

# 8 Reasons Your Data Back-up Solution Might Need a Refresh

## Table of Contents

Overview.....	2
Key SMB Considerations for Cloud Backup .....	2
#1: Security .....	3
#2: Performance and versality .....	3
#3: Pricing structure.....	3
#4: Availability .....	3
#5: Bi-Annual Backup Audits and “Always On” Support.....	4
#6: Regulatory compliance .....	4
#7: Company policy .....	4
#8: Avoiding vendor lock-in.....	5
Conclusion.....	5



## Overview

In today's climate, data is perhaps the most important asset of any business – and protecting data is the most critical aspect of any effective IT strategy. A minor interruption of service – even just a few hours of down time – can significantly impact productivity and sales.

A total data loss in the event of a natural disaster, equipment malfunction or cyber attack can cripple your business badly enough that it may not recover. One study reports that a company who experiences a computer outage lasting for more than 10 days will never fully recover financially and that 50% of companies suffering such a predicament will be out of business within 5 years.

Though most small-to-mid-sized businesses (SMBs) place a high importance on data protection, their protection strategy is often inadequate. Accelerating growth rates, budget constraints and reliance on outmoded technology can leave businesses unaware of cracks in their security, and leave data exposed.<sup>i</sup>

Increasingly, SMBs are moving to cloud-based solutions. 92% of SMBs are now using at least one cloud business solution and 87% are using at least one cloud infrastructure solution<sup>ii</sup>. This is a significant jump over the last few years.

While the cloud is the most affordable, reliable and efficient data protection solution for SMBs – not all cloud solutions are created equal. Cloud systems come in all shapes and sizes, and it can often be difficult to discern which features and functionality will serve the needs of an individual business.

The LiveVault® eGuide outlines 8 key considerations that every SMB should factor into their evaluation of their current or prospective cloud systems providers.

## Key SMB Considerations for Cloud Backup

Cloud backup and management systems offer limited upfront capital costs, reduced IT complexity, and a pay-as-you-grow model that scales cost-effectively to support business growth. Cloud backup is reliable, highly automated and easy to use. Put simply, cloud solutions are a great fit for SMBs. But cloud solutions vary in their functionality, feature sets – and in the service level of the provider. Less than stellar service can put your data in danger. Choosing the right provider is every bit as important as choosing the right solution.

LiveVault has provided cloud solutions to over 11,000 businesses over the past 11 years. Our experience and data show that the following 8 considerations top the list of choosing the right system.



## #1: Security

Security is the first and most important function of cloud data solutions. Cyber criminals are increasingly changing tactics to outsmart data encryption. Data can be vulnerable while stored in the cloud, but is most vulnerable during transfer to the cloud. Your data must be encrypted during uploading, as well as while in storage. The best providers offer “end-to-end” 256-bit encryption – but encryption is only as strong as the encryption key. Most providers will manage encryption keys for you, but due to HIPAA compliance and other regulations – or simply for additional security, some SMBs manage their own encryption keys. This can leave the provider without access to data, which can lead to security breaches. Determining what type of security logic your business needs prior to purchasing a system can save headaches down the road.

## #2: Performance and versatility

Optimal performance of a cloud backup service will help reduce backup windows and minimize data volume. The advent of faster Internet speeds combined with advances in data compression and duplication, enable quality providers to offer SMBs accelerated backups and restores with no bandwidth restriction. Lower-end providers with limited resources and infrastructure are often forced to restrict upload rates, slowing backups to a crawl.

To optimize cost and performance, choose a provider that offers a wide array of backup options. This should include incremental backups (also called delta blocking), so that only files and parts of files that are new or changed since the last backup will be included. Top providers also offer backup of open files, and support all platforms (Windows, Linux, UNIX, Mac) and applications (Microsoft Exchange, SQL Server/Dynamics, SharePoint, Hyper-V; VMWare; Oracle).

## #3: Pricing structure

SMBs must balance cost with the level of service they need to ensure their data is completely secure. Billing for cloud storage is typically based on the amount of data uploaded, stored and downloaded, along with the number and types of requests for backups and restores. Learn about each provider’s setup costs, hardware/software fees, cost per gigabyte of data stored, and whether there are additional charges for “overages.” Some providers charge for every file accessed (read, write, open) on top of per-gigabyte and download charges. If you are performing a significant number of database lookups and updates, the costs can add up fast.

## #4: Availability

Availability is based on each provider’s investment in its data center. Data centers are rated by a standard methodology that defines the level of availability they offer. Tier 1 data centers (the lowest) lack redundant capacity components (uplink and servers) and can offer 99.671% availability. At the other end of the spectrum, Tier 4 data centers offer fully redundant and fault-tolerant components (uplinks, storage, chillers, HAVC systems, servers, etc.) and can achieve 99.995% reliability. The best cloud backup providers offer Tier 4 availability along with competitive pricing.



## #5: Bi-Annual Backup Audits and “Always On” Support

Backup solutions that have not been audited for a long period of time can cause performance issues and inefficient data backup that waste resources. Additionally, key data is often missing, putting the business at risk. Choose a provider that regularly audits your backup solution to ensure your mission critical data is protected. The best providers maintain an open line of communication to determine whether your business has adopted new technologies, and if your business needs have changed.

If disaster should arrive and mission critical data has been compromised or is missing, you'll need a provider that is available 24/7 to deal with the issue. Time can be a key factor in data loss and recovery. Make sure your provider is “always on” and ready to respond.

## #6: Regulatory compliance

Government Regulations the Payment Card Industry (PCI) standard and other regulatory agencies are increasingly focusing on how third parties handle sensitive data. It is imperative to choose a provider that helps – not hinders – your chances of passing a regulatory audit. The “gold standard” for cloud backup providers is SOC 2 Type II certification, which recently replaced SAS 70. This is an independently audited attestation of controls and procedures related to security, availability, processing integrity and confidentiality/privacy. Providers with this level of certification can prove that they meet regulatory requirements.

## #7: Company policy

Does your business have an established policy for ensuring business continuity and data security? What are your recovery time objectives (RTOs) for key classes of data like financial records, contracts and client information? What is your retention and disposal policy for electronic records? These are details that should be shared with prospective providers to ensure you choose the right one for your business. Prospective cloud backup providers should agree to the service levels you need and provide a set of backup/restore procedures that match your policy.





## #8: Avoiding vendor lock-in

Providers who employ proprietary technologies incompatible with those of competitors, or who demand long-term contracts, create vendor lock-in. This can force businesses to stay with a provider that no longer meets their needs in order to avoid the complexities of moving data from one cloud service to another.

The best way to avoid vendor lock-in is to perform due diligence before signing a contract. What is the length of the contract? What service levels does the provider agree to? Are there any restrictions on moving your data elsewhere? In particular, ask whether a provider facilitates moving customer data out of its repository, and whether they provide migration tools or services for moving large volumes of data. It's also important to determine whether a provider supports emerging industry standards, such as the Cloud Data Management Interface (CDMI).

## Conclusion

Leveraging cloud backup can help SMBs save money, improve data protection, manage data growth and comply with regulations. But you must look carefully at your current or prospective cloud backup provider to ensure its services are a good fit with your business needs.

## Resources

- i. David M. Smith, PHD "The Cost of Lost Data"  
<http://gbr.pepperdine.edu/2010/08/the-cost-of-lost-data>
- ii. Wasp Barcode Technologies "The 2015 State of Small Business Report"  
<http://www.waspbarcode.com/static/waspbarcode/images/pdf/samall-biz-report-0115-web.pdf>

### About LiveVault

LiveVault® is the turnkey, fully managed cloud server backup and disaster recovery service of choice for thousands of enterprise customers worldwide. With more than 16 years of experience in SaaS data protection, LiveVault is a leader in streamlining and reducing the costs and complexities of companies' data security. LiveVault's 24/7 actively monitored, unified solution includes advanced systems for open file backup and offsite data mirroring, flexible long-term retention, legal hold support, and disaster recovery in the cloud. Learn more at [www.livevault.com](http://www.livevault.com).



---

Contact US Sales 1-844-LIVE-VLT  
email us at: [LVsupport@livevault.com](mailto:LVsupport@livevault.com)

[www.livevault.com](http://www.livevault.com)

