ORGDRIFT — SECURITY ARCHITECTURE OVERVIEW

Your data never leaves your browser.

That's not a promise — it's architecture. OrgDrift's scan engine runs entirely as client-side JavaScript. Your HRIS, payroll, and ICM exports are parsed, compared, and scored on your own computer, the way a calculator works. There is no upload step, no server-side processing, and no copy of your data for us to lose.

DON'T TAKE OUR WORD FOR IT — TWO TESTS, UNDER A MINUTE

1 · The offline test. Load the scan workspace, then turn off Wi-Fi. Run your scan. It completes — because nothing is being sent anywhere.

2 · The network-tab test. Open DevTools (Network tab), run a scan with real files, and watch the traffic. Zero requests carry your file contents.

Invite your security team to run both tests during evaluation — we designed for that audience.

WHAT LEAVES YOUR BROWSER, EXACTLY

Data	Leaves browser?	Where it goes
Your CSV / Excel files	**Never**	Processed in browser memory only
Employee names, emails	**Never**	Redacted by default before the engine sees them
Scan findings & reports	**Never**	Stored in your browser; you choose what to export
Your sign-in email	**Yes**	Authentication (magic link) + entitlement lookup
Payment details	**Yes**	Stripe — we never see card numbers
Scan count (a number)	**Yes**	Usage metering, keyed to a SHA-256 hash

There is no customer-data database. Subprocessors: Vercel (serves the application code, SOC 2 Type II), Stripe (payments), Upstash (auth/entitlement metadata only — never file data).

PII IS BLOCKED BY DEFAULT — DISCLOSURE IS YOUR DOCUMENTED DECISION

Under the OrgDrift Data Governance Framework (ODGF), restricted PII — SSNs, dates of birth, bank details, home addresses — is **hard-blocked** at file load. Names and emails are redacted automatically before any comparison runs; reconciliation works on employee IDs, not identities. If your organization decides a name column is necessary, it can be unblocked only after an explicit, per-column acknowledgment that you are disclosing PII under your organization's authority — recorded (who, when, which column) and stamped into the scan's evidence record. Even disclosed values stay in your browser.

TAMPER-EVIDENT BY DESIGN

Scan results seal into hash-chained Control Execution Records (SHA-256). Every finding ties to source rows, timestamps, and the resolution trail — evidence your auditor can verify, produced without your data ever being in our custody.

ABOUT SOC 2

Certification is on our roadmap — and our architecture keeps the certification scope small, because there is no customer-data environment to audit. The thin surface that does exist (authentication, billing) already runs on SOC 2-certified infrastructure. In the meantime we support security reviews directly: architecture walkthroughs, completed questionnaires (CAIQ / SIG), and the verification tests above. Early design partners who need a certificate on file are invited to talk to us about jointly accelerating the SOC 2 timeline.

The one question to ask any vendor in this category: “When my payroll file is being analyzed, whose computer is it on?” For workflow tools that ingest your data into their cloud, the answer is: theirs. For OrgDrift, the answer is: yours. That isn't just a security posture — it's why OrgDrift can act as an independent referee for your systems of record. A tool that holds your data can't be a neutral witness to it.