

SECURITY NODES: PROTECTING CLIENT PII IN LLM FLOWS

Security is the "Non-Negotiable" of high-ticket AI. Sending Personally Identifiable Information (PII) directly to an LLM is a security risk. we architect a buffer.

THE SANITIZATION GATEWAY

Before a user's input reaches the LLM, it passes through a **Sanitization Gateway**. We use regex and custom JavaScript blocks to strip or redact sensitive info like SSNs or private IDs, sending only the context required for the conversation to continue.

ON-PREM VS. API

For high-security clients, we offer logic flows that keep data processing within a private cloud, ensuring that your proprietary business intel never trains a public model.