Solutions Review

2020
DISASTER RECOVERY AS A SERVICE BUYER'S GUIDE

MARKET OVERVIEW

Disaster Recovery as a Service (DRaaS) is a solution category that features data replication and recovery of server workloads to a cloud environment. Solutions can be fully managed or self-service, and replication and recovery can be automated through software as well. The target location and cloud infrastructure that the workloads are replicated and recovered with can be owned by the provider or a third-party. While there are variables in play with these components, all of them must be included in the solution for it to be a true as a service product.

The marketplace for these tools is not exempt from continuous change. Elements like failback, seamless heterogeneous workload support and orchestrated recovery, which once differentiated vendors from each other a few years ago, are now essential to an effective solution. Users expect more from providers and their ability to perform more granular recovery of workloads and address a myriad of factors that cause disasters. In response to these changes, some providers have built upon their existing momentum, while others have shifted the focus of their DRaaS strategies. Additionally, a combination of DIY and business as usual solutions have emerged as the biggest competitive threat in the market.

Technically speaking, Disaster Recovery as a Service tools are often labeled as stand-alone offerings. However, they are more accurately classified as an add-on resource for colocation services or Infrastructure as a Service (IaaS). Some solution providers view DRaaS as a potential up-sell to fully managed services, or as a supplementary feature added after software or an appliance is sold. With many capabilities, DRaaS offers versatility and appeals to a variety of user needs.

Regulatory compliance and security are the driving factors in this market. While natural disasters used to be the main concern, the fear of security threats, like ransomware attacks, has made its way to the forefront. Because of this, providers that offer security-related capabilities in their products are succeeding. Because organizations look to DRaaS to fulfill a critical regulatory need, more emphasis is being placed on the providers' global reach and experience helping users meet industry-relevant requirements.

Initially, DRaaS solutions were primarily implemented by small businesses that didn't have secondary sites or that were eliminating data centers to reduce costs. However, today, we've seen that DRaaS is preferred by larger organizations, as many providers have reported an increase of large and complex environments, as well as in the volume of servers per client.

Disaster recovery has become a mainstream technology category in recent years, but that does not discount how difficult it is to find the right solution. Solutions Review has developed this buyer's guide to assist those searching for the best possible tool to fit the needs of their organization. This resource includes 10 essential questions to ask throughout the buying process, along with full, one-page vendor profiles that provide a solution overview, three key features, contact information, and our own 'Bottom Line' analysis. Companion research, such as our buyer's guide for backup and disaster recovery can be found at solutionsreview.com.

Tess Hanna, Editor

5 Questions You Should Ask When Evaluating A Disaster Recovery as a Service (DRaaS) Solution

What is my budget?

The budget of your company will be a key factor in deciding what tool you'll choose. Prices vary significantly from provider to provider because the pool of offerings is so diverse. Some providers make use of their own proprietary technology that they have created, while others use technology that has been attained through acquisition. Additionally, some vendors utilize commercial products such as Zerto. These approaches are indicative of pricing, as some offer more flexibility and features.

What problem am I trying to solve?

With an overwhelming number of providers in the market, choosing the best solution can be a daunting task. However, this process becomes simpler when you create an outline of the specific recovery problems you are working to solve. Each provider differs in their approach to replication and recovery, so attempt to align your potential options with your overarching goals.

What capabilities do I need to have?

Because these products are so varied, there are many features that you can take advantage of. Even a few years ago, certain features that were seen as advanced are now viewed as the bare essentials, such as failback and orchestrated recovery. To simplify the decision making process, buyers should record a list of must-have capabilities and use that to compare against the various solutions and find the best match for their organization.

What disasters do I need protection from?

While cyber attacks, ransomware, and natural disasters are significant threats, there are other risks which impede business operations that you need to be prepared for. Loss of power, network connectivity or unforeseen equipment failure can also cause major problems. The downtime that comes as a result of these events can cause a loss of revenue, a higher cost of operations, and a loss of credibility. Take all possible disasters into account in order to have a better idea of what capabilities you will need.

How much support will I need?

Whether during the implementation process or an actual disaster, it's likely that you will need some form of support. Providers offer this in many forms. Support can range from standard technical support to self-service or fully managed service options. Consider what service option will work best for your organization and its IT team when deciding on your disaster recovery solution.

5 Questions You Should Ask Your Potential Disaster Recovery as a Service (DRaaS) Solution Provider

Where will my data be located?

When choosing a provider, it's important to learn as much as you can about their data center. Find out where your data will live, as well as who owns the infrastructure. This will provide insight into possible compliance or data sovereignty risks for you to consider. It's also key to note the geographical area your data will be located in. Take into account if the area is prone to natural disasters or network outages. Be sure that your data exists in separate locations in order to prevent unexpected downtime.

What is your disaster recovery plan?

While your own disaster recovery strategy is of the utmost importance, your provider acts as your safety net, so they should also be prepared to step in should the worst occur. Ensure that the vendor has a well-documented disaster recovery plan that will prevent service disruptions. Any provider should be able to help itself as well as its users in the event of a disaster to maintain service.

Do you have user references?

Hearing another user's account of their experience can give you a better understanding of what working with that vendor is actually like. The users' description can provide insight into their opinions of the provider, as well as anything they learned throughout their experience. References can provide insight into the staff of the vendor as well, which is significant because those will be the people handling your infrastructure.

What efficiency and security features are included in this solution?

It's important to consider that DRaaS may have an effect on your network bandwidth. Features such as compression, WAN optimization, and data deduplication can optimize network use. Additionally, the aforementioned features can help you avoid expensive network upgrades to support utilizing the service. The security of your data is also important, and it's vital to understand how it will be secured both in-flight and at rest.

Will I retain control of my data?

Though your provider will be hosting your data, you should ensure that you will be retaining full control of it. This includes having the ability to remove it from the environment if you choose to move your disaster recovery on-prem or to another provider. It's also a good idea to check that your snapshots can be transferred in your desired format in the event that you move your data.

Solution Provider Profiles

Solution Provider Profiles

Acronis provides backup, disaster recovery, and secure access solutions. The vendor also offers data protection across any environment, including physical, virtual, cloud, and mobile. Its flagship product, Acronis True Image, delivers backup, storage, and restoration capabilities. Acronis' Disaster Recovery as a Service (DRaaS) solutions address IT requirements for backup, disaster recovery, and archiving. Additionally, the vendor offers 24 hour support to customers worldwide. Acronis was founded in 2003 and is headquartered in Switzerland.

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

Key Features

Single Pane of Glass

A central management console, which applies to all disaster recovery tasks, allows for the management of the entire disaster recovery environment. The management services include status updates and alerts through the self-service web-based recovery console. RTOs and RPOs can be set and monitored, giving users the ability to track performance against those objectives.

Push-Button Recovery

Provides users with the ability to recover groups of files or entire data centers at the push of a button with automated runbooks designed in a graphical recovery plans editor. With this feature there is no need for hand-written recovery plans. Acronis also provides support service during this process.

Automated Testing

Allows for users to regularly test their protected servers in a virtual private environment. Up to 3 servers can be activated at any time, or alternatively, the entire environment can be activated every 8 weeks.

Bottom Line

Acronis serves small and medium sized businesses. The company was issued 70 patents in the last year, with many of them focusing on unified data protection. Existing users have reported a lack of proactive monitoring and notification when servers are properly replicating. However, Acronis' implementation teams have been praised for their assistance and willingness to approach solutions creatively. Additionally, Acronis is ISO 22301, ISO 9001, and ISO 27001 certified. In early 2020, Acronis also released its cyber protection offering, Acronis Cyber Protect.

Axcient provides cloud-based disaster recovery and data protection to businesses of all sizes. The vendor's Disaster Recovery as a Service (DRaaS) product, Axcient Fusion, can mirror all of an organization's technological assets in the cloud as a means to replicate data centers on-demand. Fusion also allows users to access and restore data from any device, failover IT systems, and virtualize the business from a deduplicated copy. The solution was also built to run on public cloud and offers one-hour and eight-hour RTO options. Axcient is based in California and was founded in 2006.

Axcient
20400 Stevens Creek Blvd
Cupertino, CA
United States
+1 (800) 715-2339
www.axcient.com

Key Features

Orchestration

Axcient Fusion offers built-in workflow automation that allows users to transfer all of an organization's data into the cloud in less than an hour. Users can create pre-written workflows, including network settings, in the order in which apps are recovered to the cloud. These workflows allow users to automate the entire recovery process.

Proactive Testing

Provides organizations the ability to perform disaster recovery testing to ensure total IT resilience as well as minimize risk in the event of a failure. This preemptive testing assists in achieving increased uptime.

Deduplication

Axcient Fusion provides a single deduplicated copy of an organization's data, for a reduction of up to 30x in an organization's data storage footprint. This copy can be used for other purposes, such as testing, development, and long-term archiving.

Bottom Line

Axcient offers copy data management that enables many uses of replicated data. These include backup, data recovery, data archival and testing and development. 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. While the solution does not offer recovery for physical machines, Axcient has the rights to the intellectual property of DirectRestore for granular application recovery. This technology came to the vendor through an acquisition in 2014 and Axcient now licenses it to other businesses in the data protection marketplace.

Carbonite offers cloud and hybrid business continuity solutions for small and mid-sized businesses. The vendor also provides end-to-end data protection capabilities that include high availability, endpoint protection and workload migration. The provider's Disaster Recovery as a Service (DRaaS) solution, Carbonite Recover, allows users to pay as they go, centralizes the backup and recovery of data on all computers distributed throughout an organization's locations, and replicates critical systems from the user's primary environment to Carbonite's cloud. Carbonite is headquartered in Massachusetts and was founded in 2005.

Carbonite
2 Ave de Lafayette
Boston, MA
United States
+1 (617) 587-1102
www.carbonite.com

Key Features

Multi-Tier Apps

Carbonite Recover is organized for multi-tiered applications. It offers boot order and script points as well. The product's built-in orchestration and automation, coupled with custom script points, support these multi-tier use cases across groups of servers.

Optimized Bandwidth

Carbonite provides bandwidth that is optimized by sending byte-level changes across the wire on an ongoing basis. This is in order to create a limited network impact, both on protected servers and the network itself. Bandwidth is improved through the use of built-in compression.

Encryption

Data encryption is built-in both at rest and in-flight, secured by AES-256 encryption. Access to the Carbonite Recover portal uses reCAPTCHA as well as optional two-factor authentication to secure user accounts.

Bottom Line

Carbonite is one of few vendors that provide recovery of non-x86 workloads formally integrated as part of its DRaaS offering. The provider was also consistently considered as an option for prospects, even if it was not ultimately chosen, per Gartner's research. The vendor offers monthly and annual pricing options. While Carbonite is currently in a transitional period in terms of the user base it is targeting, the company has guaranteed service tiers with corresponding RTO and RPO based service-level targets. Additionally, in November 2019, OpenText announced its intent to acquire Carbonite.

Databarracks provides secure Infrastructure as a Service, Backup as a Service, and Disaster Recovery as Service solutions. They are member of the Cloud Industry Forum, as well as ISO 27001 certified for Information Security. Databarracks' DRaaS solution offers flexibility and scalability, and there is no need for organizations to duplicate their hardware. The provider is based in England and was founded in 2003.

Databarracks
1 Bridges Ct
London, UK SW11 3BB
+44 (0) 203 177-191-0
www.databarracks.com

Key Features

Low Recovery Point Objectives (RPOs)

Replication occurs at the hypervisor level, which is more scalable, flexible, and less expensive than traditional physical replication. In addition, Databarracks' built-in WAN optimization allows users' RPOs to be reduced down to minutes depending on the environment.

Resilience

Databarracks' systems are located 30 meters underground in a former military bunker. The bunker is flood-proof, bombproof, resistant to EMP and electronic eavesdropping, and has months worth of backup power.

24/7 Support

Users have 24/7/365 access to a technical account manager, as well as a direct line to the service delivery team from the beginning of the implementation process.

Bottom Line

Databarracks is currently developing additional tools and methods to improve user experience. Included in these services are BackupChecks, which are integrated with Asigra and Kazoup to allow file services and archiving for Software as a Service data sources. In addition, the vendor recently released its Cyber-DRaaS solution, which increases security with features such as detection, reporting, and recursive scanning. While Databarracks does not support Unix or applications like SAP or Oracle, multiple statements from Gartner Peer Insights showed that customers found the services provided to be exceptional.

Druva delivers data protection and management for the cloud era. Druva cloud platform is built on AWS and offered as-a-Service; delivering accessible, scalable and autonomous enterprise data resiliency. Druva customers can reduce costs by eliminating the need for hardware, capacity planning, and software management. The provider also offers the first and only cloud-native Software as a Service (SaaS) backup and disaster recovery solution in the market. Customers are also able to break down data silos, streamline governance, and gain insights to drive business decisions. With Druva's solution for backup, archival, and disaster recovery, organizations can meet business continuity SLAs, disaster recovery compliance, and audit requirements.

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

Key Features

Eliminate DR Complexity

An all-in-one backup and DR solution with a single-pane-of-glass for management, allowing users to eliminate a multi-vendor approach. Offers one-click recovery (data center to AWS, VMC to AWS, AWS cross region, AWS back to data center/VMC), including failback on-prem or in the cloud. Offers failover across any AWS region and clone VPC if a region is down and automated runbook execution for rapid recovery.

Reduce TCO by up to 60%

Users have the ability to eliminate hardware replication, storage, software, and the need for disaster recovery sites, which significantly reduces costs. Additionally, the provider offers a pricing plan which is on-demand, where users only need to pay for what they use.

Minimize Downtime

The solution provides users with RPOs of an hour and RTOs of minutes. VMs are also kept-at-the-ready for immediate spin-up of AWS EC2 instances at the time of failover. Also includes automated and unlimited testing of an organization's disaster recovery plan in order to assist with meeting disaster recovery compliance requirements.

Bottom Line

Druva's DRaaS solution makes it easier and more cost-effective for users to protect all of their data across complex infrastructures. 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.

Evolve IP is a Cloud Services provider. The vendor offers organizations a unified option for cloud services such as virtual servers, virtual desktops, disaster recovery, IP telephony, unified communications, and contact centers. Evolve IP's Disaster Recovery as a Service (DRaaS) suite supports fully managed disaster recovery, self-service recovery, and cloud backups. Additionally, members of the Evolve IP team are on the advisory boards of Veeam and Zerto, showing a connection to leading disaster recovery providers. The vendor is based in Pennsylvania and was founded in 2006.

Evole IP
989 Old Eagle School Rd
Wayne, PA
United States
+1 (610) 964-8000
www.evolveip.net

Key Features

Automation

The failover and failback processes are fully automated. This includes the creation of all VMs, executing custom scripts, and reconfiguring IP addresses. A self-service portal is also enabled in order to allow users control over their disaster recovery process.

Single Infrastructure

Because Evolve IP's DRaaS solution has a singular infrastructure, there is no need for users to maintain and pay for a secondary site. Organizations do not have to build and support additional infrastructure for off-site backup or disaster recovery.

Pay as You Go

Backups and replicas can be transferred off-site with a pricing model that gives users the ability to only pay for what they need.

Bottom Line

Evolve IP's approach to services beyond DraaS, such as unified communications and an industry focus, is holistic. The provider's service offerings are articulated well with respect to varying DRaaS types and backup options. Evolve IP has five recovery centers in the United States, which serve the majority of its users. While the company's pricing is slightly above average for simple virtual environments among its peers with fully managed offerings, Gartner's customer surveys showed that the Evolve IP's organizational focus and additional managed services capabilities were reasons to select it over other products.

Expedient is a cloud, collocation, and data center Infrastructure as a Service (IaaS) provider. The vendor delivers its DRaaS solution hosted within its data centers, and separately as a service for users hosting their production workloads on-prem or in other locations using On-Site Private Cloud appliances. Expedient is a part of a network of 11 data centers across the country, and offers virtualization, cloud computing, remote backups, equipment management, and storage area networks, in addition to disaster recovery. Expedient provides its services to enterprises in a broad range of industries, including commercial, education, and government organizations.

Expedient
1 Allegheny Sq
Pittsburgh, PA
United States
+1 (877) 570-7827
www.expedient.com

Key Features

Push Button DR

Delivers total network failover between disparate locations at the push of a button, without any IP or DNS changes. Additionally, RTOs and RPOs are measured in minutes, which provide confidence in the business continuity capabilities of the solution. Users can also operate applications in multiple data centers simultaneously for active workload protection.

Availability

Users have the ability to prevent unplanned downtime through the replication of critically important computing workloads. This can take place in two or more data centers and users are able to rely on automatic recovery by seamlessly failing over among interconnected locations in the event of a disaster.

Risk Mitigation

While protecting information technology workloads with disaster recovery capabilities, Expedient also complies with industry and government mandates and regulations such as the Payment Card Industry Data Security Standard (PCI DSS).

Bottom Line

Expedient is a good fit for organizations that have compute resources that can be utilized for more than just disaster recovery. The provider's Push Button DR feature can fail over entire sites with minimal interruption to external service availability by leveraging Border Gateway Protocol during failover, instead of making DNS modifications. Though Expedient depends on other vendors for most of its R&D, the provider delivers recovery assurance at no extra cost. Expedient also mitigates the risk of resource contention during a regional outage by refraining from oversubscribing clients across its resource pools.

Flexential, formerly Peak 10, provides cloud and IT infrastructure solutions, including colocation, private network services, and managed services. Cloud-based data storage and managed security are also key capabilities. Flexential has 40 data centers located across 15 states in the U.S., Canada, and the Netherlands. The company's Disaster Recovery as a Service (DRaaS) solution, Recovery Cloud, provides recovery of business-critical applications to reduce data loss in the event of a disaster. Users can choose from multiple tiers of recovery to create a custom solution. The vendor is based in North Carolina and was founded in 2000.

Flexential
8809 Lenox Pointe Dr
Charlotte, NC
United States
+1 (866) 473-2510
www.flexential.com

Key Features

Continuous Data Protection

Data is replicated as it changes, with reliable target platform resource availability. In the event of a disaster, an organization's recovery picks up where it left off, without data loss or interruption to daily business operations.

Flexibility & Customization

Users can choose disaster recovery tiers and use key controls, such as disaster recovery test frequency, performance to align workloads, and infrastructure size. Because Peak 10 has multiple data centers, users can ensure that their recovery site is a safe distance from production. There is no need for organizations to make changes to the IT environment or storage platform.

Ongoing Testing

Recovery Cloud offers varying levels of testing to allow for documentation, risk management, and multiple recovery tests. Options include free and unlimited on-demand testing, as well as pay-as-you-go on-demand testing.

Bottom Line

Flexential Recovery Cloud is recommended to organizations with a need for DRaaS, as well as those that can strategically benefit by leveraging Flexential's services. Advanced and/or customized support can be accommodated through the provider's dedicated professional services team. While Flexential's DRaaS offerings have been stagnant in terms of capabilities over the last two years, the vendor also has adjacent offerings under its data protection portfolio. That portfolio includes backup, cloud integrated storage, and object-based storage, which can be leveraged to holistically address user requirements.

IBM offers a range of technology and consulting services. In addition to its Disaster Recovery as a Service (DRaaS) capabilities, the vendor also offers predictive analytics, software development, and systems management. IBM's DRaaS solution provides continuous replication of critical applications, infrastructure, data and systems for rapid recovery. Additionally, the vendor offers fully managed services for the recovery of business-critical systems, applications, data, and business processes across a range of environments. IBM is headquartered in New York and was founded in 1911.

IBM
1 New Orchard Road
Armonk, NY 10504
United States
+1 (914) 499-1900
www.ibm.com

Key Features

Optimized Resiliency

Provides cloud testing and disaster recovery validation. Optimized resiliency is offered as a means to avoid downtime and improve recovery results without interrupting business operations. Users can also provision and orchestrate resources and workflow with a web portal that is accessible anywhere from almost any device.

Pay-as-You-Use

A pricing model that allows organizations to pay by the hour, day, or month, with no long-term contract. There are also different price and performance levels to choose from in order to best match your disaster recovery workload.

Data-Driven Service Environment

DRaaS can be set up and implemented on IBM Cloud in under an hour with no disruption to daily business operations. Users can perform disaster recovery tests as well as test patches and upgrades in this environment. Additionally, users have the ability to declare a disaster recovery incident and then switch to failover operations. IBM Cloud supports Windows, Linux, IBM, AIX, and cross-platform testing.

Bottom Line

IBM has a long history in the disaster recovery marketplace. The provider's DRaaS solution is recommended to organizations that need fully managed disaster recovery offerings and assisted DRaaS, or that need global support for IBM hardware offerings. The vendor has significant non-x86 workload and mainframe recovery experience, and has supported over 1,000 recoveries since 1989. IBM's prices for complex fully managed services scenarios were slightly lower than competing vendors. IBM is also flexible regarding contract length (four months or longer) and size (two to 15,000 VMs).

iland is a global cloud services provider. The vendor offers secure and compliant hosting for Infrastructure as a Service (IaaS), Disaster Recovery as a Service (DRaaS), and Backup as a Service (BaaS). iland provides cloud services from its data centers located throughout the Americas, Europe, Australia, and Asia. In the past year, iland has added new fully managed support offerings and expanded the platforms it can support through the use of additional service delivery partners. The vendor's DRaaS solution, iland Secure DRaaS, allows for replication from virtual and physical environments. The provider is based in Texas and was founded in 1994.

iland
1235 North Loop W
Houston, TX
United States
+1 (800) 697-7088
www.iland.com

Key Features

Legacy System Support

Legacy and physical systems can be accommodated, colocated, and integrated into your disaster recovery plan. Users gain flexibility through organization-wide support for completely virtual environments, or a combination of virtual, physical, and legacy systems.

Compliance

Offers users an in-house compliance team that is available to answer questions about meeting audit requirements and architecting DRaaS for regulatory compliance. iland also provides advanced security options to businesses that have stricter compliance or security requirements.

24/7 Failover Support

If an employee is not available to trigger the failover, an iland employee standing by has the ability to initiate it. Failover support is available 24/7 by phone, email, and an integrated ticketing system.

Bottom Line

iland provides users with direct access to Level 2 technicians. In addition, all iland engineers and support team members are certified for VMware, Cisco, Zerto, Veeam, and/or Carbonite DoubleTake. The vendor also has staff with expertise in DevOps and compliance. Users should be aware that while iland is not compatible with organizations that have immediate plans for migration to hyperscale public clouds, the vendor's existing users praised its support, portal, and Zerto-based solution. Iland's solution also offers an automated tool that helps users size their needed solutions by using data from their actual environments.

Infrascale built the first data protection cloud to automatically failover and recover applications, data, sites and systems at the push of a button. The provider serves 50,000 customers and protects over one million devices worldwide. Infrascale's Disaster Recovery as a Service (DRaaS) solution gives users the capability to choose the way they want to deploy failover for their organization. The vendor's aim is to eradicate downtime and data loss when recovering from a disaster. 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

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 can control who can decrypt and view their data.

Mobile Data Security

Offers control over what confidential data users can transfer the power to back up a range of mobile devices, and the ability to wipe data from remote devices.

Boot on the Appliance or in the Cloud

Organizations have the capability to failover a single virtual machine, servers, applications, or an entire network locally or in the cloud within minutes at no extra charge.

Bottom Line

Infrascale typically serves companies with less than 50 servers. Infrascale DRaaS includes unlimited recovery testing and disaster declarations at no additional cost beyond the initial setup fee. Gartner Peer Insights showed that customers spoke highly of the ease of implementation, customer support, and price point. Users should also consider the level of training in best practices for backup scheduling that will be provided.

InterVision acquired Disaster Recovery as a Service (DRaaS) provider, Bluelock in 2018. The provider's DRaaS services are now branded as Bluelock Solutions. The vendor offers Infrastructure as a Service (IaaS) tools that specialize in cloud computing and disaster recovery. InterVision also provides Virtual Cloud Computing by way of IaaS where users have the option to subscribe to their chosen amount of computing, storage, and bandwidth capacity. Bluelock Solutions also supports complex environments in addition to protecting sensitive data as a means to mitigate risk. InterVision's capabilities span on-prem, private, and public cloud environments.

Microsoft
16401 Swingley Ridge Rd
Chesterfield, MO
United States
+1 (314) 392-6900
www.intervision.com

Key Features

Recovery Playbook

Provides users with an outline of all recovery objectives, restoration procedures, system and network configurations, key authorizations, and failover and failback instructions. The playbook also includes user and Bluelock contact information for user support as well as determining team member's roles and responsibilities.

Managed Services

The platform offers cloud strategy optimization and experience, as Bluelock handles day-to-day management tasks such as firewalls, load balancing, monitoring, antivirus, OS patching, and networking. Bluelock's service and support team will provide users with various combinations of requested managed services.

Onboarding & Training

Trains and guides users through the process of implementing Bluelock and scheduling the first recovery test within 30 days. The training sessions are interactive, complimentary, and available to any user within an organization. Bluelock is also available for further assistance and continued training after the solution has been implemented.

Bottom Line

InterVision is recommended for enterprises that require a high-touch approach for DRaaS with heterogeneous workloads, or that need hyperscale could management and recovery. Additionally, the vendor's onboarding, training, and run book development processes are strong, as shown through its Recover Assurance program. Although Bluelock Solutions is now part of the larger InterVision organization, it is a smaller DRaaS provider, and therefore, buyers should consider its ability to scale and handle large projects. The provider also has a long-standing practice for managing availability of services for public cloud providers.

Microsoft is a multinational company that develops, manufactures, licenses, supports, and sells a variety of software services and products. The vendor offers enterprise tools through Microsoft Azure, which include virtual machines, cloud storage, application service, and cloud backup. Microsoft's Disaster Recovery as a Service (DRaaS) solution, Azure Site Recovery (ASR), provides coverage across Linux, Windows, VMware and Hyper-V virtual machines, and physical servers. The provider is based in Washington and was founded in 1975.

Microsoft
One Microsoft Way
Redmond, WA
United States
+1 (425) 882-8080
www.azure.microsoft.com

Key Features

App Consistency Failover

Users have the ability to replicate data using recovery points with application-consistent snapshots. These snapshots capture disk data, transactions in process, and all data in memory. Users can also fail over all VMs of the recovery plan to the latest app consistent recovery point that has already been processes by Site Recovery service.

Flexible Failovers

Users can run planned failovers for expected outage, as well as unplanned failovers with minimal data loss, (dependent on the frequency of replication), for unforeseen disasters. Users can also fail back to their primary site when it's accessible again.

RTO and RPO Targets

To keep RTOs and RPOs within an organization's limits, Azure Site Recovery provides continuous replication. This is offered for Azure VMs and VMware VMs. The frequency of replication is as low as 30 seconds for Hyper-V. Users can also reduce their RTOs further by integrating with Azure Traffic Manager.

Bottom Line

Microsoft's DRaaS solution is recommended to organizations with a hybrid cloud strategy that is strongly centered around Azure. Because recovery is available in every major Azure site, users have the capability to protect their data globally. The vendor has an international presence with 26 locations, including the United States, Canada, the United Kingdom, and Germany. While Azure Site Recovery needs to address non-x86 workloads via collocation or with a managed service provider, Microsoft has high success rates and speed of failover. Over 90 percent of ASR failovers are completed in ten minutes and 99.9 percent are completed within 30 minutes.

NTT Communications provides managed infrastructure solutions backed by a global infrastructure. This infrastructure includes tier-1 public and private networks that reach over 190 countries and regions. The provider's DRaaS solution offers flexible disaster recovery testing, as well as a secure web-based control panel that delivers real-time visibility into networks and servers. NTT Communications' Cloud Recovery service protects business operations by replicating all operating systems, applications, and data in real-time to a secure replica NTT cloud environment. NTT Communications was founded in 1999 and is headquartered in Japan.

NTT
757 Third Ave
New York, NY
United States
+1 (212) 661-0810
www.ntt.com

Key Features

Complete Control

Cloud Recovery service provides auto-failover and secure access to the online Control Panel. The Control Panel is a web-based interface that offers real-time visibility into protected servers and the supporting network. This is possible via the Virtual Network Operating Center, which is an automated engine that continuously watches over your network.

Managed Cloud Services

The solution is a subscription-based managed service. It eliminates the need to purchase, install, oversee, and support hardware, operating systems, and disaster recovery data center facilities. This helps organizations reduce capital expenses, deployment time, and pressure on IT resources.

Ongoing Protection

Protects organizations by replicating critical servers, operating systems, supported applications, and end-user data. The replication occurs between, or to, a 24/7-accessible, secure NTT America cloud environment. Servers and data are kept current through real-time, bandwidth-efficient continuous replication.

Bottom Line

NTT Communications is recommended for small to midsize business with less than 25 servers, but the provider also has a small number of clients with at least 100 servers under management. The provider's focus is on cloud-based server replication. Its DR Target as a Service platform is built on VCC technology, which benefits users with SLA-backed RTOs and RPOs. Additionally, NTT Communications' cloud recovery service allows for users to virtually increase the number of servers, which eliminates restrictions on the server count within a single environment.

Quorum provides instant backup, recovery, and continuity to small and midsized companies. The vendor also offers a series of appliance and hybrid cloud solutions. Quorum's flagship product, Quorum onQ, is fully encrypted and available in three versions and can be used in any combination. The product is built on an architecture that the company refers to as "High Availability Anywhere." This can combine cloud, local and remote in any configuration. The vendor is based in California and was founded in 2008.

Quorum
2890 Zanker Rd
San Jose, CA
United States
+1 (877) 997-8678
www.quorum.com

Key Features

Instant Recovery

Users can recover any failed server instantly in Quorum's browser interface, as their production servers located on the provider's virtual machines are always available and up-to-date.

Migration Tools

Quorum OnQ offers a range of failback options, which include bare metal restore and incremental failback. Users have the ability to failback to similar or different hardware. This process can be completed from physical to virtual, virtual to virtual, or virtual to physical hardware.

Sandbox

Quorum offers a fully isolated sandbox environment. This allows users to perform full disaster recovery tests that can also test new applications, patches, upgrades, and configuration changes to ensure that they will function correctly in a live production environment.

Bottom Line

Quorum's appliance can perform automated disaster recovery testing after snapshots in order to ensure recoverability. According to Gartner, the vendor offers complete recovery tools, especially in the use of the appliances when user requirements involve several small sites. While Quorum's costs for implementations of fewer than fifty virtualized servers are higher than the average, existing users praise the performance of the devices as well as the company's customer service and support.

RECOVERYPOINT

Recovery Point provides integrated business continuity and disaster recovery solutions. The provider also has a focus in cloud-based business resilience services. Recovery Point's solutions include Disaster Recovery as a Service (DRaaS), off-site tape storage, managed hosting, and subscription-based hot site, cold site, and work area recovery services. In addition to serving secure federal agencies, the provider's client base also includes commercial customers, and state and local governments. Recovery Point's DRaaS solution can be applied to any size requirement and supports hybrid solutions as well. The vendor is based in Maryland and was founded in 1999.

Recovery Point
75 West Watkins Mill Rd
Gaithersburg, MD
United States
+1 (877) 445-4333
www.recoverypoint.com

Key Features

Total Solutions Visibility

Organizations can choose fully managed or assisted services with complete visibility into their production and recovery environments via redundant management interfaces connected to Zerto's portal. The ability to proactively monitor the environment allows users to discover IT issues before they have an impact.

Security

Data is protected in-flight and at rest through end-to-end encryption. The Virtual Data Center services and Cloud Service catalog facilitate the deployment of security tools and services to protect the user's environment.

Data Loss Avoidance

Backup from Storage Snapshots for technologies such as HPE, NetApp, Veeam Cloud Connect, and EMC Data Domain. This also helps users achieve RPOs of less than 15 minutes. Built-in WAN acceleration allows users to attain lower RPOs for their critical data.

Bottom Line

Recovery Point's DRaaS solution is recommended to U.S.-based organizations with complex recovery needs for x86 or other platforms. The provider has significant experience providing recovery services for non-x86 workloads and mainframes. The vendor's private network infrastructure also functions as a national network hub, giving users the ability to cross connect to more than 700 WAN providers. While Recovery Point's service availability is currently limited to the United States, the vendor provides enhanced Federal Information Security Management Act level protection to all of its users.

StorageCraft provides backup, disaster recovery, and business continuity products for servers, desktops, and laptops. StorageCraft also offers system migration and data protection solutions. The vendor aims to provide reduced downtime and improved security and stability to enterprise organizations. 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 vendor is headquartered in Utah and was founded in 2003.

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

Key Features

Customization

Users can customize cloud storage to fit their environment, regardless of size and complexity. Additionally, they can choose from one of three Service Levels that feature pre-configured or custom Retention Tiers based on the needs of their organization.

Control and Flexibility

Users can centrally manage and monitor all of their StorageCraft Cloud Services accounts and also failover during a disaster without third-party intervention. StorageCraft Cloud Services also mitigates system downtime and data loss through the use of fully virtualized and networked systems in the cloud.

One-Click Failover

Through the use of Virtual Machine Policy, (which is available with Cloud Premium), users have the ability to configure the sequence, order, and timing of every mission-critical system, as well as the capability to press one button to test or begin site-wide failover processes.

Bottom Line

StorageCraft offers localized language support for German, French, Italian, Spanish, Portuguese and Japanese speaking users. The provider also typically serves small to medium-sized businesses. The vendor requires high levels of training for partners to achieve Platinum partner certification. Partners speak highly to the ease of implementation and simplicity of the product. However, buyers should keep in mind that although the vendor will take direct end-user calls, partners are responsible for testing and executing during disaster recovery events.

Sungard Availability Services (Sungard AS) provides managed IT services, information availability consulting, business continuity management software and disaster recovery. The vendor's Disaster Recovery as a Service (DRaaS) solution supports hybrid systems and provides scalability. Sungard AS' recovery services are composed of four portfolio categories: data protection, recovery management, workplace recovery series, and cloud and infrastructure recovery. The provider has recovery locations in the United States, Canada, the United Kingdom, and Western and Northern Europe. Sungard AS also offers its own recovery locations in addition to Recover2Cloud using AWS. The vendor is based in Pennsylvania and was founded in 1978.

Sungard AS
680 E. Swedesford Rd
Wayne, PA
United States
+1 (888) 247-2602
www.sungardas.com

Key Features

Orchestration

Sungard AS's technical support ensures successful test execution and ongoing performance improvements. This enables orderly, large-scale infrastructure recovery using application discovery and dependency mapping, automated change management, and orchestration. These tools can automate recovery tasks at the business application level.

Proactive Testing

With the help of a business continuity consulting team, users can identify business process and technology elements at risk and develop a strategy to mitigate threats. Specifically, the consulting team provides assistance with continuity strategy and planning, risk assessment, and business impact analysis services.

Deduplication

Sungard AS's DRaaS solution supports replication and recovery of vSphere, Hyper-V, Xen, and SAN-to-SAN VM replication for EMC and NetApp.

Bottom Line

Sungard Availability Services is a good fit for organizations that need fully managed DRaaS for complex environments or require global support for heterogeneous platforms. Though the provider struggles to differentiate itself through its AWS-centric approach to public cloud disaster recovery, it has significant experience providing recovery for non-x86 workloads and mainframes. Sungard AS now offers a "Value Scorecard" for its DRaaS customers that can be used as an executive dashboard to show the recovery readiness and maturity of implementations, and also offers additional support for application workloads through its Managed Recovery Program.

TierPoint helps clients deploy disaster recovery, connected data center, and cloud solutions for their overall business continuity plan. TierPoint's Disaster Recovery as a Service (DRaaS) combines features such as replication, cloud, and virtualization technologies, delivering a comprehensive solution that provides the capabilities needed to ensure critical data and applications are safe and secure. The vendor also owns over 40 data centers within 20 markets and 8 multi-tenant cloud pods, all connected via a coast-to-coast network. TierPoint's solution portfolio includes private, managed hyperscale, and hybrid cloud environments.

TierPoint
12444 Powerscourt Dr
St. Louis, MO
United States
+1 (844) 267-3687
www.tierpoint.com

Key Features

Rapid Recovery

Ensures IT continuity and resiliency by providing fast recovery and low RTOs in the event of a disaster or disruption. With flexible options and the ability to continually replicate critical services into the cloud, effectively diverting traffic from the affected environment, your business can meet mission-critical IT infrastructure recovery needs.

Enable Hybrid

Provides management and recovery capabilities across nearly all key applications and platforms to support diverse computing environments. The Resiliency Management Platform enables complete visibility as well as the ability to monitor and control all layers of an organization's disaster recovery infrastructure.

Security and Compliance

Assists in ensuring application, data and system availability and integrity for security purposes. The platform provides users with support to help understand the industry challenges impacting their business and will provide the necessary tools to comply with government and industry regulations required.

Bottom Line

TierPoint's DRaaS approach is based on a consultative partnership with each client in order to develop the solution that fits their client's needs across diverse computing environments. The provider's platform is a good fit for organizations where multiple tiers of services are priorities for medium-complexity environments. The customized solution ensures resiliency for customer data, apps, and infrastructure, thereby minimizing the impact of unexpected interruptions. The vendor offers workspace recovery in some of its locations, as well as cloud and colocation solutions to enable hybrid IT and hybrid resiliency.

Unitrends provides enterprise backup and continuity, as well as high-availability hardware and software engineering. Unitrends also offers several channeldriven recovery products. The vendor's Disaster Recovery as a Service (DRaaS) solution provides built-in automated compliance tests and compares recovery testing results with users' RPOs and RTOs. The Unitrends Recovery Series appliances also provide replication and orchestration, as well as automated recovery capabilities. The company was recently acquired by IT management solution provider, Kaseya. Based in Massachusetts, Untrends was founded in 1989.

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

Key Features

Data Retained On-Premises

Data is retained on-prem in order to quickly recover files, folders, and servers (Unitrends' DRaaS solution supports Windows, VMware and Hyper-V Instant Recovery, and Bare Metal Recovery). This occurs locally while replicating Virtual Machines for recovery in the event of an outage.

Rapid Seeding

As a means to speed up cloud implementation, users can transfer large volumes of data to Unitrends and the company will relocate it to their cloud and then return the user's device. The seeding service is supported by Unitrends Recovery Series physical appliances and Unitrends Backup virtual appliances hosted on Hyper-V, VMware, or XenServer.

Uptime

Improved uptime is achieved by launching applications in the Unitrends Cloud. Through this practice, organizations can continue normal business operations without disruption, even in the event of an outage.

Bottom Line

Unitrends typically serves companies with less than 25 servers. The vendor offers free tools, such as its RTA Calculator, which can be downloaded before purchasing. Unitrends' services are priced competitively, and include automated, monthly full validation tests, along with Recovery Time Actual (RTA) compliance reports. However, buyers may want to ask for details on how the vendor's one-hour RTO guarantee is measured to ensure remedies are understood.

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.