SecureAgent AIPrivacy Firewall for the Enterprise

Real-time prompt interception. Zero Storage. Zeroegress. Built forteams that ship AI at scale.

100% Stateless · no prompt retention	**<1s** Avg. mask time per artifact	**0 B** Data transmitted externally

WHAT IT DETECTS

Six threat classes.
One interceptor.

- **PII** Emails, phone numbers, names and identity data.
- **Credentials** API keys, tokens and authentication secrets.
- **Financial Data** Card numbers, account details and transaction records.
- **Business / Internal** Proprietary content, internal docs and org data.
- **Structured Data** JSON payloads, database dumps and log files.
- **Documents** PDFs, DOCX and images processed via OCR.

HOW IT WORKS

Intercept & Tokenize

Prompt normalized into a canonical token stream before any LLM call.

Detect

Regex + in-memory LLM analysis identifies sensitive fields across all data types.

Mask & Replace

Detected values replaced with placeholders. Structure preserved. Data discarded.

Score & Forward

Sensitivity scored on the fly. Clean prompt forwarded. Zero raw data retained.

ENTERPRISE CAPABILITIES

Policy-driven.
Zero retention.

Hybrid Detection Engine
Regex + LLM processed entirely in-memory. No request stored at any layer.

Context-Aware Masking
Structure understood: JSON, logs, DB dumps. Fields replaced, structure intact.

Policy Engine
Allow / Mask / Block rules per department. Assigned by org head in real-time.

Real-Time Risk Scoring
Sensitivity flagged on the fly — "High Risk" alerts without storing raw data.

Stateless REST API
POST /scan → returns masked prompt. Ephemeral calls. No logging at any stage.

Privacy-Safe Dashboard
Aggregated metadata only. Risk trends, scan counts — zero raw prompt storage.

DEPLOYMENT

Browser Extension	Dashboard & Policy Server	REST API
Real-time masking in any LLM interface. Toggle on/off. Zero disk writes.	Dept-level policies, aggregated analytics, audit metadata no raw prompts.	POST /scan endpoint. Stateless. Ephemeral LLM calls. Webhook alerts.

customization

> **"All features and capabilities within SecureAgent including detection logic, masking behavior, policy enforcement, risk scoring, dashboards, and integrations are fully customizable according to the specific requirements of each enterprise. This ensures that SecureAgent is not a one-size-fits-all solution, but a bespoke AI security layer tailored to your organization's workflows, risk profile, and compliance needs."**