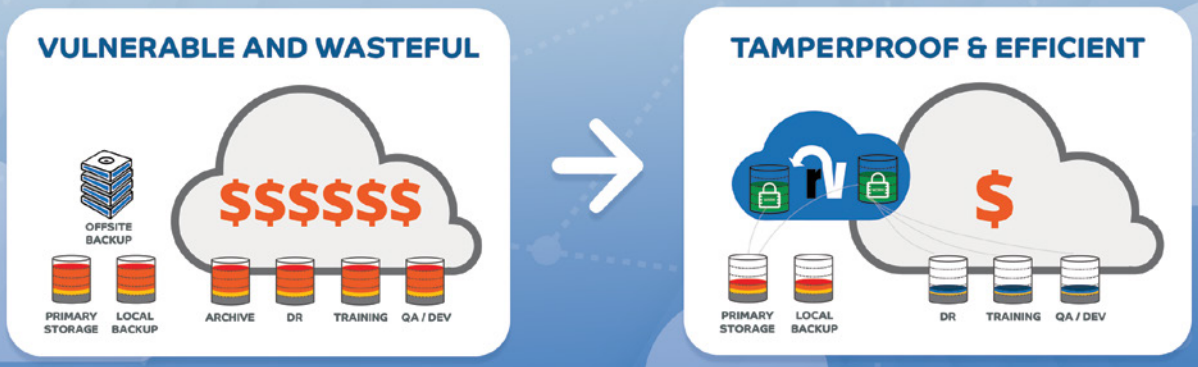
Virtual Cloud Storage



Reduce cloud storage **costs up to 80% and recover 500x** faster from Ransomware.

Storage, Archive and DR in one

According to IDC more than 80% of data on primary and cloud storage is unstructured and 60% of that is *copy data*. You don't need even more copies in order to put it in the cloud.

- Save up to 80% of the cost of storing unstructured data in the cloud
- Access archive and backup repositories from any multi-cloud server
- Recoup wasted capacity on primary and backup storage
- Avoid costly upgrades to your storage infrastructure
- Recover from disasters or Ransomware in minutes vs. days
- Access copies of protected data without using more storage

Storage Savings

Up to 80% less primary, backup and cloud capacity required

More Protection

Tamperproof cloud storage with stringent retention policies

Faster Recovery

Full recovery with 80% less downtime than conventional backups

Regulatory Compliance and Risk Mitigation

restorVault is ideal for organizations that must comply with regulatory requirements in different industries, including Healthcare (HIPAA), Financial Services (GLBA, arbanes-Oxley, SEC 17A-4, PCI DSS), and Legal (FRCP, CJIS).

restorVault exceeds the strictest requirements for data integrity, protection, privacy, security, retention and availability with full audit trails. Additionally, our automated process makes it effortless for organizations to adhere to internal and external compliance guidelines.

restorVault | 6160 Mission Gorge Road, Suite 205, San Diego, CA 92120 | 858.381.0422 | restorVault.com

Reduce the cost of storing high-value and compliance data in the cloud with Virtual Cloud Storage

Trusted Storage

restorVault provides two ways to store compliance data and other high-value unstructured data in trusted cloud vaults. They differ in version control and retention policies they apply.

Compliant Cloud Archive (CCA)

CCA provides long-term retention and on-demand access to unstructured compliance data, that must be retained for long periods of time and may not be altered in any way.

- Legal retention 7-30 years
- Automatic retention policies
- Impervious to Ransomware
- Secure real-time file access
- *Trusted Systems* compliant
- Compliance audit trail

Tamperproof Cloud Storage (TCS)

TCS provides a daily sync to a tamper-proof cloud vault that immunizes your data from Ransomware and allows for complete disaster recovery in mins or hours not days or weeks.

- 30-day version regression
- 500x faster DR than typical
- Impervious to Ransomware
- Secure real-time file access
- No data recovery fees

Virtualized Access

CCA or TCS data vaults are fully accessible from any server in the multi-cloud. So now you don't need copies of files on cloud servers any more, especially not inactive ones. They are replaced by tiny Virtual Data Files which fetch the original from a CCA or TCS vault on-demand as you use them.

Offload Data Virtualization (ODV)

ODV frees-up precious capacity on primary servers by offloading inactive files to a CCA or TCS vault, based on ageing policies.

- Only active files stay local
- Conserves primary capacity
- Allows on-demand access
- Prolongs system lifespan

Copy Data Virtualization (CDV)

CDV allows fast server replication in the cloud through the use of Virtual Data Files. With each VDF occupying only 1K in size, you can replicate a server for DR, Training, eDiscovery and other use cases, in just a few minutes, while the original files remain safely protected in trusted CCA or TCS vaults.

- Avoids data duplication
- Uses 95% less cloud storage
- Slashes cloud servers costs
- Spin up new servers in mins
- More copy servers, more savings

Data Integrity Assured

Beyond using immutable WORM drives that are impervious to Ransomware, Virtual Cloud Storage employs a combination of techniques to assure data integrity, like no conventional cloud storage can.

- **Fingerprints** – Each time a file is saved, a unique fingerprint is generated using both an MD5 and SHA1 hash of its contents and metadata, so history and contents cannot be altered after the fact.
- **Serial Numbers** – Each file is assigned a serial number to ensure no files are missing or tampered.
- **Secure Time** – System time clock is secured by using a global, redundant, authenticated time source (Stratum Level I hardware time sources).
- **Encryption** – 256 AES encryption in flight and optionally at rest.
- **Data Verification** – Files are verified every 90 days against their fingerprints, repaired using their copy if necessary, and retained per customer-defined policies.
- **Two Copies** – Each file and its fingerprint are kept twice on restorVault infrastructure, with each copy being stored in a different datacenter for redundancy.