Blockchain and the new data security paradigm
Data loss: man-in-the-middle attacks & negligence

What were the most common ways in which the breaches occurred in the past twelve months?

<table>
<thead>
<tr>
<th>Data Handling</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inadvertent misuse by insider</td>
<td>36%</td>
</tr>
<tr>
<td>Loss/theft of corporate asset (e.g., backup data, server, laptop, smartphone)</td>
<td>32%</td>
</tr>
<tr>
<td>Phishing</td>
<td>30%</td>
</tr>
<tr>
<td>Abuse by malicious insider</td>
<td>25%</td>
</tr>
<tr>
<td>External attack targeting business partner/third-party supplier's servers or users</td>
<td>15%</td>
</tr>
<tr>
<td>Loss/theft of business partner asset (e.g., backup data, server, laptop,...)</td>
<td>14%</td>
</tr>
<tr>
<td>Inadvertent misuse by business partner/third-party supplier</td>
<td>10%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Injection</td>
<td>8%</td>
</tr>
<tr>
<td>Abuse by malicious business partner</td>
<td>6%</td>
</tr>
<tr>
<td>Cross-site scripting (XSS)</td>
<td>5%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>2%</td>
</tr>
<tr>
<td>Don't know</td>
<td>8%</td>
</tr>
</tbody>
</table>
Migration to Cloud poses security challenges

Target Industries

- Large Corporations
  - Banks & Fintechs
  - Custodians of crypto exchanges
  - Mobile phone operators
  - Insurance
  - Government agencies & defense
  - Medtech & health
  - Legal firms

- GDPR Compliance
  - SMEs
  - Individuals

Enterprise Data Security

High Growth Market

- Migration to Cloud
  - Enterprises are moving to Cloud
    - CAGR 24% Cloud computing market
  - Creating the need for the next generation security

- Cyber security market
  - $248bn by 2023

- Cloud storage market
  - $207bn by 2026

KEYBOX
Cyber criminals want to get your data …

… like sharks they are ready to attack

Seals are smart, seals are agile, …

… but a shark can catch a seal with one bite
However a shark can’t attack a whole shoal of fish at once

- Safety in being dispersed
- No single point of attack
Data dispersed into fragments using DLT

Keybox splits data into multiple “fragments” – each containing no decipherable data and guaranteed unique by differential consensus (a property of Activeledger DLT)

1. The fragments are distributed across a decentralized network of private nodes
2. X of N fragments required to recreate the data (in-built redundancy and resilience)
3. Data can only be accessed through the recombination process via smart contracts
Keybox protects by fragmenting data

1. Alex adds a file to Keybox on his machine

2. Keybox sends data fragments to cloud servers

3. Belinda uses her private key to recombine the file with Keybox on her machine

- Total protection against man-in-the-middle attacks
- Safe data storage and sharing on the cloud (anti-snooping)
- Immutable data access logs + AI-powered anomaly alerts

Every fragment is undecipherable alone
Typical enterprise data use cases

- Securing PSD2 / Open Banking **data exchange** with third parties
- Sharing **AML and KYC** data
- **Securing and recovering** access keys
- Secure GDPR **compliant storage** of client & employee data
Decentralised data storage + immutable access management

This is Sheila. She needs to decide where all her company's medical records will be kept. She knows The Cloud is essential from cost, scalability, and support angles, but she can't sacrifice security. She has concerns about her data may be snooped on with a 'big name' cloud provider.

A cloud provider
Off-shoring data reduces local storage risk, but only if cloud security is set up really well; Sheila will require expensive consultants to do this for her.

Keybox decentralised cloud storage
Using Keybox to split regulatory-sensitive data across multiple Cloud providers, in a cryptographically secure way, makes it almost impossible for cyber criminals to steal.

Keybox removes snooping risk as no data is readable on any fragment on any server. Sheila chooses Keybox to certify compliance on her medical records, and to allow her business to innovate services and grow revenue without fear.

Sheila chooses Keybox for greater data security.
Technology: old and new

We use tried and tested security algorithms, such as Shamir’s Secret Sharing, and apply them using Blockchain distributed ledger technology.

We focus on usability (API, SDK) and user experience (App) to deliver enterprises a seamless experience in securely managing their data.

Keybox is built on a proven permissioned distributed ledger (Activeledger) which has several unique advantages over other existing blockchains, including territoriality, scalability and interoperability.
Benefits of distributed data storage

- **Improved Immunity to Attack and Increased Resilience via Data Fragmentation and Distribution**
- **Territoriality:** Guarantees compliance with regional/local data regulations (e.g., GDPR)
- **Software-based solution means real-time access and scalability:** No HSM needed
- **SDK’s and API’s:** Enable *vault as a service* for enterprise without changing existing infrastructure
- **Smart contracts:** Guarantee that each data fragment is unique and enable full access controls & audit trail
Blockchain powered data security

Enterprise Focus

Centralized

Decentralized

Consumer Focus

SILO
Fidelity
DIGITAL ASSETS
METACO
SWISS CRYPTO VAULT
CURTODIGIT
xapo
Vontobel
Gospel
Vault
Unbound

Centralized

Decentralized

MyEtherWallet
Ledger Wallet
Mycellium
EXODUS
keep key
sia
IPFS
afekee
Filecoin

Centralized

Decentralized

Blockchain
Jaxx
Trezor
DEFIenity
STORJ
Safety in being dispersed
Contact

Alain Falys
alain@keybox.co
+44 7825 46 9090
keybox.co