LMNTRIX
BE THE HUNTER | NOT THE PREY

DATASHEET

THE MOBILE THREAT DEFENSE MODULE OF LMNTRIX XDR

LMNTRIX Mobile

Your mobile workforce deserves real security.

Attackers see mobile as the weakest link. LMNTRIX Mobile is privacy-first mobile threat defense for iOS, Android and ChromeOS, built into LMNTRIX XDR: on-device machine learning stops phishing, malicious apps, rogue networks and device compromise where they happen, and the Cyber Defense Center validates and contains what it finds, 24 hours a day.



A mobile exploit in the LMNTRIX XDR heads-up display. An active OS exploit on an Android device, with the user, the device and the MITRE tactic already attached, beside every other module.

83%
Of organizations hit by mobile phishing

64%
Of zero-day exploits targeted iOS

45%
Suffered a mobile-related compromise

Industry figures cited in LMNTRIX mobile threat research. Yet most enterprises still treat mobile as an afterthought.

THE CORE CAPABILITIES

Protect the endpoint your security stack overlooks

Device security and compliance

- Jailbreaks, rooting, OS exploits, tampering
- Encryption, lock-screen and OS-version posture
- Quarantine or restrict devices that fall out of policy

Network and connection protection

- Rogue access points, MITM and SSL stripping
- DNS hijacking and unsafe Wi-Fi scored and blocked
- Policies by domain, address, country or certificate

Application threat defense

- Malware, spyware, banking trojans and rootkits
- Sideloaded apps, permission abuse, data harvesting
- Privacy and security ratings for every installed app

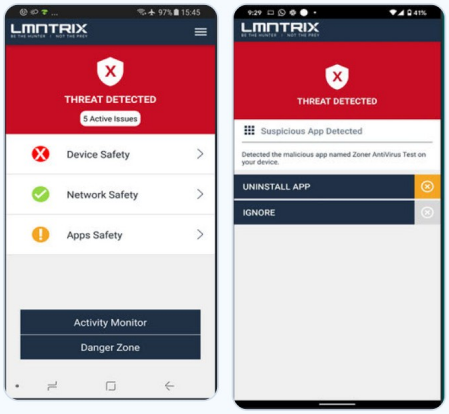
Phishing and content filtering

- Malicious links in SMS, apps, email and browsers
- Never-seen URLs caught on device, no feed required
- Web filtering across 75+ content categories

THE ENGINE

True on-device protection with machine learning

The detection engine runs on the phone itself and watches device, network, link and app behavior for deviations from normal. It needs no signatures, no cloud connection and no update to catch a threat it has never seen, so protection stays on in a lift, on a plane or on a hostile network.



On the device. A compromised device and a malicious app, each with the action the user can take on the spot.

Device threats

OS and kernel exploits, profile changes, system tampering, USB and SD-card attacks, smart-tag tracking, unpatched operating systems.

Network threats

Rogue access points, man-in-the-middle, SSL stripping and DNS hijacking, found from device behavior and traffic on Wi-Fi, cellular and Bluetooth.

Malicious apps

Spyware, ransomware, banking trojans, rootkits and adware, known or never seen, from app and device behavior rather than a signature.

Phishing and content

Links tapped in SMS, chat, email or a browser classified on the device by seven phishing classifiers, with no reliance on known-URL feeds.

WHAT THE USER SEES

A plain alert, the fix in one tap, and a response already applied by policy: the app uninstalled, the Wi-Fi blocked, corporate access held until the device is clean.

THE POLICY AND THE PRIVACY

Enforced by device group, private by design

POLICY SETS, PER DEVICE GROUP

Threats. On-device alerting, automated response and notification for 100+ device-based threat types.

Phishing. Link protection, custom filtering and web-category handling across 75+ categories.

Apps. Alerting by app ID, version or developer signature; ML malware detection on or off.

Network. Allowed Wi-Fi networks and certificates; sinkhole addresses, domains or whole countries.

Compliance. OS-risk thresholds, encryption, lock screen, and device or app inactivity.

PRIVACY, FOR BYOD AND GDPR

No content. The engine never reads messages, mail, photos or browsing; it reads behavior.

Your controls. Collection of location, network details such as SSID, app inventory and browser data can each be switched off per group.

Personal stays personal. On a BYO device, the corporate policy governs corporate access; the employee's own data is never inventoried.

Offline and on-device. Detection does not depend on sending traffic to a cloud for inspection.

Zero-day, by design

In testing, months-old exploits and simple jailbreaks were caught as zero-days with no engine update.

Phishing without a feed

Clients report efficacy above 90% on never-seen URLs they have tested against the on-device classifiers.

App vetting, not just malware

Every app rated for privacy and security, with executive and technical reports, not only a malware verdict.

THE MDR SERVICE

Detected on the phone, validated and contained by the CDC

LMNTRIX Mobile is delivered as a managed service, not a console. Every detection flows into LMNTRIX XDR, where the Cyber Defense Center validates it against everything else happening on your estate, contains the ones that matter and tells you what to fix, 24 hours a day.

01
Enroll
Zero-touch through your UEM, or the app and a QR code for BYOD.

02
Assess
Device attestation and a risk score before corporate access is granted.

03
Detect
On-device machine learning fires; the user and the CDC are told at once.

04
Correlate
XDR ties the mobile event to the user's endpoint, identity, email and cloud activity.

05
Respond
Analyst-validated containment, then remediation guidance with the evidence.

WHAT THE CYBER DEFENSE CENTER DOES

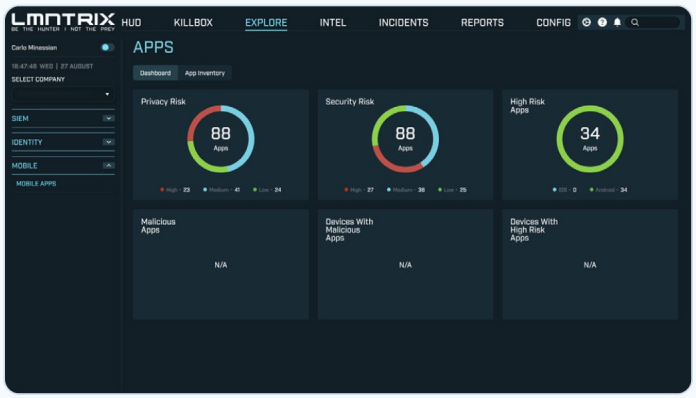
Validates every alert. A mobile detection is treated as a lead, not a verdict: analysts confirm it before it reaches you, so you never chase a false positive.

Investigates in context. The same phone's user is checked across LMNTRIX EDR, NDR, Identity, Email and Cloud; a phishing tap on mobile is read next to the login that followed it.

Contains. Isolation, notification or lockdown on the device, and conditional access through your UEM so a risky device loses corporate access until it is clean.

Hunts and reports. Device, network-connection and app forensics for threat hunting and IR; executive and technical reporting on mobile risk.

Tunes. Policy sets adjusted to your device groups and your tolerance, so alerts stay meaningful as the fleet changes.



Mobile apps in LMNTRIX XDR. Every app on the fleet scored for privacy and security risk, with the high-risk ones and the devices carrying them one click away, in the same console as the rest of your estate.

WHY MANAGED MATTERS ON MOBILE

A phone is the one endpoint your SOC cannot image, log into or pull a memory dump from. The CDC already holds the device, network and app forensics, so the investigation is finished, not started, when it reaches you.

THE DEPLOYMENT

Platforms	iOS, Android and ChromeOS, corporate-owned or BYOD.
Managed devices	Zero-touch provisioning through your MDM, EMM or UEM: Workspace ONE, Intune, MaaS360, MobileIron and others. The app activates without the user opening it.
Unmanaged devices	The user installs the LMNTRIX Mobile app and scans a QR code; no MDM needed.
Hosting	Cloud SaaS, hosted and operated by LMNTRIX; nothing to build or maintain on your side.
Integration	Single console with shared workflows for alerts, devices and app inventory; conditional access in your UEM driven by the live risk score, for Zero Trust.

THE SERVICE

Who does what

A subscription of LMNTRIX XDR, priced per device: you enroll the fleet, LMNTRIX runs the policy, the platform and the monitoring.

LMNTRIX PROVIDES

- The licensed service and everything needed to enroll devices
- Mobile security policy configuration and MDM integration help
- Validation of every mobile alert before it reaches you
- Containment, remediation guidance and forensics
- Policy tuning as the fleet and the threats change
- 24-hour access to the Cyber Defense Center

YOU PROVIDE

- The LMNTRIX Mobile section of the starter pack
- Details of the mobile endpoints and their users
- Integration with your MDM or UEM, where you have one
- Enrollment of the devices, managed or BYOD
- Your device groups and the policy each should get
- Who receives alerts, and on which channels

WHAT SETS IT APART

CAPABILITY	LMNTRIX MOBILE	STANDALONE MTD
Part of an XDR	Native; one incident across all telemetry	Separate console, manual correlation
Response	CDC-validated and contained, 24×7	Alerts; response is yours
Phishing	On-device classifiers, no URL feed	Known-URL feeds and databases
Offline	Full detection with no connectivity	Cloud lookups required
App vetting	Privacy and security ratings, reports	Malware verdict only
Privacy	No user content; per-group collection controls	Varies by product

QUESTIONS. CLEAR ANSWERS.

Can LMNTRIX read my employees' messages?

No. The engine never collects user content or messages; it analyzes behavior, and location, SSID and app-inventory collection can each be switched off.

Do I need an MDM?

No. BYOD users enroll with the app and a QR code. An MDM adds zero-touch rollout and conditional access, so a risky device loses corporate access automatically.

WHAT WE NEED TO SCOPE IT

- Number of iOS, Android and ChromeOS devices
- Corporate-owned versus BYOD, and the MDM in use
- Device groups and the policy each should carry
- Alert channels and escalation contacts

Priced per device, MDR included. Managed fleets are protected the day the UEM pushes the app.

Secure the last mile of XDR.

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