STORJ

TechTarget Custom Media
White Paper

Security and Privacy Benefits of Decentralized Cloud Object Storage

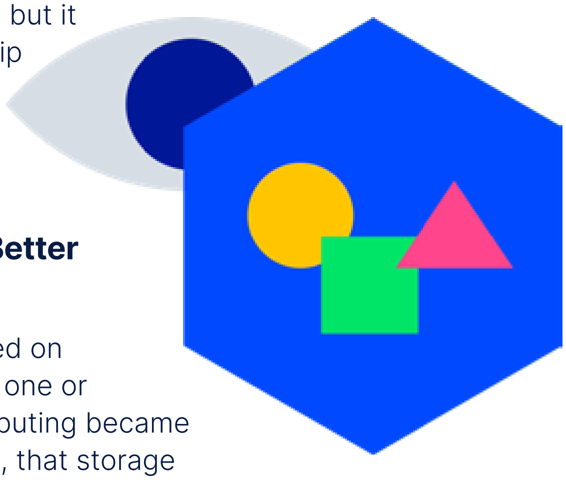
As data growth and the subsequent use of cloud storage balloons, development teams and organizations alike must address potential dynamics to enable teams to build the most private and secure applications possible. Software developers, in particular, should consider leveraging the inherent benefits of decentralized cloud object storage in order to limit risks and take control of their data.

The move toward cloud storage, underway for more than a decade, has now kicked into overdrive. Data volumes have exploded, and developers and organizations now demand more secure, private and efficient approaches to storing and sharing data. Global expenditures on cloud storage are expected to accelerate by more than 22% annually between now and 2025, when the worldwide market will exceed $137 billion.[1]

[1] "Cloud Storage Market—Global Forecast to 2025," MarketsandMarkets, September 2020

While there are many options to store increasing volumes of data in the cloud, the overwhelming bulk of those options are built around a centralized cloud storage architecture. Although centralization has been the foundation of storing data for decades, in today's increasingly cloud-first era, decentralized cloud storage offers developers the tools and resources to build more private and secure applications, so users can minimize the potential financial, operational and brand reputation risks of a data breach or hack.

Developers, in particular, are highly focused on the security posture of today's cloud storage. Cloud storage provides developers with the obvious advantages of storing and accessing very large amounts of data, but it presents challenges in terms of control and ownership of the data. It also raises doubts about whether developers can trust the safety, privacy and integrity of their data.



Why Decentralized Cloud Object Storage Is Better for Security and Privacy

When storage was exclusively deployed and managed on premises, centralization was the standard, usually in one or more traditional data centers. Even when cloud computing became prevalent and cloud-based storage grew in adoption, that storage remained largely centralized.

Centralized storage was easier for cloud service providers to deploy and manage, using very large storage clusters in their data centers—essentially the same storage architecture utilized for decades when storage was on premises except it was in the cloud. Because of the architectural consistencies, this made it relatively easy for storage administrators to manage the growing amounts and types of data being stored.

But centralized cloud storage comes with a number of drawbacks, particularly as data sets get larger and data volumes expand exponentially with the proliferation of unstructured and semi-structured data. A common complaint of centralized cloud storage is the cost structure and billing complexity that sometimes leads to surprises unaccounted for in operations budgets.

Another prominent issue in centralized cloud storage is how industry-leading controls and tools allow users to delegate control of their security profile to their storage provider. There also is the intangible factor of hackers wanting to take down high-profile public cloud services both in security and privacy breaches, even momentarily, for bragging rights in hacking into sensitive data.

Among the many security and privacy risks developers worry about when their data is stored in a centralized cloud environment are:

- Single point of failure
- Susceptibility to tampering, ransomware, bitrot and more
- As it relates to replication, broader threat surface between multiple regions as well as efforts around consensus

Failure to adequately address these issues erode developers' confidence in the confidentiality, availability and integrity of their essential data. Additionally, enterprises must address other issues that make centralized cloud storage a challenge, including:

A common complaint of centralized cloud storage is the cost structure and billing complexity that sometimes leads to surprises unaccounted for in operations budgets.

- Need for further investment to store rapidly increasing amounts of data and accommodate multiple copies of files
- Cloud service provider lock-in
- Data latency, especially for collaborative development efforts that take place in multiple locations across wide areas

Conversely, decentralized cloud object storage offers a number of benefits—especially for the increasingly number of cloud-native applications.

Decentralized cloud object storage offers the highest possible levels of security and privacy, satisfying developers' need to own their data and control its use, integrity and access. For instance, decentralized cloud object storage:

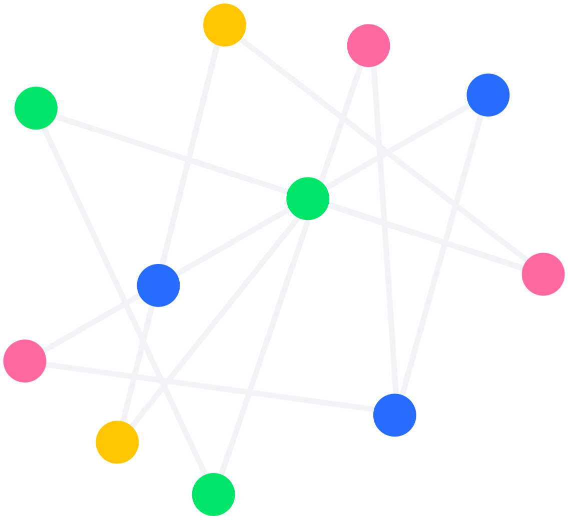
- Has no single point of failure for denial-of-service attacks.
- Contains no centralized repository for hackers to go after.
- Splits files into 80 or more pieces and stores it across statistically disparate and unrelated nodes and internet service providers.
- Uses an edge-based security model, strong encryption and delegated authorization to ensure security and privacy.
- Is resistant to ransomware and bitrot, and provides read-only credentials that are easily managed for verification and authentication.

Use Cases for Decentralized Cloud Object Storage

One of the most important reasons for adopting decentralized cloud object storage is its applicability for a wide—and growing—number of use cases. These use cases typically share a common characteristic: very large files. In fact, the bigger the files, generally the better the fit for decentralized cloud object storage. Another key driver is the need for data to be sent or accessed remotely, which of course has become a widespread, global and likely irreversible trend.

For instance, some of the most relevant and exciting use cases for decentralized cloud object storage include:

- Video storage and streaming/multimedia
- Backups
- SIEM data retention
- Large file distribution
- CCTV media storage
- NAS/SAN backup
- Hybrid cloud
- AI/ML
- Archival



Also, if your organization is storing very large amounts of data (and large data sets) in a data lake for business intelligence or is using a multi-cloud architecture, decentralized is the way to go. After all, the savings on file transfer costs alone can dramatically improve return on investment for decentralized cloud object storage.

Storj Decentralized Cloud Storage (DCS)

Few companies have made as strong and as focused a commitment to providing developers the tools required to build more private and secure applications than Storj. Storj DCS is optimized with a simple, but powerful data protection model: Private by design, secure by default.

Storj DCS provides developers with a choice of encryption solutions, delivering default end-to-end decryption for files, paths and metadata. Because developers hold their own encryption keys, their data is truly under their control.

Additionally, Storj DCS is based on a trustless security framework, meaning the absence of third parties that need to demonstrate their trustworthiness as part of the comprehensive encryption chain. User-assigned access gives users sole access to, and control of, data.

With Storj DCS, developers get predictable, easy-to-understand pricing plans, designed to scale—at a flat rate—as storage requirements grow and change.

Storj DCS also offers substantial economic benefits. As many private cloud storage customers unfortunately discover, monthly storage costs can vary widely, and users often don't know the full extent of their bill until after the costs have been incurred. With Storj DCS, developers get predictable, easy-to-understand pricing plans, designed to scale—at a flat rate—as storage requirements grow and change.

And, through the use of an attractive, easy-to-understand dashboard, developers and IT professionals have full transparency into usage patterns and costs on a real-time basis.

Conclusion

Developers have an intense, nearly fanatical desire to claim ownership of their data, and that can't be done without the highest possible confidence that the data is private by design and secure by default. Because of the limitations of traditional centralized storage, many developers are pushing their organizations to take a different approach.

Decentralized cloud object storage is the right solution for developers who need data ownership, flexibility, ease of use and favorable economics and want to avoid lock-in with public cloud service providers. Storj's Decentralized Cloud Storage delivers a solution that puts security and privacy front and center for developers, to allow them to create transformative applications with confidence for a wide range of use cases.

For more information on the unparalleled privacy and security features in Storj DCS, please visit:

Website **Developer Community** **Blog**

STORJ

Start building on the decentralized cloud.

www.storj.io

@storproject

@storproject

@storproject

This content was commissioned by Storj and produced by TechTarget Inc.