AI SECURITY & TRUST INFRASTRUCTURE

The CyberArmor.AI product family

"Do you have an AI security gateway?" Yes: the CyberArmor.AI AI Trust Gateway inspects AI traffic in line, both ways, and blocks, redacts or warns per the customer's policy, with every decision in the signed audit trail. Unlike a plain gateway, the same checks also run on the laptop, in the browser, on the phone and inside the customer's apps, so traffic that never passes a gateway is still covered.

Trust Gates: the decision points	AI Detection & Response and engines	Where protection runs	Evidence, governance & trust
URL Trust Gate links and pages checked before they load PILOT	**AI Trust Gateway** hosted in-line inspection of AI traffic both ways PILOT (response-side policy)	**Endpoint Agent** macOS, Windows, Linux: local proxy, files, clipboard, patching PILOT · PRODUCTION (signed installers)	**Signed Audit Trail** HMAC-SHA256 records, ML-DSA-87 checkpoints PRODUCTION
Context Trust Gate content checked before an AI reads it PILOT	**AI Detection** prompt injection, sensitive data and harmful output; redaction of identity, financial, health and secret data PRODUCTION	**CyberArmor.AI Protect** browser extension: Chrome, Edge, Firefox, Safari, Opera PILOT	**Compliance & Reports** 45 frameworks, 44 policy packs, attestations PRODUCTION
MCP Trust Gate tool poisoning, impersonation, rug pulls; MCP server discovery ROADMAP (tool poisoning) · PILOT (discovery)	**AI Response** isolation, process kill, firewall round-trips PILOT	**iPhone, iPad & Watch app** on-device filter, Safari extension, MDM per-app POC · ROADMAP (managed app proxy)	**AI Bill of Materials** AI inventory with KEV and EPSS vulnerability data PRODUCTION
Promptware Defense malware-like prompts, direct and indirect: hidden instructions in pages, documents, emails or tools caught before the AI acts PRODUCTION (direct injection) · PILOT (indirect)	**Runtime Decision API** one call: scan, policy, verdict	**Android app** VPN filtering, work-profile inventory POC	**Shadow AI Discovery** AI services, apps and MCP servers in use PILOT
Payment Integrity Trust Gate money only goes where approved: call-back verification by named approvers, and the approved destination checked against where the payment is actually sent PILOT (wire verification)	**Policy Engine** tenant policies, artifacts and lists PRODUCTION	**Developer & Office add-ons** Office add-in; VS Code, Cursor, Kiro, Visual Studio PILOT	**Media Provenance** C2PA Content Credentials PRODUCTION
Agent Trust Gate Claude Code and Codex: pages fetched, files read POC	**AI Router** AI provider routing and catalogue PRODUCTION	**CyberArmor.AI SDKs** build our checks into your AI apps: Python, Go, Java, Node.js, .NET, C/C++, PHP, Ruby, Rust; LangChain, LlamaIndex, OpenAI and Anthropic wrappers PILOT	**Identity & Access** SSO, MFA, directory enrichment, post-quantum keys PRODUCTION
	Agent Identity agent registration and delegation chains PRODUCTION	**CyberArmor.AI RASP** inside the running app: inspects AI-bound traffic, catches prompt injection, checks outbound fetches, reports what is loaded; same 9 languages PILOT	**AI Output Verification** schema, arithmetic, citations, groundedness ROADMAP
	Malware & Ransomware Defense signatures, quarantine, ransomware stop PILOT · POC (ransomware kill)	**Agentless Integrations** firewall EDL, SIEM, syslog/EDR ingestion, M365 PILOT	
		Robotics (ROS 2) topic and service guards, actuator policy, e-stop PILOT	

Consoles Customer Portal (a company's security team) · Partner Console (MSPs and resellers) · Operator Console (CyberArmor.AI staff)

Also included local AI models on the device · detonation sandbox · redaction as you type · card-PIN protection off the bank's own site · coverage reporting when a device is not protecting · patching · clipboard redaction · firewall block lists · Chinese AI services inspected · in-country data residency · post-quantum cryptography · training in English and Chinese

Maturity tiers as published on the CyberArmor.AI status page (cyberarmor.ai/status), 29 October 2026. CyberArmor.AI product and feature names are pending trademark clearance.