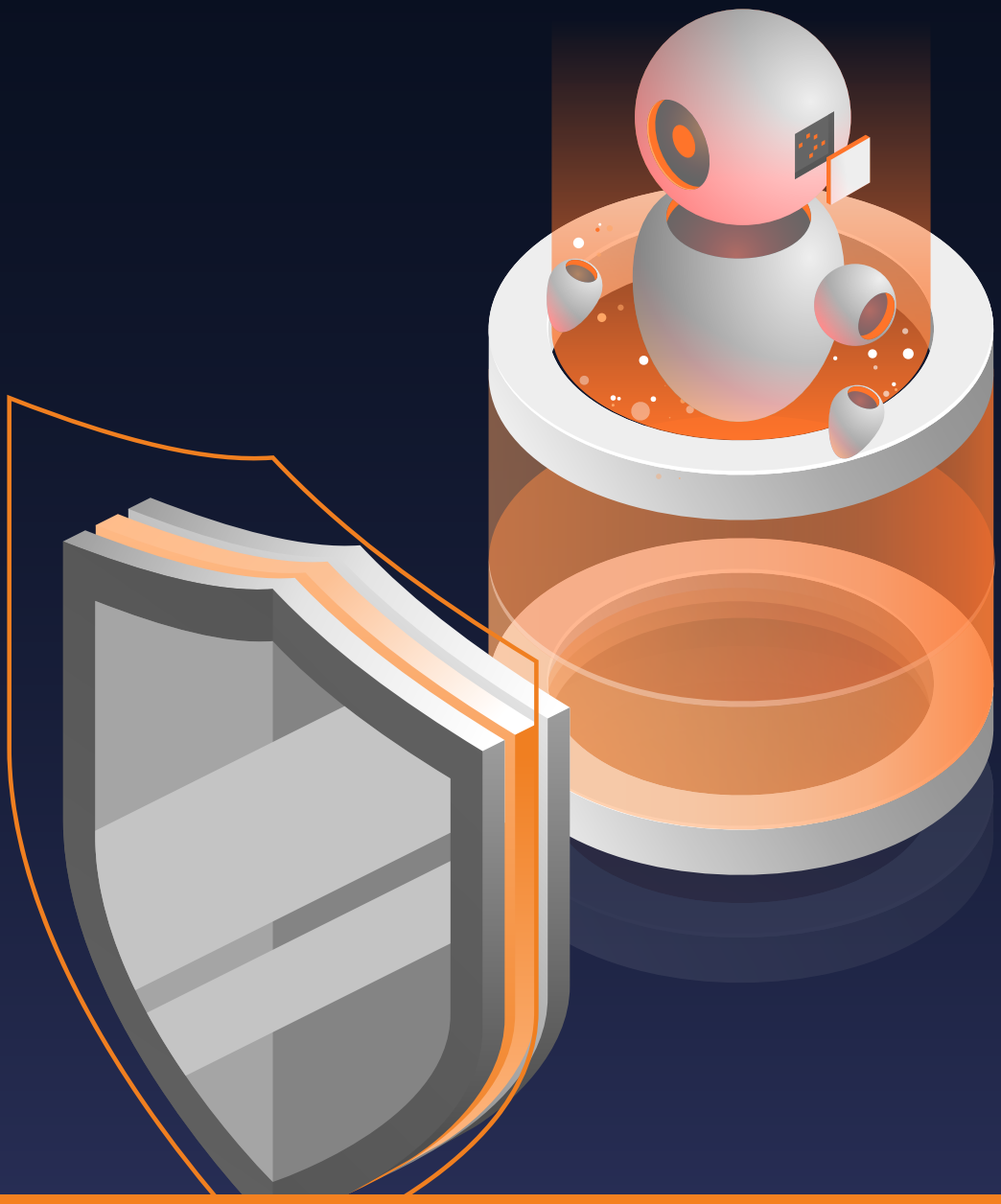
enclaive

Solution Brief

Secure Use of GenAI

How enclaive's GenAI firewall Garnet combines confidentiality, compliance and innovation



Executive Summary

Generative AI is changing the way companies use knowledge, control processes and drive innovation – but it also increases the risks to data protection, compliance and intellectual property. Many organisations are therefore faced with a key question: how can the potential of AI be exploited without losing control of sensitive information?

Garnet, enclaive's GenAI firewall, provides the answer. Garnet protects sensitive information at all stages of processing through hardware-based isolation, end-to-end encryption and automatic pseudonymisation. This allows companies to interact with GenAI without disclosing confidential data or violating regulatory requirements.

Garnet integrates seamlessly into existing IT environments, reduces costs through targeted data pre-processing (RAG) and offers flexibility across multi-cloud and on-premises scenarios. This creates a secure foundation for the responsible use of GenAI – with full data control, legal verifiability and preservation of digital sovereignty.

The Challenge: Using AI – Without Disclosing Data

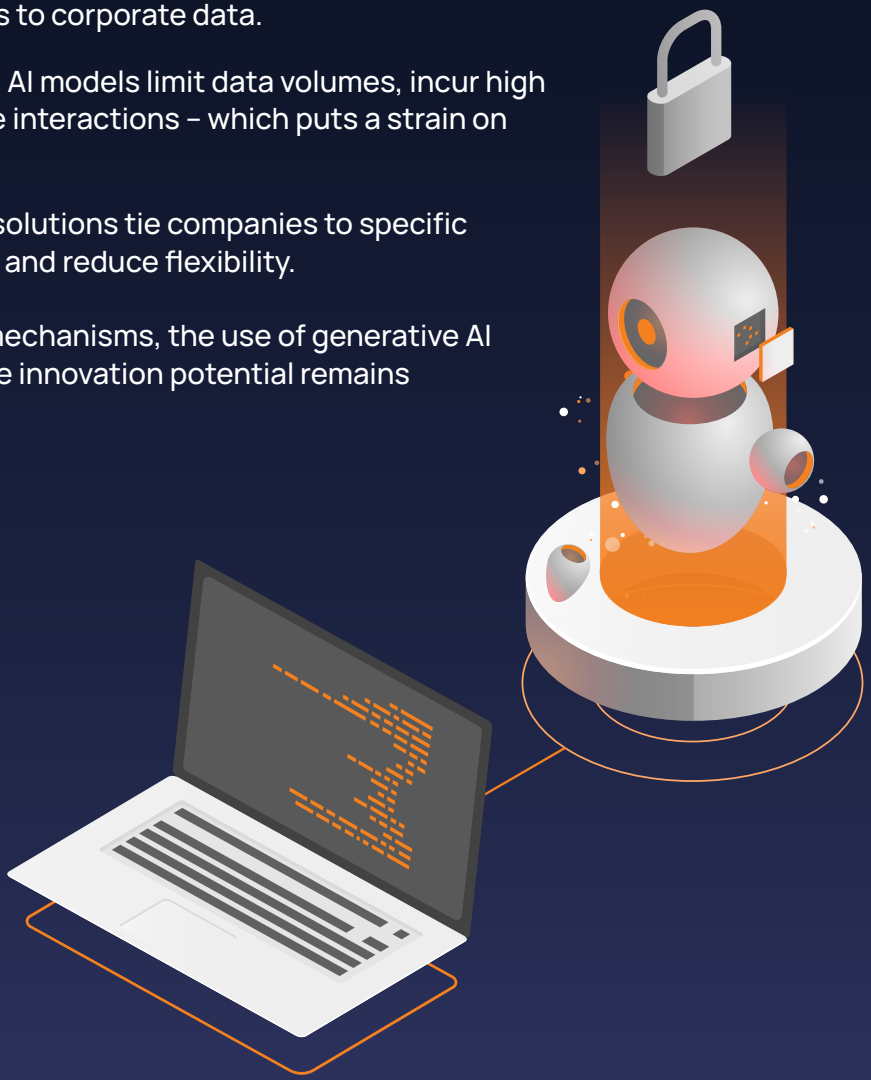
Generative AI is currently shaping the digital transformation – from large language models (LLMs) such as ChatGPT to industry-specific special models (SLMs) and internal AI applications. Companies, public authorities and institutions are already using AI extensively to automate processes, make knowledge available and improve decision-making. At the same time, new risks are emerging: sensitive data could find its way into public AI systems, regulatory requirements could be violated, or intellectual property could be disclosed.

Organisations in strictly regulated industries such as healthcare, public administration and finance face a particular dilemma: they want to harness the potential of generative AI, but cannot risk data loss, legal violations or loss of control.

The use of AI comes with a number of risks and hurdles:

- **Risk of Data Leaks:** Sensitive information can end up in public LLMs via chat entries or documents, where it can be stored, reused or disclosed without control.
- **Regulatory Pressure:** GDPR, HIPAA, DORA, NIS2 and industry-specific requirements demand the protection of personal data – even during processing. However, technical proof of confidentiality is often lacking.
- **New Attack Vectors:** Prompt injection, jailbreaking, response manipulation, and API exploitation create new threats to corporate data.
- **Operational Limitations:** External AI models limit data volumes, incur high token costs and permanently store interactions – which puts a strain on compliance and budgets.
- **Vendor Lock-in:** Many AI security solutions tie companies to specific providers, complicate integrations and reduce flexibility.

The result: without suitable security mechanisms, the use of generative AI is blocked in many areas – and valuable innovation potential remains untapped.



The Solution: Garnet – enclaive's GenAI Firewall

Garnet is a GenAI firewall developed by enclaive that enables secure interactions with generative AI systems while maintaining data sovereignty, compliance and intellectual property.

What Sets Garnet Apart

- AI communication takes place exclusively within confidential, hardware-isolated enclaves (confidential VMs).
- Data is encrypted in all three dimensions: at rest, in transit and in use (3D encryption).
- In the spirit of retrieval augmented generation (RAG), users can first chat with the company's internal database before consulting external models.
- Before each external AI query, sensitive information is automatically pseudonymised or filtered.
- Responses from external systems are decoded within the enclave, enriched with original data, and only then displayed to the user.

This creates an environment in which companies can use confidential data with generative AI systems – without losing control.

Why enclaive?

enclaive is a Berlin-based company and is therefore subject to German and European jurisdiction. The company is a leader in the field of confidential computing and develops solutions for security-critical organisations and regulated industries.

The Advantages of enclaive

Sovereignty and data protection in accordance with European law	Technology leader in confidential computing and enclave technology	No vendor lock-in: hybrid, multi-cloud and on-premises operating models
Post-quantum security and zero-trust architecture	Minimal performance overhead (<3%)	Seamless integration without code changes

How Garnet works – Technical Architecture

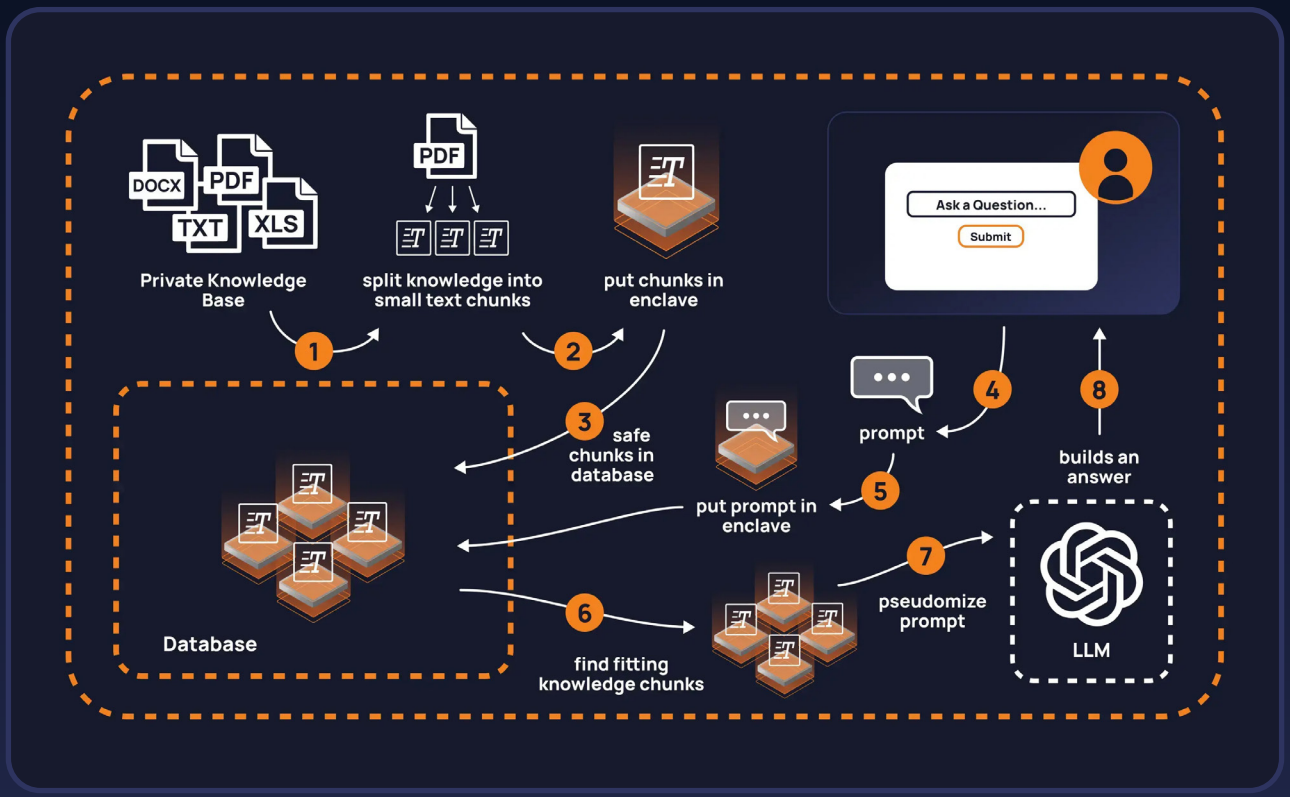
Garnet offers an end-to-end security architecture for GenAI processes:

1. Protected Database
Internal data is uploaded to a confidential VM, encrypted, vectorised and stored in a protected vector database.

2. RAG – Answers From Your own Data Sets
Users ask questions in natural language. Garnet analyses these, performs a semantic search in the internal database and provides initial answers – all within the secure enclave.

3. Pseudonymisation & External AI Communication
If external models (e.g. OpenAI, Azure OpenAI, Anthropic) are to be integrated, Garnet replaces previously identified sensitive content with pseudonyms. Personal data, customer names or IP never leave the enclave.

4. Response Consolidation
External responses are returned, decrypted, enriched with original terms and presented to the user as a complete result.



Key Benefits of Garnet

3D Encryption
Data is protected at all times: at rest, during transmission and while being processed in the working memory.

Scalability & Future-Proofing
Horizontal scaling via Kubernetes, post-quantum cryptography and API access make Garnet suitable for long-term use.

Efficient Data Usage & Cost Optimization
Pre-filtering (RAG) ensures that only relevant content is sent to LLMs – drastically reducing token consumption, costs and risks.

Legal Certainty & Proof of Compliance
Attestation checks, audit logs and GDPR-compliant processing provide verifiability for audits and certifications.

Zero Trust & Confidential Computing
Highly sensitive workloads run exclusively in isolated hardware enclaves – protected even from cloud administrators, service providers or root access.

Easy integration & no code changes
Garnet integrates into existing IT systems, multi-cloud environments or on-premises infrastructures – without any development effort.

Use Cases

- **Healthcare:** Processing patient data in AI systems without the risk of data leaks or violations of GDPR/HIPAA
- **Financial sector:** Analysis of sensitive transaction data, reports and compliance documents with AI – without disclosure of critical data
- **Public administration:** Secure use of AI despite confidentiality levels and administrative regulations
- **Industry & research:** Protection of trade secrets, construction plans, algorithms or research data in AI-supported evaluation
- **Law & consulting:** Automated text analysis, contract review and knowledge management – confidential and audit-proof

Conclusion

Garnet allows what was previously considered a contradiction: the use of powerful generative AI while maintaining absolute confidentiality and data sovereignty.

Through 3D encryption, confidential computing, pseudonymisation and RAG, enclaive creates a secure infrastructure that accelerates innovation rather than slowing it down. Companies can finally use AI without losing control over their data or compliance.

Use generative AI – without risk

Contact us for a personal consultation
or a secure test environment.

Further information can be found at:
https://www.enclaive.io/garnet-gen-ai-enterprise-firewall

Or send us an email:
contact@enclaive.io