LMNTRIX
BE THE HUNTER | NOT THE PREY

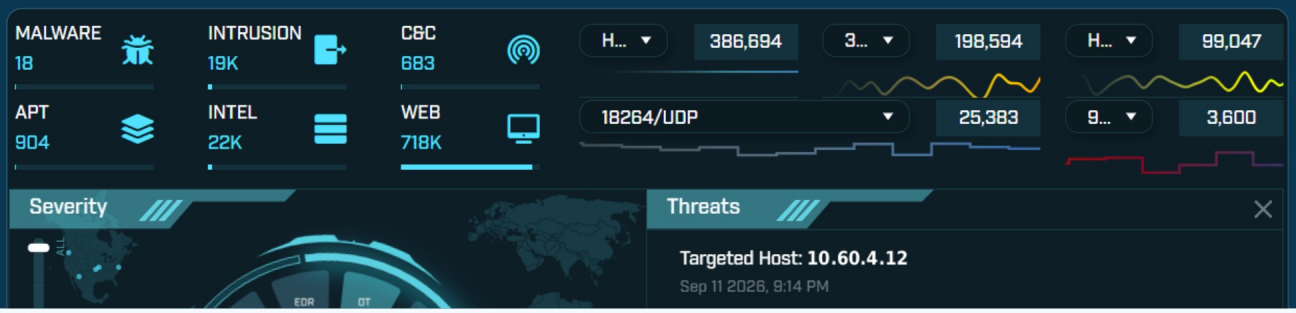
DATASHEET

THE EMAIL AND COLLABORATION SECURITY MODULE OF LMNTRIX XDR

LMNTRIX Email

Most email security stops at filtering. We stop the attack.

Email is still the front door for phishing, credential theft, ransomware, business email compromise and data loss. LMNTRIX treats it as one telemetry source inside a wider detection and response practice: automated prevention across the full lifecycle and, with the MDR uplift, every suspicious message correlated against endpoint, identity, network and cloud by the Cyber Defense Center.



The LMNTRIX XDR heads-up display. With MDR, email detections land beside endpoint, network, identity and cloud, so a phishing click is read next to the login that followed it.

<30 min
To connect Microsoft 365 or Google Workspace

0
Gateways, proxies, appliances or agents

10 yrs
Searchable archive, as an optional uplift

THE CORE CAPABILITIES

One prevention stack for email and collaboration

Phishing and impersonation protection

- Credential harvesting, lookalike domains
- Content, reputation, behavior and URL signals
- Click-time protection on every link

Malware, sandboxing and zero-day prevention

- Unknown files detonated in isolation
- Standard in every package, mail and shared files
- Zero-day threats caught before delivery

Attachment sanitization (CDR)

- Active and exploitable content stripped out
- Clean files reconstructed, delivered without delay
- Weaponized documents neutralized before opening

Account takeover protection

- Login behavior, sending anomalies, mailbox rules
- Suspicious internal messages flagged
- Compromised accounts caught before fraud

THE COVERAGE

Inbound, outbound, internal, post-delivery, and the collaboration layer

A gateway sees mail once, on the way in. LMNTRIX sits inside the mail platform by API, so it also sees internal and outbound mail, messages already delivered, and the files and chats beside email.

Data Loss Prevention

Identifies PII, financial, regulated and confidential content and applies policy to stop leakage across email and collaboration. Included in Complete Protect.

Collaboration security

Extends protection into cloud storage and chat (Teams, Slack, OneDrive, SharePoint, Google Workspace, Box, Dropbox, ShareFile): malicious files, risky sharing, sensitive-data exposure.

THE TWO TIERS

Same prevention engine; the only difference is DLP

ADVANCED PROTECT

The complete prevention stack: anti-phishing, account-takeover prevention, malicious-URL and click-time protection, anti-virus, sandboxing and CDR. For organizations whose priority is stopping inbound and internal threats.

COMPLETE PROTECT

Everything in Advanced Protect, plus Data Loss Prevention: PII, financial, regulated and confidential content identified and controlled. Choose it where outbound data control and compliance are in scope.

THE PACKAGES

Email Only, or Email and Collaboration, in either tier

CAPABILITY	ADVANCED	COMPLETE
PROTECTED APPLICATIONS		
Email Only: Microsoft 365 (Outlook) and Gmail	✓	✓
Email and Collaboration: adds Teams, Slack, Google Workspace, OneDrive, SharePoint, Box, Dropbox, ShareFile	✓	✓
THREAT PREVENTION, INCLUDED IN BOTH TIERS		
Anti-phishing for inbound and internal email · known-malware prevention · malicious-URL prevention and click-time URL rewriting	✓	✓
Account takeover prevention (anomaly detection) · shadow IT and unauthorized application detection	✓	✓
Zero-day malware prevention (sandboxing) · attachment sanitization (CDR / threat extraction)	✓	✓
DATA PROTECTION, WHERE THE TIERS DIFFER		
Data Loss Prevention (DLP)	–	✓
OPTIONAL UPLIFTS, EITHER TIER		
MDR operated by the Cyber Defense Center · archiving up to 10 years · DMARC management · security awareness training	Optional	Optional

THE MDR UPLIFT

Where email stops being a silo

The MDR uplift hands day-to-day email security operations to the Cyber Defense Center. Analysts correlate email with endpoint, identity, network and cloud telemetry, so an attack that would look like an isolated email event is caught as the campaign it belongs to.

MDR CAPABILITY	WHAT YOU GET
Release requests	Legitimate releases reviewed and processed safely by analysts
Quarantine explanations	Users and admins told exactly why a message was held
Allow-listing	Controlled sender and domain allow-lists that limit disruption and risk
Suspicious-email triage	User-reported messages investigated by security analysts
Incident and outbreak management	Confirmed threats contained; campaigns across many users get rapid response
Threat hunting	Related indicators hunted across email and every other telemetry source
Detection improvement	New detection logic built from emerging threats and user submissions
Cross-technology correlation	Email threats read beside endpoint, network, identity and cloud alerts
Continuous tuning	Policies, detections and response workflows refined over time

WHY ADD MDR

It turns a powerful platform into a fully operated email defense service: release, allow-listing and triage workload off your team, faster and better investigations, and email connected to the wider security picture.

WHAT A CAMPAIGN LOOKS LIKE

A credential-phishing email reaches twelve users. Three click. One logs in from a new country ten minutes later and creates a forwarding rule. Alone, that is three alerts in three consoles. In LMNTRIX XDR it is one incident, contained by the CDC: the message pulled from every mailbox, the session revoked, the rule removed, the user told.

THE OTHER UPLIFTS

Retention, authentication and the human layer

ARCHIVING

Long-term retention for up to 10 years, for compliance, governance, legal discovery and continuity.

- Fast search and retrieval of historical mail
- Tamper-resistant retention by policy
- Controlled user and administrator access

For: regulated industries, professional services, government, healthcare, finance, education.

DMARC MANAGEMENT

Protects your domains from spoofing and unauthorized use across SPF, DKIM and DMARC.

- Visibility of who sends as your domains
- Staged policy path: monitor, quarantine, reject
- Third-party senders (CRM, finance, marketing) validated

Result: impersonating your business becomes materially harder.

AWARENESS TRAINING

Reduces human risk: phishing, social engineering, credential theft, unsafe attachments and BEC.

- Realistic phishing simulations
- Training modules and targeted coaching for repeat clickers
- Ongoing campaigns, not one-off sessions

Result: users recognize and report suspicious mail faster.

THE SERVICE

Choosing the right package

Self-manage the platform, or add MDR and the other uplifts as your needs grow. The choice, and the control, stay with you.

YOU NEED	WE RECOMMEND
Full phishing and threat protection for Microsoft 365 or Gmail	**Email Only, Advanced Protect**
Email-only protection plus outbound data control	**Email Only, Complete Protect**
Threat protection across email, chat and cloud file sharing	**Email and Collaboration, Advanced Protect**
Email and collaboration protection plus DLP	**Email and Collaboration, Complete Protect**
LMNTRIX to operate, investigate and respond for you	**Add MDR**
Long-term retention and legal discovery	**Add Archiving**
Your domains protected from spoofing and impersonation	**Add DMARC Management**
Fewer users falling for phishing	**Add Security Awareness Training**

WHAT SETS IT APART

Platform plus expert operations

Self-manage, or add MDR for a service run end to end by the Cyber Defense Center.

Protection beyond the inbox

Email attacks end in endpoint compromise and identity abuse. With MDR, email is correlated with that telemetry, so the campaign is seen whole.

Reduced operational burden

Releases, allow-listing, suspicious-mail reviews and user questions are constant work. MDR takes it off your team.

Built for modern cloud work

Files, messages, links, users and sensitive data protected across email, cloud storage, chat and SaaS.

QUESTIONS. CLEAR ANSWERS.

Do I change my MX records or add a gateway?

No. LMNTRIX connects to Microsoft 365 or Google Workspace by API in under 30 minutes; nothing sits in the mail path.

Is sandboxing an extra?

No. Sandboxing, zero-day prevention and CDR are standard in every package; only DLP separates the tiers.

WHAT WE NEED TO SCOPE IT

- Number of mailboxes, and Microsoft 365 or Google Workspace
- Collaboration apps in scope, if any
- Whether outbound data control (DLP) is required
- Which uplifts: MDR, archiving, DMARC, awareness training

Priced per mailbox by package and tier; uplifts added to either. Live the day the API connection is approved.

Email is the front door. Guard it.

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