# Arista Zero Trust Security for Cloud Networking

A new age of edgeless, multi-cloud, multi-device collaboration on hybrid work models has redefined global frontiers and the enterprise threat landscape. As hybrid work models continue to thrive, enterprise data are increasingly exposed to a growing attack surface and newer threats every day. Additionally, with the use of BYOD, IoT devices, and cloud apps becoming the norm, enterprises have a massive increase in the number of unmanaged assets and reduced visibility into their true attack surface.

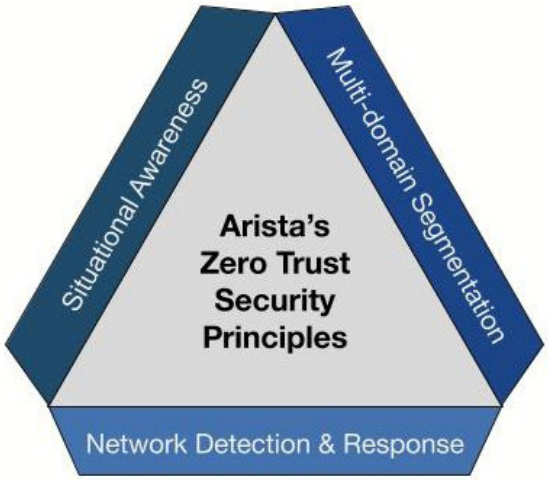
This paradigm shift has prompted best-in-class enterprises to bake security into the core of their network infrastructure. Implementing security at this layer reduces operational costs and complexity and represents the most effective way to track and successfully manage threats coming in from the wider attack surface.

This white paper discusses the Arista Zero Trust Security architecture. Based on NIST 800-207, the Arista approach delivers situational awareness, segmentation, enforcement, and continuous diagnostic and monitoring, which are key to an effective defense against today's complex threats.

# Table of contents

## Introducing Arista Zero Trust Security

A zero trust networking approach to security is paramount for organizations looking to build a robust cybersecurity ecosystem today. Based on the premise of explicit trust, zero trust security ensures complete visibility and control over any enterprise network activity, regardless of which device, application, or user is accessing that resource. This approach avoids the concept of trust inside the network that connects to an untrusted network through a traditional firewall. It also eliminates the implicit trust associated with network location and instead places the onus on continuously monitoring all device and application access for mal-intent and then responding quickly. The Arista Zero Trust Networking architecture is patterned on the NIST guidance in the 800-207 framework and leverages these fundamental pillars.




**Zero Trust Framework**

- Situational Awareness → Visibility of all assets & workloads
- Enforcement → Restrict access to required connections
- Continuous Monitoring → Never trust continually verify

**Zero Trust Assumes**

- Successful authentication is not sufficient
- Device and User visibility beyond simple fingerprinting
- Client agents are not possible with many IoT devices

Adapting each pillar is dependent on the security administrator's specific requirements and leverages the integration with Arista partners, a portfolio of best-of-breed Arista switches, CloudVision network automation, and telemetry, the Arista network detection and response (NDR) platform, and the Arista DANZ Monitoring Fabric (DMF). Notably, the Arista solution uses open standards, recognizing that all networks are composed of products from multiple vendors.

1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

## Zero Trust For All Networks

Arista helps customers build networks that are adaptable and secure by design. Arista's zero trust portfolio eliminates the need for several network monitoring and security tools by delivering a unified architecture that provides real-time visibility to the threat posture across the network and the ability to take action. Arista is uniquely positioned to deliver these capabilities across a variety of networks: from the campus to the data center and the cloud.

**Zero Trust for the Data Center**

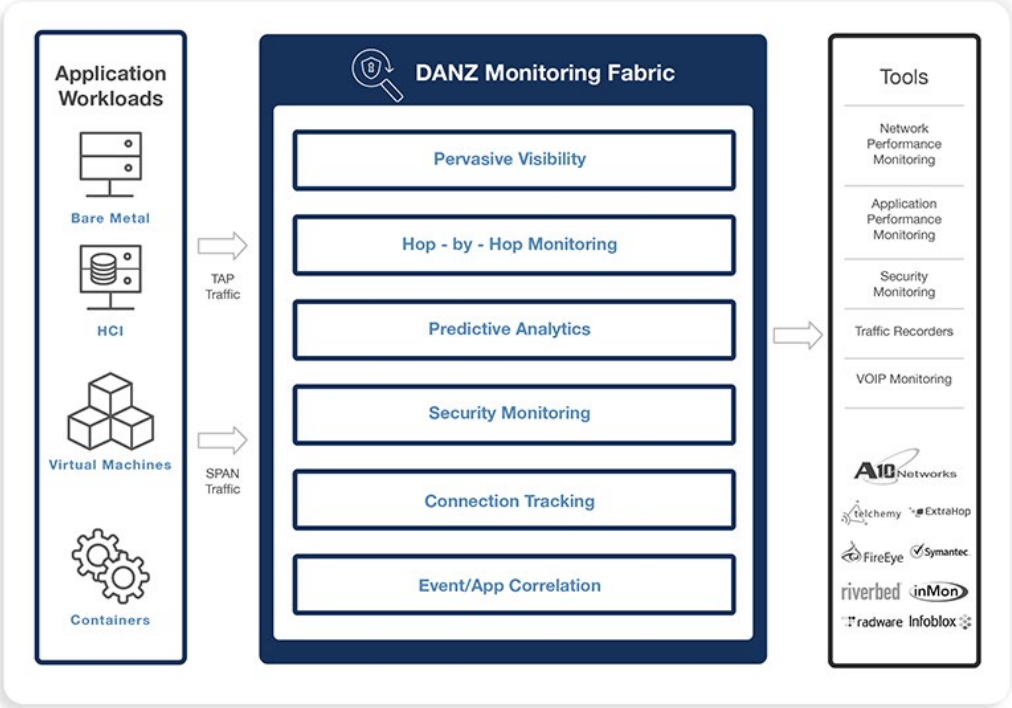
This solution combines the network packet filtering, forwarding, and storage capabilities of DANZ Monitoring Fabric (DMF) with the advanced Network Detection and Response (NDR) capabilities of the Arista NDR Platform powered by AVA. DFX (DANZ Forensic Exchange) delivers visibility at the network, device, workload, application, and user level while also enabling autonomous threat hunting, detection, and response. It also offers fully programmable and API-friendly capabilities: from selecting the specific traffic to be monitored to easily creating custom threat hunting models for threats unique to an enterprise's data center and applications.

**Deploying a Zero Trust Data Center with DANZ Monitoring Fabric**

Deploying a zero trust secure network requires the continuous collection and analysis of flow or packet information for situational analysis and Continuous Diagnostics and Mitigation (CDM). Traditionally, packet information is gathered through mirroring packets on a switch-by-switch basis. Network Packet Brokers (NPB) are frequently deployed but are largely proprietary and have proven challenging to scale for organization-wide monitoring.

DANZ Monitoring Fabric (DMF) is a next-generation NPB architected for pervasive, organization-wide visibility and security. DMF enables IT operators to pervasively monitor and mirror all traffic. In addition, DMF provides deep hop-by-hop visibility, predictive analytics, and scale-out packet capture.

The DMF dashboard controls the entire monitoring fabric and provides simplified network performance monitoring for real-time and historical context.



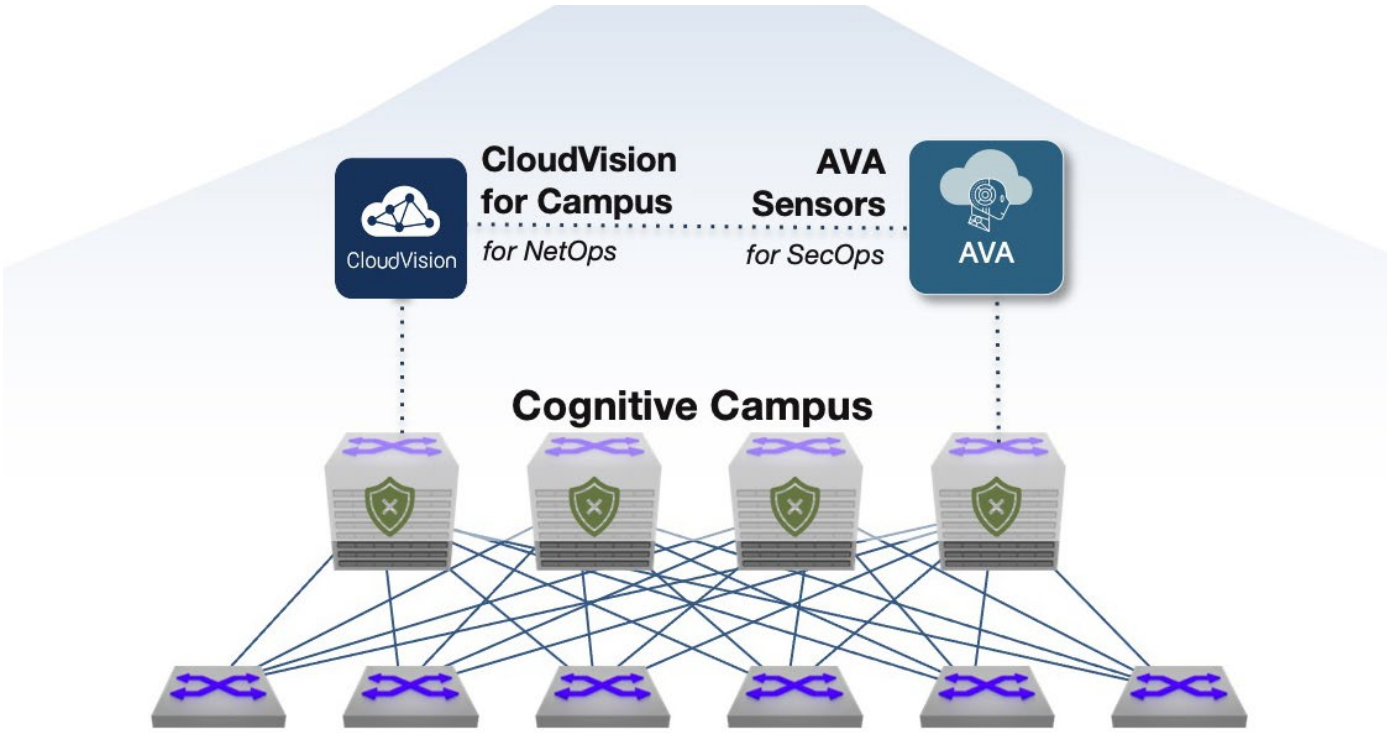
The DMF Analytics Node integrates with the DMF to provide flow analytics. The intuitive user interface quickly pinpoints suspicious traffic and anomalous behaviors. Unknown hosts, giant flows from non-business hosts, or traffic to websites that have not been approved by the security and compliance teams are identified. This is especially useful to drive zero trust decisions.

The analytics node integrates with the DMF Recorder Node to provide packet-level visibility for further detailed analysis and replay. This combination of capabilities gives a tremendous arsenal to security administrators to visualize, detect, and rectify problems across hybrid networks.

**Zero Trust for the Cognitive Campus**

Arista's zero trust campus solution embeds AVA Sensors into the switches and is thus uniquely able to offer a deep packet-inspection security analytics solution built into the campus network fabric.

With Arista's AVA Sensors embedded right at the switch layer, this solution offers increased traffic analysis, detection, and response across enterprise applications, endpoints, IoT devices, and users on the campus, while eliminating the need to deploy even more network security components. In addition, the threat hunting capabilities delivered by Arista NDR via the organization's existing switching infrastructure provide the enterprise with broader visibility across the campus and an integrated security solution that enables automated remediation while optimizing current human security workflows.



**Deploying Zero Trust Cognitive Campus with AVA Sensors**

Network administrators benefit from the real-time streaming telemetry and network-wide state delivered via Arista CloudVision and Arista NetDL (network data lake). Security teams with Arista NDR, on the other hand, have access to vital contextual data, historical forensics, and AI-driven threat hunting capabilities that speed up both time to detection and time to remediation.

AVA Sensors come in various form factors from hardware and virtual to cloud workloads and switches. These sensors are designed to keep the network topology, loads, bandwidth, and costs in mind. In addition, this solution makes security an inherent part of the new network without hampering peak performance by curating the "just right" deep packet inspection data and optimizing the transfer of data to the analytics engines.

Customers accustomed to the high-quality and reliable single OS approach from Arista Networks can now adopt a unified and integrated approach to network security. Arista consolidates security into the network architecture by:

- Providing comprehensive context and visibility to entities–-devices, users, and applications–across the entire modern campus infrastructure
- Detecting threats to and from those entities, and
- Responding to those threats by automatically identifying where those entities are on the network and then quarantining and isolating their access

## Exploring the Pillars for Zero Trust Architecture

**1. Situational awareness to understand all the resources on the network**

A fundamental tenet of the NIST ZTA Architecture is the visibility of all resources and processes. Resources are defined broadly and include all data sources, computing services, users, and IoT devices. Each resource may have a state that could include things like software version, location, time/date, observed behavior, device analytics, and more. Therefore the first step in migrating to a zero trust model requires an organization to have detailed knowledge of its resources, privileges, and business processes. This knowledge is used to define access privilege policies and enforce those policies through segmentation or other means.

Consider the example of segmentation. A group-based model places endpoints into behavioral groups, and policies are defined that regulate communication both between groups and within groups. A limited number of groups such as "production," "preproduction," and "public" may be sufficient to secure many networks, while other networks may require many groups for highly granular segmentation. Independent of the number of groups, segmentation begins with understanding connected endpoints and communication patterns.

Similarly, endpoints or network infrastructure that are susceptible to known defects such as those identified by known software defects or vulnerabilities such as PSIRTs (Product Security Incident Response Team) may also need to be identified and grouped into a high-risk group. A situational awareness strategy includes understanding the vulnerability of network infrastructure as well as the posture of the endpoint. Similar to device identification, the level of granularity required to analyze an endpoint's posture will vary based on specific customer requirements but could include, for example, OS version, connected peripherals such as removable storage devices, processes running, applications installed, memory utilization, and more.

There are many components to situational awareness, and not all components are needed for all customers. Arista provides a variety of visibility technologies for situational awareness, has established strategic partnerships with other vendors, and pursues open standards to ensure interoperability.

**2. Enforcement to implement zero trust access policies**

The second aspect of Zero Trust Security requires policy enforcement controls to ensure access is only provided based on runtime decisions made by the trust algorithm. Arista supports a variety of segmentation controls for multi-domains across clients from the data centers to campus to cloud networks.

The historical and simplest segmentation forms are port-based Access Control Lists (PACLs), VLANs or VXLANs with Routed ACLs (RACLS), and VRFs to regulate client communications. Of course, firewalls are used at the network edge for protection from external connections and in the datacenter for protecting east-west connections. In other words, the concepts of segmentation are not new, as administrators have been grouping clients and workloads into VLAN or VRF segments since the early 1990s.

Familiar segmentation methods such as VLANs and VRFs continue to be sufficient for many networks that only require a few segmentation zones. In Arista's Zero Trust model, administrators need more granular and dynamic segmentation groupings as close to the user or device as feasible. With more segments, it is operationally challenging only to associate security groups with IP addresses. For example, in a VLAN or VRF architecture, adding a new segment may require dividing an existing subnet into two smaller subnets and re-IPing the devices that were connected to the old subnet. Such network changes are cumbersome and disruptive. Standard PACLs have their own challenges as well, specifically with hardware resource scale in TCAM (Ternary Content-Addressable Memory).

Granular segmentation of campus and data center networks in a zero trust framework requires a different approach, especially with the growth of IoT and OT. Fundamentally, security segmentation groups need to be defined independent of network IP constructs. For example, to protect the organization from the well publicized Mirai botnet, an administrator might want to define a group for security cameras and a different group for the networked digital video recorders (DVRs), and yet another one for the physical security administrators. A camera, per policy, should only be allowed to communicate with the DVR and security administrator. A camera should not be allowed to communicate with another camera even if it were on the same subnet. Because there may be multiple buildings, cameras could span multiple subnets in a classic L3 network design. Security and network administrators need to have the ability to define a segment and its associated policy easily, that is independent of IP addressing and other network forwarding constructs.

### 3. AI-Driven Continuous Detection & Monitoring

Just because a device or user is on the network does not imply that it is trusted. The Arista zero trust architecture performs continuous monitoring to identify malicious intent originating from both outside the perimeter and from the inside. Threats and risk scores surfaced by Arista NDR can then be used to make segmentation decisions by the enforcement controls we discussed above. For example, an at-risk endpoint could be moved to the "high-risk" security group, where it is given restricted access.

While incident response is not directly a part of the NIST 800-207 framework, it is relevant for effective zero trust and, specifically, continuous diagnostics and mitigation. Some organizations are self-sufficient in this area, but Arista recognizes that many others want human expertise on call. As a result, Arista launched its managed network detection and response (MNDR) offering with a team of individuals that have decades of experience responding to the world's most consequential breaches. Arista's MNDR solution significantly improves the maturity of your security program by delivering a comprehensive understanding of your attack surface and then monitoring as well as threat hunting across all that infrastructure whether on-premise, cloud, IoT or operational technology. The solution combines Arista's award-winning NDR technology with decades of expertise and advanced incident response methods.

Finally, Arista can also support your organization post-breach with a variety of incident response services. It is increasingly accurate that the lasting damage of a breach is a consequence of how the organization responded to the breach rather than the fact that it was breached in the first place.

Arista recognizes the difficulties of maintaining skilled resources and having robust investigation and response processes while also dealing with technical challenges such as unmanaged devices, IoT, and cloud. These are just a few factors that hinder proactive preparedness for an incident. Arista's MNDR team can offer retainers that include pre-negotiated legal terms and rates, the right processes, both endpoint and network response technology, and expertise on demand. This saves time, brings in much needed expertise within minutes after a breach and helps contain impact in an attack, including financial costs and reputational damage.

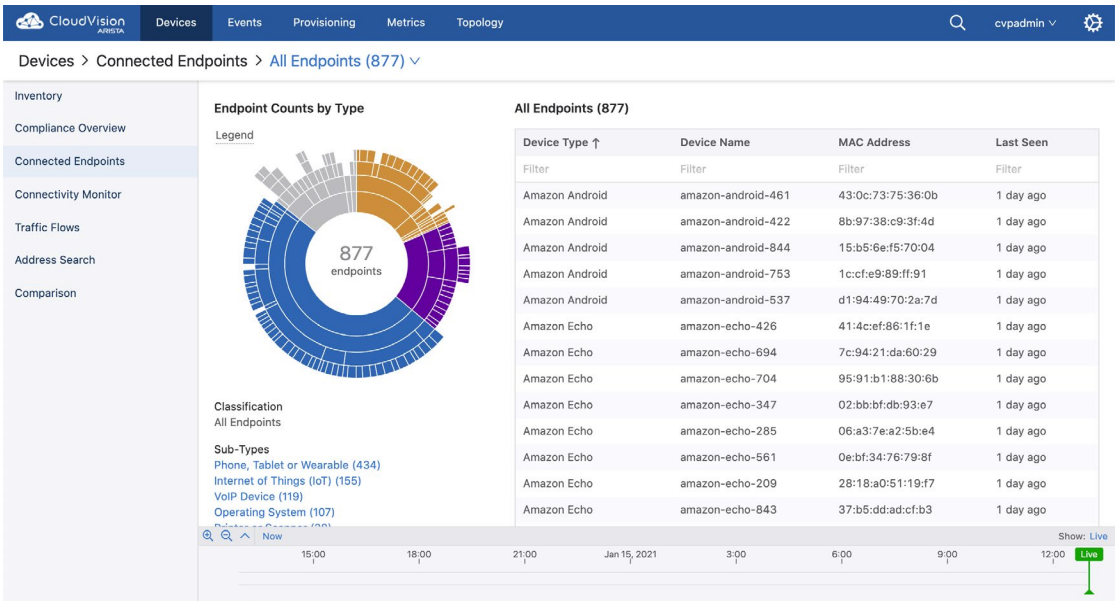
## Building a Zero Trust Network with Arista

### 1. Understanding Connected Endpoints with Arista CloudVision, Arista NDR Security and Arista Partners

Profiling or authenticating devices using network-based analytics is particularly important for IoT devices that do not leverage 802.1X or other agent-based technologies for device authentication. Users and other devices that support 802.1X leverage certificates and credentials to authenticate devices as part of the connection process. Most security architectures require a combination of agent-based and network-based techniques for device identification.

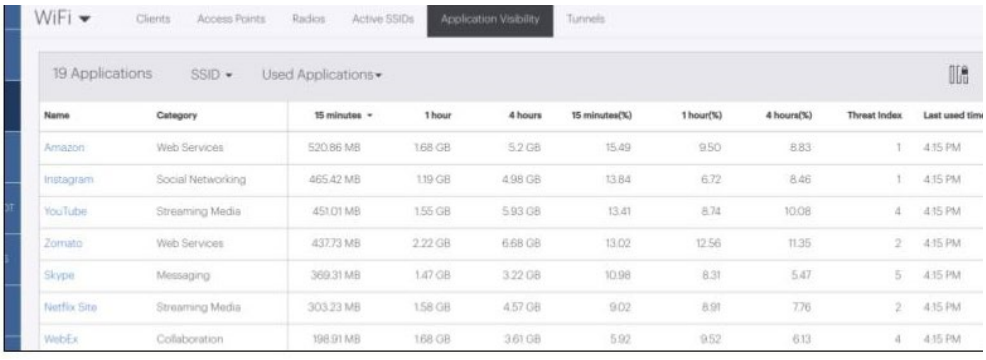
#### 1.1 Arista CloudVision Device Analyzer

Arista CloudVision Device Analyzer profiles connected endpoints using DHCP classification information. The Device Analyzer screenshot below shows 852 devices in the network. Devices are placed into various groups such as Android, phones, tablets, Amazon Echos, etc., along with their IP / MAC address and connected switch information.



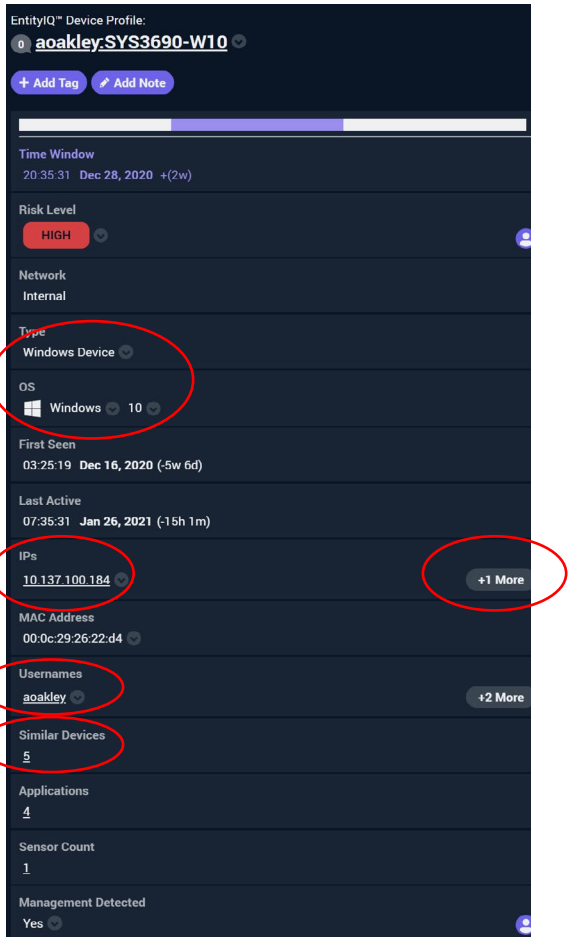

#### 1.2 Arista CloudVision Wi-Fi

CloudVision Wi-Fi can also be used for wireless devices. The solution leverages packet information to determine not only the type of device but also the applications in use. The CloudVision Wi-Fi screenshot below shows various applications, for example, Amazon, Instagram, etc. The applications are classified into multiple categories such as web services, social networking, etc. CloudVision Wi-Fi can immediately identify what endpoints are running a particular application with this kind of telemetry, as shown below.




1.3 EntityIQ

EntityIQ provides behavioral device identification via an AI-based security knowledge graph that identifies, profiles, and tracks devices, users, and applications on an enterprise network with just a network connection and without the need for agents. Full packets are mirrored to Arista NDR and analyzed along several axes beyond traditional IP address lookups. Devices are grouped into peer groups based on common behaviors and tracked as they move across the network and beyond, even as IP addresses change. For instance, TLS headers are analyzed for encrypted traffic; protocols like SMB and Kerberos are deeply parsed to identify devices and users; and DHCP/ DNS transactions can be monitored to identify everything on the network- from IoT devices to operational technology. As shown in the screenshot below, EntityIQ can determine the device is a Windows 10 device, used primarily by aoakley, and has recently had three different IP addresses.



### 1.4 Third-Party NAC

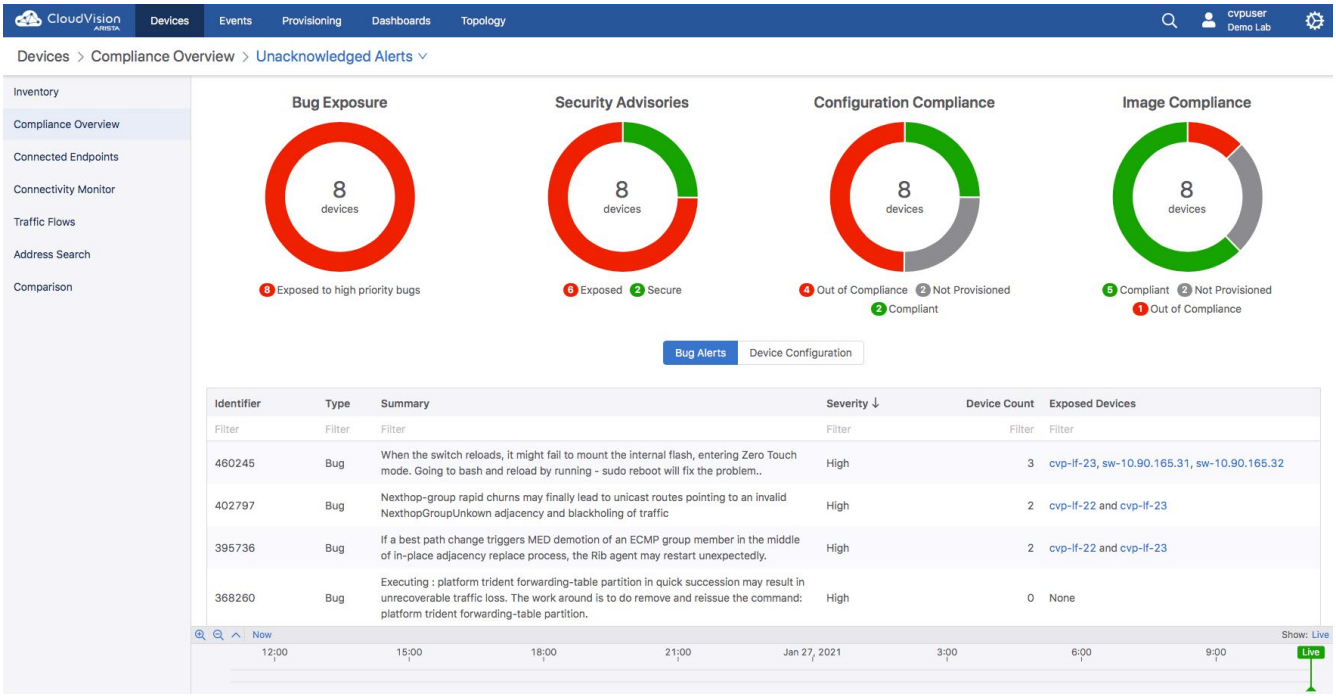
Traditional NAC products can also be used to identify and classify connected endpoints. Arista is interoperable with all the leading NAC providers, including Aruba ClearPass, Cisco ISE, and Forescout. A NAC product is also a RADIUS server responsible for authenticating devices through 802.1X or MAC Based Authentication (MBA). Authenticating IoT devices are frequently reliant on fingerprinting techniques such as DHCP, DNS, user-agent, and SNMP.

## 2 Network Switch Visibility with CloudVision

In addition to profiling and classifying connected endpoints through Device Analyzer, CloudVision provides visibility into switch performance, network compliance, and flow analytic processing.

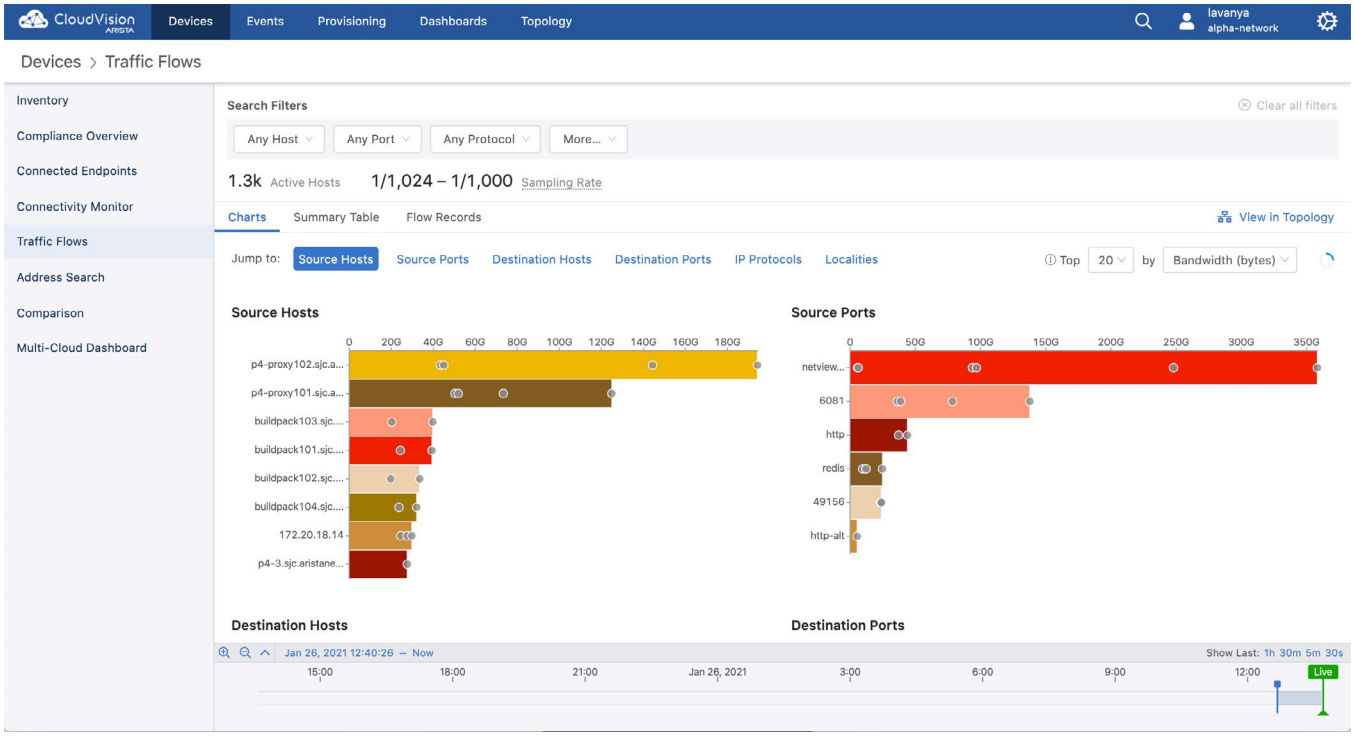
### 2.1 Network Compliance

Ensuring that networking devices are not vulnerable to industry PSIRT advisories is critical for a secure network. This is a key component of the trust algorithm in a ZTA. CloudVision provides a simple compliance dashboard that reports observed PSIRT security advisories within the network. The dashboard also reports any known exposures to software defects that are relevant as well as out-of-band non-sanctioned configuration changes made to the switches under management.




### 2.2 Flow Analysis

CloudVision analyzes sampled, or non-sampled flow information received via SFLOW or IPFIX and provides the ability to query conversations of who is talking to whom and flow traffic patterns. This information is useful for understanding business processes while designing the ZTA and monitoring the network on an ongoing basis, which we cover in detail in the next section of this paper. The figure below is a simple query showing the top 20 hosts and port numbers used. Other queries include the amount of traffic for specific host-destination pairs.

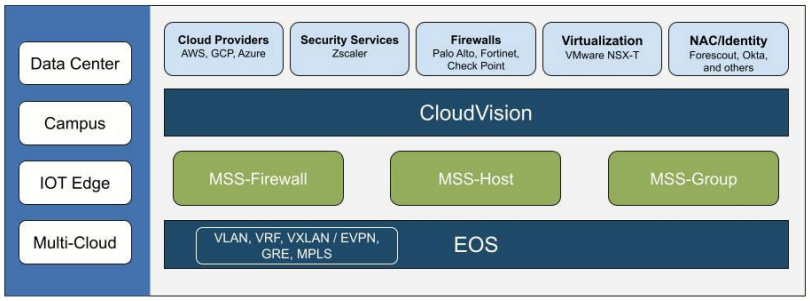



3. Arista Macro-Segmentation Service (MSS)

The Arista Macro-Segmentation Service (MSS) solution set provides several leading-edge segmentation options while supporting legacy models such as VRFs, VXLANs, and PACLs.

3.1 Multi-Domain MSS-Group Service

Arista has introduced Multi-Domain MSS-Group Segmentation as part of the MSS solution set. MSS-Group applies authorization policies to security segment groups rather than interfaces, subnets, or physical ports. IP addresses or IP subnets are placed into administratively defined security segment groups. Policies are applied to each group that defines both inter and intra-segment group communication.

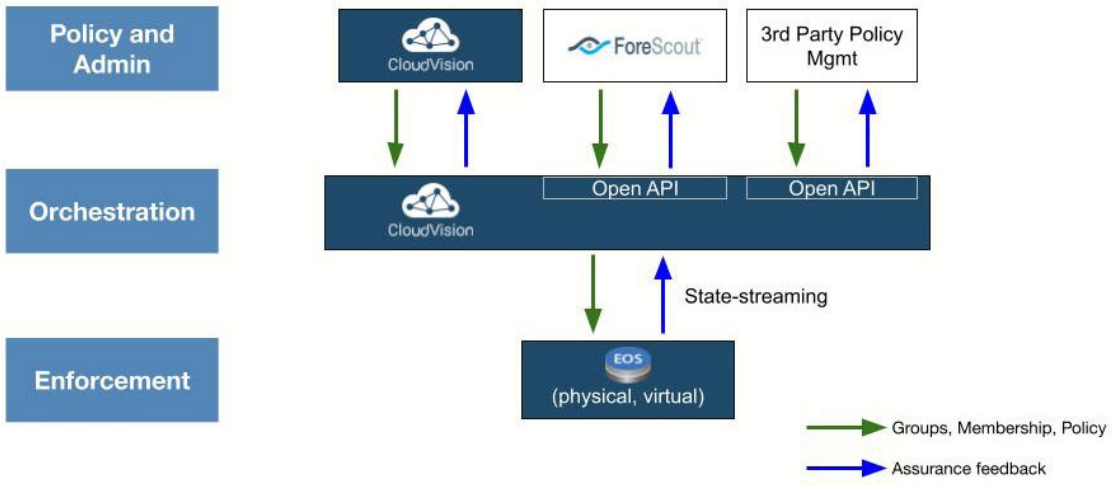



For example, to protect the organization from the well publicized Mirai botnet, an administrator might want to define a group for security cameras and a different group for the networked digital video recorders (DVRs), and yet another one for the physical security administrators. MSS-Group enables an administrator to define a segment group called "camera" that, per policy, can talk to the defined segment group "DVR" but cannot communicate with anything else, including each other. Because policies are defined on a per-segment group basis, segmentation rules policies can be created independently from IP addresses.

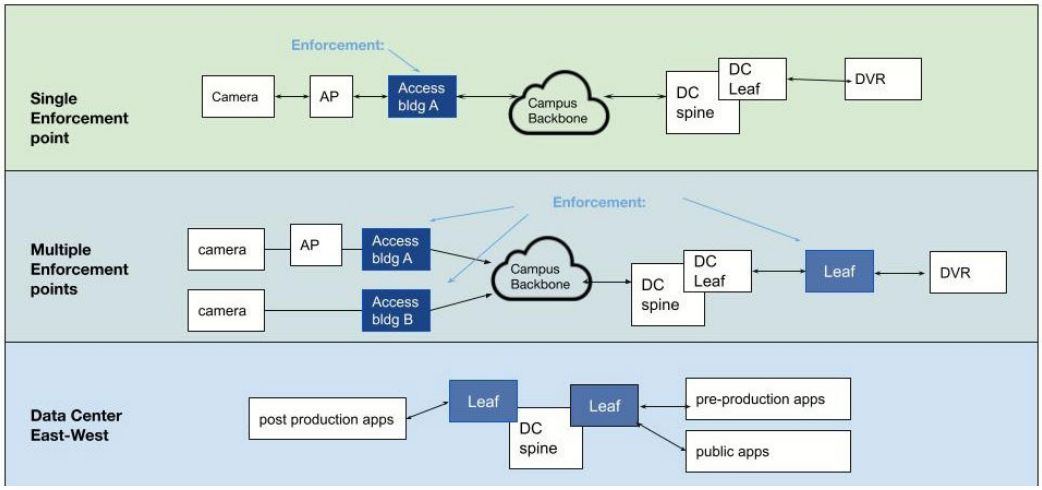
The ability to create security segments and enforce policies between segments is built into the Arista switch's hardware. The switch needs to be configured with what segment groups need to be created with a membership that defines what hosts or subnets

belong to each segment and with a policy that defines what other segments a given segment can communicate (including if it can communicate with other members on the same segment). The switch can be configured in various ways, including Arista standard CLI or EAPI which is sufficient for a few switches.

For network-wide rollout, switches should be provisioned through an orchestration layer. The orchestration layer is a CloudVision function that pushes consistent configuration to all Arista switches performing MSS-Group enforcement. The orchestration layer receives group membership and policy information from a policy layer. The policy layer is a logical layer that may also be a CloudVision function. Within CloudVision, static group segment policy and membership can be programmed by an administrator.



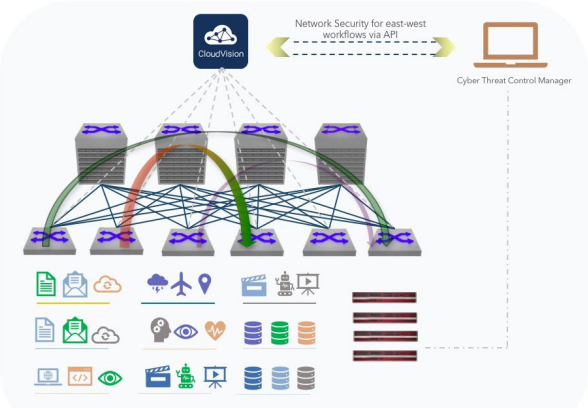

The MSS-Group solution is most powerful when CloudVision integrates with a dynamic identity layer. By leveraging APIs available in CloudVision, partners such as Forescout can ensure that different devices are put into logical groups based on device fingerprints, behavior, 802.1X authentication, and other mechanisms. The APIs allow Forescout to associate each device with its relevant security segmentation group and to apply the appropriate segmentation policies within CloudVision, which is then responsible for orchestrating the required policy to the various MSS-Group enabled switches. As new devices join the network or segmentation group membership changes, Forescout automatically updates CloudVision with these changes. In the reverse direction, CloudVision gathers hit count and segment drop information from the various switches. This information is used in CloudVision analytic reporting as well as forwarded to Forescout for Forescout reporting.

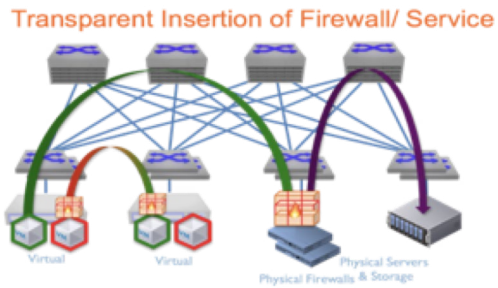



Unlike other solutions on the market, the MSS-Group segmentation architecture does not rely on proprietary ethernet tags or protocols. The upstream and downstream switches can be from any vendor. Arista MSS-Group capable switches can be deployed wherever enforcement is required. Enforcement policies can be created for any packets flowing through the switch. While it is ideal to deploy MSS-Group at the access layer, the diagram below shows how a single switch configured with MSS-Group can be used to enforce both ends of a communication flow. Of course, additional enforcement points can be added as needed.

3.2 MSS Firewall Service

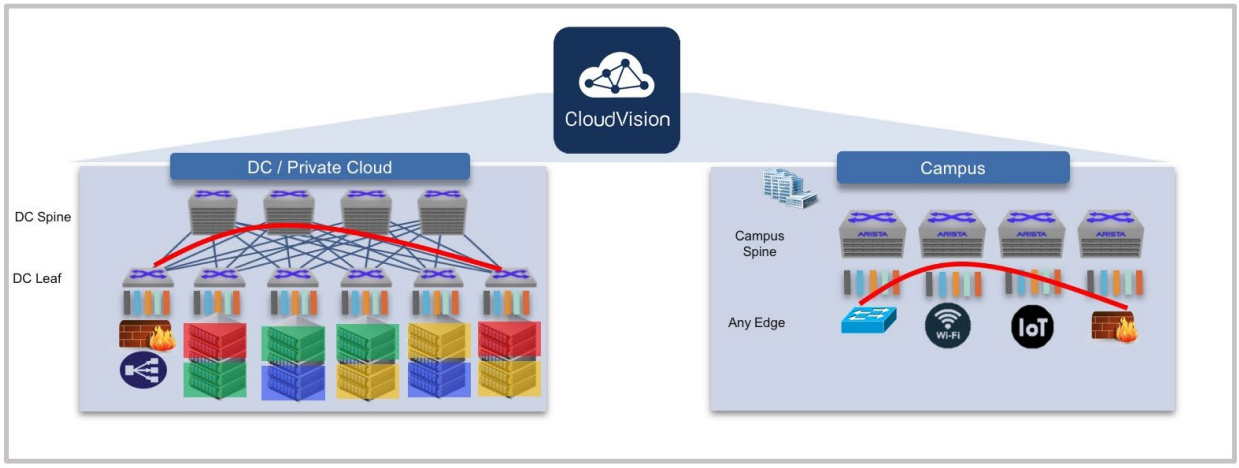
MSS Firewall is an MSS offering that enables an administrator to logically insert a Fortinet, Palo Alto Networks, or Check Point firewall dynamically into the data path for traffic inspection. CloudVision connects with a supported firewall controller; an administrator defines the traffic inspection policy in the firewall controller; the firewall controller communicates the policy to CloudVision. Arista CloudVision maintains a network-wide database of all states within the network called NetDB. NetDB is aware of where every workload is within the network; it learns in real time about new devices or workloads that are added, moved, or removed from the network. Once CloudVision learns about the traffic inspection policy from the firewall controller, it leverages the switch location information in NetDB to configure the appropriate switch. CloudVision can program the switch to redirect specific traffic to the firewall, or an ACL can be programmed to drop or forward selected traffic, thus bypassing the firewall.



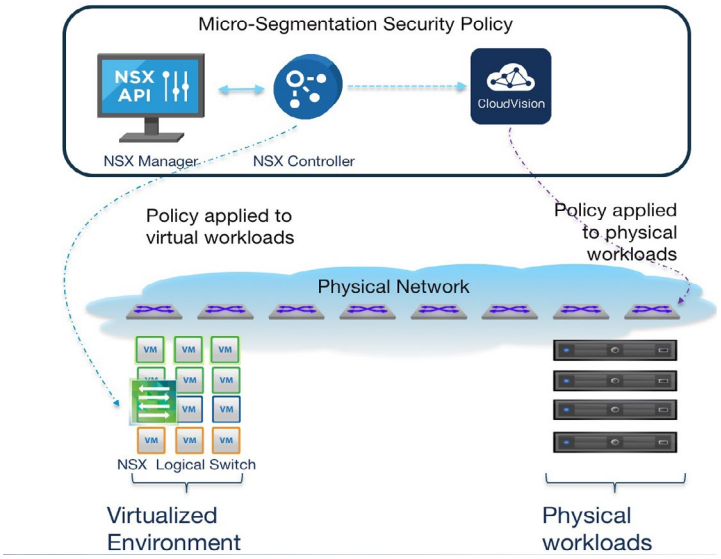

The diagram below shows how a single physical firewall can be used to inspect specific traffic from workloads that are anywhere in the network. Large data centers can centralize their firewalls in a service rack and insert them in the path between any workloads on-demand or based on a firewall policy. MSS Firewall uses standards-based forwarding to stitch service devices into the path of traffic, and it can fully function if the network is composed of devices from multiple vendors.

MSS Firewall was originally developed to segment traffic in the data center; however, MSS Firewall is also being used to segment north-south traffic in the campus. In campus use cases, MSS Firewall restricts traffic to secure applications and guards against denial of service (DOS) attacks. All flows connecting to selected applications are directed to the firewall service node for further inspections per firewall defined policy. Similarly, MSS Firewall can add additional inspection before a device is trusted or if the subject is deemed to be risky.



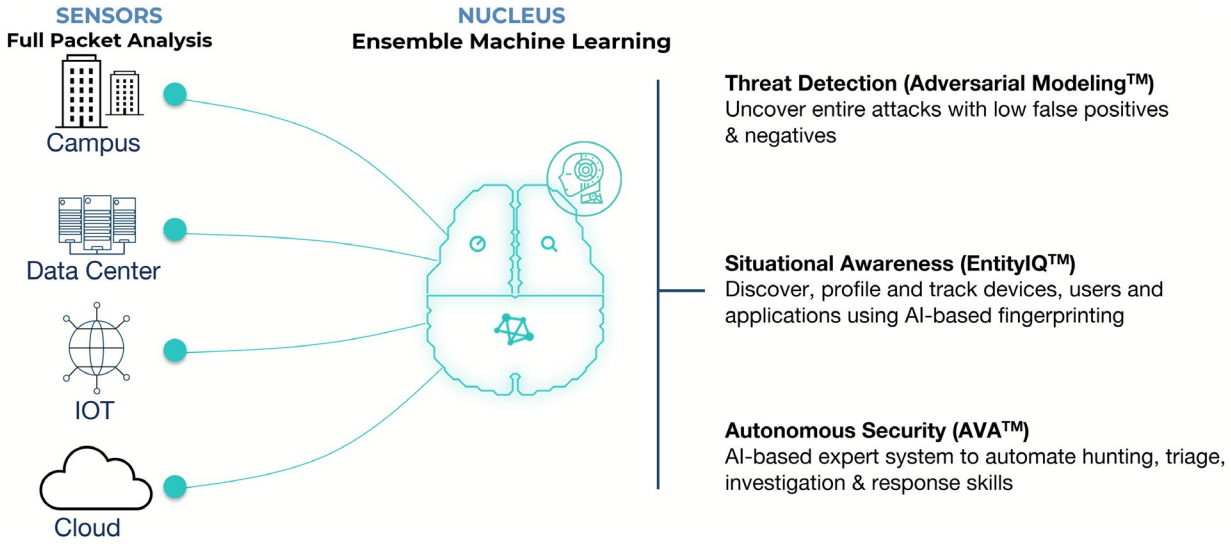

### 3.3 MSS Host Services

Arista and VMware have partnered to integrate VMware micro-segmentation technology with Arista MSS Host. The solution provides a single administrative domain to manage both VMs and physical workloads. Applying the security policy at the network edge for the physical workloads brings uniformity and consistency. In operation, Arista MSS Host will register with the VMware NSX controller and receive the policies. CloudVision will appropriately program the Arista switch or switch pairs to allow or deny conversation between the physical and virtual workloads. This allows for dynamic synchronization of security policies as new ones are created, and existing policies are modified. The MSS Host solution allows enterprises to secure all assets with uniform policy implementation at scale, mitigating the overall risk and delivering agile services.



4. Arista NDR

Arista NDR is built on a foundation of deep network analysis across the campus, data center, IoT, and cloud workload networks. Unlike other network detection and response (NDR) solutions, Arista NDR parses over three thousand protocols and processes layer 2 through layer 7 data, including performing encrypted traffic analysis. As explained above, EntityIQ uses this information to autonomously profile entities such as devices, users, and applications, while also preserving these communications for historical forensics. The AVA Nucleus then uses an ensemble of machine learning approaches to identify malicious intent hidden within.



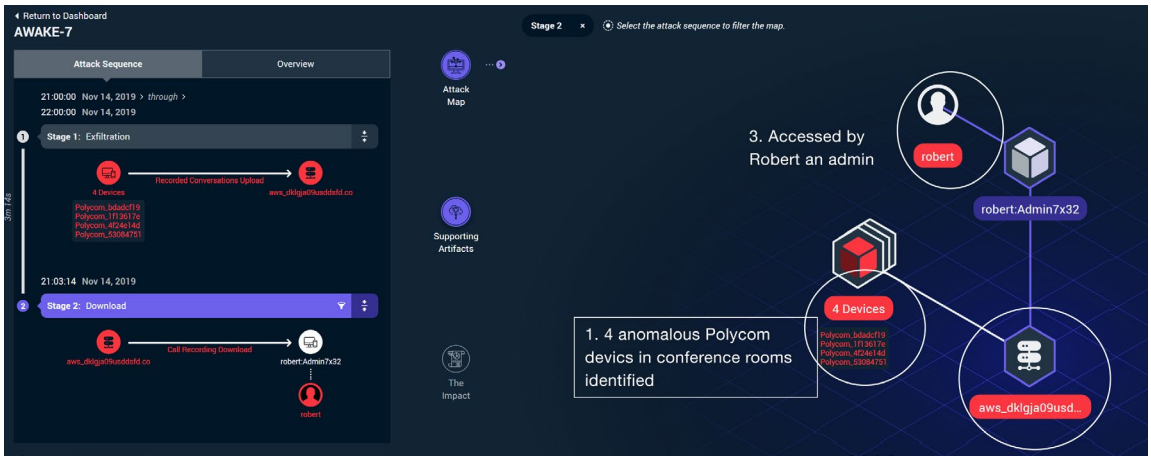

4.1 Adversarial Modeling

The Adversarial Modeling capability enables autonomous threat hunting for complex attacker tactics, techniques, and procedures (TTPs) by delivering a vocabulary to express and then identify these patterns of behavior even if they occur over extended periods of time, across a variety of protocols and impact multiple network assets.

4.2 Arista AVA

Arista AVA (Autonomous Virtual Assist), the world's first AI-based security expert system, performs autonomous threat hunting and incident triage. Using artificial intelligence, open-source intelligence, and human expertise, AVA autonomously connects the dots across the dimensions of time, entities, and protocols, enabling the solution to present end-to-end Situations to the end-user rather than atomic alerts. In addition, analysts benefit from a decision support system that visualizes the entire scope of an attack and presents investigation and remediation options on a single screen while avoiding the effort of piecing it together themselves.

The screenshot illustrates the power of Arista NDR. In this real-world case study, the platform identified four Polycom devices acting differently from other Polycom devices. Specifically, they are labeled as IP phones by EntityIQ and associated with four different conference rooms. In addition, these phones are unexpectedly communicating with an AWS hosted server. Separately, the AWS server is being accessed by an IT administrator ("Robert" in our anonymized case study). Arista NDR stitched together these disparate events and identified malicious activity. In this example, Robert recorded conversations via Polycom phones in four different conference rooms and uploaded the recordings to an AWS server. Robert then retrieved the recording for nefarious purposes. Once AVA identifies mal-intent, contextual response mechanisms are triggered to isolate the devices and resolve the zero day threat.




### 4.3 Arista Third-Party Integration

Arista NDR also integrates with and amplifies existing solutions through integrations into industry-leading SIEM such as Splunk, business intelligence such as Microsoft Power BI, ticketing and analytics such as ServiceNow, endpoint detection such as CrowdStrike, and security orchestration tools such as Palo Alto Networks' Cortex XSOAR. 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 the similar device(s) for campaign analysis. Similarly, endpoint integrations allow for one-click quarantining of compromised devices or retrieval of endpoint forensic data.

## Conclusion

Attackers have become more sophisticated and effective at subverting conventional malware-based threats and less reliant on traditional techniques such as phishing and exploits. The year 2021 witnessed an 82% increase in ransomware-related data leaks. In fact, with hybrid networks being adopted worldwide, cyber adversaries have adapted to the changing threat landscape and have cast the net wider.

Security teams are best served by assuming the environment is compromised and the perimeter has been breached. With that mindset, they then must architect their networks and systems to be resilient in that assumed compromise state. This is the premise of Arista's zero trust networking architecture that combines an AI-Driven security model with segmentation and observability.

2 CrowdStrike 2022 Global Threat Report

**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