How Verillian is designed for trust

Verillian governs your organization's AI usage without taking custody of your data. It runs inside your environment, and the content it handles is encrypted with a key only you hold. **Verillian never receives, stores, or processes your prompts, responses, tool calls, or audit logs.**

Where your data lives

- The admin service, ingest service, and database run on **your infrastructure**. Verillian does not host them.
- The Sentinel proxy runs on **your developers' devices** and intercepts AI traffic locally.
- Verillian delivers signed software and a license key. Nothing about your traffic flows back to us.

How your content is protected

- **Client-side encryption.** Content is encrypted with your organization's key (X25519 envelope encryption) before it is stored. Your server holds metadata and opaque ciphertext, not readable content.
- **You hold the key.** Decryption happens in your authorized users' browsers. Verillian has no access to your key and cannot decrypt your data.
- **Tamper-evident audit.** Every record is SHA-256 hash-chained and Ed25519-signed. Any modification breaks the chain and is detectable.

How enforcement works

- **Decided at execution.** The decision is made on the device before any content reaches a provider: ■ ALLOW, ■ REDACT, or ■ BLOCK. A blocked request never leaves.
- **Fail-closed.** When a decision is uncertain, Verillian blocks. It never defaults to allow.
- **Signed policy.** Policies are Ed25519-signed by your admin service and verified by each sentinel before enforcement.
- **Best-effort redaction.** PII detection and redaction run before egress. This is best-effort and does not guarantee recall; it complements your data-handling controls.

Questions security teams ask first

QUESTION	ANSWER

Where is our data stored?	On your infrastructure, encrypted with your key. Verillian stores none of it.
Can Verillian see our prompts or outputs?	No. We never receive them, and content is encrypted with your key.
Do you train on our data?	No. We never receive it.
Is the audit log tamper-proof?	It is tamper-evident: hash-chained and signed, so tampering is detectable.
How is the software authenticated?	Server components build from reviewed, tagged source; the Sentinel is code-signed and notarized; policies and licenses are Ed25519-signed.
Does it work air-gapped?	Yes. License verification and core operation require no Verillian connectivity.
What does Verillian hold about us?	Business-contact and billing information only.

Verillian's internal security posture

Verillian maintains a documented security program: enforced MFA on all critical systems, a password-manager standard, least-privilege access control, a documented incident response plan, backup and recovery procedures, code-repository controls (branch protection, secret scanning, signed releases), and strict protection of our offline license-signing keys. Summaries are available to customers under NDA.

Your responsibilities

Because Verillian runs in your environment, you are responsible for your infrastructure and its security, backing up the database, safeguarding your encryption key (losing it means losing the ability to decrypt your own data, by design), managing your users, and applying the updates we provide.