management of data protection across complex enterprise environments. They must also ensure reliable recovery by protecting backup data against a constantly changing threat landscape, and expedite and orchestrate data recovery responses to traditional disaster and ransomware events.

Must-have capabilities of a backup and recovery solution include:

- Backup and recovery of data located in on-premises data center infrastructure, including operating systems, files, databases, virtual machines and applications
- Backup and recovery of data located in public cloud infrastructure, including multicloud and hybrid cloud, architectures, and environments such as infrastructure as a service (IaaS), platform as a service (PaaS) and SaaS
- Create multiple point-in-time copies of the backup to support resiliency, disaster recovery and other use cases
- Assignment of multiple backup and retention policies that align with the organization's recovery point-and-time objectives
- Report success and failure of backup/recovery tasks

Standard capabilities of a backup and recovery solution include:

- Tier backup data to multiple targets, including public cloud, backup and recovery provider, and object storage
- Integration with immutable backup storage target(s) or backup and recovery vendor's own immutable storage
- Orchestrate disaster and ransomware recovery testing and processes
- Centralized console for management of distributed backup solution infrastructure

Optional capabilities that can be provided by the solution include:

- Expand backup data use cases to support data discovery, compliance, copy data management, test/development and e-discovery
- Protect other workloads, including containers, object storage, edge/remote branch office sites and endpoints
- Vendor-developed or integrated ransomware data anomaly and malware detection
- Immutable data vaults and/or isolated recovery environments
- Bare-metal recovery

Magic Quadrant

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

Vendor Strengths and Cautions

Acronis

Acronis is a Niche Player in this Magic Quadrant. Acronis's backup portfolio consists of its on-premises solution Acronis Cyber Protect and cloud-hosted offering Acronis Cyber Protect Cloud. Both provide integrated backup, security and endpoint management for physical servers, on-premises virtual machines (VMs), SaaS workloads, public cloud IaaS workloads and endpoints. Most of its clients are in the midmarket. The products are delivered by a direct sales force and more than 20,000 service providers through 52 Acronis data centers spread across all major geographies. During the evaluation period, Acronis added several new features. These include support for the Dell PowerProtect DD retention lock feature, One Click Recovery, an end-user-initiated recovery from last

known backup, machine learning (ML)-assisted backup validation, and disaster recovery and failback for Microsoft Azure VMs to the Acronis Cloud.

Strengths

- **Integrated cyber and data protection capabilities for endpoints, application servers and public cloud IaaS deployments:** Acronis delivers a single, agent-based offering that combines security, backup and disaster recovery (DR), and IT management for endpoints, workstations, application servers and public cloud IaaS deployments in Azure and AWS.
- **Broad hypervisor support:** Acronis offers support for a broad set of hypervisors beyond VMware and Microsoft such as, Citrix XenServer, Virtuozzo, Red Hat, Oracle VM, Nutanix, Linux KVM and Scale Computing.
- **Global coverage in multiple languages:** Acronis offers a globally available and differentiated data protection solution for remote sites/edge locations for servers and endpoints localized in more than 25 languages.

Cautions

- **Limited enterprise and public cloud capabilities:** Acronis lacks critical enterprise capabilities, with limited support for enterprise databases, cluster architectures, operating systems, network-attached storage (NAS), enterprise storage integration, storage pooling, deduplication and public cloud application support.
- **Limited scalability:** Acronis's agent configured direct-to-backup-storage architecture is less suitable for large enterprise deployments due to missing enterprise functionalities and limited scalability.
- **Commercial focus on managed service providers (MSPs):** Acronis focuses mostly on selling through MSPs to provide a managed solution delivering backup, DR, cybersecurity, collaboration and endpoint management. With this go-to-market approach, commercial relationships and customer experience, including support, security and performance, will be a primary responsibility of the chosen MSP.

Arcserve

Arcserve is a Challenger in this Magic Quadrant. Arcserve's backup portfolio includes Arcserve UDP, Arcserve Backup, Arcserve UDP Appliances, Arcserve Cloud Direct, Arcserve UDP Cloud Hybrid Secured by Sophos, Arcserve OneXafe storage appliances and Arcserve SaaS Backup. Arcserve's operations are geographically diversified, and most of its clients are in the midmarket segment. During the evaluation period, Arcserve released UDP 9.0, which included enhancements for database support, a SaaS-based, cloud-hosted multitenant management console, and the ability to write backups directly to S3-compliant object storage. In addition to the UDP enhancements, Arcserve also made changes to backup appliances and storage appliances to improve performance and scalability.

Strengths

- **Broad workload support:** The combination of Arcserve Backup and Arcserve UDP give Arcserve the ability to support many enterprise workloads in data centers and public cloud. This broad workload support in combination with a scalable platform and multiple storage target integration options is able to protect multiple petabytes of data.
- **Direct-to-cloud object storage:** UDP allows customers to backup data direct-to-cloud object storage with deduplication. It is compatible with AWS S3, Wasabi and Google Cloud Storage.
- **Performance and capacity improvements for OneXafe storage appliances:** OneXafe enhancements provide faster recoveries and larger scale at a smaller footprint with available solid-state drive (SSD) storage and individual disk drive capacity greater than 24TB.

Cautions

- **Limited detection and recovery capabilities:** Arcserve UDP bundled with Sophos anti-malware lacks anomaly detection capabilities and guidance to the recommended recovery points.
- **Limited OneXafe immutability:** The immutable design of OneXafe storage appliances lacks object storage locking and multiperson authentication controls, which limits its optimal data loss protection capabilities against ransomware and insider threats.
- **Lacks container backup:** Arcserve does not provide backup capabilities for container workloads.

Cohesity

Cohesity is a Leader in this Magic Quadrant. Its backup product portfolio consists of DataProtect and a BaaS offering called DataProtect delivered as a service. Cohesity's operations span across North America, Western Europe and Asia/Pacific. Its clients tend to be in the upper midmarket and enterprise segments. During the evaluation period, Cohesity introduced a vendor-managed cloud vault storage called FortKnox, which can be combined with threat detection and data classification capabilities in a new solution called DataHawk. It added DataProtect database integrations to expand SAP coverage and support PostgreSQL and Couchbase. Additionally, it announced an OEM partnership with IBM to include Cohesity's data protection as part of IBM's new Storage Defender solution.

Strengths

- **Unified and simplified management:** Cohesity Helios, a SaaS-based control plane, provides a centralized administrative experience that is common and intuitive for all products in its backup offering.
- **Multicloud BaaS and storage:** Cohesity DataProtect delivered as a service and FortKnox products allow customers to choose from multiple cloud data plane storage locations, including AWS and Azure.

- **Security alliance strategy:** Cohesity has proactively engaged multiple vendors with varying disciplines in the security market. The goal of its Data Security Alliance is to drive collaborative solutions and develop integrated products to more broadly address data security and resilience concerns of customers.

Cautions

- **New investments introduce reliance on third-party technology:** Cohesity's DataHawk solution includes dependencies on two new OEM partnerships to bolster its investments in recent add-on offerings.

- **Limited BaaS capabilities compared to customer managed:** Cohesity products and related features of FortKnox and DataHawk are not yet available to customers protecting their data with its BaaS offering, DataProtect delivered as a service.

- **Less geographic coverage:** Cohesity lags other leading vendors in market presence and execution in South America.

Commvault

Commvault is a Leader in this Magic Quadrant. Its portfolio includes Commvault Backup & Recovery, Commvault Disaster Recovery, Commvault HyperScale X, Metallic SaaS portfolio and Metallic ThreatWise. Commvault's operations are geographically diversified, and its clients tend to be large enterprises. During the evaluation period, Commvault introduced support for MongoDB Atlas, Hyper-V Live Recovery, Couchbase and Amazon VPC Protection, and a capability that scans backup content for malware during recovery. Commvault enhanced its Metallic offering by adding support for Azure databases, including SQL Server, Cosmos DB, MariaDB, MySQL and PostgreSQL, as well as support for self-service restores for Exchange Online and OneDrive.

Strengths

- **BaaS scope of coverage:** Commvault Metallic's comprehensive coverage of SaaS applications, multicloud, on-premises and endpoints is complemented by the addition of Oracle Cloud Infrastructure (OCI) protection, bring your own OCI object storage, and new offerings Metallic File and Object Archive, and Metallic ThreatWise.

- **Comprehensive software-based interoperability:** Commvault Backup & Recovery software provides broad coverage and capabilities for on-premises, hybrid and multicloud environments. Public cloud support now includes extensive support for Azure, AWS, GCP and OCI.

- **Bringing enterprise features to competitive pricing levels:** Commvault has priced its per-VM licensing for Commvault Backup & Recovery to gain entry into new market segments that may have otherwise been unavailable before.

Cautions

- **On-premises innovations lag cloud update cadence:** Commvault's product strategy updates Metallic BaaS before equivalent features are available for Commvault Complete Data Protection and HyperScale X products. This results in new features initially being available to the cloud-based subset of the Commvault customer base.

- **Variable Commvault Metallic customer experience:** Some Gartner clients have voiced concerns with challenges associated with inconsistent Metallic performance and initial configuration difficulties.

- **Inconsistent management capabilities:** Gartner Peer Insights reviews indicate that unified command and control between the Commvault Command Center HTML5 user interface lacks some features of the local application console.

Dell Technologies

Dell Technologies is a Leader in this Magic Quadrant. Its backup and recovery software portfolio consists of PowerProtect Data Manager, PowerProtect Cyber Recovery, CyberSense, Dell NetWorker, Dell Avamar, Dell APEX Backup Services, and PowerProtect DP series and PowerProtect DD series appliances. Dell's operations are geographically diversified, and its clients tend to be large enterprises, with presence in the midmarket. In the last 12 months, it enhanced PowerProtect Data Manager to include Microsoft Distributed File System backup and recovery, file-level recovery for Dynamic NAS Protection, and PowerProtect Cloud Snapshot Manager support for Google Cloud. New offerings include PowerProtect Data Manager Appliance (DM5500), PowerProtect Cyber for Azure and Google, and CyberSense for AWS.

Strengths

- **PowerProtect Cyber Recovery for cloud and on-premises:** Dell's data vault and ransomware recovery solution, called PowerProtect Cyber Recovery, now includes deployment options for on-premises, and AWS, Azure and Google cloud environments.

- **PowerProtect DD appliance scale:** Dell's introduction of Smart Scale allows PowerProtect Data Manager customers to combine capacity of multiple PowerProtect DD appliances, allowing simplified backup data balancing and migration between them.

- **PowerProtect Data Manager multicloud support and availability:** PowerProtect Data Manager provides consistent and comprehensive support for workloads in AWS, Azure and GCP. It is also readily available from the respective marketplaces and includes licensing for APEX Protection Storage.

Cautions

- **No SaaS-based control plane:** Dell lacks a comprehensive SaaS-based control plane and common administrative interface for all components of its solution, often found in leading vendor solutions.

- **Limited backup storage options:** PowerProtect DD appliances remain a requirement for use of most Dell data protection solutions, limiting the use of alternative backup targets.

- **Advanced ransomware data analysis requires a dedicated environment:** Advanced anomaly and malware detection requires a separate and dedicated PowerProtect DD appliance and additional compute infrastructure.

Druva

Druva is a Visionary in this Magic Quadrant. The Druva Data Resiliency Cloud platform is a BaaS offering that leverages AWS infrastructure for running, storing and managing backups. The platform consists of multiple products that provide on-premises and cloud VM backup and DR; AWS cloud-native and Kubernetes backup and DR; and SaaS application and endpoint backup. Druva's operations are geographically diversified, with most of its customers in North America. Its clients tend to be in the midmarket and enterprise segments. During the evaluation period, Druva added Salesforce Data Archiver, Data Lock, Unusual Data Activity and new integrations such as Windows Server 2022 Hyper-V virtual machine hosts, SAP HANA, VMware on Azure, VMs on Azure Stack and AWS S3. It also enhanced support for Nutanix AHV and accelerated incremental backup for NAS with Advanced Smart Scan.

Strengths

- **Scope of guarantee:** Druva Data Resiliency Guarantee offers a comprehensive scope of service-level objectives, including backup success rate, availability, immutability, durability and confidentiality.

- **Cloud-native BaaS solution architecture:** Building off its mature BaaS solution, Druva has made significant investment in a nondisruptive-to-customer redesign of its backup architecture platform to establish a new framework for future scalability, agility and multicloud capabilities.

- **Data center to cloud client experience:** Many customers convey a positive experience in use of Druva's BaaS for protecting SaaS application data, on-premises environments and cloud VMs.

Cautions

- **Limited native cloud workload protection capabilities:** Druva has been slow to expand its native cloud protection offerings compared to leading vendors. It lacks agentless integration with Azure VM, Google Compute Engine (GCE) and OCI. Workload integrations with Azure SQL, Azure Blob Storage, MongoDB and Cassandra are unsupported.

- **Narrow multicloud capabilities:** Druva's BaaS solution remains solely based on AWS cloud architecture for its control and data planes. It lags leading vendors that provide customer choice of multicloud data plane locations for their BaaS and vendor storage offerings.

- **Less comprehensive SaaS application backup integration:** Druva's expansion of protecting new SaaS applications is limited. It lacks support for MS Dynamics, Azure AD, ServiceNow, Azure DevOps and GitHub.

HYCU

HYCU is a Visionary in this Magic Quadrant. HYCU Protégé is a hybrid and multicloud BaaS platform that spans across Azure, AWS and Google to support IaaS, DBaaS, PaaS, SaaS and on-premises workloads. HYCU's operations are geographically diversified, with the majority of its customers in North America. Its clients tend to be in the upper midmarket. During the evaluation period, HYCU introduced several new capabilities like a free tier for AWS, added support for Azure Government, impact-free file share backup, and edge and ROBO workloads. In addition, HYCU introduced R-Cloud, a low-code development platform for vendors to develop SaaS backup on the HYCU platform, together with R-Graph, an observability and dependency mapping tool for SaaS workloads.

Strengths

- **Ease of use:** Gartner client inquiries indicate a high level of satisfaction for ease of use, product stability, and management of backup and disaster recovery for the HYCU Protégé hybrid management solution.
- **Multicloud and hybrid support:** HYCU Protégé simplifies protection of multicloud and hybrid environments by supporting Azure, AWS, Google and data center workloads with a single unified SaaS solution.
- **SaaS backup:** R-Cloud has the potential to accelerate support for SaaS backup beyond the most popular SaaS applications, like Microsoft 365 and Salesforce.

Cautions

- **On-premises limitations:** HYCU's on-premises offering lags leading vendors in features such as global data deduplication, continuous data protection (CDP), support for container workloads and enterprise clusters such as Oracle RAC, and support for non-x86 workloads such as Power/AIX.
- **Limited ransomware detection capabilities:** HYCU is missing advanced backup data analysis-based ransomware detection, such as encryption and entropy detection, and recovery point guidance capabilities found in competitive offerings.
- **Customer responsible for on-premises storage and security:** HYCU has no direct control over on-premises storage and storage security, making customers responsible for setting up a secure solution for protecting backups against cyber attacks.

IBM

IBM is a Visionary in this Magic Quadrant. Its primary backup portfolio consists of IBM Storage Protect, IBM Storage Protect Plus, IBM Storage Protect Snapshot, IBM Storage Copy Data Management and IBM Storage Protect for Cloud. IBM's operations are geographically diversified, and its clients tend to be large enterprises. In the past year, the vendor released four updates for Storage Protect and Storage Protect Plus. Storage Protect additions include immutable storage on IBM Cloud Object Storage, object lock on Amazon S3 and operations center updates. Storage Protect Plus additions include support for Red Hat OpenShift clusters for IBM Z, SAP HANA and incremental forever backup for containers. Storage Protect for Cloud introduced support for Azure VM, BLOB, AD and File, Salesforce and Microsoft Dynamics 365.

Strengths

- **Product strategy:** IBM announced a strategic shift in its backup and recovery offerings by integrating it with its primary storage product line and multiple complementary OEM products. Storage Defender is positioned to deliver an integrated and unified cyber protection solution under a common control plane. IBM has partnered with Cohesity to replace its current VM protection capabilities and to provide the new SaaS-based control plane.

- **OpenShift container backup:** IBM has continued to make significant investments in IBM Storage Protect Plus for Red Hat OpenShift Kubernetes and IBM Cloud Paks backup and recovery. Recent additions include protection of Red Hat OpenShift environments that are attached to clusters, and cluster-scoped and namespace-scoped resources and updated CSI integrations with Ceph, IBM block storage and Hitachi NAS.

- **Microsoft 365 protection:** IBM Storage Protect for Cloud offers end-user, self-service restore for Microsoft Exchange Online, SharePoint Online, Teams, OneDrive and Groups.

Cautions

- **Portfolio shift in progress:** IBM's strategy and execution on the announced portfolio change is a work in progress. This new portfolio will impact existing and prospective customers as new replacement products are released. IBM customers will require multiple products, based on a greater number of ISV and OEM technologies, to meet their multicloud and hybrid data protection requirements.

- **Limited execution:** IBM has often changed its vision and product strategy for the integration and positioning of the former Spectrum Protect and Spectrum Protect Plus products, and has demonstrated limited success in its execution of these changes. This includes previous efforts to position Spectrum Protect Plus as its market-leading offering.

- **Limited cross-platform recovery capabilities:** IBM Storage Protect Plus requires customer or ISV API integrated disaster recovery solutions or use of ISV partner solutions to support cross-platform recovery.

Microsoft

Microsoft is a Niche Player and a new entrant in this Magic Quadrant. Its backup and recovery portfolio includes Azure Backup, Azure Site Recovery (ASR), Microsoft Azure Backup Server (MABS), System Center Data Protection (DPM) and Microsoft Azure Recovery Services (MARS) agent. Microsoft's operations are geographically diversified, and its clients tend to be of all sizes. In the last 12 months, Microsoft added several improvements to Azure Backup, like Azure Backup Instant Restore, Cross Zonal Restore of Azure VMs, Azure Vault-Archive, smart tiering, backup cost analysis, immutable vaults, multiuser authentication and improved encryption.

Strengths

- **Optimized offering for Microsoft dedicated customers:** Azure Backup and Azure Site Recovery are suitable offerings for backup and disaster recovery that protect workloads for a wide range (small to large enterprise) of customers primarily using on-premises Microsoft Windows and Azure VMs.
- **Comprehensive roadmap:** Microsoft articulates a very comprehensive roadmap with deep integration of existing and new upcoming features to enhance its backup security portfolio with several capabilities in public or private preview mode.
- **Low total cost of ownership (TCO):** Azure Backup and Azure Site Recovery offer a low TCO when compared to competitive third-party offerings.

Cautions

- **Minimal workload coverage:** Azure backup support matrix is limited to protection of on-premises Microsoft Windows Servers or Microsoft Windows VMs, Azure VMs, SQL Server in Azure VM, SAP HANA in Azure VM, Azure Files, Azure Postgres, Azure Blobs and Azure Disks. Other Microsoft PaaS and SaaS services such as Azure SQL Server, Azure AD, Azure DevOps, Dynamics 365 and Microsoft 365 are not covered.
- **No multicloud support:** Azure backup does not offer support for protection of AWS, Google, or other cloud services or SaaS services as it is dedicated to Azure and on-premises workloads.
- **Overlapping product offering:** Microsoft backup and recovery options are a complex mix of multiple, interconnected and overlapping products.

OpenText

OpenText is a Niche Player in this Magic Quadrant. It completed its acquisition of Micro Focus in January 2023. Its enterprise backup product portfolio primarily consists of two products: Data Protector for on-premises workloads and Data Protector for Cloud Workloads covering cloud IaaS and SaaS workloads. The vendor's operations are geographically diversified, and its clients tend to be in the midmarket segment. In the past year, OpenText enhanced Data Protector by improving support

for SAP HANA, role-based access control (RBAC), MongoDB and deduplication. Data Protector for Cloud Workloads added VM support for Azure Cloud, Azure Stack HCI, Google Cloud and Virtuozzo, and enhanced export and API integrations for Microsoft 365.

Strengths

- **Capacity-based pricing:** OpenText has improved its licensing model by simplifying a large number of SKUs into a single capacity-based part number. This approach gives customers an easily understood operating expenditure option for entry into a capacity-based, pay-as-you-go pricing model.
- **Traditional enterprise data center support:** Data Protector has broad data center backup capabilities. It supports a large number of workloads at low TCO compared to other vendors.
- **Broad storage target support:** Data Protector supports a broad range of purpose-built backup appliances, multiple storage protocols and tape libraries.

Cautions

- **Lacks anomaly and malware detection:** Data Protector significantly lags other vendors in ransomware anomaly and malware detection capabilities. These capabilities are in the OpenText ecosystem but have not yet been integrated into Data Protector.
- **Core product integration:** Covering a full range of data center and cloud workloads requires two separate products: Data Protector and Data Protector for Cloud Workloads, which lack any meaningful integration.
- **Unclear product positioning:** At this time, it is unclear if the product technology will be fully integrated into the larger OpenText portfolio or if it will continue as a stand-alone product.

Rubrik

Rubrik is a Leader in this Magic Quadrant. Its backup product portfolio consists of Rubrik Security Cloud, which is inclusive of multiple backup offerings, data security and advanced recovery. Rubrik's operations are geographically diverse, and its clients are mainly large enterprises. During the evaluation period, Rubrik introduced multiple new or enhanced capabilities. These include a new machine learning model for ransomware detection, support for ransomware detection in Nutanix and Microsoft hypervisors, improved recovery for VMware environments, a Data Security Command Center that helps organizations assess their overall security posture, and threat containment features to isolate malware in backups.

Strengths

- **Innovation in product strategy, pricing, branding and bundling:** Rubrik is innovative in its approach to expanding its security-focused offerings around backup and recovery, providing new pricing

options with competitive, capacity-based user tiers for Microsoft 365, and simplifying its branding and bundling of product packages.

- **Ransomware protection and recovery features:** Rubrik has a comprehensive and secure product offering that protects the backup system and data against cyberattacks, includes capabilities to detect anomalies and malware within the backup data, and provides efficient recovery features.
- **Enterprise adoption:** Rubrik's scaling capabilities and differentiated customer support continue to attract large enterprise organizations, replacing a variety of different competitive solutions.

Cautions

- **Balance of security with backup:** Some customers have expressed concern with Rubrik's ability to balance its data security offering initiatives while maintaining focus on emerging market requirements for backup.
- **Limited SaaS application coverage:** Rubrik has limited support of SaaS applications beyond Microsoft 365. Coverage is not yet available for applications such as Salesforce, Google Workspace, Microsoft Dynamics 365, Azure AD, ServiceNow, Azure DevOps and GitHub.
- **Narrow vendor-managed cloud storage offerings:** Rubrik only offers Azure storage for its BaaS and vendor-managed vault solutions.

Unitrends

Unitrends, a Kaseya company, 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 introduced a BaaS offering for Microsoft Azure VM backup and disaster recovery. Unitrends also automated license management for Microsoft 365 backup through Azure AD Security Groups, and enhanced Unitrends security with two-factor authentication through UniView. Additionally, Unitrends continues to extend UniView integration with other Kaseya infrastructure and security management products.

Strengths

- **Unified administration:** Unitrends UniView offers single administrative access to all components of the solution, including management of appliances, endpoint backup and SaaS applications.
- **Complete portfolio:** Unitrends continues to expand its software and appliance offerings with the addition of integrated cloud disaster recovery services.
- **Kaseya integration:** Unitrends continues to focus integration into the Kaseya IT Complete portfolio. This will streamline access to technical, billing and support resources, and provide more features for its customers.

Cautions

- **Narrow enterprise suitability:** With its focus on SMB and midsize enterprise markets, Unitrends' growth initiatives and limited scalability of appliances contribute to reduced suitability for large enterprise accounts.

- **Limited multicloud capabilities:** Unitrends Backup for Microsoft Azure only supports Azure VMs and lacks support for other workloads in Azure, such as Azure SQL and Azure Blob. Expansion to support other cloud providers, such as AWS and GCP, is work in progress.

- **Limited BaaS strategy:** Unitrends lags behind other major players whose vendor-managed BaaS solutions support multiple cloud and on-premises workloads, and other SaaS applications, such as Azure AD, ServiceNow and Microsoft Dynamics 365.

Veeam

Veeam is a Leader in this Magic Quadrant. Its backup portfolio consists of Veeam Data Platform, which is composed of Veeam Backup & Replication, Veeam ONE and Veeam Recovery Orchestrator.

Veeam's operations are geographically diversified, and its clients tend to be in the enterprise, midmarket and SMB segments. In the last 12 months, Veeam released 24 product updates, including Veeam v12, which contains several new features such as direct-to-object storage, immutability for Azure, improved NAS protection and deeper integration with Kasten. Veeam also introduced new pricing packages containing new combinations of its Data Platform products.

Strengths

- **Loyal and satisfied customer base:** Veeam's customer growth and retention, and its customers' participation level in user group communities and forums such as Veeam Community, indicate a loyal and satisfied customer base.

- **Hybrid and multicloud support:** The Veeam Data Platform is available for all three major public cloud providers where it offers a consistent hybrid, multicloud and cross-cloud recovery experience for the most commonly used workloads.

- **Large network of partners and MSPs:** Veeam offerings are available through an extended global network of authorized partners. This includes reseller, alliance, implementation and MSP partners.

Cautions

- **Slow response to key market trends:** Veeam has been slow to react to key market trends and customer expectations in offering vendor-hosted services, such as BaaS, SaaS-based control plane and storage vaults, and native, data analysis-based ransomware anomaly detection capabilities.

- **Overall complexity:** Some Gartner clients indicate that Veeam can be more complex to manage as the size of the backup environment increases. This includes deployment of separate Veeam agents per protected environment, management of multiple backup and storage proxies, and

proper selection and management of compute and storage infrastructure to align to performance and storage requirements.

- **Secure by implementation requirement:** Implementing a secure Veeam Data Platform requires clients to thoughtfully design, configure and manage the deployment to mitigate cyberthreats, integrating ransomware immutability and detection provided by third-party solutions.

Veritas

Veritas is a Leader in this Magic Quadrant. Its backup product portfolio consists of NetBackup, NetBackup Appliances and Backup Exec, and its Veritas Alta cloud offerings, which include Alta View, Alta BaaS, Alta Data Protection, Alta Recovery Vault and Alta SaaS Protection. Veritas's operations are geographically diversified. Its clients tend to be large enterprises, and it has some presence in the midmarket. In the last 12 months, it introduced its Alta cloud offerings, including its cloud-based SaaS control plane, BaaS, and expanded SaaS application support to include Salesforce and Google Workspace backup. NetBackup added support for 13 new database PaaS workloads, isolated recovery on Flex Scale appliances, malware scanning of NAS and GCP immutability.

Strengths

- **Comprehensive backup and management options:** The Veritas Alta cloud offerings, combined with the capabilities of NetBackup software and its scale-out and scale-up hardware appliances, provide enterprise clients with a comprehensive portfolio of backup and recovery capabilities, and multiple deployment and management options.

- **Cloud-native architecture:** NetBackup and Alta services run in Kubernetes clusters that run natively in Azure, AWS and GCP. In this design, the data plane services run independent of the management plane to deliver an elastic and inherently flexible multicloud architecture.

- **Broad geographical coverage:** Veritas and its partners can sell, deploy and support Veritas solutions in every major geography. This makes it easier for customers with worldwide responsibilities to find a backup solution that meets their technical and business requirements.

Cautions

- **Certain cloud products are new to market:** Veritas's new Alta BaaS and Alta View SaaS-based management offerings are new to the market. Little data is available regarding market adoption or customer satisfaction, requiring a comprehensive proof of concept (POC) to determine the customer experience levels of onboarding and performance.

- **Enterprise-centric product and services strategy:** Veritas's primary focus is on large enterprise customers in its Alta and NetBackup product and services strategy, making it potentially less suitable for midsize, commercial and SMB customers.

- **Less comprehensive SaaS application support:** Veritas lags other vendors in supporting other SaaS applications such as Microsoft Azure AD, Azure DevOps, Microsoft Dynamics 365 and

GitHub with Alta BaaS.

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

Microsoft — This vendor met this year’s inclusion criteria.

OpenText — This vendor was included in this year’s Magic Quadrant having completed the acquisition of Micro Focus in January 2023.

Dropped

Zerto, an HPE Company — This vendor did not meet this year’s inclusion criteria.

Inclusion and Exclusion Criteria

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

- 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, BaaS hoster or managed services provider offerings.
    - The vendor must have generated license (perpetual and/or subscription) and maintenance revenue (generally accepted accounting principles [GAAP]) of greater than $50 million over the last four quarters ending 28 February 2023 (or)
    - The vendor must have generated licenses (perpetual and/or subscription) and maintenance revenue (GAAP) of greater than $25 million, combined with a year-on-year growth rate of 20%, over the last four quarters ending 28 February 2023.
- The vendor’s qualifying backup and recovery solution(s) 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’s qualifying backup and recovery solution must focus on protecting enterprise customers running in hybrid/multicloud environments, which includes data center environments (traditional data center or a colocation facility) and cloud-based IaaS and PaaS workloads. Remote site protection is seen as an extension to these core capabilities.

- New products or updates to existing products that were released in the last 12 months must be generally available on or before 31 March 2023 to be considered for evaluation. All components must be publicly available, shipping and included on the vendor's published price list as of this date. Products shipping after this date will only have an influence on the Completeness of Vision axis.

- The vendor must actively sell and support its backup and recovery products under its own brand name in at least three of the following major geographies — North America, EMEA, Asia/Pacific and South America. At least 25% of total revenue must originate from outside of its major geography.

- The vendor must serve an installed base of at least 1,000 customers within the market as defined in the Market Definition/Description. In addition, at least 250 of the 1,000 customers must have deployed the backup solution for a minimum of 100 physical servers or 300 virtual servers in a single deployment site or cloud region. This excludes endpoint backups.

- The product must be installed in at least three of the following major geographies (North America, EMEA, Asia/Pacific and South America). Vendor will provide evidence of a minimum of 50 production customers brought to revenue in each of the three geographies.

- The vendor must employ at least 100 full-time employees in engineering, sales and marketing functions combined as of 31 March 2023.

- The vendor must have at least one qualifying backup and recovery solution commercially available for use by enterprises for three calendar years prior to 01 March 2023, i.e., it must have been commercially available at least as early as 01 March 2020.

- Product may be sold either as a software-only offering, as an integrated backup storage or virtualized appliance (backup application plus backup storage in a single integrated offering) or a vendor-developed and SaaS-based, BaaS offering.

The following exclusion criteria apply:

- Vendors offering products or solutions whose software is sourced primarily 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, storage area network (SAN), NAS or object storage.

- Vendors that back up directly to the public cloud without storing a local copy on-premises.

- Vendors whose main source of product revenue (more than 75% of total revenue) is from data center hosters and managed service providers.

- Products or solutions that are designed and positioned mainly as solutions for backing up endpoints such as laptops, desktops and mobile devices.
- Products or solutions that are designed and positioned mainly as solutions to backing up SaaS applications.
- Products or solutions that are designed and positioned mainly as solutions to back up remote offices, edge locations and lower midmarket/SMB environments.
- Products or solutions designed and positioned mainly as solutions for homogeneous environments — such as tools designed to back up only AWS EC2, Azure Virtual Machines, Microsoft Hyper-V, VMware, Red Hat or containers.
- Products or solutions designed to back up specific storage or hyperconverged systems vendors.
- Products that serve only as replication and disaster recovery tools.
- Products that serve primarily for managing snapshot and replication capabilities of storage arrays.
- Products that are positioned mainly for copy data management (CDM) or DevOps testing.
- Products that are positioned mainly for continuous data protection (CDP).

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	Medium
Market Responsiveness/Record	High

Evaluation Criteria	Weighting
Marketing Execution	Low
Customer Experience	High
Operations	NotRated

Source: Gartner (August 2023)

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

Evaluation Criteria ↓	Weighting ↓
Geographic Strategy	Medium

Source: Gartner (August 2023)

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 to support data protection requirements of hybrid and multicloud IT environments. They have a proven track record of established market presence and financial performance. For their 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. 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. However, a large market share alone is not a primary indicator of a Leader. Leaders are strategic vendors that are well-positioned for the future, having established success in meeting the needs of upper-midsize and large enterprise 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. However, it may not have 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 may 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. They 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 Leaders. Often, this is due to limited sales and marketing, and is sometimes due to scalability, scope of workloads protected, or breadth of functionality and/or platform support. These vendors are predominantly differentiated by product innovation and perceived customer benefits. However, they have not yet achieved solution completeness or sustained broad sales and marketing. They have not achieved mind share success or 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 (i.e., 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. 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 or 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 assess and rearchitect 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, hybrid, multicloud and edge environments. Favor solutions that offer a single pane of glass to manage these distributed environments.
- Choose backup solutions that provide a built-in or integrated offering for protecting backup data from a ransomware attack, ransomware anomaly and malware detection, and expedited recovery capabilities 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, such as cloud, supporting object lock, immutable data vaults or tape.

- Choose products that offer secure and granular recovery testing capabilities.

- Align the backup architecture with the organization's operational recovery needs. Optimize backup storage usage by using disk-based storage such as purpose-built backup appliances or distributed file system, object or SAN storage for operational recovery, and either use of on-premises tape, or object storage, or public cloud or vendor-hosted storage for long-term retention and air gap copies.

- Determine 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, universal-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 and in the public cloud to save on backup storage costs. Choose solutions that support recovery of applications from backup copies in the public cloud to address ransomware recovery, test/development or DR use cases.

- Select vendors that are able to augment the value of backup data beyond recovery events. Prioritize solutions that offer sensitive data scanning and e-discovery, address compliance requirements, support analytics and other data enrichment, reuse backup data for test/development, 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 focus on the following areas:

- **Centralized control plane:** As enterprises move toward a hybrid and mutlicloud 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 in the public cloud, in the main data center or, increasingly, as a service hosted in the public cloud.

- **Multicloud protection:** As organizations deploy applications and workloads to multiple cloud environments, the requirement of solutions to integrate with and protect multicloud environments

is now more critical. The flexibility to choose which cloud provider is used to store backup data is ideal.

- **Ransomware resilience:** The increase in the number of ransomware attacks has resulted in vendors taking concrete steps toward advancing a resilient backup infrastructure. Most vendors are aiming to make the primary backup repository more resilient by supporting immutable storage for first copies. While most vendors support the creation of immutable second copies of backup through write once, read many (WORM)-enabled storage, such as object storage locking, leading backup vendors have introduced on-premises, cloud and vendor-hosted immutable data vaults.

- **Ransomware detection and remediation:** Leading vendors have built capabilities to detect ransomware attacks by monitoring behavioral anomalies of protected data and are adding malware detection provided by partnering with security vendors or by developing these capabilities in-house. Most vendors also aim to simplify the ransomware recovery process by expediting the identification of the best and cleanest recovery point, creating curated recovery points, which combine multiple recovery points, and creating an isolated test and recovery environment.

- **BaaS offerings:** Leading backup vendors are expanding BaaS capabilities to include on-premises, IaaS, PaaS and SaaS environments. While generally not replacing on-premises backup deployments, Gartner clients are investing in BaaS offerings to complement these deployments to simplify protection of environments, including selected on-premises workloads, and edge and public cloud.

- **Use of artificial intelligence/machine learning:** Leading vendors have introduced AI/ML-based algorithms in ransomware anomaly detection capabilities and to enhance customer support practices. Newer capabilities include advancements in automated data classification and conversational-based administrative activities.

- **Support for public cloud IaaS and PaaS backup:** Most on-premises backup vendors have increased their investment to expand capabilities to protect cloud-native workloads, particularly VMs and applications hosted in AWS, Microsoft Azure and Google Cloud Platform. Leading backup vendors are expanding backup support of DBaaS products such as Amazon RDS, Amazon Aurora and Microsoft Azure SQL. Some vendors integrate their backup software with the native snapshot capabilities offered by these cloud providers; others 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:** I&O leaders have begun to include SaaS applications such as Microsoft 365, Google G Suite and Salesforce as a part of their backup strategy. Most vendors evaluated in this research support Microsoft 365 and Salesforce backup via partners or developed these capabilities in-house. Leading vendors are protecting other SaaS applications, such as Microsoft Azure Active Directory, Microsoft Dynamics 365, Microsoft Power Apps, Atlassian and ServiceNow.

- **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 Amazon 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:** Traditional enterprises continue to run their core business applications on relational database management system (RDMS) databases such as Oracle and Microsoft SQL. However, 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 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, virtual machines and file systems:** 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. Vendors such as Cohesity and Rubrik offer instant recovery of databases such as Microsoft SQL and Oracle, while Veeam also offers point-in-time file share access from backups via read-only SMB file share.

- **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, as more containers using persistent storage are deployed to support production workloads.

- **Licensing models:** While some perpetual licensing options remain available, all major vendors in this market have transitioned to providing their software offerings through subscription-based licensing models. Most subscription-based licensing offers are multiple-year-term agreements. Consumption-based licensing is an emerging trend for licensing that provides the ability to license what is in use based on metering at more frequent intervals.

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.