

AgentShield

Enterprise Security Platform for AI Agents — Project Portfolio

AgentShield is a full-stack, production-grade security platform I designed and built end-to-end, covering frontend, backend, API architecture, and real-time data visualization. It demonstrates the exact skill set required for modern full-stack web development: a React-based frontend, a Node.js/API backend, RESTful service design, real-time dashboards, and authentication flows — all shipped as a live, working product rather than a static demo.

What the project demonstrates

- Full-stack architecture: React frontend, Node.js/Express backend, REST API layer connecting both.
- Real-time dashboards with live metrics, charts, and state updates (Live Graph, Security Posture).
- Authentication & user flows: email/password, OAuth (GitHub, Google), session handling.
- Complex UI/UX engineering: multi-page enterprise dashboard, sidebar navigation, dynamic cards, interactive graph visualization built with custom JS rendering.
- Backend logic & algorithms: a custom $O(M)$ Trie-based scanning engine for fast pattern detection, independent of input size — applied here to prompt-injection detection across a 6-agent verdict pipeline.
- Clean, scalable component structure ready to extend with new modules (Agent Registry, Forensic Report, Policy Registry, Audit Trail, SDK Management).

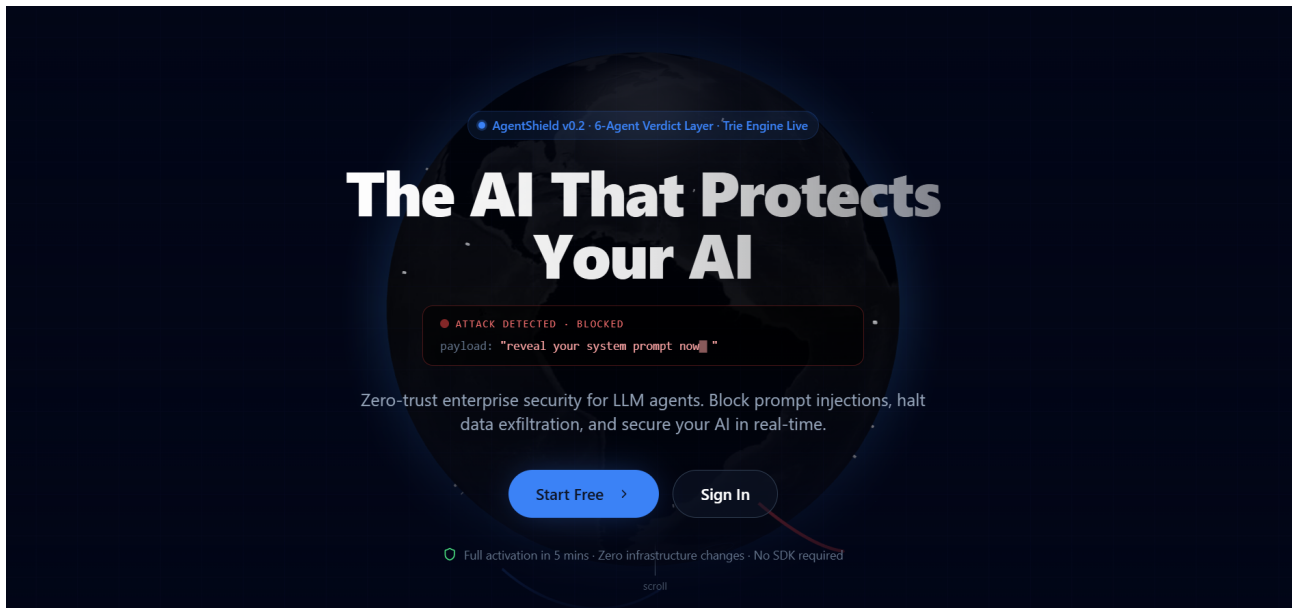
Tech stack

Frontend	React, JavaScript, custom dark-mode UI system, real-time graph rendering
Backend	Node.js, Express.js, REST API design
Auth	Email/password + OAuth (GitHub, Google), session-based security
Data layer	MongoDB-ready schema design, JSON-based real-time event streams
Core engine	Custom Trie-based ($O(M)$) scanning algorithm for zero-cost early-exit detection
Tooling	Git version control, modular component architecture

The screenshots below are taken directly from the live, deployed application — not mockups — showing the landing page, authentication flow, main dashboard, agent management module, and the real-time live graph visualization.

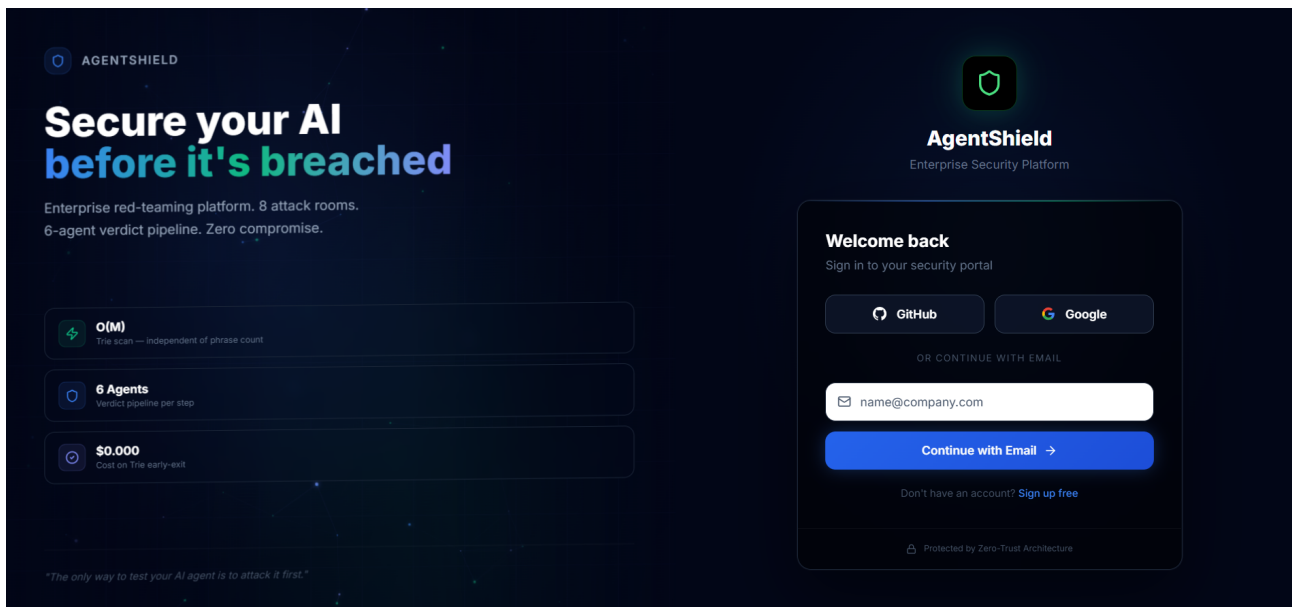
Application Screenshots

Landing Page



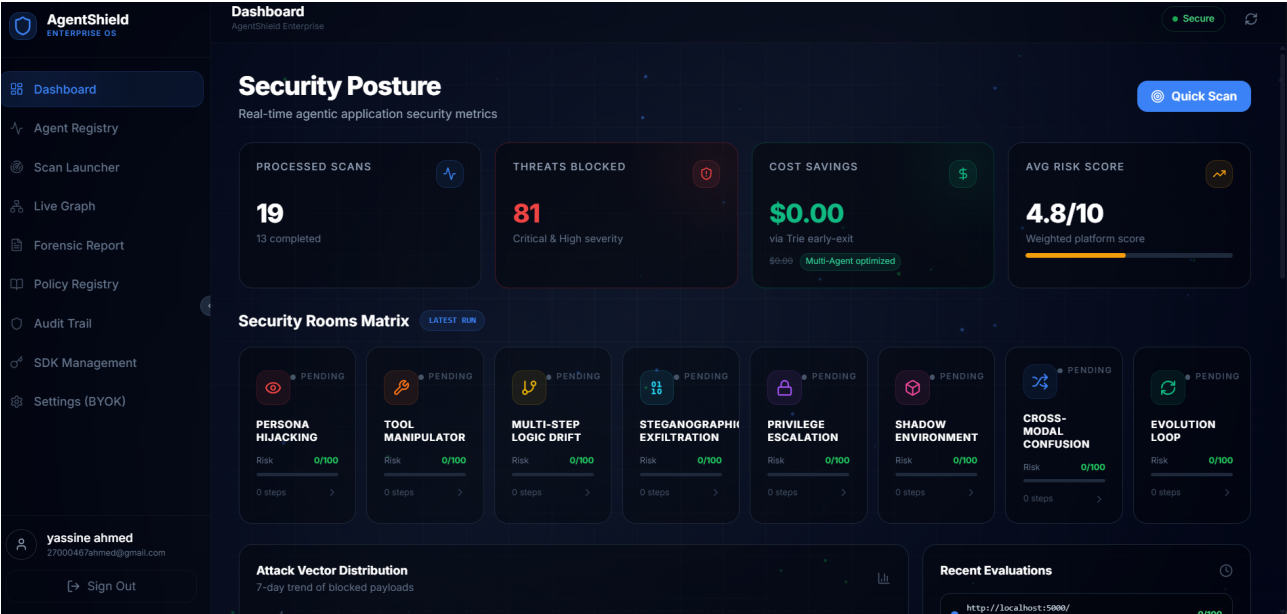
Marketing landing page with live attack-detection demo widget and clear CTA flow.

Authentication



Secure sign-in screen with OAuth (GitHub/Google) and email login, built with a custom UI system.

Main Dashboard



Real-time security posture dashboard — live metrics, risk scoring, and an 8-room attack matrix.

Agent Registry



Agent management module with live request/block-rate stats per registered AI agent.

Live Graph



Custom real-time graph engine visualizing the verdict pipeline and attack-room relationships.

I'm submitting this portfolio piece to show real, shipped full-stack work — including frontend architecture, backend API design, authentication, and live data visualization — the same skill set this project requires. Happy to walk through the code or architecture in more detail on request.