Logs are not proof

The gap in ordinary logging

Most logs are mutable, held by the same system or vendor that produced them, and assembled after the fact. Each of those is a reason a regulator or a court will discount them. If the keeper of the log could have changed it, its word against a determined challenge is weak. The moment that matters is not when you write the log. It is years later, when an auditor, an inspector general, or opposing counsel asks you to produce the record and show it was not altered.

$4.44M

Global average total cost of a data breach in 2025, the first decline in five years as faster AI-assisted containment cut costs. The U.S. average reached a record $10.22 million, and shadow AI added roughly $670,000 to the average breach. Source: IBM Cost of a Data Breach Report 2025.

The figure that falls when controls work is the same figure that rises when you cannot prove what your AI did. In regulated sectors the gap is widest. Healthcare remained the costliest industry at $7.42 million per breach, and financial services the second-costliest at $5.56 million (IBM Cost of a Data Breach Report 2025). For 2024, HHS reported that roughly 243 million individuals had protected health information exposed in healthcare breaches that occurred that year, driven largely by the single Change Healthcare incident (HHS Office for Civil Rights, reports to Congress, 2024). The exposure is not abstract, and neither is the obligation to account for it.

What turns a record into evidence

Signed at the source

Each entry is cryptographically signed by the device that produced it, so its origin cannot be repudiated later. The signature is made before the record reaches any server, so no server, and no one at Verillian, can forge it.

Tamper-evident

Entries are hash-chained: each one carries a fingerprint of the one before it. Change any captured entry and every fingerprint after it breaks. Alteration is not prevented, it is made undeniable. The control is tamper-evident, not tamper-proof, and that distinction is the honest one to make to an auditor.

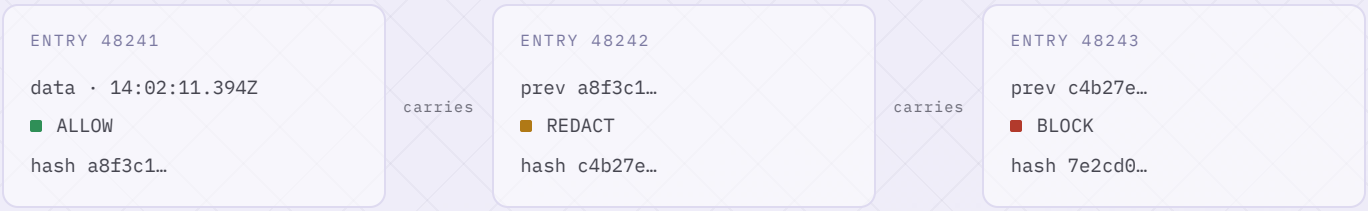
Independent of the vendor

Content is encrypted under keys the institution holds, on a server that stores ciphertext it cannot read. Even Verillian cannot read the record. You verify its integrity mathematically, independent of vendor attestation, rather than taking anyone's word for it.

Captured, not reconstructed

The record is written before content leaves the device, on every captured interaction, not assembled afterward from samples. The sentinel governs any tool that reaches a provider over HTTPS, including unsanctioned shadow AI tools, and audit content is fully parsed for Anthropic, Claude, and Claude Code today, with best-effort detection across other providers. Detection and redaction at the boundary are best-effort, so the evidence claim is about the captured record, not a guarantee that nothing escaped.

The hash chain, in one picture



Each entry carries the fingerprint of the one before it. Edit entry 48241 and its hash changes, which means the "prev" in 48242 no longer matches, which breaks 48243, and on to the end of the chain. One change is visible everywhere after it.

Why an ordinary log fails when it counts

When the PowerSchool student-information breach surfaced in early 2025, the threat actor claimed to hold data on roughly 62.4 million students and 9.5 million teachers; PowerSchool did not confirm a total affected (BleepingComputer, January 2025). Cases like this turn on what a system actually did and when, and on whether the record of it can be trusted. Government targets are not spared: there were 276 ransomware attacks on government organizations in the first nine months of 2025, a 41 percent increase over the same period in 2024, with 443,522 records known to have been breached in confirmed attacks (Comparitech, Government Ransomware Roundup, Q1 to Q3 2025). The FBI's Internet Crime Complaint Center logged 220 ransomware complaints from the Government Facilities sector for 2024, the third-most of any critical-infrastructure sector (FBI IC3, 2024 Internet Crime Report). In every one of these, the after-the-fact question is the same: produce the record, and show it was not changed. A log the keeper could have edited does not answer it.

Why this matters where you operate

The CJIS Security Policy v6.0 calls for tamper-evident audit and one year of retention, mapped to the NIST 800-53 AU (audit and accountability) controls. HIPAA expects six years of documentation retention. Litigation holds, public-records requests, and any proceeding that turns on what a system did all demand a record that survives challenge. A signed, hash-chained record held under your own keys is one you can stand behind without asking anyone to take your word for it. Verillian is aligned to these frameworks, not independently certified, and CJIS alignment is validated through your agency's state-agency audit. This is the evidence half of the job: the record is built to prove itself.

Anyone can keep a log. Evidence is a log that can prove it was not changed.

To see the signed, hash-chained record built on your own infrastructure, under your own keys, name a sponsor and a technical contact and we will scope a pilot.

hello@verillian.ai