Duality

Fact Sheet

# Secure Collaborative AI

# Unlock Data and Protect IP for AI model Training and Customization

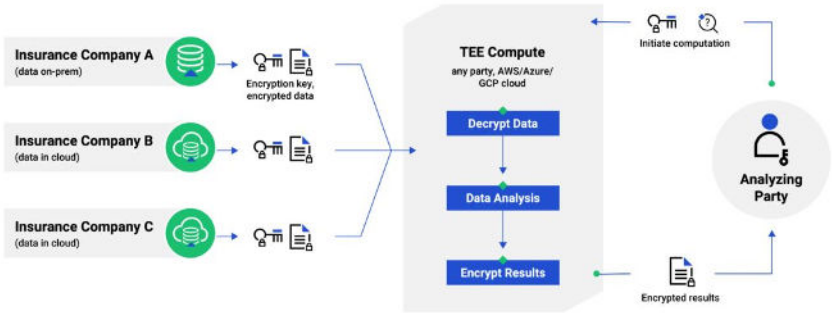
## Secure Collaborative AI

A new gold rush has been ignited, this time with AI and Machine Learning models. As the market crowds, it will be the organizations with the best speed and scale of data that survive. The reason is that models need efficient streams of high-quality data for development, training, inference, and customization. To satisfy the data demand, AI teams must often work with third-party organizations (TPOs) to create market-worthy applications or to customize a foundational model for a particular client. This necessary collaboration in AI strategies is challenged by concerns over both data and model protections and confidentiality. The Duality Secure Collaborative AI solution eliminates those challenges by providing a flow in which both the input data and model IP are protected during training, tuning, and customization.

Such a solution creates new, exciting questions for organizations to answer and wishlists to satisfy. What's a dataset that couldn't be used by your team because of data localization requirements? What's a dataset that couldn't be shared with your team because of the sensitivity of the data? What if you could customize a model on real client data while protecting your IP and the input data? What if you could prove a model's value on your customers' real data earlier in your sales process? How many AI vendors could benefit from training on our data? These are just a few of the growth opportunities that come with Secure Collaborative AI.

## How it works

- Choose a confidential computing option (TEE or Secure Enclave) from any provider: AWS, GCP, Azure
- Install the Duality Software
- Use the Duality interface for user and data management and governance
- Encrypted data is moved to the TEE along with the encrypted models
- Operations are confidentially and securely performed within the TEE
- Encrypted results are generated and returned to analyst for further analysis or review




## Security and Privacy by Design

The Duality Platform offers a broad set of privacy technologies – including hardware and software solutions – to enable models of all types to be deployed while protecting IP, data privacy, and data security. Organizations use the cloud-agnostic Duality Platform to collaborate with customers, partners, and data providers while ensuring the necessary governance and controls to enable privacy-protected collaboration.

# How Duality Helps

### Monetize AI Models and Protect Your IP

Duality allows for models to be deployed without risking IP leakage, enabling AI Vendors to extract and provide the utmost value from their hard work without the risk.

### Build Better Models with Better Data

Developing AI models requires access to real data. Duality allows organizations to leverage the most sensitive real data (rather than just synthetic data) for model development while satisfying privacy, security, and legal concerns by default.

### Unlock Better Data to Gain Critical Insights

The existence of data does not mean it's usable or accessible. Duality's solutions unlock data from privacy and security concerns so you can deploy models against any sensitive data to drive better insights in less time.

### Enhance Customer Value with Personalized AI Models

Personalize models on sensitive customer data. Streamline model personalization without exposing your models' IP and without needing the client to expose their sensitive data to you.

# Use Cases

### Government: Collaborative Model Training

Build and deploy cybercrime, financial crime, and national security models with public and private sector partners, without exposing sensitive data or the models themselves.

### Healthcare: Predicating Pathologies

Deploy AI models to predict and detect pathologies using imagery data linked with PII and PHI. Overcome data localization issues by moving the compute to where the data lives, knowing that your model IP is protected.

### Financial Services: Risk Scoring

Build better risk models by combining features across data vendors and financial institutions while ensuring sensitive data and models are protected.

### Data Service Providers: Fast, Secure Trials

Allow clients to securely test models on real data before proceeding with a purchase decision. Ensure data is protected at all times and speed up time to value for clients during customization and deployment.

## Get Started Today
## Visit www.dualitytech.com for more information

Or, reach our public sector team by emailing gov@dualitytech.com

## Recognized across the Public and Private Sectors

DARPA · NIH · IBM · Deloitte. · aws · CACI · Microsoft · carahsoft · ORACLE · ico. · intel · Scotiabank · Google Cloud · Lloyds Banking Group · Globant

## About Duality

Duality is the leader in privacy enhanced data and AI collaboration, empowering organizations worldwide to maximize the value of their data without compromising on privacy, security, or compliance. Founded and led by world-renowned cryptographers and data scientists, Duality operationalizes privacy enhancing technologies (PETs) to accelerate data insights by enabling analysis and AI on encrypted data, while preserving data privacy, compliance and protecting valuable IP.


**HEADQUARTERS**

5 Marine View Plaza
Hoboken, NJ 07030

**CONTACT US**

info@dualitytech.com
Duality Technologies

dualitytech.com