fragmentiX CLUSTER®
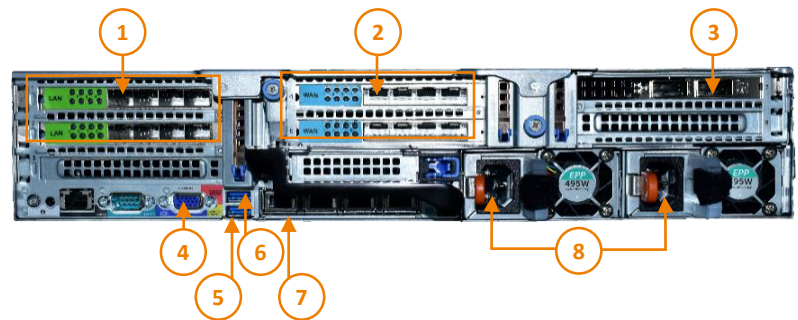## ... to use hybrid/multi cloud storage without risks

fragmentiX CLUSTER® is the high-performance model of the fragmentiX® storage appliance product family for GDPR-compliance, privacy protection, and data loss protection enabling real digital sovereignty. The highly efficient and redundant design of the cluster hardware is perfectly suited for use in datacenters of enterprises, service providers and governments.

First and only world-wide commercially available quantum-computer safe standard cloud storage solution

➤ Privacy by design

➤ Highest protection against several traditional cyber risks and quantum computer attacks

➤ High availability of data and strong resilience against data loss

➤ Compatible with all relevant cloud storages

➤ Easy-to-use with the fragmentiX® desktop client software for Windows and MacOS environments or directly as S3 proxy

➤ 5 years mission-critical hardware support & repair within 4 hours worldwide – performed by DELL

❖ Two fault-tolerant industrial grade hardware cluster nodes which act as a 'failover system'

❖ Hardened frXOS operating system

❖ Secret-sharing algorithms

1 | 8 x 10 Gbit/s LAN SFP+
2 | 8 x 10 Gbit/s WAN SFP+
3 | 2 x CLUSTERNET
4 | 1 x VGA console
5 | 1 x USB CONFIG ENABLE
6 | 1 x USB CONFIG STORE
7 | 1 x 1 Gbit/s CONFIG NET
8 | 2 x 495 W power supply

Technical specification of a single fragmentiX CLUSTER® NODE

Application environments	datacenters	LAN interfaces	8 x 10 Gbit/s SFP+
Max. storage LOCATIONs	26	WAN interfaces	8 x 10 Gbit/s SFP+
fragmentiX desktop client	unlimited, 50 licenses incl.	Size	19", 2U
fragmentiX NANO satellites	unlimited, not included	Weight	ca. 23 kg
frXOS firmware/OS updates	1 year included	AC input	100-230 V AC, 50/60 Hz
HW mission critical support	5 years included	Power supply	2 x 495 W redundant

Privacy by design: Information-Theoretic Security with Secret Sharing
Secret sharing algorithms guarantee information-theoretic security (ITS) for the data stored with the fragmentiX CLUSTER®. The data - no matter what files or directory structures - are divided into a number of fragments and each of them is stored on a different storage LOCATION. Any single fragment does not contain any information about the original data. Not even a small number of stolen / hacked fragments means a threat to your data's privacy - only a sufficient number of fragments allows the data to be restored.

Highest protection against several traditional cyber risks and quantum computer attacks
The fragmentiX® product range brings protection against storage (data on rest) related traditional cyber risks.
A data leak from your cloud provider or a misconfigured S3 bucket will not lead to disaster - because no provider or bucket alone contains abusable content. Typical insider and administrator threats can be largely mitigated by splitting responsibilities and using

a fragmentiX® central design principle: There is no longer a need to trust a single storage provider or your storage administrators. Many countries and large companies are investing billions of USD/EURO/RMB every year in the development of larger quantum computers. Among many positive effects, quantum computers will also pose additional risks to existing encryption technologies and products in the near future - leading to a new kind of arms race in information warfare.

The fragmentiX® product range protects your sensitive data stored in cloud storages against the newly emerging cyber risks posed by large quantum computers: Several attackers are already collecting encrypted data streams on a large scale in order to be able to decrypt and abuse this stolen information later on with quantum computers.

As a result, there is already a high urgency to protect cloud data.

fragmentiX® products are the best way to increase the protection of sensitive data against traditional and quantum computer threats - today and tomorrow!

High availability of data and strong resilience against data loss

Regionally or globally distributed, redundant storage LOCATIONs in different regions or data centers used by the fragmentiX® appliance increase the availability of data even if individual parts of the internet or the company's own networks fail. The use of multiple redundant fragments provides a high level of robustness against data loss even if individual fragments fail.

Easy-to-use with fragmentiX® desktop client software or directly as S3 proxy

In a typical scenario, the fragmentiX® appliance provides network drives on its LAN side to the existing desktop PCs and servers with the fragmentiX® desktop client. On its WAN side, the fragmentiX® appliance stores the created fragments in the configured LOCATIONs, e.g. S3 buckets at your cloud providers.

If your applications already use S3 storage you can simply add the fragmentiX® appliance as an S3 proxy without having to change your application and without any additional client software.

Multiple storage types reachable over multiple WAN/LAN/VPN connections

The following storage types can be used with fragmentiX CLUSTER®:

- S3 and S3 compatible hybrid/multi cloud storage on the internet and/or intranet
- Microsoft Azure Blob storage
- NFS compatible storages

All data stored with the fragmentiX CLUSTER® is divided into fragments using threshold cryptography and stored on the predefined LOCATIONs - NO user data remains locally on the fragmentiX CLUSTER®. Choosing and combining up to 26 LOCATIONs allows to achieve better security and resilience than any other single storage solution can offer.

Hardened operating system frXOS

frXOS - the fragmentiX CLUSTER®'s hardened operating system - was developed by fragmentiX® to make it both secure and easy to use for users and administrators. All functions are kept up to date through regular updates, which can be carried out locally by the administrator. A valid maintenance contract is required to receive the latest frXOS updates beyond the first year after delivery of your system.

Industrial grade hardware and advanced protection measures

All fragmentiX CLUSTER® systems are prebuilt by DELL Technologies and the sensitive components and software are finished in Austria, to guarantee no backdoors or intended weaknesses are built into our products. The use of state-of-the-art Crypto-USB sticks ensures that all security-relevant data can only be read on the respective fragmentiX CLUSTER® and modified by the authorized administrator. Optionally, QKD devices and advanced link encryptors can be added to increase the level of data protection, if required.

For further information:

www.fragmentix.com | sales@fragmentix.com | +43 2243 24203

fragmentiX Storage Solutions GmbH
IST Austria Technology Park, Ploecking 1
3400 Klosterneuburg
Austria, Europe

In cooperation with