StrongSalt Platform

strongsalt.com

Whitepaper Summary
V2.0

Table of Contents

Intro

We believe that everyone is born with the right to privacy. Privacy is what makes us unique, what makes each of us an individual person.

Unfortunately, the two biggest hurdles to privacy are the proliferation of business models that rely on targeting users and the technical challenges of providing usable privacy-preserving apps. We believe that business models can and will evolve as people care about and demand privacy so we will focus on the latter challenge. Even though we are starting with a much smaller platform than existing cloud platforms, we strongly believe that privacy focused apps will be bigger, many times bigger, than traditional apps in the near future because privacy is fundamentally a horizontal need. We call this new paradigm StrongSalt; A *strong* dose of *salt* that makes encryption more secure and more usable.

With your help, StrongSalt will build a world-class privacy-focused app platform. By laying the foundation of how apps can be built without infringing on user privacy, StrongSalt will power the future of app development so that all apps and enterprise applications be built with privacy as the default.

> In cryptography, a **salt** is random data that is used as an additional input to a one-way function that "hashes" data, a password or passphrase. **Salts** are used to safeguard passwords in storage.
>
> https://en.wikipedia.org/wiki/Salt_(cryptography)

Problems

Privacy is currently unachievable without significantly impacting usability.

As more and more data are either entrusted from individuals to companies or from on-premise to the cloud, more private data are being seen by more third parties and other automated systems than ever before.

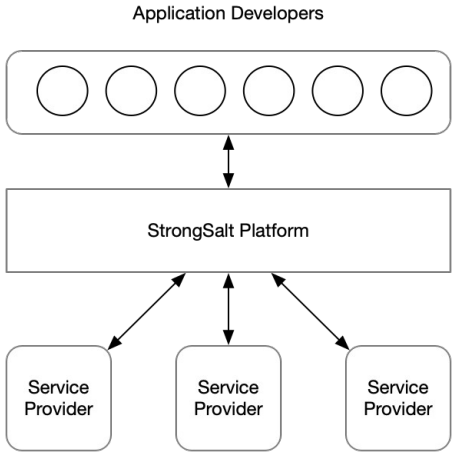
On paper, encryption could have been the perfect tool for both security and privacy, but encryption makes it impossible to analyze, search, or process data. As such, companies and cloud providers are forced to rely on ineffective "wall-and-alert" model to protect data as evident by the increasing rate of data breaches.

Bring-your-own-key solutions don't work either because big or even small data requires the ability to search and understand data. Not only are academic approaches such as multi-party computation or homomorphic encryption simply too slow, but also comparing to the advances in searching and data processing in general, almost all solutions for encrypted data are frankly unusable in real-life situations.

StrongSalt Platform

> "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it."
>
> Mark Weiser

StrongSalt platform is an app platform where app and enterprise application developers can develop privacy-focused applications that can manipulate data which is secured by "always-on" encryption, as if such data were unencrypted. Such capability has never been possible without the advances of cryptography and decentralization in the last decade.



Searchable Encryption

Searchable encryption is a cryptographical way of structuring data so that data can be searched while encrypted. StrongSalt focuses on performance and usability, which are two of the most difficult problems of searchable encryption.

Sharable Searchable Encryption

StrongSalt shareable searchable encryption combines searchable encryption with a cryptographical way of managing keys so that the data can be shared and restricted to the exact recipient(s) along with the ability to search the shared data.

Decentralized Searchable Encryption

StrongSalt searchable encryption is decentralized so that much of the searchability is available offline, while providing enhanced experience online.

Decentralized Object Store

StrongSalt provides an object store storage abstraction to present a uniform interface to cloud, on-premise, or even other decentralized storage clusters. StrongSalt will take care of chunking, erasure coding, and consistent hashing to fully realize the benefits of decentralization.

StrongVault

StrongVault is the first ever encrypted file-sharing and group messaging app with searching and sharing that is as easy as normal unencrypted apps. The target users are privacy-minded individuals or professionals working in a privacy-focused enterprise.

StrongVault reimagines encrypted application by demonstrating how privacy-focused apps can offer the superior usability while providing unparalleled security and privacy on the StrongSalt platform.

A user of StrongVault does not need to register with username, password email, phone number or any other personal details with StrongVault because the app does not create or maintain any online profile in the backend. All data such as file content, messages and all metadata are encrypted by default. However all encrypted contents can be searched via StrongSalt Searchable Encryption. StrongVault also demonstrates the ability to have image recognition capability on encrypted images.

StrongVault also showcases the first ever real-world use case of a blockchain by allowing any user to view directly in the app all events associated with their files. The platform continuously monitors the data so that any event that happens are recorded.

Release Rollout

We are launching StrongVault Individual as the first app on the StrongSalt AppStore first.

Soon after, we will launch StrongVault Team for professional teams needing additional team collaboration, enterprise integration, device management, and security features.

We are also releasing the StrongVault API as the first API service to enable other developers to build apps on the StrongSalt platform.

In the future, we will add more API services such as machine learning and natural language processing that can work on the encrypted data pipeline offered by the StrongSalt platform.

Cross-Platform Support

We will provide cross-platform clients for StrongVault for:

- Android
- iOS
- Web-based (Mobile-first)

And in the future:

- Windows native client
- MacOS native client
- Linux native client

We will provide SDK clients for StrongVault API for:

- JavaScript
- REST

And in the future:

- GraphQL
- gRPC
- Go
- Dart
- Java
- Kotlin
- Swift

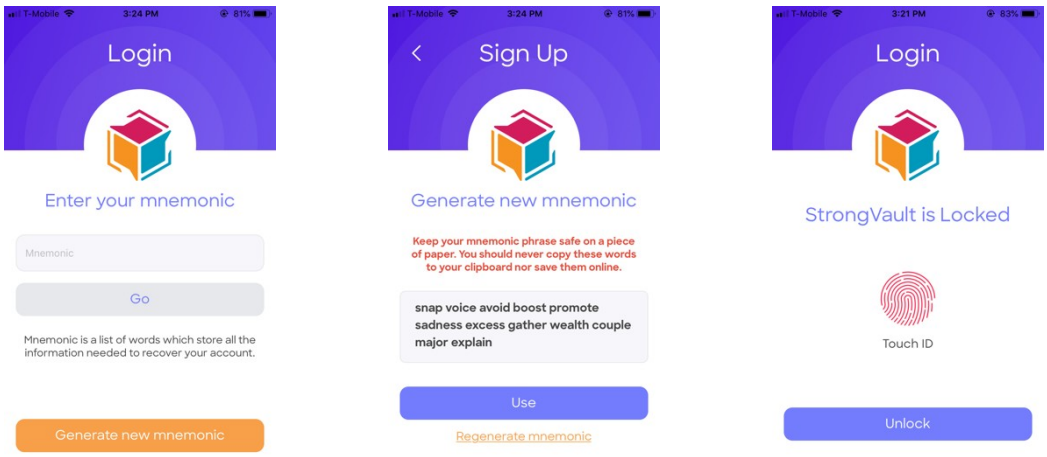
Internationalization and Localization Support

We will support English for both the StrongVault app and the StrongVault API documentation initially.

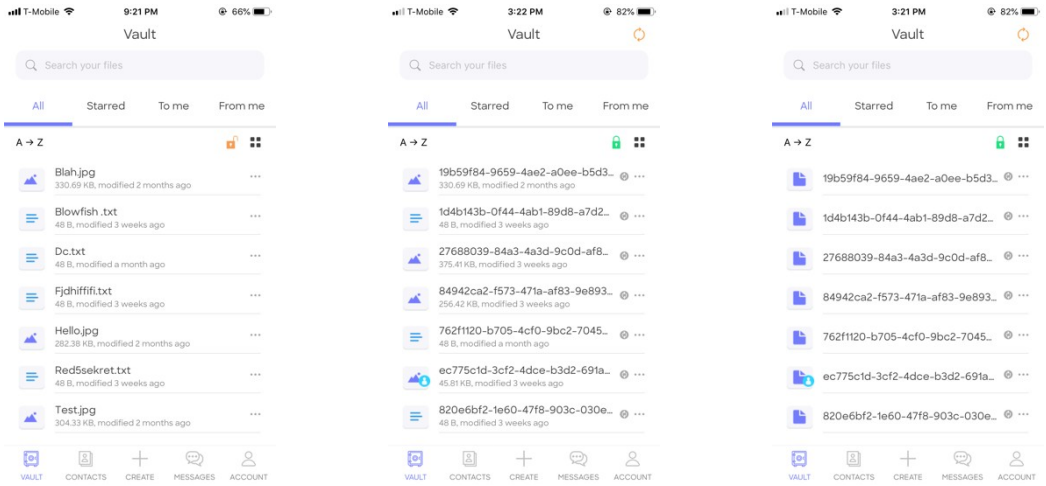
We will strive to support Chinese, Japanese, Korean and Spanish on the StrongVault app in the near future.

More languages will be added over time until we have supported at least 1 language for every privacy-minded individual and developer in the world.

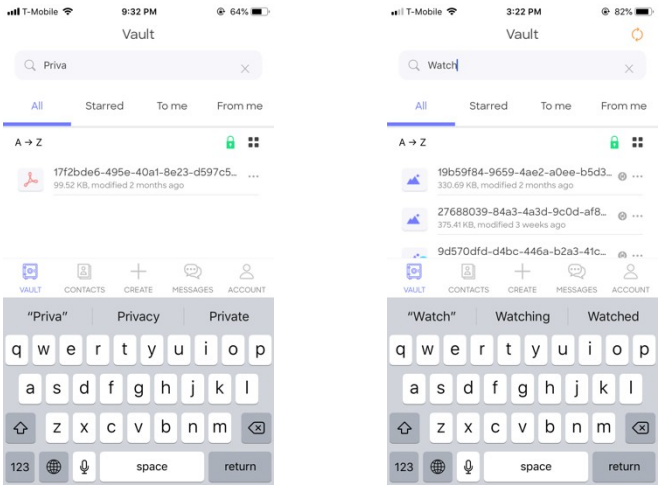
UI Preview



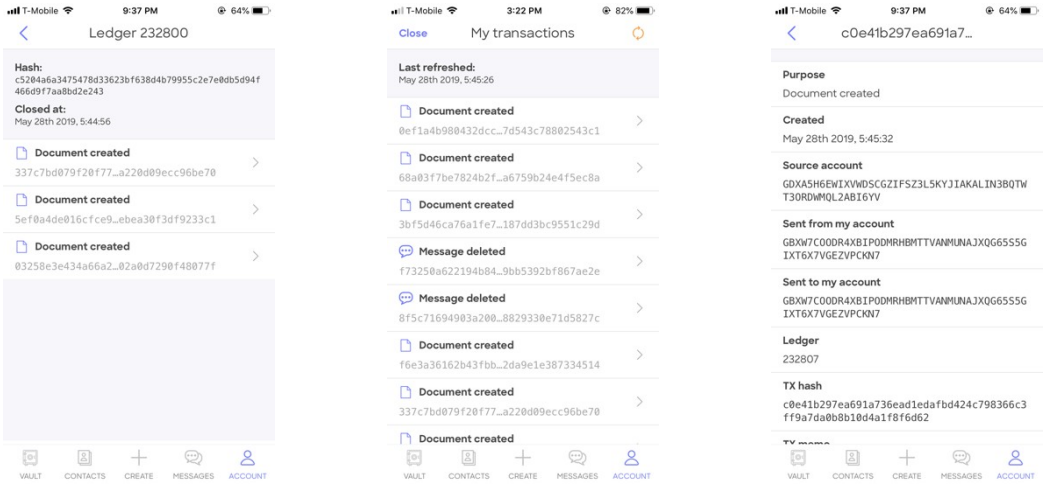
Login and Registration Screens (No Personal Information Needed)



Vault Views in Low, Medium, and High Privacy Settings



Search Screen for Encrypted PDF (and other text files) and Images



Blockchain Views

Fee Model

The fees charged by the StrongSalt platform will initially be from the following services:

Source	Description
StrongVault App	Freemium with possible additional subscription fee for power users based on usage level
StrongVault OEM	Whitebox solution for privacy-focused team-based collaboration
StrongSalt API SaaS	SaaS model for API service
StrongSalt API Enterprise Services	Consult services and support services basedConsult fees for enterprise teams for education and custom development
StrongSalt API Professional Services	Custom development based on StrongSalt API

We decided not to charge the typical developer program fees, app listing fees, or app store revenue-split because these are not in line with our vision for the StrongSalt platform. We'd like to have our token economics of the platform to be self-sustaining without charging these fees.

Team

We have a solid team lead by Ed Yu, with both enterprise and security experience. We have a track record of IPO, startup, academic, enterprise, and public sector successes under our belts.

Ed Yu – CEO

LinkedIn Profile

Ed Yu was the Founding Engineer of FireEye and has also worked as VP and Director of Engineering in various enterprise and software companies. He has worked both in startups and large corporations such as Oracle, Sun, SGI, and McAfee.

Ed graduated from the California Institute of Technology with a Bachelor's degree in Computer Science.

Ed loves cryptography and has patents on encrypted search include areas on unique searchable encryption with arbitrary index construction, zero-trust encrypted storage, and encrypted indices sharing.

Ed currently is actively working on StrongSalt with the help and collaboration of both Dan Boneh of Stanford and Matt Green of Johns Hopkins on cryptography and security.

Tony Scott – Advisor

LinkedIn Profile

Tony Scott was the third Chief Information Officer of the United States, appointed by President Obama on February 5th, 2015.

Prior to his position in the White House, Mr. Scott led the global information technology group at VMware Inc., a position he had held since 2013. Prior to joining VMware Inc., Mr. Scott served as Chief Information Officer (CIO) at Microsoft from 2008 to 2013. Previously, he was the CIO at The Walt Disney Company from 2005 to 2008. From 1999 to 2005, Mr. Scott served as the Chief Technology Officer of Information Systems & Services at General Motors Corporation.

Dan Boneh – Chief Security Advisor

LinkedIn Profile

Dan is a Professor of Computer Science and Electrical Engineering, Stanford University. Professor Boneh heads the applied cryptography group and co-direct the computer security lab. Professor Boneh's research focuses on applications of cryptography to computer security. His work includes cryptosystems with novel properties, web security, security for mobile devices, and cryptanalysis. He is the author of over a hundred publications in the field and is a Packard and Alfred P. Sloan fellow. He is a recipient of the 2014 ACM prize and the 2013 Godel prize.

Matt Green – Security Advisor

LinkedIn Profile

Matt is an Assistant Professor at the Johns Hopkins Information Security Institute. Matt's research includes techniques for privacy-enhanced information storage, anonymous payment systems, and bilinear map-based cryptography. He was one of the creators of the Zerocash protocol, which is used by the Zcash cryptocurrency.

Risks

There are many risks involved in running a successful enterprise platform business with a token model on a decentralized infrastructure. We understand this and have the skills, experience, and the team to overcome them.

Market Competition

We are the forerunner of the nascent privacy space and we do have a huge lead on the technology front. However, many of our value propositions overlap in the related security and compliance spaces, which are competitive and fragmented. In addition, StrongVault app is in the more competitive enterprise collaboration, messaging, and file-sharing space where there are already some new but successful entrants in addition to established enterprise players staking a foothold.

However, no other company combines privacy and usability the way we can either because of business model differences or the lack of technological advances. The programmable API services market is huge and expanding and our privacy-focused API is both unique and horizontal. Therefore, we can work collaboratively with almost all existing players in both the app and programmable API service spaces, and our effective addressable market is unlimited.

We believe our unique blend of vision, technology, and execution gives us an unfair advantage in the programmable privacy platform market and that our success in either the StrongVault app or the StrongVault API can compound the success of the other. We hope you can join our fight for the most basic right—the right to be an individual.