


Competitive Analysis

Vehere Vs Vectra

August 2025

THE NEED FOR NETWORK DETECTION AND RESPONSE



“Vehere's NDR is a high speed and extremely scalable network security solution designed for enterprises that demand real time network forensics. Built on experience safeguarding national security agencies, it has an advanced session reconstruction and AI driven behavioral analytics- all while ensuring personal data remains masked. Powered by advanced AI and machine learning, it continuously adapts to evolving threats, enabling faster detection, investigation, and response before risks escalate into breaches.”

Despite investing billions in cybersecurity, organizations still face persistent threats from attackers who bypass traditional defenses. In 2024, ransomware attacks surged by 75%, with hackers moving undetected within networks for days before striking. Once inside, these threats can remain undetected for months, putting critical data at risk of theft or corruption.

Perimeter security alone is no longer enough.

Legacy security tools that rely on known malware signatures and static indicators of compromise (IoCs) play a role, but they lack the real-time visibility needed to detect evolving threats. To stay ahead, organizations need solutions that continuously monitor network activity, identify anomalies, and respond before damage is done.

This is where Network Detection and Response (NDR) comes in. By leveraging advanced analytics, machine learning, and real-time traffic monitoring, NDR detects and contains threats across an organization's network. Unlike traditional tools, it provides visibility into both external attacks and internal movements, ensuring a faster, more effective defense against modern cyber threats.

Vehere is a security-first company, built from the ground up with threat detection, investigation, and real-time response as its foundation. Originating in Counter terrorism, Vehere has evolved its capabilities to deliver the same level of mission-critical protection to enterprise environments through its Network Detection and Response (NDR) platform. Security isn't an add on. Instead, it's at the core of every product decision and capability.

In contrast, Vectra originated as a SIEM overlay company in 2011, designed to provide IoCs across the network. While it has marketed itself in the XDR space over time, there remains ambiguity around its prime focus- whether it is positioned as an XDR, an NDR or a potential SIEM replacement.

NETWORK VISIBILITY

VEHERE



VECTRA

- Ingests **full packets** and **flow data**. **Built-in PCAP viewer** to analyse the full PCAPs in a few clicks
- Can run **advanced analytics** on both- raw data and flow data
- Offers **full session reconstruction**

- Ingests **Packet metadata only**. Requires 3rd party solutions for full PCAPs.
- **Analytics** are **limited** to metadata findings
- Due to its narrow scope, Vectra **doesn't provide full session reconstruction**

- Smart Storage feature to enable admins to configure the storage based on requirement
- Vectra sensors do not include onboard storage, limiting their ability to replay or reconstruct full sessions. This architectural constraint also reduces support for effective root cause analysis



VEHERE



VECTRA

- **Integrated File detonation in a safe environment**
 - Vehere's **integrated** IDS engine combines over **35,000 signatures** with **behavior, static and dynamic analysis** techniques to identify malware
 - Supports both **automated scans** and **on-demand scans** on files. In the event of exfiltration, the system provides a **comprehensive breakdown of extracted file contents**
 - Analysis includes **Process activity, Network behavior, Registry modifications** and **File level activity**
 - **Cannot execute or detonate files**
 - Vectra's **add-on** and **charge-able** 'Vectra Match' detects malware through **behavioural analysis**
 - **Lacks the ability to inspect files.** Hence, in cases of **data exfiltration**, it **cannot reveal the specific contents** that were extracted
 - Analysis **doesn't include registry modifications** and **file level** activity
- Vehere provides a built-in Dynamic file analysis to scan threats pro-actively and execute suspicious files in a safe environment

DATA PRIVACY AND SECURITY

VEHERE

- **Built-in PII hashing or masking**
- Vehere understands the critical need for PII protection. It offers built-in PII masking and hashing, along with **configurable rules** to meet each organization's specific compliance requirements.



VECTRA

- **No PII masking and hashing**
- Vectra claims it doesn't require PII masking as it doesn't perform decryption. However, leaving **usernames un-hashed** and **IPs un-masked** by default can introduce significant security risks.

- Personally Identifiable Information (PII) such as usernames, IP addresses, device IDs, and other data that can trace back to an individual must be safeguarded through masking, hashing, and customisable privacy rules.

PRICING & SUPPORT

VEHERE

- **Throughput driven** licensing model
- Vehere's pricing is structured on:
 - Throughput with **no IP restrictions**
- Vehere supports **500,000 concurrent IPs**



VECTRA

- **IP driven** licensing model
- Vectra's pricing is structured around three key factors:
 - Number of IPs
 - Number of logs
 - Size of the environment
- Vectra supports **300,000 concurrent IPs**

- Vehere imposes no IP based restrictions and doesn't charge extra for log processing

THANK YOU

