Choosing a New Cloud Storage Provider

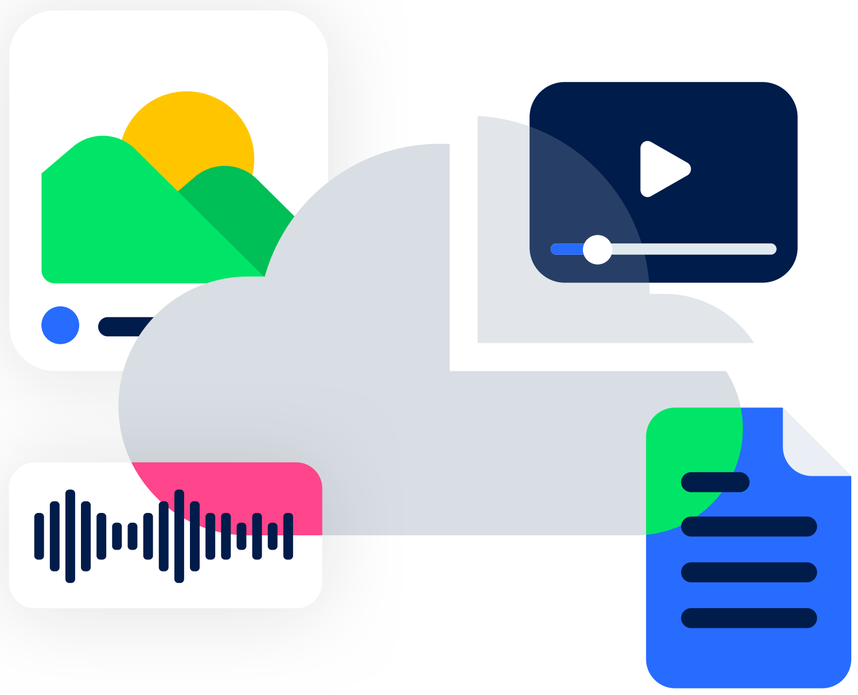
The 5 Deciding Factors

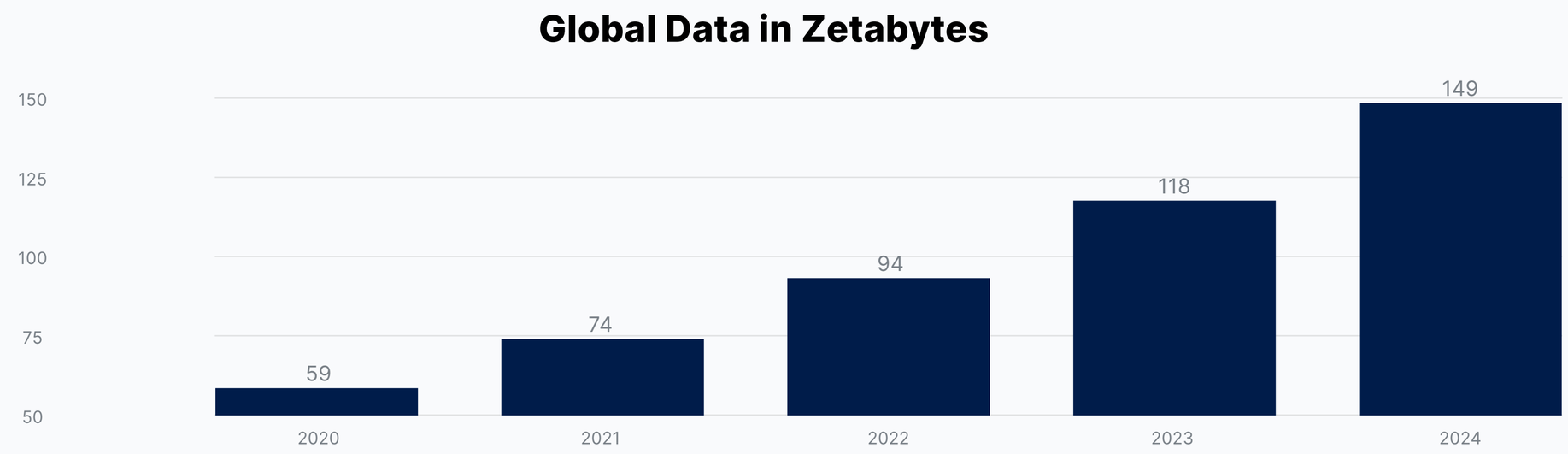
STORJ

www.storj.io

Data storage is an increasingly strategic priority.

Data growth is exploding, with no signs of slowing down. What's driving it? The rapidly increasing volume and complexity of mobile applications, social media, multimedia, gaming, big data, and the burgeoning development and adoption of technologies including Internet of Things (IoT) devices and artificial intelligence (AI). These massive amounts of unstructured data and the amount of data stored by organizations is, according to Gartner, estimated to grow between 30% to 60% every year – tripling by 2024.

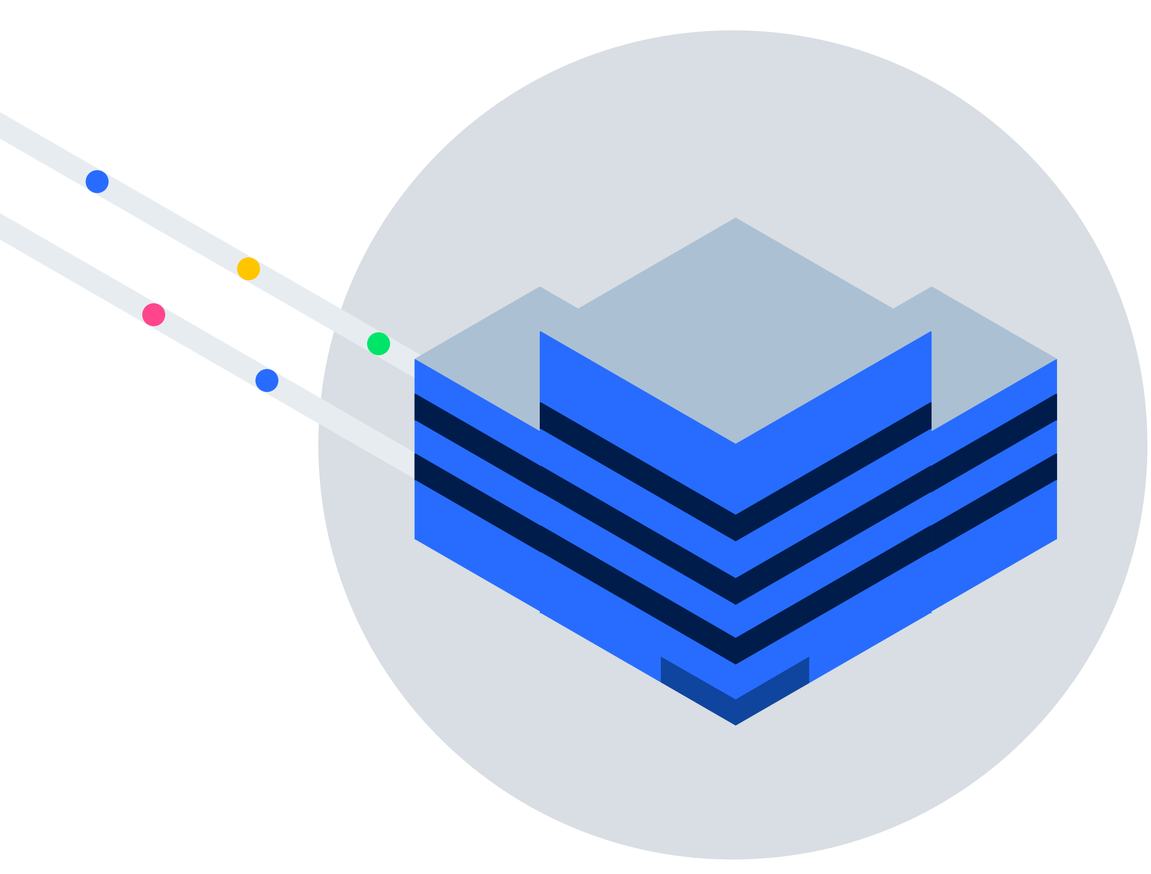


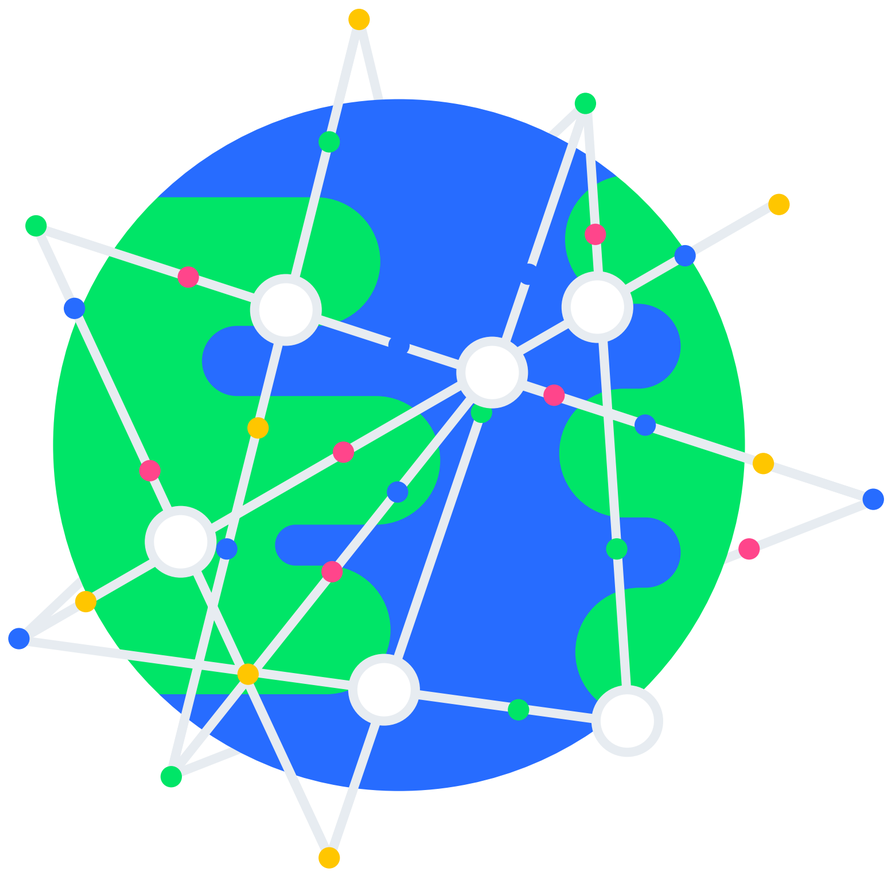


By 2022, the majority of this data will migrate to the cloud from on-premise data centers, cementing the rise of cloud storage as the preferred choice for organizations and developers alike. This creates new opportunities as technology leaders seek alternatives outside of the traditional big tech players in cloud storage. There's an ever-increasing demand for better privacy, security, reliability, availability, and lower costs.

Which Cloud Storage Model Is Right For You?

Most cloud storage providers use centralized architectures, so data is susceptible to a single point of failure, limited encryption, and minimum privacy policies—meaning your data's security and privacy can be compromised. However, providers with decentralized architectures offer inherent data integrity benefits that appeal to developers, product owners, and CTOs, including complete privacy as files are encrypted by default, split up, and distributed across a globally decentralized network. There are currently three well-known cloud storage providers, and they control 60% of the market, with the remaining 40% represented by a multitude of companies' solutions. So, how do you know which cloud provider you should choose to cover your top priorities? What features or requirements should help guide your decisions?





Centralized

In a centralized architecture, data is stored in one place within the four walls of a data center.

Decentralized

A decentralized architecture is globally distributed with no single point of failure or vulnerability.

We asked.
They answered.

To get better answers, we recently polled more than 300 developers and business/tech leaders for a cloud storage research survey. We asked them what their top priorities were when choosing a cloud storage provider and uncovered some interesting results. After compiling the data from the participants, we determined the top five factors in choosing a cloud storage provider are security, privacy, cost, reliability, and availability.

1. Security is sacred

24% of those surveyed ranked security as the most critical concern when choosing a cloud storage provider. It’s easy to see why: many mainstream cloud providers struggle with data security and privacy breaches that can expose vast amounts of sensitive data from logins to passwords, personal information, and more.

> “Security is the most appealing concern to us as a whole as it can cost us millions of dollars if we were to suffer a security breach.”

Data loss and the leakage of sensitive information are easily the top two significant threats when it comes to data protection. Some of the security risks faced by cloud storage providers include misconfiguration, insecure interfaces, APIs, and unauthorized access due to a lack of proper access controls.

One recent example of a serious security breach is the data vulnerability presented by the hack of SolarWinds. The compromised SolarWinds Orion code was discovered by FireEye, which was conducting a forensic investigation of a breach that occurred on its own network. The inquiry led them to the Orion platform as the possible culprit. They reviewed 50,000 lines of the SolarWinds Orion code and discovered a backdoor had been injected by attackers. When traced, the backdoor initiated active connections to command and control servers. In total, around 18,000 SolarWinds customers were hacked, about 50% of SolarWinds Orion's customers.

2. Privacy is Paramount

The second-most important factor for our participants was privacy, coming in at 18%. It's easy to understand why: developers and organizations alike want to take full ownership of their data. Amazon AWS, Azure, Google Cloud, or Dropbox can't ensure absolute privacy, and many users just don't trust big corporations to keep their data private.

> "My files are mine."

In fact, privacy is so important that when customers recently misunderstood an upcoming WhatsApp privacy change as a shift in the app's data-sharing practices (believing that the company could now read people's conversations and other personal data), they flocked to competing messaging services like Signal and Telegram – whom they perceived to have tighter privacy controls/measures.

WhatsApp had to hurry and reinforce its stance on end-to-end encryption – assuring customers that it can not read users' messages and that its services are more secure than most competitors.

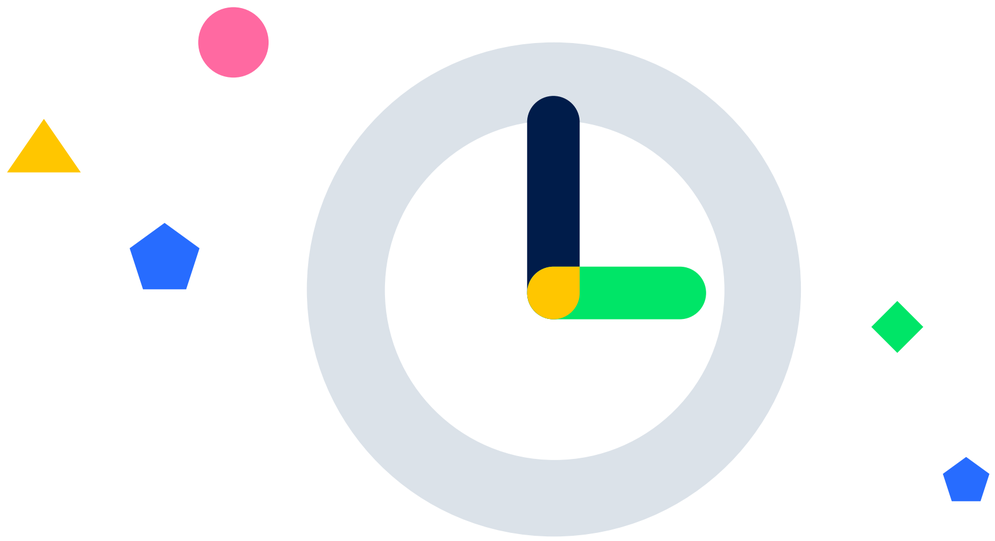
3. Cost is Key

The third most important factor for respondents was cost – specifically, cost reduction/efficiency was critical to their organization. Cloud storage is often a company’s largest operating expense, and it's become increasingly more costly.

> “Cost is one of the biggest barriers to cloud storage, and we have to make choices that are financially smart.”

Additionally, those using one of the centralized cloud storage options are most often locked into recurring cost structures that deliver specific amounts of capacity, functionality and services – limiting flexibility and scalability. Up until now, competition for a customer’s cloud storage business has been fairly limited, with a few companies dominating the space. This market is ripe for innovation – and a new, more cost-efficient category – decentralized cloud storage.

4. Reliability Rules



Another top factor for our group is reliability. Traditional cloud storage providers have a single point of failure, making for possible issues with true redundancy and reliability. Cloud service outages can seriously impact workloads of enterprise systems, user data and applications -- which means lost revenue.

On the other hand, decentralized cloud storage splits up files, and then distributes and stores redundant segments on nodes (storage devices) located across the globe. This eliminates any single point of failure and ensures uptime that traditional cloud providers can't deliver.

> "It's very important that any uploaded data is secure and can be reliably retrieved. If data can't be reliably retrieved when requested, that's a major issue."

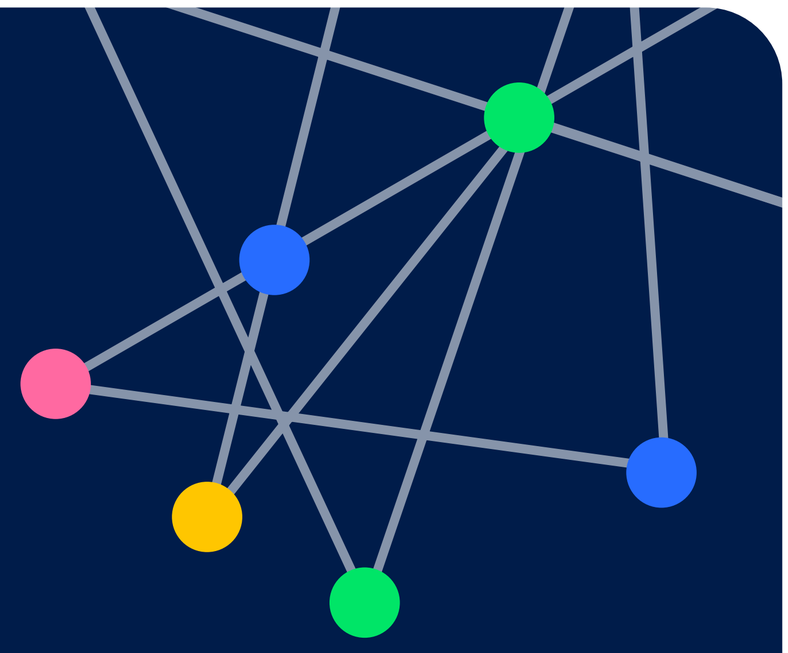
5. Availability Matters

Data availability is also important to our group. If a centralized option, such as Amazon S3, goes down and there isn't another copy or a multi-region architecture, access to data may be delayed or completely unavailable.

Many files are also prone to bit rot (aka data degradation) or can even be lost due to a malicious attack or other errors. The whole point of the cloud is to store your data safely; if you can't get to your data when you need it, it defeats the whole purpose.

> "Availability must be 24X7 with no errors or data fragmentation."

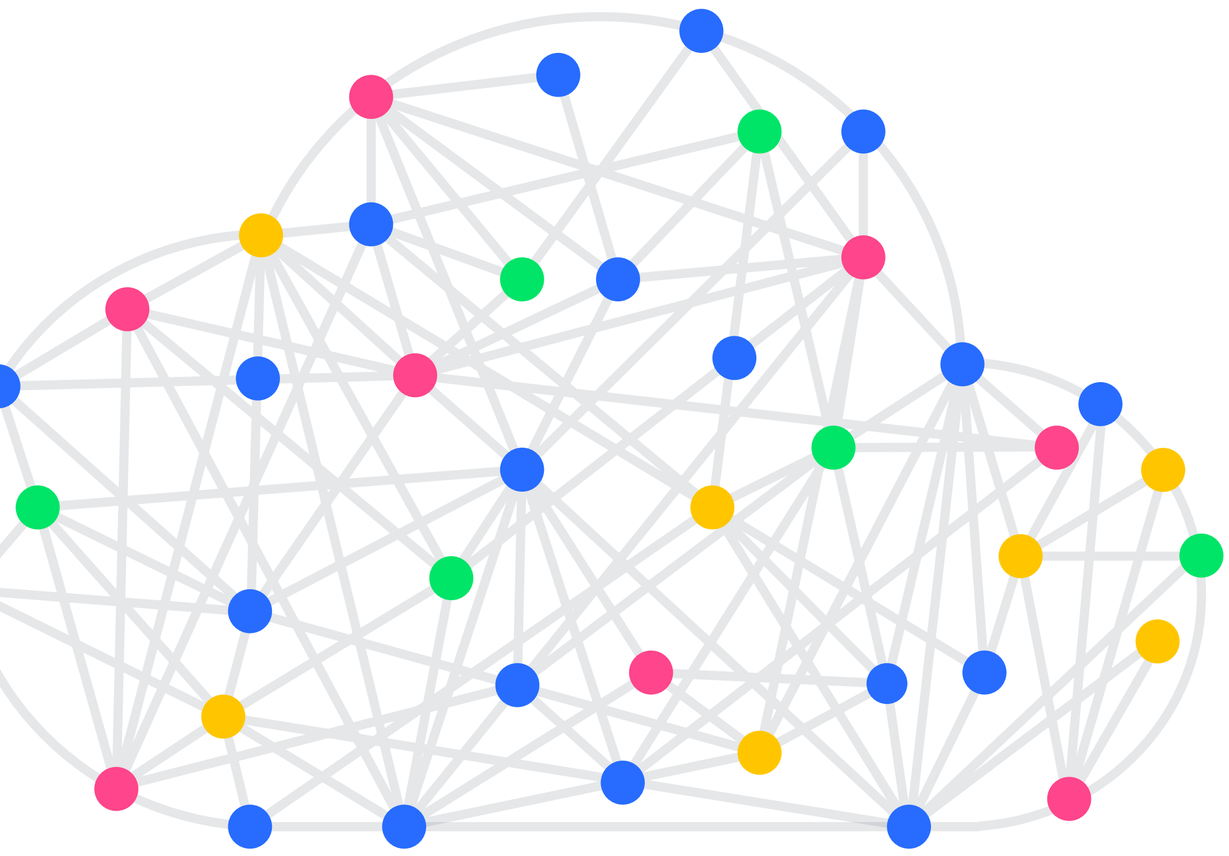
A Case for the Decentralized Cloud



Now that we've identified users' most critical decision factors for cloud storage, it's easy to see the decentralized model uniquely delivers on all fronts: security, privacy, cost, reliability, and availability.

Decentralized cloud storage solutions offer enhanced security and privacy by splitting files up into many pieces, distributing them across various locations, providing files with redundancy that is similar to multi-region architectures, and eliminating centralized honeypots. Enhanced encryption technologies and erasure codes can ensure data integrity and protection against attacks, like ransomware.

Regarding privacy, all decentralized cloud storage users control their own data because only they have access to their encryption keys/access controls. No one can access it outside of who you actually share your encryption keys or grant access to view your data. That means no third party can see your data, it's virtually impossible to hack, and due to the decentralized nature of these networks, you can access your data when you need it.



With thousands of vetted storage devices (Nodes) hosting your data, the amount of available storage is significantly higher than centralized storage. This, in turn, leads to substantially lower costs. Decentralized storage is also more efficient: traditional client-servers often result in network bottlenecks if traffic is larger than the network can handle. By employing P2P technology and eliminating a central server, multiple copies are stored on different Nodes, therefore allowing more copies of the data which then leads to faster download speeds.