Competitive Landscape: Enterprise Data Center and Cloud Backup and Recovery Market

Published 26 October 2020 - ID G00721220 - 21 min read

By Analysts Robert Preston, Chandra Mukhyala, Michael Hoeck

Initiatives: Technology Market Essentials

The data center and cloud backup and recovery market is rapidly changing under increased demand for simpler, more agile and cost-optimized solutions to protect workloads across core, cloud and edge environments. This research compares critical market strategies of selected vendors.

Additional Perspectives

- Invest Implications: Competitive Landscape: Enterprise Data Center and Cloud Backup and Recovery Market
(28 October 2020)

Overview

Key Findings

- The journey of applications and infrastructure to public and hybrid cloud is accelerating, resulting in increased demand for backup solutions that provide backup to cloud and backup of applications running in the cloud, including SaaS applications.

- Increased attacks on backup targets by ransomware are driving the need to deploy adaptive security services (anomaly detection, prevention and predictive capabilities).

- Subscription-based pricing is gaining more traction due to the need to preserve capital spend in the face of a global recession in addition to providing the benefits such as cloud-like elasticity and pay-per-use elements.

Recommendations

Technology strategic planners seeking to expand backup opportunities at backup and recovery vendors should:

- Prioritize integration with public cloud services to support backup to and from core, cloud and edge, and drive appropriate go-to-market programs by working closely with the three major public cloud vendors.

- Develop and demonstrate ransomware remediation features that help mitigate threats, preserve backup environments and show the ability to quickly restore applications to preattack state.

- Emphasize upfront and continuous cost-saving benefits compared with traditional buying because enterprises will look for cost containment measures to cope with tight IT budgets resulting from the COVID-19 pandemic.

Analysis

This document was revised on 29 October 2020. The document you are viewing is the corrected version. For more information, see the Corrections *page on gartner.com.*

Introduction

The backup and recovery software and appliance market is forecast to hit $9 billion in 2024 with a 2019 through 2024 compound annual growth rate of 1.7%. The data center backup and recovery market is changing as enterprise needs for simple, secure and cost-optimized solutions that can backup and restore from core, cloud and edge environments are increasing.

Most organizations are at various stages of adoption on the journey to the cloud. They are accelerating use of cloud architectures, applications and solutions as they modernize infrastructure, which must be properly protected. They face an increasing threat of ransomware and other cyberattacks, requiring heightened measures to ensure that their data is recoverable. They are expecting a simpler, more cost-efficient and cloudlike adoption strategy for data protection. Backup and recovery vendors must rapidly transform product features, functionality, services and licensing options to meet these challenges.

- The initial backup use case for cloud has been sending either all backups, or tiering older backups, to the cloud. New challenges are facing backup and recovery vendors to improve protection of application data as organizations spread infrastructure across core, cloud and edge. Enterprises are rapidly adopting SaaS applications; however, SaaS applications can make the underlying data inaccessible to the backup and recovery vendor as it is under the control of the SaaS vendor.

- Backup and recovery vendors must play a role in ransomware mitigation to augment the efforts of network and security technologies. The ability to provide ransomware mitigation capabilities, either while backing up or in postprocess to accelerate recovery, is now essential.

- Heightened by the economic environment, organizations are looking for new and innovative financing options to procure backup solutions. Backup and recovery vendors need to update pricing models to offer enterprises greater pricing flexibility and adapt to modern as-a-service offerings.

This research focuses on enterprise backup and recovery providers, and it describes how providers respond to the top three competitive trends in the market.

Market Definition

Gartner defines the backup and recovery market as a software- or hardware-appliance-based solution that enables an enterprise to deploy and manage backups in the core, cloud or edge. Find more details on backup and recovery definition in the Market Definition/Description section of the Magic Quadrant for Data Center Backup and Recovery Solutions.

Competitive Situation and Trends

The data center backup and recovery market is changing as enterprise needs for simpler, secure and cost-optimized solutions that can backup and restore from core, cloud and edge environments are increasing. This research provides analyses of current offerings and the benefits and challenges in each backup and recovery solution. Table 1 summarizes Gartner's analysis of the current competitive situation and trends in the enterprise backup and recovery market.

Table 1: Backup and Recovery Vendors Measuring Up Against Competitive Trends

	Acronis	*Actifio*	*Cohesity*	*Commvault*	*Dell Technol*
Cloud Backup Agentless					
Amazon Web Services (AWS)		X	X	X	X
Microsoft Azure		X	X	X	X
Google Cloud Platform (GCP)		X	X	X	
Ransomware					
Detection Real Time	X			X	

↓	*Acronis* ↓	*Actifio* ↓	*Cohesity* ↓	*Commvault* ↓	*Dell Technol*
Detection Postprocess			X		X [2]
Immutability (Primary copy)		X [1]	X	X	
Ransomware Analysis-Based Recovery			X		
Purchase Option					
Perpetual	X	X	X	X	X
Subscription	X	X	X	X	X
Backup as a Service (BaaS) (Vendor-Hosted)	X	X		X	X
Cloud SaaS Data Management			X	X	

Cloud SaaS data management: Complements hybrid backup with additional services like management, analytics

X [1] Dependent on storage target used with vendor offering.

X [2] OEM license

Source: Gartner (October 2020)

Backup to Cloud and Backup of Applications in the Cloud Are Key Selection Criteria in Modernizing Backup Environments

IT leaders selecting a new backup application are incorporating requirements to back up data to the cloud, and backup of applications and infrastructure running in the cloud. Backup to cloud comes with an implicit requirement for restoring the data either back on-premises, or more frequently restoring, in the cloud as part of a response to a DR event. Organizations further along the journey to cloud must also protect applications running in the cloud, including SaaS applications like Microsoft 365 and Salesforce, infrastructure as a service (IaaS), including virtual machines and cloud-native infrastructure and platform as a service (PaaS) like managed databases such as Amazon RDS.

Most vendors in this report support backups to at least one of the public clouds if not all three major clouds: AWS, Azure and GCP. Most vendors also support backup of simple virtual machines in the public cloud (IaaS) and have their backup application available in the public cloud marketplace. The differences are in how broad the support for the various public cloud targets is or the list of applications supported, including the integration or protection of cloud-native workloads. Another big differentiator is the use of native SaaS services to complement the hybrid backup environment with management, analytics or orchestration services.

Ransomware Targeting Backup Will Drive the Need to Deploy Additional Security Features

The potential complexity, unknown variants and growing sophistication of ransomware attacks against corporate data centers challenge the readiness of data protection solutions to recover from an attack. The number of cybercrime attacks in the past 12 to 24 months has accelerated and will continue to grow, driven by the changing agendas of attackers.

Backup and recovery vendors have different approaches when it comes to detection, protection and recovery of ransomware attacks to the backup system. Some start with real-time detection using AI technologies where others use postprocess scans on copies in a vault. For protection, vendors protect backup copies by either using WORM technologies or using immutable (primary copies) techniques to restrict access and changes from occurring. For recovery, some backup vendors notify the backup admin of an attack and use ransomware-analysis-based recovery techniques to identify the right point of recovery and clean backup data of malware.

Due to increasing number of ransomware attacks, the need to improve ransomware detection in real time and orchestrate fast recovery are forcing enterprises to rearchitect their backup infrastructure. In the wake of ransomware attacks, backup and recovery vendors have innovated or partnered with external solutions to enhance their technology to analyze ransomware's effects, mitigate impact and expedite recovery.

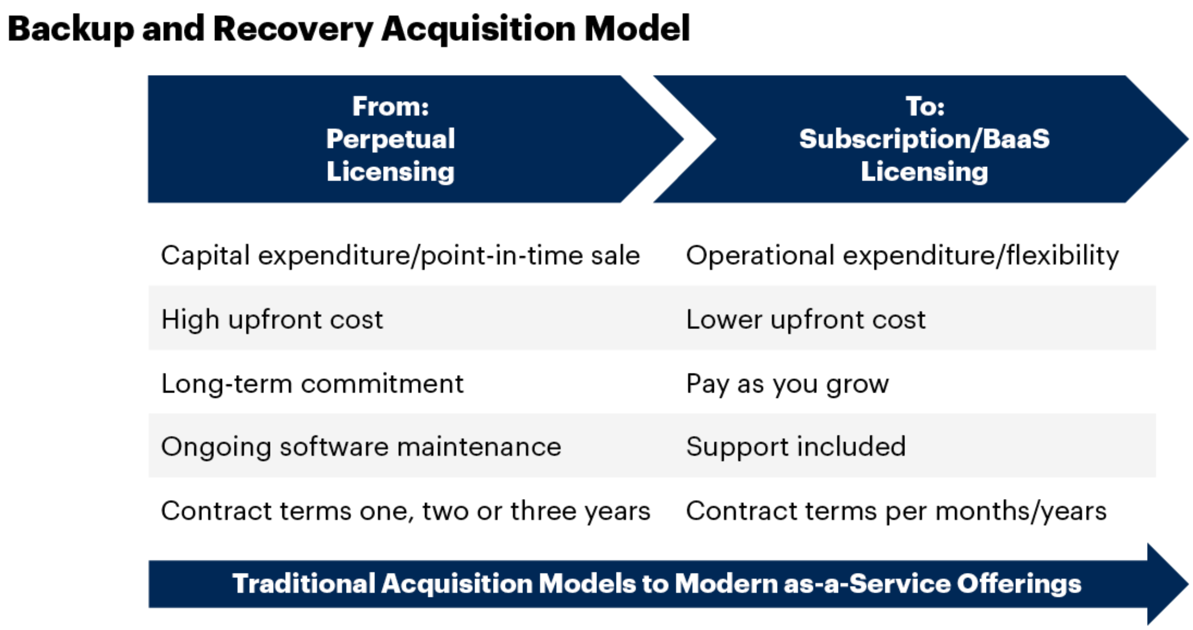
Cost-Containment Efforts Are Leading to Consumption-Based Pricing Demand

IT spending is continuing to shift toward subscription and utility models where IT services are delivered as a service and consumed. Multiple factors are driving this trend across enterprise organizations:

- The heightened awareness of global economic concerns has accelerated an already growing caution of enterprise IT capital expenditures.
- Uncertainties in business environments are challenging enterprises to predict the amount of resources needed.
- Organizations are looking for more flexibility in how they consume software to avoid the higher upfront payments of perpetual licensing.
- IT administration skills are increasingly difficult to maintain and increasingly harder to justify use of IT skills to manage commodity hardware in a hybrid cloud era.

Backup and recovery vendors are evolving their pricing strategies and expanding delivery options to enable enterprises greater flexibility to acquire data protection solutions. Most backup and recovery vendors provide subscription pricing for their solutions. As illustrated in Figure 1, subscription-based pricing can provide several benefits over traditional acquisition models. It aligns with how organizations are acquiring modern as-a-service offerings.

Figure 1: Backup and Recovery Acquisition Model



Backup and Recovery Acquisition Model

From: Perpetual Licensing	To: Subscription/BaaS Licensing
Capital expenditure/point-in-time sale	Operational expenditure/flexibility
High upfront cost	Lower upfront cost
Long-term commitment	Pay as you grow
Ongoing software maintenance	Support included
Contract terms one, two or three years	Contract terms per months/years

Traditional Acquisition Models to Modern as-a-Service Offerings

Source: Gartner
721220_C

Even though the promise of subscriptions looks good, vendors do not take the opportunity to maximize the flexibility of subscriptions and mostly still sell subscriptions as multiyear prepaid agreements eliminating the benefits of subscriptions. Additionally, the backup as a service (BaaS) market is growing and expanding the delivery options available to organizations. This provides a complete solution that can expand and contract in a consumption-based pricing model.

Traditionally provided through managed service provider offerings, backup and recovery vendors have begun launching their own BaaS.

Competitive Profiles

Acronis

Product or Portfolio Overview

Acronis is a privately held company that was founded in 2003 with dual headquarters in Schaffhausen, Switzerland, and Singapore and 30 offices in the U.S., Europe and Asia. Acronis delivers backup/recovery for on-premises and hosted data center environments, workstations and end-user devices as well as public clouds.

Acronis Cyber Backup protects cloud-based data, data center workloads, remote offices and endpoints like workstations with a single product. Acronis' backup solutions are integrated with security for the protection of backups and primary data, and Acronis agents protect against malware and offer blockchain-based service for data authenticity certification and validation.

How Acronis Competes

Acronis provides an integrated data protection and security solution that covers on-premises, cloud and edge environments. Its support for cloud workloads is limited to supporting: Microsoft 365, Google Workspace, Azure and Amazon Elastic Compute Cloud (Amazon EC2). Acronis requires an agent to be installed on each virtual machine (VM) running in Azure or AWS.

Acronis' approach to ransomware is providing an integrated backup and security in one solution. Acronis Active Protection includes AI-powered active ransomware and anti-cryptojacking protection, which constantly observes patterns in how data files are being changed on a system.

Acronis products are available for purchase as a perpetual license, subscription or a consumption model based on the backup solution.

Actifio

Product or Portfolio Overview

Actifio is a privately held company, founded in 2009 with headquarters in Waltham, Massachusetts, U.S. Actifio software comes as a virtual appliance called Actifio Sky. Actifio CDX is a preintegrated software/hardware offering on a dual-node, high availability (HA) appliance. Actifio GO is the SaaS-based offering for on-premises and cloud workloads.

How Actifio Competes

Actifio competes in the public cloud by leveraging copy data management (CDM) features, which is a core foundation of its backup and recovery solution. CDM enables direct and quick access to data from edge, core and cloud. Actifio Sky is available in the marketplace for AWS, GCP and Azure. Actifio Sky has native, agentless protection of VMs running in AWS, Azure and GCP.

Actifio ransomware strategy is in the form of easy-to-perform recoveries but lacks proactive scanning of possible attacks. Actifio provides customers with the ability to parallelize instant recovery of “multiple” point-in-time copies of VMs/physical servers/file systems/databases in an isolated network to find a safe point to restore. Clients can use Actifio workflows to instantly mount and recover daily backup, to scan the image for ransomware infections. Scans are performed by using customer malware and ransomware tools to detect ransomware infection on a daily basis.

Actifio does not sell hardware, thus acquiring a license can be perpetual or subscription-based. Actifio GO is a BaaS offering that is subscription-based and priced based on source TB protected.

Cohesity

Product or Portfolio Overview

Cohesity is a privately held company with headquarters in San Jose, California, U.S., focused on consolidation of secondary data with cloud integration. It released its first product in 2015 and has been rapidly growing in both number of customers and revenue since then.

Cohesity’s backup and recovery portfolio consists of Cohesity DataProtect. It is the all-in-one web-scale backup software to protect both traditional and modern workloads including VMs, containers, relational and distributed databases, SaaS-based applications and network-attached storage (NAS) running on-premises, in the cloud or edge. Cohesity DataProtect enables rapid recovery from disasters, including ransomware attacks, by maintaining fully hydrated immutable snapshots that can be instantly mounted at scale.

Cohesity DataPlatform is the foundational software for Cohesity and is a scale-out distributed file system that provides the underlying backup storage for Cohesity DataProtect but can also serve as a stand-alone scale-out file and object storage.

Cohesity Helios is a SaaS-based management tool combined with built-in machine learning that provides global operational insights. And it provides actionable recommendations to operate all Cohesity clusters irrespective of where they are located — on-premises, cloud or edge — through a web browser.

How Cohesity Competes

Cohesity offers both native snapshot and VM agent-based protection on the three major cloud providers, AWS, Azure and GCP. Cohesity supports Microsoft 365; however it lacks the feature to backup Microsoft Teams.

Cohesity provides machine-learning-based ransomware detection and automatic ransomware attack detection to enable action sooner, with WORM backups that even a compromised admin account can’t delete.

Cohesity leads with a subscription-based pricing model with the ability to use the software across any combination of public cloud or certified hardware appliances from OEM partnership and Cohesity. Cohesity continues to offer perpetual licenses for customers who still wish to purchase a perpetual license. Cohesity offers SaaS-based backup and data management services (ransomware and backup management, and DR orchestration as a service) in the public cloud.

Commvault

Product or Portfolio Overview

Commvault is a publicly traded data protection and information management company with its headquarters in Tinton Falls, New Jersey, U.S. Commvault's core product for backup and recovery is called Commvault Backup & Recovery and is available as a software-only offering or as part of an integrated appliance called Commvault HyperScale X. Commvault has additional related products that are not for backup and recovery but fall under the data management umbrella. Commvault provides instant DR failover and failback operations as well as copy data management for DevOps. Commvault Activate provides file storage optimization, sensitive data governance and advanced search and discovery.

How Commvault Competes

Commvault strategy is a unified multicloud approach to backup and recovery across the clouds. Commvault Backup & Recovery supports multicloud (AWS, Azure and GCP) by installing virtual server agents on every VM in the environment. Metallic, a division of Commvault, offers BaaS for on-premises and cloud workloads, including Microsoft 365, Salesforce and Google Workspace. Commvault ransomware detection and protection strategy leverage intelligent data management.

Commvault uses a combination of machine learning algorithms, air gap and honeypot mechanisms to detect ransomware attacks. The backup catalog can be backed up to Commvault-managed cloud and can be retrieved from multiple cloud locations in native format during the recovery process. Commvault also allows users to validate backup copies by performing isolated recoveries of data to a networkless VM environment for verification. Commvault allows customers to do a proper analysis before initiating a recovery after a ransomware event. Commvault can do isolated recoveries for analysis and validation using one of its core DR capabilities (backup validation). Customers can also use anomaly alerts to understand what to recover in parallel with backup validation.

Commvault licensing is based on front-end capacity, number of VMs, physical CPUs or instances being protected in either a subscription-based or traditional purchasing model. Metallic is offered in one-year increments in a cost per GB per month format.

Dell Technologies

Product or Portfolio Overview

Dell Technologies Storage & Data Protection business unit is part of the Dell Technologies Infrastructure Solutions Group. EMC was acquired by Dell in 2016, after which Dell decided to focus entirely on the EMC data protection portfolio and sold its Quest data protection portfolio.

The Dell Technologies data protection portfolio consists of three backup applications and two appliances.

Dell EMC backup applications:

- Avamar
- NetWorker
- PowerProtect Data Manager

Appliances:

- Dell EMC PowerProtect DD Series appliances (next generation of Data Domain appliances)
- Integrated Data Protection Appliance (IDPA) based on Avamar and Data Domain

How Dell Technologies Competes

The Dell Technologies cloud strategy incorporates multiple backup solutions. Some have a reliance on agents to protect cloud workloads, and some support snapshots in AWS and Azure. Its solution supports backup to the cloud directly from any of its backup applications to PowerProtect DD Virtual Edition deployed in the public cloud. On-premises appliances can also tier to AWS, Azure, GCP and Alibaba Cloud. Avamar and NetWorker are available in AWS and Azure. PowerProtect Data Manager is available in AWS.

Dell's ransomware strategy is built on Dell EMC PowerProtect Cyber Recovery, which is a separate offering in Dell's backup portfolio. The solution creates an additional copy of customer-defined critical application data to a dedicated and air-gapped infrastructure. Cybersense for PowerProtect Cyber Recovery is separately licensed to scan and detect the additional copy for anomalies.

Dell licensing for backup solutions includes both traditional perpetual and subscription-based licensing. Dell Financial Services provides several payment structures such as:

- Pay as you grow (determine payment structure based on anticipated business growth)
- Flex on demand (commit to baseline capacity, then pay for buffer capacity as you need it)
- Datacenter Utility (pay per use across IT infrastructure)

IBM

Product or Portfolio Overview

IBM is a technology conglomerate headquartered in Armonk, New York. IBM's first backup product launched in 1988 as ADSM. Rebranded in 1999 as Tivoli Storage Manager, it transitioned to IBM Spectrum Protect in 2018.

IBM's backup and recovery portfolio consists of three products:

- IBM Spectrum Protect: Proven in large-scale environments, this is the core backup and recovery solution for physical and virtual environments with native support for backup to tape and support for both on-premises and cloud-based object storage.
- IBM Spectrum Protect Plus is a modern backup solution that provides agentless backups of VMs, databases, applications, SaaS workloads, containers and cloud environments with support for data retention in WORM-compliant object storage. Spectrum Protect Plus also has integration with Spectrum Protect.
- IBM Spectrum Copy Data Management manages and orchestrates hardware snapshot copies of data providing self-service-based access to end users across on-premises and cloud environments.

How IBM Competes

IBM's Spectrum Protect portfolio supports AWS, Azure and IBM Cloud cloud providers' storage, including the various storage tiers offered, as backup targets. IBM Spectrum Protect can back up applications running as a guest inside the VM instances of all major public cloud providers, but it lacks snapshot integration in the cloud that is required for faster and efficient backups. Spectrum Protect Plus supports Microsoft 365 and agentless backups by managing Amazon EC2 snapshots.

The IBM Spectrum Protect portfolio provides ransomware detection and offers native support for tape and immutable object storage, making data resilient to ransomware attacks. A global catalog/search and native data format support enables fast data recovery.

IBM supports both perpetual licensing and subscription-based pricing. Spectrum Protect Suite is licensed per TB. Spectrum Protect Plus is licensed by virtual machine or per TB. Multiple IBM partners offer BaaS based on IBM Spectrum Protect and IBM Spectrum Protect Plus.

Rubrik

Product or Portfolio Overview

Rubrik is a privately held company founded in 2014, based in Palo Alto, California, U.S. Rubrik released its first product in 2015 and has seen significant increase in both the number of customers and revenue since then. The Rubrik Cloud Data Management (RCDM) platform is a scale-out-architecture-based data protection solution with cloud integration and native immutability against ransomware.

How Rubrik Competes

Rubrik's public cloud strategy is built on their SaaS-based offering, Polaris. This orchestrates on-premises edge and cloud deployments of Rubrik and protection of cloud and SaaS-based applications. Rubrik supports snapshots on AWS, Azure and GCP, and Microsoft 365 Exchange Online and OneDrive.

Polaris Radar provides ransomware detection and remediation. Radar monitors file system changes (file change rates, file entropy changes, abnormal system sizes, etc.) to flag for any anomalous activity. Rubrik Polaris Radar provides guidance to recover point and instant recovery.

Rubrik technology is platform-agnostic, and RCDM is offered as plug-and-play Rubrik appliances on third-party hardware or as a software instance running in the cloud, sold as a dollar per TB per year license. Rubrik Go is a subscription-based program, along with Polaris SaaS-based, that offers many flexible operational expenditure models.

Veeam

Product or Portfolio Overview

Veeam is a private software company that was acquired by Insight Partners and based in the U.S. Veeam was founded in 2006 and has become one of the largest independent data protection software companies. Over the past few years, Veeam has adopted support for more heterogeneous operating systems, enterprise applications and tape support capabilities to satisfy its growing enterprise customers' needs.

Veeam's portfolio consists of:

- Veeam Availability Suite
- Veeam Backup & Replication
- Veeam Agent for servers
- Veeam Backup & Replication for AWS
- Veeam Backup & Replication for Microsoft Azure
- Veeam ONE
- Veeam Availability Orchestrator

How Veeam Competes

Veeam supports agentless image-based backups in Amazon EC2 and Azure. Veeam does not support agentless image-based backups on GCP; however, the option of protecting VMs with agents is available. Veeam has a very comprehensive solution for Microsoft 365.

Ransomware detection is performed by Veeam ONE, which has logic in place to help detect anomalous activities on VMs. The new Veeam v10 update includes logic that alerts the user of suspicious increment sizes of backup and immutable backups using AWS S3 Object Lock.

Veeam delivers multiple pricing options for software or by leveraging a subscription model. For traditional purchases, pricing is per physical CPU being protected. Veeam's subscription model utilizes a license per protected VM that is offered as an annual or multiyear term. Veeam's NAS backup option is based on a cost per protected TB with a subscription model. Veeam offers backup and recovery as a service through MSPs to deliver BaaS using Veeam products.

Veritas Technologies

Product or Portfolio Overview

Veritas is a privately held company based in Santa Clara, California. It was founded in 1983, before being purchased by Symantec in 2004 and subsequently sold to The Carlyle Group, a global investment firm in 2016.

Veritas' backup product portfolio consists of NetBackup software, NetBackup Appliance, Flex Appliance, Backup Exec and SaaS Backup. New NetBackup 8.3 now includes NetBackup CloudPoint and Resiliency for in-cloud backup and recovery, and orchestrated mobility and disaster recovery.

The majority of Veritas' business comes from large enterprises with complex, heterogeneous and large-scale environments. NetBackup is Veritas' core backup application that powers its appliance portfolio.

How Veritas Competes

Veritas provides certified integration with all three major public clouds and private cloud, including integration with multiple storage tiers, IaaS, PaaS and SaaS. NetBackup CloudPoint provides native in-cloud protection and recovery of IaaS and PaaS across Azure, AWS and Google. Veritas SaaS Backup, delivered by a third-party SaaS backup vendor, provides hosted backup and recovery for SaaS-based workloads including Microsoft 365, Google Workspace, Microsoft Dynamics 365, Salesforce.

NetBackup has introduced immutability management support that is agnostic to immutable storage solutions (Veritas or third party). This new management capability supports first copy, duplicate and auto image replication. Veritas has comprehensive workload protection coverage and the ability to simplify recovery at scale. Veritas has multiple recovery methods: Instant Access, Continuous Data Protection, CloudPoint, Bare Metal Restore and traditional recovery to meet the various recovery requirements. NetBackup Resiliency offers automated and orchestrated recovery to streamline complex recovery scenarios. From a ransomware detection capability, Veritas offers Data Insight, which provides malware and anomaly detection before the backup environment.

Veritas supports both perpetual and subscription licensing for its backup software. Veritas NetBackup pricing is primarily based on a front-end TB-protected model. Veritas offers backup and recovery as a service through its partner network using NetBackup.

References and Methodology

This research is based on numerous inquiries with clients as well as discussion with technology vendors.

It is based on the detailed vendor survey for the Magic Quadrant for Data Center Backup and Recovery Solutions.

Recommended by the Authors

Market Share Analysis: Data Center Backup and Recovery Software, Worldwide, 2019

Forecast: External Storage Systems, Worldwide, All Countries, 2017-2024, 3Q20 Update

Market Share: External Storage Systems, All Regions, 2Q20 Update

Market Share Analysis: External Controller-Based Disk Storage, Worldwide, 2019

Recommended For You

Forecast: Data Centers, Worldwide, 2017-2024, 2020 Update

Market Share Analysis: Data Center Backup and Recovery Software, Worldwide, 2019

Market Trends: Who Sells Servers for Hyperscale Data Centers?

Forecast Analysis: Data Center Workload Accelerators, Worldwide

Market Trends: Evolving Enterprise Data Requirements — How Much Is Not Enough?

Supporting Initiatives

Technology Market Essentials

Track

as statements of fact. While the information contained in this publication has been obtained from sources

believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."