CARBONITE an opentext company | WEBROOT an opentext company

Five reasons to choose DRaaS

Find out five good reasons to consider disaster recovery as a service (DRaaS) and use our buyer's cheat sheet to make sure you are asking the right questions when evaluating a DRaaS solution.

Defining DRaaS

Disaster recovery as a service (DRaaS) is rapidly gaining popularity, and is offered by an increasing number of service providers.

The simplest way to define DRaaS is a third-party managed service provider (MSP) providing a remotely hosted disaster recovery service to protect your data and applications. The range of DRaaS varies greatly from provider to provider. Most are offered under a plan whereby disaster recovery software is hosted by an MSP and licensed to users on a subscription basis.

The level of recovery capability can vary. A DRaaS offering can protect just data files, one or more critical applications, a single server, or every server in the data center. But replication to the MSP's disaster recovery site is always required, and a common component to these solutions.

How data or servers are recovered, and how quickly they can be recovered, can vary also. Some solutions, in addition to replicating the server and application data in real time, take over processing

functions immediately in order to provide a lower recovery time objective (RTO). This ensures the server's program and operating system (OS) settings are also replicated continuously and that applications on existing cloud-hosted VMs can be activated immediately. That means a DRaaS solution might automatically provision an entirely new VM—recovered, configured, and activated—within a few minutes.

Five reasons to consider DRaaS

When deciding on DRaaS as a strategy for your IT shop, it can be helpful to examine the chief benefits. Here are the top five reasons to consider DRaaS:

1. Reduce DR costs

If you currently have a secondary site for disaster recovery purposes, then you are already familiar with the high costs associated with it. Beyond the unavoidable investments in replication software and the required software licenses for servers, storage, and security, there are a number of significant additional costs. Most of these additional costs are effectively eliminated by using DRaaS through an MSP:

A DRaaS offering eliminates the need for the following expenses:

- Owning or leasing space for your secondary data center
- Monthly costs associated with power, cooling, and internet bandwidth at the secondary site
- Purchase or lease of servers, storage, and network equipment for the secondary site
- Travel to and from data centers or onsite staff at the secondary data center

2. Reduce complexity

As demonstrated in the list above, building and maintaining a secondary DR site can be both costly and complex. If all of that infrastructure could be eliminated, then the administration, upgrade requirements, and maintenance contracts could be eliminated as well.

3. Achieve interoperability

DRaaS solutions work with dissimilar systems so that you can protect servers across different hypervisors and replicate data between dissimilar storage systems. These DRaaS solutions are hardware-, hypervisor-, and application- independent.

4. Reduce IT resources spent on DR

If you have yet to deploy your own disaster recovery site, you'll be able to deploy DRaaS within hours or days (depending on the number of servers) as compared to the weeks or months it can take to deploy your own site. And by reducing complexity and simplifying your DR solution with a single provider, IT groups will save a tremendous amount of time—when compared to managing their own DR site.

5. Provide a comprehensive DR solution

Many times companies who implement their own disaster recovery site have to start by protecting the most critical servers first. In some cases, they are never able to protect all their servers. Because DRaaS is much easier and more affordable than do-it-yourself DR, many companies are able to protect all of their servers (physical and virtual) within a reasonable time frame and budget.

Cheat sheet: choose the right DRaaS solution

1. Multi-platform support

Make sure that all of your physical, virtual, and cloud-hosted production servers can be protected.

2. Multi-cloud support

You should be able to use more than one cloud service or platform concurrently (e.g., AWS, Azure, Google, etc.) to mitigate the risk of your cloud service suffering a major outage. This also frees you to switch from one cloud service vendor to another in the future.

3. Cloud failover

Rather than having just a recoverable backup image in the cloud, you want to be able to actually switch all your critical operations to your cloud backup servers in the event of a disaster.

4. Flexible licensing

Your technology provider should offer DR with subscription-based, service-oriented licensing and billing options.

5. Real-time replication

True real-time replication captures changes as they happen, eliminating the risk of losing critical data.

6. Scalability

Your DRaaS solution should be able to grow as you grow, whether you are a small business with just a few servers or your data center is expanding to thousands of physical and virtual machines.

Summary

Carbonite provides data protection solutions for businesses and the IT professionals who serve them. Our product suite provides a full complement of backup, disaster recovery, and high availability solutions for any size business in any location around the world, all supported by a state-of-the-art global infrastructure.

DRaaS solutions built on Carbonite DoubleTake™ provide the ability to respond on demand to all your workload protection and recovery needs with a single easy-to-manage technology. Best of all, Carbonite DoubleTake solutions support even the most scalable hypervisor and cloud computing technologies by enabling many-to-one protection of physical, virtual, and cloud-based server workloads.

Contact us to learn more – Carbonite US

Phone: 877-542-8637

Email: carb-data_protection_sales@opentext.com

[1] Footnote

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.