Solutions Review

2020
BACKUP & DISASTER RECOVERY
BUYER'S GUIDE

MARKET OVERVIEW

Backup and disaster recovery solutions are vital for organizations that want to maximize uptime and protect themselves from threats like cyber crime and natural disasters. Backup and recovery technology is steadily advancing, and it is expected that nearly half of organizations will replace the backup applications they deployed as recently as 2018 in the coming months. This shows how critical it is for companies to remain up-to-date with backup and disaster recovery planning. When business-critical enterprise data is on the line, data management leaders should consider forward-looking technologies first.

Data backup is a replication of data placed on a separate device or in a different location. Disaster recovery allows for the recovery of data in the event that it is lost. Solutions Review notes a move among backup and recovery vendors past basic functionality. The providers in this space are increasingly offering integrated data storage capabilities to assist customers with IT resilience. Offering clients a complete backup and data protection product can help to ensure that data loss does not impact an organization's bottom line.

Though backup and recovery practices have existed for years, there have been major changes and challenges in the space. New developments in deployment options like the proliferation of cloud technologies, as well as recovery techniques, pricing models and venture-backed startups all promise to disrupt the market. Vendors also continue to struggle when protecting server-virtualized environments, emerging next-generation databases, very large databases, and big data applications. The need exists for more simplistic functionality, though just how that aligns with the complex needs of enterprise organizations remains to be seen.

Modernization is essential in today's market; without it, businesses will be unable to manage new data types and deployment models, or increased workload volumes. Key requirements for modern backup and disaster recovery solutions are components such as ease of deployment and administration, and instant recovery. A full-featured product will also deliver data management to support analytics, test/dev, automation, and ransomware detection on cloud copies of backup data.

There are growing instances of organizations implementing multiple backup solutions in order to best protect their vital data, manage product costs, and empower end-users. As a result, larger vendors are not necessarily the safest choice. New and emerging providers are offering the most innovation per dollar spent, and the market is undergoing an important shift to include these providers as staples for their respective niches. We expect this trend to continue through the end of 2020, and the backup and recovery products covered in this resource represent that fact.

Solutions Review has developed this buyer's guide to assist buyers in search of the best possible tool to fit the needs of their organization. This resource features 10 important questions to ask during the buying process, and full, one-page vendor profiles that provide a solution overview, three key features, contact information, and our own 'Bottom Line' analysis. Companion research, including our Disaster Recovery as a Service (DRaaS) Buyer's Guide, can be found at solutionsreview.com.

Tess Hanna, Editor
Solutions Review

5 Questions You Should Ask When Evaluating A Backup And Disaster Recovery Solution

How much and what kinds of data do we need to back up, and how quickly?

Determining the quantities and kinds of data you need to back up can help you to narrow your focus when looking at vendors. "Different kinds of data" refers to files, programs/applications, and entire operating systems; the former being easier to store and the latter two being more difficult. Be aware that there is often a tradeoff between the quantity and complexity of the data you need to back up against the speed and ease with which that backup can happen, a good solution will reduce tradeoff costs.

How much time/people are available to set up and operate any solution?

Figuring out how much time and how many employees are actually available to perform the implementation and operation of a new backup and disaster recovery solution will be critical. When establishing what your organization's requirements are for a solution's technical specifications, such as various types of automation and support services, consider the resources that your provider is making available to you in order to best gauge what will work.

How much and what kinds of support will we need?

Support can come in various forms. Some types of support are old fashioned technical support, support for backing up applications, support of backing up operating systems, internal and external audit assistance, and assistance with disaster recovery. Pick out what you will need given your available resources so you know what to ask for and compare when talking with vendors. This will help you to pare the number of possible vendors down, as not all of them will offer every form of support you need.

What will our business need to back up in the future?

With any solution you plan to keep for a while, you have to plan for not just what you need now, but also what you plan to need in the foreseeable future. A good place to start would be listing out the kinds of business critical data, programs, and operating systems you know you will need to back up within the lifetime of the solution. Afterwards, create another list detailing those that will possibly need to be backed up in the future.

How much are we willing to pay?

If you don't want to pay for features such as automation, you will still need to figure in the costs of the IT administrator's time and effort to do the job manually. A complete accounting picture also needs to include the costs and risks associated with a disruptive event, which in many cases can be disastrous for a business. Will the "cheaper" solution really be less expensive in the long run if it can't back up and then restore critical types of data after a crash?

5 Questions You Should Ask Your Potential Backup And Disaster Recovery Solution Provider

How does the solution perform?

A solution's performance goes beyond speed of data transfer and data durability. You should also assess ease of use, how protected physical backup sites are from various natural and man-made elements, and the types of data and devices the solution can handle. Those last three points should include the rest of the time you plan on having the solution in place. You can measure a solution's performance based on how they improve the speed and accuracy of data transmission and disaster recovery.

How scalable is your solution?

Scalability brings flexibility, especially if your provider offers cloud capabilities. While scalability is often linked with backup, it is also important for disaster recovery. In fact, a lack of scalability can make deploying the solution to new environments more complex. Details can include additional licenses, increased functionality, and any limits on the amount of data that the solution can handle. Consider your organization's projected growth when taking a solution's scalability into account.

What is the total cost of ownership?

While one provider may headline a solution with a more inexpensive cost per gigabit of storage, it behooves you to read into the fine print to make sure they're not charging you in other ways to make up the difference and then some. Total cost of ownership also means looking at the resources your company has to expend to run the solution, so that should be taken into account as well. Finally, a "cheaper" solution that leaves you more vulnerable to an event may not be cheaper in the long run.

What kinds of support are offered as part of the package?

If it's important that you be able to reach your provider at any time, look into solutions that offer 24/7 customer support. Other types of support can include technical, cloud, integration, heterogeneous OS, database, and file system support. Evaluate which support elements are necessities for your organization in order to see who matches up best with your needs for the best price, and you will be one step closer to choosing a winning product.

How do you approach data security?

Ask how and where data is encrypted, and avoid companies that don't encrypt data on their own servers, or give many of their own workers access to the encryption key if they do encrypt. The best providers will offer end-to-end encryption while adopting data security best practices to ensure that any breaches that occur are dealt with swiftly, before much damage can be inflicted. Cloud solutions may be cheaper on average once you get into the terabyte range of data storage, but they can be more vulnerable.

Solution Provider Profiles

Solution Provider Profiles

Acronis

Acronis offers backup, disaster recovery, and secure file sync and share solutions. The company also provides data protection in any environment, including virtual, physical, cloud, and mobile. Acronis True Image 2020 is personal backup software that enables users to make a duplicate of their system, effectively capturing all of their data for system recovery or disk migration. Acronis Cyber Backup is aimed towards businesses of all sizes and offers proactive ransomware protection. The provider operates 14 data centers globally and offers support to customers around the world 24 hours a day, seven days a week.

Acronis
1 Van de Graaff Dr
Burlington, MA
United States
+1 (781) 782-9000
www.acronis.com

Key Features

Expansive Protection

Protect everything on Windows and Linux servers, any hypervisor, PCs, Macs, iPhone, iPad and Android devices along with Office 365 mailboxes. Users also have the ability to consolidate the backup of all of their workloads, hypervisors, and cloud applications to protect data from every endpoint. Users can also offload VMware VM backup snapshots to NetApp SAN storage.

Flexible Storage

Users have the option to store their backups in a range of locations, such as local disks, NAS, SAN, Acronis Cloud Storage, tape drives, autoloaders, and tape libraries. Backups can also be stored via variable block-size deduplication, which reduces disk storage capacity use and network bandwidth requirements. With cloud storage, users retain control of data location by storing backups in one of 14 Acronis Cloud Data Centers.

Acronis ASign

This eliminates miscommunications with users, suppliers and clients by supporting the authenticity of your customers' files with signatures enabled by blockchain. Electronically signed files are notarized and protected through Acronis Notary. Acronis ASign can be used for many common files, including rental or lease agreements, sales contracts, financial documents, and loan agreements.

Bottom Line

Acronis serves small and medium-sized businesses with less than 25 servers. However, it has at least one client with more than 200 servers under management. Acronis Backup is recommended for edge deployments and highly distributed environments. Large enterprises in manufacturing and retail with such environments can use the platform in an edge-to-cloud architecture without a local appliance in each location. The provider was recently named a Gartner Peer Insights Customers' Choice for Data Center Backup and Recovery Software.

actifio

Actifio enables Virtual Data Pipeline (VDP) technology, as well as a "data time machine," for the enterprise, eliminating backup and restore windows and creating virtual, point-in-time copies of data on demand, for use by any business application. Instant data recovery means no delays in restoring data for any use, and it's enabled through a simple consumer grade interface that is SLA-driven and application centric in applying data protection. Actifio's differentiated features in backup and recovery deliver functionality that can speed up backup modernization, improve recovery point and recovery time service levels, and apply granular protection at the application level and at the VM level.

Actifio
333 Wyman St
Waltham, MA
United States
+1 (781) 790-7500
www.actifio.com

Key Features

Fine-tuned Service Levels

Built around the SLA Architect, the SLA describes how frequently data is ingested, how long that data is retained in an instantly available snapshot pool, when that data is moved to a deduplicated and compressed pool, and how and when that data is replicated to a remote location. These SLAs can be applied to any discovered application, delivering automated lifecycle data management.

Remote Data Protection

At set intervals, based on SLAs, change blocks are asynchronously replicated. The SLA may also specify for the data to be rehydrated into the remote instant access snapshot pool to become available for immediate use. Since Dedup Async only replicates change blocks, it only uses a fraction of bandwidth most other replication technologies do. This enables remote site data protection for a broad set of applications.

Broad Compatibility

Works across physical and virtual environments and supports a broad range of operating systems, storage systems, and application environments, thereby eliminating any possible incompatibility and delivering functionality that includes physical and virtual systems. Actifio has also tailored deep integrations for many application APIs including VMware, Oracle, and major Microsoft applications.

Bottom Line

Actifio delivers a single platform that integrates disaster recovery, backup and long-term data retention. It protects a range of workloads, including large-scale applications and virtual environments. Actifio pioneered copy data management and offers scalable instant recovery for apps, files and virtual machines. This can be used for data management on a larger scale, including app development and performing multidirectional hybrid cloud deployments. Though initial deployments can require additional effort to configure the solution correctly, Actifio offers excellent customer support.

ALTARO

Altaro provides users with Virtual Machine Backup and recovery solutions. The provider's flagship product, Altaro VM Backup, has a straightforward UI that facilitates its use, while being full-featured as to create a strong backup strategy. The solution comes equipped with an outstanding support team determined to help clients succeed in protecting their environment. Everything can be managed and monitored from a single dashboard or by using the vendor's online management console. Altaro was founded in 2009.

Altaro
3737 Glenwood Ave
Raleigh, NC
United States
+1 (919) 251-6280
www.altaro.com

Key Features

Augmented Inline Deduplication

Deduplication saves space, which ensures that common blocks of data are transferred and stored in the backup location once. As a result, users are enabled to drastically reduce backup storage requirements on both local and offsite locations without taxing server performance.

User Interface Design

Altaro's user interface takes an intuitive, logical approach to backup and restore configuration and execution, meaning that no additional software is required. Because of the intuitive nature of the user interface, any employee can use the solution without training.

Advanced Backup Control

The tool provides a central management console, which delivers total control over Altaro VM Backup through a single view. It allows users to run concurrent backups, queue or pause jobs, back up virtual machines to multiple primary locations, back up live VMs on the fly or back up cluster shared volumes.

Bottom Line

Altaro VM Backup is an easy-to-use backup solution for Hyper-V and VMware. The solution boasts VM backup in less than 15 minutes. Though user reviews from G2 Crowd show that large, offsite backups to USB drives can take time to update, users also state that the solution's Continuous Data Protection (CDP) enables them to protect virtual machines as often as every five minutes. Users report quick deployment and implementation times as well.

arcserve®

Arcserve offers organizations several different backup products, including Arcserve Unified Data Protection (UDP), Arcserve Replication and High Availability, Arcserve UDP Cloud Direct, UDP Cloud Hybrid, and a legacy offering. UDP provides comprehensive Assured Recovery for virtual and physical environments with a unified architecture and an easy-to-use console. The product enables organizations to scale their IT environments easily while delivering against recovery point and recovery time objectives, on-prem or in the cloud. It also allows for the automated disaster recovery testing of business-critical systems, applications and data, without business downtime or impact on production systems.

Arcserve
8911 Columbine Rd
Eden Prairie, MN
United States
+1 (866) 576-9742
www.arcserve.com

Key Features

Recovery Point Server (RPS)

Generates, catalogs, and deletes expired backups. The tool also stores backup data sets, replicates data to other RPS machines, controls the bandwidth needed to move recovery points from site to site, and manages backup and restore operations. The RPS Data Stores also allow for unique compression and encryption settings for each store.

Backup Plans

The solution offers easy-to-administer named policies that explain exactly how to make backup copies of business data. Each plan contains instructions for copying data, replicating data, making secondary and tertiary copies of data (typically offsite), setting up and maintaining Virtual Standby machines, and notifying administrators that a backup job succeed or failed.

Bare Metal Recovery (BMR)

Restores a Windows or Linux system's complete operating environment, including files, settings and operating system, to a different hard disk, to a similar but different computer or to a dissimilar computer. Arcserve UDP Agent for Windows captures the data and information related to installed applications, configuration settings, and necessary drivers.

Bottom Line

Arcserve Unified Data Protection is most popular in Europe and Asia and appeals to mid-market companies. The solution provides continuous data protection, comprehensive backup, high availability, and disaster recovery for virtual, physical, and cloud environments. Additionally, Arcserve UDP provides comprehensive support for Microsoft Azure, AWS, and Azure Stack backup and recovery use cases. The vendor offers a range of packaging, deployment, and pricing options, which allows customers to choose exclusively the functions they need, as well.

Asigra

Asigra is built for cloud computing environments and designed to offer backup efficiencies by allowing enterprises to capture, ingest and store less data. Designed for compatibility with public, private and hybrid cloud architectures, the Asigra Cloud Backup solution is equipped with agentless software architecture, global deduplication and data compression technology along with NIST FIPS 140-2 certified security. In addition, the vendor reduces recovery time objectives and eliminates silos of backup data.

Asigra
79 Brisbane Rd
Toronto, Ontario
Canada
+1 (416) 736-8111
www.asigra.com

Key Features

Unified Platform

Asigra's unified platform covers against all data-loss scenarios. Whether users need to protect data on endpoint devices such as desktops, laptops, tablets, and smart phones, or protect critical servers and enterprise applications in physical and virtual environments, the single integrated platform will support the entire enterprise.

In-Flight and At-Rest Encryption

The solution's data encryption modules are FIPS 140-2 certified by the US National Institute of Standards and Technology. Corporate data is encrypted at the source before it leaves the company LAN, so users can be sure that all their data is secure as it travels over public networks and is stored in backup repositories. Unauthorized users will not have access to the backup information through the use of encryption.

Storage and Network Resource Efficiency

Global deduplication, encryption, and data compression technologies minimize the quantity of data that is transferred over the network and ensures that it is efficiently and securely stored in a safe location. This makes it easier and more cost-effective for users to keep all the data in their organization's environment protected.

Bottom Line

Asigra Cloud Backup is an enterprise-class backup and recovery solution that provides a single data protection interface for physical servers, virtual machines, endpoint devices, and cloud apps. The company was recently named the Hot IT Company of the Year in the 2019 IT World Awards. Asigra also has a strategic relationship with storage and data management solution provider, NetApp. Though some Gartner Peer Insights users believe the interface needs a makeover, they also stated that the provider's pricing is lower than competitors.

AXCIENT™

Axcient offers a single solution that incorporates data protection, disaster recovery, archiving, and test/dev. The vendor provides two self-service platform options that can be managed by a single user: Axcient Business Recovery Cloud, which is the legacy solution, and Axcient Fusion, which was unveiled in 2016. Axcient Fusion is built to run on public cloud, and both platforms offer one-hour and eight-hour RTO options. Axcient enables users to mirror their entire business in the cloud, thereby simplifying data access and restore, failovers, and virtualization. The company is headquartered in Colorado and was founded in 2006.

Axcient
707 17th St
Denver, CO
United States
+1 (720) 204-4500
www.axcient.com

Key Features

Reverse Incremental Technology

The latest backup is always compiled of previous backups. As a result, if one backup is accidentally damaged or deleted, it does not affect the latest version. With this functionality, there is no need to wait for the latest image to be reassembled from past incremental backups before using your data.

Off-Site Storage

Axcient stores your data in a SSAE 16 certified data warehouse. Company data is further protected because a copy of your data and server images are automatically sent to Axcient's secure data center at customizable intervals. If your server fails, the appliance will keep your organization up and running.

Agentless

This agentless solution requires no installation on the destination server and does not require a reboot after installation. This enables the deployment and update processes to be completed faster. The vendor uses VSS to backup in-use files like Exchange or SQL, and the tool reduces the load on primary systems, as much of the work is distributed to the Axcient Business Recovery Cloud.

Bottom Line

Axcient typically serves small and mid-size businesses. The vendor's Business Recovery Cloud tool is recommended for smaller physical and virtual x86 environments, while Axcient Fusion is a better fit for larger VMWare environments. Though Fusion does not offer recovery for physical machines, its prices are competitive and there are no hidden fees when it comes to testing four times a year, the number of restore points, disaster declaration, retention for up to seven years, and public cloud network charges. Axcient also offers copy data management.

Barracuda Backup offers a complete cloud-integrated solution for protecting physical and virtual environments that includes software, appliance, and offsite replication. The solution is simple to deploy, easy to manage, and offers users unlimited cloud storage. With an extensive range of supported environments and integration with copy file sync and share services, organizations can replace multi-vendor piecemeal backup solutions with an all-in-one appliance. The platform supports replication to another Barracuda appliance for private-cloud data protection or secure transfer to the Barracuda Cloud. Barracuda also offers an email archiving product.

Barracuda Networks
3175 Winchester Blvd
Campbell, CA
United States
+1 (408) 342-5400
www.barracuda.com

Key Features

Inline Deduplication

Occurs the moment data is written to storage and minimizes the time for completion of the full backup and replication process. This reduces the amount of redundant data in an application and the capacity needed for the backup disk targets, in comparison to post-process deduplication.

Data Recovery

Those with physical servers are provided the ability to execute bare metal restores in case of failure, while virtual environments benefit from fast image-based restores. For customers with Instant Replacement, Barracuda will preload the most recent data and configuration settings store in Barracuda Cloud Storage onto the replacement unit for emergency restores in the event of a complete site disaster.

Live Boot

Offers businesses protecting their VMWare and Microsoft Hyper-V environments with Barracuda Backup the choice to leverage Barracuda Cloud Storage if their virtual environment goes down. Users can use their local backup as storage, booting the VM from a deduplicated state. Users subscribed to Instant Replacement who replicate to Barracuda Cloud Storage can use Cloud LiveBoot to boot VMs from deduplicated storage as well.

Bottom Line

Barracuda Backup is an all-in-one hybrid cloud backup solution that is easy to set up and manage. Midsized businesses and enterprises tend to do very well with hybrid cloud platforms like Barracuda Backup. Though migration of archiving off the system can be slow at times, users praise the solution's easy to use interface. Additionally, the provider offers 24/7 user support via phone call, Skype, live chats, or email. Gartner peer reviewers have also noted the ease of implementation.

CARBONITE

Carbonite offers enterprise cloud-based backup, recovery, and storage solutions. The Carbonite Data Protection Platform allows organizations to deploy the right form of protection for each type of data in their systems—from long-term backup to rapid recovery, data migration, and endpoint protection. The vendor's Cloud Disaster Recovery centralizes the backup and recovery of data on all computers distributed throughout an organization's locations. Agents automatically back up the data over the internet to a highly secure data center. Carbonite has three recovery centers in the United States.

Carbonite
2 Avenue de Lafayette
Boston, MA
United States
617-587-1100
www.carbonite.com

Key Features

Comprehensive Protection

Carbonite's all-in-one platform includes hardware, software and cloud options for flexible deployment. The technology spans physical, virtual and legacy systems and provides support for over 200 operating system versions, applications and platforms. The software, cloud service, and optional hardware are fully integrated and supported by the provider.

Built-In Cloud Integration

All Carbonite backup and disaster recovery products are directly integrated to secure offsite storage in the Carbonite Cloud. Transmitted data is compressed and encrypted using AES 256-bit in-flight and at rest. The automatic cloud integration, on-site data recovery, and bare metal restore for an unlimited number of servers allows businesses to avoid downtime.

Compression and Deduplication

Advanced compression and dynamic bandwidth throttling reduce bandwidth utilization and preserve network performance during peak hours. In addition, Carbonite's patented global deduplication technology optimizes network and storage efficiency for endpoints.

Bottom Line

Carbonite's Data Protection Platform offers local and cloud backup for physical, virtual and legacy servers. The solution provides high availability for tier-one systems, workload migration to lessen the impact of planned and unplanned downtime, and endpoint protection for highly mobile workforces. The installation and implementation of the solution is simple, according to Gartner Peer Insights user reviewers. Carbonite's certified experts provide award-winning customer service, and its product is available in monthly and annual installments. Additionally, in November 2019, OpenText announced its intent to acquire Carbonite.

cobalt IRON®

Cobalt Iron's flagship SaaS-based backup solution, Compass™, reduces complexity and the amount of time spent on backup. Additionally, the software improves overall data protection performance. The enterprise data protection platform offers four main product components: Commander, Analytics Engine, Accelerators, and Accelerator Operating System. With this solution, users have access to a range of analytics-driven data management capabilities through a unified web user experience. Additionally, the solution offers ransomware detection, alerting and notification, remediation capabilities, and is available in AWS, Azure, Google, IBM, and Alibaba.

Cobalt Iron
1421 Research Park Dr
Lawrence, KS
United States
+1 (888) 584-4766
www.cobaltiron.com

Key Features

Automation

Compass automates 90% of daily backup operations, as well as updates, patches, and upgrades across the backup landscape. The platform also provides continuous monitoring and alerts with proactive problem avoidance.

Remote Operation & Management

Offers a unified web management dashboard for the entire backup environment. Additionally, Compass eliminates the need to log in to backup servers. The solution also delivers global policy management and role-based access controls.

Enhanced Security

Compass offers encryption at rest and in-flight, WORM-by-default, containment security by design, and Airgap by design in order to provide enhanced security.

Bottom Line

Cobalt Iron serves medium to large enterprises with multiple petabytes of data. Cobalt Iron's Compass platform is recommended for enterprises looking to cut CapEx and OpEx expenses, move off of legacy solutions, incorporate cloud workloads, or reduce backup times while increasing backup success rates. Compass was recently named one of DCIG's Top Five Anti-Ransomware Enterprise Backup Solutions, as well as one of CRN's Top 20 Coolest Data Protection Companies.

CODE42

Code42 offers backup, disaster recovery, and data loss protection solutions. The provider's data loss protection solution, (Next-Gen DLP), detects insider threats, satisfies regulatory compliance requirements, automatically monitors file activity across computers and cloud, and facilitates incident response. The vendor's security, IT, and compliance professionals have the ability to protect endpoint and cloud data from loss, leak, and theft while maintaining a collaborative culture for employees. Code42is backed by Accel Partners, JMI Equity, NEA, and Split Rock Partners and was founded in 2001.

Code42
100 Washington Ave S
Minneapolis, MN
United States
+1 (844) 333-4242
www.code42.com

Key Features

Continuous File Monitoring

Users can to track creation, modification, and movement of files on Windows, Mac, and Linux computers. File content and associated metadata can also be collected to speed up insider threat investigations. Data movement is monitored within corporate cloud environments like OneDrive, Google Drive, and Box.

Suspicious Behavior Identification

Detect when users move files to removable media, web browsers/applications, and cloud sync folders. Users can also identify files that were shared externally through corporate OneDrive, Google Drive, and Box accounts. Alert criteria can be defined based on user, data exfiltration vector, and file count or size for data protection.

Insider Threat Navigation

Users gain access to comprehensive file details, including file hash, owner, path, size, and category along with device information such as hostname and IP address. All file activity is automatically indexed and made searchable in order to reduce the time it takes to detect and respond to insider threats.

Bottom Line

Code42 offers an intuitive backup solution that does not require training for end-users. This solution is recommended for backing up user data in cloud or on-prem for compliance and simple recovery. The provider is praised for its platform's easy implementation process, as well as the capability to run the tool automatically in the background of business operations. While the platform does not detect bugs and notify the user, incremental backups are smooth and do not require any interaction.

COHESITY

Cohesity is a data management company that manages, protects, and extracts value from enterprise data. The provider's flagship tool, Cohesity DataProtect, safeguards a wide range of data sources on a single web-scale platform. The solution can be deployed on-premises on qualified platforms in the data center, in the public cloud, and on the edge. Additionally, the platform utilizes a scale-out architecture that starts with a minimum of three nodes and scales without disruption by adding nodes to the cluster. Through this solution, users have the ability to use backup data directly on the platform without needing to restore it, which allows for the consolidation of other use cases including dev/test and analytics.

Cohesity
300 Park Ave
San Jose, CA
United States
+1 (855) 926-4374
www.cohesity.com

Key Features

Web-Scale Simplicity with Broad Application Support

he solution provides comprehensive enterprise-class protection for a broad set of data sources - including leading hypervisors (VMware, Microsoft Hyper-V, Nutanix, AHV, RedHat Enterprise and KVM), traditional and modern databases (Oracle, SQL, NoSQL and Hadoop), NAS (EMC Isilon, NetApp, Cisco, Pure Storage) and modern applications (Office 365 and Kubernetes-based apps).

Instant Recovery at Scale

Combined with Cohesity Helios, users are able to search and recover data from any Cohesity cluster, from any location. The solution also reduces downtime through the ability to instantly mass restore any number of Virtual Machines (VMs) to any point in time.

Integrated Cybersecurity

Cohesity SpanFS is an immutable file system that delivers DataLock, the industry's first WORM implementation for backup, stopping malware from modifying or deleting backup data. Users can also uncover cyber exposures, vulnerabilities, and detect potential ransomware attacks with the platform's machine learning capabilities.

Bottom Line

Cohesity was named a market leader by Forrester Research in "The Forrester Wave" Data Resiliency Solutions for Q3 2019. The vendor also exports the backup data in native formats to allow for additional use cases, such as test and development, disaster recovery, and analytics. Cohesity also offers an integrated appliance that scales both backup performance and storage capacity linearly, along with cloud tiering, replication, and recovery capabilities. Cohesity consolidates multiple point solutions on a single software-defined data management platform for web scale that allows IT organizations to meet their business SLAs.

COMMVAULT®

Commvault provides data protection and information management software to assist organizations with protecting, accessing, and using all of their data economically. The vendor has a long list of supported public cloud providers, hypervisors, big data support, and database protection as well. The platform is primarily offered as a software-only solution, but Commvault also has an appliance option. Recently, Commvault announced its intent to acquire data storage solution provider, Hedvig. The vendor's software, solutions, and services are available directly through the company, as well as through a global ecosystem of partners. Commvault is headquartered in New Jersey.

Commvault
1 Commvault Way
Tinton Falls, NJ
United States
+1 (732) 728-5310
www.commvault.com

Key Features

IntelliSnap

Features the industry's broadest support for integrating with and exploiting storage hardware platform snapshots, directly supporting over two dozen of the top-selling storage arrays. This technology provides a layer of intelligence between storage and applications, ensuring the integrity of snapshot data, executing policies and schedules, automating array discovery, and indexing and cataloging snapshot data.

VMs and the Cloud

Back up and recover your virtual machines and structured and unstructured data with speed and scale while remaining agile by moving data between clouds. Commvault offers VM recovery with live recovery options, backup to and in the cloud, custom-fit data protection for every SLA, and workload portability across physical, virtual, and cloud platforms.

Unified Interface

Users have the ability to gain control and insight managing multi-platform disaster recovery on-prem and in the cloud from a single interface. The data management features that come as a result include data backup, recovery, management, reduced deployment complexity and eDiscovery. Users can recover data to any region, on-prem data center, or to other cloud providers.

Bottom Line

Commvault is recommended to enterprise customers in need of strong data proctection management, hardware snapshot management, and cloud integration capabilties. Commvault Complete Backup and Recovery supports the public cloud providers, databases, and storage arrays. Additionally, IntelliSnap offers support for integrating with and exploiting storage hardware platform snapshots. They also introduced administrator-persona-oriented and simplified user interfaces to improve ease of use. Though implementing the solution is reportedly somewhat complex and can require professional assistance, customers state that they are likely to repurchase the platform.

datto

Datto offers backup and disaster recovery appliances, Software as a Service (SaaS) data protection, and managed networking products. The provider has more than 5,000 managed service providers across the globe that sell its products. Datto also boasts nine data center locations worldwide, in locations including the U.S., Canada, Iceland, the U.K., Germany, Australia, and Singapore. Datto is offered for data on-prem in a physical or virtual server, or in the cloud via SaaS applications. The vendor is completely channel-driven and recently released SIRIS 4, a business continuity and disaster recovery solution built for MSPs.

Datto
101 Merritt 7
Norwalk, CT
United States
+1 (888) 294-6312
www.datto.com

Key Features

Image-Based Backup

Using image-based backup allows the provider to take an image of a workstation, server, or entire system, which contributes to improved Recovery Time Objectives (RTO) and the ability to boot virtual machines. In addition, image-based backup provides faster full restores, restoration of individual files, verification of images, and the ability for bare metal restores.

Multiple Appliance Platforms

Datto virtual appliances now support VMware and Hyper-V. The vendor's Intelligent Business Continuity solution can be purchased as a virtual appliance on virtual infrastructure, in addition to their physical hardware. Virtual appliances easily integrate with the Datto cloud and come with a predictable cloud billing model.

Encryption

All data is protected by AES 256 encryption both in-transit and in the cloud. Users also have the option to encrypt data locally, and passwords can be specified per appliance or per protected machine to meet compliance regulations. Corporate data is protected during synchronization, storage, and replication. Backups are encrypted at rest, using a key that can only be generated with the password held by the MSP or end-user.

Bottom Line

Datto is recommended for small to mid-sized businesses and is cost-effective. The vendor does not limit the number of vCPU and vRAM in the cloud. However, there is a limit of 8 vCPU and 16 GB vRAM per machine on the portal without customization. The platform also offers a Backup Report page, which displays information on the status of backups. Datto recently introduced 24/7/365 technical support, so MSPs can directly access support by phone at any time. Additionally, user reviews show that the solution's user interface is intuitive and easy to use.

DELLEMC

Dell EMC's backup and recovery solution is a prepackaged backup suite made up of several different components that are available for individual sale. These include Avamar, Networker and Data Protection Adviser, with options for cloud backup and archiving. Dell EMC's solutions give a full range of data protection, from archive to continuous availability for physical, virtual and cloud environments. The provider enables digital transformation through hybrid cloud and big-data solutions built on a modern data infrastructure, which brings together converged infrastructures, storage, and servers. The recently launched all-in-one Integrate Data Protection Appliance combines Data Domain with Avamar and DD Boost for Enterprise Applications.

Dell EMC
176 South St
Hopkinton, MA
United States
+1 (508) 435-1000
www.dellemc.com

Key Features

Efficiency

Through a complete software and hardware solution, Avamar offers variable-length deduplication, which reduces backup time significantly by only storing daily changes while maintaining full backups for immediate, singlestep restore. Avamar facilitates these backups for virtual environments, remote offices, enterprise applications, network-attached storage (NAS) servers, desktops, and laptops.

Optimized Bandwidth

Deduplicated backup technology sends only changed blocks, and in doing so, reduces network traffic. Users also have the ability to utilize existing local area network (LAN) and wide area network (WAN) bandwidth for remote and branch office backup and recovery. Through this technology, users can more easily transfer their data to the correct location.

Reliability

Avamar Data Store features redundant power and networking, redundant array of independent disks (RAID), and patented redundant array of independent nodes (RAIN) technology to provide uninterrupted data accessibility. The solution also allows for daily data systems checks to ensure recoverability whenever necessary.

Bottom Line

Dell EMC's solutions are a good fit for large on-prem environments that include physical systems and virtual machines. Though the data protection portfolio often results in lock-in with Data Domain and other proprietary hardware, it's important to note that the vendor offers low-cost cloud object storage for backup-based disaster recovery. Dell also offers aggressive discounts, often with high attach rates of its backup solution to its primary storage sales. The provider's Integrated Data Protection Appliances are partially addressing long-standing complications of managing DP Suite plus Data Domain components.

druva

Druva delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service. Druva Phoenix simplifies data protection, improves visibility, and significantly reduces the risk, cost, and effort of managing complex data. The solution operates seamlessly and can be managed from one location, giving IT administrators full visibility and control over server backups and data composition. Druva is used worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and was founded in 2008.

Druva
800 W. California Ave
Sunnyvale, CA
United States
+1 (650) 241-3501
www.druva.com

Key Features

Simplicity

Druva provides automated policy management and a unified data model – breaking down existing silos and simplifying administration. Customers don't have to worry about hardware, software or patching and upgrading. The solution also provides a global view across server data and can centrally manage the backup, disaster recovery, and archival systems.

Scalability

Druva's solution allows for infinite, on-demand scale into the multi-petabyte range. With Druva, built on AWS, customers achieve a global data center reach, and 150PB+ under management, with over 4m backups occurring each day. Additionally, Druva's data centers offer data durability and map backup policies, while enabling alignment with regional data residency requirements.

Security

Druva Phoenix offers automated archiving, which ensures that data is automatically moved to lower cost, cold storage, effectively remaining secure for decades. Druva also offers security benefits such as data isolation, storage architecture, encryption design and certifications, including HIPAA, SOC-2, FIPS, and FedRAMP.

Bottom Line

Druva Phoenix makes it easier and more cost-effective for users to protect all of their data across complex infrastructures with cloud backup, disaster recovery, and archival. The provider's solution is recommended for small to mid-sized companies and offers a pay-as you-go pricing model. Reviews from Gartner Peer Insights show that users find Druva Phoenix easy to use, implement, and install on data center applications, while also being consistent during operations. Druva also provides 24/7 customer support, as well as a library of training materials.

FalconStor

FalconStor provides data protection and recovery. The tool automates complex recovery processes to ensure data can be recovered before business operations are impacted. Users can proactively detect and alert performance bottlenecks and health risks using a real-time analytics module with historical and real-time trends and reports and streaming analytics. FalconStor also enables wide area network (WAN)-optimized replication options for disaster recovery and remote office protection. Users have the ability to reduce or eliminate backup windows and recover data as well.

FalconStor
701 Brazos St
Austin, TX
United States
+1 (631) 777-5188
www.falconstor.com

Key Features

Proactive Centralized Monitoring

Provides proactive centralized monitoring, analytics, and configuration across heterogeneous storage infrastructures to keep problems from happening. Users have the ability to break down data silos and utilize storage based on use case and policy with a view of their entire environment. This technology also includes embedded security and allows users to leverage their existing IT investments.

Reduce Backup Windows

Reduce or even eliminate backup windows and recover data to any point with FalconStor snapshot technology. FalconStor's Continuous Data Protection (CDP) provides protection for a longer period of time than traditional snapshot-supported tape backup. The tool also maintains instant disaster recovery and hourly snapshot protection, with or without journaling.

Convert

Users are able to recover to dissimilar hardware, convert from physical to virtual environments on-the-fly, and convert from virtual to different virtual environment. As a result of this technology, the solution enables organizations to migrate locally, remotely, or to and from cloud environments.

Bottom Line

FalconStor supports application-specific data protection for most business applications including Microsoft, Oracle, and SAP. The vendor works with a variety of clients in different verticals but is recommended for small to mid-sized businesses. According to Gartner Peer Insights, users find FalconStor's predictive analytics and intelligent action particularly advanced. The vendor makes use of Core-to-Edge insight, and the administrative interface also allows for customization. Though support is difficult to reach at times, the initial installation, setup, and configuration processes are straightforward and intuitive.

HITACHI

Hitachi Vantara is a wholly owned subsidiary of Hitachi, Ltd., and offers an expansive portfolio of products for integrating, managing and analyzing data. Hitachi's portfolio of data management solutions are best suited for modern environments, and can help organizations to quickly improve their key performance metrics, including business continuity, backup windows, operational recovery and disaster recovery. The tool also provides data protection and recovery for complex enterprise architectures.

Hitachi Vantara
2845 Lafayette St
Santa Clara, CA
United States
+1 (866) 660-7555
www.hitachivantara.com

Key Features

Data protection and recovery

IT professionals can enact simple data protection and recovery operations using the right tools for each job but managing them all in one place. Users can also combine local and remote requirements in a single policy-based workflow for faster and more frequent data protection. Hitachi eliminates the need for backup windows as well.

Automated Copy Creation

Application and database administrators can automate copy creation and gain control of copy management to support secondary business functions like DevOps, finance and marketing.

Compliance and Governance

Hitachi Vantara enables the use of backup data to support e-discovery, analysis and auditing operations. Security is a key tenet of the product, providing an integrated approach to data management that allows organizations to bridge the gap between traditional and emerging cloud technologies.

Bottom Line

Hitachi Data Instance Director is expanding the data protection conversation to encompass enterprise-scale copy data management. The company's backup and recovery capabilities feature an In-System Replication Bundle with volume-cloning and space-efficient snapshots. Hitachi provides AI-driven data center management as well, and offers machine learning and advanced analytics to optimize your data center. Solutions Review recently named Hitachi Vantara a Backup and Disaster Recovery Vendor to Watch in 2019.

IBM offers a wide range of technology and consulting services, including predictive analytics and software development. The vendor's backup and disaster recovery solution, Spectrum Protect, is a data protection platform that gives enterprises a single point of control and administration for backup and recovery. It enables backups and recovery for virtual, physical, and cloud environments. The tool also offers VM protection with searchable catalog and role-based administration. IBM Spectrum Protect is a suite of software offerings designed to help organizations manage and protect their data by simplifying backup administration. IBM is based in New York.

IBM
1 New Orchard Rd
Armonk, NY
United States
+1 (800) 426-4968
www.ibm.com

Key Features

Simplified Restores

ith OpenStack backup drivers and VMware vCloud integration, organizations can extend automated backups and simplified restores to their cloud applications. This technology reduces load on the source, network bandwidth consumption, and overall media costs. VMware administrators can also manage backups and restores using intuitive interfaces.

IBM Components and Patented Technology

Spectrum Protect utilizes IBM components and patented technology that are not available in other backup and recovery products. Users have the ability to safeguard their data with an integrated IBM Spectrum Protect IBM Cloud Object Storage backup solution with automated, simplified administrative data and recovery processes.

Protection

Protect all types of data for virtual, physical, cloud and software-defined environments with one solution by one provider end-to-end. The platform enables advanced data protection for current and next-gene environments. Protection is also provided to core applications and remote facilities. Data managed by IBM Spectrum Protect is replicated to offsite recovery facilities.

Bottom Line

Protect all types of data for virtual, physical, cloud and software-defined environments with one solution by one provider end-to-end. The platform enables advanced data protection for current and next-gene environments. Protection is also provided to core applications and remote facilities. Data managed by IBM Spectrum Protect is replicated to offsite recovery facilities.

Infrascale™

Infrascale offers an enterprise-grade disaster recovery solution that provides failover to a second site with the flexibility to boot from the appliance or cloud. The product is delivered as a physical or virtual appliance and includes disaster recovery software. Infrascale's dashboard simplifies the management of data protection by providing a single view through which the entire suite of services is deployed. An administrative dashboard, accessible from any browser or device, makes it easy to recover mission critical applications and systems with pushbutton simplicity. Infrascale is headquartered in California and was founded in 2011.

Infrascale
999 N. Sepulveda Blvd
El Segundo, CA
United States
+1 (310) 878-2626
www.infrascale.com

Key Features

Triple Layer End-to-End Encryption

Corporate data is encrypted initially at the source, then transmitted through a secure connection and encrypted once more in the cloud. Organizations hold the encryption key so users have control over who can decrypt and view data. The solution is also compliant with SSAE 16, SAS 70, Sarbanes-Oxley, HIPAA, FIPS, and CJIS.

Flexible deployment

Customers choose how to deploy failover, as Infrascale DRaaS is delivered as software, physical or virtual appliance, and flexible cloud storage targeting. Businesses can also decide to use their existing hardware or Infrascale's during the deployment process. The vendor also provides a wide range of deployment model options for users to choose from.

Any cloud

Infrascale's disaster recovery flexibility provides the ability to choose where data is located. Users can replicate to one of Infrascale's twelve global data centers, deploy to a private cloud, or leverage a popular third-party cloud such as AWS, Google Cloud Platform, or Windows Azure.

Bottom Line

Infrascale is a good fit for organizations with a hybrid infrastructure that does not include a mainframe or that has needs outside of backup for Unix or IBM system servers. The vendor offers a storage-based monthly pricing fee that includes unlimited testing as well. Though Infrascale can have a bit of a learning curve during initial implementation, its support staff is responsive and well-equipped to provide deployment assistance.

MICRO FOCUS®

Micro Focus offers scalable solutions with built-in hybrid IT management analytics, security, and data management. The vendor merged with HPE in the fall of 2017 and now offers Data Protector, a comprehensive, centrally managed backup and recovery software for physical and virtual environments. Data Protector offers high-performing backup and recovery across various data repositories, applications and remote sites in physical and virtual environments. It standardizes and consolidates backup and recovery processes so that businesses can improve reliability, gain business resiliency and reduce costs.

Micro Focus
700 King Farm Blvd
Rockville, MD
United States
+1 (301) 838-5000
www.microfocus.com

Key Features

Built-in Disaster Recovery

Users can automate disaster recovery with centralized bare metal recovery from physical to physical, physical to virtual, virtual to virtual, and virtual to physical from any backup set and at no additional cost. Enhanced Automated Disaster Recovery (EADR) allows users to collect relevant information automatically at backup time, as well as package the OS data and configuration files in a single image.

Application Recovery

Ensure granular recovery with native integrations with core enterprise applications and databases to extend backup, automate point-in-time recovery, and enable application owners to manage, drive and service their own backup and recovery requirements. In the event that an application breaches the set Recovery Point Objective (RPO) or Recovery Time Objective (RTO), Backup Navigator sends an alarm to the administrator.

Snapshot Protection

Users can quickly recover their critical data thanks to array-based snapshot integrations while removing the burden that traditional backup technologies have on the production environment. This capability reduces overall downtime and facilitates the process of meeting backup window demands.

Bottom Line

Micro Focus Data Protector is a good fit for physical environments protecting mission-critical databases and business applications. Data Protector is a unified, meaning-based data protection solution that utilizes an intelligent data management approach to protect data. Users are able to immediately install and configure the infrastructure to meet the needs of their organization, as well as set up a support IT community within the company's support model. Though the solution does not back up cloud-native IaaS workloads, reference users have praised the tool's adaptive technical engineer support for components like documentation, training, and security.

MSP360
#1 MSP BACKUP

MSP360 (formerly CloudBerry Lab) offers cloud-based backup, disaster recovery, and file management solutions that are integrated with major public cloud services. The vendor's offerings include easy-to-use backup management capabilities and military-grade encryption using customer-controlled keys. Customers can choose to store their backup data with more than 20 online storage providers, including Amazon S3, Microsoft Azure, Google Cloud, HP Cloud, Rackspace, IBM Softlayer, and others. MSP360 also partners with thousands of VARs and MSPs to provide them with turnkey, white label data protection services.

MSP360
16192 Coastal Hwy
Lewes, DE
United States
+1 (415) 301-7773
www.cloudberrylab.com

Key Features

Cloud VM Resore

MSP360 Managed Backup allows users to deploy a Windows Server image from a backup copy image as an Amazon EC2 or Azure VM instance. In the event that your local infrastructure goes down, this technology enables you to be operational quickly by deploying your server images as Amazon EC2 or Azure VM instances.

256-bit AES Encryption

Encrypt backups with up to 256-bit strong keys on source side, as well as the whole data protection in the path using SSL protocols. All data sent to the cloud is also encrypted using the SSL protocols to protect it while in transit. MSP360 also supports AES encryption with key sizes of 128, 192, and 256 bits. The higher the key size, the stronger the encryption is.

Cloud and Local Backup

Users have the ability to back up their data to the cloud of their choice or, alternatively, set up local backup in the event that they only want to send a portion of their data to the cloud and keep the remaining data on their local backup. Users can also automate VMware cloud backup to local storage, external, or network drive.

Bottom Line

MSP360 Managed Backup is an intuitive backup and disaster recovery solution, which is aimed towards small and mid-sized businesses. MSP360 Backup and MSP360 Managed Backup are both user-friendly and straight forward, meaning that they can be easily managed by non-technical users. MSP360 Backup allows users to back up various types of servers to multiple destinations. Businesses can also connect the platform to a range of cloud services.

NAKIVO

NAKIVO offers a data protection solution for VMware, Hyper-V, cloud, and AWS EC2 environments. The vendor boasts five-star online community reviews, impressive scores for customer support, and more than 10,000 global deployments. Over 150 hosting, managed, and cloud services providers are using NAKIVO's software in order to deliver virtual machine Backup as a Service (BaaS) and Disaster Recovery as a Service (DRaaS) to their customers. The vendor also has over 4,200 channel partners in 140 countries. NAKIVO is headquartered in Nevada and was founded in 2012.

NAKIVO
4894 Sparks Blvd
Sparks, NV
United States
+1 (408) 335-7367
www.nakivo.com
sales@nakivo.com

Key Features

NAS-based VM Backup Appliance

NAKIVO can be installed on servers made by several notable manufacturers, such as ASUSTOR, QNAP, Synology, and Western Digital NAS servers. Once installed on NAS, the solution helps customers use less storage space to store backup data.

VM Protection

NAKIVO Backup & Replication provides native, agentless, image-based, application-aware protection, backup, and replication for VMware, Hyper-V, and AWS Virtual Machines. Through this technology, users can protect both individual Virtual Machines and containers (such as hosts, clusters, folders). Users have the ability to automate Virtual Machine protection with VMware backup policies as well.

Smaller Backup Size

The product automatically excludes swap files, global backup deduplication, variable backup compression, truncation of SQL, exchange logs, and partitions from VM backups to save storage space. All backups are automatically deduplicated across an entire backup repository and then compressed to further save storage space.

Bottom Line

NAKIVO Backup & Replication is a reliable VM backup solution for protecting virtualized and cloud environments. Users describe it as easy to implement and use, but the vendor does not offer support on weekends or federal holidays. NAKIVO offers a built-in chat option that allows users to instantly speak to its support team directly, reducing the learning curve for the solution. The ability to download the tool as a VM reduces the workload on an organization's server as well. While current users report that the UI is a bit outdated, getting backups up and running is simple and easy.

NOVASTOR

Backup for the rest of us.

NovaStor's NovaBACKUP is a centralized backup product for heterogeneous IT environments including Windows and Linux, VMware and Hyper-V. The provider also enables MSPs to offer Software as a Service (SaaS) solutions for offsite cloud backup, archive, and long-term data retention. NovaStor is stable and reliable, and includes support for the newest technologies. With multi- tenancy functions, users have the option to setup and maintain multiple locations, departments and users within the company's backup infrastructure. The premium support for NovaBACKUP DataCenter includes unlimited phone and email communications from NovaStor's US-based technical support team.

NovaStor
29209 Canwood St
Agoura Hills, CA
United States
+1 (805) 579-6700
www.novastor.com

Key Features

Failover Media pPools

When a storage medium, local drive or backup server is not available, backups are automatically redirected to an alternative location, including another storage space or backup server. With this capability, organizations experience improved availability and less of a need for manual intervention.

Multi-Streaming

Backup and restore one server to the storage using multiple streams, and run multiple backup jobs at the same time. Users are also able to reduce backup windows without incurring any additional infrastructure costs. This technology enables higher backup speeds, as well as scalability, all while keeping hardware purchases to a minimum.

High-Performance Data Mover

Organizations are enabled to perform processes including multithreading and optimized compression in order to distribute the computational load to both the user's business and the storage medium. This technology minimizes system loads while maintaining the highest data throughput at the same time.

Bottom Line

NovaBACKUP is fast and easy to use, especially if the user does not have the space to sacrifice for a backup program. The vendor's target network size is 5 to 200 servers, and NovaStor also addresses the requirements of small and medium-sized IT environments. The process of setting up scheduled backups for workstations and servers through the network is easy, according to G2 Crowd user reviews. While the solution can time out if the connection to the cloud server is severed, users praise the solution for its simple network setup and its "set it and forget" function, which runs and reports through email automatically.

Rubrik primarily provides data protection and data management in hybrid IT environments with its flagship product. Rubrik Cloud Data Management (RCDM) is a scale-out-architecture-based data protection tool with cloud integration, live mount for Oracle Databases, and support for Office 365 backup, and SAP HANA backup. In, 2018 Rubrik acquired Datos IO, a company specializing in data protection of NoSQL databases. The vendor also offers Polaris Radar, a solution which provides ransomware detection and remediation. Rubrik is headquartered in California and was founded in 2014.

Rubrik
1001 Page Mill Rd
Palo Alto CA,
United States
+1 (844) 478-2745
www.rubrik.com

Key Features

Point-in-Time Recovery

Users can find and recover the relevant point-in-time snapshot. For Oracle and SQL databases, users can apply transaction logs to restore back to the desired point. When dealing with virtual machines, users can leverage a continuous stream of recovery points to restore to moments before a failure or ransomware attack.

Flash-Optimized Ingest

Minimizes impact to production and eliminates application stun for highly transactional applications. The solution quickly ingests large volumes of data by maximizing the number of parallel data streams processed. Through global deduplication across a scalable user, the platform can maximize storage efficiency.

Policy-Based Management

Users can click to assign Service Level Agreement (SLA) policies to their virtual machines, databases, and applications. To perform these actions, simply select desired snapshot capture frequency, retention duration, and the desired location of the restore.

Bottom Line

Rubrik's solution is recommended for those looking to protect highly virtualized on-prem environments and hybrid environments that leverage Microsoft Azure and Amazon Web Services (AWS). Many users reportedly utilize RCDM for the protection of physical and virtualized databases. Rubrik also provides a granular set of features for backing up data to the cloud and protecting public-cloud-Infrastructure as a Service- based instances in AWS and Microsoft Azure. The solution's Live Mount capability also provides automated recovery and test/dev for Oracle and SQL databases, as well as for Hyper-V and VMware virtual machines.

SolarWinds MSP is an IT infrastructure management software provider. The vendor's data backup tool is called SolarWinds Backup and provides cloud-focused data protection services to both physical and virtual servers, workstations, business documents, and Microsoft Office 365. The solution is compatible with on-prem, cloud, and hybrid environments. SolarWinds also offers storage in its global private cloud. The provider's other related capabilities include threat monitoring, mail protection and archiving, remote support, and remote monitoring. SolarWinds MSP was founded in 2003 and is headquartered in North Carolina.

SolarWinds MSP
3030 Slater Rd
Morrisville, NC
United States
+1 (855) 679-0817
www.solarwindsmsp.com

Key Features

Flexible Recovery

Users receive multiple recovery options with no additional cost for other recovery methods. The tool provides file and folder-level recovery and full system recovery with bare-metal restore or virtual disaster recovery. Users can create a standby server through the provider's continuous recovery option. The solution also allows for recovery at LAN speed via the LocalSpeedVault option.

Hardware Simplicity

There is no need to install or maintain a local application server. Additionally, no physical appliance is needed, which can lower costs. Users don't need to purchase, provision, or manage local data storage for their backups. Users can also keep an optional local copy of their data using an existing network share or other hardware with LocalSpeedVault.

Cloud-Centric

SolarWinds Backup provides the ability to back up to the cloud, as well as TrueDelta deduplicatoin, compression, and WAN optimization, which speeds up daily backups by sending only changed bytes. Cloud storage and archiving are included in data centers located globally. AES 256-bit encryption is used in the standalone and N-central integrated versions, and AES 128-bit is the default for backup integrated with SolarWinds RMM.

Bottom Line

SolarWinds Backup is recommended to small- to mid-sized businesses. The provider offers technical support for installation, configuration, setup, operation, and other product-related issues 24 hours a day, 7 days a week. SolarWinds also provides a customer portal for additional support. According to reference customer reviews, easy installation and end-user UI were major benefits. While some users reported difficulty when using the solution with multiple backup sets, each backup is encrypted from the beginning and remains encrypted when in transit or at rest.

StorageCraft

StorageCraft offers backup, disaster recovery, and business continuity solutions for servers, desktops, and laptops. Their solutions reduce downtime, improve security and stability for systems and data, and lower the total cost of ownership. The vendor boasts four offices globally, 11,000 partners and has backed up over one million devices. StorageCraft's business is focused on data protection and restoration tools that are offered via value-added and channel partners. However, it also offers scale-out storage, replication, recovery, integrated data protection, and more. The solution is supported by on-prem and cloud-based environments, as well as hybrid deployments.

StorageCraft
380 Data Dr
Draper, UT
United States
+1 (801) 545-4700
www.storagecraft.com

Key Features

Comprehensive Backup

StorageCraft ShadowXafe allows users can backup an entire system including the operating system, applications, settings, services and data. Users also have the ability to view and manage backup images directly from within the patented job timeline, as well as write backup images to any internal, removable, or network storage locations.

Instant Recovery

ShadowXafe enables users to recover files and folders in seconds or entire systems in minutes. By replicating your backup images to StorageCraft's disaster recovery cloud, you are able to continue day-to-day operations normally, with a lower risk of downtime.

Cross-Platform Operability

Customers can recover to dissimilar hardware or virtual environments with StorageCraft Hardware Independent Restore. This technology supports a range of hypervisor platforms. In addition, users have the ability to perform a cloud restore from a true failover VM running within StorageCraft cloud services, as well as verify backup images in order to ensure data integrity.

Bottom Line

StorageCraft typically serves small to medium-sized businesses. The vendor also provides support in various languages including German, French, Italian, Spanish, Japanese, and Portuguese. Buyers should keep in mind that though StorageCraft will accept calls from end-users, partners are responsible for testing and disaster recovery events. According to reviews from Gartner Peer Insights, StorageCraft's software is simple to install and configure. The tool can be installed on multiple computers and begin backing up to any location. Though users state that the interface could be more intuitive, they praise the continuous incremental backup option.

Unitrends Enterprise Backup provides a package of on-prem backup, backup to the cloud, cloud-to-cloud Infrastructure as a Service (IaaS) backup, and Disaster Recovery as a Service (DRaaS) via integrated appliances and softwareonly offerings. The provider leverages high-availability hardware and software engineering with support services to provide all-in-one backup and continuity. Unitrends also offers hypervisor host-level security for VMWare, Hyper-V and XenServer, as well as more traditional security for physical servers and databases. The company was recently acquired by IT management solution provider, Kaseya.

Unitrends, a Kaseya Company
200 Summit Dr
Burlington, MA
United States
+1 (866) 359-5411
www.unitreds.com

Key Features

Continuous Data Protection

Users have the ability to significantly improve Recovery Point Objectives (RPO), because backups can be performed as often as once every sixty seconds. Near-Continuous Data Protection (CDP) allows IT administrators up to 10,000 snapshots per week, which creates smaller backup windows and improved network bandwidth efficiency.

Adaptive Byte-level Deduplication

Offers a hybrid data reduction combining inline compression with post-processing data deduplication that adapts dynamically to multiple factors. This technology enables users to perform block-level deduplication, as well as content-aware byte-level deduplication for a more cost-effective backup retention.

Unitrends Bare Metal

Unifies the bare metal backup and master backup so only one backup type is needed. The advantages include increased retention, improved replication performance, and allowing bare metal backups to be restored to different size targets. Restores for both physical and virtual systems are supported.

Bottom Line

Unitrends is a veteran in the backup and recovery software marketplace, and it appeals to enterprises with limited staff because of unified solution for data protection and disaster recovery. Its all-in-one licensing and centralized management are also popular. While the solution only offers NAS backup over NFS or CIFS, Unitrends provides users with a predictive analytics algorithm that can detect a ransomware infection. In addition, the vendor offers Recovery Assurance, available with Enterprise Plus, which delivers automated, application level consistency sandbox testing of physical servers, Microsoft Hyper-V, or VMware vSphere VMs.

veeAM

Veeam Backup & Replication is a data protection and disaster recovery solution for virtual environments of any size. It provides fast, flexible and reliable recovery of virtualized applications and data. The provider unifies backup and replication in a single solution, increases value of backup and reinvents data protection for VMware VSphere and Microsoft Hyper-V virtual environments. Veeam offers free promotions for physical server backup and O365 Exchange Online. The solution also features data center functions, including tape support and snapshot storage integration, along with key deduplication backup integration. Veeam has headquarters in Switzerland, France, Ohio and Dubai.

Veeam
Linden Park, Lidenstr, 16,
Ch-6340 Baar
Switzerland
+41 (41) 766 71 31
www.veeam.com

Key Features

End-to-End Encryption

Allows customers secure backup data with end-to-end AES 256 encryption at source (during backup), in-flight and at-rest without a negative impact on built-in compression, deduplication and WAN Acceleration. Organizations do not need to rely on third-party encryption tools, as the capabilities are built-in to the solution from the start. Users also have lost password protection of encrypted backups without compromising security.

Customizable Reporting and Monitoring

Advanced report building allows users to pull data from any field or report into one all-purpose document. Reports included with this capability are backup infrastructure custom data, custom infrastructure, inventory, VMware and Hyper-V custom performance, VMware and Hyper-V raw performance data, and report builder.

Replication

Deliver advanced, image-based VM replication and streamlined disaster recovery, thereby ensuring availability of your mission-critical applications. This feature allows users to achieve Recovery Time Objectives (RTOs) of less than 15 minutes for all applications. When users replicate a VM, the solution creates an exact copy of it in the vSphere format on a spare host, and maintains this copy in sync with the original.

Bottom Line

Veeam works well for companies of all sizes and offers a rich capabilities portfolio along with recovery options for the VMWare and Hyper-V environment. While Veeam users report that pricing options and license management could use some improvement, the provider continues to be one of the fastest-growing companies in the backup industry. Users should be aware that the proper sizing and configuration at initial deployment may require attention. Veeam also stands out as a result of its agentless VM recovery options and functions to overcome hypervisor-native limitations.

VERITAS™

Veritas Technologies provides backup and recovery, business continuity, information governance, and storage management tools. Its NetBackup product is a single and scalable solution that can protect physical, virtual and cloud workloads. Multitenant support is optional, and the solution is available on a converged platform that requires minimal administration, even in large environments. It eliminates point products and improves productivity within a business using centralized, policy-based management. Vetitas also incorporates innovative technologies for data reduction and bandwidth efficiency, while providing extensive indexing and search capabilities.

Veritas
500 East Middlefield Rd
Mountain View, CA
United States
+1 (866) 837-4827
www.veritas.com

Key Features

Efficient Administration

NetBackup Intelligent policies for virtual machines and databases automatically discover new virtual machines and database instances and include them in future backups to help ensure all of a user's data is protected. Operations are load-balanced in order to avoid performance bottlenecks, and configuration is centralized for maximum simplicity.

Comprehensive Integration

Veritas supports a wide array of environments and integrates with each layer of the infrastructure stack to help assure reliable, consistent backups. The capability also provides protection to those volumes regardless of its location. The solution discovers virtual machines automatically, and adds them to a default data protection group.

Enterprise-level Scalability

This solution combines innovative design with the latest technical advancements to deliver impressive notable numbers with minimal impact. Users can simplify and shorten protection windows for application virtual machines as well. NetBackup also provides scalable protection for hybrid environments.

Bottom Line

Veritas offers a broad support matrix and boasts positive reference customer user reviews. Continued compliance audits reportedly cause some clients to look for alternative solutions, but the quality and strength of the product have been rated highly for the last three years. Users should be aware that the vendor's field support team, regarding sales people and support engineers in particular, has seen some turnover in recent years. NetBackup also integrates with a wide range of storage arrays; object storage; private and hybrid cloud targets; and tape device providers.

ABOUT
SOLUTIONS REVIEW

Solutions Review is a collection of technology news sites that aggregates, curates, and creates the best content within leading technology categories. Solutions Review's mission is to connect buyers of enterprise technology with the best solution sellers.

Over the past four years, Solutions Review has launched ten technology buyer's guide sites in categories ranging from cybersecurity to wireless 802.11, as well as mobility management, business intelligence and data analytics, data integration, and cloud platforms.

Information for this report was gathered via a meta-analysis of available online materials and reports, conversations with vendor representatives, and examinations of product demonstrations and free trials. Solutions Review does not endorse any vendor, product or service depicted in this publication and does not advise technology users to base their vendor selection entirely on this research. Solutions Review disclaims all warranties, expressed or implied, regarding this research, including any warranties of merchantability or fitness for a particular purpose.