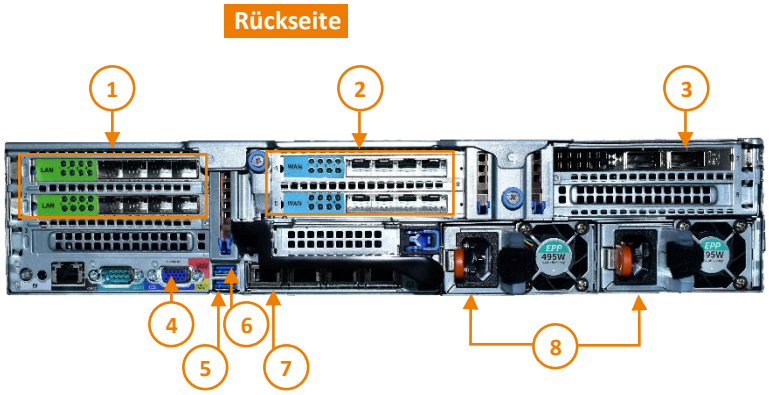
fragmentiX®
QUANTUM SAFE STORAGE SOLUTIONS

IT SECURITY MADE IN AUSTRIA

Digitale Souveränität mit fragmentiX® CLUSTER

Ihre Vorteile:

- Kryptografische Garantie durch Secret Sharing und dadurch Quantum Safe
- Hohe Datenverfügbarkeit für eigene Nutzung oder zur Bereitstellung einer informationstheoretisch sicheren Speichermöglichkeit
- Gehärtete Appliance mit einfachster Nutzung und voller Integration in Windows, Linux und Apple Umgebungen
- 5 Jahre mission critical Support & Reparatur vor Ort weltweit



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

fragmentiX® CLUSTER ist das mandantenfähige High Performance Modell der fragmentiX® Storage Appliance. Die höchst leistungsfähige und redundant ausgelegte Cluster Hardware ist für den Gebrauch in Rechenzentren und Firmenhauptsitzen sowie für Serviceprovider konstruiert und besteht aus zwei fehlertolerant ausgeführten Cluster Nodes.

fragmentiX® CLUSTER stellt mit Secret Sharing sicher, dass Daten mit echter s.g. ITS (Informationstheoretischer Sicherheit) geschützt sind. Daten werden für den Administrator vollkommen transparent auf bis zu 26 frei definierbare Speicherlokationen in S3 kompatiblen Buckets abgelegt. Es kann für jeden Anwendungsfall über eine Szenariodefinition die optimale Mischung aus Public und Private S3 Speicherlokationen gewählt werden. Für jede AnwenderInnengruppe oder jeden/jede Einzelkunden/in kann der gewünschte Effekt erzielt werden:

- Hohe Datenresilienz
- Günstige Langzeitarchivierung
- ITS geschützte Backupdateien in der Cloud
- High-Performance-Datenspeicherung
- Nextcloud Services für Mandanten
- S3 Integration als Proxy in bestehende Anwendungen ohne Änderung der Applikation

Mandantenfähig stellt das frXOS Betriebssystem an den grün markierten „LAN- Anschlüssen“ des fragmentiX® CLUSTER Netzlaufwerke für alle gängigen Netzwerkprotokolle zur Verfügung. Auch in gemischten Umgebungen können für Windows, Apple und Linux Geräte die passenden Laufwerkfreigaben gleichzeitig bereitgestellt werden.

Verzeichnisse und Dateien, die auf diese „fragmentiX® Laufwerke“ kopiert oder verschoben werden, sind nach einer kurzen Verarbeitungszeit in mehrere Fragmente aufgeteilt und auf den dafür definierten Speicherlokationen abgespeichert. Zum „Lesen“ oder Bearbeiten werden diese Fragmente dann von diesen Speicherlokationen wieder den AnwenderInnen am Netzlaufwerk/Share zur Verfügung gestellt. Für die AnwenderInnen ist es nicht erkennbar, dass nicht am lokalen Fileserver gespeichert wird, sondern besonders zu schützende Daten mit fragmentiX® abgelegt werden.

SECRET SHARING – Sicherheit durch Teilen

Für jeden denkbaren Anwendungsfall kann eine eigene Konfiguration angelegt werden. Durch das Festlegen des „frX Ratio“ legen Sie selbst fest wie viele der erzeugten Fragmente erforderlich sind um die Originaldaten wiederherstellen zu können. Der kleinste „frX Ratio“ von 2/3 oder „2 aus 3“ bedeutet, dass von 3 erzeugten Fragmenten zumindest 2 zum Wiederherstellen der Daten erforderlich sind.
Es spielt dabei keine Rolle „welche 2“ Dateien aus der Menge der 3 Fragmente verfügbar sind – alle Fragmente sind gleichwertig.

INFORMATIONSTHEORETISCHE SICHERHEIT

Durch ihre abgesicherte und gehärtete Architektur und die Nutzung langjährig geprüfter Secret Sharing Algorithmen bietet der fragmentiX® CLUSTER eine Lösung mit kryptografischer Garantie. Kein einzelnes Fragment enthält für einen Angreifer/eine Angreiferin nutzbare Informationen. Es kann auch kein Teil der ursprünglichen Datei wiederhergestellt oder geknackt werden.
Durch die selbst festgelegte Anzahl an erzeugten und zum Lesen erforderlichen Fragmenten kann garantiert werden, dass erst durch den Besitz der Mindestanzahl an Fragmenten das Zugreifen und Lesen ermöglicht wird.

Unterstützte Systemumgebungen

fragmentiX® CLUSTER kann mit folgenden Protokollen in bestehende IT-Umgebungen eingebunden werden:

- SMB Samba Shares für Windows und Linux Netzwerke inkl. AD
- NFS Version 3 und 4 für Linux und Unix Betriebssysteme
- AFP für aktuelle Apple MacOS Umgebungen
- Apple Time Machine Backup & Restore
- Nextcloud Services
- Zahlreiche kommerzielle und Open Source Backuplösungen
- S3 basierte Storagelösungen

Speicherlokationen

Alle mit dem fragmentiX® CLUSTER gespeicherten Daten werden nach der kryptografischen Teilung in Fragmente als Fragmente auf den definierten Speicherlokationen abgelegt - es bleiben keine Daten lokal auf dem fragmentiX® CLUSTER zurück. Als Speicherlokationen können folgende Speichertypen gewählt werden:

- S3 kompatibler Cloudspeicher im Internet
- Im LAN / VPN verfügbarer lokaler S3 kompatibler Speicher

Die unterschiedlichen Speicher können beliebig kombiniert werden und es wird eine Vielzahl von Effekten wie extreme Widerstandsfähigkeit oder digitaler Langzeitverfügbarkeit ermöglicht.
Durch die, von dem fragmentiX® CLUSTER gelieferte, erhöhte Redundanz können günstigere Speicheranbieter gewählt werden oder mit Premiumanbietern und/oder lokalem S3 Storage kombiniert werden.

Konfiguration und Schutzmechanismen

Änderungen an der Konfiguration können nur über ein besonders geschütztes WEB-Interface von einem Administrator durchgeführt werden.

Durch die Nutzung modernster Crypto-USB-Sticks wird sichergestellt, dass alle sicherheits-relevanten Daten nur auf der jeweiligen fragmentiX® CLUSTER gelesen und vom berechtigten Admin verändert werden können. Ohne den gelben „CONFIG ENABLE“ USB-Stick kann niemand auf die sensitiven Informationen zugreifen.

Mandantenfähigkeit

Dienstleistern bietet der fragmentiX® CLUSTER die Möglichkeit jedem Mandanten/Kunden eine datentechnisch isolierte Nutzungsumgebung zur Verfügung zu stellen. Abhängig vom Leistungsbedarf der einzelnen Kunden können mit einem fragmentiX® CLUSTER auch mehrere hundert Einzelkunden bedient werden. Eine kundenabhängige Leistungsverrechnung (CDR) ist prinzipiell möglich und kann basierend auf den Anforderungen kostenpflichtig implementiert werden.

Industrielle Hardware

Der, in Österreich endgefertigte fragmentiX® CLUSTER, ist für langjährigen stabilen Betrieb ohne Hardwarewartung ausgelegt. Zum Schutz gegen Diebstahl und Manipulation durch Unberechtigte ist das Gerät für die Montage in geschützten Räumen mit 19 Zoll Serverracks vorbereitet.

Gehärtete frXOS Softwareumgebung

Um die Nutzung für Anwender und Administratoren sowohl sicher aber dennoch einfach zu gestalten wurde frXOS – das gehärtete Betriebssystem der fragmentiX® CLUSTER entwickelt. Durch regelmäßige Updates, die wahlweise entweder via Internet oder zugesendetem USB Sticks erfolgen können, werden sämtliche Funktionen auf dem aktuellen Stand der Technik gehalten. Voraussetzung zum Erhalt der aktuellen frXOS Updates ist nach Ablauf des ersten Jahres ein gültiger Wartungsvertrag.

Multi WAN

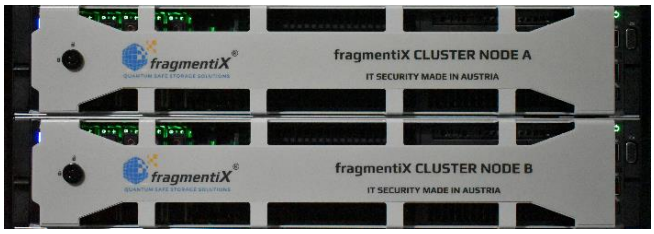
Um Angreifern und Angreiferinnen das Abfangen von Fragmenten zu erschweren sollten möglichst mehrere WAN Anbindungen und ISP‘s genutzt werden.

Technische Merkmale pro Node:

fragmentiX® CLUSTER	
Max. Anzahl an Speicherlokationen	26
Anzahl von LAN interfaces	8 x 10 GBit/s
Anzahl von WAN interfaces	8 x 10 GBit/s
Größe (W x D x H) in mm	19“ 4U
Gewicht (kg)	ca. 60
Anwendungsumgebungen	Datacenter, Provider
frXOS 1 Jahr Updates	inkludiert
HW 5 Jahre mission critical Support	inkludiert

Power	
AC Input	100 - 230 V AC
Netzteilleistung	2 x 495 W

Vorderseite



Für weitere Informationen:
www.fragmentix.com | sales@fragmentix.com | +43 2243 24203

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

Entwickelt in Kooperation mit dem AIT – Austrian Institute of Technology