

# Garnet: The enclave GenAI Enterprise Firewall

A Comprehensive Solution to  
leverage LLMs and SLMs in  
Enterprise



**You will read about:**

1. Introduction.....	3
2. Benefits of Using Garnet.....	4
3. Challenges Solved by eMCP.....	5
4. Technical Features of Garnet.....	7
5. Architectural Overview.....	11
6. Design Principals.....	12
7. Conclusion.....	13
8. About enclave.....	14

## Introduction

Companies today face significant challenges when using Generative AI, large language models (LLMs), and specialized language models (SLMs). Beyond the need to comply with regulations and protect personal data, there is a critical need to safeguard internal data and intellectual property (IP). Additionally, companies must manage large volumes of data cost-effectively for analysis.

Garnet, developed by enclave, addresses these challenges by **providing a secure and compliant solution for interacting with AI systems**. This whitepaper explores Garnet's relevance across various sectors and its robust technical foundations that ensure data security and privacy.

## What is Garnet?

- Garnet is an advanced product developed by enclave. It **allows secure interactions with AI systems**, particularly LLMs, while ensuring data privacy and regulatory compliance.
- Garnet's architecture, which includes **data vectorization, pre-filtering, and pseudonymization**, makes it suitable for various AI applications beyond just LLMs.

# Benefits of Using Garnet

## Enhanced Privacy

Garnet ensures no sensitive company data is exposed, maintaining high standards of data privacy.

## Cost-Effectiveness

Garnet allows companies to ingest vast amounts of internal data without the constraints of external model limitations, reducing financial burdens and eliminating the need for additional security measures.

## Trustworthy Environment

Garnet builds trust through comprehensive 3D encryption, securing data at rest, in transit, and during processing. This ensures that all data is completely shielded and protected at every stage.

## Scalability

Suitable for organizations of any size, from small businesses to large enterprises.

## Improved Efficiency

Streamlines secure data interactions, enhancing productivity.



# Challenges Solved with Garnet

## Did you know?

- In 92% of Fortune 500 companies, employees are already using ChatGPT at work.

### **Regulatory Compliance**

Regulated industries must adhere to strict data protection laws such as GDPR and HIPAA. Garnet ensures compliance by encrypting all data interactions and maintaining confidentiality.

### **Data Leakage**

Leakage of sensitive/customer data due to public or misconfigured LLM.

### **Data Volume and Confidential Integration:**

Garnet breaks down data volume limitations, enabling the confidential integration of internal data from any source. This allows companies to leverage vast amounts of data securely and efficiently, without being bound by external model constraints.

### **Data Privacy**

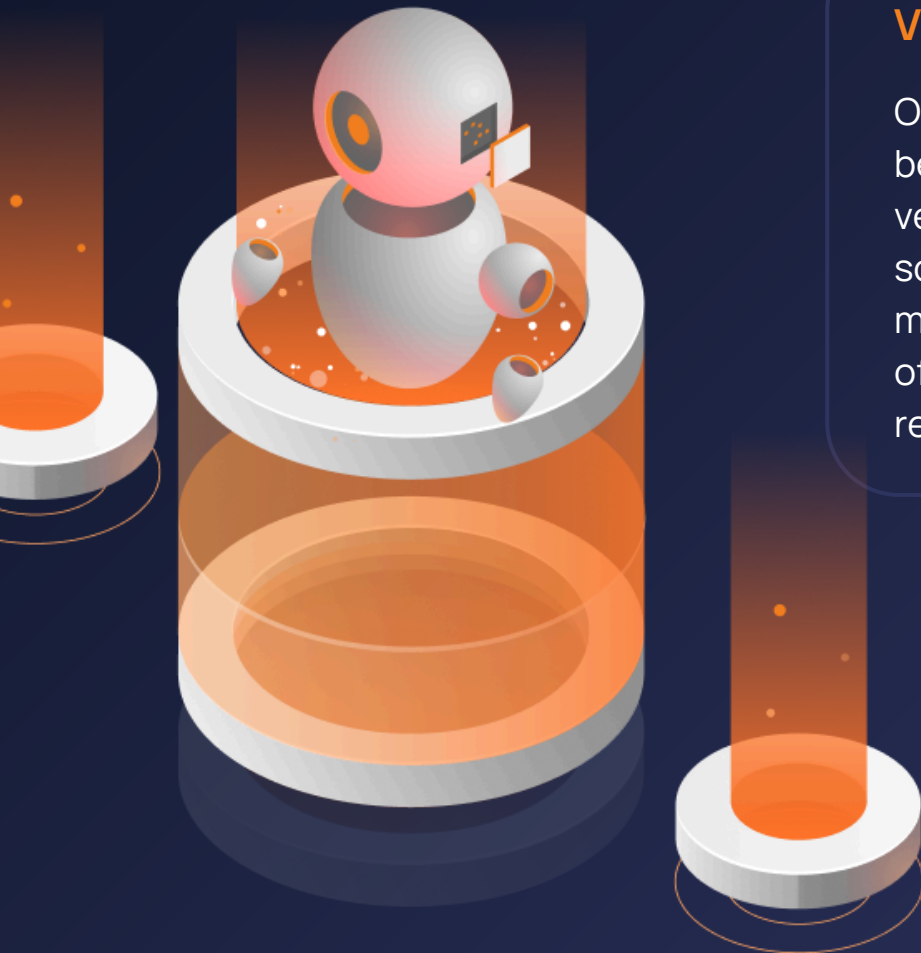
Safeguarding sensitive information and intellectual property is crucial. Garnet pseudonymizes data before interacting with AI systems, ensuring no identifiable information is exposed.

### **AI Exploits**

Newly introduced AI attack vectors like prompt injection, jailbreaking, malicious code/data retrieval, and more. Make sure you get visibility across your GenAI activity through threat detection.

### **Vendor Dependency**

Organizations often become reliant on specific vendors for their security solutions. Garnet's design minimizes vendor lock-in, offering flexibility and reducing costs.



# Technical Features

## Overview

### **Confidential Computing Environment**

Garnet runs on confidential virtual machines (VMs) with hardware-based isolation, ensuring data security from unauthorized access, even by cloud service providers.

### **Retrieval Augmented Generation**

With retrieval-augmented generation, users essentially have conversations with data repositories containing their own documents, opening up new kinds of experiences.

### **Prompt Pseudonymization**

Before a prompt is sent to an external LLM or SLM, sensitive data is context-aware pseudonymized, replacing identifiable information with pseudonyms.

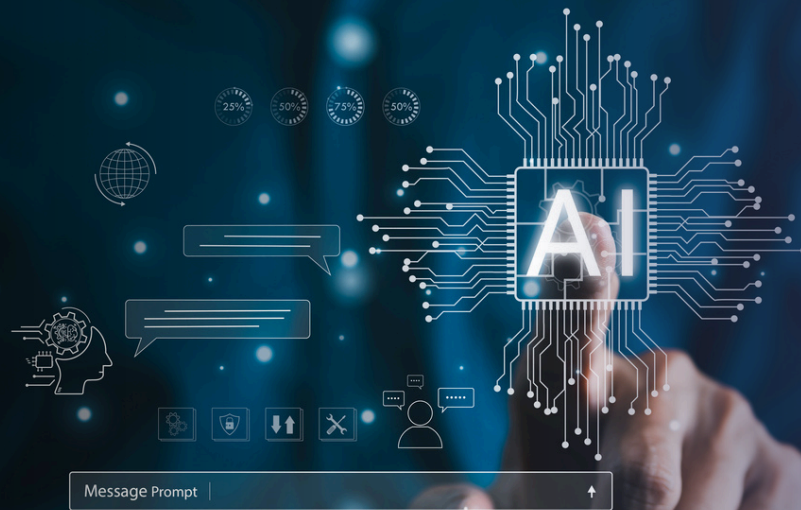
### **Groundbreaking End-to-End Encryption**

Garnet ensures end-to-end encryption for all data and document interactions, maintaining confidentiality throughout the pipeline in transit, at rest and most notably in use.

### **Customizable Security Policies and Seamless Integration**

Organizations can tailor security policies to meet specific regulatory and operational requirements. Garnet integrates seamlessly with existing IT infrastructures, supporting on-premise, cloud, and hybrid environments.





## UI Features

### **User-Friendly Interface**

Designed for ease of use without compromising security, providing an intuitive interface for users to interact with the system, upload documents, and perform queries.

### **Secure File-Based Chatting**

Enables conversational data interactions through secure file uploads and natural language queries, supporting both German and English languages.

### **Customizable Prompts and Editable Responses**

Allows customization of prompts sent to AI systems, tailoring responses to specific needs. Users can adjust the number of sentences returned from searches for flexible data interaction.

### **Authentication and Secure Rooms**

Secure user login facilitated through Auth0, ensuring secure access. Supports creating different rooms for various contexts, enhancing data organization and security.

### **Demo Mode**

Includes a demo mode with preloaded files, allowing users to explore the application's capabilities without risking sensitive data.



# Architectural Overview

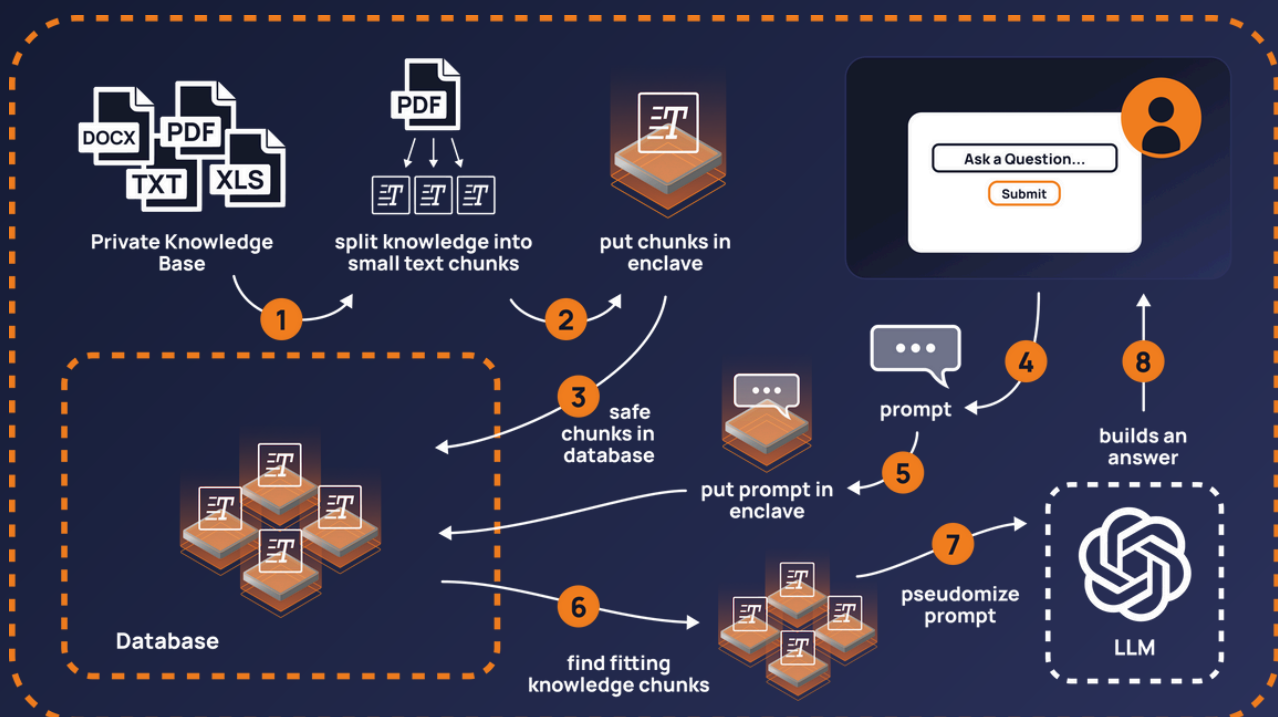
Garnet is structured into distinct layers:

**Data Ingestion Layer:** Handles secure data upload and initial processing.

**Pre-Processing Layer:** Implements data vectorization, pre-filtering, and pseudonymization.

**Core Processing Layer:** Executes secure queries and interactions with AI systems within secure enclaves.

**Output Layer:** Manages the delivery of encrypted and pseudonymized responses to users.



# Design Principals

## Isolation and Confidentiality

- Garnet employs buckypaper virtualization for creating secure enclaves.
- Data remains encrypted throughout the processing lifecycle, ensuring confidentiality and integrity.

## Performance and Scalability

- Garnet is designed to scale horizontally, supporting increased loads by adding more instances.
- Utilizes Kubernetes for orchestration, ensuring efficient resource management and high availability.

## Compliance and Auditing

- Garnet maintains logs for all data interactions, facilitating auditing and compliance with regulations like GDPR and HIPAA.
- Provides detailed reporting capabilities to demonstrate compliance efforts.



# Conclusion

Garnet by enclave stands as a pioneering solution for regulated industries seeking to **leverage advanced AI technologies** while **ensuring data privacy and regulatory compliance**.

Its robust security features, seamless integration capabilities, and cost-effective approach make it an **indispensable tool** for businesses in sectors such as government, healthcare, and financial services.

# Further Reading

For a deeper understanding of confidential computing and its benefits, refer to the following resources:

- [Confidential Computing 101](#)
- [enclave Garnet](#)
- [Get a free demo](#)

For personalized advice and deployment options, contact enclave at [contact@enclave.io](mailto:contact@enclave.io).

## About enclave

enclave GmbH, an **award-winning** start-up based in Berlin, Germany, helps businesses protect their **sensitive data and applications in untrusted cloud environments** through Confidential Computing.

Its comprehensive, multi-cloud operating system allows for **Zero Trust security** by encrypting data in use and shielding applications from both the infrastructure and solution providers.

With enclave, businesses can confidently **build, test, and deploy a wide range of cloud applications**, all while maintaining **complete control over their confidential information**.

enclave's goal is to provide **a universal, cloud-independent technology** for enclaving sophisticated multi- cloud applications, that can be deployed with confidence and ease.

### Contact details

[github.com/enclave](https://github.com/enclave)

[contact@enclave.io](mailto:contact@enclave.io)

[linkedin.com/company/enclave](https://linkedin.com/company/enclave)

+49 302 33 29 29 73

[youtube.com/@confidentialcompute](https://youtube.com/@confidentialcompute)

Chausseestr. 40, Berlin, Germany