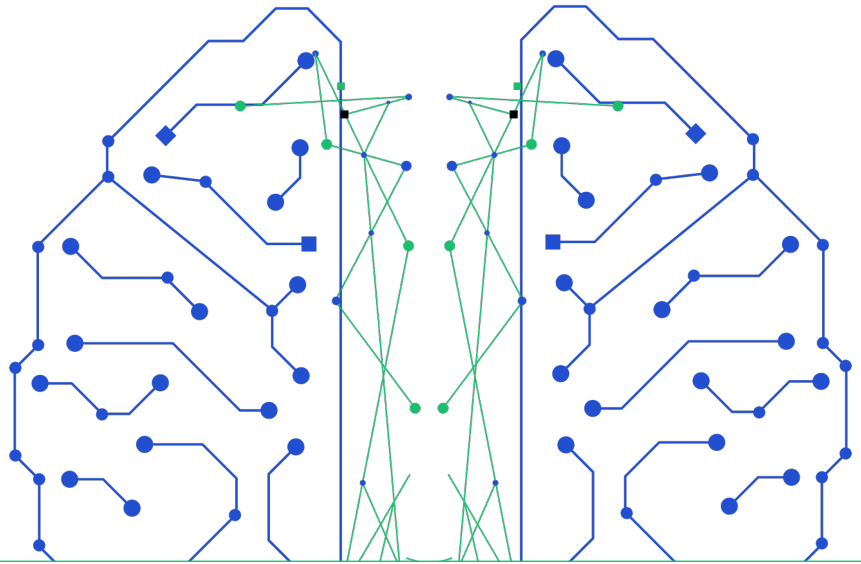# Duality

The Duality Platform

Today's data driven enterprise must harness the power of data and realize its value. However, in many cases, organizations are limited due to the complexity of their data footprint, compliance, and privacy regulation factors, as well as competitive, business policy, and budget assignment concerns.

The conflict between data utility and data privacy impacts several industries. Here is a snapshot of the problems that data-driven enterprises face today:

Budget – Organizations have limited resources for their security tools – and privacy tools, which extend beyond security and can affect multiple parts of an organization's infrastructure, can be particularly expensive.

Visibility – As organizations expand their global data footprint, it can be difficult to determine exactly where data privacy is at risk and via which activities or parts of an organization.

Ownership – Enterprises are just beginning to embrace hiring and/or assigning a privacy-specific role to monitor privacy across the organization. For many enterprises this role has been spread out amongst multiple professionals, leaving a severe gap in ownership for handling data privacy issues as they arise.

Lack of Urgency – Like in many security-related issues, data privacy often is a non-issue for business professionals until problems arise – whether it be an issue of a breach or navigating the complex world of regulatory compliance.

Here are a few examples of how those conflicts play out in different industries and use cases.

Fraud and Cybercrime
Detecting scams, fraud, and cybercrime requires cooperation and information sharing, not only across financial services organizations, but sometimes between branches of the same organization.

Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF)
Tracking funds requires inter-institution cooperation, which may not be possible due to any number of data localization laws and internal regulations, as well as competitive concerns.

Healthcare Providing more accurate statistics through Real-World Evidence (RWE) gathering or building better machine learning models drives the development of more effective drugs and treatments but requires large and varied pools of patient data that are normally difficult to access due to various national and international patient confidentiality laws.

Co-Marketing, Personalization, and Open Banking Personalizing the customer experience and optimizing marketing programs means enterprises and their partners must collaborate on sensitive data, yet privacy concerns and/or regulations typically prevent this.

> **Additional utility and privacy conflicts are sure to rise in the next decade in nearly every regulated industry. Resolving these conflicts will be a major determinant of business growth.**

## Unlocking the Power of Data with Collaborative Computing

Duality enables multiple parties to securely compute sensitive data while preserving privacy, confidentiality, and regulatory compliance.

Our applications – Query, Analytics & Machine Learning, and Collaboration Hub — enable enterprises to run descriptive statistics; train, tune, and deploy AI/ML inference models; and deploy SQL-like queries, all while using encrypted data or models. Securely collaborate with partners in any environment to unlock the value of your data, drive revenue, and amplify efficiency across your organization.

Best of all, Duality seamlessly integrates with existing systems so you can set up collaboration projects quickly and at scale.

How Duality Works

Our technology leverages cryptographic methodologies that support several Privacy-Enhancing Technologies (PETs). PETs allow complex computations on data while the data or the model itself is encrypted, without ever revealing more than the computational result.
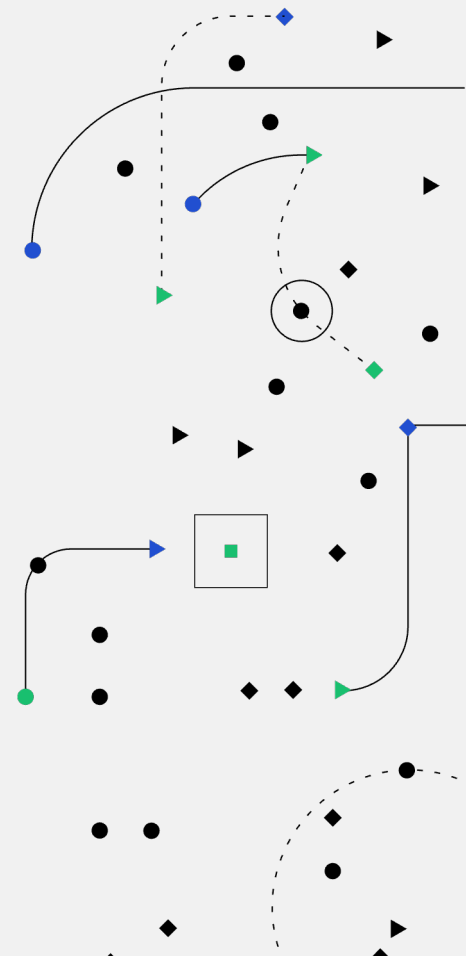
According to Gartner **60%** of large enterprises will be using privacy-enhanced computations by 2025.

Duality combines multiple PETs with cutting-edge data science

to allow anything from basic computations on encrypted data to training and inference of machine learning models. How it works:

1. User at Bank A encrypts query and sends to Hub
2. Hub distributes masked and encrypted query
3. Encrypted query runs against each bank's database
4. Results remain encrypted and are returned to Hub
5. Hub aggregates and produces encrypted results or anonymizes encrypted results
6. Anonymous results returned to Bank A
7. Bank A decrypts responses and takes appropriate action

7 Results decrypted and actioned

BANK A
BANK F
BANK B
BANK E
BANK C
BANK D

5
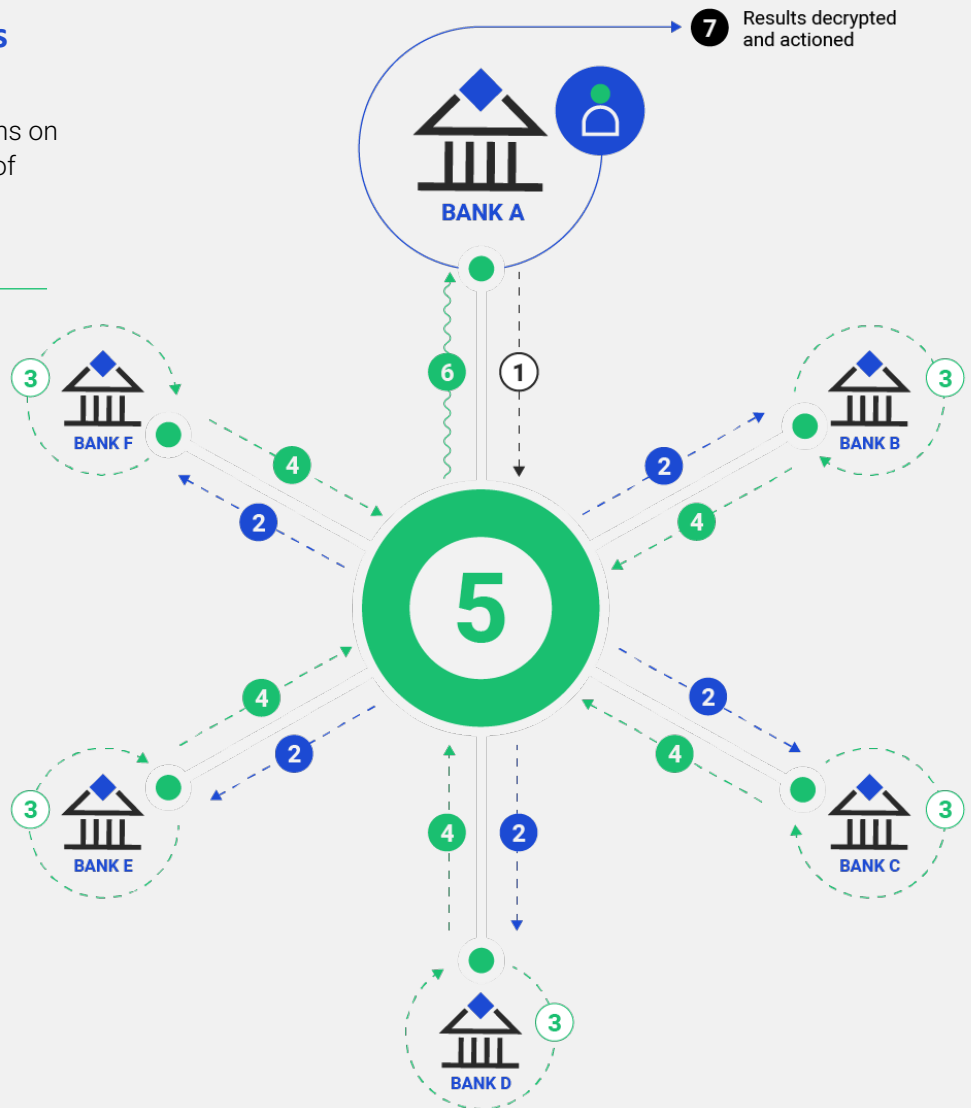
Features

Analyze Encrypted Data
Encrypt and link disparate data sets to train and tune models or deploy analytics on aggregated data - without exposing the underlying information to third parties.

Deploy Encrypted Models
Encrypt and deploy models and queries on decentralized data sets - while keeping them secure and protected from reverse engineering.

Manage Collaborations
Set up and manage your own secure collaboration network to enable your customers and partners to securely collaborate with one another. Or share data between two parties for analysis, while keeping the data encrypted.

Easy Integration and Deployment in the Environment of your Choice
Seamlessly integrate with your data assets and infrastructure using the Duality RESTful API and Python SDK and deploy on the cloud or on premises.

Benefits

Enterprise-Grade Performance and Scalability
Utilize the latest advances in cryptography and data science to compute on data and get insights as you need them, instead of waiting weeks and months for lengthy and cumbersome legal and business processes.

Full Compliance with Global Regulations
Leverage data while complying with global privacy and data regulations like CCPA, GDPR, HIPAA, GLBA, and more.

End-to-End Control
Control your projects from end-to-end, including collaboration roles, data, models, and computations.

Post-Quantum Ready
Protect your data and models while in use with scalable, standardized and quantum-safe fully homomorphic encryption (FHE).

" **Duality has enabled us to fully leverage the data in our extended client and partner networks. We are now able to open new lines of business in a variety of industries - all for the greater good of our customers, and all without infringing on their privacy or their rights."**

Hiroyuki Yamanaka
Manager of the Data Secure Team, NTT DATA

Applications

Our platform can support all aspects of data sharing across any vertical, enterprise and infrastructure. Conduct secure queries, collaborate for analytics and machine learning on a pooled data set, and/or set up a privacy preserving information sharing network for your partner and client ecosystem.

Query
Securely share insights by performing privacy preserving queries on decentralized data sets.

Analytics & Machine Learning
Train and use machine learning and other computations using encrypted data and models.

Collaboration Hub
Create and manage your own privacy protected network.

Leverage Duality to run the specific data science operations your organization needs.

Query

Looking to ask specific questions about a particular person, project, or data point without exchanging PII or other sensitive data? The Query application enables your organization to derive insights with specific partners or collaborators without violating data localization, confidentiality, or privacy laws.

Multiple organizations can collaborate on decentralized data by performing privacy-enhanced SQL-like queries. Query parameters and results remain protected by homomorphic encryption, and underlying data never leaves the owner's environment.

The Query Application provides cooperating parties with a set of tools to define collaboration projects and controls, such as user roles, authorized queries, approval processes, data policies as well as the ability to flexibly create custom queries using the out-of-the box query builder. Queries can be deployed to single parties or many parties at the same time - there are a variety of collaboration and deployment options to fit your needs.

Highlights

Get access to data faster, without lengthy legal processes or manual intervention.

Deploy custom-built or predefined queries on decentralized data sets.

Collaborate with partners of your choosing or join an existing collaboration network.

Ensure regulatory compliance and retain full control over your data.

Use Cases

Financial Crime and Compliance Collaborate across organizational boundaries to better detect, prevent, and investigate financial crimes

Cybercrime Information Sharing Securely share information with your peers to mitigate cybercrime threats

Sensitive Investigations Enable law enforcement agencies to engage in confidential and privacy protected investigations

Client onboarding Collaborate with your peers to reduce client friction and resource duplication, and make onboarding decisions faster

Data Monetization and Consumption Access new high-value data sets in a privacy-protected and compliant manner

Analytics and Machine Learning

Duality Analytics and Machine Learning provides a collaborative analytics application which enables organizations to compute using pooled or decentralized data without revealing sensitive information, PII or IP.

With Duality, organizations can utilize a variety of data science, statistics, and machine learning and AI models while ensuring privacy throughout the analytics lifecycle. Companies can choose to work with encrypted data or encrypted models; run analytics or train and tune models; easily configure and control which data and models are used and ensure that every party remains in control of their owned assets, no matter in which environment they are computing.

Highlights

Securely generate insights by deploying encrypted analytics models or analyzing encrypted data.	Analyze large-scale data sets and get answers faster - without lengthy manual processes.	End-to-end control for your collaboration projects -- including roles, data, and models deployed.
Deploy custom-built or predefined computations.	Deploy statistics and models built on a variety of ML algorithms, such as regression and decision trees.	Ensure compliance with industry and privacy regulations -- including GDPR, CCPA, HIPAA, and more.

Use Cases

Data Monetization - Create new revenue sources from data analysis without compromising privacy and regulatory compliance.

Co-Marketing and Personalization - Deliver personalized customer experiences and upsell with partners while preserving privacy.

Secure Transitioning to the Cloud - Protect sensitive data and models while transitioning AI workloads to the cloud.

Model Training, Testing and Validation - Train, tune and validate AI and ML models on sensitive data without exposing it.

Cross-Border Data Analysis - Work collaboratively across borders while meeting data privacy and residency requirements.

Medical Multi-Center Studies - Analyze sensitive medical data across centers to gain deeper insights and to speed research and discovery.

Real-World Evidence (RWE) Studies - Access real patient data to better determine the effectiveness of different drugs and treatments without violating national and international patient confidentiality laws.
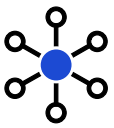
Collaboration Hub

With Duality's Collaboration Hub, organizations can now build and manage their own privacy protected networks -- allowing their partners and clients to work together to share intelligence, build new products and services, and monetize their data, while keeping privacy and confidentiality top of mind.

This 'privacy-protected network as-a-service' offering enables organizations to add value to their customers and partners by providing innovative collaboration services aimed at driving new revenues and reducing churn.

Customize your Collaboration Hub to meet your network's specific needs - whether that's by type or number of computations, level of anonymization, data schema, or more. And do it all without falling into the "data processor" categorization under GDPR and other privacy laws.

Highlights

Collaboration without collusion: Enable members to collaborate on sensitive data through your Collaboration Hub, without exposing the underlying data.

Combined insights: Aggregate results to provide a coherent and valuable network-level response.
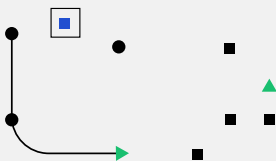
Manage roles: Each member may initiate computation requests, serve as a data provider, or both.

Scale and adapt: Easily add new computations and collaboration models as your network grows and your needs change.

	Query Application	Analytics and Machine Learning Application	Collaboration Hub
Leverage open-source and standardized encryption	x	x	x
End-to-end control for -- including roles, data, and models deployed	x	x	x
Ensure precise, accurate results	x	x	x
Ensure compliance with data privacy and industry-specific regulations	x	x	x
Analyze decentralized data sets	x		x
Analyze pooled data		x	x
Leverage ML, AI, and other data science model library		x	
Leverage Descriptive Statistics Library		x	
Leverage SQL-like query library	x		
Maintain anonymity of analyzers and data owners			x
Build and manage collaboration networks for your clients and partners			x
Route, aggregate, and analyze encrypted data for networks			x

Schedule a Demo