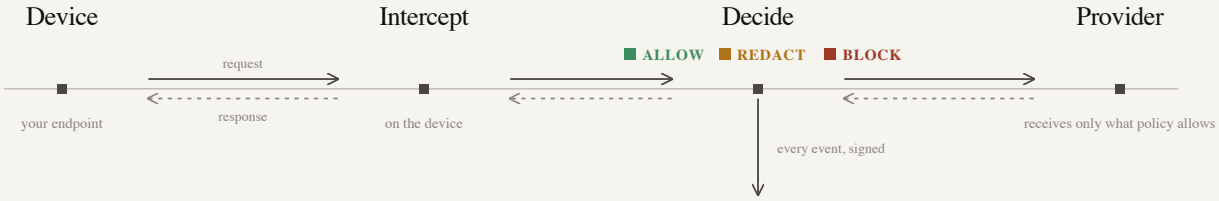
Architecture and data flow

Atlas Interrex runs entirely inside your environment. The decision is made on the device, before any content reaches an outside model, and the record of that decision stays with you. **Verillian does not receive, store, or process your traffic.** This document describes the components, the path data takes, and the boundaries it never crosses.



SIGNED CHAIN ENTRY

TIME	DECISION	CHAIN ENTRY
2026-05-29 14:02:11.394Z	ALLOW	9f2c4a…d1e0
2026-05-29 14:02:11.881Z	REDACT	0b77e1…4ca9
2026-05-29 14:02:14.118Z	BLOCK	ee50a2…1d4f

Request and response travel the same axis. The policy decision happens on the device before egress; only permitted content continues to the provider; every event is signed into a chain held by your institution, under your keys.

Components

Sentinel

A TLS interception proxy that runs on each developer device. It intercepts LLM API traffic, evaluates policy, encrypts content with your organization's key, signs each entry, and uploads to the admin service. It enrolls through your identity provider and receives all configuration from the server.

Admin service

The control plane: users, policy authoring, enrollment, event streams, and the audit viewer. Distributes Ed25519-signed policy bundles to sentinels. Runs on your infrastructure.

Ingest service

Receives signed records over gRPC, verifies the hash chain, and stores them. Runs on your infrastructure.

Database (PostgreSQL)

Stores metadata and opaque ciphertext. Holds no readable content. Runs on your infrastructure.

What crosses each boundary

BOUNDARY	WHAT CROSSES
Device → provider	Only the content your policy permits, after any required redaction. A blocked request never leaves the device.
Device → your admin/ingest	Signed audit records: metadata plus content encrypted with your key (opaque ciphertext to the server).
Admin → device	Ed25519-signed policy bundles and configuration.
Anything → Verillian	**Nothing.** Verillian receives no traffic, no records, and no keys.

What Verillian never receives

- Your prompts, model responses, or tool calls
- Your audit log or its contents
- Your organization's encryption key
- Any data used to train models, because none is ever sent

Cryptographic properties

Content encryption	X25519 envelope encryption with your organization's key. The server stores metadata and opaque ciphertext; decryption happens in your authorized users' browsers.
Tamper-evidence	Each record is SHA-256 hash-chained and Ed25519-signed. Any modification breaks the chain and is detectable.
Policy integrity	Policies are Ed25519-signed by your admin service and verified by each sentinel before enforcement.
Licensing	Ed25519-signed, time-limited license keys verified locally. Works air-gapped; no outbound call.

Deployment

The admin, ingest, and database run on your infrastructure (cloud or on-premises, including air-gapped). The Sentinel installs as a code-signed, notarized package on macOS, with Windows support. Enrollment is through your identity provider over OIDC. You operate the system; you hold your data, your backups, and your key.