



TECHNISCHE
UNIVERSITÄT
DARMSTADT

TRUSTWORTHY DATA SHARING

TECHNOLOGY AS AN ENABLER

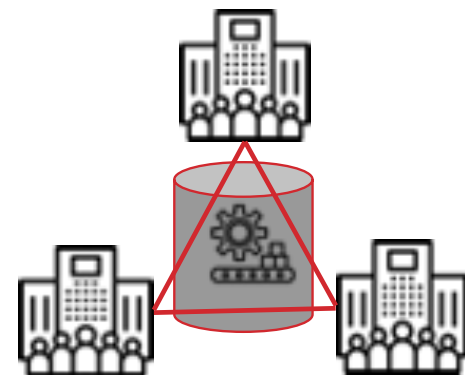
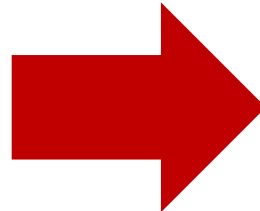
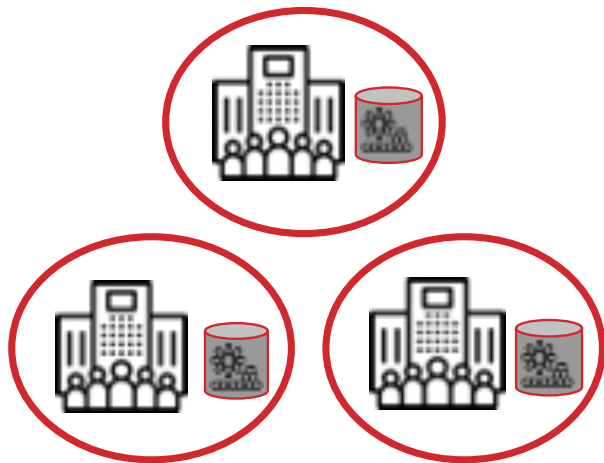
CARSTEN BINNIG (DATA AND AI SYSTEMS LAB)

THE VALUE OF DATA SHARING


From Data Silos ...

... to Shared Data

Organization C



Value of data sharing
(in manufacturing):

 ~ 1,5 Tri €¹

¹EU Data strategy: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN>

IS DATA SHARING IMPORTANT?

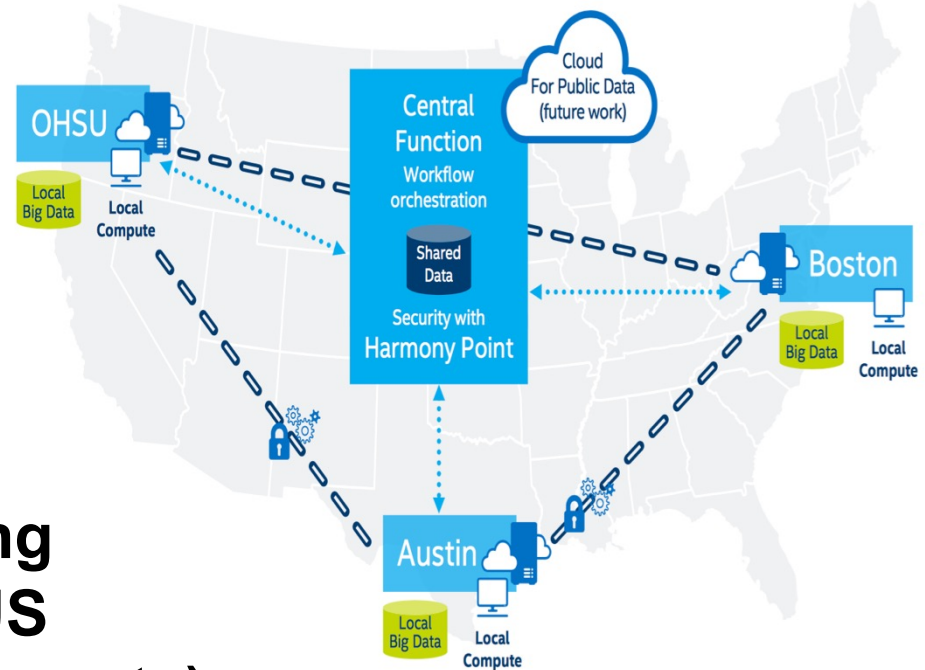


Different Reasons

- **Combining Data** across Multiple Organizations
- **Sharing Data** with Data Experts
- ...

CASE 1: COLLABORATIVE CANCER CLOUD

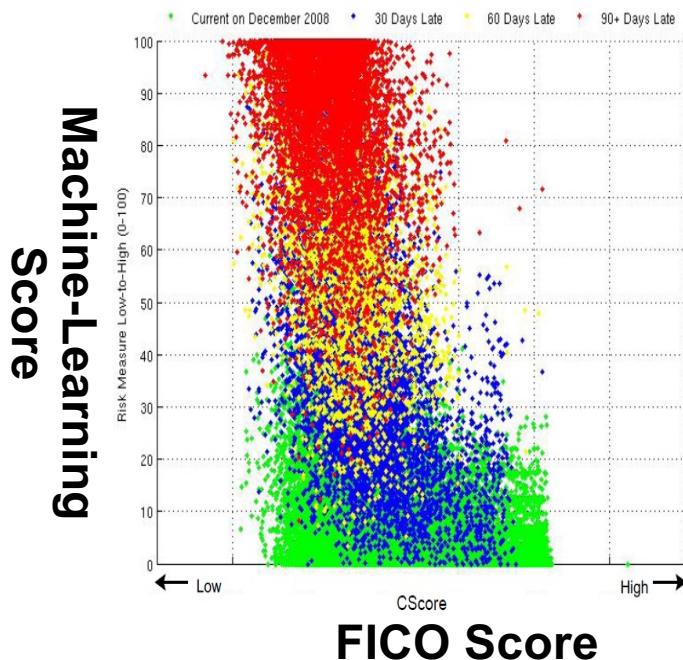
Goal: Securely analyze data sets across multiple institutions



**Secure medical data sharing
across institutions in the US
(e.g. for better cancer treatments)**

CASE 2: SHARING FINANCIAL DATA

Goal: Allow experts to estimate creditworthiness of individuals



1% sample, 10Tb

- Current
- 30-days late
- 60-days late
- 90+ days late

*Andrew W. Lo et al.
(MIT Sloan School)*

**Sharing with data experts can help to better
“understand” data**

OPPORTUNITIES OF DATA SHARING

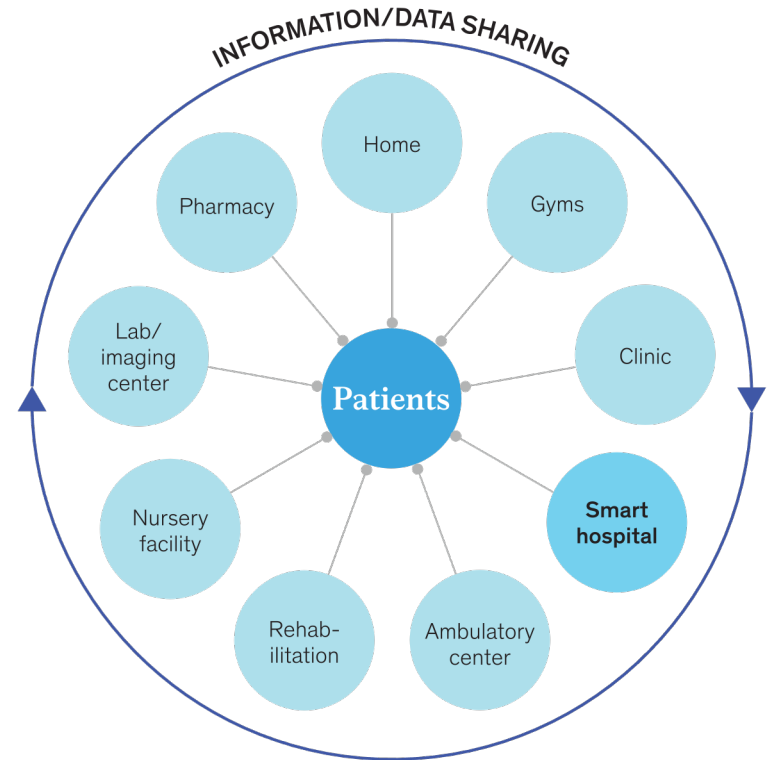
Important for various domains:

- Financial data
- Medical data
- Manufacturing data
- ...

Many new applications

- More data to train better ML models
- Sharing data to optimize manufacturing processes
- ...

Enterprise and private data (or a mix)



SO, DATA SHARING IS GREAT?



Isn't it?

BUT IN REALITY



Data Sharing often Fails!

DATA SHARING IS HARD / MANY BARRIERS

Many Regulations – all kinds of regulations (e.g., legal restrictions, company policies) - fear of doing something “wrong”

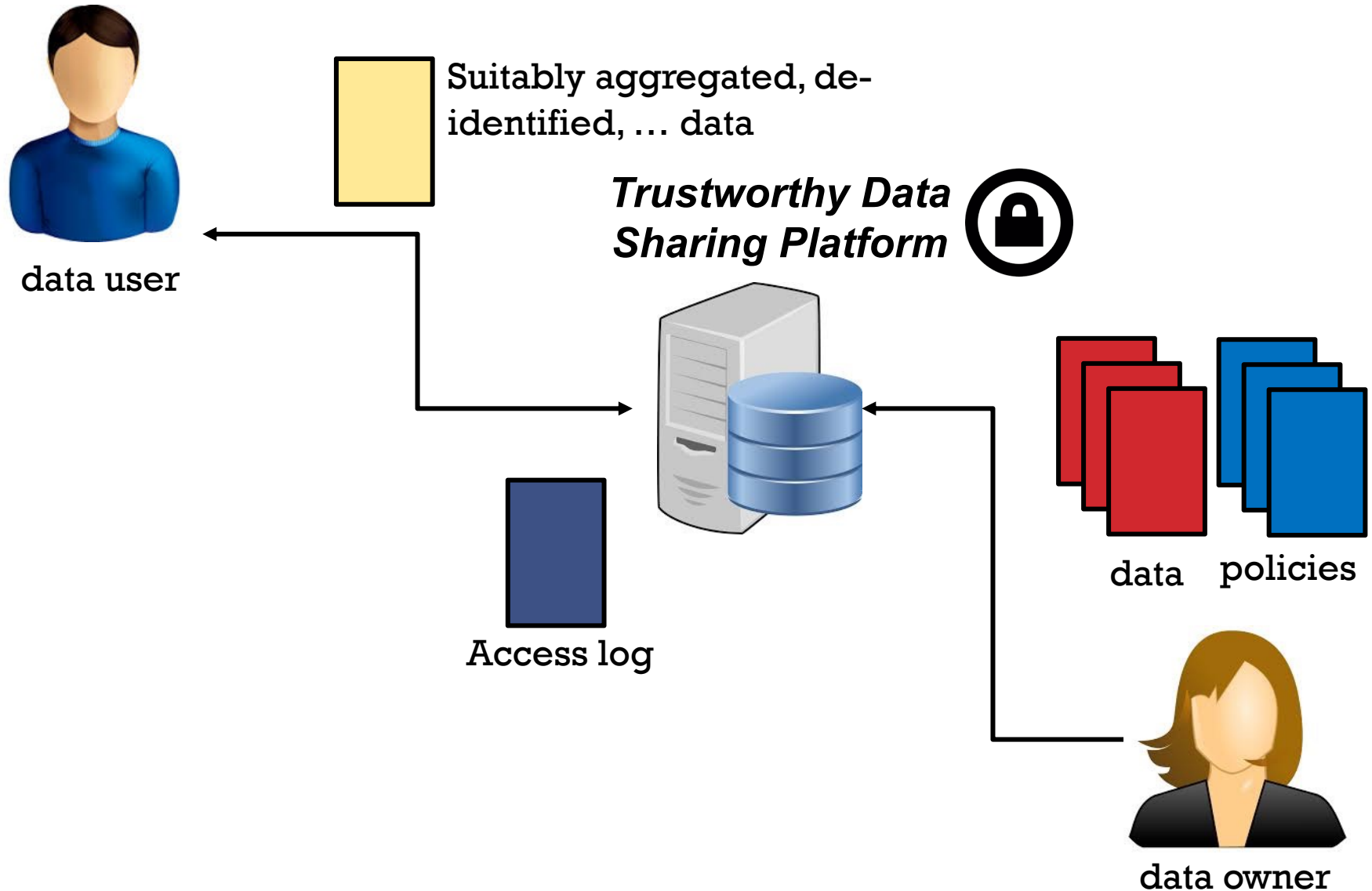
Concerns of revealing too much information

Simply: companies do not just “thru all data over the wall”!

- People prefer that data stays “on premise”
- Do not want to loose control over data!
- Can I get my data back?
- ...

Unclear Incentives – why would someone go to all the effort to share their valuable data?

TECHNOLOGY AS AN ENABLER ...



TRUSTWORTHY DATA SHARING = TECHNOLOGY ✕ SHARING AGREEMENTS

Tech

Access control &
rights management

Expiration

Logging & auditing

Provenance/Fingerp
rinting

Secure Hardware

Differential Privacy

Agreement Clauses

Controlled access (who &
where)

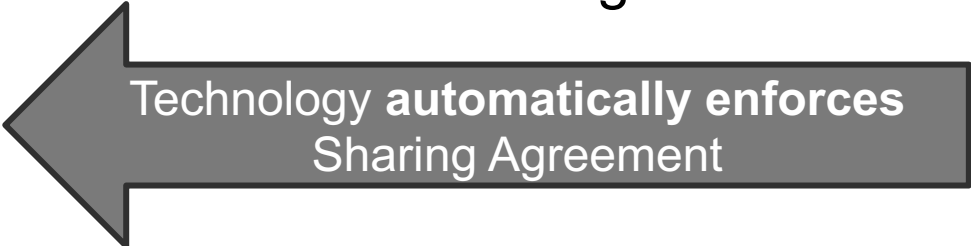
Tracking of access

Usage rights (e.g., publication,
copying)

Duration of use

Warrantees of
correctness/completeness/avail
ability

Privacy requirements and other
regulations



Technology automatically enforces
Sharing Agreement

TRUSTWORTHY DATA SHARING = TECHNOLOGY ✕ SHARING AGREEMENTS

Tech

**Access control &
rights management**

Expiration

Logging & auditing

Provenance/Fingerprin
ting

Secure Hardware

Differential Privacy

Agreement Clauses

**Controlled access (who &
where)**

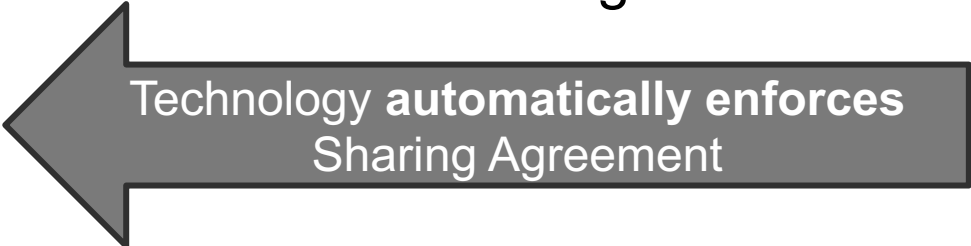
Tracking of access

Usage rights (e.g., publication,
copying)

Duration of use

Warrantees of
correctness/completeness/availa
bility

Privacy requirements and other
regulations



Technology automatically enforces
Sharing Agreement

TRUSTWORTHY DATA SHARING = TECHNOLOGY ✕ SHARING AGREEMENTS

Tech

Access control &
rights management

Expiration

Logging & auditing

Provenance/Fingerp
rinting

Secure Hardware

Differential Privacy

Agreement Clauses

Controlled access (who & where)

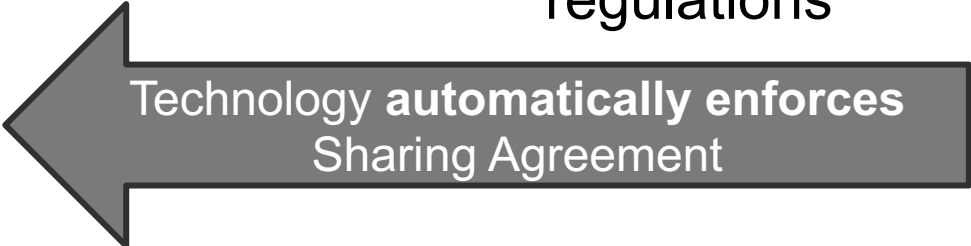
Tracking of access

Usage rights (e.g., publication,
copying)

Duration of use

Warrantees of
correctness/completeness/availab
ility

Privacy requirements and other
regulations



Technology automatically enforces
Sharing Agreement

TRUSTWORTHY DATA SHARING = TECHNOLOGY ✕ SHARING AGREEMENTS

Tech

Access control &
rights management

Expiration

Logging & auditing

Provenance/Fingerp
rinting

Secure Hardware

Differential Privacy

Agreement Clauses

Controlled access (who & where)

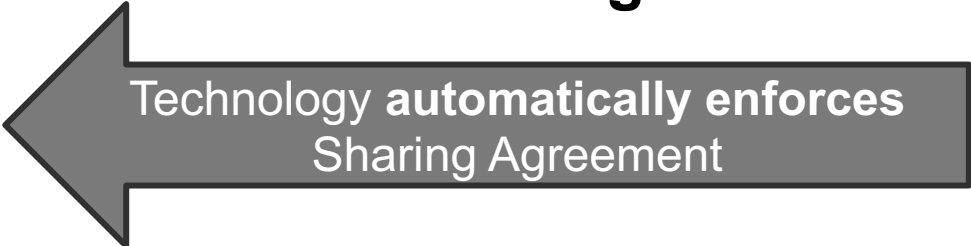
Tracking of access

Usage rights (e.g., publication,
copying)

Duration of use

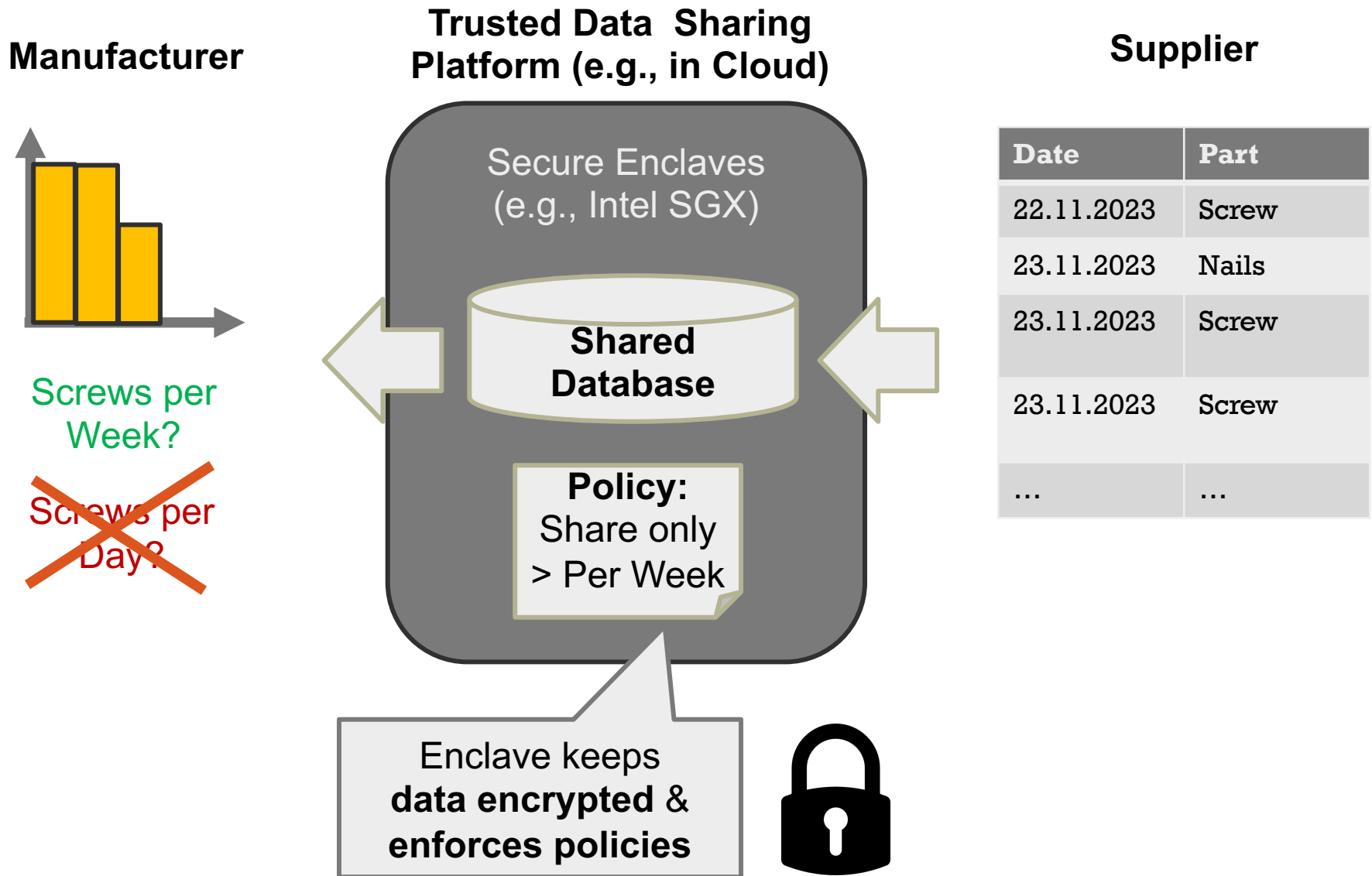
Warrantees of
correctness/completeness/availa
bility

**Privacy requirements and other
regulations**



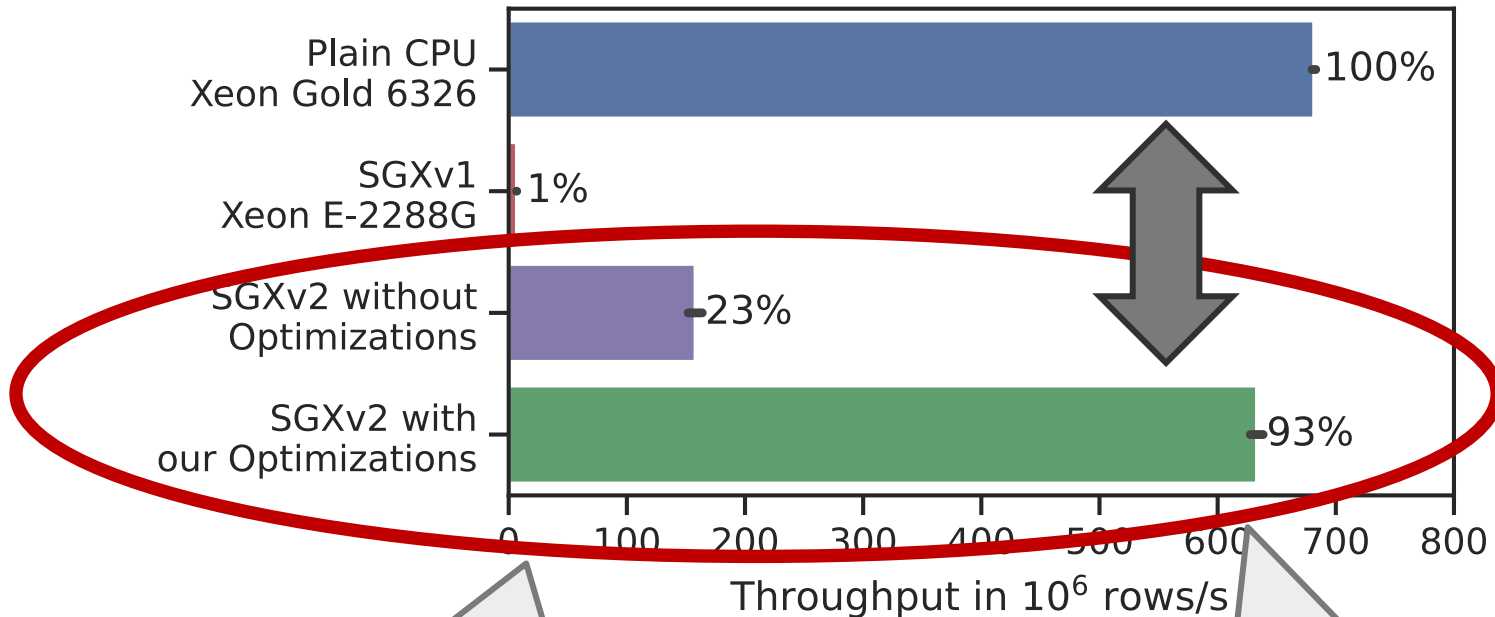
Technology automatically enforces
Sharing Agreement

SHARING DATA WITH SECURE ENCLAVES



SHARING DATA WITH SECURE ENCLAVES

Trusted Data Sharing Platform (e.g., in Cloud)



... But you need to **optimize your shared database** in the enclaves

... you can achieve **high performance** with recent enclaves

RESEARCH AT TUDA & PARTNERS



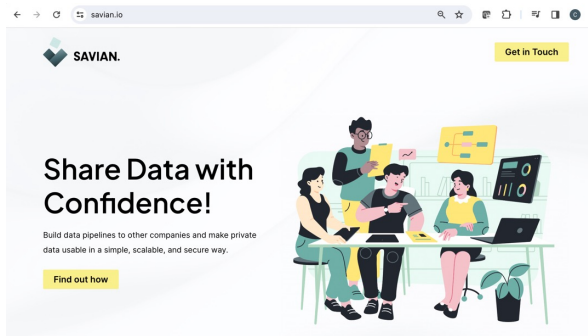
Athene Center: Research on Cybersecurity

- Research on various Aspects of Security
- Our Focus: Trustworthy Data Ecosystems



SafeFBDC: Data Sharing in Finance

- Focus on AI on Shared Financial Data
- 5 Use cases from Finance
- Industry & Academia. Part of GAIA-X



Savian: Secure & Simple Data Sharing

- Platform for Collaborative Data Use
- Startup from my Lab

THANK YOU FOR YOUR ATTENTION!

