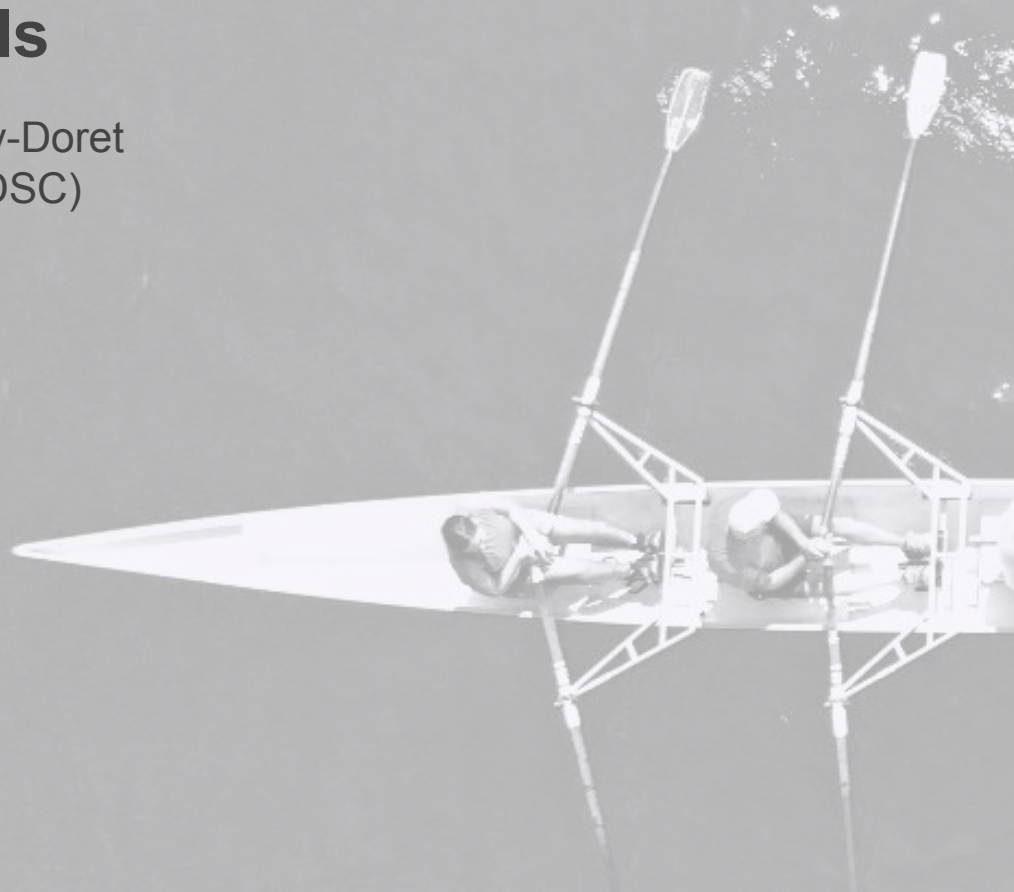


Security and Infrastructure in the LUCID Project: A National Registry of Quality of Care in Swiss University Hospitals

Martin Fontanet & Cyril Matthey-Doret
Swiss Data Science Center (SDSC)



LUCID – National Data Stream

- Overarching goal: Build a National Registry to monitor and foster research in the field of quality of care of hospitalized patients.
- More precisely, study **low-value care**.

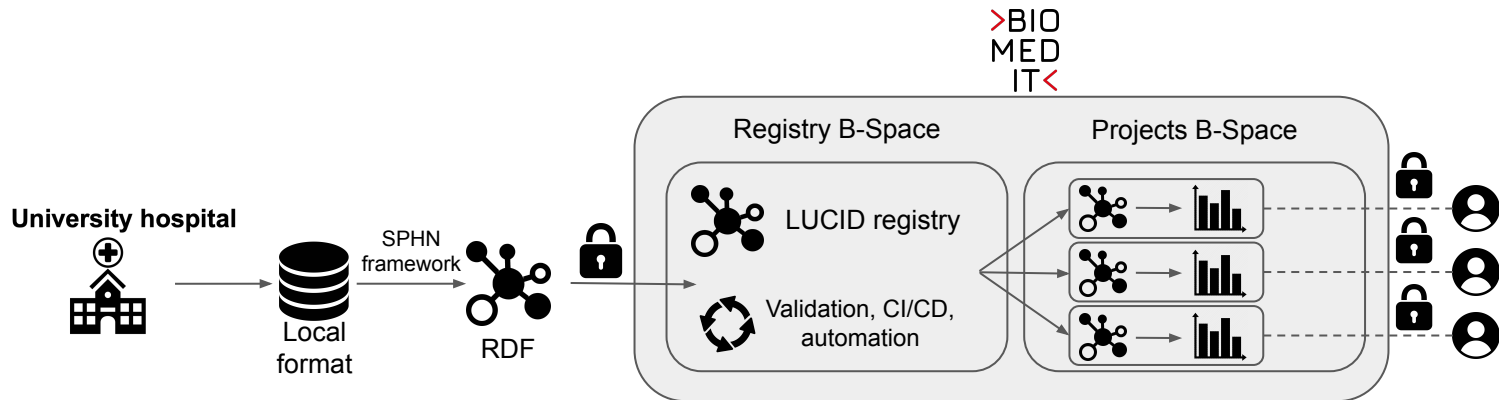
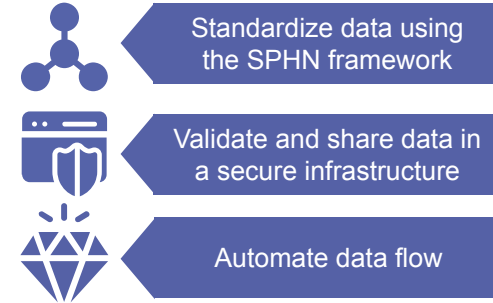
Low-value care: Practices that provide little or no benefit to patients, have the potential to cause harm, incur unnecessary cost to patients, and/or waste healthcare resources. (~20% of Healthcare Expenditures)

Data flow overview

Hospital data is scattered and not standardized

Researchers' access to clinical data is difficult

Only necessary data must be provided

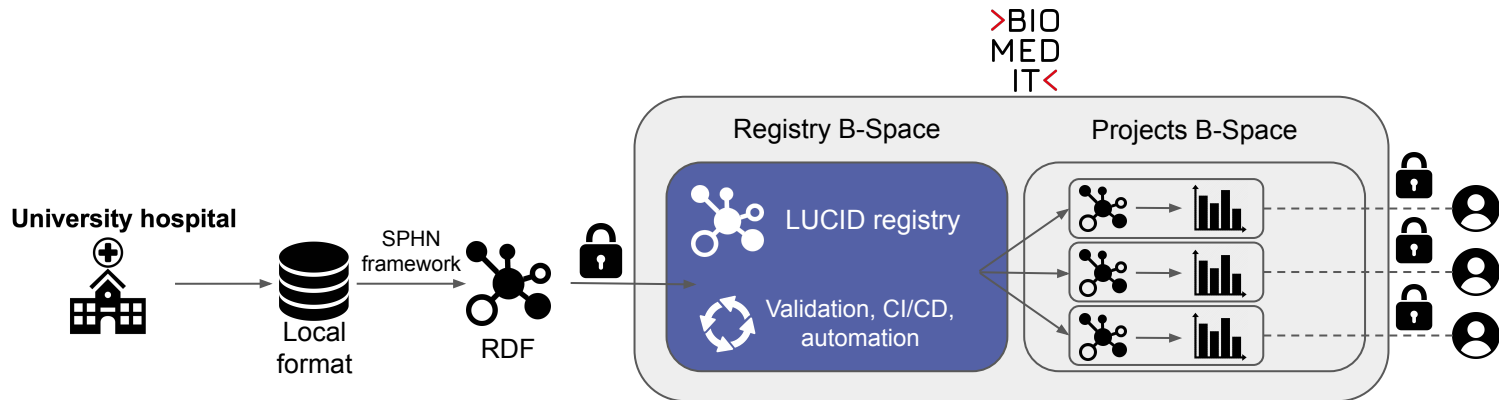
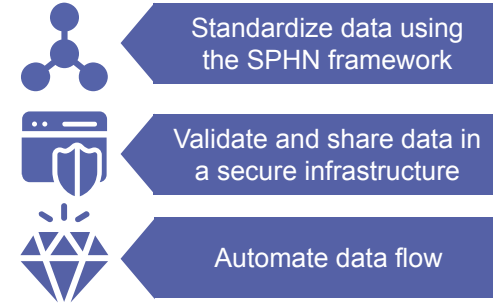


Data flow overview

Hospital data is scattered and not standardized

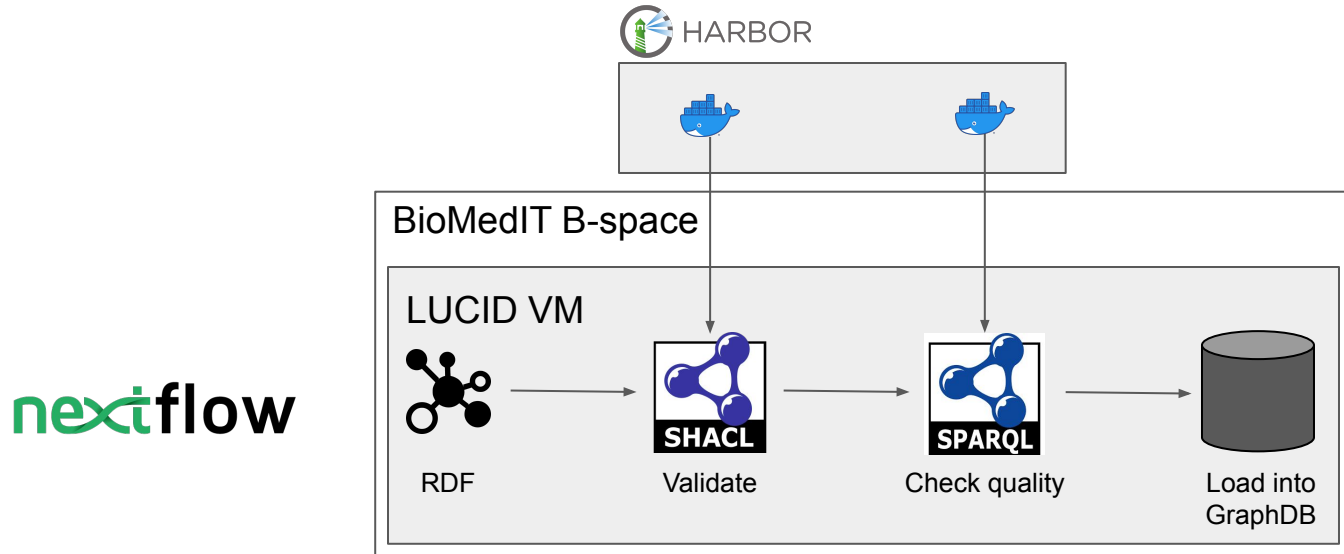
Researchers' access to clinical data is difficult

Only necessary data must be provided



Data flow setup

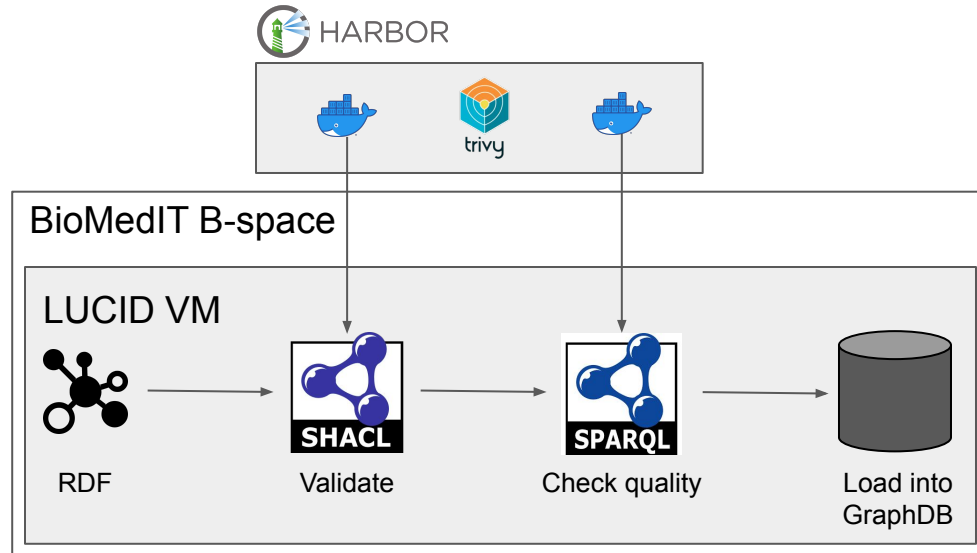
- Execution in a secure environment (aka B-space)
- Containerized software hosted on internal Harbor registry
- We use Nextflow to orchestrate containerized workflow steps



Container image management

- Images undergo vulnerability scans (trivy) in the registry
- Images may have potentially harmful software or insecure configuration
- We require more granular container access policies than Harbor allows

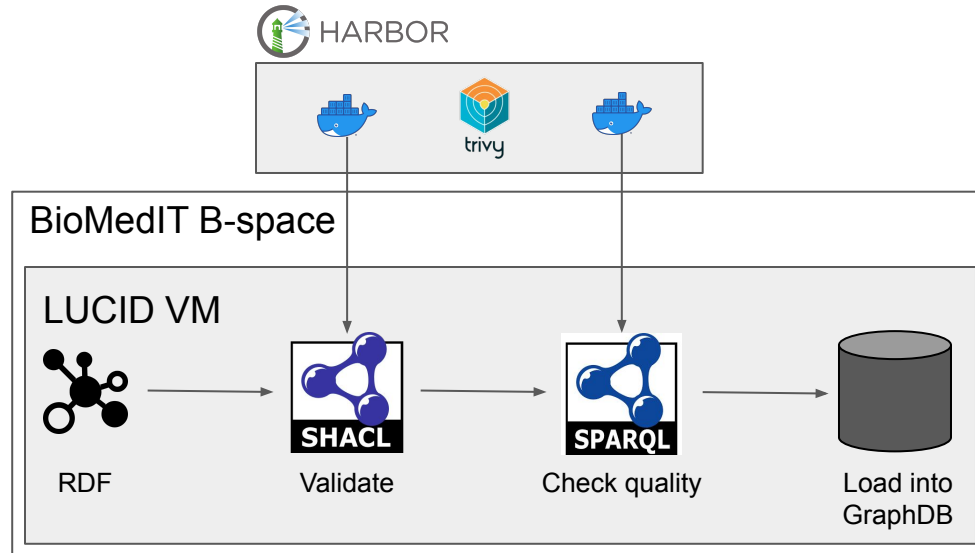
nextflow

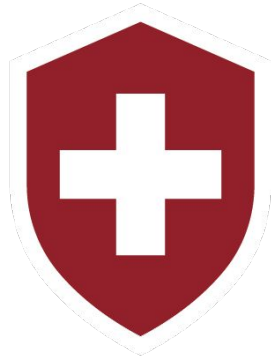


Container image management

- Images undergo vulnerability scans (trivy) in the registry
- Images may have potentially harmful software or insecure configuration
- **We require more granular container access policies than Harbor allows**

nextflow





Swiss Data Custodian

Why Custodian: Simplifying Privacy Protection

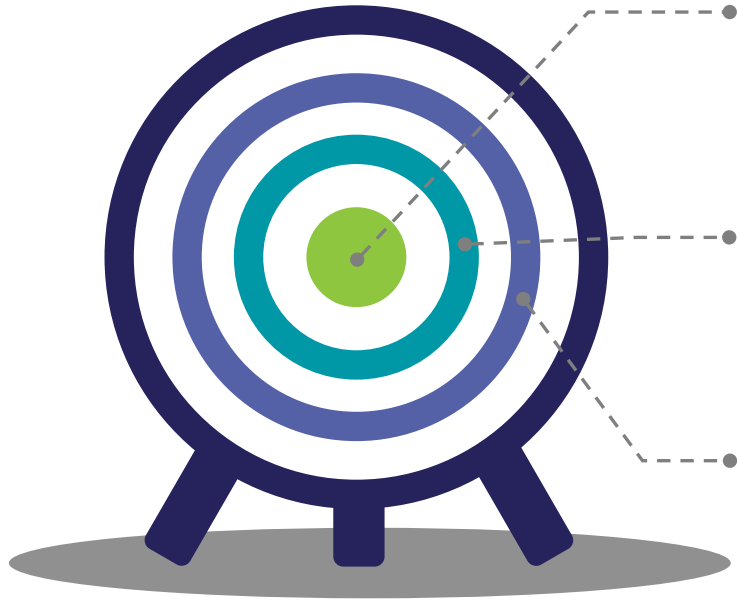
Challenge:

- Compliance with data privacy regulations
- Evolution of the legal requirements

Solution: The Swiss Data Custodian

- Simplifies privacy protection
- Helps organizations stay ahead of the compliance curve
- Eases compliance with GDPR and nFADP

The Swiss Data Custodian aims to



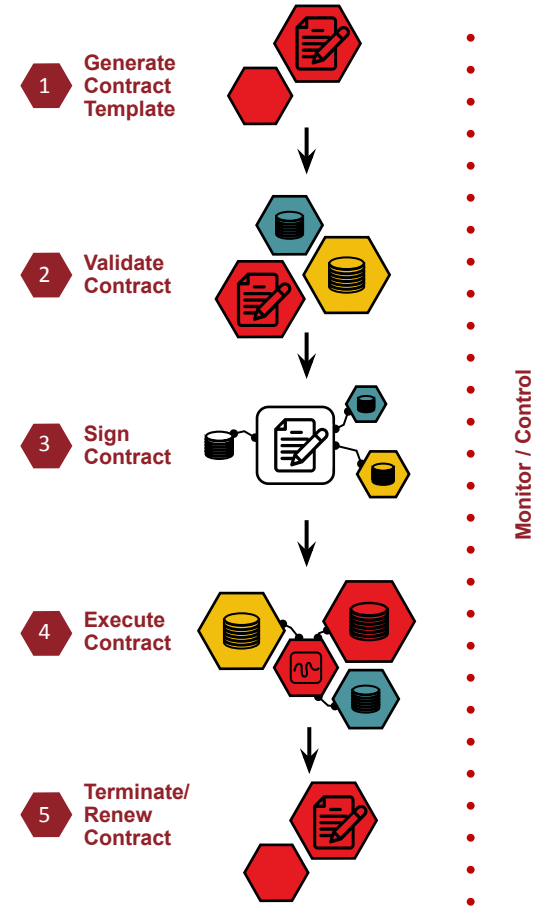
Give data subjects control over their data

Enhance sensitive data reuse and sharing

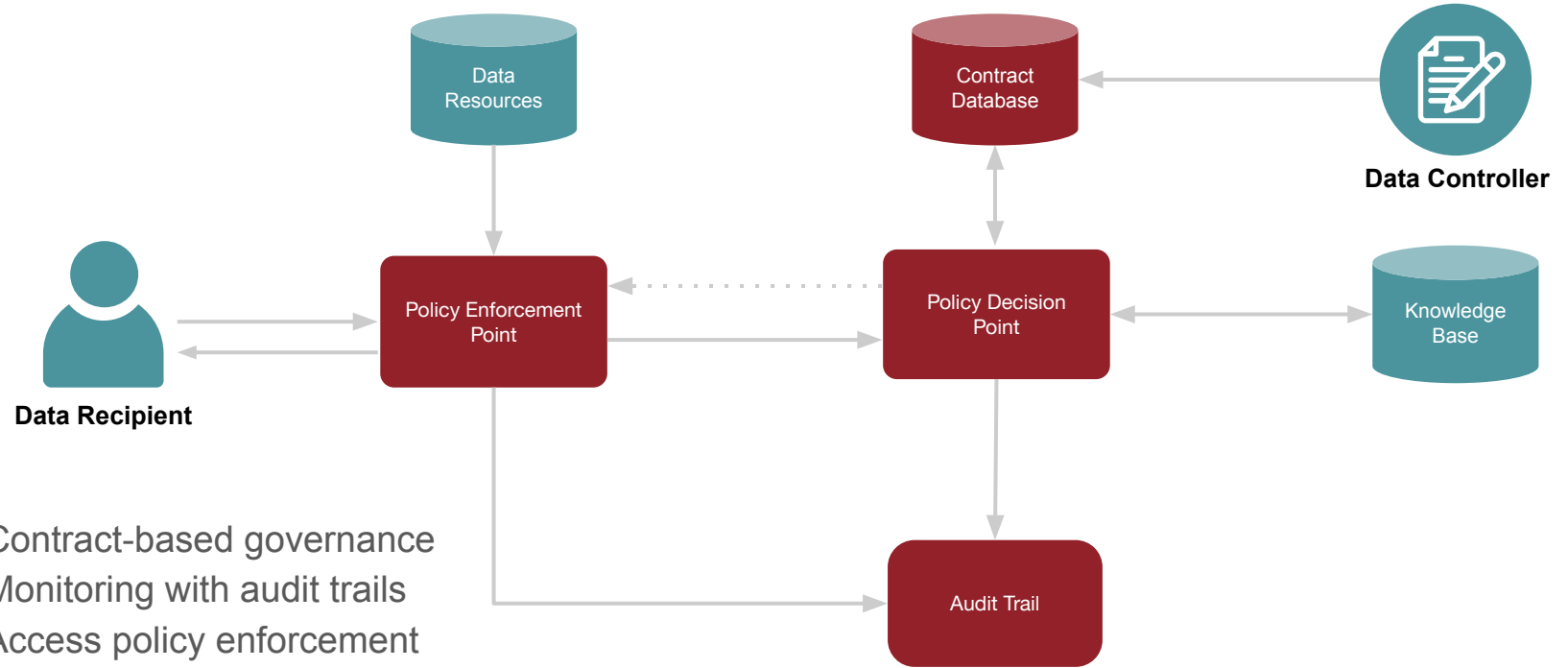
Enable value-added services using sensitive data resources

End-User Agreement Contracts

- Clear and informative description:
 - What data is being accessed
 - Where it is being stored
 - By whom it can be accessed and how
- Unforgeable, non-repudiable, and revocable
- Low overhead for users

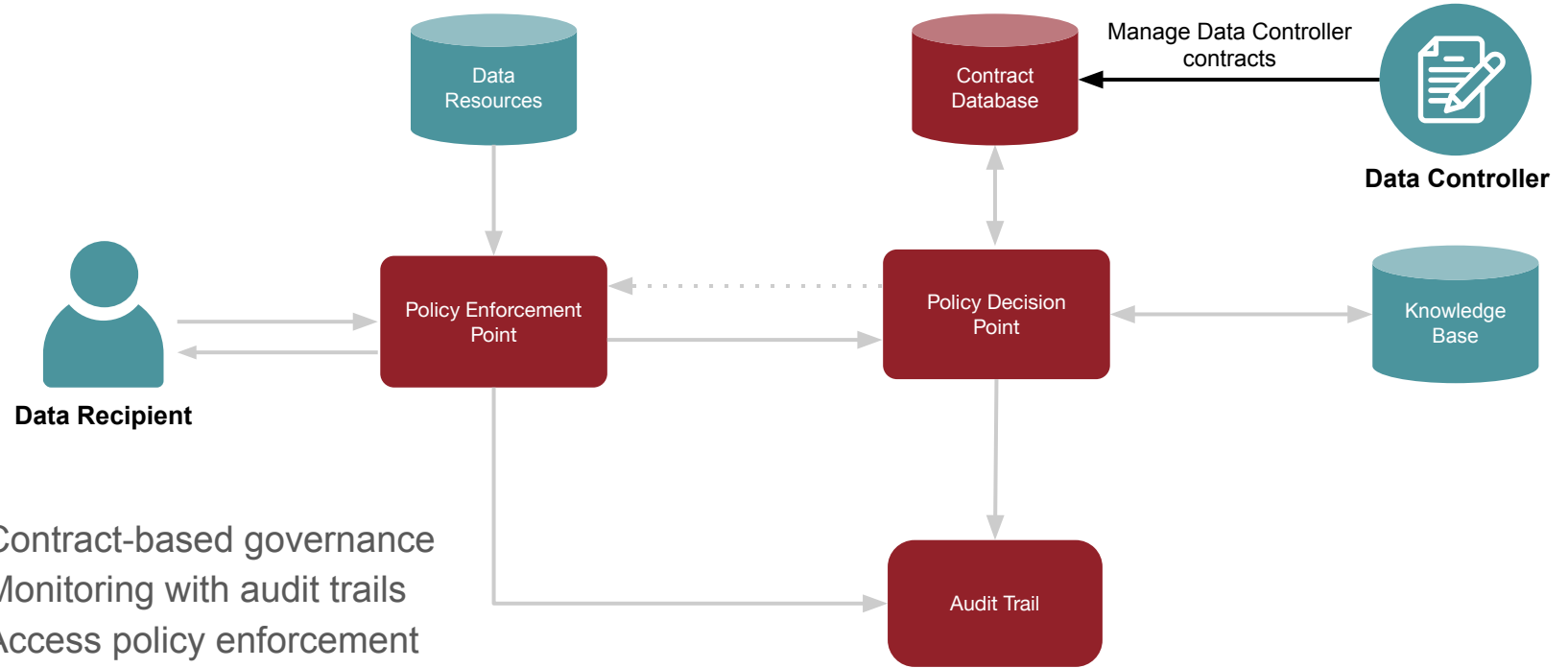


Privacy-Centric Data Governance



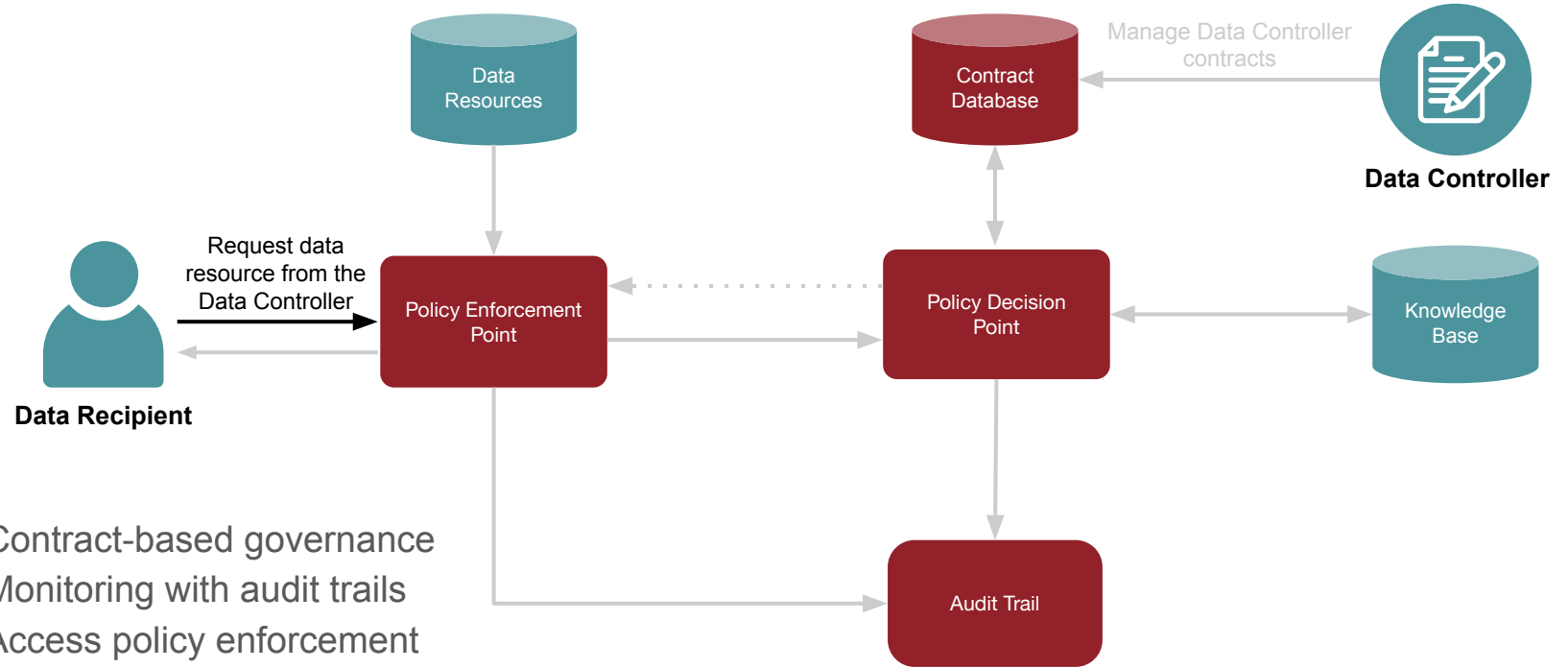
- Contract-based governance
- Monitoring with audit trails
- Access policy enforcement

Privacy-Centric Data Governance



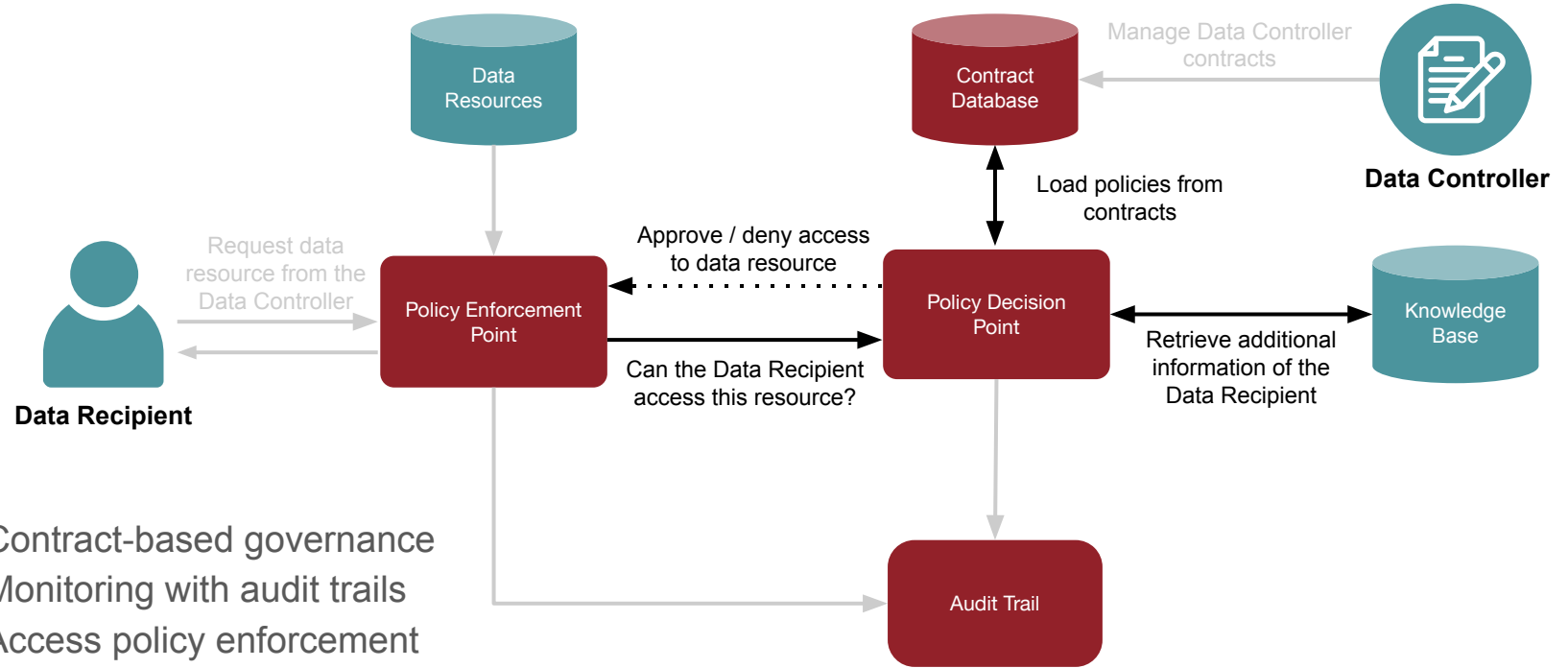
- Contract-based governance
- Monitoring with audit trails
- Access policy enforcement

Privacy-Centric Data Governance



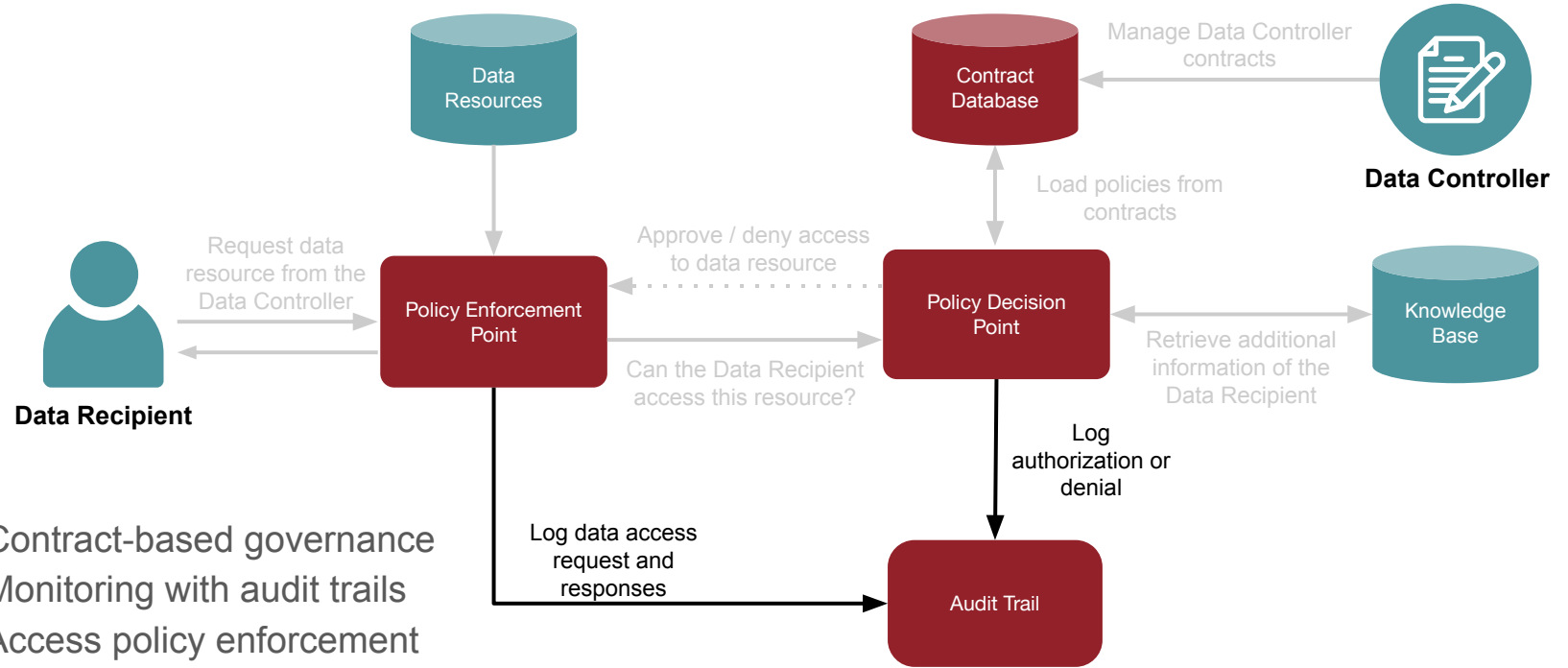
- Contract-based governance
- Monitoring with audit trails
- Access policy enforcement

Privacy-Centric Data Governance



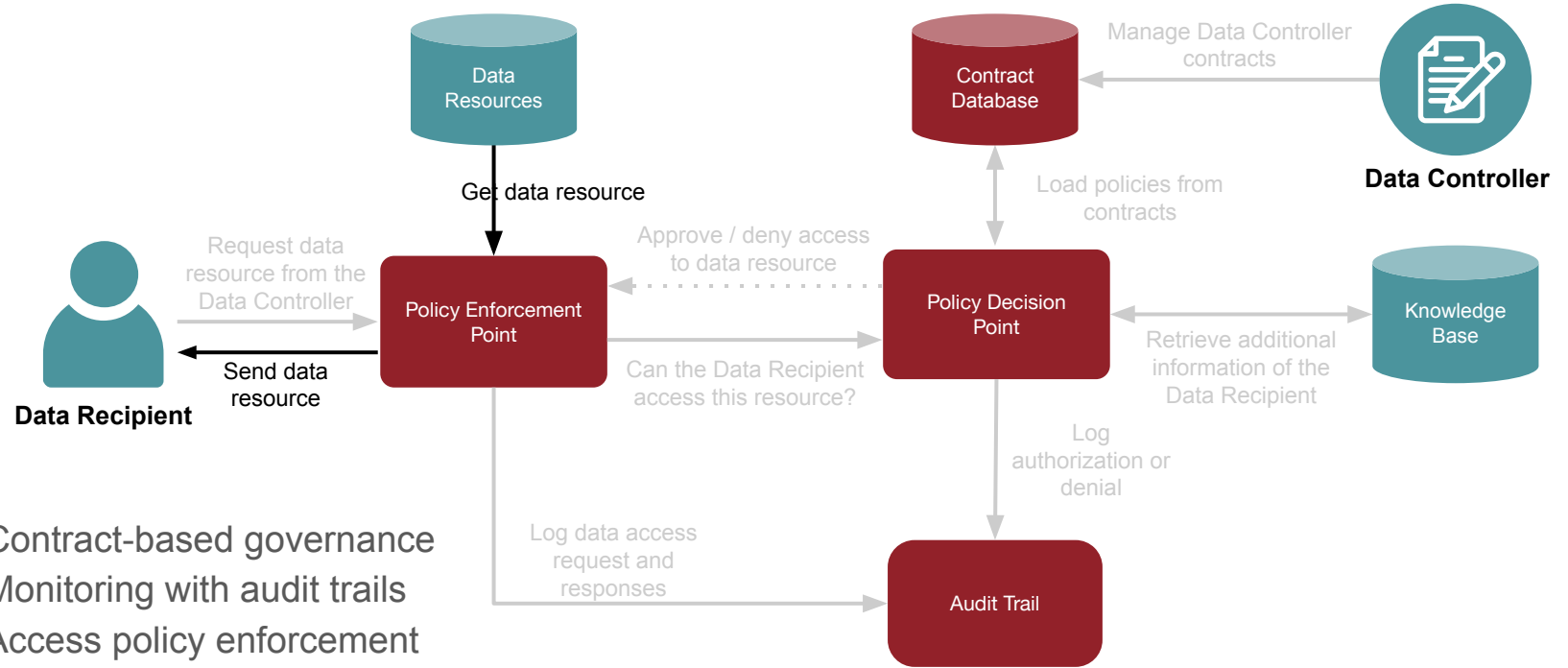
- Contract-based governance
- Monitoring with audit trails
- Access policy enforcement

Privacy-Centric Data Governance



- Contract-based governance
- Monitoring with audit trails
- Access policy enforcement

Privacy-Centric Data Governance

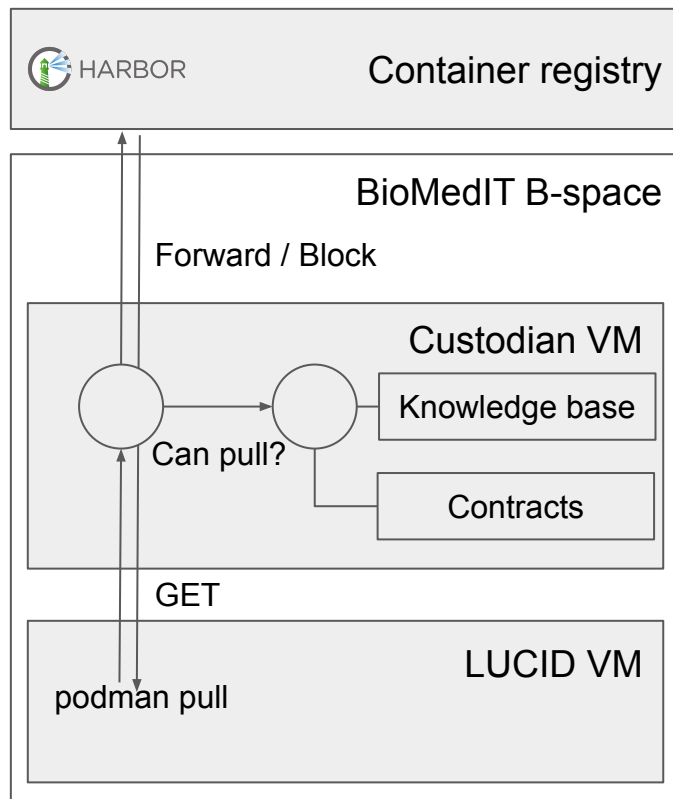


- Contract-based governance
- Monitoring with audit trails
- Access policy enforcement

Custodian for LUCID

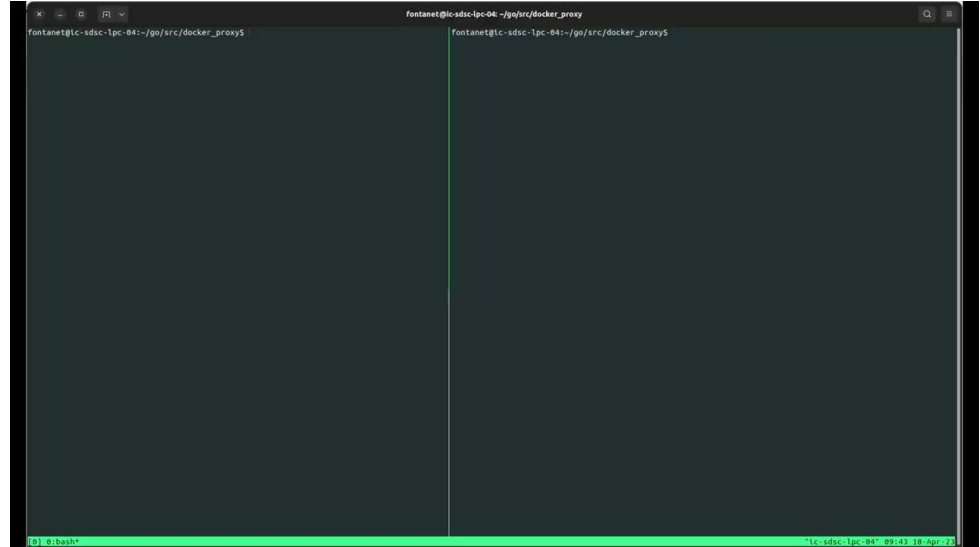
Custodian for container image governance in LUCID

- Between LUCID and Harbor
- Contracts govern image access
- Blocks disallowed requests



Setup Demo (Video)

1. User attempts to pull image
2. Access denied
3. User signs contract
4. Access granted
5. Contract revoked
6. Access denied

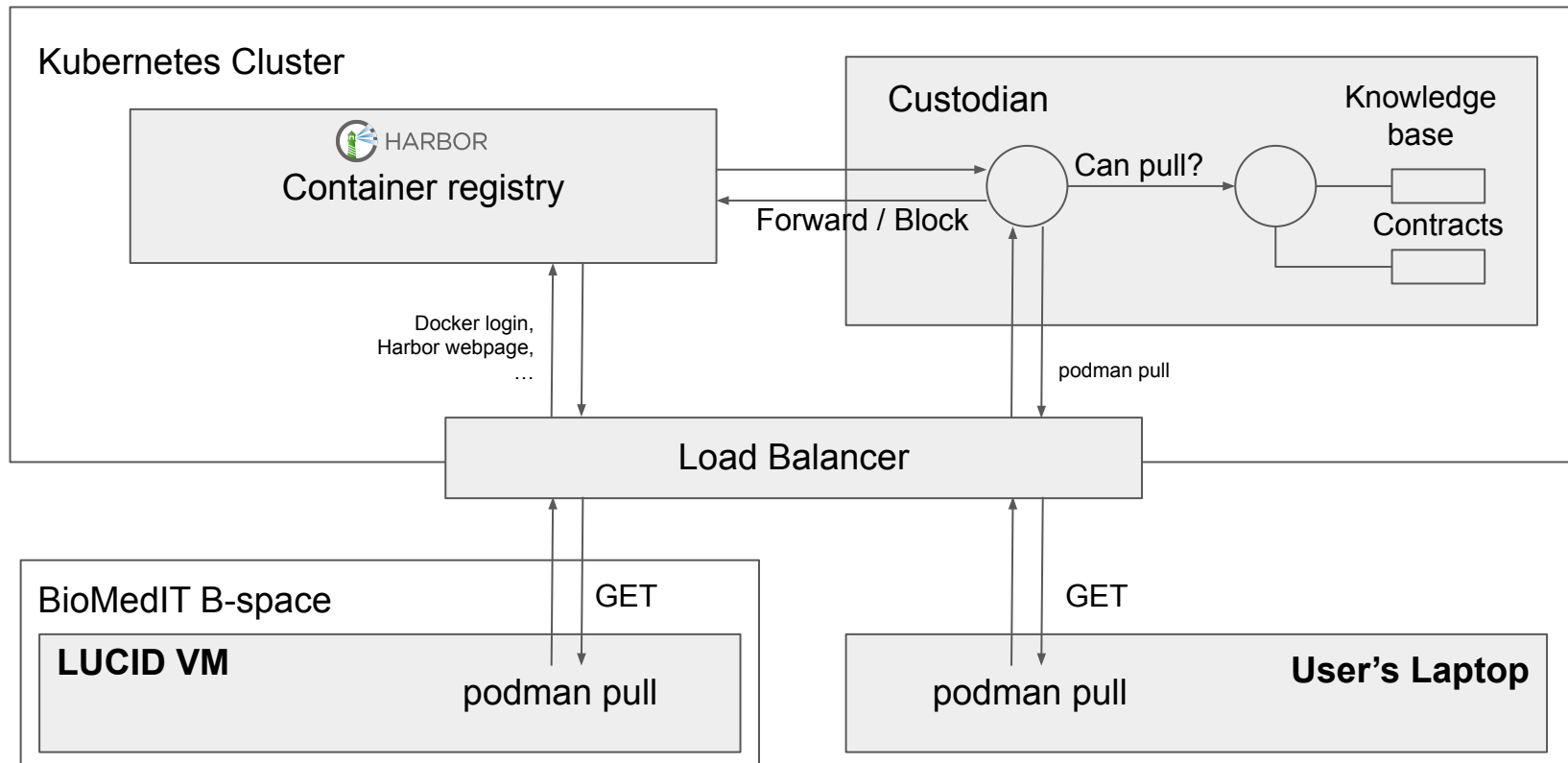


Custodian VM

LUCID VM

[Video link](#)

Scaling up governance: Your feedback is welcome



Thank You!



**Swiss Data
Custodian**



<https://datascience.ch/swiss-data-custodian-whitepaper>

LUCID Consortium



CONSORTIUM AND PARTNERS



Directors

PD Dr. Méan

Dr. Obaszinski

Internal Medicine Experts



PD Dr. Vallelian

PD Dr. Baumgartner

Prof. Aujesky

PD Dr. Strinemann

Prof. Bassetti

Prof. Meier



IT/Data Science Experts

Prof. Lovis

Dr. Raisaro

Dr. Steljes

Prof. Leichte

Dr. Riba-Grognuz

PPI and Experts Partners



Dr. Despraz

Dr. Rueter

Prof. Chioléro

Prof. Eicher

NAME & LUCID CONSORTIUM



LUCID Consortium



CONSORTIUM AND PARTNERS



Dr. Guffi

Project
Management



M. Martin



M. Bayrem Kaabachi



Dr. Ehram

PROMS/Data
Science/Semantic



Dr. Matthey-Doret



Dr. Milosavljevic

SDSC-EPFL:
Data Management



Dr. Riba



M. Fontanet



Dr. Ossey

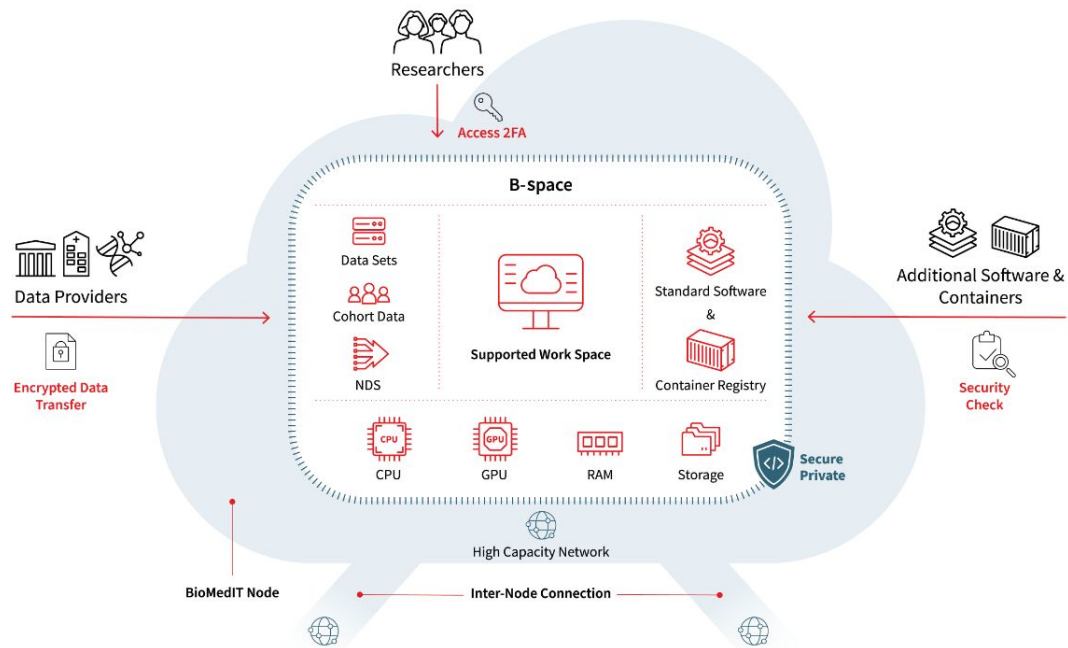
SDSC: ORDES
Security & Privacy
experts



Additional slides

Computational environment

- LUCID uses the BioMedIT infrastructure
- Workflows executed in a “B-space”
- A.k.a. Virtual Private Cloud



Custodian Brings Secure and Flexible Access Governance

- **Fine-grained access control:** Enforce specific, detailed, and context-driven access policies to protect data resources.
- **Flexible governance layer:** Complement existing systems with Custodian's digital contract-based governance layer.
- **Unified policy enforcement & compliance:** Simplify policy enforcement and ensure compliance with regulations through a unified interface.

Custodian helps ensure GDPR compliance: *Articles 5(1), 6(1), 9, 25, 28, 30, 32*

