LMNTRIX
BE THE HUNTER | NOT THE PREY

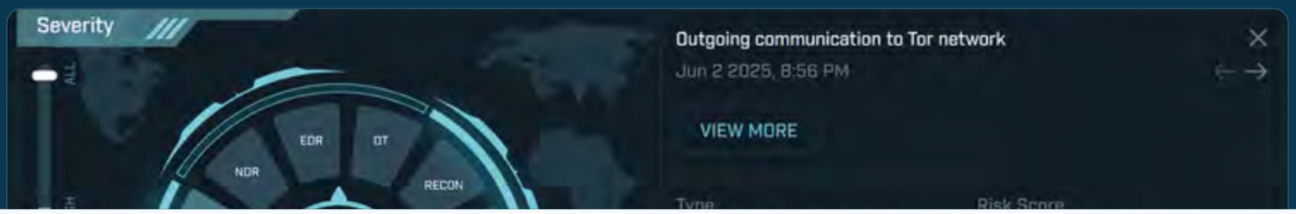
DATASHEET

THE CLOUD SECURITY MODULE OF LMNTRIX XDR

LMNTRIX Cloud

Secure every cloud. Eliminate every blind spot.

Posture management, runtime detection and response, entitlement management, continuous compliance and AI red teaming in one agentless XDR module for AWS, Azure, GCP and Kubernetes. Cloud telemetry lands beside your endpoint, identity, email and network signals, and the Cyber Defense Center investigates and contains what it finds, 24 hours a day.



A Cloud alert in the LMNTRIX XDR heads-up display. A workload talking to the Tor network, mapped to its MITRE tactic and scored.

1,100+
Posture checks across 11 cloud and SaaS platforms

200+
Runtime detection rules, plus machine-learning models

40+
Compliance frameworks, plus your own custom ones

Agentless: read-only API roles and your cloud's own audit logs. Nothing installed, nothing in the data path, about an hour to connect each cloud.

THE FIVE CAPABILITIES

Posture, identity and runtime defense in one module

01
Posture management
Misconfigurations, exposure and attack paths, found and ranked.

02
Detection & response
Runtime threats in your audit and flow logs, contained by the CDC.

03
Entitlement management
Granted versus used permissions, right-sized to least privilege.

04
Continuous compliance
40+ frameworks measured on demand, audit-ready reports exported.

05
AI red team
Attack paths and detections validated by safe, scoped simulation.

THE THREAT COVERAGE · THE MISCONFIGURATIONS AND PERMISSIONS ATTACKERS EXPLOIT

Exposure discovery
Public services, open ports, weak auth, unencrypted data.

Permission hardening
Excessive privileges, unused access, toxic combinations.

Runtime threat detection
Credential misuse, escalation, lateral movement, exfiltration.

Multi-cloud visibility
Accounts, regions, workloads and users in one XDR view.

Continuous compliance
Recognized standards measured, audit-ready reports.

Controlled remediation
Guided fixes, or automation under your conditions.

THE CAPABILITIES IN DEPTH

Posture, runtime and identity, in one data lake

The posture engine inventories and scores every cloud; the detection platform watches what happens inside it; both land in the same XDR data lake as your endpoints, identities and network, so no cloud finding is investigated alone.

01 · CLOUD SECURITY POSTURE MANAGEMENT

Breadth. 1,100+ checks across AWS, Azure, GCP, Kubernetes, Microsoft 365, GitHub and more, 11 platforms in one engine, plus infrastructure-as-code before it deploys.

Prioritization. Every finding carries a threat score, and attack paths are graphed from your inventory, so the exposure that actually reaches a crown jewel is fixed first.

Transparency. Every check is readable code mapped to its control, so an auditor can see exactly what was tested; custom checks cover your own standards.

02 · CLOUD DETECTION & RESPONSE

Sources. CloudTrail, Azure Activity, GCP Audit, VPC and NSG flow logs, Kubernetes audit and identity sign-ins, streamed in near real time.

Detection. 200+ rules built for these log sources, from simple correlations to machine-learning models, plus entity risk scoring that sequences behaviors into an attack storyline.

What it catches. Credential misuse, privilege escalation, persistence, lateral movement, data exfiltration and crypto-mining, mapped to MITRE ATT&CK.

03 · CLOUD INFRASTRUCTURE ENTITLEMENT MANAGEMENT

Granted versus used. The inventory of every permission on every user, role and service identity, compared with what each one actually exercised over time.

What it finds. Unused and excessive permissions, over-privileged identities, risky trust relationships and toxic combinations that add up to admin.

What you get. A right-sized least-privilege policy drafted for each identity, delivered as incidents in XDR, the same way across all three clouds.

04 · COMPLIANCE MONITORING & REPORTING

Frameworks. 40+ built in: CIS, NIST CSF and 800-53, ISO 27001, SOC 2, PCI DSS, HIPAA, GDPR, NIS2, FedRAMP and MITRE ATT&CK among them.

Yours too. Regional and sector standards, SAMA, NCA ECC, UAE IAS, Essential Eight and the ISM, are mapped as custom frameworks on request.

Reporting. On-demand reports by account, region and provider, with the failing controls and the fix, exported for the auditor.

05 · AI RED TEAM

Findings are theory. Exploitability is proof.

An AI red-team agent takes the attack paths the posture engine has mapped and attempts them, safely and within an agreed scope, in your own account: can this exposed role really reach that bucket, and does the detection fire when it does? Paths that prove exploitable become priority incidents; detections that stayed silent become new rules. It runs on the schedule you choose, so the score reflects what an attacker could do, not what a scanner noticed.

THE LIFECYCLE

Discover, prioritize, detect, remediate, prove

01
Discover
Every account, asset and identity inventoried by API.

02
Prioritize
Findings scored, paths graphed, exploitability tested.

03
Detect
Rules and ML on the logs, risk sequenced into storylines.

04
Remediate
Guided fixes, or automated under your conditions, by the CDC.

05
Prove
Compliance reports and incident evidence, on demand.

THE MDR SERVICE

A cloud finding becomes a validated, contained incident

LMNTRIX Cloud is a managed service, not a console. Every alert is validated by an intrusion analyst in the Cyber Defense Center before it becomes an incident, correlated with everything else XDR knows about the user and the workload, and contained under the runbooks you approve, 24 hours a day.

01
Detect
Posture findings, runtime rules and ML anomalies land in the kill box.

02
Validate
An analyst confirms it is real, and what the attacker can reach.

03
Contain
Key revoked, user disabled, workload isolated, bucket closed.

04
Harden
The misconfiguration and the permission that allowed it, fixed and tracked.

05
Prove
The incident, its evidence and the compliance delta, reported.

WHAT THE CYBER DEFENSE CENTER DOES

Tunes the detections. The 200+ rules and ML jobs are adjusted to your accounts and workloads, so real threats surface and noise does not.

Validates every alert. A false-positive assessment before anyone is paged; what reaches you is an incident with the identity, the asset, the blast radius and the evidence.

Correlates across XDR. A CloudTrail anomaly is tied to the same user's identity sign-in and endpoint process tree; a standalone cloud tool can never show that.

Contains in the cloud. Access keys revoked, users disabled, instances isolated, public access removed, under pre-agreed runbooks or with your approval.

Hardens on a cadence. Posture, entitlement and compliance findings arrive as prioritized incidents with the fix, and the CDC tracks them to closure.

Hunts in the raw logs. Full cloud audit and flow logs are retained in XDR for hunting and forensics, not just a vendor's verdict on them.



A compliance report in LMNTRIX XDR. Checks passed and failed, the failure pareto by control group, and the accounts dragging the score down, exported to PDF for the auditor.

WHAT YOU RECEIVE

Validated cloud incidents in XDR with the action taken; posture and entitlement findings as prioritized incidents; on-demand compliance reports; red-team validation results each cycle; and an analyst you can reach 24 hours a day.

THE DEPLOYMENT · AGENTLESS, ABOUT AN HOUR PER CLOUD

CLOUD	WHAT LMNTRIX COLLECTS	WHAT YOU GRANT
AWS	Configuration metadata; CloudTrail (with S3 data events) and VPC Flow logs from S3	A cross-account role with the Security Audit policy; read access to the log buckets
Azure	Subscription metadata, Activity and NSG flow logs, Entra users and roles	Reader on subscriptions, directory read on the tenant, blob reader on the log account
GCP	Project metadata and Cloud Audit logs via Pub/Sub	A viewer service account with a Pub/Sub subscription
Kubernetes	Cluster configuration and audit logs	A read-only service account per cluster
M365, GitHub	Tenant and organization security settings	A read-only app registration or token

THE SERVICE

Who does what

A subscription module of LMNTRIX XDR: you grant read-only access; LMNTRIX scans, watches, validates, contains and reports.

LMNTRIX PROVIDES

- Onboarding of every cloud, with a project manager
- Posture checks, detection rules and ML, tuned to your estate
- Entitlement analysis and least-privilege policy drafts
- Compliance frameworks, including custom and regional
- Scheduled AI red-team validation
- 24×7 validation, containment and 24-hour CDC access

YOU PROVIDE

- The LMNTRIX Cloud section of the starter pack
- Read-only roles and service accounts per the guides
- Audit and flow logging enabled on the accounts in scope
- Awareness of your cloud provider's logging fees
- Response runbooks: what we may contain, when to ask
- Remediation of posture findings, with our guidance

WHAT SETS IT APART

CAPABILITY	LMNTRIX CLOUD	A STANDALONE CLOUD TOOL
Scope	All five, in one module	One or two of these
Context	Correlated with endpoint, identity, network	Cloud only
Validation	Analyst-confirmed, exploitability tested	Raw findings, your triage
Data	Raw logs retained in LMNTRIX XDR, yours to hunt	Verdicts in a vendor SaaS
Frameworks	40+, plus custom and regional	A fixed list
Response	CDC contains in your cloud, 24×7	Alert handed to you

QUESTIONS. CLEAR ANSWERS.

Does it need agents or appliances?

No. Read-only API roles and your cloud's own audit logs; each cloud connects in about an hour.

Where does our cloud data go?

Into LMNTRIX XDR, hosted and operated by LMNTRIX, with retention set by your subscription. Nothing is modelled in a third party's platform.

WHAT WE NEED TO SCOPE IT

- Clouds, accounts, subscriptions and projects in scope
- Cloud asset footprint and daily log volume
- Compliance frameworks you report against
- Response authority: notify, confirm or auto-contain

Priced by cloud asset footprint and log volume, MDR included. First posture report within days.

Misconfigurations are the new perimeter. Close them first.

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