fragmentiX NANO®

... to use hybrid cloud storage without risks

The fragmentiX NANO® acts as a satellite appliance to the fragmentiX CLUSTER® storage appliances. Every fragmentiX CLUSTER® administrator can configure an unlimited number of fragmentiX NANO® appliances to enable home office and nomadic users to access sensitive data even when at home or in a hotel. It ensures data protection and strong resilience for your valuable data in the cloud like backups, documents or any other sensitive data to be protected in hybrid/multi cloud storages.
The fragmentiX NANO® comes bundled with the fragmentiX® desktop client software for Windows and MacOS. It enables new work models such as working from home or working while traveling with highest security. Your data can easily be mapped as Windows or Mac network drive. The fragmentiX NANO® uses three storage LOCATIONs and up to two independent internet connections.

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

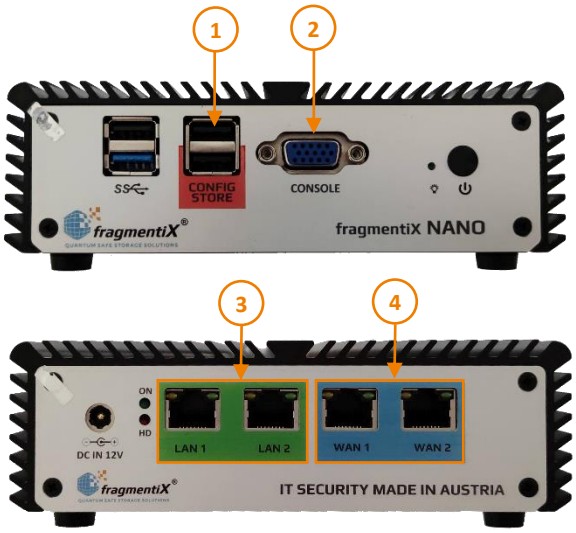
High availability of data and strong resilience against data loss

Compatible with all relevant cloud storage protocols and providers

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

Hardened frXOS operating system

Secret-sharing algorithms



1 | 1 x USB CONFIG STORE
2 | 1 x VGA CONSOLE
3 | 2 x 1 Gbit/s LAN
4 | 2 x 1 Gbit/s WAN

Technical specification of fragmentiX NANO®

Application environments	Working from home or while traveling in conjunction with fragmentiX CLUSTER®	**LAN interfaces**	2 x 1 Gbit/s
		WAN interfaces	2 x 1 Gbit/s
		Size	154 x 128 x 49 mm
Max. # of storage LOCATIONs	3	**Weight**	0.7 kg
fragmentiX desktop client	unlimited, 1 licence incl.	**AC input**	100-230 V AC
frXOS firmware/OS updates	1 year included		

Privacy by design: Quantum Computer Safe Storage with Secret Sharing

Secret sharing algorithms guarantee Quantum Computer Safe Storage for the data stored with the fragmentiX NANO®. 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 future 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 won't 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 hybrid 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 future 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 with the fragmentiX® desktop client.
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

On its WAN side, the fragmentiX® appliance stores the created fragments in the configured LOCATIONs, e.g. S3 buckets at your cloud providers.
The following storage types can be used with fragmentiX NANO®:

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

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

Hardened operating system frXOS

frXOS - the fragmentiX NANO®'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.

Advanced protection measures

The use of state-of-the-art Crypto-USB sticks ensures that all security-relevant data can only be read on the respective fragmentiX NANO® and modified by the authorised 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
xista science park, Ploecking 1
3400 Klosterneuburg
Austria, Europe

In cooperation with