Send the bundle. Keep the network.

Send the bundle without exposing the network — and satisfy your own release policy before anything leaves.

THE PROBLEM

Every network team that runs Cisco, Check Point, Radware, Fortinet or Infoblox gear eventually opens a case with the vendor's technical assistance centre, and the TAC asks for the diagnostic bundle. That bundle is the network in a box — addresses and subnets, hostnames that encode sites, serial numbers, SNMP communities and RADIUS secrets, certificates and private keys, usernames. The vendor is honest but foreign-jurisdiction, under no duty to protect the topology, and may keep the bundle indefinitely. Today the team has three choices, all bad: **send it raw** and accept the exposure; **scrub it by hand** for days, with no way to know what was missed; or **do not send it** and live with the outage while the case stalls.

WHAT IT DOES

LogVeil, from Zindagi Technologies, takes an OEM diagnostic bundle in and gives back the same bundle with every sensitive value rewritten consistently under the customer's own policy, plus a signed Sanitisation Attestation stating exactly what was done, what was checked and what is not asserted — so the bundle can go to the vendor's technical assistance centre without exposing the network it came from.

FIVE PILLARS

- **Structure-aware, whole-bundle.** LogVeil understands the anatomy of the bundle — every member, every nested archive, every filename and header — and has no file-size ceiling.
- **Your policy, your dictionary, your key.** The customer writes the rules and holds the key; Zindagi never sees either.
- **Verified — and honest about what isn't.** A separate verification stage re-scans the output with independent scanners, fails closed, and signs an attestation that also says what is not claimed.
- **Reversible under control.** When the TAC replies about a masked address, your engineer can translate it back — and nobody else can.
- **Built for the air gap.** An offline kit for your own VMs; nothing phones home; AI is optional, off by default, and never touches the result.

FORMATS — THE PUBLIC ROADMAP

supported in early access	Cisco FMC troubleshoot bundle · Cisco FTD troubleshoot bundle (incl. high-availability pairs) · Cisco ISE support bundle · Cisco Catalyst Center RCA and support bundles
in development	Check Point Gaia cpinfo · Cisco IOS-XE show tech-support and btrace archives · Radware Alteon / vADC techdata · Radware DefensePro / NIPS support bundle
planned	Cisco Catalyst 9800 WLC debug bundle · Fortinet FortiGate TAC report and console log · Infoblox NIOS support bundle · Juniper Junos RSI · Palo Alto Networks PAN-OS tech support file (TSF) · packet captures (pcap, pcapng) · generic text archive (unknown bundle types)

Three statuses only; nothing here says "supported" without its qualifier. Register as at 5 September 2026.

> **LogVeil is in development. An early-access programme opens after our first field trial.** Early access is a free, guided proof-of-concept on your own bundles inside your own network — you write the policy with our help, and you keep the key. **Next step:** talk to us at **sales@zindagi.tech** or **+91 97739 73971**.

MEASURED ON REAL BUNDLES IN OUR LAB

The figures describe OEM bundle formats, not any customer.

11,412 files	**40,821 files**	**11,529 files**	**4.98 GB**	**fifteen-fold**
seven levels deep — Cisco FMC troubleshoot	nine deep — Cisco FTD HA troubleshoot	eleven deep — a third bundle	one member — Cisco ISE support bundle	expansion, to 73 GB — Catalyst Center RCA

Across nine bundles: 66,802 files, 2,216 nested archives, 113.8 GB of content from 11.4 GB on disk. Nobody hand-scrubs that.

The OEMs' own switches do not help much: they mask credentials only, and none touches location, serials, certificates or packet captures.

WILL THE VENDOR ACCEPT A SANITISED BUNDLE?

> We have not put the question to the OEMs. Some support processes ask for a bundle unmodified, and we would rather tell you that than pretend otherwise. LogVeil's value does not depend on the answer: it is also how you satisfy your own release policy before anything leaves your network — what may go out, under whose rules, with what record — and that decision is yours whatever a vendor's process says.

ABOUT ZINDAGI TECHNOLOGIES

Zindagi Technologies is a systems-engineering organisation building sovereign, large-scale, mission-critical infrastructure for government and defence, predominantly as the technical delivery partner to system integrators. Founded 2017; bootstrapped. ISO 9001:2015 and ISO 27001:2022 certified; DPIIT-recognised Startup; Udyam MSME (Small); incubated inside DSCI. Engineering team in-house — no outsourcing, no freelancers. Our flagship product is CriticalRange™ (criticalrange.com), a sovereign cyber range platform; LogVeil comes from the same engineering team. Corporate office: 301, 3rd Floor, Bakshi House, Nehru Place, New Delhi 110019.

Zindagi Technologies Private Limited · 301, 3rd Floor, Bakshi House, Nehru Place, New Delhi 110019 · sales@zindagi.tech · +91 97739 73971 · logveil.com · 2026-09-05_Z26-050_LogVeil-One-Pager-Public_v1.0