Proposition Summary

In an era of unprecedented data volumes (much of it personal and sensitive), increased data privacy regulation (GDPR, HIPAA, CCPA etc.) and frequent high-profile data breaches (Equifax, Google+, Cambridge Analytica etc.), there has never been a greater need for companies who handle user data to employ the industry's most robust data security solutions. Data leaks and hacks can take a number of forms. Many are a result of human error, some are due to poorly architected technology but, most importantly, all are preventable. Data exposure can be devastating to companies that are affected. The 2017 Equifax hack which leaked personal information belonging to over 145 million users led to a financial loss of USD$439 million, the most costly data breach in corporate history[1]. Companies recognise that data privacy and cybersecurity is a major risk but there are currently no cohesive solutions to the problem available on the market. Evervault leverages novel on-chip security technologies, coupled with secure rendering technology, to ensure the integrity of encrypted data and allows companies to process personal data without seeing, storing or handling it through simple developer tools that are easy to implement and scale, fast. If companies were wishing to build this functionality themselves, they would need deep in-house technical expertise from browser-level through to chip-level.

Technical Implementation

Evervault utilises the new enclave functionality of Intel's Software Guard Extensions (SGX). SGX is a set of central processing codes that allow the allocation of private regions of memory, called enclaves, that are protected from processes running at higher privilege levels. Data is never decrypted until it is held safely within the enclave and as such, there is no risk of an individual's data being stolen. Malicious actors with physical or admin access on an SGX-enabled node are unable to observe processes within a secure enclave. This is of particular relevance for sensitive processes running in a shared environment such as a public cloud, for example, AWS, Google Drive or Microsoft Azure. These technologies are still in their nascent stages, with the first publicly available cloud SGX platform released in October 2018 by Microsoft Azure. Evervault is built on top of Microsoft Azure. Our platform allows for easy integration of similar processor-based privacy-preserving technologies such as AMD's Secure Encrypted Virtualization or ARM's TrustZone once ready for production use. This is a particularly exciting opportunity and opens up a wealth of new application opportunities given the prevalence of ARM chips in mobile phones and other embedded devices.

[1] Reuters: "Equifax breach could be most costly in corporate history"
https://www.reuters.com/article/us-equifax-cyber/equifax-breach-could-be-most-costly-in-corporate-history-idUSKCN1GE257

Evervault also provides a novel *Secure Rendering* technology that allows sensitive information to be displayed in a secure manner within isolated browser elements, powered by a new HTML5/JavaScript primitive known as Shadow DOM. Originally built for isolating individual components from the rest of the webpage and third-party scripts for browser video players, the developer APIs have since been exposed to developers. We are the first company to use this technology for secure data display. With this approach, malicious companies or developers are entirely separated from the secure elements making it impossible to retrieve the sensitive data and transfer it to an unsecured third-party server, for example.

Client Integration Steps

1. Create account on Evervault where they will be issued API keys
2. Include Evervault SDK in their web application source code
3. Isolate sensitive data processing components of application and deploy to Evervault secure enclave (e.g. the quotation algorithm in an insurance broker use case)
4. Create Results Returned function within application (e.g. return quotation to end user)

Strategic Positioning

While there are multiple cloud storage companies as well as specialty data security companies, there are none who are currently offering end-to-end (enclave to browser), turnkey solutions for ensuring that there is BIOS-level separation between encrypted data and the encryption key. Evervault will launch this service in Q3 2019. In practice, this means that even if the network is compromised (including through hardware-based attacks), the encryption key remains completely hidden. Unauthorised access to the encrypted data can therefore be prevented entirely.

Product

The Web Platform will enable a new paradigm in Artificial Intelligence and Machine Learning, allowing corporations and research organisations to build models for solving major world problems that are highly data-dependent, including cancer research and DNA sequence analysis. The Web Platform will enable consumer facing companies collect, process and securely return sensitive information.

Example Use Cases

Industry	Use Case	Example Company
FinTech	Secure import of customer transaction history	Challenger Banks (Revolut, N26, Monzo)
Insurance	Secure end-to-end data capture of temporary and sensitive customer information for policy pricing	Insurance Broker or Price Comparison Website (CompareTheMarket.com)

Finance KYC	Regulatory compliant gathering of Know Your Customer (KYC) PII	Brown Brothers Harriman (BBH)
BioMed	Secure processing of high sensitivity Personally Identifiable Information (PII)	TBD
AI / Machine Learning	Secure processing of commercially sensitive IP	TBD
Ride Sharing	Anonymised processing of aggregate customer data e.g. location/time trends	Uber, Lyft