OBSYDIA TECHNOLOGIES

Self-Hosted Security Infrastructure

for the Privacy-First Enterprise

Technical Whitepaper · March 2026

obsydia.tech

GENESIS

Why Obsydia Exists

Obsydia Technologies was founded on a simple observation: European businesses are caught between increasingly strict data protection regulations and technology infrastructure they cannot fully control. GDPR's promise of data sovereignty rings hollow when your encryption keys live in AWS, your audit logs flow through Google Cloud, and your compliance posture depends on the security practices of American technology giants.

The founders — seasoned infrastructure engineers who spent years implementing compliance frameworks for regulated industries — recognized that self-hosted infrastructure was not just a technical preference, but a legal and business necessity for European companies serious about data protection.

The Problem We Set Out to Solve

Existing solutions fell into two camps: cloud-based services that traded control for convenience, and complex enterprise software that required dedicated platform teams to deploy and maintain. Neither addressed the core need of European SMBs: military-grade data protection infrastructure that could be deployed and operated without a team of DevOps specialists.

GDPR's technical requirements — particularly around data minimization, purpose limitation, and the right to erasure — demanded more than bolt-on security. They required infrastructure designed from the ground up to treat personal data as a special, protected class of information.

Our Approach

Obsydia Core0 embodies three design principles that distinguish it from alternatives:

Zero Trust by Default: Every service-to-service connection uses mutual TLS. There are no shared secrets, no default passwords, no configuration that weakens security for convenience.

Operator-Grade Simplicity: One-hour deployment from bare metal to production-ready cluster. The complexity is hidden, not eliminated — but hidden behind interfaces that non-specialists can operate safely.

European Data Sovereignty: Your data, your servers, your jurisdiction. No dependencies on cloud providers, no international data transfers, no vendor access to your infrastructure.

EXECUTIVE SUMMARY

The Problem with Sensitive Data in the Modern Enterprise

Every organisation that handles personal data faces the same fundamental tension: business systems need access to sensitive information, but regulators, customers, and security teams demand that access be controlled, audited, and reversible. Most organisations resolve this tension poorly — they bolt security onto existing systems after the fact, accept the terms of cloud providers they cannot fully control, or spend millions on enterprise vault software that takes months to deploy.

Obsydia Core0 takes a different approach. It is security infrastructure designed from the ground up to be self-hosted, operator-grade, and deployable in under an hour. Built for European SMBs and regulated industries that cannot afford to get data protection wrong.

Problem it solves	Secure storage and management of PII, encryption keys, and secrets — without cloud dependency
Target customers	European SMBs · fintech · healthtech · legaltech · any organisation handling regulated data
Deployment	Self-hosted on your infrastructure — bare metal or private cloud
Time to deploy	Under one hour with Bootstrap wizard — no DevOps expertise required
Compliance	GDPR Art. 17/25/30/32 · designed for ISO 27001 environments

THE PROBLEM

Why Existing Solutions Fall Short

Cloud Vaults Create New Dependencies

AWS Secrets Manager, Azure Key Vault, and HashiCorp Vault Cloud solve the technical problem of key management — but they introduce a new one. Your most sensitive data and the keys to decrypt it now live in someone else's infrastructure. For European companies subject to GDPR, this creates real legal exposure around data residency, international transfers, and vendor access.

> *"We needed to demonstrate to our auditors that no third party — including our cloud provider — had the technical ability to access our customers' personal data. No cloud vault could give us that guarantee."*
> ***— Chief Security Officer, European fintech***

Self-Hosted Alternatives Are Too Complex

HashiCorp Vault Enterprise is a powerful tool. It is also a product that requires dedicated platform engineers to deploy, maintain, and operate. For a 20-person startup or a 200-person regulated business, the operational overhead is prohibitive. Configuration mistakes in a complex system create exactly the vulnerabilities the system was meant to prevent.

The Compliance Gap

GDPR's right to erasure (Article 17) is not just about deleting a database record. It requires that the data is truly gone — from all storage layers, including write-ahead logs, backups, and replication streams. Most systems cannot demonstrate this. Obsydia Core0 was designed specifically to close this gap.