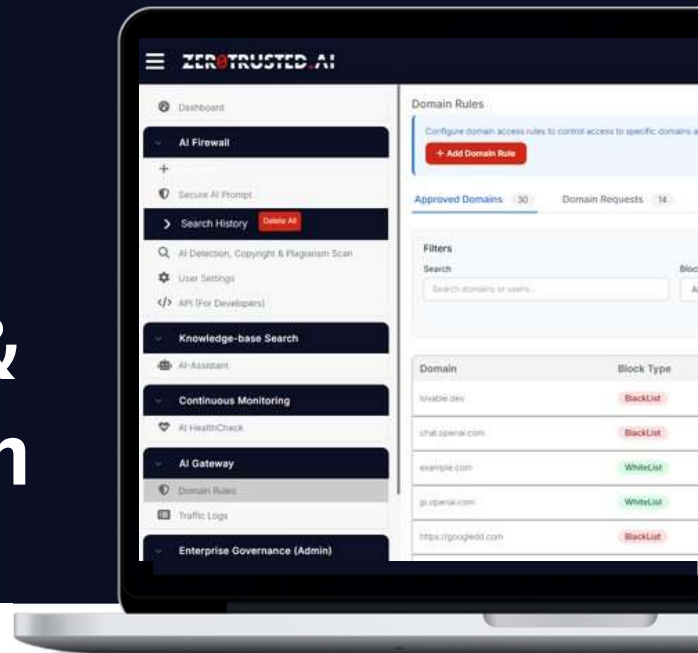


## Our Solution: A Unified AI Security & Governance Platform



### The Challenge

Artificial Intelligence is transforming how organizations operate—but with this transformation comes hidden risks and lack of real control. Shadow AI, unsecured APIs, MCP, A2A, and fragmented governance create vulnerabilities that threaten data integrity, compliance, and business continuity.

#### ZT Shadow AI Protection



- Blocks unsanctioned AI use
- Detects unsafe prompts & anomalies
- Logs and observes all activity
- Deployable in Chromium-based browsers (Chrome, Edge, Firefox)
- Extends protection beyond the browser to all applications

#### ZT AI Gateway / Firewall



- Protective proxy for APIs, MCP, A2A and cloud AI
- Enforces secure, policy-driven access
- Real-time risk detection, monitoring, and blocking

#### ZT AI Governance System AGS



- Centralized oversight of AI usage
- Compliance, auditing, and reporting
- Aligns every interaction with business standards

**ZTProxy**  
Safe, Secure, and Trustworthy AI

Proxy Status: Active - AI domains routed to ZTProxy

**ZTProxy Host:** localhost

**ZTProxy Port:** 8081

**Enforcement Mode:** Block (Block GET & POST when detected)

**Request Filtering:** Monitor POST Chat (PII threshold)

Save Configuration

Current: localhost:8081 (POST Chat (PII threshold); block)

Domains are managed by the server blacklist/whitelist and synced automatically.

Enable AI Monitoring

Refresh Routing Domains

Disable AI Monitoring

Test Connection

ZTProxy Extension v1.0 - Configure your proxy settings above

Request Blocked by ZeroTrusted.ai: PII threshold met (3 findings)  
chatgpt.com

Request Allow | Proceed anyway | Dismiss