enclaive

Solution Brief

Sichere GenAI-Nutzung in Unternehmen

Wie die GenAI-Firewall Garnet von enclaive Vertraulichkeit, Compliance und Innovation miteinander vereint

Executive Summary

Generative KI verändert die Art, wie Unternehmen Wissen nutzen, Prozesse steuern und Innovationen vorantreiben – doch mit ihr wachsen auch die Risiken für Datenschutz, Compliance und geistiges Eigentum. Viele Organisationen stehen daher vor einer zentralen Frage: Wie lässt sich das Potenzial von KI nutzen, ohne die Kontrolle über sensible Informationen zu verlieren?

Garnet, die GenAI-Firewall von **enclaive**, liefert die Antwort. Garnet schützt sensible Informationen in allen Phasen der Verarbeitung durch hardwarebasierte Isolation, durchgängige Verschlüsselung und automatische Pseudonymisierung. Unternehmen können so mit GenAI interagieren, ohne vertrauliche Daten offenzulegen oder regulatorische Vorgaben zu verletzen.

Garnet integriert sich nahtlos in bestehende IT-Umgebungen, reduziert Kosten durch gezielte Datenvorverarbeitung (RAG) und bietet Flexibilität über Multi-Cloud- und On-Premises-Szenarien hinweg. So entsteht eine sichere Grundlage für die verantwortungsvolle Nutzung von GenAI – mit voller Datenkontrolle, rechtlicher Nachweisbarkeit und Wahrung der digitalen Souveränität.

Die Herausforderung: KI nutzen – ohne Datenpreisgabe

Generative KI prägt aktuell die digitale Transformation – von Large Language Models (LLM) wie ChatGPT über branchenspezifische Spezialmodelle (SLMs) bis hin zu unternehmensinternen KI-Anwendungen. Unternehmen, Behörden und Einrichtungen arbeiten bereits intensiv mit KI, um Prozesse zu automatisieren, Wissen verfügbar zu machen und Entscheidungen zu verbessern. Gleichzeitig entstehen neue Risiken: Sensible Daten könnten in öffentliche KI-Systeme gelangen, regulatorische Vorgaben verletzt oder geistiges Eigentum preisgegeben werden.

Besonders Organisationen in streng regulierten Branchen wie dem Gesundheitswesen, der öffentlichen Verwaltung oder dem Finanzsektor stehen vor einem Dilemma: Sie möchten das Potenzial generativer KI nutzen – dürfen aber keine Datenverluste, Gesetzesverstöße oder Kontrollverluste riskieren.

Der Einsatz von KI bringt jedoch eine Vielzahl an Risiken und Hürden mit sich:

- **Gefahr von Datenlecks:** Sensible Informationen gelangen über Chat-Eingaben oder Dokumente in öffentliche LLMs, wo sie gespeichert, weiterverwertet oder unkontrolliert preisgegeben werden können.
- **Regulatorischer Druck:** DSGVO, HIPAA, DORA, NIS2 und branchenspezifische Vorgaben verlangen den Schutz personenbezogener Daten – auch während der Verarbeitung. Häufig fehlt jedoch der technische Nachweis der Vertraulichkeit.
- **Neue Angriffsvektoren:** Prompt Injection, Jailbreaking, Manipulation von Antworten oder das Ausnutzen von API-Schnittstellen schaffen neue Bedrohungen für Unternehmensdaten.
- **Operative Einschränkungen:** Externe KI-Modelle begrenzen Datenmengen, verursachen hohe Token-Kosten und speichern Interaktionen dauerhaft – was Compliance und Budget belastet.
- **Vendor Lock-in:** Viele KI-Sicherheitslösungen binden Unternehmen an spezifische Anbieter, erschweren Integrationen und reduzieren Flexibilität.

Das Ergebnis: Ohne geeignete Sicherheitsmechanismen ist der Einsatz generativer KI in vielen Bereichen blockiert – und wertvolle Innovationspotenziale bleiben ungenutzt.

Die Lösung:
Garnet – die GenAI-Firewall von enclaive

Garnet ist eine von enclaive entwickelte GenAI-Firewall, die sichere Interaktionen mit generativen KI-Systemen ermöglicht – unter Erhalt von Datenhoheit, Compliance und geistigem Eigentum.

Was Garnet auszeichnet

- KI-Kommunikation findet ausschließlich innerhalb vertraulicher, hardwareisolierter Enklaven (Confidential VMs) statt.
- Sämtliche Daten sind in allen drei Dimensionen verschlüsselt: at rest, in transit und in use (3D-Verschlüsselung).
- Im Sinne einer Retrieval Augmented Generation (RAG) können Nutzer zunächst mit dem unternehmensinternen Datenbestand chatten, ehe sie externe Modelle hinzuziehen.
- Vor jeder externen KI-Anfrage werden sensible Informationen automatisch pseudonymisiert oder gefiltert.
- Die Antworten externer Systeme werden innerhalb der Enklave dekodiert, mit Originaldaten angereichert und erst dann dem Nutzer angezeigt.

So entsteht eine Umgebung, in der Unternehmen vertrauliche Daten mit generativen KI-Systemen nutzen können – ohne Kontrollverlust.

Warum enclaive?

enclaive ist ein Berliner Unternehmen und unterliegt damit der deutschen sowie europäischen Rechtsprechung. Das Unternehmen ist führend im Bereich Confidential Computing und entwickelt Lösungen für sicherheitskritische Organisationen und regulierte Industrien.

Die Vorteile von enclaive

Souveränität & Datenschutz nach europäischem Recht	Technologieführer bei Confidential Computing und Enklaven-Technologie	Kein Vendor Lock-in: Hybride, Multi-Cloud- und On-Premises-Betriebsmodelle
Post-Quanten-Sicherheit und Zero-Trust-Architektur	Minimaler Performance-Overhead (< 3 %)	Nahtlose Integration ohne Änderungen am Code

Wie Garnet funktioniert – Technische Architektur

Garnet bietet eine durchgängige Sicherheitsarchitektur für GenAI-Prozesse:

1. Geschützte Datenbasis

Interne Daten werden in einer Confidential VM hochgeladen, verschlüsselt, vektorisiert und in einer geschützten Vector Database gespeichert.

2. RAG – Antworten aus eigenen Datenbeständen

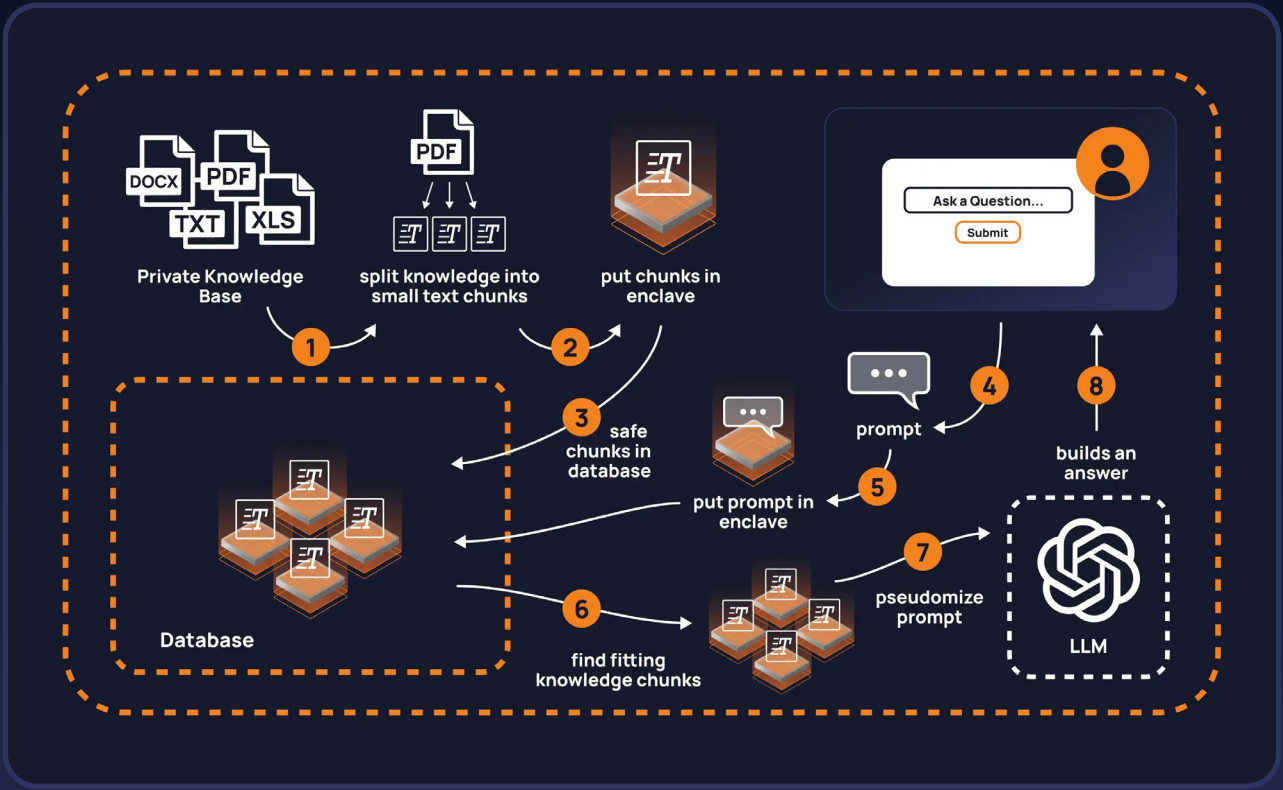
Nutzer stellen Fragen in natürlicher Sprache. Garnet analysiert diese, führt eine semantische Suche im internen Datenbestand durch und liefert erste Antworten – vollständig innerhalb der sicheren Enklave.

3. Pseudonymisierung & externe KI-Kommunikation

Sollen externe Modelle (z. B. OpenAI, Azure OpenAI, Anthropic) eingebunden werden, ersetzt Garnet zuvor identifizierte sensible Inhalte durch Pseudonyme. Persönliche Daten, Kundennamen oder IP verlassen nie die Enklave.

4. Antwortzusammenführung

Externe Antworten werden zurückgeführt, entschlüsselt, wieder mit Originalbegriffen angereichert und dem Nutzer als vollständiges Ergebnis präsentiert.



Die Vorteile von Garnet auf einen Blick

3D-Verschlüsselung
Daten sind durchgehend geschützt: im Ruhezustand, bei der Übertragung und während der Verarbeitung im Arbeitsspeicher.

Skalierbarkeit & Zukunftssicherheit
Horizontale Skalierung via Kubernetes, Post-Quanten-Krypto-grafie und API-Zugriff machen Garnet langfristig einsetzbar.

Effiziente Datennutzung & Kostenoptimierung
Durch Vorfilterung (RAG) werden nur relevante Inhalte an LLMs geschickt – Tokenverbrauch, Kosten und Risiken sinken drastisch.

Rechtssicherheit & Compliance-Nachweis
Attestation-Prüfungen, Audit-Logs und DSGVO-konforme Verarbeitung schaffen Nachweisbarkeit für Audits und Zertifizierungen.

Zero Trust & Confidential Computing
Hochsensible Workloads laufen ausschließlich in abgeschotteten Hardware-Enklaven – geschützt sogar vor Cloud-Admins, Service-Providern oder Root-Zugriffen.

Einfache Integration & keine Codeänderungen
Garnet integriert sich in bestehende IT-Systeme, Multi-Cloud-Umgebungen oder On-Premises-Infrastrukturen – ohne Entwicklungsaufwand.

Use Cases

- **Gesundheitswesen:** Verarbeitung von Patientendaten in KI-Systemen ohne Risiko von Datenlecks oder Verstößen gegen DSGVO/HIPPA
- **Finanzsektor:** Analyse sensibler Transaktionsdaten, Reports & Compliance-Dokumente mit KI – ohne Offenlegung kritischer Daten
- **Öffentliche Verwaltung:** Sichere KI-Nutzung trotz Geheimhaltungsstufen und Verwaltungsregularien
- **Industrie & Forschung:** Schutz von Betriebsgeheimnissen, Bauplänen, Algorithmen oder Forschungsdaten bei KI-gestützter Auswertung
- **Recht & Beratung:** Automatisierte Textanalyse, Vertragsprüfung und Wissensmanagement – vertraulich und revisionssicher

Fazit

Garnet ermöglicht, was bislang als Widerspruch galt: den Einsatz leistungsfähiger generativer KI bei gleichzeitiger Wahrung absoluter Vertraulichkeit und Datenhoheit.

Durch 3D-Verschlüsselung, Confidential Computing, Pseudonymisierung und RAG schafft enclaive eine sichere Infrastruktur, die Innovation nicht bremst, sondern beschleunigt. Unternehmen können KI endlich nutzen – ohne die Kontrolle über ihre Daten oder Compliance zu verlieren.

Nutzen Sie Generative KI – ohne Risiko

Kontaktieren Sie uns für eine persönliche Beratung oder eine sichere Testumgebung.

Weitere Informationen finden Sie unter:
https://www.enclaive.io/de/garnet-gen-ai-enterprise-firewall

Oder schreiben Sie uns eine Mail:
contact@enclaive.io