

How to build a confidential cloud?

A platform for next generation medical research

Florent Dufour

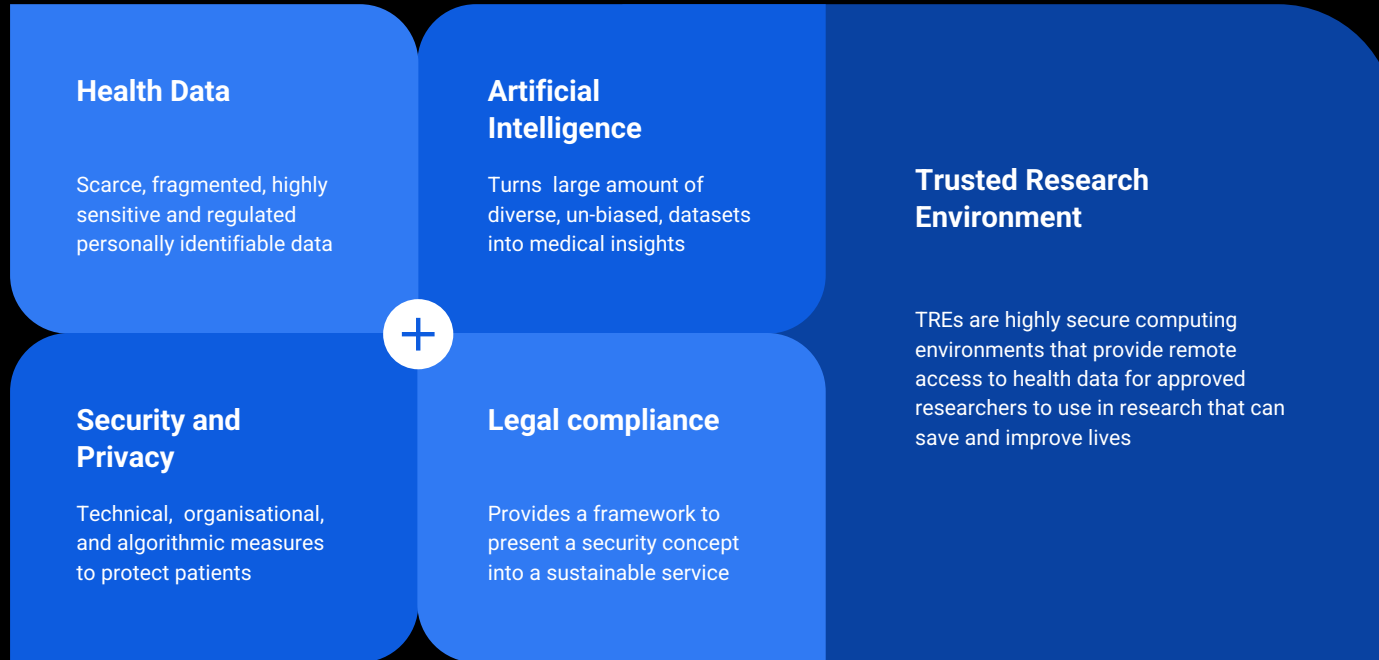
Leibniz Supercomputing Centre
Technical University of Munich

Jan Peschke

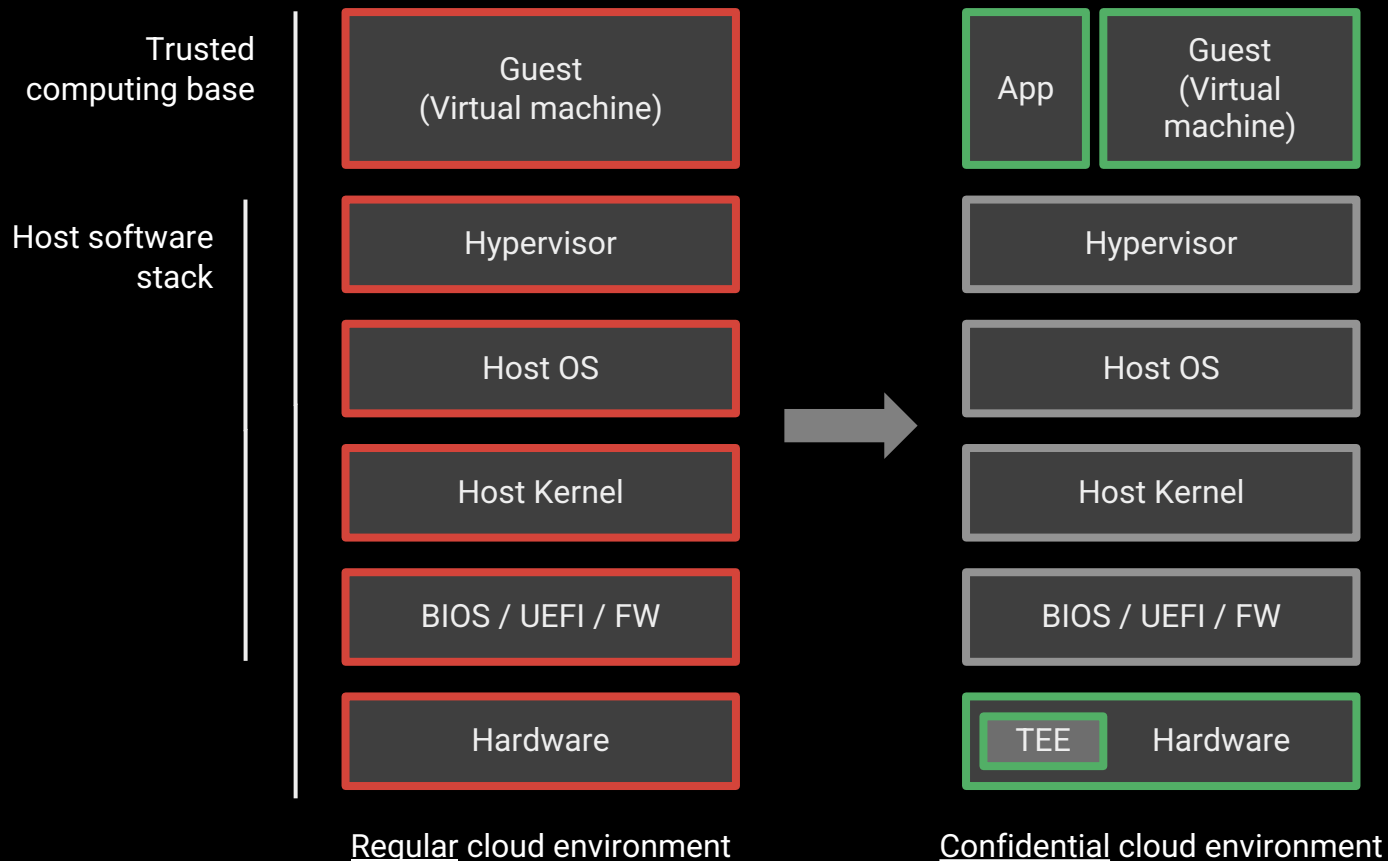
Quobyte GmbH

Context and rationale

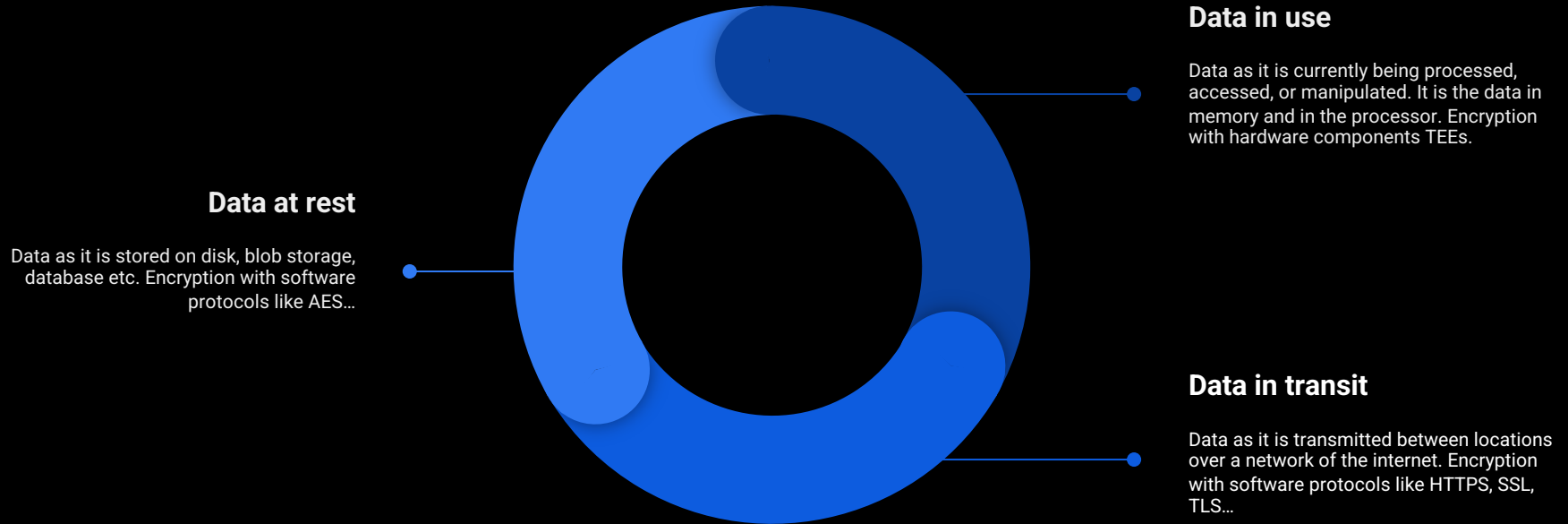
The situation: we need trust



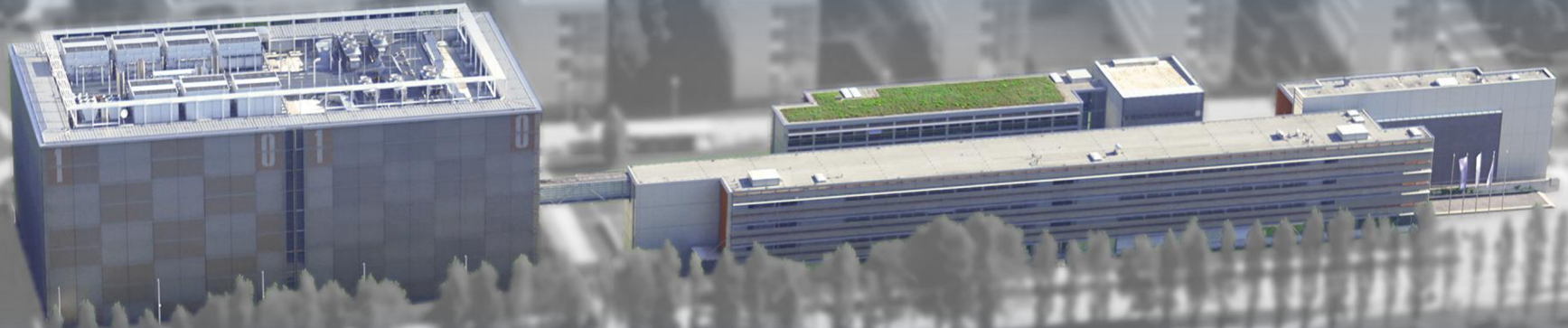
The problem: where does the trust come from?



Confidential computing: Data is end-to-end encrypted

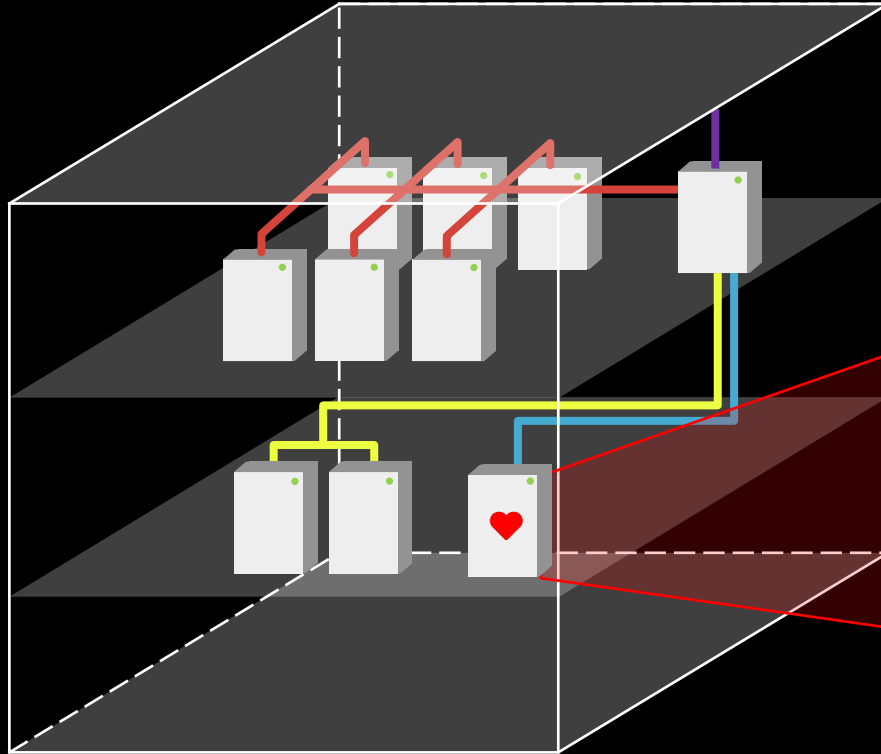


Blue print



Leibniz Supercomputing Centre
Partner for the digitalization of Science since 1962

The DigiMed Secure Cloud: A sovereign OpenStack platform



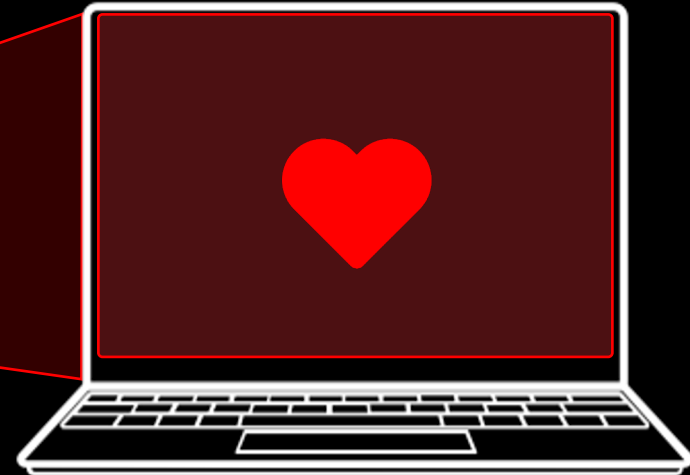
Community Infrastructure as a Service

100% Self service

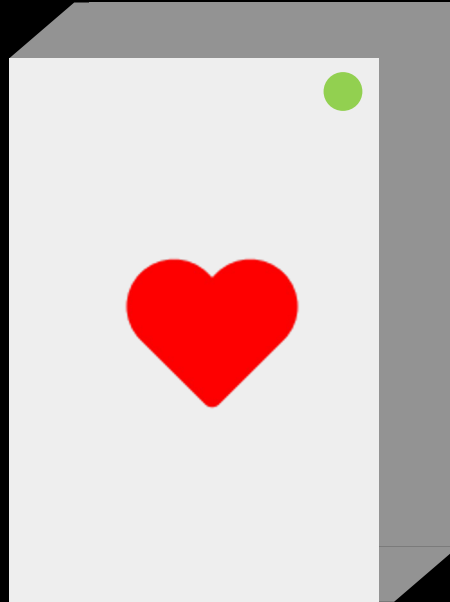
Sovereign Cloud Stack infrastructure platform

Fully encrypted, no code modification required

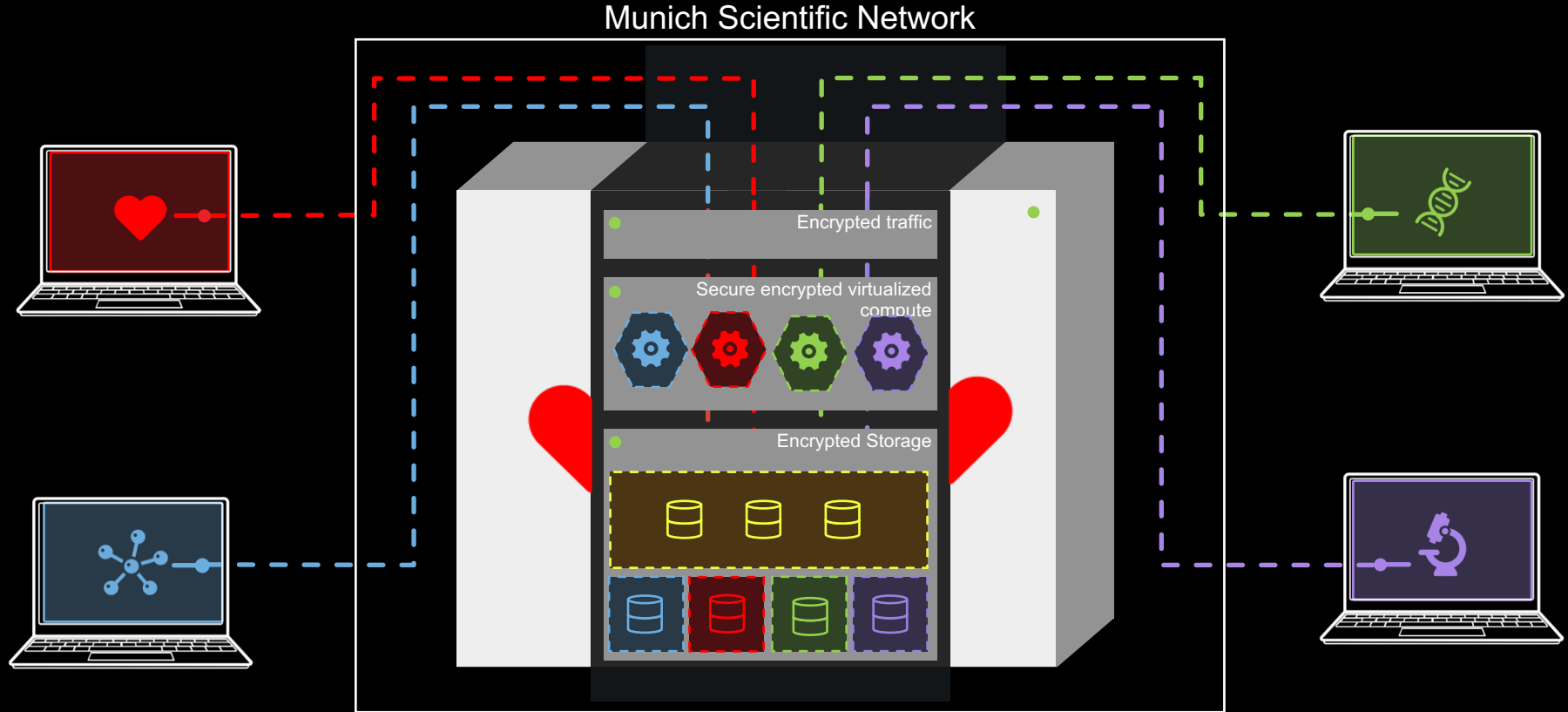
Not even cloud admins can get unauthorized access or tamper with data



The DigiMed Secure Cloud: What's inside the box?



The DigiMed Secure Cloud: What's inside the box?



Data is encrypted in all states: at rest, in flight, in use.
Data access is controlled.

The DigiMed Secure Cloud: six design principles

> 150
documents

Zero-trust

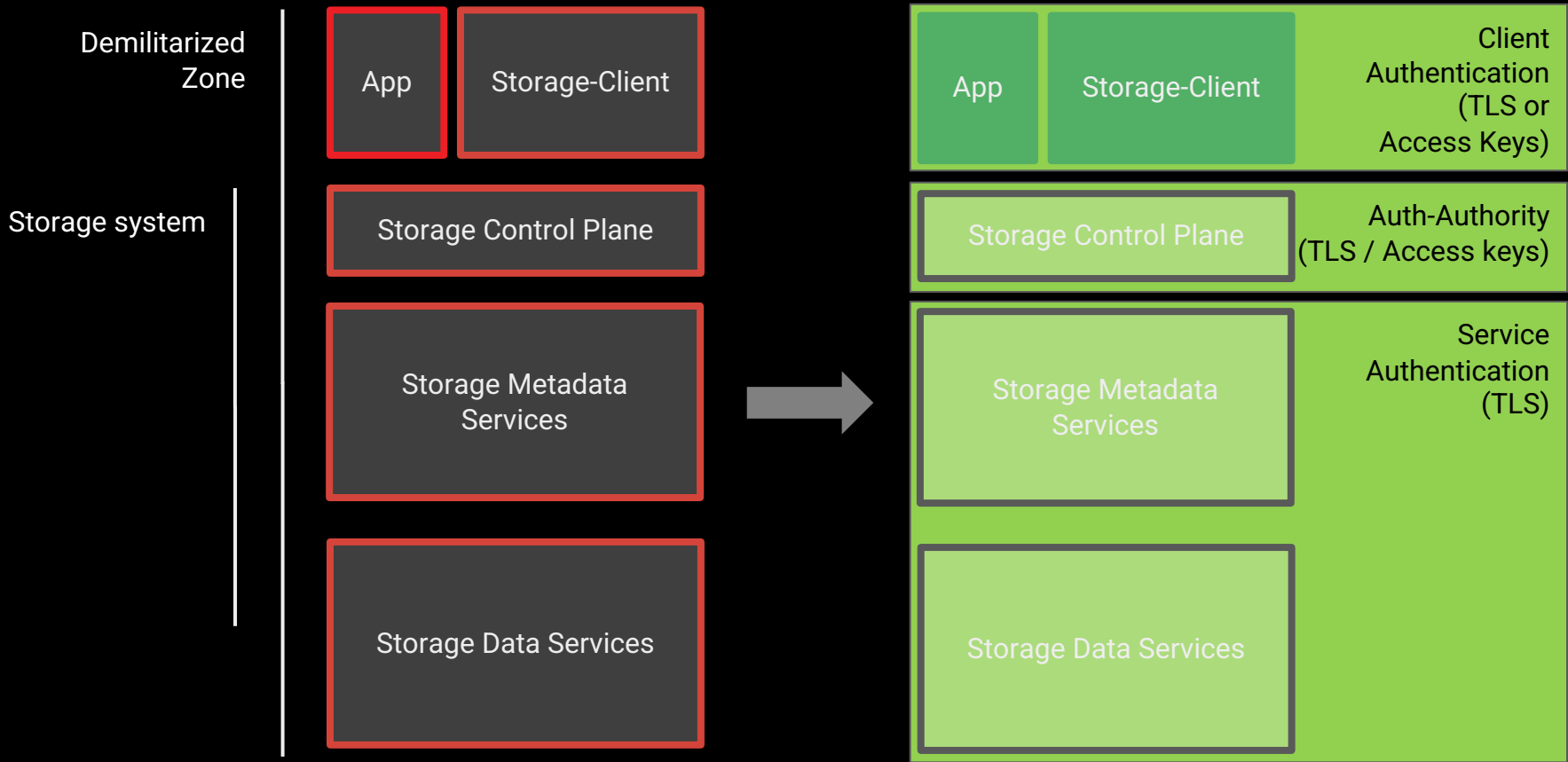
End-to-end
data encryption

Access control and
identity management

Data anonymization
and pseudonymization

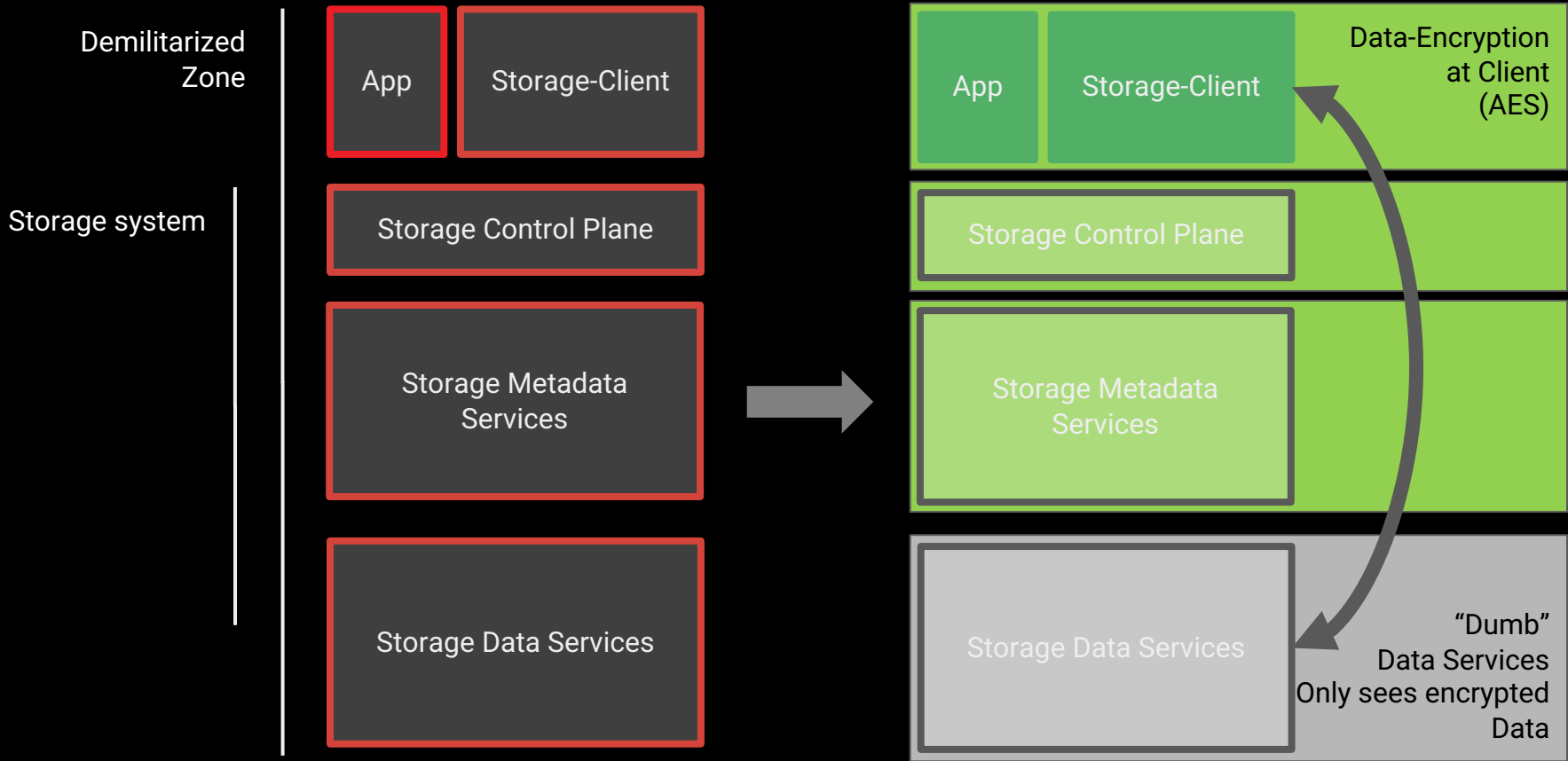
Continuous monitoring
and user training

Compliance and
regulatory frameworks



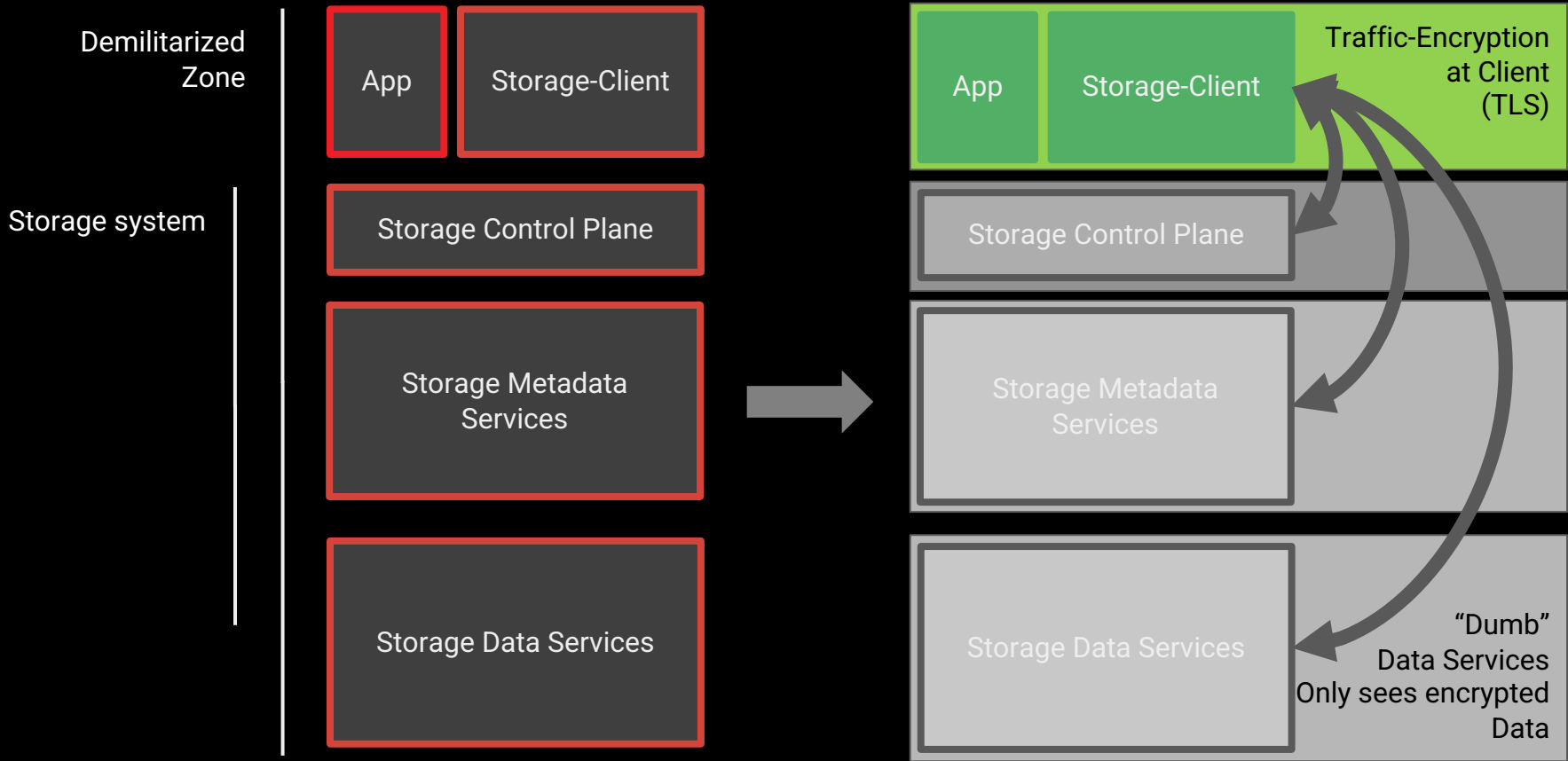
Demilitarized storage: Each party is trusted.

Confidential storage environment: Trust needs to be granted



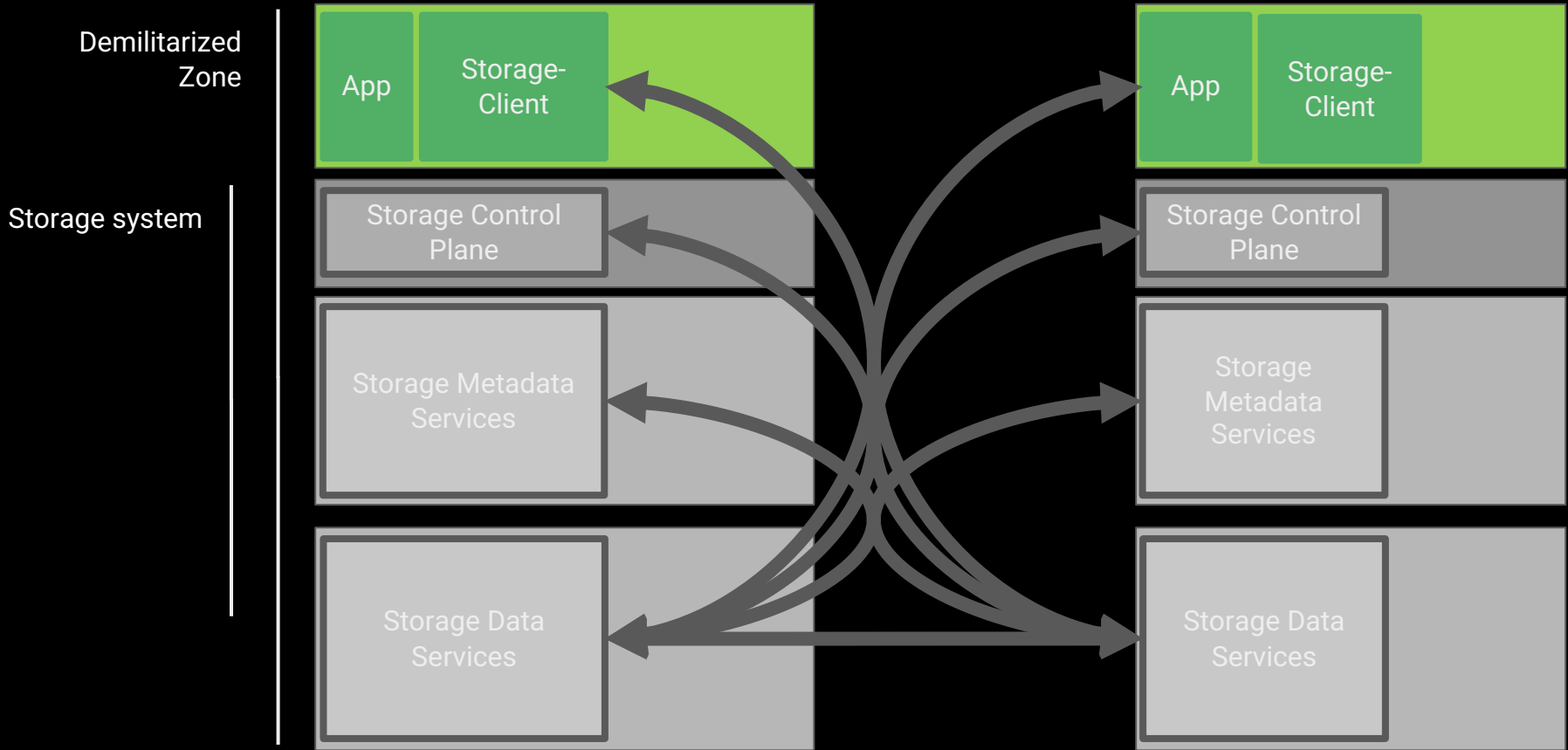
Demilitarized storage: Each party is trusted.

Confidential storage environment: Trust needs to be granted



Demilitarized storage: Each party is trusted.

Confidential storage environment: Trust needs to be granted



There is not "the storage system", but a bunch of distributed computers

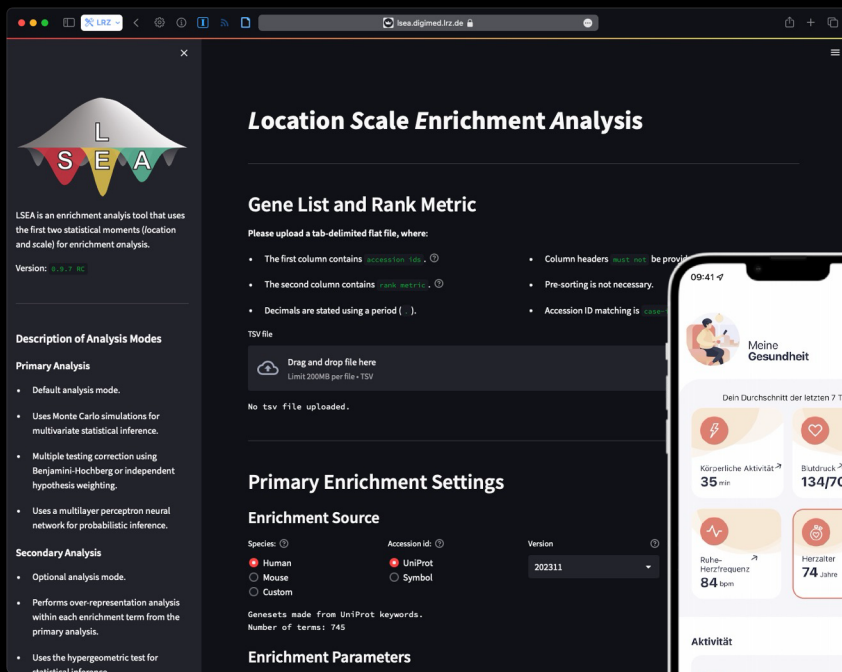
How to achieve it?

1. Block any unauthenticated access
Trusted Networks: "NONE"
2. Transport-Security as default
3. Grant access between storage nodes
TLS Certificates
4. Grant access to clients
TLS Certificates
Access Keys

X.509 Certificates & Access Keys

- X.509 Certificates: Ideal for untrusted networks/hosts. Certificates are verified locally. Restrictions can be assigned and modified in real-time: Tenant access, Operations limits (user/group), Volume access, Read-only access, Root squash.
- Access Keys: Granular user session authentication (like S3 credentials). Clients access only assigned tenants. Enforces IO mapping to user's uid/gid, crucial for containerized environments. Used by Quobyte's CSI plugin.

The DigiMed Secure Cloud: Use case examples



Location Scale Enrichment Analysis

Gene List and Rank Metric

Please upload a tab-delimited flat file, where:

- The first column contains **accession_id**.
- The second column contains **rank_metric**.
- Column headers must not be provided.
- Pre-sorting is not necessary.
- Accession ID matching is **case-insensitive**.

TSV file

Drag and drop file here
Limit: 200MB per file • TSV

No tsv file uploaded.

Primary Enrichment Settings

Enrichment Source

Species: ☐ Human ☐ Mouse ☐ Custom
Accession id: ☐ UniProt ☐ Symbol
Version: 202311

Genesets made from UniProt keywords.
Number of terms: 745

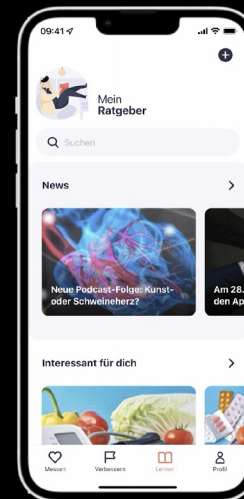
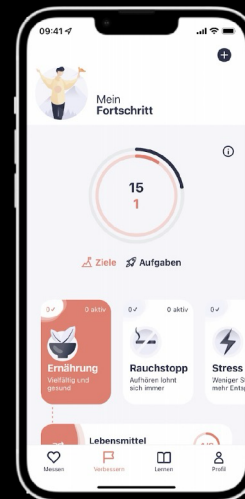
Enrichment Parameters

Primary Analysis

- Default analysis mode.
- Uses Monte Carlo simulations for multivariate statistical inference.
- Multiple testing correction using Benjamini-Hochberg or independent hypothesis weighting.
- Uses a multilayer perceptron neural network for probabilistic inference.

Secondary Analysis

- Optional analysis mode.
- Performs over-representation analysis within each enrichment term from the primary analysis.
- Uses the hypergeometric test for statistical inference.



You need **MORE** people than you think

Establish a clear **escalation** process

Don't make it just **secure**

Manage *expectations*

👉 You can do it!

Any question?

Acknowledgments

LRZ

Prof. Dieter Kranzlmüller

Dr. Roland Pichler

Dr. Nicolay J. Hammer

Dr. Peter Zinterhof

Dr. Naweiluo Zhou

Vinzent Bode

Valentin Pfeil

Yassine Sfar

DigiMed

Dr. Jens Wiehler

Dr. Tim-Henrik Bruun

Anja Kroke

All partners

Quobyte team

