

 [@schlomo@floss.social](mailto:schlomo@floss.social)
 [@schlomoschapiro](https://twitter.com/schlomoschapiro)



Backup and Disaster Recovery

Business as Usual or
What Needs to Change Now?

18. June 2025, DevOpsCon 2025, Berlin

Schlomo Schapiro, Associate Partner / Principal Engineer, Tektit Consulting

DevOpsCon
+KUBERNETES
BOOTCAMP



Agenda

1. Introduction to the Basics
2. Data Center Best Practices
3. The 8 Challenges
4. Facing the New Reality
5. Conclusion



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.

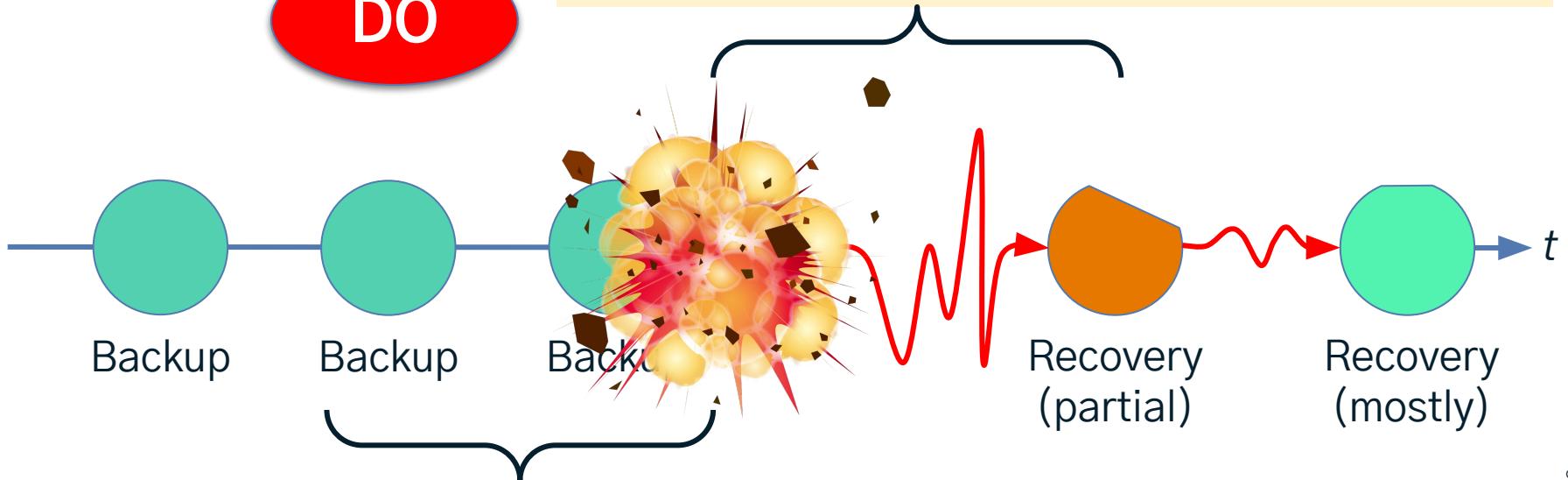
Staying in business, no matter what!

The Timeline

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 ...

Disaster Recovery

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

When we have

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

When we don't have TIME

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

Guiding Principles

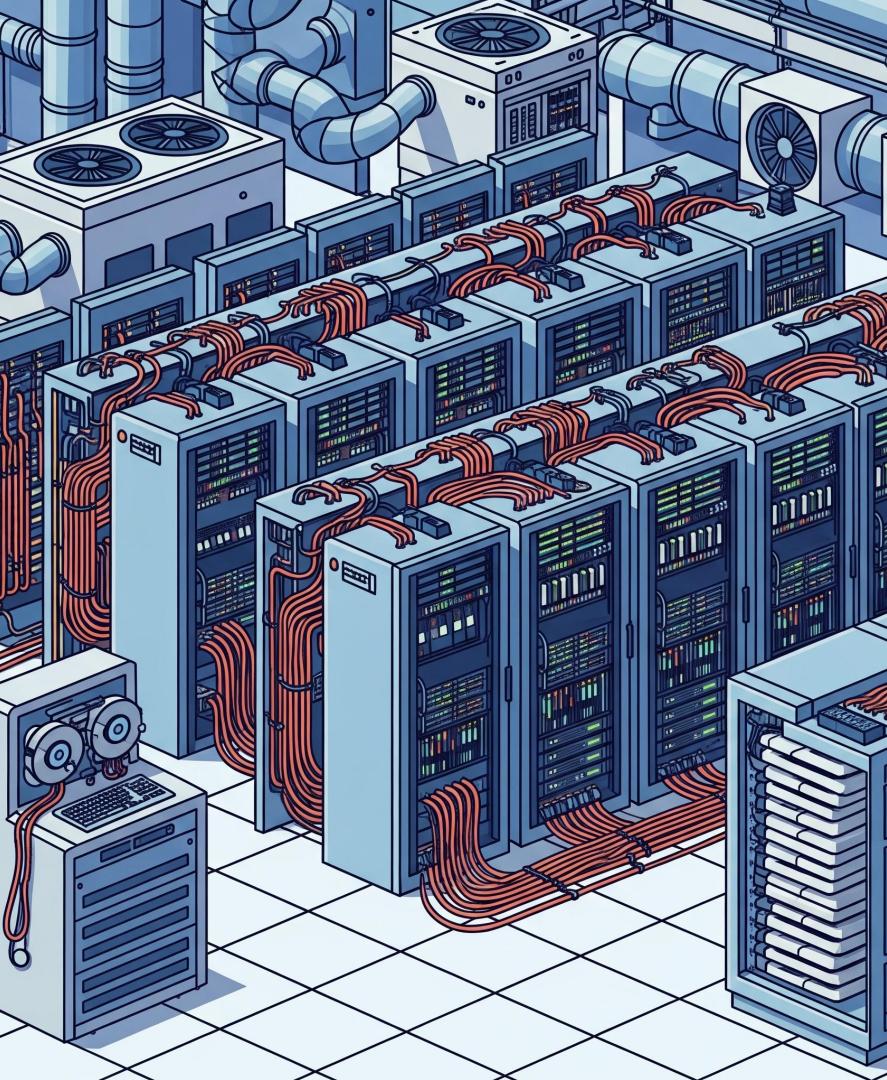
Backup is the means to enable **Restore**

Comprehensive Backup & Restore Automation

is the means to enable

Disaster Recovery and Business Continuity

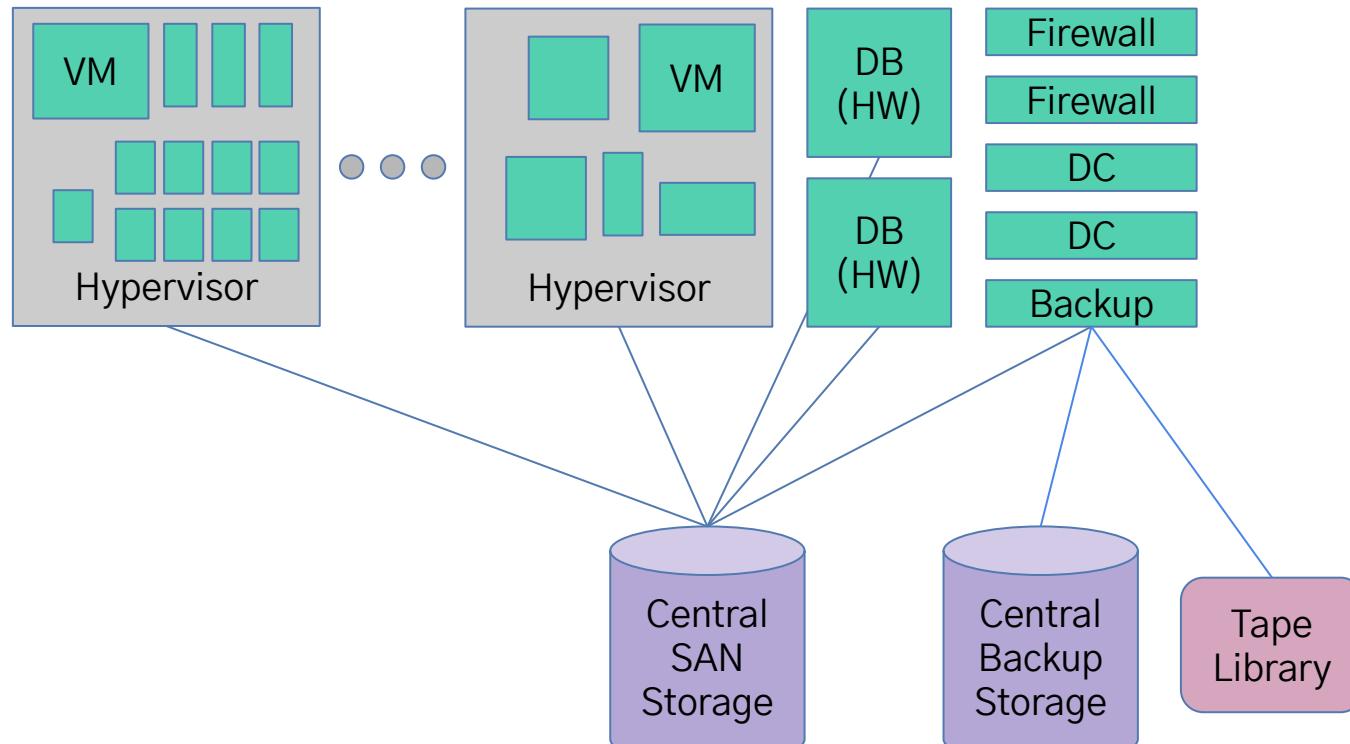
Use the **Same Backup** for
Restore and Disaster Recovery



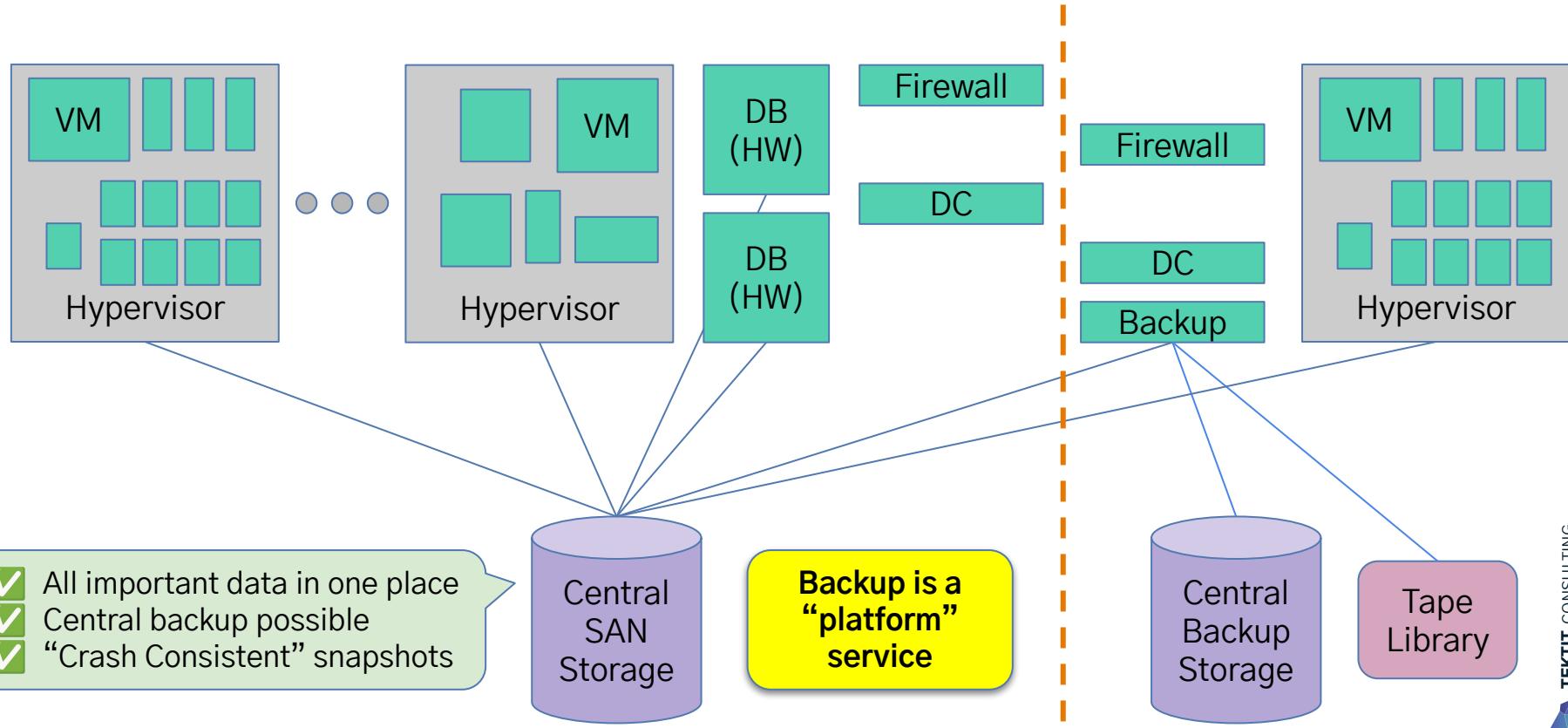
Data Center



Data Center Architecture

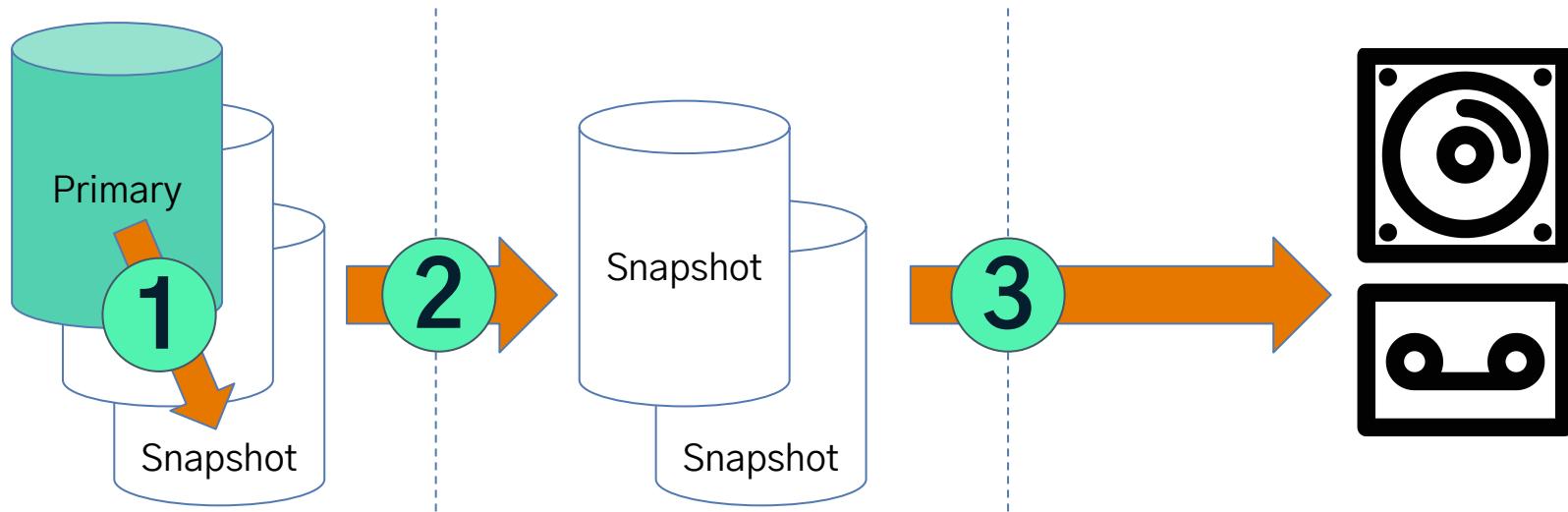


Data Center Architecture (Extended)



Backup 1-2-3

Reducing RPO: Snapshots + Replication + Offsite Backup

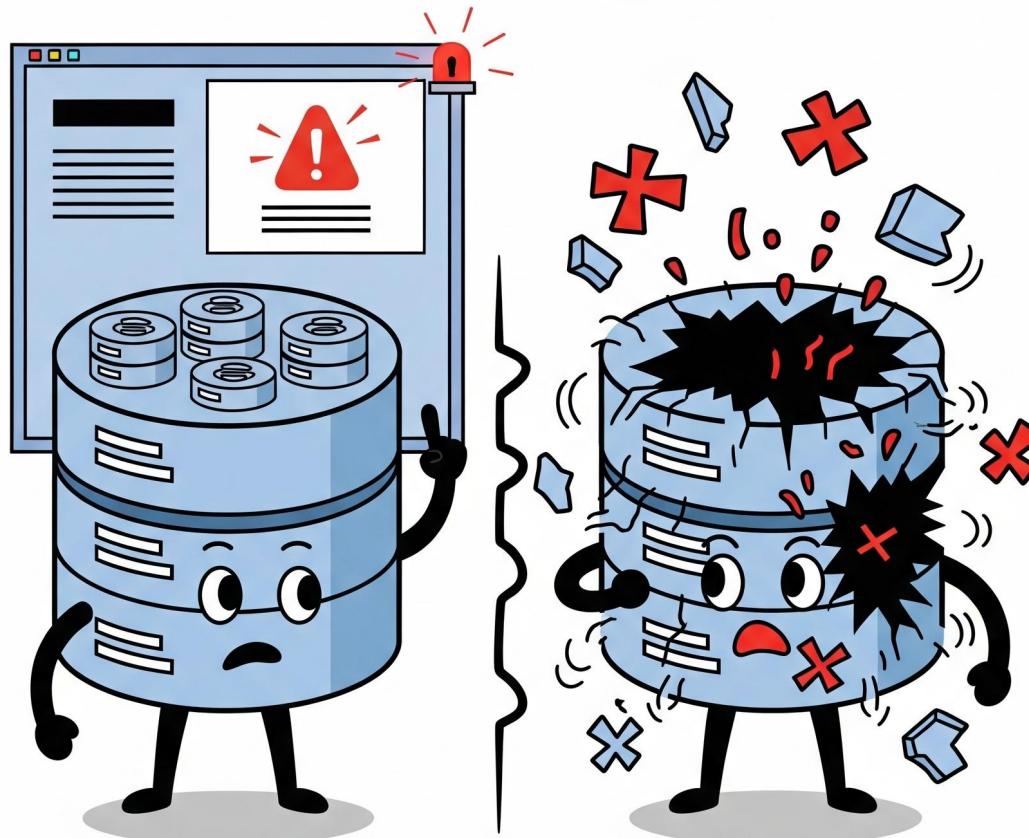


1. Snapshots

2. Replication

3. Offsite Backup

The Consistency Challenge



The Consistency Challenge

Applications use multiple servers and services, **assuming** they always match, e.g.:

- Database has metadata for files on file server
- Multiple databases or file shares

Multiple applications are part of a business process

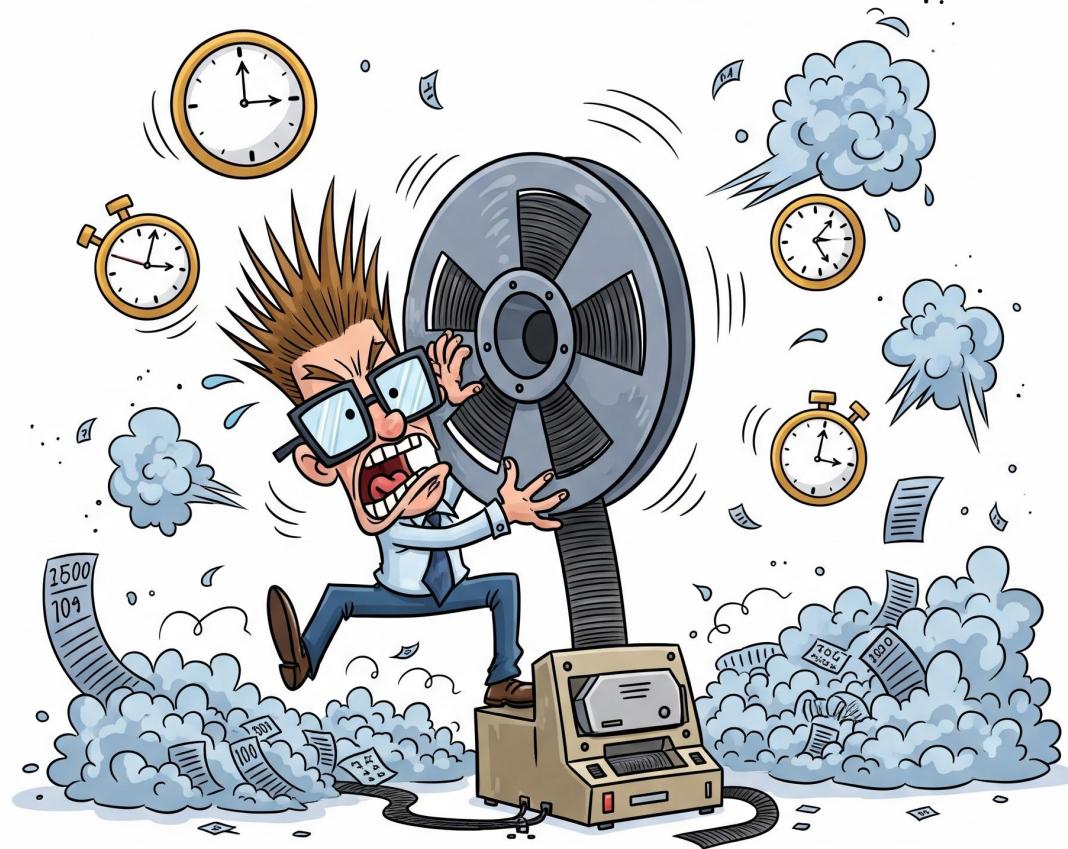
- Business transactions spanning multiple servers and databases
- Business transactions take a long time or are not even transactional

Problem: How to create a backup with **data consistency**?

Solutions:

- Stop all services – take snapshot or backup – resume all services, e.g. at night
- Find inconsistencies and rebuild data consistency after restore — automatically!
- Ignore the problem and hope for the best

The Restore Time Objective (RTO) Challenge



RTO Example: Catastrophic SAN failure (worst case)

Context:

- 140 TB SAN storage
- LTO-9 tape library
($400 \text{ MB/s} = 1.44 \text{ TB / hour}$)

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

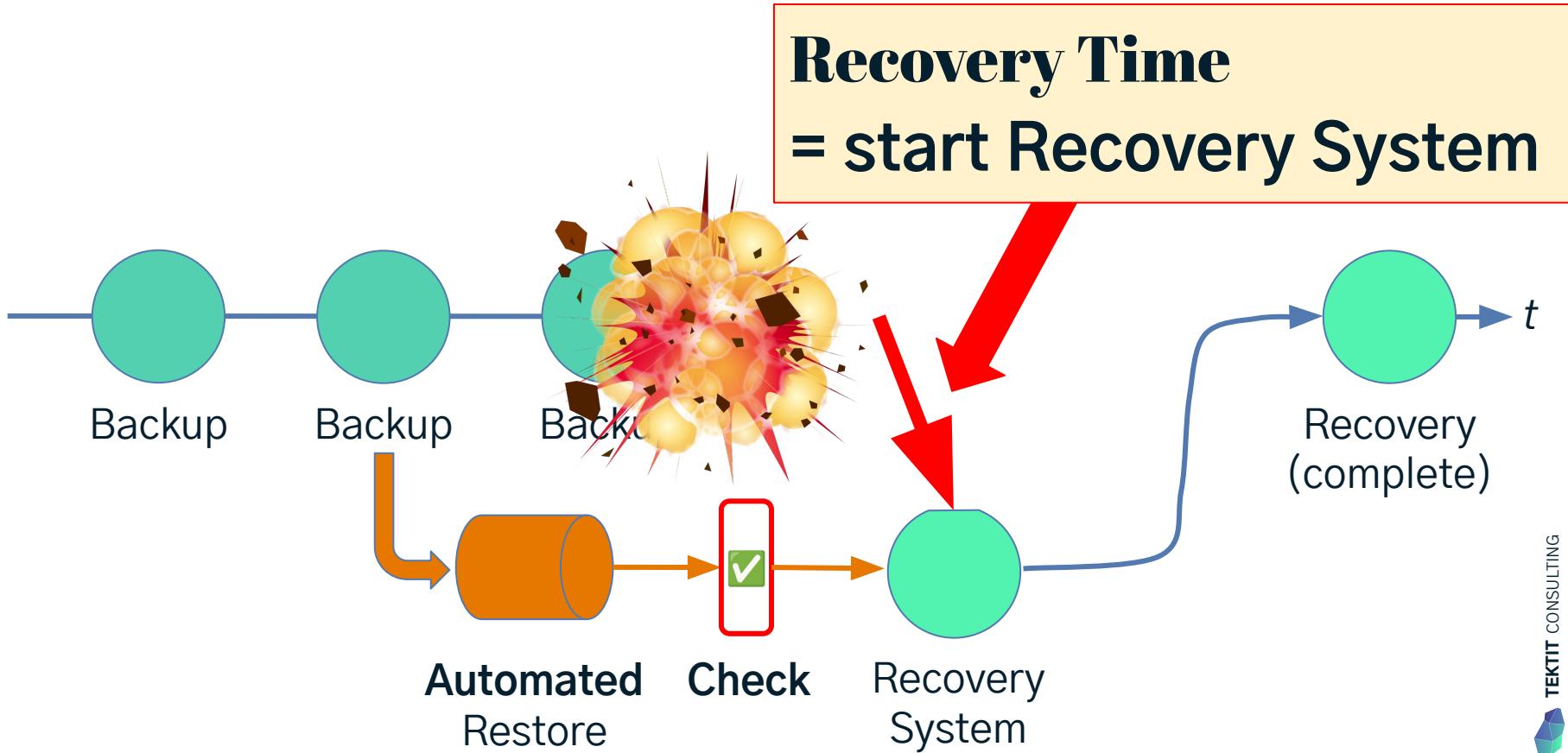
Try to **restore** when needed

Switch to working &
verified recovery system

Fixed
RTO



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!”



Regulation

Main Obligations

KRITIS (Critical Infrastructure)

[BSI-Gesetz \(BSIG\):](#)
§ 8a

Resilience of Essential Services:

- Implement appropriate organizational and technical measures based on the "state of the art" to avoid disruptions to the availability, integrity, authenticity, and confidentiality of IT systems essential for providing critical services.
- This requires robust business continuity planning and disaster recovery capabilities.
- Conduct a Business Impact Analysis (BIA) to determine Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).
- Provide proof of implementation and effectiveness to the Federal Office for Information Security (BSI) at least every two years.

NIS2 Directive

[Directive \(EU\)](#)

[2022/2555 \(NIS2\):](#)

Article 21

Mandatory Risk Management Measures:

- Implement a baseline of cybersecurity risk-management measures, which must include policies and procedures for:
 - Backup management and disaster recovery.
 - Business continuity and crisis management.
- Address the security of the supply chain, ensuring that dependencies on third-party providers do not compromise operational continuity.
- Establish plans for incident handling and response to maintain or restore operations.

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.

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

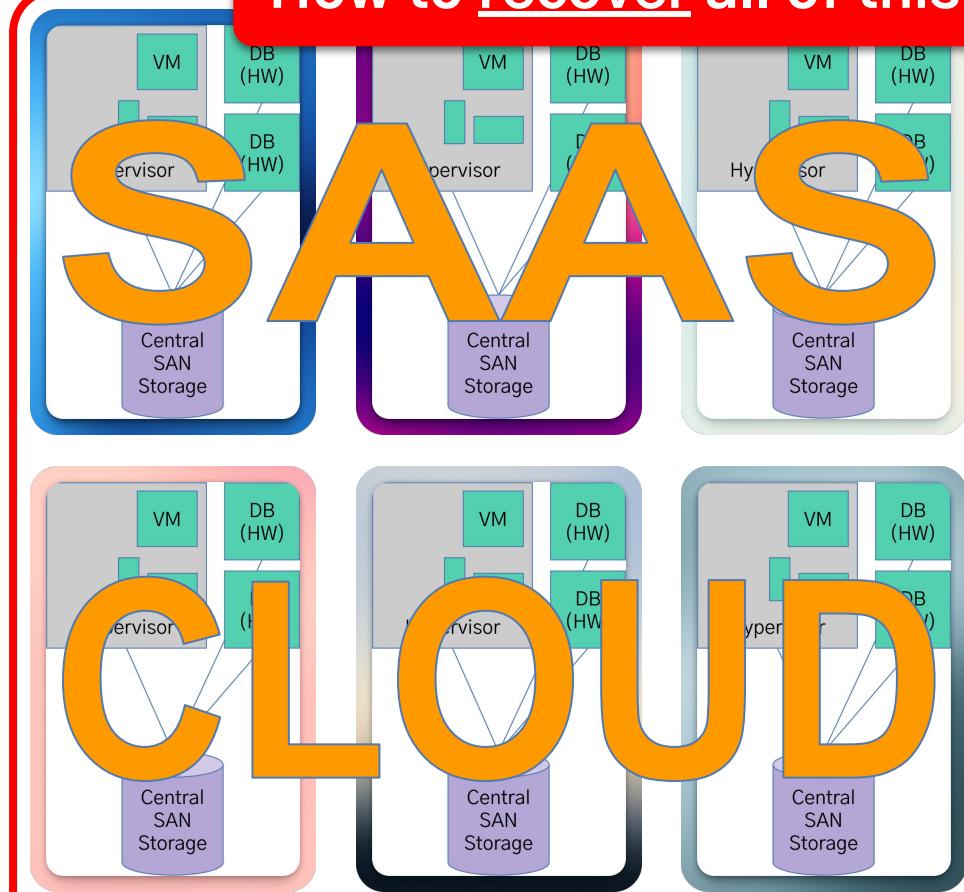
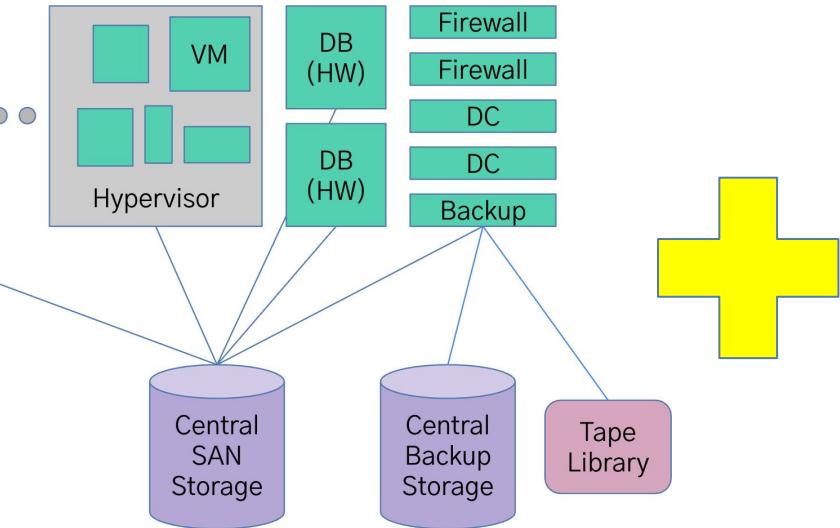


The Cloud & SaaS Challenge

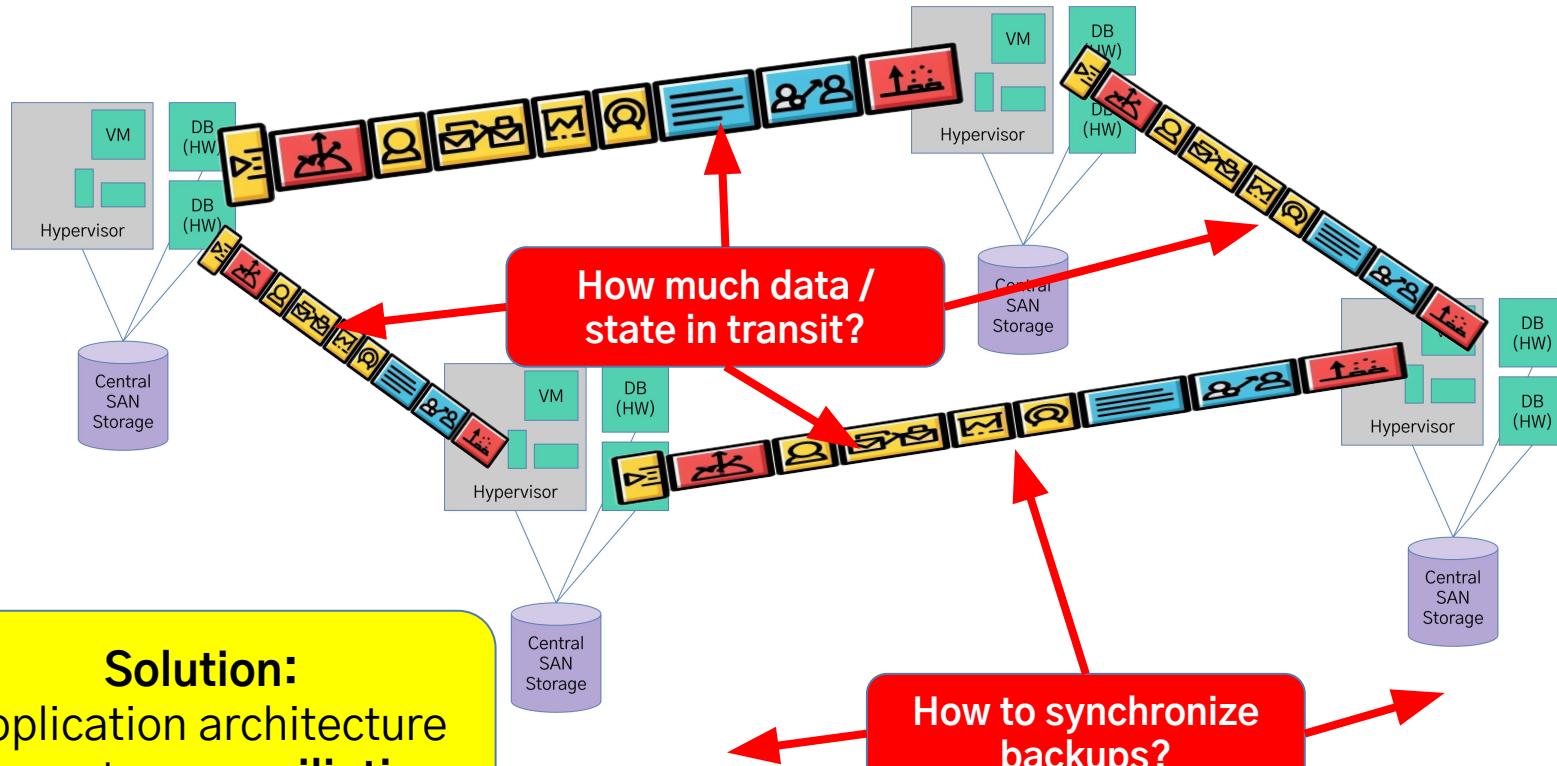


Decentralize Everything

How to recover all of this?



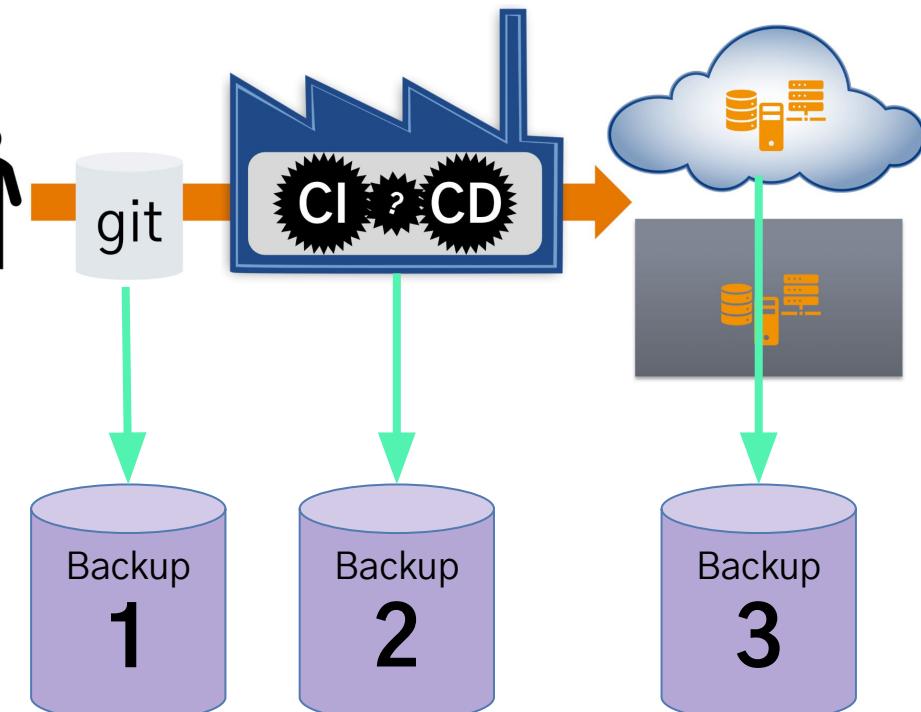
Decentralized Consistency Challenge & Queues



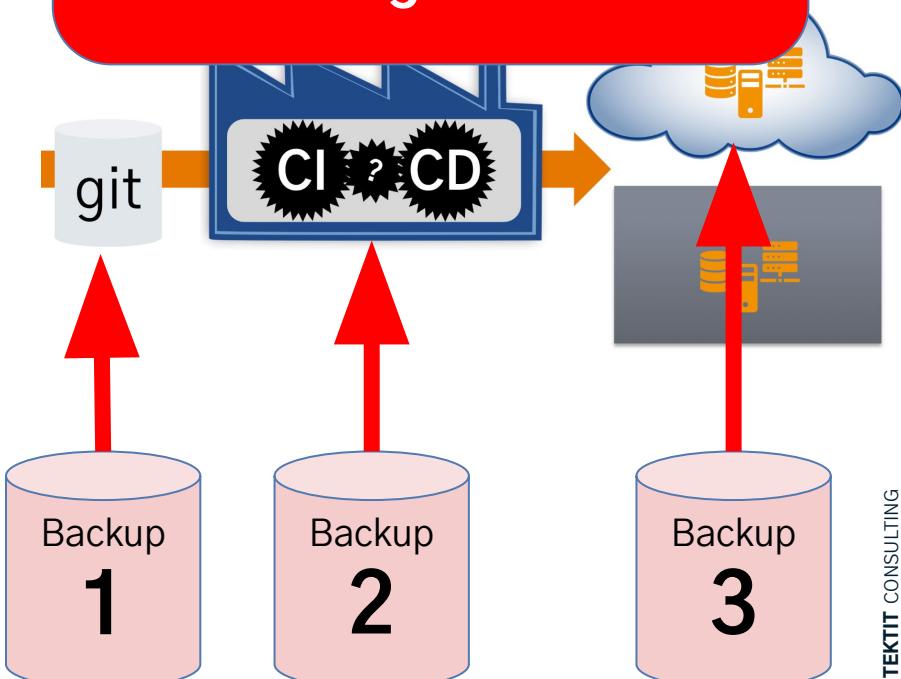
The IaC Challenge



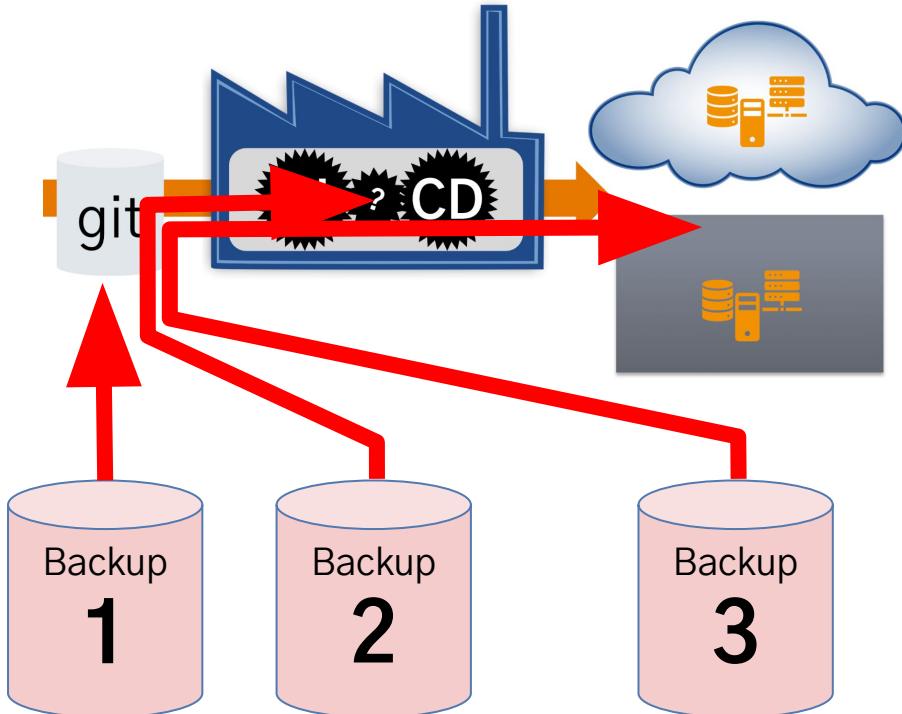
The IaC Challenge



How will
Data, Code & Config
fit together?



The IaC Challenge — Solution



- **Guiding Principle:**
Everything gets deployed via the **same** tooling
- **“Application” responsibilities**
 - Deploy **code & config**
 - Deploy **backup tool**
 - **Restore data if missing**
 - Ensure **consistency**
- **Automate** restore & recovery



The Shattered Restore Challenge

SAAS: NO RESTORE

Original:

docs.google.com/presentation/d/1P8tgUjHlkWIG4wFbBaiv1otqPRWm4BWAb0Z5BfoSxGc/

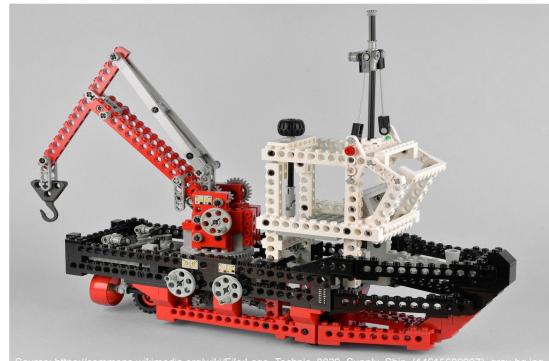


Restored:

docs.google.com/presentation/d/1hpuOs42vEFHF7Ancp3F136v83PZxqRS6B273mQ8ecLY/



Your Data before Backup:



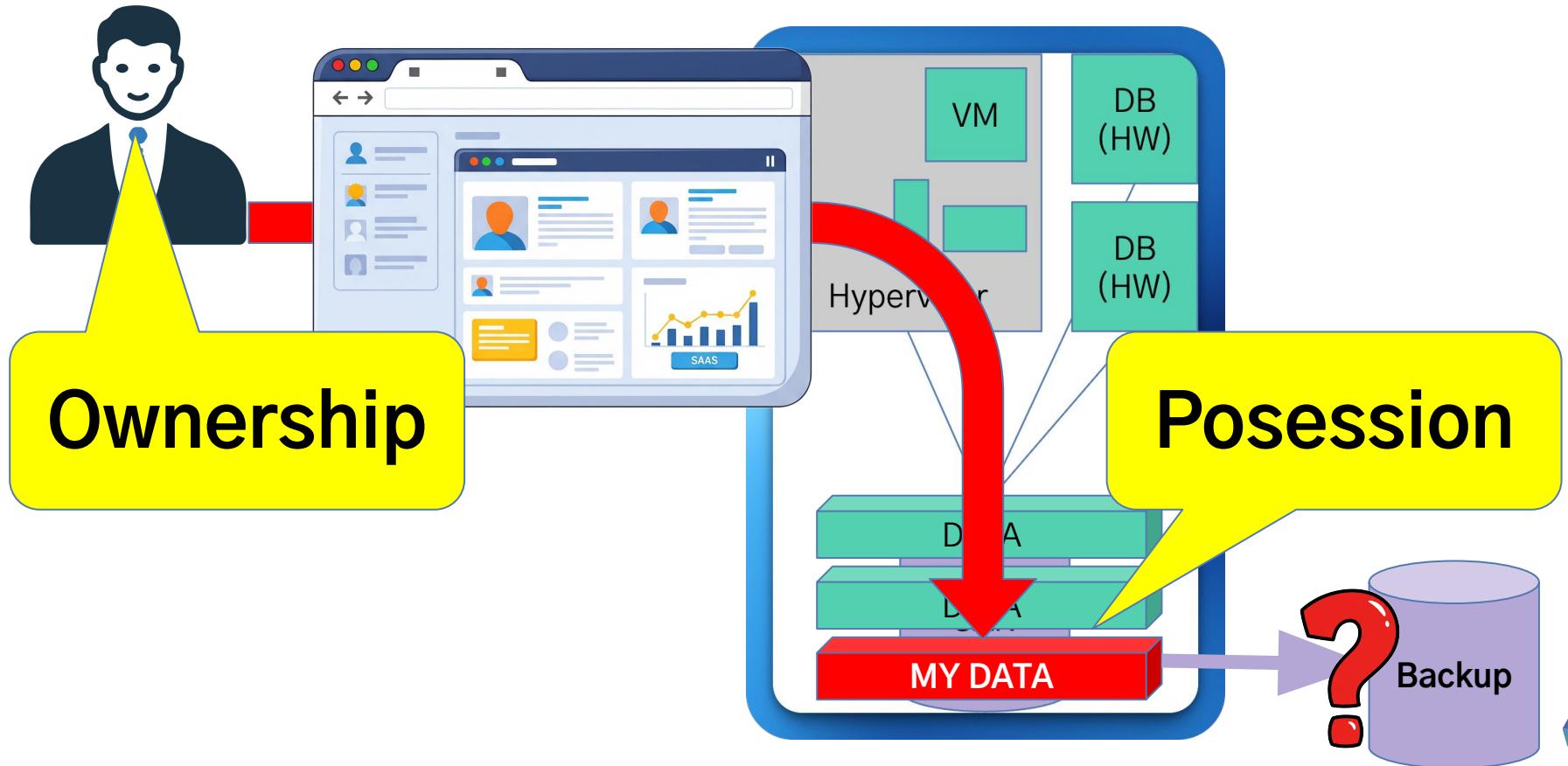
Your Data after Restore:



The Data Posession Challenge

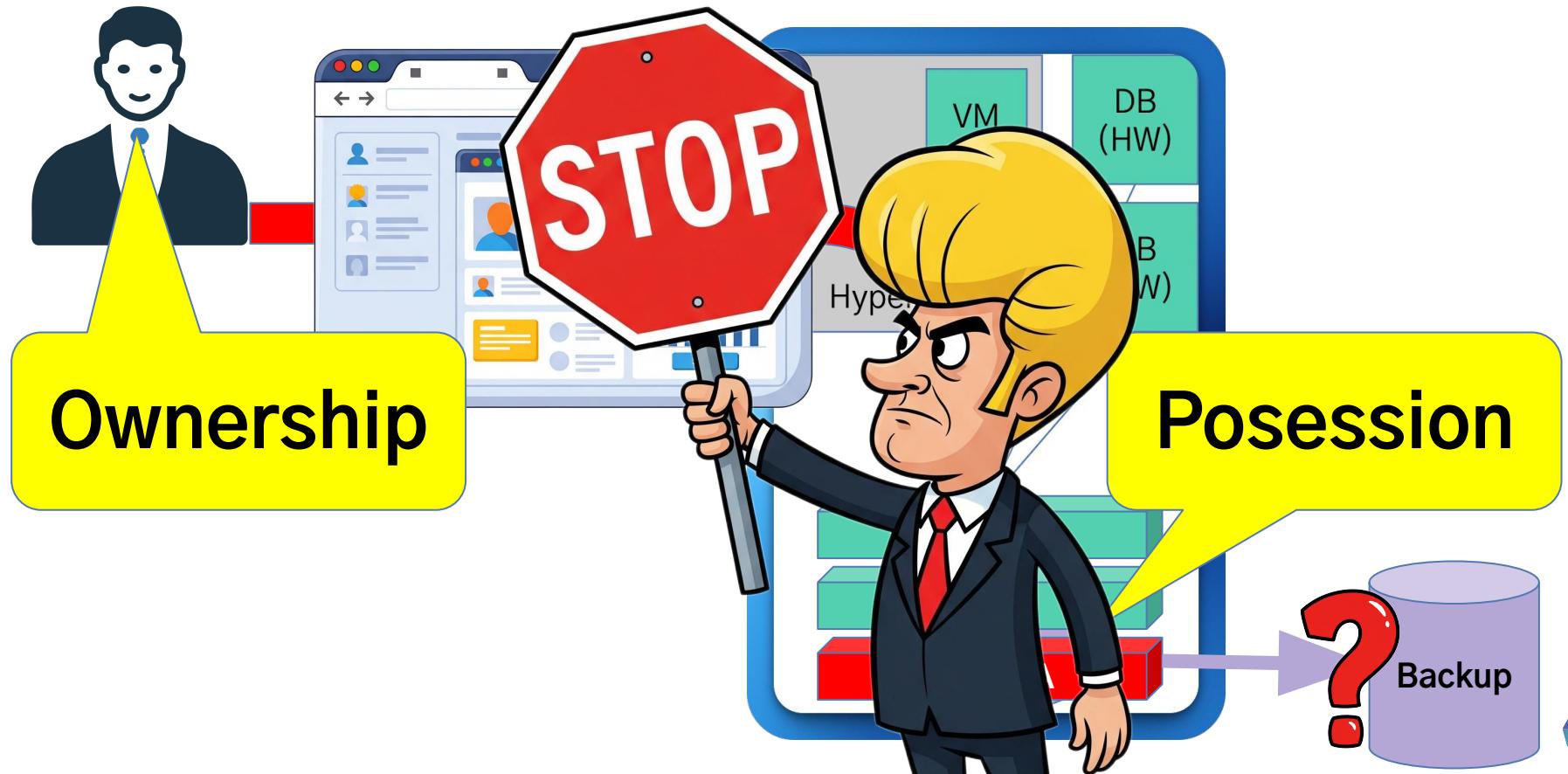


The Data Possession Challenge of SaaS



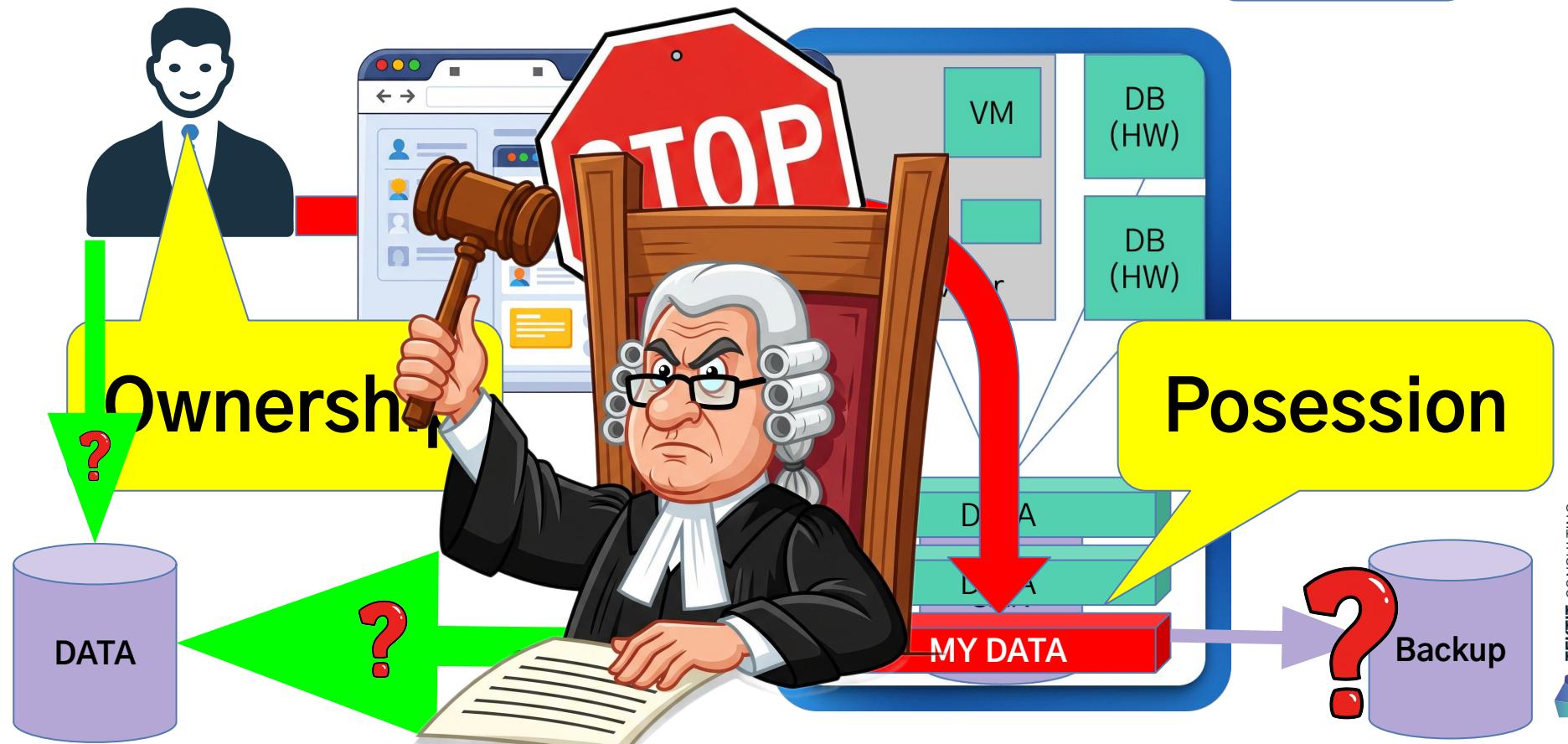
The Data Posession Challenge of SaaS

NO DATA



The Data Possession Challenge of SaaS

NO DATA



The SLA Challenge



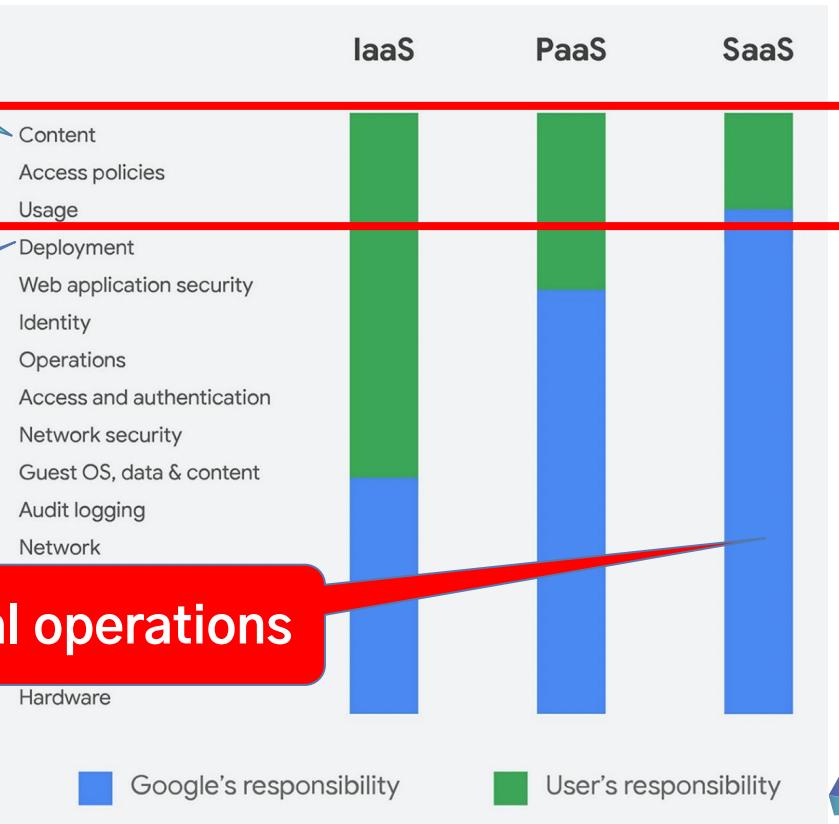
The SLA Challenge: We don't care about your data!

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

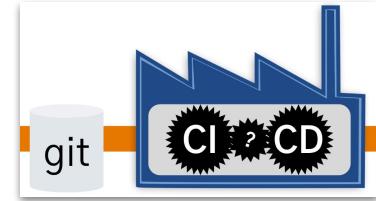
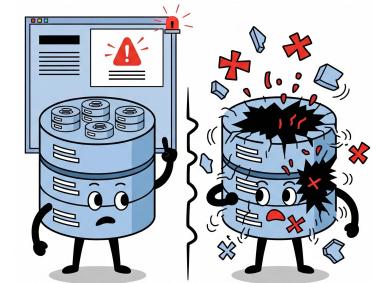
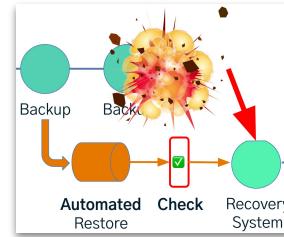


Some Personal Materials

- Relax and Recover (ReaR) Open Source Project (since 2006),
Automated Linux Disaster Recovery (Video stackconf 2024)
- The Simple High Available Linux File Server (SambaXP 2008),
Virtualisierte Cold-Standby-Server für Linux (iX 4/2008)
- “easyVCB” Open Source Project, VMware “No Restore Solution” (2008),
now “VMware Live Recovery” & “Veeam Recovery Orchestration”
- Mission Impossible: Complete Disaster Recovery for Google Workspace
(Research, Article, Video 2022)
- DevOps Risk Mitigation – Test Driven Infrastructure
(Video euroPython 2014)

The New Era of Backup & Disaster Recovery

- Backup 💪, Restore 💪💪 & Disaster Recovery 💪💪💪 is hard to solve
- Fixed RTO: “No Restore Solution”
- Applications own Data Consistency
- Know your Regulatory Obligations
- Automate Restore & Recovery
- Beware of SaaS: No SLA for Data, No Data Possession, No Restore



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