LMNTRIX
BE THE HUNTER | NOT THE PREY

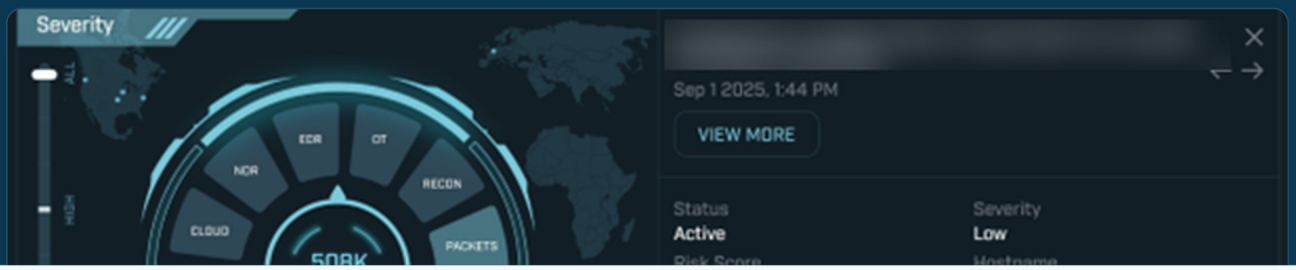
DATASHEET

THE NETWORK FORENSICS MODULE OF LMNTRIX XDR

# LMNTRIX Packets

## Logs only tell part of the story. Packets tell the rest.

LMNTRIX Packets is a time machine for your network. It records every packet, or every session's metadata, at your egress, core, DMZ and cloud, keeps it for up to a year, and lets the Cyber Defense Center replay the past: rebuild sessions, pull out files, hunt for behavior no signature matched, and prove what happened.




**A Packets alert in the LMNTRIX XDR heads-up display.** The detection lands as an incident beside every other module, with the full session one click away.

**30 days**
Default retention of captured traffic

**12 months**
Maximum retention, on request

**3,000+**
Protocols parsed, layer 2 to layer 7

Full-packet or metadata-only capture from 100 Mbps to 10 Gbps and beyond, licensed on aggregate throughput, not on the number of sensors.

THE CORE CAPABILITIES

## Capture everything. Rebuild anything. Prove what happened.

### Full-fidelity capture

- Every packet, or rich session metadata, at line rate
- Egress, core, DMZ and cloud capture points
- Nothing sampled, nothing summarized away

### Session reconstruction

- Rebuild HTTP, SMTP, FTP, DNS and SMB conversations
- See what was sent, by whom, to where, and when
- An evidence-grade timeline of the intrusion

### File and evidence extraction

- Carve transferred files, attachments and executables
- Hash, detonate and extract indicators from each one
- Chain-of-custody ready for legal and insurers

### Retrospective analysis

- Replay stored traffic against today's intelligence
- Find yesterday's unknown threat the day it is named
- Answer "were we hit?" with evidence, not opinion

THE FOUR CAPABILITIES

# One sensor, four jobs

Packets records the network so the Cyber Defense Center can go back in time. The same stored traffic serves four purposes: forensics after a breach, behavior-based detection as it happens, retrospective matching against fresh intelligence, and analyst-led threat hunting.

### 01 · POST-BREACH FORENSICS

**Memory for your network.** Full packets or session metadata stored for up to a year, so the evidence exists before anyone knows it is needed.

**What it answers.** How did they get in, where did they move, what did they take, where did it go, and how long were they inside.

**What you get.** Rebuilt sessions, carved files, a timeline you can hand to legal, insurers and regulators.

### 02 · BEHAVIOR-BASED DETECTION

**Behavior, not signatures.** A curated library of network behavior rules, engineered and tuned by LMNTRIX, runs across every session the sensor sees.

**What it catches.** Lateral movement, command-and-control beaconing, DNS tunneling, data staging, protocol misuse, anomalies against each entity's baseline.

**Depth.** 3,000+ protocols parsed from layer 2 to 7; encrypted traffic profiled by its metadata, or inspected in full with external decryption.

### 03 · RETROSPECTION

**Today's intelligence, yesterday's traffic.** Every new indicator from LMNTRIX Intelligence is replayed against the stored capture, automatically.

**Why it matters.** A domain, hash or IP named today was unknown last month. Retrospection finds the connection that was already made and missed by every live control.

**The result.** "Were we hit?" answered in hours, with the session as proof.

### 04 · THREAT HUNTING

**Indicators of activity, not signatures.** Hunters work the session metadata for the patterns attackers cannot avoid: who talked to whom, how often, how much, over what.

**Living off the land.** Legitimate tools used illegitimately show up in traffic shape long before any alert fires.

**Compounding.** Every confirmed hunt becomes a new behavior rule, so the next one is caught automatically.

THE LIFECYCLE

# From raw traffic to proof

**01**
### Capture
A sensor on a SPAN or TAP records every packet, or every session's metadata.

**02**
### Reconstruct
Sessions are rebuilt, files carved out, conversations made readable.

**03**
### Enrich
Every session is tagged with threat intelligence, entity profile and risk.

**04**
### Hunt
Behavior rules run live; analysts hunt the metadata on a cadence.

**05**
### Prove
The incident ships with the session, the file and the timeline attached.

SEE WHAT OTHERS MISS

# Answer the questions logs cannot

### Lateral movement
A log shows a login. The packets show the SMB session, the file that was copied and its hash.

### Encrypted command and control
Beacon cadence, TLS fingerprints and odd certificate chains give a channel away without decrypting a byte.

### Insider and exfiltration
The upload, its size, its destination and the file itself, recovered from the capture.

THE MDR SERVICE

# A network detection becomes a hunted, proven, contained incident

Packets is a managed capability, not a sensor you have to staff. The Cyber Defense Center engineers the detection content, runs the hunts, investigates every detection in the raw traffic and contains what it confirms through LMNTRIX XDR, 24 hours a day.

**01**
### Detect
Behavior rules and intelligence matches fire on live and stored traffic.

**02**
### Investigate
An analyst opens the session behind the alert and rebuilds what happened.

**03**
### Hunt
Hypothesis-driven hunts across the metadata, on a published cadence.

**04**
### Contain
Isolate the host, block the destination, disable the account, via XDR.

**05**
### Prove
The incident ticket carries the session, the file and the timeline.

## WHAT THE CYBER DEFENSE CENTER DOES

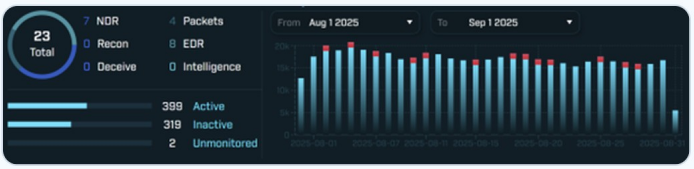
**Engineers the detections.** LMNTRIX maintains and tunes the behavior rule library to your environment. There are no signatures for you to write, update or own.

**Pivots into the packets.** When NDR, EDR, SIEM, Deception or Email raises an alert, the analyst opens the matching session, rebuilds it and extracts the file.

**Runs retrospection.** Each new indicator from LMNTRIX Intelligence is replayed against the stored capture; a hit becomes an incident with the historic session attached.

**Hunts on a cadence.** Hypothesis-driven hunts across the session metadata, maturing from ad-hoc searches to analytics-led, automated hunting.

**Contains through XDR.** Confirmed threats are isolated at the endpoint, blocked at firewall, DNS and email, and the account disabled, under pre-agreed rules.




**One kill box for every module.** Packets detections sit beside NDR, EDR, Recon, Deceive and Intelligence, so an analyst sees the whole attack, not one sensor's view of it.

### WHAT YOU RECEIVE

Incidents in LMNTRIX XDR with the session evidence attached; forensic reports after any breach; hunt reports each cycle; retrospection results as intelligence lands; and an analyst you can reach 24 hours a day.

THE DEPLOYMENT

### The sensor

- Virtual appliance or physical server, supplied by you, validated by LMNTRIX
- Two interfaces: management (static IP) and capture (SPAN or TAP)
- Placed after perimeter controls at egress, core, DMZ or cloud; can share the NDR appliance
- Outbound only to the XDR cloud: 443, 80, 22, DNS and NTP
- Encrypted traffic profiled by metadata; full inspection needs your decryption feed
- Licensed on aggregate throughput, however many sensors

| THROUGHPUT | CORES | RAM | FILE STORE |
|---|---|---|---|
| **160 Mbps** | 4 | 12 GB | 1 TB |
| **320 Mbps** | 8 | 24 GB | 4 TB |
| **560 Mbps** | 12 | 42 GB | 10 TB |
| **800 Mbps** | 16 | 60 GB | Sized at scoping |
| **1 Gbps** | 20 | 78 GB | Sized at scoping |
| **2 Gbps** | 36 | 150 GB | Sized at scoping |

Per capture point. The file store holds five days of extracted files locally; traffic is retained in LMNTRIX XDR. Above 2 Gbps, sizing is agreed at scoping.

THE SERVICE

# Who does what

A subscription module of LMNTRIX XDR: you provide the host and the mirror port; LMNTRIX does everything else, from implementation to the 3 a.m. investigation.

### LMNTRIX PROVIDES

- Sensor license, image and configuration
- Remote implementation with a named project manager
- Behavior detection content, intelligence feeds and hunting
- 24×7 monitoring, investigation and containment via XDR
- Sensor health monitoring and capture-gap alerts
- 24-hour access to the Cyber Defense Center

### YOU PROVIDE

- A virtual or physical host to the sizing table, validated by LMNTRIX
- A SPAN or TAP feed after your perimeter controls
- Management IP, DNS and outbound firewall rules
- Internal IP ranges and a network diagram
- The throughput and capture points to cover
- Who receives escalations, and on which channels

WHAT SETS IT APART

| CAPABILITY | LMNTRIX PACKETS | FLOW LOGS OR SIEM ALONE |
|---|---|---|
| **Evidence** | Full packets, rebuilt sessions, the files | Flow summaries and log lines |
| **Retention** | 30 days default, up to 12 months | Days, if captured at all |
| **Detection** | Behavioral, plus retrospective | Thresholds and known signatures |
| **Encrypted traffic** | Profiled by metadata, decrypted on request | Opaque |
| **Hunting** | Analyst-led, included | Your team, if time allows |
| **Response** | CDC investigates and contains, 24×7 | Alert handed to you |

QUESTIONS. CLEAR ANSWERS.

**How is Packets different from LMNTRIX NDR?**

NDR detects and blocks on the wire, in real time. Packets keeps the evidence and lets us go back. NDR says something happened; Packets shows exactly what.

**Can the capture stay on our premises?**

Yes. Retention is 1, 2 or 3 months in LMNTRIX XDR by default, up to 12 on request, with optional on-premises retention for data-residency needs.

WHAT WE NEED TO SCOPE IT

- Full-packet or metadata-only capture
- Aggregate throughput, 100 Mbps to 10 Gbps+
- Capture points: egress, core, DMZ, cloud
- Retention period and on-premises option

Priced by throughput subscription, MDR included. Typical go-live within two weeks of the host being ready.

## Attackers leave footprints in your traffic. Keep the evidence.

Every engagement starts with a free 30-day proof of concept on a sensor at your own egress, plus a complimentary quarterly value-add assessment.

BOOK A DEMO

sales@lmntrix.com

Major Player — IDC MarketScape: Worldwide MDR/MXDR Services for the Enterprise 2026 · Representative Vendor — 2024 Gartner Market Guide for Managed Detection and Response · #19 — MSSP Alert Top 250

© 2026 LMNTRIX. All rights reserved.