OpenInfra FOUNDATION

How to build a confidential cloud?

A platform for next generation medical research

Florent Dufour

Leibniz Supercomputing Centre
Technical University of Munich

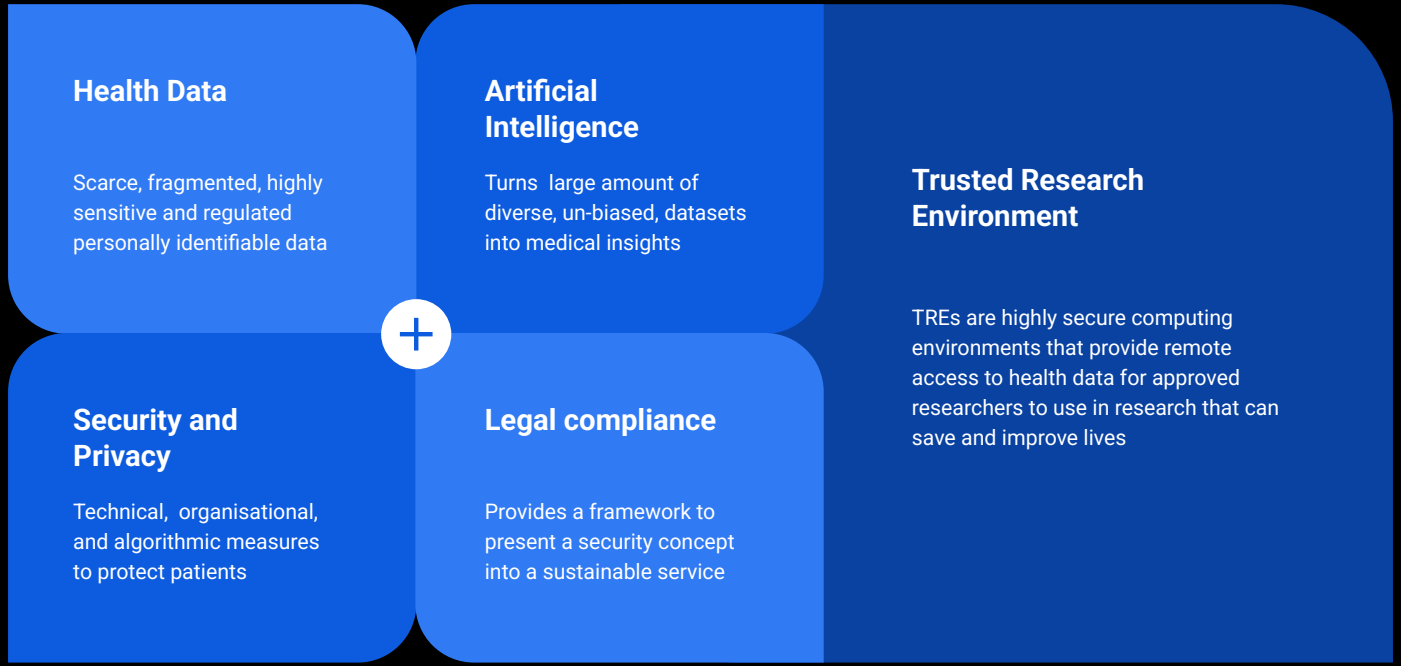
Jan Peschke

Quobyte GmbH

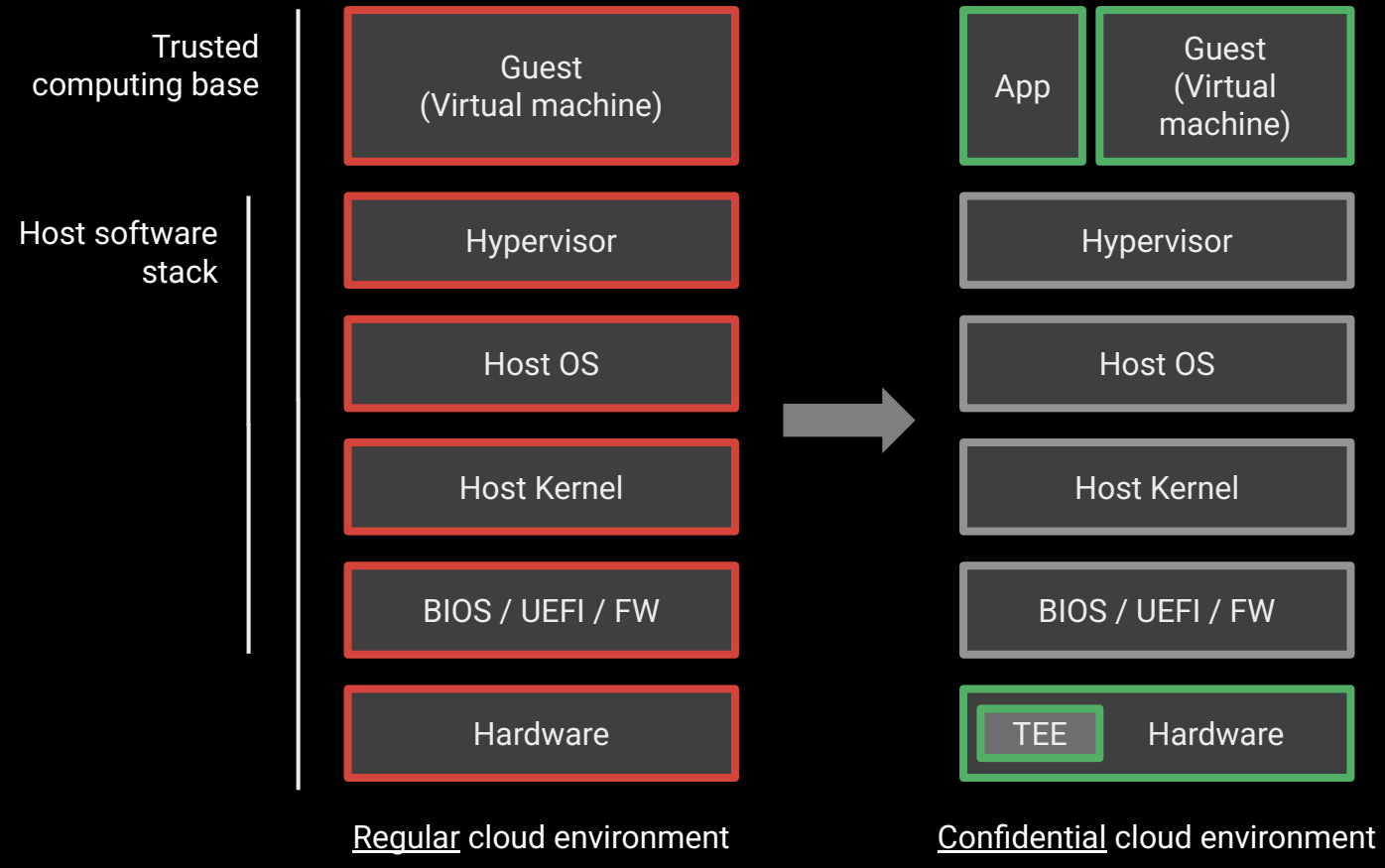
Context and rationale

Confidential Computing

The situation: we need trust



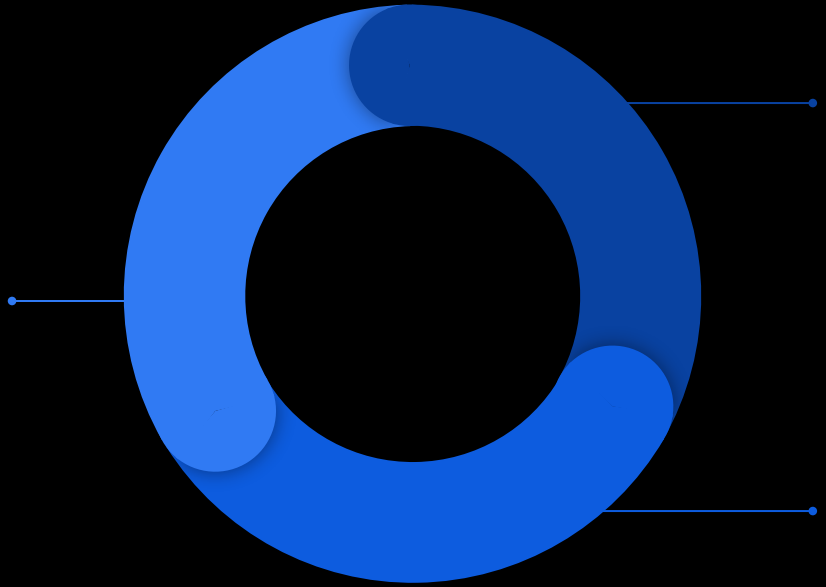
The problem: where does the trust come from?



Confidential computing: Data is end-to-end encrypted

Data at rest

Data as it is stored on disk, blob storage, database etc. Encryption with software protocols like AES...



Data in use

Data as it is currently being processed, accessed, or manipulated. It is the data in memory and in the processor. Encryption with hardware components TEEs.

Data in transit

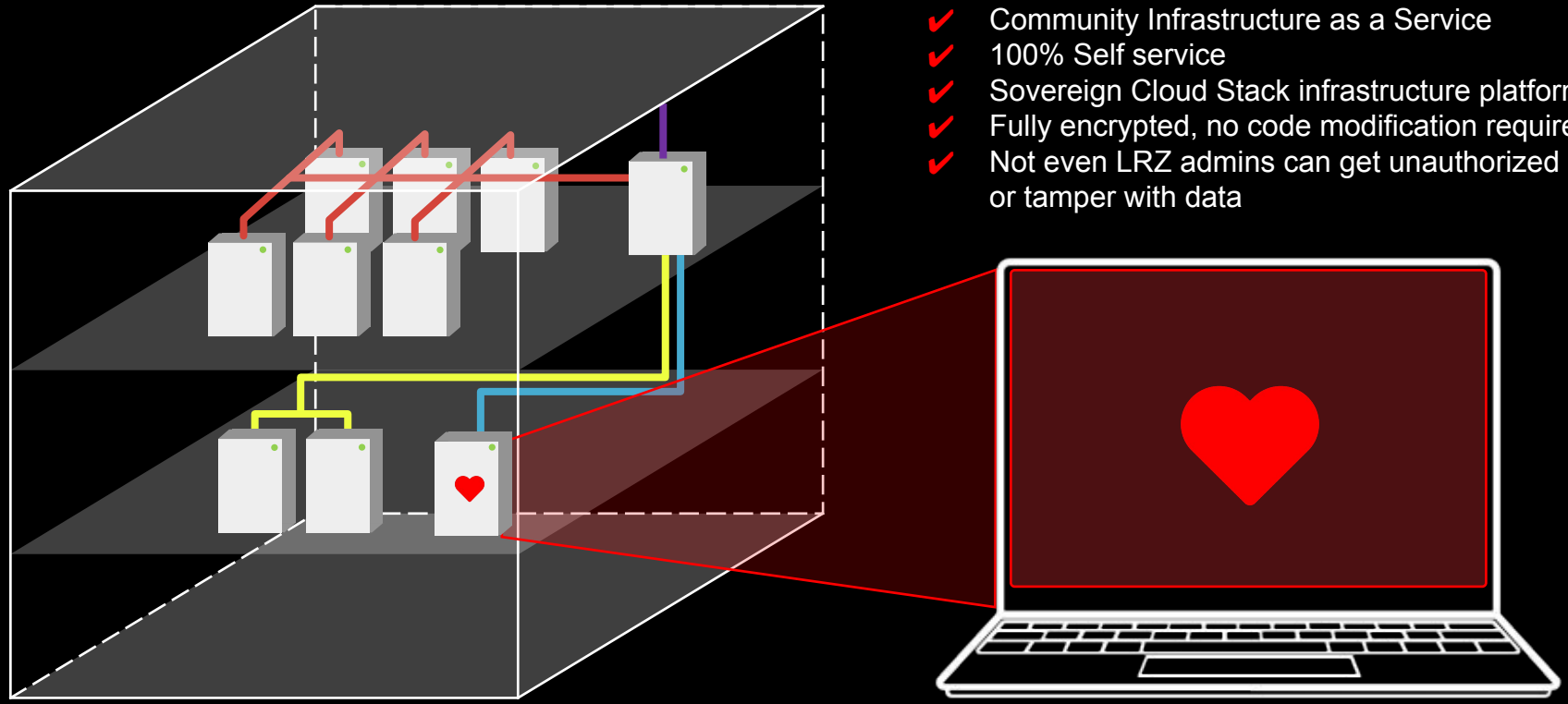
Data as it is transmitted between locations over a network of the internet. Encryption with software protocols like HTTPS, SSL, TLS...

Blue print

Leibniz Supercomputing Centre

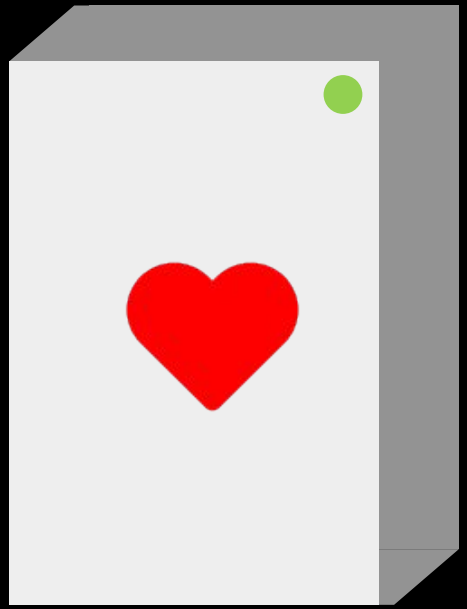
Partner for the digitalization of Science since 1962

The DigiMed Secure Cloud: A sovereign OpenStack platform

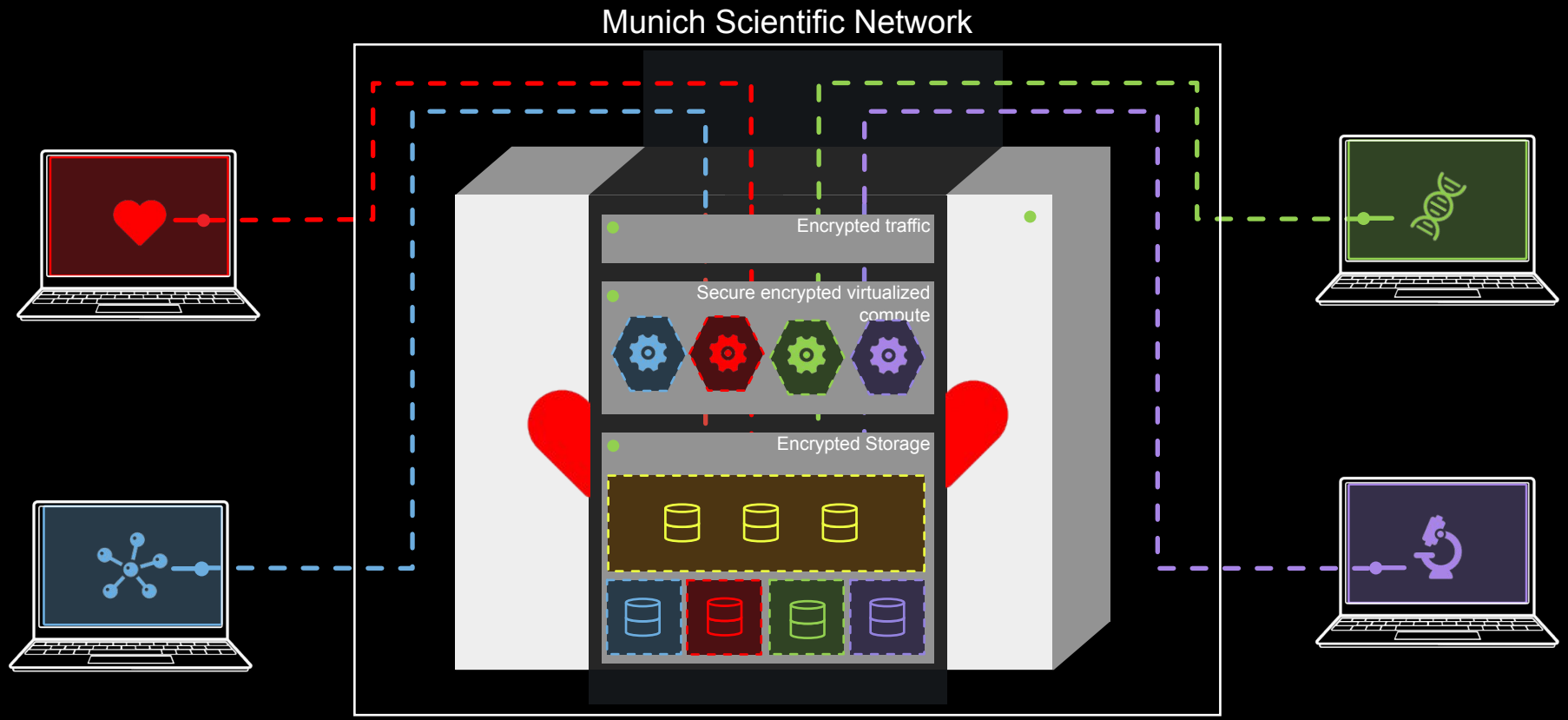


- ✔ Community Infrastructure as a Service
- ✔ 100% Self service
- ✔ Sovereign Cloud Stack infrastructure platform
- ✔ Fully encrypted, no code modification required
- ✔ Not even LRZ admins can get unauthorized access or tamper with data

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

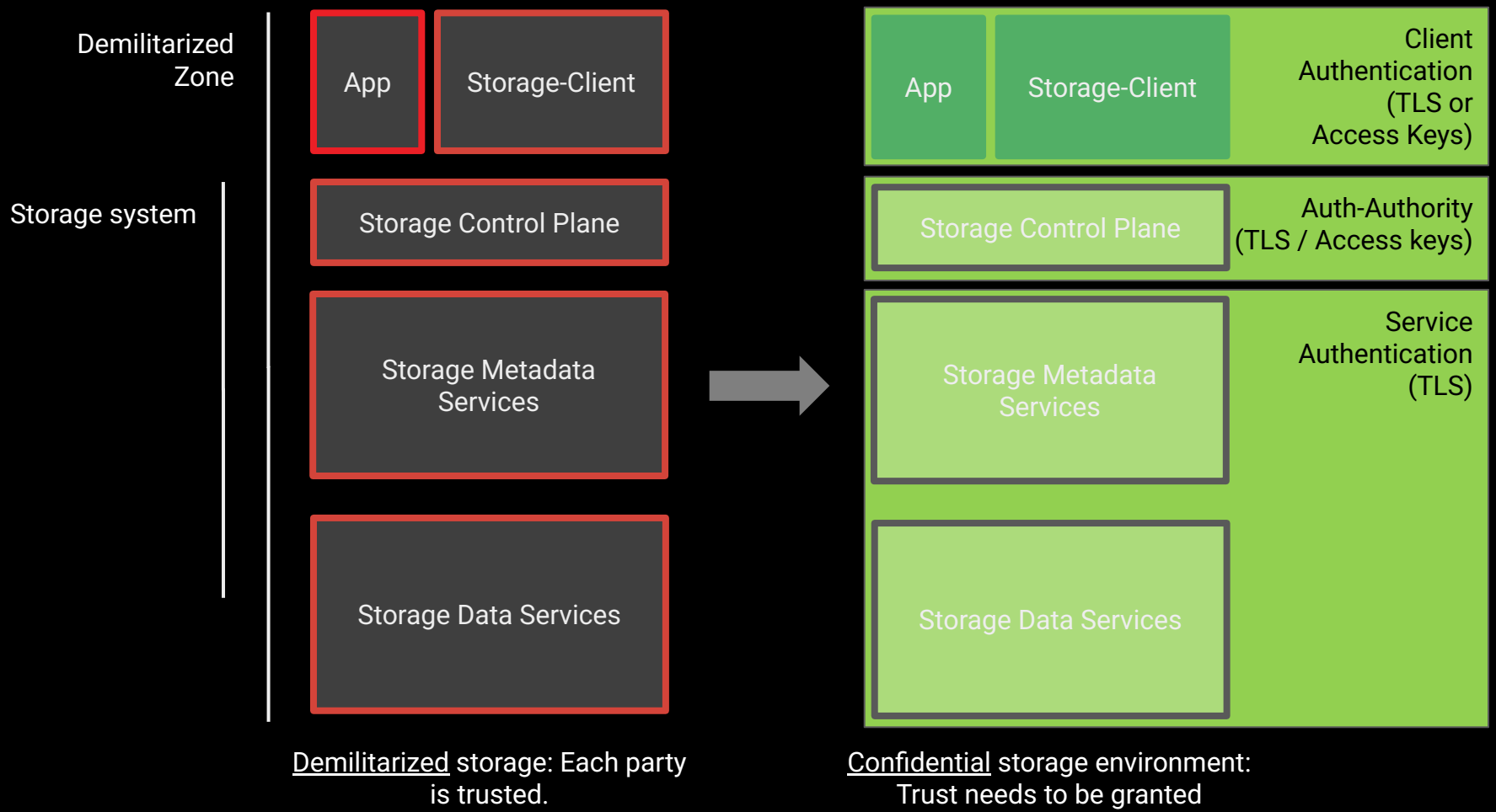
End-to-end data encryption

Access control and identity management

Data anonymization and pseudonymization

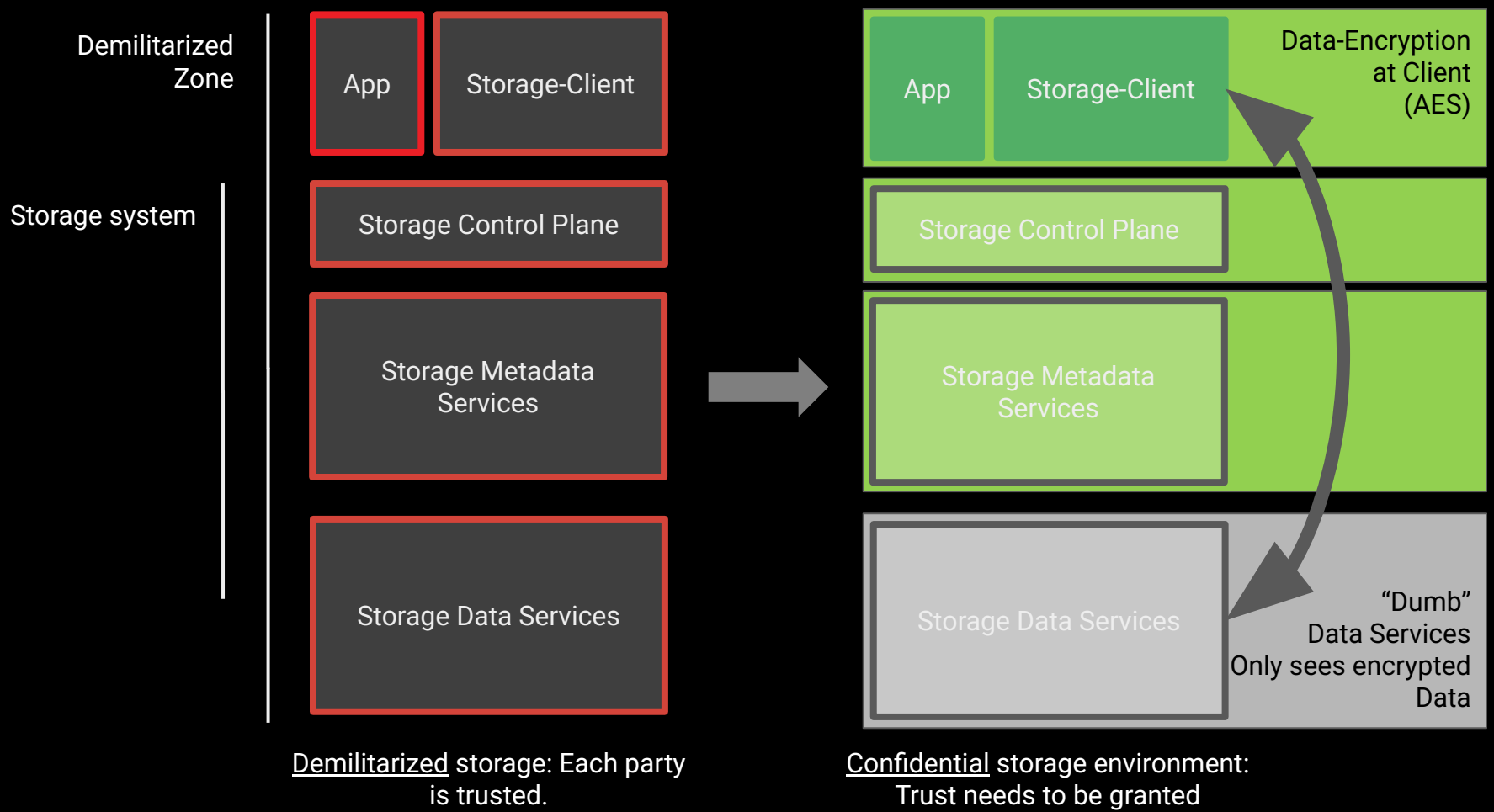
Compliance and regulatory frameworks

Continuous monitoring and user training



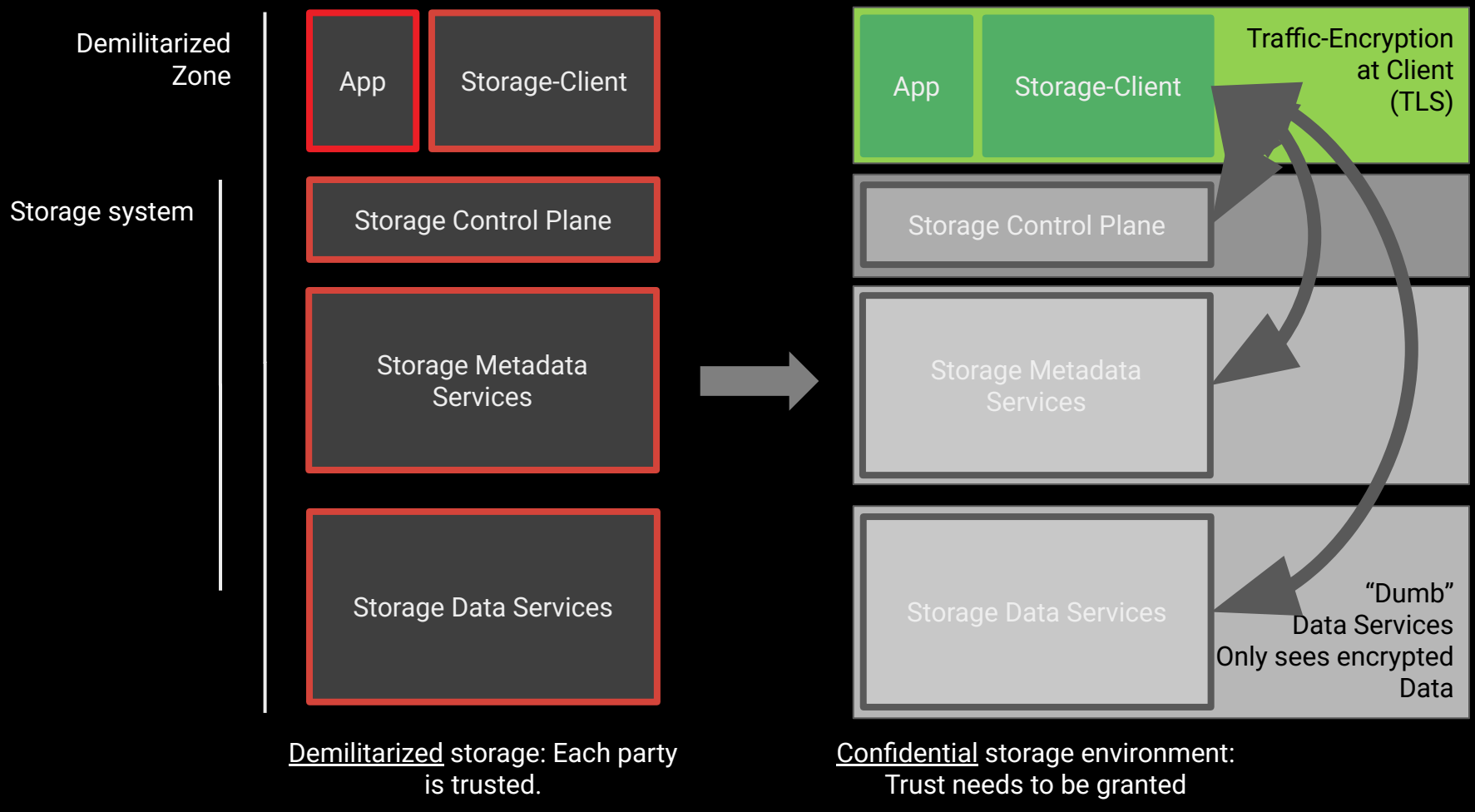
Demilitarized storage: Each party is trusted.

Confidential storage environment: Trust needs to be granted



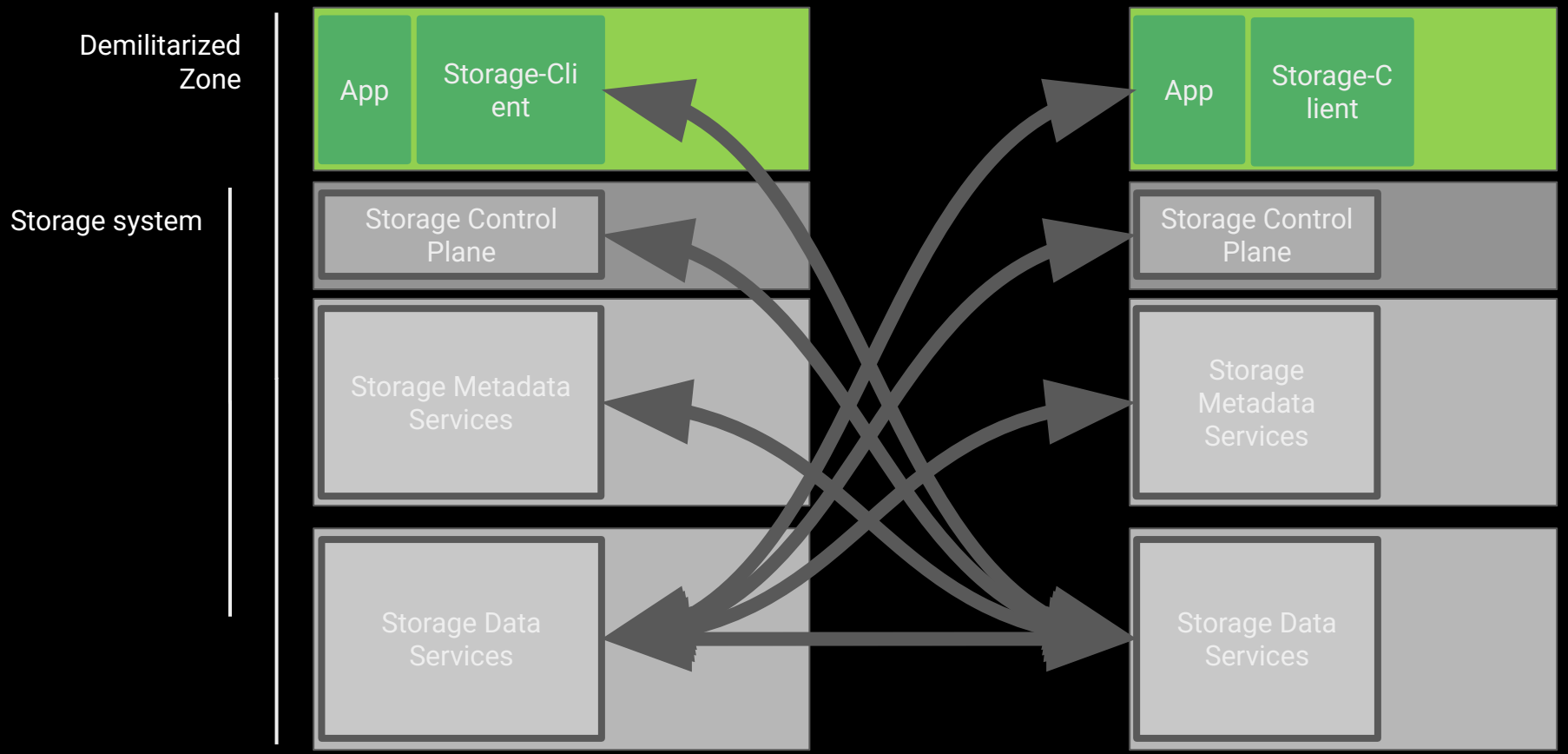
Demilitarized storage: Each party is trusted.

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

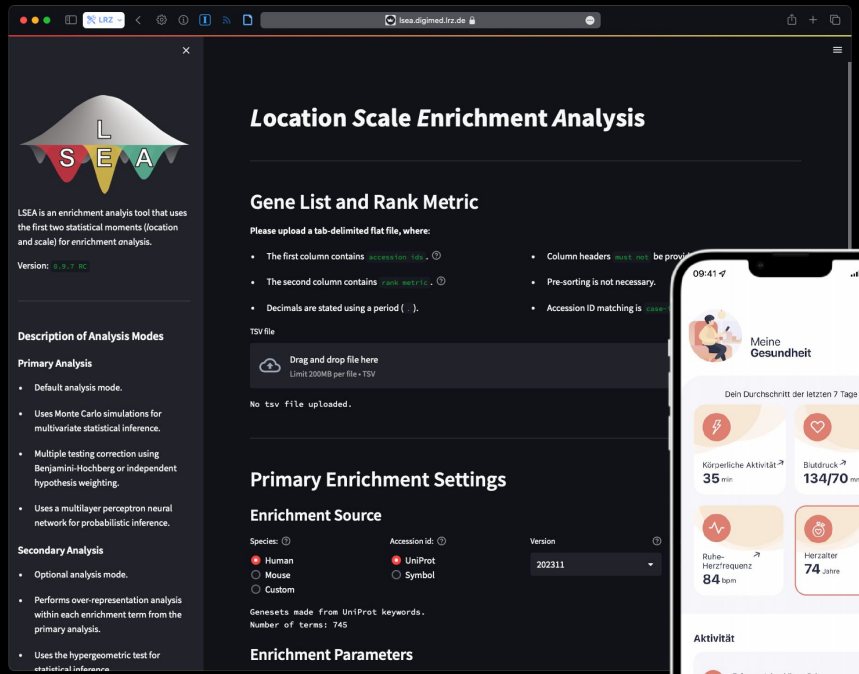
- X.509 Certificates: Ideal for untrusted networks/hosts. Certificates are verified locally. Restrictions can be assigned and modified in real-time: Tenant access, Operations limits (user/group), Volume access, Read-only access, Root squash.
- Access Keys: Granular user session authentication (like S3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

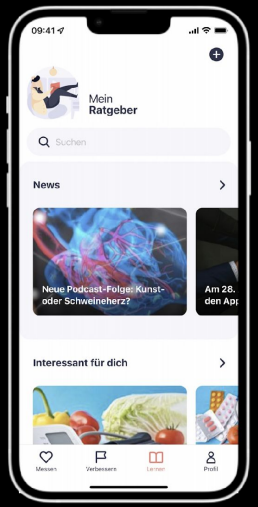
End-to-End Encryption & TLS

- 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





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

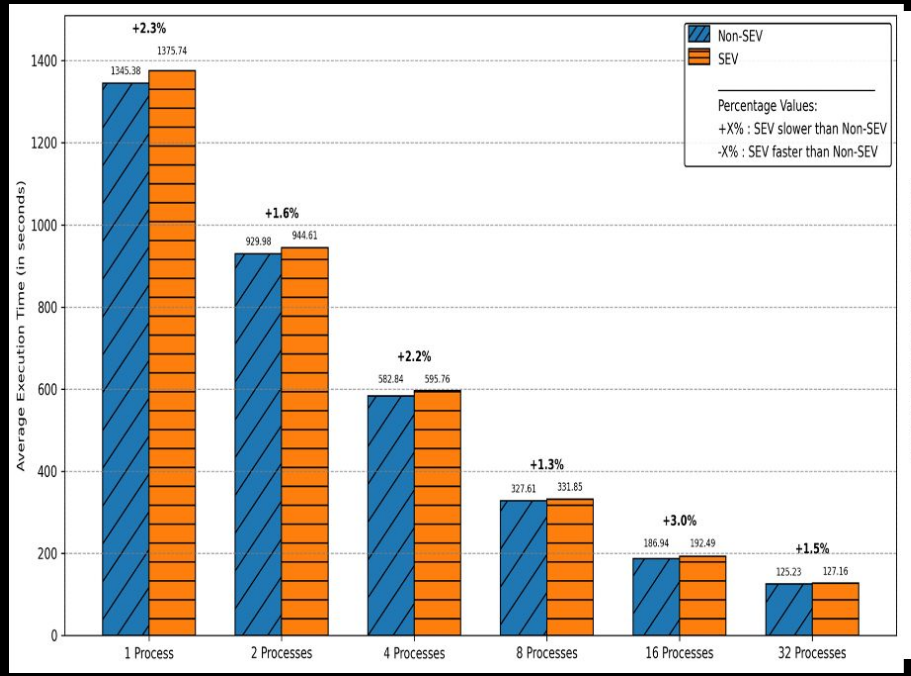
DigiMed

Dr. Jens Wiehler
Dr. Tim-Henrik Bruun
Anja Kroke
All partners

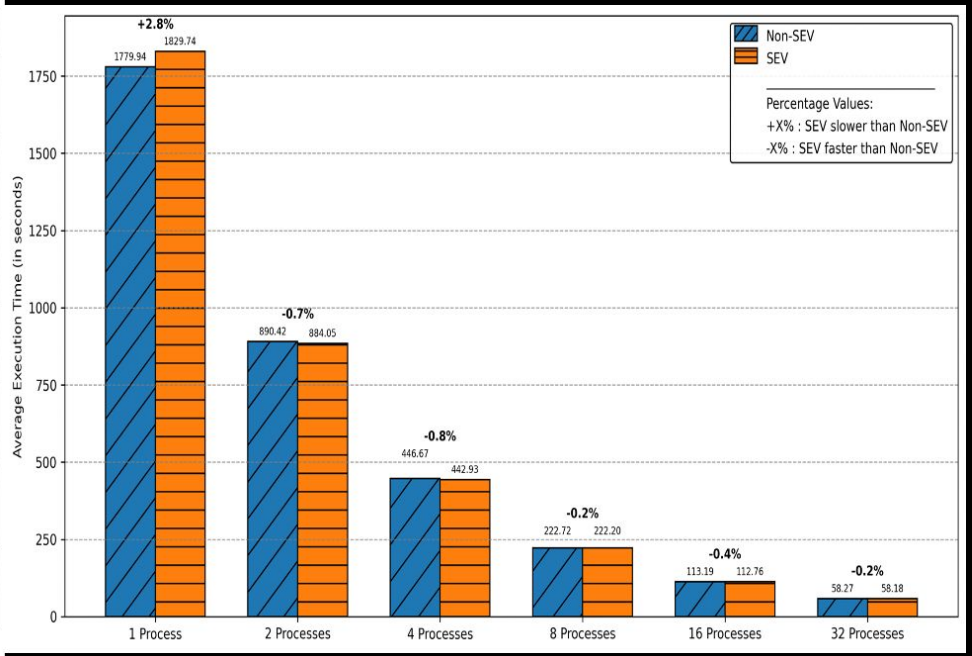
Quobyte team

OpenInfra FOUNDATION

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

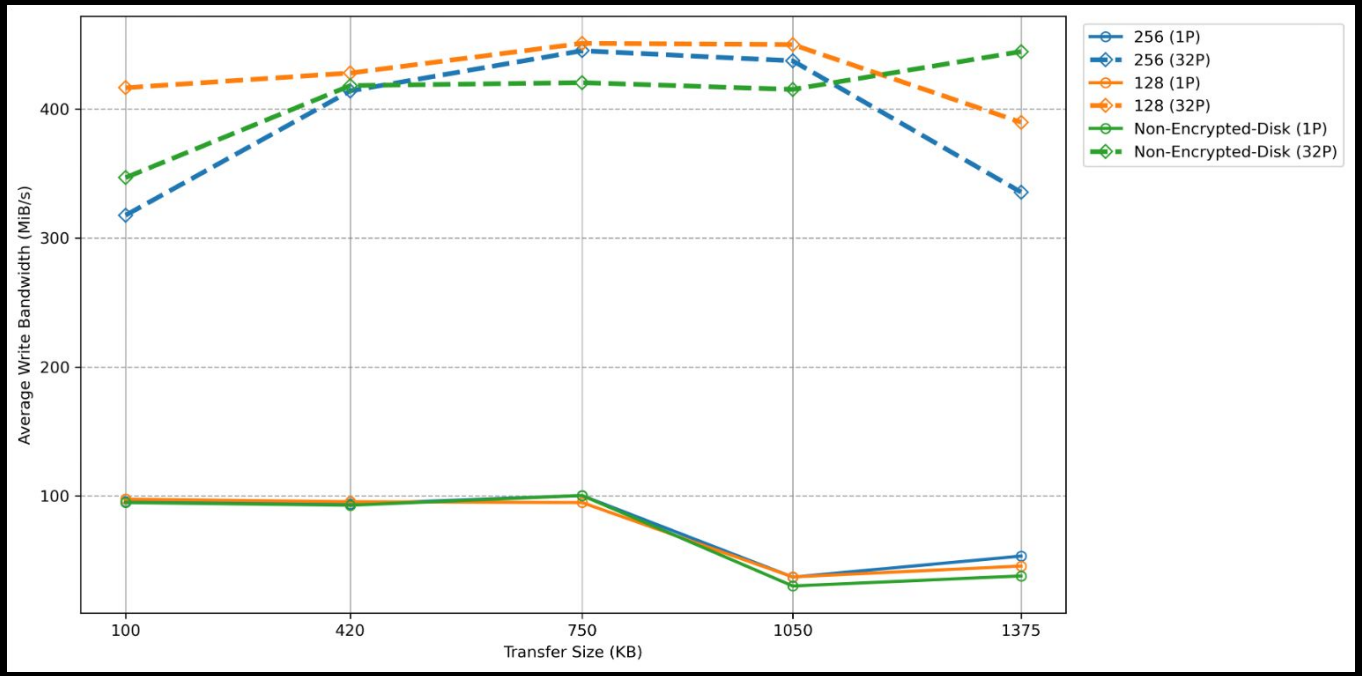


Performance for memory encryption (BPMF)



Performance for memory encryption (sysbench)

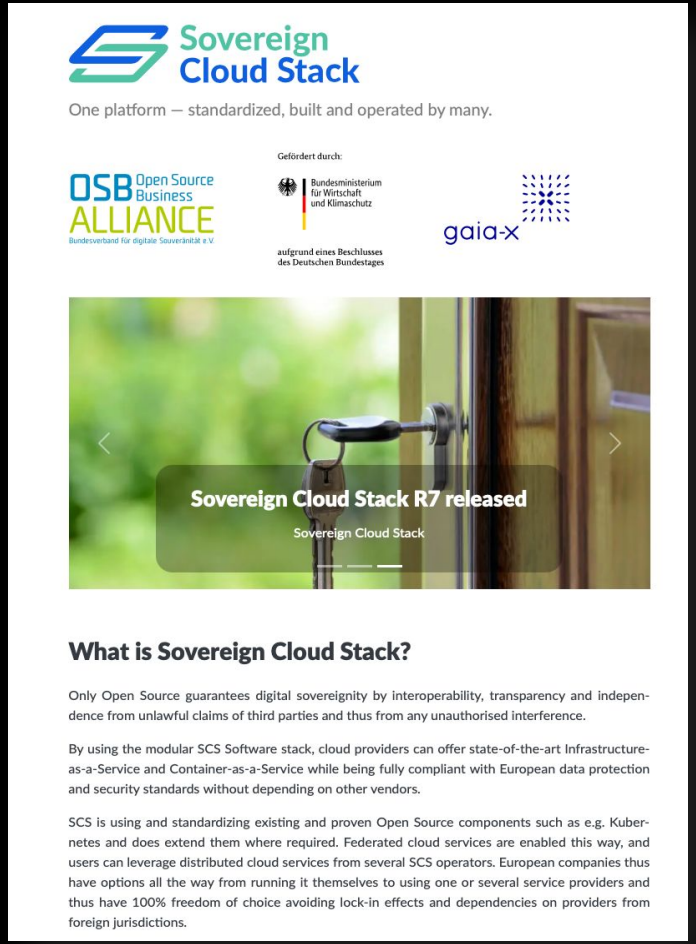
Cloud Performance in Healthcare:
A Benchmarking and Analysis Study of the DigiMed Secure Cloud



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



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