Magic Quadrant for Backup and Data Protection Platforms

29 June 2026 - ID G00840544 - 48 min read

By Michael Hoeck, Jason Donham, and 2 more

Modern backup and data protection platforms simplify enterprise data protection across hybrid, multicloud, and SaaS environments. Heads of I&O must use this research to evaluate and select vendors that enhance cyber resilience, mitigate critical data risks, and meet operational recovery needs.

Strategic Planning Assumptions

By 2030, 70% of organizations will prioritize the recoverability of identity systems alongside preventive identity and access management (IAM) controls, up from less than 15% in 2026.

By 2030, 35% of enterprises with external SLA obligations will include minimum viable recovery in their incident response plans, up from near 0% today, recognizing that standard broader-environment recovery timelines are incompatible with contractual uptime commitments.

By 2030, 35% of organizations will utilize cloud application infrastructure recovery solutions to complement infrastructure as code (IaC)-based disaster recovery orchestration, up from less than 5% in 2026.

By 2030, 40% of regulated organizations operating in jurisdictions with active data sovereignty or operational resilience mandates will deploy jurisdiction-specific backup and recovery architectures to ensure regulatory compliance and independent recovery, up from fewer than 10% today.

By 2029, 70% of enterprises will have shifted cloud backup responsibilities from cloud operations teams to IT operations teams, 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.

Market Definition/Description

Gartner defines backup and data protection platforms as platforms that capture point-in-time copies of enterprise data for multiple use cases. Primarily used for recovering data from multiple data loss scenarios, they enhance data protection initiatives to improve cyberreadiness and risk management, extract new data insights, and expand data access capabilities. These platforms protect enterprise data 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 data, regardless of the underlying application, infrastructure type and its location, is more important than ever. As enterprises operate in more complex environments, among an expanding threat landscape, backup and data protection platforms must protect enterprise data across hybrid, multicloud and SaaS environments.

These platforms are vital to organizations' ability to recover data following events that cause data, business and operations disruption. Whether such an event is accidental or due to hardware or software failure, operational errors, malicious attacks, or environmental incidents, organizations use these platforms to reliably recover and restore access to the affected data and applications accurately and efficiently.

Platforms must offer effective capabilities to simplify the management of data protection and recovery across increasingly complex and diverse environments. As a result, they must integrate and support roles beyond I&O teams, such as CloudOps, DevOps, identity and access management, applications, and security teams. They must also offer automation capabilities to reduce day-to-day manual administration overhead to protect mission-critical data and test, expedite and orchestrate data recovery responses for both traditional disaster and cyber events.

Platforms 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- and application-driven enablement, such as enhanced data protection and infrastructure integrations and expanded data insights and access.

Enhanced protection capabilities include application and data discovery, automated data-driven policy management, and enhanced cyberrecovery readiness features including identity and access protection, multiple cyber detection capabilities, and automated recovery. Integrations extend to bidirectional operational insights with other infrastructure and operations platforms, such as networking, storage and security.

Expanded data insights and access capabilities enable vendor platforms to present data and augment business processes for new personas beyond the backup administrators. New personas include others in IT, such as security, DevOps, and data and analytics, as well as 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 major public cloud service provider environments (such as AWS, Azure and GCP) and 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 requires policy-driven backup and data management 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 including vendor-provided storage such as immutable file systems; appliances and data vaults; and third-party purpose-built, immutable backup appliances.

- Cyberattack detection capabilities, such as vendor-developed or third-party integrated, postbackup anomaly and entropy detection.
- Centralized console for management of distributed backup platform infrastructure across hybrid and multicloud environments.
- Protection of additional workloads and support for use cases such as edge and remote branch office sites.

Optional Features

- Native cloud or agentless integrated protection of mission-critical data in major public cloud platform as a service (PaaS) applications, such as Amazon Relational Database Service (RDS), Google Bigtable and Microsoft Azure SQL.
- Protection of identity and access management (IAM) systems such as Microsoft Active Directory, Microsoft Entra ID, Okta Platform and Ping Identity Platform.
- Protection of additional mission-critical data in SaaS applications, such as Atlassian Jira, Github, Microsoft Azure DevOps, ServiceNow and Slack.
- Data discovery capabilities for on-premises and cloud application data, including data not protected, to automate identification of critical data and its assignment to protection policy, drive cost optimizations, and improve disaster readiness.
- Application discovery capabilities for on-premises and cloud applications to identify application components, dependencies, infrastructure as code (IAC) and data protection status and perform backup and recovery of the application.
- Enhanced cyberreadiness capabilities, such as vendor-developed or integrated third-party real-time (during backup) anomaly and entropy detection; postbackup and on-demand malware and signature-based detection; account- and user-based behavioral analysis; identification of clean recovery points; and immutable data vault and isolated recovery environment offerings.
- Multiple-layer cyberattack detection capabilities that integrate signals from multiple systems, such as access management, data usage and anomaly/malware detection.
- Support for infrastructure, such as data and control planes, administration and recovery capabilities dictated by data sovereignty, and local regulatory requirements.

- A vendor-hosted, SaaS-based platform control plane to administer and orchestrate complex and distributed environments.
- A vendor-hosted BaaS offering to deliver backup and recovery services for hybrid, multicloud and SaaS environments.
- Generative and agentic AI automation features to simplify administration; improve support services; and accelerate backup, recovery and data protection outcomes.
- Enhanced security capabilities, such as multifactor authentication, role-based access controls and multiperson change validation; integration with security information and event management (SIEM) and security orchestration, automation and response (SOAR) integration; and advanced security reporting and logging.
- Orchestration of disaster and cyberrecovery testing, integrity validation and processes.
- Support for expanded platform use cases to assist data protection compliance and backup data insights, analytics and access.
- Protection of additional workloads and support for use cases such as endpoints, AI agents, large language model (LLM) infrastructure and data.

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 primary backup offering is Arcserve Unified Data Protection (UDP), available as software-only and integrated with Arcserve Cyber Resilient Storage, and Arcserve Cloud Direct, a backup as a service (BaaS) offering. Its operations are geographically diversified, with the majority of its revenue coming from Asia/Pacific, EMEA and North America. Its clients are mainly small and midsize businesses (SMBs) and midsize enterprises. In the last 12 months, Arcserve introduced AI-driven anomaly detection and encryption detection, automated disaster recovery (DR) runbooks and expanded SaaS backup support to include Microsoft Power

BI, Jira, Confluence and Azure DevOps. Additionally, Arcserve launched UDP and data protection expert chatbot. It also developed agentless protection for Proxmox and introduced a new on-premises immutable storage option, fully integrated with UDP.

Strengths

- **AI-Driven Support and Backup Optimization:** Arcserve integrates its AI chatbot, ArcGenie, directly into the product to assist with Level 1 support and guided troubleshooting. Arcserve is also expanding its AI capabilities to continuously monitor backup health, flag deviations, and recommend policy optimizations to help ensure that administrator-defined recovery time objectives (RTOs) and recovery point objectives (RPOs) are consistently met.
- **Assured Recovery and Resilient Data Protection:** Arcserve UDP's Assured Recovery feature ensures backups are fully recoverable, consistent and trustworthy by automatically validating recovery workflows. It also integrates malware scanning and AI-driven anomaly detection to identify suspicious encryption or mass changes, along with layered immutability through cloud object lock, copy-on-write snapshots and write once, read many (WORM) tape to protect against data tampering and ransomware.
- **Cross-Hypervisor and Hybrid Mobility:** Arcserve supports cross-hypervisor restoration and migration across VMware vSphere, Microsoft Hyper-V, Nutanix AHV and Proxmox. It provides physical-to-virtual (P2V) and physical-to-cloud (P2C) conversion capabilities, along with direct restore and virtual standby functionality for recovery to Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

Cautions

- **Lacks Cloud-Native Support:** Arcserve lacks cloud-native, agentless integrations to protect infrastructure as a service (IaaS) and platform as a service (PaaS) workloads, including fully managed cloud databases and object data stores. It does not support Amazon Relational Database Service (RDS), Aurora, Amazon DynamoDB, Amazon S3, Microsoft Azure SQL, Azure Cosmos DB, Azure Blob, Google Cloud SQL, or Google BigQuery.
- **Missing Security Information and Event Management (SIEM) and Threat Hunting Integrations:** Arcserve lacks out-of-the-box integrations with third-party incident

response tools or SIEM platforms for communicating indicators of compromise (IOCs) or ransomware alerts.

- **Agent Reliance for Public Cloud Virtual Machines (VMs):** To protect virtual machines, such as Amazon EC2, Azure VMs, or Google Compute Engine, a backup agent must be installed and managed within each VM. Arcserve does not support agentless backup for cloud VMs, whereas many other vendors offer agentless alternatives that simplify deployment and management.

Cohesity

Cohesity is a Leader in this Magic Quadrant. Its primary offering is Cohesity Data Cloud, which is managed via the unified Helios control plane and available as SaaS or self-managed software. Its operations are geographically diversified, and its clients tend to be midsize to large enterprises, including Fortune 1000 organizations in the financial, healthcare and public sectors. In the last 12 months, Cohesity introduced a self-managed, fully air-gapped on-premises deployment option for Gaia, its GenAI assistant for conversational search. It also launched native Data Security Posture Management powered by Cyera, and added support for federated search via Microsoft 365 Copilot using a Model Context Protocol (MCP) server, enabling users to securely query governed backup data directly from AI tools without switching contexts.

Strengths

- **Recovery Orchestration:** Cohesity introduced RecoveryAgent, a cyber recovery capability that orchestrates AI-driven blueprint automation, cloud application recovery, multiplatform workflows, cleanroom operations, threat scanning, application-level recovery groups, and playbook creation to accelerate complex disaster recovery and cleanroom rehearsals.

- **Advanced Cyber Readiness:** Cohesity continues to enhance its cyber readiness capabilities through its FortKnox offering across cloud and on-premises environments, providing isolated, immutable recovery. Expanded integrations with Sophos and Google Threat Intelligence improve threat scanning and detection, helping customers identify compromised data earlier and enable more reliable recovery from cyber incidents.

- **Workload Coverage:** Cohesity provides extensive workload coverage, driven by the Helios control plane's ability to manage both DataProtect and Veritas NetBackup

environments. Flexible licensing lets customers choose between the platforms or use both. This, combined with expanded support for Proxmox, Nutanix AHV, Azure Database PaaS, Azure Blob, AKS and IKS/ROKS, strengthens coverage across hybrid and multicloud environments.

Cautions

- **Reliance on Third-Party Integrations:** Cohesity relies on OEM partnerships and recent third-party integrations for certain backup and data protection platform (BDPP) capabilities, such as Semperis for orchestrated Active Directory Forest Recovery (ADFR) and Cyera for data discovery and classification. This requires customers to rely on Cohesity to maintain seamless technical and commercial integration over time.
- **Limited SaaS protection:** Compared to other leading vendors, Cohesity lacks SaaS protection for Microsoft 365 Dynamics, Power Platform and Azure DevOps, Okta, and GitHub.
- **Deployment and Integration Complexity:** Some Gartner clients indicate Cohesity deployments in complex hybrid environments may require deliberate planning and design work for its integration with existing infrastructure, policy alignment and workload onboarding to achieve desired outcomes.

Commvault

Commvault is a Leader in this Magic Quadrant. Its primary backup offering is Commvault Cloud, available as software-, appliance- and backup as a service (BaaS)-based models. Commvault's operations are geographically diversified, and its clients tend to be large enterprises. In the last 12 months, Commvault introduced Cloud Unity to centralize administration, and Recovery Groups and reusable runbooks to orchestrate complex, multiworkload recovery. It also enhanced its Arlie AI capabilities and BigQuery protection, and added support for Azure Databricks lakehouse, GitHub, Git Lab and monday.com. Commvault also acquired and integrated Satori to expand the Commvault Cloud Risk Analysis offering to include data access governance capabilities, and support for structured and unstructured data sources.

Strengths

- **Expanded GenAI-based Administration and Assistance:** Commvault has expanded use cases and features of its Arlie GenAI-based assistant. Arlie Data Sense provides AI-

driven visibility of protected data and identifies potential data exposure and operational risks. Arlie Advisor provides AI-generated recommendations to improve configurations and policies. Arlie Recover enables guided recovery workflows with AI-assisted identification of clean recovery points.

- **Synthetic Recovery Point:** Commvault introduced Synthetic Recovery, which builds an ideal recovery point from multiple backup sets. By selectively identifying and curating a clean list of files while quarantining and excluding malware threats, the function avoids reverting to a single, older point in time, accelerating recovery operations and minimizing potential data loss.
- **Cleanroom Recovery Orchestration:** Commvault's Cleanroom Recovery feature offers an automated and dynamically provisioned, isolated recovery environment on Microsoft Azure and Amazon Web Services (AWS). It reduces customer cloud operating costs by orchestrating on-demand deployment and decommissioning of required recovery infrastructure, such as virtual networks, storage, hosts and security groups, for cyber recovery testing and operational tasks.

Cautions

- **Mixed Customer Support Experiences:** Some Gartner clients report first-line support can be inconsistent, slow and overly procedural to escalate for complex support interactions.
- **Licensing Complexity:** Some Gartner clients have described Commvault's licensing and pricing as complex, requiring product knowledge, negotiation and careful planning to understand entitlements, forecast long-term cost and manage growth.
- **Lacks Microsoft 365 Curated Clean Recovery:** Commvault lags other leading vendors in built-in capabilities to detect cyberattacks in Microsoft 365 data and curate a verifiably clean recovery dataset.

Dell Technologies

Dell Technologies is a Leader in this Magic Quadrant. Dell's backup and data protection portfolio is Dell PowerProtect, consisting of software-defined, backup as a service and appliance offerings. Its operations are geographically diversified, and its clients tend to be large enterprises, with some presence in the midmarket. In the last 12 months, Dell introduced the PowerProtect AI Assistant, an on-premises GenAI chatbot. It also added

support for archive to object storage integrating Dell ObjectScale and public cloud targets such as Azure Blob and Wasabi, and machine learning (ML)-based detection for mass backup data deletion. Additionally, Dell added a new PowerProtect integrated appliance, a customer-managed unified management dashboard, the Dell PowerProtect DD9910F all-flash appliance, and support for CyberSense on Azure deployments.

Strengths

- **Integrated Dell Portfolio Strategy:** Dell's integration of its PowerProtect portfolio with its storage portfolio optimizes backup and recovery operations with Dell PowerStore, PowerMax and PowerScale offerings and enables near real-time anomaly detection in PowerStore snapshots.
- **Deep Content Analytics:** Dell's PowerProtect Cyber Recovery solution performs full-content machine learning analytics to evaluate change patterns and detect ransomware corruption, with a validated 99.99% detection accuracy rate when identifying the last known good recovery point.
- **On-Premises AI Assistant:** Dell's introduction of PowerProtect AI Assistant is designed for customer-managed deployments without reliance on public clouds. It offers bring-your-own large language models (BYOLLM) for customers to use their own LLM.

Cautions

- **Inconsistent Sensitive Data Identification:** Dell's PowerProtect portfolio provides inconsistent support for sensitive data identification and classification. Its PowerProtect Data Manager lacks insights into sensitive data to assist the identification of critical data and protection gaps, and optimize data protection policies and practices.
- **Limited Cloud Application Discovery and Protection:** Dell lags leading vendors in multicloud application discovery and protection capabilities, such as comprehensive discovery and tracking of dynamic cloud-native application dependencies; identifying configuration and infrastructure as code (IaC) gaps; and streamlining disaster recovery testing and recovery.
- **Operational and Architectural Complexity:** Some Gartner clients indicate Dell's multiproduct PowerProtect offering can introduce operational and architectural complexity that requires significant planning, expertise and coordination to design, deploy and operate.

Druva

Druva is a Leader in this Magic Quadrant. Its primary backup and data protection offering is Druva Data Security Cloud, a fully managed SaaS platform. Its operations are diversified geographically across North America, EMEA, and Asia/Pacific, targeting enterprise and midmarket segments. In the last 12 months, Druva has focused on autonomous capabilities, featuring DruAI agents for automated investigation and recovery workflows. Other platform investments include Azure/AWS cross-cloud resilience and sovereign vaulting enhancements, integrations with Microsoft Sentinel for automated response, and protection of Microsoft Copilot AI artifacts, including per user protection of queries, AI prompts, model outputs, and metadata accessed by Copilot.

Strengths

- **Data Mapping and Integration:** Dru MetaGraph links backup data with metadata and identity signals to create a map of environment relationships. This allows administrators to perform recovery tasks based on specific user context rather than just file location.
- **Agentic AI Diagnostics and Automation:** DruAI agents automate activities such as forensic analysis, threat investigation and operational troubleshooting. This includes autonomous resolution of misconfigured backup policies and failed backups, restore validation and technical incident summaries.
- **Security Architecture and Monitoring:** Druva's SaaS model isolates backup data and credentials from the primary network to limit the attack surface. Security is maintained through multiperson authorization for critical changes and 24/7 monitoring for behavioral anomalies.

Cautions

- **BaaS Deployment Constraints:** Because Druva is delivered exclusively as a fully managed BaaS platform, it does not offer options for customer-managed deployments or bring-your-own-storage (BYOS) architectures. Enterprises with strict mandates that require localized control over their backup infrastructure or dedicated on-premises repositories may find this architecture does not fully align with their deployment preferences.
- **Limited Google Cloud Platform Integration:** Druva offers limited cloud-native, agentless integration to protect IaaS and PaaS workload on Google Cloud Platform

(GCP). It requires agents and use of export workflows to protect workloads such as Google Compute Engine, Cloud SQL and BigQuery.

- **Limited Kubernetes support:** Druva lags other leading vendors in API-integrated Kubernetes backup for container platforms such as Amazon EKS, Azure AKS and Red Hat OpenShift.

Huawei

Huawei is a Challenger in this Magic Quadrant. Its primary backup offerings are OceanProtect, delivered as both software and integrated backup appliances, and OceanCyber appliances, managed via the Data Management Engine (DME). Its operations are mostly focused in Asia/Pacific, EMEA and South America, and its clients tend to be large enterprises in government, finance and manufacturing. In the last 12 months, Huawei introduced the OceanCyber 310 data security appliance, offering a 99.99% ransomware detection rate. It expanded multiplatform BaaS across AWS, Azure and Alibaba, released high-density appliance configurations featuring up to 122TB quad-level cell (QLC) SSD capacity, added protection for AI workloads (including model weights and vector databases), and launched AirGap 2.0 with Clean Room.

Strengths

- **Tailored Industry Strategy:** Huawei employs dedicated, industry-specific solution architects and compliance experts to build tailored solutions for finance, government and manufacturing sectors. This strategy includes a stringent 3-2-1-1-0 data protection architecture for financial institutions and dedicated BaaS with tenant management on Huawei Cloud Stack for government agencies.

- **Advanced Cyber Readiness:** Huawei uses its Flash-to-Flash-to-Anything (F2F2X) architecture to accelerate backup, detection and recovery operations. This enhances its multilayer ransomware protection (MRP) capabilities, which combine detection, immutability and isolation to enhance resilience and support faster, more reliable recovery from cyber incidents.

- **Backup Appliance Innovation:** Huawei has introduced the use of QLC flash storage in its OceanProtect portfolio. This enables high-density, cost-efficient flash appliances that balance capacity and performance, supporting faster recovery and scalable data protection.

Cautions

- **Narrow Go-to-Market Strategy**: Huawei's go-to-market strategy and strongest technological differentiators are deeply intertwined with its own hardware ecosystem. The company relies heavily on upselling BDPP solutions to its existing primary storage customer base.
- **Geographic Market Concentration:** Huawei's marketing penetration and sales execution are concentrated in the Asia/Pacific, EMEA and South America regions. Global enterprises with a significant U.S. footprint face limitations in adopting Huawei solutions due to geopolitical constraints.
- **Limited Identity Protection:** Huawei offers limited identity protection capabilities within its backup platform, lacking orchestrated Active Directory Forest Recovery (ADFR) and requires customers to rely on third-party tools for Microsoft Entra ID and Okta protection.

HYCU

HYCU is a Visionary in this Magic Quadrant. HYCU's primary backup offering is the HYCU R-Cloud Platform. It is a BaaS-based offering for on-premises, cloud and SaaS backup. R-Cloud is complemented by R-Graph for SaaS application discovery and R-Shield for cyber resilience. HYCU's operations are primarily in North America and EMEA, and its clients tend to be upper-midmarket. In the last 12 months, HYCU introduced its Data Exfiltration Protection capability in R-Shield by integrating Halcyon and added native protection of Microsoft 365. HYCU also added support for Microsoft Azure SQL, Azure SQL Managed Instance and Hyper-V, and Citrix XenServer, and expanded GCP BigQuery protection to include models, row-level security policies and metadata.

Strengths

- **Comprehensive Identity and Access Management (IAM) Backup:** HYCU offers broad protection coverage of multiple IAM sources that includes granular restore and cross-tenant recovery for Microsoft Entra ID, Okta Workforce Identity, Okta Auth0 and AWS IAM.
- **Broad Storage Options for All Workloads:** HYCU's open storage architecture allows customers to select bring-your-own-storage for storing all protected workloads, including cloud, SaaS and on-premises. This accommodates many data residency, privacy and regulatory requirements.

- **Extensive Cross-Hypervisor Mobility:** HYCU offers extensive mobility with automated cross-hypervisor recovery and physical-to-cloud (P2C) conversions, allowing organizations to failover, recover or migrate workloads across VMware, Nutanix, Hyper-V, AWS, Azure and GCP. This also facilitates restoration workflows for test/dev use cases, disaster recovery scenarios and infrastructure transitions.

Cautions

- **Limited Complex Deployments:** HYCU's customers often align its offerings to requirements for protecting a distinct set of workloads. This requires customers to further evaluate its suitability for use in diversified and complex environments.
- **Lacks GenAI and Agentic Automation:** HYCU lacks GenAI and agentic AI capabilities. Features such as conversational assistants, AI-based guided recovery and troubleshooting, and autonomous policy optimization are not currently available.
- **Limited Instant Recovery:** HYCU's reliance on platform-native storage layer snapshots does not provide run-from-backup recovery storage capabilities for virtual machines or databases, which can potentially increase recovery time objectives (RTOs) for large workloads. Organizations with aggressive RTO requirements should account for the need to fully restore data before workloads become operational.

IBM

IBM is a Visionary in this Magic Quadrant. Its primary offering is IBM Storage Defender, a SaaS-based and customer-installable control plane that orchestrates multiple IBM and partner solutions for backup and recovery operations. Its operations are geographically diversified, and clients tend to be large enterprises within the public sector, financial services, manufacturing and healthcare industries. In the last 12 months, IBM enhanced Defender Sensors with the ability to scan storage snapshots for ransomware indicators, improving detection of threats within backup data. It also introduced a mixture-of-experts (MoE) machine learning model to improve detection accuracy and reduce false positives at scale. In addition, IBM expanded workload protection across AWS, GCP (BigQuery, Spanner) and Microsoft 365 (Dataverse), while introducing AI-driven application auto-grouping to simplify and accelerate recovery.

Strengths

- **Advanced Threat Detection:** The platform utilizes an MoE machine learning model combined with multilayered Defender Sensors to reduce false positives and accurately ascertain cyberattacks.
- **Regulatory Recovery Certification:** IBM integrates Storage Defender with IBM Security X-Force threat intelligence and Cyber Range simulations, allowing customers to practice recovery procedures and generate certifiable proof of recovery readiness for regulatory audits.
- **AI-Based Application Auto-Grouping:** IBM uses GenAI and metadata analysis to discover and group dependencies belonging to the same application, and automates generation of application recovery guides.

Cautions

- **Multivendor Platform Strategy Limitations:** IBM's multivendor management platform strategy may require multiple preselected third-party solutions to accommodate customer protection requirements. This requires IBM to maintain seamless technical and commercial integration over time and offers customers limited product options toward protecting specific workloads.
- **Identity Recovery and Resilience Limitations:** IBM's Storage Defender lacks support for orchestrated Active Directory Forest Recovery (ADFR) and protection of Okta.
- **Manual Host-Based Agent Deployment:** IBM lacks native auto-deployment capabilities for host-based backup agents, requiring customers to rely on manual downloads or third-party distribution tools like Ansible.

OpenText

OpenText is a Niche Player in this Magic Quadrant. Its primary offering, OpenText Data Backup & Recovery 360 (DB&R360), is available as software. Its operations are geographically diversified, and clients are mostly large enterprises and upper midmarket. In the last 12 months, OpenText introduced SafeZone Recovery for clean room restore orchestration and added support for Microsoft Entra ID protection. It expanded immutability across its integrations with HPE StoreOnce and Dell PowerProtect Data Domain. OpenText also added support for KVM, Red Hat OpenShift, OpenStack and VMware TKG; modernized its web user interface (UI); added malware scanning for at-rest

backups; and embedded OpenText Aviator to deliver AI-assisted anomaly detection, guided troubleshooting and compliance reporting.

Strengths

- **AI-Assisted Operations and Intelligence:** The integration of OpenText Aviator and OpenText Intelligence, OpenText's business intelligence and analytics platform, provides contextual AI capabilities, guided troubleshooting and advanced operational analytics. Additionally, its native data discovery and classification helps organizations identify sensitive data and compliance risks directly within backup sets.
- **Broad Enterprise Workload and Hybrid Support:** OpenText offers application-aware protection for mission-critical databases such as SAP HANA, Oracle, Microsoft SQL Server and IBM Db2. It supports bare-metal recovery and protection for virtual and container environments, including VMware, Hyper-V, Nutanix, Kubernetes, OpenShift and Proxmox.
- **Security-First Cyber-Resilience and Cleanroom Recovery:** OpenText provides cyber-recovery capabilities, such as SafeZone Recovery, for an isolated recovery environment and validation of clean recovery. The platform features AI-based backup anomaly detection, scan-before-restore and at-rest malware scanning via Webroot, OpenText's cybersecurity solution with endpoint protection and threat intelligence capabilities.

Cautions

- **Fragmented Management Interfaces:** OpenText does not provide a single, monolithic unified user interface for all components across the DB&R360 portfolio. While it provides shared identity and centralized reporting, administrators still need to navigate specialized interfaces for specific capabilities, such as CloudAlly for SaaS backup.
- **Active Directory (AD) Recovery Limitations:** OpenText does not support searchable AD metadata, granular recovery of specific AD objects natively, or automated recovery of an entire AD Forest or multidomain environment.
- **No Cloud Application Infrastructure Recovery Services (CAIRS) Capabilities:** OpenText does not provide CAIRS capabilities such as dependency-aware discovery, configuration capture, or full-stack reconstruction of cloud environments across AWS,

Azure or GCP. Its cloud approach is limited to workload-level backup and recovery and does not support coordinated recovery of interconnected cloud services.

Rubrik

Rubrik is a Leader in this Magic Quadrant. Its primary offering is Rubrik Security Cloud, available as a SaaS-based or customer-installable control plane to orchestrate appliance- and cloud-based deployments. Rubrik's operations are primarily focused on North America and EMEA, and its clients tend to be midsize to large enterprise customers. In the last 12 months, Rubrik introduced Rubrik Agent Cloud, with the Semantic AI Governance Engine (SAGE) to govern AI-agents, and Agent Rewind to rollback data or systems impacted by an AI agent. It added identity protection for Microsoft Entra ID and Okta, and support for GitHub, Azure DevOps and Google Workspace. Rubrik enhanced its threat-hunting capabilities to scan indicators of compromise (IOCs) in unstructured data through its network-attached storage (NAS) Cloud Direct offering and cloud workloads on AWS, Azure and GCP. It also added cloud support for Oracle Cloud Infrastructure (OCI) and expanded Rubrik Cloud Vault to Google Cloud Platform (GCP).

Strengths

- **Market innovation:** Rubrik continues to innovate its backup and data protection platform by introducing its AI-agent semantic-based monitoring and action rollback, identity protection capabilities including change monitoring, rollback and recovery, and prenegotiated, consumption-based pricing.
- **Simplified, Unified Platform Administration:** Rubrik Security Cloud retains its simplified administration as the platform expands to broader data, identity and AI-agent backup and data protection capabilities. It provides an intuitive, unified SaaS interface to manage all administration, policies, reporting and analytics across all protected environments.
- **Identity Protection Scope:** Rubrik integrates identity access management change monitoring and protection for Active Directory, Entra ID and Okta into its Identity Resilience offering. For the supported identity providers, it performs continuous monitoring and risk analysis of configuration changes, and provides granular, comparison-based rollback and recovery capabilities.

Cautions

- **Lacks Native Isolated Recovery Environment:** Rubrik lags other leading vendors in providing a packaged, native isolated recovery environment.
- **Limited BaaS offering:** Rubrik's vendor-hosted BaaS offering requires customer-managed cloud infrastructure to support AWS and Azure environments.
- **Limited Cloud Application Recovery:** Rubrik's cloud application recovery currently lacks native orchestration, requiring organizations to manage infrastructure-as-code components separately from data backups.

Veeam

Veeam is a Leader in this Magic Quadrant. Its primary offering is Veeam Data Platform, available as software and virtual appliances. Veeam's operations are geographically diversified, with the largest revenue share in EMEA followed by North America. Veeam customers cover a broad range of market segments, maintaining large SMB and midmarket activity while generating over half its revenue from large enterprises. In the last 12 months, Veeam introduced its Linux-based Veeam Software Appliance, BaaS protection for Microsoft Entra ID, anomaly detection for Microsoft 365, and natural language querying of platform telemetry to its GenAI-assistant. Veeam also acquired Securiti AI and released Agent Commander, which combines AI agent governance and action rollback.

Strengths

- **Securiti AI Integration With Veeam:** Veeam's acquisition of Securiti AI adds the DataAI Command Graph to its portfolio, providing data security posture management (DSPM) and classification for both live and backup data. This integration provides more precise backup policies, improves regulatory compliance and enables prioritized recovery, allowing organizations to restore the most sensitive data first during an incident.
- **Cyber Extortion and Incident Response Services:** Coveware by Veeam natively offers cyber extortion readiness services and 24/7 incident response with a 15-minute SLA. This includes forensic triage, expert threat actor negotiation, decryption assistance, end-to-end incident handling, and ransomware-specific tabletop exercises.
- **Linux Software Appliance:** Veeam has released the Veeam Software Appliance (VSA), a preconfigured Linux backup server that removes the need for a Windows operating

system. It comes prehardened to DISA Security Technical Implementation Guides (STIG) standards and includes built-in security features such as multifactor authentication and immutable storage.

Cautions

- **Lack of Unified Management Console Experience:** Veeam's management experience is fragmented, requiring separate consoles for Veeam Data Platform and Veeam Data Cloud solutions.
- **Limited SaaS Application Coverage:** Veeam lacks support for enterprise SaaS workloads such as Microsoft Power Apps, Dynamics 365 and Azure DevOps, Atlassian Jira and Google Workspace.
- **Slow Progress on Identity Recovery and Resilience:** Veeam lags other leading vendors in identity protection capabilities. It lacks support for orchestrated Active Directory Forest Recovery (ADFR) and protection of Okta.

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

Kaseya (Unitrends) was dropped.

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 protection platform multicloud requirement must support protection of infrastructure as a service (IaaS) for at least two public cloud environments that have qualified for inclusion in the 2025 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's qualifying backup and data protection platform SaaS requirement must support protection of data on two or more major SaaS applications, such as Microsoft 365, Salesforce, Google Workspace, Microsoft Entra ID, Microsoft Dynamics 365, Microsoft Azure DevOps, Atlassian Jira, Github, ServiceNow, Slack, and Okta.
- The vendor must have at least one qualifying backup and data protection platform offering generally available for use by enterprises for three calendar years prior to 01 April 2026, i.e., it must have been generally available at least as early as 01 April 2023.
- 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 31 December 2025 OR
    - The vendor must have generated over $30 million in reported ARR on 31 December 2025, combined with a year-on-year (31 December 2024 vs. 31 December 2025) ARR growth rate of 20%.
- The vendor must serve an installed base of at least 1,000 customers within the backup and data protection platform market. In addition, at least 250 of the 1,000 customers must have deployed the backup platform 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 largest geography.
- The vendor's qualifying backup and data protection platform(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 2026 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 31 January 2026.

The following exclusion criteria apply:

- Vendors offering backup and data protection products or solutions whose software is sourced primarily from a third-party ISV.
- Vendors whose main source of backup and data protection platform revenue (more than 75% of total revenue) is from hosting data centers and managed service providers.
- Vendors offering products that serve only as a target or destination for backup but do not actually perform the backup and restore management function. Examples include purpose-built deduplication appliances, storage area network (SAN), network-attached storage (NAS) or object storage.
- Vendors whose primary backup and data protection offering is designed and positioned mainly to support one or more of the following:
    - Back up only 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.

- Back up only SaaS applications.
- Back up only endpoints such as laptops, desktops and mobile devices.
- Back up only remote offices, edge locations and lower midmarket/SMB environments.
- Back up only specific storage or hyperconverged systems vendors.
- Serve only as replication and disaster recovery tools.
- Serve primarily for managing snapshot and replication capabilities of storage arrays or public cloud infrastructure.
- Serve primarily for copy data management (CDM) or DevOps testing use cases.
- Serve primarily for continuous data protection (CDP).

Honorable Mentions

The providers that are most relevant to our clients were selected for evaluation in this Magic Quadrant. However, the decision not to evaluate a provider does not mean that the provider lacks viability. The following are noteworthy providers not included in the formal analysis. These providers could be appropriate for clients, contingent on their requirements:

- **Acronis:** This backup and data protection platform vendor is headquartered in Switzerland. Acronis provides software-, appliance- and BaaS-based offerings.
- **Bacula Systems:** This backup and data protection platform vendor is headquartered in Switzerland. Bacula Systems provides software-based offerings as open-source and as commercially licensed and supported products.
- **Kaseya:** This backup and data protection solution platform is headquartered in the United States. Kaseya provides software-, appliance- and BaaS-based offerings.
- **Synology:** This backup and data protection solution platform vendor is headquartered in Taiwan. Synology provides software-, appliance- and BaaS-based offerings.

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 its 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

Source: Gartner (June 2026)

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 its product vision, based on its 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

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 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	Low
Sales Strategy	Medium
Offering (Product) Strategy	High

Evaluation Criteria	*Weighting*
Business Model	Medium
Vertical/Industry Strategy	Low
Innovation	High

Source: Gartner (June 2026)

Quadrant Descriptions

Leaders

Leaders have the highest combined measures of Ability to Execute and Completeness o Vision. They have the most comprehensive and scalable product portfolios to support backup and recovery requirements of hybrid, multicloud and SaaS IT environments. Leaders 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 cyber recovery 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. To develop a strategy that accounts for the continued changing scope of critical workloads, the use of cloud, and demands for increased data protection and cyber resilience, heads of I&O must:

- Invest 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.
- Choose backup solutions that combine built-in or integrated offerings for protecting backup data from a cyberattack, performing anomaly and malware detection, alerting to indicators of compromise (IOCs), and expediting recovery from cyberattacks.
- Evaluate the organization’s use of AI and the requirements of safeguarding the protection of critical AI datasets such as AI models, vector databases, training/fine-tuning datasets, and inference logs.
- Refine cyber recovery readiness focusing on zero-trust architecture principles, recovery of minimum viable business (MVB), isolated recovery environments (IREs) and clean rooms.
- Evaluate vendors that include data discovery and backup intelligence capabilities to identify overprotected and underprotected data and workloads, flagging inefficient retention policies and predicting operational issues.

- Prioritize use of backup solutions that implement GenAI and agentic AI features to simplify, accelerate, orchestrate and troubleshoot backup administration activities.
- Evaluate the use of vendor-hosted BaaS offerings to offload infrastructure management, reduce capital expenditures (capex), and easily scale across edge, remote, and cloud environments.
- Select vendors that support cloud application infrastructure recovery services (CAIRS) to discover cloud application infrastructure components, and routinely test and orchestrate recovery of applications and data.
- Prioritize identity and access management resilience for solutions such as Microsoft Active Directory and Entra ID, and Okta.
- Evaluate the level of resilience of backup copies with the requirement to have multiple immutable copies as soon as possible in the backup process.
- Align the backup architecture with the organization's operational and regulatory recovery requirements. Distinguish backup storage targets for their use in operational recovery, long-term retention and cyber recovery purposes.
- Include applicable sovereign backup operations and data residency requirements in the vendor selection process.
- Weigh 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.
- Select 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 (RAG) and API-based data access.

Market Overview

The backup and data protection platforms (BDPP) market continues to rapidly evolve to keep pace with the demands of protecting new workloads across complex applications and data structures. Client requirements for data protection are driven by the

expectations for continued simplification and automation of backup operations, mitigating data loss to new cyberthreats and responding to new regulatory demands. 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 the following.

Platform:

- Prioritizes the centralized management and orchestration of data protection platforms.
- Increased scope of requirements delivered via backup as a service (BaaS).
- GenAI assistance and agentic 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 cyber recovery readiness and robust anomaly detection capabilities.
- Emerging capabilities to perform and expedite malware scanning of backup data and alerts to indicators 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.

Cyber recovery and detection capabilities:

- **Ransomware detection and recovery:** Most vendors have built capabilities to detect ransomware attacks by monitoring 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.
- **Isolated recovery environments and clean rooms:** Leading vendors are expanding packaged IREs and clean rooms offerings to provide improved orchestration services to facilitate routine testing, cleaning and validation, and performing recovery.
- **Data discovery:** Vendors are integrating data discovery capabilities, including the correlation of data and user identities, to automate identification of critical data and its assignment to protection policies, drive cost optimizations, and improve cyber and disaster readiness.

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 service provider

target options.

- **Sovereign data and operations offerings:** Vendors are introducing deployment options and expanding backup storage capabilities to address the demands of sovereign-based regulatory requirements.

Implementation of artificial intelligence/machine learning (AI/ML) and GenAI:

- **Use of AI/ML:** Vendors have introduced AI/ML-based algorithms into 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 to assist with backup administrative tasks and troubleshooting. Implementations include the use of chatbots, natural-language conversational chats and AI-based responses. In addition, recent innovations include AI agent access via vendor-developed Model Context Protocol (MCP) servers.
- **Accelerating use of agentic AI:** Vendors are accelerating the addition of agentic AI capabilities to automate more backup tasks. Leading vendors have introduced governed and autonomous features such as recovery planning, identification of unprotected data, step-by-step recovery guidance, failure diagnosis, and forensic investigations.
- **Protection of AI infrastructure:** Vendors are introducing specific AI workload protection extending beyond protection of persistent layers such as object storage, NoSQL and relational databases. AI data includes categories such as vector databases, feature stores, streaming systems and caching layers.

Cloud environment protection:

- **Cloud-native data protection:** Vendors in this market are expanding their coverage of additional cloud services to increase their clients' abilities to protect cloud-native data. The scope of requirements requires vendors to keep pace with the expanding scope of 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 their own, third-party or public cloud services, to back up and protect the application, test and perform failover, and recover the entire application and data environment. This includes extending protection capabilities to identify gaps in infrastructure as code (IaC) and protect application development platform offerings such as GitHub and Microsoft Azure DevOps to orchestrate infrastructure recovery.

SaaS application protection:

- **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:** Most 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. This includes orchestrated forest-level recovery of Microsoft Active Directory, following Microsoft best practices. Additional use cases extend to IAM monitoring and change log management to detect, identify and roll back changes caused by administrators as well as malicious actors.

⊕ Evaluation Criteria Definitions