PRODUCT BRIEF

inpher

SECRET COMPUTING®

PIONEERING PRIVACY-PRESERVING
MACHINE LEARNING

Inpher Secret Computing®

Industry's First Enterprise-Ready Privacy-Preserving Computing Platform Built for Data Scientists

THE ERA OF PRIVACY-PRESERVING ML IS HERE

Enterprises are tapping into the power of ML for faster innovation and a competitive edge. Yet, increasing data privacy concerns and regulatory barriers hold them back from moving into the new era of intelligence, where data accessibility is the key to developing high-quality ML models.

Problem: The Paradox of AI and Data Privacy

AI and advanced analytics require easy access to data, whether across teams, geographies, or even across organizations. Unfortunately, too many AI initiatives are stalled due to stringent data privacy laws, organizational policies, and confidentiality concerns. Hence data science efforts become time-consuming, costly, and sometimes even impossible.

Fragmented data silos lead to lost insights. Unifying data takes weeks to months, and is often error-prone, resulting in privacy leakage.

Compromising model accuracy for data privacy. Existing approaches inject noise or eliminate critical features. Tradeoffs are expensive, especially for mission-critical apps.

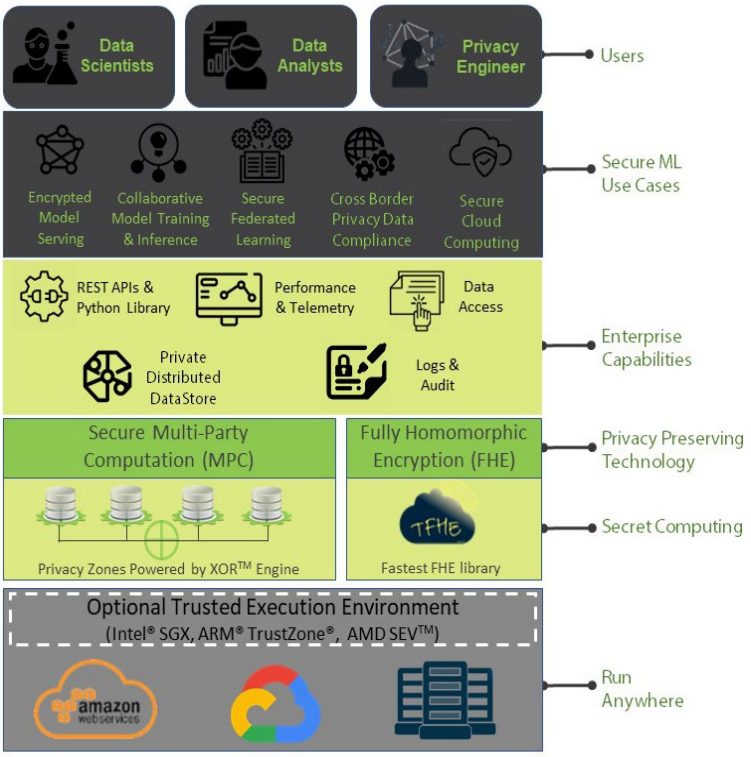
Fines are no longer just monetary. Beyond negative reputation and lost customer trust, newer stringent laws mandate companies to purge valuable models and algorithms that violate privacy rules.

Privacy-Preserving ML (PPML) Done Right!

With Inpher Secret Computing® technology, enterprises can eliminate tradeoffs between data usability and data privacy as sensitive data is no longer exposed or transferred, thereby maintaining regulatory compliance.

+ Inpher's XOR™ product is built with the most advanced cryptographic solution that supports both Secure Multi-Party Computation (MPC) and Federated Learning (FL)
+ Inpher's award-winning Fully Homomorphic Encryption (FHE) solution is available through the popular open-source TFHE library

Secret Computing® empowers data science teams to build and deploy privacy-preserving ML applications without knowing the nuances of data privacy or advanced cryptographic functions.



SECRET COMPUTING ARCHITECTURE

Unify Silos with Secure Data Collaboration

+ XOR's Private Set Intersection (PSI) allows businesses to collaborate across different parties' data without exposing or transferring them. Additionally, data or trained models are stored in Private Distributed DataStore (PDDStore), so no single party can ever access another's data.
+ Train on more features or more data by collaborating across multiple privacy zones.

Build High-Precision, Accurate Models

+ Existing data privacy approaches like anonymization reduce predictive features while differential privacy injects noise, compromising model accuracy. XOR leverages advanced cryptographic and cloud computing technology to maintain privacy and high precision for accurate models.
+ With the XOR Python library (XOR-py), data scientists can build accurate models in familiar interfaces like Jupyter notebooks.

Exceed Regulatory Compliance Needs

+ Encrypted computation through MPC and FHE keeps your data secure while computing. With MPC, the data is split in such a way that no party has sufficient information to reconstruct the personal data in whole or in part. Exceed your privacy needs while unlocking business values
+ Open a world of possibilities with PPML, from distributed training to federated learning and secure model serving

Privacy-Preserving ML Use Cases

Collaborative Model Training & Inference

Improve model training and inference accuracy by leveraging data across multiple parties – either using more data or using more features from different sources.

Secure Federated Learning

Federated Learning doesn't guarantee privacy by default as model parameter updates can lead to model inversion and inference attacks. Build federated learning models with secure aggregation.

Encrypted Model Serving

Protect your models from competitive threats while delivering Model-as-a-Service (MaaS). Additionally, guarantee inference input and output privacy for your customers.

Cross Border Data Privacy Compliance

Deploy encrypted models to analyze data that can't leave the country of origin. Guarantee compliance to country & regional-specific data required with mathematical proof.

CUSTOMER HIGHLIGHTS

> **The 'bad guys' have all the same technologies we do. But the one thing they cannot obtain is the scale of training data we can through collaborative sharing, such as through what Inpher offers with Secret Computing.**

Hayes. W "Skip" McCormick
Data Science Lead BNY MELLON

Privacy Advocacy with Leading Regulators

edpb European Data Protection Board recommends MPC for cross-border data transfer- "Split or Multi-Party Processing." With MPC, the data exporter can let the personal data be processed jointly by two or more independent processors located in different jurisdictions without disclosing the data to them.

HM Treasury highlights Inpher in their report. "Inpher XOR Secret Computing project. The project enables a bank to incorporate data from foreign subsidiaries to inform a machine learning sale-prediction model without any cross-disclosure of underlying data. Data from the foreign subsidiaries increased the training data for the machine-learning model. The project used MPC and FHE techniques.

Get Started Today

aws Google Cloud