Virtual Cloud Storage

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

Secure, economical cloud archive and backup, with ultra-fast recovery and on-demand access.

According to IDC more than 80% of data on primary and cloud storage is unstructured and 60% of that is *copy data*. You should not have to pay premium rates to store and protect it in the cloud.

- Save up to 80% costs, storing compliance data in the cloud
- Get secure on-demand access to archive and backup repositories
- Preserve capacity on expensive primary storage equipment
- Reduce backup infrastructure requirements and CapEx
- Recover from disasters or ransomware in minutes vs. days
- Access copies of protected data without using more storage

More Protection

Tamperproof cloud storage with retention policy enforcement

Faster Recovery

500x faster file access restoration than from conventional backups

Large Savings

Up to 80% less primary and cloud capacity required

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, Sarbanes-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 easy for organizations to adhere to internal and external compliance guidelines.

Reduce the lifetime costs of retaining, protecting and accessing compliance data up to 80%

Secure Data Retention

restorVault provides two ways to economically store compliance data and other high-value unstructured data in the cloud, in protected vaults. They differ in the version control and retention policies applied.

Compliant Cloud Archive (CCA)

CCA provides long-term retention and on-demand access to unstructured compliance data, that 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

Secure Cloud Backup (SCB)

SCB provides a hot-standby cloud backup capability that allows for complete disaster or ransomware recovery in mins not days.

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

Virtualized Data Access

With immutable CCA or SCB data vaults now made accessible in the cloud, virtualized access to that data can lower your on-prem and cloud capacity needs up to 80%.

Offload Data Virtualization (ODV)

ODV frees-up precious capacity on primary servers by offloading inactive data to a protected CCA or SCB vault, based on policies.

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

Copy Data Virtualization (CDV)

CDV allows fast data replication in the cloud through virtualized access to protected CCA or SCB data vaults for functions such as Q/A, Dev, Training, DR test etc.

- Avoids data duplication
- Uses 80% less cloud storage
- Spin up new servers in mins
- More servers, more savings
- Fraction of usual costs

Data Integrity Assured

- **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 continually verified against their fingerprints, repaired using their copies, and safeguarded by RAID disk arrays for as long as needed
- **Two Copies** – Each file and its fingerprint are kept twice on restorVault infrastructure. Each copy is stored on different equipment in different datacenters for redundancy.