Arista NDR vs. Extrahop Reveal(x)

This comparison highlights the difference between an adapted network performance monitoring tool and a true advanced Network Detection and Response solution.

A comparison of solutions from ExtraHop and Arista NDR highlights the difference between a tool that was borne out of a network performance monitoring and diagnostics heritage and adapted for security use, and a tool that was built from the ground up to provide security-focused advanced Network Detection and Response.

Introduction

Organizations worldwide have collectively invested billions of dollars in solutions and technologies intended to keep adversaries out of their networks. Nevertheless, tenacious attackers are still able to find their way around perimeter defenses to gain access to a targeted network. Once that foothold is established, the attacker might go unnoticed for months—and data assets are at high risk of theft or corruption.

Though legacy point-in-time preventative solutions that focus on signatures of known malware or static indicators of compromise (IoC) are still necessary, they aren't enough for comprehensive network security coverage. Solutions providing real-time detection of and response to suspicious activity are now a necessary complement to traditional security solutions. A new technology known as Network Detection and Response (NDR) is at the forefront of this market.

In its February 2019 Market Guide for Network Detection and Response, the analyst firm Gartner described the technology as using "a combination of machine learning, advanced analytics and rule-based detection to detect suspicious activities on enterprise networks. NDR tools continuously analyze raw traffic and/or flow records (for example, NetFlow) to build models that reflect normal network behavior. When the NDR tools detect abnormal traffic patterns, they raise alerts. In addition to monitoring north/south traffic that crosses the enterprise perimeter, NDR solutions can also monitor east/west communications by analyzing network traffic or flow records that it receives from strategically placed network sensors."[1]

Choosing the Right Software Platform

Two companies whose Network Detection and Response solutions are featured in the Gartner market guide are Arista NDR and ExtraHop with their respective products Arista NDR platform and Reveal(x). Many enterprises that are selecting their NDR platform narrow their choices to these two companies, given their market leading positions and their strong product offerings.

Choosing an NDR platform that is the best fit for an organization will have a strong impact on the company's ability to detect and quickly respond to suspicious activity, and subsequently attain a stronger security posture. A comparison of solutions from ExtraHop and Arista NDR highlights the difference between a tool that was borne out of a network performance monitoring and diagnostics heritage and adapted for security use, and a tool that was built from the ground up to provide security-focused advanced Network Detection and Response. This document compares the two companies' platforms according to the critical criteria that matter most to enterprise customers: the data being processed, the machine learning and other data science techniques applied to this data, the use cases thus enabled, the operational considerations around deployment and extensibility, and the security expertise behind the companies themselves.

Data

The lifeblood of any NDR platform, activity data tells the story of the traffic on the network—where it originates, where it's going, who the sender is, what device it came from, and so on. The deeper the data that can be consumed and analyzed, including current and past (stored) data, the better, as it tells a more complete and contextual story—one where the cast of characters includes devices, users, applications, and organizations rather than just IP addresses.

Richness of Data Sources

ARISTA NDR	EXTRAHOP
L2 - L7 network data	Wire data (a proprietary form of metadata)

This criterion looks at the depth of the data the platform analyzes. While ExtraHop does process and store the full packet, it runs detection analytics on "wire data" (a proprietary form of metadata). Arista NDR, on the other hand, runs analytics and machine learning against both extracted activity data as well as full packet information. This helps uncover a broader set of threats, especially those that blend in with business-justified activity; i.e., "living off the land" threats.

Network Visibility

Devices, Users, Applications, External Networks, Organizations and Domains	Limited to network parameters

Visibility is defined relative to the data source. If a platform is only looking at metadata, it's really only getting network protocol information—the ports, IP addresses, etc. By looking at the whole stack of the network, the NDR platform can resolve the relationships among devices, users, applications, domains, etc. This provides entity context that enables uncovering threats within both north-south and east-west communications.

ExtraHop is a network performance management tool attempting to deliver security capabilities. A prime example of the challenges with this approach is that the entity context it presents is not as relevant to a security practitioner. In addition, it limits detections to uncovering anomalies solely based on network protocol parameters. Arista NDR understands the entities– devices and users as well as external networks, organizations, and domains–communicating along with the traffic, so it can uncover threats within both north-south and east-west communications. Unlike ExtraHop, Arista NDR is also able to stitch these threats together to identify end-to-end campaigns and other potential victims.

Organizational Data Privacy

Data kept within customer environment; analytics can be deployed in private cloud if needed	Customer wire data uploaded to ExtraHop cloud on Amazon Web Services (AWS)

Oftentimes, organizations have data privacy policies or compliance requirements that prevent their network data from leaving their own environment. ExtraHop uploads customer wire data to its own cloud hosted on Amazon Web Services. Arista NDR keeps all customer data within the customer environment and does not upload it outside the organization's infrastructure. This also means that only Arista NDR enables customers to deploy analytics in private cloud environments or in those that are air-gapped; e.g., within government and military installations.

Data Science

Of course, collecting the data is only the first step. Data science delivers the ability to obtain insights and information out of the data that is collected from across the network. An NDR platform uses various scientific methods, processes, algorithms, and systems to extract these insights from structured and unstructured data. Arista NDR provides a fully integrated suite of advanced AI and machine learning analytics. ExtraHop provides a much more limited range of traditional machine learning tools-primarily unsupervised learning that is prone to false positives and lack of explainability.

Automated Entity Correlation

✓ Yes Plug and play AI-based behavioral fingerprints for tracking entities such as devices, users and applications	🕓 Limited Automatic names generated by monitoring protocols such as SMB and DNS or users can also manually name a device; analytics appear to be primarily IP based

This function provides an even deeper dive into network visibility by looking at behavior at the entity level, rather than the IP address level. Arista NDR automatically determines what entities/devices are using the applications and tracks those entities as they move around. For instance, if a device is in the New York City office today and in the Dallas office tomorrow, Arista NDR will track that device and associate all activity to that entity. ExtraHop's analytics appear to be primarily IP address-based. While both ExtraHop and Arista NDR have an understanding of the application/function of the device, only Arista NDR uses an understanding of the source, the destination and the traffic to perform detection of behavioral threats and malicious intent.

Extracted Detection Features

~1200 security specific features	~4700 network performance metrics

Because ExtraHop has evolved from a network performance monitoring solution to an NDR solution, it uses a large set of features that have little or no security impact. This represents a significant limitation if the goal is detecting modern threats with low false positives and negatives. Arista NDR, on the other hand, extracts a rich set of security-specific features that are based on the net effect of network communications rather than just the port and protocol information. This enables high-fidelity detection with low false positives.

Security Knowledge Graph

✓ Yes	⊗ No

The knowledge graph extends on entity correlation that identifies where the entities are as well as the relationships among them, the attributes that they share, and which entities are similar to others. So, for example, within the graph, all the digital phones are grouped together, all the devices in Finance are grouped together, and so on. The knowledge graph is essentially an underlying data store that Arista NDR created and patented, and it helps to understand an entity's behaviors that may differ from its peer group. In comparison, ExtraHop primarily views each IP address in isolation, other than some limited manual grouping capabilities and automated peer-identification for any network transaction.

Behavioral Analytics

✓ Yes	🕓 Limited
Source and destination entity analytics in addition to traffic analytics	Anomaly detection

ExtraHop's detections are based on traffic anomaly detection and thus suffer from an inherent challenge given that network information like IP addresses are ephemeral and unreliable. Arista NDR behaviorally fingerprints every entity on the network, performs similarity analytics, and uses all this information to detect threats.

Machine Learning

✓ Yes	🕓 Limited
Combination of supervised, unsupervised and federated machine learning	Cloud-based service that relies solely on unsupervised machine learning

There are different ways to teach a computer system about behaviors. ExtraHop primarily uses unsupervised learning to ascertain a device's normal behavior. This approach suffers from a challenge of being noisy since "normal behaviors" change often for very legitimate business purposes such as new software deployments, etc. In addition, this approach also fails when devices are already compromised before the baseline is established. Arista NDR's ensemble approach to learning compares against past behaviors, but also to similar entities and across the rest of the organization. This helps eliminate both the false positives and negatives that are prevalent with solutions like ExtraHop.

Explainability

✓ Yes	🕓 Limited
Fully transparent	

This pertains to the system providing sufficient context as to why something has been tagged as malicious. ExtraHop delivers detections with very little context and explainability, which presents a challenge for a security analyst to then understand why something is being detected or what to do about it. The product also does not provide the ability for the security analyst to tweak the detection model. This is because of the anomaly detection / unsupervised learning approach where anomalies are treated as malicious. Arista NDR offers every customer the ability to create their own detection models as well as view and modify Arista NDR's own models.

Time to Value

🕓 Hours	📅 4+ weeks training period

Unlike ExtraHop, Arista NDR avoids temporal baselining and instead performs behavioral analytics based on an understanding of the entities involved, behaviors of similar entities and behaviors prevalent across the enterprise. This approach also avoids the need to engage in constant and cumbersome retraining of the system (as is needed for ExtraHop) when legitimate behaviors change—for example when new software is deployed, or other organizational changes occur.

Use Cases

How can an organization use its Network Detection and Response platform? The more use cases a solution can support and the more specific they are to security practitioners, the better value and quicker ROI it provides.

User Experience and Workflows

Security Specific	Not Security Specific

ExtraHop is attempting to repurpose a network performance monitoring tool into a security solution. The user experience and workflows supported by the ExtraHop Reveal(x) product clearly show the challenges this presents. They tend to be much more focused on network metrics and less on security parameters. Arista NDR was built from the ground up to focus on security workflows and has the benefit of input from over 200 security teams.

Detect Known Attacker TTPs (Tactics, Techniques, and Procedures)

✓ Yes Detect non-malware and other threats that blend in with business-justified activity	⊗ No

Historically, the way most threat detection has occurred is through indicators of compromise (IoCs). These days attackers are smart enough to keep changing those indicators, so the more effective way to detect threats is by searching for an attacker's TTPs. ExtraHop focuses primarily on anomaly detection and "unusual changes" and therefore struggles to detect non-malware threats that abuse "normal" or legitimate privileges. Nor does ExtraHop provide a mechanism for security teams to build custom detection models for known attacker TTPs. This hurts efficacy since not every anomaly is malicious and not every malicious activity is an anomaly. Arista NDR's rich query language provides a vocabulary to codify even the most complex attacker TTPs and then have the system look for those on an automated and ongoing basis. These detection models are provided by Arista NDR but can also be built and customized by the customer.

Retrospective Detection

✓ Yes	🕓 Limited to network IOCs, e.g. IP addresses

Whenever a new attacker TTP emerges, organizations often want to know if that TTP has been observed in their environment in the past. ExtraHop offers retrospective detection of known IOCs but cannot do the same for attacker TTPs. Arista NDR can go as far back in time as needed and automatically surface relevant behaviors.

Encrypted Traffic Visibility

✓ Yes Patented approach	🕓 Limited Decrypts SSL/TLS traffic using an agent on every server and/or every client

More and more network traffic is getting encrypted and customers are increasingly hesitant to decrypt it due to the policy and privacy implications involved. Moreover, attackers increasingly use encrypted traffic as a way of evading network detection. Arista

NDR's innovative approach ensures customers' and their stakeholders' privacy is maintained at all times and avoids the need to deploy agents (as ExtraHop requires for this purpose) while also using encrypted data analysis to identify the applications (browsers vs. Microsoft Office apps vs. PowerShell etc.) and nature of traffic; e.g. interactive shell, web browsing, video, telephony, etc.

Automated Campaign Analysis

✓ Yes Automated incident triage that correlates across entities, kill chain activities and time	🕓 Limited

Most attacks today involve multiple devices and numerous actions. An attacker typically moves around within a network – for example, going from endpoint to server – as they try to achieve their end objective. With many security solutions, security analysts have to connect those dots themselves manually. Because Arista NDR has a historical view that is entity-centric, the "Situations" capability integrates, correlates and connects the dots across time and protocols. This reduces alert fatigue and makes the information more actionable for the security team. In comparison,while ExtraHop does classify detections by stage of the kill chain, it still treats every detection as an individual alert, leaving it to the security analyst to triage, connect the dots and stitch together the larger attack campaign manually.

Query Language and Threat Hunting

✓ Yes Extensible programing language that can interrogate incidents, the security knowledge graph, activities and raw packet data	🕓 Limited Drop-down list of network packet filters

ExtraHop has a network performance monitoring heritage as is clearly evident from its search capabilities that are focused on traditional networking parameters such as Tx and Rx stats, network type, ports, protocols, etc. These raw primitive types are not as usable by themselves for security use cases like threat hunting. Only Arista NDR offers the strength of a powerful programming language so a single search can identify complex combinations of behaviors across time and protocols, and consequently identify end-to-end attacker TTPs. Any queries and threat hunts can be saved for automated detections in the future.

Full Digital Forensics

✓ Yes Continuous packet capture	✓ Yes Continuous packet capture

Both ExtraHop and Arista NDR provide continuous packet capture. However, the packet capture and storage are separate capabilities in ExtraHop not tied to the detection and security functions in the product, thus breaking the analyst workflow. Additionally, ExtraHop uploads the resulting "wire data" to Amazon Web Services (AWS), whereas Arista NDR keeps all captured data within the customer's infrastructure.

Deployment and Extensibility

A Network Detection and Response platform needs to reach all parts of the network to collect its vital information, and it shouldn't operate in isolation, as many security products do today.

Deployment Considerations

✓ Yes Uses consequential artifacts to minimize the number of sensors needed	🕓 Limited Requires several network sensors and configuration for comprehensive coverage

Arista NDR is unique in its ability to process consequential artifacts. This key innovation uses the fact that many communications result in network artifacts that are produced as a side effect. As a result, Arista NDR is able to minimize the need for large numbers of network sensors. For instance, observing and deeply parsing Kerberos tickets being issued from the data center provides evidence of lateral movement between devices in a remote network without the need to witness the communication firsthand.

In addition, Arista is unique in its ability to use existing Arista network switches to monitor, preprocess and forward data to the Arista NDR Nucleus for analysis. These key innovations greatly reduce the need for large numbers of dedicated network sensors taps etc. in comparison to an ExtraHop deployment.

Supported Deployments

Sensors Physical, Virtual, and Cloud	Sensors Physical, Virtual, and Cloud
Analytics Physical, Cloud	Analytics Cloud

Arista NDR and ExtraHop support similar deployment form factors with one significant difference. Only Arista NDR enables customers to deploy analytics in on-premise or private cloud environments. This enables a variety of customer use cases including those in heavily regulated or government and defense establishments.

Corporate Background

Expertise and Security DNA

✓ High	🕓 Limited

There is no substitute for deep subject matter knowledge and expertise. The ExtraHop team has very limited expertise in the security field. Most of the team comes from the network performance management space. Arista NDR's platform is built by security industry veterans from companies ranging from Symantec and McAfee to FireEye and Cylance, and more than 50% of the company's employees have advanced degrees or PhDs.

Conclusion

While there are numerous NDR platforms on the market today, Arista NDR has been named a "Value Leader" by Enterprise Management Associates (EMA) in its recent Network Security Analytics report. Arista NDR was recognized for providing the greatest balance between features and costs when compared to ExtraHop and other solution vendors. Most importantly, the EMA vendor analysis included interviews and insights from real customers who find strong value in Arista NDR's security platform.

The Arista NDR platform delivers network detection and response capabilities so organizations can detect and hunt for threats missed by traditional security solutions. Importantly, unlike many other Network Detection and Response platforms including ExtraHop Reveal(x), Arista NDR does so without uploading customer data outside their infrastructure. Arista NDR's approach minimizes false positives and negatives and thus reduces workloads for already stretched security teams while delivering effective risk management.

Sources

1. Gartner, Inc., Market Guide for Network Detection and Response, February 2019

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062