

RESEARCH PAPER

Security Model

Version 1.2.0 is frozen. This paper restates the public model for a general technical reader. It is not a certification. A green test run is necessary, not proof.

COMPANY OS SECURITY BASELINE 1.2.0 · 2026-08

Threats in scope

A confused or prompt-injected worker in the same Unix user; a second tenant directory on the same host; a browser on loopback or LAN; a malicious backup zip; a hostile public HTTP resource; a malformed tenant.json.

Out of scope: kernel/process sandbox, host root, WAN-published dashboards, LLM supply chain, executing scraped text as code.

Composition rule

Two steps that are each “safe” must not combine into an unsafe outcome. That was the defect class we actually broke and then fixed:

- Webhook kind=publish copied secrets into approval details, then status echoed them.
- Untrusted zip installed secrets .env; vault then read process environment.
- Two roots with the same id; find_root was first-wins.
- Second complete wrote another receipt; spend could self-approve.
- Acquire on already-done work succeeded; lease stuck.
- Explicit empty capability object was treated as missing and upgraded to ALLOW intake.

Frozen guarantees (summary)

1. **Isolation.** A's work, receipts, and sqlite are not visible to B.

2. **Path jail.** state_dir / logs_dir inside the tenant root, not inside Money Hunter.
3. **Restore safety.** Default restore does not install secrets. Zip traversal and symlinks refused.
4. **Credential boundary.** World-readable secrets refused. Process env is not an implicit vault.
5. **Approval gates.** propose_external does not execute HOLD/DENY. Approving a row does not run the action. Spend cannot self-approve.
6. **Scoreboard.** Funnel code cannot invent collected cash.
7. **Audit.** Completing done work does not add a second completion receipt. Event payloads omitted from status.
8. **Intake.** GET only. Loopback, RFC1918, file, and numeric loopback aliases refused.
9. **Bind.** Never 0.0.0.0. Mutating POSTs check Origin/Referer against Host when present.
10. **Leases.** One active holder per (work, stage). Closed work cannot be leased.
11. **Registry.** One registered root per tenant id.
12. **Config fallbacks.** Missing capabilities → catalog defaults. Explicit empty object → deny all.

Machine-readable map lives in the public repository as docs/security/guarantees.json.

What approval means

An approved row is evidence that an owner clicked. It is not a capability change and not an executor. External actions stay HOLD in governance even if someone later sets a grant to allow in a file the restore is not allowed to sneak in.

Limitations

Not SOC 2. Not a pentest report. Not a promise about models. The frozen text is behavior we will not silently weaken. Fixes that keep the same claim (tighter enforcement) keep the version.

HTML is canonical. A PDF companion is offered where generated. Experimental laboratory results are labeled as such. This is not a product-market-fit claim and not a certification.

[← All papers](#) · [PDF](#)

TheCriners LLC · Coshocton, Ohio

Money Hunter, Packet Press, Pullsheet, Hearthlabel, Seatpack, and Company OS are projects of TheCriners LLC — not separate legal entities.