enclaive Garnet

enclaive Garnet

The GenAI enterprise firewall for secure AI interactions

The use of AI tools such as ChatGPT or Gemini is growing rapidly, promising enormous productivity gains. At the same time, data protection concerns and regulatory uncertainty are slowing down the adoption of generative AI—even though highly regulated sectors such as government, healthcare, and finance have an urgent need for it.

With **Garnet**, enclaive's GenAI Enterprise Firewall, all AI interactions remain encrypted in confidential server and vector databases, ensuring continuous protection for sensitive information. Garnet vectorizes, filters, and pseudonymizes data before it reaches a LLM, enabling organizations to use generative AI in full compliance with GDPR—without risking data exposure.

Challenges

Enterprises face a wide range of challenges when deploying generative AI—from regulatory compliance and data security to vendor lock-in and model constraints:

Compliance

Companies must comply with increasingly strict data protection and information security regulations such as GDPR, DORA, or NIS2.

Security

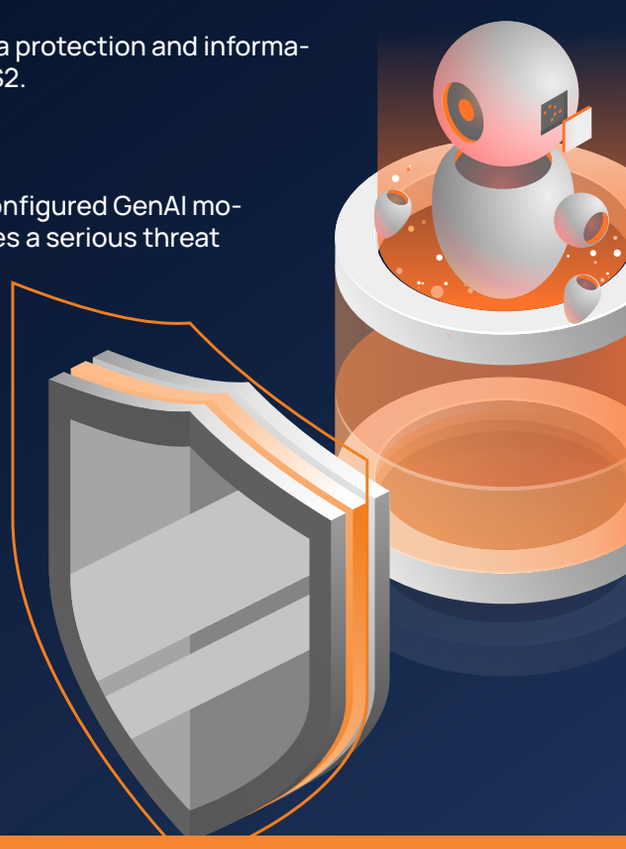
Leakage of confidential data through public or misconfigured GenAI models—or through emerging AI-specific exploits—poses a serious threat to sensitive information and intellectual property.

Vendor Lock-In

Organizations are often dependent on specific vendors (and their pricing), which limits flexibility in selecting or adapting a GenAI firewall.

External Model Constraints

Common GenAI models operate on token-based pricing, where computational cost directly correlates with input volume. As a result, companies must either restrict data usage or accept rapidly increasing costs.



Our Solution

Garnet, enclaive's GenAI Firewall, intelligently combines multiple state-of-the-art technologies to ensure that you can leverage generative AI models securely, efficiently, and economically.

3D Encryption

Garnet is built on Confidential Computing, ensuring data encryption across all three dimensions—at rest, in transit, and in use. Communication with external GenAI models occurs only from within secure enclaves.

Vectorization

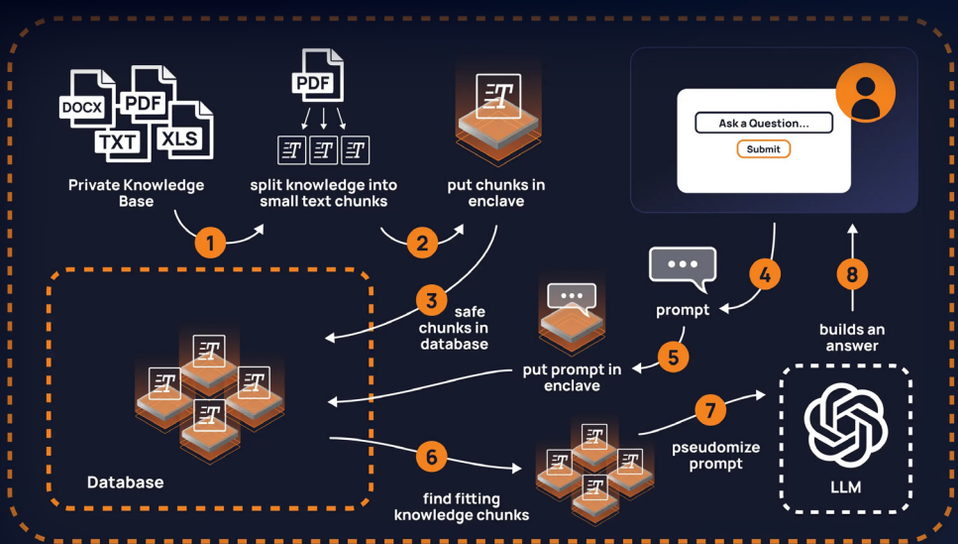
Garnet converts enterprise data into encrypted vector representations stored in a metadata-enriched vector database. This enables secure retrieval-augmented generation (RAG) using internal knowledge.

Pre-Filtering

By extracting only the relevant context before each AI interaction, Garnet significantly reduces the data volume transmitted to external models—improving cost efficiency and minimizing the risk of data exposure.

Pseudonymization

Before interacting with GenAI tools, Garnet automatically replaces sensitive information with pseudonymized data—based on a customizable replacement map. Personal and confidential details never leave your secure environment.



Why Choose Garnet

- **Maximum Security:** Confidential Computing protects data even during processing in memory or on the CPU. Not even cloud service providers or administrators have access.
- **Intuitive Use:** Users interact naturally via a graphical user interface, enhancing acceptance and preventing shadow IT.
- **Seamless Compliance:** Robust encryption and pseudonymization mechanisms allow even organizations in critical sectors to safely benefit from generative AI.
- **Cost Efficiency:** Smart pre-filtering minimizes the data volume and reduces GenAI costs. Additionally, vendor independence and seamless integration into existing infrastructures simplify implementation.

Learn more:
enclaive.io/garnet-gen-ai-enterprise-firewall

Mail: contact@enclaive.io
Tel.: +49 302 33 29 29 73
Chausseestr. 40, Berlin, Germany