Confidential ML Training

We change how the world accesses data

Sensitive data is a valuable asset and a reputational risk for companies. Accessing data is fundamental to the AI revolution, but it is still gated behind inefficient processes that add complexity and increase the risk of data breaches. These risks prevent access to the world’s most valuable datasets. We are changing this. We are making data collaborations simple and safe.

Confidential ML Training enables you to train machine learning models based on data that nobody ever can access; not you, not us, not the infrastructure provider, nobody. This removes the risk for data breaches or data misuse.

Unlock new data and protect it at all times

We make accessing previously unattainable data an effortless process. We make developing models on any data without worrying about confidentiality seamless. Data is kept confidential and private at all times.

Minimize the risk of data leakage while taking full advantage of the underlying data value. And all this, without changing your workflow.

How we do it

Powered by Confidential Computing we employ the latest advancements in cloud computing and cryptography to enable a new way to interact with data. Our technology ensures that data is protected at all stages of the data science workflow from keeping it safe at rest, at transit and even during computation.

Technical specs in a nutshell

- Python API resembling Scikit-learn that enables ingesting, encrypting, and training on the data.
- Linear based models with limited scope hyperparameter tuning
- Attestation service that validates that everything runs encrypted in the cloud

Future plans

- Supporting all commonly used ML algorithms
- Privacy-preserving data exploration through synthetic data generation

About decentriq

We change the way we see data. For the first time, we make possible using Machine Learning solutions on sensitive data without any security or confidentiality compromise.

Based in Switzerland and members of the Confidential Computing Consortium, we work with enterprise customers to make sure that every company uses their most sensitive data; safely, scalable, and seamlessly.

To read more about us visit www.decentriq.ch

Contact us for a demo at info@decentriq.ch