

Evidra: security overview

Enterprise Response Intelligence. Last updated September 2026. The current version of this document is at <https://evidra.xyz/security>.

Architecture overview

The platform is a single web application with a small number of managed services behind it. Each service holds one kind of data and nothing else.

- Next.js application hosted on Vercel, serving the marketing site and the product.
- Firebase Authentication on Google Cloud for sign in: email and password with verified addresses, and Google accounts.
- Firestore on Google Cloud for organizations, members, documents, passages, questionnaires, answers, evidence, comments, usage and the activity trail. The browser never reads the database; every query runs on the server, scoped to one organization.
- Cloud Storage on Google Cloud holds the original files in a private bucket, keyed by organization, with public access prevented.
- The evidence pipeline reads each file page by page, splits it into passages that keep their page numbers, embeds them and retrieves with a hybrid keyword and vector search over one logical index per organization. Drafting uses only the passages retrieved for the question.

Tenant isolation

Every record carries the identifier of the organization it belongs to. The browser has no direct access to the database or the file store; every read and write goes through the server, which takes the organization from the signed in member's session and filters by that identifier before any other condition. Files are checked against the owning record before they are served.

Passages are indexed per organization and file storage is keyed by organization. Retrieval for a question only ever searches the passages of the organization that owns the questionnaire.

Encryption

Connections between browsers and the platform, and between the platform and each managed service, use TLS. Data at rest is encrypted by Google Cloud for the database, the passages and the files. The platform does not hold its own encryption keys at MVP; provider managed keys are used throughout.

Access control and roles

Users sign in with an email address and password, which must be verified before a workspace opens, or with a Google account. Sessions are server side cookies that expire after 14 days. Each user belongs to one or more organizations with one of three roles: Contributor, Reviewer or Approver. Roles are checked on the server for every action, not only in the interface.

- Contributor: uploads documents, corrects extracted questions, comments.
- Reviewer: edits drafts, keeps or removes evidence, flags and approves answers that have evidence.
- Approver: signs off and exports questionnaires, changes member roles, and may approve an answer without evidence, which is recorded as an override.

Retention and deletion

Customer documents, questionnaires and answers are retained for as long as the organization keeps them. Deleting a document removes its chunks from the search index within minutes and deletes the file from storage. Deleting a questionnaire removes its questions, answers, evidence links, comments and activity. Closing an organization removes all of its data from the database, the index and file storage.

An organization can export its documents, answers and activity at any time from the settings page or by request to the security contact below.

No model training on customer data

Customer documents, questionnaires, answers and comments are not used to train or fine tune any model, by the platform or by its providers. Drafting uses only the passages retrieved for the question. If a hosted model provider is introduced for drafting, it is used under terms that exclude customer content from training and is listed as a subprocessor on this page before it processes any customer content.

Subprocessors

The following providers process customer data on the platform's behalf. Changes to this list are published on this page before they take effect.

- Google Cloud: Authentication (Firebase Authentication), application database (Firestore) and file storage (Cloud Storage). Region: European Union multi region.
- Vercel: Web hosting, serverless compute and edge network. Region: Global.

Incident contact

Security issues, suspected incidents and vulnerability reports go to security@evidra.xyz. Reports are acknowledged by email, and affected organizations are informed of confirmed incidents that involve their data without undue delay.

Certifications

No certification is held at MVP. SOC 2 Type II is planned. No badges are shown until a report exists.

A data processing addendum is available on request, and the platform can complete a customer's own security questionnaire on request.