Magic Quadrant for Backup and Data Protection Platforms

24 June 2025 - ID G00824107 - 48 min read

By Michael Hoeck, Jason Donham, and 3 more

Backup and data protection platforms vendors are continually enhancing their backup offerings to improve enterprise data protection across multicloud, SaaS and data center environments. Heads of I&O should use this research to identify and select vendors to address their enterprise data protection needs.

Strategic Planning Assumptions

- By 2029, 75% of enterprises will use a common solution for backup and recovery of data residing on-premises and in cloud infrastructure, compared with 25% in 2025.
- By 2029, 80% of enterprises will prioritize backup of SaaS applications as a critical requirement, compared with 20% in 2025.
- By 2029, 95% of backup and data protection platforms products will include embedded technology to detect and identify cyberthreats, compared with 55% in 2025.
- By 2029, 85% of large enterprises will adopt backup as a service (BaaS), alongside customer-managed deployments, to back up cloud and on-premises workloads, compared with 25% in 2025.
- By 2029, 90% of backup and data protection platforms products will integrate generative AI (GenAI) to improve management and support operations, compared with fewer than 25% in 2025.
- By 2029, 35% of enterprises will implement agentic AI capabilities to perform autonomous backup operations, up from less than 2% in 2025.

- By 2029, 30% of enterprises will integrate backup copies as a data source for analytics and inference, up from less than 5% in 2025.

Market Definition/Description

Gartner defines backup and data protection platforms as technologies that capture point-in-time copies of enterprise data for the purpose of recovering it from multiple data loss scenarios, enhancing data protection initiatives, and expanding data insights and access capabilities. These technologies protect enterprise data, applications and infrastructure in hybrid, multicloud and SaaS environments. Backup and data protection platforms are available as software-only, integrated appliances and vendor-developed and hosted backup as a service (BaaS).

Protecting and recovering an organization's application data, regardless of the underlying infrastructure type and its location, are more important than ever. As enterprises operate in more complex environments, backup and data protection platform solutions protect enterprise data, whether they reside in hybrid, multicloud or 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 or due to hardware or software failure, operational errors, malicious attacks or environmental incidents, organizations use these solutions to reliably recover and restore access to the affected data accurately and efficiently.

Solutions must offer effective capabilities to simplify the management of data protection across increasingly complex and diverse environments. This includes capabilities to test, expedite and orchestrate data recovery responses for both traditional disaster and cyberevents.

Solutions also extend beyond traditional recovery use cases to drive further business value from the data that is copied to the platform. It incorporates use cases that are focused on data-driven enablement, such as enhanced data protection and infrastructure integrations and expanded data insights and access.

Enhanced protection capabilities include application discovery, enhanced cyberrecovery readiness capabilities, orchestration of disaster and cyberrecovery testing and processes,

data discovery and access tracking. Integrations extend to bidirectional operational insights with other infrastructure and operations platforms, such as networking, storage and security.

Data insights and access capabilities enable vendor solutions to present data to new personas beyond the backup administrators. New personas include additional IT personas such as security, DevOps, and data and analytics, as well as other business users such as compliance and legal.

Mandatory Features

- Backup of data and systems across hybrid, multicloud and SaaS environments:
  - Hybrid includes support for on-premises and public cloud infrastructure. Hybrid requirements include protection of operating systems, hypervisors, files, databases, virtual machines and applications.
  - Multicloud and SaaS requirements include protection of infrastructure as a service (IaaS) across two or more public cloud service provider environments and two or more major SaaS applications, such as Microsoft 365, Salesforce and Google Workspace.
- 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 targets or delivery of vendor-provided immutable storage.
- Cyberrecovery readiness capabilities, such as vendor-developed or third-party integrated, postbackup anomaly and entropy detection.
- Centralized console for management of distributed backup solution infrastructure across hybrid and multicloud environments.

Common Features

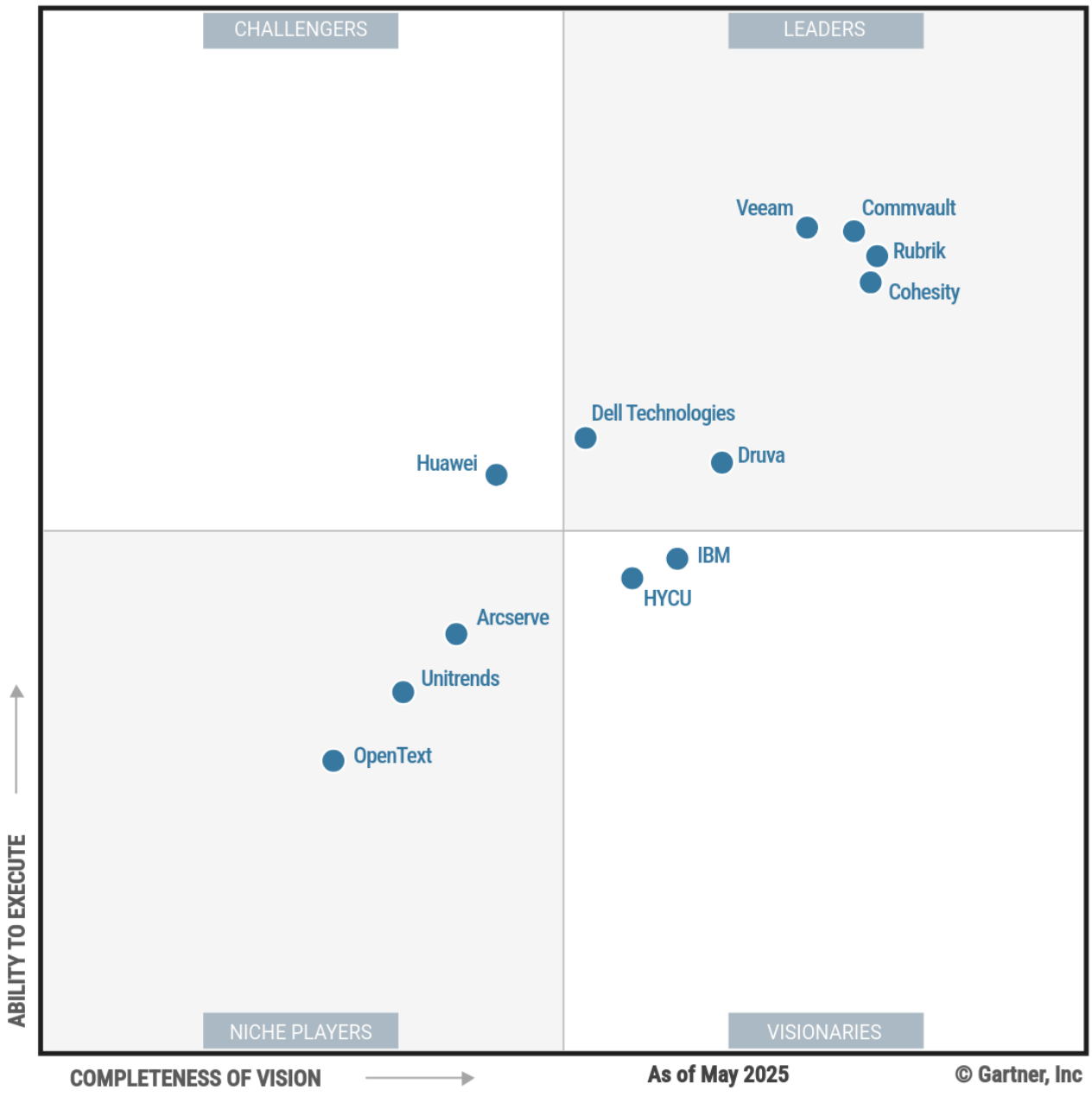
- Native cloud or agentless integrated protection of mission-critical data in cloud provider platform as a service (PaaS) applications, such as Amazon Relational Database Service (RDS), Google Bigtable and Microsoft Azure SQL

- Protection of mission-critical data in SaaS applications, such as Atlassian Jira, Microsoft Entra ID, ServiceNow, Slack and Workday
- 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
- Application discovery capabilities for on-premises and cloud applications to identify application components, dependencies and data protection status and perform backup and recovery of the application
- A vendor-hosted, SaaS-based control plane to manage and orchestrate complex and distributed environments
- A vendor-hosted 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
- Enhanced security capabilities, such as multifactor authentication, role-based access controls and multiperson change validation; integration with privileged access management solutions, security information and event management (SIEM) and security orchestration, automation and response (SOAR) integration; and advanced security reporting and logging
- Application of zero-trust principles across solution design, architecture and deployment practices to ensure the highest level of security and data integrity
- Enhanced cyberrecovery readiness capabilities, such as vendor-developed or third-party integrated real-time anomaly and entropy detection; postbackup and on-demand malware and signature-based detection; and immutable data vault and isolated recovery environment offerings
- Orchestration of disaster and cyberrecovery testing and processes
- Support for expanded platform use cases to assist data protection, compliance, copy data management, and testing and development requirements
- Support for expanded backup data insights and access capabilities such as data categorization and classification, sensitive data scanning, search, investigations, business intelligence, retrieval-augmented generation (RAG) and other API retrieval

- Role-based access controls to provide backup data access to personas outside of the backup administrative teams, such as security, legal, compliance, and data and analytics

Magic Quadrant

Figure 1: Magic Quadrant for Backup and Data Protection Platforms



Gartner

Vendor Strengths and Cautions

Arcserve

Arcserve is a Niche Player in this Magic Quadrant. Arcserve's backup and data protection portfolio includes Arcserve Unified Data Protection (UDP), Arcserve Backup, Arcserve 10000 Series Appliances, Arcserve UDP Cloud Hybrid 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 10 and 10.1, which include the addition of Assured Security for disaster recovery testing, on-demand virtual standby to cloud, and concurrent replication. It also refreshed its hardware appliance offerings with its 10K appliance that offers improved RTOs and RPOs, malware detection, in-line encryption and automated disaster recovery testing. Arcserve also introduced Arcserve Cloud Storage, its managed cloud storage offering, and Arcserve Cyber Resilient Storage, its software-defined storage target for backup.

Strengths

- **Flexible pricing options:** Arcserve offers customers a choice between perpetual and term-based subscription licensing with multiple metrics, including front-end terabytes, sockets and virtual machines, to meet a variety of buyer requirements for pricing models.
- **Renewed product investment:** During the research period, Arcserve demonstrated an improved cadence of new products and features, including an updated version of its UDP software, a refreshed UDP appliance series and a disaster recovery testing platform.
- **Software-defined immutable storage:** Arcserve introduced Cyber Resilient Storage, a software-defined backup storage target for its UDP offering for a choice of on-premises and cloud storage options. It provides integrated immutable storage capabilities that can be deployed as an ISO for bare-metal installation, as a virtual machine and in an Arcserve-managed cloud.

Cautions

- **Narrow large enterprise alignment:** With its focus on midsize enterprise markets and increased delivery of its solutions through managed service providers, Arcserve's growth initiatives and product strategy may limit its suitability for large enterprise accounts.
- **Limited emphasis for cloud backup:** Beyond SaaS application protection, Arcserve's product portfolio offers limited multicloud support and native cloud integrations, and requires the use of agents. Its offerings of software, software-defined backup storage and appliances primarily target on-premises uses and provide integrations of cloud storage as a backup target.

- **Lacking use of AI:** Arcserve's current portfolio and near-term product roadmap lack AI implementation in areas such as ransomware anomaly detection, advanced cyberrecovery and use of GenAI for administration and support.

Cohesity

Cohesity is a Leader in this Magic Quadrant. Its DataProtect and NetBackup portfolios are available for customer-managed deployment for on-premises and in the cloud, as well as an as-a-service offering. Cohesity's operations are geographically diversified. Its clients span from the upper midmarket to very large enterprises. During the evaluation period, Cohesity introduced NetBackup 11, including features such as postquantum encryption, Sheltered Harbor endorsement, hash-based threat hunting and risk engine monitoring of suspicious policy and login changes. Additionally, it enhanced NetBackup recovery orchestration with scheduled rehearsals, cross-cloud/region recovery and automated recovery point recommendations. It enhanced DataProtect, adding immutable cloud backups, improved threat detection, and support for Couchbase NoSQL using a connector agent and Cohesity Gaia, adding new data sources and filetypes, a topic visualizer, and faster response times. Cohesity also updated DataProtect as a Service by introducing support for Microsoft Entra ID, recovery for Microsoft 365 Groups and integration of Microsoft 365 Backup Storage and added a self-managed deployment option for its Helios control plane.

In December 2024, Cohesity completed its transaction to combine Veritas' enterprise data protection portfolio as part of its business. Cohesity now includes the NetBackup and Alta Data Protection product lines.

Strengths

- **Comprehensive product portfolio:** With the addition of Veritas' NetBackup and Alta Data Protection, Cohesity gains a wider breadth of technical expertise and product capabilities to support complex enterprise ecosystems, while providing comprehensive workload coverage for on-premises, multicloud and SaaS.
- **Broad geographic coverage:** With the acquisition of the Veritas data protection portfolio and its expansive global infrastructure and support teams, Cohesity can now reach global markets where Veritas had an established presence.
- **Enhanced cyberincident response services:** Cohesity's Cyber Event Response Team (CERT) service provides incident response (IR) services to help manage response and recovery during cyberevents. CERT is partnered with industry-leading third-party

providers, such as Mandiant and Palo Alto Networks, to further augment its incident response capabilities.

Cautions

- **Overlapping products postmerger:** Cohesity's acquisition of NetBackup may lead to resource limitations for the combined product lines, potentially slowing the pace of product development across the portfolio. The combined portfolio of NetBackup and Alta Data Protection with Cohesity's offerings results in overlapping products and capabilities.
- **Inconsistency in pricing and discounting:** Some clients have questioned Cohesity's pricing norms and discounting, as Cohesity solutions can be more costly during initial negotiations compared with direct competitors.
- **Limited cloud application infrastructure recovery:** Cohesity has limited full-stack application/infrastructure recovery capabilities to capture infrastructure-as-code (IaC) deployments and cloud configurations, making application recovery more complex in large-scale recovery scenarios.

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 Microsoft Active Directory forest-level recovery support, Cloud Rewind, Clumio Backtrack, improved its Cleanroom Recovery cyberresilience operations and added Amazon Web Services (AWS) storage support to its Air Gap Protect offering. Commvault also introduced enhancements to Commvault Cloud Threat Scan and Command Center for Oracle and SAP HANA, as well as new bidirectional integrations with CrowdStrike Falcon Insight XDR and Splunk SOAR. In April 2024, Commvault acquired Appranix and in October 2024, acquired Clumio. These acquisitions expand Commvault's cloud application infrastructure recovery and AWS support, respectively.

Strengths

- **Comprehensive cloud workload coverage:** Commvault's coverage of cloud IaaS and PaaS is broad, including native support for Oracle, Microsoft Azure DevOps, and government cloud coverage for AWS, Azure and Oracle Cloud Infrastructure (OCI).

- **Cloud Rewind strategy:** Commvault's acquisition of Appranix provides improved capabilities for cloud application infrastructure discovery, protection and recovery. This includes complete orchestrated application stack protection and accelerated recovery speeds.
- **Active Directory orchestrated recovery:** Commvault's forest-level orchestrated Active Directory recovery aligns with Microsoft best practices and accelerates Active Directory recovery. Forest recovery is integrated with the granular recovery capabilities of Microsoft Active Directory and Entra ID backup.

Cautions

- **Complex initial configuration:** Some Gartner clients indicate difficulty with initial product design principles when choosing between customer-managed and BaaS architectures, and challenges in finding proper documentation for self-directed configuration troubleshooting efforts.
- **Delayed customer support experience:** Customers have voiced concerns regarding their experience working with the Commvault support team, reporting that subject matter experts (SMEs) are not readily available beyond first-tier support.
- **Lacks unified management console:** Commvault's transition of Commvault Command Center to a feature parity offering with the Java console is incomplete, requiring two different administration tools for complete management. Documentation refers to both management methods, rather than directing users to the web console exclusively.

Dell Technologies

Dell Technologies is a Leader in this Magic Quadrant. Its backup and data protection portfolio consists of PowerProtect Data Manager, PowerProtect Cyber Recovery, CyberSense, NetWorker, PowerProtect Backup Services and PowerProtect 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 the addition of Storage Direct Protection for PowerMax and PowerStore, anomaly detection for virtual machines and file systems, and protection for Red Hat OpenShift Virtualization. Dell also introduced new Data Domain appliances, including an all-flash reference architecture, and new PowerProtect Backup Services

packages to bundle Microsoft 365, Google Workspace and endpoint protection into a single license, and Salesforce Data Archiver as a stand-alone product offering.

Strengths

- **Dell storage protection:** PowerProtect Data Manager integrates with Dell PowerStore and PowerMax storage arrays, using its Storage Direct Protection and DD Boost. This provides efficient data protection for large workloads, particularly benefiting performance-sensitive application requirements.
- **Dell AI Factory integration:** Dell's AI Factory offering for on-premises AI infrastructure includes integration with PowerProtect Data Manager. This integration protects its Kubernetes metadata, training data models, vector DBs, configurations and parameters.
- **Enhanced managed detection and response:** Dell has introduced a managed detection and response service that includes CrowdStrike Falcon XDR Platform licensing and enhanced integration with PowerProtect Data Manager and PowerProtect Data Domain activity logs. The Dell service analyzes and alerts customers to indicators of compromise (IOCs), based on detected activity.

Cautions

- **Lagging market differentiating features:** Dell lags behind other market-leading vendors in full-stack cloud application discovery and recovery capabilities, and extending backup data to additional use cases, such as sensitive data scanning, RAG and other API data retrieval methods.
- **Complex solution administration:** Some Dell customers report its multiproduct administration is too complex to orchestrate and manage its backup and data protection deployment.
- **Multiproduct cyberdetection requirement:** Dell PowerProtect Data Manager provides metadata-based anomaly detection, requiring implementation of Dell PowerProtect Cyber Recovery and CyberSense offerings to perform full file integrity inspection, YARA rule scanning and malware forensics.

Druva

Druva is a Leader in this Magic Quadrant. Its primary backup and data protection offering is Druva Data Security Cloud. Druva's operations are geographically diversified and most of its

clients are in the enterprise and midmarket segments. During the evaluation period, Druva added cross-cloud backup with Azure Storage, integration with Microsoft Sentinel and Microsoft Security Copilot, and Managed Data Detection and Response (MDDR) services. Druva also introduced the AI-powered tool Dru Investigate, which accelerates threat analysis and response, as well as AI-powered anomaly detection for Microsoft 365 and VMware, and Druva Microsoft 365 Backup Express, leveraging Microsoft 365 Backup Storage.

Strengths

- **Strong product strategy execution:** Building upon its enhanced SaaS-based platform architecture hosted on AWS, Druva has accelerated the delivery of new critical offerings and integrations. They include the introduction of an Azure Cloud storage tenant option for backing up AWS EC2 and Azure VMs, support for Microsoft Entra ID, Microsoft Dynamics 365 and agentless backup for Microsoft Azure SQL. Additionally, it has introduced optimized protection capabilities for Amazon S3, Amazon RDS and network-attached storage (NAS).

- **AI-powered operational assistance and security insights:** Dru Assist improves user experience through interactive reporting, guided workflows and smart troubleshooting. It features Dru Investigate for security, detecting insider threats, analyzing anomalies and speeding up incident response.

- **Proactive ransomware defense:** Druva provides a free managed service as a native capability within its data protection platform, delivering proactive cyberresilience for customer backups. This service offers 24/7 monitoring, advanced threat detection and incident response using tailored playbooks, emphasizing early threat neutralization and ensuring reliable data recovery.

Cautions

- **AWS-centric dependency:** Druva's platform management and orchestration layer is built on AWS infrastructure, posing challenges for organizations favoring alternative cloud infrastructure partners or single-cloud avoidance policies.

- **Limited support for Google Cloud Platform (GCP):** Protection for Google Cloud Compute Engine relies on agent-based methods and native support for GCP PaaS services lags when compared to its support for other major cloud providers, warranting careful evaluation for specific GCP workload protection needs.

- **Limited support for MongoDB and Cassandra:** Druva lacks native-application-aware backup for MongoDB and Apache Cassandra databases. Organizations using them would have to rely on other third-party tools or native backup features, which in turn will lead to operational complexity or reliance on complex scripting for backup.

Huawei

Huawei is a Challenger in this Magic Quadrant. Huawei's backup and data protection portfolio consists of OceanProtect DataBackup software and appliances, OceanProtect Backup Storage, OceanCyber Data Security Appliance, OceanStor BCManager and Cloud Backup and Recovery. Huawei's operations are primarily in Asia/Pacific, EMEA and South America, with the majority of its customers in Asia/Pacific. Its clients tend to be in the midmarket and enterprise segments. During the evaluation period, Huawei released OceanProtect DataBackup 1.6.x, which includes support for Nutanix and Microsoft Hyper-V hypervisors, Apsara Stack on Alibaba Cloud, and Microsoft 365 and Entra ID. It also introduced the OceanProtect E series scale-out architecture appliance, and X3000 and X9000 all-flash backup storage appliances.

Strengths

- **Flash-based, scale-out appliance architecture:** Huawei offers a complete portfolio of all flash-based backup appliances. The scope of its portfolio addresses the price and performance expectations of small and midsize businesses (SMBs) to large enterprise customers and provides the benefits of reduced power utilization, energy efficiency, and optimized backup and recovery performance.
- **Multilayer ransomware detection:** Huawei integrates its network and storage solution to proactively detect and block cyberattacks. Its OceanCyber appliances integrate with OceanProtect Backup Storage to protect against ransomware.
- **Data anonymization on copy data reuse:** OceanProtect Data Backup includes the ability to identify sensitive data and perform anonymization on copy data management backup copies.

Cautions

- **Limited multicloud protection:** Huawei OceanProtect agentless cloud integrations are limited to its support of IaaS and PaaS workloads on Huawei Cloud, impeding data

protection and cost efficiencies across other widely adopted cloud environments such as AWS, GCP and Azure.

- **Scope of innovation beyond Huawei portfolio:** Huawei's BaaS offering is limited to deployment on Huawei Cloud, and its Multilayer Ransomware Protection capabilities are limited to integration of Huawei network and storage components.
- **Lacks ransomware recovery warranty or guarantee:** Huawei lags behind market leaders in offering a ransomware recovery warranty or guarantee.

HYCU

HYCU is a Visionary in this Magic Quadrant. HYCU R-Cloud is a hybrid and multicloud BaaS-based backup and data protection 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 into applications and their data protection status in 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 new capabilities to R-Cloud, including R-Shield for ransomware detection and recovery, expanded coverage to Microsoft Azure Local and integration capabilities with Dell's PowerProtect Data Domain using DD Boost integration. It also enhanced R-Cloud, adding support for SaaS and PaaS offerings, such as Box, Nutanix Database Service, Atlassian Bitbucket and Confluence, Microsoft Entra ID, Amazon Virtual Private Cloud, AWS Web Application Firewall, and GitLab.

Strengths

- **Comprehensive SaaS protection strategy:** HYCU's approach to SaaS application protection using an AI-based, low-code development methodology has resulted in a broad list of supported SaaS applications across multiple vendors' application environments.
- **Strong GCP protection:** HYCU provides comprehensive protection of the most common GCP IaaS and PaaS offerings, as well as support for Google BigQuery, Firestore, Artifact Registry, Cloud Functions and Cloud Run.
- **BaaS with customer-selected storage:** HYCU's R-Cloud, its BaaS offering, allows customer flexibility in choosing their own backup storage, including on-premises and cloud targets.

Cautions

- **Limited enterprise market segment:** HYCU's customer base primarily aligns to midsize enterprise organizations, with limited implementations by large enterprise organizations protecting diversified and complex environments.
- **Lagging ransomware strategy:** HYCU lags leading vendors in ransomware detection and response capabilities. Its current R-Shield source-based, snapshot-scanning feature is limited to virtual machines on Nutanix. It lacks anomaly detection during backup operations and integrated threat-hunting capabilities to scan existing backup data, without restoration and third-party malware scanners, for the purpose of identifying cleanest recovery points.
- **Native cloud integration limitations:** R-Cloud requires the use of third-party tools to protect Azure Blob Storage and lacks support for multiple Azure and AWS containers and PaaS workloads. This includes Azure Cosmos DB, Azure SQL Database, Amazon Elastic Kubernetes Service (EKS), Red Hat OpenShift on AWS, and Amazon Elastic Container Service (ECS).

IBM

IBM is a Visionary in this Magic Quadrant. Its backup and data protection portfolio consists of IBM Storage Defender, IBM Storage Defender Data Protect, 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 enhanced the Storage Defender platform by adding integration to protect IBM Storage FlashSystem and Dell's PowerMax storage. It also introduced recovery policy abstraction for enterprise applications such as Oracle, SAP HANA, and VMware. IBM continues to enhance its AI capabilities with watsonx, providing improved capabilities in the areas of backup and recovery operations, failure resolution, and efficiency.

Strengths

- **Integration of AI:** Utilizing IBM watsonx AI models and tools, IBM enhances behavioral analytics, real-time anomaly detection and application-aware insights to identify cyberthreats using its agent-based sensors. This improves operational efficiency and provides some autonomous capabilities, such as incident mitigation, capacity planning and resource allocation.
- **Integrated early threat detection:** Storage Defender offers near-real-time ransomware detection, inferring from multiple sensors distributed across a customer's virtual

machines, file systems, storage and selected applications.

- **Automatic recovery group generation:** Storage Defender leverages insights into protected assets across multiple storage snapshots and backup copies to orchestrate recovery and apply consistent policies to related workloads.

Cautions

- **Dependencies on third-party products:** IBM's Storage Defender Data Protect and Storage Protect for Cloud solutions require dependencies on other vendors for its product and control plane, placing product development outside of IBM's control.
- **Limited multicloud protection:** IBM's Storage Protect for Cloud offers limited protection of IaaS and PaaS services across multiple clouds, including AWS, GCP and OCI. It lacks cloud application discovery and infrastructure recovery capabilities, as well as customer choice of cloud storage.
- **Product rebranding confusion:** IBM clients report confusion and lack of clarity regarding its consistency of capabilities across hybrid, multicloud and SaaS environments in its backup and data protection portfolio.

OpenText

OpenText is a Niche Player in this Magic Quadrant. Its backup and data protection portfolio consists primarily of two products: Data Protector Express and Premium editions 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. During the evaluation period, OpenText enhanced Data Protector by integrating with OpenText Webroot malware detection and by introducing SafeZone Recovery secure backup analysis. It also introduced OpenText Magellan BI & Reporting as the reporting server solution, support for Impossible Cloud, and updates to its web user interface.

Strengths

- **Broad OpenText product integrations:** OpenText provides strong integration with its Webroot offering for malware detection, protection of OpenText Documentum data, and enhanced reporting capabilities using OpenText Magellan BI & Reporting.
- **SaaS application protection:** OpenText offers both customer-managed and vendor-hosted options for Microsoft 365 backup. Data Protector for Cloud Workloads supports

Microsoft 365 customer-managed deployments, while hosted solution CloudAlly supports Microsoft 365 as well as Salesforce, Google Workspace, Box and Dropbox.

- **Broad hypervisor support:** OpenText Data Protector Premium, combined with Data Protector for Cloud Workloads, integrates with most major hypervisors. These include, but are not limited to VMware VMs, Microsoft Hyper-V, Proxmox Virtual Environment, Red Hat Virtualization, Nutanix AHV, OpenStack, Huawei FusionCompute and Scale Computing HyperCore.

Cautions

- **No vendor-hosted BaaS solution:** OpenText does not offer an enterprise-customer-focused BaaS solution for cloud workloads and on-premises.
- **Internal integration focus impacting innovation:** OpenText's focus on investments to integrate Data Protector into the greater OpenText solution stack has limited its innovations in trending areas of the backup and data protection platforms market.
- **No SaaS-based control plane:** OpenText lacks a SaaS-based control plane and common administrative interface for all its solution components, features often found in leading vendor solutions.

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

Rubrik

Rubrik is a Leader in this Magic Quadrant. Its backup and data protection 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 data protection solutions. Rubrik's 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 added data protection and support for Salesforce, Microsoft Dynamics 365, Azure DevOps, GitHub, Microsoft 365 Backup Storage, and virtual machines and databases on OCI. It also introduced anomaly detection and threat scanning for Azure and AWS environments, a new Turbo Threat Hunting capability integrated with Mandiant threat intelligence, and prioritized recovery for M365 to enhance cyberresilience. Along with these improvements, Rubrik released Identity Recovery for Active Directory and EntraID, and Annapurna by Rubrik for GenAI application development.

Strengths

- **Strong cyberrecovery and detection:** Rubrik Security Cloud provides comprehensive cyberrecovery and detection capabilities for data and identity. Features include AI-based in-line anomaly detection, and advanced threat monitoring and hunting capabilities to identify clean recovery points, and orchestrated recovery across hybrid identity environments.
- **Pricing strategy innovation:** Rubrik's Universal SaaS Application License supports unlimited storage capacity per user. The license is portable between any SaaS application supported by Rubrik.
- **Annapurna GenAI RAG solution:** Rubrik Annapurna allows clients to securely build GenAI applications on enterprise backup data in Rubrik Security Cloud, with built-in access controls and sensitive data management.

Cautions

- **Limited geographic coverage:** Customers experience limited engagement with Rubrik outside of North America and EMEA. This is due to limited enabled partners in other geographies, compared with other leading vendors.
- **No cross-hypervisor restore:** Rubrik Security Cloud lacks support for cross-hypervisor restore in data center environments, which limits its ability to support use cases such as disaster recovery, migration and data mobility in multihypervisor customer environments.
- **Limited reporting features:** Some customers have voiced concerns with out-of-the-box reporting features, citing limited capabilities, complex customization needs, and reliance on Rubrik support for assistance.

Unitrends

Unitrends, a Kaseya company, is a Niche Player in this Magic Quadrant. Its backup and data protection 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. During the evaluation period, Unitrends optimized its Backup Software integration with VMware to reduce backup sizes and updated its product tours to walk through common tasks. It also introduced its new Alma 9 operating system and two-factor authentication for its backup appliances. Spanning Backup is now available as part of the Kaseya 365 user subscription

and includes storage options in South Africa. Its updates also include improved Microsoft Exchange Online and OneDrive restore views, and new features such as unlimited shared mailbox protection and mail export to PST file format.

Strengths

- **Unitrends and Datto consolidation:** Kaseya has announced its intention to combine Unitrends with its Datto business. This action is expected to enrich the portfolio available to its customers.
- **Cost-effective cloud storage:** Unitrends provides an egress-free cloud storage for long-term retention and off-site storage. Integrated with its DRaaS offering, it provides the ability to test compliance against customer-defined RTOs and RPOs.
- **Strong integration with Kaseya offerings:** Unitrends UniView provides centralized management of its backup and recovery offering, while also integrating with Kaseya security and service desk solutions. The Kaseya 365 user subscription also includes entitlement to Spanning Backup for Microsoft 365.

Cautions

- **Narrow enterprise suitability:** With its focus on SMB markets and delivery of its solutions through managed service providers, Unitrends' growth initiatives and its limited scalability of appliances contribute to reduced suitability for large enterprise accounts.
- **Lack of SaaS application expansion:** Unitrends Spanning Backup has not added any additional new SaaS workloads during the research period. It lacks support for SaaS applications, such as Microsoft Entra ID, Microsoft Dynamics 365, Slack, Box and GitHub.
- **No GenAI for backup capabilities:** Unitrends' portfolio lacks any features utilizing GenAI to improve and simplify backup administrative tasks.

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 primary backup and data protection offerings are Veeam Data Platform (VDP), Veeam Backup for M365, Veeam Backup for Salesforce, Veeam Kasten, Veeam Data Cloud (VDC) and Veeam Data Cloud Vault. Veeam's operations

are geographically diversified and most of its clients are in the enterprise, midmarket and SMB segments. During the evaluation period, Veeam released multiple product updates, including VDP v12.3, which contains new features like support for Microsoft Entra ID, IOC detection, and proactive threat analysis through tools like Recon Scanner and Veeam Threat Hunter. Key enhancements include support for Proxmox Virtual Environment, AI-driven insights with Veeam Intelligence, and support for Microsoft Hyper-V disaster recovery plans.

Strengths

- **Established market presence:** Veeam has a strong market presence and broad adoption across geographies, supported by a wide network of partners. This enables consistent service delivery, rapid support and access to local expertise, which is important for organizations with global operations.
- **Strong ransomware protection and cyberresilience:** Veeam's comprehensive ransomware protection includes AI-based in-line scanning, Veeam Threat Hunter and IOC detection. Veeam Cyber Secure, a program to offer customers support before, during and after incidents, includes a ransomware recovery warranty and provides real-time first-party incident response during active breaches.
- **Versatile data restoration and mobility:** Veeam supports cross-hypervisor restorations between major hypervisors like VMware vSphere, Microsoft Hyper-V and Nutanix AHV. It also offers direct restore functionality from on-premises workloads to AWS, Azure and GCP.

Cautions

- **Reactive approach to market innovation:** Veeam's offerings and enhancements are generally introduced as a response to competitive offerings and customer demand, rather than leading with novel and differentiating capabilities in the market.
- **Microsoft infrastructure dependency:** Veeam Data Cloud is deployed in Azure, which could be a concern for organizations that rely primarily on other cloud providers. VDC also lacks the flexibility to store backup data in locations managed by other cloud providers, such as AWS and GCP.
- **Limited breadth of SaaS protection:** The Veeam portfolio lacks coverage for the evolving array of SaaS applications other than Microsoft 365, Microsoft Entra ID and Salesforce. This can be a concern and a competitive shortfall for enterprises requiring wider SaaS data protection coverage.

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

Huawei

Dropped

- Microsoft was dropped from this year’s research, as it didn’t meet all mandatory feature requirements. Its Azure Backup product lacks support to protect multicloud environments.
- Veritas has been removed from this year’s research, as its qualifying products have been combined with Cohesity, as a result of the completed transaction to merge Veritas’ enterprise data protection business with Cohesity in December 2024.

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 data protection platform must meet all “Mandatory” features as defined in the Market Definition.
- The vendor’s qualifying backup and data platform multicloud requirement must support protection of infrastructure as a service (IaaS) on TWO public cloud environments that had qualified for inclusion in the 2024 Magic Quadrant for Strategic Cloud Platform Services. Those vendors are Alibaba Cloud, Amazon Web Services, Google, Huawei Cloud, IBM, Microsoft, Oracle and Tencent Cloud.

- 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 April 2025, i.e., it must have been commercially available at least as early as 01 April 2022.
- 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 managed services provider (MSP) sales.
    - The vendor must have generated over $75 million in reported Annual Recurring Revenue (ARR) on 28 February 2025, OR
    - The vendor must have generated over $30 million in reported ARR on 28 February 2025, combined with a year-over-year (28 February 2024 vs. 28 February 2025) ARR growth rate of 20%.
- The vendor must serve an installed base of at least 1,000 customers within the market as defined in section 2. 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 data protection platform products under its own brand name in at least three of the following major geographies: North America, EMEA, Asia/Pacific and Central/South America. At least 25% of total ARR must originate from outside of its major geography.
- The vendor must have a minimum of 50 brought to revenue customers, installed and in production use of its qualifying backup and data protection platform product or solution, in each of at least three of the following major geographies (North America, EMEA, Asia/Pacific and Central/South America). Twenty of the 50 customers, per geography, must have deployed the backup solution for a minimum of 100 physical servers or 300 virtual servers. This excludes endpoint backups.
- 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 12 months must be generally available before 01 April 2025 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 employ at least 100 full-time employees, dedicated to backup and data protection platforms, in engineering, sales and marketing functions combined as of 28 February 2025.

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, SAN, NAS or object storage.
- Vendors whose main source of product revenue (more than 75% of total revenue) is 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, Amazon EC2, Azure Blob, Azure Virtual Machines, Microsoft Hyper-V, VMware, 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 for managing 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, 12 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 backup and data protection 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.

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 backup and data protection 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 product issues impacting customer experience. BDPP use cases include protection of on-premises, hybrid/multicloud and SaaS environments; data services; disaster recovery; and ransomware protection, detection and recovery.

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

Sales execution/pricing: This criterion covers the assessment of a vendor's success in the BDPP market. Considerations include results of new versus repeat business, growth of new backup and data protection customers, and changes in the level of customer investments of

its offerings. 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 BDPP products and capabilities that are first-to-market and differentiating compared to the competition, while also continuing to meet market demands and close 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 BDPP market.

Customer experience: This criterion evaluates the vendor's ability to deliver positive customer experience in their use of BDPP solutions. We look at the 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

Evaluation Criteria	*Weighting*

Source: Gartner (June 2025)

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 for the backup and protection of enterprise environments. We look at the ability of the vendor to 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 BDPP marketing vision that highlights competitive differentiation and an understanding of personas engaged in the selection of backup and data protection solutions.

Sales strategy: This criterion evaluates the vendor's ability to establish and update its BDPP 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 for its BDPP offering, emphasizing its alignment to shortcomings, commitment to differentiation, improvement of existing capabilities, and its extent of using OEM or ISV offerings in its BDPP products.

Business model: This criterion evaluates the vendor's strategies to sustain its business in the BDPP 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 and unique innovations in BDPP product design, marketing, sales and presales, and customer support. We assess whether the vendor's most recent and planned

innovations will add enterprise customer value, whether they're unique or differentiated, and whether they're disruptive to the BDPP market.

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 (June 2025)

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 hybrid IT environments.

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

Heads of I&O responsible for backup operations must assess and rearchitect their backup strategy to include aspects of technology, operations and consumption appropriate for their organizations. The strategy must account for the continued change scope of critical workloads, the use of cloud and demands for increased data protection and cyberresilience by:

- Investing in backup solutions that address data protection requirements in the hybrid, multicloud and SaaS environments. Favor solutions that offer a single pane of glass to manage these distributed environments.
- Choosing backup solutions that combine a built-in or integrated offering for protecting backup data from a cyberattack, performing anomaly and malware detection, alerting to incidents of compromise (IoCs), and expediting recovery from cyberattacks.
- Implementing backup and recovery solutions that offer zero-trust architecture principles.
- Prioritizing use of backup solutions that implement AI, such as GenAI for backup features, to simplify and accelerate backup administration activities, including orchestrated recovery.
- Focusing on solutions that provide capabilities to discover cloud application infrastructure components, and routinely test and orchestrate recovery of applications and data.
- Evaluating the level of resilience of backup copies with the requirement to have multiple immutable copies as soon as possible in the backup process.
- Aligning the backup architecture with the organization's operational recovery requirements. Distinguish backup storage targets for their use in operational recovery, long-term retention and cyberrecovery purposes.
- 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 can augment the value of backup data beyond recovery events. Prioritize solutions that offer added use cases for backup data. This includes sensitive data scanning, classification, investigations, supporting analytics and other data enrichment, and retrieval-augmented generation and API-based data access.

Market Overview

The backup and data protection platforms (BDPP) market is an evolution of the former enterprise backup and recovery software solutions market. This evolution reflects the new

and changing requirements of enterprise organizations as they address the demands of protecting their sprawling and complex data estate. Multiple factors influenced the change in the market definition and evaluation criteria for this year's Magic Quadrant and Critical Capabilities research. Key attributes include:

Platform

- Prioritizes the centralized management and orchestration of data protection platforms.
- Increased scope of requirements delivered via backup as a service (BaaS)
- Autonomous backup operations.
- Expands platform use cases to assist data protection, compliance, copy data management, and testing and development requirements.
- Expands backup data insights and access capabilities such as data categorization and classification, sensitive data scanning, search, investigations, business intelligence, retrieval-augmented generation (RAG) and other API retrieval methods.

Data Protection

- Constant expansion of hybrid, multicloud and SaaS environments that must be protected.
- Emphasizes the requirement for cyberrecovery readiness and robust anomaly detection capabilities.
- Emerging capabilities to perform and expedite malware scanning of backup data and alerts to incidents of compromise (IoCs).
- Application-focused discovery, backup, recovery and disaster recovery.
- Expanded common features, such as zero-trust principles and expanded recovery orchestration.

Backup and data protection platforms vendors evaluated in this Magic Quadrant are innovating and changing the market in the following areas:

Cyberrecovery and Detection Capabilities

- **Ransomware detection and recovery:** Most vendors have built capabilities to detect ransomware attacks by monitoring behavioral anomalies of protected data. They 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.

- **Malware detection:** Vendors are adding malware detection in backup copies by partnering with security vendors or developing these capabilities in-house. They are differentiating in their ability to identify known ransomware variants and zero-day attacks. Recent innovations include malware detection using YARA rule scanning and integrated security vendor feeds and advanced threat hunting using hash-based tracking to flag IoCs.

- **Vendor-hosted storage:** 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 as-a-service offerings by introducing orchestration services to facilitate routine testing, cleaning and validation, and performing recovery.

Administration and Deployment Options

- **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.

- **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.

- **Multicloud storage options:** Vendors are expanding their hosted data plane architecture, allowing customers to choose from multiple cloud storage target options.

Cloud Environment Protection

- **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 keep pace with the expanding scope of more IaaS and PaaS infrastructures, and multiple cloud data locations.

- **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.

- **Cloud application and infrastructure recovery:** Leading vendors are adding application infrastructure and cloud services discovery, and integration with its own, third-party or public cloud services, to backup and protect the application, test and perform failover, and recover the entire application and data environment.

SaaS Application Protection

- **Support for SaaS application protection:** 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 Dynamics 365, Microsoft Power Apps, Atlassian Jira and ServiceNow.

- **Identity access management (IAM) backup and recovery:** Vendors have introduced backup and recovery capabilities for critical identity access management data. They simplify protection and granular recovery of IAM offerings such as Microsoft Active Directory, Microsoft Entra ID and Okta. Recent advancements include orchestrated forest-level recovery of Microsoft Active Directory, following Microsoft best practices.

Implementation of AI/ML and GenAI

- **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.

- **Expanding GenAI capabilities:** Leading vendors in this market have rapidly introduced GenAI-based 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 conversational chats and AI-based responses. The use of GenAI is expected to lead to expanded levels of automation to accelerate recovery and further simplify administration and accelerate recovery.

- **Emergence of agentic AI:** Vendor capabilities to automate tasks through the use of backup agents is emerging. Current capabilities operate in a guidance-based mode of operations.

⊕ Evaluation Criteria Definitions