The Forrester Wave™: Data Resiliency Solutions, Q3 2019

The 10 Providers That Matter Most And How They Stack Up

by Naveen Chhabra
September 12, 2019

Why Read This Report

In our 40-criterion evaluation of data resiliency solution vendors, we identified the 10 most significant ones — Actifio, Cohesity, Commvault, Dell EMC, Druva, IBM, Micro Focus, Rubrik, Veeam, and Veritas — and researched, analyzed, and scored them. This report shows how each provider measures up and helps infrastructure and operations (I&O) professionals select the right one for their needs.

Key Takeaways

Commvault, Rubrik, Cohesity, And Veeam Lead The Pack

Forrester's research uncovered a market in which Commvault, Rubrik, Cohesity, and Veeam are Leaders; Veritas, Druva, and Actifio are Strong Performers; IBM and Micro Focus are Contenders; and Dell EMC is a Challenger.

Policy Management, Recoverability, And Security Are Key Differentiators

As firms embrace hybrid environments, I&O pros need improved capabilities like single-pane-of-glass management across all data sources, a comprehensive policy framework, recoverability, and security. Vendors that can provide these capabilities natively fare better.

The Forrester Wave™: Data Resiliency Solutions, Q3 2019

The 10 Providers That Matter Most And How They Stack Up

by Naveen Chhabra
with Glenn O'Donnell, Matthew Flug, and Bill Nagel

September 12, 2019

Table Of Contents

2 Data Resiliency Solutions Go Beyond Data Protection And Recovery

3 Evaluation Summary

5 Vendor Offerings

6 Vendor Profiles

Leaders

Strong Performers

Contenders

Challengers

11 Evaluation Overview

Vendor Inclusion Criteria

13 Supplemental Material

Related Research Documents

Design For Dependability By Embracing A Future Of Trusted Technology

The Forrester Wave™: Disaster-Recovery-As-A-Service Providers, Q2 2019

Six Important Considerations That Affect Backup Data Location

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Data Resiliency Solutions Go Beyond Data Protection And Recovery

Fast-paced digital transformation has technology and business leaders scrambling to become competent in multiple domains and is forcing I&O leaders to bolster their data resiliency practices. Privacy regulations like GDPR and CCPA stipulate how firms can process, store, and use data. Ransomware attacks have increased in frequency, intensity, and impact. Agile application development and new platforms like containers make data protection an afterthought. Multicloud environments, edge computing, and containers distribute data closer to business applications; this scattering of data requires I&O to take a fresh approach to data resiliency. Vendors are approaching this problem in several ways, including developing new capabilities for existing on-premises data protection, delivering data protection in a software-as-a-service (SaaS) model, creating appliances that can double as recovery targets, and running test workloads. As a result of these trends, data resiliency solution customers should look for providers that:

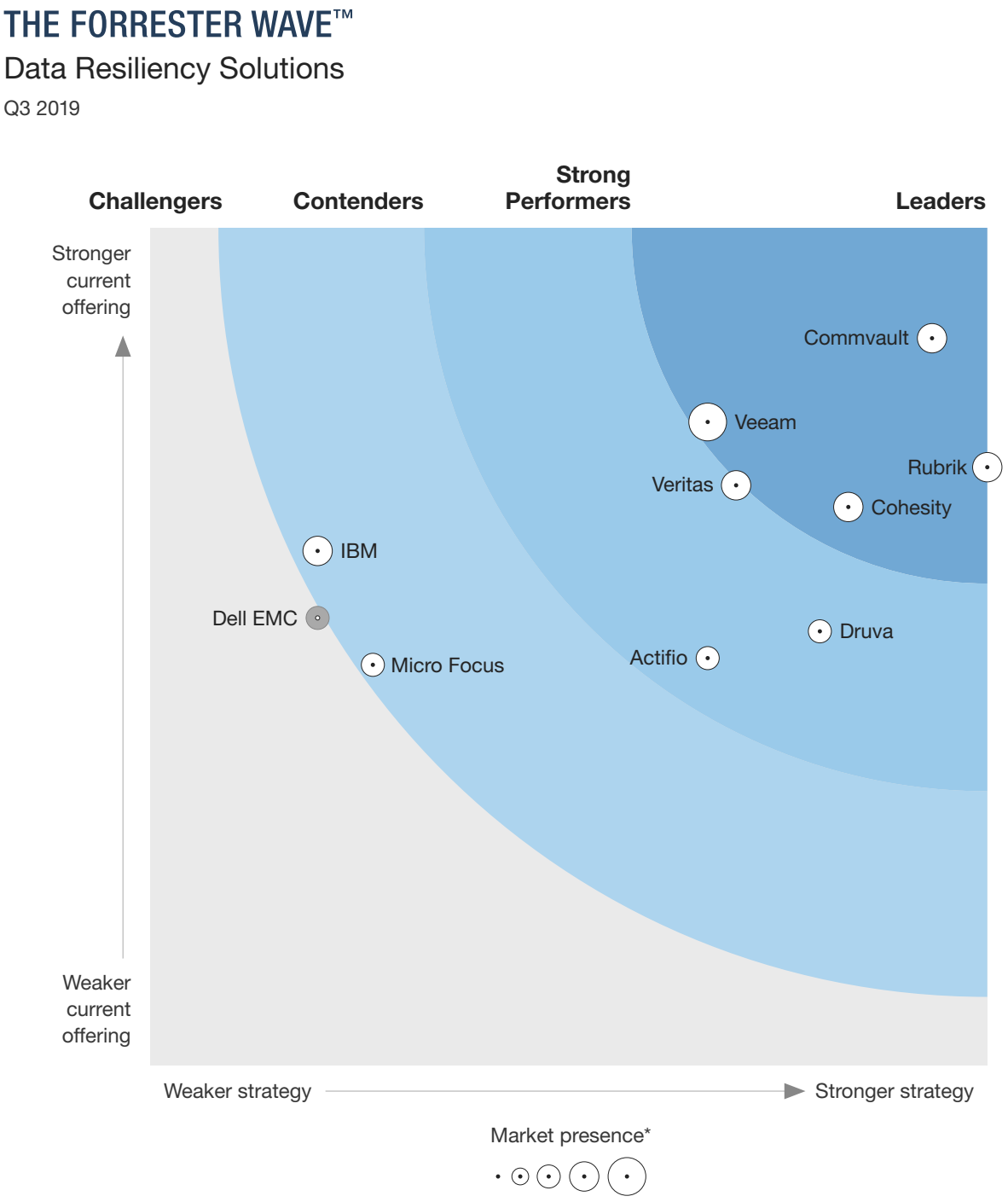
- **Drive policy-based execution.** Firms today distribute their business applications — and, by extension, their data — across multiple on-premises data centers, at managed data centers, and in the public cloud via infrastructure-as-a-service (IaaS) and SaaS. Their storage targets are in private data centers, in public cloud storage, on tape, and in service provider environments. Managing a plethora of data sources and targets while trying to fulfill service-level agreements (SLAs) is a major challenge. It's not practical for firms to operate the backup infrastructure using individual jobs that govern everything — so I&O leaders need a comprehensive, policy-driven framework to manage the entire infrastructure landscape.
- **Assure recoverability.** As I&O pros protect huge volumes of data across a variety of workloads, they place the protected data where it makes sense from economic, security, and SLA standpoints. The ultimate objective is to be able to recover when needed. Companies' business requirements do not permit any downtime — and business stakeholders don't want you working on a trial-and-error basis during a crisis.[1] Vendors must view recoverability as a key tenet and apply different techniques to ensure recoverability to give both business and I&O leaders confidence in their business operations. I&O pros must aim to generate visibility into what is recoverable and what is not in the moment of need.[2]
- **Secure backup infrastructure and data.** Security is everyone's business, and it has to be viewed from different perspectives. While it's important to protect primary business data, it's also pertinent for I&O leaders to protect all copies of this data as well as the data protection infrastructure itself. Ransomware aims to besiege or crash the backup infrastructure while taking control of primary applications and data, such that organizations under attack lose the ability to fall back to their last line of defense: backups.

Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market and does not represent the entire vendor landscape.

We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt criteria weightings using the Excel-based vendor comparison tool (see Figure 1 and see Figure 2). Click the link at the beginning of this report on Forrester.com to download the tool.

FIGURE 1 Forrester Wave™: Data Resiliency Solutions, Q3 2019



*A gray bubble indicates a nonparticipating vendor.

FIGURE 2 Forrester Wave™: Data Resiliency Solutions Scorecard, Q3 2019

	Forrester's weighting	Actifio	Cohesity	Commvault	Dell EMC*	Druva	IBM	Micro Focus	Rubrik	Veeam	Veritas
Current offering	50%	2.43	3.33	4.34	2.67	2.59	3.11	2.39	3.57	3.84	3.46
Data sources	14%	1.88	3.25	4.75	3.00	1.88	2.63	1.88	3.25	2.13	3.00
Backup targets	14%	3.00	3.00	4.00	3.00	4.00	4.00	4.00	3.00	5.00	4.00
Backup optimizations	14%	3.80	3.20	4.60	2.00	2.40	3.80	2.00	4.60	3.40	3.80
Manageability	14%	3.33	2.83	4.00	1.67	2.83	2.33	2.83	3.17	3.33	2.17
Recoverability	14%	1.00	3.00	3.00	1.00	1.00	1.00	0.00	3.00	5.00	1.00
Security	14%	1.00	5.00	5.00	3.00	5.00	3.00	3.00	5.00	5.00	5.00
Scalability	14%	3.00	3.00	5.00	5.00	1.00	5.00	3.00	3.00	3.00	5.00
Strategy	50%	3.33	4.17	4.67	1.00	4.00	1.00	1.33	5.00	3.33	3.50
Product strategy	50%	3.67	4.33	4.33	1.00	5.00	1.00	1.67	5.00	3.67	3.00
Corporate strategy	50%	3.00	4.00	5.00	1.00	3.00	1.00	1.00	5.00	3.00	4.00
Market presence	0%	3.00	3.33	4.00	2.75	2.25	3.08	2.83	3.50	4.83	4.00
Installed base	25%	3.00	3.00	5.00	4.00	2.00	4.00	3.00	3.00	5.00	5.00
Customer feedback	25%	2.33	4.33	3.00	1.67	3.00	3.00	2.33	3.00	4.33	3.67
Partnership	25%	3.00	2.33	4.33	2.33	1.00	2.33	3.00	4.33	5.00	3.00
Professional services and consulting	25%	3.67	3.67	3.67	3.00	3.00	3.00	3.00	3.67	5.00	4.33

All scores are based on a scale of 0 (weak) to 5 (strong).
*Indicates a nonparticipating vendor.

Vendor Offerings

Forrester included 10 vendors in this assessment: Actifio, Cohesity, Commvault, Dell EMC, Druva, IBM, Micro Focus, Rubrik, Veeam, and Veritas (see Figure 3).

FIGURE 3 Evaluated Vendors And Product Information

Vendor	Product name	Product version
Actifio	Actifio Sky (perpetual-license product), Actifio Go (SaaS offering)	v9.0
Cohesity	DataProtect	V6.3.0
Commvault	Commvault Complete Backup & Recovery Software	v. 11, SP 16
Dell EMC	Networker, Avamar	Networker 9.2 Avamar 19.1
Druva	Phoenix, CloudRanger	N/A (delivered as SaaS)
IBM	SpectrumProtect, SpectrumProtect Plus	IBM Spectrum Protect 8.1.7, IBM Spectrum Protect Plus 10.1.3
Micro Focus	Data Protector	v10.40
Rubrik	Rubrik Cloud Data Management	v 5.0
Veeam	Veeam Backup & Replicaton	Suite v9.5 U4 Office 365 v3
Veritas	NetBackup, CloudPoint	NetBackup 8.1.2 CloudPoint 2.2

Vendor Profiles

Our analysis uncovered the following strengths and weaknesses of individual vendors.

Leaders

› **Commvault suits companies that plan to consolidate their backup and recovery tools.** Commvault is redesigning its solution and offerings for enterprises' data resiliency needs. It also offers its solution in a subscription model so its clients can turn to opex and gain commercial advantage. Commvault's appliance-based solution delivers on customer demand for quick time-to-market. The solution helps clients not only consume cloud services as an archive data target, but also enables them to adopt public cloud by protecting cloud-based data sources. It offers the most comprehensive support for widely deployed infrastructure platforms and applications both in the data center and in public cloud services.

Commvault has added a capability to aid ransomware detection. It enables firms to embrace the cloud and modernize data resiliency operations. Its solution offers a "recovery readiness" dashboard to help customers perform what-if simulations that help identify the virtual machines (VMs) or applications that are likely to fulfill the business's recovery expectations. Solution interfaces are split in two: The first one is the web interface that administrators use to manage the virtual infrastructure and new workloads like containers, public cloud services, and SaaS. The second is a thick Java UI, for the rest of the infrastructure and for admins to operate the workflow engine. Commvault's solution does not provide any inputs on the effectiveness or efficiency of the governing policies.

- **Rubrik suits firms aiming to simplify, modernize, and consolidate data resiliency.** Rubrik is making large R&D investments to meet its goal to increase innovation and radically simplify backup and recovery needs. It has acquired strong engineering talent to gain fresh, out-of-the-box thinking to solve longstanding backup and recovery problems. Rubrik's simple, intuitive, and powerful policy engine governs data protection tasks irrespective of source type, location, or target. On-premises virtual infrastructure, database instances, network-attached storage, and public clouds can be sources. Rubrik's Polaris is a unified system of record across all Rubrik on-premises and public cloud deployments. It enables multiple data management applications including multi-cloud control, security, governance, and third-party SaaS protection. Rubrik's acquisition of Datos IO enables its customers to protect data for several NoSQL databases.

  Rubrik added a ransomware detection capability by tracking file attributes like overall change rate, file size, and entropy changes.[3] A single policy engine makes data protection simpler than with legacy solutions using a "backup job" paradigm. The solution's components and design allow it to search the entire data repository at a blazing fast speed and access the desired data much quicker. Rubrik customers speak highly of its solution, although they're looking forward to deeper and better platform support. Rubrik has yet to support distributed file systems. The tool offers simple policy management but does not report on policy effectiveness. Rubrik has yet to integrate the policy management and reporting functions of Datos IO (now called Mosaic) into its solution. It will enable a consolidated operating and reporting platform for all supported platforms.

- **Cohesity addresses data sprawl challenges and helps firms leverage secondary data.** Cohesity has taken the mass data fragmentation challenge head-on; its value propositions include its consolidated secondary data management platform. The platform includes a marketplace portal where Cohesity publishes certified apps that clients can run on its infrastructure. Possible application use cases include compliance checks or analytics on otherwise dormant data. As a recent market entrant, Cohesity had the opportunity to use the latest technologies, like a NoSQL database to store operational metadata. This metadata holds the index and enables quick search regardless of the data's physical location. The immutable file system offers the potential to protect backup instances from ransomware attack. Cohesity's solution detects anomalous behavior by analyzing file usage patterns; this increases the odds of successful detection but can also raise false alarms. Admins can perform a mass restore once they have identified a clean copy of the data.

Cohesity's solution has a web interface that is easy to navigate and use and which admins can use to perform all tasks. Its policy management engine is comprehensive yet easy to use. The solution does not evaluate the effectiveness or efficiency of policies. With its acquisition of Imanis Data, Cohesity now offers data protection capabilities for distributed file systems and NoSQL workloads. While the current solution has a dashboard for each managed cluster, Cohesity plans to integrate the Imanis Data solution such that policy management and operations will have a single interface. Reference customers highlighted superior support and solution scalability.

› **Veeam serves complex, heterogenous environments — not just virtual ones.** Firms of all sizes use Veeam Backup & Replication; service providers use it to deliver backup-as-a-service. Veeam has deep integrations for virtual infrastructure and support for heterogenous data center infrastructure. It has invested in tech partnerships with data center infrastructure vendors to support heterogeneous data center infrastructure and has joint go-to-market partnerships with vendors like Cisco, HPE, Lenovo, Nutanix, NetApp, and Pure Storage. Veeam offers enterprises a unique capability that invokes vulnerability scanning tools during recovery to ensure that all recovering systems comply with additional security policies enforced after the backup was taken. Scanners can automatically remediate known vulnerabilities in the recovering VMs to improve the overall security posture of the VMs being recovered.

In addition to supporting virtual infrastructure, Veeam recently forged tech partnerships with storage vendors like NetApp and Pure Storage to support storage replication. It does not support distributed file systems or unstructured databases. Its support for SaaS services is limited to Office 365, although it offers a lot of flexibility around data location. Veeam clients are very satisfied with the quality of its support. Challenging the common belief that it is only for virtual infrastructure, Veeam now serves some of the most complex, distributed, and large-scale client deployments. These clients also want proactive recommendations based on current SLA achievements that can help improve their backup operations to meet or exceed the SLAs. Veeam can analyze logs to identify deployment issues, compare them to a list of known issues, and proactively suggest actions like configuration changes.

Strong Performers

› **Veritas serves firms with heterogeneous data across on-premises and public cloud.** Veritas offers NetBackup as its lead solution for data resiliency; modules like CloudPoint complement its capabilities with support for public-cloud-native services. Veritas continues to support clients that have legacy and traditional systems. The combination of NetBackup and CloudPoint broadly supports on- and off-premises workloads. Serving both traditional and newer workloads isn't easy, and that's evident in that solution modules independently address client requirements. They don't integrate very well; each module has its own policy management, administration, and operational interfaces and its own reporting. Veritas's acquisition of APTARE will ease central

and comprehensive reporting. As the solution does not manage on-premises and cloud sources collectively through a single policy framework, it can neither offer recommendations for data placement decisions nor determine whether protection policies are efficient and effective.

The Veritas solution comprehensively covers heterogeneity in an enterprise technology environment from a perspective of infrastructure, applications, and cloud resources. Its support of SaaS also remains thin. It augments backup infrastructure security by providing write-once, read-many storage via its appliance. It is a good fit for firms that have heterogeneous technologies and manage different silos of data protection operations.

- **Druva's SaaS delivers immense value and quick time-to-market.** Druva stands firm with its unique position of delivering data resiliency as a service. It attracted series G funding of $130 million in June 2019 and is investing in improving its offering and increasing its go-to-market and technology partnerships. Druva recently acquired CloudRanger and CloudLanes to complement its homegrown InSync and Phoenix offerings. The Phoenix service supports data center infrastructure and applications; the CloudRanger service offers data protection for public-cloud-native workloads. Druva has been awarded a patent for its deduplication technology, which reduces total storage requirements. Its easy-to-understand solution offers comprehensive reporting. However, the products from these recent acquisitions have yet to merge completely.

  Druva offers decent coverage for virtualized infrastructure, public cloud hosted services, and SaaS applications like Office 365. It supports on-premises physical servers and databases like MS SQL and Oracle but lacks support for distributed file systems or NoSQL databases. Druva customers speak highly of its transparent subscription services business model; the reference customers we spoke with expect the firm to improve the quality of its support. Druva is a good fit for organizations that want to augment existing data protection solutions that do not cover cloud deployments.

- **Actifio serves DevOps and copy data management along with data protection needs.** Actifio software is available in two forms: virtual appliance Actifio Sky and SaaS offering Actifio GO. The Actifio GO service supports tiering protected data into public cloud storage like Amazon Web Services (AWS) S3, Google Cloud Storage, and IBM Cloud Storage. Actifio GO supports backup for data residing in SaaS services like Office 365 and GSuite. It OEMs parts of its solution to vendors like IBM and Dell EMC. Actifio pioneered copy data management and continues to lead the marketplace with that focus. It has deep integrations with databases and virtual infrastructure and can keep backups in their respective native formats even while placing the data on object storage. This enables the solution to deliver its services at significantly higher speeds than its competitors.

  Actifio is well placed to deliver data services in form of backup, recovery, and data access with a focus on databases. It supports tiering data to the public cloud. Its road map includes adding support for cloud-native workloads. The visual depiction of all policy components in its policy engine makes it extremely easy to understand, interpret, and operate. Its strength lies in delivering data services for database instances; however, it has yet to add support for unstructured databases and distributed file systems. Actifio clients that we spoke with said that they expect better support quality.

Contenders

› **IBM suits mixed environments needing single-vendor support.** IBM's solution has two main components: Spectrum Protect and Spectrum Protect Plus. Spectrum Protect protects legacy infrastructure including physical systems and several different storage systems; it can also archive data to tape. It caters to complex deployments, especially supporting legacy infrastructure. Spectrum Protect Plus is for all virtualized infrastructure. As the two products focus on different infrastructure, each has its own control plane; capabilities like dashboard, inventory management, reporting, and policy and job management are split between the two tools, which also have different administrative experiences. IBM has forged go-to-market partnerships with vendors like AvePoint, Catalogic, Cristie Software, Repostor, and Storware that deliver specialized capabilities. It has also developed technological integrations with a few of these partners.

IBM has yet to add native support of public-cloud-native infrastructure or SaaS applications. Spectrum Protect can perform GPFS file system backup using the native mmbackup utility. The primary control framework for data protection operations in Spectrum Protect is job-oriented. IBM Spectrum Protect Plus has workflow management and REST APIs to automate recoverability testing. IBM's solution does not offer recommendations to improve backup infrastructure operations. Spectrum Protect can analyze attributes of protected data sources such as the amount of data processed and the deduplication ratio. Once it has identified these changes, Spectrum Protect can present the changes on its console, generate alerts, and notify IT operations. Customer references say that IBM must rationalize the licensing for its offerings.

› **Micro Focus fits firms needing to protect legacy or proprietary infrastructure.** Micro Focus goes to market with Data Protector; it has forged go-to-market partnerships with technology vendors like HPE and an OEM relationship with H3C that complement each other's offerings and strategy. Micro Focus has radically simplified Data Protector licensing. It supports many proprietary or legacy infrastructures; this induces customers to stick with Data Protector. MicroFocus boasts several managed service providers as key clients; it has a significant route to market via systems integrators and service providers like Wipro and DXC. Micro Focus has invested in enhancing its orchestration tool by developing the Data Protector content pack, which enables managed service providers to define process workflows and deliver backup-as-a-service powered by Data Protector. Its job management framework allows administrators to specify granular priority levels that can automatically resolve backup job conflicts during runtime.

Data Protector lacks deep support for some newer deployment infrastructures like public cloud, virtual infrastructure, SaaS, and unstructured databases. Reference customers report that they use Data Protector to support their legacy infrastructure. These clients noted that they expect Micro Focus to improve its overall support quality and understanding of overall customer requirements.

Challengers

› **Dell EMC's solution works well when organizations buy its full tech stack.** Networker and Avamar are Dell EMC's key tools for data protection. Dell EMC recently unveiled the Power Protect X400 appliance, powered by software that the firm developed from scratch; however, we did not evaluate it, as it's still in its nascent stages.[4] Dell EMC's approach to recovering from ransomware is to create an operational "air gap" between the production environment and the protected zone. In today's technology environment, where ransomware tends to lie dormant in the IT setup for months at a stretch, the air gap methodology is not very effective; it only works when ransomware infection and detection occur within two consecutive backup events.[5] Dell EMC offers Cloud Snapshot Manager as SaaS; it protects cloud workloads and databases native to AWS.

The overall Dell EMC solution has several modules in addition to Networker and Avamar; each has its own operational and administrative interface. This limits its ability to offer a unified experience to enterprise clients that need to consolidate data protection operations regardless of the data source location and type. The current solution creates policy islands in each operating module. Efficient search and timely recovery may become an issue for a company that centralizes data protection operations. The Dell EMC solution is a fit for organizations that want a specialized a backup and recovery use case for each application or deployment type and that don't see the need for consolidated operations. Dell EMC declined to participate in the Forrester Wave evaluation process.

Evaluation Overview

We evaluated vendors against 40 criteria, which we grouped into three high-level categories:

› **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering. Key criteria for these solutions include support of diverse and heterogeneous data sources, backup targets, backup optimization capabilities, manageability of the backup infrastructure, recoverability, security of the backup infrastructure, and scalability.

› **Strategy.** Placement on the horizontal axis indicates the strength of a vendor's strategy. We evaluated vendors' unique value, approach, and the vision that drives investments. We evaluated how the vendor takes its products to market and how it invests in product R&D.

› **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's installed base, technology and go-to-market partnerships, professional services and consulting capabilities, and customer feedback.

Vendor Inclusion Criteria

Forrester included 10 vendors in the assessment: Actifio, Cohesity, Commvault, Dell EMC, Druva, IBM, Micro Focus, Rubrik, Veeam, and Veritas. Each of these vendors has:

- **A software offering for data resiliency.** The solution is delivered as standalone software, as an appliance, or as SaaS. If a vendor offers both software and an appliance, we only assessed its software capabilities.
- **Support for heterogeneous data center platforms.** The solution supports backup and recovery of all major versions of Windows; Linux distributions like Red Hat Enterprise Linux, SUSE, and Ubuntu running on hypervisors from VMware and Microsoft. Support for Unix flavors like HP UX, AIX, and Solaris is optional. Support for cloud-native workloads like those residing in AWS EC2 and Microsoft Azure is optional.
- **Support for major enterprise databases and applications.** The solution offers native backup and recovery of enterprise databases like Oracle and SQL and business applications like those from EPIC, Microsoft, IBM, Oracle, and SAP. It natively supports writing to disk and supports writing to hyperscale public cloud storage targets.
- **Software available with a perpetual license.** The solution is available for purchase on a perpetual license (deployable on-premises or as an appliance) or available as a SaaS subscription from the vendor itself.
- **Many clients with petabyte-scale data sets under protection.** The vendor must have more than 100 current customers with more than 1 petabyte (PB) each of backup data under management and at least one customer with more than 10 PB of backup data under management. It must also have provided 10 active instances for which it protects at least 1 PB on heterogeneous platforms and data sources.
- **Significant revenue from data resiliency solutions.** In the past two years, the vendor has garnered more than $30 million in annual revenue from its data resiliency solutions serving enterprise data center requirements — not end user devices.
- **Presence in at least two geographic regions.** The vendor markets its data resiliency solution in at least two of the following three regions: the Americas, Europe, and Asia Pacific.
- **Significant interest from Forrester clients.** The vendor solution generates significant interest in Forrester clients and a significant number of inquiries for the product or solution.

Supplemental Material

Online Resource

We publish all of our Forrester Wave scores and weightings in an Excel file that provides detailed product evaluations and customizable rankings; download this tool by clicking the link at the beginning of this report on Forrester.com. We intend these scores and default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs.

The Forrester Wave Methodology

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester follows The Forrester Wave™ Methodology Guide to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos/briefings, and customer reference surveys/interviews. We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that compares each vendor against the others in the evaluation.

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by July 2, 2019 and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with The Forrester Wave™ Vendor Review Policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. Vendors marked as nonparticipating vendors in the Forrester Wave graphic met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. We score these vendors in accordance with The Forrester Wave™ And The Forrester New Wave™ Nonparticipating And Incomplete Participation Vendor Policy and publish their positioning along with those of the participating vendors.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with the Integrity Policy posted on our website.

Endnotes

[1] In almost all situations, organizations don't know what and how much data is recoverable. I&O pros invest in data resiliency tools hoping to recover 100% of their data, but that's not the case. Even if they do, it comes at a huge cost. Source: Paul Gessler, "Baltimore Ransomware Attack | What's Working And What's Still Down," CBS Baltimore, June 11, 2019 (https://baltimore.cbslocal.com/2019/06/11/baltimore-ransomware-attack-whats-working-whats-still-down/).

[2] To get more details on recovery readiness, see the Forrester report "Develop A Recovery Readiness View To Gain Insights Into Your Recovery."

[3] Entropy is a function of the state of the system, so the change in entropy of a system is determined by its initial and final states. The amount of entropy is also a measure of the disorder, or randomness, of a system.

[4] Dell EMC Power Protect X400 is in early stages of development and we expect that it will be ready to serve wider enterprise requirements in near future.

[5] Bayer declared that a ransomware lay dormant in its IT environment for close to a year. Source: Patricia Weiss and Ludwig Burger, "Bayer contains cyber attack it says bore Chinese hallmarks," Reuters, April 4, 2019 (https://www.reuters.com/article/us-bayer-cyber/bayer-says-cyber-attack-detected-and-contained-idUSKCN1RG0NN).

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
- Infrastructure & Operations

Security & Risk
Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.