A control can only catch what it can see

A control inherits the blind spot of wherever it sits. The further it sits from the device, the more paths slip past it unrecorded: an unsanctioned tool, a browser tab, a command-line client all reach a provider with no gateway in the way. A control placed at the device, before content reaches a provider, sees the paths a downstream control never does.

WHERE DOWNSTREAM CONTROLS SIT

- **At an API gateway** Sees only the one wired path; anything reaching a provider another way is unseen.
- **At the provider** The data is already there, in their record and not yours.

WHERE VERILLIAN SITS

- **On the device** Watches every path it covers, applies policy before content leaves, and fails closed when none applies. Detection is best-effort.
- **Your record, not theirs** Every captured interaction is signed and hash-chained into a tamper-evident record, encrypted under keys your institution holds. Aligned to CJIS Security Policy v6.0, not certified.

A control catches only what it can see. Position decides what it can see.

This document describes Verillian, runtime governance and tamper-evident evidence for regulated AI.

hello@verillian.ai