CERTifAI

AI-Native Security & Compliance Platform

CERTifAI is a **GDPR-compliant, data-sovereign AI platform** combining autonomous security scanning with intelligent compliance automation. We help enterprises **secure their code**, **enforce compliance at scale**, and **maintain full data sovereignty** — powered by 200+ atomic security controls, AI-driven triage, and a complete audit trail for every finding.

Compliance Scanner

AUTONOMOUS AI SECURITY AGENT

- **200+ Atomic Controls** — Fine-grained security checks with full provenance tracking per finding
- **SAST + DAST + SBOM** — Full-spectrum security testing with dependency vulnerability tracking
- **AI-Driven Pentesting** — Autonomous LLM-orchestrated penetration testing with encrypted reports
- **Automated PR Reviews** — Security-aware code review comments on every pull request
- **Audit Trail** — Immutable finding lifecycle tracking from detection to remediation
- **LLM-Powered Triage** — Intelligent false-positive filtering with confidence scoring
- **Code Knowledge Graph** — Architecture visualization with impact & data-flow analysis
- **Multi-Tracker Sync** — Auto-creates issues in GitHub, GitLab, Jira, Gitea
- **MCP Server** — Live security data in Claude, Cursor & other AI dev tools

CERTifAI Platform

SOVEREIGN GENAI INFRASTRUCTURE

- **Multi-Provider LLM Management** — Unified interface for LiteLLM, OpenAI, HuggingFace, Anthropic
- **AI Agent Orchestration** — LangGraph integration with live monitoring & agent registry
- **Enterprise SSO** — Keycloak-based OAuth2/PKCE, LDAP, multi-realm authentication
- **Usage & Billing Analytics** — Token tracking, per-model breakdown, seat management
- **News Intelligence** — AI-powered news summarization, trend analysis, follow-up chat
- **Developer Toolchain** — LangFlow, Langfuse, LangChain integrations out of the box
- **RBAC & Feature Flags** — Role-based access with controlled GenAI rollout per org
- **Full i18n** — Multi-language support (DE, FR, ES, PT) for global teams
- **RAG-Powered Chat** — Natural language Q&A grounded in your codebase

$15B+	200+	80%	10×	100%
APPSEC TAM BY 2027	ATOMIC SECURITY CONTROLS	COMPLIANCE REVIEW TIME SAVED	CHEAPER THAN MANUAL PENTESTS	DATA SOVEREIGNTY GUARANTEED

WHY CERTIFAI WINS

AI-Native Security
LLM-driven pentesting & triage replace $5K–$50K manual engagements. No competitor offers autonomous AI pentests.

Full Provenance
Every finding traces back to its control, rule, and source. Complete audit trail from detection through remediation.

Data Sovereignty
Zero data leaves your infrastructure. GDPR-compliant by architecture. EU-hosted deployment options.

Shift-Left PR Reviews
Security findings surface as PR comments before code merges. Developers fix issues at the source, not in production.

Built in Rust
Memory-safe, high-performance stack. Fullstack WASM + SSR with Dioxus. Enterprise-grade reliability.

Unified Control Plane
Security + AI infrastructure in one dashboard. Competitors require 5+ separate tools to match.

ROADMAP — COMING SOON

SOC2 & ISO 27001
Pre-built control mappings for certification readiness

Policy-as-Code
Custom compliance rules via declarative YAML policies

CI/CD Gates
Block deploys on critical findings with pipeline integration

Executive Reports
Auto-generated compliance posture reports for leadership

BUSINESS MODEL

- → **SaaS Cloud** — Managed multi-tenant platform for SMBs
- → **Enterprise License** — Dedicated deployment with support & custom integrations
- → **Professional Services** — Custom rules, pentest reports, compliance audits
- → **API Tiers** — Free community tier, paid enterprise API access

TARGET MARKETS

- → **Regulated Industries** — Finance, healthcare, government (GDPR, HIPAA, SOC2)
- → **Enterprise DevSecOps** — Shift-left security for engineering teams
- → **EU Data Sovereignty** — Companies requiring sovereign AI infrastructure
- → **Security Consultancies** — Automated pentesting & report generation