Leonovus

MULTI-CLOUD DATA CONTROLLER

MULTI-CLOUD IS THE SOLUTION, NOT THE PROBLEM

80% of enterprise data is unstructured, and it's growing at more than 55% per year. IT organizations are spending a disproportionate amount of time and resources in managing this growth. A variety of business factors like quick capacity ramp-up in a region or overflowing data sets are leading organizations to a hybrid or multi-cloud path. It is generally agreed – across industries – that hybrid and multi-cloud infrastructure are, or will soon be, the new normal.*

Why Security leaders should be concerned

As the number of clouds and – in general – the amount of data stored increases, the threat surface for an organization increases dramatically. User privacy and data security policies need to be consistently - and verifiably - applied across various clouds. This is a barrier worth breaking because the public cloud offers transformative services that may form the core of your business.

5 CLOUD SECURITY CHALLENGES

- **Data security through its lifecycle**
- **Cloud vendor lock-in**
- **Inflexibility breeds Shadow-IT**
- **Data residency is not data sovereignty**
- **Compliance for long-term retention**

* https://www.datamation.com/big-data/structured-vs-unstructured-data.html

Five cloud security challenges:

• Data security through its lifecycle

Despite the best controls and leading-edge infrastructure, the largest cloud players assure the security "of" their cloud and not data "in" their cloud. Applying policy on a per-cloud level creates security and compliance inconsistencies that can lead to administrative errors and data breaches. You need an overarching data-centric approach to maintain confidentiality, integrity, and availability of your data - whether inflight or at-rest.

• Cloud vendor lock-in

Large public cloud vendors create a Hotel California problem. Getting data in is cheap; however retrievals are expensive and make data migration and external access impractical. Relying entirely on a public cloud vendor for security and compliance leads to migration issues like maintaining long-term retention rules through a migration.

• Inflexibility breeds Shadow-IT

Lock-in or over-reliance on cloud provider infrastructure may create conflict with the ever-evolving needs of your LOBs. With their needs unmet, the LOBs tend to procure alternative solutions and further complicate policy and security compliance.

• Data residency is not data sovereignty

Data sovereignty cannot be taken for granted with the public cloud. Cloud vendors, in recent years, have increasingly deployed data centres local to specific regions but that alone is not enough to assure sovereignty of your data. The fine print allows them to move data across borders and to expose your data and keys -without notice - to agencies outside of your sovereign borders. You need a strategy and the tools that give you exclusive access to your data and keys.

• Compliance for long-term retention

Auditable integrity and long-term secure retention of data is a common requirement for businesses. Migrating workloads across multiple clouds makes it difficult to maintain policy-based controls. Also, you likely lose the chain of custody when you distribute or migrate workloads across your ecosystem. You need a data-centric approach to implement policy associated with the data, and not back-end storage infrastructure.

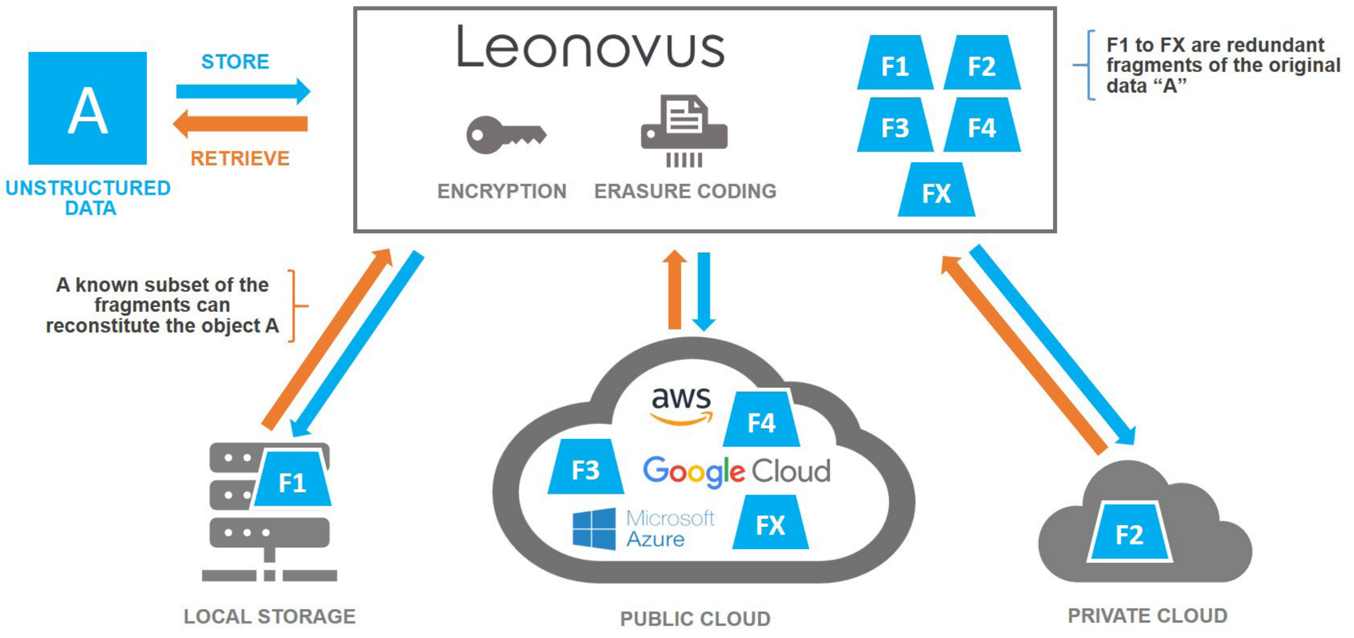
The more broadly you spread your data - the more secure your data will be.

Embrace the multi-cloud with Leonovus

Leonovus is a multi-cloud data controller that acts as a unified storage target for all applications and storage. You can now create a long-term security strategy that:

- Puts you in control of your data's security by decoupling data from the underlying infrastructure
- Mitigates data breaches and establishes true data sovereignty by storing discretely indecipherable data in public clouds
- Minimizes administrative error through a single pane of glass for applying consistent security policy
- Is tailored to each of your data sets with granular control of data placement, key management and long-term retention
- Provides an immutable chain of custody and mechanisms to ensure data integrity

THE MULTI-CLOUD DATA CONTROLLER APPROACH



TECHNICAL INFORMATION

- Software-based solution deployed as a virtual appliance on-premises or in-cloud
- Supports S3 and Glacier-compatible storage interfaces
- Data optimization through proprietary erasure-coding algorithm and de-duplication
- AES-256 Encryption and SHA-256 crypto hashes for integrity checks
- FIPS 140-2 compliant
- Chain of custody through Hyperledger-based private blockchain

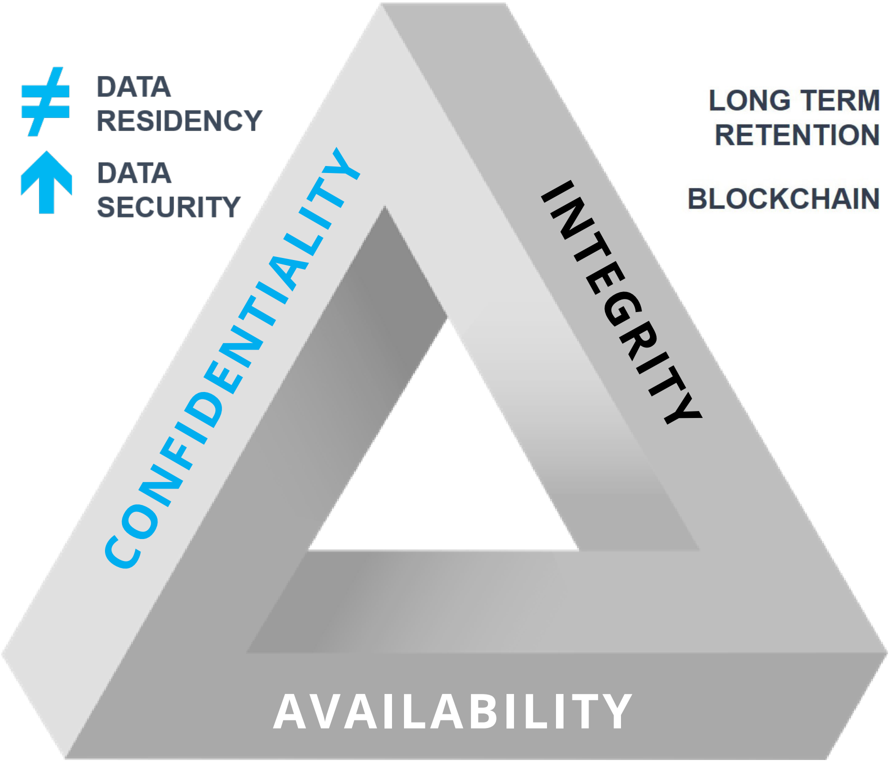
Realities of Cloud Storage Security

DATA SOVEREIGNTY ≠ DATA RESIDENCY

MULTI-CLOUD ↑ DATA SECURITY

LONG TERM RETENTION > POLICY

BLOCKCHAIN = CHAIN OF CUSTODY



CLOUD PROVIDER SLAs ≠ DATA DURABILITY

HIGH AVAILABILITY = MULTI-CLOUD

CONFIDENTIALITY

- Implement true data sovereignty that goes beyond data residency offered by cloud provider regions
- Spread your data across multiple clouds while ensuring that data is never exposed to cloud providers

INTEGRITY

- Adopt storage strategies that allow you to benefit from ever-evolving cloud offerings and address long term data retention requirements
- Harness private blockchain technology to establish a cryptographically-verifiable history of all access to your data

AVAILABILITY

- Ensure you never lose your data by providing data durability beyond the limits of cloud provider SLAs
- Achieve higher availability of your data by minimizing the affects of cloud or network outages

Visit leonovus.com to learn how multi-cloud data controller can address your business needs.
Follow us on: LinkedIn | Twitter (@LeonovusInc) | Facebook