

DRaaS levels the playing field for IT

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



DRaaS growth indicates a shift in strategy

The core technology behind Disaster Recovery as a Service (DRaaS) has evolved for decades. More recently, DRaaS has linked to the cloud, and finally hit its stride. Today it can provide unprecedented availability options to companies who don't have secondary data centers dedicated to business continuity. Before now, only IT teams with additional IT budget, staff and geographic locations could effectively hedge against downtime, and disasters.

But today's DRaaS means that businesses of all sizes have the peace of mind that comes with knowing a replica of their data and systems is hosted at a remote site that they can fail over to—without bearing any of the infrastructure costs or maintenance responsibilities. All infrastructure and maintenance is the responsibility of the DRaaS provider. And the technology ensures that a replica is not only available, but always current and immediately available. This attractive value proposition led Gartner to predict that global DRaaS revenue will reach \$3.4 billion by 2019¹.

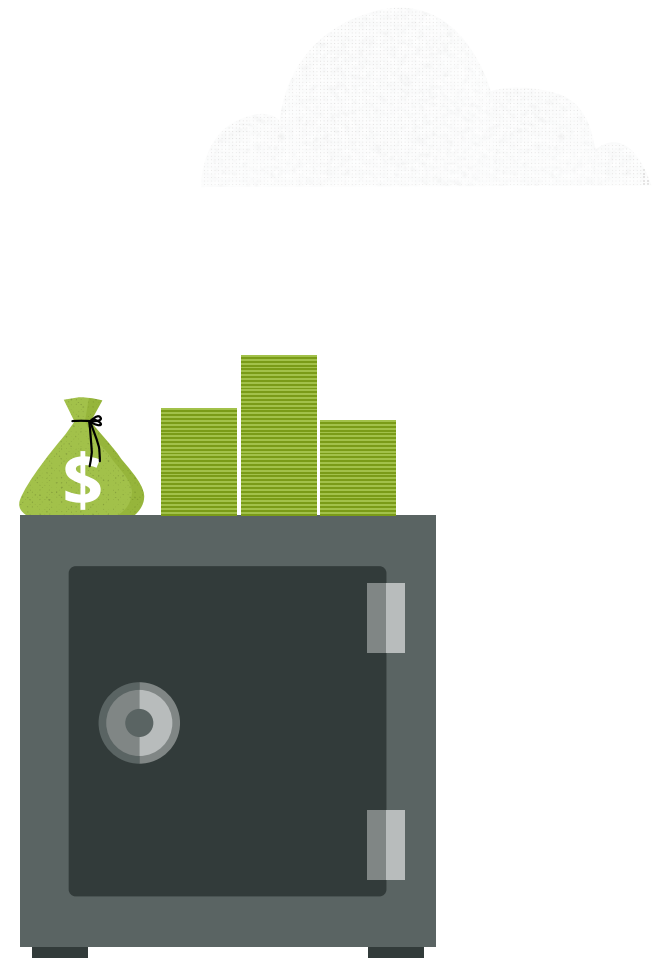
As the DRaaS market heats up, end users are finding that different DRaaS providers offer different service levels. While most offer cloud failover, they differ in the degree of self-management required to configure protection, perform recovery and execute test failovers. There are also different levels of dependency mapping and orchestration available, which can affect the speed of recovery. The challenge for decision-makers is to make sure any solution can, in fact, deliver on the promises of DRaaS.



How DRaaS helps reduce cost

With DRaaS, you don't need secondary hardware to store replicated data for recovery purposes. Stagnant 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.

Several reports from analyst firms like Gartner, Forrester and Aberdeen highlight the escalating cost of downtime for today's data-dependent businesses. While methodologies and calculations vary, according to most, the cost of an hour of downtime runs in the thousands for small businesses, tens of thousands for midsize businesses and hundreds of thousands of dollars for large enterprises. 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 a Big Bang 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

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. Since DRaaS sends data continuously, the amount of data traveling over the wire is much smaller, which reduces the impact on the network. Agents capture changes at the byte level, ensuring that only very small amounts of data are sent. Minimizing the amount of data traveling over the wire enables businesses to reduce the potential for data loss down to the time it takes for data to transmit. With DRaaS, a business can conceivably reduce its recovery point objective (the amount of time elapsed since the last recoverable backup) down to seconds.

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 platforms

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.

Question #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.

Question #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.

Question #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 x86 servers, with support for legacy systems available through our Carbonite Disaster Recovery offering. By pairing Carbonite Recover for Windows and Linux systems with Carbonite Disaster Recovery for legacy environments like AIX and iSeries, customers can ensure complete data protection and minimize downtime across their entire IT footprint.



Critical questions for DRaaS providers [cont.]

Question #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.

Question #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 will provide them with the most cost-effective and flexible networking solutions for their unique IT environments.

Question #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 the continuous replication of our DoubleTake technology and the 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.



Critical questions for DRaaS providers [cont.]

Question #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.

Question #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.

Question #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.

Question #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 DoubleTake 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

Carbonite Recover is designed to leverage the scalability and flexibility of the cloud to deliver cost and operational efficiencies no matter the current state of your IT infrastructure. Our DRaaS offering is specifically engineered to support the blended data protection strategy recommended by industry analysts. While many DRaaS offerings are complicated, Carbonite's is built for simplicity.

Carbonite Recover helps businesses enjoy all the advantages of having a secondary copy of critical data available for failover in the cloud, without any of the hassle associated with managing a secondary data center or colocation facility. This keeps both downtime and costs to a minimum, while strengthening resiliency where it's needed most.

Carbonite Recover is designed to support complex environments. It automates the orchestration of multi-tier applications to ensure proper boot order across groups of servers when applications are reconstituted. Using continuous byte-level replication, Carbonite Recover minimizes performance impact, both on the servers being protected and on the network. All data is secured by AES-256 encryption, both in flight and at rest. During a failover, Carbonite Recover automates DNS updates to seamlessly redirect your users to the new systems. With Carbonite Recover, total downtime (or RTO), is measured in minutes, and the recovery point (RPO) is only seconds old, virtually eliminating the business impact of the outage. Carbonite Recover enables IT to perform regular, self-service testing without causing any disruption in production. The entire solution is simple from configuration to failover and failback. Plus, our award-winning professional services team is always available to troubleshoot and help test the solution.

How it works

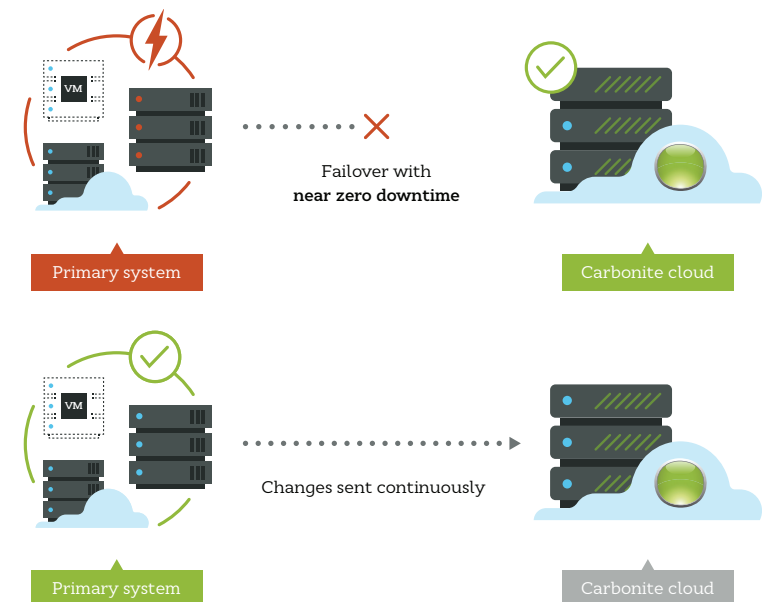
Central console – From the console, you can choose the source system you want to protect and automatically push the software agents to the source and target, and configure protection.

Real-time replication – Once configured, as changes occur at the source server, they're sent continuously at the byte level to the Carbonite cloud, keeping the source and secondary target perfectly synchronized.

Push-button failover – If an outage occurs, you can trigger a failover from the Carbonite console. Users are rerouted to the secondary server, usually within minutes. When the underlying issue is resolved, simply fail back to the original source or replacement hardware.

Professional support – Our award-winning professional services team will walk you through the configuration process and help you perform your first test failover.

System support – Carbonite Recover, combined with our Carbonite Disaster Recovery service, can support a wide range of operating systems and applications, including IBM iSeries and AIX, Solaris and Linux and modern virtual platforms like VMware and Hyper-V.



Smart and strategic data protection

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 cheap storage—combined with advancements in data protection—changes 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.

Contact us to learn more

Phone: 877-542-8637

Email: DataProtectionSales@carbonite.com

¹ Gartner: Predicts 2016: Business Continuity Management and IT Service Continuity Management

² Gartner: 10 Strategic Questions to Ask Potential DRaaS Providers

