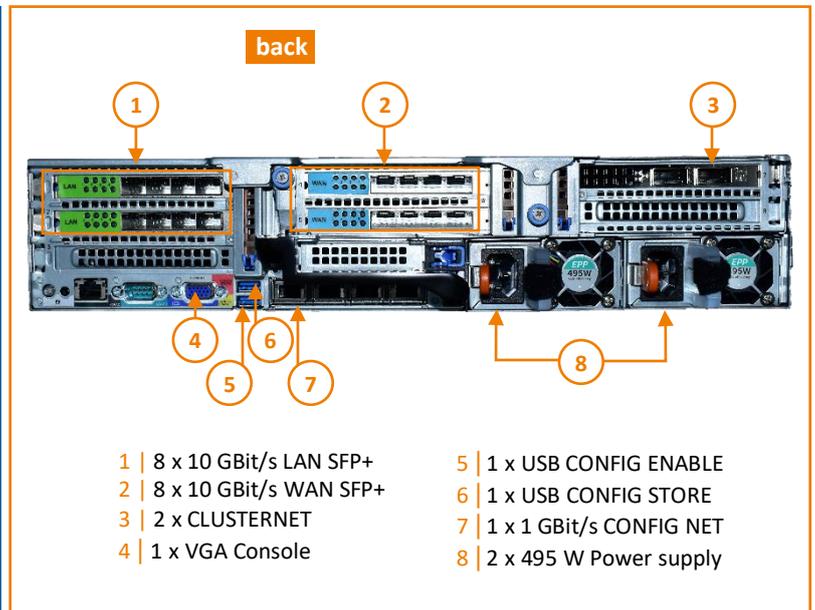


Digital Sovereignty with fragmentiX[®] CLUSTER

Your advantages:

- Cryptographic guarantee through Secret Sharing and thereby Quantum Safe
- High data availability for own use or for the provision of an information theoretically secure storage possibility
- Hardened appliance with simplest use and full integration in Windows, Linux and Apple environments
- 5 year mission critical hardware support & repair worldwide



fragmentiX[®] CLUSTER is the multi-client capable high performance model of the fragmentiX[®] Storage Appliance. The highly efficient and redundantly designed cluster hardware is designed for use in data centers and company headquarters as well as for service providers and consists of two fault-tolerant cluster nodes.

fragmentiX[®] CLUSTER ensures with Secret Sharing that data is protected with real so-called ITS (Information Theoretical Security). Data is stored completely transparently for the administrator on up to 26 freely definable storage locations in S3 compatible buckets. The optimal mix of public and private S3 storage locations can be selected for each use case using a scenario definition. The desired effect can be achieved for each user group or each individual customer:

- High data resilience
- Low-cost long-term archiving
- ITS protected backup files in the cloud
- High-performance-data storage
- Nextcloud services for clients
- S3 integration as proxy in existing applications without changing the application

The frXOS operating system provides multi-client capability at the green marked "LAN ports" of the fragmentiX[®] CLUSTER network drives for all common network protocols. Even in mixed environments, the appropriate drive shares can be provided simultaneously for Windows, Apple and Linux devices.

Directories and files that are copied or moved to these "fragmentiX[®] drives" are divided into several fragments after a short processing time and stored on the storage locations defined for them. For "reading" or editing, these fragments are then made available to the users by these storage locations at the network drive/share. For the users, it is not recognizable that the data is not stored on the local file server, but is stored with fragmentiX[®].

SECRET SHARING – Safety through sharing

A separate configuration can be created for each conceivable use case. By specifying the "frX Ratio" you determine how many of the generated fragments are required to restore the original data. The smallest "frX Ratio" of 2/3 or "2 out of 3" means that of 3 generated fragments at least 2 are required to restore the data. It does not matter which 2 files from the set of 3 fragments are available - all fragments are equal.

INFORMATION-THEORETICAL SECURITY

Thanks to its secure and hardened architecture and the use of secret sharing algorithms, tested over many years, the fragmentiX[®] CLUSTER offers a solution with a cryptographic guarantee. No single fragment contains usable information for an attacker. No part of the original file can be recovered or cracked. The self-defined number of fragments generated and required for reading guarantees that access and reading is only possible by having the minimum number of fragments.

Supported system environments

fragmentiX[®] CLUSTER can be integrated into existing IT environments with the following protocols:

- SMB Samba Shares for Windows Networks incl. AD
- NFS versions 3 and 4 for Linux and Unix operating systems
- AFP for current Apple MacOS environments
- Apple Time Machine Backup & Restore
- Numerous commercial and open source backup solutions
- S3 based storage solutions

Storage locations

All data stored with the fragmentiX[®] CLUSTER are stored as fragments on the defined storage locations after the cryptographic division into fragments - NO data remains locally on the fragmentiX[®] CLUSTER.

The following storage types can be selected as storage locations:

- S3 compatible cloud storage on the Internet
- Local S3 compatible memory available in LAN / VPN

The different storages can be combined in any way and a variety of effects such as extreme resistance or digital long-term availability are made possible.

Due to the increased redundancy provided by the fragmentiX[®] CLUSTER, cheaper storage providers can be selected or combined with premium providers and/or local S3 storage.

Configuration and protection measures

Changes to the configuration can only be made by an administrator via a specially protected web interface.

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 authorised administrator. Without the yellow "CONFIG ENABLE" USB stick, no one can access the sensitive information.

Technical specifications per node:

fragmentiX[®] CLUSTER

Max. number of storage locations	26
Number of LAN interfaces	8 x 10 GBit/s
Number of WAN interfaces	8 x 10 GBit/s
Size (W x D x H) in mm	19" 4U
Weights (kg)	ca. 60
Application environments	Datacenter, Provider
frXOS 1 year updates	included
HW 5 year mission critical support	included

Power

AC Input	100-230 V AC
Power Supply Capacity	2 x 495 W

Multi-client capability

The fragmentiX[®] CLUSTER offers service providers the possibility to provide each client / customer with a data-technically isolated usage environment. Depending on the performance requirements of the individual customers, several hundred individual customers can also be served with a fragmentiX[®] CLUSTER. In principle, a customer-dependent cost allocation (CDR) is possible and can be implemented for a fee based on the requirements.

Industrial Hardware

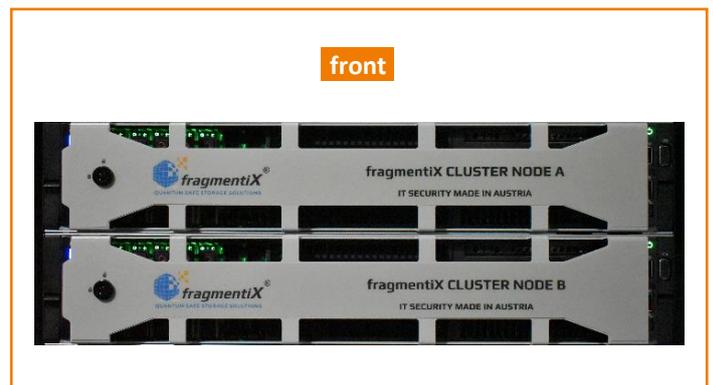
The fragmentiX[®] CLUSTER, which is finished in Austria, is designed for long-term stable operation without hardware maintenance. To protect against theft and manipulation by unauthorized persons, the device is prepared for installation in protected rooms with 19 inch server racks.

Hardened frXOS software environment

frXOS - the hardened operating system of the fragmentiX[®] CLUSTER - was developed in order to make the use for users and administrators both secure and simple. All functions are kept up to date through regular updates, which can be carried out either via the Internet or via USB sticks sent to the user. A valid maintenance contract is required to receive the latest frXOS updates at the end of the first year.

Multi WAN

In order to make it more difficult for attackers to intercept fragments, several WAN connections and ISPs should be used.



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 AIT – Austrian Institute of Technology

