vehere

Competitive Analysis

Vehere Vs NetScout

March 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. Its adaptive ML models detect 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.

MAKING THE RIGHT CHOICE- VEHERE vs NETSCOUT

Vehere is a security-first company, built from the ground up with threat detection, investigation, and real-time response as its foundation. Security isn't an add-on. Instead, it's at the core of every product decision and capability.

In contrast, **NetScout** entered the NDR space through its 2015 acquisition of Arbor networks and continues to rely heavily on hardware centric deployments. Its security capabilities are layered onto a visibility-first architecture, with performance tied to certified appliances.

TRAFFIC ANALYSIS

VEHERE	NETSCOUT
• Network Behavioural analysis **with entity profiling**	• Network behavioural analysis **without entity profiling**

NetScout's detection remains network-flow and signature-centric, with limited behavioural insights tied to entities.

THREAT HUNTING & CONTAINMENT

VEHERE	NETSCOUT
• **Has Malware sandboxing** • **Admins can optimize their storage** based on their metadata and IP filters	• **No Malware sandboxing** • **No admin facing storage optimization** capability

Vehere offers real-time file analysis and sandboxing whereas NetScout lacks sandboxing emulation

SCALABILITY & DEPLOYMENT

VEHERE	NETSCOUT
• On-prem and private cloud deployment	• On-prem, cloud & hybrid options

THIRD PARTY INTEGRATION

VEHERE	NETSCOUT
• Can integrate with **SIEM , SOAR** seamlessly with API integrations	• Supports integration with **SIEM, SOAR,** XDR, Splunk, AWS, Cisco XDR, ServiceNow, CrowdStrike

NetScout provides a wider integration support but may require more configuration effort due to its tightly coupled infrastructure

ALERT EFFICIENCY

VEHERE

- Doesn't support decryption but **analyzes behavioral attributes of encrypted traffic**
- **MITRE Attack mapped alert** summaries with **risk scoring and severity levels**
- **Custom querying** ability with queries **available immediately** in the UI

NETSCOUT

- **Supports decryption** via nGenius appliance
- MITRE mapping supported with severity levels, but **alerts lack device attribution and entity level risk scoring**
- **Custom querying** and **correlation** requires exporting data, **manual config** and APIs

- Vehere provides behavioural visibility on encrypted traffic, and instant UI-based querying.
- NetScout lacks device behavioural context, and depends on external configuration for custom queries

PRIVACY & SECURITY

VEHERE	NETSCOUT
• **Masks PII, agnostic** of **hardware**	• **Packet masking and slicing using PFX hardware** but is **limited** to **advanced tier switches**
• **Supports dynamic user-defined PII masking policies** at runtime	• **Doesn't support dynamic user-defined PII masking policies** at runtime

Vehere has advanced PII masking regardless of hardware. In contrast, NetScout's masking is limited to their advanced modular switch series (2200, 4200, 6000) while basic switches lack masking ability

CUSTOMER BASE

VEHERE

- Optimized for **large enterprises**
- Ideal for **diverse industries** including telecom, finance, defense, manufacturing, education, etc.
- Spans multiple regions including **APAC, EMEA** and **North America**

NETSCOUT

- Primarily adopted by **mid to large enterprises** especially in **$50M-$1B revenue** bracket
- Strong presence in **telecom** (27%), education and manufacturing sectors (18%).
- **73% of its customers** are based **in North America**

Vehere AI Network Security is optimized for large businesses while NetScout is primarily designed for mid to large enterprises

THANK YOU