druva

5 Things You Didn't Know About Cloud Backup

1. Data privacy can easily be compromised by encryption key holders.

Encryption is vital to data protection and most backup solutions offer it. However, encryption is not always a guarantee of security and privacy of business data. After all, if an employee at your data backup company can access your encryption keys, is your data truly secure?

Some service providers have responded to this concern by purporting to "escrow" the key, saving it separately from data, and rotating it frequently. But no matter the steps taken, as long as the service provider has access to your encryption keys, your data is just not private. And a subpoena will force service providers to produce unencrypted customer data – even when encryption keys have been escrowed.

If your service provider has access to your encryption keys, **your data** is **just not private**.

Another response to securing encryption keys has been to use an onsite server, behind the client's firewall, to house encryption keys in order to guarantee sole ownership. However, this is not a true solution for cloud-based backups since there is still hardware to manage and maintain, defeating the purpose of cloud services. Additionally, an onsite server adds another point of potential failure, requiring additional data protection.

For maximum privacy, two-factor encryption key management is the recommended solution. With two-factor encryption key management, the encryption key is further encrypted using customer admin credentials, and only a token is stored in the cloud. With this solution, the service provider has zero access to encryption keys and customers avoid the hassle of supporting key servers on-premises.

Only customers have access to the key and, subsequently, their data, once authenticated. And to truly guarantee privacy, the key is destroyed at the end of each customer session.

2. Choosing the wrong cloud could mean permanent data loss.

Of course, most of "the cloud" actually exists at ground-level, supported by many connected servers and other devices which require electricity and protection from the elements. As much as dependability of data centers has increased over time, these server farms are still vulnerable to power outages, sabotage, and natural disaster.

Server farms are still vulnerable to power outages, sabotage, and natural disaster.

This is why it's important to understand the Service Level Agreements for any backup providers under consideration. Many cloud service providers don't offer data redundancy across multiple data centers. In the event of a power supply disruption, service is suddenly unavailable and files are out of reach until the problem is corrected. A natural disaster, such as a flood, could even result in permanent loss of your critical corporate data.

Leading service providers offer data redundancy across multiple facilities, each of which is physically separate, located in lower risk flood plains and fed via distinct grids from independent utilities. These facilities are connected to different networks to ensure the highest data availability and durability possible.

Many cloud service providers don't offer data redundancy across multiple data centers.

3. Local cloud backups can violate data residency laws.

Traditionally, cloud backup providers have employed a limited number of data centers and housed those data centers within the borders of a single country. Adding

storage typically requires following a multi-step process, often cumbersome and not immediate.

If your business has global reach, these localized backup providers are simply unable to offer a premium, worry-free experience.

By definition, a global enterprise supports internal systems which are utilized by employees and other users all over the world, subjecting the enterprise to a specific set of laws in each country. Using localized cloud backup providers from a single country is not only inefficient but, in many cases, it results in a violation of local data residency laws.

Using localized cloud backup providers is inefficient and often results in violation of data residency laws.

By contrast, leading cloud backup providers are equipped with multiple redundant data centers across the globe, enabling customers to control which data centers are used for their data backups. Leading providers also utilize an "elastic storage" concept, enabling customers to add storage instantly in any data center without having to worry about scaling their storage requirements.

4. Without deduplication, your backup speed is a fraction of what it could be.

One of the reasons traditional cloud backup systems can be very slow is that the software must compare the last file and directory structure with the latest file and directory structure in order to determine what's changed. Unfortunately, as much as 80 percent of data is duplicated across a typical enterprise. This is because users often have multiple copies of an identical file stored locally, as well as on shared or removable drives. This causes storage requirements to boom, considerably slowing cloud data transfer.

When backup solutions practice global deduplication, cloud backup and restore times are dramatically improved because an enormous amount of duplicate data has been identified and removed.

Traditional cloud backup systems without global deduplication can be very slow.

To perform enterprise restores quickly, a backup solution must also use multi-threaded restores in order to allow parallel transfers of multiple files. Using multi-threaded restoration significantly accelerates the time it takes to restore data to a user's computer.

WAN optimization will also speed up endpoint backups because WAN optimization makes best use of the available bandwidth. If there's a network interruption, WAN optimization ensures that the dropped backup automatically resumes at precisely the right point.

5. Outdated backup solutions severely restrict IT control.

Using older principles of storage technology, some backup companies are not able to leverage federated search, which can quickly locate information anywhere on the network. This is a challenge when attempting to track down a file or to enforce a new policy. Because federated search looks across every file and device in the enterprise, it becomes easy to locate files, gather or even collect them for legal hold, in order to preserve custodian data for e-discovery.

Without federated search, it is a challenge to **track down a file** or enforce a policy

On the other hand, modern backup solutions empower IT with visibility and make it easy to enforce policies on data backup, restore, and access. These leading backup companies also make use of detailed audit trails to strengthen IT's oversight and to prevent material information, such as intellectual property, from being compromised due to the increasingly mobile workforce. Detailed audit trails preserve a record of all user and admin activity, as well as provide real-time visibility, enabling organizations to support their governance and compliance needs.

If the enterprise is subject to industry regulation, it's well worth it to select a service provider that already has passed the requisite certifications (e.g., HIPAA, PCI-DSS, ITAR) for its data centers and operations.

About Druva

Druva offers a full suite of endpoint data management solutions for enterprise laptops, PCs, smartphones, and tablets. Its flagship product, inSync, empowers an enterprise's mobile workforce with award-winning backup, secure file sharing, data loss prevention, and rich analytics. Deployed on the cloud or on premise, inSync is the only solution built with both IT needs and end-user experiences in mind. Druva has over 1,500 customers and protects a million endpoints across 46 countries. With offices in the United States, India and the United Kingdom, Druva is privately held and is backed by Nexus Venture Partners and Sequoia Capital. Information on Druva is available at **www.Druva.com.**

druva

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44.(0)20.3150.1722
APJ: +919886120215
sales@druva.com
www.druva.com