



Sapherbox

SECURITY OVERVIEW

Your documents stay yours. Even from us.

How Sapherbox protects your files, who can see what, and what that means for your organisation. Written for decision makers; technical detail is available to your security team on request.

DOCUMENT

Security Overview · Version 1.2

DATE

October 2026

AUDIENCE

**Management, procurement, data
protection officers**

ORGANISATION

Sapherbox

• **PUBLIC — MAY BE SHARED FREELY**

Sapherbox

Security Overview

Sapherbox is a document platform for organisations that need to know exactly who can read their files. Every document is encrypted on your own device before it is sent anywhere. What reaches our servers, and what sits in storage and in backups, is ciphertext that we cannot open. We hold no key that could open it, there is no provider backdoor, and there is no recovery key on our side. The only recovery path is an escrow key your organisation can create and keep itself. All of this is designed to withstand not only today's attackers but also the quantum computers of the coming decades.

"Not just a policy that says we won't look. A design in which we can't."

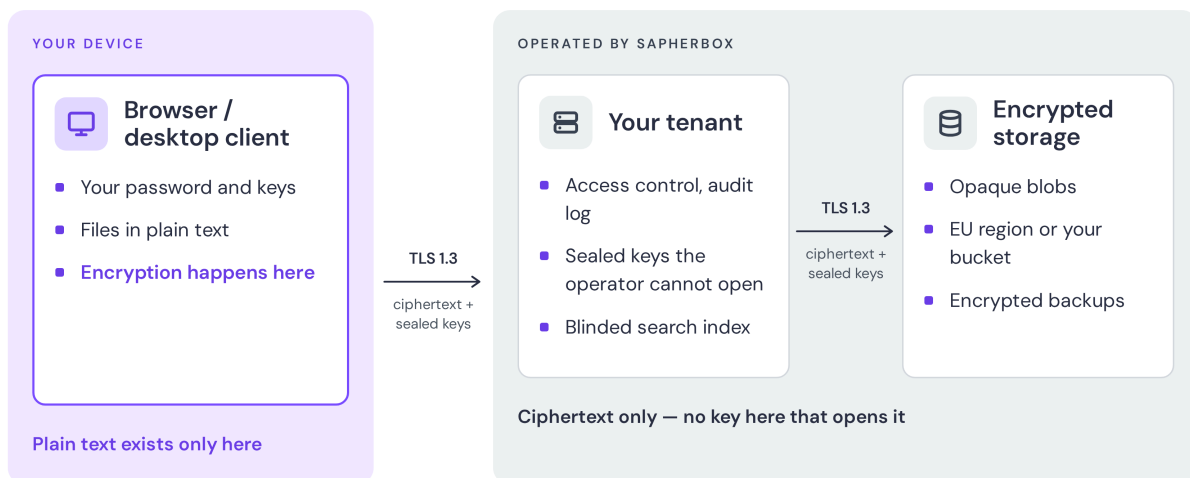


Figure 1· Where plain text exists, and where it never does

Two layers: what travels is already ciphertext, and the connection carrying it is TLS 1.3 encrypted as well.

1. What this means for you



Encrypted before it leaves

Files, file names and folder names are encrypted in your browser or desktop client before anything is sent. Our servers store and forward ciphertext only; plaintext never reaches them.



No key on our side

Each user holds their own keys, unlocked by password or passkey on their device. There is no administrator key, no master key and no provider key that could open your files.



Ready for the quantum era

Every key that protects your files is wrapped with a classical and a post-quantum algorithm at once, so ciphertext recorded today cannot be decrypted later. The connection itself uses classical TLS and carries no plaintext.



Sharing you can trust

Sharing hands the key to the recipient on your device and signs the grant cryptographically. A compromised server cannot redirect a share or slip in a key of its own.



Search without exposure

Full-text search works on blinded tokens computed on your device. The server matches them without ever learning the words behind them, and what it can still see is documented.



Evidence when you need it

A tamper-evident audit trail records who did what and when, with retention you configure, ready for GDPR, NIS2 and DORA reviews and verifiable at any time.

2. What we can and cannot see

Honesty about the limits of encryption is part of the promise. Encrypting content does not make a service invisible: to run the platform we still see some information about your data,

and you should know what it is.

The short version

We can see: how large your files are, when they were created or changed, how your folders are organised, who has access to what and with which role, who signed in and what they did, and which blinded search tokens occur in which file. In other words: the shape of your data and how it is used.

We cannot see: the content of any file, the names of files and folders, notes and previews, search terms, passwords, or any key that could unlock any of these.

If you need the complete list, our security team will provide it item by item on request.

3. How your keys work, in plain words

- **Your password never leaves your device.** It unlocks your personal key on the device itself; we only ever see a one-way, salted verifier that is deliberately slow to compute, used to check that it is you. A stolen copy of that verifier still has to be guessed against, which is why password policy, second factors and passkeys matter.
- **Every user has their own key.** There is no company-wide key that could open everything. An administrator who has not been given a file cannot read it.
- **Every file has its own key.** That key is sealed to the people and groups who may read the file, and only they can unseal it.
- **Sharing means handing over a key, on your device.** When you share a folder, the recipient receives the keys for it and everything inside, sealed to them. Their identity is pinned the first time you share with them, so a later substitution is detected. That first share is the moment of trust: for a new person, confirm through a channel you already trust, such as a phone call, that the address is theirs and that the share has arrived.
- **Revoking means changing the locks.** When someone leaves a share or the company, the affected keys are rotated. It is not enough to remove a permission entry; the old keys simply stop working. Revocation locks the door going forward; it cannot take back copies a person already downloaded or cached while they had access.

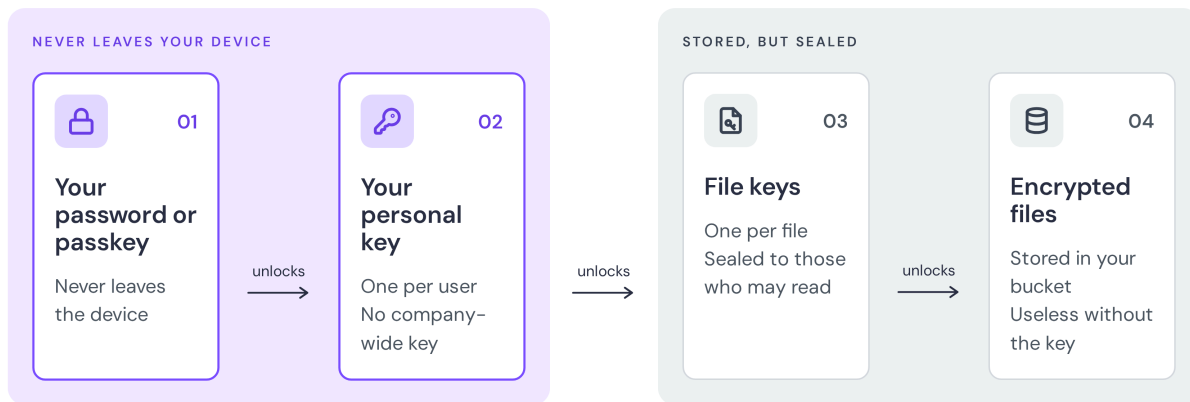


Figure 2 · How your keys chain together

4. When people leave and passwords get lost

End-to-end encryption has a consequence: if nobody holds a key, nobody can reset it for you. Sapherbox addresses this without giving the provider a way in.

- **Recovery code.** Every user receives a recovery code at registration that can restore access to their own keys. It is shown once and never stored by us.
- **Escrow key, held by you.** Optionally, your organisation creates an escrow key pair in the browser and keeps the private half. From then on, file keys are additionally sealed to it, so an authorised administrator can recover the files of a leaver or a lost account. Every use is written to the audit log. If you never enable it, no such key exists anywhere.

Many products marketed as end-to-end encrypted quietly keep a recovery key of their own for this purpose. We think that decision belongs to you, and that it should be visible in the audit trail whenever it is used.

5. Working with people outside your organisation

External partners are invited as guests. A guest sees only what was shared with them, with the role you chose (view, edit or co-own), and can be removed at any time, which rotates the keys. Upload links let outsiders send you files that are encrypted on their device before

upload; download links let you hand out a single file, optionally password-protected and time-limited. Groups give teams shared access with one grant instead of dozens.

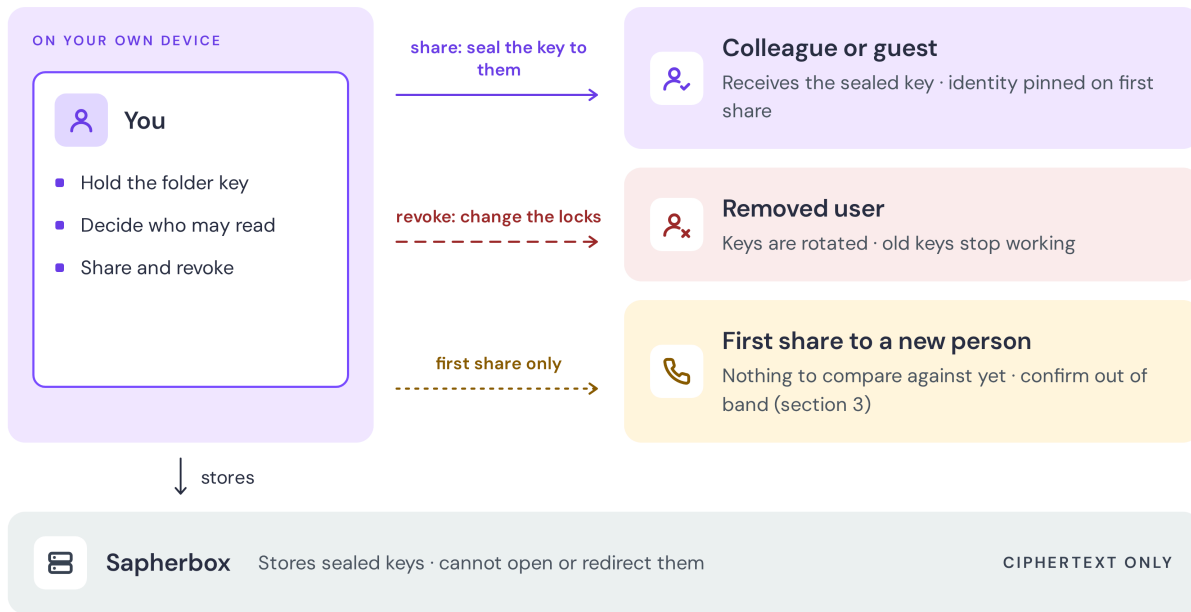


Figure 3 · Sharing hands over a key; revoking changes the lock

Sharing and revocation are cryptographic acts on your device, not permission flags on the server.

6. Safe uploads

Because we cannot scan encrypted content on the server, Sapherbox cleans files before they are encrypted, on the device that uploads them. Macros, scripts, embedded objects, hidden metadata and other active content are removed from Office documents, PDFs, images and web files while the readable content is preserved. Files of a supported type that cannot be decoded are blocked rather than passed through. File types the cleaner does not handle, such as plain text, archives, audio and video, are stored unchanged and marked as not sanitised, so your endpoint antivirus remains the control for those. Administrators decide per tenant whether this is mandatory, selective or optional, and every outcome is recorded.

Limitation. The cleaner removes active content; it is not a malware scanner and does not detect every threat. Sapherbox therefore assumes that endpoint protection, including up-to-date antivirus, is in place on every device that uploads, syncs or opens files. Providing and

maintaining that protection is the customer's responsibility and is outside the scope of the platform.

7. Analysing your data

Sapherbox Compute lets you run analytics, SQL queries and reports over your documents. Because the server holds only ciphertext, this happens where the plaintext is: the data is decrypted in your browser and the computation runs there. Results stay on your device unless you choose to save them to the vault, where they are encrypted like any other file before upload, or export them to your own systems, including an optional webhook that sends a job's result from your browser to a URL you configure. What our servers see of an analysis is the same as for any other file: sizes, timestamps and access events, never the content or the result.

8. Signing in

- **Passkeys** for phishing-resistant, password-free sign-in, or password plus a second factor.
- **Single sign-on** with your Microsoft Entra directory, so joiners and leavers are handled where you already manage them.
- **Sessions you control**: a limited number of active devices per user, immediate revocation, automatic sign-out when idle, and lockout policies you configure.
- **Service accounts** with narrowly scoped API keys for integrations, instead of a person's credentials.

9. Where your data lives

- **Your own tenant**. Every customer runs in a dedicated environment with its own database, its own encrypted storage and its own settings. Tenants share nothing.
- **In the EU**. Application hosts are located in Germany and Finland.
- **Your own storage, if you prefer**. Point your tenant at your own S3-compatible bucket, at a cloud provider or on premises, and choose region, storage class and replication yourself.

The monthly base price is reduced accordingly.

- **Encrypted backups.** Backups are encrypted with a key whose private half is kept offline; storage credentials alone cannot expose them.
- **Self-hosting** for enterprise customers who want the whole platform in their own data centre.

10. Evidence and compliance

Security you cannot demonstrate is hard to defend in an audit. Sapherbox keeps an append-only audit trail in which every entry is cryptographically linked to the previous one, so deleted or altered entries are detectable. Retention is configurable per tenant, entries can be shipped to your SIEM, and admin reports show who has access to what across the organisation. The controls are mapped to **BSI IT-Grundschutz**, the **BSI C5** criteria catalogue and the cryptographic recommendations of **BSI TR-02102**, and they support the technical and organisational measures required by **GDPR Art. 32**. The control-by-control mapping for your reviewers and a data processing agreement are available on request.

11. What we do not claim

No design protects against everything, and we would rather say so than let you find out later.

- **A compromised device** can see what its user can see. Passkeys, second factors and session limits reduce the risk; they do not remove it.
- **Metadata is visible**, as described in section 2. Patterns of use can be inferred from it.
- **Revocation works forward, not backward.** Rotating keys stops a removed person from reading anything new or re-fetching what they had. It cannot recall files they already copied or keys their device already cached while access was legitimate. Sharing is a decision about who may see something from now on.
- **Post-quantum protection covers content and keys, not yet the network connection.** Files, names and every key wrap are hybrid classical + post-quantum. The TLS connection between your device and the tenant still uses classical key exchange; it carries only ciphertext and metadata, so a future break would expose metadata of the kind listed in section 2, never content.

- **The client software must be trustworthy.** Encryption happens in software we deliver to your browser. Our build pipeline, signed releases and integrity checks protect that delivery; enterprise customers can self-host it.

12. Next steps

- **Try it:** a 14-day trial tenant with 10 users and 100 GB, set up in a day.
www.sapherbox.com/trial
- **Need the details:** the full technical documentation is available to your security team on request.
- **Talk to us:** www.sapherbox.com/contact

© 2026 Sapherbox B.V. i.o. (in formation) · Oliver Detjen · c/o flexdienst 20785 · Kurt-Schumacher-Straße 76 · 67663 Kaiserslautern, Germany · hello@sapherbox.com · All rights reserved.

Security Overview v1.2 · October 2026