

LogVeil — Glossary

v1.0 · 5 September 2026 · PUBLIC

LogVeil, from Zindagi Technologies, sanitises the diagnostic bundles that network teams send to their equipment vendors' support centres. Its documents, its screens and its attestation use a small, fixed vocabulary. Where an internet standard already has a word for the thing — RFC 6235, the IETF's vocabulary for anonymising network measurement data — LogVeil uses that word, so an evaluator with a network background can read an attestation without a translator. This page defines the words in plain language.

The things

Bundle — the file a device or a management system produces for the vendor's support centre: an archive (tar, tgz, zip, or an encrypted container), a single very large text file, or a packet capture. To the vendor it is diagnostics; to anyone else it is the network in a box.

Container — anything that holds other files: tar, gzip, zip, bzip2, xz, zstd, 7z, an encrypted container, or a section stream inside a single-file bundle. Containers nest inside containers.

Member — one file inside a container, at any depth. A container's own metadata — file names, owners, timestamps, comments, the original filename a compressor recorded — counts as a member's content, because it leaks like content.

Profile — LogVeil's description of one vendor's bundle family: how to recognise it, which members are what, which to drop, how to split sections, how to decrypt, what to leave alone. A profile is a declarative text file. A new vendor or a new product is added by writing a profile, not by changing the engine.

Policy — the customer's complete instruction set for a job: the dictionary, the treatment of each sensitivity class, the preserve list, member actions, the output address pool, attestation options and review thresholds. A policy is versioned and signed, and it belongs to the customer. Zindagi never sees it.

Dictionary — the explicit part of a policy: this subnet becomes that subnet, this site name becomes SITE-07, this keyword becomes that keyword. Dictionary rules always win over the automatic transforms.

Preserve list — values deliberately left as they are: loopback and broadcast addresses, documentation ranges, well-known resolvers, object-identifier roots, product version strings. The policy may extend or narrow it.

Map — the complete table of every original value and its replacement, compiled for one job before anything is rewritten. The map is stored encrypted. Reading it back is a privileged, audited, one-value-at-a-time operation (see reversal).

Transform — the rule that produces a replacement for a class of value: a dictionary pin, a prefix-preserving cipher, a keyed token, a drop, or a redaction.

Recogniser — a detector for one sensitivity class — an address, a hostname, a serial number, a credential — with context, plausibility filters and test vectors. Recognisers ship in packs.

Canary corpus — synthetic bundles with deliberately planted sensitive values and deliberately planted look-alikes (version strings, object identifiers). A policy is tested against it before it is signed, so the customer knows what it catches and what it leaves alone before a real bundle is processed.

What LogVeil does to a value

Sanitisation — the headline verb: rewriting or removing sensitive values under a policy so that the output can be released. LogVeil sanitises; it does not "clean" or "scrub", which suggest a search-and-replace that cannot say what it missed.

Pseudonymisation — what most transforms do: replacing a value with a stand-in that is consistent (the same original always gives the same stand-in under the same key) and reversible only under the customer's key.

Prefix-preserving — the property of the address transform: two addresses that share a prefix of a given length before rewriting share a prefix of the same length after it, so subnet structure survives and the vendor's engineer can still reason about the topology.

Redaction (black-marker) — what happens to secrets: passwords, community strings, shared secrets, private keys and certificate bodies are dropped and marked, never turned into stand-ins.

Anonymisation — a word LogVeil avoids as a description of itself, because it implies that the original can never be recovered. Controlled reversal is a feature, so the precise word is pseudonymisation.

Truncation, binning — coarser transforms from the same standard, available where a policy wants them: cutting a value short, or replacing it with the range it falls in.

What LogVeil says about a result

Verification — a separate stage, with its own code, that examines the output bundle rather than the engine's memory: the engine re-scans its own output; a differential canary scan searches for every original value in every encoding; independent secret scanners run unmodified; container metadata is checked against a catalogue of known leak paths; every passed-through binary is listed. A job with a hit, an unresolved review item or a scanner error produces no output — it fails closed.

Sanitisation Attestation — the signed manifest that accompanies every output: what went in and what came out, per member, with hashes; which policy, profile and packs were used, by version; which scanners ran and what they found; the time source; and the non-assertions. It is the product's honesty mechanism.

Non-assertion — a statement, mandatory in every attestation, of what is not claimed: sensitivity classes the policy did not cover, encodings outside the enumerated list, binaries passed through unread (by name), structural information that was not rewritten, unknown member formats, anything a reviewer overrode.

Offline verify — a standalone command that checks an output bundle against its attestation — hashes, membership, signature — without the LogVeil server.

Review queue — where ambiguous hits go: a candidate the recognisers could not decide about is neither silently masked nor silently kept; a person accepts, overrides or preserves it, and the decision is recorded in the attestation.

Reversal — translating one masked value back to its original when the vendor's reply refers to it. It is done one value at a time, with a written justification, under a two-person rule — the person asking and the person approving are different — and every reversal is written to the audit log. Bulk export of the map is not a function of the product.

Audit log — an append-only, hash-chained record of every action that changes state: policy signatures, key operations, reversals, review decisions. Hash-chained means each entry commits to the one before it, so an altered or missing entry is detectable.

How LogVeil is delivered

Offline kit — the delivery artefact: signed container-image tarballs, a pinned compose file, an installer, database migrations, a software bill of materials per image, signed checksums, and the source archive or written offer for every open-source component that requires one. It installs into the customer's own virtual machines.

Zero egress — the kit's network posture: a full job runs with outbound network blocked and no connection attempt is observed. There is no telemetry, no update check, no external font or script.

SBOM (software bill of materials) — a machine-readable list of every component in an image and its version, in the CycloneDX format; one per image, shipped in the kit.

Appliance — the hardware-and-software form on the roadmap: a server with fast local scratch storage, an optional GPU for local AI, sealed keys and a tamper-evident case.

Local AI — an optional assistant, off by default, that may look only at what is on the same host, with its network egress blocked, and that can open review items but can never change a map or an attestation. External AI services, if a customer enables one, receive only verified output or synthetic data.

TAC — the vendor's technical assistance centre: the recipient of the bundle. Honest, foreign-jurisdiction, under no duty to protect the topology, and keeping the bundle for as long as it likes.

Early access — a free, guided proof-of-concept on the customer's own bundles inside the customer's own network. LogVeil is in development. An early-access programme opens after our first field trial.

LogVeil is a product of Zindagi Technologies Private Limited · 301, 3rd Floor, Bakshi House, Nehru Place, New Delhi 110019 · sales@zindagi.tech · +91 97739 73971 · Document 2026-09-05_Z26-050_LogVeil-Glossary_v1.0 · PUBLIC