Company Overview

Dr Ellison Anne Williams founded Enveil in 2016. Enveil was established with a vision to revolutionise data security and privacy.

Enveil uses homomorphic encryption to enable scalable, in-place data processing while maintaining privacy. It enables users to 'derive insights, cross match, and search third party data'[1] without revealing the search parameters and while respecting data ownership. The company focuses on protecting data while in use rather than while at rest and in transit[2].

Product details

Zeroreveal search – the company claims to securely search data, cross match and extract insights without revealing the search parameters or compromising the data security, working on data where it is and without changes to the data structure or existing systems[3]. It does not expand on how this is achieved, though implies that homomorphic encryption is used.

Zeroreveal machine learning – the company claims it can enable encrypted machine learning and model development using federated learning on decentralised datasets[4].

Zeroreveal compute fabric – the foundation of both the search and machine learning solutions offered by Enveil. This is what enables the processing of data without making changes to the system architecture and data structures.

Similarities to our use cases

1) Our use cases included homomorphic encryption.

Differences to our use cases

2) Our use cases considered data at rest and in transit as part of the solution, they did not isolate one aspect of the processing cycle for attention.

Enveil Partners

Thales	Terradepth	Deliverfund Commercial ops
AWS	Sayari	Novetta
Azure	Exovera	Intel

Enveil Customers

Mastercard	Refinitiv	Cyber Mentor Fund
CS Capital	USAA	iqt

[1] https://www.enveil.com/about-us/#div_block-445-14
[2] https://www.enveil.com/privacy-enhancing-technologies/
[3] https://www.enveil.com/products/
[4] https://www.enveil.com/products/

Bloomberg BETA	Capital One Ventures	Thomas Reuters

PTFI viability in replicating products or services:

Our team could realistically develop a method to use homomorphic encryption (HE) to replicate some of this company's services. We have demonstrated the ability to employ HE; however, we might lack the infrastructure to test machine learning and model development in a realistic fashion. We could certainly attempt to a more limited feasibility test to prove our ability to replicate a product.

Company overview

Secretarium pitches technology to enable digital service providers to 'capture valuable insights' without an intermediary[5] by using secure enclave distributed ledger technology which it touts as being orders of magnitude faster than homomorphic encryption[6].

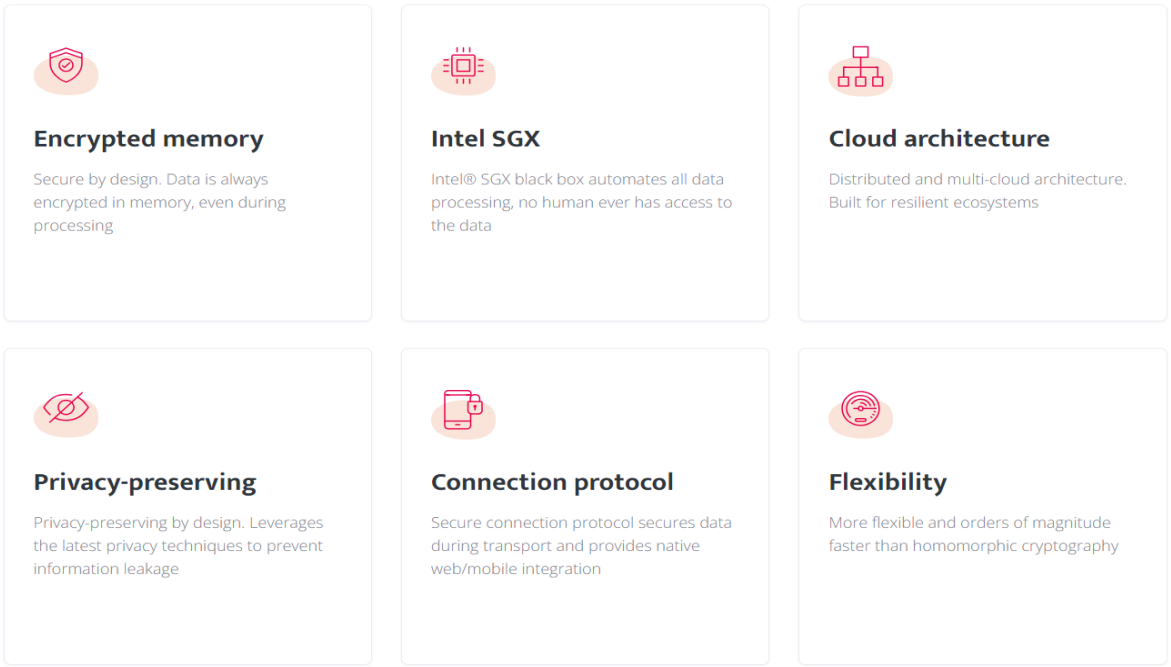
Product details

The technology appears to rely on sophisticated encryption and privacy techniques which protect the data until it is decrypted in a secure enclave where operations are performed before the results are encrypted and provided to selected participants.

The website claims that data is always encrypted, even during operations, but does describe it being decrypted within a secure hardware enclave during operations.

The product uses an SDK and API to make its service available to users.

Secretarium services enables organisations to use their technology to collaborate while keeping data safe. Secretarium provides privacy-first data commoditisation. It combines cryptography and secure hardware. Secretarium provides the services below:



Source: https://secretarium.com/technology

Secretarium platforms:

- **Klave:** An easy-to-use network for developers to build and deploy trust-less applications.
- **Amlytic**: A secure multi-party transaction data pooling tool for financial institutions.

[5] https://secretarium.com/about
[6] https://secretarium.com/technology

- **Datalign**: A data quality and benchmarking reconciliation engine.
- **Semaphore**: A real-time solution for KYC, AML, and fraud detection in the financial services industry.

Similarities to our use cases

1) Enables collaboration across different participants to process data and gain insights; this could include a matching operation or data science techniques. If the data is decrypted and then operated on in a secure hardware environment, the possible operations are likely to be unrestricted, unlike when using homomorphic encryption.

Differences to our use cases

1) Our use cases did not foresee the use of secure hardware enclaves as a tool to enable efficient privacy preserving operations.
2) Our use cases did not require a private intermediary company to enable information sharing and operations on data. [this company claims no intermediary is required but seems to be functioning as an intermediary between participants].

Secretarium Partners

IQ Capital[7]	Societe Generale[8]	Intel
ANZ[9]	Capgemini	Swisscom[10]
Thales	UK Research and Innovations	

[11]

PTFI viability in replicating products or services:

Our team could probably replicate a model of a secure enclave in software, but certainly wouldn't have the resources or expertise to replicate it in hardware. Developing an API to transmit and securely deal with encrypted data prior to processing inside a secure, though unencrypted, environment would be an option for the team.

[7] https://iqcapital.vc/secretarium-receives-5m-seed-investment-from-iq-capital-and-emerges-from-stealth-mode/

[8] https://www.securities-services.societegenerale.com/en/insights/views/news/reinventing-confidential-intermediation-with-secretarium/

[9] Maintaining digital payments in an offline world (anz.com)

[10] Exchange of confidential commercial documents | Swisscom

[11] https://iqcapital.vc/secretarium-receives-5m-seed-investment-from-iq-capital-and-emerges-from-stealth-mode/

Company overview

Duality Tech markets privacy preserving technologies to organisations in financial services, healthcare and government sectors.

Product details

Query engine – the company claims its duality query engine can perform SQL-like queries which are protected via homomorphic encryption; both the parameters and results[12]. It allows the data to remain in the owner's environment. It has additional controls to define and enforce policies approval processes, user roles and query types.

The product is built to mimic the functionality of SQL while including an algorithm which will enable fuzzy matches of names and addresses.

The product describes its method as a 'zero footprint investigation'[13]. It requires cooperation between the investigator and the data owner, it encrypts the search query, runs matching against the target dataset while encrypted, encrypts the results and returns them to the investigator. The demonstration on Duality Tech's website suggests the search queries are limited to full name and address, with a fuzzy matching capability.

The product is available via API and on AWS marketplace; it appears to also have a web-based interface.

Similarities to our use cases

3) Collaboration across organisations to detect, prevent and investigate financial crimes[14] using a match function for name and address selectors.

Differences to our use cases

3) Includes fuzzy matching capability.

[12] https://dualitytech.com/platform/duality-query/
[13] https://play.vidyard.com/jdqLFSHSvVaXBUm7qpAfuY.jpg
[14] https://dualitytech.com/platform/duality-query/

4) Does not foresee a public intermediary as a hub for information sharing, but rather decentralised opt-in fully encrypted data matching where private entities can query each other's data without revealing their query[15].

Duality Tech Partners

IBM Collaboration Hub	Oracle	Google
Intel	IBM	

Duality Tech Customers

AWS	IBM	Deloitte
Azure	Intel	DARPA
Google	Oracle	

PTFI viability in replicating products or services:

We could probably replicate this functionality using the results of experiment 01 from this trimester. The SQL-like functionality would probably be possible using the Pyfhel operations (-+*). Other python libraries might be better suited to this task though, so some effort would need to be expended on researching alternatives and benchmarking these against the performance in experiment 01 using Pyfhel for HE.

[15] https://www.youtube.com/watch?v=qKReJTqUq18