LMNTRIX
BE THE HUNTER | NOT THE PREY

Will it work with what we have?

Yes. LMNTRIX XDR ingests from the security stack you already run and contains through it.

600+ pre-built integrations: 400+ IT, cloud and security sources, 215 ICS/OT protocols, and any source that speaks syslog, CEF or JSON. Every entry is a telemetry source correlated in LMNTRIX XDR. Entries carrying a response badge are also enforcement points: the Cyber Defense Center pushes the action into that control by API, from the LMNTRIX console, with no login to your tool.

RESPONSE BADGES

▲ BLOCK IOC	IP, domain, URL or hash blocked at the control
▲ ISOLATE	Host isolated from the network
▲ QUARANTINE	Message removed from mailboxes, sender blocked
▲ DISABLE	Account disabled, sessions revoked
▲ 2-WAY	Incidents created and updated in your tool

ENDPOINT & EDR

Ingest: process, file, registry, network and authentication events, EDR detections · Native: LMNTRIX EDR (Windows, macOS, Linux)

Microsoft Defender for Endpoint ▲ ISOLATE	CrowdStrike Falcon ▲ ISOLATE	Microsoft 365 Defender
SentinelOne ▲ ISOLATE	SentinelOne Cloud Funnel	Palo Alto Cortex XDR
VMware Carbon Black EDR	VMware Carbon Black Cloud	Cisco Secure Endpoint
Sophos Central	Trellix EDR Cloud	Trellix ePO
Trend Micro Deep Security	Trend Vision One	Fortinet FortiEDR
Fortinet FortiClient	Symantec Endpoint Protection	ESET Protect
Bitdefender	Tanium	Jamf Protect
Google Santa (macOS)	Sysmon (Windows and Linux)	Osquery
Windows event logs	PowerShell logging	Linux auditd, systemd journal

FIREWALLS, WAF & NETWORK SECURITY

Ingest: traffic, threat and policy logs · Response: IOC pushed to the block list by API

Palo Alto Networks ▲ BLOCK IOC	Fortinet FortiGate ▲ BLOCK IOC	Check Point ▲ BLOCK IOC
Cisco ASA / Firepower ▲ BLOCK IOC	Cisco Meraki ▲ BLOCK IOC	Juniper SRX ▲ BLOCK IOC
AWS Network Firewall ▲ BLOCK IOC	Azure Firewall ▲ BLOCK IOC	Google Cloud Firewall ▲ BLOCK IOC
SonicWall	Sophos XG Firewall / UTM	Barracuda CloudGen Firewall
Arista Firewall	pfSense	Fortinet FortiManager ▲ BLOCK IOC
iptables ▲ BLOCK IOC	AWS WAF ▲ BLOCK IOC	Azure WAF / Front Door ▲ BLOCK IOC
Imperva WAF / Cloud WAF ▲ BLOCK IOC	Barracuda WAF	Citrix WAF
Cloudflare ▲ BLOCK IOC	Akamai	F5 BIG-IP / APM
ModSecurity	Radware DefensePro	Zero Networks
AWS / Azure / GCP VPC flow logs		

NDR SENSORS & NETWORK TELEMETRY

Ingest: detections, flow and packet metadata, switch and wireless logs · Native: LMNTRIX NDR and Packets sensors

Darktrace	Vectra Detect	FireEye Network Security
Zeek	Suricata	Snort
NetFlow / IPFIX	Network packet capture	Cisco IOS, Nexus, Aironet
Cisco ISE	SNMP (v1, v2, v3)	Syslog (any device)

WEB, DNS & SASE

Ingest: web, proxy and DNS logs · Response: domain or URL added to the block policy by API

Zscaler Internet Access ▲ BLOCK IOC	Netskope ▲ BLOCK IOC	Cisco Umbrella ▲ BLOCK IOC
Infoblox BloxOne DDI / NIOS ▲ BLOCK IOC	Zscaler Private Access	Forcepoint Web Security
Menlo Security	Google Cloud DNS	Cloudflare (DNS and proxy) ▲ BLOCK IOC

EMAIL & COLLABORATION

Ingest: message trace, threat verdicts, file and chat activity · Response: message pulled from mailboxes, sender blocked · Native: LMNTRIX Email

Exchange Online (Microsoft 365) ▲ QUARANTINE	Mimecast ▲ QUARANTINE	Proofpoint TAP ▲ QUARANTINE
Microsoft Exchange Server	Exchange Message Trace	Cisco Secure Email Gateway
Fortinet FortiMail	Gmail / Google Workspace	Microsoft Teams
Slack	SharePoint Online / Server	OneDrive
Google Drive	Box	Dropbox, Confluence, GitHub

IDENTITY & ACCESS

Ingest: sign-ins, directory changes, privilege use, MFA and vault events · Response: account disabled and sessions revoked by API · Native: LMNTRIX Identity

Microsoft Entra ID ▲ DISABLE	Active Directory (via Windows event logs)	Okta
Cisco Duo	Ping Identity PingOne	ForgeRock
Keycloak	JumpCloud	Cisco ISE
CyberArk PAS / PTA	Thycotic Secret Server	HashiCorp Vault
1Password, Bitwarden, LastPass	LDAP / LDAPS, Kerberos, RADIUS	Google Workspace audit

CLOUD PLATFORMS & SAAS POSTURE

Ingest: control-plane audit, native threat findings, posture, workload and network logs · Response: cloud firewall block by API · Native: LMNTRIX Cloud

AWS CloudTrail	Amazon GuardDuty	AWS Security Hub, Inspector
AWS Network Firewall ▲ BLOCK IOC	AWS: EC2, ECS, Lambda, S3, RDS +15 services	Azure Activity and Audit Logs
Azure Event Hub	Microsoft Defender for Cloud	Azure Firewall ▲ BLOCK IOC
Azure: VM, App Service, Functions +12	Google Cloud Audit	Google Security Command Center
Google Cloud Firewall ▲ BLOCK IOC	GCP: GKE, Compute, VPC, DNS +10	Microsoft 365 audit
Wiz	Palo Alto Prisma Cloud	Kubernetes, containers (17)

SIEM, LOG & TELEMETRY SOURCES

Ingest: any log via agent, collector or API; retained in LMNTRIX SIEM · Alerts forwarded to your SIEM by syslog, CEF or API · Native: LMNTRIX SIEM

Syslog, CEF, JSON, generic log files	Webhook / HTTP endpoint	Cribl
Windows, custom Windows channels	Linux, System Audit	File Integrity Monitoring
NGINX, Apache, Tomcat, HAProxy	SQL Server, MySQL, Oracle, DB2 +10	Observability sources (194)

THREAT INTELLIGENCE

Ingest: IOC feeds matched to your telemetry · Native: 300+ sources in LMNTRIX Intelligence

Recorded Future	Mandiant Advantage
CrowdStrike Falcon Intelligence	Anomali ThreatStream
ThreatConnect	ThreatQuotient
EclecticIQ	OpenCTI, MISP
Rapid7 Threat Command	Cybersixgill
ESET Threat Intelligence	ZeroFox
AlienVault OTX, Abuse.ch	Maltiverse, CIF

VULNERABILITY & EXPOSURE

Ingest: findings for prioritization · Native: LMNTRIX Validate, Recon

Qualys VMDR	Tenable VM / Security Center
Rapid7 InsightVM	AWS Inspector
Microsoft Defender for Cloud	Wiz, Snyk
CISA Known Exploited Vulns	Tenable Security Center

TICKETING, NOTIFICATION & SOAR

Response: incidents opened, updated and closed in your tools

ServiceNow ITSM / ... ▲ 2-WAY	Jira Cloud / Server /... ▲ 2-WAY
Slack, Microsoft Te... ▲ 2-WAY	PagerDuty, OpsGe... ▲ 2-WAY
Email, Webhook ▲ 2-WAY	Swimlane SOAR ▲ 2-WAY
Tines, Torq ▲ 2-WAY	IBM Resilient ▲ 2-WAY

ICS / OT & IOT · 215 PROTOCOLS AND VENDORS

Passive, deep-packet inspection by the LMNTRIX ICS/OT sensor; no agents on controllers, no downtime · Native: LMNTRIX ICS/OT

Modbus TCP / RTU, Schneider Unity	OPC UA / HDA / Classic	DNP3, IEC 60870-5-101/104	IEC 61850, GOOSE, Sampled Values
Siemens S7, S7 Plus, Sinec H1	Rockwell EtherNet/IP, CIP Security	PROFINET DCP, EtherCAT, Sercos III	BACnet IP / Ethernet
ABB 800xA, Emerson DeltaV, Ovation	Honeywell, Yokogawa, Valmet	Mitsubishi MELSEC, Omron FINS	DICOM, HL7, IntelliVue (IoMT)
+200 more at lmntrix.com/explore-i...			

Not on the list? Ask.

Anything that emits syslog, CEF or JSON, or has an API, can be onboarded. Coverage is confirmed in your environment during the free 30-day POV.

START A FREE 30-DAY POV

sales@lmntrix.com

© 2026 LMNTRIX. All rights reserved. Product names are trademarks of their respective owners.