

Enrico Signoretti, Arjan Timmerman
Jun 14, 2021

GigaOm Radar for Hybrid Cloud Data Protection for the Enterprise v1.0

Hybrid Cloud Data Protection

GigaOm Radar for Hybrid Cloud Data Protection for the Enterprise

Table of Contents

- 1 Summary
- 2 Market Categories and Deployment Types
- 3 Key Criteria Comparison
- 4 GigaOm Radar
- 5 Vendor Insights
- 6 Analyst's Take
- 7 About Enrico Signoretti
- 8 About Arjan Timmerman
- 9 About GigaOm
- 10 Copyright

1. Summary

Data is among the most important assets of any enterprise today, and keeping that data safe is paramount. This is especially the case with the transition to the cloud, which is radically changing where data is created and consumed, and this transformation, combined with evolving business and regulatory needs, makes data protection services vital for the enterprise.

In the enterprise, moving data to the cloud using SaaS applications and re-platforming, re-factoring and rehosting on-premises applications to hybrid cloud platforms is difficult enough. Making sure the data generated stays protected is even more challenging.

With the disruption in the data protection industry brought on by innovative startups, and the well-established vendors rethinking their strategy to bridge the gap between legacy and modern solutions, hybrid cloud infrastructures have become the go-to environment, and the data protection market is moving fast to cover that area.

The enterprise market is trending toward additional services built on top of data protection, and these services are becoming instrumental in collecting and consolidating data across the entire organization (no matter where it is created or stored), with the goal of reusing it for other purposes. In most cases, the enhancements are still about improving and expanding data protection processes, as is the case of protection against ransomware. Still, areas like security, compliance, data governance, and management are getting a lot of attention as well.

When the COVID-19 pandemic struck, most of the workforce ended up working from home, and organizations needed to restructure to protect data created by users in disparate locations. For data protection suppliers, this means endpoints need to be included in the portfolio as well. This is also the case for the growing edge market, where data collected by sensors and devices at the edge also needs protection.

Today, the modern workplace generally involves a combination of SaaS applications and virtual desktops, whether on-premises or in the cloud, with increasing demand for NAS (file) protection in both environments. Along with this scenario, enterprises are building hybrid cloud infrastructures and need solutions that can support their data-driven initiatives adequately. Furthermore, a growing number of enterprises are taking advantage of Kubernetes to redo their business applications, and protecting these assets is becoming crucial. This is why the market is so active, with both startups and incumbents looking at ways to disrupt traditional backup models, as well as increase the value of the protected data by adding data management and data reuse capabilities to their solutions.

HOW TO READ THIS REPORT

This GigaOm report is one of a series of documents that helps IT organizations assess competing solutions in the context of well-defined features and criteria. For a fuller understanding consider reviewing the following reports:

Key Criteria report: A detailed market sector analysis that assesses the impact that key product features and criteria have on top-line solution characteristics—such as scalability, performance, and TCO—that drive purchase decisions.

GigaOm Radar report: A forward-looking analysis that plots the relative value and progression of vendor solutions along multiple axes based on strategy and execution. The Radar report includes a breakdown of each vendor's offering in the sector.

Solution Profile: An in-depth vendor analysis that builds on the framework developed in the Key Criteria and Radar reports to assess a company's engagement within a technology sector. This analysis includes forward-looking guidance around both strategy and product.

2. Market Categories and Deployment Types

For a better understanding of the market and vendor positioning, we categorized solutions for hybrid cloud data protection by the target market segment (small-medium, large enterprise, internet service provider/managed service provider (ISP/MSP), and highly specialized), along with their predominant deployment models: on-premises, cloud-hosted, and as a service, as shown in **Table 1**. The goal is to give the reader a broader perspective and context regarding the different solutions available in the market and how they can fit with his/her organization and business needs:

Market Segments

- **Large enterprise solutions:** These solutions can cover a majority of enterprise user needs with diverse and distributed infrastructures. They are sometimes less efficient than the others, but the feature set is extensive and has multiple deployment options, vast scalability, and support for legacy systems and applications.
- **ISP/MSP:** In this category, we find solutions that have features specifically designed for service providers. The backup infrastructure is not managed by the end user, which is usually subscribed to a service.
- **Specialized:** These types of solutions have particular feature sets that make it difficult to position them in traditional enterprise-size market segments. Sometimes they can be considered niche players, but usually, they offer innovative approaches and solutions to several challenges posed by modern infrastructure and application development cycles.

Deployment Models

- **On-premises:** Deployed as software-defined or appliances, these solutions focus on on-premises infrastructures but can also provide support for SaaS applications and VM instances in the cloud, as well as other public cloud services. A primary backup repository is on-premises but usually can extend to different clouds.
- **Cloud-hosted:** These are similar to on-premises solutions, but installed in the public cloud. The user retains full control of the infrastructure; the licensing model conforms to public cloud standards (subscription-based); and the primary goal is to protect cloud resources and SaaS applications.
- **SaaS:** Based on a cloud backend and usually provided as-a-service, these solutions work in a manner contrary to that of the products in the on-prem category. Backup data is stored in the cloud, and the backup service is also delivered on-premises through agents or specialized proxies. This type of solution is usually optimized more for cloud instances, cloud services, and mobile/edge use cases.

Table 1. Vendor Positioning

	MARKET SEGMENT			DEPLOYMENT MODEL		
	Enterprises	ISP/MSP	Specialized	On-Premises	Cloud-Hosted	SaaS
Acronis	++	++	+	+++	++	+++
Arcserve	++	++	—	+++	+	—
Bacula	+++	++	++	+++	++	—
Clumio	+	—	+++	—	—	+++
Cohesity	+++	+++	++	+++	+++	+++
Commvault	+++	+++	++	+++	+++	+++
Dell Technologies	+++	++	++	+++	++	+++
Druva	+++	++	+++	—	—	+++
IBM	+++	++	+	++	++	+++
Rubrik	+++	+++	++	+++	++	++
Veeam	+++	+++	++	+++	+++	—
Veritas	+++	+++	+	+++	++	+++
Zerto	+++	+++	++	+++	+++	+

+++ Exceptional: Outstanding focus and execution

++ Capable: Good but with room for improvement

+ Limited: Lacking in execution and use cases

— Not applicable or absent

Source: GigaOm 2021

3. Key Criteria Comparison

Following the general indications introduced with the Key Criteria for Evaluating Hybrid Cloud Data Protection Report, **Table 2** quickly summarizes how each vendor included in this research performs in the areas we consider differentiating and critical for modern data protection. The objective is to give the reader a snapshot of the technical capabilities of various solutions and define the perimeter of the market landscape. **Table 3** then compares the vendors in terms of the evaluation metrics relevant in this sector.

Table 2. Key Criteria Comparison

	KEY CRITERIA					
	Analytics	Disaster Recovery Orchestration	Security	Data Mgt and Governance	Kubernetes Support	Breadth of Solution
Acronis	++	+++	+++	++	—	+++
Arcserve	—	++	++	+	—	+
Bacula	++	++	+++	++	+++	++
Clumio	+	+	+	—	—	+
Cohesity	+++	+++	+++	+++	++	+++
Commvault	+++	+++	+++	+++	+++	+++
Dell Technologies	++	+++	++	+++	++	+++
Druva	+++	++	+++	++	+	++
IBM	+++	+++	+++	++	++	+++
Rubrik	+++	+++	+++	++	—	++
Veeam	++	+++	+++	+	+++	+++
Veritas	+++	+++	+++	++	+	++
Zerto	++	+++	+++	+	+++	++

+++ Exceptional: Outstanding focus and execution
 ++ Capable: Good but with room for improvement
 + Limited: Lacking in execution and use cases
 — Not applicable or absent

Source: GigaOm 2021

Table 3. Evaluation Metrics Comparison

	EVALUATION METRICS					
	Architecture	Scalability	Flexibility	Efficiency	Manageability & Ease of Use	Ecosystem
Acronis	++	++	+++	++	+++	++
Arcserve	++	++	++	++	++	++
Bacula	++	+++	++	+++	++	+
Clumio	+++	++	+	+++	+++	+
Cohesity	+++	+++	+++	+++	+++	+++
Commvault	+++	+++	+++	+++	+++	+++
Dell Technologies	++	+++	++	++	++	+++
Druva	++	+++	++	+++	+++	++
IBM	++	+++	+	++	++	++
Rubrik	+++	++	++	++	+++	+++
Veeam	+++	++	+++	+++	+++	+++
Veritas	++	+++	++	++	++	++
Zerto	+++	++	++	+++	+++	++

+++ Exceptional: Outstanding focus and execution

++ Capable: Good but with room for improvement

+ Limited: Lacking in execution and use cases

- Not applicable or absent

Source: GigaOm 2021

By combining the information provided in the tables above, the reader can develop a clear understanding of the technical solutions available in the market.

4. GigaOm Radar

This report synthesizes the analysis of key criteria and their impact on evaluation metrics to inform the GigaOm Radar graphic in **Figure 1**. The resulting chart is a forward-looking perspective on all the vendors in this report, based on their products' technical capabilities and feature sets.

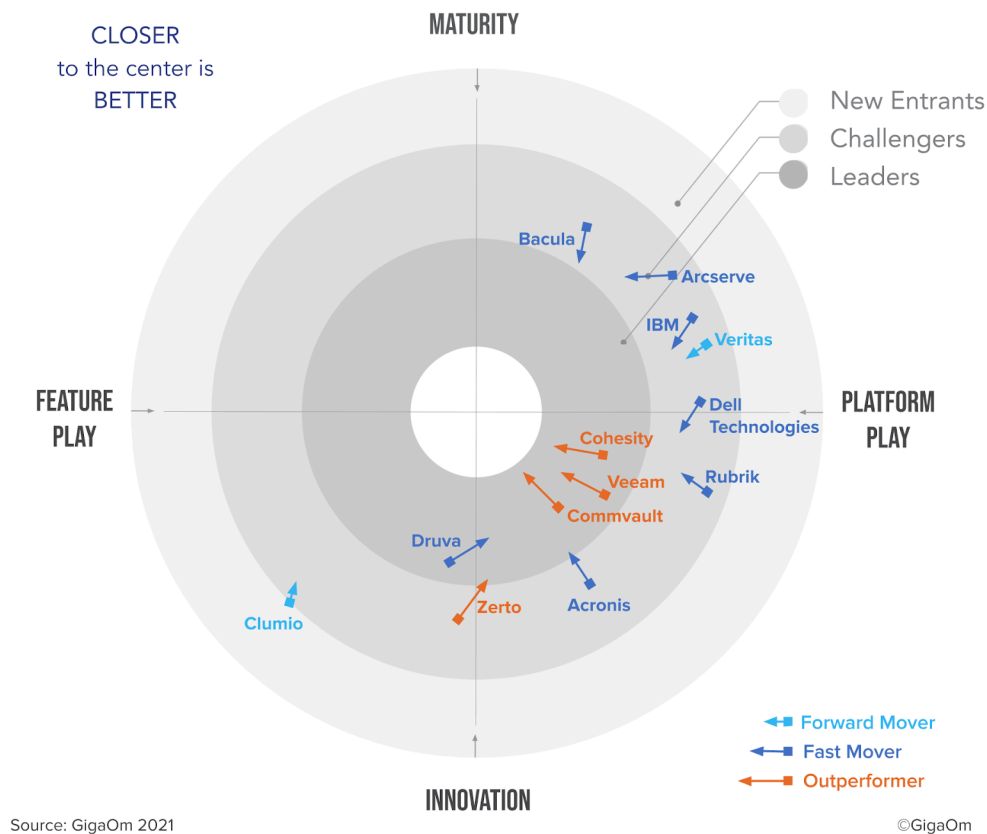


Figure 1: GigaOm Radar for Hybrid Cloud Data Protection (Enterprise)

The Innovation and Platform Play quadrant of the Radar chart features three frontrunners in the form of Cohesity, Commvault, and Veeam, which are clearly well placed in the high-end market with regard to overall strategy and capacity to execute on it. Their solutions do overlap to some extent, and they show different levels of integrations, with product portfolios and feature sets going in different directions lately.

Rubrik is an innovative and interesting solution, but lacks some of the advanced data management features enterprises want nowadays.

Veritas and Dell are still market leaders in enterprise data protection, but cloud and data management capabilities remain limited, though with an interesting roadmap ahead. IBM's situation is similar. Its solution has been split into two products, one for legacy environments and the other designed to

serve virtualized and hybrid infrastructures. To cover all key criteria discussed in this report, customers unfortunately need two products at this time. The companies are working hard to integrate the tools, but this is still an ongoing process, in which Veritas integrated its SaaS, IaaS and traditional solution into NetBackup.

Acronis is a strong challenger in the enterprise, especially because of its broad and integrated features set and its SaaS offering. It also has a compelling solution for ISPs, as do Veeam and Zerto, which is very commonly used to build DRaaS, and now backup, for its customers. Zerto has an innovative approach to data protection, starting with continuous data protection with replication and journaling for disaster recovery, which is now the foundation for its backup and mobility capabilities. However, Zerto is still missing data management functionality.

ArcServe and StorageCraft together are building a product line based on proven technology, including a series of point solutions for the SME market and distributed enterprises. ArcServe is now in the process of integrating them to create a complete end-to-end solution, enabling users to choose either simple and cost-effective products or a comprehensive data protection environment.

Druva and Clumio are part of the next wave of data protection solutions for hybrid cloud environments. Both of them are SaaS offerings, with Druva—a Leader in this report—ahead in maturity and the number of use cases at the moment. Easy to adopt and manage without needing an on-prem infrastructure, they are compelling solutions for cloud-first strategies and organizations looking to migrate as much as possible to the cloud.

Bacula is very capable of protecting large environments. Open source and free to use (although most enterprises will buy the Enterprise license), it provides a very broad set of services that are in high demand. Because Bacula is an open platform, enterprises with a good developer base and Linux knowledge could leverage this and build on top of an already well-designed data protection tool to suit their particular needs. However, the solution's lack of SaaS protection and GDPR compliance functionality will impede the company's ability to grow its customer base in the enterprise segment.

INSIDE THE GIGAOM RADAR

The GigaOm Radar weighs each vendor's execution, roadmap, and ability to innovate to plot solutions along two axes, each set as opposing pairs. On the Y axis, **Maturity** recognizes solution stability, strength of ecosystem, and a conservative stance, while **Innovation** highlights technical innovation and a more aggressive approach. On the X axis, **Feature Play** connotes a narrow focus on niche or cutting-edge functionality, while **Platform Play** displays a broader platform focus and commitment to a comprehensive feature set.

The closer to center a solution sits, the better its execution and value, with top performers occupying the inner Leaders circle. The centermost circle is almost always empty, reserved for highly mature and consolidated markets that lack space for further innovation.

The GigaOm Radar offers a forward-looking assessment, plotting the current and projected position of each solution over a 12- to 18-month window. Arrows indicate travel based on strategy and pace of innovation, with vendors designated as Forward Movers, Fast Movers, or Outperformers based on their rate of progression.

Note that the Radar excludes vendor market share as a metric. The focus is on forward-looking analysis that emphasizes the value of innovation and differentiation over incumbent market position.

5. Vendor Insights

Acronis

Acronis is a solid data protection company with a clear strategy and product portfolio. It focuses primarily on enabling MSPs (and the IT channel in general) to effectively target small and medium-sized enterprises, but has an ambitious roadmap and products that are quickly becoming more appealing to larger organizations. Its solutions for service providers are well designed and easy to deploy.

Acronis's solution covers a broad range of systems: cloud compute instances, edge infrastructures, and SaaS applications. It can be deployed on-premises, in the cloud, or consumed as a SaaS application directly or through partners.

Acronis' biggest strength is the very strong focus on cybersecurity, which is often lacking in other data protection solutions. Acronis leverages an AI-driven engine that analyzes data in real time, detects anomalies, and is even able to determine if data is being encrypted. These features are complemented by anti-malware scanning and vulnerability assessment capabilities.

Acronis' excellent cybersecurity protection capabilities, along with other data governance and management features, such as data analytics and blockchain-based file notarization, expand the range of use cases and are helpful for customers with pressing compliance requirements, such as the General Data Protection Regulation (GDPR). Acronis is also expanding its cloud presence and adding more SaaS data protection capabilities.

With its strong focus on cybersecurity, other much needed capabilities have lagged, leaving Acronis behind the competition in terms of features such as Kubernetes support. This is a concern in the enterprise market, where Kubernetes is being used more and more and enterprises often want a single solution to protect their valuable data.

Strengths: Acronis has a strong focus on cybersecurity that really helps enterprises keep their data safe. With safe recovery, fail-safe patching, and malware scans in the Acronis cloud, the company provides security at a level that is unique.

Challenges: Acronis focuses heavily on cybersecurity, possibly to the detriment of data management. Those capabilities are nascent; there is potential but they need to be developed into a coherent set of features.

Arcserve

With over 30 years in the field, Arcserve is well known in the data protection world. Its Unified Data Protection (UDP) offers multiple deployment options, with proven and effective capabilities needed by

enterprises to protect their valuable data resources.

ArcServe and StorageCraft recently announced they will join forces. It is expected that ArcServe will continue to focus on the small to medium enterprise while shifting gradually toward the upper mid-market and enterprise segments. Eventually StorageCraft will be fully integrated into the Arcserve portfolio and provide data protection for a range of business environments.

Arcserve UDP offers fast and reliable backup and recovery options, with Instant Virtual Machine (IVM) and Virtual Standby (VSB). IVM uses data reconstituted in real time from the data backup repository to create a VM, while VSB enables a fully formed image to be built as a warm standby in whatever environment the customer chooses.

The UDP software is delivered as an on-premises solution, managed through an on-premises console. There is also a cloud-based backup solution, called Arcserve Cloud Hybrid, which is delivered as a service and has the same look and feel as the on-premises console.

Arcserve partners with security vendor Sophos to build a solution that integrates UDP with Sophos Intercept X Advanced for Server to offer protection against ransomware. This advanced security protection with UDP is now provided for both the cloud hybrid and the on-premises appliance-based solution. Since March 2021, any Arcserve UDP software-only deployment acquired under the Arcserve Universal License offers this integration as well.

Arcserve UDP integrates with AWS S3 buckets and uses its Object Lock facility to deliver a cloud-based immutable storage repository. The merger with StorageCraft also provides an immutable storage repository for on-premise backup operations.

Strengths: Arcserve offers a mature solution with robust and flexible deployment options. Hybrid cloud support capabilities are good, and the partnership with Sophos enables malware and ransomware protection.

Challenges: The lack of integration between solutions may create unnecessary complexity, and the absence of protection for Kubernetes environments, which are increasingly prevalent in enterprises, is concerning.

Bacula

With its unique architecture and modular design, Bacula is scalable from a single node system to systems consisting of thousands of nodes. Bacula is made up of six major components and services: Director, Console, File, Storage, Catalogue and Monitor. This modularity provides flexibility and allows users to build in security.

Bacula's robust backup and recovery software is designed for companies with a good knowledge of Linux that deal with a lot of data and varied applications and data types. Bacula fits especially well in

organizations concerned with HPC and big data that require high levels of security.

Bacula offers agentless backup and recovery for all the major hypervisors, with its Instant Recovery and Single File Restore features that provide fast and flexible data recovery in mission-critical situations. Bacula's catalog database and flexible restore approaches enable users to customize and tune for special use cases and they integrate well with third-party software.

Bacula provides services for many protection needs in enterprise environments, such as virtual environments, databases, containers, and endpoints, as well as protection for Microsoft and Linux, and strong Kubernetes support. All of these are needed in the enterprise environments and provide the customer a good tool for protecting their resources.

Although Bacula has a lot to offer, it requires a good understanding of Linux and is therefore not the best fit for companies that rely on Microsoft technology. Bacula needs to work on GDPR and data management and analytics capabilities, and while backup of SaaS-based solutions is now included in the Bacula offering with Microsoft 365 support, other SaaS-based solutions like Salesforce are not supported at this moment.

Strengths: Bacula is a very capable solution. Companies with Linux expertise can utilize it to its fullest. Because it is open source, they can start using the free software and only buy support if needed.

Challenges: Bacula's reliance on Linux makes it less suitable for Microsoft-based companies. Its lack of support for GDPR and support for only a SaaS solution like Microsoft 365 are challenges in modern hybrid environments.

Clumio

Clumio is a SaaS-based solution that does not require managing or deploying any AWS resources to start using it. Clumio is a consumption-based service with infinite scale built in; users can start small and then scale to protect massive amounts of data without having to do any planning or management. It is all seamlessly handled by the platform. The onboarding process is so simple that users can start protecting their AWS assets in 15 minutes or less.

Clumio enables fast backup by automating the entire process through global policies that work across different AWS assets and accounts. Using massive serverless compute in parallel to run backup jobs as well as doing incremental backups results in reducing the backup window significantly. Clumio enables quick recovery to ensure business continuity, too. It provides a quick and simple way to find the data (snapshots, instances, files, records, and so forth) that needs to be recovered and then restores it. By enabling rapid and granular recovery of data, Clumio reduces recovery times significantly.

The Clumio platform is designed with a security-first mindset. Backups are saved to a Clumio service that is independent and separated from the user's AWS account. This provides true air-gap

functionality and protection against ransomware and other attacks. Backups are immutable and in order to safeguard against bad actors, there is no delete option. Moreover, all data processing and storage is handled with end-to-end encryption. The platform is also compliant with the latest security certifications and standards, such as ISO, HIPAA, PCI, SOC 2, and others.

Clumio focuses heavily on AWS, and while support for VMware Cloud on AWS exists, there are no disaster recovery options for it, which is a concern as this is key for many enterprises. Clumio's strong bond with the AWS ecosystem makes the solution best suited for organizations with a cloud-first approach in which Amazon Web Services is the preferred cloud provider. At this time, the solution is suitable primarily for customers in the North American market.

Strengths: Clumio is specifically designed for cloud-native applications and workloads in, for now limited, hybrid cloud infrastructures. It is an easy-to-use SaaS application, and the company plans to build a data protection/data management platform.

Challenges: The notable lack of disaster recovery capabilities as well as Kubernetes support is a concern in the enterprise segment. As a cloud-first company, support for public cloud vendors other than AWS is lacking. The current focus on the North American market limits broader adoption.

Cohesity

The Cohesity multi-cloud data management platform was created in the cloud era using hyperscaler principles. It lets customers spin up data protection, data management, disaster recovery, and much more, whether on-premises or SaaS, through the same unified experience.

Cohesity's primary focus is on the enterprise segment—organizations with masses of data and strong data management requirements. That does not mean the solution's excellent capabilities would not be very compelling to SMBs as well, but in the past, the company's physical appliance deployment model was a financial barrier for adoption by that segment. This barrier has been removed by Cohesity as it now provides software-only versions of its solutions, for both on-premises and the cloud (SaaS).

The SaaS version is easy to use and offers granular policy control combined with configurable data retention options and tiers. Cohesity's pace of innovation should lead to substantial leveling up in terms of parity of features between the SaaS and customer-managed software versions of its solution.

Cohesity DataProtect is a software-defined backup and recovery solution that offers flexible deployment options: on-premises, in the public cloud managed by the customer, or as a service (BaaS) that Cohesity manages. It allows enterprise customers to protect both traditional and modern data sources on a single platform, all managed through a global user interface.

The Helios multi-cloud platform addresses the challenge of mass data fragmentation. Enterprise customers can protect a wide range of applications using NFS, SMB, and S3 protocols. Support for

sequential and random IO ensures that the data can be protected and made available for other business use cases, such as accelerating application development (copy data management), running analytics, or meeting compliance regulations, without making unnecessary data copies.

Cohesity has a strong vision and the capacity to execute, and it offers innovative solutions and features that enable customers to protect and consolidate data on a single platform. It also allows customers to improve infrastructure efficiency, data management, and data governance processes. The SaaS based version of DataProtect Service now makes Cohesity appealing to organizations of all sizes, especially from a pricing and consumption perspective.

Strengths: Cohesity is a very competitive and well-rounded offering that is able to provide data protection and management as a service, on-premises, or in the cloud.

Challenges: Although almost every box is ticked, a solid Kubernetes solution is still in the works, so that might keep large enterprises already invested in that area from using Cohesity.

Commvault

Commvault is one of the few data protection companies whose solution is capable of managing and protecting a broad ecosystem of workloads across physical servers, VMs, the cloud, containers, SaaS, and more. This reduces complexity for customers by combining all recovery SLAs in one solution and managing these complex environments through a single interface. The options to buy Commvault products include software, appliances, and SaaS.

The range of options to protect customer environments makes Commvault well suited to all market segments, especially to larger enterprises with complex environments where a unified solution that simplifies the complexity is highly valued. Commvault's ability to solve complex data management challenges extends beyond backup and includes capabilities to further protect customer data.

These capabilities include data protection across on-prem and hybrid/multi-cloud environments, including backup and disaster recovery; data security with protection and recovery from security threats, including data breaches and ransomware; data compliance and governance to conform to privacy regulations such as GDPR and CCPA; data transformation to shift and repurpose data across environments including virtual, physical, cloud, Kubernetes, and SaaS; data insights, including the use of data patterns and machine learning, to drive operational efficiency.

Commvault includes management, protection, and support for containers, and it stores, protects, and migrates Kubernetes apps in all locations on hybrid multi-cloud environments. Commvault auto-discovers and protects Kubernetes applications and containers, simplifying data protection for any IT generalist or DevOps professional who needs to work in a containerized workspace. Commvault was an early adopter of the Container Storage Interface (CSI), which enables the application-consistent protection of both persistent Kubernetes data and other data in the application landscape. That protection of data is a key differentiator for Commvault.

Commvault backup software Metallic BaaS and the software-defined Commvault Distributed Storage both integrate natively with Kubernetes through CSI. This support across traditional enterprise workloads and storage infrastructures stores, protects, replicates, and migrates persistent data and containers across hybrid multi-cloud environments. With hybrid cloud-native software-defined storage and complete data protection, Commvault delivers the most comprehensive and flexible container solution portfolio.

Strengths: Commvault is a well-known, well-respected solution provider with a broad portfolio of services that includes almost all aspects of data protection, and that is why they are one of the three frontrunners in this Radar report.

Challenges: Although Commvault covers most of the data protection an enterprise might need, an even tighter integration between products and better options in the SaaS offering would be useful and are on the roadmap.

Dell Technologies

Dell Technologies Data Protection solutions are applicable to organizations of any size or industry. PowerProtect DD series appliances scale from 4TB to 1.5PB of usable capacity. For customers working in a hybrid cloud environment, Dell Technologies offers on-premises data protection as well as protection in all major cloud providers. Dell EMC PowerProtect Data Manager will be of interest to enterprises building a modern data infrastructure that includes cloud-native and container (Kubernetes) applications.

PowerProtect Data Manager enables the protection of traditional workloads, including Oracle, Exchange, SQL, SAP HANA, and file systems, as well as Kubernetes containers and virtual environments. It allows customers to discover, protect, and restore production workloads in Kubernetes environments, and protects production and dev/test workloads to ensure the data is easy to back up and restore.

Dell EMC PowerProtect Cyber Recovery Solution protects customers' data and infrastructure with a secure on-premises vault, and with an operational air gap and multiple layers of physical and logical security. PowerProtect Cyber Recovery offers compliance-level, hardware-based immutability and NTP tamper protection, and includes CyberSense for identifying threats and enabling assured recovery.

Dell EMC PowerProtect Backup Service is a cloud data protection solution designed to deliver SaaS-based protection without increasing IT complexity, while ensuring predictable, controllable costs. This solution uses Druva Technology through a partnership that Dell Technologies and Druva announced. This provides Druva services for Dell Technologies PowerProtect Backup Service customers.

Enterprises can use PowerProtect Data Manager to protect Kubernetes in AWS, Azure, and Google Cloud; to protect Kubernetes clusters in multi-cloud environments; and to protect EKS, AKS and GKE. PowerProtect Data Manager builds on top of the open-source Velero to provide a data protection

solution that enables application-consistent backups and restores and that is always available for Kubernetes workloads, VMware hybrid cloud environments, and Tanzu modern applications.

Strengths: The Dell Technologies products have been protecting enterprise environments for a very long time now. With a good set of upgrades and the addition of new features from the Druva partnership, these products enable enterprises to protect a great many assets.

Challenges: Like most longtime data protection providers, Dell Technologies offers its services in a solution that has been around for decades. Integrating all products into a single solution is still ongoing and adds complexity. Data management is basic and needs more options.

Druva

Druva is a SaaS data protection solution that helps enterprises protect and manage backup data across data center, cloud, and endpoint workloads. This solution is built on AWS, making the Druva Cloud Platform extremely scalable and always available to meet the business needs of enterprise customers.

Enterprise data sources these days are spread across a variety of systems and services, such as endpoints, physical and virtual servers, SaaS applications like Microsoft 365 and Salesforce, and cloud infrastructure (IaaS/PaaS). Protecting data in all of these sources typically requires multiple vendor solutions, resulting in backup data silos, administrative complexity, and increased costs.

The Druva Cloud Platform changes all that by providing cloud data protection and management across endpoints, data centers, and cloud workloads. Druva Cloud Platform's architecture provides the centralized management and consolidated view of data that enterprises need to improve cyber-resiliency, streamline governance, and gain critical data insights to uncover opportunities and expedite decision making.

Druva's global deduplication works across all backup data (so far except for Salesforce data or AWS native workloads) regardless of location, ensuring servers, cloud applications, and end-user devices all benefit from efficient bandwidth utilization while also minimizing the amount of data that needs to be transferred. Data stored in the Druva cloud is deduplicated in both warm and cold storage tiers, driving additional storage and cost efficiencies for long-term retention.

Multiple layers of security ensure that backup data stays protected, in flight and at rest, and includes data encryption in flight to customer-specific access keys. Druva maintains multiple security certifications, including FedRAMP ATO, SOC-2 Type II, FIPS, and HIPAA. Comprehensive audits performed by AWS at the infrastructure layer provide additional security and assurance.

With AWS data centers around the globe providing very high data availability, Druva Cloud Platform enables compliance with regional data residency requirements as well as workload mobility.

Strengths: A well-designed platform with innovative features, Druva produces a quick ROI and a good overall TCO, with strong data management capabilities, ease of use, and a SaaS deployment model. Ideally suited for organizations with a cloud-first approach to the AWS ecosystem. Druva also provides great eDiscovery and compliance features.

Challenges: The solution isn't ideal for large customers with an on-premises strategy but Druva offers software appliances that customers must deploy to meet strict RPOs and RTOs. Druva provides backup of on-premises + Azure + GCP workloads to the Druva Cloud (on AWS), but Druva does not offer native backup services in other cloud environments like GCP or Azure.

IBM

IBM has two solutions for data protection: IBM Spectrum Protect, which is aimed at legacy environments and fits best in the SMB market, and Spectrum Protect Plus, which has a more modern architecture, and is therefore more focused on virtualized and next-generation infrastructures. The Spectrum Protect Plus offering is best suited for the enterprise market because it offers good data protection coverage for on-premises and cloud workloads through a unified and easy-to-use management console.

The IBM Spectrum Protect offerings provide multiple deployment options including a cloud-based solution that is available on most of the major public cloud marketplaces. Spectrum Protect Plus is able to protect the most common workloads as well as cloud workloads on AWS, Azure, and IBM Cloud. SaaS application support is currently limited to Microsoft 365.

This platform offers basic data management capabilities and a decent set of disaster recovery capabilities both on-premises and in the cloud. Companies can opt to recover to a second data center, a cloud environment, or via additional recovery options.

IBM Spectrum Protect Plus supports Kubernetes with integrated support for containers through OpenShift APIs for Data Protection (OADP). The solution offers a number of capabilities, including CSI snapshots for persistent data, the ability to create simple SLAs, and the ability to manage the protection of container data and to add Kubernetes labels and namespaces awareness. It also protects data (PVCs) and metadata, including cluster resources, containerized SPP servers, and more.

Strengths: IBM solutions are robust and mature. Spectrum Protect Plus is a good choice for IBM customers migrating from legacy to modern infrastructures.

Challenges: IBM added some basic data management features to its data protection products, but there is no clear path for extending protection of SaaS applications beyond Microsoft 365, which limits the effective reach of its data protection portfolio in cloud environments.

Rubrik

Rubrik is one of the newer data protection companies that are introducing fresh approaches to data protection. Its product portfolio is quickly evolving to cover an increasing number of applications and workloads, with a flexible architecture that enables users to design hybrid cloud infrastructures efficiently. Rubrik provides protection for on-premises, cloud, and SaaS offerings and is scalable to meet the needs of enterprise environments. The product is easy to use and provides its customers a well-balanced and very usable protection tool.

Enterprises can run Rubrik through appliances on-premises, as software on qualified hardware, or as software in the cloud. With Rubrik, you can search for a backup and then select the right point in time to recover from for near-zero RTOs/minimal business interruption/near-instant recovery.

Rubrik stores all data in an immutable format that prevents ransomware from accessing backed-up data. Additional security measures include multi-factor user authentication, zero-trust cluster design, and retention lock support. With Rubrik's Radar, data is proactively analyzed and flagged when any unusual activity occurs.

Rubrik provides its customers an easy-to-use data protection tool with a centralized management UI that allows the expansion of the infrastructure across on-premises and cloud environments. It is flexible, with a modern approach to data protection and a growing number of features for data governance and basic data management.

In comparison with its direct competitors, Rubrik is still a bit lacking in data management and data governance, although the Polaris SaaS product is updated regularly. The suite of data governance and management features is still limited, and even though the ecosystem is quite large, the tools for in-depth data analysis are lacking compared to the competition.

Strengths: The ease of use of the Rubrik tooling as well as its integration with the cloud and applications provides a flexible and scalable platform that helps enterprises protect their data.

Challenges: Although Rubrik has a great solution, its development seems slow compared with its main competitors. Some features, especially on the data management side, are still missing, as is support for Kubernetes environments.

Veeam

Veeam has a mature product line for data protection of on-premises infrastructures and has expanded its reach to cloud and SaaS applications.

The company had most of its success with small and medium enterprises and remains a leader in that space, while adoption of its products also has hugely increased in large enterprises. Veeam has been

able to do very well with service providers, thanks to spot-on products, licensing, and services.

The Veeam platform protects a very broad spectrum of workloads, has a robust, flexible, and scalable architecture, and allows organizations to use a wide range of backup targets and tiers. The company has built a strong and reliable partner ecosystem, which translates into several strategic partnerships with major storage vendors. This enables deeper data protection integrations and simplifies backup and recovery operations. And with the Kasten acquisition, Veeam has one of the best Kubernetes data protection products currently available and is working on fully integrating it into the Veeam product line.

Veeam Disaster Recovery Orchestrator offers thorough and varied options, catering to the most complex DR use cases, and analytics capabilities are provided through Veeam ONE. MSP capabilities are best-in-class, and their partner-delivered solution ensures worldwide professional coverage.

SaaS application coverage currently includes only Microsoft 365. Veeam includes some proactive malware/ransomware detection capabilities that exist in the product, and it allows data immutability to be enabled. This immutability parameter is then cascaded across its scale-out backup repository, on both the capacity and archival tiers, where Amazon S3 immutability capabilities are used. Veeam also has the v11 Hardened Linux Repository to support immutability without requiring S3 Object Lock.

Although Veeam has one of the most complete platforms for enterprises, its lack of data management capabilities is a key area that needs improvement. Another aspect that must be considered relates to data protection consumption. Backup as a Service (BaaS) is on the rise. Many organizations see value in this new delivery model and Veeam may need to make a decision as to whether this is a growth area worth exploring. Because of Veeam's distribution model, BaaS offerings currently are delivered through partnering MSPs.

Strengths: Veeam's strength comes from simplicity, efficiency, and the ability to build solutions that strike the right balance between features and usability. Its community of partners and satisfied users is vast, making it very easy to find certified professionals in every region of the world.

Challenges: More data protection vendors are offering turnkey SaaS-based data protection solutions. Veeam does not have such an offering without using a service provider, and this may become a challenge in the future as more organizations look at simplifying their data protection architecture and experience.

Veritas

Veritas has comprehensive data protection solutions for the enterprise market that cover many platforms and applications. Although the solution is good, cloud and Kubernetes support is limited at the moment. However, the company is investing heavily in these solutions, through integration of Trilio, for example. The company has been in business for over 30 years now, modernized its user interface a couple years ago with NetBackup version 8.1, and continues to provide a better, simpler user experience.

Veritas provides three essential layers of cyber resiliency: Protect, Detect and Recover. NetBackup protects all data—edge, core, and cloud—from a centralized platform. It writes and stores that data in a secure and encrypted manner and can write it to immutable storage. NetBackup Resiliency provides simple execution of recovery at scale, and easy-to-use tools to ensure recovery success.

Beginning with NetBackup version 9, Veritas added a number of improvements to make managing complex hybrid cloud environments easier. With the addition of better RBAC capabilities, customers now have an easier way to delegate ownership, visibility, and control over specific cloud tenants. In addition, admins can assign specific actions to take for each role created to further granularize the permissions a single user has with regard to the backup and recovery of cloud-based assets.

The Veritas portfolio includes NetBackup SaaS Protection, with options for Microsoft 365, Slack, Dropbox, and more, but some essential SaaS options are still lacking, such as Salesforce and Google Cloud Workspace. For enterprises, it is important to have these SaaS offerings built into the product because they are being used more and more in this market segment.

Strengths: Veritas is a widely deployed solution in the enterprise market with a rock-solid and mature architecture that supports traditional backup operations, and a promising roadmap.

Challenges: Data management and data governance still need attention, and Veritas has limited native cloud protection for AWS, Azure, and GCP. Kubernetes support is another challenge for enterprises looking for a data protection solution.

Zerto

Zerto is an interesting solution with well-designed and efficient DR and backup features that are ideal for the enterprise market. It is rapidly evolving from a feature-oriented solution toward a platform-oriented approach with central management capabilities.

The solution is granular and flexible, setting the standard in terms of advanced DR capabilities. Its robust disaster recovery orchestration offers ample workload recovery options, including different target on-premises and cloud platforms.

Service providers will find a good technology partner in Zerto. It allows them to build efficient data protection and DRaaS solutions for their customers, no matter what type of virtualized infrastructure stack is in place, and at a reasonable cost.

From a security perspective, Zerto offers data-at-rest encryption and immutable storage capabilities for long-term retention copies. For infection and ransomware protection, Zerto relies on its journaling architecture and point-in-time backups to restore an environment to a time before the infection happened.

Finally, Zerto is stepping into the world of SaaS workload protection through a partnership with

Keepit. This solution covers popular SaaS applications such as Microsoft Office 365, Salesforce, GSuite, and Microsoft Dynamics.

The solution has a lot of potential in hybrid and multi-cloud environments, with many use cases still to explore, including data and application migrations, dev/test, and more. Zerto's consistent focus on expanding its solution moves the company gradually toward a platform-oriented approach.

The SaaS protection partnership with Keepit is a good tactical move, but customers will expect better integration—a 100% consistent experience—within a single management pane. Data management capabilities are still non-existent and remain an area needing improvement.

Strengths: Zerto really understands the way companies rely on their IT resources and data. Its solution builds on years of experience and provides very solid and flexible data protection to enterprise customers.

Challenges: Many features have just been released and the integration is not optimal. This needs to be addressed in future releases so enterprise customers can use all functionality to its full potential.

6. Analyst's Take

We're living in challenging times, and they're challenging for enterprises as well. With a workforce that may be working both from home and from the office, data protection is becoming both more necessary and more demanding. As the pandemic hopefully nears its end, other changes in the way people create and work with data will occur, along with changes in how data needs to be protected.

With digital transformation impacting enterprises heavily, perhaps even more so due to the COVID pandemic, SaaS applications are a focus area for enterprise vendors. Most vendors already have some capabilities in this area, with Microsoft 365 being the common denominator. SaaS applications will continue to grow even in the post-COVID world, and data protection vendors will need to add more popular solutions.

Another area of focus will be the protection of Kubernetes platforms, as more and more enterprises rebuild their applications onto these platforms and need a suitable data protection solution. Most of the solutions offer some sort of protection for Kubernetes, but most still don't cover all of the platforms an enterprise might use.

The fast-growing edge environment will need to be protected as well. Some data protection providers have invested in this area already, while others have not yet, but all will need to do so soon. When enterprises use IoT, edge, AI, and ML to expand their data intake, data protection becomes even more crucial.

But that data protection involves a broad spectrum of possibilities. We are still living in a hybrid world, and enterprise environments range from mainly on-premises to those that are using the cloud almost completely. This means that data protection solutions should not only be able to provide services across the entire spectrum, but also to keep evolving when new technologies emerge.

In this Radar, we see a mixture of companies, some operating at the cutting edge and developing as quickly as possible to provide the right services to emerging markets, and others relying on their proven technology to expand more gradually as demand increases. For enterprises, this means there are many great choices, and the challenge lies in figuring out which ones best fit their needs.

7 About Enrico Signoretti



Enrico has more than 25 years in technical product strategy and management roles. He has advised mid-market and large enterprises across numerous industries, and worked with a range of software companies from small ISVs to global providers.

Enrico is an internationally renowned expert on data storage—and a visionary, author, blogger, and speaker on the topic. He has tracked the evolution of the storage industry for years, as a Gigaom Research Analyst, an independent analyst, and as a contributor to the Register.

8 About Arjan Timmerman



Arjan Timmerman is an independent industry analyst and consultant with a focus on helping enterprises on their road to the cloud (multi/hybrid and on-prem), data management, storage, data protection, network, and security. Arjan has over 23 years of experience in the IT industry and worked for organizations across various verticals such as the Shared Service Center for the Dutch Government, ASML, NXP, Euroclear, and the European Patent Office to just name a few.

Growing up as an engineer and utilizing that knowledge, Arjan currently provides both technical and business architectural insight and management advice by creating High-Level and Low-Level Architecture advice and documentation. As a blogger and analyst at TECHunplugged.io blog, Gestalt IT, Amazic World, and other outlets, Arjan is also from time to time participating in podcasts, discussion panels, webinars, and videos. Starting at Storage Field Day 1 Arjan is a long-time Tech Field Day Alumni, former NLVMUG leader, and active member of multiple communities such as Tech Field Day and vExpert.

Arjan is a tech geek and even more important he loves to spend time with his wife Willy, his daughters Rhodé and Loïs and his son Thomas sharing precious memories on this amazing planet.

9. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

10. Copyright

© [Knowingly, Inc.](#) 2021 "*GigaOm Radar for Hybrid Cloud Data Protection for the Enterprise*" is a trademark of [Knowingly, Inc.](#). For permission to reproduce this report, please contact sales@gigaom.com.