

SecuriX for SMBs

The Neutral Observability & Audit Gateway for AI Development

Gain total visibility into your engineering team's AI traffic while maintaining your existing seat-based subscriptions. SecuriX acts as a transparent proxy layer, bringing clarity and governance to your team's AI accounts.

The Challenge: The AI Black Box

Growing engineering teams rely on seat-based AI provider subscriptions (e.g., Claude, ChatGPT) for their developers. While keeping costs predictable, managing these accounts creates an operational black box: limited visibility into individual usage, no audit trails for compliance, and a high risk of sensitive company data leaking into external models.

The Solution: Frictionless Visibility

SecuriX provides a pass-through observability gateway designed specifically for engineering workflows. By simply routing your developers' coding agent traffic through our endpoint, you instantly unlock powerful analytics, auditing, and data protection—all while keeping your existing seat-based AI provider agreements intact.

Core Capabilities

Instant Observability & Usage Tracking

De-mystify your team's seat usage. Our dashboard provides real-time analytics on consumption, allowing engineering managers to see exactly where usage limits are being hit and track request volume across all provisioned accounts.

Audit-Ready Trails

Bring order to the chaos. SecuriX maintains a complete, immutable log of all AI prompts and responses. This ensures your organization is always ready for internal reviews and compliance audits, giving you the historical visibility you currently lack.

PII Shielding & Data Security

Protect your proprietary data automatically. The gateway scans outbound requests to detect and redact sensitive information (such as API keys, customer PII, and internal IP) before it ever reaches the external AI models.

Out-of-the-Box MCP Server

Connect your AI agents to your repositories and internal data safely. Our native Model Context Protocol (MCP) server applies the exact same observability and layered security policies to your internal tools, giving you full Zero-Trust control over what an AI agent or app can see, fetch, and execute.

Zero-Friction Integration

No rip-and-replace required. We operate strictly as a neutral observability layer. Update your API endpoint configurations to point to SecuriX, and we will forward the traffic to your AI provider identically. We manage the auditing; you manage your provider relationships.

Catalyst Ops Private Limited | securix.app
Next-Generation AI Infrastructure & Governance