LMNTRIX
BE THE HUNTER | NOT THE PREY

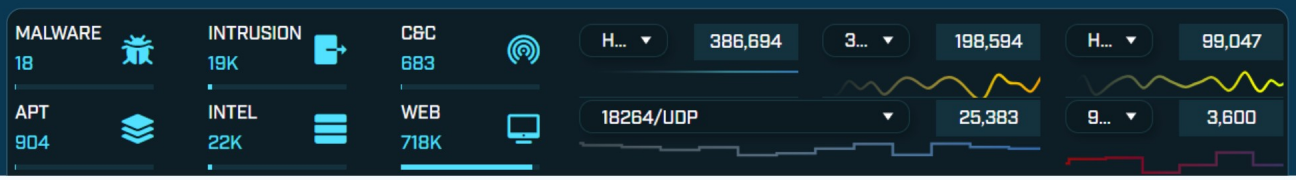
DATASHEET

THE NETWORK DETECTION AND RESPONSE MODULE OF LMNTRIX XDR

LMNTRIX NDR

See everything. Stop anything.

LMNTRIX NDR turns your network into a transparent, intelligent defense system. A passive sensor behind your perimeter controls runs ten threat-detection engines against every ingress, egress and east-west flow, 24 hours a day, and hands what it finds to LMNTRIX XDR and the Cyber Defense Center for validation and containment, before an attacker can cause business disruption.



The LMNTRIX XDR heads-up display. Network events from NDR sensors arrive as C&C, intrusion, malware and web counters, beside the endpoint, identity and cloud modules, with the targeted hosts listed as they are hit.

95%
Reduction in mean time to detection

85%
Decrease in false-positive alerts

3×
Improvement in SOC team efficiency

Customer success metrics across LMNTRIX NDR deployments. Source: lmntrix.com/lmntrix-ndr

THE CORE CAPABILITIES

Visibility, detection, response and context in one sensor

Complete network visibility

- East-west and north-south traffic analyzed from SPAN or TAP
- Every connected device discovered and classified
- Deep inspection with no impact on production traffic

Multi-engine threat detection

- Ten engines: pre-infection, post-infection and data leakage
- Behavioral baselines and machine learning for unknown threats
- 300+ intelligence feeds correlated against every flow, hourly

Autonomous response and containment

- Confirmed breaches contained automatically; uncertain ones validated by analysts first
- Compromised hosts isolated, lateral movement blocked
- Playbooks tuned to your environment, with escalation to the CDC

Unified XDR context

- Network signals beside endpoint, identity, email, mobile and cloud
- IP addresses resolved to users and machines through Active Directory
- Pivot from an alert to full packet capture with LMNTRIX Packets

THE TEN ENGINES

Ten engines against every flow, in and out

Every engine runs on the sensor against live traffic. The Cyber Defense Center tunes each policy to the asset types on every segment, and signatures refresh hourly.

PRE-INFECTION

Intrusion detection	Known exploits, protocol misuse, tunneling and risky peer-to-peer apps.
Web application detection	Attacks on internally hosted applications, tuned to the apps you declare.
Anti-malware	Files in and out classified against known malware; malware-hosting URLs checked on access.
Emulation (sandbox)	Unknown files detonated on multi-OS virtual machines; CPU-level emulation catches evasive and zero-day samples.
Email security and anti-spam	Zero-hour and signature detection on SMTP and POP3, plus pattern-based spam detection that keeps content private.

POST-INFECTION

Bot detection	Infected machines found by command-and-control addresses, botnet-family patterns and click-fraud behavior.
Threat intelligence	300+ feeds aggregated into one, refreshed hourly, and matched against every inbound and outbound flow.

DATA, PEOPLE AND POLICY

Data leakage detection	Deep content inspection of outbound traffic and attachments against predefined and customer-specific data types.
Context awareness	IP addresses mapped to users and machines from Active Directory, so every incident names a person, not a number.
Web security	Application control and URL categories surface illicit browsing and bandwidth abuse before they become incidents.

FROM EVENT TO CONTAINMENT

Metadata in, validated incidents out

01
Mirror
A SPAN or TAP copies the segment to the sensor. Nothing sits in line.

02
Detect
Ten engines inspect the flow. Only threat metadata leaves, encrypted.

03
Validate
LMNTRIX XDR validates each event and correlates it with endpoint, identity and cloud telemetry.

04
Contain
Confirmed breaches are contained automatically; if unsure, an intrusion analyst confirms first.

05
Escalate
Remediation runs, or the incident is escalated to you with the evidence attached.

Privacy by design
No packet capture, no connection logs on the sensor. Events are threat metadata only; this is not a log store.

Encrypted traffic
Flows are watched for abnormal patterns as they are; for inspection inside TLS, your firewall's SSL inspection feeds the sensor.

Negligible footprint
The metadata sent to LMNTRIX XDR is minimal, with no measurable impact on your Internet link.

THE DEPLOYMENT

Passive, behind your perimeter, wherever traffic matters

The sensor is deployed after your perimeter controls (firewalls, IPS, WAF, web and mail gateways) so it sees cleaned traffic, and at the segments where high-value assets live. It must at minimum watch the inside interface of the perimeter firewall; for east-west detection it also watches the server segment.

Internet egress

The inside of the perimeter firewall: outbound command-and-control, data leakage, inbound malware that got through.

Internal core

Traffic to and from servers: lateral movement, bots inside, misuse of internal protocols.

DMZ

Inbound traffic to exposed servers and web applications.

Cloud and OT

A virtual sensor in your cloud VPC or VNet; optional monitoring of OT networks through LMNTRIX ICS/OT.

THE SENSOR

Form factor	Pre-configured physical appliance, or a virtual machine on VMware, Hyper-V or KVM; cloud-native in AWS, Azure and Google Cloud.
Interfaces	One management NIC with a private IP for the encrypted link to LMNTRIX XDR and Active Directory; one or more capture NICs on SPAN, mirror or TAP ports. Taps must copy both directions to one interface.
Connectivity	Bi-directional management access to LMNTRIX XDR over VPN, or direct Internet with ports opened from the XDR to the sensor; outbound to threat-update clouds.
Agentless	Nothing is installed on endpoints or servers; the sensor sees them through their traffic.
Scale	One sensor per segment; small branch to enterprise core. Memory scales with concurrent connections: 2 GB for one million, 12 GB for five million.
Retention	Nothing retained on the sensor. Pivot to LMNTRIX Packets for full packet capture and network forensics when the engagement includes it.

SIZING THE VIRTUAL SENSOR

CPU cores	SPAN / TAP throughput
2	200 Mbps
4	300 Mbps
8	600 Mbps
12	800 Mbps
16	1 Gbps
20	1.2 Gbps
24	1.4 Gbps

Minimums with dedicated virtual cores; scale beyond the minimum to allow for growth. The most efficient point is eight cores. Hardware is validated by LMNTRIX before deployment.

THE USE CASES

Advanced persistent threats

Bots and command-and-control seen on the wire long after the implant has blinded the endpoint.

Ransomware and lateral movement

Staging, scanning and spread across the core caught before encryption starts.

Insider and supply-chain risk

Data leaving by the wrong path, and compromised third-party software calling home.

THE SERVICE

Who does what

A managed subscription of LMNTRIX XDR: you provide the mirror port and rack space, LMNTRIX does the rest.

LMNTRIX PROVIDES

- The pre-configured sensor, direct or via an authorized partner
- Remote implementation with a project manager
- Management connectivity to LMNTRIX XDR
- Engine tuning and validation of every alert
- Sensor maintenance and remote health monitoring
- 24-hour access to the Cyber Defense Center

YOU PROVIDE

- Rack space, power and network, or a hypervisor host
- Sensor hardware sized to throughput, validated by LMNTRIX
- A SPAN or TAP per segment and a management IP
- The IP ranges in scope, and updates when they change
- An AD service account; data-leakage keywords and domains
- Internal app, DNS, proxy and scanner addresses for tuning

WHAT SETS IT APART

CAPABILITY	LMNTRIX NDR	STANDALONE NDR
Part of an XDR	Native; one incident across all telemetry	Siloed console, manual correlation
Detection engines	Ten, pre- and post-infection, plus DLP	Anomaly detection, often alone
Identity context	Users and machines, from Active Directory	IP addresses
Response	Automated containment, analyst-validated	Alerts; response is yours
Operations	Tuned and monitored 24×7	Your team, your tuning

QUESTIONS. CLEAR ANSWERS.

Is this a SIEM or a log platform?

No. The sensor sends threat metadata only; LMNTRIX SIEM and LMNTRIX Packets cover retention and forensics.

Will it slow the network?

No. It is out of band on a mirror port; it never sits in the traffic path.

WHAT WE NEED TO SCOPE IT

- Number of sites and network segments to monitor
- Peak throughput on each SPAN or TAP
- Physical, virtual or cloud sensor per site
- Whether LMNTRIX Packets is in scope for full capture

Subscription is sized to monitored throughput, CDC service included. The sensor is live the day the SPAN or TAP is available.

Know your network. Detect the undetectable.

Every engagement starts with a free 30-day proof of concept on your own network, 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.