Enable AI without becoming the cautionary tale.

Your staff are already using AI. The board wants the productivity; the regulator wants the controls. Verillian lets you say yes to both, with coverage that includes the tools you never approved and a record you can stand behind years later.

THE EXPOSURE YOU OWN

- **Shadow AI.** Unsanctioned tools, personal accounts, and browser sessions that no gateway or closed assistant can see.
- **Agentic actions.** Modern tools run shell commands, read files, and query databases. The risk is no longer pasted text; it is actions on your systems.
- **No record.** When the subpoena arrives, "our dashboard showed it" is not an answer.

WHAT CHANGES WITH VERILLIAN

- **Full coverage.** Every AI interaction leaving the device, any provider, sanctioned or not.
- **Decided before egress.** ■ allow ■ redact ■ block. Fails closed when uncertain.
- **Keys you hold.** Content is encrypted under your key; the server stores ciphertext it cannot read.
- **Evidence you hold.** Every event signed and hash-chained. Tamper-evident by construction.
- **Air-gapped, no integration.** Runs on your infrastructure; no changes to the AI tools.

THE MATH

The average healthcare breach runs **$7.42M**. A per-seat control that prevents one unauthorized action, or produces the one record that closes an audit, has already paid for itself. Verillian is priced to be a rounding error against the incident it prevents.

Start a pilot →