

enclave Garnet

The enclave GenAI Enterprise Firewall



Secure Your Conversations:

Garnet is a cutting-edge solution designed to **meet the needs of regulated industries**, such as government and eHealth, which have stringent data privacy requirements.

Leveraging confidential computing, Garnet enables secure interactions with large language models (LLMs) like ChatGPT. This product **ensures that sensitive information remains protected** throughout the data interaction process.

By using advanced security measures, including confidential servers and vector databases, Garnet keeps all sensitive information confidential while **allowing users to benefit from the power of LLMs**.

Why Garnet?

In today's regulated industries, the demand for utilizing LLMs like ChatGPT is high, but **regulatory constraints make it difficult**.

Discussions with enclave.io customers, particularly in government and eHealth, highlight a significant need - they want to use these technologies but aren't allowed to due to **data privacy concerns**.

Garnet targets these sectors by taking documents, vectorizing them, pre-filtering, generating prompts, and pseudonymizing them before contacting ChatGPT or another LLM.

This process **ensures that no sensitive company data is exposed to the LLM**, maintaining GDPR compliance. Technically, it uses a Qdrant vector database and runs entirely in a confidential enclave cloud.



Key Features



Complete Data Security

All data interactions are encrypted to prevent unauthorized access.



Confidential Server

The server environment is isolated and secure, ensuring data privacy.



Seamless Integration

Easily integrates with existing IT infrastructure and workflows.



Advanced Authentication

Supports multi-factor authentication to enhance security.



Customizable Policies

Tailor security policies to meet specific organizational needs.



Real-time Monitoring

Continuous monitoring and alerts for any suspicious activities.



User-friendly Interface

The platform is designed for ease of use without compromising on security.

Benefits

▶▶ Enhanced Privacy

Ensures that sensitive information remains confidential.

▶▶ Cost-effective

Reduces the need for additional security measures, saving costs.

▶▶ Regulatory Compliance

Adheres to data protection regulations, helping organizations stay compliant.

▶▶ Operational Flexibility

Supports various deployment models, including on- premise, cloud, and hybrid environments.

▶▶ Scalability

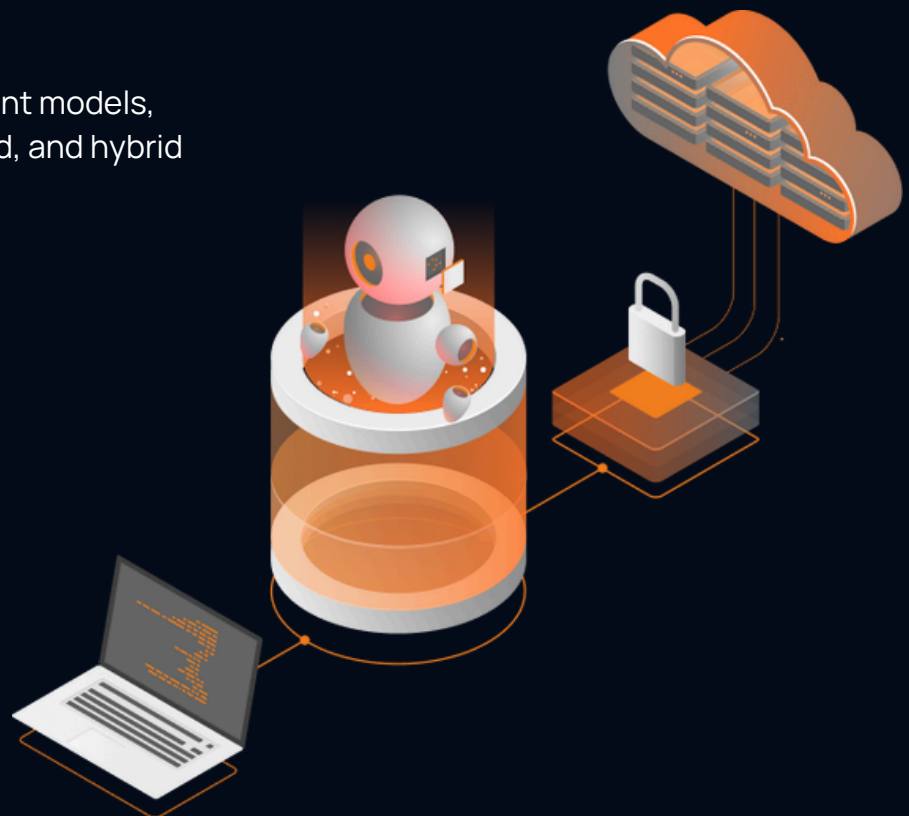
Can be scaled to fit organizations of any size, from small businesses to large enterprises.

▶▶ Improved Efficiency

Streamlines secure data interactions, improving productivity.

▶▶ Trustworthy Environment

Builds trust with clients and stakeholders by ensuring data security.





Detailed Use Case

Healthcare Sector:

Problem:

Healthcare providers need to access and share sensitive patient information while maintaining strict privacy standards and complying with regulations like HIPAA.

Solution:

Garnet allows healthcare professionals to securely interact with patient data using natural language queries. It ensures that all data interactions are encrypted and confidential, protecting patient information from unauthorized access.

Implementation

Secure Data Upload

- Patient records are securely uploaded to the platform.

Confidential Queries

- Healthcare providers can query patient data using ChatGPT without exposing sensitive information.

Protected Responses

- The platform provides encrypted responses, ensuring data privacy.

Compliance

- Ensures all interactions meet HIPAA and other regulatory requirements.



Detailed Use Case

Healthcare Sector:

Benefits

▶▶ Enhanced Data Security

Keeps patient data secure and confidential.

▶▶ Improved Access

Facilitates easy and secure access to patient information.

▶▶ Regulatory Compliance

Helps healthcare providers comply with data protection regulations.

▶▶ Operational Efficiency

Streamlines data access and interaction, improving patient care.

Learn more

About enclave

enclave enables businesses to securely **protect their sensitive data and applications in untrusted cloud environments** by leveraging the use of 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



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



<https://enclave.io>



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

CONTACT

contact@enclave.io

+49 30233292973

Chausseestr. 40, 10115 Berlin, Germany
enclave.io



Making the Cloud the safest place for digital businesses