CLOUD BACKUP
Myths busted!

Top ten cloud backup myths busted to ease any cloud backup security fears

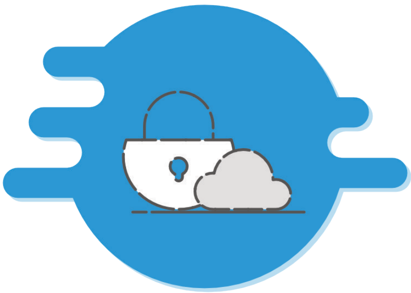
XOPERO
WORKS, SO YOU CAN TOO!

INTRODUCTION

While cloud computing still induces mixed feelings among entrepreneurs, companies are more eager to transfer their data to the cloud. According to Xopero Software S.A. research, 58,3% of entrepreneurs find it secure while still 41,7% of them, do not trust in the cloud.

Despite concerns, the cloud solutions market is steadily growing. According to IDC, 9 out of 10 companies use cloud computing solutions - among the most commonly used are e-mail, storage, synchronization, and sharing tools. There is still low usage of more advanced tools. However, its foreseen that by 2025, the businesses will put 60% of their data in the cloud.

92% of companies admit that cloud facilitates everyday work. They appreciate it for, among others, automatization of many processes, availability and low costs. On the other hand, it arouses distrust. Are there any reasons for that? In this document, we will try to confront the most common myths about backup in the cloud with rational arguments.



Cloud backup is less secure

This myth is rooted in the fear of transferring significant company data outside of its headquarters. Where will the data go? To the cloud? So where? The rational answer to this question can quickly dispel all fears.

Backup solutions producers use only trusted data centers which store client backups. Those data centers provide a complex and high level of security, confirmed by appropriate certificates and verified by regular audits. They have infrastructure adapted to the continuous operation of network devices and servers - appropriate interiors and buildings, power generators providing constant energy supply, uninterruptible power supply (UPS) as well as air conditioning ensuring the right temperature, humidity and, cleanliness of indoor air. Everything is carefully designed and maintained by specialists. The implementation of such a level of security in a single enterprise is not unprofitable - it’s simply impossible.

Speaking of the security of Xopero solutions, it is impossible not to mention that before data is sent to the backup server in the cloud using 128-bit SSL certificate, so still at the user computer, they are encrypted with the AES 256 algorithm, recognized as impossible to fractures (it is used, among others, by banks in the execution of payment transactions and the American National Security Agency). Further, the data is encrypted using a key known only to the client or a default key (stored on the backup vendor's site). Theoretically and practically - if someone could even gain access to the server - the data will be useless to him. The decryption process takes place only on the user's computer when restoring data.

Summary

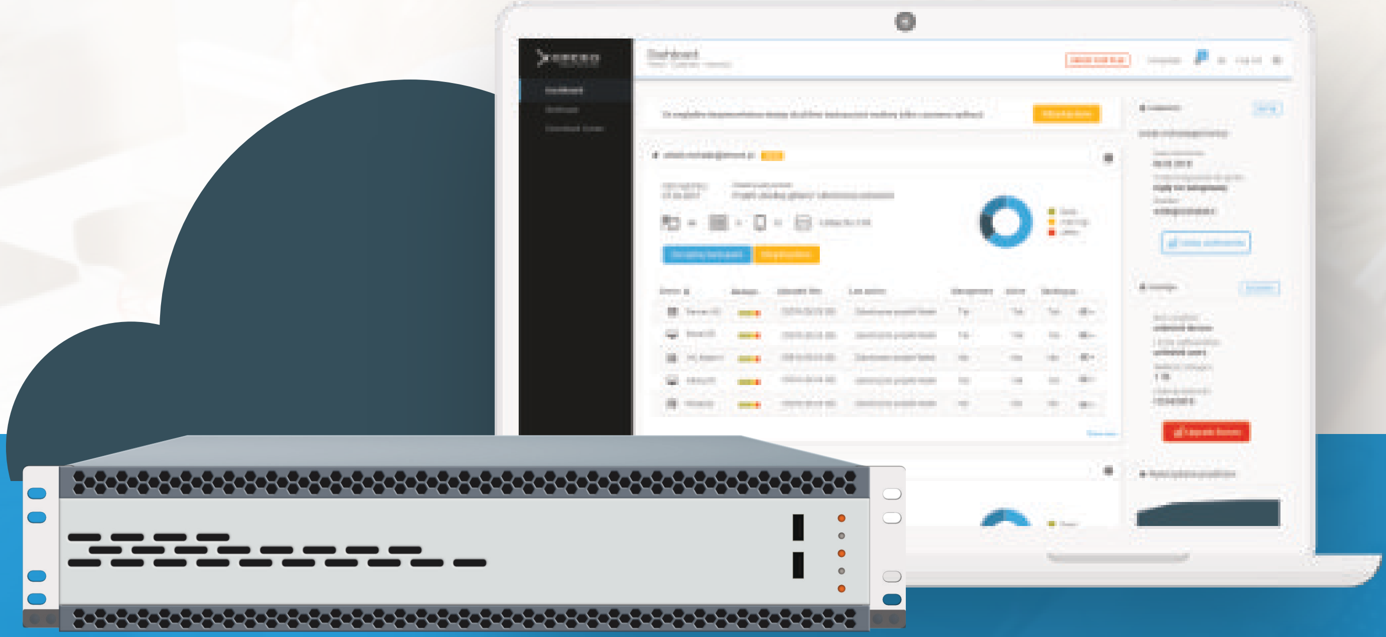
High security standards, data encryption, appropriate infrastructure, 24/7 monitoring, teams of specialists, security audits and compliance with standards as well as certificates make these concerns unfounded.

Verdict: **MYTH IS DEBUNKED!**

Xopero Cloud

PROTECTING BUSINESS DATA CAN NOT BE MORE SIMPLE

Backup unlimited amount of data and devices
to the secure cloud



Easy configuration

Install the app on the device you want to automatically back up and stop worrying about the data - it's already protected

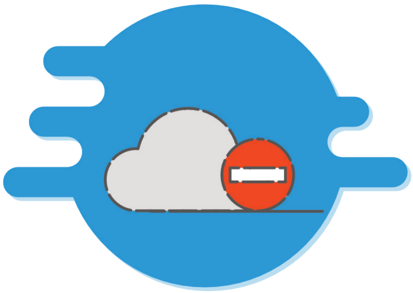
No limits

"Pay-as-you-go" model lets your customer back up data and devices on storage crafted to his needs. If wants more - can upgrade it anytime!

Low cost

Xopero Cloud has everything you might need to maintain comprehensive data protection policy

Try for free



Cloud backups are less available

Data centers are classified according to availability (TIER). Usually, they guarantee access to data at the level of 99,98% (TIER III) or 99.99 % (TIER IV) - it's possible due to redundant server rooms, power and, cooling systems, multiple backbone network or internet provided by several operators. Can the data be more accessible? Can local storage give us more guarantee and certainty?

What about the situation of the event of failure or periodic maintenance of the data center? How will the availability of our data look like then?

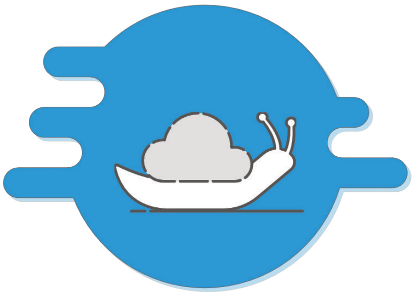
Backups stored in the data center are repeatedly duplicated. They are stored not only on several disks and in several different machines, but also in more than one physical location. Most data centers have several locations, which additionally protects data against various random events, natural disasters (such as flood or fire), as well as temporary breakdowns or maintenance work. If they occur in one location, the customer can always download his data from the other.

Summary

Redundant infrastructure, multiple data duplication and nearly 100% data availability guarantee - do you need to know anything else?

Verdict: **MYTH IS DEBUNKED!**

#2



Backup in the cloud is slow...

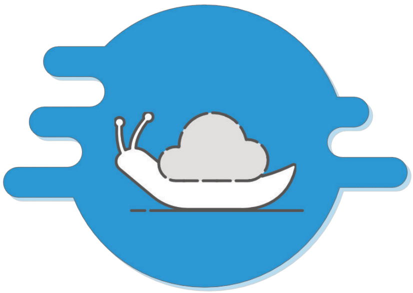
Backup in the cloud requires stable and fast internet connections. The speed of its performance depends on the speed of the Internet connection, and although the times of slow internet have gone forever, it is true that it performs a bit slower than local backup. Entrepreneurs are sometimes afraid that the backup will affect the speed of the Internet - the Xopero Cloud solution allows such a backup configuration that use only part of the internet link, without limiting the bandwidth.

Summary

The fact that nowadays we watch TV series and HD movies online without hanging or buffering proves that data transmission through the Internet is not a problem at all. The dynamic improvements of Internet connections, new technologies and growing standards of mobile network (eg 5G) show us that it will be only better. Keep it in mind.

Verdict: **OVER TIME, THE MYTH LOSES ITS RELEVANCE, ALTHOUGH WE MUST ADMIT THAT THERE IS STILL A GRAIN OF TRUTH IN IT.**

#3



...so is recovery

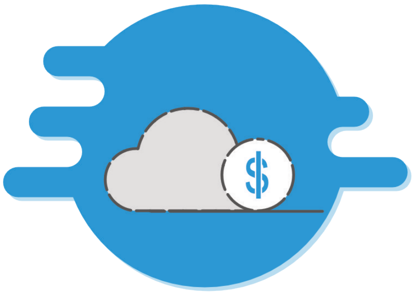
Recovering data from backup in the cloud also requires stable and fast internet connections. However, the recovery time depends not only on the bandwidth of the Internet but also on the amount of restoring data. It is not always necessary to recover the entire backup copy. Most often, data loss means accidental deletion of a single file or folder. In such situations, all you have to do is to recover only the lost data - not entire copy and it will happen immediately.

Summary

The progressive processes of deduplication and data compression, dynamic improvements of Internet connections and the ability to quickly restore only selected files and folders make the strength of this myth negligible.

Verdict: **IN THIS CASE, THE SAME AS IN THE PREVIOUS ONE, THERE IS A SMALL GRAIN OF TRUTH THAT DIES OUT TOGETHER WITH INTERNET SPEED IMPROVEMENTS.**

#4



Cloud backup is expensive

The price you pay for storage in the cloud is higher than purchasing the equivalent disk - true. However, this simplified calculation does not take into account the costs of maintaining local infrastructure. Add here the costs of the physical environment, i.e. rooms, electricity or additional security and what have you got? The result is not so obvious, right?

In the price of cloud backup, you receive the already mentioned professional data centers security level. Redundant infrastructure, data duplication, 24/7 monitoring, security certificates, protection against random situations and catastrophes - all of this is included in the package. You do not have to worry, plan and pay for implementing this type of protection internally in your organization.

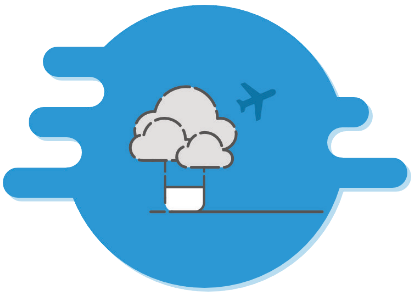
Also, remember that in cloud solution you pay for the storage you use and you increase it only while your needs are growing. We can say that cloud backup is a tailored solution for every business needs.

Summary

Wider glance and more accurate calculation prove that the cloud solution turns out to be more economical, especially considering the level of security received "in a package" and “pay-as-you-use” billing model.

Verdict: **MYTH IS DEBUNKED!**

#5



Cloud backup is less efficient than local solution

Cloud backup is driven through the same technology as the local solution. The difference is the place of backup storage - locally and physically, at the company's headquarters or in the cloud.

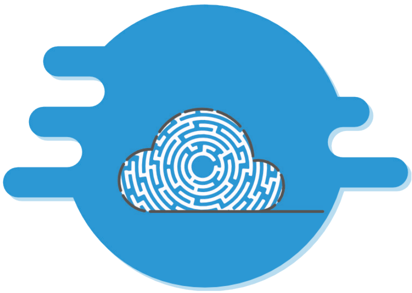
Each solution differs slightly in terms of functionality, but it is difficult to clearly say which ones work better. The choice of the backup ecosystem should be preceded by an analysis of the enterprise's needs and infrastructure. Nevertheless, both in local and cloud backup solution data is secured and possible to recover at any time.

Summary

Since both types of backups differ mainly in the place of data storage, the issue of efficiency is strongly related to the needs and internal conditions of the company.

Verdict: **MYTH IS DEBUNKED!**

#6



Cloud backup management is more complicated than in local solution

Both types of backup - as we have already determined - are driven by the same technology, including the one responsible for managing backups. In both solutions, there is the possibility of central and remote management of the backup process. In the same way, you define the policy of creating backup copies, define data and devices for protection and backup execution schedule so technically it doesn't differ in both ecosystems.

Summary

If we realize that the main difference between local backup and cloud copy is the storage location, we understand that this is not important for the functionality of the solutions - also in the aspect of management.

Verdict: **MYTH IS DEBUNKED!**

#7

Antivirus&anti-malware software are sufficient protection against ransomware

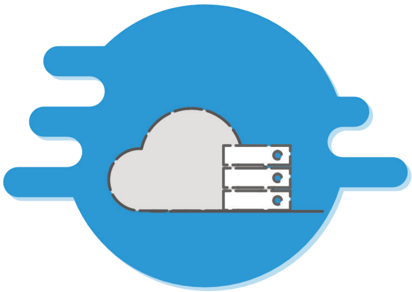
- *I don’t need backup.* - Not really... many entrepreneurs are convinced that the antivirus effectively protects a business against ransomware attacks. Although the producers of anti-malware programs constantly improve their products, they are also constantly facing hacker’s new methods and ideas. It’s a constant war. Of course, such solutions are every business “must have” but they won’t protect you against the effects of attacks - like encryption of data by attackers and downtime as a result. Have you ever wondered what would you do then? As you can see, the antivirus itself is not enough. The backup will protect you against the effects of attacks. Instead of paying a horrendously high ransom, you will restore the data from the cloud and...immediately return to your work. Therefore, treat antivirus and backup as two-step protection of your data against ransomware.

Summary

Forewarned is forearmed - it is better to protect company data with a double shield consisting of antivirus and backup software.

Verdict: **ADVOCATES OF SAYING THAT PREVENTION IS BETTER THAN CURE, SHOULD TAKE THIS MYTH AS DEBUNKED.**

#8



Cloud backup and cloud storage mean exactly the same

- I have Dropbox, thus I don't need backup...

Again - not really. Keeping your data in the cloud - cloud storage is not the same as cloud backup, which is the process of creating backups of encrypted data that you can quickly recover and ensure work continuity while any attack, incident or employee mistake occurs. Cloud storage as Google Drive or Dropbox lets you keep copies of company data - agreements, invoices and documents in the cloud but it won't protect your server and computer together with your data against any event of failure.

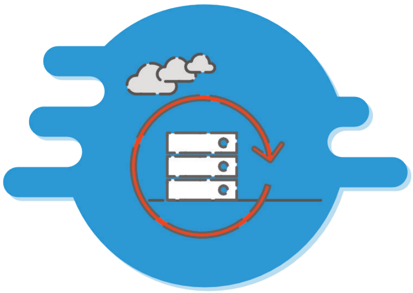
While executing a backup of company data, we store the copy on storage. However, these are not copies of selected files or company documents, but specially crafted backup files that are encrypted, stored in packs of data in a fragmented form (chunks), thus remain illegible for third parties.

Backup in the cloud allows us to perform not only copies of selected files but also to protect entire disks or selected partitions thanks to HDD image backup. In a situation when a computer hard disk will get damaged, the data and applications collected will be restored from the backup copy to any other computer. Everything will work and look exactly like on the previous one.

Summary

Commonly confused with each other cloud storage and cloud backup are two completely different concepts. Cloud storage is a modern and convenient alternative to a removable disk or flash drive. It's a huge abuse to identify it as a cloud backup and protection of company data against unexpected incidents.

Verdict: **MYTH IS DEBUNKED!**



I do local backup so there is no need to make copies to cloud

Company data can be protected not only locally or in the cloud. The most effective way to protect them is to combine both of these solutions in the hybrid backup. Thus, mixing the stability of local solutions with cloud flexibility you gain 100% guarantee of data security.

A copy stored locally allows you to quickly restore company data in the event of a failure or attack while a copy in the cloud is excellent protection in the event of a natural disaster (i.e. fire or flood) and losing local copy.

Summary

Hybrid backup is the fulfillment of the golden backup rule. The "3-2-1" rule indicates that to ensure data security, a company should have at least 3 backups stored in at least 2 different locations, of which at least one should be located outside the company's headquarters. The redundant data center infrastructure and multiple duplications allow to keep the data on several disks in different machines and more than one physical location - in at least two of data center and locally in company headquarters.

Verdict: **MYTH IS DEBUNKED!**

#10

XOPERO

WORKS, SO YOU CAN TOO!