CloudEndure

Finally, Affordable Enterprise-Grade Disaster Recovery Using the Cloud

Until recently, enterprise-grade disaster recovery had been prohibitively expensive for most organizations. Thanks to the rapid development of cloud infrastructure, organizations can now attain top-of-the-line disaster recovery capabilities at a fraction of the cost.

An enterprise-grade disaster recovery (DR) solution is no longer something that is "nice to have." Neither can it be a 50-page document that was approved by the Board of Directors but nobody has touched or tested in years. Why not? Just ask Delta Airlines. A mere 5-hour outage that took place in August 2016 cost Delta over $150 million.

The Challenge

The airlines are not alone, of course. If your organization is like any large-scale business today, you understand the critical need to recover rapidly from IT outages, application failures, or malicious attacks in order to ensure business resilience, stay competitive, and avoid regulatory risks. Not only do your employees need to access company systems 24/7, but your global customers also expect constant availability. And if they don't get it, get ready for outage outrage -- a worldwide social media phenomenon that can ruin an enterprise's hard-earned reputation overnight.

So what's the problem? Why don't all enterprises have airtight, 100% reliable business continuity disaster recovery strategies in place? Can't IT departments just set up multiple data centers that continually replicate workloads, and when a disaster strikes, redirect to the DR site?

It turns out that for many organizations, enterprise-grade DR -- with near-zero RPO and RTO -- is prohibitively expensive due to heavy capital expenditures (CAPEX) and/or expensive third-party software and services. As a result, some organizations choose to take the risk of having only a backup system, which can save data but cannot prevent costly downtime due to long recovery times. Other companies choose to protect only the most essential servers, which at the end of the day leaves their business vulnerable. Some companies lay out a huge initial investment in DR, but then forget about it in order to dedicate resources to more pressing IT needs. But "set it and forget it" doesn't work for DR -- a system that quickly becomes obsolete if not tested frequently.

The solution to this weighty challenge lies in the cloud. Today, **businesses can attain top-of-the-line IT resilience at a fraction of the cost** by moving their DR to a public cloud platform.

In this white paper, we will examine the three main DR strategies that are currently used by enterprises -- **On-Premise Disaster Recovery, Disaster Recovery as a Service (DRaaS), and Cloud-Based Disaster Recovery** -- with a focus on the expected costs of each strategy. We will also touch on the benefits and risks of each strategy.

So if your organization is still trying to figure out if it's really worth it to move your DR to the cloud, or wants to know the best way to leverage the cloud for DR, this white paper is for you.

On-Premise Disaster Recovery

Handling IT disaster recovery internally is what enterprises have traditionally done. To keep a robust on-premise DR solution in place and up-to-date requires a large investment of resources.

Hardware: Most on-premise DR strategies depend on the purchase of duplicate servers on-site or at a secondary location to be used in the event of an outage. These servers incur both CAPEX and ongoing IT operating expenses (including power and cooling). Moreover, they typically require a hardware refresh every three to five years.

Software Licenses: In order to launch your recovery machines when source machines fail, on-premise DR solutions commonly require maintaining duplicate third-party software licenses and, in some cases, application or DR-specific replication software. This can lead to unexpectedly high expenditures, especially for enterprises that use costly applications such as Oracle, Microsoft, or SAP, just to name a few.

DR Infrastructure & Services: Any IT resiliency solution needs to be able to restore entire systems to their pre-disaster state. On-premise DR solutions require the purchase of data protection software and, in certain cases, replication appliances. If the organization needs enterprise-grade RTO and RPO, they will have to pay for duplicate compute and storage infrastructure in their DR site.

Management & Monitoring: IT staff resources are necessary to continually manage and monitor the DR hardware, software, and infrastructure.

Disaster Recovery as a Service

In light of the high costs and expertise needed to implement on-premise DR, many organizations turn to third-party Disaster Recovery as a Service providers to administer failover support in the event of a disaster. The quality of this kind of DR service depends on the particular DRaaS provider's technology, processes, and service-level agreements (SLAs).

Hardware: When using DRaaS, organizations do not need to purchase duplicate servers or maintain a duplicate data center on their own. Rather, their duplicate servers are located in data centers or colocation centers run by the DRaaS providers.

Software Licenses: Depending on the applications protected and replication methods used, organizations may still need to purchase duplicate licenses for their applications if they want them to be available quickly during a disaster.

DR Infrastructure & Services: Given the underprovisioning of hardware based on the assumption that not all customers will require failover at the same time, DRaaS providers are normally able to offer lower costs for standby machines as opposed to an on-premise DR implementation. Nonetheless, a DRaaS provider's ability to underprovision servers effectively is negligible compared to the economies of scale provided by public cloud providers, and is therefore still very costly. This does not even take into account the added costs associated with third-party application licenses that may be required depending on the replication method being used.

Management & Monitoring: Organizations rely on their DRaaS provider to handle most of the management and monitoring of their DR site. While they do not have to pay for additional on-premise IT staff, they do have to pay their DRaaS provider. Such costs differ among the various vendors.

Cloud-Based Disaster Recovery

The real revolution in disaster recovery began a few years ago with the advancement of cloud technology and the enormous growth of public cloud infrastructure, which al-

Table 1: Cost* Comparison of 3 Disaster Recovery Strategies

	Small Enterprise			Large Enterprise		
# of servers	250			750		
DR Strategy	On-Premise	DRaaS	Cloud-Based	On-Premise	DRaaS	Cloud-Based
DR Hardware	$1,997,000	$378,000	$39,000	$6,818,000	$1,309,000	$118,000
DR Infrastructure, Licensing, & Services	$1,284,000	$984,000	$205,000	$4,500,000	$3,237,000	$532,000
Total	**$3,281,000**	**$1,362,000**	**$244,000**	**$11,318,000**	**$4,546,000**	**$650,000**

*Estimated annual cost

lows you to pay only for what you use. In parallel, replication technologies evolved to leverage cloud infrastructure in a cost-effective manner, forming a "perfect marriage" between DR and the cloud. As a result, organizations can now achieve enterprise-grade DR at a dramatically lower cost than was previously possible. There are numerous cloud-based DR technology vendors. Top-of-the-line solutions provide enterprise-grade agnostic protection for any application or database, without any impact on your servers. When evaluating a solution, make sure to ask the right questions about the software capabilities and limitations based on your environment details and recovery objectives.

Hardware: As is always the case when using the public cloud, no hardware is needed and you only pay for what you use, when you use it. This means no CAPEX investment or unnecessary duplicate provisioning of resources. Only pay for a lightweight "replication staging area" to keep your server data in sync during normal operations, and get billed for your actual recovery environment only when you decide to launch it.

Software Licenses: One of the easily overlooked but quite significant cost savings factors of using the cloud and an appropriate replication tool for disaster recovery is eliminating the need to purchase duplicate software licenses for your standby DR site. The reason for this is that when an appropriate replication technology is used, there's no longer a need to maintain a duplicate standby system with a standby license (of an Oracle DB, for example).

Instead, servers are kept in real-time sync in a dormant "staging area" that is not running any licensed OS or application. In the event of a disaster or a DR test, you may launch your servers within minutes and only then require the third-party OS and application licenses. In other words, you get the resilience of a highly available system with near-zero RPO and RTO, at the cost of a cold standby solution.

DR Infrastructure & Services: Whereas traditional enterprise-grade DR solutions require duplicate compute and storage infrastructure provisioned in the DR site, cloud-based DR keeps an organization's workloads in real-time sync using lightweight compute and storage, so that you only pay for fully provisioned workloads in the event of an actual disaster, thereby dramatically cutting DR costs.

Management & Monitoring: Cloud-based DR solutions normally leverage the elasticity of the cloud and provide much better automation for DR, which means fewer IT resources are required to launch or maintain the service. Automated machine conversion technologies ensure that the heavy lifting typically involved in converting machines from one infrastructure to another is rapid and simplified. As a result, machines can boot natively in the designated target DR infrastructure even if it originated from a dissimilar infrastructure.

Lastly, automated orchestration of the application stacks, which can be done in advance during the implementation stage, eliminates the need for time-consuming, manual network configurations during a disaster.

Additional Benefits of Cloud-Based Disaster Recovery

While it is clear that cloud-based disaster recovery is the least expensive approach, you may be wondering whether this "cheaper" option is as effective and enterprise-grade as an on-premise or DRaaS solution. The answer is yes. Not only does cloud-based disaster recovery provide top-of-the-line DR, but it provides capabilities not available with other strategies, including:

Table 2: Breakdown of DR Infrastructure Costs*: Warm Standby DR vs. CloudEndure Lightweight Staging Area DR

	Warm Standby DR	CloudEndure DR
Compute	$48,000	$228
Storage	$10,200	$3,000
OS Licenses	Windows, RHEL, SLES, Oracle Linux, etc.	$0
Third-Party Application Licensing	Oracle DB, Sharepoint, Exchange, SAP, etc.	$0
Total	**$58,200 + OS and application licenses**	**$3,228**

*Estimated annual costs

- **Easy Testability** -- Quickly spin up machines for your periodic DR drills without disrupting your source environment.
- **Self-Service DR** -- Configure your cloud environment, replicate your servers, and perform your DR drills whenever you want. Deployment is easy, and access to cloud resources is instantaneous.
- **Flexibility Between Infrastructures** -- Protect physical, virtual, or cloud-based machines; use the public cloud of your choice; and easily move to a different cloud provider if desired.

FAQs About Cloud-Based Disaster Recovery

For some enterprises, moving DR to the public cloud may seem like a radical move. However, in recent years, more and more enterprises, government entities, and flagship academic institutions have moved to the public cloud. The leading public cloud platforms have matured and now offer enterprise-grade security, compliance, and data integrity. As such, many organizations have declared cloud-first initiatives to outsource infrastructure to the public cloud wherever possible, with DR being one of the first candidates.

The technology you choose for your cloud-based DR can vary greatly from one vendor to another. Some solutions cannot guarantee consistency or support all of your applications, which would impact your implementation success rate. Other technologies may impact your server performance or deliver inadequate RPO or RTO. The right technology, however, will enable you to achieve the enterprise-grade resilience and performance of on-premise and DRaaS solutions, but with the dramatic cost reduction of the cloud.

Below, we address some of the concerns you may have specific to disaster recovery in the cloud as well as questions to consider in order to choose the right technology for your enterprise.

What RPO can I achieve when using the cloud to protect my workloads? How much data loss might I experience during a disaster?
When using continuous block-level replication technologies, you should expect near-zero RPO (normally seconds), depending on the latency and network quality between your source servers and the cloud.

What RTO can I achieve when using the cloud for DR? How long will it take me to recover into the cloud during a disaster?
Two key capabilities that enable quick recovery into the cloud are automated conversion of your source server from any infrastructure into the appropriate public cloud format and mass-scale DR orchestration. Cloud-based DR technologies that include these two capabilities deliver recovery times of minutes, and can launch your target servers in parallel on a mass scale.

Can a cloud-based DR solution support my physical and virtual machines? What about legacy applications?
Replication must be done at the OS level (rather than hypervisor or SAN level) in order to support any type of infrastructure, including physical, any type of virtual hypervisor, cloud-based, colocated servers, etc. When the replication is conducted at the block-level, any file system or application is transparently supported. Common workloads include the suite of databases and applications from vendors such as Oracle, SAP, and Microsoft.

Is it possible to use the cloud for disaster recovery without moving my primary workloads to the cloud?
Yes, of course. When you use the cloud for disaster

Table 3: Features & Benefits of 3 Disaster Recovery Strategies

	On-Premise	DRaaS	Cloud-Based
Enterprise-Grade	✓	✓	✓
Total Cost of Ownership	High	Medium	Low
One-Touch Deployment & Maintenance	✗	✓	✓
Easy Testability	✗	✗	✓
Easy Scalability	✗	✓	✓
Self-Service DR	✗	✗	✓
Flexibility Between Infrastructures	✗	✗	✓
Software-Defined DR Site	✗	✗	✓

recovery you are simply making a dormant copy of your workloads in the cloud, which can then be launched whenever you choose to do so.

Isn't putting my DR in the cloud a security risk?
As long as your cloud DR solution uses proper data-at-rest and data-in-transit encryption, your data is secure. It is also important to ensure that the cloud provider you use as a DR target for hosting your data meets the regulatory compliance relevant to your business. Finally, if desired, ensure that your DR solution allows you to be in control of the data path for the replication traffic over your private networks.

Won't setting up DR in the cloud disrupt my source system?
This entirely depends on the solution. Some cloud-based DR solutions require rebooting your system, take frequent snapshots, and may impact system performance or require local storage at the expense of your primary applications, while others are designed to be non-intrusive.

How can I conduct DR drills with a cloud DR solution?
DR drills are much easier when using cloud. When using an on-premise or DRaaS DR strategy, you have to ensure that the resources needed for the drill are provisioned and paid for in advance. In some cases, initiating a DR drill requires disrupting your source applications to avoid network conflicts.

When using cloud for DR, you can simply request the resources when needed, and only pay for them upon usage. Furthermore, you can spin up your DR servers easily in complete isolation, thereby performing DR drills without any impact or conflict with your source applications.

If I run my DR servers in the cloud, once the disaster is over, how time consuming and costly will the fail-back be into my on-premise facility?
With some solutions, this can be a cumbersome manual process of setting up your source servers and applications from scratch, moving the data, and then keeping it in sync until the point of failback. Other solutions allow you to simply reverse the replication directly, and keep the data in real-time sync back to your on-premise site until you're ready to flip the switch and failback within minutes.

What if my servers experience a virus, hacker, or ransomware attack that compromises my data, or a mere database corruption that requires me to recover to a previous point in time. Is point-in-time recovery possible?
With the appropriate cloud-based DR solution, you can recover back to previous consistent points in time.

CASE STUDY

ClickSoftware

Time Matters: CloudEndure DR Solution Cuts ClickSoftware's RPO From 24 Hours to "Last Transaction"

Company Background
Founded in 1996, ClickSoftware offers automated mobile workforce management and service optimization solutions to a range of customers including Best Buy, HP, and Liberty Mutual.

The Need
In 2011, ClickSoftware began selling its products as SaaS offerings, expanding its customer base and the amount of data being entered into its platforms. Although the company's homemade disaster recovery (DR) solution had initially served them well, they could no longer afford to risk a day's worth of data by relying on snapshots to back up information. It was clear that they needed an enterprise-grade DR solution.

The Solution
ClickSoftware knew that they wanted to use AWS as its DR infrastructure, and a system integrator recommended CloudEndure for its enterprise-grade DR solution that was easy to integrate into AWS.

After implementing CloudEndure DR, it didn't take long for ClickSoftware to see the value in CloudEndure's continuous replication to the cloud, which took less than five minutes to begin and created an exact replica of all the company's workloads without disrupting performance.

ClickSoftware now has a cost-effective and reliable cloud-based DR solution. Its customer data is in safe hands and won't be lost during a disaster. Annual DR drills are no longer a source of concern thanks to CloudEndure's non-disruptive, easy-to-launch drills. And the DevOps team no longer has to pull out large log files and copy details of the smallest of data transactions.

In Their Own Words
"One of the things I love about CloudEndure is that it replicates not only the machines and data, but the entire application stack. And with CloudEndure we were able to move from losing up to a day's worth of data to what we call 'up to the last transaction.'"
-Igal Korach, Director of Cloud Operations at ClickSoftware

CloudEndure™

Disaster Recovery & Live Migration to the Cloud

Mobilize any workload to the cloud and back, cutting infrastructure costs by up to 85%.

About CloudEndure

CloudEndure provides Cloud Migration and Cloud Disaster Recovery for any application, allowing companies to mobilize entire applications with their data to and across clouds with near-zero downtime and no data loss. CloudEndure enables truly consistent, block-level, real-time replication using continuous data protection. Founded in 2012, CloudEndure's Cloud Workload Mobility technology creates an exact copy of the entire application at an alternative cloud location — at the touch of a button, within minutes, and with the latest data. CloudEndure supports physical, virtualized or cloud-based applications as the source and Amazon Web Services (AWS), Google Cloud Platform, Microsoft's Azure and OpenStack as target cloud locations. For more information, visit www.CloudEndure.com.

Discover how CloudEndure can help your organization achieve affordable enterprise-grade disaster recovery using the cloud.

Contact Us Now