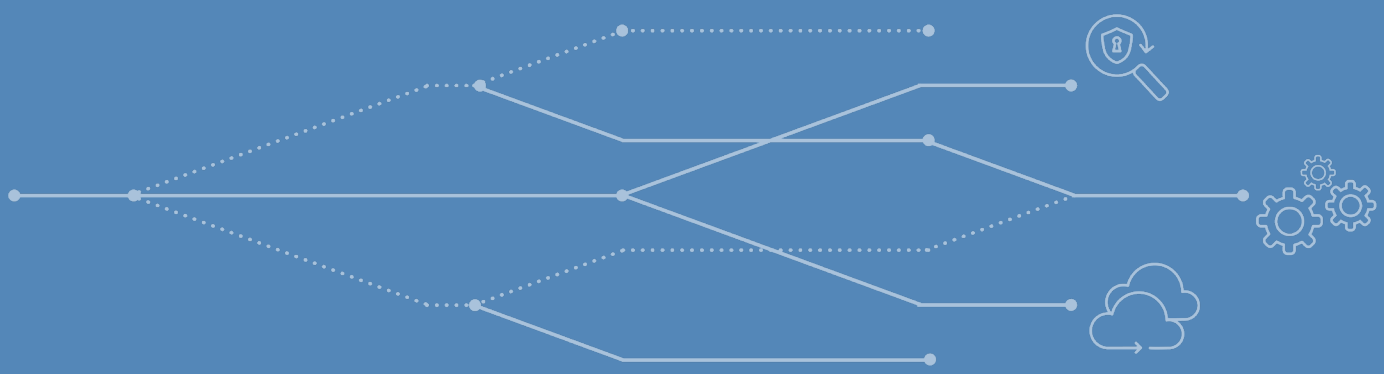


Arista NDR Campus Edition

As digital transformation efforts accelerate and organizations look to formulate new strategies for in-person workspaces, the campus network has evolved tremendously. Building automation and other IoT devices today often form a significant portion of the endpoints connecting to the network. Primarily driven by the adoption of SaaS applications, traffic from these campuses is rarely backhauled to the data center; instead, it is routed directly to the Internet. This architecture renders traditional network security approaches blind to many of these locations. Agent-based solutions, on the other hand, are often incompatible with the devices to be protected. Consequently, attacker lateral movement, ransomware, malware-free and insider threats, and credential abuse can go unnoticed. Organizations need a network-based threat detection and response solution that can efficiently identify such threats at each campus location while not requiring additional hardware deployments and security expertise in these places.

Arista is uniquely situated to address these security gaps, given its position at the foundation of the wired and wireless network. Security built into the network eliminates the need for multiple disparate network security overlays and, along with the rest of the Arista Zero Trust Networking portfolio, reduces operational costs, complexity, and the need for experts at each location.

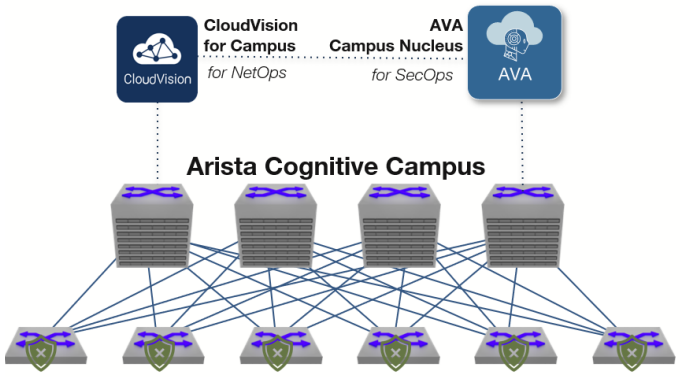
The Arista NDR Campus Edition uses an easy-to-deploy software **AVA Sensor** extension on existing Arista Cognitive Campus switches. This sensor can be deployed easily using Arista CloudVision or Ansible playbooks and is designed to parse over three thousand protocols and process layer 2 through layer 7 data. The platform also analyzes encrypted protocols to identify essential context such as the nature of traffic (file transfer, interactive shell, etc.), the applications communicating, and the presence of remote access, all without forcing data decryption. Arista's **EntityIQ™** technology uses this information to autonomously profile entities such as devices, users, and applications while preserving these communications for historical forensics.

Arista NDR Campus Edition

- Delivers EntityIQ™ to autonomously discover & profile every device, user & application (managed or unmanaged) in the organization.
- Deploys directly on network switches to deliver granular visibility while eliminating the operational overheads of additional hardware.
- Automates triage and investigations through AVA™ AI, providing a decision support system to analysts.
- Requires no agents, manual configuration, or lengthy training periods.

[1] https://www.arista.com/assets/data/pdf/Arista-ZTNO-Solution-Brief.pdf

"Arista NDR has exceeded our expectations and empowered us to secure our connected workplace more effectively and autonomously than ever."
– Rich Noguera, Fmr. CISO, Gap Inc.



Network Detection and Response (NDR) for the Cognitive Campus

- Campus-optimized NDR Nucleus along with switch-based sensor and optional managed threat hunting expertise
- Eliminate the need for overlay networks, TAP/SPAN, additional rack space for security gear
- Eliminate threat detection blind spots in campus environments including IoT, lateral movement, insider threats, ransomware etc.
- NetOps-SecOps workflow integration via security-specific dashboards in CloudVision
- Seamless remediation via NAC, segmentation, firewalls, proxies, endpoint security, SIEM, and more

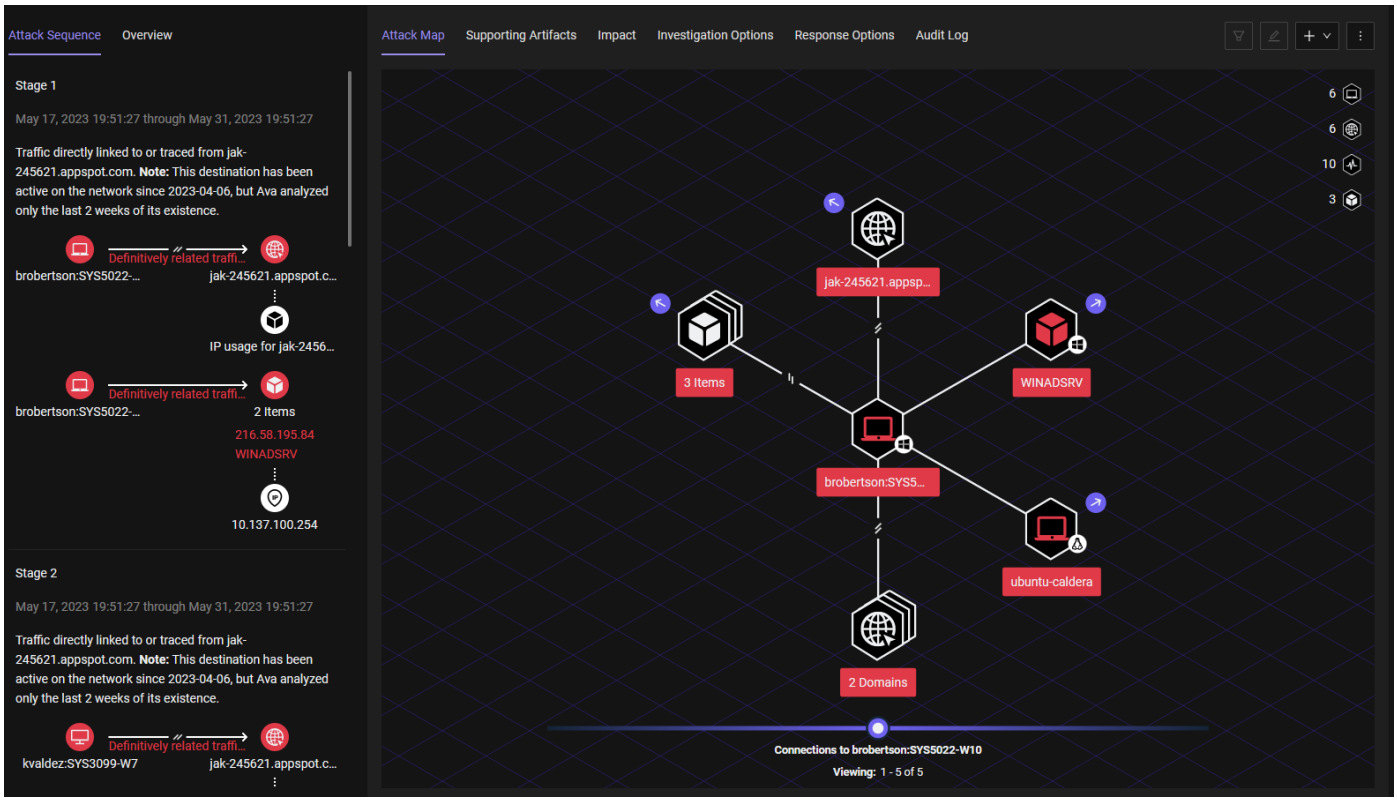
Extracted activity data feeds into the **AVA Campus Nucleus**, which uses a combination of detection models to uncover malicious intent. An ensemble of machine learning approaches avoids reliance on simplistic and noisy anomaly detection or unsupervised learning.

Arista's **Adversarial Modeling™** capability uncovers even the most complex attacker tactics, techniques, and procedures (TTPs). The Arista Threat Research Team uses Adversarial Modeling to build and maintain AI-driven models that zero in on suspicious activity and then gather corroborating evidence to support the conviction. This process reduces both false positives and negatives.

AVA, Autonomous Virtual Assist, is Arista's AI-driven decision support system that automates threat hunting and incident triage. AVA automatically 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 a plethora of meaningless alerts. Analysts thus see the entire scope of an attack along with investigation and remediation options on a single screen while avoiding the effort of piecing it together themselves. Importantly, federated machine learning allows Arista customers to gain these capabilities while keeping their private data firmly within their infrastructure.

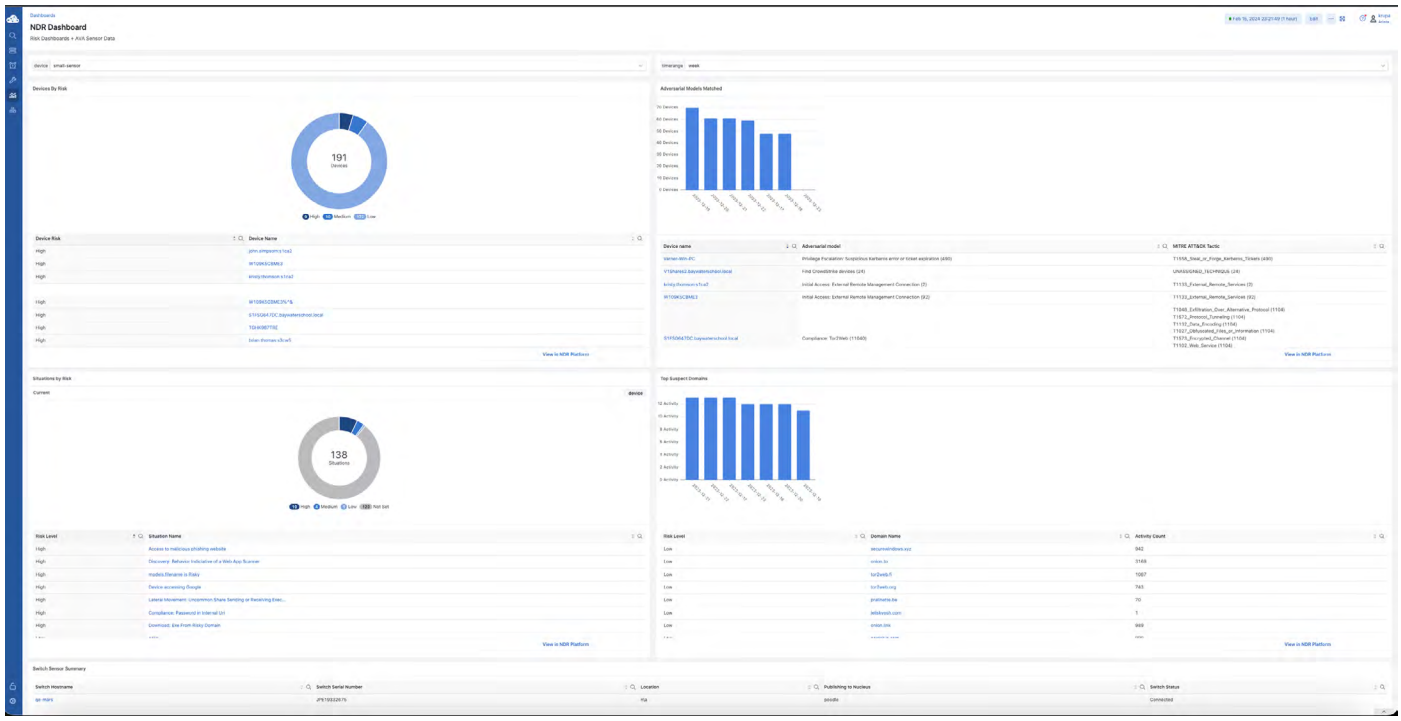
Use Cases

Detection	Response	Situational Awareness
Detect mal-intent & behavioral threats from both insiders & outside attackers and triage based on the MITRE ATT&CK framework mappings.	Investigate and respond rapidly with access to necessary decision support context, correlated by AVA across entities, time, protocols, and attack stages.	Gain comprehensive visibility into the campus via a platform that learns & tracks managed & unmanaged IT/IoT devices, including those from contractors and third parties.



Integrations

The Arista NDR Campus Edition integrates with solutions such as SIEM, endpoint detection, and response tools, as well as firewalls/proxies. For instance, an analyst can pivot from any SIEM alert containing just an IP or email address to an EntityIQ profile that includes the operating system, device details, and associated user(s). Similarly, endpoint integrations allow one-click quarantining of compromised devices or retrieval of endpoint forensic data. In addition, the platform supports deep integrations with Arista's Networking and Zero Trust solutions, including CloudVision and CV AGNI (network access control).



Model # (Hardware AVA Campus Nucleus)	DCA-NDR-NCC10
PERFORMANCE & CAPACITIES	
Function	Campus Nucleus
Protected Throughput	Up to 10 Gbps
Meta Data Storage	15 Days
SYSTEM REQUIREMENTS	
Rack Unit	1U
CPU Cores	16
RAM	64 GB
Non-volatile Memory	3.2 TB
Network	2x 10/25 Gbps SFP 1x Out-of-Band Management Interface
Power Supply	2x 800W –Redundant and Hot Swappable

Model # (SaaS AVA Campus Nucleus)	SS-NDR-NCCG10-1M
PERFORMANCE & CAPABILITIES	
Cloud	Google Cloud Platform
Function	Campus Nucleus
Protected Throughput	Up to 10 Gbps
Meta Data Storage	15 Days

Model #	SS-NDR-G-SWITCH-1M	SS-NDR-G-T1-1M	SS-NDR-G-T2-1M
Tier	Up to 149 switches	150-499 switches	500+ switches
Function	Sensor Only	Sensor Only	Sensor Only
SYSTEM REQUIREMENTS			
Supported Arista Switches	Please refer to the link below, pick one or more switch models, select "Campus Features" under Product Features, and look for the "AVA switch sensor" checkmark. https://www.arista.com/en/support/product-documentation/supported-features		

Model #	SS-SEC-AMNDR-Switch-1M
Tier	This service is available per switch for 30 or more switches.
Function	Managed Network Detection and Response
SYSTEM REQUIREMENTS	
Supported Arista Switches	Gain access to a 24x7x365 team of expert threat hunters and incident responders with this optional add-on service. Please refer to the following datasheet for service details. https://www.arista.com/assets/data/pdf/Datasheets/Managed-Network-Detection-and-Response-MNDR-Datasheet.pdf

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