

How to build a confidential cloud?

A platform for next generation medical research

Florent Dufour

Leibniz Supercomputing Centre
Technical University of Munich

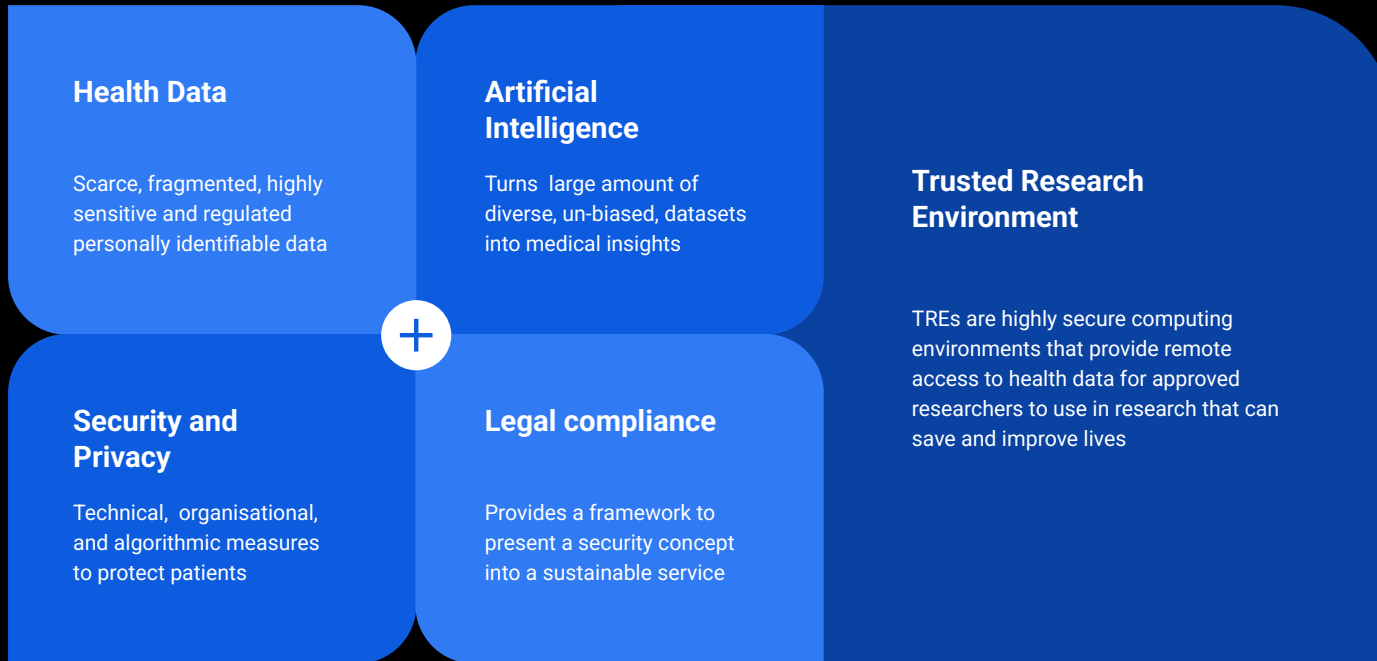
Jan Peschke

Quobyte GmbH

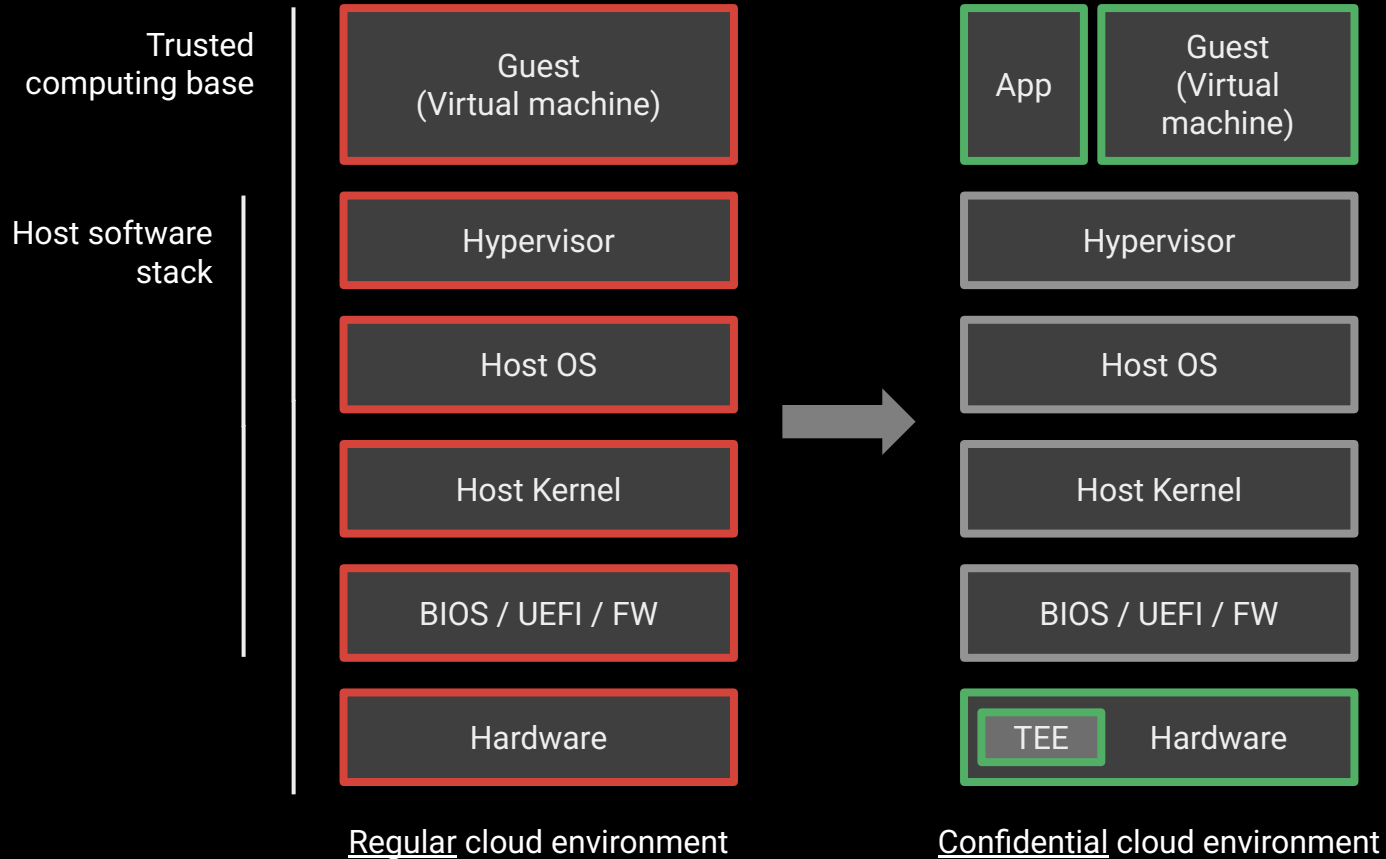
Context and rationale

Confidential Computing

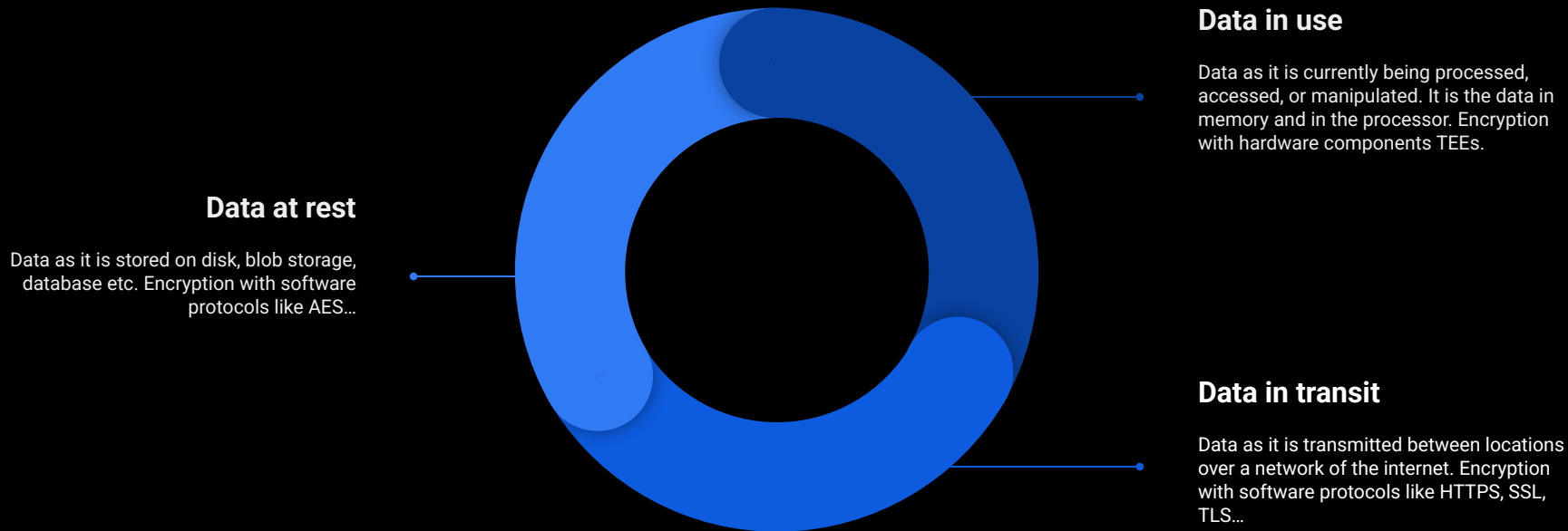
The situation: we need trust



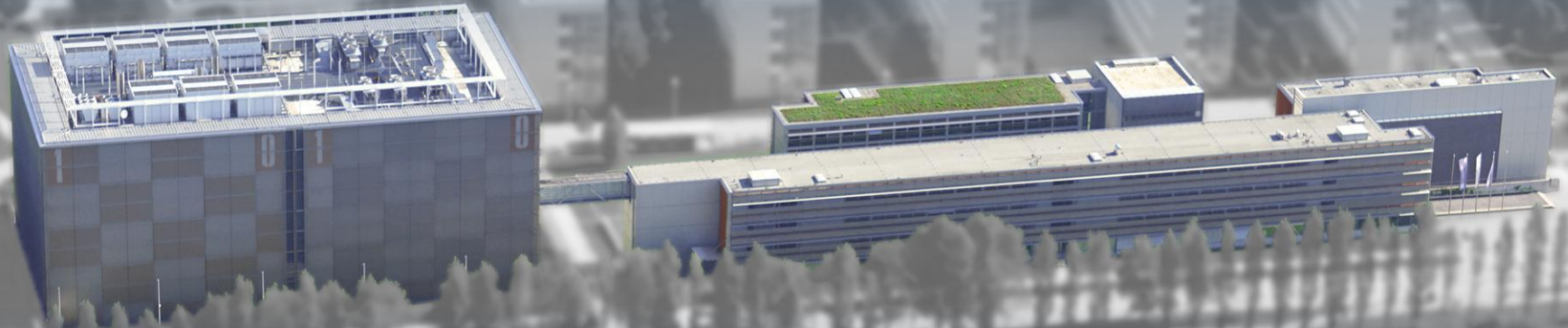
The problem: where does the trust come from?



Confidential computing: Data is end-to-end encrypted

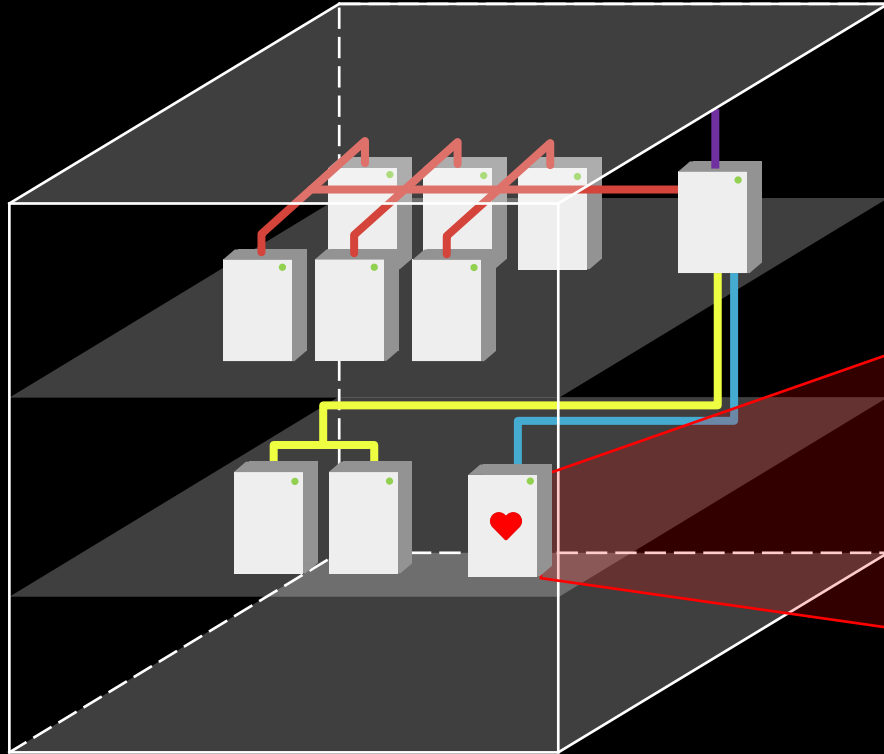


Blue print

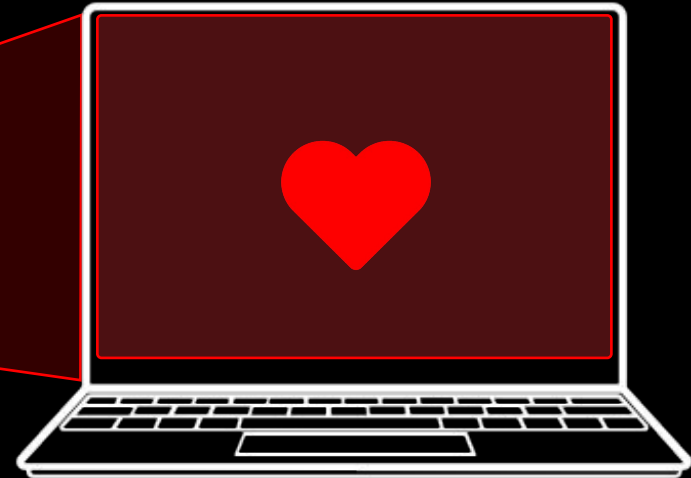


Leibniz Supercomputing Centre
Partner for the digitalization of Science since 1962

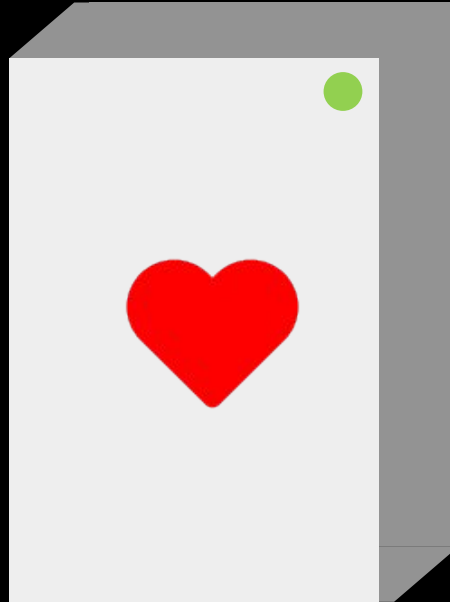
The DigiMed Secure Cloud: A sovereign OpenStack platform



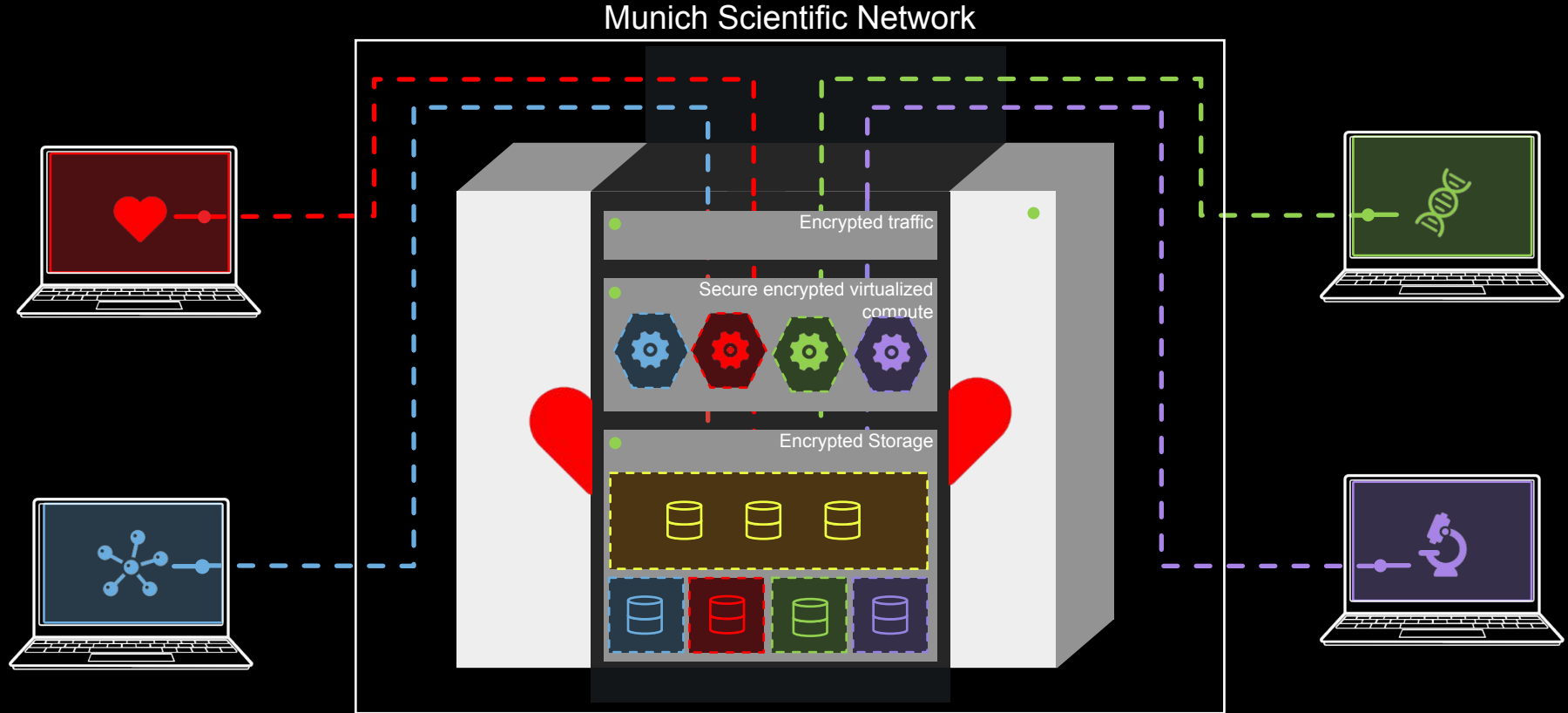
- ✓ Community Infrastructure as a Service
- ✓ 100% Self service
- ✓ Sovereign Cloud Stack infrastructure platform
- ✓ Fully encrypted, no code modification required
- ✓ Not even LRZ admins can get unauthorized access or tamper with data



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

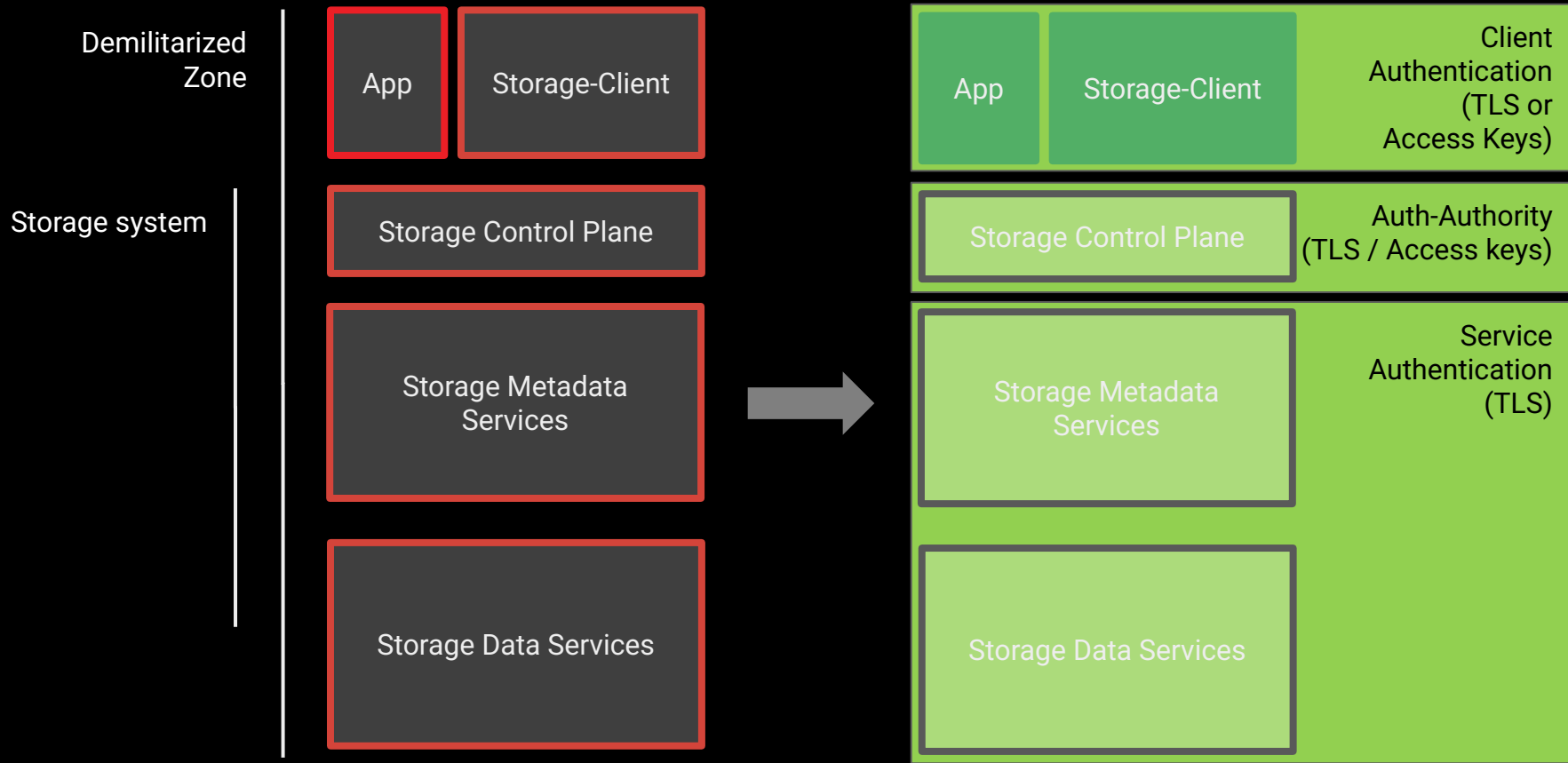
End-to-end
data encryption

Access control and
identity management

Data anonymization
and pseudonymization

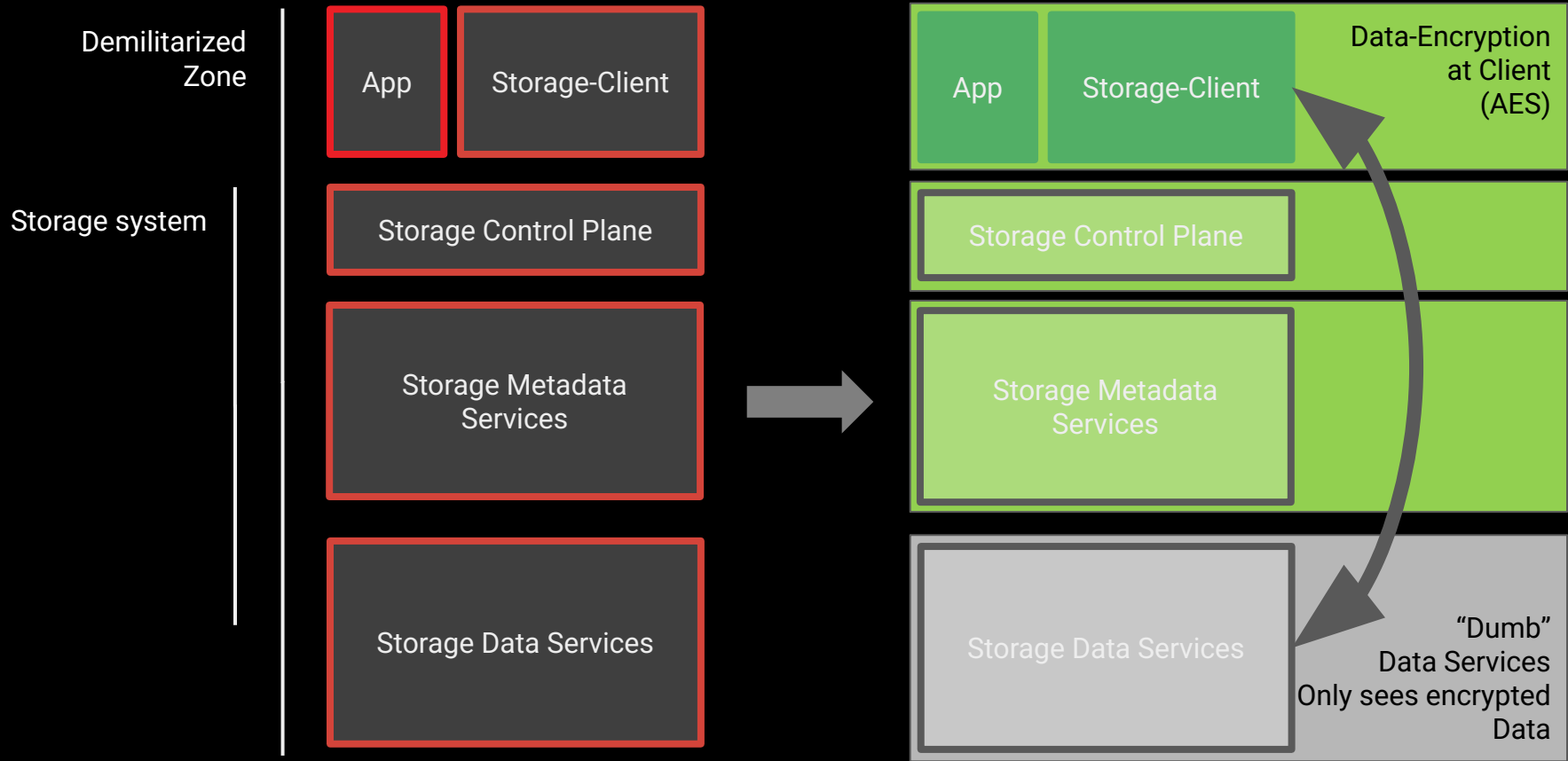
Compliance and
regulatory frameworks

Continuous monitoring
and user training



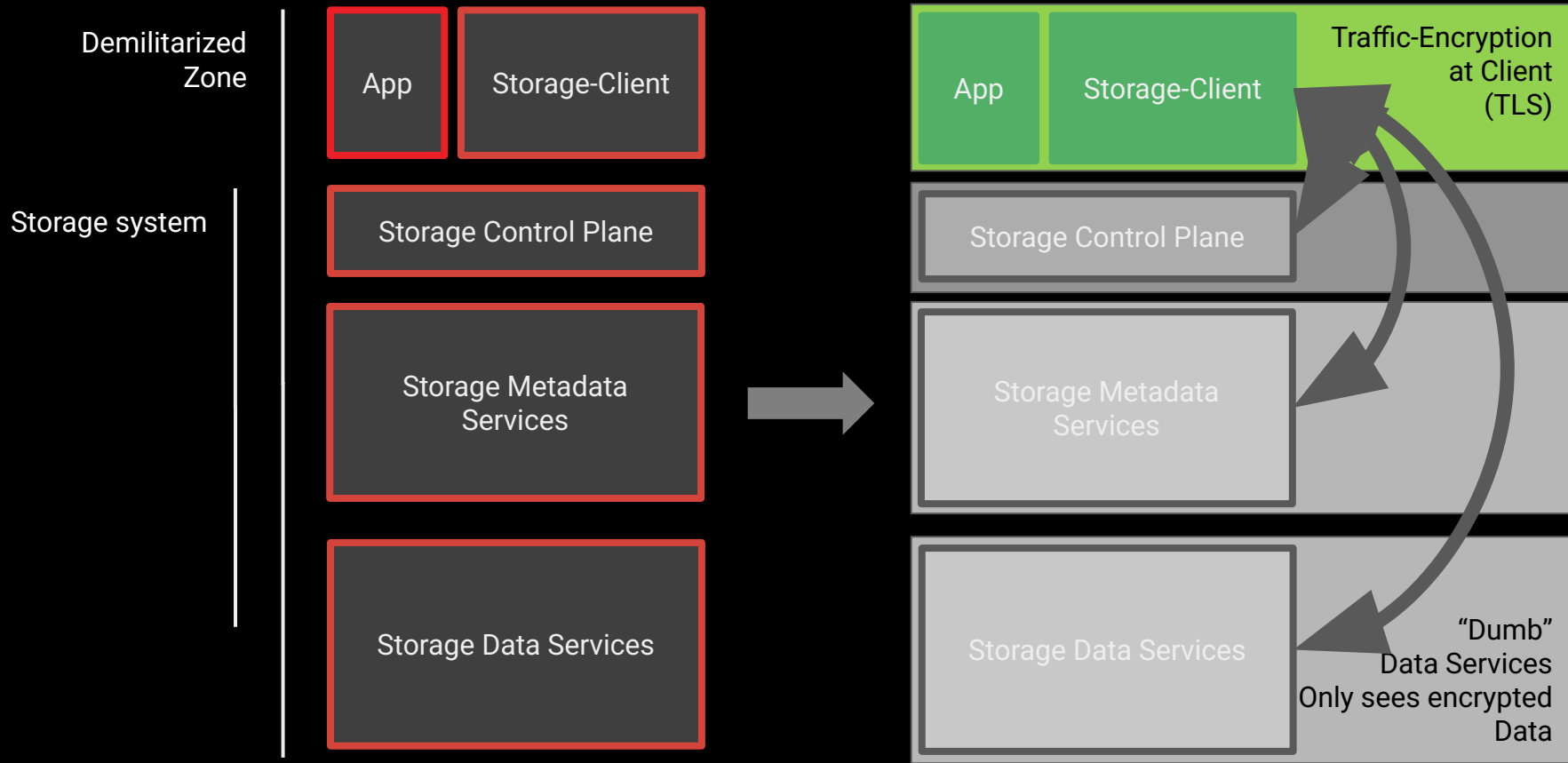
Demilitarized storage: Each party is trusted.

Confidential storage environment: Trust needs to be granted



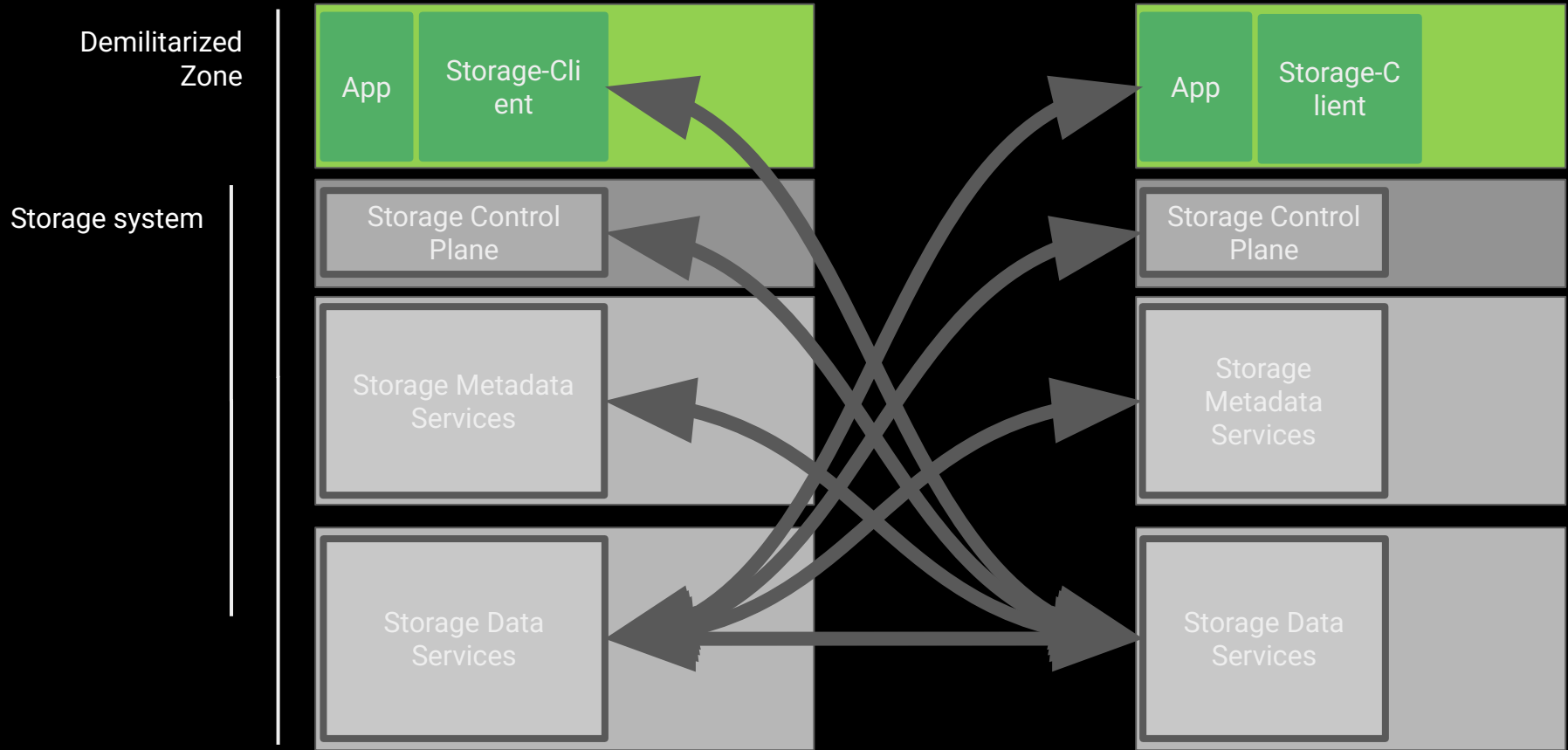
Demilitarized storage: Each party is trusted.

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)
- 3. Grant access to clients

File System Authentication & Access Control

- Services and clients require authentication to join the cluster and access volumes.
- Quobyte supports machine-level authentication.
- Enhanced security with per-mount and per-user authentication for shared client environments.
- Key Mechanisms: IP Filters, X.509 Certificates, Access Keys.

IP Filters & Trusted Networks

- Trusted Networks: Traditional approach, assumes secure network. Allows access to all tenants and volumes, overrides IP filters and Access Keys (but not X.509). Defined by IPv4/IPv6 networks.
- Tenant IP Networks: Define client-to-tenant relationships based on IP. Clients can belong to multiple tenants.
- Volume IP Networks: Control volume visibility. Enables read-only access for specific networks. Can be combined with policy rules for granular control (e.g., root permissions).

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.

End-to-End Encryption & TLS

- End-to-End Data Encryption: Data encrypted at the source, decrypted only at the destination. Offers highest level of protection. Hardware-accelerated AES-XTS encryption with negligible performance impact. Protects data even from administrators and drive theft. Per-file keys distributed via TLS.
- In-transit Encryption (TLS): Encrypted communication between clients and servers, and between servers. Can be enabled for specific networks. High throughput due to distributed load across Quobyte servers, ideal for cluster synchronization and transfers. Can be used in conjunction with end-to-end encryption.

Discussion and outlook

The DigiMed Secure Cloud: Use case examples

Location Scale Enrichment Analysis

LSEA is an enrichment analysis tool that uses the first two statistical moments (location and scale) for enrichment analysis.

Version: 0.9.7 RC

Description of Analysis Modes

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.

Gene List and Rank Metric

Please upload a tab-delimited flat file, where:

- The first column contains **accession** (40).
- The second column contains **rank metric** (1).
- Column headers **must not** be provided.
- Pre-sorting is not necessary.
- Accession ID matching is **case**.

TSV file

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

No tsv file uploaded.

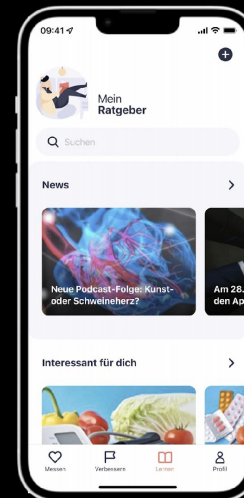
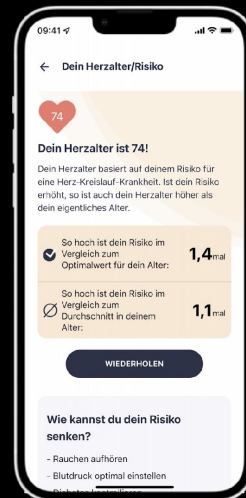
Primary Enrichment Settings

Enrichment Source

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

Genesets made from UniProt keywords.
Number of terms: 745

Enrichment Parameters



You need **MORE** people than you think

Establish a clear escalation process

Don't make it just **secure**

Manage *expectations*

👉 You can do it
Or not?

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

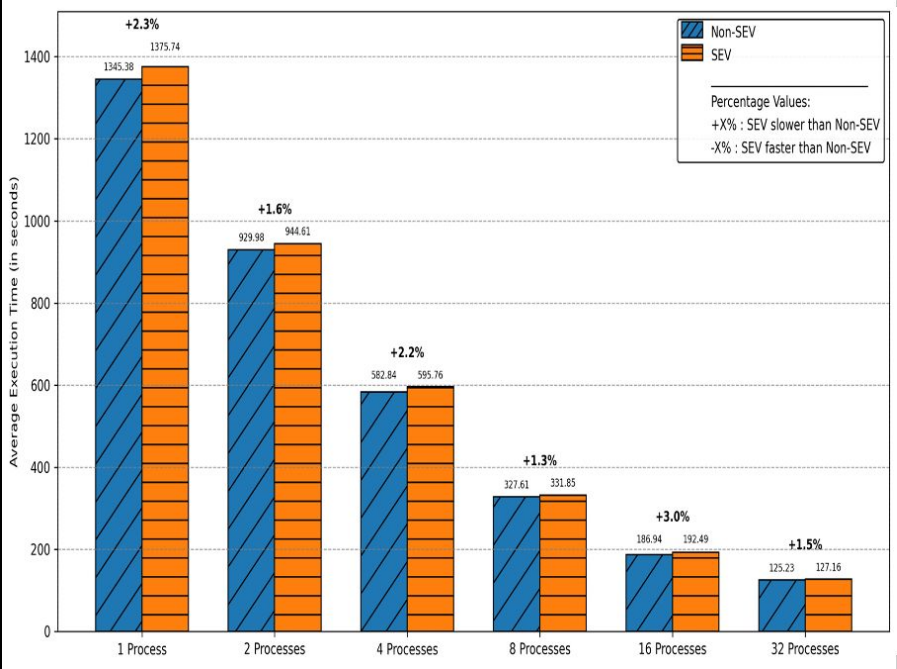
Anja Kroke

All partners

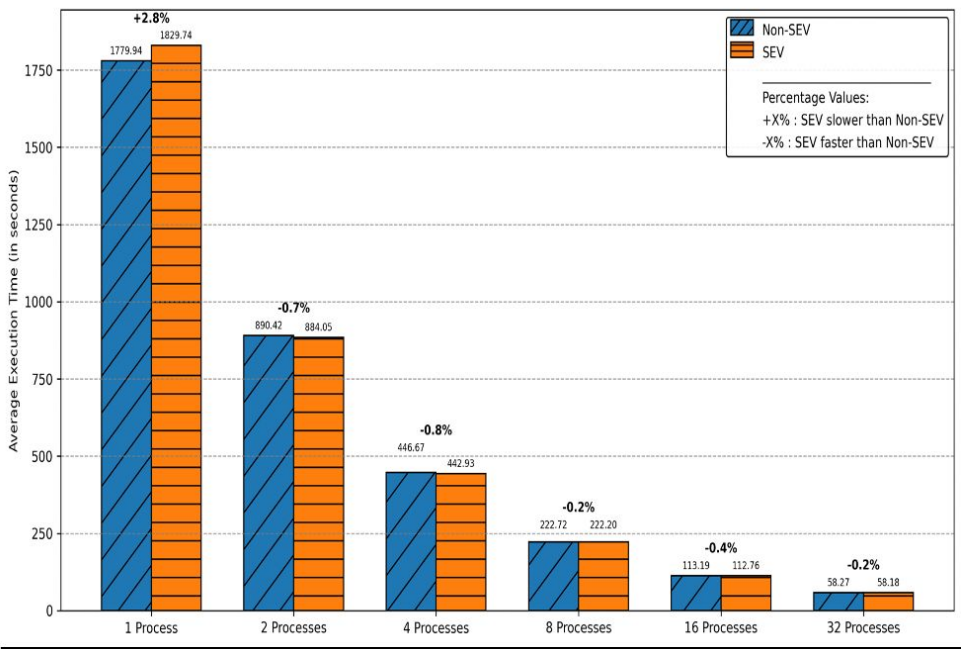
Quobyte team



Cloud Performance in Healthcare: A Benchmarking and Analysis Study of the DigiMed Secure Cloud

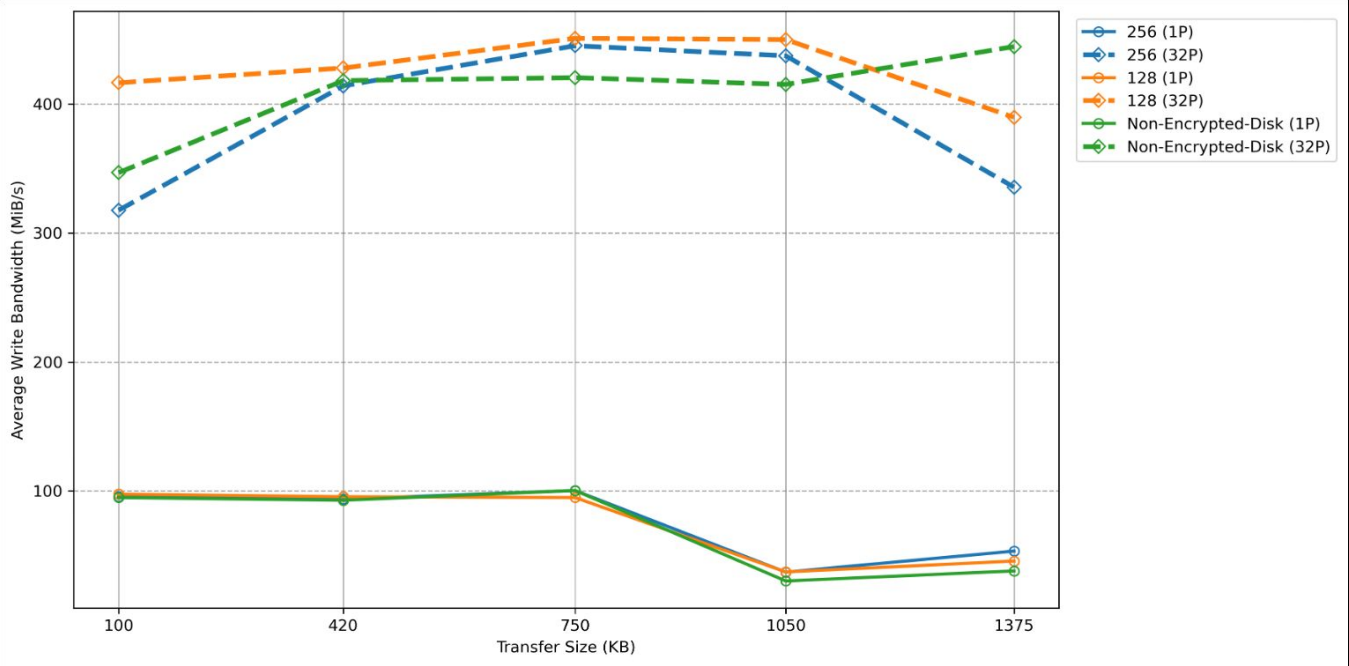


Performance for memory encryption (BPMF)



Performance for memory encryption (sysbench)

*Cloud Performance in Healthcare:
A Benchmarking and Analysis Study of the DigiMed Secure Cloud*



Performance for disk speed (write bandwidth)

- ✓ State of the art open-Source cloud platform built on top of OpenStack
 - ✓ Technical foundation of the European GAIA-X Cloud project
 - ✓ Aim to create federated cloud infrastructure
 - ✓ Ensure compliance with European data protection and security standards
 - ✓ SCS is being developed by the Open Source Business Alliance (OSB Alliance) with funding from the German Federal Ministry for Economic Affairs and Climate Action
-
- ✓ IaaS: Users can replicate what they have in the clinics
 - ✓ Community (≠ public) cloud
 - ✓ Supported by European companies and organizations



One platform — standardized, built and operated by many.



Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages



What is Sovereign Cloud Stack?

Only Open Source guarantees digital sovereignty by interoperability, transparency and independence from unlawful claims of third parties and thus from any unauthorised interference.

By using the modular SCS Software stack, cloud providers can offer state-of-the-art Infrastructure-as-a-Service and Container-as-a-Service while being fully compliant with European data protection and security standards without depending on other vendors.

SCS is using and standardizing existing and proven Open Source components such as e.g. Kubernetes and does extend them where required. Federated cloud services are enabled this way, and users can leverage distributed cloud services from several SCS operators. European companies thus have options all the way from running it themselves to using one or several service providers and thus have 100% freedom of choice avoiding lock-in effects and dependencies on providers from foreign jurisdictions.

Limitations

- OpenStack full support for AMD SEV-SNP
- OpenStack support for GPU TEE
- Accounting model

Perspective

- Scale-out (~10PB, 1200vCPUs, 5GPUs)
- Bring your own key with Hardware Security Module
- IaaS → PaaS → SaaS
- Off-site backups