Intelligent Observability and Security Operations with Arista DANZ Forensic Exchange

Document Version 1.0

Introduction

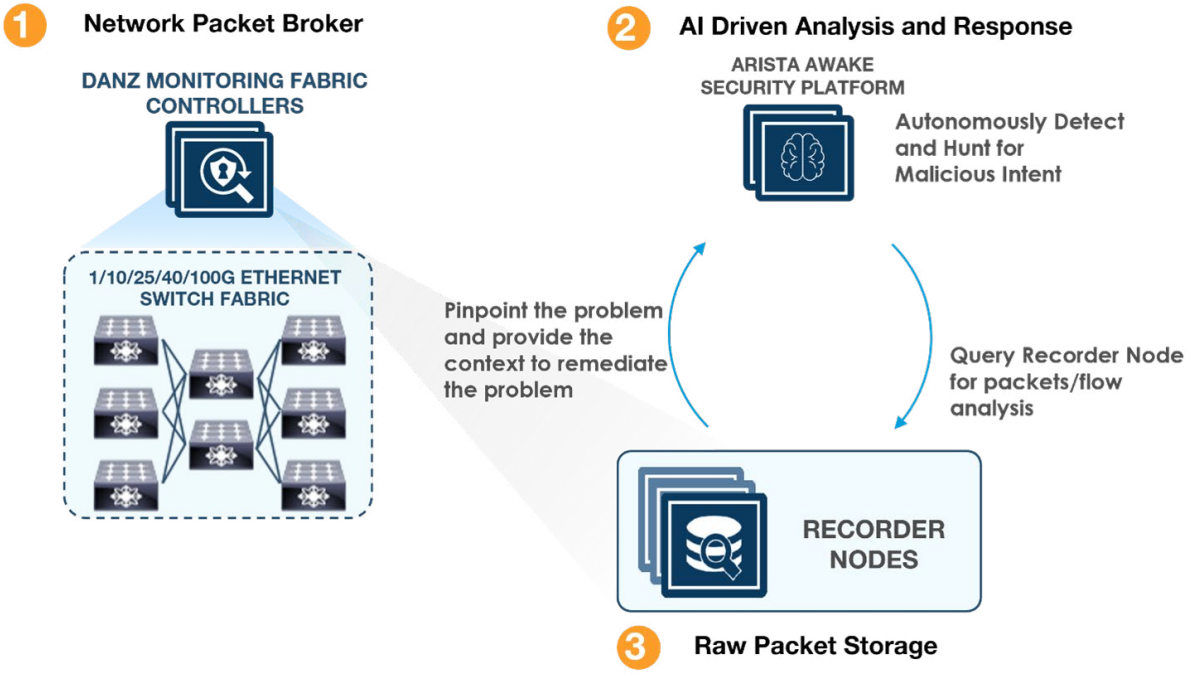
Over the last decade organizations have transformed their digital infrastructure, a trend that certainly accelerated during the COVID pandemic-related "work from anywhere" trend. This has resulted in networks that have expanded both in terms of the type and nature of devices and connectivity, but also architecturally as traditional perimeters are no longer meaningful security boundaries. Additionally, continuous cyberattacks seen in recent years have driven enterprises towards a zero-trust architecture. Traditional network monitoring, threat detection and response tools simply do not scale and have not kept up with these modern challenges. Legacy offerings rely on all or nothing approaches that offer limited ability for customers to curate the visibility based on their own risk profile. They are restricted in their ability to scale, lack autonomous (AI/ML-driven) intelligence for fine-grain threat detection and tend to be cost (capex and opex) prohibitive for enterprise-wide deployment. As a result, organizations are increasingly blind to much of this "new network" and the attack surface that it represents.

Arista's DANZ Forensics Exchange (DFX) solution provides (enterprise-wide) observability, detection, and response for the new network. This scale-out solution is delivered in a variety of form factors so organizations can monitor on-premise, hybrid and cloud-based infrastructure. Specifically, for enterprise data centers, the DFX solution's scale-out architecture applies to user-to-app (north-south) as well app-to-app (east-west) traffic, latter requiring up to 5X amplification of traffic. As data center networks transition from 10G/40G to 25G/100G link speeds, DFX's high-performance design supports all bandwidths and is architecturally ready for the upcoming 100G/400G speeds. Further, the network protocols and systems to be monitored can easily be curated to the "just right" set for the organization. This allows the system to provide comprehensive coverage for both present and past events while ensuring it delivers manageable decision support data for the organization's analysts. As a result, both up front costs of deploying the solution and ongoing operational costs are kept to a minimum.

The DFX solution supports a wide variety of end-user use cases from network performance monitoring and AI-ops to AI-driven threat hunting, detection and response, all from a single vendor solution. Arista's open and documented API as well as out-of-the-box integrations can help deliver these benefits to other parts of the IT infrastructure and automate actions that today require significant human involvement. Finally, customers have the option to engage Arista's Awake Labs team for 24x7x365 monitoring of the solution, threat hunting and incident response expertise.

Solution Architecture

Digital transformation, in today's landscape, is key to an organization's competitive advantage. As organizations have embarked on this digital transformation journey, it has led not only to an exponential growth of their datacenters' size, bandwidth and traffic, but also uncovered a paramount need for pervasive network observability to ensure performance, security and integrity of their datacenters. As security threats continue to increase, ensuring application performance meets the needs of the business is critical.



Organizations, especially those that operate their own data centers and / or host their own SaaS applications struggle with visibility into:

- The scale of enterprise-wide traffic (including high performance DC east-west app-to-app traffic);
- High performance network link speeds, including 40G/100G and emerging 400G;
- The services and applications running on that infrastructure, and;
- The protocols used to communicate within and to / from the infrastructure, and;
- The users, devices and applications accessing the infrastructure.

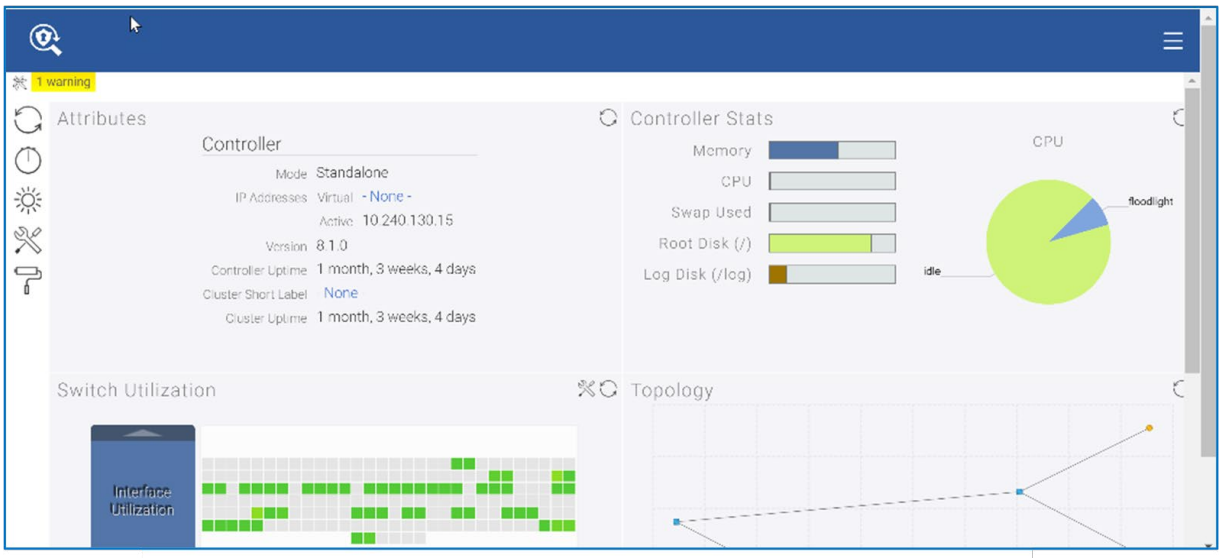
The DFX solution combines the network packet filtering, forwarding and storage capabilities of the DANZ Monitoring Fabric (DMF) with the advanced Network Detection and Response (NDR) capabilities of the Arista NDR Platform powered by AVA. DFX provides a scalable and flexible solution that delivers visibility at the network, device, workload, application and user level, while also enabling autonomous threat hunting, detection and response. The solution is highly programmable, allowing the organization to monitor only what is most appropriate for their needs e.g. monitoring east-west traffic within a data center.

Only Arista offers a single solution with individual best of breed components that can curate the appropriate data set to support observability, compliance, forensics and threat detection and response use cases. The solution can span on-premise, cloud and hybrid-cloud networks and consolidate multiple tools currently deployed within the environment. Arista's managed services deliver expertise from individuals that collectively have hundreds of years of experience, including responding to some of the world's most consequential breaches.

Modern data centers require intelligent, agile, flexible and secure monitoring architecture that provides a single pane of glass management, zero-touch scale and automation. The DFX solution achieves these with Zero Touch Networking (ZTN), which automatically discovers all switches and Recorder Nodes. No user configuration is required on switches.

Network traffic is monitored from a large range of sources including switch SPAN ports (Arista and others), network taps, sFlow IPFIX and virtual environments. The DMF Controller maintains and distributes policy-based forwarding configurations to the infrastructure components enabling centralized control and monitoring of desired traffic at a granular level to both the Awake Nucleus (central security analytics node) and the DMF Recorder (scalable intelligent packet storage). Real-time traffic is forwarded directly from the switch to the Nucleus which deeply analyzes billions of network communications to discover, profile & classify every device, user & application using an AI-driven approach. The Recorder Node stores data provided by the infrastructure under control of the policies distributed by the DMF controller.

The Nucleus is directly integrated via API to the Recorder Node(s) enabling storage and analysis of long-term full packet data for compliance reporting and threat hunting. This allows for packets analyzed by the Nucleus to be stored within DMF and retrieved on-demand and in the context of a threat or entity the analyst is investigating. Additionally, the Nucleus supports integration with a wide range of network and security infrastructure such as SIEMs including Splunk and QRadar, EDR solution from Sentinel1 and CrowdStrike etc. for attack containment and mitigation.



Programmable Observability – The DMF Controller

DFX Solution Components

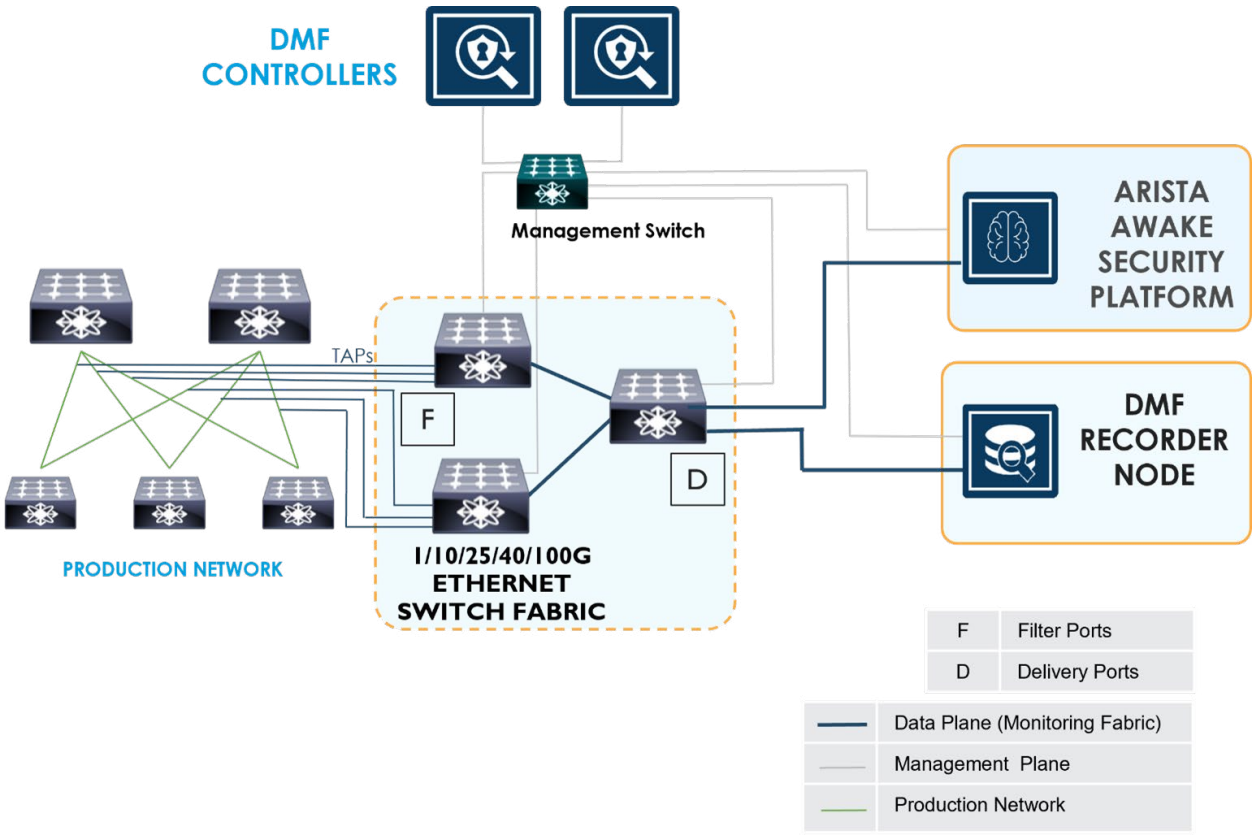
The DFX solution consists of the following components:

- DMF Controller and switch licenses
- DMF Recorder Node (plus optional Service Node and Analytics Node)
- AVA Nucleus

Hardware and Software Options

Following are the hardware and software components used in this solution:

Component	Hardware/Software
DMF Controller	Hardware Appliance or VM Software
Recorder Node	Hardware Appliance
Ava Nucleous	Hardware Appliance (licensed by Mbps analyzed)

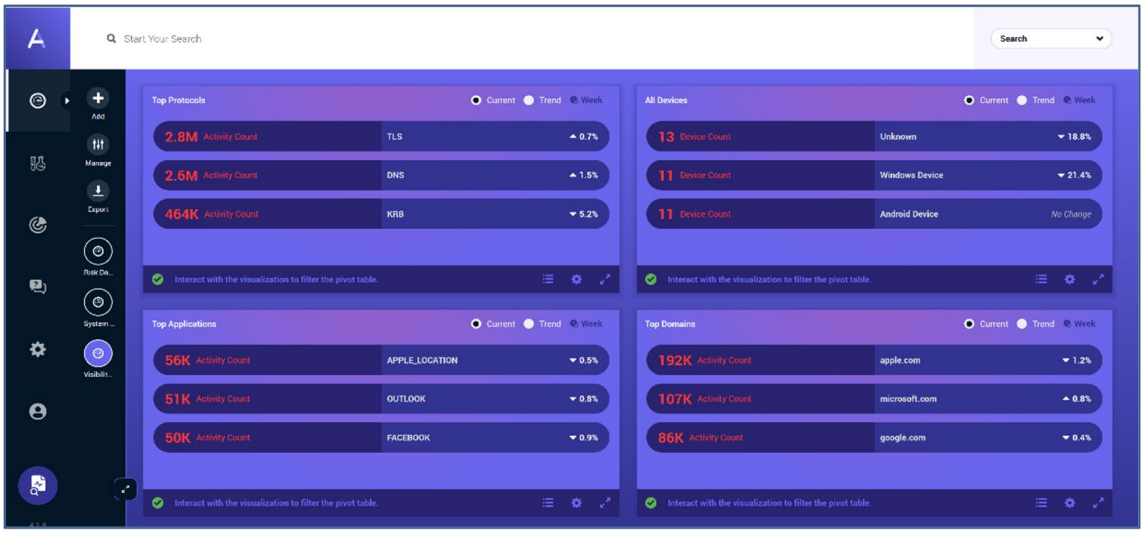


In this solution guide we will focus on the operational workflow from raw network data to visibility through security analysis. The DMF controller is responsible for defining, distributing and monitoring the traffic filtering and forwarding policies for the network fabric. This is how operators can account for the organization's threat model and accordingly ensure once the appropriate traffic is flowing from the network through the monitoring fabric and to the AVA Awake Nucleus.

Workflow

Network traffic is a dynamic and ever-changing mix of devices, users, IP address, applications, services and workloads communicating with a myriad of destinations, internal and external. The Awake Nucleus analyzes, correlates, and integrates all of these elements automatically and presents the results in an easy to digest format.

The Arista NDR Dashboards offer a customizable view of the data that is most important to the operator and provides numerous "widgets" that can be selected and arranged to suit each individual's or groups' needs. The dashboard represents the starting point for the typical operator's visibility workflow. For instance, IT operations pro's typically monitor the network to ensure availability and compliance with industry and organizational policies.

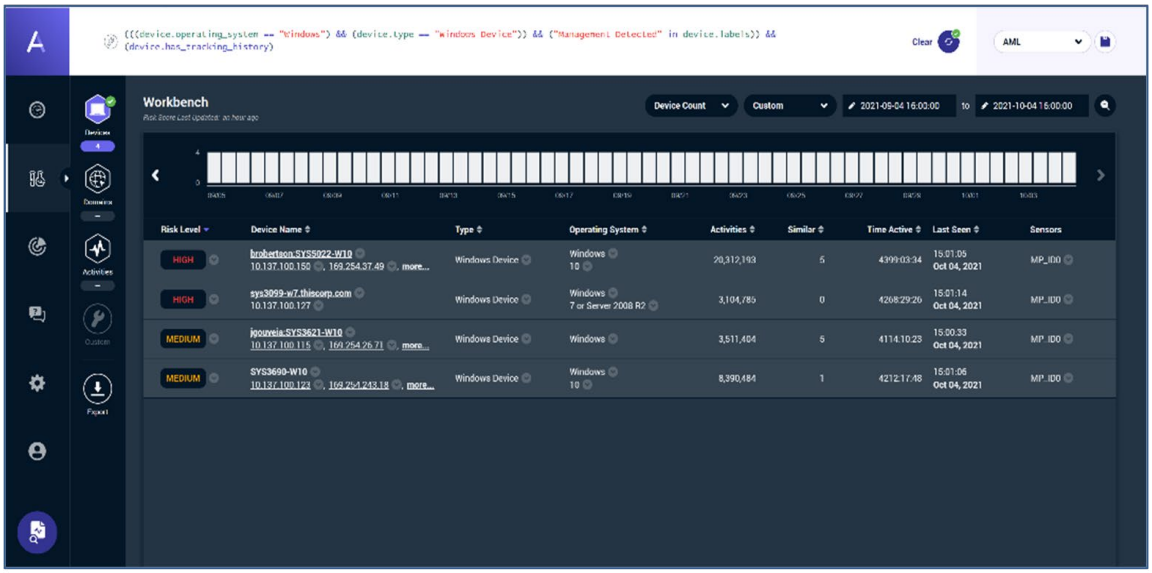


Nucleus Custom Interactive "Visibility" Dashboard

The advanced AI engines within the Nucleus correlate and track all the key elements an organization's IT Ops team needs visibility into. The hierarchical displays provide full drill-down capability ultimately to the packet itself from which the data originated. Changes in the levels of activity associated with a protocol, application etc. are also automatically calculated and displayed enabling the operator to observe trends and spikes in activities that may indicate problems within the network or variance from policy occurring and take appropriate action to further investigate or remediate problems as described later in this solution guide, operators can also build custom models to alert them to changes like these automatically.

DFX uses an advanced fingerprinting technique to determine which devices are actively managed by applications such as Endpoint Detection and Response (EDR) agents or Endpoint Protection Platforms (EPP). Reports can then be created that enable the team to track compliance with a wide range of elements such as applications, operating system versions, domains and protocols in use, the percentage of managed devices etc.

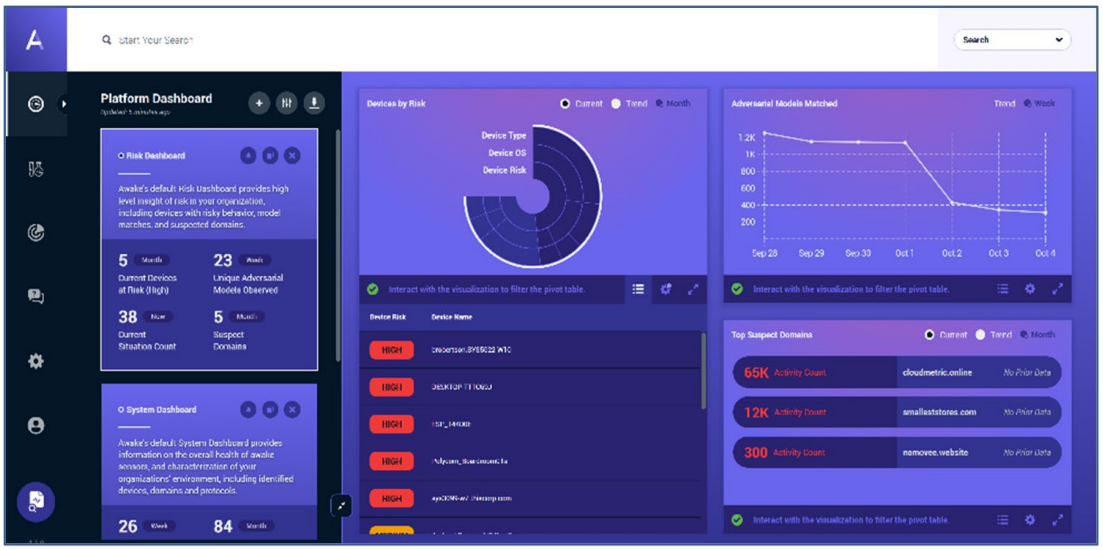
Having the solution pre-compute these values reduces the amount of time and effort needed for these routine, but important tasks and enables easy correlation of IT policies with security risks. A common view of important network data optimized for use by both the IT and Security ops teams allows for a seamless workflow as policy violations are often precursors of future security events.



"Managed Devices" Interactive View

Threats detected autonomously by the system are tracked, weighted and displayed on the Risk Dashboard. This provides the security operator with "at a glance" visibility into new threats detected that are prioritized automatically by the system thus enabling the team to address the most pressing issues first.

Pivoting from the dashboard to the Devices at Risk display is a common next step in the workflow when evaluating a new threat detected by the system. The operator can continue directly to explore the details of the new alert via the EntityIQ engine which displays current and historical information correlated automatically by the system. Alternatively, the analyst can manually create a new Situation which instructs the AVA AI to initiate an automated investigation by expanding and correlating additional context and tracking of the entity's activities e.g. are there other victims within the organization, what is the set of attacker infrastructure being used in the threat etc.



Threat Detection – The Risk Dashboard

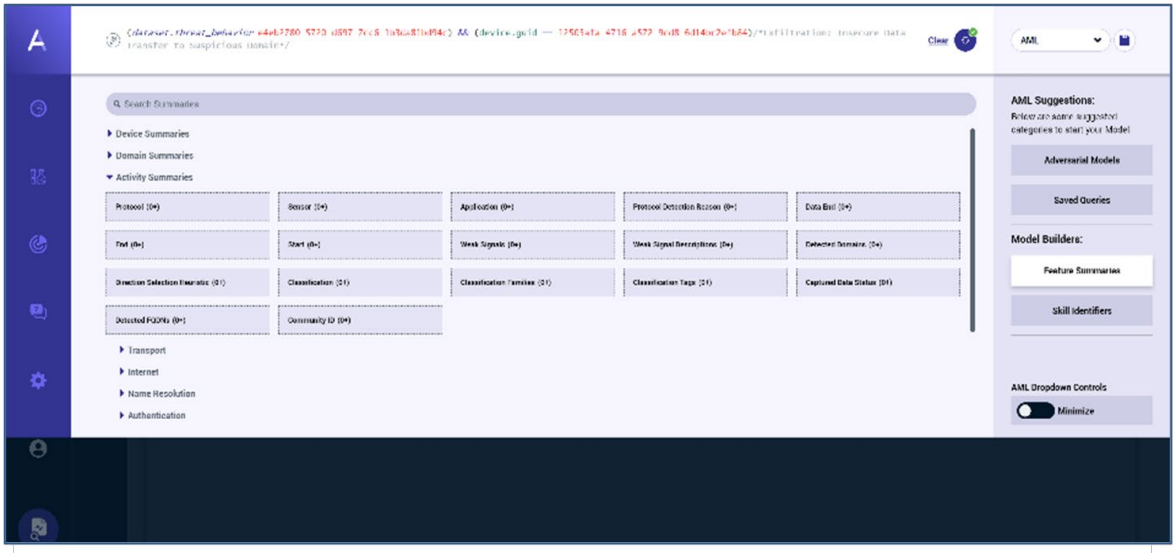
Incidents that have been detected and are being remediated or investigated are tracked using the AVA AI powered "Situations" display. "Situations" expand, correlate and track all aspects of a detected attack and provide guidance for the operator to maximize their effectiveness and efficiency. In parallel, AVA continues to autonomously work on the Situation in the background, adding additional context and data over time as it becomes available.

AVA powered "Situations" – Autonomous Attack Workflow

Guidance on additional research options and detailed remediation steps are provided by the system. Responses to attacks, such as isolating a compromised system via an EDR agent, re-segmenting the affected device to a quarantine subnet etc. can be performed either manually by the operator or programmatically via integrations with ticketing or orchestration tools.

Programmable Threat Detection

Organizations often need to proactively hunt for indications of an unknown attack or data breach when new information becomes available. This can include newly discovered CVE vulnerabilities, threat actor techniques or indicators of compromise. On the other hand they might want to look for network behaviors that are threats unique to their environment or violations of corporate policy. For instance, a DFX customer in the retail space uses this programmability to audit and log all access from outside of a whitelist of devices and users to their PCI enclave. The Adversarial Modeling Language (AML) enables operators to initiate advanced, in-depth threat hunts without the need for years of advanced training or extensive knowledge of machine learning and data science.



The AML "Point and Click" Model Builder

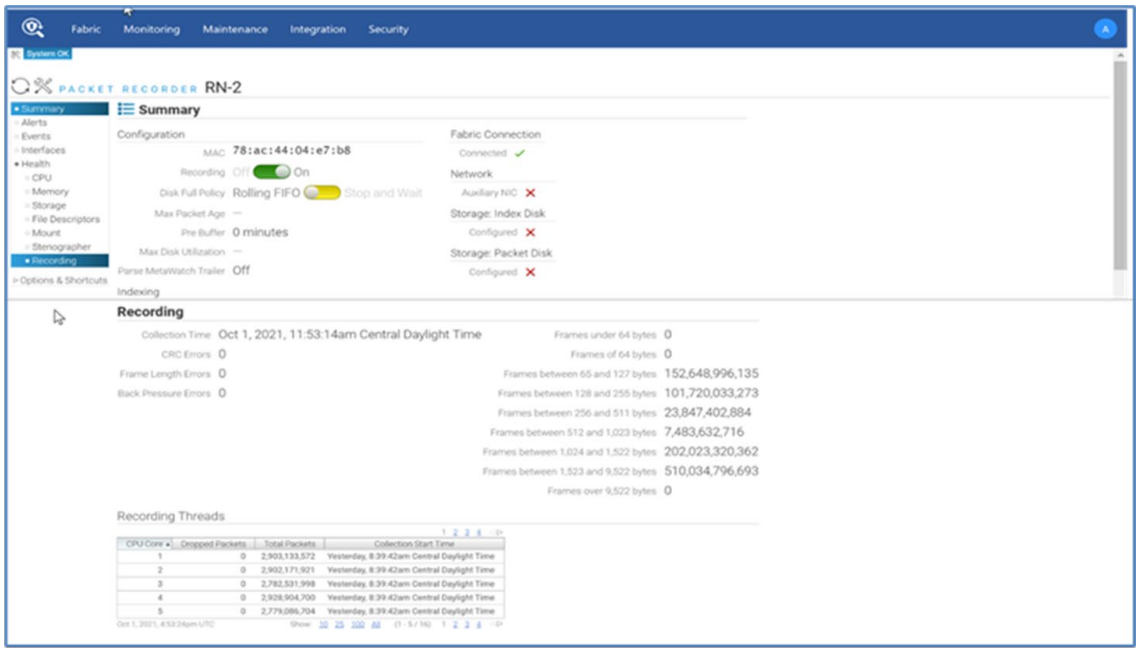
The AML extends and harnesses the autonomous AI engines within the Nucleus to search for relationships and activities between entities located both on and outside of the network. The AI engines automatically precompute and store data that can then be accessed by a simple "point and click'' interface which builds powerful threat hunting models from modular and reusable "recipes" provided within the product.

For instance, analysts can easily compose hunts for sophisticated threat actor behavior without having to become an expert in every lateral movement or credential abuse technique. These new threat hunting queries can be saved and added to the ongoing detection capabilities of the Nucleus, ensuring that the entire organization benefits from the tailored workflows. In other words, when one of these custom threats are discovered all of the elements described above from dashboards to Situations are updated much like they are for out of the box detections.

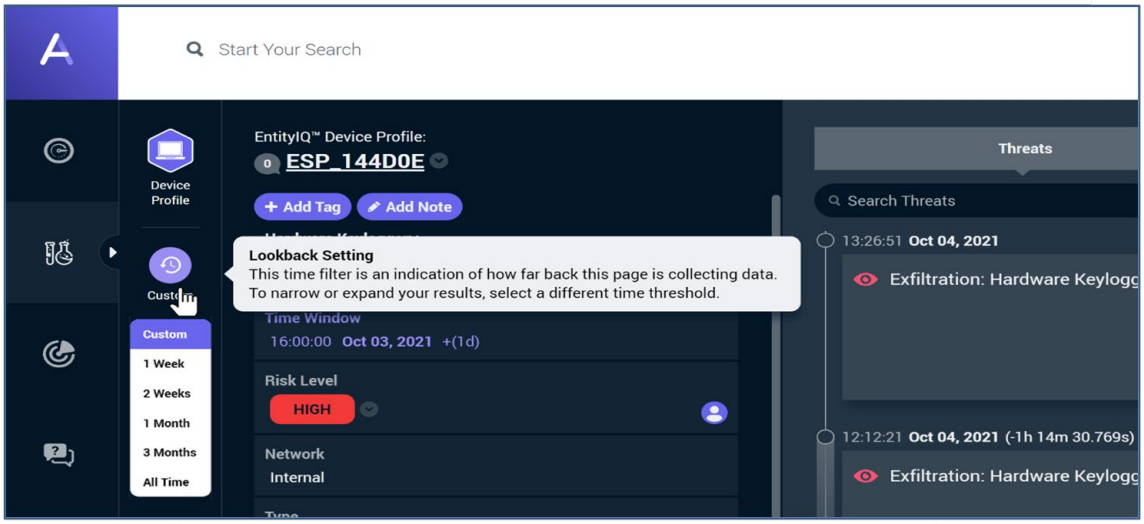
Compliance and Forensic Investigations

In highly regulated environments, organizations are required to maintain historical network records that act as an audit trail or to enable investigative use cases. For instance, FFIEC and NY DFS regulations mandate the need for forensics in the context of cyber incident response for threats ranging from ransomware to insider attacks. Traditional network forensic systems are complex to deploy, cumbersome to use and have high upfront as well as day to day operational costs. Leading vendors often attempt to lock in customers into long term contracts and proprietary storage. Customers see little ongoing utility of these systems, other than checking a compliance need, or in the few occasions when they need the forensic data.

The DFX solution provides rich network forensics with extensible storage, time machine and replay capabilities. In addition, the solution provides ongoing value beyond historical forensics with support for autonomous network monitoring, threat detection and response. The solution is designed to be accessible to even relatively junior analysts but customers can also benefit from a team of Arista experts that perform 24x7x365 threat monitoring, hunting and incident response on behalf of the customer.



DFX Recorder Node – Simple, Scalable Packet Storage



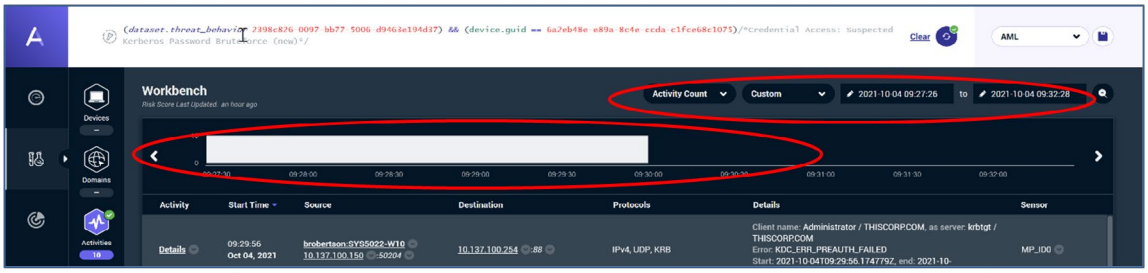
EntityIQ High Level Lookback Settings

This in turn saves the customer the cost of building or expanding their in-house expertise. The extensibility of the platform allows for the creation of custom compliance models that can automatically hunt for regulatory issues and provide alerts that can meet audit requirements. Customers can also use the solution for non-cyber security purposes such as human resource investigations.

DFX offers a simple, but powerful workflow for historical compliance and forensic analysis requirements faced by organizations today. Every entity on the network is analyzed and tracked over time by the powerful EntityIQ engine in the Nucleus. EntityIQ functions as the authoritative source for both historical compliance activities and for forensic analysis of past actions and behaviors.

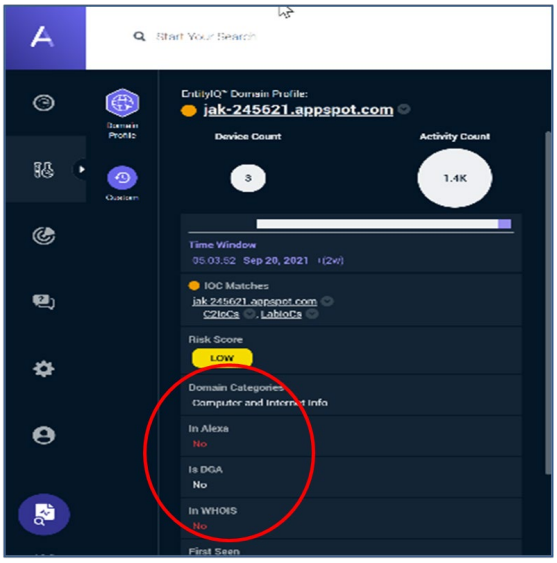
EntityIQ is transparently integrated with the DMF recorder via an API ensuring context-sensitive and quick access to the full packet store maintained by the fabric. A full suite of forensic tools is integrated into the EntityIQ engine to provide a "single pane of glass" view for the security analyst and standardization of tools across the security team.

EntityIQ provides predefined lookback intervals for the operator to select from. Extremely precise time intervals can be defined by the analyst to speed time to resolution and eliminate unwanted background noise when performing analysis of historical events. The activity time line enables the analyst to visually determine what time period is of most interest and retrieve just the packets associated with their analysis.



Detailed Lookback Settings and the Activity Timeline

There are a number of forensic tools integrated directly into the Nucleus such as the "Whois" domain lookup tool, the "Alexa" domain ranking system, and the "DGA" or Domain Generated Algorithm list and the category type for the domain. Additionally, packets may be exported for analysis by customer created and assembled tools via the user interface or API . These tools reduce the overall time required for the forensic research workflow.



Integrated Forensic Tools

Summary

The Arista DFX solution delivers advanced programmable monitoring and detection to streamline the visibility and threat monitoring workflow across the IT and security operation teams. Zero Touch deployment and the unique capability of scaling to hundreds of gigabits per second delivers the quickest time to value available on the market today. DFX offer a complete, integrated end to end solution with programmable policy-based packet filtering, scalable packet storage and advanced compliance, threat detection, and custom "point and click" threat hunting in a comprehensive platform from an industry leader in networking and security.

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