CARBONITE® RECOVER

CARBONITE® an opentext™ company | WEBROOT® an opentext™ company

DRaaS ushers in changes to data protection strategy

Businesses are headed in a new direction with regards to backup and disaster recovery.

DRaaS growth indicates a shift in strategy

As businesses continue to change the way they use and store data, the methods they use to protect the data has changed too. Studies show they're reconsidering traditional backup and recovery while looking more favorably at disaster recovery as a service (DRaaS).[1] With DRaaS, businesses enjoy the luxury of keeping a replica of their data hosted at a remote site that they can fail over to in an emergency—without bearing any of the infrastructure costs or maintenance responsibilities. All infrastructure and maintenance is the responsibility of the provider. There are several reasons for the shift in DRaaS adoption rates:

- Backup applications that were designed for outdated environments and use cases
- Frustration over backup challenges leading to a greater willingness to modernize
- Snapshots and replication taking a more active role in recovery

As adoption of DRaaS increases, companies will find it easier to deploy the right type of protection by determining exactly how much support they may need in a disaster recovery scenario.

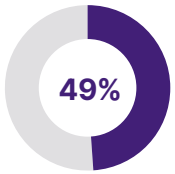
Many businesses rely on self-service software to meet their basic needs. These self-service solutions can be effective for those that have in-house skills for applying the proper configuration settings to meet their recovery objectives, and have resources in place to manage the solution. But other companies need a more assisted option to help with disaster recovery protection monitoring, periodic failover testing, auditing, compliance and hands-on management should a disaster strike.

The challenge for decision-makers is to make sure any solution can, in fact, deliver on the promises of DRaaS.

How DRaaS helps reduce costs

With DRaaS, you don't need secondary hardware to store replicated data for recovery purposes. Limited budgets are forcing IT departments to weigh investments more carefully, and shift spending from capital expenditures to operational expenditures. With DRaaS, businesses can enjoy all the benefits of resilient IT without owning the hardware or being responsible for maintenance. It also frees IT teams from having to keep disaster recovery experts on staff.

In analyzing cost of disaster recovery services, the more important factor to consider is what the cost of downtime or lost data means to a business. According to a recent 451 survey, 30% of respondents reported that they had a significant outage in the past two years. For larger organizations, with over 1,000 employees, nearly 40% experienced an outage in the past two years.[2] The cost of these outages?



Nearly half (49%) experienced losses over $100,000 with larger organizations (10,000+ employees) reporting more than $1m in losses.

Reputation damage is harder to estimate but no doubt real and costly. The high cost of downtime—combined with the changing economics in storage and the growth of public cloud offerings—have made DRaaS attractive for all organizations, from large enterprises down to small businesses. According to Gartner, 40% of the installed base of DRaaS is represented by large and very large enterprises, while 34% is represented by midsize organizations and 26% by small organizations. In most cases, businesses are moving away from an all-or-nothing approach—failing over an entire production center—and transitioning toward a more flexible approach that seeks to achieve selective application failover for critical systems.

Improved recovery with DRaaS

Not all disaster recovery solutions are created equal. Basic core competencies of any disaster recovery solution should include:

- recovery times measured in minutes, not hours, with minimal data loss
- solution is highly automated and orchestrated
- pre-configured network and application settings that allow systems to come online quickly after failover
- non-disruptive testing

Additional features and capabilities are available but the above represents the basic features to expect.

Let's explore them more in detail.

The type and frequency of replication will affect the speed of recovery and the potential for data loss. With traditional backup, bandwidth will determine the frequency and time of day for scheduling backups. In an effort to eliminate disruptions to normal network traffic, IT typically schedules backups for evening hours. A backup schedule of once per evening can result in the potential loss of 24 hours of data. This is often more data loss than a business can tolerate, especially for mission-critical applications.

The type of replication typically found with DRaaS can reduce or eliminate the need for backup scheduling. Not all disaster recovery offerings are the same - some use backup tech to power the solution, and these solutions do not provide real-time, byte-level replication. While byte-level replication is key for achieving ultra-low RPOs and RTOs, snapshots are still important for preserving clean backup data in the event of a virus or device corruption. If a ransomware virus ever penetrates the network, it's important to have a clean point in time to return to without having to pay a bounty. For this reason, historical backups are still an essential component in a data protection strategy.

Support for legacy plaforms

Just because organizations are modernizing at a rapid rate doesn't mean they're abandoning their iSeries and AIX platforms entirely. In fact, the more common use case is to have a combination of modern and legacy systems operating side-by-side in a single, heterogeneous environment. Not all DRaaS vendors support legacy systems, but for businesses that rely on IBM Power platforms, like iSeries and AIX, support for these systems is critical.

Using DRaaS to modernize

In addition to cost savings and IT productivity, DRaaS also has the potential to help organizations modernize their infrastructure gradually, with less risk to the business. A DRaaS solution provides an easy way to move a production workload to the cloud. Once that instance is deployed, it can act as a sandbox for further experimentation. IT can test how application updates may affect interoperability without first rolling out the update in production. And if there are hiccups once the update is rolled out, the cloud instance is there as a safety net. The same holds true for hardware updates. With DRaaS, IT organizations can eliminate the typical downtime associated with integrating new servers into production. Many organizations are deciding they're better off running certain applications in the cloud. This often involves a "lift and shift" operation for moving the application and data to the cloud and then mapping users to the new instance. DRaaS already performs many of these functions in the normal course of configuring and testing the solution. For any organization considering transitioning to infrastructure as a service (IaaS), DRaaS can act as a stepping stone to full virtualization.

Critical questions for DRaaS providers

Getting the most out of DRaaS depends on finding the right combination of tools in a single provider. Gartner suggests 10 strategic questions to ask providers.[2] Each question below is followed by contextual analysis for Carbonite's DRaaS offering.

1 Pricing methodology and storage

"How will the service provider ensure that reductions in monthly storage costs are consistent with storage technology price and performance improvements?"

The Carbonite® Recover offering is structured at a metered price based on storage. Customers only pay for their compute usage if they fail over into our cloud. We offer monthly and annual pricing options, volume discounts and white-glove premium service. Carbonite is committed to excellent customer service and will offer fair market pricing for all solutions and services.

2 WAN

"What topology strategies are recommended, what technical features do you provide today, and what will you deliver in the future with respect to WAN acceleration, compression and deduplication?"

The Carbonite Recover solution is optimized for bandwidth by sending byte-level changes across the wire on an ongoing basis. Carbonite Recover further improves bandwidth by using built-in compression. In the event of a network interruption, Carbonite Recover efficiently resynchronizes by only sending the data that has changed since the interruption. Bandwidth throttling helps minimize the performance impact, both on the servers being protected and on the network.

3 Bare metal

"How will bare metal restores be accommodated in a hybrid configuration?"

Carbonite Recover is engineered for the complex IT environment. Carbonite Recover provides protection and recovery of physical, virtual and cloud-based Windows and Linux severs, with support for legacy systems available through our Carbonite® Disaster Recovery offering.

4 Multiple cloud DRaaS and hybrid cloud management

"What level of support exists for virtual machine storage and activation within other cloud infrastructures (especially hyper-scale) that have compelling service usage pricing advantages? What is on the roadmap?"

Carbonite Recover can currently protect servers running in public cloud environments. Leveraging the infrastructure of large hyper-scale cloud providers (such as Google, Microsoft Azure and Amazon Web Services) as recovery platforms is an option we will continue to explore in order to provide our customers with the highest level of performance and value.

Critical questions for DRaaS providers

Getting the most out of DRaaS depends on finding the right combination of tools in a single provider. Gartner suggests 10 strategic questions to ask providers.[2] Each question below is followed by contextual analysis for Carbonite's DRaaS offering.

5 Software-defined networking (SDN)

"What are the service provider's plans toward bringing SDN, network virtualization and NFV capabilities to DRaaS, and what benefits shall I expect?"

Software-Defined Networking (SDN) is a foundational component of the Carbonite Recover software stack that helps accelerate provisioning resources during onboarding. We will continue to monitor the needs of our customers and provide them with the most cost-effective and flexible networking solutions for their unique IT environments.

6 Copy data management

"What level of role-based visibility and restoration capabilities will be available on the portal, and does it allow for both file and object-level restores for file systems and applications?"

Carbonite Recover brings together continuous replication technology and secure Carbonite cloud. Continuous replication at the file system level offers our customers excellent recovery times and recovery points, measured in minutes or seconds. This "full-server" replication technology alleviates data management problems. For customers needing to recover a few files or folders, the system supports granular restoration options as well.

7 Security

"In 24 months' time, what will be your differentiated strengths when it comes to security in your DRaaS service?"

Security is our top priority, and all Carbonite Recover data is currently secured by AES-256 encryption—both in flight and at rest. Access to the Recover portal uses reCAPTCHA and optional two-factor authentication to secure the user accounts. Carbonite takes security very seriously and will continue to look at ways to assure that the data replicated into the cloud is protected and usable.

8 Containers and micro-services

"To what extent does your service provide support for containers and micro-services — whether for a private on-premises deployment or cloud deployment?"

Carbonite Recover is an ideal solution for customers with limited IT resources and budget, who have historically had to make do with basic backup. While there are benefits to the technologies, containers and micro-services are not widely adopted among our customer base. We will continue to monitor all advancements in the DRaaS market and provide our customers with the most up-to-date technology that fits their environments and budgets.

Critical questions for DRaaS providers

Getting the most out of DRaaS depends on finding the right combination of tools in a single provider. Gartner suggests 10 strategic questions to ask providers.[2] Each question below is followed by contextual analysis for Carbonite's DRaaS offering.

9 OpenStack, big data and real-time data analytics

"What capabilities exist for the recovery of OpenStack implementations and support for on-premises or cloud-based big data or real-time data analytic deployments?"

Carbonite Recover is a complimentary solution to a traditional backup product, for organizations that have limited IT resources and budget, but have critical systems to protect. We have not seen wide adoption of OpenStack capabilities for our target market, but we are committed to providing our customers with a solution that meets the market needs, and as such will continue to add supported target platforms.

10 Increased and differentiated business value

"Relative to the marketplace three years from now, in what areas do you expect to provide more comparative business value from DRaaS deployments, beyond what was captured in the prior questions, and why do you believe your company is best positioned to deliver on the vision? In addition to your own examples, include specific examples around multiuse of DRaaS (such as dev/test), as well as enablement for end-to-end IT resilience management, protection of cloud-native applications and automated planning, management and execution for deployments spanning many."

Carbonite Recover is built upon the same continuous replication technology that our Carbonite® Availability product offers, also at a reasonable price point. This continuous replication promises near-zero downtime for the midmarket, with RPOs and RTOs measuring in minutes or seconds. We will continue to differentiate ourselves in this market by offering broad platform support for legacy systems, premium service offerings to improve ease of use and manageability, as well as key features and functionalities that will improve IT performance. Our future efforts will center on enhancing ease of use, increasing value, and ensuring customers have the right data protection options for their IT environments. We intend to provide additional value to this market by leveraging the complete range of data protection solutions available in the Carbonite portfolio, such as server and endpoint backup.

Carbonite® Recover

Instead of living with the risk of unexpected downtime, companies can trust Carbonite, which offers small and midsize businesses options for disaster recovery that fits any business needs and resources available.

Carbonite® Recover, offered as self-service disaster recovery software, reduces the risk of unexpected downtime by securely replicating critical systems to the cloud, providing an up-to-date copy for failover when needed. Replication from the primary server to the cloud happens continuously at the byte level. When an outage occurs that exceeds a pre-established failure threshold, businesses can immediately fail over to the secondary environment. Total downtime or RTO is measured in minutes, and the recovery point, or RPO, is only seconds old, virtually eliminating the impact of the outage.

For businesses that require a more hands-on approach, Carbonite combines Carbonite Recover with a remotely monitored and managed service to help you protect your critical systems. The Carbonite® Managed Disaster Recovery service includes initial setup, software deployment, ongoing management and validation. This ensures that the disaster recovery solution is operational and performing as epxected.

How It Works

The Carbonite® Managed Disaster Recovery service includes not only the initial setup and deployment of Carbonite® Recover software but also ongoing management and validation that the disaster recovery solution is functioning correctly, ensuring the business can be brought back online in the event of a disaster.

Delivered by the Carbonite Professional Services Team, Carbonite Managed Disaster Recovery service focuses on the areas of monitoring, reporting, testing, maintenance, and disaster recovery failover initiation and support.

Carbonite Recover is offered as a term-licensed subscription service with pricing based on the overall size of the protected data footprint. Carbonite Managed Disaster Recovery service is available as an add-on to the Carbonite Recover software fees on a per server basis that matches the contract in servers and length. Our managed services apply specifically to server protection jobs, monitoring, testing, live failover and failback. Production network management remains the responsibility of the end-user.

Benefits include:

- Continuous, real-time replication for always-on data protection
- Recovery times (RTO) measured in minutes, and recovery point (RPO) in seconds, reducing the risks of lost productivity and revenue
- Push-button failover and failback reduces complexity surrounding moving workloads to and from the cloud
- Optional professional services support from initial deployment and testing and full DRaaS managed services
- Optional managed service provides software maintenance and upgrades, assistance with compliance auditing, and industry certification or regulation needs

Smart and strategic data protection

The two most common roadblocks to effective disaster recovery are inaction and settling for a solution that is “good enough.” Disaster recovery options that meet the specific needs of your business and meet basic competencies are key in making the right decision.

The methods and technologies that allow IT organizations to protect their investments have evolved to offer more levels of protection with far easier implementation and much faster time-to-protection. While DRaaS was once a high-maintenance and prohibitively expensive proposition, that is no longer the case.

Many businesses have decided that, while their data is crucial for their success and survival, it’s not necessary to invest in a secondary data center as a precaution. The emergence of inexpensive storage combined with advancements in data protection change the way IT decision-makers think about backup. It’s now far easier and more cost effective to ensure high availability for critical applications through DRaaS while protecting secondary and archival systems through traditional backup. This explains recent trends indicating a greater reliance on DRaaS and the strategic use of backup as part of a holistic data protection strategy.

[1] Gartner: Predicts 2016: Business Continuity Management and IT Service Continuity Management
[2] 451 Research, With costly outages on the rise, disaster recovery is still a top issue, August 2020.

Contact us to learn more – Webroot US

Email: wr-enterprise@opentext.com

Phone: +1 800 772 9383

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That’s why we’ve combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.