

MADE IN GERMANY

SILVERBACK ONE FINANCE · SICHERHEIT

Sicher ist, was nur Sie lesen können.

Wie Silverback ONE Ihre
Vermögensdaten schützt.



SOVERÄN · DSGVO-KONFORM · EIGENE SERVER IN DEUTSCHLAND



DREI FRAGEN, DIE UNS ZUERST GESTELLT WERDEN

Wo liegen meine Daten?

Wer kann sie lesen?

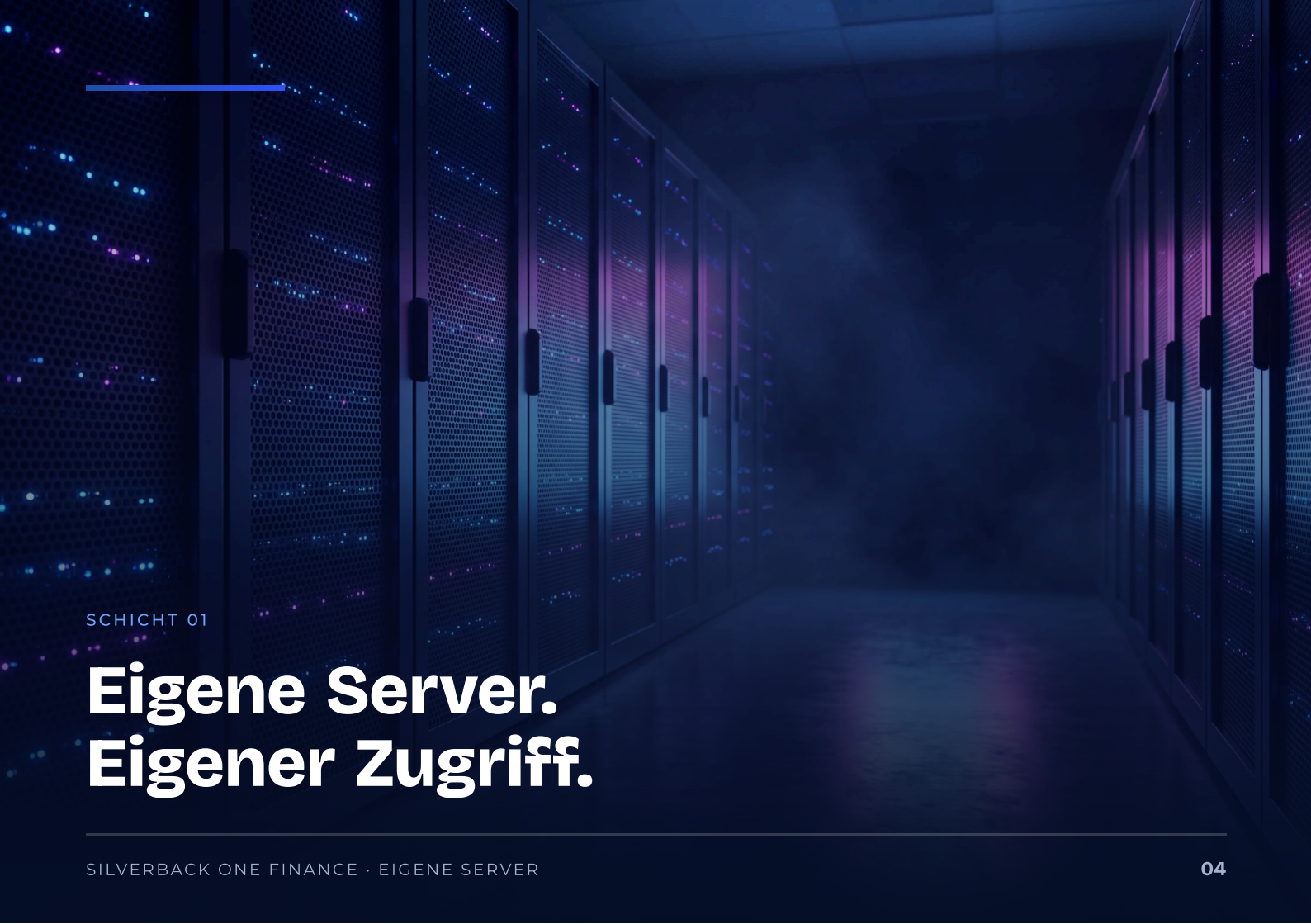
Wer garantiert mir, dass niemand den Stecker zieht?

Wer privates Vermögen souverän verwaltet, stellt diese Fragen zu Recht. Auf den folgenden Seiten beantworten wir sie. Schicht für Schicht, vom Zaun um das Rechenzentrum bis zum Schlüssel, den nur Sie besitzen.

Sicherheit in sieben Schichten.

Jede Schicht schützt für sich. Zusammen ergeben sie ein System, das Ihre Vermögensdaten souverän, unabhängig, neutral und sicher hält.

01	Eigene Server Rechenzentrum in Deutschland, jederzeit physischer Zugriff	04
02	Serversicherheit DDoS-Schutz, Firewallcluster, tägliche Sicherung	06
03	Zutrittskontrolle Elektronische Zutrittssysteme, Video, Hochsicherheitszaun	07
04	Ende-zu-Ende-Verschlüsselung Ein Schlüssel je Kunde, AES-256-GCM	08
05	Sichere Anwendung Externe Angriffstests, Anmeldung in zwei Schritten	11
06	Standort Deutschland Helsinki und Singapur in Vorbereitung	12
07	Künstliche Intelligenz Ohne Datenabfluss in öffentliche Modelle	13



SCHICHT 01

Eigene Server. Eigener Zugriff.

Ihre Daten liegen bei uns. Wörtlich.

Weil uns die Sicherheit Ihrer Daten wichtig ist, betreibt die SAI Silverback Group eigene physische Server in einem deutschen Rechenzentrum. Alle Ihre Daten liegen ausschließlich dort. Nicht bei einem US-Konzern, nicht auf fremden Servern, nicht in anderen Rechenzentren.

Wir können zu jeder Zeit physisch auf diese Server zugreifen. Das ist der Unterschied zwischen einer gemieteten Wolke und einem eigenen Haus. Wer das Haus besitzt, entscheidet, wer hinein darf.

SAI Silverback Group

betreibt eigene Server,
nicht gemietet

Rechenzentrum in Deutschland

volle Kontrolle über die
Technik

Physischer Zugriff

für uns zu jeder Zeit
möglich

Mehrere Verfahren. Ein Ziel.

Abwehr vor dem Tor

Noch bevor ein Angriff den Firewallcluster erreicht, filtert ihn ein vorgelagerter Schutz heraus, etwa bei DDoS-Attacken, also massenhaften Anfragen, die ein System lahmlegen sollen.

Eigener Firewallcluster

Dahinter schützt ein eigener Cluster die Server. Angenommen werden ausschließlich verschlüsselte Verbindungen, auch die zwischen Browser und System.

Regelmäßige Prüfläufe

Ein zyklischer Healthcheck kontrolliert die Systeme fortlaufend. Auffälligkeiten zeigen sich, bevor daraus ein Problem wird.

**Täglich gesichert.
Verschlüsselt. Doppelt.**

Alle Daten werden täglich gesichert. Die Sicherung ist ebenfalls verschlüsselt und wird in ein zweites Rechenzentrum übertragen, das dieselben Sicherheitskriterien erfüllt.



SCHICHT 03 · ZUTRITTSKONTROLLE

Wer hinein will, wird protokolliert.

Der Zutritt zu den Servern ist ausschließlich über elektronische Zutrittssysteme möglich. Jeder Zutritt wird protokolliert.

Alle relevanten Bereiche werden durchgehend videoüberwacht. Die Bilder und ihre Zeitstempel werden gespeichert und sind für uns einsehbar.

Das Rechenzentrum ist von einem Hochsicherheitszaun mit Übersteig- und Untergrabschutz umgeben. Die Zugänge sind zusätzlich durch Sicherheitstore und Sicherheitstüren geschützt.



SCHICHT 04

Verschlüsselt, bevor es Ihr Gerät verlässt.

Nur Ihr Schlüssel öffnet Ihre Daten.

Ihre Daten sind ab dem Moment verschlüsselt, in dem sie Ihr Gerät verlassen. Entschlüsseln kann sie nur Ihr Schlüssel. Deshalb können auch wir Ihre Daten nicht lesen.

Würde jemand die Daten während der Übertragung abgreifen, könnte er sie weder entschlüsseln noch lesen. Jeder Kunde hat bei uns einen eigenen Schlüssel, mit dem seine Daten verschlüsselt werden.

Selbst nach einem Einbruch.

Selbst im nahezu unmöglichen Fall eines Einbruchs in den Server bleiben Ihre Daten verschlüsselt. Ohne Ihr Passwort kann niemand die Daten entschlüsseln. Auch wir nicht.

WELCHE SCHLÜSSEL WERDEN VERWENDET?

AES-256-GCM

**Der stärkste Verschlüsselungsstandard.
Derselbe, der das Online-Banking
schützt.**

Wir verwenden zum Verschlüsseln Ihrer Daten branchenübliche Protokolle, konkret AES-256-GCM. Ihr Schlüssel liegt verschlüsselt in einem eigenen Tresor und wird nur für die Dauer Ihres Zugriffs in den Arbeitsspeicher geholt, niemals auf einen Datenträger geschrieben.

**Ein Schlüssel je
Kunde**
für alle Ihre Daten

Ein Schlüssel je Vault
für jeden einzelnen
Datentresor

Erst geprüft, dann freigegeben.

1

Sicherheitskonzept

Bevor unsere Anwendung auf das Produktivsystem übertragen wird, wird ein umfangreiches Sicherheitskonzept abgearbeitet, um Fehler von vornherein zu verhindern.

2

Externe Angriffstests

Externe Fachfirmen führen PEN-Tests durch, also gezielte Angriffe auf die Anwendung. Erst wenn alle Tests ohne Sicherheitslücke durchlaufen sind, geht die Anwendung in Betrieb.

3

Anforderungen des BSI

Neue Vorgaben des Bundesamts für Sicherheit in der Informationstechnik fließen in jeden PEN-Test ein. Das Protokoll zeigt danach, ob wir sie erfüllen.

4

Anmeldung in zwei Schritten

Das Login ist nur über eine 2-Schritt-Authentifizierung möglich. Selbst wer Benutzername und Passwort kennt, kommt ohne den zweiten Schritt nicht an Ihre Daten.

Ihre Daten liegen in Deutschland.

Unsere eigenen Server stehen heute in Deutschland.
Dort werden Ihre Daten verschlüsselt gespeichert.
Weitere Standorte sind in Vorbereitung, damit Sie den Ort künftig selbst wählen können.

- **Deutschland** im Betrieb
- **Helsinki** in Vorbereitung
- **Singapur** in Vorbereitung

Am Schutz ändert der Ort nichts. Ihre Daten bleiben überall allein mit Ihrem Schlüssel lesbar.



Künstliche Intelligenz ohne Datenabfluss.

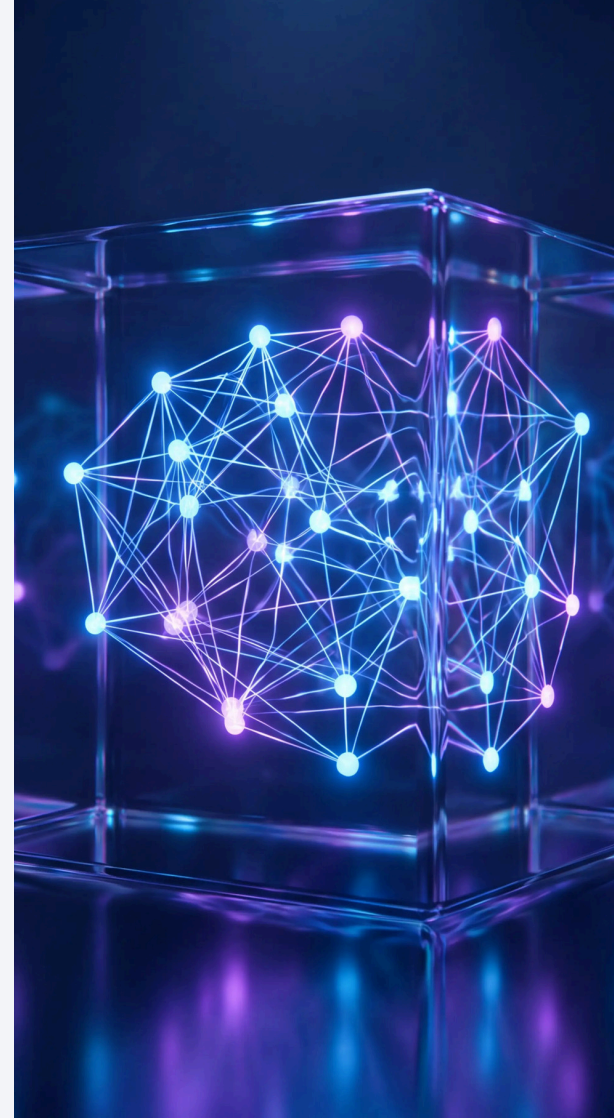
Auch bei der Verwendung von KI geben wir Ihre Daten niemals in öffentliche KI-Modelle. Damit Ihre Daten nicht an große Konzerne übertragen werden, gehen wir zwei Wege.

Allgemeine Analysen

Für allgemeine Auswertungen, etwa zu Aktien oder Immobilien, nutzen wir öffentliche KI-Rechenzentren mit sehr hohem Datenschutz. Diese Anfragen enthalten keine personenbezogenen Daten und werden zusätzlich verschleiert.

Bewertung Ihrer Daten

Geht es um Ihre persönlichen Angaben, arbeitet die KI anonymisiert oder auf einem Modell im eigenen Haus. Dieser Server hat keine Verbindung nach außen.



Souverän. Unabhängig. Neutral. Sicher.

- ✓ Eigene Server der SAI Silverback Group in einem deutschen Rechenzentrum
- ✓ DDoS-Schutz vor einem eigenen Firewallcluster
- ✓ Tägliche verschlüsselte Sicherung in ein zweites Rechenzentrum
- ✓ Elektronische Zutrittskontrolle, Videoüberwachung, Hochsicherheitszaun
- ✓ Ende-zu-Ende-Verschlüsselung mit AES-256-GCM, ein Schlüssel je Kunde
- ✓ Externe Angriffstests vor jeder Freigabe, Anmeldung in zwei Schritten
- ✓ Server in Deutschland, weitere Standorte in Vorbereitung
- ✓ Künstliche Intelligenz ohne Datenabfluss in öffentliche Modelle

Voraushandeln heißt auch, die Sicherheit zu klären, bevor die Frage entsteht.

Sicherheit, die man prüfen kann.

Sie möchten die Sicherheitsarchitektur von Silverback ONE im Detail sehen, vom Rechenzentrum bis zum Schlüssel? Wir zeigen sie Ihnen. Für private Vermögen heutiger und kommender Generationen.

Gespräch vereinbaren.

kontakt@silverbackgmbh.de
SAI Silverback Group GmbH · Oberursel



Vermögensschutz ist Wissensvorsprung.

Vermögensintelligenz. Souverän. Unabhängig.
Neutral. Sicher. Made in Germany.



Die Bildmotive dieser Broschüre wurden mit künstlicher Intelligenz erzeugt.

SAI Silverback Group GmbH
Erich-Ollenhauer-Straße 35c · 61440 Oberursel
kontakt@silverbackgmbh.de