KeepItSafe®

How to Choose the Right Online Backup Solution

Selecting the right online backup solution for your data can mean the difference between resting easy knowing that your data is protected and readily accessible, versus losing your data in a disaster or outage or finding yourself in legal trouble because of a data privacy breach.

So, what are the most important factors to look into when comparing online backup solutions? Following are some things to keep in mind:

1. Security and Data Protection

A solid backup solution will have several layers of security built in. Not only should your data be encrypted from the second it leaves your computer and throughout the entire backup process, but both the client — and provider — side should have controls in place that prevent unauthorized access to your data. Authentication protocols should also be implemented to ensure that no one can restore your data to alternate hardware without authorization.

2. Full Support, Management & Monitoring

If you run into backup issues, do you have a number you can call 24/7? You must make sure that, if you need it, there will always be a competent person at the other end to help you solve the issue as soon as possible — so you can focus on your business. The same goes for managing the solution. You don't want to spend lots of time managing and monitoring the solution and getting distracted from your business. If the solution is fully managed and monitored, you can just rest and focus in what is important.

3. Knowledge, Expertise & Accreditations

When you're dealing with sensitive data and stringent compliance mandates, you need real experts who are readily available and understand your requirements. An online backup provider must have a track record helping organizations protect their data. A good way to measure this is by checking that it is certified in ISO 27001, FIPS 140-2, SAS 70 and approved by Gartner.

Never assume a solution is compliant without learning what requirements you must adhere to. Before signing up with a vendor, get to know the people who will be responsible for the daily monitoring and support of your account and ask for references who can vouch for the viability of the solution.

4. Provider's Storage Location

Before signing with a backup provider, ask out about their data center(s) locations. Data center location is critical for meeting federal data-protection guidelines. As a reference, KeepItSafe's tier-4, ISO 27001 certified data centers are located throughout the country, with 24/7 security. Storing your data in your business's country of residency is the recommended method; this offers two advantages, addressing data-privacy guidelines and timely restores in the event of a full-scale disaster. If a business losses hundreds of gigabytes or multiple terabytes, a physical restore from the data center is a more efficient and timely option. As a rule of thumb, the provider should be able to offer a full physical recovery next business day. Not all providers offer this data shuttle service so check before you sign.

5. Business Continuity & Disaster Recovery

Imagine you walked into your office tomorrow and found your server room destroyed due to a flood, fire or other catastrophe. What would you do? How would you get your business back up and running? Could your staff access critical files and remain productive? A competent backup and recovery provider should be able to provide a viable solution. KeepItSafe DR, for example, is a virtual disaster recovery solution that enables businesses to recover their servers from the KeepItSafe cloud after a disaster. In just minutes after a disaster, KeepItSafe can have your servers up and running and accessible via a virtual desktop.

KeepItSafe offers comprehensive cloud data availability solutions — contact us

888 965 9988 | www.keepitsafe.com | sales@keepitsafe.com