Arista NDR vs. Darktrace

This comparison highlights the difference between the first-generation approach to behavioral analytics and the newer advanced network traffic analysis solutions.

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 to subsequently attain a stronger security posture.

Introduction

Organizations worldwide have 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 and static "indicators of compromise" (IoC) are still necessary, they aren't enough for comprehensive network security coverage. Solutions which detect and respond to suspicious activity, without the need for signatures or IoC's are now a necessary complement to traditional security solutions. New technology known as Network Detection and Response(NDR) is at the forefront of this market.

In its June 2020 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 suspicious or malicious activity, they raise alerts or take actions. 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 from strategically placed network sensors."

Choosing the Right Software Platform

Two companies whose network detection and response solutions are featured in the Gartner market guide for NDR[1] are Arista NDR and Darktrace with their respective products Arista NDR Platform and Enterprise Immune System. Many enterprises that are selecting their NDR platform narrow their choices to these two companies, given their leading positions in the market 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 to subsequently attain a stronger security posture. A Darktrace comparison to Arista NDR highlights the difference between the first generation of behavioral analytics approaches and the emergence of newer advanced network detection and response solutions. 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, and the operational considerations around deployment and extensibility.

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	DARKTRACE
L2 - L7 network data	BRO Alerts (L2-L4)

This criterion looks at the depth of the data the platform analyzes. Darktrace uses BRO (Zeek) alerts on L2 - L4 data, whereas Arista NDR consumes L2 - L7 network data. This gives Arista NDR the advantage of uncovering malware and non-malware threats by looking at more than just the metadata of protocol headers.

Network Visibility

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

Visibility is defined relative to the data source. If a platform is only looking at metadata, it's 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 north-south and east-west communications. Darktrace is focused on detecting anomalies based on IP addresses. Arista NDR recognizes that not every anomaly is malicious and not every malicious activity is anomalous and therefore goes further by stitching threats together to identify end-to-end campaigns.

For example, Darktrace can identify as anomalous that a user has connected to Twitter—something they haven't done before but likely does not raise a concern from a security perspective. However, with its more detailed network visibility, Arista NDR also knows that the connection came to Twitter from Microsoft Word, a tactic that attackers frequently use but legitimate users don't. Darktrace would completely miss this context and thus can either flood the analyst with every anomalous Twitter connection or miss this advanced attacker tactic entirely.

Organizational Data Privacy

Data kept within customer environment – analytics can be deployed in private cloud if needed	Data kept within customer environment

Data Science

Of course, collecting the data is only the first step. Data science delivers the ability to obtain insights and information from the data collected 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. Darktrace 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 IP address-based and requires integrations with technologies like Active Directory and observation of DNS and DHCP traffic

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 use 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. If the visibility is limited to network information, as is the case with Darktrace, the device likely has an entirely different IP address tomorrow, and so it is considered to be a different entity. Trying to correlate that information manually creates more work for the security analyst.

Extracted Detection Features

~1200	~300

Darktrace is limited to broad features for its machine learning—network messages, ports, and protocols. This presents a challenge when detecting modern threats that often blend in with business-justified traffic, especially with a low rate of false-positive alerts. Arista NDR extracts a rich set of features based on the net effect of network communications rather than just the port and protocol information, e.g., it is one thing to identify a packet as Kerberos and another to differentiate between a successful and failed login attempt. This enables high-fidelity detection of malicious behavior with low false positives and negatives.

Security Knowledge Graph

✓ Yes	⊗ No

The knowledge graph is a buildup on entity correlation that identifies where the entities are and the relationships among them, the attributes they share, and which entities are similar to others. So, for example, within the graph, all the digital phones are grouped, all the devices in Finance are grouped, 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, Darktrace views each IP address in isolation, so there is no facility like a security knowledge graph to correlate entities.

Machine Learning

✓ Yes Combination of supervised, unsupervised and federated machine learning	◷ Limited Traffic analytics (network port, protocol and bandwidth based)

There are different ways to teach a computer system about behaviors. Darktrace primarily uses unsupervised learning on data samples to establish a device's "pattern of life," or the normal behavioral pattern. While improving traditional pattern-matching detections, this approach remains noisy since "patterns of life" often change for legitimate business purposes – For example, new software deployments, organizational realignments, etc. However, it fails when devices are already compromised before the pattern of life is learned; in other words, the malicious behavior will be treated as the norm. Arista NDR's ensemble approach to machine learning compares against past behaviors and to similar entities across the organization, thereby eliminating false positives and the false negatives rampant with solutions like Darktrace.

Time to Value

Hours	1-2 weeks training period

Darktrace and Arista NDR vary significantly in the required machine learning training period. Arista NDR can be operational in hours since it doesn't rely only on unsupervised learning, whereas Darktrace needs a week or more. Moreover, the Darktrace platform needs to be retrained when legitimate behaviors change, such as when new software is deployed, or other organizational changes occur. The extra training time is lost value for the customer.

Behavioral Analytics

✓ Yes Source and destination entity analytics in addition to traffic analytics	Limited Traffic analytics (network port, protocol and bandwidth based)

Use Cases

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

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

✓ Yes Detect non-malware and other threats that blend in with business-justified activity	Limited Capabilities

Historically, most threat detection has occurred through indicators of compromise (IoCs) which reflect data from prior attacks. These days attackers are smart enough to keep changing their tactics and techniques as well as those indicators, so the more effective way to detect threats is by searching for an attacker's TTPs. Darktrace struggles to detect non-malware threats and provides no mechanism for security teams to build custom detections for known attacker TTPs. Arista NDR's rich query language provides a vocabulary to codify these TTPs and then have the system look for them on an automated and ongoing basis. These detections are provided by Arista NDR but can also be built and customized by the customer.

Retrospective Detection

✓ Yes	🕓 Limited

Whenever a new attacker TTP emerges, organizations want to know if their environment has been susceptible (to that TTP) in the past. Darktrace doesn’t offer retrospective detection, instead giving customers the ability to run searches through the underlying BRO logs over approximately a 30-day period. Arista NDR can go as far back in time as needed and automatically surface relevant behaviors.

Encrypted Traffic Visibility

✓ Yes Patented approach	🕓 Limited Uses open source JA3 for application fingerprinting

More and more network traffic is getting encrypted, and customers are unwilling to decrypt it due to the policy and privacy implications. Moreover, attackers increasingly use encrypted traffic to evade network detection. The Arista NDR solution can draw inferences from the encrypted data without the need to peek into the actual payload itself to combat this trend. This is done through encrypted traffic analysis that identifies the nature of the traffic and communicating applications. Unfortunately, Darktrace has limited abilities to do this because it relies on the open-source JA32 library, and as a result, significant suspicious activities can be overlooked.

Automated Campaign Analysis

✓ Yes Automated incident triage that correlates across entities, kill chain activities and time	⊗ No

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, Darktrace views detections of activities as individual alerts with very limited correlation based on IP address and fails to tell a complete story about an attack campaign.

Query Language and Threat Hunting

✓ Yes Extensible programing language that can interrogate incidents, the security knowledge graph, activities and raw packet data	🕓 Limited Elastic search through BRO logs

Arista NDR offers the strength of an extensible programming language that can interrogate incidents, the security knowledge graph, activities, and raw packet data.

A single query 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. Darktrace provides a much more limited elastic search capability through BRO logs.

Full Digital Forensics

✓ Yes	✓ Yes
Continuous packet capture	Limited full-packet forensics

Arista NDR provides forensic evidence and historical records even when there is no apparent threat. This enables threat hunting and delivers evidence needed after the fact. Without full packet capture, Darktrace doesn't provide this historical perspective.

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	🕓 Limited
Uses consequential artifacts to minimize the number of sensors needed	Requires large numbers of network sensors for comprehensive coverage

Darktrace requires large numbers of network sensors for comprehensive coverage. Arista NDR uses ”consequential artifacts” to minimize the number of sensors needed. 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. in comparison to a Darktrace deployment.

Integration with Other Security Tools

✓ Yes	🕓 Limited
Covers all the major security solution types from SIEM and SOAR to EDR and Network Packet Brokers	

Arista NDR delivers a large range of integration capabilities with existing security tools out of the box. These range from firewalls, network switches and SIEMs to orchestration solutions and Endpoint Detection and Response systems. Darktrace is much more limited in its approach to integration with other tools.

Threat Intelligence Integration

✓ Yes	ⓧ No

Most enterprises get threat intelligence feeds from external sources. Arista NDR can utilize these feeds to detect known indicators of compromise, both on an ongoing basis and retrospectively. Darktrace doesn't support this capability.

API

✓ Yes Rich, documented and supported API	🕓 Limited

Arista NDR enables organizations to extend and customize the platform's capabilities through an API. Customers can integrate the platform into existing security and business processes and inject and draw relevant context to and from the Arista NDR platform. Darktrace is limited in this capability.

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 Darktrace 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 helps organizations detect and hunt for threats missed by traditional security solutions. The platform analyzes every packet on the network to automatically discover, track and build profiles of devices, users, applications and who they interact with, while flagging and ranking suspicious activity. This gives security teams the tools to rapidly investigate that activity and take the required action.

By applying artificial intelligence to the only real source of truth – network data – Arista NDR automates the manual and time-consuming work that only the most experienced threat hunters can perform to find and react to modern threats.

Sources

1. Gartner, Inc., Market Guide for Network Detection and Response, June 2020

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