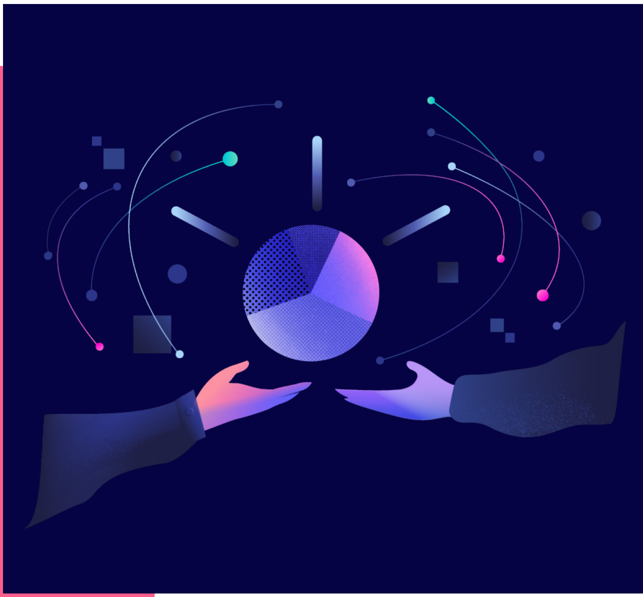
Cape Privacy



Better data science results through encrypted learning.

Encrypt sensitive data for the most impactful AI.

4 min. read

AI, specifically machine learning and data science usage have seen huge adoption in recent years. However, the presence of proprietary, confidential and sensitive data in many datasets represents a barrier for companies to fully realize the value of their AI strategy. Many applications including financial investment platforms, drug discovery analytics and medical diagnosis systems are currently siloed at different institutions or between departments. With Cape, companies can benefit from secure and trusted access to all data to create more powerful AI solutions. Furthermore, Cape uniquely achieves collaborative machine learning without exposing any confidential data.

Advancing AI through collaborative privacy-preserving machine learning

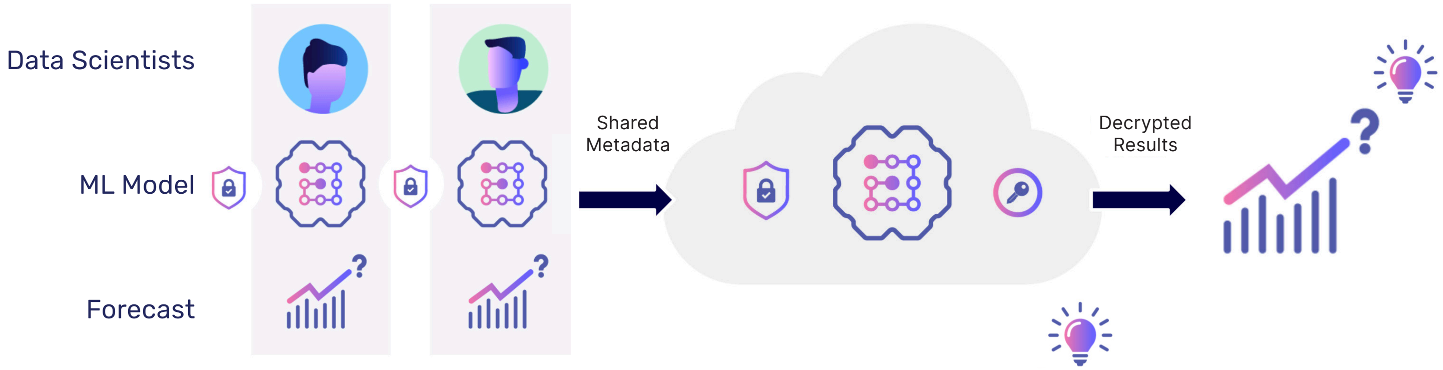
A shift has already happened from a single data scientist having a local copy of the entire data set, to data scientists working with data lakes governed by distinct data owners. This will continue where a typical data science task will involve the collaboration between one or more data scientists, as well as one or more data owners, in the pursuit of advanced applications; for instance, model training. In other words, data science and machine learning are on a natural progression toward a more collaborative process between parties.

Powered by core technologies, such as federated learning and encrypted learning, Cape Privacy tackles this increasing need by providing the framework and tools needed to address the entire data science workflow. Furthermore, Cape makes secure collaborative machine learning more accessible by integrating with existing data science ecosystems.

FINANCIAL SERVICES USE CASE

Generating alpha using confidential computing

- Financial Services Company A wants to collaborate on a data science model with Financial Services Company B.
- Today there are numerous organizational constraints preventing the two companies from collaborating on model development (including, but not limited to regulatory, security and competitive reasons).
- As a direct result, both companies yield improvement to their individual models which in turn generates in the order of $MM (potentially $B) in business value creation.
- By leveraging Cape's Encrypted Learning features, the two companies are able to collaborate without exposing any confidential data and without sharing their individual models. Cape is able to securely encrypt each company's data at the source and only share a decrypted results (without ever breaching any confidential or sensitive information to either party of the individual inputs).



Individual Model accuracy limited by the depth and breadth of a single organization.

Increased Model accuracy through collaboration yielding $MM/B in potential value creation.

Cape Privacy

Get started today

Cape's mission is to help data solve important problems without compromising privacy.

Contact us