ARISTA

White Paper

Arista NDR

Introduction

Networks have become more important than ever before as they seamlessly connect a variety of devices-- traditional desktops, laptops, IoT and OT devices, cloud, SaaS, work-from-anywhere, supply chain, and contractor devices. This advent of hybrid work has introduced a great level of flexibility (and choice) in the way businesses can run today. With multi-cloud, and multi-device collaboration becoming a mandate for hybrid work, the new network needs to be truly edge-less. Unfortunately, network security has simply not kept up with this powerful "new network". As a result, organizations face issues around excessive costs of security operations, high impact due to extended attacker time, access within the victim network, and elevated risk of missed attacks.

Security measures need to pivot from reactive to a more proactive approach of continuous contextual network monitoring that ensures a threat is detected before it can proliferate to a data breach. Arista's zero trust networking principles, based on NIST 800-207, help customers build a more proactive security ecosystem that focuses on maintaining complete 360-degree visibility and control over the enterprise threat landscape.

Arista NDR is a key component of this strategy and focuses on tackling challenges in the areas of network detection and response, digital forensics, and threat hunting. This award-winning platform enables customers to tackle use cases ranging from non-malware and insider threat protection to performing forensic investigations.

Background

Increasingly, many breaches are now the result of attackers using hard-to-detect threat vectors such as:

- the abuse of legitimate tools (Microsoft Office, remote access services, etc.) that already exist within the victim's environment,
- the misuse of insider access,
- the use of popular websites and network destinations as covert communication channels.

At the same time, despite increased investments in security budgets, customers still struggle to see, let alone secure the "new network," including public and private cloud, sensors, and other Internet of Things (IoT) devices, bring your own device (BYOD), and third-party supplier and contractor devices.

Solving these challenges today demands a high level of manual efforts and human expertise that is hard to find and retain. Customers, therefore, need a zero trust focused platform that provides visibility into the entire network, correlates different threat vectors to understand mal-intent, and automates hunting and investigation of malicious intent even when it blends with business-justified activity. This minimizes tedious and challenging tasks for the most experienced analysts and enables junior analysts to be far more productive.

How does Arista NDR fit in

Arista NDR quickly uncovers and correlates complex adversarial behaviors to support threat investigation and incident response. Additionally, the platform provides quick time to value since customers can have it up and running without requiring lengthy machine learning training periods and operational overhead.

Arista NDR analyzes billions of network communications to autonomously discover, profile and classify every device, user, and application across the new network—perimeter, core, IoT, and cloud networks. Based on this deep understanding of the attack surface, the platform then detects threats to and from these entities, while providing the context necessary to respond rapidly.

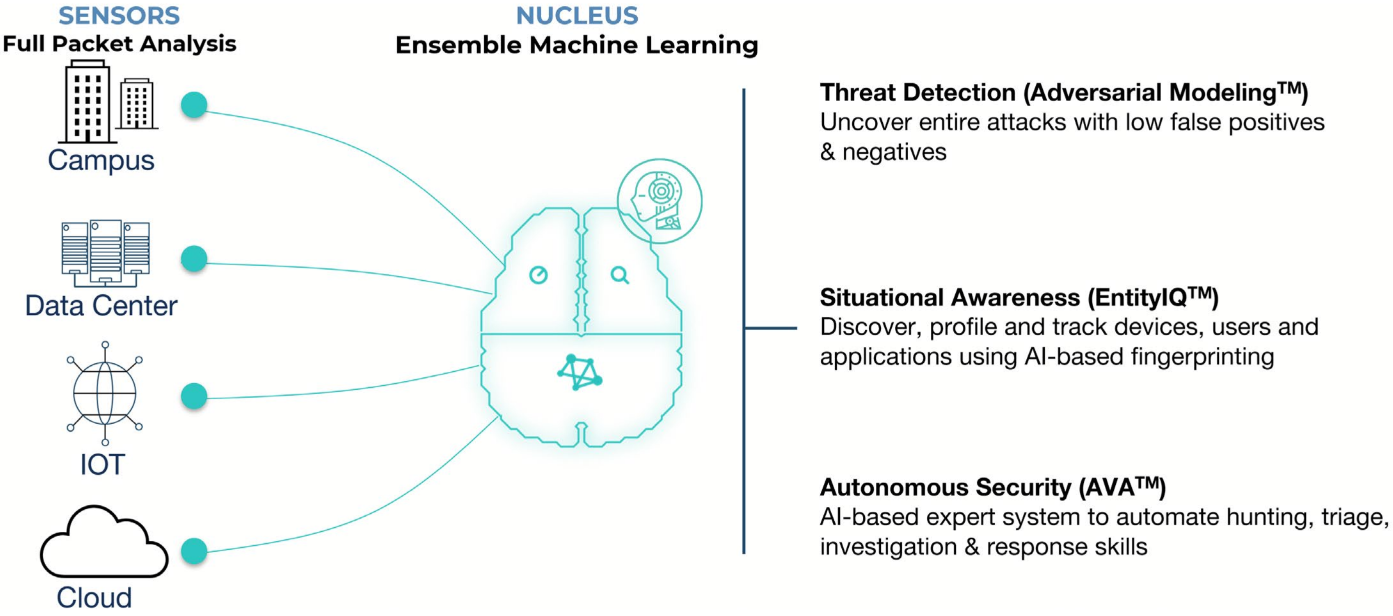
The analysis begins with AVA Sensors that span the "new network" and perform deep packet inspection. These sensors are available in a variety of form factors: physical hardware, virtual, cloud-based, and now also incorporated into Arista campus switches.

Extracted activity data from the sensors feed into the AVA Nucleus, either on-premises or in the cloud. This component uses a combination of detection models to uncover malicious intent. Using a multi-dimensional machine learning (ML) approach, the platform models complex adversarial behaviors and connects the dots across entities, time, protocols, and attack stages. Unlike prior generations of network detection and response tools, this approach delivers threat detections with low false positives and negatives and provides the context necessary for triage, incident response, and remediation.

The Nucleus also integrates with other IT and security solutions within the environment and can thus provide automated response and remediation.

Underlying Arista NDR lie three key innovations that enable enterprises' zero trust security strategy:

- EntityIQ™ is the world's only artificial intelligence-based security knowledge graph that identifies, profiles, and tracks all the devices, users, and applications on the new network.
- AVA™ is the world's first security expert system that uses machine learning, threat intelligence, and codified human expertise to perform autonomous triage and investigations while keeping customer data firmly within their infrastructure.
- Adversarial Modeling™ is another industry-first capability that uses heuristics with EntityIQ™ to identify attackers based on their intent. By understanding mal intent, versus looking for only specific indicators of an attack, Arista NDR greatly improves the ability to see and stop attackers, especially those that have malicious intent but still blend into normal activity. This capability also enables customer security analysts to build customized detection for threats that are unique to their organization.



Threat Detection (Adversarial Modeling^{TM})
Uncover entire attacks with low false positives & negatives

Situational Awareness (EntityIQ^{TM})
Discover, profile and track devices, users and applications using AI-based fingerprinting

Autonomous Security (AVA^{TM})
AI-based expert system to automate hunting, triage, investigation & response skills

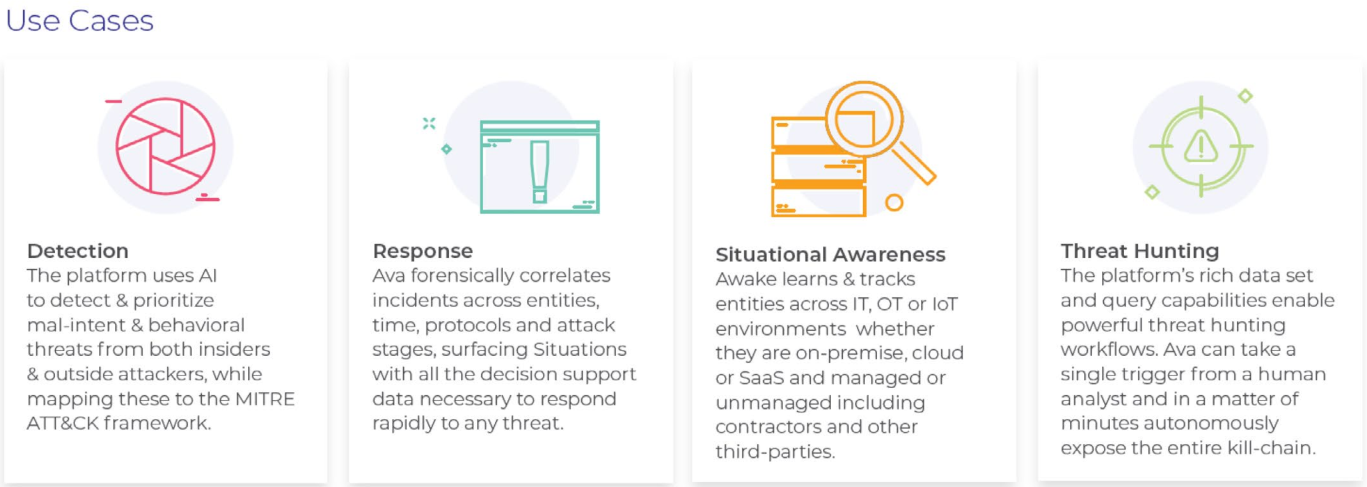
Figure 1: Three Key Innovations behind Arista NDR

Customer Benefits

- Faster Detection and Response: Arista NDR customers have seen up to an 88% reduction in the time to detect and time to respond to attacks, and a 3x average improvement in situational awareness of the environment.
- Lower False Alerts: Independent comparative testing by the Tolly Group[1] showed that Arista NDR had the lowest false negative rate, ensuring critical threats do not go unnoticed. This contributed to a signal-to-noise ratio of 95%--almost fifteen times better than the competition. Arista NDR thus dramatically lowers day-to-day operational costs compared to competitive solutions that generate high numbers of false alerts and therefore add to analyst workloads.
- Rapid Investigations: The Tolly testing also showed that the NDR platform is best-in-class for threat validation by supporting investigative workflows with the context and information necessary for rapid remediation.
- Analyze Encrypted Traffic: Arista NDR parses data deeper than any other solution on the market, looking at the full network packet and drawing inferences based on data science even if the traffic is encrypted.
- Quick Time to Value: Importantly, the platform is up and running in under 30 minutes without any impact on end-user devices or the rest of the infrastructure. Metrics like these have prompted analyst firms such as Kuppinger Cole[2] to identify Arista NDR as a leader in this critical security technology space.

Key Use Cases

Arista NDR supports a variety of use cases spanning situational awareness of the new network, threat detection and incident response, threat hunting, and forensics.



Use Cases

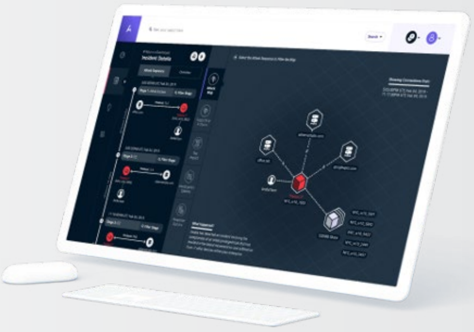
Detection
The platform uses AI to detect & prioritize mal-intent & behavioral threats from both insiders & outside attackers, while mapping these to the MITRE ATT&CK framework.

Response
Ava forensically correlates incidents across entities, time, protocols and attack stages, surfacing Situations with all the decision support data necessary to respond rapidly to any threat.

Situational Awareness
Awake learns & tracks entities across IT, OT or IoT environments whether they are on-premise, cloud or SaaS and managed or unmanaged including contractors and other third-parties.

Threat Hunting
The platform's rich data set and query capabilities enable powerful threat hunting workflows. Ava can take a single trigger from a human analyst and in a matter of minutes autonomously expose the entire kill-chain.

Figure 2: Key use cases Solved by Arista NDR



[1] https://awakesecurity.com/white-papers/tolly-test-report-darktrace-enterprise-immune-system-vs-awake-security-platform/

[2] https://www.arista.com/assets/data/pdf/Analysts/

Case Study: Tapping IP Phones in Sensitive Locations

Background:

A major consumer finance institution in the U.S. with more than 17,000 IP phones on its network used Arista NDR to determine that four of its phones were being electronically tapped by a trusted but malicious insider.

Challenges:

The organization's large security team struggled with visibility into the IP phones since existing security controls were blind to these devices. They also exist for the sole purpose of communicating with destinations outside the company, so large volumes of traffic being exchanged with external sources is not unusual. However, it was unusual that only a small number of phones were uploading data to a particular suspect destination every so often.

Solution:

To find this activity, the Arista NDR analytics did not simply compare the current behavior of these devices to what was observed in the past. In this case, the devices were compromised long before the Arista platform was deployed in the environment so a more basic anomaly analysis would have considered the malicious activity to look "normal" compared to what had been previously observed. Instead, Arista NDR first identified all of the devices with similar behavioral fingerprints and then compared these devices to each other. This allowed it to spot four devices that were outliers from the norm. Using encrypted traffic analysis the platform was able to profile the source and destination of the communication and factor that information into the threat assessment.

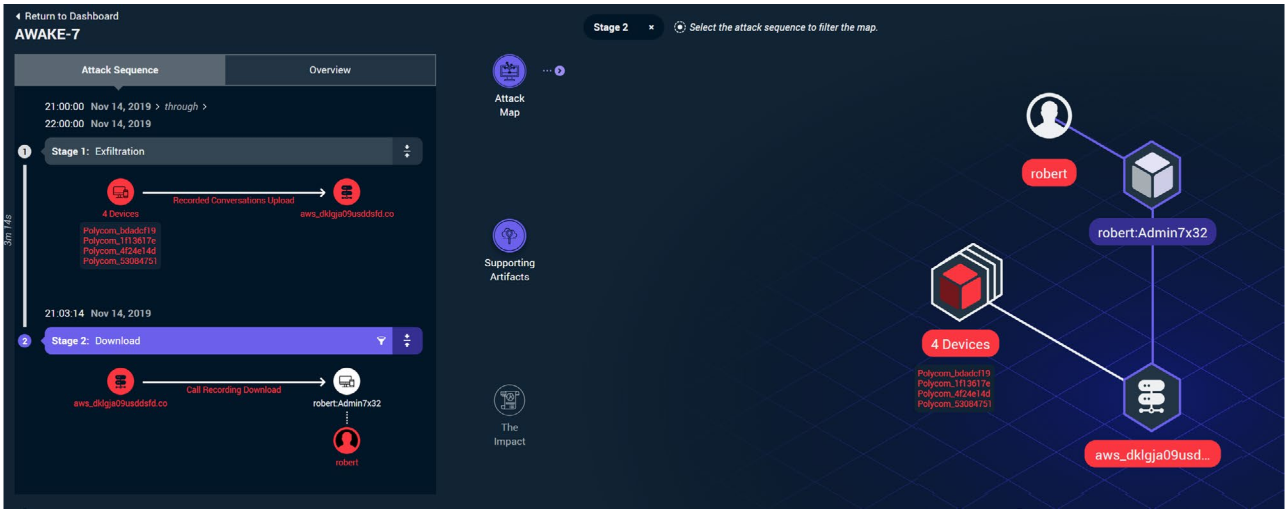


Figure 3: Arista NDR performs multi-stage analysis of an insider threat

Result:

The security team determined that an IT employee was responsible for this attack. He was attempting to use the information collected for extortion and ransom operations. The platform's analysis enabled the security team to quickly find the compromised phones which were stationed in executive conference rooms and other sensitive locations that were frequently the site of high-level and confidential company discussions. The detailed information gained from Arista NDR enabled the company to immediately stop the activity and gain evidence for legal action.

The Arista NDR Advantage

The platform profiles entities such as devices, users, and applications. And, like an experienced threat hunter, the platform models hunt for and visualize attacker tactics, techniques, and procedures. Arista NDR's ability to autonomously connect the dots across the dimensions of time, entities, and protocols enable the security analyst to get an understanding of the entire scope of the attack rather than just individual alerts. The analyst can then trigger relevant, investigation, and remediation options much faster and with more accuracy.

Better Data Sources ➔ Higher Fidelity Results

Arista NDR is built by security analysts for security analysts. The platform, therefore, focuses heavily on not creating busy work for the analyst. Unlike other platforms that trigger alerts and leave it to the security team to sort through them, identify which are real issues and which are benign or false positives, Arista NDR avoids flagging issues unless there is compelling evidence that indicates maliciousness. Core to this is ingesting as rich data as possible rather than just packet headers or NetFlow.

Other NDR solutions primarily process layer 3 and 4 metadata like protocol headers or NetFlow information, because full packet data through layer 7 is significantly more voluminous and harder to process in real-time. But that volume also means much more signal—signal that is useful to improve detection fidelity, track entities, and, perhaps ironically, actually help the solution scale to large and complex networks. For instance, signals like the user information available in Kerberos packets wouldn't show up in protocol headers or NetFlow. Full packets also allow you to understand and store the activity record, the actual transaction occurring between the entities on the network rather than somewhat meaningless protocol bits and bytes. This forensic data allows the platform and investigators to go back in time and retrospectively detect behaviors that may not have been recognized as being malicious when they first occurred. Importantly, this activity record is also significantly smaller in storage footprint than the full packet data.

With the AVA Sensor on the Arista campus switches, this analysis can be performed even closer to the original devices and has the advantage of observing non-NATed traffic, the source IP address, etc. This deep packet inspection capability on the leaf switch can therefore detect lateral movement, credential abuse, and other such East-West threats far more effectively than network security devices placed at perimeters that are often multiple hops away from the real activity. And just as importantly, Arista's ability to deploy on the campus switches provides NDR capabilities without any additional network security hardware deployments, thereby decreasing operations costs and effort.

Integrations

Arista NDR integrates with and amplifies existing solutions through integrations into industry-leading SIEM, business intelligence, ticketing and analytics, endpoint detection, and security orchestration tools. In addition, the platform supports a full API for custom workflows and integrations. For instance, the SIEM integration allows an analyst to pivot from an alert containing an IP or email address to a device profile with the associated user(s) and roles, operating system and application details, a forensic threat timeline as well as a listing of similar device(s) for campaign analysis. Similarly, endpoint integrations allow for one-click quarantining of compromised devices or retrieval of endpoint forensic data.

Advanced Data Science

Legacy data science approaches run into some significant challenges given the scale and diversity of the modern network. Any artificial intelligence (AI) model is only as effective as the labeled samples used to train it. However, volumes of data and the types of conditions on even the simplest of today's networks make effective labels scarce. In addition, given how aspects such as threats evolve rapidly, the labels themselves become obsolete quickly, requiring frequent retraining and operational costs entailed in that effort. Even if these challenges are overcome, the resulting models are often massive, monolithic, and opaque, making them less useful, as they are slow and not explainable. In other words, a human analyst seeing the result often has no idea why something is flagged as a network or security issue. Consequently, they have no idea what they should do next given the information at hand.

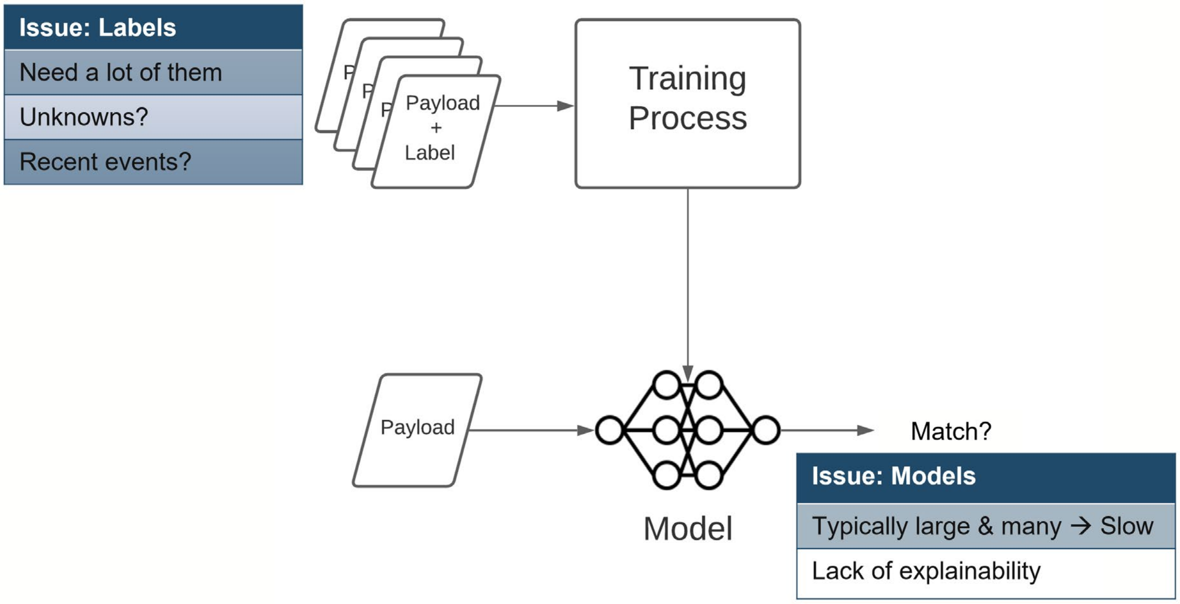


Figure 4 : Challenges to Traditional Artificial Intelligence Approaches to Network Security

Competitive solutions rely primarily on unsupervised learning to spot anomalies from "normal" baselines. However, anomalies often are not malicious resulting in false positives and conversely pre-existing compromises are missed because they are assumed to be "normal." These false negatives are even more dangerous because security teams unknowingly live with the risk.

Instead, Arista NDR starts by learning what is normal and, dare we say, mundane for each network. In most cases, this includes traffic such as email, patching, and even department or workgroup-specific application usage. There is an abundance of labels to train the AVA models to find these kinds of network behaviors. Unlike the legacy approach described above which attempts to learn what "bad traffic" looks like, Arista NDR works to eliminate much of the hay from the proverbial haystack of network data. This, in turn, leaves a significantly smaller consideration set within which the platform can then look for the needles.

Arista NDR helps identify and pinpoint behavioral anomalies of entities when the behavior changes over time. The platform does this without relying on a one-time "training" static snapshot, but by continuously learning what is "normal." This unique approach to data science overcomes the challenges with prior generation approaches. First and foremost, is the knowledge graph or EntityIQ™. The data the platform consumes is first processed with techniques that convert packets into people, or IPs into devices, applications, etc. EntityIQ also maps the relationships between them. This forms the core of the knowledge graph. The graph can then be enhanced iteratively by knowledge from domain experts in the form of heuristics, as well as ongoing feedback from human operators. Given the size of the knowledge graph is significantly smaller than the raw features, additional AI approaches can be applied iteratively. This not only allows for better AI analysis but, unlike traditional ML models, with Arista NDR, the algorithmic outputs are captured as real-world entities and their properties. The human-readable and understandable outputs deliver explainable AI with clearly defined next steps for the analyst.

Arista considers artificial intelligence a means to the end: improving customer security outcomes, in this case. The platform, therefore, uses a variety of data science methods towards this end goal. These include:

- a combination of unsupervised supervised, and federated machine learning algorithms including deep neural networks for classification e.g., identifying malicious and suspect domains,
- decision tree for classification e.g., with encrypted traffic analysis,
- multi-dimensional clustering for entity tracking,

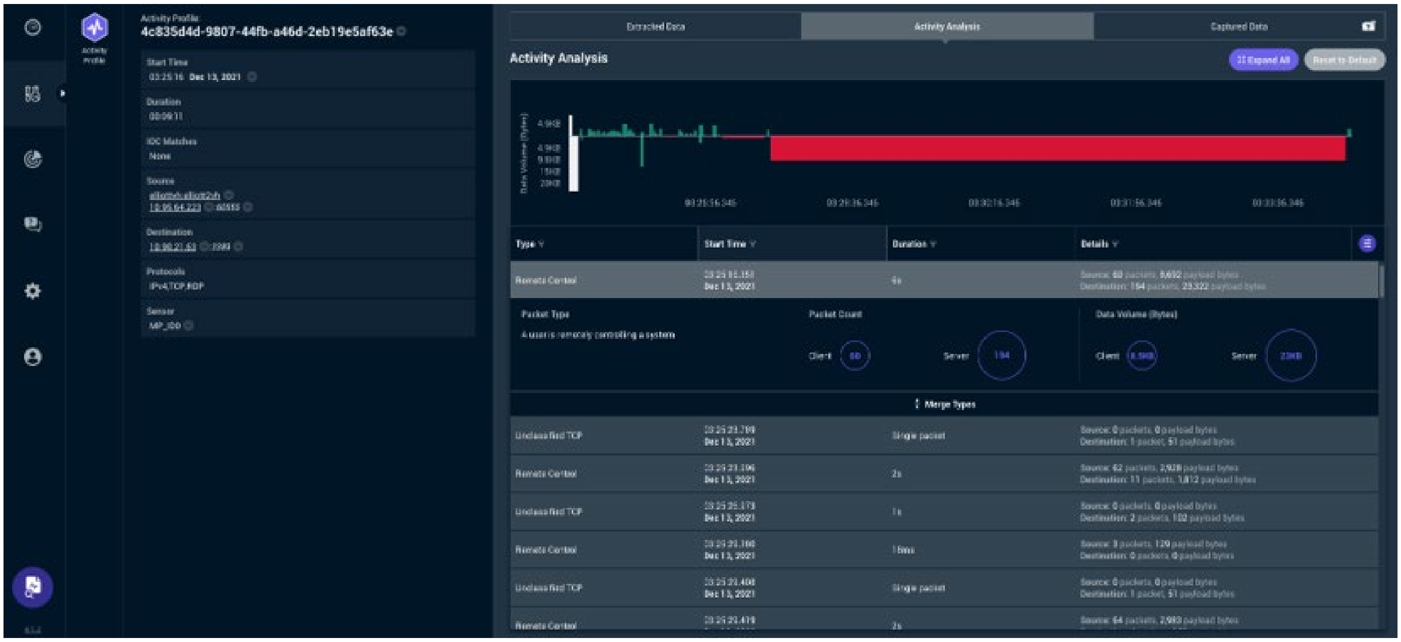
- outlier detection for spotting anomalies,
- belief propagation for risk scoring, and
- topic modeling and natural language processing to automatically perform open-source intelligence and threat research in much the same way as an expert human investigator does.

Machine Learning for Encrypted Traffic Analysis

Network traffic is these days encrypted for the most part and organizations are increasingly hesitant to decrypt it due to the policy and privacy implications involved. For instance, with TLS 1.3 it is harder to rely on traditional methods of intercepting and decrypting network traffic. Attackers are also increasingly using encrypted traffic as a way of evading network detection. In fact, as per Gartner, over 70% of malicious traffic is now encrypted.

Arista NDR uses data science to perform encrypted traffic analysis, thus working within privacy and policy constraints while also ensuring security teams do not have to fly blind. Some of the use cases include identifying applications that are communicating, as well as the nature of the traffic that is going over the wire. For example, it might not be of concern when an encrypted file is transferred over a web conference meeting session, but if that file is transferred from a PowerShell script to a non-sanctioned external location, it might be more concerning.

To enable encrypted traffic analysis Arista NDR uses a variety of data science techniques. For instance, supervised ML is used to identify patterns of activity that relate to attacker TTPs e.g., identifying remote access tools, reverse shells, unauthorized applications used for command and controls; identifying domains being used for data exfiltration, etc. even when the domain has no or a good reputation. The platform also uses deep neural networks and decision trees for classifying encrypted sessions based on the nature of traffic such as an interactive shell session, web browsing, video conferencing, file transfers.



Activity Profile
4c835d4d-9807-44fb-a46d-2eb19e5af63e

Start Time
03:25:16 Dec 13, 2021

Duration
00:09:11

IOC Matches
None

Source
elliottvh.elliott2vh
10.95.64.223 : 60555

Destination
10.90.21.63 : 3389

Protocols
IPv4,TCP,RDP

Sensor
MP_100

Activity Analysis

Type	Start Time	Duration	Details
Remote Control	03:25:15.158 Dec 13, 2021	6s	Source: 60 packets, 8,602 payload bytes Destination: 194 packets, 23,322 payload bytes

Packet Type
A user is remotely controlling a system

Packet Count
Client 60
Server 194

Data Volume (Bytes)
Client 8.5KB
Server 23KB

Type	Start Time	Duration	Details
Unclassified TCP	03:25:23.799 Dec 13, 2021	Single packet	Source: 0 packets, 0 payload bytes Destination: 1 packet, 51 payload bytes
Remote Control	03:25:23.396 Dec 13, 2021	2s	Source: 62 packets, 2,928 payload bytes Destination: 11 packets, 1,812 payload bytes
Unclassified TCP	03:25:25.173 Dec 13, 2021	1s	Source: 0 packets, 0 payload bytes Destination: 2 packets, 102 payload bytes
Remote Control	03:25:23.160 Dec 13, 2021	16ms	Source: 3 packets, 129 payload bytes Destination: 0 packets, 0 payload bytes
Unclassified TCP	03:25:23.408 Dec 13, 2021	Single packet	Source: 0 packets, 0 payload bytes Destination: 1 packet, 51 payload bytes
Remote Control	03:25:23.419	2s	Source: 64 packets, 2,983 payload bytes

Figure 5: Encrypted traffic analysis identifies unauthorized remote control via the Remote Desktop Protocol (RDP)

Human Expertise on Demand

Arista's Awake Labs offers comprehensive security strategy, operations, and advisory solutions focused on an organization's unique security resilience and incident response needs. This team of practitioners has more than two hundred years of collective security experience, including responding to some of the most significant breaches in the world as well as speaking and delivering training at some of the biggest security conferences. Customers who engage with Awake Labs thus directly benefit from a unique combination of hands-on incident response skills, executive management experience, and strategic business acumen.

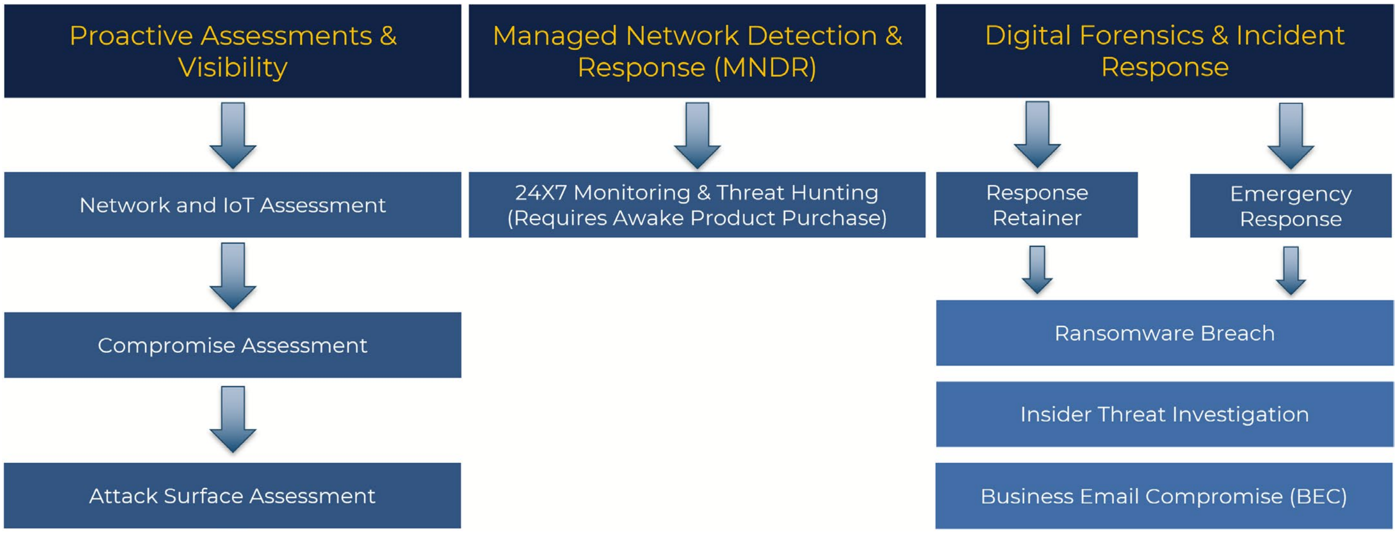

Proactive Assessments & Visibility
Managed Network Detection & Response (MNDR)
Digital Forensics & Incident Response
Network and IoT Assessment
24X7 Monitoring & Threat Hunting (Requires Awake Product Purchase)
Response Retainer
Emergency Response
Compromise Assessment
Ransomware Breach
Insider Threat Investigation
Attack Surface Assessment
Business Email Compromise (BEC)

Figure 6: Human expertise to support customer needs such as incident response and managed threat hunting

This team offers proactive network-oriented security assessments to help organizations understand their attack surface, assess their readiness for a potential breach, and determine if they have already been compromised. With many years of frontline incident response experience, these experts can help mitigate and contain the impact of breaches ranging from ransomware, insider threat, and business email compromise. Finally, Awake Labs also offers a managed NDR service that provides 24x7 monitoring and threat hunting.

Engaging with Awake Labs helps customers improve their risk posture with proactive threat hunting and monitoring across the core, perimeter, cloud, IoT, IT, and OT networks. It helps reduce the cost burden of hiring and retaining skilled resources with niche security expertise, while at the same time enabling the existing team to focus on the organization's primary business while Awake Labs prioritizes threats targeting their critical assets. With access to industry-leading playbooks for network investigations and remediation and expertise on demand, customers can reduce ongoing costs of security operations as well as mitigate impact.

Multi-Disciplinary Innovation Drives Better Customer Security Outcomes

Arista views innovation through a few different lenses when it comes to the NDR platform. The first lens is focused on applying the artificial intelligence built within the platform to a wider variety of data sources e.g., data from operational technology devices, cloud, and SaaS applications. This delivers on the promise of detection and response for all digital assets, no matter where they are.

Of course, data is only as good as the data science applied to it. As discussed above, Arista has already broken much new ground on the application of data science to security. The company however continues to invest in areas such as encrypted traffic analysis, lightly supervised models, natural language processing, and topic modeling. These approaches allow the platform to further augment the customer's human analysts by eliminating both mundane tasks and those that require an elevated level of skill. Instead of focusing on data gathering and analysis, these analysts can focus on decision making.

Arista's AI-driven approaches are also centered on the evolution of attacker tactics, techniques, and procedures. Innovations such as adversarial modeling detect core elements of attacks and identify these before they become headline news. This allows customers to quickly identify, understand, contain, and remediate incidents and thereby reduce breach impact. To achieve this goal, Arista also invests heavily in a threat research team that is constantly staying in sync with evolving attacker tactics.

Finally, innovation on the user experience is a major focus. Arista recognizes that a level 1 or junior analyst uses security technology very differently from how a Level 3 analyst or threat hunter does. Given that mindset, the company continually innovates on role-specific user experiences and workflows. Rather than simply dumping data for the human to make sense of the platform presents storyboards and dashboards that keep the user's perspective and needs in mind.

Summary

Arista NDR offers a unique combination of AI-driven technology along with access to human security experts if and when you need them. This platform helps identify threats including the early warning signs of ransomware, supply chain, IoT attacks, and insider attacks. By delivering the context necessary to respond, Arista NDR also enables speedy and effective remediation. Perhaps just as importantly, these capabilities can be delivered through the existing Arista switching fabric, thus reducing operational burdens on IT and Security teams.

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