**INDUSTRY** Life Sciences

**USE-CASE** Accelerating Time to Market

myngl.io

For pharmaceutical and life science companies, data sharing has many benefits: reducing duplications in human testing, increasing the reproducibility of research results, speeding up research, fostering new businesses and accelerating time to market for new devices and drugs. While most organizations recognize the importance of sharing data, concerns relating to loss of intellectual property, data misuse, and the difficulty of making data interoperable continue to impede direct data sharing partnerships.

## The Problem

### Sharing highly sensitive, proprietary and regulated data for analytics

Business, clinical and analytics teams need to combine rich, raw data sets from multiple owners for analytics and machine learning. The data generated by life science firms is enormously valuable, but also highly sensitive and regulated.

Teams find it difficult to share raw data across internal departments, let alone with ecosystem partners. Sharing clinical and related data for analytics has been an overly cumbersome and complex process - raw data.

The problem is that conventional databases and big data systems are not designed to securely commingle sensitive data from multiple owners.

With centralized controls for security and governance. conventional systems can be configured to allow users to extract or change data belonging to other owners.

Consequently, data owners asked to share data in a conventional system cannot be assured that their granular security and governance rules will be enforced. Legal agreements cannot address these challenges or prevent data misuse.

Life science business and data teams require access to rich diverse data sets for analytics and the ability to prove to each data owner that their data cannot be misused or extracted.

# Accelerating Time to Market

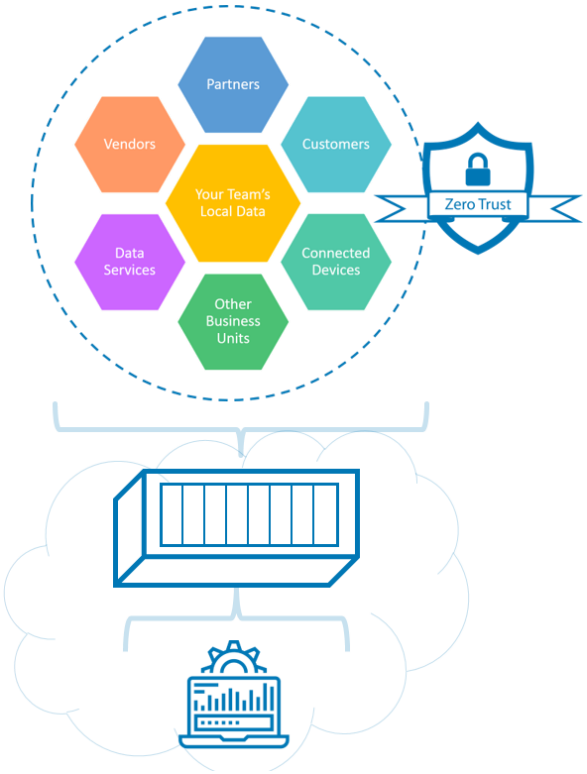
## Accelerating Innovation with Myngl Concordance

### Finding an Different Approach

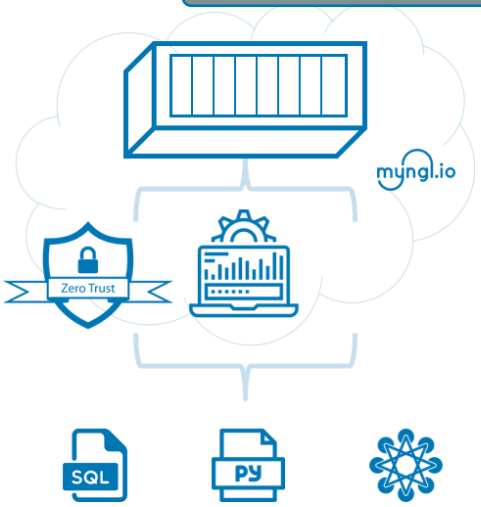
Myngl invented Concordance™ Secure Analytic Containers to work differently than conventional systems: decentralizing granular security and governance controls to data owners. Owners define "Need-to-Know rules that are embedded into every data element and cannot be edited or overridden by any user.

Subscribers must request explicit "Need-to-Know" authorization from each data owner to make use of shared data. Analytic jobs designed by Subscribers use, but cannot not expose, raw shared data. Users are blocked from directly extracting data to prevent data misuse, risks and breach.

This removes the mandate for trust to share sensitive data and accelerates mission-critical data projects.




## Commingling Data for Analytics and ML




### Accelerating Self-Service Analytics by 5x

Deployed in private and SaaS clouds, Secure Analytic Containers allow users to perform self-service analytics or machine learning on securely commingled data without exposing it. Popular open source notebooks make it easy to utilize SQL, Python, TensorFlow and other tools.

Business teams, analysts and data stewards coordinate in a secure and collaborative data sharing workflow that accelerates analytic projects 5x faster than any alternative.

Visit www.myngl.io to schedule a demo or contact sales@myngl.io for more information.