VIEW POINT

THE PROMISE OF PRIVACY FIRST DATA SHARING

Abstract

Business and IT leaders struggle to securely share the data with partners, suppliers, or vendors outside their organization. There is a risk of re-identification of personal data and a potential data breach while sharing data at scale including the need to protect privacy, address commercial concerns, maintain ethical standards, and comply with legal obligations.

This point of view provides a blueprint of how Infosys Enterprise Data Privacy Suite (iEDPS) powered by Opaque can enable enterprises to securely share data and perform analytics on sensitive data through secure hardware enclaves and advanced encryption techniques.

Opaque

Infosys®
Navigate your next

Table of Contents

1. Overcoming impenetrable Data Siloes across Enterprises..... 3
2. Key Challenges in Sharing Data..... 3
3. Unlocking the potential of Privacy First Data Sharing..... 5
4. References and Further Reading..... 7
5. About the Authors..... 7

Overcoming impenetrable Data Siloes across Enterprises

In this age of data-driven economy, organizations remain overwhelmed by the sheer volume and variety of the data at their enterprise. The pace at which data is collected and exchanged across internal and external networks has increased manifold times.

Enterprises across the globe are significantly investing in AI capabilities for many use cases like quality control, customer care, fraud detection, and in-depth end consumer behavior analysis.

Organizations are heavily investing in sentience and automation through machine learning but are yet to realize the right ROI on their investments. The primary challenge they face is their inability to share data within the organization or outside the organization to partners, suppliers, or vendors. There is a risk of re-identification of personal data and a potential data breach. Data Sharing at scale needs is a need for an organization to realize ROI on their AI investments.

This point of view provides a blueprint of how Infosys Enterprise Data Privacy Suite (iEDPS) powered by Opaque can enable enterprises to securely share data and perform analytics on sensitive data through secure hardware enclave and advanced encryption techniques.

Key Challenges in Sharing Data

For example, meet David is moving from North America to the UK for a new job. These two continents have different privacy regulations and many different sections across which David's data will flow. Data needs to be shared, across a wide range of entities, from road transport companies to logistics providers across both the origin and the destination.

	Door Origin	Transport to Port	Port Origin	Port Destination	Transport to Home	Door Destination
Data Needed for Transport	• Raise a request on the Portal	• Address data and key documentation shared with the Transport Company	• Travel Documents • Visa	• Customs Form • Visa / EIN	• Personal data shared with local transport companies	• Updates to the end customer
Personal Data Shared	• Customer purchase behavior shared for local business in the current city	• Transport company shares the data to local suppliers, retailers and other services	• Port logistics and demand prediction	• Port logistics and demand prediction	• Transport company shares the data to local suppliers, retailers and other services	• Customer purchase behavior shared for local business in the new city

Moment of data flow goes along with multiple personal data breach risks such as data theft, data leakage, account/service hijacking, data sharing across unprotected interfaces & APIs, denial of service attacks, or technology vulnerabilities -- especially in shared environments.

Furthermore, stringent data privacy regulations such as the General Data Protection Regulation (GDPR) in Europe impose a high risk of penalties for stakeholders leveraging David's data to predict demand and provide customer service. David requires the ability to erasure data at his request, while non-erasure—full traceability is also needed. The flow of data also leaves a passive digital footprint. This footprint can be analyzed offline and stored in files making it prone to breaches.

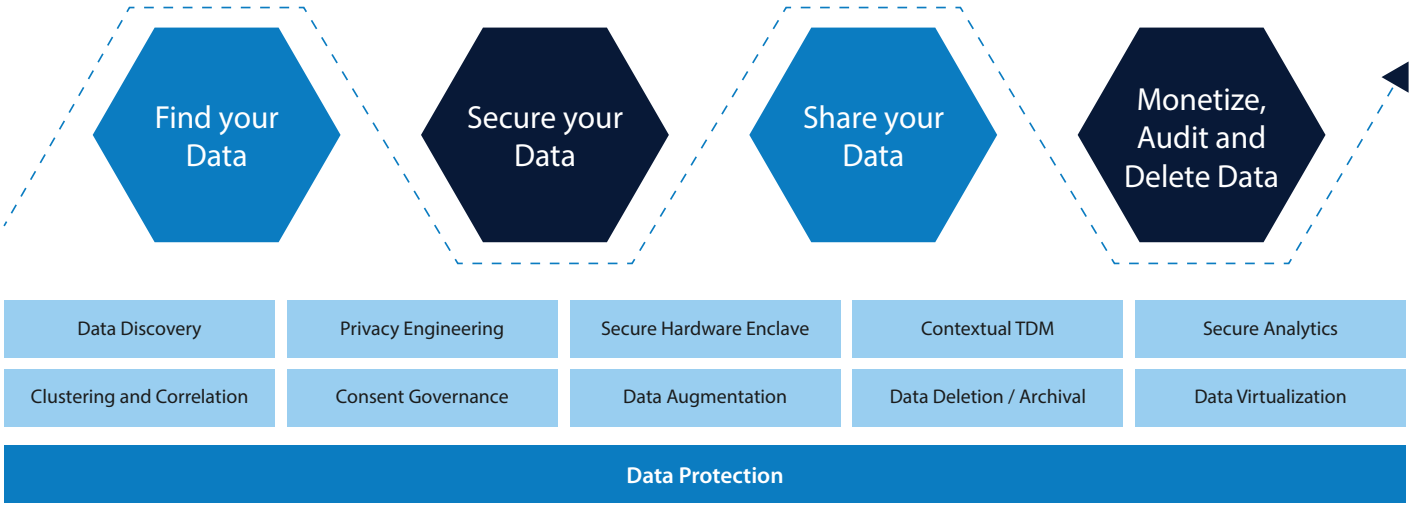
This risk of a data breach is the major hurdle for industrialized AI models that depend on the availability of high-quality data -- the more a model ingests, the more accurate is its analysis and better decision making. The problem gets compounded by the unavailability of data or the inability to share data with third parties.

Unlocking the potential of Privacy First Data Sharing

There is an urgent need to share data across technology stacks in an anonymized privacy-first way without compromising the ability to extract insights. Share data securely is one piece of the puzzle the other is successfully monetize the same. Data valuation and trading across enterprises facilitate eliminating data siloes across enterprises, leading to shared insights that would not otherwise be possible.

We are already seeing examples of secure data collaboration in the pharma industry. Pharma producers are exploring the formation of consortiums to share drug research data for R&D purposes, so that consortium members can securely share data and collaboratively analyze the collective data in a privacy-first way (for example, using federated learning - a decentralized form of machine learning). Similarly, manufacturing or retail supply chains, sharing data across value chains and between different providers in a customer journey can yield benefits. This need for secure data sharing extends across other industries, such as fintech, shipping, logistics and telco.

Through the Infosys Innovation Network (IIN), a well-orchestrated partnership between select startups and Infosys to provide innovative services to our clients, we integrate startups into broader Infosys platforms and de-risk their implementation for clients. With 10-years of experience in the data privacy industry and 60+ successfully implementations - Infosys Enterprise Data Privacy Suite (iEDPS) Platform powered by IIN startup partner Opaque Systems provides a comprehensive set of capabilities that can enable enterprises to truly unlock the potential of data by classifying and identifying personal data, securing personal data, sharing it across multiple stakeholders and aiding in the monetization of data.



Opaque Systems has proven expertise in the field of secure computing to safeguard information. Opaque's proprietary technology allows multiple data owners to individually encrypt their data, pool their encrypted data together in the cloud, and jointly analyze the collective data using advanced analytics models or machine learning. Opaque ensures the data is never exposed, unencrypted to the cloud even when it's in use, keeping the data protected throughout the lifecycle of the analysis. These capabilities combined with Infosys Enterprise Data Privacy Suite (iEDPS) capabilities enable organizations to share data across complex technology ecosystems, remain compliant with key regulations, and provide effective personal data protection.

iEDPS (Infosys Enterprise Data Privacy Suite) provides enterprise-class data privacy capabilities and enables an organization to adhere to global regulatory standards such as GDPR, CCPA, HIPAA, PIPEDA, GLBA, ITAR, and various local regulations. Built-in with deterministic, selective, dynamic, and static masking features, Data Discovery, and Data Generation capabilities, iEDPS can be deployed on any platform and supports all major databases and file systems.

With 60+ successful customer implementations and a dedicated team focusing on Data Privacy Consulting, Product Engineering and Customer success – iEDPS enables a Privacy First Organization and unparalleled protection to your data.

References and Further Reading

- https://www.infosys.com/services/incubating-emerging-technologies/insights/data-protection-privacy.html
- https://www.infosys.com/services/incubating-emerging-technologies/offerings/enterprise-data-privacy-suite.html
- https://opaque.co/
- https://iapp.org/media/pdf/resource_center/Guide_to_Data_Sharing.pdf
- Opaque one-pager

About the Authors

Rishabh Poddar

Rishabh Poddar is the CEO and Co-Founder of Opaque Systems, a platform for secure analytics and machine learning on confidential data. Rishabh holds a PhD in computer science from UC Berkeley, specializing in computer security, systems, and applied cryptography.

Vijayalaxmi Suvarna

Vijayalaxmi Suvarna is a Senior System Engineer at Infosys Center for Emerging Technology Solutions, she leads the Marketing initiatives for Infosys Enterprise Data Privacy Suite (iEDPS) Platform. Her focus includes User Experience and online branding of Infosys Data Privacy offerings.

Karthik Nagarajan

Karthik Nagarajan is an Industry Principal Consultant at Infosys Center for Emerging Technology Solutions (ICETS). He has more than 15 years of experience in Data Privacy, and Cx Strategy. He currently works with the product team of Infosys Enterprise Data Privacy Suite.

About Us

The incubation center of Infosys called 'Infosys Center for Emerging Technology Solutions' (iCETS) focuses on the incubation of NextGen services and offerings by identifying and building technology capabilities to accelerate innovation. The current areas of incubation include AI & ML, Blockchain, Computer Vision, Conversational interfaces, AR-VR, Deep Learning, Advanced Analytics using video, speech, text, and much more.

To know more, please reach out to iCETS@infosys.com

For more information, contact askus@infosys.com

Navigate your next