Magic Quadrant for Enterprise Backup and Recovery Software Solutions

5 August 2024 - ID G00800390 - 45 min read

By Michael Hoeck, Jason Donham, and 2 more

I&O leaders are challenged to protect and recover critical business applications and data from multiple threats. The enterprise backup and recovery software solutions market is responding with more workload coverage, ransomware recovery capabilities and delivery models, and focus on simplicity.

Strategic Planning Assumptions

- By 2028, 75% of enterprises will use a common solution for backup and recovery of data residing on-premises and in cloud infrastructure, compared with 20% in 2024.
- By 2028, 75% of enterprises will prioritize backup of SaaS applications as a critical requirement, compared with 15% in 2024.
- By 2028, 90% of enterprise backup and recovery products will include embedded technology to detect and identify cyberthreats, compared with fewer than 45% in 2024.
- By 2028, 75% of large enterprises will adopt backup as a service (BaaS), alongside on-premises tools, to back up cloud and on-premises workloads, compared with 15% in 2024.
- By 2028, 75% of enterprise backup and recovery products will integrate generative AI (GenAI) to improve management and support operations, compared with fewer than 5% in 2024.

Market Definition/Description

Gartner defines enterprise backup and recovery software solutions as technology that captures a point-in-time copy (backup) of enterprise data in on-premises, hybrid, multicloud and software as a service (SaaS) environments. These solutions write this data to one or more secondary storage targets for the primary purpose of recovering it in case of loss.

Protecting and recovering business application data, irrespective of the underlying infrastructure type and its location, is more important than ever. As enterprises move toward more complex environments that include large and expansive amounts of business-critical data, enterprise backup and recovery software solutions protect these workloads, whether they reside in on-premises, hybrid, multicloud or software as a service (SaaS) environments.

These solutions are vital to organizations' ability to recover data following events that cause it to become inaccessible. Whether such an event is accidental, malicious or environmental, organizations use these solutions to recover and restore access to the affected data accurately and efficiently.

Solutions must offer effective capabilities to simplify the management of data protection across complex enterprise environments. They must also ensure reliable recovery not just from accidental or operational errors but also from data loss arising from constantly changing threats, and expedite and orchestrate data recovery responses to traditional disaster and ransomware events.

Must-Have Capabilities

Must-have capabilities of enterprise backup and recovery software solutions include:

- Backup of data and systems across on-premises and hybrid multicloud environments. On-premises requirements include protection of operating systems, files, databases, virtual machines and applications. Cloud requirements include protection of infrastructure as a service (IaaS), platform as a service (PaaS), database as a service (DBaaS) and SaaS.
- Recovery of data and systems from any failure or data loss scenario, such as operational, system or application failure, accidental error, natural disaster and cyberattack. This demands capabilities to implement backup and data management policies to support an enterprise's business requirements for recovery point objectives (RPOs), recovery time objectives (RTOs), resilience, data life cycle and compliance.

- Integration with immutable backup storage target(s) or delivery of vendor-provided immutable storage.

Standard Capabilities

Standard capabilities of enterprise backup and recovery software solutions include:

- Protection of critical data in SaaS or PaaS applications, such as Google Workspace, Microsoft 365, Microsoft Entra ID, Salesforce applications, and other sources including object storage and containers.
- A centralized console for management of distributed backup solution infrastructure across hybrid and multicloud environments.
- Enhanced security capabilities, such as integration with privileged access management solutions, multifactor authentication, role-based access controls and multiperson change validation; security information and event management (SIEM) and security orchestration, automation and response (SOAR) integration; and advanced security reporting and logging.
- Enhanced cyber recovery readiness capabilities, such as vendor-developed or third-party integrated anomaly and entropy detection; malware and signature-based detection; and immutable data vault and isolated recovery environment offerings.
- Orchestration of disaster and cyber recovery testing and processes.

Optional Capabilities

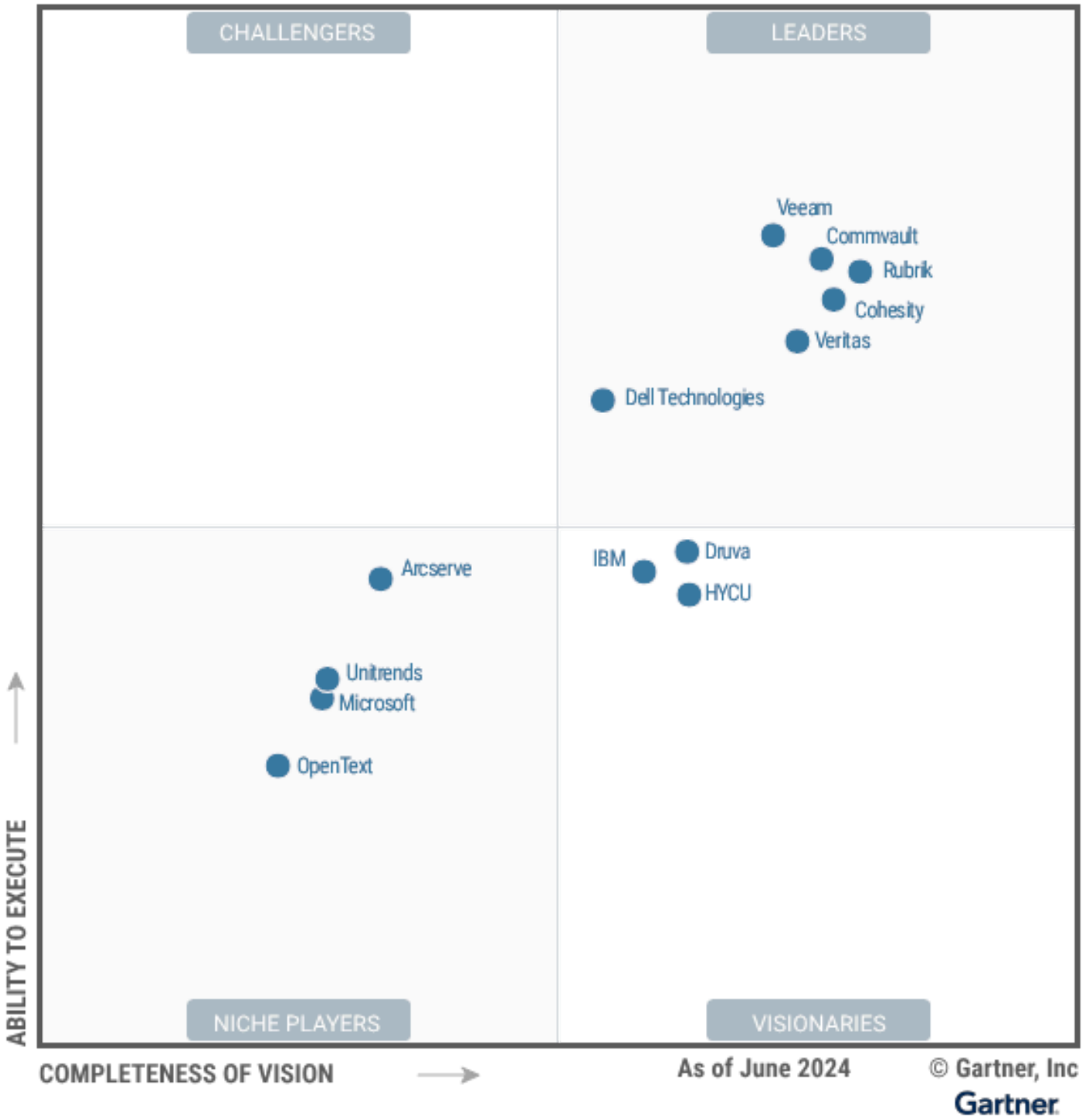
Optional capabilities of enterprise backup and recovery software solutions include:

- Protection of additional workloads and support for use cases such as edge/remote branch office sites, endpoints and large language model (LLM) infrastructure and data.
- A vendor-hosted, SaaS-based control plane to manage and orchestrate complex and distributed environments.
- A vendor-hosted backup as a service (BaaS) offering to deliver backup and recovery services for hybrid and multicloud environments.
- Generative AI features to simplify administration, improve support services, and accelerate backup and recovery procedures.

- Support for expanded data backup use cases to assist data discovery, security, compliance, copy data management, testing and development, and e-discovery processes.

Magic Quadrant

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



Vendor Strengths and Cautions

Arcserve

Arcserve is a Niche Player in this Magic Quadrant. Arcserve's backup portfolio includes Arcserve Unified Data Protection (UDP), Arcserve Backup, Arcserve 9000 Series Appliances, Arcserve UDP Cloud Hybrid, 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 9.1 and 9.2, which include improved password security for backup and recovery operations, currency with new Linux distributions, security patches and enhanced security for its use of the SQL Express database.

Strengths

- **Flexible pricing options:** Arcserve offers clients a choice between perpetual and term-based subscription licensing, as well as multiple metrics, including front-end terabyte, socket and virtual machine, to optimize pricing in alignment with their requirements.
- **Comprehensive SaaS application protection:** Arcserve SaaS Backup, through an OEM relationship with Keepit, provides protection for Microsoft 365, Salesforce, Microsoft Entra ID, Google Workspace, Zendesk, Microsoft Power BI and Azure DevOps.
- **Geography coverage:** Arcserve's comprehensive geographic strategy combines territory managers, value-added resellers (VARs) and managed service providers (MSPs) across all major geographies.

Cautions

- **Customer experience impacting innovation:** Arcserve's focus and investments to address issues with solution hardening, client support and prospective client experience have limited its innovations in trending areas of the enterprise backup and recovery market.
- **Lagging use of AI:** Arcserve's current portfolio and short-term roadmap lacks implementation of AI in areas such as ransomware anomaly detection, advanced cyberrecovery and GenAI use cases.
- **Agent-based cloud-native protection:** Arcserve's offerings remain heavily reliant on agent-based backup to protect cloud-native workloads, such as platform as a service (PaaS) and infrastructure as a service (IaaS). This creates complexity in administering deployment and managing these cloud environments.

Cohesity

Cohesity is a Leader in this Magic Quadrant. Its DataProtect backup portfolio is available for customer-managed deployment for both on-premises and cloud, as well as an as-a-service offering. Cohesity's operations span across North America and Western Europe, with limited presence in Asia/Pacific and Latin America. Its clients tend to be in the upper midmarket and enterprise segments. Major developments during the evaluation period include Cohesity Gaia, a GenAI-based conversational search and response solution powered by backup data. Cohesity added AI capabilities to improve threat detection and guide operators in cyberrecovery, administration and to troubleshoot product issues. Other notable enhancements include custom threat scan rules, on-demand data classification, support for Azure virtual machines (VMs), Azure SQL, Amazon RDS for PostgreSQL, Amazon Aurora, VMware Cloud on Amazon Web Services (AWS), and instant recovery of Nutanix AHV VMs.

In February 2024, Cohesity announced its acquisition of Veritas NetBackup and Alta data protection assets, which is expected to close by the end of the year. This represents the most significant merger or acquisition in this market in over a decade. The combined backup and recovery portfolio will contain complementary and overlapping technologies.

Strengths

- **Innovation and execution:** Cohesity has delivered a steady stream of innovative capabilities across data protection, security and management, as well as as-a-service delivery, for data across on-premises, cloud and SaaS apps.
- **GenAI for business data:** Cohesity is the first vendor to offer a GenAI-based solution powered by the backup data repository that provides a natural language, conversational solution to provide answers to business questions.
- **Cohesity Marketplace:** Cohesity offers a number of native and third-party applications through its Marketplace that leverage backup data for more value beyond restore operations.

Cautions

- **Limited SaaS application coverage:** Cohesity has made limited progress in expanding its portfolio of SaaS application coverage beyond Microsoft 365 and Salesforce.
- **Lack of stand-alone backup software:** Cohesity's solution is an integrated offering of backup and storage software. It does not offer a backup-only offering that can write the

first copy to third-party storage.

- **Veritas integration:** Pending the close of Cohesity's acquisition of Veritas's enterprise data protection operations, it is possible the integration could take up resources across multiple business functions, potentially impacting Cohesity's future speed of innovation.

Commvault

Commvault is a Leader in this Magic Quadrant. Its platform, Commvault Cloud, includes solutions for data protection, risk analysis and cyberrecovery for on-premises and cloud/SaaS-based workloads. Commvault's operations are geographically diversified, and its clients tend to be large enterprises. During the evaluation period, Commvault introduced Arlie, an AI-based threat analysis and operations assistant solution, as well as Threatwise threat detection decoys, Threat Scan Predict malware detection and Cleanroom Recovery to orchestrate and test recovery in an isolated environment. In addition, Commvault introduced further enhancements for Oracle Cloud Infrastructure, advanced Microsoft Active Directory and Microsoft Entra ID recovery support, and support for protecting MySQL and PostgreSQL workloads in Azure.

Strengths

- **Broad ecosystem support:** Commvault is both comprehensive in coverage and responsive to adding new workloads to its backup and recovery offering. This includes a diverse set of workloads across on-premises, multicloud and SaaS applications.
- **Focus on cyberresiliency and recovery:** Commvault Cleanroom Recovery, combined with its Arlie AI and third-party security integrations, simplifies customers' efforts to plan, exercise and execute complex recovery efforts.
- **Simplified licensing:** Commvault has improved SKU management licensing for its cloud and on-premises products, enabling customers to better understand Commvault licensing.

Cautions

- **Support process concerns:** Customers have voiced concerns regarding their experience working with the Commvault support team, when it comes to their responsiveness to escalate incidents beyond first-tier support.
- **Customer enablement concerns:** Some Gartner clients indicate that they need to engage support when implementing new features and functions. This leads them to question if

Commvault is elevating features and functions to general availability (GA) without consistently providing complete documentation for proper implementation.

- **Product rebranding confusion:** Despite its product rebranding to Commvault Cloud, clients report confusion and lack of clarity regarding Commvault's consistency of capabilities across its on-premises, BaaS and appliance offerings.

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, NetWorker, Avamar, APEX Backup Services, and PowerProtect DP and DD series appliances. Dell's operations are geographically diversified, and its clients tend to be large enterprises, with presence in the midmarket. During the evaluation period, notable enhancements to PowerProtect Data Manager include Storage Direct agent integration with Dell PowerStore and Dell PowerMax, Microsoft Active Directory granular recovery, and stand-alone agent support for Apache Hadoop. It also introduced PowerProtect DM5500 integration with PowerProtect Cyber Recovery, APEX Backup Services features (including cloud-native backups for AWS and Azure), APEX Protection Storage in Oracle Cloud VMware Solution, and APEX Subscriptions support for backup appliances.

Strengths

- **Comprehensive solution offering:** Dell bundles its data center portfolio of servers, storage, networking, and backup and recovery offerings to deliver a single vendor solution that minimizes the number of vendors that clients need and improves the overall customer experience.

- **Storage Direct Protection:** Storage Direct Protection embeds differential block-level backup in both PowerMax and PowerStore solutions. PowerProtect Data Manager orchestrates and manages crash-consistent backup and recovery directly to and from PowerProtect appliances, without any backup software installation on the PowerMax and PowerStore systems.

- **APEX Subscription adds backup target:** Dell has expanded its APEX Subscriptions offer to include PowerProtect Data Domain appliances, enabling clients to acquire PowerProtect Data Domain appliances via a pay-as-you-go license. This allows clients to start small, grow and align to performance requirements.

Cautions

- **Following leaders in market trends:** Dell has followed market leaders in addressing recent market trends, such as vendor-hosted cloud backup storage vaults and expanded ransomware detection and recovery capabilities beyond its PowerProtect Cyber Recovery offering.
- **Unbalanced innovation across backup software portfolio:** Dell's focus on the PowerProtect Data Manager offering limits innovation to its other backup and recovery products, such as Avamar and NetWorker.
- **Limited SaaS-based control plane:** Dell lacks a comprehensive SaaS-based control plane and common administrative interface for all components of its solution, which are features often found in leading vendor solutions.

Druva

Druva is a Visionary in this Magic Quadrant. The Druva Data Security 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 disaster recovery (DR), AWS cloud-native and Kubernetes backup and DR, and SaaS application and endpoint backup. Druva's operations are geographically diversified, with the majority of its customers in North America. Its clients tend to be in the midmarket and enterprise segments. During the evaluation period, Druva added Azure VM backups, anomaly detection of VMware VMs, direct backup from SAP HANA, Sandbox Recovery, and group-level backups in Microsoft 365. Druva also introduced Dru, its AI copilot for backup and recovery, and added curated recovery for Microsoft OneDrive and SharePoint Online data.

Strengths

- **Cloud-native BaaS:** Built as a cloud-native and SaaS platform from Day 1, Druva's BaaS platform provides ease of use and automatic scaling of resources for all data.
- **Cloud-first organizations:** Druva's BaaS platform is best-suited for cloud-first organizations with end-to-end self-serve product trials, enabling easy onboarding and simple operations.
- **Global coverage with Dell:** Druva has an OEM partnership with Dell Technologies, which makes the offering additionally available across the globe as a Dell-branded solution.

Cautions

- **Limited enterprisewide deployments:** Compared with the Leaders in this Magic Quadrant, Druva has minimal presence in large enterprises as a single data protection solution.
- **Less comprehensive multicloud support:** Druva's support for backup of applications and infrastructure in Azure and Google Cloud Platform (GCP) is limited compared with AWS.
- **Lagging hybrid environment coverage:** Druva lags market leaders in coverage of hybrid environment requirements, such as protection of containers, object storage, and modern databases, including MongoDB, MariaDB and NoSQL; bare-metal recovery capabilities; and instant database recovery.

HYCU

HYCU is a Visionary in this Magic Quadrant. HYCU R-Cloud (previously Protégé) is a hybrid and multicloud BaaS platform that spans across Azure, AWS and GCP to support IaaS, database as a service (DBaaS), PaaS, SaaS and on-premises workloads. HYCU R-Graph provides insight to application and data architectures across on-premises, cloud and SaaS environments. HYCU's operations are primarily focused on North America and EMEA, 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 to R-Graph, including customizable view options and insights to native application protection capabilities. It also enhanced R-Cloud, adding support for SaaS and PaaS offerings, such as Google Cloud Bigtable, Atlassian Trello, Docusign, GitHub, Amazon DynamoDB, AWS CloudFormation and AWS Key Management Service.

Strengths

- **Broad cloud support:** HYCU's strong focus on SaaS and PaaS integrations has led to a large list of supported services not commonly found within other market offerings.
- **Enhanced visibility of data protection estate:** R-Graph collects data across a customer's application environment and reports data protection deficiencies, allowing clients to easily identify unprotected assets.
- **GenAI-developed integrations:** HYCU uses generative AI to help accelerate development of data protection modules for new SaaS and PaaS workloads.

Cautions

- **On-premises limitations:** HYCU's product releases tied to on-premises requirements, such as AIX, Solaris, SUSE, and Ubuntu Linux and database cluster support, lags behind market leaders.
- **No orchestration for disaster recovery:** R-Cloud lacks built-in orchestration capabilities to help simplify disaster recovery operations and testing capabilities.
- **Limited geographic coverage:** HYCU has limited market presence and execution in South America and Asia/Pacific.

IBM

IBM is a Visionary in this Magic Quadrant. Its primary backup portfolio consists of IBM Storage Defender, IBM Storage Protect, IBM Storage Protect Plus, IBM Storage Protect Snapshot and IBM Storage Protect for Cloud. IBM's operations are geographically diversified, and its clients tend to be large enterprises. During the evaluation period, IBM released Storage Defender, which uses AI to analyze data from multiple sensors for threat detection and monitoring. Other notable capabilities in Storage Defender include integration of IBM FlashSystem application-aware threat detection, immutable primary storage snapshots, Defender SaaS control plane, a subscription licensing model with flexible resource units and expanded support for OpenShift Virtualization. IBM also introduced Storage Defender Data Protect through a partnership with Cohesity.

Strengths

- **IBM storage focus:** IBM backup products offer superior backup performance and data resilience for IBM storage. IBM has focused on improving backup and recovery integrations with IBM storage, improving backup performance and data resilience with these integrations.
- **OpenShift container backup:** IBM continues significant investments in IBM Storage Protect Plus for container backup and recovery. Recent additions include protection of Red Hat OpenShift, Kubernetes and Tanzu environments.
- **Implementation of AI for threat detection:** IBM Storage Defender uses an IBM-developed AI model to perform behavioral analytics, in-line corruption detection, and application-aware anomaly detection for early threat detection of malware and ransomware.

Cautions

- **Product sprawl:** IBM made significant changes to its product portfolio, including a wider range of available products and recent product name changes. As a result, there is the potential for confusion as to which product is the best fit for customer needs.
- **Scope of capabilities outside IBM portfolio:** IBM has heavily focused its Storage Defender offering and marketing message based on integrations with its own storage portfolio. This requires clients to fully validate the scope of capabilities for use with non-IBM storage.
- **Dependencies on third-party products:** IBM's Storage Defender Data Protect and Storage Protect for Cloud solutions include dependencies on third-party OEM partnerships for their product and control plane, placing product innovation and development outside of IBM control.

Microsoft

Microsoft is a Niche Player 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 Manager (DPM) and the 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 introduced Azure Backup Server (MABS) V4, SAP HANA System Replication database backup support, enhanced software delete for Azure Backup, Azure Kubernetes Service backup and cross-region restore support for PostgreSQL.

Strengths

- **Alignment with Microsoft Azure cloud adoption:** Microsoft's backup and recovery portfolio is well-suited for clients transitioning infrastructure from on-premises to Microsoft Azure using lift-and-shift strategies.
- **Soft delete with Azure Backup:** Microsoft introduced a soft delete feature, which provides a recycle bin logic with an extended retention period to easily restore deleted backup data, whether it was deleted accidentally, intentionally or maliciously.
- **Isolated backup vaults:** Azure Recovery Services for vaulted copies of Azure Backup data isolates data from production backup copies using a Microsoft-managed Azure subscription and tenant, which limits unauthorized users' access to the data.

Cautions

- **Fragmented data protection strategy:** Microsoft's overall backup and recovery portfolio strategy indicates no apparent plans to align to a single or combined portfolio strategy. There is no indication of combining, planning, orchestrating or designing backup capabilities across Microsoft services such as Microsoft 365, Microsoft Entra ID, Microsoft Azure SQL, Microsoft Power Apps or Microsoft Dynamics 365.
- **Limited Microsoft PaaS protection capabilities:** Azure Backup lacks integrations with key Microsoft PaaS services, including Azure SQL, Azure Cosmos DB and Microsoft Entra ID.
- **Azure Backup management complexity:** Azure Backup does not provide native deduplication features, requiring clients to deploy and manage an instance of MABS/MARS. Additionally, it does not support common capabilities such as automatic clock adjustment for daylight saving time.

Microsoft did not respond to requests for supplemental information or to review the draft contents of this document. Gartner's analysis is therefore based on other credible sources.

OpenText

OpenText is a Niche Player in this Magic Quadrant. Its enterprise backup product portfolio consists primarily 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 introducing support for OpenText Magellan reporting, anomaly detection and OpenText Documentum. It also enhanced backup and restore of sparse files on Linux systems and immutability of replicated data. Data Protector for Cloud Workloads introduced support for OpenShift Virtualization, Kubernetes and Red Hat OpenShift Data Foundation, and OpenNebula. It has also added protection of contact pictures in Microsoft 365.

Strengths

- **OpenText broader portfolio integrations:** OpenText has made key investments to prioritize integration and protection of OpenText solutions, including integrations to protect OpenText Documentum data and expanded reporting capabilities using OpenText Magellan.

- **OpenText pricing options:** OpenText offers multiple pricing options to best align total cost of ownership with customer requirements and their workloads, including capacity-based and socket-based pricing.
- **Broad hypervisor support:** OpenText Data Protector integrates with multiple hypervisors, including VMware VMs, Microsoft Hyper-V, Proxmox VE, Oracle Linux Virtualization Manager, oVirt, Red Hat virtualization, Nutanix AHV, OpenStack, OpenNebula, Virtuozzo, Oracle VM VirtualBox, XenServer, XCP-ng, Huawei FusionCompute and Scale Computing HyperCore.

Cautions

- **Limited innovation progress:** OpenText has made limited progress in multiple backup and recovery trends, such as advancement of ransomware beyond anomaly detection, introduction of a vendor-hosted SaaS-based control plane, and implementations of GenAI.
- **Lacks vendor-hosted BaaS solution:** OpenText lacks an enterprise-customer-focused BaaS solution for SaaS, cloud workloads and on-premises.
- **Narrow integrations with SaaS applications:** OpenText Data Protector for Cloud Workloads supports only Microsoft 365. It lacks support for other SaaS applications, such as Microsoft Entra ID, Salesforce, Google Workspace and Microsoft Power Apps.

Rubrik

Rubrik is a Leader in this Magic Quadrant. Its backup product portfolio consists of Rubrik Security Cloud, which includes multiple backup offerings related to data security and advanced recovery. Rubrik offers appliance-based on-premises and cloud-based BaaS/SaaS data protection solutions. Rubrik operations are primarily focused on North America and EMEA, and its clients tend to be midsize to large enterprise customers. During the evaluation period, Rubrik introduced multiple new or enhanced capabilities, including Ruby, a generative AI tool to help with security and operational tasks, and it also acquired and integrated Laminar to Rubrik's data security posture management capabilities. Along with these improvements, Rubrik added advanced data and security monitoring features focused on anomaly and threat detection, virtual machine encryption detection, and support for Microsoft Entra ID, Microsoft Active Directory, Amazon Simple Storage Service (Amazon S3) and Atlassian Jira.

Strengths

- **Market innovation:** Rubrik continues to innovate its product offerings through the integration of new data security technology from its Laminar acquisition, expansion of cyberthreat detection and recovery capabilities, and new product bundles.
- **Focus on simplicity and efficiency:** The SaaS-based control plane of Rubrik Security Cloud provides simplified customer administration capabilities and automated updates, using its services to control and orchestrate deployment of releases and patches to a customer's deployment.
- **Competitive pricing:** Gartner clients report that Rubrik has engaged in aggressive negotiations to provide competitive pricing for renewals and net new deployments.

Cautions

- **Selected PaaS, SaaS and multicloud support availability:** Rubrik's support and go-to-market pace for popular PaaS, SaaS and cloud platforms outside of Azure, AWS, GCP, Atlassian Jira and Microsoft 365, as well as its multicloud-storage-plane choices, are slower than market competitors.
- **Limited geographic coverage:** Customers experience limited engagement with Rubrik outside of North America and EMEA due to a lack of enabled partners in Asia/Pacific and South America.
- **Rubrik financial expectation:** New public market expectations, as a result of its recent initial public offering (IPO), may change Rubrik's continued pace of innovation.

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 appliances and Spanning Backup for SaaS application backup. Its operations are geographically diversified, and its customers tend to be in the midmarket segment. In the last 12 months, Unitrends introduced direct-to-cloud backup for remote, distributed and cloud workloads, an all-flash architecture for cloud disaster recovery as a service (DRaaS), and new Recovery Series Generation 10 appliances. Additionally, Unitrends enhanced abilities for administrators to add new protected endpoints and enroll in backup policies without logging into each on-premises appliance.

Strengths

- **Unified administration:** The Unitrends UniView offers single administrative access to all components of the backup and recovery solution, including management of appliances, endpoint backup and SaaS applications. It also extends integrations to other Kaseya offerings, such as KaseyaOne, Kaseya IT Glue and Kaseya Service Desk.
- **Kaseya integration:** Kaseya 365 licensing bundles Unitrends's backup and recovery capabilities with Kaseya solutions that offer antivirus protection, managed detection and response, and ransomware rollback capabilities.
- **Expanded DRaaS with guaranteed recovery time objectives (RTOs):** Unitrends expanded the capabilities of its DRaaS offering. It is deployed within Unitrends cloud data centers, supports on-premises VMware and Hyper-V virtual machines, and can be procured with contractually guaranteed RTOs.

Cautions

- **Narrow enterprise suitability:** With its focus on small and midsize business (SMB) markets and delivery of its solutions through managed service providers, Unitrends's growth initiatives and limited scalability of appliances contribute to reduced suitability for large enterprise accounts.
- **Limited multicloud capabilities:** Unitrends Backup for Microsoft Azure supports only Azure VMs and lacks support for other workloads in Azure, such as Azure SQL and Azure Blob Storage. Expansion to support native integrations with other cloud providers, such as AWS and GCP, remains a work in progress.
- **Limited SaaS protection strategy:** Unitrends continues to lag behind providers that have introduced support for other SaaS applications, such as Microsoft Entra ID, ServiceNow and Atlassian Jira.

Unitrends did not respond to requests for supplemental information. Gartner's analysis is therefore based on other credible sources.

Veeam

Veeam is a Leader in this Magic Quadrant. Its backup portfolio consists of Veeam Data Platform, Veeam Data Cloud, Veeam Data Cloud Vault and Veeam Kasten for Kubernetes. 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 multiple

product updates, including Veeam Data Platform v.12.1, which contains new features such as in-line malware detection, YARA-based content analysis, Veeam Threat Center, Veeam AI Assistant, instant recovery of PostgreSQL and backup of object storage. Veeam introduced its own vendor-managed backup services, including Veeam Data Cloud for protecting Microsoft 365 and Microsoft Azure, and Veeam Data Cloud Vault. In March 2024, Veeam also acquired Coveware, a cyberrecovery incident response services and technology company.

Strengths

- **Market responsiveness:** During the evaluation period, Veeam addressed coverage gaps in recent market trends and customer demands by introducing its vendor-hosted BaaS solution for Microsoft 365 and Azure, and a cloud vault service. It also expanded its cyberrecovery capabilities by introducing malware scanning, real-time entropy detection and an improved reporting dashboard.

- **Coveware acquisition:** The acquisition expands Veeam's customer support capabilities for incident response, as Coveware is capable of working with customers of other backup vendors. Coveware also includes technologies such as Recon for forensic collection and Unidecrypt for decrypting data.

- **Self-describing backup data format:** Veeam's backup solutions employ a self-describing backup data file. The format allows portability of backup data between storage systems and other Veeam deployments, and the self-describing design eliminates the requirement of managing, protecting and reconstructing a catalog.

Cautions

- **Market follower approach to innovation:** Veeam's backup offerings are often introduced and enhanced as a response to competitive offerings and customer demand, rather than leading with new, innovative and differentiating capabilities and offerings in the market.

- **Core components rely on Windows infrastructure:** The core management components for the Veeam Backup & Replication server remain reliant on Windows server infrastructure, creating dependencies that may have architecture, security and cost implications.

- **Limited SaaS application protection:** Veeam's product portfolio lags other Magic Quadrant vendors that have innovated to add SaaS application protection capabilities beyond Microsoft 365 and Salesforce.

Veritas

Veritas is a Leader in this Magic Quadrant. Its backup product portfolio consists of NetBackup software and appliances for on-premises deployments, and Veritas Alta, which includes Veritas Alta View, Veritas Alta BaaS, Veritas Alta Data Protection, Veritas Alta Recovery Vault and Veritas Alta SaaS Protection for cloud deployments. Veritas's operations are geographically diversified, and its clients tend to be large to very large enterprises, with some presence in the midmarket. Notable developments during the evaluation period include Veritas Cyber Resilience Assessment Service, new higher performance NetBackup appliances, comprehensive support for Microsoft Entra ID, enhanced support for Oracle VLDB, and multiple security and usability enhancements. Additionally, Veritas introduced Veritas Alta Copilot for AI-assisted troubleshooting and operations.

In February 2024, Cohesity and Veritas announced the intent to merge their enterprise data protection businesses by the end of the calendar year.

Strengths

- **In-house REDLab for cyber resiliency:** REDLab is Veritas's in-house lab for adding and testing new signatures for detecting cyberattacks that provides its clients with up-to-date cyberthreat detection capabilities.
- **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 in all major geographies.
- **Cloud-native architecture:** NetBackup and Veritas 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, delivering an elastic and inherently flexible multicloud architecture.

Cautions

- **Inconsistent NetBackup upgrade experience:** Several customers have cited that NetBackup software and appliance upgrades from older versions have not gone as planned, and that upgrades require careful preparation and working with technical support.

- **Lack of focus on midsize organizations:** Direct sales support for midsize organizations is limited due to Veritas's primary focus on its large-enterprise installed base.
- **Pending transaction with Cohesity:** Following the completion of Cohesity's merger with Veritas's enterprise data protection business, cost management initiatives may impact the ability of the combined organization to meet roadmap commitments.

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

No vendors were added.

Dropped

Acronis was dropped because its focus on prioritizing MSPs and edge/endpoint device workloads resulted in its inability to meet the 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's qualifying backup and recovery solution must meet all "must-have" capabilities as defined in the Market Definition section above.
- The vendor must have at least one qualifying backup and recovery solution commercially available for use by enterprises for three calendar years prior to 1 April 2024 (i.e., it must have been commercially available at least as early as 1 April 2021).

- 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 through MSP sales.
    - The vendor must have generated over $70 million in reported annual recurring revenue (ARR) as of 28 February 2024, or
    - The vendor must have generated over $30 million in reported ARR as of 28 February 2024, combined with a year-on-year (28 February 2023 versus 28 February 2024) ARR growth rate of 20%.
- The vendor must serve an installed base of at least 1,000 customers within the market, as defined in the Market Definition 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 300 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 three of the following four major geographies — North America, EMEA, Asia/Pacific and South America. At least 25% of total ARR must originate from outside of its major geography.
- 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'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.
- New products or updates to existing products that were released in the last twelve months must be generally available before 1 April 2024 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 have an influence only on the Completeness of Vision axis.
- The vendor must employ at least 100 full-time employees in engineering, sales and marketing functions combined as of 28 February 2024.

- 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-hosted, SaaS-based, backup-as-a-service offering.

The following exclusion criteria apply:

- Vendors offering products or solutions with software that is sourced primarily from a third-party independent software vendor (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 networks (SANs), network-attached storage (NAS) or object storage.
- Vendors that back up directly to the public cloud without storing a local copy on-premises.
- Vendors that get most of their product revenue (more than 75% of total revenue) from hosting data centers and managed service providers.
- Products or solutions designed and positioned mainly as solutions for homogeneous environments, such as tools designed to back up only Amazon S3, Azure Blob, Amazon EC2 or Azure Virtual Machines, or Microsoft Hyper-V, VMware or Red Hat, or containers.
- Products or solutions that are designed and positioned mainly as solutions to back up only SaaS applications.
- 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 back up remote offices, edge locations and lower midmarket/SMB environments.
- Products or solutions designed and positioned mainly to back up specific storage or hyperconverged systems vendors.
- Products that serve only as replication and disaster recovery tools.
- Products that serve primarily to manage snapshot and replication capabilities of storage arrays.

- Products that are positioned mainly for copy data management or DevOps testing.
- Products that are positioned mainly for continuous data protection.

Honorable Mentions

Gartner tracks more than 30 vendors in this market. Of those, 13 met the inclusion criteria for this Magic Quadrant. However, the exclusion of a provider does not mean that the vendor and its products lack viability. The following are noteworthy vendors that did not meet all inclusion criteria but could be appropriate for clients, contingent on requirements:

- **Bacula Systems:** This enterprise backup and recovery software solution vendor is headquartered in Switzerland. Bacula Systems provides software-based offerings as open-source and as commercially licensed and supported products. Bacula Systems was excluded from this Magic Quadrant, as it didn't meet the revenue criteria.
- **Huawei Technologies:** This enterprise backup and recovery software solution vendor is headquartered in China. Huawei Technologies provides software-, appliance- and BaaS-based offerings. Huawei was excluded from this Magic Quadrant, as its qualifying product didn't meet the required global general availability timeline criteria.
- **NAKIVO:** This enterprise backup and recovery software solution vendor is headquartered in the U.S. NAKIVO provides software-based offerings. NAKIVO was excluded from this Magic Quadrant, as it didn't meet the revenue criteria.

Evaluation Criteria

Ability to Execute

The Ability to Execute criteria for this Magic Quadrant are as follows:

Product or service: This criterion covers the assessment of vendor capabilities to deliver and differentiate features and functionality supporting market use cases, diversification of customer use across the vendor's portfolio, and the scope of issues impacting customer experience.

Overall viability: This criterion covers the assessment of a vendor's key financial, staffing and customer base growth metrics.

Sales execution/pricing: This criterion covers the assessment of a vendor's success in the market. Considerations include results of new versus repeat business, growth of new backup and recovery customers, and changes in customer investments. Adaptations to sales and presales efforts and levels of pricing transparency are also considered.

Market responsiveness/record: This criterion evaluates the vendor's ability to deliver products and capabilities that are first-to-market and differentiating compared to the competition, while also continuing to meet market demands and gaps in their portfolio.

Marketing execution: This criterion evaluates the vendor's ability to create mind share, expand to new markets and build sales pipeline in the market.

Customer experience: This criterion evaluates the vendor's ability to demonstrate continued client satisfaction and its improvements, and provide distinct customer support capabilities.

Operations: This criterion was excluded from this research due the limited differentiation of vendors and resulting impacts to customers.

Ability to Execute Evaluation Criteria

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

Source: Gartner (August 2024)

Completeness of Vision

The Completeness of Vision criteria for this Magic Quadrant are as follows:

Market understanding: This criterion evaluates the ability of the vendor to understand customer requirements, align those requirements to its products and services, and evolve their product vision, based on their own established perspectives of the market's direction.

Marketing strategy: This criterion evaluates the clarity of the vendor's marketing vision that highlights competitive differentiation and an understanding of personas engaged in solution selection.

Sales strategy: This criterion evaluates the vendor's ability to establish and update a sales strategy that aligns with company goals and customer interest. Factors also include the vendor's ability to reach customers directly and expand coverage through its network of partners.

Offering (product) strategy: This criterion evaluates the vendor's product planning, emphasizing its alignment to shortcomings, commitment to differentiation and improvement of existing capabilities.

Business model: This criterion evaluates the vendor's strategies to sustain its business in the market.

Vertical/industry strategy: This criterion evaluates the vendor's strategy to direct its product offerings, its alignment with industry specific technology providers and its resources to meet specific vertical market requirements.

Innovation: This criterion evaluates the vendor's strategy for reinvestment and its differentiating innovations in product design, marketing, sales and presales, and customer support.

Geographic strategy: This criterion evaluates the vendor's strategy to direct resources, skills and product offerings to meet the needs of across the four major geographies — North America, EMEA, Asia/Pacific and South America.

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	Low
Innovation	High
Geographic Strategy	Medium

Source: Gartner (August 2024)

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 backup and recovery requirements of hybrid, multicloud and SaaS 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. They also have well-articulated plans for expanding general recovery and cyberrecovery capabilities, expanding workload coverage, improving ease of deployment and administration, including use of GenAI 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, as well as 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 responsible for backup operations must assess and rearchitect their backup infrastructure to include aspects of technology, operations and consumption appropriate for their organizations by:

- Investing in backup solutions that address data protection requirements in the data center, hybrid, multicloud and SaaS environments. Favor solutions that offer a single pane of glass to manage these distributed environments.
- Choosing 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.
- Focusing on solutions that provide capabilities to routinely test and orchestrate recovery of applications and data.

- Expanding resilience capabilities by using vendor solutions that support or provide immutable data vault and isolated recovery environment offerings.
- Evaluating 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.
- Choosing products that offer secure and granular recovery testing capabilities.
- Aligning 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 systems, object or SAN storage for operational recovery, and use of either on-premises tape, object storage, public cloud or vendor-hosted storage for long-term retention and air gap copies.
- Weighing 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 your organization's application and infrastructure roadmap.
- Selecting vendors that support tiering of backup copies to the public cloud and within 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.
- Selecting vendors that can 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. Enterprise backup and recovery vendors evaluated in this Magic Quadrant are innovating and changing the market the following areas:

- **SaaS-based control planes:** Vendors are offering centralized management platforms that are increasingly backup-vendor-hosted, replacing customer-managed deployments in

their own public cloud or data center infrastructure.

- **Expanding GenAI capabilities:** Vendors in this market have rapidly introduced their initial offerings of GenAI capabilities. The primary focus of these solutions is intended to assist with backup administrative tasks and troubleshooting. Implementations include the use of chatbots, natural-language question dialogues and AI-based responses. The use of GenAI is expected to lead to expanded levels of automation to accelerate recovery and further simplify administration.

- **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.

- **Cloud-native application and data protection:** Vendors in this market are expanding their coverage of additional cloud services to increase their clients' abilities to protect cloud-native applications. The scope of requirements requires vendors to expand protection to more DBaaS, IaaS and PaaS infrastructures, multiple cloud data locations and cloud application configuration. Vendor capabilities may include automated application discovery, integration with cloud services to orchestrate and store native snapshots, and reuse of existing backup software "as-is" in the cloud to provide agent-based backup of the applications hosted in the cloud.

- **Ransomware detection and recovery:** Vendors have built capabilities to detect ransomware attacks by monitoring behavioral anomalies of protected data and are adding malware detection by partnering with security vendors or developing these capabilities in-house. Most vendors also aim to simplify the ransomware recovery process by expediting identification of the best and cleanest recovery point, creating curated recovery points that combine multiple recovery points, and creating an isolated test-and-recovery environment. Vendors are also introducing curated snapshot recovery. It combines multiple snapshots with the latest, clean and safe scanned file version available for restore. This feature eliminates the need to perform multiple granular restores from various snapshots and restores the most recent update.

- **BaaS offerings:** Leading backup vendors are expanding BaaS capabilities to include on-premises, IaaS, PaaS and SaaS environments. Gartner clients are investing in BaaS offerings to complement on-premises backup deployments, which simplifies the

protection of environments, including selected on-premises workloads, as well as edge and public cloud.

- **Expanded as-a-service offerings:** Leading vendors are introducing new services to complement their backup and recovery offerings. The focus of these new services center around expanding services to support ransomware protection and recovery. Multiple vendors now have vendor-hosted cloud storage offerings. These are often referred to as immutable data vaults (IDVs) or cloud vaults. Leading vendors are expanding this service to include anomaly and malware detection capabilities. In addition, some vendors are introducing orchestration services to facilitate routine testing, cleaning and validation, and performing recovery.

- **Use of artificial intelligence/machine learning (ML):** 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 SaaS 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 have developed these capabilities in-house. Vendors are innovating to protect other SaaS applications and accelerate the integration with new applications. Additional SaaS application protection is available in the market for applications, such as Microsoft Entra ID, Microsoft Dynamics 365, Microsoft Power Apps, Atlassian Jira and ServiceNow.

- **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 network file system. VMs can thus become instantly available while the actual recovery process is 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 Server Message Block file share.

- **Licensing models:** Some perpetual licensing options remain available, but most vendors in this research 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