

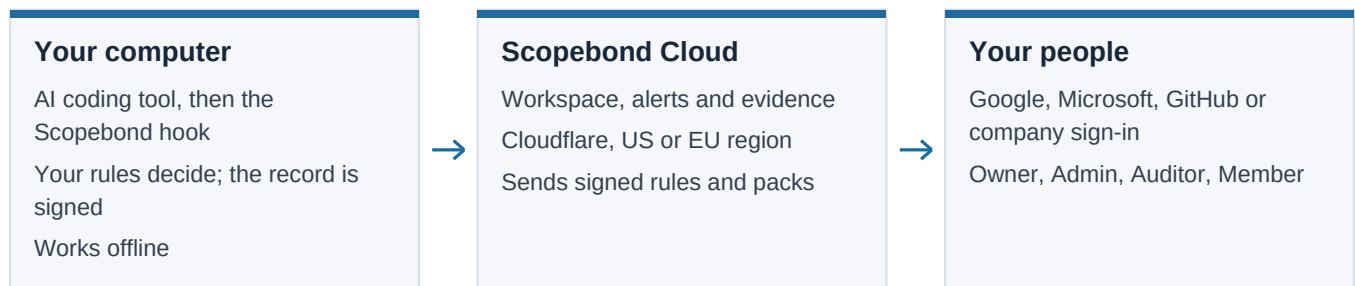
Scopebond security overview

Avouro LLC · As of 2026-10-20

Architecture

Scopebond has two parts. The engine runs on your computers: the Scopebond hook sits between each AI coding tool and the actions it takes, checks each action against your rules, blocks what a rule on Block forbids, and signs a record of the decision with that computer's own Ed25519 key. The hook, the Scopebond Agent and the starter protections are open source under the Apache-2.0 license and work offline.

Scopebond Cloud is the hosted workspace. It runs on Cloudflare Workers with Cloudflare D1 databases and R2 object storage, in separate Production and Staging accounts, and runs no servers of its own. It receives signed records, shows them, sends alerts, keeps the evidence, and delivers signed rules and protection packs to computers.



Data flow

1. An agent asks to run a command, edit a file, push code, install a package or call a tool.
2. The hook checks the action against your rules on the computer and allows or blocks it. Input it cannot read is blocked.
3. The hook signs a record of the decision. Before signing, it keeps only the first 64 characters of a command, with a fingerprint of the whole command, and removes common secret shapes from commands, paths and web addresses; this is best effort.
4. The Scopebond Agent sends the signed records to Scopebond Cloud over HTTPS. Cloud checks them, stores them in the workspace's region and groups them into evidence segments signed with Scopebond's segment key.
5. Owners and admins see Activity, get alerts and export the evidence. Anyone with a computer's public key can check its records offline.

Providers. Stripe for billing, Resend for email, Sentry in Germany for scrubbed error reports, and PostHog in Germany for product analytics without cookies. The full list, with locations, is at scopebond.com/subprocessors.

What we never collect

- **Prompts and conversations.** What the agent was told and what it answered stay on the computer.
- **File contents.** A record names a file path, never what is in the file.
- **Signing keys.** Each computer's private key stays on that computer.
- **Passwords.** Sign-in goes through Google, Microsoft, GitHub or your company's identity provider.
- **Card numbers.** Payment details are entered on Stripe's own pages.
- **Productivity scores.** Scopebond offers no per-person productivity scoring.

MCP tool arguments are kept only as a fingerprint. Folder and computer names can identify a person, such as a user name in a folder path.

How it is protected

- **Encryption.** TLS for every request, with HTTP Strict Transport Security; storage encrypted at rest by Cloudflare; nightly database backups encrypted with AES-256-GCM, kept for 30 days and restore-tested every month.
- **Access.** Every workspace route checks membership and permission, and tests try each route with another workspace's credentials on every change. Changes from the operations console need a second factor and a recent sign-in.
- **Change.** Every change goes through a pull request, the full test suite and required secret, workflow and code-quality scans, and reaches Staging before production.
- **Incidents.** Written procedures for each known incident type; a personal data breach is notified to workspace owners with a 48-hour target.
- **Retention.** 1 year of history on Audit and Enterprise; a deleted workspace is purged after a 7-day undo period.

About this document

It describes how the service works as of the date above. The measures may change as the service changes, without reducing overall protection. It is not an audit report: Avouro LLC holds no SOC 2 report and no ISO 27001 certificate. Questions: security@scopebond.com.