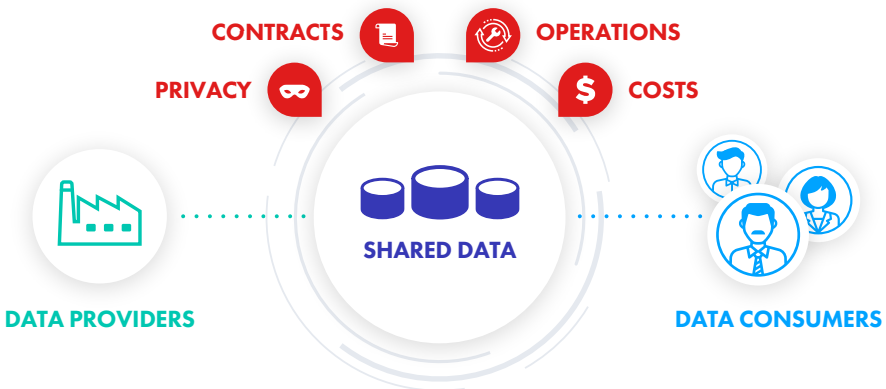
IMMUTA™

Secure External Data Sharing

Many organizations are discovering new sources of revenue by monetizing their data assets, and are becoming data *providers* for business partners and affiliated data *consumers*.

These data consumers are unlocking competitive insights, creating new opportunities, and reducing the overall cost and complexity of their analytics environments. Modern cloud capabilities are enabling data providers and data consumers to facilitate mutually beneficial data exchange transactions.

- Data providers can easily package and publish data with built-in security, compliance, and governance, and make it available to broader data consumers.
- Government agencies can improve city planning and citizens' experiences by anonymously sharing aggregated citizens' data, traffic patterns, and infrastructure data so it can be shared securely with other agencies and public utilities.
- Banks, insurers, and asset managers can make real-time decisions with trading strategies, build comprehensive risk models, and offer new advisory services by securely leveraging external data sources such as industry profiles, company information, market valuations, and aggregated demographics data.
- Healthcare providers, payers, and pharmaceutical companies can improve patient care, optimize clinical trials, and deliver affordable insurance plans faster by securely combining internal data with external data on drug usage patterns, life expectancy, and aggregated claims.
- Media and Entertainment providers can optimize customer experience and personalized recommendations by combining their own data with audience segmentation, current events, and social sentiments.



Barriers to Data Sharing

Organizations with valuable data assets are often reluctant to share their data for fear of **privacy** implications, data sharing **operational** hassles, and unpredictable infrastructure **costs**. These data providers also struggle to keep up with the constantly changing data sharing laws and local regulations, as well as **contractual** auditing requirements. These limitations discourage many data providers from sharing any data, instead locking most of it to ensure compliance. As a result, data monetization opportunities are limited and data consumers are prevented from accessing valuable and critical business data.

How Immuta Helps

Data sharing technologies have matured beyond file sharing and direct SQL access. Now, data providers are able to maximize the value of their data assets, while data consumers are gaining a competitive advantage with deeper insights. The modern data sharing solution consists of offerings from cloud vendors and from Immuta.

The cloud vendors provide solutions to eliminate the need to maintain data sharing infrastructure.
Some of the vendor offerings include:

AWS Data Exchange: Gives data providers a secure and efficient distribution channel to share data. Data consumers can easily find and access the data in the cloud.

Databricks Delta Sharing: An open-source project that simplifies real-time cross-organization sharing of large data sets.

Snowflake Data Marketplace: Provides access to third party data for deeper insights and data from SaaS vendors.

A single Immuta access control policy can replace

100+

identity access management roles, saving time and increasing agility.

Immuta's dynamic policy enforcement increases efficiency by more than

90%

Immuta provides critical data sharing capabilities to make it easier for data *providers* and data *consumers* to take advantage of their data assets. As a result, Immuta improves IT productivity by 40% and provides comprehensive cloud data access control.

Universal Cloud Data Compatibility

Enables data *providers* and *consumers* to leverage data sharing capabilities natively within AWS Data Exchange, Databricks Delta Exchange, and Snowflake Data Exchange. This centralized data sharing approach reduces the operational costs and complexities.

Scalable, Policy-Based Access Control

Allows data *providers* to build simple access control policies to protect sensitive data. The policies are written in plain English to ensure data *consumers* have the right level of access to the right data. Immuta provides fine-grained access control at the column-, row-, and cell-level. Immuta also provides consent workflows to comply with 'intended' purpose regulations, creating attribute-based controls that enforce who can use what data and why, with auditing.

Advanced Masking & Anonymization

Enables data *providers* to leverage Immuta's advanced privacy-enhancing technologies (PETs) – backed by math and Immuta's expert team of legal engineers – to accelerate data sharing by dynamically masking and anonymizing sensitive data.

Sensitive Data Detection & Classification

Automatically discovers, catalogs, and registers sensitive data, such as PII or PHI, helping data *providers* save time and eliminate the risk of manual errors. Once the data is registered, data teams can tag direct, indirect, and sensitive identifiers with certified workflows, mapping to privacy protection laws (CCPA, HIPAA, GDPR, and COPPA), and auditing for compliance and governance.

Dynamic Policy Enforcement & Auditing

Immuta provides centralized real-time insights and detailed reports showing what data was accessed, by whom, when, and for what purpose. Immuta automatically monitors and logs all actions so data *providers* can be confident data is used securely and prove contractual and regulation compliance.

To see what you can accomplish with Immuta when you request a demo today.

REQUEST A DEMO

IMMUTA™

115 Broad Street, 6th Floor, Boston, MA 02110 | immuta.com | (800) 655-0982