fragmentiX CLUSTER®

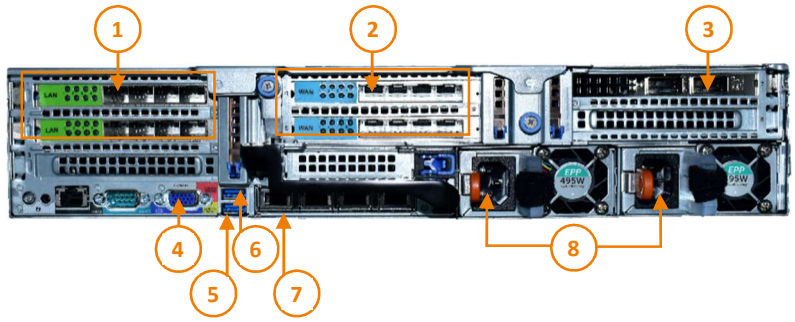
Hybrid-/Multi-Cloud-Speicher ohne Risiken zu nutzen

fragmentiX CLUSTER® ist das High-Performance-Modell der fragmentiX® Storage Appliance Produktfamilie für DSGVO-Compliance, Datenschutz und Absicherung gegen Datenverlust für echte digitale Souveränität. Das hocheffiziente und redundante Design der Cluster-Hardware eignet sich perfekt für den Einsatz in Rechenzentren von Unternehmen, Dienstleistern und Behörden.

Erste und einzige weltweit kommerziell verfügbare, quantencomputersichere Standard-Cloud-Speicherlösung

- Datenschutz durch Design
- Höchster Schutz gegen verschiedene traditionelle Cyber-Risiken und Quantencomputer-Angriffe
- Hochverfügbarkeit der Daten und hohe Ausfallsicherheit
- Kompatibel mit allen relevanten Cloud-Speichern
- Einfache Nutzung mit der fragmentiX® Desktop-Client-Software für Windows- und MacOS-Umgebungen oder direkt als S3-Proxy
- 5 Jahre unternehmenskritischer Hardware-Support & Reparatur innerhalb von 4 Stunden weltweit - durchgeführt von DELL

- Zwei ausfallsichere, industrietaugliche Hardware-Cluster-Knoten, die als "Failover-System" fungieren
- Gehärtetes frXOS-Betriebssystem
- Secret Sharing Algorithmen



1 | 8 x 10 Gbit/s LAN SFP+
2 | 8 x 10 Gbit/s WAN SFP+
3 | 2 x CLUSTERNET
4 | 1 x VGA Konsole
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 Stromanschluss

Technische Spezifikation eines einzelnen fragmentiX CLUSTER® NODE

Anwendungsumgebungen	Datacenter	**LAN Schnittstellen**	8 x 10 Gbit/s SFP+
Max. # Speicher-LOCATIONs	26	**WAN Schnittstellen**	8 x 10 Gbit/s SFP+
fragmentiX Desktop-Client	unlimitiert, 50 Lizenzen incl.	**Größe**	19”, 2HE
fragmentiX NANO Satelliten	unlimitiert, nicht inkludiert	**Gewicht**	ca. 23 kg
frXOS firmware/OS Updates	1 Jahr inkludiert	**Spannung, Frequenz**	100-230 V AC, 50/60 Hz
HW-Mission-Critical Support	5 Jahre inkludiert	**Stromversorgung**	2 x 495 W redundant

Privatsphäre durch Design: Informationstheoretische Sicherheit mit Secret Sharing

Secret-Sharing-Algorithmen garantieren informationstheoretische Sicherheit (ITS) für die mit dem fragmentiX CLUSTER® gespeicherten Daten. Die Daten - egal ob Dateien oder Verzeichnisse - werden in eine Anzahl von Fragmenten aufgeteilt und jedes dieser Fragmente wird auf einer anderen Speicher-LOCATION gespeichert. Jedes einzelne Fragment enthält keine Informationen über die ursprünglichen Daten. Nicht einmal eine kleine Anzahl gestohlener/gehackter Fragmente stellt eine Bedrohung für die Privatsphäre Ihrer Daten dar - nur eine ausreichende Anzahl von Fragmenten ermöglicht die Wiederherstellung der Daten.

Höchster Schutz gegen verschiedene traditionelle Cyber-Risiken und Quantencomputer-Angriffe

Die fragmentiX®-Produktpalette bietet Schutz gegen traditionelle Cyber-Risiken im Zusammenhang mit der Speicherung („data on rest“). Ein Datenleck bei Ihrem Cloud-Provider oder ein falsch konfigurierter S3-Bucket führt nicht zu einer Katastrophe - denn kein Provider oder Bucket allein enthält missbrauchbare Inhalte. Typische Bedrohungen durch Insider und Administratoren

können durch die Aufteilung der Verantwortlichkeiten und der Anwendung eines fragmentiX®-zentrierten Designprinzips weitgehend entschärft werden: Es ist nicht mehr notwendig, einem einzigen Speicheranbieter oder Ihren Speicheradministratoren zu vertrauen. Viele Länder und große Unternehmen investieren jedes Jahr Milliarden von USD/EURO/RMB in die Entwicklung größerer Quantencomputer. Neben vielen positiven Effekten werden Quantencomputer in naher Zukunft auch zusätzliche Risiken für bestehende Verschlüsselungstechnologien und -produkte mit sich bringen - was zu einer neuen Art von Wettrüsten in der Informationskriegsführung führen wird.
Die fragmentiX®-Produktpalette schützt Ihre sensiblen Daten, die in Cloud-Speichern liegen, vor den neu entstehenden Cyber-Risiken, die von großen Quantencomputern ausgehen: Einige Angreifer sammeln bereits im großen Stil verschlüsselte Datenströme, um diese gestohlenen Informationen später mit Quantencomputern entschlüsseln und missbrauchen zu können. Daher besteht bereits jetzt eine hohe Dringlichkeit, Cloud-Daten zu schützen.
fragmentiX® Produkte sind der beste Weg, um den Schutz sensibler Daten gegen traditionelle und Quantencomputer-Bedrohungen zu erhöhen - heute und morgen!

Hohe Datenverfügbarkeit und starke Resilienz gegen Datenverlust

Regional oder global verteilte, redundante Speicher-LOCATIONs in verschiedenen Regionen oder Rechenzentren, die von der fragmentiX®-Appliance genutzt werden, erhöhen die Verfügbarkeit der Daten auch bei Ausfall einzelner Teile des Internets oder der unternehmenseigenen Netzwerke. Der Einsatz mehrerer redundanter Fragmente bietet ein hohes Maß an Robustheit gegen Datenverlust, selbst wenn einzelne Fragmente ausfallen.

Easy-to-use mit fragmentiX® Desktop Client Software oder direkt als S3-Proxy

In einem typischen Szenario stellt die fragmentiX®-Appliance auf ihrer LAN-Seite den vorhandenen Desktop-PCs und Servern mit dem fragmentiX®-Desktop-Client Netzlaufwerke zur Verfügung. Auf der WAN-Seite speichert die fragmentiX®-Appliance die erstellten Fragmente in den konfigurierten LOCATIONs, z.B. S3-Buckets bei Ihren Cloud-Anbietern.
Wenn Ihre Anwendungen bereits S3-Speicher nutzen, können Sie die fragmentiX®-Appliance einfach als S3-Proxy hinzufügen, ohne Ihre Anwendung ändern zu müssen und ohne zusätzliche Client-Software.

Mehrere Speichertypen über mehrere WAN/LAN/VPN-Verbindungen erreichbar

Die folgenden Speichertypen können mit fragmentiX CLUSTER® genutzt werden:

- S3 und S3-kompatibler Hybrid-/Multi-Cloud-Speicher im Internet und/oder Intranet
- Microsoft Azure Blob-Speicher
- NFS-kompatible Speicher

Alle mit dem fragmentiX CLUSTER® gespeicherten Daten werden mittels Schwellenwertkryptographie in Fragmente aufgeteilt und auf den vordefinierten LOCATIONs gespeichert - KEINE Nutzerdaten verbleiben lokal auf dem fragmentiX CLUSTER®. Durch die Auswahl und Kombination von bis zu 26 LOCATIONs wird eine bessere Sicherheit und Ausfallsicherheit erreicht, als es jede andere Speicherlösung bieten kann.

Gehärtetes Betriebssystem frXOS

frXOS - das gehärtete Betriebssystem des fragmentiX CLUSTER® - wurde von fragmentiX® entwickelt, um es für Benutzer und Administratoren sowohl sicher als auch einfach zu bedienen zu machen. Alle Funktionen werden durch regelmäßige Updates, die lokal vom Administrator durchgeführt werden können, auf dem neuesten Stand gehalten. Um die neuesten frXOS-Updates über das erste Jahr nach Auslieferung Ihres Systems hinaus zu erhalten, ist ein gültiger Wartungsvertrag erforderlich.

Industrietaugliche Hardware und fortschrittliche Schutzmaßnahmen

Alle fragmentiX CLUSTER® Systeme werden von DELL Technologies vorgefertigt und die sensiblen Komponenten und Software werden in Österreich fertiggestellt, um zu garantieren, dass keine Hintertüren oder beabsichtigte Schwachstellen in unsere Produkte eingebaut werden. Durch den Einsatz modernster Crypto-USB-Sticks wird sichergestellt, dass alle sicherheitsrelevanten Daten nur auf dem jeweiligen fragmentiX CLUSTER® gelesen und vom autorisierten Administrator verändert werden können. Optional können QKD-Bausteine und fortschrittliche Link-Encryptors hinzugefügt werden, um das Datenschutzniveau zu erhöhen.

Für weitere Informationen:

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

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

In Kooperation mit

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY