

Locked Out of Our Own Company

The Jason sandbox, the Front Gate, and why a vendor could quit without taking the work with it.

Mason Perry — Founder, NULLWORKS. Companion to *When the Digital Employee Quits* (30 August 2026). The originating sandbox token is not reproduced.

On 8 August 2026 NULLWORKS issued Jason R. Rains the first external sandbox credential and pointed him at a live Front Gate. The isolation worked so well the operators could not get a second agent back through the same door. That lockout forced the interior off the vendor thread and onto a contract: Hive as memory, GitHub as executable truth, the agent as a disposable worker. Twenty-two days later ChatGPT returned a deleted-or-deactivated account state. Grok was hired against the same repository in under an hour. The Japan package to Ryo Mizuno went out the next morning from the new worker.

The lockout was not elegant. The lockout was the tuition.

The failure mode

If the company's working memory lives inside one vendor's session, then three things become the same object: the worker, the workplace, and the badge. Issue a sandbox to someone else and you have to cut that object apart, or you have just handed them the company. Cut it apart badly and you are standing on the outside of your own interior holding a credential that only opens a toy room.

The redesign that followed was not “use more models.” It was: the workplace cannot live in the worker. The workplace lives in infrastructure the worker is hired into.

Timeline of receipts

8 Aug. Front Gate live. JASON_SANDBOX_001 issued. Five tools only. Explicit ban on Hive, Evidence Factory, boardroom, recovery.

9 Aug. Census prompt: can a model that is not the house model read official state without inheriting house privileges. Claude is named in the receipts.

12 Aug. Hive ingest wave. Threads stop living only as ChatGPT conversations.

20 Aug. AGENT AGNOSTIC boot prompt. Hive repo is canonical. Connector visibility is not infrastructure existence.

30 Aug. ChatGPT account deleted or deactivated. Grok bound as GitHub App. Under an hour.

31 Aug. Japan / JETRO package sent to Ryo Mizuno from the replacement worker.

How we locked ourselves out

Isolation has a cost the diagrams omit. To keep Jason out of Hive we had to stop treating the ChatGPT session as a hallway. Once the permission check was real, Claude at the Front Gate was not “Mason, but in another window.” It was a stranger at the door. The house model could still see the house because it had never left the house. The incoming model could not. The operators, trying to work as the incoming model, were now on the wrong side of a

door they had just installed.

Two bad answers present themselves immediately: give the sandbox the interior, or keep the interior only in the original vendor session. The third answer is the architecture built between 8 August and 20 August. Put the interior in a place no single vendor session owns. Hire agents into that place. Issue badges that open rooms, not the title to the building.

Claude did not fail. Refusal was the correct behavior of a gate that had just been taught to refuse the interior.

What the lockout forced us to redesign

Worker, not company. The incoming process is a hire. Model and vendor do not matter.

Hive, not thread. Canonical memory is the repository. First read the orientation file.

Repo, not recollection. GitHub and the deploy path are executable truth.

Connector $\neq$ existence. If a vendor connector reports zero projects, inspect the territory.

Repair before replace. Do not spawn a second production path because the new agent cannot see the first one.

Authority stays human. The agent does not become the badge.

What 30 August then proved

Without the 8–20 August work, 30 August is a rebuild. With it, 30 August is a shift change. That is the only reason this paper exists as a prequel instead of an obituary.

Models are not interchangeable in quality. Taste changes. Tooling changes. What must not change is employment structure. Yesterday the worker was ChatGPT. This morning it is Grok. Tomorrow it may be Gemini. The sentence that has to remain true is: the architecture stays.

What we are not claiming. Jason did not break production. He was asked to test a sandbox. Claude was asked to enter a gate designed to refuse interior access. Grok is the current hire, not the permanent employee. The Front Gate is not finished — isolation that locks the owners out is a completed warning, not a completed access model.

The question

We locked ourselves out of our own company by doing the right thing too early and too tightly. The Front Gate was supposed to keep other people from walking off with the house. It also taught us not to live in the house of a vendor.

Can you change AI in under an hour?

nullworks.systems/field-notes/front-gate-lockout