

Arista NDR vs. RSA NetWitness

This comparison highlights the difference between a platform built on legacy security and network monitoring modules and advanced network detection and response solutions.



Introduction

A comparison of the RSA NetWitness platform with Arista NDR's advanced network detection and response highlights the huge strides in artificial intelligence and cognitive automation made over the last few years. NetWitness is a complex and expensive series of legacy modules that require the customer to write extensive rules and complex search queries before any results are delivered. The complicated manual configuration and integration labor associated with NetWitness deployments drives high costs and long deployments, constrains usability, and delivers error-prone results.

Compared to NetWitness, Arista NDR delivers an easy to deploy platform that shows value in hours rather than months. Moreover, the Arista NDR Platform is designed to be used by analysts of all skill levels—from the junior analyst simply looking to perform triage to the expert threat hunter. Analyst firm EMA conducted an independent competitive review of network detection and response solutions and named Arista NDR the "Value Leader," ranking it #1 for time to value because of its frictionless approach that delivers answers rather than alerts.

This document compares the two companies' platforms according to the critical criteria that matter most to Network Detection and Response (NDR) 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 corporate focus and security expertise behind the companies themselves.

Data

As 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		RSA NETWITNESS
L2 - L7 network data		L2 - L7 network data

This criterion looks at the depth of the data the platform analyzes. NetWitness can capture complete packets, but these need to be defined by the user in the Network Decoder appliance. It also supports the use of SNORT IDS signatures. Arista NDR automatically provides full visibility for layers 2 through 7 and can detect sophisticated application layer attacks without signatures while minimizing false positives and reducing management overhead.

Network Visibility

Devices, Users, Applications, External Networks, Organizations and Domains		IP Addresses

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 Arista 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.

Arista NDR builds models of the entities – devices and users, as well as external networks, applications, organizations and domains – communicating along with the traffic so users can uncover threats within both north-south and east-west communications. NetWitness Network, on the other hand, requires extensive configuration and integrations to provide visibility beyond IP addresses.

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. RSA NetWitness lacks any significant data science capabilities as explained in this section.

Automated Entity Correlation

<p>✓ Yes</p> <p>Plug and play AI-based behavioral fingerprints for tracking entities such as devices, users and applications</p>		<p>🕒 Limited</p> <p>Requires integration with Active Directory (AD). Only covers the limited devices in AD</p>
----------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------

This function provides an even deeper dive into network visibility by looking at behavior at the entity level rather than the IP address level. Unfortunately, the NetWitness Network module tracks all activities by the IP address. Integration into Active Directory (AD) with the Context Hub component of the Event Stream Analysis engine is required to add “data enrichments.” Data enrichments are not correlated by the system but rely on the analyst to “connect the dots.”

Extracted Detection Features

<p>~1200</p> <p>security specific features</p>		<p>✍ Manual</p> <p>Varies based on protocol decoder rules created by the user</p>
------------------------------------------------	-------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------

Arista NDR extracts a rich set of features 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 and minimal configuration and maintenance.

Security Knowledge Graph

<p>✓ Yes</p> <p>Autonomously built</p>		<p>⊗ None</p>
----------------------------------------	-------------------------------------------------------------------------------------	---------------

Arista NDR automatically builds a security knowledge graph that identifies the entities – the devices, applications, users, etc. – and their behaviors, the relationships between them, and any malicious activity across the kill chain.

The NetWitness “Respond” module offers a graphical display of the results of user-configured rule sets. However, this limits its capabilities as the user must predict possible incidents in advance and create, debug, test and deploy the rules needed to detect future attacks.

Machine Learning

 Yes Combination of supervised, unsupervised and federated machine learning		 Limited ML is limited to unsupervised learning of detection of known command and control domains
------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

There are different ways to teach a computer system about entities' behaviors. Arista NDR takes a comprehensive approach to data science by using supervised, unsupervised, and federated learning to identify suspicious activities, supported by distributed cognitive services to eliminate false positives.

NetWitness machine learning is limited to monitoring possible command and control activity from external domains flagged as C&C sources by publicly available information. It is unclear why this would need machine learning since detections like these typically use signatures.

Time to Value

 Hours		 28+ days
------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------

Arista NDR performs behavioral analytics based on understanding the entities involved, behaviors of similar entities, and behaviors prevalent across the enterprise. This approach avoids the need to retrain the system (as is needed for NetWitness) when legitimate behaviors change; for example, new software is deployed, or other organizational changes occur.

NetWitness recommends a 28 to 60 days training period when deploying their UEBA product. Arista NDR's platform is usable within hours of deployment and continually learns as the length of visibility increases.

Behavioral Analytics

 Yes Source and destination entity analytics in addition to traffic analytics		 None NetWitness Network does not include a behavioral analysis engine
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------

Arista NDR behaviorally fingerprints every entity on the network, performs similarity analytics, and uses this information to detect threats.

NetWitness offers User and Entity Behavior Analysis (UEBA) as an additional licensed product that runs in conjunction with the NetWitness Network and provides behavioral analytics derived from system logs. This standard feature in Arista NDR doesn't require integration with log sources.

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.

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

 Yes Including complex low-and-slow behaviors		 Manual Limited to individual session characteristics
--------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------

Arista NDR can identify complex behaviors involving any number of systems and can analyze low-and-slow behaviors over long periods. This allows Arista NDR to deliver the industry's first true TTP capable Adversarial Modeling Language.

NetWitness detection is limited to whatever patterns can be identified in a single session.

Retrospective Detection



Whenever a new attacker TTP emerges, organizations often want to know if that TTP has been observed in their environment in the past. Arista NDR automatically maintains historical data and is continually retrospectively comparing past activities across devices to current threat behaviors. This enables both manual historical auditing as well as automated threat hunting.

NetWitness requires the user to manually define the rules needed for data retention, increasing management overhead and increasing the likelihood of human error.

Encrypted Traffic Visibility



Arista NDR's innovative approach enables classification of session type – e.g., interactive shell, web browsing, video, telephony, etc. – and identification of applications, detecting remote access etc., all without having to decrypt the traffic. This allows Arista NDR to detect threats in both encrypted and unencrypted traffic.

The NetWitness approach requires resource-intensive hardware and configuration labor to implement out-of-band decryption which violates many organizations' privacy policies. The NetWitness approach is ineffective if decryption capabilities are unavailable.




Automated Campaign Analysis



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.

NetWitness requires multiple, separately licensed modules, servers and sensors to identify the scope of a threat and even then leaves significant manual effort for the security analyst.

Query Language and Threat Hunting

 Yes Extensible programming language that can interrogate incidents, the security knowledge graph, activities and raw packet data		 Outsourced Rules-based query builder and third-party query language
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------

Only Arista NDR offers the strength of a powerful adversarial modeling language so a single query can identify complex combinations of behaviors across time and protocols, and consequently identify end-to-end attacker tactics, techniques & procedures. Queries and threat hunts can be saved for automated detections in the future.

NetWitness uses a combination of rules and third-party event processing language owned by Espertech Inc.

Full Digital Forensics


 Yes Full packet capture plus forensic automation		 Manual & Error Prone Full Packet Capture
----------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------

Both systems provide a full packet capture platform, but only Arista NDR provides a distributed cognitive services layer on top of the packet store to automatically detect threats and precompute the answers that analysts need most when investigating network data.

Deployment and Extensibility

An NDR 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. Arista is unique in offering direct integration with Arista network switches that function as Ava Sensors which preprocess and forward the traffic to the NDR Nucleus for comprehensive analysis ensuring that all traffic is effectively monitored.

Deployment Considerations


 Yes Uses consequential artifacts to minimize the number of sensors needed		 Requirements Requires multiple product modules, large numbers of network sensors, multiple servers and extensive configuration efforts 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 first-hand.

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.


NetWitness requires multiple sensors, brokers, concentrators, and servers to implement a complete solution. This greatly increases costs and complexity.

Integration with Other Security Tools

<p>✓ Yes</p> <p>Covers all the major security solution types from SIEM and SOAR to EDR and Network Packet Brokers</p>		<p>⌚ Limited</p> <p>"Network" product limited to other NetWitness products. Additional "Orchestrator" product required for third party integration.</p>
-----------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------


Arista NDR offers "no cost" integrations with a wide range of security tools, from Firewalls and SIEM consoles to Endpoint Detection and Response solutions. NetWitness requires the purchase, installation, integration, and configuration of a separate product to integrate with existing solutions.

Threat Intelligence Integration

<p>✓ Yes</p>		<p>✓ Yes</p> <p>via additional product license</p>
--------------	-----------------------------------------------------------------------------------	----------------------------------------------------

Arista NDR enables customers to natively detect known indicators of compromise both on an ongoing basis and retrospectively. NetWitness provides threat intelligence via their proprietary subscription-based intelligence feed, "Live Connect."

API

<p>✓ Yes</p> <p>Rich, documented and supported API</p>		<p>✓ Yes</p>
--------------------------------------------------------	-------------------------------------------------------------------------------------	--------------

Arista NDR enables organizations to extend and customize the platform capabilities through an API, integrate the platform into existing security and business processes, and inject and draw relevant context to and from the Arista NDR platform. This is not provided by NetWitness.

Performance

<p>✓ 10Gbps</p> <p>sustained or higher with scale out deployment</p>		<p>✓ 10Gbps</p> <p>when configured for minimal packet decoding</p>
----------------------------------------------------------------------	-------------------------------------------------------------------------------------	--------------------------------------------------------------------

Arista NDR's deployments minimize the hardware / virtual appliance footprint by offering Switch integrated "Ava Sensors" as well as traditional hardware, virtual and cloud based sensors and scales to hundreds of gigabits of traffic.

Corporate Background

Corporate Focus

Advanced Network
Security Analytics



RSA Ecosystem Focus

Arista NDR delivers next-generation network detection and response utilizing state of art technology.

NetWitness was an early entrant into network analytics and focused on large government agencies which drove the development of an incredibly complex, resource and manpower intensive solution that has failed to keep pace with the rapidly changing technology in the Network Detection and Response (NDR) field.

Summary

Customers looking for NetWitness alternatives, or a replacement, would do well to consider a solution built on the latest technology. The NetWitness Network module is a reactive system based on user-defined rules that are inherently focused on past behavior and cannot detect new or novel approaches developed by threat actors.

NetWitness provides minimal correlation of threats across the kill chain. Arista NDR's entity tracking capability allows the platform to automatically correlate complex attacker activities, identifying all of the devices, network activities, and threats that are a part of the overall campaign. This, in turn, helps reduce alert fatigue and makes the information more actionable and easily consumable for the security team.

The NetWitness UEBA Essentials module uses unsupervised learning to ascertain a device's normal behavior. This approach is 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 machine learning compares past behaviors, but correlates with similar entities across the rest of the organization to increase accuracy. This helps eliminate both the false positives and negatives that are rampant with solutions like NetWitness.

The anomaly detection approach has another significant drawback. NetWitness 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 UEBA Essentials product also does not provide the ability for the security analyst to tweak the detection model. Arista NDR offers every customer the ability to create their own detection models as well as view and modify Arista NDR's models.

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

