ExaGrid Tiered Backup Storage
Disaster Recovery in the Cloud

Many organizations own and run their own data centers. As a result, data backup is run locally using a backup application to a disk-based backup appliance with data deduplication. For offsite disaster recovery (DR), there are many options depending on the requirements, whether an organization has a second data center, and whether a capital equipment budget (CAPEX) or operating expense budget (OPEX) will be used. The options are:

Private Cloud – Private 2nd Site

- Run an offsite disk-based backup appliance at your second data center.

Private Cloud – 3rd Party Colocation

- If you don't have a second data center or your second data center is full, you can run the offsite disk-based backup appliance at a third-party hosting or colocation facility.

Hybrid Cloud

- Have a cloud service own and run the disk-based backup appliance as a cloud service and charge by the GB per month. This is called a "hybrid cloud" service. This approach uses OPEX budget by allowing you to pay monthly versus purchasing the offsite appliance with capital budget.

Public Cloud

- Replicate to a public cloud service such as Amazon AWS or Microsoft Azure. This approach uses OPEX budget by allowing you to pay monthly versus purchasing the offsite appliance with capital budget.

ExaGrid offers all four options above and works with organizations to understand their requirements in order to provide the right solution for each situation.

As with all options, there are pros and cons to each. In the chart on the following page, you can see the benefits and trade-offs of each approach. Some of the major points to consider are:

- Financially, are you planning to use CAPEX or OPEX budget? Do you plan to pay up front or over time? Paying up front is always less expensive over a three-year period; however, some organizations want to use OPEX budget as it is accounted for differently on their balance sheet.

- What are the RTO (recovery time objective) and RPO (recovery point objective) goals for DR? How much of the environment has to be operational over what period of time, and what recovery point is acceptable? The RTO is determined by where the data is and how quickly it can be recovered, while the RPO determines how often backups are run and how often backup data is replicated.

- Do you need to be able to stand up VMs in the case of DR, and where do they need to be operational? Do they need to be operational where the DR data is stored or at a different data center?

- What are your security policies (i.e., does the data need to be encrypted over the WAN while replicating, does the data need to be encrypted at rest once stored, and can the data be comingled on the same storage as the data of other organizations)?

- How do you copy the first backup to the DR location? Most organizations don't have the required bandwidth for a large bulk load, and the initial backup can take months to seed. Then a lengthy synchronization process is required to have the offsite backup data be synchronized to all the changes that occurred at the primary site during the months of initial data seeding.
- How long does it take to recover the data in the event of a disaster?
- What are your security policies (i.e., does the data need to be encrypted over the WAN while replicating, does the data need to be encrypted at rest once stored, and can the data be comingled in the same storage with data from other organizations)?
- Are the costs clear (e.g., hybrid cloud providers charge by the GB per month but is all data access and retrieval included)? The public cloud solutions offer a lower per-GB price but then have a number of a-la-carte charges for data access. The actual monthly bill from the public cloud provider can be many times higher per GB than the publicly stated per-GB per month price.

	Private 2nd Site Dedicated Appliance	3rd Party Colocation Dedicated Appliance	Cloud Service Dedicated Appliance	Public Cloud AWS or Azure
Price over 3 years	Lowest	Medium	Medium	Medium
Budget	CAPEX	CAPEX	OPEX	OPEX
Pay	Up front	Up front for appliance, over time for colo	By the GB per month	By the GB per month
All data available for DR	Within 24 hours	Within 24 hours	Within 24 hours	Months
WAN replication / encryption	Yes	Yes	Yes	Yes
Encryption for data at rest	Optional	Optional	Optional	Optional
Only your organization's data on the storage, no comingling	Yes	Yes	Yes	No
Recovery time (RTO)	Minutes to hours; assumes the data is at the DR site	Minutes to days	Minutes to days	Days to months
Recovery point (RPO)	Last night's data	Last night's data	Last night's data	Last night's data only after the initial seeding and synchronization are complete
Audit recovery tests	Yes	Yes	Yes	Yes
Time to get system or data back if contract is terminated	N/A	24 to 48 hours	24 to 48 hours	Months