Enable AI without becoming the cautionary tale

$670K

What unsanctioned shadow AI added to the average breach cost, the year the global average total hit $4.44 million. Source: IBM, 2025.

THE EXPOSURE

- **Shadow AI.** Unsanctioned tools and personal accounts no network gateway sits in front of, so they never reach your logs.
- **Agentic actions.** Coding assistants run shell commands and query databases. The exposure is now actions on your systems, not text.
- **No defensible record.** A log an insider or attacker could have quietly edited is not evidence of what was actually sent.

WHAT CHANGES WITH VERILLIAN

- **Coverage you can scope.** Every captured interaction is recorded across the AI tools that reach a provider, before content leaves the device.
- **Decided before egress.** Policy is enforced on the device: allow, redact, or block. Redaction is best-effort, and the sentinel fails closed.
- **Keys you hold.** Audit content is encrypted under a key only you hold. The server stores ciphertext Verillian cannot read.
- **Evidence you hold.** Every captured interaction is signed and hash-chained. The record is tamper-evident, verifiable independent of vendor attestation.

What you can put in front of oversight

Signed at the source and hash-chained, the record maps to controls your frameworks require: CJIS Security Policy v6.0 audit logging, HIPAA documentation retention, the NIST 800-53 audit family. Aligned, not independently certified.

To pressure-test this against your own environment, name a sponsor and a technical contact and we will scope a 60-day pilot on your infrastructure, under your keys.

hello@verillian.ai