LMNTRIX
BE THE HUNTER | NOT THE PREY

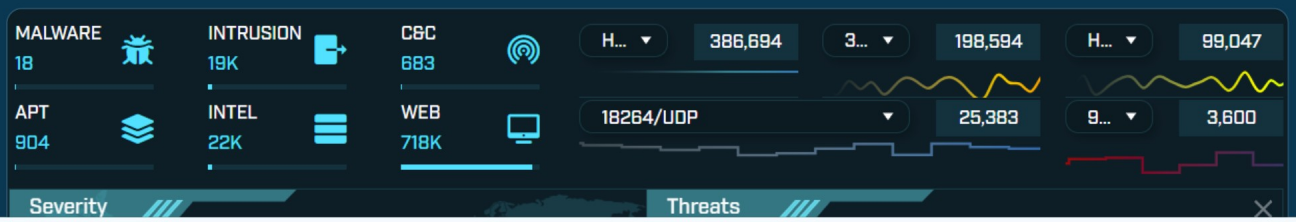
DATASHEET

THE PLATFORM BEHIND EVERY LMNTRIX MODULE

LMNTRIX XDR

One platform. One data model. One console. Built to run behind your controls.

Most XDR is a vendor's own products stitched together. LMNTRIX XDR was built as one platform: fourteen native modules writing into one data model, investigated in one console, operated by one Cyber Defense Center. It consumes what your existing stack sees and adds what it cannot: independent ground truth behind the controls you already own.



The LMNTRIX XDR heads-up display. Threat counters, the module wheel, severity and the latest targeted hosts, live.

14
Native detection modules on one data model, one console

300+
Threat intelligence sources enriching every detection

≤ 5%
False-positive rate after automated validation and supervised ML

Every alert is validated and enriched before it becomes an incident. Your team sees incidents with the story attached, not a queue of raw alerts.

THE ARCHITECTURE

Sense everywhere. Correlate once. Act from one place.

01
Sense
Agent, network sensors, cloud and identity APIs, mobile app, email API and log collection: native telemetry from every surface.

02
Unify
Every event lands in LMNTRIX Grid: one data lake and one data model shared by all fourteen modules.

03
Detect
Machine learning, behavioral analytics, detection rules, deception triggers and 300+ intelligence sources run against the same data.

04
Validate
Automated alert validation and supervised ML confirm, enrich and group alerts into incidents at a 5% false-positive rate or less.

05
Act
Artemis builds the case, analysts decide, and containment goes out through your own controls from one console.

Native, not stitched
One codebase and one deployment model across every module. Add a module and it writes into the same data, the same console, the same incident.

Behind your controls
Your firewalls, endpoint and email security keep running. LMNTRIX sensors sit behind them and assume they have already been bypassed.

Never sold empty
Every module ships with the MDR service: the Cyber Defense Center monitors, hunts, investigates and responds 24×7 in the same console you see.

THE CONSOLE

From first signal to closed incident, without leaving the console

Your team works in the same console the Cyber Defense Center does: every alert and incident in real time, the evidence behind each one, and the actions taken. Nothing sits hidden behind a service desk.

HUD

The live view across every module: threat counters, the module wheel, a severity filter, the threat map and the latest targeted hosts. The first screen every analyst opens.

Killbox

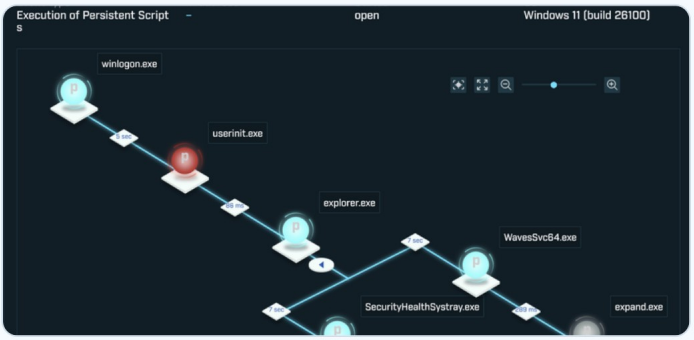
The incident workbench. Each detection opens as an attack chain: process tree or session graph, timing between steps, MITRE ATT&CK techniques, the affected asset and user. Take Action is one click away: isolate host, kill process, quarantine file, block indicator, disable account.

Explore and hunt

Search any field of any module's telemetry. Launch hunts by type: applications, file system, IOC search, network, persistence, process and registry. Saved hunts rerun on a schedule.

Incidents and reports

Every incident with its timeline, analyst notes, actions and SLA clock. Monthly technical reports and quarterly business reviews generated from the same data, and an audit trail of who changed what, and when.



A detection in the Killbox. The chain of processes, the seconds between them and the technique behind the alert, before an analyst has typed a single query.

ARTEMIS · THE AUTONOMOUS AI SOC

Artemis works every detection the way a senior analyst would: it pulls the related telemetry from all fourteen modules, reconstructs the attacker's path, scores the blast radius and drafts the containment plan, in seconds. Analysts validate and act. Nothing is contained on a machine's say-so alone.

LISA · YOUR CHATOPS ASSISTANT

Ask about any incident, host, user or threat in plain language, from the console, Slack or Teams, and get an answer grounded in your own telemetry. "What happened on this host last Tuesday" is a question, not a ticket.

LMNTRIX GRID

One data lake under all fourteen modules

Endpoint, network, packet, cloud, identity, email, mobile, deception, OT and log telemetry land in one schema. A host, user or IP seen by one module is instantly queryable against every other: correlation is a property of the data, not a rule someone has to write. One codebase and one deployment model mean a new module is switched on, not integrated. Retention is set per module and per client, from 30 days to 12 months, longer for log archives where compliance requires it.

THE AUTOMATION

Automated validation

Detection, alert validation, enrichment and incident creation run without a human in the loop. Analysts start from a validated incident.

Automated intelligence

300+ sources curated and de-duplicated continuously, matched against live telemetry and replayed against stored data as indicators land.

Automated response

Under rules you approve, confirmed indicators are pushed to your controls and hosts isolated the moment an incident is validated.

THE DEPLOYMENT

Cloud-delivered. Sensors where the attacker is.

LMNTRIX XDR is delivered as a cloud service. The only things inside your environment are the sensors that give it ground truth: lightweight, outbound-only over TLS, deployed without downtime.

SURFACE	SENSOR	FOOTPRINT	TIME TO TELEMETRY
Endpoint	Lightweight agent: Windows, macOS, Linux	No reboot; coexists with your existing AV or EDR	Minutes per host; a fleet in about two weeks
Network	Virtual or physical sensor on SPAN or TAP (NDR, Packets)	Management and capture interfaces; outbound only; sized by throughput	About two weeks
Cloud	API integration, read-only roles, agentless	AWS, Azure, Google Cloud and SaaS tenants; nothing installed	Within an hour per account
Identity	Directory agent plus Entra ID, Okta and Workspace APIs	Account blocking through an app registration you control	Days
Email	API, behind your native mail filter	No MX change, no interruption to mail flow	Hours
Mobile	App, pushed by your MDM or self-enrolled	iOS, Android and Chromebook; your MDM stays in charge of the device	Days
Logs	Syslog, API and agent collection (SIEM)	Your sources, your retention; or forward from the SIEM you keep	Weeks, paced by your IT
ICS/OT	Passive sensor on a mirror port	No agents, no traffic injected, no downtime	Days

Deceive seeds decoys and breadcrumbs through the same directory integration and sensors; AI Security adds a browser extension and an agent gateway. Every sensor authenticates with certificates and talks outbound only.

THE INTEGRATIONS

INGEST FROM, AND CONTAIN THROUGH, WHAT YOU OWN

LMNTRIX XDR is pre-integrated by pull, push and API with the major next-generation firewall, web security, DNS security, endpoint, email and identity platforms. It ingests their telemetry and, when it is time to contain, pushes the block, the isolation or the indicator straight into them. No console logins, no ticket to another team, nothing ripped out.

FITS THE WAY YOU ALREADY OPERATE

- Native ServiceNow integration; an API for every other service desk
- Keep your SIEM: we forward incidents to it, or consume its logs
- Slack and Teams through LISA; email and phone escalation on your rules
- Your existing AV or EDR keeps running alongside the agent
- A two-hour training session at onboarding, then on demand

THE TRUST

Certified

Platform and service certified to SOC 2, ISO 27001 and PCI DSS; GDPR-aligned.

Hosted

Cloud-hosted as a service; in-region hosting where data residency requires it.

Controlled

MFA enforced for every user, role-based access, audit trail of administrative change.

Separated

Your own tenant, encrypted in transit and at rest, retained only for the period you agree.

THE MDR SERVICE

The platform is never sold empty

Every module carries the MDR service: Cyber Defense Centers in seven countries monitor, hunt, investigate and respond 24×7 in the console you see, with unlimited containment and forensics included.

LMNTRIX PROVIDES

- Platform, sensors and detection content
- 24×7 monitoring, investigation and response
- Threat hunting; unlimited DFIR and containment
- Monthly reports, QBRs and a real-time portal
- A complimentary quarterly value-add assessment
- Dedicated account and technical account managers

YOU PROVIDE

- Sensor hosts and SPAN or TAP feeds
- API access for cloud, identity and email
- Response rules: notify, confirm or auto-contain
- Escalation contacts and change windows
- Console users and their roles
- The controls containment is pushed through

WHAT SETS IT APART

DIMENSION	LMNTRIX XDR	SUITE XDR OR MANAGED SIEM
Built as	One platform, one data model, one codebase	Acquired products behind one logo
Telemetry	Native sensors behind your controls, plus your logs	Your tools' logs only
Detection	ML, behavior, rules, deception, intel: one data set	Per-tool alerts, rules you maintain
Validation	Automated before an incident; 5% false positives or less	Your analysts triage the queue
Response	Through your controls, one console, unlimited	A recommendation by email
Operated by	LMNTRIX Cyber Defense Centers 24×7, included	Your SOC, or a third party sold separately

QUESTIONS. CLEAR ANSWERS.

Do we have to replace what we have?

No. LMNTRIX runs behind your controls and contains through them. Most clients retire overlapping tools at renewal, once they see what was missed.

Where does our data live, and for how long?

In your own tenant of a certified cloud service, in-region where residency requires it, for the retention agreed per module.

WHAT WE NEED TO SCOPE IT

- Hosts, network throughput, identities, mailboxes and cloud accounts in scope
- Controls you want integrated for containment
- Data residency and retention requirements
- Service desk and collaboration tools

Priced per module on its own unit, MDR included. Start with one module and add others on the same data model; nothing to re-platform.

One platform behind every control. Operated for you, 24×7.

Every engagement starts with a free 30-day proof of concept on your real environment: sensors deployed, incidents worked, report delivered, 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.