vehere

Competitive Analysis

Vehere Vs Arista

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. 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.

MAKING THE RIGHT CHOICE- VEHERE vs ARISTA

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, **Arista** originated as a networking company focused on high-performance switching for data centers and cloud infrastructure. Security was not its core focus until its 2020 acquisition of Awake Security. Arista has positioned NDR as an extension of its networking expertise.

TRAFFIC ANALYSIS

VEHERE

- Captures **full packets** (E-W and N-S) **without** any **challenges in NAT environments**
- Detection techniques include Signature, behaviour based unsupervised ML, DNN based supervised algorithm
- Offers **Entity Behaviour Analysis and Entity Profiling**
- Can ingest and analyse NetFlow and sFlow data

ARISTA

- Captures **full packets** but its **sensors face challenges** in co-relating **both sides of traffic in NAT environments**
- Detection techniques include Signature, Behavioural based supervised and unsupervised ML
- Offers **UEBA**, **Entity profiling**, though **accuracy in entity identification** has been reported as **inconsistent** by users.
- Doesn't ingest or analyse Netflow data. Supports sFlow data.

- Arista's sensors struggle to track both sides of traffic when NAT is used as IP address modifications disrupt traffic visibility between internal and external networks.
- Arista's entity resolution often misidentifies entities, leading to inaccuracies.

THREAT HUNTING & CONTAINMENT

VEHERE

- **Malware sandboxing** is a native and an **inbuilt** feature
- **Automatically configure IoC's** through STIX/TAXII
- Enables **full session reconstruction**
- Provides **default metadata retention of 30 days for all models**
- Admins can **optimize** their **storage** based on their packet requirements

ARISTA

- **Malware sandboxing is absent.** Integrates with 3rd party applications for sandboxing
- Requires **IoC's** to be **manually configured**
- **Doesn't provide session reconstruction**
- Provides **no metadata retention in its base models**
- **No storage optimization options** available for admins

- Vehere provides 30-90 days of metadata retention in all models while Arista reserves this capability for higher-tier models, with base models lacking metadata retention
- Arista lacks full session reconstruction which limits its depth of analysis during security incidents.

vehere

SCALABILITY & DEPLOYMENT

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

Arista requires hardware and licensing upgrades for mid-sized businesses scaling beyond 149 switches.

THIRD PARTY INTEGRATION

VEHERE	ARISTA
• Can integrate with **SIEM , SOAR** seamlessly with API integrations	• Can integrate with **SIEM, SOAR** but has a **tightly bound architecture**

Arista's NDR solution is designed to work seamlessly with its own network infrastructure, which may make integration smoother for existing Arista users but would require additional effort for those without its switches.

ALERT EFFICIENCY

VEHERE

- Detects **malware** and builds a **comprehensive report** on the exfiltration
- **Customized querying** ability with queries **available immediately** in the UI
- **Baseline period** for behavioral analysis is **7-14 days**

ARISTA

- Detects **malware** but **lacks visibility** into exfiltrated data and does not generate detailed malware reports
- **Customized querying** ability requires **ARISTA team's support**
- **Baseline period** for behavioural analysis is **30 minutes** (as claimed)

- Establishing an effective and reliable baseline typically requires several days to weeks. A baseline established within minutes may be neither comprehensive nor reliable.

vehere

PRIVACY & SECURITY

VEHERE	ARISTA
• **Masks PII** information • In-built **custom PII rule configuration** • Certifications: - ISO 9001:2015, - ISO 27001:2022	• **Doesn't have PII masking** • **Lacks PII rule configuration** • Certifications: - SOC 2, Type 1 - ISO 27001/18

Arista acknowledges security limitations on their website, lacks built-in data anonymization/masking, leaving sensitive information more vulnerable to insider threats

PROTOCOL SUPPORT

VEHERE	ARISTA
• Supports **5000+** protocols	• Supports **3000** protocols

Arista's 3,000-protocol limit may restrict coverage, reducing insight into certain traffic types.

vehere

MAJOR USE CASES

VEHERE	ARISTA
• Optimized for large enterprises with or without existing data centers.	• Better suited for large enterprises & customers with **established data centres**
• Diverse customer base **across multiple regions**	• Customer base **concentrated in North American regions**

Arista provides managed NDR service which is primarily designed for large enterprises with existing network infrastructure and the resources to engage Arista's security professionals.

COMPLIANCE

VEHERE	ARISTA
• Provides an audit trail of user system activity, combined with **full metadata** and **all PCAPs** (packet capture) for an **in-depth forensic analysis**	• Provides an audit trail of user system activity , metadata and **selectively captured PCAPs** which can **limit forensic depth** during unanticipated incidents

Vehere's full packet capture ensures complete forensic visibility unlike Arista's policy based selective capture

THANK YOU