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

Buyer's Guide

DRaaS Features & Functionality

Disaster recovery that fits any business

Disaster Recovery for the Mid-Market

When a critical system goes down, whether from ransomware, natural disaster or human error, businesses suffer lost revenue and productivity until normal operations resume. The fastest way to recover is to mirror the workload on another server often at a secondary location. But for most businesses, the redundant hardware, data center space and additional IT resources are too costly to make this a viable option, leaving many small and medium businesses unprepared in the event of a disaster. With few resources available to manage a full disaster recovery program, many businesses rely on self-service software to meet their basic needs. These self-service solutions can be effective for those with in-house skills for configuring a disaster recovery environment and the resources to manage it. But many companies need a more assisted option to handle more complex tasks, like monitoring, periodic failover testing, auditing, compliance and hands-on execution should disaster strike.

Today, instead of living with the risk of unexpected downtime, small and midsize businesses have options available for implementing a disaster recovery approach that fits their business needs and fills any gaps in resources that may exist.

This guide offers tips on key features and functionality that, when provided in a disaster recovery solution, can give you the benefits of having a secondary site —without many the infrastructure or administrative costs.

Disaster Recovery Myths

Myth: DRaaS is only for the enterprise.

Fact: Traditional DRaaS requires an offsite location, one that only large enterprises can afford. But technology advancements and the availability of inexpensive public clouds enables even small and midsize businesses to enjoy the same level of protection.

Myth: Backup is enough.

Fact: Traditional backup times do not provide the rapid RPO and RTO needed for true disaster recovery. DRaaS gives you a secondary site that you can run on while you perform disaster recovery on your primary site.

What to Look for in a Disaster Recovery Solution

What	Why
Continuous replication	Achieve recovery times measured in minutes and recovery points measured in seconds.
Self-service or managed testing	Feel confident that your DRaaS solution will work when a disaster occurs.
Orchestration for multi-tier applications	Ensure applications are failed over seamlessly and reconstructed correctly.
Automated discovery	Reduce the number of manual steps required and the likelihood of human error.
Bandwidth optimization	Maximize performance and bandwidth by only sending small amounts of data on an ongoing basis.
Recovery point options	Recover to the most current replicated data or fail back to a specific point in time.
DNS redirect	Automatically update DNS and redirect requests to the new system.
Failback	Get systems and data back to the production site once the issue has been resolved.
Built-in encryption	Maintain security with encryption in flight and at rest in the cloud.
Built-in encryption	Keep legacy applications like iSeries, AIX and Solaris systems protected during an outage.
Professional support	Don't do it alone. Make sure there's a team of experts available.

Buying Tips

Since different systems require different levels of protection, it is important to align your recovery objectives for each system with the right level of data protection. After you have established which systems require immediate failover, set up a technical demo. During the demo, ask about the recovery performance of the solution, and whether it enables you to easily run a test failover when you need to. We recommend businesses perform test failovers once a quarter.

At the end of the demo, ask about customer support and determine whether a premium support option would best fit your business needs. Because disasters don't follow a schedule, it's important to have the resources available when you need them. Before you end your call, ask whether the vendor can protect less critical systems as well. A complete data protection strategy incorporates both high availability and traditional backup. Having a single data protection provider can save time and money.

The Carbonite Advantage

With Carbonite® Recover, replication from the primary server to the cloud happens continuously at the byte level, which is highly efficient on the network. The replica at the secondary cloud location is constantly synchronizing with the source, ensuring the currency of the data. When there's an outage that meets the pre-established failure threshold, there's an option to immediately fail over to the cloud-based replica. The total downtime or RTO is measured in minutes, and the recovery point or RPO is only seconds old, virtually eliminating the business impact of the outage.

Once configured, systems send data continuously to the Carbonite cloud at the byte level, minimizing any performance impact to the systems or the network, and without the need for specialized resources to configure, maintain and operate the disaster recovery environment.

Key features:

- Automated discovery of systems in your environment
- Non-disruptive, self-service testing and reporting
- Orchestration and failover scripting support for multi-tier applications
- Bandwidth-optimized for limited network impact
- Built-in encryption both in flight and at rest
- Multiple recovery points using historical snapshots
- Replicates between disparate physical, virtual and cloud-based systems

Supported Platforms:

- Windows
- Linux
- VMware and Hyper-V

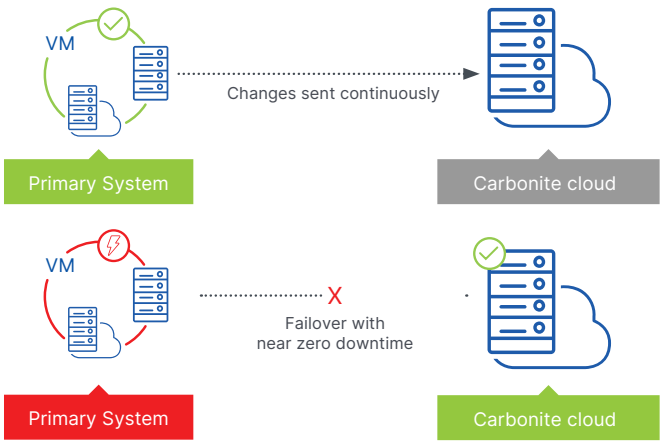
Carbonite® Managed Disaster Recovery Service

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 not only the initial setup and deployment of Carbonite Recover software, it also provides ongoing management and validation that the disaster recovery solution is functioning correctly, ensuring the business can be brought 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. The service is available as an add-on to Carbonite Recover software fees on a per-server basis that matches the contract in servers and length.

Carbonite Managed Disaster Recovery service applies only to the Carbonite Recover software and server availability components and does not include infrastructure services, network services, infrastructure monitoring, application monitoring, application services, application uptime, user availability, application maintenance or upgrades.



Managed service features:

- Daily monitoring to validate that systems are online and protected
- Reporting includes a weekly uptime/protection report that shows the health of the job as well as any issues that were corrected and the remedy to that issue; and a bi-annual report as part of the quarterly testing cycle with demonstration of failover that will assist in meeting audit needs.
- Testing capabilities can be performed without any impact to the customer environment, with the most critical being bi-annual testing of all servers under management, resulting in after-action reporting that shows servers brought online in a test mode and how long failover took.
- Software maintenance and upgrades for Carbonite software is included and will be performed within 30 days of release. Disaster declaration and failover where, in the event of a disaster, the customer would contact Carbonite to declare a disaster for their environment, initiating the escalation process defined by their SLA. The site would be failed over and brought online in the Carbonite cloud.

Contact us to learn more – Carbonite US

Phone: 877-542-8637
Email: carb-data_protection_sales@opentext.com

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.