

# SynaptoSec Security Architecture

## Whitepaper - Executive Brief

VERSION: v2.4 (September 2026)

AUTHORS: SynaptoSec Infrastructure & Systems Security Group

SOURCE: [synaptosec.com/legal/security](https://synaptosec.com/legal/security)

**DRAFT - PENDING LEGAL REVIEW. This text is not yet in force.**

### Summary

Comprehensive public analysis of our zero-trust infrastructure in Amsterdam, Argon2id key derivation, and MITRE ATLAS matrix compliance.

### In this brief

- EU-hosted infrastructure (Amsterdam) without US hyperscaler virtualization dependencies
- Strict TLS 1.3 ingress and mTLS inter-process communication
- Operational security lifecycle of the inspection path
- Cryptographic Argon2id salted API token storage and token bucket rate limits

*From the published security page ([synaptosec.com/legal/security](https://synaptosec.com/legal/security))*

Every blocked event is mapped to a MITRE ATLAS technique, tactic, and URL. Examples: Prompt injection - AML.T0051 (LLM Prompt Injection); Tool result injection - AML.T0053 (LLM Plugin Compromise); MCP tool poisoning - AML.T0053 (LLM Plugin Compromise).

Breach notification: customers within 72 hours (Art. 33 GDPR). Responsible disclosure: we do not pursue legal action against good-faith security researchers.

Operational limitations, as published: current deployment is single-node (HA topology documented but not yet deployed); the LLM guard runs on external providers with graceful degradation - degradation is verified: 13/15 hardest attacks still block even with the LLM guard fully unavailable; state persistence flushes every 5 seconds.

### About this document

This executive brief is distilled from the published page listed above, which remains the full, current version. It contains no data beyond what is published there. These are self-published whitepapers - cite as SynaptoSec whitepapers.

