

RESEARCH PAPER

Multi-Tenant Governance for Autonomous Agents

Two companies on one host is the interesting case. One company with one bot can be a folder of scripts. Two companies is how you learn whether isolation is real.

THECRINERS LLC · 2026

Problem

Autonomous workers are useful because they do not wait. They are dangerous for the same reason. Governance is the set of rules that still apply when nobody is watching the terminal.

The unit of governance in Company OS is the tenant directory, not the Unix user. Two tenants may share a user and still be forbidden to see each other's work, receipts, or sqlite.

What isolation means here

- Tenant A cannot complete Tenant B's work id.
- Opening B's database as A raises an isolation error.
- Paths for state and logs must resolve inside the tenant root.
- Restore into the Money Hunter tree is refused — that laboratory is not a tenant to be overwritten.

Live public proof that two faces can look different on the same idea:

packetpress.thecriners.com versus thecriners.com. Operator surfaces stay on loopback.

Org chart as data

Owner, director, supervisors, workers. Rank is not a grant. A "CEO" worker can write a brief; it cannot flip spend to ALLOW by having a prestigious title. Delegations to support or to

the parent company are listed per tenant, and they are narrower than the tenant's own capabilities.

Implementation

Each tenant has sqlite in WAL mode, a secrets file that is refused if world-readable, and a dashboard bind that cannot be 0.0.0.0. The registry stores paths, not secrets. Duplicate tenant ids are an error, not first-wins.

Tests

Isolation tests attempt the confused-deputy moves: wrong db, wrong work id, restore into a protected tree, empty capability maps upgrading to ALLOW. Those last ones failed in the laboratory and then became frozen guarantees.

Limitations

This is same-Unix-user isolation. A hostile peer with the owner's shell is a different threat. We do not pretend otherwise. Multi-tenant here means "two companies, two directories, two grants," not "a cloud region."

Lessons

If you need a second company to prove the first architecture, build the second company. Packet Press exists because Money Hunter could not be the only example. Pullsheet, Hearthlabel, and Seatpack exist because civic briefs are not seating charts. Governance that cannot survive a second mission is a comment in a README.

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](#)

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