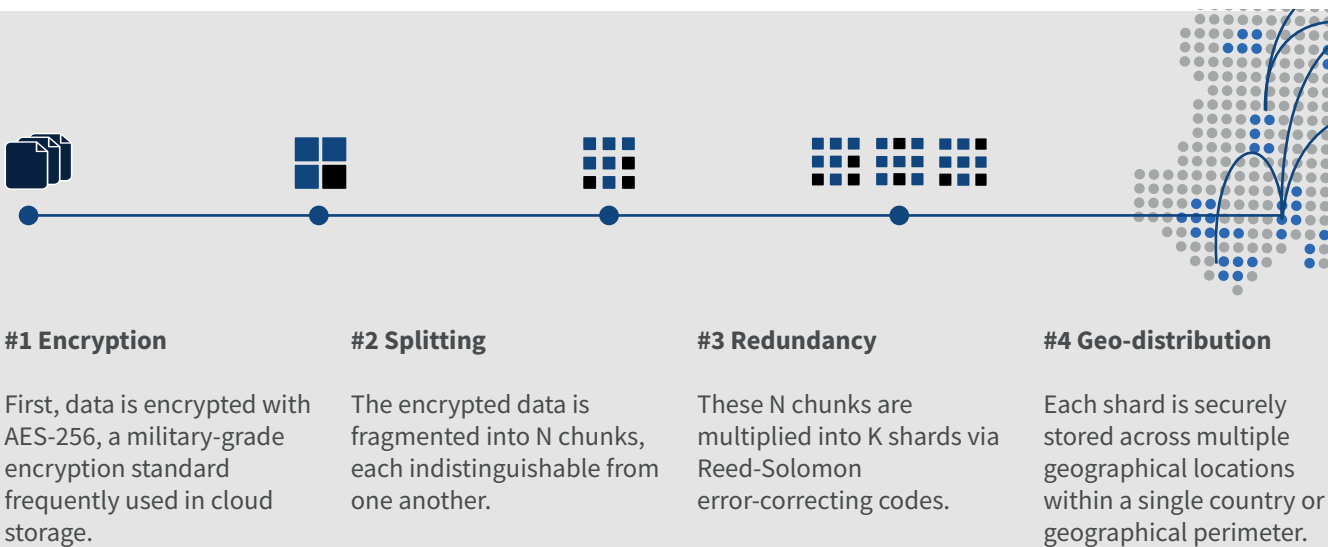


DS3 is Europe's 1st geo-distributed cloud storage:
hyper-resilient, sovereign, 100% S3 compatible — with no cost for egress, deletion and redundancy.

Unlike traditional cloud storage, DS3 doesn't store data in a few centralised data centres. Instead, files uploaded to DS3 are protected by several layers of security:



#1 Encryption

First, data is encrypted with AES-256, a military-grade encryption standard frequently used in cloud storage.

#2 Splitting

The encrypted data is fragmented into N chunks, each indistinguishable from one another.

#3 Redundancy

These N chunks are multiplied into K shards via Reed-Solomon error-correcting codes.











#4 Geo-distribution

Each shard is securely stored across multiple geographical locations within a single country or geographical perimeter.

This ensures that data remains inaccessible in the event of individual node breaches, as no information is stored anywhere in its entirety. Also, if a hacker accesses and encrypts a network node, the service will keep working without interruptions.

You only need a subset of shards to download a file from DS3's geo-distributed cloud storage network. Suppose a storage node goes offline. In that case, its fragments are automatically redistributed, and the DS3 Coordinator promptly repairs the node, all without ever gaining access to the shards.

DS3 main quality stamps

-  Geo-redundant, at no extra cost
-  ISO 9001 & 27001 certified
-  GDPR compliant
-  100% S3 compatible
-  No deletion fees & egress fees
-  Up to 15 9s of durability
-  Object Lock
-  S3 Versioning
-  Lifecycle data management
-  IAM policies

Benefits of the solution

Geo-redundant, at no extra cost

Get a simple, CapEx-friendly price — with no fees for egress, deletion, and redundancy.

Ransomware resistant

Make your data ransomware-proof thanks to multi-site object lock, versioning, IAM policy, encryption, and geo-distribution.

Digital sovereignty

Geofence the area where your data is stored, in full compliance with your nation’s specific data regulation (e.g. GDPR, ISO, CCPA).

Sustainability

Thanks to geo-distributed technology and by choosing green data centres, we extend the storage hardware lifespan and minimise your carbon footprint.

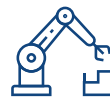
Main industries



Public sector



Healthcare



Manufacturing



Media & Entertainment

Use cases

Cloud backup

Enable a hyper-resilient, geo-redundant, GDPR-compliant cloud backup — at a fraction of the cost.

Ransomware protection

Make your data ransomware-proof thanks to encryption, S3 Versioning, S3 Object Lock, and IAM policy.

Data archiving

Enforce ISO compliance, security, and affordability in your archiving practices.

Hybrid cloud

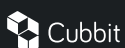
Enable a secure, off-site backup to NAS without paying licenses.

Cloud-to-cloud

Automate scripting processes, stay compliant, and easily migrate large amounts of data.

Applications

Build applications in the cloud with ease and performance.



Cubbit, a partner of Gaia-X, is Europe’s first geo-distributed cloud object storage. Its groundbreaking technology addresses nations’ specific data sovereignty concerns, helping businesses check all the compliance boxes (e.g., GDPR and ISO) while ensuring the best overall total cost of ownership (TCO), data control and providing hyper-resiliency against ransomware and disasters.

Today, Cubbit technology is adopted by 200+ European companies and partners, including Exclusive Networks (a \$4.9B global distributor in cybersecurity, listed on the Paris Stock Exchange) and Leonardo (a \$14B world leader in defence and cybersecurity).