

enclave Garnet

Die GenAI Enterprise Firewall für sichere KI-Interaktionen

Die Nutzung von KI-Tools wie ChatGPT oder Gemini wächst rasant und verspricht enorme Produktivitätsgewinne. Gleichzeitig bremsen Datenschutzbedenken und regulatorische Unsicherheiten die Verwendung von generativer KI – dabei besteht gerade in regulierten Branchen wie der Verwaltung, dem Gesundheitswesen und dem Finanzsektor immenser Bedarf.

Mit der GenAI Enterprise Firewall **Garnet** von enclave bleiben alle KI-Interaktionen in vertraulichen Server- und Vektordatenbanken verschlüsselt und sensible Daten durchgehend geschützt. Garnet vektorisiert, filtert und pseudonymisiert Dokumente, bevor sie die KI erreichen und ermöglicht es so, GenAI DSGVO-konform und ohne Risiko für die eigenen Daten zu nutzen.

Herausforderungen

Unternehmen stehen bei der Nutzung von generativen KI-Systemen vor einer Reihe komplexer Herausforderungen. Dazu zählen die Einhaltung interner und externer Vorschriften, die Sicherheit sensibler Unternehmensdaten, die Abhängigkeit von einzelnen Anbietern und externe Modellbeschränkungen:



Compliance

Unternehmen müssen sich an zunehmend strenge Datenschutz- und Informationssicherheitsvorschriften wie die DSGVO, SGB IV, DORA oder NIS2 halten.



Sicherheit

Das Durchsickern vertraulicher Daten aufgrund öffentlicher oder falsch konfigurierter GenAI-Modelle sowie durch neuartige KI-Exploits stellt eine große Bedrohung für den Schutz sensibler Informationen und geistigen Eigentums dar.



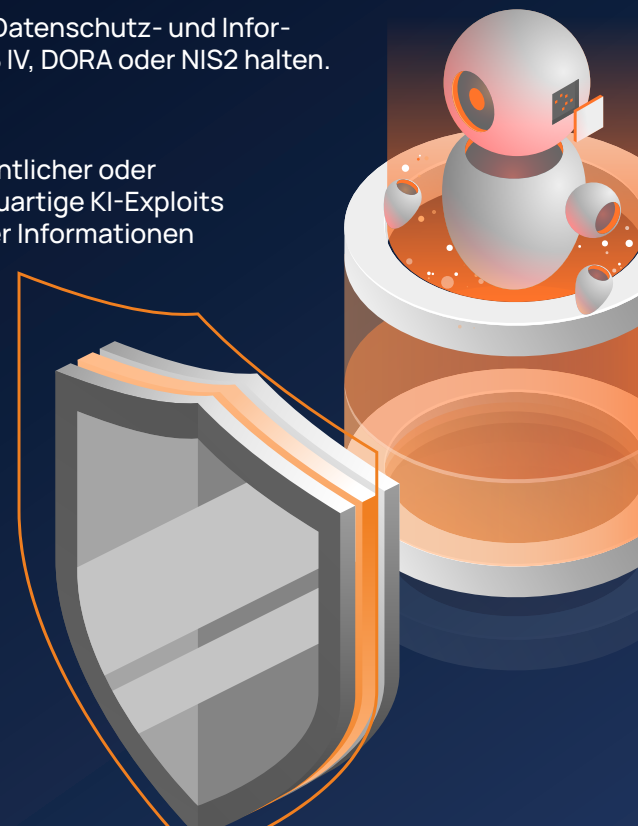
Herstellerabhängigkeit

Organisationen sind oft abhängig von den spezifischen Lösungen und dem Pricing eines Security-Herstellers, was die Wahl einer passenden GenAI-Firewall stark einschränken kann.



Externe Modellbeschränkungen

Gängige GenAI-Modelle rechnen nach dem Token-Pricing-Modell ab, wodurch die Kosten stark mit der genutzten Rechenleistung korrelieren. Unternehmen stehen vor dem Dilemma, entweder das Datenvolumen zu begrenzen oder ausufernde Kosten in Kauf zu nehmen.



Unsere Lösung

Unsere GenAI-Firewall Garnet kombiniert intelligent eine Reihe moderner Technologien, um sicherzustellen, dass Sie generative KI-Systeme sicher und wirtschaftlich nutzen können.

3D-Verschlüsselung

Garnet basiert auf Confidential Computing, der durchgängigen Verschlüsselung von Daten in allen drei Dimensionen (at rest, in transit, in use). Die Kommunikation mit externer GenAI erfolgt aus sicheren Enklaven.

Vektorisierung

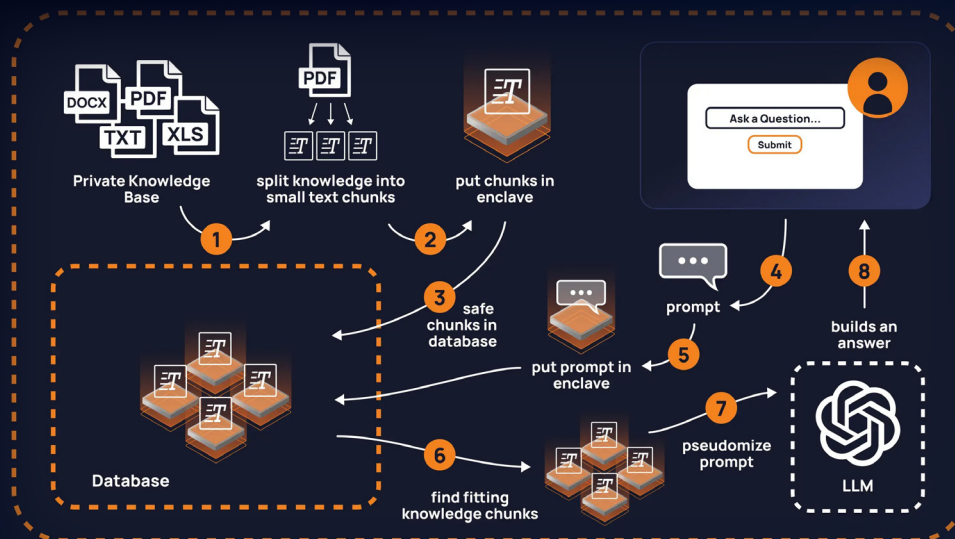
Garnet vektorisiert eigene Datenbestände in einer mit Metadaten angereicherten Vector Data Base. Interne Informationen lassen sich so im Sinne einer Retrieval Augmented Generation (RAG) sicher nutzen.

Vorfilterung

Da Garnet bei einer Interaktion bereits zielführende Informationen herausfiltert, reduziert sich das in die externe KI-Kommunikation eingespeiste Datenvolumen signifikant.

Pseudonymisierung

Vor der Interaktion mit GenAI-Tools ersetzt Garnet schützenswerte Daten automatisch durch pseudonymisierte Informationen – auf Basis einer individuellen Replacing Map.



Warum Sie auf Garnet setzen sollten

- **Maximale Sicherheit:** Confidential Computing schützt Daten auch während der Verarbeitung in RAM oder CPU. Sogar Cloud Service Provider oder Administratoren haben jetzt keinen Zugriff.
- **Intuitive Nutzung:** Nutzer kommunizieren in natürlicher Sprache über ein grafisches User Interface, was Akzeptanz steigert und den Einsatz von Schatten-IT verhindert.
- **Lückenlose Compliance:** Durch die robusten Verschlüsselungs- und Pseudonymisierungsmechanismen können jetzt sogar Unternehmen aus kritischen Sektoren von modernen KI-Systemen profitieren.
- **Kosteneffizienz:** Die intelligente Vorfilterung verringert das eingespeiste Datenvolumen und damit die Kosten generativer KI. Die Herstellerunabhängigkeit und nahtlose Integration in bestehende Infrastruktur minimiert zudem den Implementierungsaufwand.