

Built to run inside your boundary. Tested, and the evidence kept.

Groundwork Cloud runs on an endpoint your organization approves. It does not scan your network, install agents or call home, and its core work needs no AI service. This brief describes the architecture, its data boundaries and what we tested.

01 · HOW IT RUNS

A reviewable local workbench.

Three parts, and only the first is required. Nothing in the engagement kit crosses a boundary by itself; moving material is your own approved process.

On your approved endpoint, and around it.

01

The engagement kit · Required

Static pages opened from disk, in the browser you already manage
Work saved in the browser's local storage and in files you download
A SHA-256 manifest to verify every delivered file

02

The local reader · Optional, on a managed laptop

A language model on the same machine, reached on 127.0.0.1 only
Reads only the folder it is given, quotes each page it cites, never scores



The hosted demonstration · Fictional data, behind sign-in

The studio answers only after sign-in Never a place for client material

02 · DATA BOUNDARIES

What it keeps, and where.

AREA	BEHAVIOUR AND LIMIT
Inputs	Envelopes are checked for schema, record and known sections before anything applies; a refused import changes nothing. Pasted data is bounded before it is read (16 MiB, 64 levels, 250,000 values).
Decisions	Every readiness level is a person's decision. A typed name records who confirmed; it is not a signature.
Storage	Plain text in the browser's local storage and in downloaded files, on your endpoint. Access control, encryption, backup and retention are yours.
Integrity	SHA-256 manifests let you verify the delivered bytes. A checksum does not authenticate the publisher.
Telemetry	None: no analytics, no remote fonts, no call home. Nothing in the tested paths left the machine.
This site	Static pages with nothing from another origin. Every response carries a content security policy, HSTS, nosniff, a referrer policy and a framing policy.

03 · WHAT WE TESTED

Measured on 18 October 2026, with fictional data.

TEST	OBSERVED RESULT
Full test suite	255 passed, 0 failed
Every page in the kit	55 pages in Chromium and WebKit with any off-machine request blocked and counted: 0 attempted, 0 page errors
A walk through the studio	19 requests per browser, all to local files; 0 left the machine
Hostile import	Script and event-handler payloads in every free-text field ran on 0 pages; 0 dialogs opened
Workflow checks	76 of 76 passed, from disk and over HTTP, in both browsers
Oversized input	Refused before it is read; a normal envelope passes
Local reader and proxies	With proxy settings inherited from the machine, 0 requests reached the proxy; the model is reached directly
This site and the studio	Each served with its own headers and walked in both browsers: 0 policy violations. 7 of 7 studio addresses sent an unsigned visitor to sign-in
Third-party code	None: no packages and no lockfile; the tools use the Node.js standard library

What we found and fixed in this review

1. Pasted data had no size or depth limit before it was read. It now does.
2. With proxy settings inherited from the machine, the local reader's request to the model could be routed through a proxy. It now never is.

3. The test instructions named probes the kit did not carry. They now travel with it.
4. This site sent no security headers. It now does.

04 · LIMITS

An engineering self-assessment. Not a signature.

These are developer-run tests with synthetic information, prepared from retained results. They are not an independent penetration test, a benchmark assessment, malware clearance or validation on your endpoint, and they claim no approval, certification or authorization of any kind: your own assessor, auditor, regulator or quality unit decides. Browser binaries, extensions, the operating system and endpoint controls are outside them. The full review, its evidence and the probes to repeat every test come with an engagement, in the security packet beside the security reference architectures.

Groundwork Cloud · Security self-assessment · 18 October 2026 · fictional data only. Public references and examples only. Do not send credentials, regulated or controlled data, client evidence or production data.