



Sapherbox

SICHERHEITSÜBERBLICK

Ihre Dokumente bleiben Ihre. Auch vor uns.

Wie Sapherbox Ihre Dateien schützt, wer was sehen kann und was das für Ihre Organisation bedeutet. Geschrieben für Entscheider; technische Details erhält Ihr Sicherheitsteam auf Anfrage.

DOKUMENT

Sicherheitsüberblick · Version 1.3

DATUM

Oktober 2026

ZIELGRUPPE

**Geschäftsführung, Einkauf,
Datenschutzbeauftragte**

ORGANISATION

Sapherbox

• **ÖFFENTLICH — DARF FREI WEITERGEGEBEN WERDEN**

Sapherbox

Sicherheitsüberblick

Sapherbox ist eine Dokumentenplattform für Organisationen, die genau wissen müssen, wer ihre Dateien lesen kann. Jedes Dokument wird auf Ihrem eigenen Gerät verschlüsselt, bevor es irgendwohin gesendet wird. Was unsere Server erreicht und was im Speicher und in Backups liegt, ist Chiffretext, das wir nicht öffnen können. Wir halten keinen Schlüssel, der es öffnen könnte, es gibt keine Anbieter-Hintertür und keinen Wiederherstellungsschlüssel auf unserer Seite. Der einzige Wiederherstellungsweg ist ein Escrow-Schlüssel, den Ihre Organisation selbst anlegen und behalten kann. All das ist so ausgelegt, dass es nicht nur heutigen Angreifern standhält, sondern auch den Quantencomputern der kommenden Jahrzehnte.

„Keine Richtlinie, die verspricht, dass wir nicht hinsehen. Eine Architektur, in der wir es nicht können.“

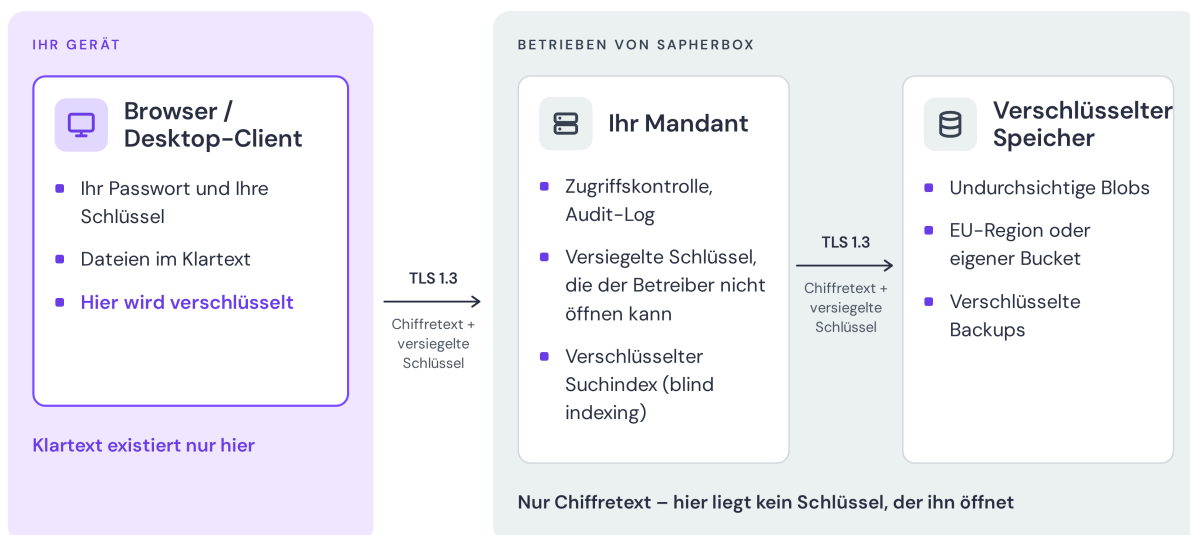


Abbildung 1 · Wo Klartext existiert – und wo nie

Zwei Schichten: Was übertragen wird, ist bereits Chiffretext – und die Verbindung ist zusätzlich per TLS 1.3 verschlüsselt.

1. Was das für Sie bedeutet



Verschlüsselt, bevor es das Gerät verlässt

Dateien, Dateinamen und Ordernamen werden im Browser oder im Desktop-Client verschlüsselt, bevor etwas gesendet wird.

Unsere Server speichern und übertragen ausschließlich Chiffprat; Klartext erreicht sie nie.



Kein Schlüssel auf unserer Seite

Jeder Nutzer hält eigene Schlüssel, die auf seinem Gerät per Passwort oder Passkey entsperrt werden. Es gibt keinen Administrator-, keinen Master- und keinen Anbieterschlüssel, der Ihre Dateien öffnen könnte.



Bereit für das Quantenzeitalter

Jeder Schlüssel, der Ihre Dateien schützt, ist zugleich klassisch und post-quantum verpackt. Heute aufgezeichnetes Chiffprat lässt sich auch später nicht entschlüsseln. Die Verbindung selbst nutzt klassisches TLS und transportiert keinen Klartext.



Teilen, dem Sie vertrauen können

Beim Teilen wird der Schlüssel auf Ihrem Gerät an den Empfänger übergeben und die Freigabe kryptographisch signiert. Ein kompromittierter Server kann sie weder umleiten noch einen eigenen Schlüssel unterschieben.



Suchen ohne Preisgabe

Die Volltextsuche arbeitet mit verschlüsselten Such-Token (blind indexing), die auf Ihrem Gerät berechnet werden. Der Server gleicht sie ab, ohne die Wörter dahinter zu kennen; was er dennoch sieht, ist dokumentiert.



Nachweise, wenn Sie sie brauchen

Eine manipulationssichere Audit-Spur hält fest, wer wann was getan hat, mit einer Aufbewahrung, die Sie festlegen — bereit für DSGVO-, NIS2- und DORA-Prüfungen und jederzeit überprüfbar.

2. Was wir sehen können – und was nicht

Ehrlichkeit über die Grenzen von Verschlüsselung gehört zum Versprechen. Inhalte zu verschlüsseln macht einen Dienst nicht unsichtbar: Um die Plattform zu betreiben, sehen wir weiterhin einige Informationen über Ihre Daten, und Sie sollten wissen, welche.

Die Kurzfassung

Wir sehen: wie groß Ihre Dateien sind, wann sie erstellt oder geändert wurden, wie Ihre Ordner organisiert sind, wer mit welcher Rolle worauf Zugriff hat, wer sich angemeldet und was er getan hat, und welche verschlüsselten Such-Token (blind indexing) in welcher Datei vorkommen. Kurz: die Form Ihrer Daten und wie sie genutzt werden.

Wir sehen nicht: den Inhalt irgendeiner Datei, Datei- und Ordnernamen, Notizen und Vorschauen, Suchbegriffe, Passwörter oder irgendeinen Schlüssel, der das alles öffnen könnte.

Die vollständige Liste stellt Ihnen unser Sicherheitsteam auf Anfrage Punkt für Punkt bereit.

3. Wie Ihre Schlüssel funktionieren, in einfachen Worten

- **Ihr Passwort verlässt Ihr Gerät nie.** Es entsperrt Ihren persönlichen Schlüssel direkt auf dem Gerät; wir sehen nur einen gesalzenen Einweg-Prüfwert, der absichtlich langsam zu berechnen ist und mit dem wir prüfen, dass Sie es sind. Eine gestohlene Kopie dieses Prüfwerts müsste immer noch durchprobiert werden – deshalb zählen Passwortrichtlinie, zweiter Faktor und Passkeys.
- **Jeder Nutzer hat einen eigenen Schlüssel.** Es gibt keinen unternehmensweiten Schlüssel, der alles öffnen könnte. Ein Administrator, dem eine Datei nicht freigegeben wurde, kann sie nicht lesen.
- **Jede Datei hat einen eigenen Schlüssel.** Dieser ist für die Personen und Gruppen versiegelt, die die Datei lesen dürfen, und nur sie können ihn öffnen.
- **Teilen heißt, einen Schlüssel zu übergeben – auf Ihrem Gerät.** Wenn Sie einen Ordner teilen, erhält der Empfänger die Schlüssel für den Ordner und alles darin, versiegelt für ihn. Seine Identität wird beim ersten Teilen festgeschrieben, sodass ein späterer Austausch

erkannt wird. Dieses erste Teilen ist der Moment des Vertrauens: Bestätigen Sie bei einer neuen Person über einen Kanal, dem Sie bereits vertrauen – etwa per Telefon –, dass die Adresse ihr gehört und die Freigabe angekommen ist.

- **Entziehen heißt, die Schlösser zu wechseln.** Verlässt jemand eine Freigabe oder das Unternehmen, werden die betroffenen Schlüssel rotiert. Es genügt nicht, einen Berechtigungseintrag zu löschen; die alten Schlüssel funktionieren schlicht nicht mehr. Der Entzug verschließt die Tür für die Zukunft; Kopien, die jemand während seines berechtigten Zugriffs bereits heruntergeladen oder zwischengespeichert hat, holt er nicht zurück.

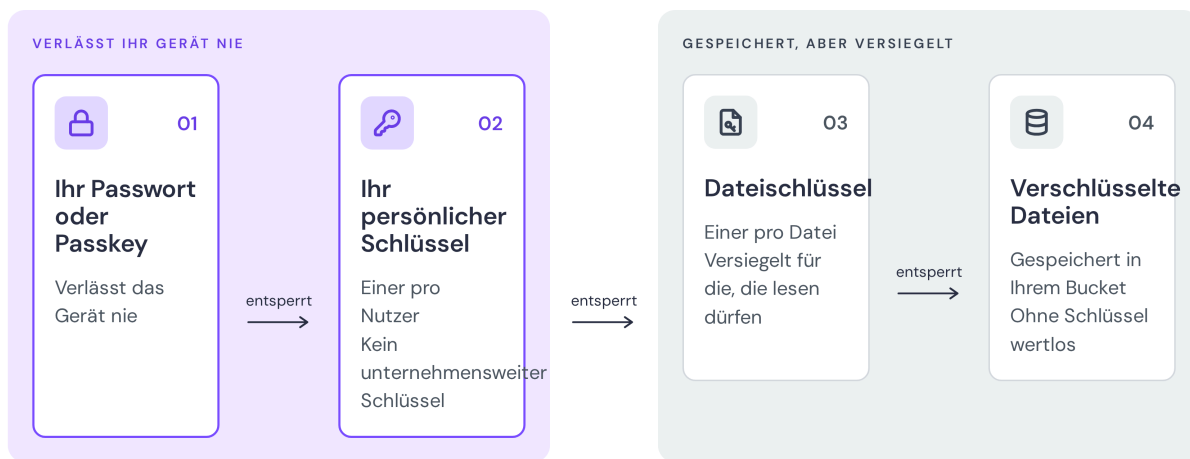


Abbildung 2 · Wie Ihre Schlüssel ineinandergreifen

4. Wenn Mitarbeiter gehen und Passwörter verloren gehen

Ende-zu-Ende-Verschlüsselung hat eine Konsequenz: Wenn niemand einen Schlüssel hält, kann ihn auch niemand für Sie zurücksetzen. Sapherbox löst das, ohne dem Anbieter einen Zugang zu geben.

- **Wiederherstellungscodes.** Jeder Nutzer erhält bei der Registrierung einen Wiederherstellungscodes, der den Zugriff auf die eigenen Schlüssel wiederherstellen kann. Er wird einmal angezeigt und von uns nie gespeichert.

- **Escrow-Schlüssel, von Ihnen gehalten.** Optional erzeugt Ihre Organisation im Browser ein Escrow-Schlüsselpaar und behält den privaten Teil. Von da an werden Dateischlüssel zusätzlich dafür versiegelt, sodass ein berechtigter Administrator die Dateien eines ausgeschiedenen Mitarbeiters oder eines verlorenen Kontos wiederherstellen kann. Jede Nutzung landet im Audit-Log. Aktivieren Sie ihn nie, existiert ein solcher Schlüssel nirgends.

Viele als Ende-zu-Ende-verschlüsselt vermarktete Produkte halten dafür still einen eigenen Wiederherstellungsschlüssel. Wir finden, diese Entscheidung gehört Ihnen – und jede Nutzung gehört in die Audit-Spur.

5. Zusammenarbeit mit Externen

Externe Partner werden als Gäste eingeladen. Ein Gast sieht nur, was für ihn freigegeben wurde, mit der Rolle, die Sie gewählt haben (Ansehen, Bearbeiten oder Miteigentum), und kann jederzeit entfernt werden, was die Schlüssel rotiert. Upload-Links lassen Externe Ihnen Dateien senden, die auf deren Gerät vor dem Hochladen verschlüsselt werden; Download-Links geben eine einzelne Datei heraus, optional passwortgeschützt und zeitlich begrenzt. Gruppen geben Teams gemeinsamen Zugriff mit einer Freigabe statt Dutzenden.



Abbildung 3 · Teilen übergibt einen Schlüssel; Entziehen tauscht das Schloss

Teilen und Entziehen sind kryptografische Vorgänge auf Ihrem Gerät, keine Berechtigungsflags auf dem Server.

6. Sichere Uploads

Weil wir verschlüsselte Inhalte auf dem Server nicht prüfen können, bereinigt Sapherbox Dateien, bevor sie verschlüsselt werden – auf dem Gerät, das sie hochlädt. Makros, Skripte, eingebettete Objekte, versteckte Metadaten und andere aktive Inhalte werden aus Office-Dokumenten, PDFs, Bildern und Webdateien entfernt, der lesbare Inhalt bleibt erhalten. Dateien eines unterstützten Typs, die sich nicht dekodieren lassen, werden blockiert statt durchgereicht. Dateitypen, die die Bereinigung nicht behandelt – etwa Klartext, Archive, Audio und Video –, werden unverändert gespeichert und als nicht bereinigt gekennzeichnet; für sie bleibt Ihr Endpunkt-Virenschutz die maßgebliche Maßnahme. Administratoren legen pro Tenant fest, ob das verpflichtend, selektiv oder optional ist, und jedes Ergebnis wird protokolliert.

Einschränkung. Die Bereinigung entfernt aktive Inhalte; sie ist kein Malware-Scanner und erkennt nicht jede Bedrohung. Sapherbox setzt daher voraus, dass auf jedem Gerät, das Dateien hochlädt, synchronisiert oder öffnet, ein Endpunktschutz einschließlich aktuellem

Virenschutz vorhanden ist. Diesen bereitzustellen und zu pflegen liegt in der Verantwortung des Kunden und außerhalb des Leistungsumfangs der Plattform.

7. Ihre Daten auswerten

Mit Sapherbox Compute führen Sie Analysen, SQL-Abfragen und Berichte über Ihre Dokumente aus. Weil der Server nur Chiffre hält, geschieht das dort, wo der Klartext ist: Die Daten werden in Ihrem Browser entschlüsselt, und die Berechnung läuft ebenfalls dort. Ergebnisse bleiben auf Ihrem Gerät, es sei denn, Sie speichern sie im Vault – dann werden sie vor dem Hochladen wie jede andere Datei verschlüsselt – oder exportieren sie in Ihre eigenen Systeme – etwa über einen optionalen Webhook, der das Ergebnis eines Jobs aus Ihrem Browser an eine von Ihnen konfigurierte URL sendet. Was unsere Server von einer Auswertung sehen, ist dasselbe wie bei jeder anderen Datei: Größen, Zeitstempel und Zugriffsereignisse, nie den Inhalt oder das Ergebnis.

8. Anmeldung

- **Passkeys** für phishing-resistente Anmeldung ohne Passwort, oder Passwort plus zweiter Faktor.
- **Single Sign-on** mit Ihrem Microsoft-Entra-Verzeichnis, sodass Ein- und Austritte dort abgewickelt werden, wo Sie sie ohnehin verwalten.
- **Sitzungen unter Ihrer Kontrolle:** eine begrenzte Zahl aktiver Geräte pro Nutzer, sofortiger Widerruf, automatische Abmeldung bei Inaktivität und Sperrregeln, die Sie festlegen.
- **Service-Accounts** mit eng begrenzten API-Schlüsseln für Integrationen, statt der Zugangsdaten einer Person.

9. Wo Ihre Daten liegen

- **Ihr eigener Tenant.** Jeder Kunde läuft in einer eigenen Umgebung mit eigener Datenbank, eigenem verschlüsselten Speicher und eigenen Einstellungen. Tenants teilen nichts.
- **In der EU.** Die Anwendungsserver stehen in Deutschland und Finnland.

- **Ihr eigener Speicher, wenn Sie möchten.** Verbinden Sie Ihren Tenant mit Ihrem eigenen S3-kompatiblen Bucket, bei einem Cloud-Anbieter oder im eigenen Rechenzentrum, und wählen Sie Region, Speicherklasse und Replikation selbst. Der monatliche Grundpreis reduziert sich entsprechend.
- **Verschlüsselte Backups.** Backups werden mit einem Schlüssel verschlüsselt, dessen privater Teil offline verwahrt wird; Speicherzugangsdaten allein geben sie nicht preis.
- **Self-Hosting** für Enterprise-Kunden, die die gesamte Plattform im eigenen Rechenzentrum betreiben möchten.

10. Nachweise und Compliance

Sicherheit, die man nicht belegen kann, ist in einer Prüfung schwer zu verteidigen. Sapherbox führt eine Audit-Spur, in der jeder Eintrag kryptographisch mit dem vorherigen verknüpft ist, sodass gelöschte oder veränderte Einträge erkennbar sind. Die Aufbewahrung ist pro Tenant konfigurierbar, Einträge können an Ihr SIEM übergeben werden, und Admin-Berichte zeigen organisationsweit, wer worauf Zugriff hat. Die Maßnahmen sind dem **BSI IT-Grundschutz**, dem Kriterienkatalog **BSI C5** und den kryptographischen Empfehlungen der **BSI TR-02102** zugeordnet und unterstützen die technischen und organisatorischen Maßnahmen nach **Art. 32 DSGVO**. Die Zuordnung Maßnahme für Maßnahme für Ihre Prüfer und ein Auftragsverarbeitungsvertrag sind auf Anfrage erhältlich.

11. Was wir nicht behaupten

Keine Architektur schützt vor allem, und wir sagen das lieber selbst, als dass Sie es später feststellen.

- **Ein kompromittiertes Gerät** sieht, was sein Nutzer sieht. Passkeys, zweite Faktoren und Sitzungsbegrenzungen verringern das Risiko; sie beseitigen es nicht.
- **Metadaten sind sichtbar**, wie in Abschnitt 2 beschrieben. Nutzungsmuster lassen sich daraus ableiten.
- **Entzug wirkt nach vorn, nicht zurück.** Die Schlüsselrotation verhindert, dass eine entfernte Person Neues liest oder Bekanntes erneut abrufen. Dateien, die sie bereits kopiert hat, oder Schlüssel, die ihr Gerät während des berechtigten Zugriffs zwischengespeichert

hat, lassen sich nicht zurückholen. Teilen ist eine Entscheidung darüber, wer etwas ab jetzt sehen darf.

- **Post-Quanten-Schutz gilt für Inhalte und Schlüssel, noch nicht für die Netzverbindung.** Dateien, Namen und jede Schlüsselpackung sind hybrid klassisch + Post-Quanten. Die TLS-Verbindung zwischen Ihrem Gerät und dem Tenant nutzt weiterhin klassischen Schlüsselaustausch; sie transportiert nur Chiffre und Metadaten, sodass ein künftiger Bruch Metadaten der in Abschnitt 2 genannten Art offenlegen würde, nie Inhalte.
- **Die Client-Software muss vertrauenswürdig sein.** Die Verschlüsselung geschieht in Software, die wir an Ihren Browser ausliefern. Unsere Build-Pipeline, signierte Releases und Integritätsprüfungen schützen diese Auslieferung; Enterprise-Kunden können sie selbst hosten.

12. Nächste Schritte

- **Ausprobieren:** ein 14-tägiger Test-Tenant mit 10 Nutzern und 100 GB, eingerichtet an einem Tag: www.sapherbox.com/trial
- **Details gewünscht:** die vollständige technische Dokumentation erhält Ihr Sicherheitsteam auf Anfrage.
- **Mit uns sprechen:** www.sapherbox.com/contact