

ZYVOR

NETRA PRODUCT PERSPECTIVE

OBSERVE · DIAGNOSE · CONTAIN · FAIL OPEN

Network observability and emergency control, without CNI lock-in — now with metadata Surfaces for encrypted traffic, shadow SaaS, and fleet risk.

Standalone eBPF · Kubernetes · Linux · Leased enforce · Optional Cilium

The network problem enterprises face

01

Blind spots at the node

CNI dashboards miss softnet, qdisc, and kernel drops.

02

CNI lock-in for visibility

Mixing networks should not erase observe + emergency control.

03

Encrypted without decrypt

Buyers need JA3 / DoH / shadow SaaS — not SSL break.

04

Dangerous permanent denies

Kill-switches that never expire become tomorrow's outage.

05

Tool sprawl

Capture, alerts, SIEM, AI each live in a different console.

06

Payload risk

Evidence without bodies, argv, or secrets.

What Netra is

Standalone eBPF observability and leased emergency control.

Node agent owns programs under `/sys/fs/bpf/netra`. Cilium/Hubble are optional enrichment. Custom enforcement is time-leased and fails open to observe.

OBSERVE

Flows, DNS/SNI/Host, JA3/JA4 samples, topology, TCP health
— metadata only.

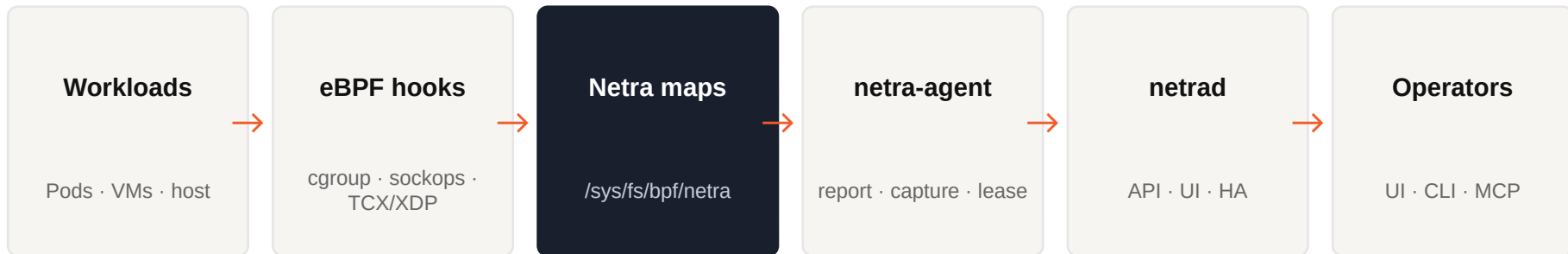
DIAGNOSE

Path, Drop, Congestion Map,
Explain, filtered capture + auto-PCAP.

CONTAIN

Emergency deny/rate/Shield
behind an observe → enforce
lease that auto-reverts.

How Netra works



Default datapath is CNI-independent. Agent never pins over Cilium-owned maps. Surfaces boards consume the same agent metadata — no second datapath.

Hard boundary: no application payloads, argv/cmdline, or Secret contents. TLS is ClientHello metadata (SNI, JA3/JA4, ECH flag) — never decrypt.

Surfaces — P0–P5 observe boards

One console page for every metadata fit surface. Observe-only. Wired to L7, Fleet, and Report.

Encrypted

JA3/JA4 · JA3 risk · DoT/DoH · ECH / missing SNI

Fit

Shadow SaaS · Experience · Dest risk · ZT / microseg / packs / identity

Threat

Intel feed · DNS intel · Exfil · Lateral · Category deny

Ops

App categories · Compliance · AI destinations · Auto-mitigate · Prevention

Fleet

Multi-cluster peers · Tenant risk scores (MSSP)

Encrypted traffic — without decrypt

01

Always-on JA3/JA4

Standalone bpf/netra_tlsfp.c samples ClientHello (rate-limited). Own verifier budget vs L7. Capture still feeds the same parser.

02

DoT / DoH

Port 853 for DoT; known DoH hosts via SNI / HTTP Host / DNS — no payload open.

03

Risk & ECH boards

Rare JA3, missing SNI, ECH extension 0xfe0d, and CDN blindness — where hostname visibility is weak.

Fit maps buyers ask for (metadata only)

Shadow SaaS

Sanctioned host allow-list vs observed SNI/Host/DNS

Workload DX

Latency / retrans / DNS fail scorecard — no endpoint agent

Destination risk

Intel + categories + DoH/DoT + exposure + volume

Policy / identity drafts

Review-only CNP / SA-keyed sketches — never auto-applied

Threat intel + AI dest

Live feed hits; GenAI/MCP SaaS catalog; optional leased deny

Fleet tenants

MSSP partner rollups with RiskScore across peers

Observe — metadata the kernel already sees

L2/L3

IPv4 · IPv6 · direction ·
hooks

L4

TCP · UDP · ICMP · flags
· ports

L7 meta

DNS · SNI · HTTP Host ·
JA3/JA4

Identity

Namespace · Pod ·
comm · UID · cgroup

Hard boundary: no application payloads, argv, or Secrets. HTTP is method + Host only — never bodies or paths.

Diagnose — five surfaces, one investigation story

- 1 Path** Connect latency, cwnd, retransmits, edge TCP intel
- 2 Drop** kfree_skb reasons, softnet, qdisc — where packets die
- 3 Congestion Map** Stack stages colored by severity across the cluster
- 4 Explain** DNS rcode, ICMP MTU/unreachable, next-checks
- 5 Capture** Filtered live capture + opt-in auto-PCAP

Contain — leased emergency control

Stop the bleed. Automatically return to observe.

- ▶ Exact IP / CIDR deny (+ SYN-drop)
- ▶ Port · DNS · SNI · UID · process
- ▶ PPS / BPS ceilings · conn-rate
- ▶ Optional XDP Shield on selected NICs

01 Observe

02 Plan + confirm

03 Enforce (leased)

04 Auto-revert

Safety model

Observe-first

Enforcement is never the silent default.

Plan + risk confirm

Policy apply stays behind plan-token and confirmation.

Fail open

Lease expiry, agent loss, restart, HA handoff → observe.

Blast-radius preview

Review-only deny preview against live counters.

Map isolation

Never pins over Cilium-owned BPF maps.

No secret harvesting

No payloads, argv, or Secrets in reports or AI.

Operate & integrate

Dashboard

Overview, Surfaces, Firewall, Health, Congestion, Capture, Insights

Alerting

Webhook, email, Slack, Teams, Twilio — HA leader-only

SIEM / metrics

JSON/CEF/syslog/OTLP pull, Prometheus, optional Snowflake

ChatOps

Slack & Teams: status, health, ask — mode needs confirm

AI briefs

Ask / digest / explain / draft — read-only; never flips enforce

MCP

Tools for AI agents; mutations gated off by default

How a day looks

01

Signal

Alert / Congestion
critical / intel hit / rare
JA3

02

Evidence

Surfaces board · live
or auto-capture PCAP

03

Decide

Blast-radius preview ·
plan token · confirm

04

Contain

Leased deny / rate /
SYN-drop on the
scope

05

Revert

Lease ends →
observe · full audit trail

Why buy Netra

CNI-independent

Keep observability when the stack changes or is mixed.

Fail-open by design

Emergency controls that cannot silently become permanent.

Encrypted-traffic intel

JA3/JA4 + DoH/DoT + ECH boards — no SSL inspection.

Stack-deep diagnostics

Softnet to socket — not just CNI verdicts.

Surfaces for SecOps

Shadow SaaS, dest risk, intel, fleet tenants in one UI.

Zyvor Production License

Free for non-production; a commercial license for production.

Suite placement — Netra & PacketWolf

Suite counterparts, not a wired pipeline. No control-plane sync today.

	Netra	PacketWolf
Job	Observe + diagnostics + leased emergency	Observe + AutoPolicy + healer depth
CNI	None required (Cilium optional)	Cilium-first
Policy	Review drafts; enforce time-leased	Durable Cilium policy
Maps	Owns /sys/fs/bpf/netra only	Works with Cilium datapath

NEXT

**See the network.
Contain the incident.
Fail open by default.**

[Buyers guide](#) · [docs/sales/buyers-guide.md](#) · [zyvor.dev/netra](#) · sales@zyvor.dev