



Sapherbox

BEVEILIGINGSOVERZICHT

Uw documenten blijven van u. Ook voor ons.

Hoe Sapherbox uw bestanden beschermt, wie wat kan zien en wat dat betekent voor uw organisatie. Geschreven voor beslissers; technische details zijn op aanvraag beschikbaar voor uw beveiligingsteam.

DOCUMENT

Beveiligingsoverzicht · Versie 1.2

DATUM

oktober 2026

DOELGROEP

**Management, inkoop,
functionarissen
gegevensbescherming**

ORGANISATIE

Sapherbox

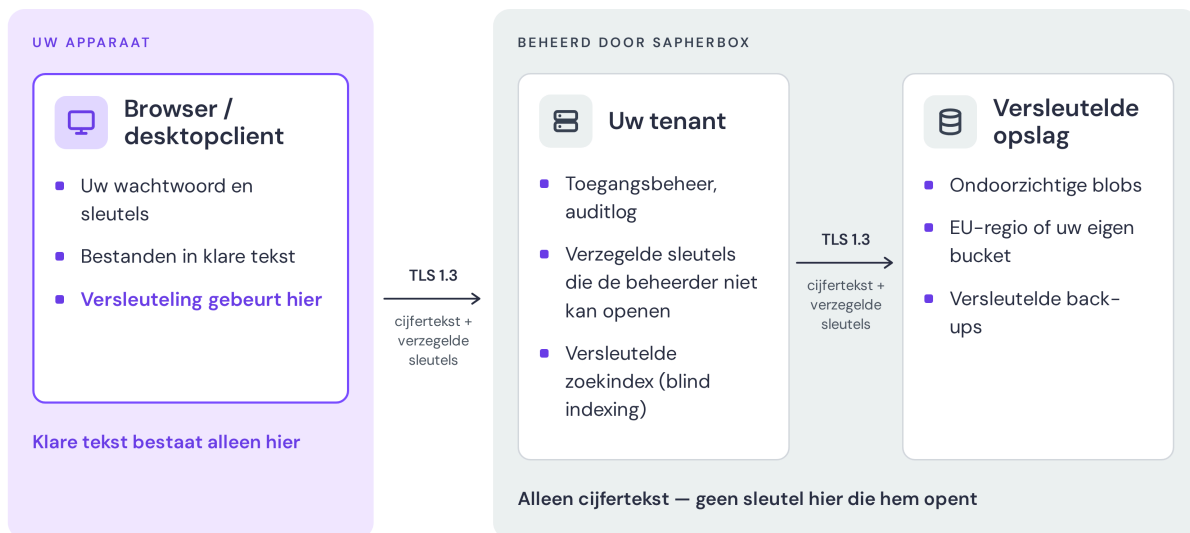
• **OPENBAAR — MAG VRIJ WORDEN GEDEELD**

Sapherbox

Beveiligingsoverzicht

Sapherbox is een documentplatform voor organisaties die precies willen weten wie hun bestanden kan lezen. Elk document wordt op uw eigen apparaat versleuteld voordat het ergens naartoe wordt gestuurd. Wat onze servers bereikt, en wat in de opslag en in back-ups staat, is cijfertekst die wij niet kunnen openen. Wij hebben geen sleutel die hem zou kunnen openen, er is geen achterdeur van de aanbieder en er is geen herstelsleutel aan onze kant. De enige herstelroute is een bewaringssleutel die uw organisatie zelf kan aanmaken en bewaren. Dit alles is ontworpen om niet alleen de aanvallers van vandaag te weerstaan, maar ook de kwantumcomputers van de komende decennia.

"Niet alleen een beleid dat zegt dat wij niet kijken. Een ontwerp waarin wij het niet kunnen."



Figuur 1 · Waar klare tekst bestaat, en waar nooit

Twee lagen: wat wordt verzonden is al cijfertekst, en de verbinding die het draagt is bovendien met TLS 1.3 versleuteld.

1. Wat dit voor u betekent



Versleuteld voordat het vertrekt

Bestanden, bestandsnamen en mapnamen worden in uw browser of desktopclient versleuteld voordat er iets wordt verzonden. Onze servers slaan alleen cijfertekst op en geven die door; klare tekst bereikt ze nooit.



Delen dat u kunt vertrouwen

Bij het delen wordt de sleutel op uw apparaat aan de ontvanger overhandigd en wordt de toekenning cryptografisch ondertekend. Een gecompromitteerde server kan een deling niet omleiden of een eigen sleutel binnensmokkelen.



Geen sleutel aan onze kant

Elke gebruiker heeft eigen sleutels, die met wachtwoord of passkey op het eigen apparaat worden ontgrendeld. Er is geen beheerderssleutel, geen hoofdsleutel en geen aanbiederssleutel die uw bestanden zou kunnen openen.



Zoeken zonder blootstelling

Zoeken in de volledige tekst werkt met verblinde tokens die op uw apparaat worden berekend. De server vergelijkt ze zonder ooit de woorden erachter te kennen, en wat hij nog wel kan zien is gedocumenteerd.



Klaar voor het kwantumtijdperk

Elke sleutel die uw bestanden beschermt wordt tegelijk met een klassiek en een post-kwantumalgoritme ingepakt, zodat cijfertekst die vandaag wordt opgevangen later niet kan worden ontsleuteld. De verbinding zelf gebruikt klassieke TLS en vervoert geen klare tekst.



Bewijs wanneer u het nodig hebt

Een manipulatiebestendig auditspoor legt vast wie wat wanneer deed, met een bewaartermijn die u instelt, klaar voor AVG-, NIS2- en DORA-beoordelingen en op elk moment verifieerbaar.

2. Wat wij wel en niet kunnen zien

Eerlijkheid over de grenzen van versleuteling hoort bij de belofte. Het versleutelen van inhoud maakt een dienst niet onzichtbaar: om het platform te laten draaien zien wij nog steeds bepaalde informatie over uw gegevens, en u hoort te weten welke.

De korte versie

Wij kunnen zien: hoe groot uw bestanden zijn, wanneer ze zijn gemaakt of gewijzigd, hoe uw mappen zijn georganiseerd, wie toegang heeft tot wat en met welke rol, wie zich heeft aangemeld en wat die persoon deed, en welke verblinde zoektokens in welk bestand voorkomen. Met andere woorden: de vorm van uw gegevens en hoe ze worden gebruikt.

Wij kunnen niet zien: de inhoud van welk bestand dan ook, de namen van bestanden en mappen, notities en voorbeelden, zoektermen, wachtwoorden, of welke sleutel dan ook die een van deze zou kunnen ontgrendelen.

Als u de volledige lijst nodig hebt, verstrekt ons beveiligingsteam die op aanvraag punt voor punt.

3. Hoe uw sleutels werken, in gewone taal

- **Uw wachtwoord verlaat uw apparaat nooit.** Het ontgrendelt uw persoonlijke sleutel op het apparaat zelf; wij zien alleen een eenrichtings-, gezouten verificatiewaarde die opzettelijk traag te berekenen is en waarmee wordt gecontroleerd dat u het bent. Een gestolen kopie van die waarde moet nog steeds worden geraden, en daarom doen wachtwoordbeleid, tweede factoren en passkeys ertoe.
- **Elke gebruiker heeft een eigen sleutel.** Er is geen bedrijfsbrede sleutel die alles zou kunnen openen. Een beheerder aan wie een bestand niet is gegeven, kan het niet lezen.
- **Elk bestand heeft een eigen sleutel.** Die sleutel is verzegeld voor de personen en groepen die het bestand mogen lezen, en alleen zij kunnen hem ontzegelen.
- **Delen betekent een sleutel overhandigen, op uw apparaat.** Wanneer u een map deelt, ontvangt de ontvanger de sleutels ervoor en voor alles erin, voor hem of haar verzegeld. De identiteit van de ontvanger wordt bij de eerste deling vastgepind, zodat een latere

vervanging wordt gedetecteerd. Die eerste deling is het moment van vertrouwen: bevestig bij een nieuwe persoon via een kanaal dat u al vertrouwt, zoals een telefoongesprek, dat het adres van die persoon is en dat de deling is aangekomen.

- **Intrekken betekent de sloten vervangen.** Wanneer iemand een deling of het bedrijf verlaat, worden de betrokken sleutels geroteerd. Een rechtenvermelding verwijderen is niet genoeg; de oude sleutels werken simpelweg niet meer. Intrekking sluit de deur voor de toekomst; kopieën die iemand al heeft gedownload of in de cache had terwijl de toegang bestond, kunnen niet worden teruggehaald.



Figuur 2 · Hoe uw sleutels aan elkaar zijn geketend

4. Als mensen vertrekken en wachtwoorden verloren gaan

End-to-end-versleuteling heeft een consequentie: als niemand een sleutel heeft, kan niemand die voor u opnieuw instellen. Sapherbox lost dit op zonder de aanbieder een ingang te geven.

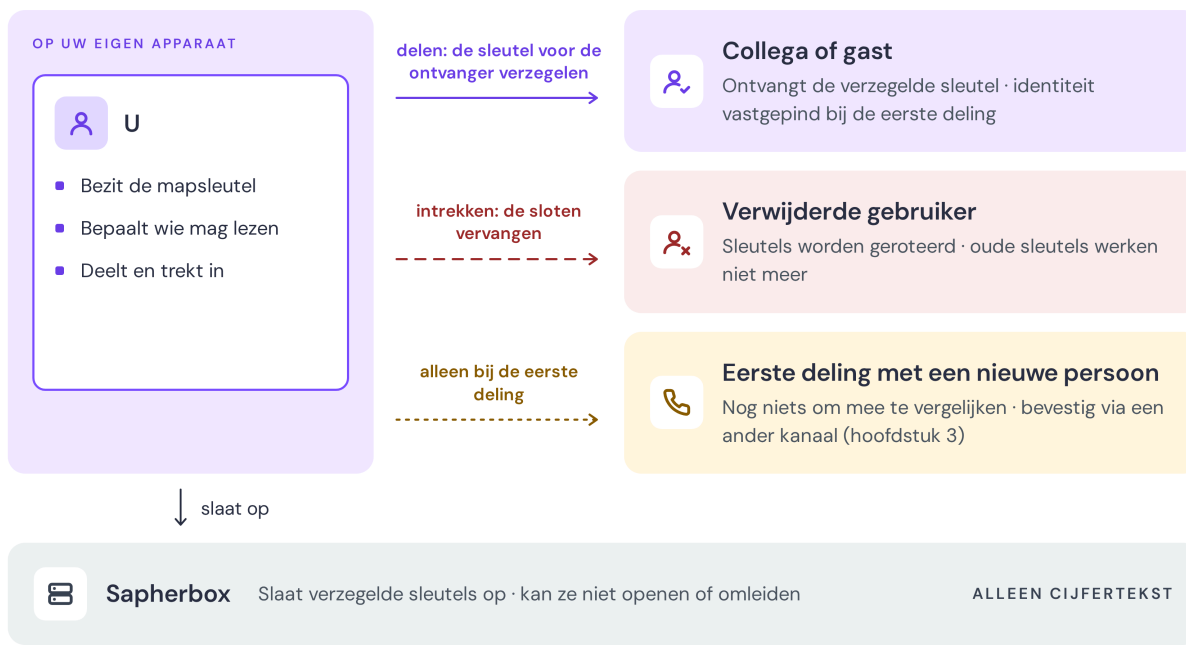
- **Herstelcode.** Elke gebruiker ontvangt bij registratie een herstelcode waarmee de toegang tot de eigen sleutels kan worden hersteld. Die wordt eenmalig getoond en nooit door ons opgeslagen.

- **Bewaringssleutel, in uw handen.** Optioneel maakt uw organisatie in de browser een bewaringssleutelpaar aan en bewaart zij de private helft. Vanaf dat moment worden bestandssleutels er aanvullend voor verzegeld, zodat een bevoegde beheerder de bestanden van een vertrekkende medewerker of een verloren account kan herstellen. Elk gebruik wordt in het auditlog vastgelegd. Als u dit nooit inschakelt, bestaat zo'n sleutel nergens.

Veel producten die als end-to-end versleuteld worden aangeprezen, houden hiervoor stilletjes een eigen herstelsleutel achter. Wij vinden dat die beslissing bij u hoort, en dat elk gebruik ervan zichtbaar moet zijn in het auditspoor.

5. Samenwerken met mensen buiten uw organisatie

Externe partners worden als gast uitgenodigd. Een gast ziet alleen wat met hem of haar is gedeeld, met de rol die u koos (bekijken, bewerken of mede-eigenaar), en kan op elk moment worden verwijderd, waarbij de sleutels worden geroteerd. Met uploadlinks kunnen buitenstaanders u bestanden sturen die vóór de upload op hun apparaat worden versleuteld; met downloadlinks geeft u een enkel bestand uit, optioneel met wachtwoord en beperkt in tijd. Groepen geven teams gedeelde toegang met één toekenning in plaats van tientallen.



Figuur 3 · Delen overhandigt een sleutel; intrekken vervangt het slot

Delen en intrekken zijn cryptografische handelingen op uw apparaat, geen rechtenvlaggen op de server.

6. Veilige uploads

Omdat wij versleutelde inhoud niet op de server kunnen scannen, schoont Sapherbox bestanden op voordat ze worden versleuteld, op het apparaat dat ze uploadt. Macro's, scripts, ingesloten objecten, verborgen metadata en andere actieve inhoud worden uit Office-documenten, PDF's, afbeeldingen en webbestanden verwijderd, terwijl de leesbare inhoud behouden blijft. Bestanden van een ondersteund type die niet kunnen worden gedecodeerd, worden geblokkeerd in plaats van doorgelaten. Bestandstypen die de opschoner niet verwerkt, zoals platte tekst, archieven, audio en video, worden ongewijzigd opgeslagen en als niet-opgeschoond gemarkeerd, zodat uw endpoint-antivirus daarvoor de controle blijft. Beheerders bepalen per tenant of dit verplicht, selectief of optioneel is, en elk resultaat wordt vastgelegd.

Beperking. De opschoner verwijdert actieve inhoud; het is geen malwarescanner en detecteert niet elke bedreiging. Sapherbox gaat er daarom van uit dat op elk apparaat dat bestanden uploadt, synchroniseert of opent, endpointbeveiliging aanwezig is, inclusief

actuele antivirussoftware. Het leveren en onderhouden van die beveiliging is de verantwoordelijkheid van de klant en valt buiten de reikwijdte van het platform.

7. Uw gegevens analyseren

Met Sapherbox Compute voert u analyses, SQL-query's en rapporten uit over uw documenten. Omdat de server alleen cijfertekst bevat, gebeurt dit waar de klare tekst is: de gegevens worden in uw browser ontsleuteld en de berekening draait daar. Resultaten blijven op uw apparaat, tenzij u ze in de kluis opslaat, waar ze vóór de upload net als elk ander bestand worden versleuteld, of ze naar uw eigen systemen exporteert, inclusief een optionele webhook die het resultaat van een taak vanuit uw browser naar een door u ingestelde URL stuurt. Wat onze servers van een analyse zien is hetzelfde als bij elk ander bestand: groottes, tijdstempels en toegangsgebeurtenissen, nooit de inhoud of het resultaat.

8. Aanmelden

- **Passkeys** voor phishingbestendig, wachtwoordloos aanmelden, of wachtwoord plus een tweede factor.
- **Single sign-on** met uw Microsoft Entra-directory, zodat in- en uitdiensttrekkingen worden afgehandeld waar u ze al beheert.
- **Sessies die u beheerst:** een beperkt aantal actieve apparaten per gebruiker, onmiddellijke intrekking, automatisch afmelden bij inactiviteit en blokkeringsbeleid dat u instelt.
- **Serviceaccounts** met nauw afgebakende API-sleutels voor integraties, in plaats van de inloggegevens van een persoon.

9. Waar uw gegevens staan

- **Uw eigen tenant.** Elke klant draait in een eigen omgeving met een eigen database, eigen versleutelde opslag en eigen instellingen. Tenants delen niets.
- **In de EU.** De applicatiehosts staan in Duitsland en Finland.

- **Uw eigen opslag, als u dat wilt.** Koppel uw tenant aan uw eigen S3-compatibele bucket, bij een clouddaanbieder of on-premises, en kies zelf regio, opslagklasse en replicatie. De maandelijkse basisprijs wordt dienovereenkomstig verlaagd.
- **Versleutelde back-ups.** Back-ups worden versleuteld met een sleutel waarvan de private helft offline wordt bewaard; opslagreferenties alleen kunnen ze niet blootleggen.
- **Self-hosting** voor enterpriseklanten die het hele platform in hun eigen datacenter willen.

10. Bewijs en compliance

Beveiliging die u niet kunt aantonen, is in een audit moeilijk te verdedigen. Sapherbox houdt een auditspoor bij waaraan alleen kan worden toegevoegd en waarin elke vermelding cryptografisch aan de vorige is gekoppeld, zodat verwijderde of gewijzigde vermeldingen detecteerbaar zijn. De bewaartermijn is per tenant instelbaar, vermeldingen kunnen naar uw SIEM worden doorgestuurd en beheerdersrapporten tonen wie in de hele organisatie toegang heeft tot wat. De maatregelen zijn gekoppeld aan **BSI IT-Grundschutz**, de criteri catalogus **BSI C5** en de cryptografische aanbevelingen van **BSI TR-02102**, en zij ondersteunen de technische en organisatorische maatregelen die **art. 32 AVG** vereist. De koppeling per maatregel voor uw beoordelaars en een verwerkersovereenkomst zijn op aanvraag beschikbaar.

11. Wat wij niet beweren

Geen enkel ontwerp beschermt tegen alles, en wij zeggen dat liever meteen dan dat u het later ontdekt.

- **Een gecompromitteerd apparaat** kan zien wat de gebruiker ervan kan zien. Passkeys, tweede factoren en sessielimieten verkleinen het risico; ze nemen het niet weg.
- **Metadata is zichtbaar**, zoals beschreven in hoofdstuk 2. Gebruikspatronen kunnen daaruit worden afgeleid.
- **Intrekking werkt vooruit, niet terug.** Het roteren van sleutels voorkomt dat een verwijderde persoon iets nieuws leest of opnieuw ophaalt wat hij of zij had. Het kan bestanden die al zijn gekopieerd, of sleutels die het apparaat al in de cache had terwijl de

toegang legitiem was, niet terughalen. Delen is een beslissing over wie iets vanaf nu mag zien.

- **Post-kwantumbescherming dekt inhoud en sleutels, nog niet de netwerkverbinding.** Bestanden, namen en elke sleutelinpakking zijn hybride klassiek + post-kwantum. De TLS-verbinding tussen uw apparaat en de tenant gebruikt nog klassieke sleuteluitwisseling; zij vervoert alleen cijfertekst en metadata, zodat een toekomstige doorbraak metadata van het soort uit hoofdstuk 2 zou blootleggen, nooit inhoud.
- **De clientsoftware moet betrouwbaar zijn.** Versleuteling gebeurt in software die wij aan uw browser leveren. Onze buildpipeline, ondertekende releases en integriteitscontroles beschermen die levering; enterpriseklanten kunnen haar zelf hosten.

12. Volgende stappen

- **Probeer het:** een proeftenant van 14 dagen met 10 gebruikers en 100 GB, binnen een dag ingericht. www.sapherbox.com/trial
- **Details nodig:** de volledige technische documentatie is op aanvraag beschikbaar voor uw beveiligingsteam.
- **Praat met ons:** www.sapherbox.com/contact

© 2026 Sapherbox B.V. i.o. (in formation) · Oliver Detjen · c/o flexdienst 20785 · Kurt-Schumacher-Straße 76 · 67663 Kaiserslautern, Duitsland · hello@sapherbox.com · Alle rechten voorbehouden.

Beveiligingsoverzicht v1.2 · oktober 2026