Let the desk use AI. Hold a record that survives an exam.

$5.56M

Average financial-services breach cost, second only to healthcare. IBM Cost of a Data Breach Report 2025.

THE EXPOSURE

- **Shadow AI on the desk** AI in use across desks, personal accounts, browsers, and command-line clients, invisible to controls downstream of the device.
- **Sensitive data in prompts** Customer financial data, account numbers, and material nonpublic information sent to AI tools with no record of what crossed.
- **No reconstructable record** Nothing an SEC or FINRA exam, internal audit, or model risk management can rely on to show model activity.

WHAT CHANGES WITH VERILLIAN

- **A decision before egress** A sentinel on each device governs any tool reaching a provider over HTTPS: allow, redact, or block, failing closed without valid policy.
- **Customer data held at the boundary** Outbound requests are scanned and configured PCI and PII types redacted before egress. Detection is best-effort, not guaranteed.
- **Tamper-evident model evidence** Every captured interaction is signed on the device with Ed25519 and hash-chained, so any change is detectable.
- **Your keys, your infrastructure** The admin server runs on infrastructure you control, storing ciphertext under a key only you hold. Even Verillian cannot read your content.

Maps to the frameworks you answer to: SR 11-7 model evidence, GLBA boundary redaction, SOX policy change history, and SEC and FINRA recordkeeping, retained on your infrastructure and aligned to your retention.

To start a pilot, name a sponsor and a technical contact and we will scope the first week on your own infrastructure, under your own keys.

hello@verillian.ai