

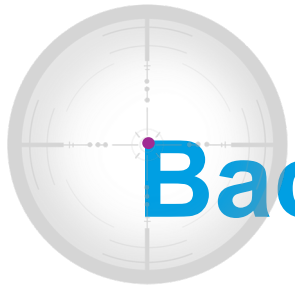


# 3 Schritte zum sicheren Restore

Eurebis AG

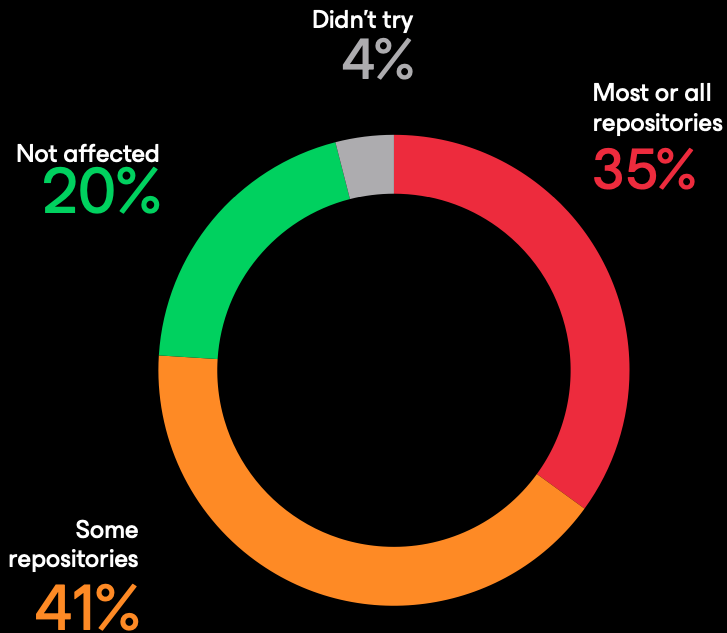
23. Juni 2025





# Backups im Fadenkreuz

Did the threat actor attempt to modify/delete backup repositories as part of the ransomware attack?

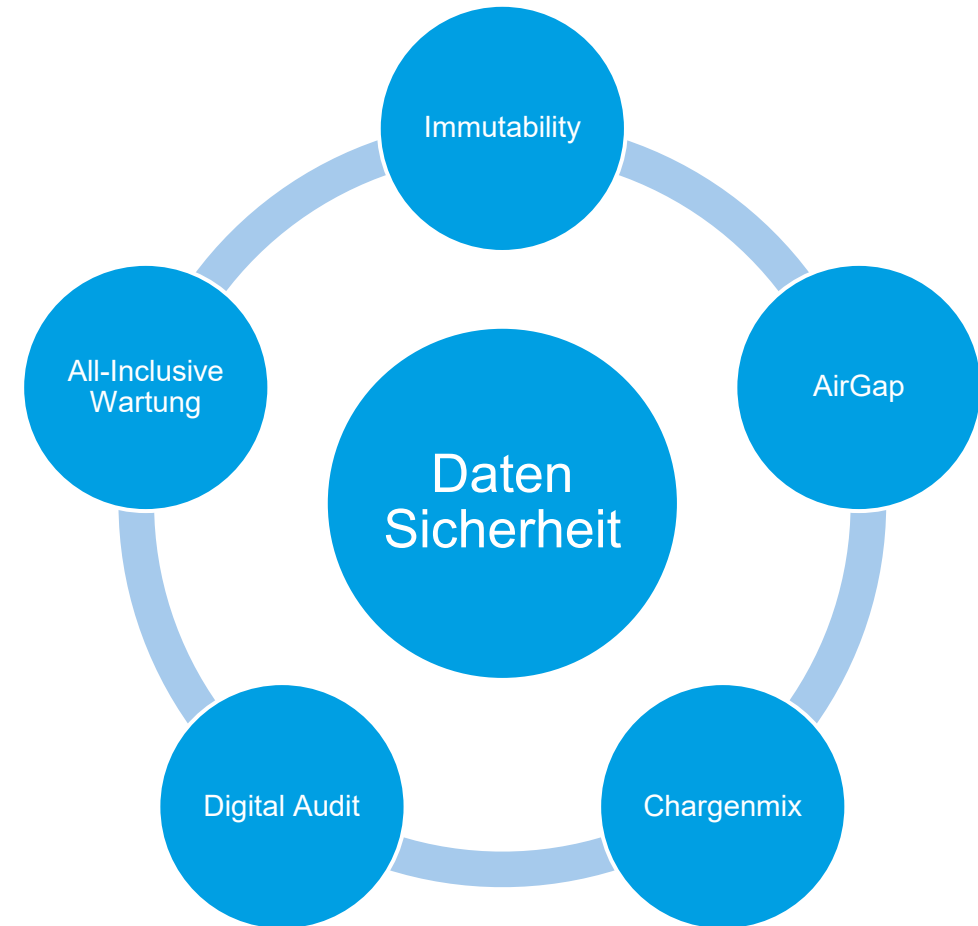


„Mit dem wachsenden Wert Ihrer Backups steigt auch die Zahl der Angreifer, die es auf sie abgesehen haben. Tatsächlich sind Backup-Repositories das Ziel von 96 % der Angriffe, wobei die Angreifer in 76 % der Fälle erfolgreich auf die Backup-Repositories einwirken.“

*VEEAM Ransomware Trends Report 2024*

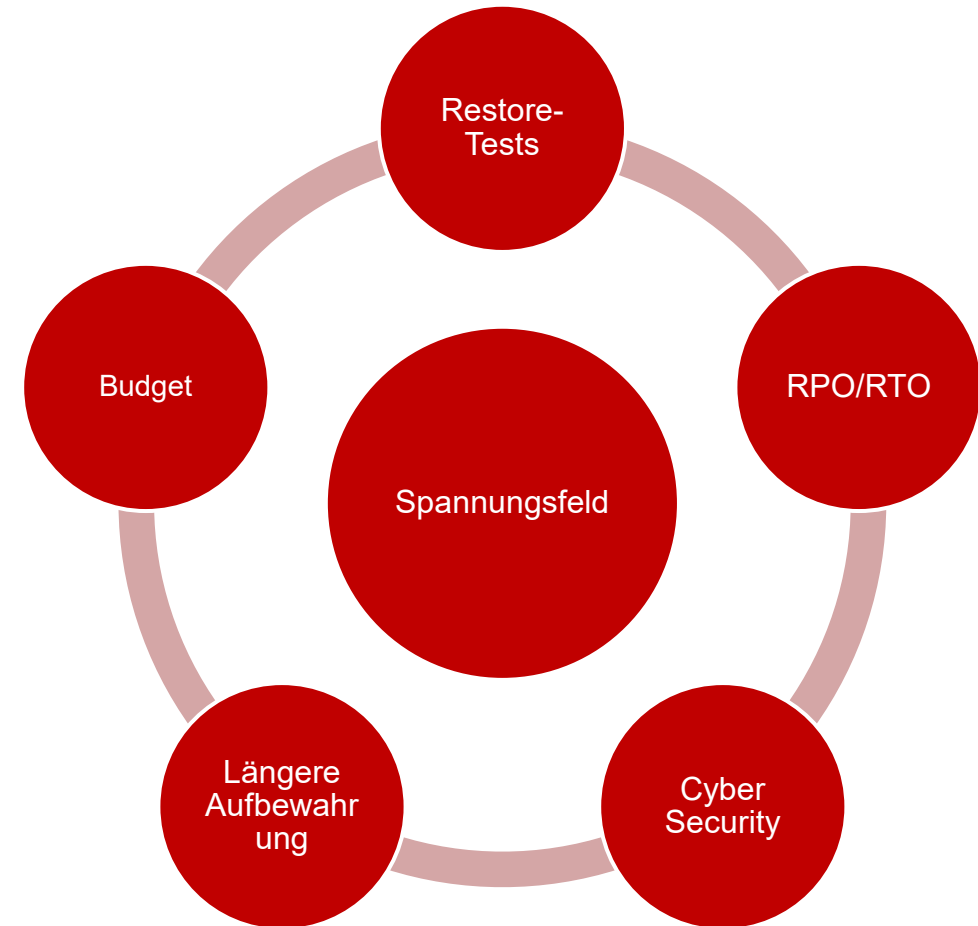
# Maximale Sicherheit...

- Sicherheit auf Hardware-Ebene
- Sicherheit auf logischer Ebene
- Sicherheit auf Zugriffs-Ebene



# ...birgt Herausforderungen.

- Speichergrösse vs. Geschwindigkeit
- Geschwindigkeit vs. Budget
- Budget vs. Sicherheit...



# Mehrstufiges Backup.

1. Backup Ziel



2. Backup Ziel



3. Backup Ziel



# 1. Backup Ziel

## Ziel

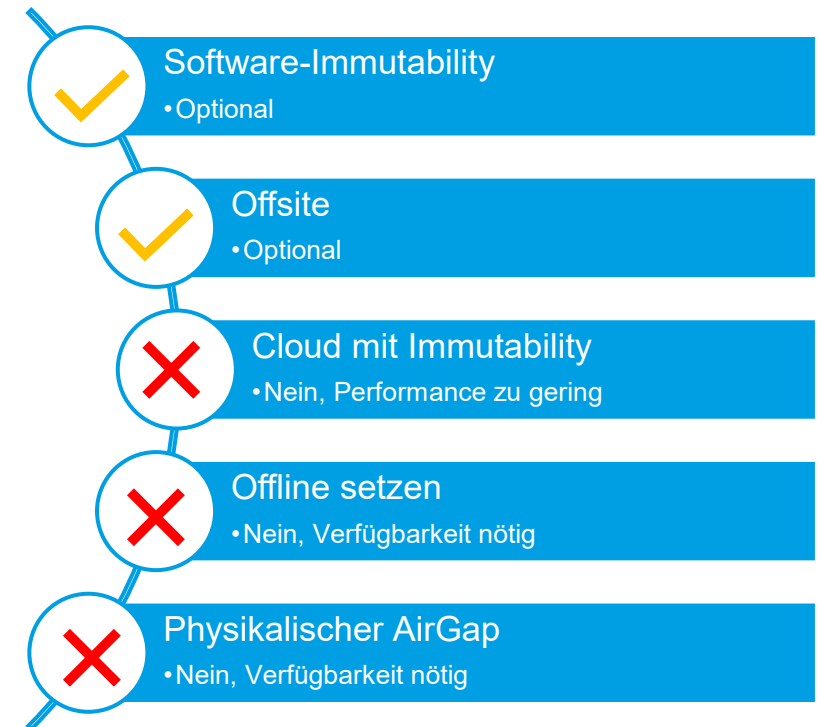
- Maximale Restore Geschwindigkeit für einen möglichst aktuellen Stand

## Anforderungen

- I/O
- Kurze Aufbewahrung
- Minimaler RPO/RTO

## Herausforderung

- CHF/TB



## 2. Backup Ziel

### Ziel

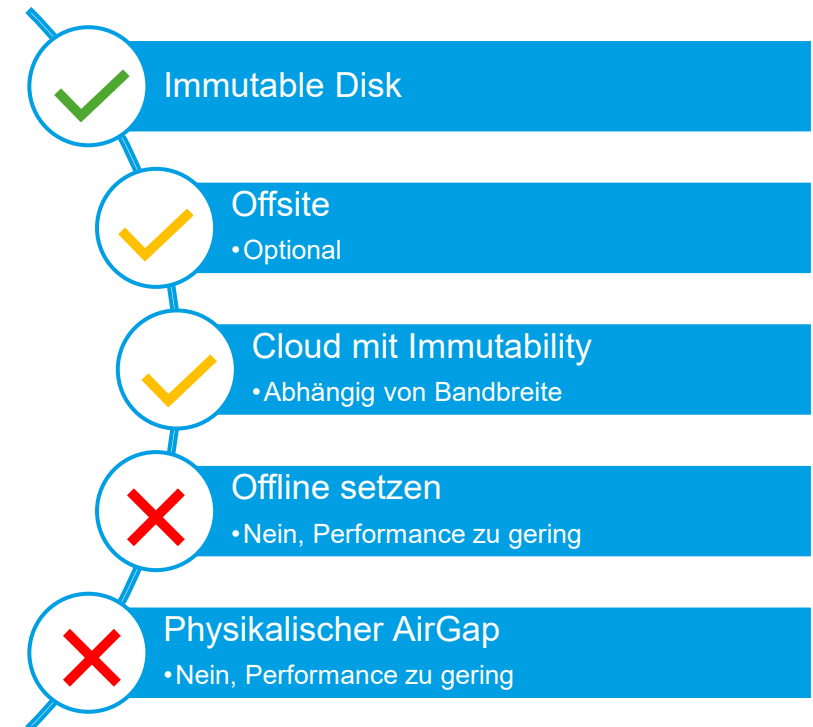
- Sichere Aufbewahrung für einen längeren Zeitraum

### Anforderungen

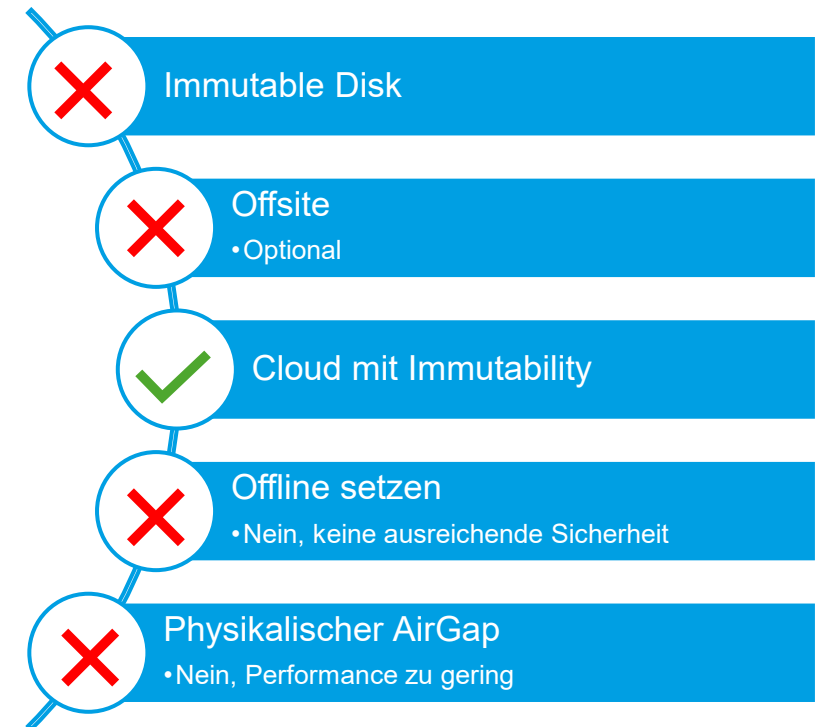
- CHF/TB
- Software-Immutability
- Durchsatz

### Herausforderung

- Geschwindigkeit und Kapazität



## 2. Backup Ziel – Cloud?





## 2. Backup Ziel – Cloud?

- Im Restore-Fall und im Recovery Test wird der Egress zum Flaschenhals
- Gegebenenfalls entstehen hohe Egress-Kosten
- Möglicherweise sinnvoll bei Wiederherstellungskonzepten, bei denen die gesamte Infrastruktur in der Cloud gestartet wird.



## 2. Backup Ziel – Cloud?

- **Achtung: CloudAct**

*Der Cloud Act ermöglicht es US-Behörden, auf Daten zuzugreifen, die von US-Cloud-Providern gespeichert werden, selbst wenn diese Daten auf Servern ausserhalb der USA, etwa in Europa, liegen, was die Vertraulichkeit und Sicherheit von Backups in der Cloud gefährdet und im Widerspruch zur DSGVO steht.*

- **Achtung: Haftung und Verantwortung**

*Letztverantwortung und Organisationshoheit beim verantwortlichen Unternehmen;  
Die rechtliche Verantwortung für die Durchführung der Datensicherung ist nicht delegierbar an bspw. einen IT-Auftragnehmer und insb. Auftragsverarbeiter*



## 3. Backup Ziel

### Ziel

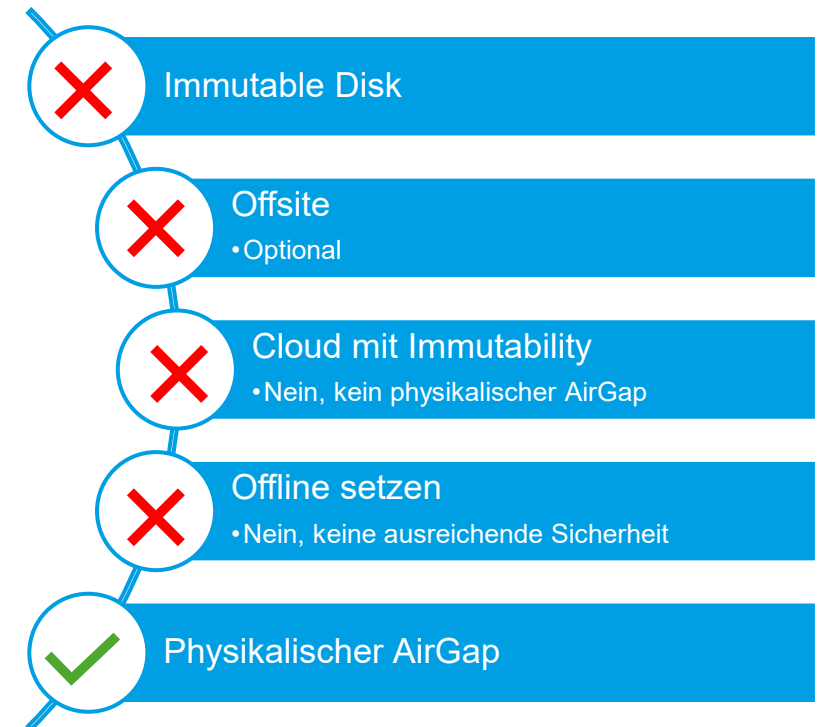
- Last Line of Defense

### Anforderungen

- Maximale Absicherung auf Hardware Ebene

### Herausforderung

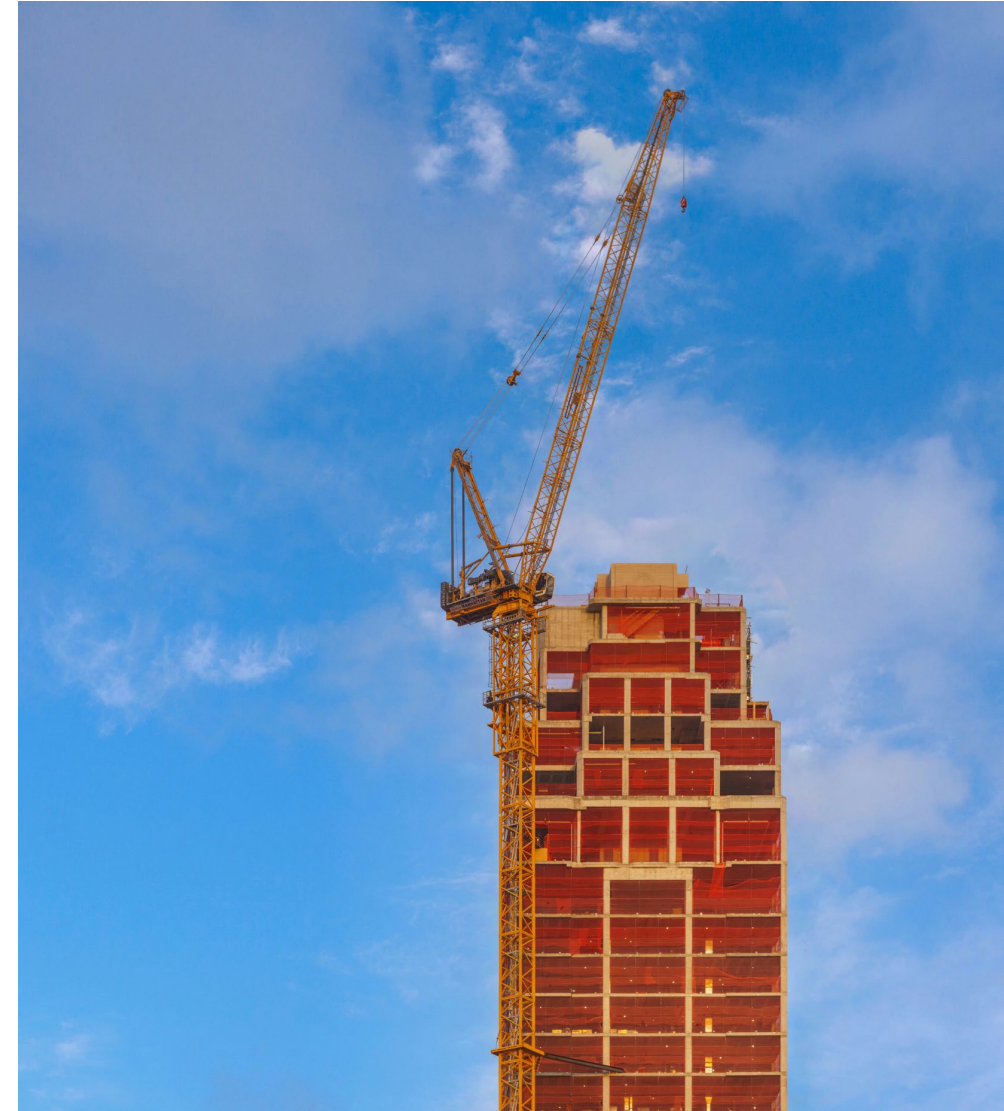
- Restore Geschwindigkeit
- Manueller Aufwand
- Medienmenge



# Herausforderung Datenwachstum

- RPO/RTO
- Restore Tests
- AirGap grosser Datenmengen

**Wachsende Performance-Anforderungen**





# Neu: Silent Brick Pro

1. Backup Ziel

2. Backup Ziel

3. Backup Ziel



12xNVME pro Medium  
768TB NVME in 2HE  
5 GB/s (SMB)  
2 GB/s (S3, pro Medium)  
Physikalischer AirGap

# Ein Partner für alle Schubladen!

- ✓ Speicher für Primäre & Sekundäre Backups
- ✓ Speicher für Backup Kopien Job
- ✓ Speicher für Ransomware Sicherheit
- ✓ Speicher für statische Daten
- ✓ Speicher für physikalische Entnahme
- ✓ On-Premises Objectstore S3
- ✓ Speicher für Archivdaten (Worm)



# Höchste Sicherheit mit dem 3-2-1-1-0 - Prinzip

Multi-immutable Storage



**01**

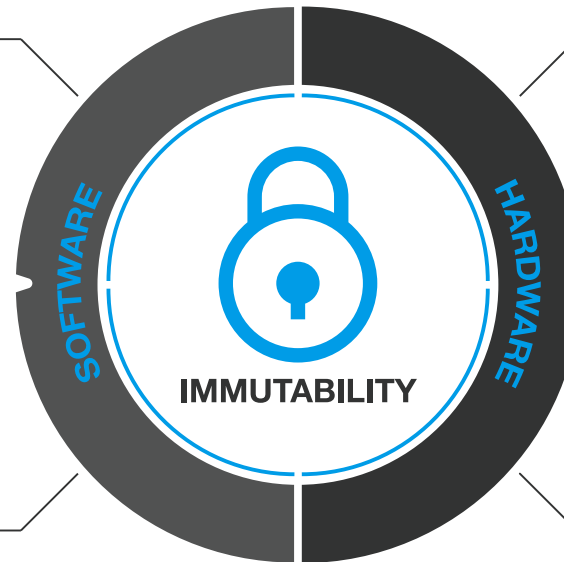
## Continuous Snapshots

Automatisch,  
Freigabe nach Retention

**02**

## Object Locking

Automatisch,  
Freigabe nach Retention



## Air Gap

Manuell,  
Freigabe durch Überschreiben

**03**

## Hardware WORM

Automatisch,  
keine Freigabe

**04**

# Danke.

---

Daniel Tessié

System Engineer & Sales

