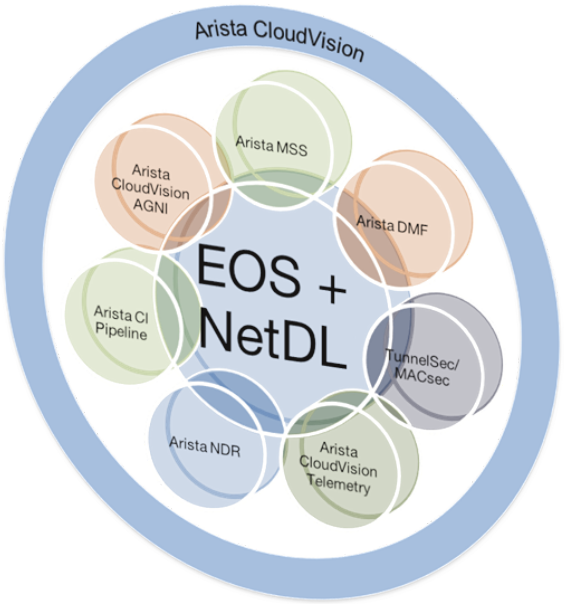
The Arista Solution for Zero Trust Networking

Zero trust architectures attempt to mitigate risk associated with cyber threats by eliminating implicit trust in a device simply because it is on the internal network. However, this is easier said than done, given today's changing definition of the network that spans campus, data center, cloud, and more. Adding multiple network security layers such as firewalls, network access control, and threat detection, among others, comes at tremendous cost, complexity, and brittleness, whereas the benefits are often hard to quantify. As a result, many organizations must roll the risk management dice, especially deep inside the network where the organization's crown jewels are often housed.

Arista offers a full suite of security solutions built on the foundations of our unified operating system in **EOS®** (Extensible Operating System) and the common management plane in **CloudVision™**. These solutions map to the **CISA Zero Trust Maturity Model**[1] and help organizations accelerate their journey toward optimal maturity. Moreover, these network security controls can help compensate for gaps in the organization's zero trust posture in domains such as identity, devices, workload, and data. Most importantly, this integrated security toolset uses the underlying network infrastructure from switches to WAN routers to deliver key security capabilities and integrates seamlessly with the organization's existing security program and tools.



Network Segmentation

Arista's **Macro Segmentation Service (MSS)** enables the creation of microperimeters through the edge switches that can protect or isolate each asset without requiring the deployment of extra firewalls across the campus network. MSS-Group applies authorization policies to security segment groups rather than interfaces, subnets, or physical ports. These groups, in turn, can be constructed around application workflows, allowing policies defined by administrators within CloudVision to control both inter and intra-segment group communication. Arista also supports segmentation via flexible placement of firewall policies across DMZ edge, data center, and campus networks. Additionally, security policies can be extended to virtualized and cloud workloads.

Arista's **Edge Threat Management (ETM)** solutions, consisting of NG Firewall, Micro Edge, and ETM Dashboard, help mid-market businesses and distributed enterprises protect, monitor, and control all devices, applications, and events on a network, putting IT back in control of dispersed networks, hybrid cloud environments, IoT and mobile devices.

Network Traffic Management

The Arista **DANZ Monitoring Fabric (DMF)**[2] enables IT operators to pervasively monitor all user, device/IOT, and application traffic (north-south and east-west) by gaining complete visibility into physical, virtual, and container environments. Deep hop-by-hop visibility, predictive analytics, and scale-out packet capture — integrated through a single dashboard — provide unprecedented observability to monitor, discover, and troubleshoot network and application performance issues and accelerate the discovery of root causes of security breaches and other outages.

[1] https://www.cisa.gov/zero-trust-maturity-model

[2] https://www.arista.com/en/products/danz-monitoring-fabric

Traffic Encryption

Arista network infrastructure natively supports encryption capabilities such as **MACsec** and **TunnelSec**. These capabilities, implemented on the switches, enable organizations to encrypt data to and from legacy applications and workloads without having to change those systems, instead relying on the network to protect data from unauthorized access, interception, and tampering.

Network Resilience

The key to resilience in a zero trust context lies in the ability to dynamically expand or reduce with network demands. Arista's **CloudVision**[3] and EOS work hand in hand to provide onboarding and connectivity to any public utility clouds securely and with optimal performance. In many instances, customers striving for zero trust maturity in this function deploy data centers in active/active configuration using robust EOS features such as EVPN that provide the entire capacity as a single virtual data center while still providing geo-specific fault tolerance.

Visibility and Analytics Capability

Arista **NDR**[4] is an AI-enabled platform that 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 detects threats to and from these entities while providing the context necessary to respond rapidly. Arista NDR can deliver visibility and analytics enterprise-wide by utilizing existing deployed switches as network security sensors. As a result, organizations can benefit from broad situational awareness without the need to deploy additional network-tapping infrastructure or network visibility solutions.

Automation and Orchestration Capability

The Arista **CI Pipeline**[5] provides an advanced CI environment for managing network and security operations built upon the visibility the Arista CloudVision platform provides. This capability, along with **Arista Validated Designs (AVD)**, offers additional features and integrations that greatly simplify and enhance the automation of network and security operations workflows.

Governance Capability

CloudVision **Arista Guardian for Network Identity™** [6] **(CV AGNI)** is a software as a service network access control (NAC) solution that simplifies the onboarding and ongoing governance of network identity across users, their associated devices, and the Internet of Things (IoT), for both wired and wireless networks. CV AGNI uses existing identity providers such as Microsoft Azure AD or Okta. CV AGNI performs dynamic authorization via real-time posture assessments based on data from Arista NDR and third-party technologies such as endpoint detection and response solutions.

[3] https://www.arista.com/en/solutions/telemetry-analytics

[4] https://www.arista.com/en/products/network-detection-and-response

[5] https://www.arista.com/assets/data/pdf/Arista-CI-Pipeline-Tech-Brief.pdf

[6] https://www.arista.com/en/products/network-access-control

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

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