GIGAOM

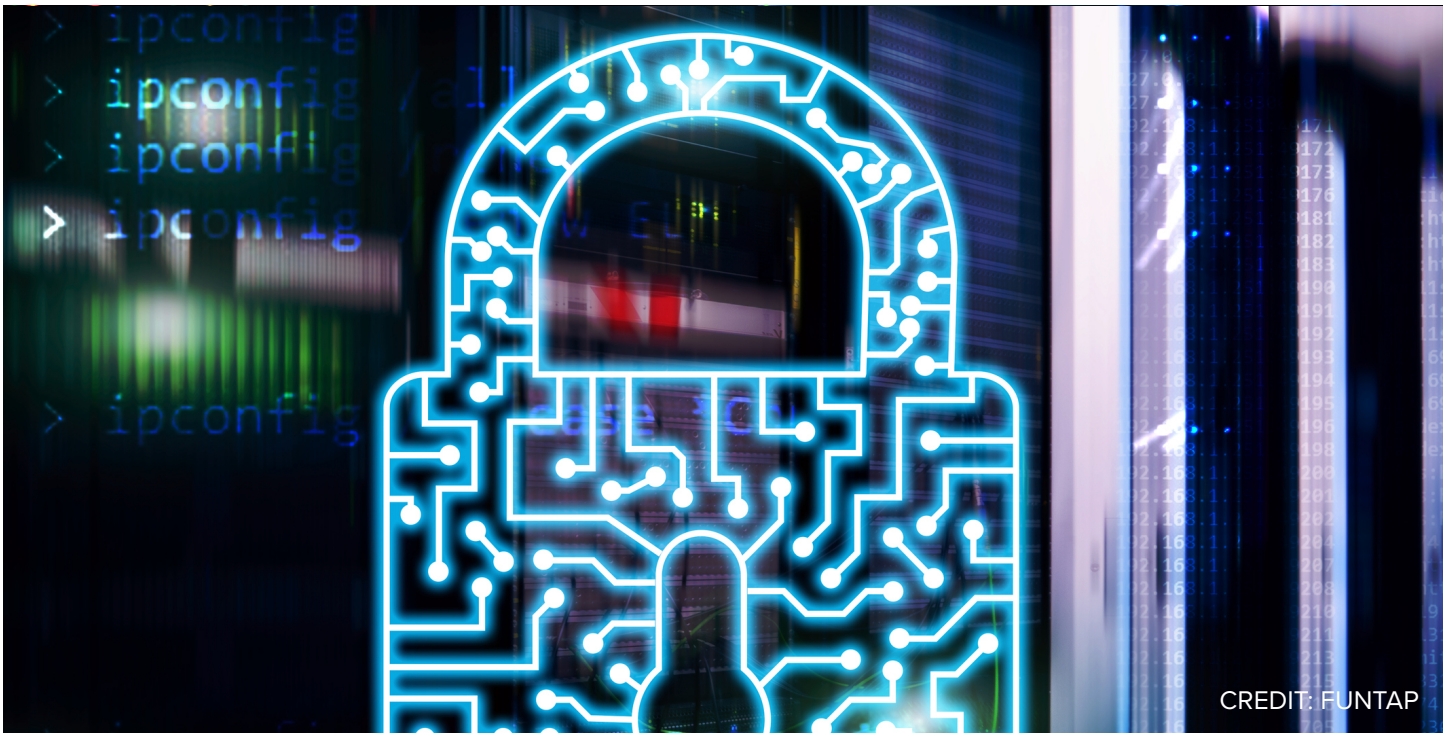
REPORT

Secure Multi-Cloud Storage for Highly Regulated Environments

A Forward-Looking Solution Analysis

ENRICO SIGNORETTI

TOPIC: MULTI CLOUD AND HYBRID CLOUD



CREDIT: FUNTAP

SPONSORED BY Leonovus

GIGAOM

Secure Multi-Cloud Storage for Highly Regulated Environments

A Forward-Looking Solution Analysis

TABLE OF CONTENTS

1 Summary

Security, privacy, level of data protection, and compliance requirements have become noticeably challenging in highly regulated industries. Most storage systems do not have the proper characteristics to comply with these kinds of requests, nor the flexibility (or costs) that would make this type of infrastructure sustainable over time. In fact, all recent regulations impose very strict rules on several aspects of data storage, including:

- **Auditability,** including immutability of logs,
- **Retention times**, mandating duration or whether it is necessary,
- **Data sovereignty,** mostly concerned with protecting personal information from access by foreign countries,
- **Data security,** often involving not only privacy but data integrity and availability as well.

Even more so, cloud storage, which has been a very flexible solution adopted by many organizations, is not always a viable option and can not be adopted as-is, because of lack of control on where data actually resides, and concerns on how it is managed by the provider. It is an issue which has been debated for quite some time now.

Most organizations have reacted to these ever demanding requirements on their organizational and infrastructure levels by introducing the position of CDO (Chief Data Officer). A role responsible for data assets and governance, while also seeking out innovative tools that can bring together the flexibility and agility of cloud storage, with the level of security and control required by the regulations in place.

2 Challenges of Multi-Cloud

The list of unique requirements for highly regulated industries is quite long and demanding. Let us consider data retention: medical records that have to be kept safe and retrievable for more than 100 years in some countries, government documents which have a practically unlimited lifespan, or finance and banking environments in which many documents must be preserved for several years post-transaction for legal reasons. It is just one of many aspects that play a role in the data governance needed to meet statutes.

Object storage is ideal in terms of flexibility and cost for data that has to be stored practically forever, while also remaining quickly accessible when needed. It is accessible from everywhere because of standard APIs and HTTPS protocols, and has a better TCO than file and block storage. Most products offer scalability, storing huge amounts of data for a long time for industries that require the long term archiving of sensitive documents. At the same time, the structure of the object is self-consistent, meaning that data and metadata (i.e. information about the content) are saved together; this makes the content easily searchable, durable, and long-lived, even if the application that created it becomes obsolete and is no longer accessible.

Unfortunately, on premises object stores have some of the same limitations as other traditional storage systems:

- Scalability is limited to the resources available, and it is necessary to plan in advance to have them when needed.
- Infrastructure has to be carefully planned and managed.
- The infrastructure is not flexible enough to answer increasing business requirements.
- Hardware obsolescence forces infrastructure upgrades every few years.

For these reasons and others, several organizations are migrating to hybrid infrastructures or moving to the cloud entirely, offloading part or the entirety of their data to the cloud. But the cloud also poses challenges:

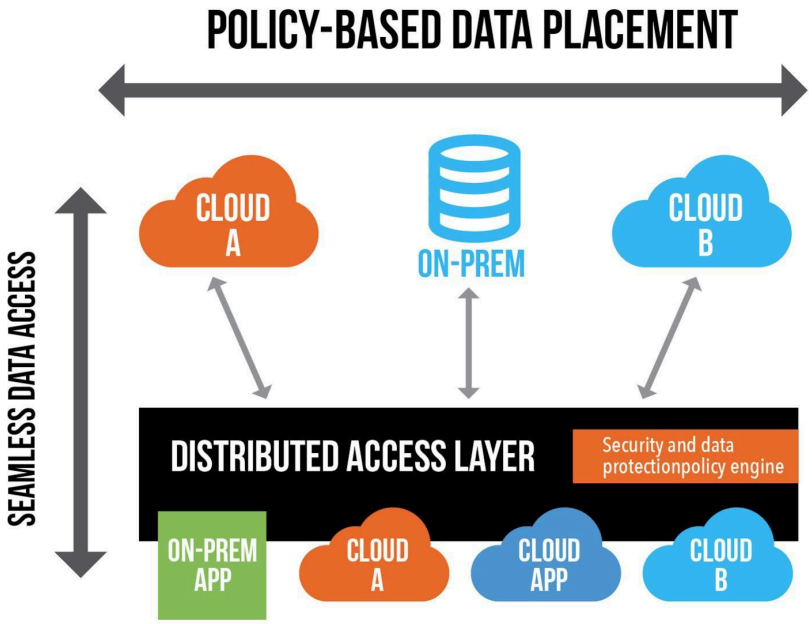
- A single cloud provider strategy is at risk of cloud vendor lock-in, especially when considering that data is hard to move seamlessly.
- Business needs, or commercial conditions, offered by the cloud provider change over time and this could easily be an issue for large scale and long term archives.

A multi-cloud approach is the right way to go, but there are several important aspects to consider before adopting it. First and foremost, it is really important to avoid the creation of cloud silos. Storing data in different places will only increase complexity, while increasing security and management issues. It is practically impossible to place data in the right place efficiently without the right tools, and

this can lead to security issues as well as unpredictable costs when it is time to retrieve data.

A multi-cloud data controller, designed to provide an abstraction layer for several public clouds and on-premises resources in the back-end, while also providing a standard access interface for users and applications, is the most likely choice. However, it needs some key characteristics to be an effective solution for highly regulated environments:

- Strong security features
- Ability to move data seamlessly, at the back-end
- S3-compatibility
- Policy-based data placement for getting the best from every cloud, while avoiding performance or cost issues



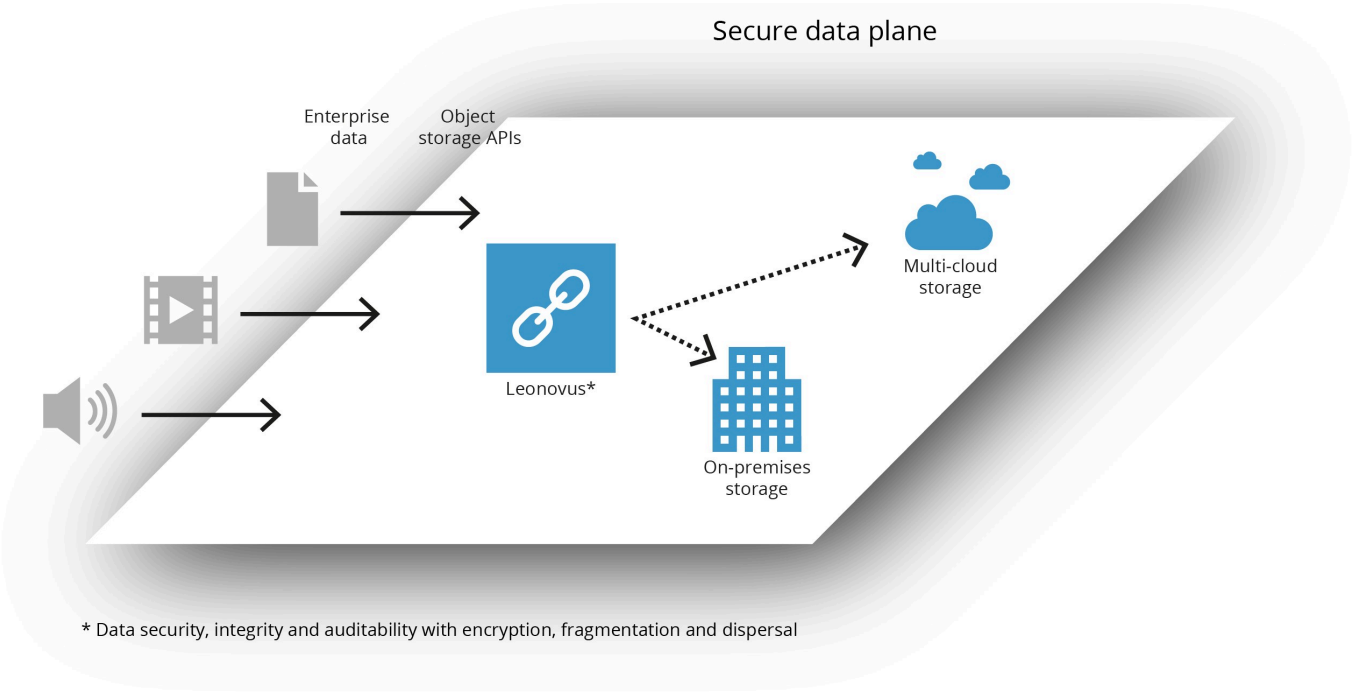
GIGAOM

3 Leonovus for Secure Multi-Cloud Storage

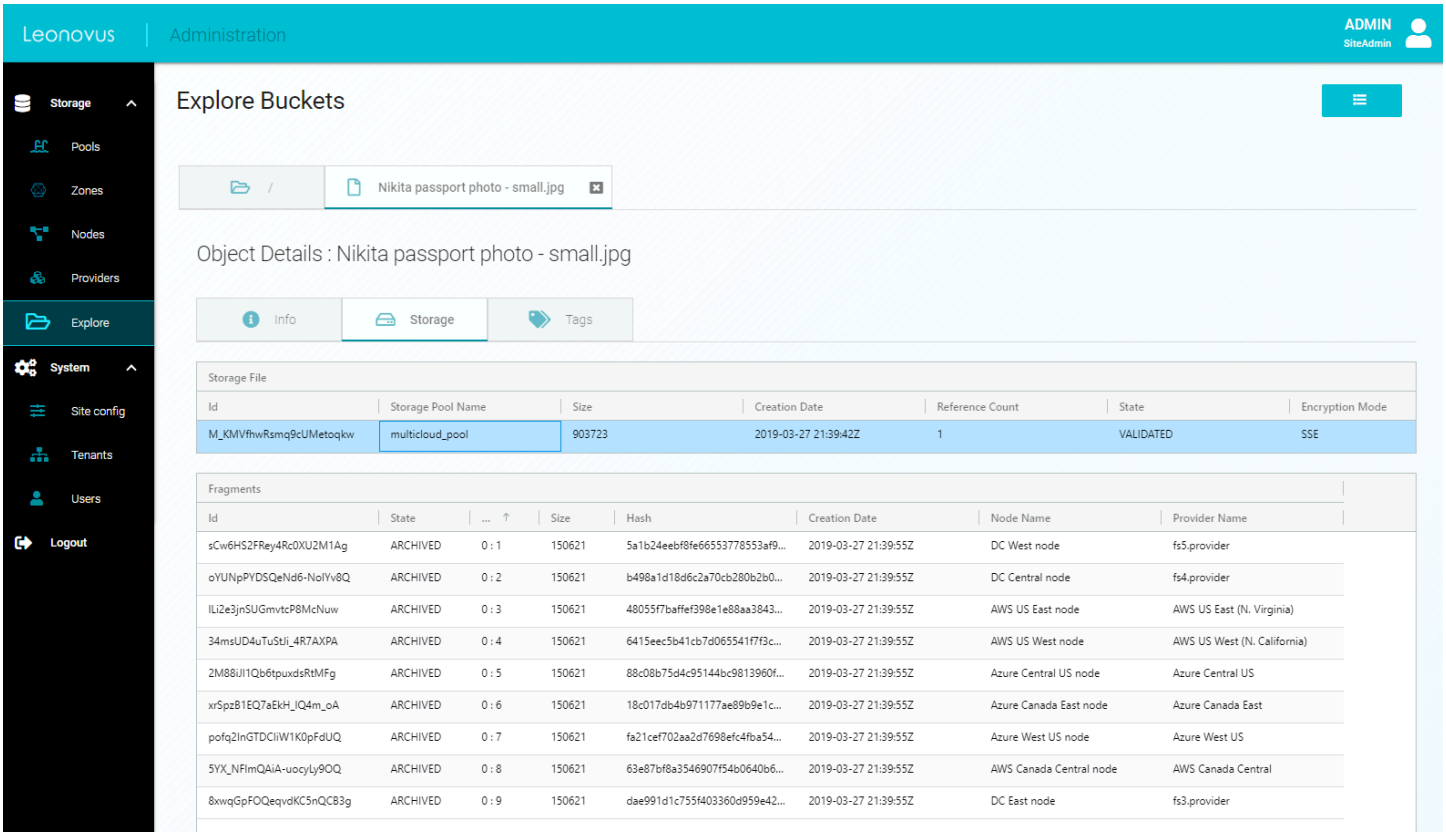
Leonovus offers a compelling solution that unburdens organizations of management and the limitations of traditional enterprise object store infrastructures while providing the benefits of a seamless multi-cloud approach. It creates an abstraction layer (secure data plane) which exposes Amazon S3 and Glacier APIs to applications in the front-end, both on-premises and in the cloud, while managing data placement (with it's unique administrator's user interface) in the backend according to specific policies defined by the end user.

Compared to other multi-cloud data controllers available in the market, Leonovus offers superior security features of particular interest in highly regulated environments, such as healthcare and finance:

- **Encryption and Erasure coding (EC)**: All data is encrypted before leaving the front-end access layer and then segmented and distributed to several back-end repositories (buckets) thanks to EC. This makes it impossible to retrieve information by accessing the backend directly and establishes true data sovereignty.
- **Blockchain:** Every data access transaction can be recorded in a blockchain-based ledger, making it almost impossible to tamper with system logs, while also improving observability and audit activities on every data and metadata operation.
- **Data Integrity**: Leonovus calculates cryptographic hashes of all data it stores and all EC fragments it generates to prevent corruption and tampering.
- **Write-Once-Read-Many (WORM) Locks**: Leonovus allows administrators to place WORM locks on data stored to prevent modification or deletion of data for either a specified period or indefinitely. This capability helps address long term retention requirements mandated by many regulations
- **Data placement policy engine:** Leonovus offers a sophisticated policy engine that allows end users to define rules aimed at placing data where it is most convenient, while respecting durability and allowing for the retrieval of EC segments from cheaper cloud storage providers first, limiting egress fees.
- **Ease of use:** Leonovus offers a straightforward and easy to use web user interface that enables end users to get infrastructure insights quickly from the dashboards, set up policies, and manage object store endpoints.



* Data security, integrity and auditability with encryption, fragmentation and dispersal



Thanks to its innovative architecture and feature set, Leonovus enables enterprises to build large scale multi-cloud data repositories which can be accessed from everywhere with increased security, and that are ready to support applications with strict compliance requirements. This solution also increases freedom of choice for end users by eliminating the risk of obsolescence of on-premises infrastructure and all the costs of painful migrations, while avoiding lock-in with a single service provider, or the creation of cloud storage silos.

4 Key Takeaways

Managing storage in highly regulated environments is becoming more and more challenging. On one side, we have the need for strong security and compliance while; on the other, there are concerns about managing added complexity, costs, scalability, and data outliving several infrastructures and application generations.

Traditional approaches are no longer effective and increasingly riskier, especially in the long term. A multi-cloud strategy seems the most reasonable because of the added infrastructure flexibility but, to make it work properly, a multi-cloud data controller is crucial.

Leonovus offers a multi-cloud controller which presents a feature set that is strongly recommended for highly regulated industries. This platform allows storing data on several public clouds and on-premises infrastructures concurrently and seamlessly, improving the overall level of security while allowing data movement on the back-end transparently to applications and users. Furthermore, administrators can take advantage of Leonovus' policy engine to define rules for optimal data placement and prioritized retrieval, allowing them to keep the right balance between performance and cost.

5 About the Analyst

Enrico has 25+ years of industry experience in technical product strategy and management roles. He has advised mid-market and large enterprises across numerous industries and software companies ranging from small ISVs to large providers.

Enrico is an internationally renowned visionary author, blogger, and speaker on the topic of data storage. He has tracked the changes in the storage industry as a Gigaom Research Analyst, Independent Analyst and contributor to the Register.

6 About GigaOm Research

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

To learn more about how we help transform enterprises in AI-enriched data-driven world, visit https://gigaom.com/about/.