## **MCP\_Guarda-Pitch**

## **One‑liner & Value Prop**

## **MCP\_Guarda** is a lightweight **policy proxy + consent gateway** that sits between any MCP client and MCP servers to enforce **deny‑by‑default** policies, **human approvals** for risky actions, and **sandboxed side‑effects** (filesystem & network), with complete **audit trails**. It reduces the new attack surface introduced by MCP tool integrations without touching the MCP spec.

# **Packaging strategy (open-core, add-on modules)**

* **Core (OSS, Apache-2.0)**: JSON-RPC proxy, policy engine (allow/ask/deny), consent UI (local), write quarantine, network/exec gates, audit logs, local YAML policies.
* **Pro (license key)**: WebAuthn/biometric approvals, diff viewer for writes, short-term approval caching (“remember 10 min”), host/path templates, log export (NDJSON→CSV), auto-updates, GUI installer.
* **Teams (SaaS or self-host)**: Central policy sync, device enrollment, SSO (OIDC/SAML), role-based rules, team audit console, slack/email alerts.
* **Enterprise (annual)**: Container sandbox runner (Docker/NSJail), OPA/Cerbos integration, MDM/Intune profiles, on-prem policy server, priority support, security reviews.

# **Feature matrix (what’s in each edition)**

| **Capability** | **Core (free)** | **Pro** | **Teams** |
| --- | --- | --- | --- |
| Deny-by-default policy engine | ✅ | ✅ | ✅ |
| Human consent UI (local) | ✅ | ✅ | ✅ |
| File write quarantine & apply on approve | ✅ | ✅ | ✅ |
| Network/exec allowlists | ✅ | ✅ | ✅ |
| WebAuthn/biometric approvals |  | ✅ | ✅ |
| “Remember for N mins / 1 request” |  | ✅ | ✅ |
| Rich diff (side-by-side) |  | ✅ | ✅ |
| Log export & redaction rules |  | ✅ | ✅ |
| Central policy sync & device fleet |  |  | ✅ |
| SSO (OIDC/SAML), RBAC |  |  | ✅ |
| Alerting & dashboards |  |  | ✅ |
| Container sandbox + least-priv runtime |  | Add-on | Add-on |

# **Pricing (clean, procurement-friendly)**

* **Pro**: $7/user/month or $60/year. 14-day trial. License key in the app.
* **Teams**: $3–5/user/month (min 10 seats) + $99/month tenant. Annual: 20% off.
* **Enterprise**: custom. Per-org license + support SLA. Optional on-prem policy server.