

Private vs. Public: Cloud Backup

What You Need To Know

With more and more MSPs looking to add cloud backup services, the decision to build a private or to buy a public cloud requires a close look at all factors including the **true cost of building a**

redundant cloud backup infrastructure, the added **price tag of disaster recovery**, the required **backup and recovery speeds**, evaluation of **appliance-based vs. cloud technologies** and **selecting the right cloud provider**.



With profit margins continually under pressure, MSPs are looking to value-added services such as backup as a means of boosting profitability.

Recently Zetta.net did a State of Backup survey and discovered that **52% of companies intend to add cloud-based backup** in the near future. This represents a major opportunity for MSPs to add cloud backups to their service offerings.

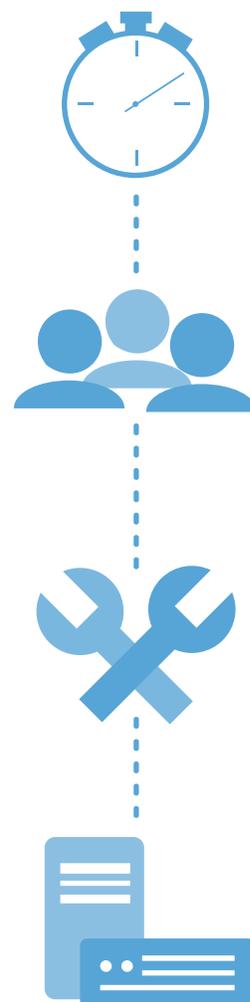
As many MSPs have not assembled the platform required to offer enterprise-class backup to customers, they are faced with the question of whether to invest months in erecting their own infrastructure or to utilize the services of a cloud provider.

Building Your Own Private Cloud Infrastructure

Any MSP contemplating building their own storage sub-system should become fully aware of the many aspects of supporting and managing storage. Significant time and resources are taken up in product evaluation, selection and acquisition.

Once purchased, there is much to be concerned about when it comes to implementation and integration. And once the storage assets are in place and functioning, they need to be maintained. All this assumes, of course, that the necessary storage management and administration resources exist internally. This means having adequate storage personnel with the skill sets to efficiently manage your customers' storage.

The key points to take into account, then, are the **true costs of the necessary hardware and software, ongoing support costs, the capabilities of existing personnel, and establishing a time to recovery** that is in keeping with the needs of the business in the event of a disaster.



1. Build: The True Cost

The primary expense is the acquisition cost of the storage unit itself, capital expense (CAPEX). Many firms underestimate the CAPEX element. As well as disk-based storage arrays, those requiring high-performance must include more expensive flash. But the storage alone is not enough. It has to be backed up by supporting compute and networking resources.

Once the hardware purchase has been made, MSPs will need to factor in operating costs (OPEX) such as software and support, hosting, scalability and people costs. In simple terms, the following OPEX costs apply:

- **Scalability costs (to be able to ramp up): 5% of CAPEX**
- **Hardware support: 18% of CAPEX**
- **Software support: 5% of CAPEX**
- **Data center hosting: \$24,000 per year**
- **Networking costs: \$12,000 per year**
- **Personnel costs per year: \$100,000 or more**

When all this is tallied up, it gives the MSP a more accurate evaluation of the build vs. buy equation. Those electing to build may indeed retain control, but the cost is usually far higher than they realize.



2. Retaining Two Copies Of Data



Those MSPs considering building their own infrastructure must also take into account the added cost of disaster recovery (DR). That means it is important to possess two copies of the data in different locations to ensure customer data can be recovered at any time which adds considerable costs. In the event of a disaster, the MSP has to guarantee that its own systems won't be down and can be relied upon.

One way to achieve this is to add tape storage and send tapes to an offsite facility.

- Tape cartridge are relatively inexpensive and readily available but buying a tape silo comes with similar expenses to those of a disk storage subsystem
- Contract with an offsite storage company is required to store and retrieve tapes
- Since tape drives tend to upgrade every 18 months, legacy drives must be stored should you have to restore data from older backups
- In most backups, tapes are read sequentially, especially if you are trying to recreate a system from a full backup. If one of those tapes are bad, your disaster recovery efforts will be lost

Gartner analyst Dave Russell placed tape backup failure rates at anywhere from 10% to 25%. MSPs can't afford to risk their reputation by relying on tape.



3. Security and Compliance



There is another hidden cost to building your own DR infrastructure which few MSPs consider – the requirement for security and compliance. With data breach headlines being an almost daily occurrence, the last thing an MSP needs is to see their name in the news as being responsible for another massive data breach. Such an incident could deal a fatal blow to customer confidence in the MSP.

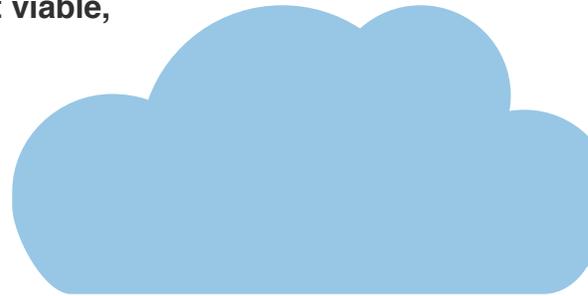
And once again, the budget for adequate security, these days, can be staggering. MSPs have to add in such items as:

- **Firewalls**
- **Anti-virus**
- **Anti-malware**
- **Intrusion prevention**
- **Encryption of data in flight & at rest**
- **Access control**

Additionally, compliance requirements can be daunting. Many organizations, these days, have to comply with HIPAA, Sarbanes-Oxley, ITAR and other regulations. There is no room here for error. So once again, those electing to build their own DR capabilities are faced with yet more expenditures for compliance systems and personnel.

Cloud Backup

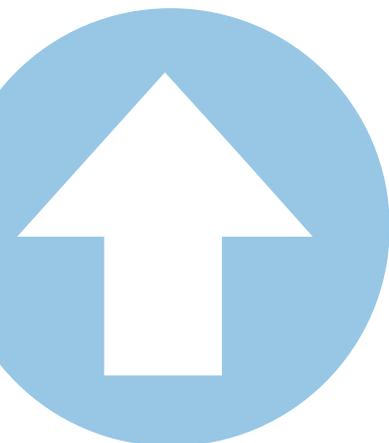
Within the last five years, **the cloud has become the most viable, cost effective solution for MSP's**. Instead of high upfront costs and operating expenses, the cloud provider incurs all CAPEX and OPEX costs. As they service a large number of clients, they can afford to utilize hardened data centers equipped with the latest technology.



By using a cloud-based backup provider, MSP's have single and predictable line item expense for backup and recovery services. But achieving that goal is contingent on choosing the right cloud provider. Some provide only consumer-level services, some are priced cheaply but gouge the MSP with hidden costs and others lack an understanding of the needs of the MSP. The selection process is crucial.

Selecting the Right Cloud Provider

Only the best cloud providers offer access to a state-of-the-art storage and backup infrastructure. This should be accompanied by the ability to use geo-diverse data replication that securely encrypts the data in transit and at rest to two or more data centers. By partnering with a company that can provide this, MSPs can offer backup services to existing customers with confidence that SLAs will always be met.



Beyond having the infrastructure MSPs can trust, other important factors to consider include transfer rates, the value of throttling and actual costs vs. hidden costs. Be aware, for example, that the cost per GB is typically only a portion of the total charge. When you see lowball figures, therefore, understand that they come with hidden

costs. Others are going to provide consumer-level services or offerings with poor support and performance.

It is also vital, then, to conduct a test of the solution in your environment to see how long a backup takes, and how long it takes to recover that data set.

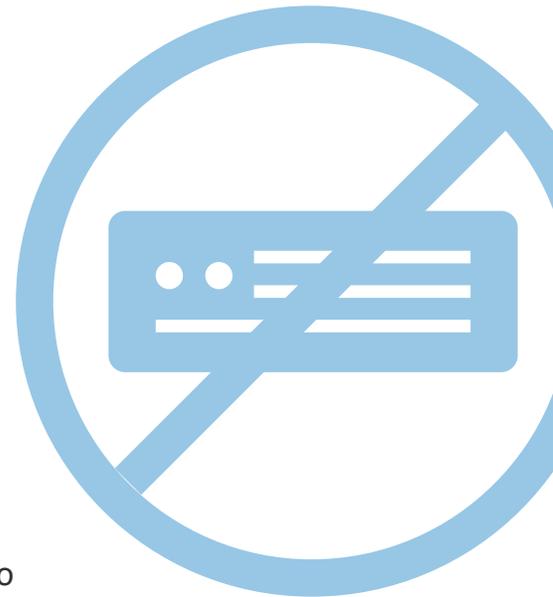
Appliance or Not?

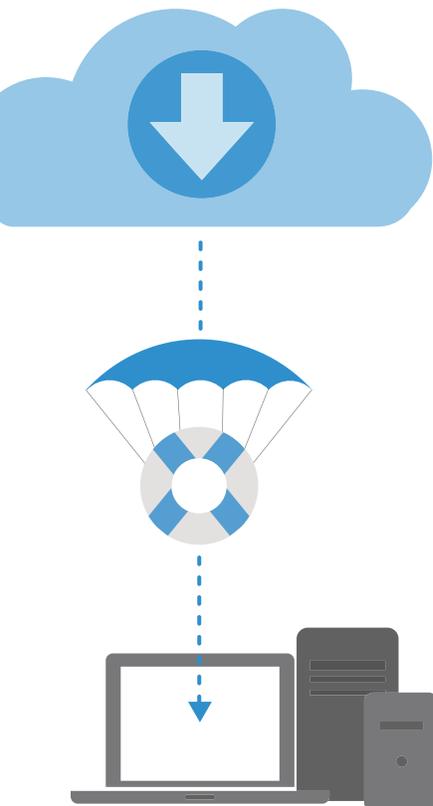
Most cloud providers will offer either an appliance-based or software-based solution for your backup needs. If it is appliance based, you will incur the cost and maintenance of the appliance, in addition to the storage you use. Additionally, there will be a cost for support of that appliance should it stop working, sometimes called an advanced replacement cost.

An appliance-based approach encumbers MSPs with managing additional infrastructure and have been found to be far slower and can cause recovery delays having to wait for a replacement hardware during a major disaster than direct-to-cloud backup services.

An independent test for example, found Zetta.net was:

- **13x faster than appliance-based cloud backup speeds**
- **2.5x faster than backups performed locally to backup appliance**





Bottom Line

Many MSPs have turned to cloud-based backup and recovery services to eliminate time-to-market and huge CAPEX/OPEX associated with having to build out a new data center. The growing interest is due primarily to lower total cost of ownership, fast deployment capability, ease of use, increased security in protecting data and the ability to easily scale up or down depending on their clients' needs.

But not all cloud server backup solutions are created equal. If you're looking for a turn-key cloud backup and recovery service, seek a software-only solution that was **born in the cloud** to take full advantage of its benefits — eliminates unnecessary expenses, streamlines deployment and management, scales infinitely, and minimizes disruption in recovering data.

You'll also need a solution that takes speed and performance with built-in WAN optimization into consideration, to quickly transfer large data sets above 1TB over the Internet.

Zetta.net is an award-winning provider of enterprise-grade cloud backup and disaster recovery as a service solution. Its **direct-to-cloud approach with built-in WAN acceleration** enables them to simplify backups, speed data recovery and reduce overall cost.

The bottom line is that when you tally up the true cost of building your own private cloud, it is going to be much more cost effective to use a cloud backup provider such as Zetta.net.

To find out how Zetta.net can address your cloud backup and disaster recovery needs, contact us at www.zetta.net or 1.877.469.3882.