vehere

DATASHEET

Battle-tested Network Detection and Response

- Built for Combat
- Engineered for Scale
- On-premises by design

Petabyte-scale, AI-powered NDR that's trusted by the world's most demanding cybersecurity teams

Modern cyber-attacks are stealthy, persistent and built to evade traditional defenses. Threat actors abuse legitimate credentials, encrypted channels and trusted protocols to blend into normal activity, often remaining undetected for weeks to months. Traditional tools like EDR rely on agents and logs - visibility that can be disabled, bypassed or simply never generated.

The network, however, cannot be bypassed or tampered with. Every command, lateral movement and byte of exfiltrated data must traverse it. Real time network analysis provides an independent security control that attackers cannot silence or evade.

Vehere NDR, originally built for national-scale cyber operations, delivers to enterprises the same high-performance platform and advanced security capabilities battle-tested in mission-critical environments. Engineered for true terabit throughput and petabyte-scale data volumes, it performs complete packet inspection at line rate. It decodes thousands of protocols and correlates millions of indicators of compromise in real time, across encrypted, east-west, north-south and hybrid traffic.

Unlike "event-based" NDR solutions, Vehere NDR delivers full, continuous capture, enabling precise threat reconstruction and powerful retrospective analysis for deep investigations.

Powered by Vehere Vision AI, a fully on-premises intelligence fabric that unifies LLMs, supervised and unsupervised learning, enabling security analysts to respond to threats with speed, precision and confidence.

Widest Threat Coverage

5000+
Protocols

2 mil+
IoCs

35000
IDS signatures

AI/ML

Multi-agent AI
Autonomous Correlation

Behavioral
Anomaly Detection

Proven Scale and Performance

500,000
Hosts

Petabyte
Scale Data Lake

Terabit
Processing Throughput

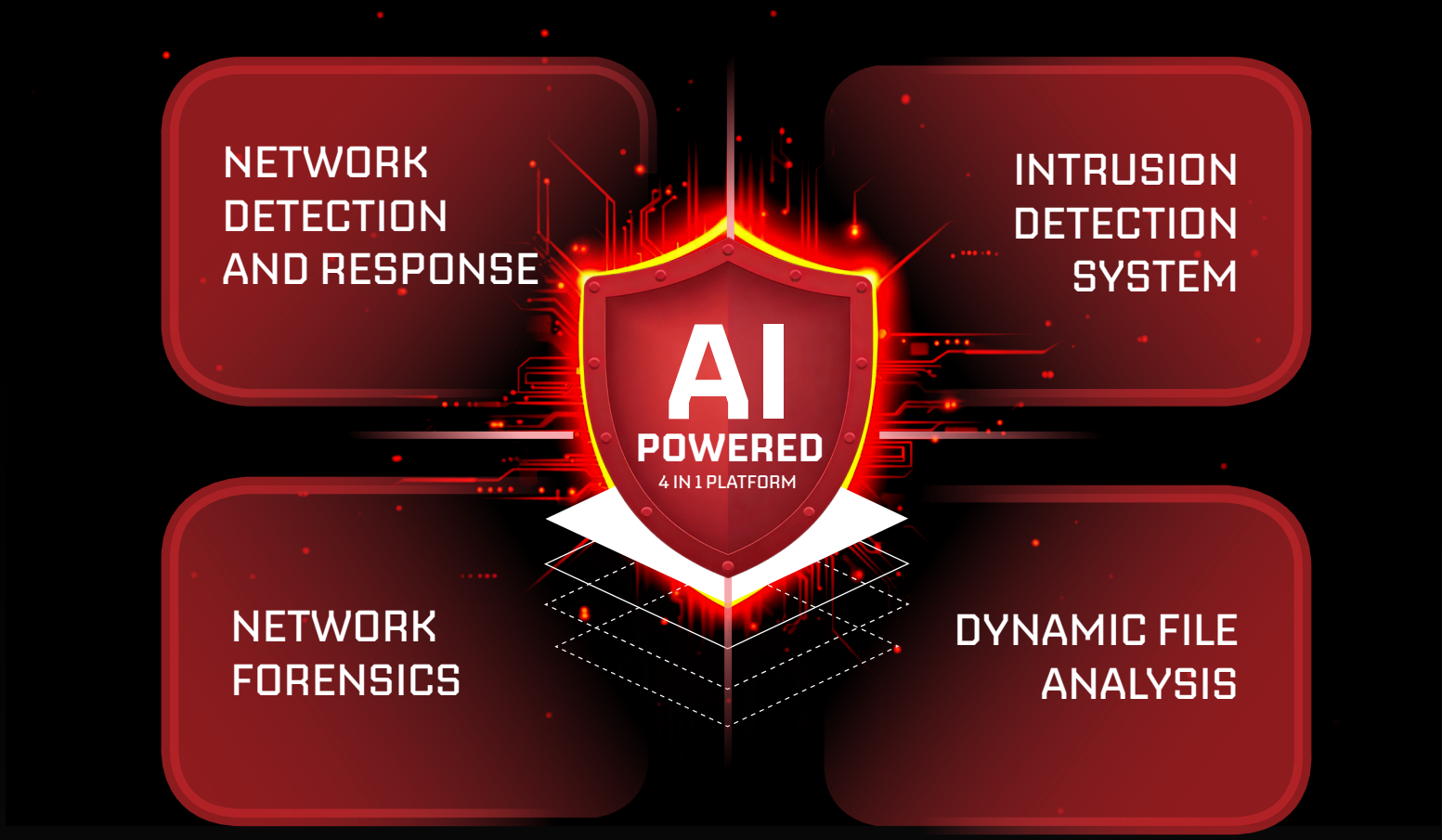
Full Packet Forensics

Full, Continuous
Packet Capture

180 days
Retrospective Hunting

Data Control

100%
On-premises



Key Highlights

- AI-powered behavioral anomaly detection
- ML-generated alert rationale
- Line rate detection
- Full, continuous packet capture
- Built-in and external threat intelligence
- Patent-pending Indexed-Raw technique for faster retrieval of packets
- Encrypted traffic analysis
- 180 days retrospective hunting
- Multi-Agent AI for autonomous threat detection, hunting and response
- Native PCAP viewer
- Full-packet session reconstruction
- On-demand dynamic file analysis
- Proprietary SIGINT-grade IDS
- Smart storage technology
- Custom detection rules
- Custom PII rules

Features

AI/ML-powered threat detection with AI precision

Unsupervised ML model learns normal network behaviour, dynamically calculates thresholds and generates alerts

AI provides deep threat insights and identifies complex threats such as zero-day attacks or APTs by analysing subtle behaviour anomalies

Supports early detection of lateral movement and potential data hoarding behaviour

ML learns user and device behaviour to establish baselines

Identifies risky behaviours such as non-standard protocol usage, abnormal session resets, high-entropy communications, suspicious UDP transfers, and SSH activity on non-standard ports

AI agent for automated and proactive threat hunting

AI agent evaluates alerts and provides verdicts on whether they are true or false positives

ML generated alert rationale for clear, explainable reasoning behind each alert

Multi-layered Threat Correlation

Recognizes threats by decoding 5000+ protocols, analysing 2mn+ IoCs, MD5 hashes and signatures

Classifies alerts across the full MITRE attack kill chain, with drill-down into tactics, techniques and affected assets

Analytics on 400+ L2-L7 metadata fields

Enables custom detection rules

Protocol-specific visibility across DNS, HTTP(S), TLS, SMTP, SSH, FTP, SMB, SIP, Kerberos, LDAP, ICMP, IoT protocols

Identifies relationships across users, devices, sessions etc. to reveal attack paths

Agentic AI that dynamically correlates alerts, behavior and contextual signals

ML automatically consolidates repetitive alert triggers within a defined time window into a single enriched alert

Correlates sessions with asset inventory, device intelligence, geolocation, identities, file analysis, and risk indicators (entropy, failed logins, non-standard protocols)

Risk scoring for prioritization of high risk incidents

Correlates among unknown threats, abnormal behaviour and application behaviour

Distinguishes between various types of attacks, such as DDoS, phishing, or malware, for more targeted responses

Provides structured case and change management workflows to help SOC teams track and manage investigations

Full, Continuous Packet Capture

Full fidelity attack reconstruction with forensics on raw packets, intelligence grade insights compared to “Event-based” forensics offered by competitors

Patent-pending Indexed-Raw technique for faster retrieval of packets

Rebuilds complete user sessions from raw packets

AI analyses past network traffic to identify long dwelling threats including APTs

Documents all evidence, reports and conclusions

Built-in Packet Analysis*

Upload packets from other monitoring platforms to analyse for threats

Performs a quick search across all packets

Enables quick pivots from alerts to PCAP details

*Included in NDR Pro

Features

Encrypted Traffic Visibility*

Encrypted Traffic Analysis without Decryption

Analyzes TLS fingerprints (JA4/JA4S, JA3/JA3S), handshake metadata, packet sizes, flow behavior and beaconing patterns to identify anomalies using machine learning

Encrypted Traffic Analysis with On-Demand TLS Decryption

Enables deep payload inspection by decrypting encrypted traffic

Provides full visibility into HTTP headers and URLs, extracts and analyzes files, inspects malware signatures, detects data exfiltration and enforces policy-based decryption controls

Line-rate Monitoring

Monitors network traffic at packet, session, host, user, application, protocol, and domain levels

Rebuilds complete user sessions from raw packets

Tracks file transfer sessions across applications and protocols for potential data exfiltration

Analyses remote access sessions, applications accessed remotely and session sources to detect unauthorized access, misuse of credentials, lateral movement etc

Actively tracks valuable assets. Risk scores vary based on asset criticality

Native, Patent pending IDS*

Identifies threats instantly using single-pass packet to rule-set correlation, not rule-by-rule scanning

Consistent latency and accuracy, regardless of rule-set size

Alerts in real time independent of session termination

Efficient CPU and memory utilization, even during continuous peak traffic

Threat Containment and Integrations

AI-powered structured, playbook-friendly response actions designed for seamless forwarding and automation

Supports API integrations such as DNS servers, firewalls, SIEM solutions for enhanced visibility

Bi-directional SOAR integration for a two-way exchange of intelligence and response actions

Supports LDAP/LDAPS for user credentials and access controls

Syslog integration and alert forwarding to one or multiple external syslog servers over TCP/UDP using RFC-compliant formats (RFC3164/RFC5424) and CEF/JSON schemas

Setup policy based actions for rapid response*

Supports Active Directory login and dynamic User-IP mapping to associate sessions with AD users, access control and session attribution

Configure email alerts. Supports secure and non-secure SMTP configurations with customizable alert criteria, formats, and batching

Integrates with firewalls to automatically block malicious IPs, domains, or connections

Integrates with vulnerability management platforms to correlate network threats

Dynamic file analysis*

Lightweight on-demand dynamic file analysis

Isolates suspicious files and executes them in a controlled environment

Examines processes and file actions such as changes to the registry, file system, or network connections, to detect malicious intent

*Included in NDR Pro

Features

Privacy and Compliance Support

Masks PII information with custom PII rules

Robust multi-factor authentication to prevent unauthorized access

Provides audit trail of all user activities

Storage Optimization

Smart Storage to set a predefined criteria to store only the high value traffic*

Categorizes traffic in categories, with granular filtering

Reporting

Automated report generation and distribution via email using report scheduler

Continuously monitors the system resources including CPU health, memory, backend processes etc.

Supports building customized reports using configurable metrics, aggregations, sorting, sample sizing, and time-based filters

Multi-Agent AI for Autonomous Threat Detection, Hunting and Response

Vehere Network Detection and Response embeds AI-powered agents and machine learning into its analysis pipeline, converting raw packet and flow telemetry into contextual, actionable intelligence. The AI framework improves detection precision, automates alert triage, and enables proactive threat discovery across both encrypted and non-encrypted traffic, reducing analyst workload while accelerating response.

Network Alert Analyzer Agent

Automatically triages high-volume ML alerts using alert context, session metadata, and historical behavior. Classifies true vs. false positives and triggers automated response actions (NGFW enforcement, TCP RST, adaptive tuning) to suppress noise and accelerate threat response.

Deep Threat Insight Agent

Transforms raw NDR alerts into context-rich intelligence by correlating alert telemetry with session metadata, threat intelligence feeds, and historical network activity.

Autonomous Threat Hunting Agent

Continuously analyzes packet and flow telemetry including NetFlow, JFlow and sFlow; to generate anomaly hypotheses, detect multi-stage kill-chain activity, suppress false positives, and raise correlated

Behavioral Anomaly Detection

Performs large-scale ML-powered anomaly detection across encrypted and non-encrypted traffic. Detects DNS anomalies and data exfiltration using 106 contextual metadata signals, entity-specific baselines, and MITRE ATT&CK-aligned behavioral analytics, with automation-ready outputs for SIEM/SOAR workflows.

*Included in NDR Pro

Why choose Vehere?

AI-powered Hunting, Detection and Response	Investigate, validate and respond with on-premises Vehere Vision AI	**Full, Continuous Capture**	Full fidelity, long term capture, lossless evidence
Widest threat coverage	Native threat intel feed, 5k+ protocols, 500k hosts, 2Mn+ IOCs	**SIGINT grade threat protection**	Built for national scale signal operations
Built-in PCAP analysis tool	View PCAPs without relying on tools like Wireshark	**Native On-demand dynamic file analysis**	For instant verdict on suspicious files
Native IDS	35k signatures, AI-powered IDS with true real-time, line rate threat detection	**Custom queries**	SOC Team can write custom queries without JSON knowledge
PII Masking	Built-in PII Masking with no telemetry sent to cloud	**Extremely Scalable**	Models start from 100 Mbps and can be scaled beyond 100 Gbps

About Vehere

Vehere is a new-age software company specializing in AI Cyber Network Intelligence. For more than a decade, Vehere has been supporting counter-terrorism analysts in Defence & Intelligence communities. Vehere is now trusted by cyber-analysts in Fortune 500 companies, including Telecom, Financial Institutions, and Smart Cities to protect their critical infrastructure against real-time cyberattacks. Vehere preserves fundamental principles of privacy and civil liberties.

E: sales@vehere.com

w: www.vehere.com