LMNTRIX
BE THE HUNTER | NOT THE PREY

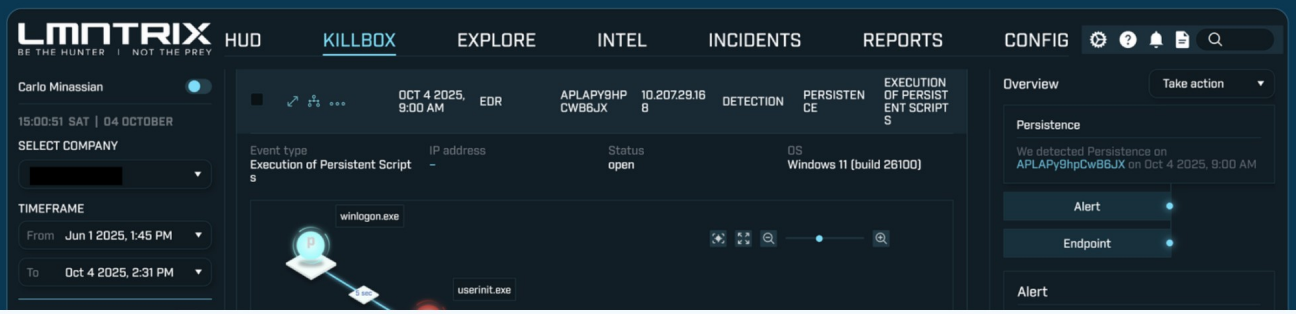
DATASHEET

THE ENDPOINT SECURITY MODULE OF LMNTRIX XDR

LMNTRIX Endpoint Security

Stop threats at the endpoint. Detect faster. Respond smarter.

Ransomware, credential theft, living-off-the-land attacks: one missed alert can become a breach. LMNTRIX Endpoint Security is a lightweight agent for Windows, macOS and Linux that prevents at the point of execution, records everything that happens on the device, and hands LMNTRIX Cyber Defense Centers what they need to contain an attack in minutes, online or offline.



Killbox, the LMNTRIX XDR incident view. A persistence attempt on a Windows 11 host reconstructed as a process tree, mapped to ATT&CK T1064, T1060 and T1053, with the endpoint and the response actions one click away.

<1 min
Detect. Autonomous prevention and detection on the agent, in milliseconds.

<5 min
Investigate. The CDC validates the breach and takes action on your behalf.

<30 min
Remediate. Who, what, when and how, with containment built into the XDR.

Every second counts: the LMNTRIX endpoint service targets, from first signal. Source: LMNTRIX XDR for Endpoint Security, 2026.

THE DETECTION ENGINES

Four cascading engines in one agent

Next-generation antivirus and endpoint detection and response, with no signature database to update and no daily disk scan. Each engine catches what the one before it lets through.

01
Reputation
Real-time verdicts from global threat intelligence on files and downloads, before anything else runs.

02
Static AI
Every file scored by an on-agent machine-learning model as it is written or executed, and quarantined before it runs. Replaces signature antivirus.

03
Behavioral AI
Running processes judged by what they do: fileless attacks, exploits, macros, scripts, cryptominers, ransomware.

04
Active EDR
Every process, file, registry change and connection recorded and linked, so the whole story is there when it matters.

THE PREVENTION

Block what's bad. Contain what's suspicious.

Layers of prevention on the agent itself: some act before a file ever runs, most watch everything that happens after, so a threat that slips one layer meets the next.

PRE-EXECUTION PREVENTION

Malware prevention

On-agent machine learning scores every file as it is written or executed and quarantines it before it runs. No signature database, no daily scan.

Reputation service

Real-time verdicts from global threat intelligence catch low-reputation and known-bad binaries the moment they are downloaded.

Blocklist and trusted applications

Policy-level control of what may run: block named applications outright, trust the ones your business depends on.

POST-EXECUTION PROTECTION

Memory threat protection

Shellcode and process injection, and other in-memory techniques that leave no file behind, stopped as the thread is created.

Ransomware behavioral prevention

Low-level process behavior plus canary files planted where ransomware strikes first; the offending process is killed and Windows hosts self-heal with rollback.

Malicious behavior protection

Adversary tradecraft caught by what a process does, including macros, scripts and living-off-the-land binaries, mapped across the MITRE ATT&CK matrix.

Credential hardening

Over-permissive access to the Windows credential store (LSASS) removed, so dumped credentials stop being the attacker's next step.

Device control

USB storage on Windows and macOS set to allow, read-only, block-execute or block, with trusted-device exceptions and a connection dashboard.

Tamper protection

The agent runs with kernel-level visibility and protects itself; it cannot be stopped or uninstalled without authorization.

Registered antivirus

Registers with Windows Security Center as the host antivirus, so compliance checks and conditional access see it as such.

THE DIFFERENCE

Endpoints are your front line

INCIDENT RESPONSE WITHOUT LMNTRIX ENDPOINT SECURITY

Attack occurs	Day 1	Day 2	Day 3–4	Day 5–8	Day 9+
Undetermined dwell time	Help desk ticket: a user notices something odd	Incident ticket raised, device shipped or collected	Manual forensic analysis of one machine	Other affected machines found, one at a time	Manual report; full extent of breach still unknown

WITH LMNTRIX ENDPOINT SECURITY

Minutes

Attack occurs	Milliseconds	Seconds	Minutes	Minutes	Same day
Dwell time near zero	Agent blocks the technique and records the chain	XDR correlates the alerts into one incident	CDC validates, isolates and hunts every endpoint	Forensic evidence and rollback across all affected hosts	Detailed report; full extent of breach known

Correlated alerts, one incident

Related detections across hosts are stitched into a single incident with its root cause, not left as a queue of raw alerts.

Built-in ATT&CK mapping

Every detection carries its tactic and technique IDs, so triage starts from what the attacker is doing.

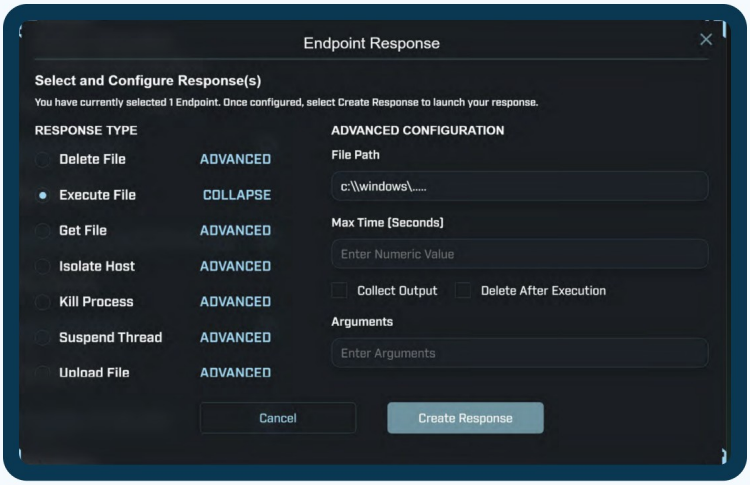
Zero-day coverage by behavior

Techniques are caught by how they act, so a never-seen sample meets the same wall as a known one.

THE RESPONSE

From alert to action in minutes

Built-in response, not an add-on. Automated where it is safe, analyst-driven where it matters, with a manual override for your team at every step.



Endpoint Response. Select one or many endpoints, choose the action, add arguments and a time limit, and launch. Every action is logged against the incident.

RESPONSE ACTIONS

Isolate and release	One click. The device is cut from the network while the LMNTRIX channel stays open; release it when the host is clean.
Kill, suspend, scan	List running processes, terminate or suspend by PID or entity ID, quarantine files, and scan any path on demand.
Memory dump	Capture a process, kernel or full physical-memory dump for forensics: in-memory malware, injected payloads, credentials.
Live Response console	Get and upload files, run commands and scripts from a managed script library, with every command and its output recorded.
Playbooks and rollback	Prebuilt remediation playbooks, self-healing rollback on Windows, and manual override at every step.
Offline hosts	Actions queue for a host that is off the network and run the moment it reconnects. Identity and cloud actions follow from the same incident.

THE VISIBILITY

Hunting and forensics, included

90 days of telemetry

Rich endpoint telemetry retained and searchable, so a hunt can go back to the first sign of a campaign.

Saved hunts and queries

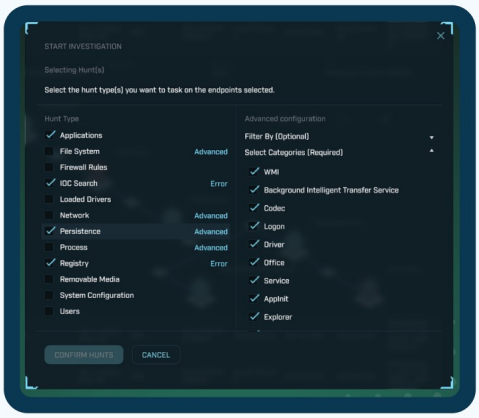
Recurring hunts saved and scheduled; IOC and Sigma-style queries across the whole estate from one indicator.

What the agent records

Process, file, network, DNS, registry, DLL and driver load, API and security events; full session view with terminal output on Linux.

Unlimited DFIR, no extra cost

Automated and manual artifact collection, auto-parsing, and live telemetry combined into one picture by the Cyber Defense Center.



Start Investigation. Twelve hunt types, from IOC search to persistence and loaded drivers; pick the endpoints, confirm.

THE SPECIFICATIONS

A lightweight agent, a cloud console, no VPN

WINDOWS

Workstation
Windows 10 · Windows 11

Server
2012 R2 · 2016 · 2019 · 2022 · 2025

x64, standard desktop and server editions, including Server Core. Physical, virtual and VDI.

LINUX

RHEL 7, 8, 9, 10 · CentOS Stream 8, 9
Ubuntu 18.04, 20.04, 22.04, 24.04
Debian 10, 11, 12, 13 · SLES 15
Oracle Linux 8, 9 · AlmaLinux 9 · Rocky 9, 10
Amazon Linux 2, 2023

x64 everywhere; ARM64 (kernel 5.4+, Graviton included) on RHEL, Ubuntu, Debian, SLES, Rocky 10 and Amazon Linux.

MACOS

macOS 13 Ventura · 14 Sonoma
macOS 15 Sequoia · 26 Tahoe

Intel and Apple silicon. Silent deployment through MDM with pre-approved system extension and full-disk access.

Support follows each OS vendor's lifecycle; a version is retired six months after vendor support ends.

<2%
Average CPU usage

500 MB
Resident memory, maximum

1 GB
Disk, including local logs and event store

0
Reboots. Deploys in minutes, no end-user impact

Console	LMNTRIX XDR, cloud-hosted SaaS. Managed and monitored by LMNTRIX Cyber Defense Centers.
Connectivity	Agent connects to LMNTRIX XDR over TLS from anywhere; no VPN for home or remote users. Isolation keeps that channel open.
Proxy	Proxy-aware agent pack for networks without direct Internet access; unauthenticated proxies, with SSL inspection bypassed for agent traffic.
Offline	Prevention and recording run locally. Protection continues without a connection; events sync and queued response actions run on reconnect.
Scale	Proven in estates of more than 200,000 endpoints.

Replaces	Legacy antivirus, next-generation antivirus and standalone EDR. Runs alongside an existing AV during transition if you prefer.
Protection updates	Malware models, behavioral rules and other protection artifacts update automatically from LMNTRIX, or on a schedule you set; nothing for you to train.
Policy	Per-group policies with detect or prevent per layer, trusted applications and devices, event filters, isolation exceptions and blocklists; agents started, stopped, updated or removed remotely.
Deployment	Guided Onboarding; gradual rollout through your software distribution, two to eight weeks depending on size.
Not included	File integrity monitoring and DLP, which LMNTRIX integrates with rather than duplicates.

TECHNOLOGY + PEOPLE = OUTCOMES

24×7 monitoring and hunting

LMNTRIX analysts validate every breach, hunt across your estate and guide remediation. No large security team needed on your side.

Reports that stand up

Post-incident reports, monthly service reports, on-demand reports by field, OS or application, and an annual business review for executives.

Cut risk. Prove it.

Faster MTTD and MTTR, fewer false positives, and audit-ready ATT&CK coverage reporting. Customers report 12× faster investigation and 98% less alert volume.

Prove it in 30 days.