@schlomo@floss.social
@schlomo @schlomo

TEKTIT CONSULTING

#SLAC 2026

Digital Sovereignty Is More Than a Piece of Paper

Why Backup Is the Only Way Out of the SaaS Trap

13.05.2026, Secure Linux Administration Conference 2026, Berlin

Schlomo Schapiro, Associate Partner / Principal Engineer, Tektit Consulting

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

Agenda

01. We ❤️ SaaS

02. Backup & Disaster Recovery
Business as Usual or What Needs to Change?

03. The SaaS Trap

04. Escaping the SaaS Trap

05. Our Rebellion: Data Jailbreak

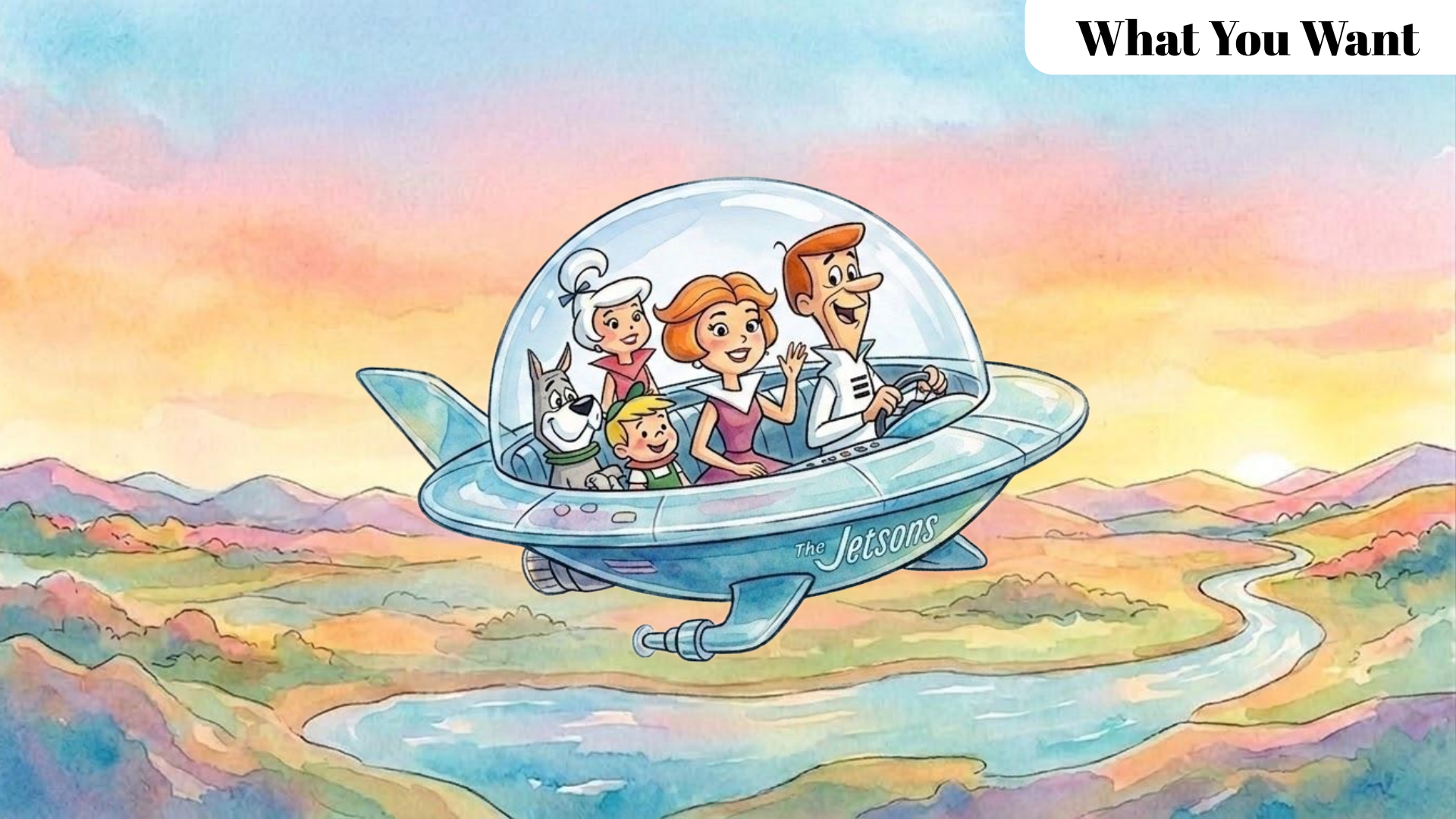
06. Fortress: Minimum Viable Company

07. Recap: Master Plan & First Step

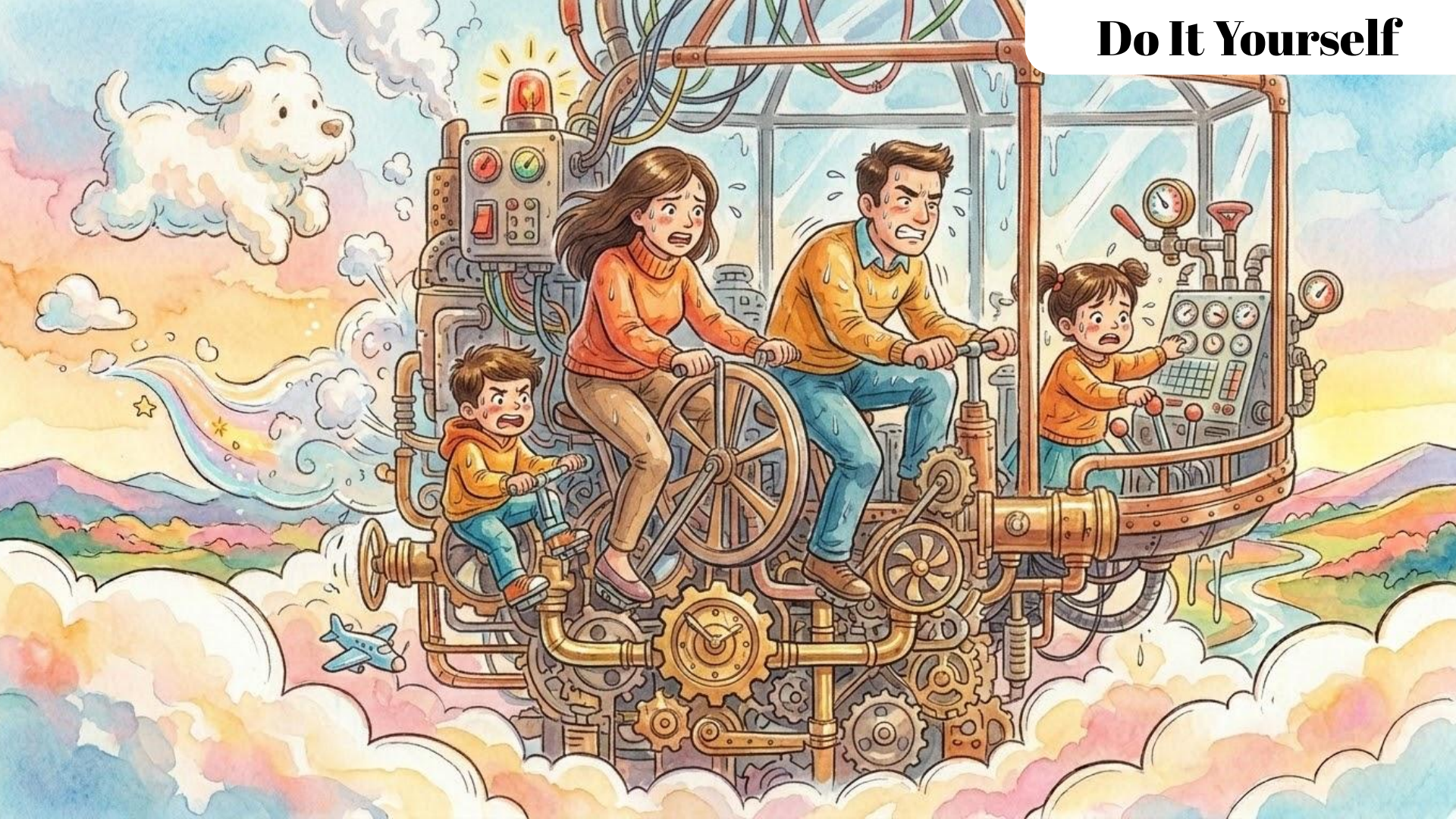
08. Q&A

Why we need SaaS

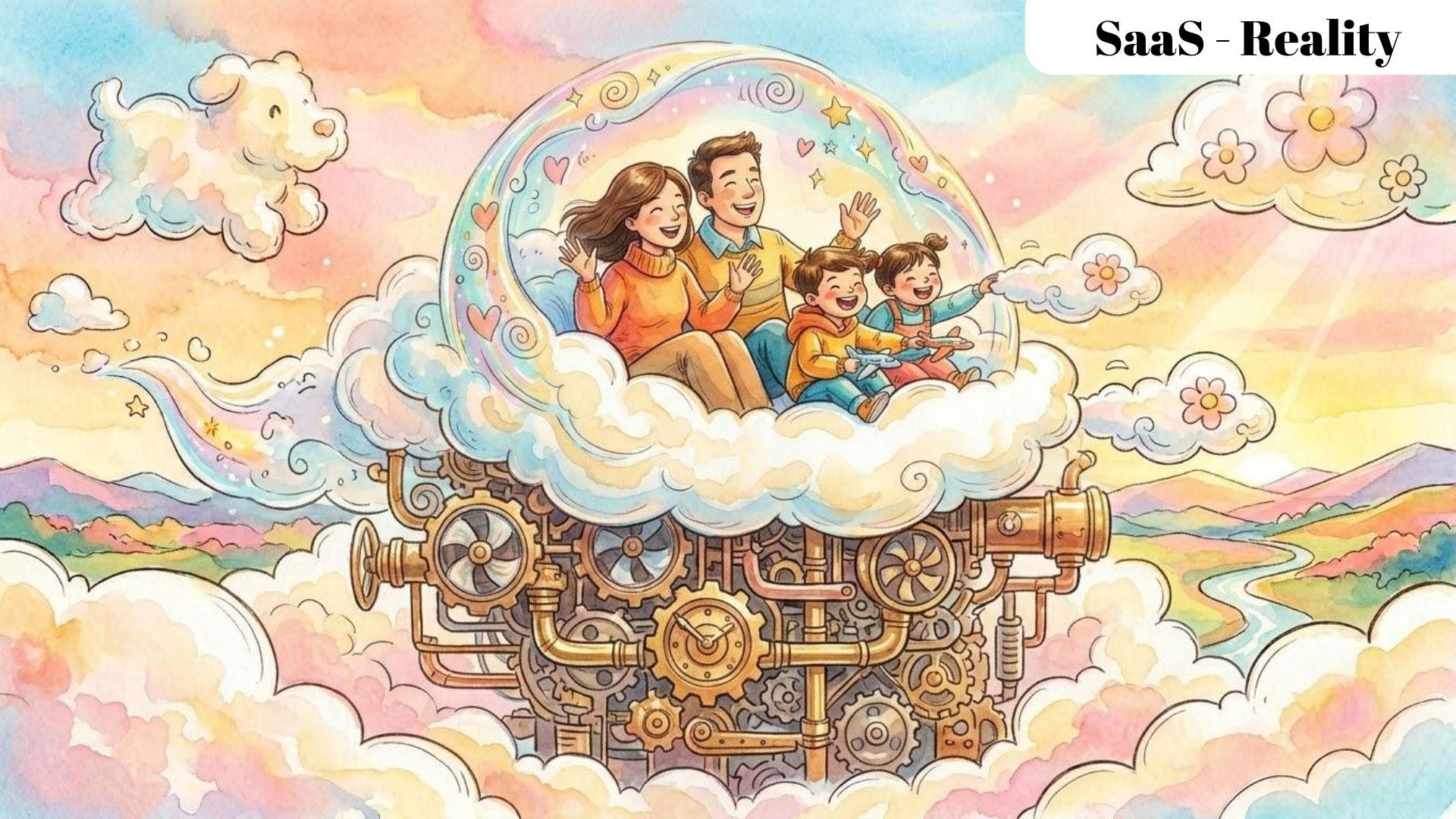
What You Want



Do It Yourself



SaaS - Reality



SaaS - Perception

Example: 8 Terabyte Photo Storage & Processing

300€

1100€

600€ / Year

853€ / Year

Features & Convenience

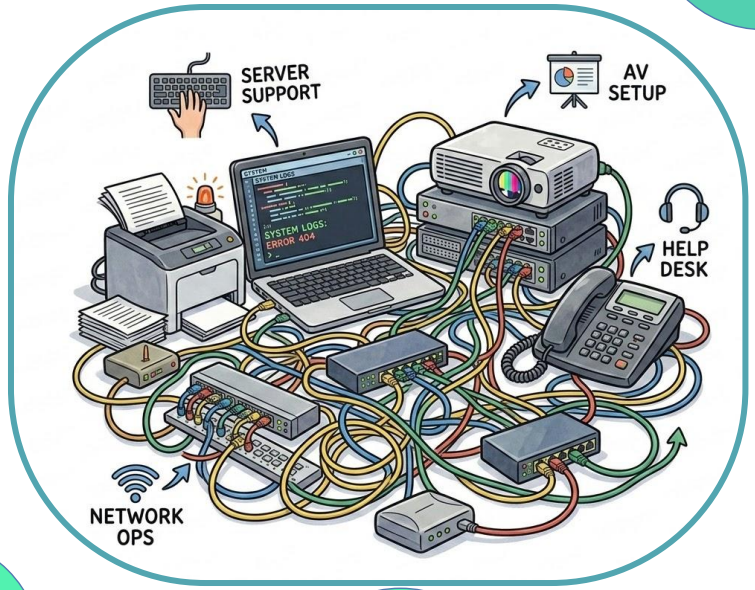
EFFORT 🤷 COST

Sovereignty & Control

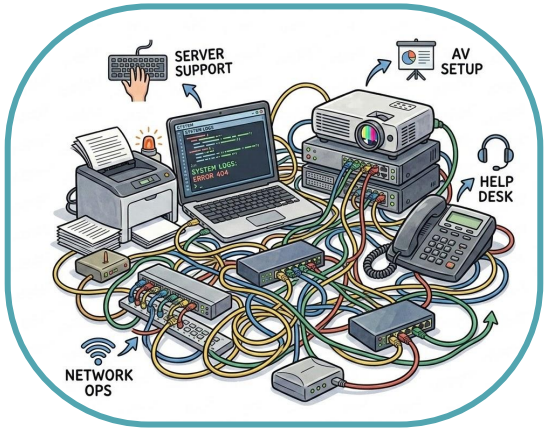
Check also Immich & hosters (e.g. pixelunion.eu), Ente ...

The IT Landscape Problem

CMS
CRM
MAP
ATS
HRIS
HCM
SCM
CRM
CLM
LMS
FP&A
WMS
GRC
MDM
IAM
ITSM
CPQ
PLM
ERP
KYC



The IT Landscape Problems, Problems …



ATS	HRIS HCM	CMS	MAP	ERP
CLM	LMS	CRM	CPQ	CRM
GRC	PLM	FP&A	WMS	SCM
KYC	MDM	IAM	ITSM	?

- IT “drives” business
- Every business unit and department needs their “special” IT solution
- Tight coupling:
  business ⇔ process in software solution ⇔ IT
- Application growth exceeds IT staff growth
- Applications getting more specialized and complex
- Business Units introduce applications on their own

⇐ Application Silos

⇐

⇐ Problems …

⇐

TEKTIT CONSULTING

❤️ SaaS


DATA VICTORY
DATA VICTORY FLAG
Global Reach
Global Reach
PRODUCTIVITY ROCKET
customer
SAVED by SaaS
SOFTWARE AS A SERVICE
AUTOMATION BOOST!
SALES FUNNEL
MARKETING PERFORMANCE
LEAD MANAGEMENT
Security Shield
SECURITY ENHANCED!

SaaS Benefits

Financial Predictability Efficiency

Shift from CapEx to OpEx

Faster Time-to-Value

Business Agility Flexibility

Elastic Scalability

Democratized Access to Best-in-Class Tools

Strategic Focus Productivity

Focus on Core Mission, Not Maintenance

Empowering the Modern Workforce

Always Up-to-Date

KYC MDM IAM ITSM GRC PLM FP&A WMS SCM CLM LMS CRM CPQ CRM ATS HRIS HCM CMS MAP ERP

Let's learn first about Backup & DR ...

youtu.be/f17pFD_Q3hM

Business Continuity

A comprehensive strategy ensuring an organization can continue operating and delivering critical functions during and after unexpected disruptions, minimizing downtime and maintaining essential business processes.

Staying in business, no matter what!

Source: Claude.ai

TEKTIT CONSULTING

The Basics

Recovery Time Objective (RTO)

*How **long** to recover?*

DO

Recovery Point Objective (RPO)

*How **old** is the recovery data?*

HAVE

Backup is not Disaster Recovery

Restore (not just Backup)

- single file
- single mailbox
- single database
- single LUN
- single server
- single …

When we have

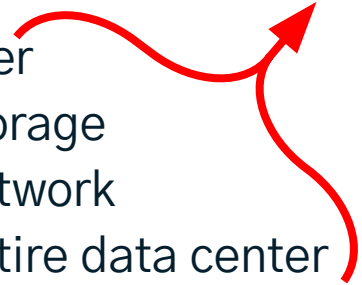
- the file server
- the mail server
- the database server
- the storage

Disaster Recovery

- all files
- all mailboxes
- all databases
- all the LUNs
- all servers
- everything!

When we don't have TIME

- a server
- our storage
- the network
- our entire data center



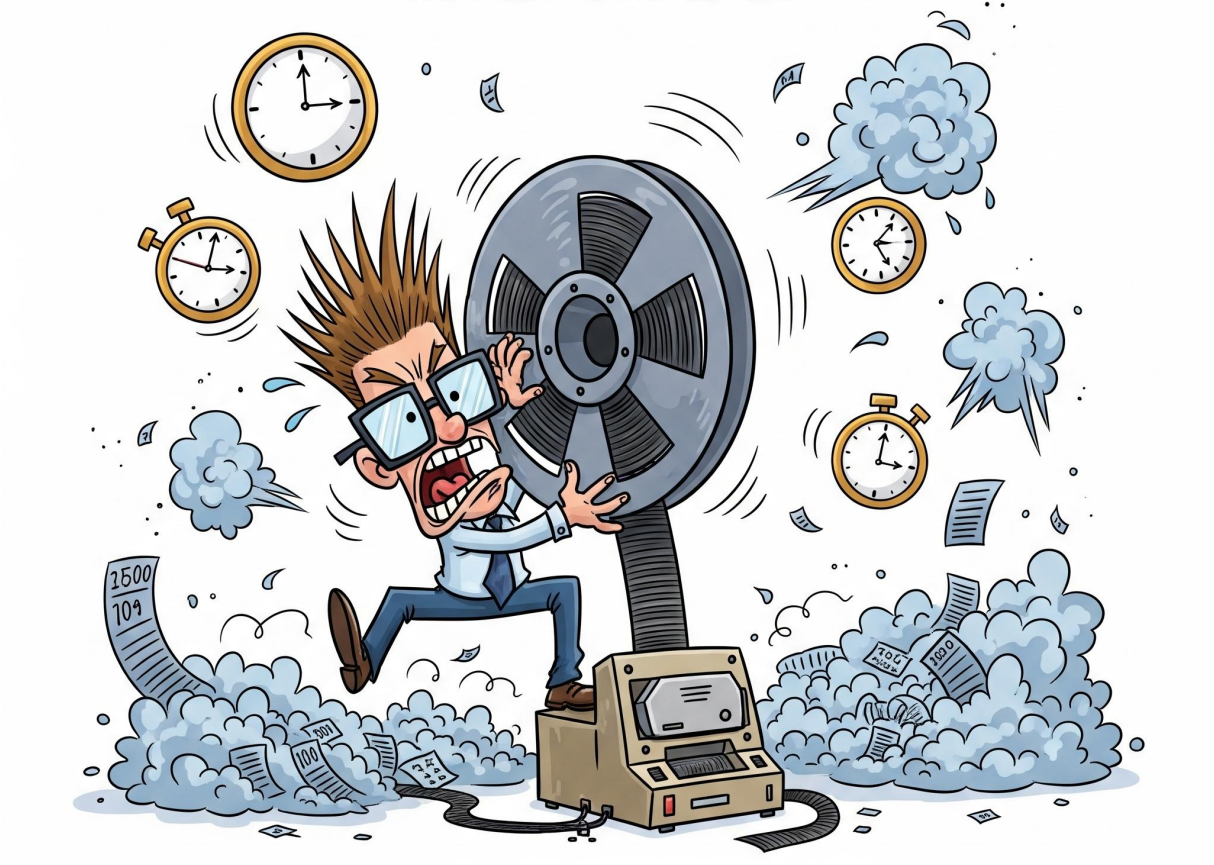
Guiding Principles

Backup is the means to enable Restore

Comprehensive Backup & Restore Automation
is the means to enable
Disaster Recovery and Business Continuity

Use the Same Backup for
Restore and Disaster Recovery

The Restore Time Objective (RTO) Challenge



RTO Example: Catastrophic SAN failure (worst case)

Context:

- 140 TB SAN storage
- LTO–9 tape library
  (400 MB/s = 1.44 TB / hour)

Full Restore:

- 1 day for “fixing” the SAN storage
- 4 days for full restore
- 1 day overhead

→ minimum 5 days to recover SAN

Questions:

- 1 week recovery time from major outage OK?
- how to manage external relationships & communication during 1 week outage? Stop external processes?
- What if all the local hard disks / physical servers where also affected?
- how can we **test this & validate the projected recovery time?**

SLA = RPO + RTO + 🤞 🙏 ❤️ 🩼 🩹 ?

Restore Time = Biggest **Problem & Unknown**

Let's get rid of the restore time!
Let's exercise restore all the time!

Restore **every** backup immediately

Replacement system is **ready** for usage

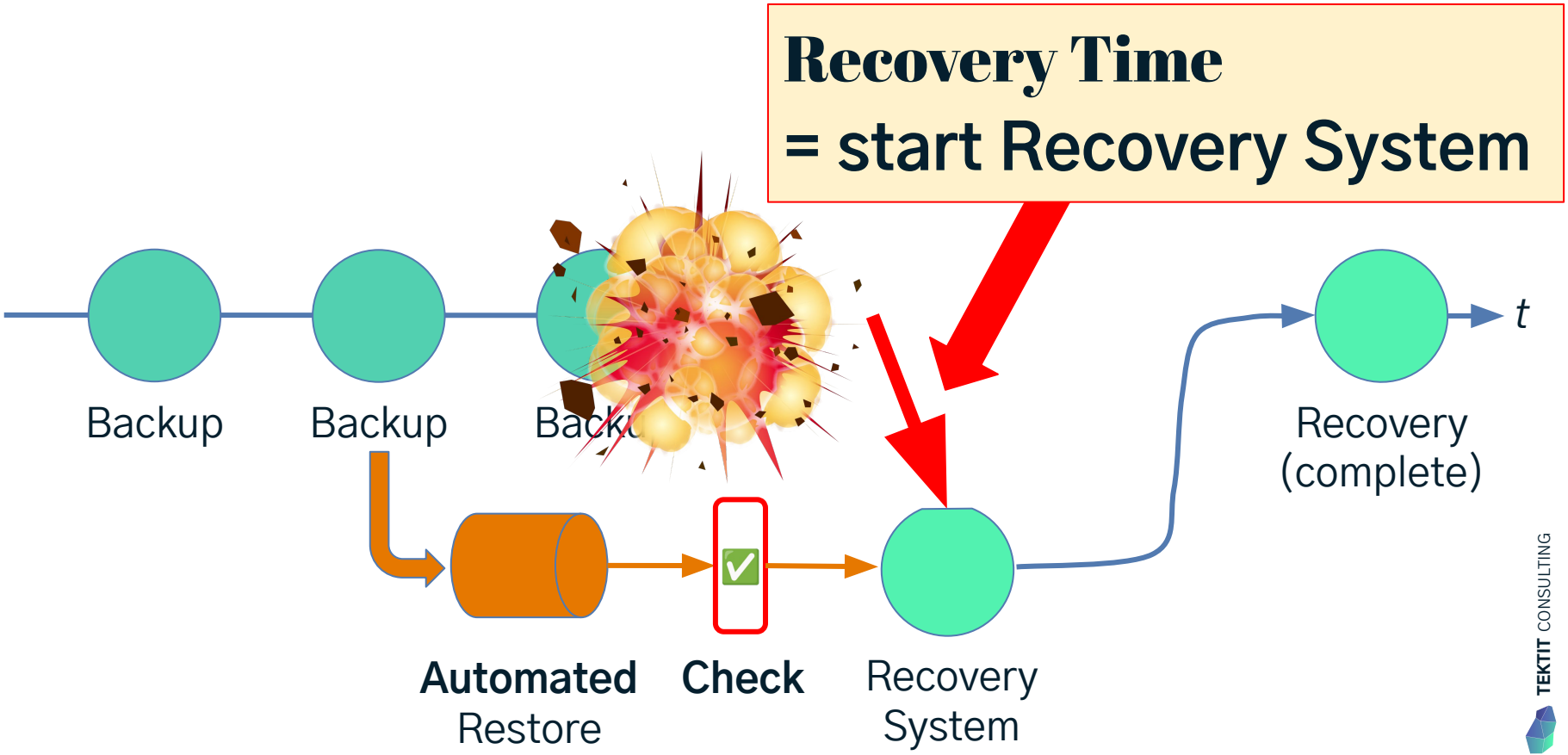
Fixed RTO

Try to **restore** when needed

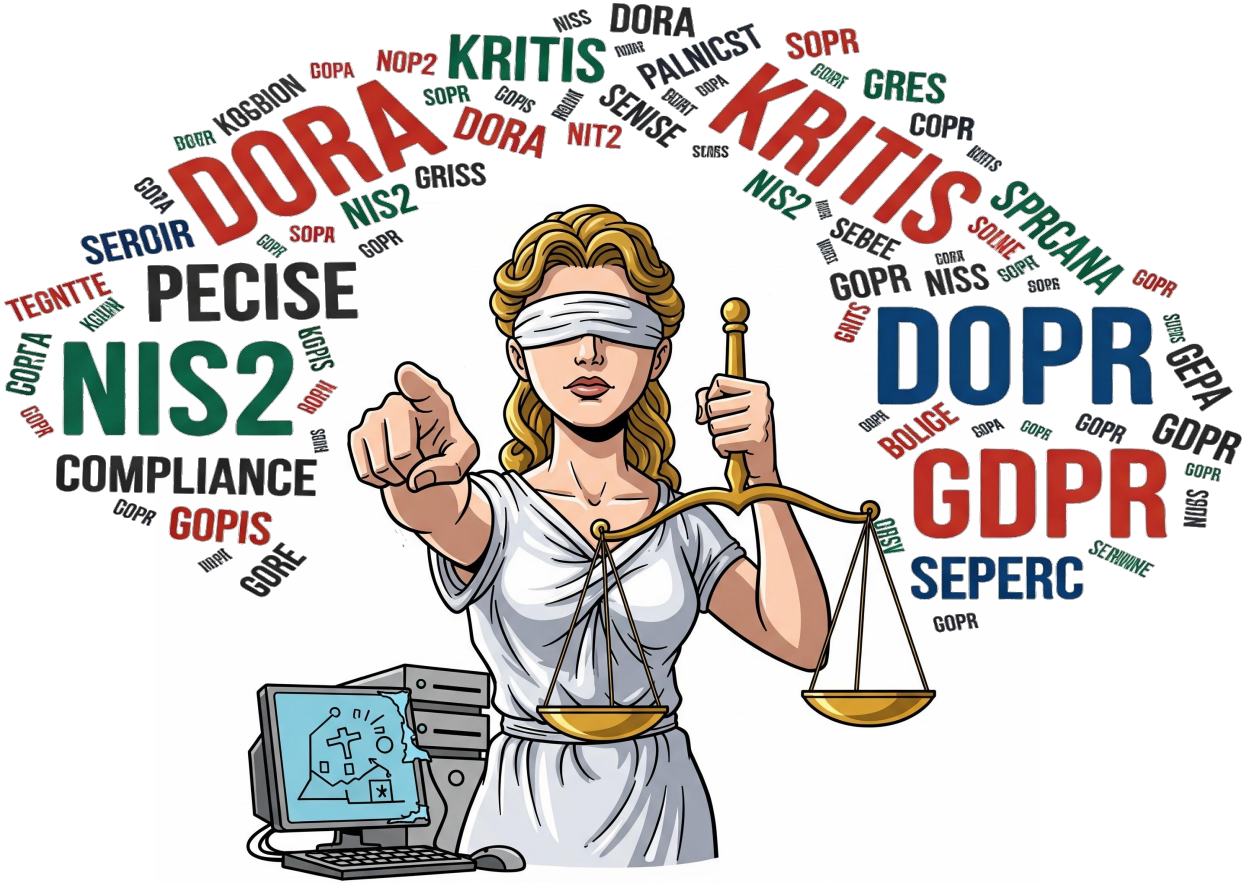
→

Switch to working & verified recovery system

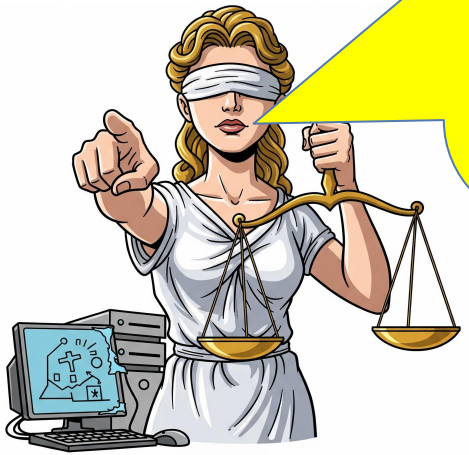
The "No Restore" Solution



The Regulatory Challenge



The 11th Commandment



Thou shalt build thy Works upon a Foundation of Order, that in Calamity they may be swiftly Restored.

… “just take care of all the hard stuff, now!”

Source: Schlomo & AI

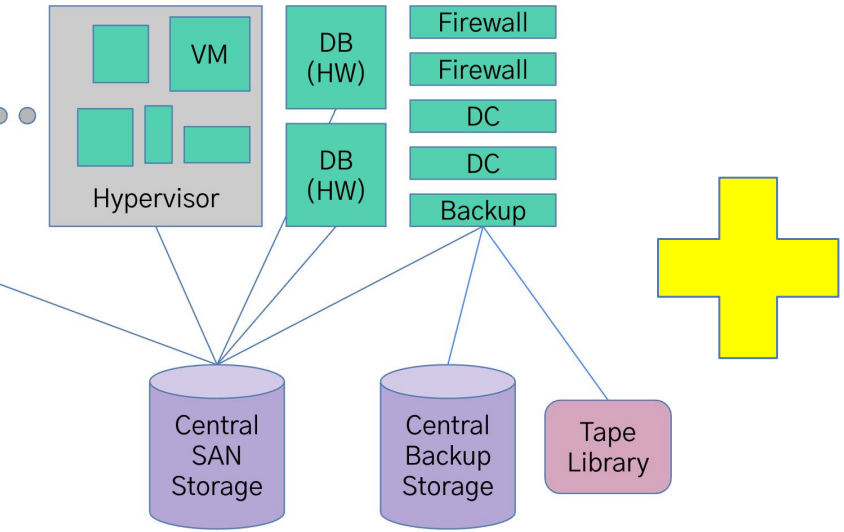
Regulation	Main Obligations
KRITIS (Kritische Infrastruktur) BSI-Gesetz (BSIG) 2025: § 2, 30, 32, 38, 39 (includes NIS2)	Resilience and Incident Management • **Broad Incident Definition (§ 2):** "Security incidents" explicitly include *availability* outages. They are "significant" if they cause severe operational disruptions or financial losses. • **Risk & Resilience Capabilities (§ 30):** Organizations must implement state-of-the-art measures including incident management, backup/disaster recovery, crisis management, and secure emergency communications. • **Strict Reporting Rules (§ 32):** Significant incidents require an initial report within 24 hours (updated at 72 hours) and a detailed final report on root causes and recovery within one month. • **Executive Accountability (§ 38):** Management is legally required to enforce resilience measures, complete mandatory cyber training, and faces personal financial liability for culpable damages. • **Mandatory Audits (§ 39):** Operators of critical installations must independently prove compliance via audits or certifications every three years and fix any identified flaws.
DORA (Digital Operational Resilience Act) Regulation (EU) 2022/2554 (DORA): Article 6, 11, 12	Comprehensive ICT Resilience Framework: • Establish a comprehensive ICT Business Continuity Policy and associated ICT Disaster Recovery Plans. • Implement backup policies defining the scope and frequency of backups based on data criticality. Backup systems must be logically and physically separate from source systems. • Define specific recovery plans, including procedures for restoring ICT systems and data from backups. • Annually test the ICT business continuity and recovery plans, including scenarios for cyber-attacks and switchovers to redundant infrastructure. • Maintain redundant ICT capacities, potentially including a geographically separate secondary processing site. • **Provisions on ensuring access, recovery and return in an easily accessible format … data processed by … third-party …**
GDPR (General Data Protection Regulation) Regulation (EU) 2016/679 (GDPR): Article 32	Data Availability and Restoration: • Implement appropriate technical and organizational measures to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services. • Maintain "the ability to restore the availability and access to personal data in a timely manner" in the event of a physical or technical incident. • Implement a process for regularly testing, assessing, and evaluating the effectiveness of these measures. • While not explicit, this effectively mandates reliable backups and tested recovery plans as a core security safeguard for personal data.

Compliance Self Check: Regulatory Requirements

- Comprehensive backups
- Comprehensive documentation
- Business Impact Analysis
- Recovery times match business requirements, especially for a complete site-wide outage
- Proven restore and disaster recovery capabilities
- Regular exercises of abilities and procedures
- 3rd party solutions:
  - Responsibility for operational resilience and recovery capabilities
  - Exit strategies with easily accessible data formats

The Cloud & SaaS Challenge

Decentralize Everything

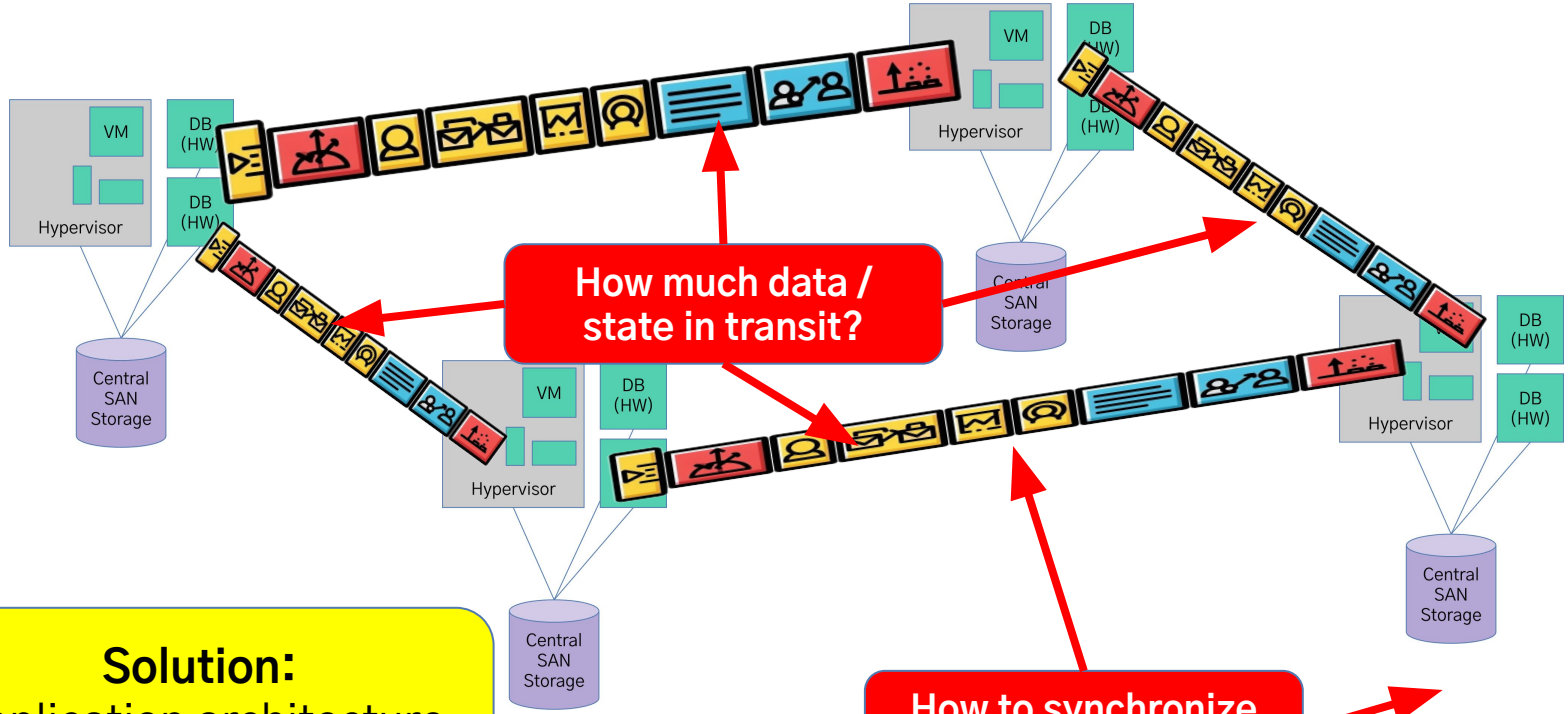


How to recover all of this?

SAAS

CLOUD

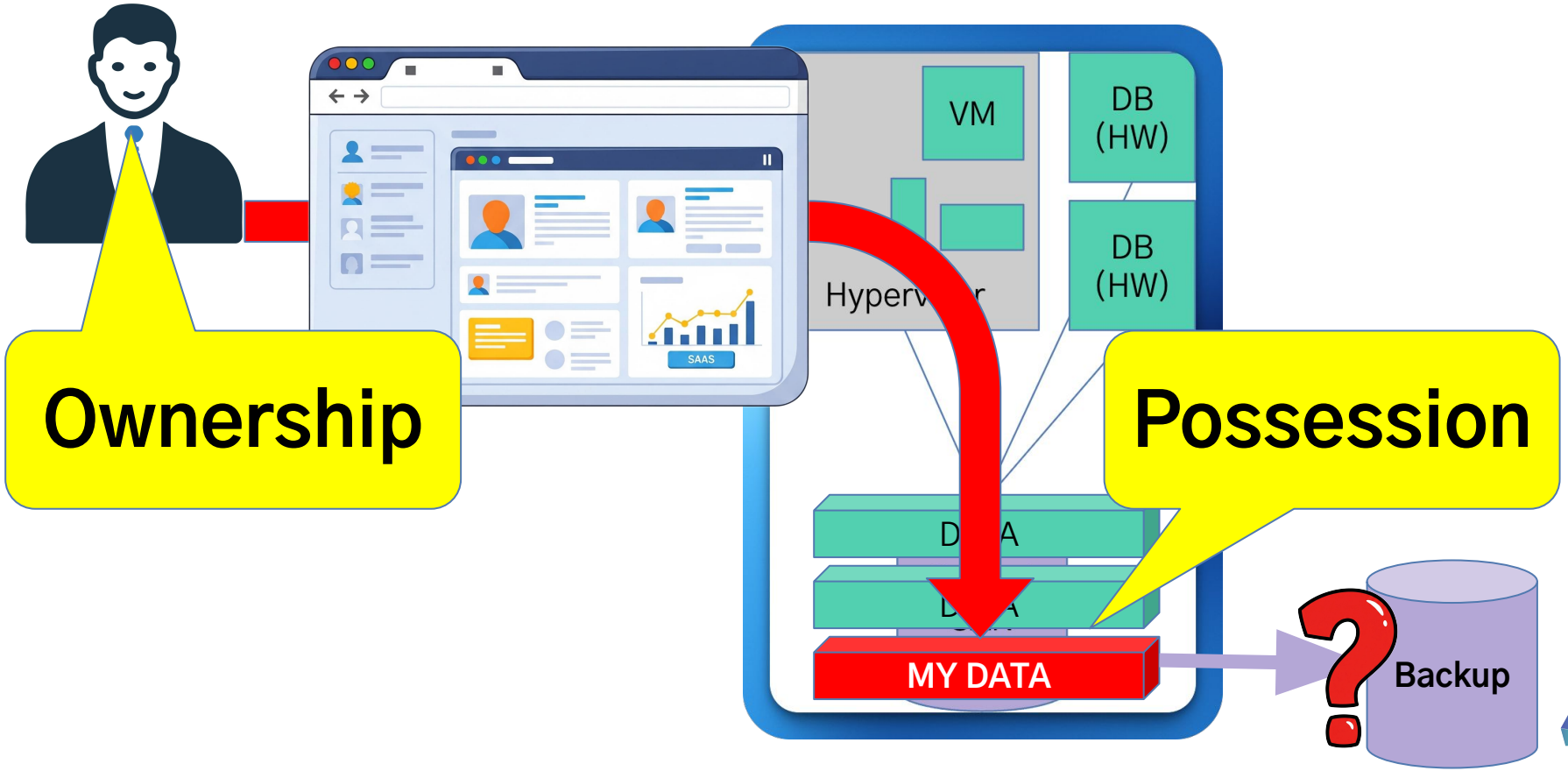
Decentralized Consistency Challenge & Queues



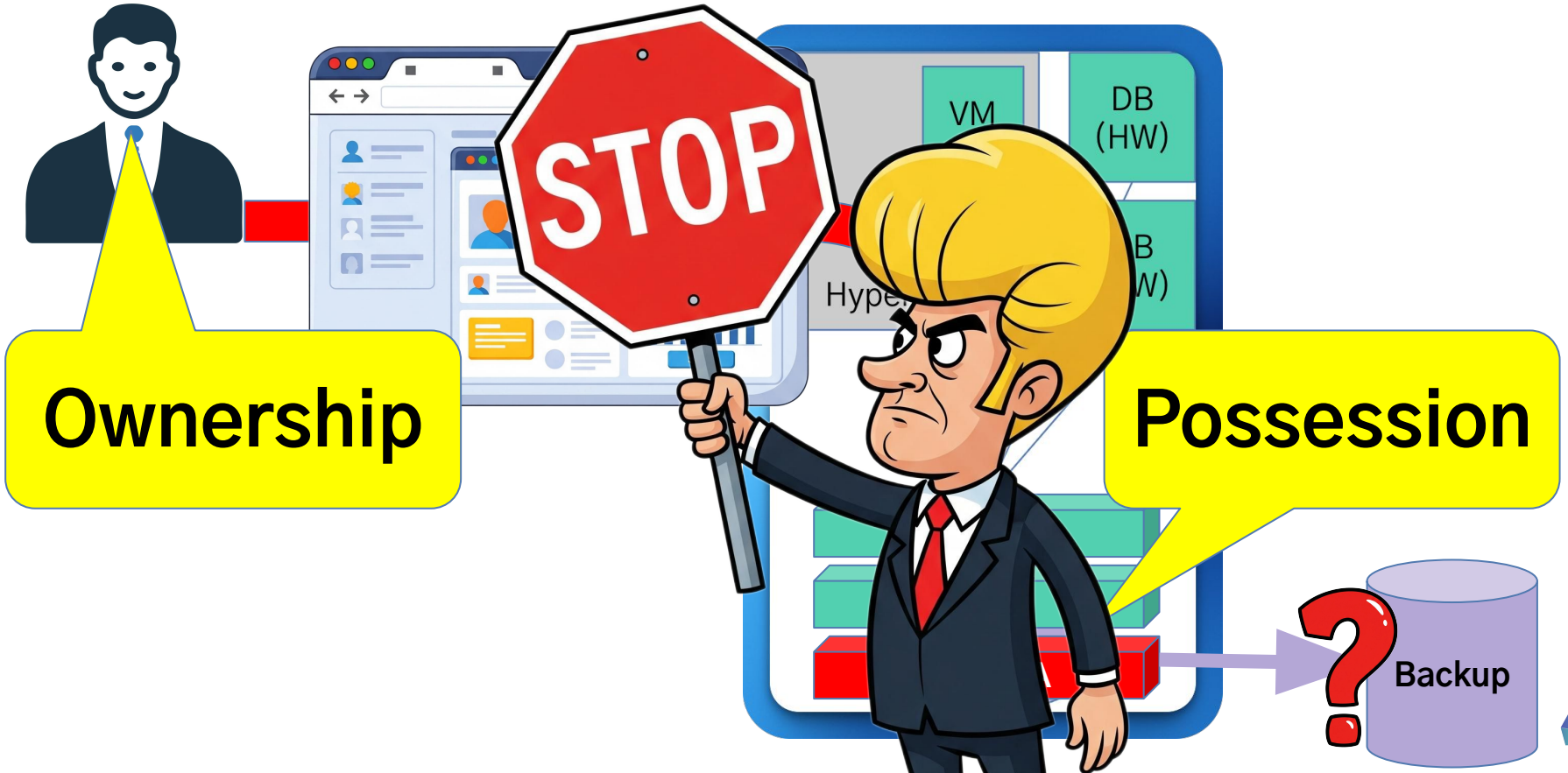
Solution:
Application architecture supports **reconciliation**

The Data Possession Challenge

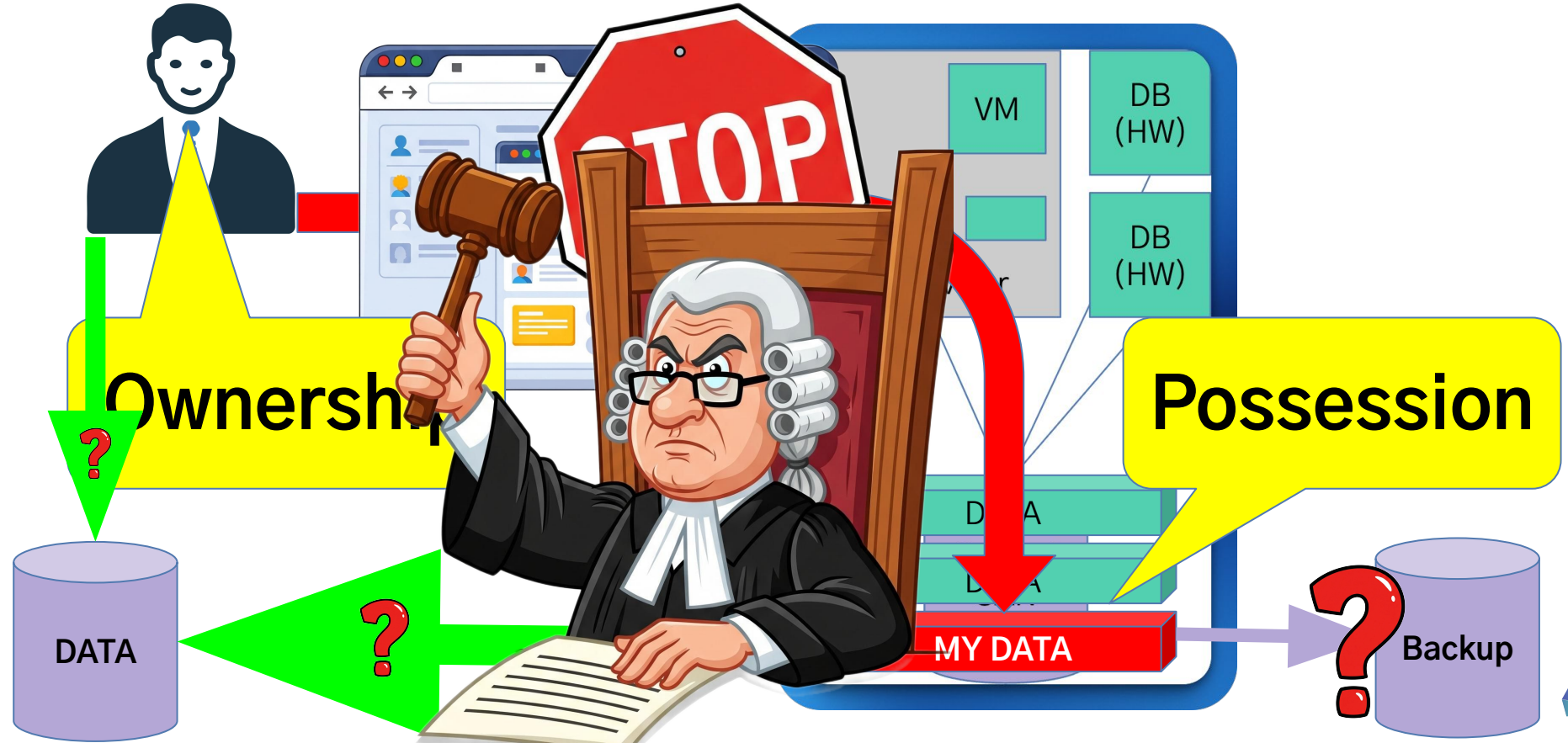
The Data Posession Challenge of SaaS



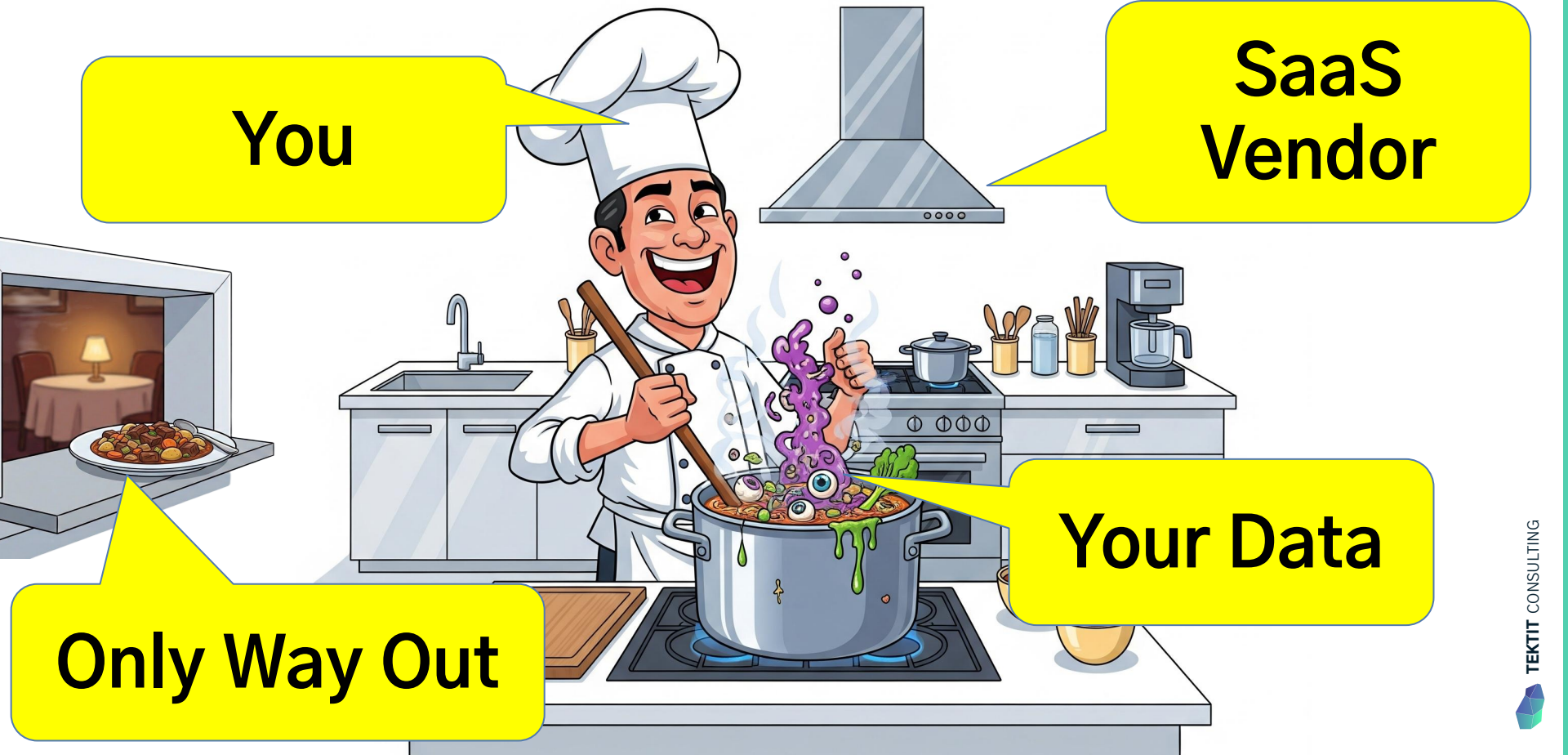
The Data Posession Challenge of SaaS



The Data Posession Challenge of SaaS



The SLA Challenge



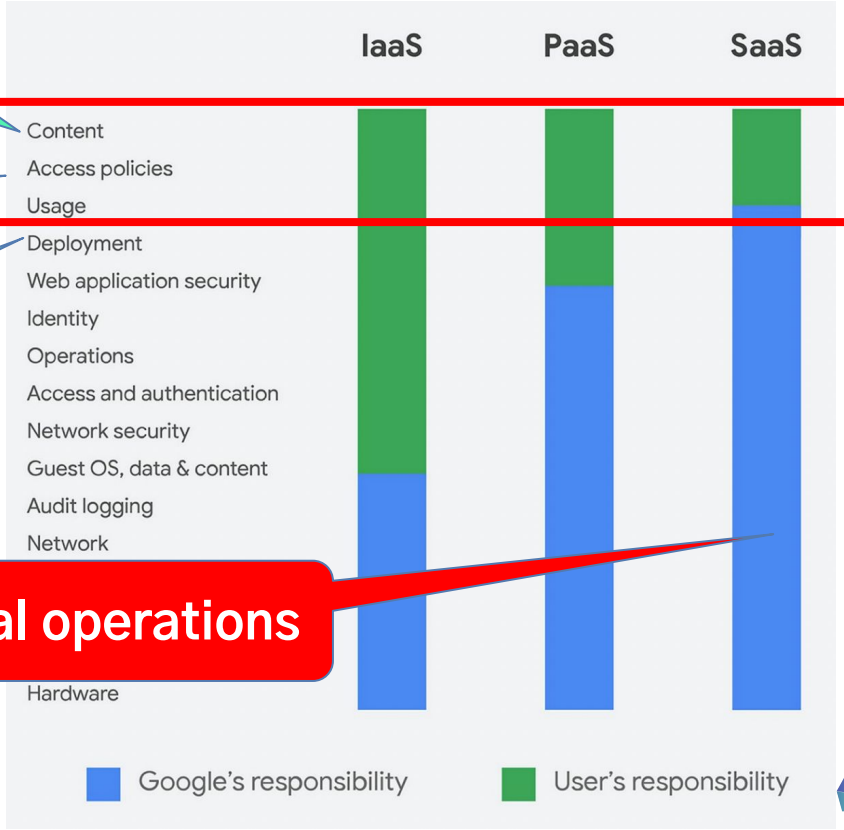
The SLA Challenge: We don't care about your data!

Accidentally or maliciously deleting data?

Granting access to malicious apps?

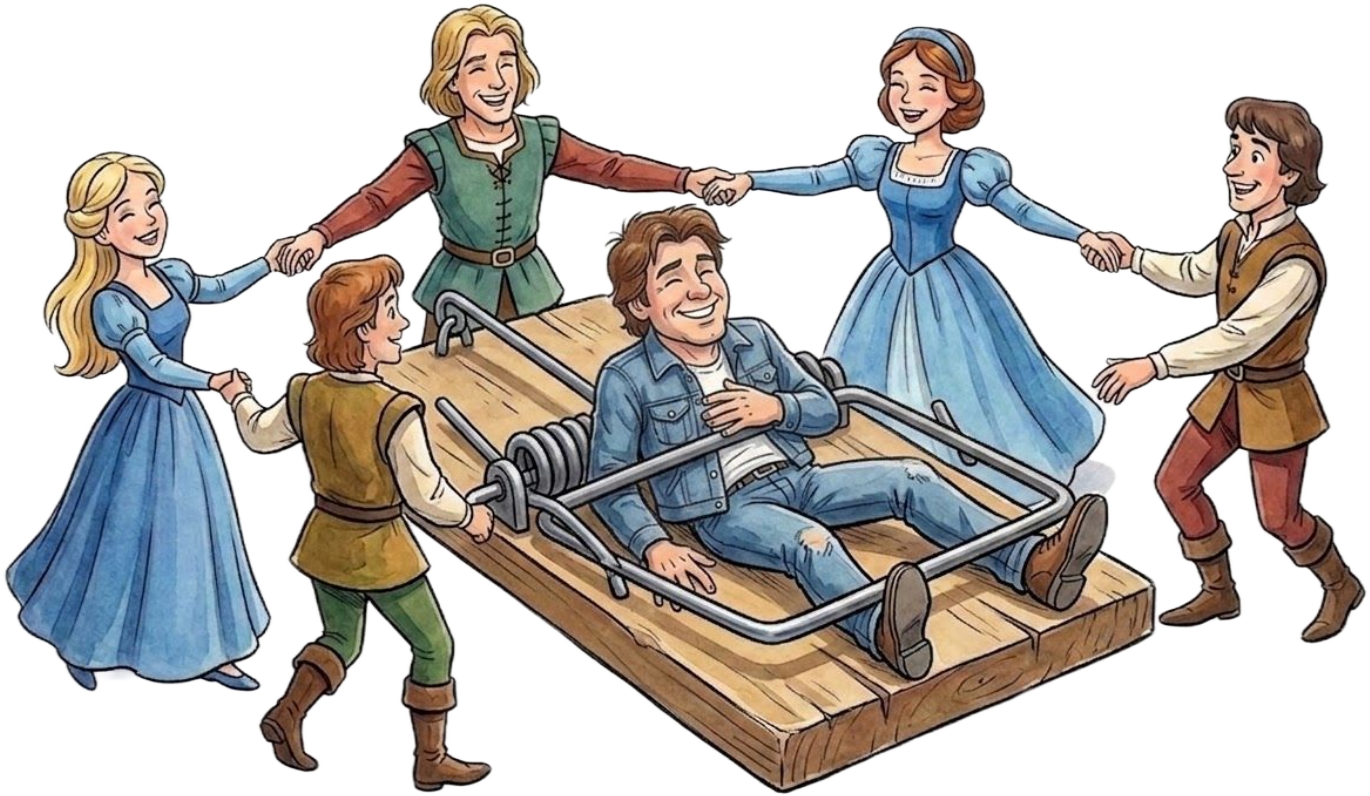
Deleting entire user account or Tenant?

SaaS Vendor only guarantees technical operations

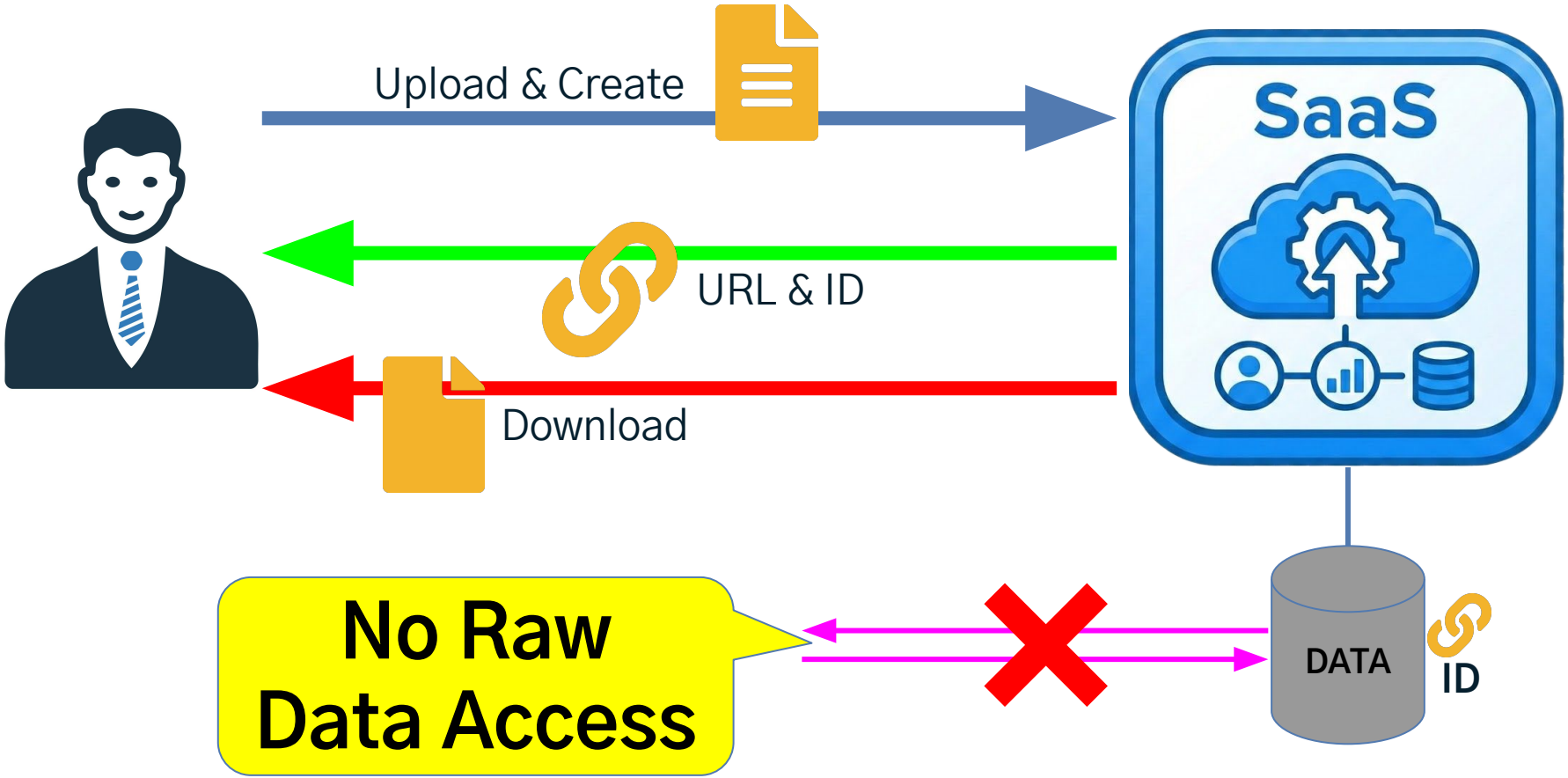


Source for Example:
Google Workspace data protection implementation guide
Released 12/2020

The SaaS Trap



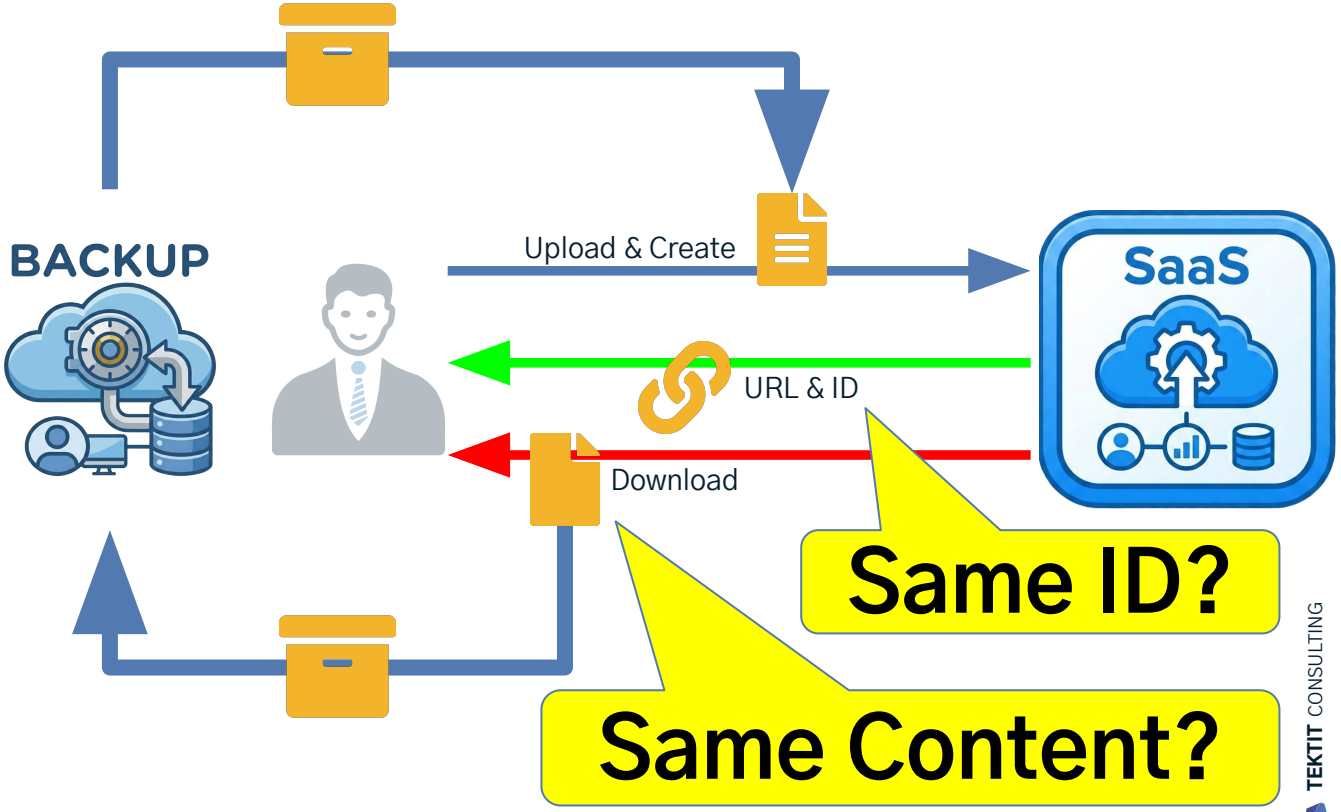
SaaS Application High Level Architecture



SaaS Application High Level Architecture

Include?

- Configuration
- Metadata
- Permissions
- Groups
- Comments
- Approvals
- Relationships
- Sharing



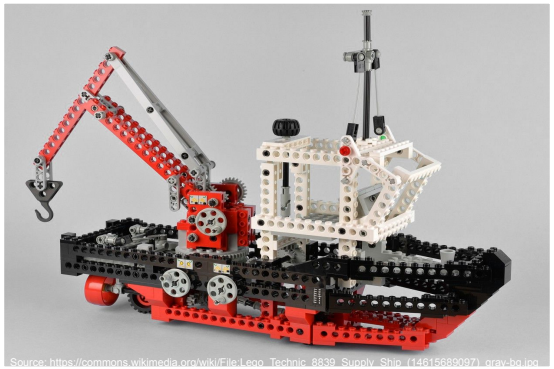
The Shattered Restore Challenge

SAAS: NO RESTORE

Original:
docs.google.com/presentation/d/**1P8tgUjHlkWIG4wFbBaiv1otqPRWm4BWAb0Z5BfoSxGc/**

Restored:
docs.google.com/presentation/d/**1hpuOs42vEFHF7Ancp3F136v83PZxqRS6B273mQ8ecLY/**

Your Data before **Backup**:



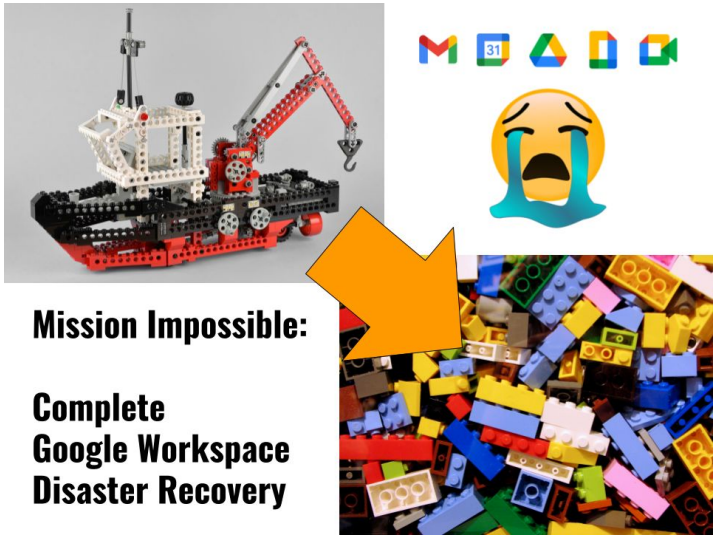
Your Data after **Restore**:

TEKTIT CONSULTING

Case Study: Google Workspace Backup & DR

- Core Services without restore (➡ export only):
  - Google Chat
- Core Services without backup (➡ no restore, too!):
  - Groups content
  - Forms
  - Sites
  - Keep
  - Vids
  - Gemini
- No Backup: Additional Services
  - YouTube, Earth, … everything else

- Backup & Restore: Mails, Contacts, Calendar, Drive (mostly), Directory (mostly)



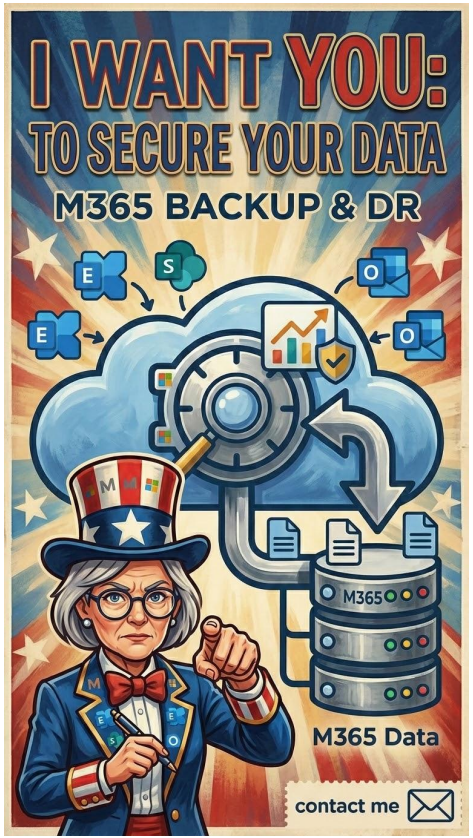
No Chat restore: afi.ai/docs/gw/backup-and-recovery/chats/
No Drive file ID restore: afi.ai/docs/gw/backup-and-recovery/gdrive/#in-place-recovery

schlomo.schapiro.org/2022/04/

Case Study: Microsoft 365 Backup & DR

Gemini: Microsoft 365's highly fragmented architecture and restrictive APIs structurally prohibit a true, full-fidelity backup and restore cycle, forcing modern collaboration workloads into compromised "export-only" recoveries and leaving applications like Microsoft Forms completely unprotected.

Perplexity: Even with Afi, Microsoft 365 only allows full-fidelity backup and in-place restore for some core workloads (Exchange, OneDrive, SharePoint, parts of Entra ID), while others such as Teams chats/private channels, Copilot, Power Platform, many Entra objects, and Microsoft Forms are export-only or unsupported, so you cannot truly "back up everything and restore it exactly as before."



AI-based deep dive research based on Afi.ai (05/2026)

Case Study: Atlassian Jira & Confluence

Atlassian Cloud Security Shared Responsibilities

Information

What Atlassian does	Your role
☑ Access your data only if there is a specific support need to do so	☐ Set up your Atlassian products to reflect the information accessibility that fits your needs
☑ Notify you of any breach we become aware of that affects your data	☐ Create backups of your data
☑ Maintain system-level back-ups (which includes your information)	

YOU!

Source: atlassian.com/whitepapers/cloud-security-shared-responsibilities (PDF)

Case Study: Atlassian Jira & Confluence - Backup

User Count	Jira Family	Confluence
1,000	$7,000	$5,000
3,000	$18,000	$13,000
5,000	$30,000	$21,000
10,000	$55,000	$39,000
30,000	$139,000	$92,000
50,000	$206,000	$122,000

- internal backup only
- 30 days retention only
- no download of backup data
- restore only to empty apps (only full restore)

➢ **Note: Better check out 3rd party backup tools ...**

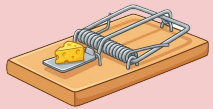
Sources:

- atlassian.com/platform/infrastructure/backup (PDF)
- support.atlassian.com/organization-administration/docs/what-data-is-backed-up-and-restored/ (Coverage)
- support.atlassian.com/migration/docs/supported-products-and-types-of-links/ (Link fixing)

SaaS in a Nutshell

- Focus on the problem
- Use software “as a service”
- No IT operations
- Pay as you go
- Continuous improvement
- Endless scale as needed
- Very reliable
- Very secure
- Benefit from economies of scale
- Specialised solutions can excel
- Certified compliance

- Make do with “standard problem”
- Accept “standard solution” and “standard processes”
- Accept “price adjustments”
- Can’t change core behaviour
- Can’t extend core features
- Blind trust in vendor for reliability, security and compliance
- No or limited perimeter security
- No backup, no restore
- No or limited export
- No means to act in case of problems or outages
- **No data possession**



Perspective of SaaS Vendor

Core Business Model

- Buy commodity storage & compute
- Develop product software
- Implement automated operations
- Sell convenient solution to business problem

Standardization = Economy of Scale

- Standardize problem, solution & processes
- Prioritize new over existing users
- Only good enough to lure users in (“looking good”)
- Capitalize user lock–in via pricing

Benefits of Data Gravity

- Adding data is free & easy
- Taking out data costly / not possible
- Data attracts more data
- Compute goes to data to avoid transfer costs

Skip the Hard Problems

- SLA promise *service availability*, not *data*
- Don’t care about actual customer data
- Abuse by 3rd party: Works as designed
- Protect only against own failures

SaaS Backup & Recovery: Ungraceful Degradation

Original

Restore

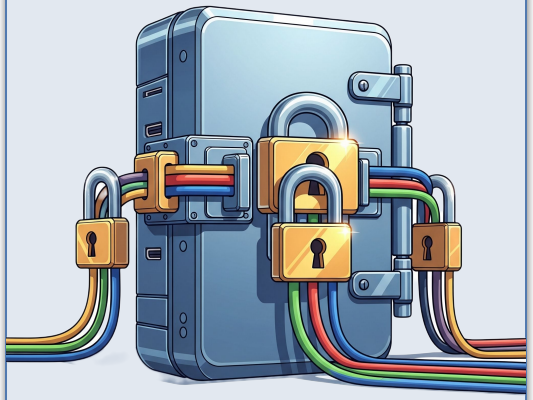
Recover

- Comprehensive Backup Tooling
- Exit Strategies
- Data Sovereignty
- Change Management
- Identity Federation
- Delegated Privilege Management
- Complete API Access
- Neutral Data Formats

⚠️ Non-Functional Requirements ⚠️

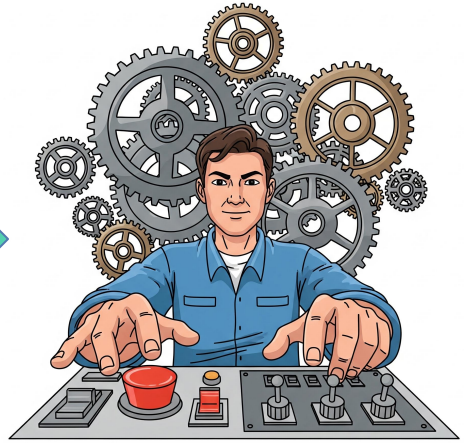
Escaping the SaaS Trap

The Path to Sovereignty



Data Sovereignty

We have our data



Technical Sovereignty

We own our processes and operations

Political / Legal Sovereignty

We own our decisions & destiny

Example: Affordable Offline Backup Google/M365

- Synology Plus models (also QNAP)
- Backup Mail, Calendar, Contacts, Drive
- Export to MS Office formats
- Local data export without Internet & Cloud possible
- Cost scales with data volume, not user count
- Data on-premise, not in Cloud
- Full data ownership and sovereignty
- Lowest total cost (< 1000€)
- ✔ for 10 user domain and more

TODO for larger domains:

- Compare QNAP Boxafe and Synology Active Backup for Google Workspace
- Check manual efforts (auto add new users, expunge deleted users, user self-service ...)
- QNAP has Enterprise version

Could be that a NAS appliance is also the best solution for large domains. I don't recommend cloud-based solutions as they don't provide true data sovereignty.

schlomo.schapiro.org/2022/04/

Example: AI Coding for Backup Tooling

Context: Harvest time tracking operative backbone for consultancy firm

Problem: SaaS vendor offers no backup

Solution:

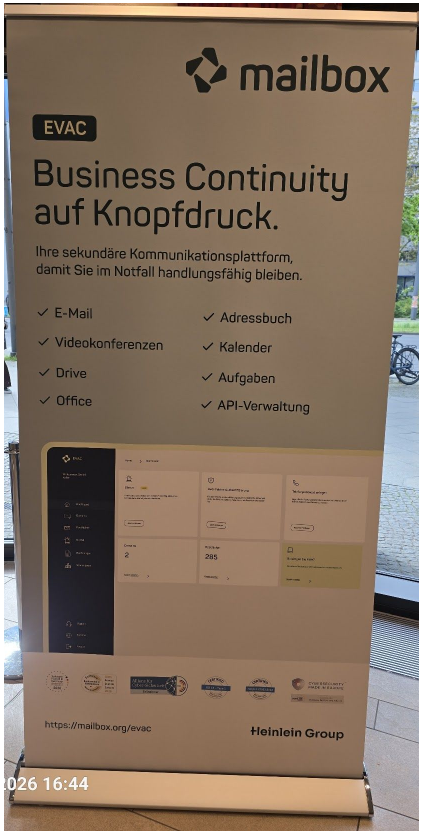
- Cursor AI: *Based on Harvest API spec, create a backup tool that runs in a Docker container and downloads all data incrementally, storing it in the plain JSON formats used by the API*
- Cost: 50€ & 2 days occupation as background task
- Save raw JSON from API
- Recovery strategy
  1. Restore via API to Harvest (HTTP PUT)
  2. Use AI to convert data to future **different** tool

Having our own data is good enough!

schlomo.schapiro.org/2026/01/no-export-button-no-problem-how-i-used.html, Open Source

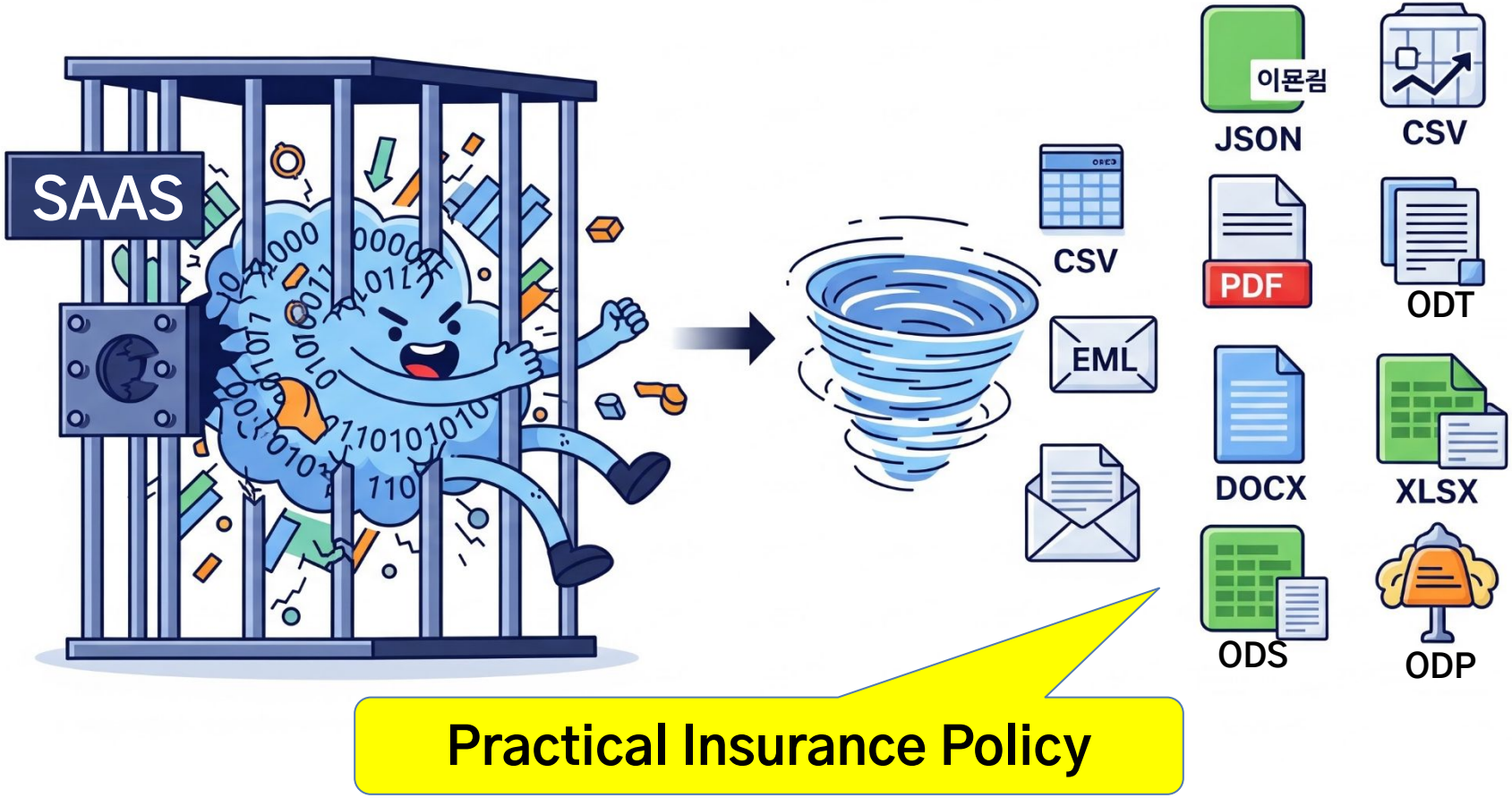
Example: Mailbox.org EVAC

- On demand PIM environment
- Ready-to-use in case primary PIM not available
- Ultra low cost, contains no data
- Enables quick recovery of critical communication and collaboration capabilities after a major outage
- Managed services on top of Mailbox.org, providing full Mailbox.org featureset when needed at regular pricing.



mailbox heinlein

Data Jailbreak: Export to Open Data Formats



Lifeboat Architecture: Use SaaS, Have Data

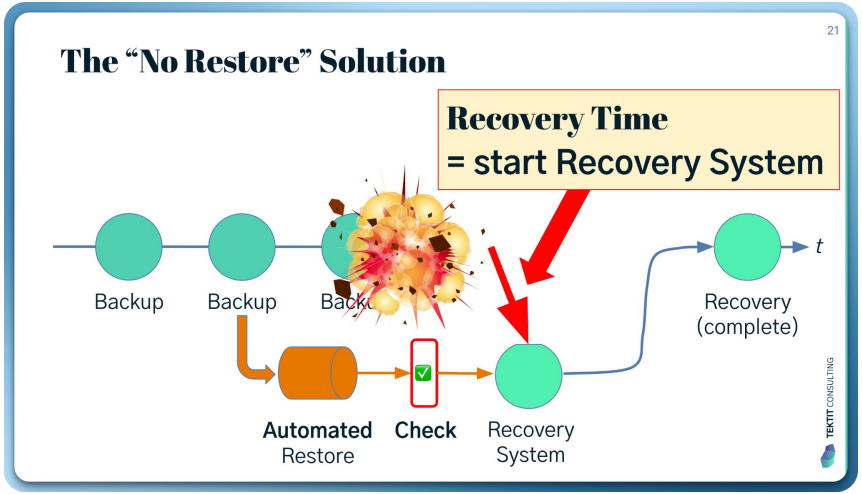
Keep a full copy of your data in **your own possession** while making full use of SaaS offerings.

schlomo.schapiro.org/2026/02/the-sovereignty-bluff-tenants-in-our-own-business.html

Building your “Minimum Viable Company”

Mission Critical Systems:

- Core business applications
- Communication & Collaboration
- External Facing web / phone / …
- … what **keeps the money coming** in …



Recap: Digital Sovereignty = Exit the SaaS Trap

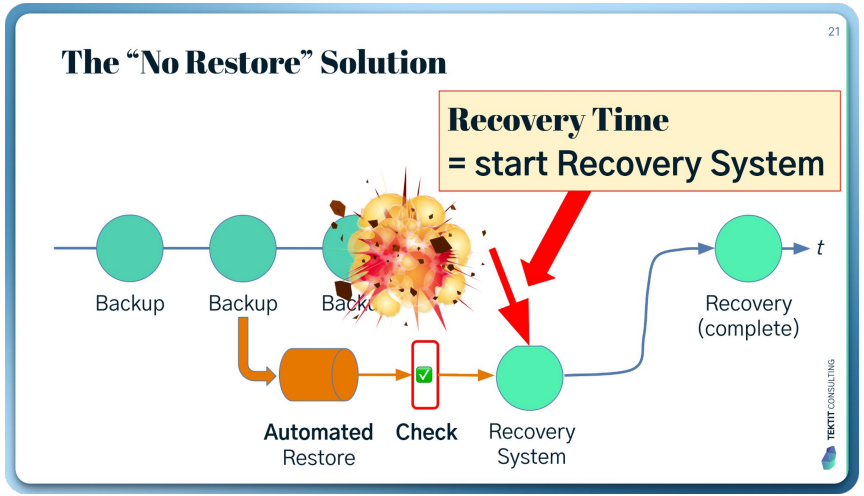
Guiding Principles

Backup is the means to enable Restore

Comprehensive Backup & Restore Automation
is the means to enable
Disaster Recovery and Business Continuity

Use the Same Backup for
Restore and Disaster Recovery

TEKTIT CONSULTING



Master Plan:

- Backup everything – Lifeboat Architecture
- AI-development to create backup tooling
- Minimum Viable Company – **Instant recovery** for **critical systems**
- Accept data loss after SaaS outage, focus on company survival

FIRST STEPS

TRIAGE

TEKTIT CONSULTING

Q&A — How may I help you?

tkt.dev/schlomo

We are not consultants. We are Partners, Coaches, Humans, Enablers, Catalysts, Sparring Partners, Experts … and sometimes a little annoying.

I focus on **IT strategy**, IT governance, technology and architecture management, security and compliance automation, related organisational changes, business continuity, open source and cloud technologies – and I'm available as a Principal Engineer or Technical Product Owner for short-term / interim support.

Examples:

- **Business-IT alignment & leveraging**, developing required skills and abilities for 21st century IT, leverage AI
- **SaaS compliance & governance**, data possession vs. ownership, IAM, integrations, backup & DR, shadow IT
- **Compliance Automation**, finding the "golden path" to a "golden state" via **Platform Engineering**
- **Secrets Management** for Datacenter, Cloud Infrastructure, IaaS/PaaS/SaaS
- **Open Source**, from usage to contribution, writing policies, using SBOM, establishing Open Source Stewardship
- **Good Engineering Practices**, GitOps, test driven development, good architecture decisions, known tech strategy
- **Business Continuity and Disaster Recovery** for office, Cloud infrastructure, data center & SaaS, with quality assurance, emergency communication & collaboration, hot & cold standby, no-restore solution, ransomware protection, Linux Disaster Recovery / Bare Metal Restore with "Relax and Recover (rear)" Open Source tooling

schlomo@tkt.dev

TEKTIT CONSULTING