Put AI to work in the agency. Keep a record oversight can verify.

276

Comparitech, Government Ransomware Roundup, ransomware attacks on government organizations in the first nine months of 2025.

THE EXPOSURE

- **Citizen data in the path.** Citizen data sent in prompts to AI tools, with no control between the workstation and the provider.
- **Shadow AI on agency hosts.** Personal accounts, browser sessions, and command-line clients, outside any sanctioned route and invisible to downstream controls.
- **Nothing to produce for oversight.** No verifiable record to answer an inspector general, a records request, or an oversight inquiry.

WHAT CHANGES WITH VERILLIAN

- **Decision before egress.** Policy enforced before content reaches a provider: allow, redact, or block, and fail closed with no valid policy.
- **Redaction at the device.** Outbound requests scanned at the device; SSNs and configured types redacted or blocked. Detection is best-effort.
- **Your keys, your record.** Audit content encrypted under a key only the agency holds; even Verillian cannot read your content.
- **Evidence oversight can verify.** Each captured interaction is signed and hash-chained into a tamper-evident record an inspector general can verify.

undefined

Built for FedRAMP-aligned and FISMA environments, with deny-by-default policy and audit controls mapped to NIST 800-53 AU. Where criminal justice data is in scope, the record aligns to CJIS Security Policy v6.0. Aligned, not certified.

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

hello@verillian.ai