PROJECTS

EMOS

Hardened OS Overlay with Local AI Orchestration

Lead Architect · 2026

EMOS (External Matrix Operating System) is a hardened operating-system overlay built on stock Qubes OS that combines strong compartmentalization and anonymity with local AI orchestration across isolated security domains — deployed as a Salt overlay, with a local AI assistant reachable across qubes through controlled interfaces.

---

1. Overview

EMOS turns a stock Qubes OS install into a hardened, AI-capable workstation without forking the base system. Delivered as a Salt overlay on Qubes OS 4.2, it adds domo tooling, purpose-built service and workspace qubes, and a local “Ask EMOS” AI assistant — all while preserving Qubes' strong isolation guarantees. Strong compartmentalization and anonymity are combined with local inference so the AI never leaves the machine and never crosses a trust boundary it shouldn't.

2. Key Features

- **Salt-Overlay Deployment** Installs as a Salt overlay on stock Qubes OS 4.2 rather than a hard fork, so the trusted base stays intact and upgradeable.
- **Compartmentalized Qubes** Adds domo tools plus dedicated service and workspace qubes with explicit trust boundaries between domains.
- **Local AI Assistant** An “Ask EMOS” assistant runs locally and is reachable across qubes through a controlled bridge, so inference stays on-device.

- **qrexec-Mediated Interfaces** Cross-qube capabilities are exposed through qrexec interfaces, keeping the AI request flow and bridge flow inside defined trust boundaries.
- **Signed, Source-Traceable Releases** Architecture is C4-documented and source-traceable to install.sh, the Salt states and src/, with a signed release process.

3. Architecture

EMOS is implemented primarily in Python with Salt-based provisioning over stock Qubes OS 4.2. The active runtime spans dom0 tooling (src/emos-dom0), the local AI service (src/emos-ai) and Salt states (salt/emos), wired together through qrexec interfaces that mediate the AI request flow, the cross-qube bridge flow and deployment orchestration. The architecture follows a C4-aligned, current-state documentation model with explicit trust boundaries between dom0, service qubes and workspace qubes.

TECH STACK

Qubes OS 4.2 · Python · SaltStack · qrexec · MLX / local inference · Shell · gRPC

LINKS

https://www.jonathandumitru.com/projects/emos