ARISTA

Solution Brief

Arista Networks Multi-Domain Segmentation Services (MSS) For Zero Trust Networking

Microsegmentation solution mitigates threats across east-west lateral networks from Data Center to Campus and Branch

Enterprises are going through digital transformation driven by trends such as hybrid and mobile workforce, explosion of managed and unmanaged IT, OT & IoT devices, distributed Cloud applications causing the notion of traditional network security perimeter to collapse.

This accelerated pace of change coupled with an ever-changing threat landscape is posing many security challenges, the biggest one being minimizing any lateral movement to contain the lateral spread of ransomware and other cyberattacks. These growing threats need to be identified & contained quickly otherwise could result in huge losses of revenue and customers as well as risk the company's reputation.

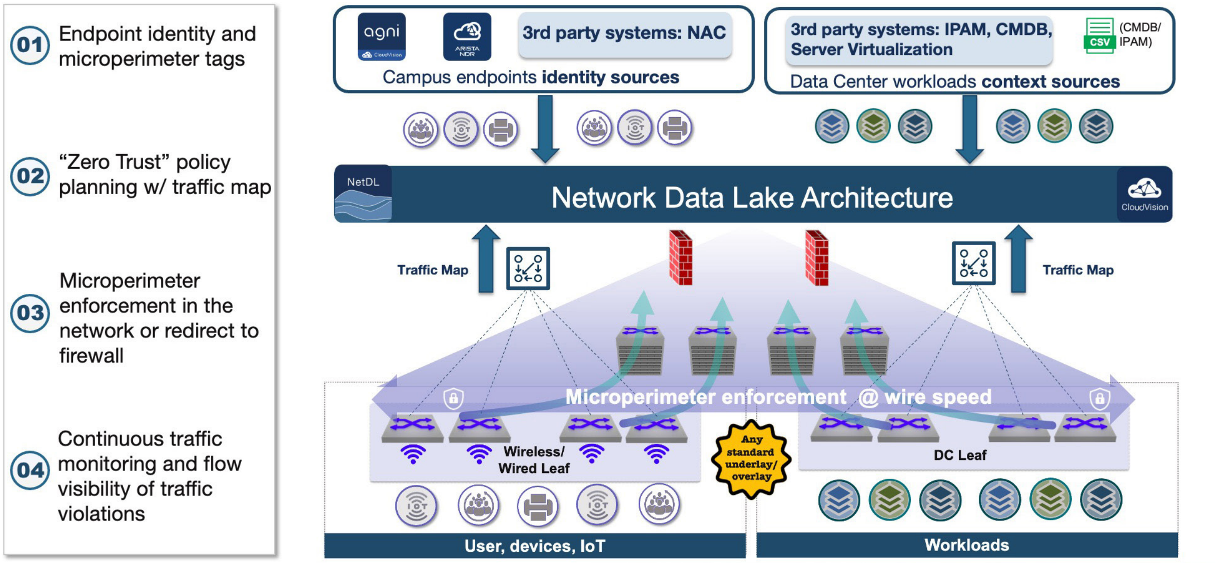
Zero trust is a framework for securing enterprises in today's modern digital transformation.

Zero trust assumes there is no network perimeter & based on the "Never Trust Always Verify" approach, that requires organizations to continuously monitor and validate all users, devices, and applications against appropriate access privileges and security policies to explicitly allow only trusted traffic.

Arista Multi-domain Segmentation Services implements the following key principles of zero trust frameworks like the Cybersecurity and Infrastructure Security Agency (CISA) "Zero Trust Maturity Model":

- **Minimize lateral movement** with identity-aware microperimeters
- **Trust nothing** with zero trust policies to explicitly allow only trusted traffic
- **Always verify** with visibility into policy violations and permitted traffic to update and validate zero trust policies

Arista MSS provides four core services to successfully plan, deploy and operate microsegmentation at scale with a consistent operational model from data center to campus and branch:


01 Endpoint identity and microperimeter tags
02 "Zero Trust" policy planning w/ traffic map
03 Microperimeter enforcement in the network or redirect to firewall
04 Continuous traffic monitoring and flow visibility of traffic violations
agni
CloudVision
ARISTA NDR
3rd party systems: NAC
Campus endpoints identity sources
3rd party systems: IPAM, CMDB, Server Virtualization
CSV
(CMDB/ IPAM)
Data Center workloads context sources
NetDL
Network Data Lake Architecture
CloudVision
Traffic Map
Traffic Map
Microperimeter enforcement @ wire speed
Wireless/ Wired Leaf
Any standard underlay/ overlay
DC Leaf
User, devices, IoT
Workloads

1. **Endpoint identity and microperimeter tags**

   The first step in planning a microsegmentation strategy consists of binding endpoints, workloads, and even networks to specific microperimeter tags. CloudVision MSS powered by Arista NetDL automates the management of microperimeters by connecting to external sources and dynamically identifying and then tagging the endpoints and workloads. Arista MSS can connect to various external sources like NAC systems, CMDBs, IPAMs and virtualization infrastructure management solutions.

2. **"Zero Trust" policy planning with traffic map**

   Zero trust architecture principles require that all traffic on the network must be explicitly allowed by security policies. To create zero trust policies, it is vital to have complete visibility into existing traffic flows on the network. This ensures that policies protect the right resources while at the same time not impeding legitimate business-justified flows.

   Arista MSS maps all the communications within and across different parts of the network and provides a set of recommended policies to only permit trusted communications based on the observed traffic map.

3. **Microperimeter enforcement in the network or redirect to Firewall**

   Arista MSS then distributes the zero trust policies to EOS-powered network switches. In turn, the switches can perform wire-speed distributed enforcement themselves or redirect the traffic to a third-party firewall for stateful L4-7 inspection. Importantly, Arista's switch-based enforcement overcomes the challenges associated with traditional ACL-based segmentation such as TCAM exhaustion, by leveraging an advanced tagging engine that optimizes hardware utilization and maximizes scalability. Furthermore, because the tags are internal to a switch and are not shared across the network infrastructure, Arista MSS can seamlessly insert into any multi-vendor network. This approach also avoids any proprietary protocols that force organizations into single-vendor networks.

4. **Continuous Traffic monitoring and visibility of policy violations**

   Once the zero trust policies are deployed, MSS can monitor for policy violations and report on the specific flows dropped in the network. This provides vital intelligence to the administrator to update the zero trust policies when valid, yet new, services are denied as well as monitor specific endpoints that are attempting to violate traffic rules.

Arista MSS Key Benefits

1. **A single operational model for Campus, Branch and Datacenter Microsegmentation**

   Predicated on a single EOS binary, common across all switching platforms, a single Arista CloudVision® policy orchestration platform, and an aggregated Network Data Lake (Arista NetDL™) infrastructure for state management and monitoring.

2. **Standards-based networking with no custom protocols or hardware**

   Unlike other switch-based microperimeter segmentation solutions, Arista MSS is not dependent on any custom protocol or custom hardware and is thus able to be integrated into any standard brownfield and multi-vendor network (wired and wireless).

3. **Flexible to any endpoint with no custom agents or software**

   Since MSS does not require any software agents on endpoints and workloads, it seamlessly extends microperimeter segmentation from campus, to branch, factory, and IoT endpoints as well as virtualized and bare metal workloads in the data center. There is no limitation of specific operating system or virtualization platforms.

4. **Simplified management of zero trust microperimeters**

   CloudVision integrates with multiple campus endpoint and datacenter workload identity sources, such as network access control solutions, IP address management offerings, IT service management tools and virtualization platforms. Arista MSS is thus able to dynamically establish and enforce identity-aware microperimeters across the entire enterprise.

5. **Eliminates "blind spots" for safe deployment of zero trust policies**

   Using the data in Arista NetDL, MSS generates a map of all traffic sessions and then provides a set of zero trust police recommendations based on the observed traffic map. Once policies are deployed, MSS can continuously monitor traffic violating policies and stream the flow information to CloudVision for monitoring and rule update purposes. Importantly, MSS can also connect to other sources of context such as network detection and response (NDR) and endpoint detection and response (EDR). Thus, Arista MSS can quickly react to endpoints and workloads that might be misbehaving or compromised and isolate them as appropriate, minimizing breach impact on the organization.

Who can benefit from implementing Arista MSS

Organizations with existing microsegmentation deployments that are looking to:

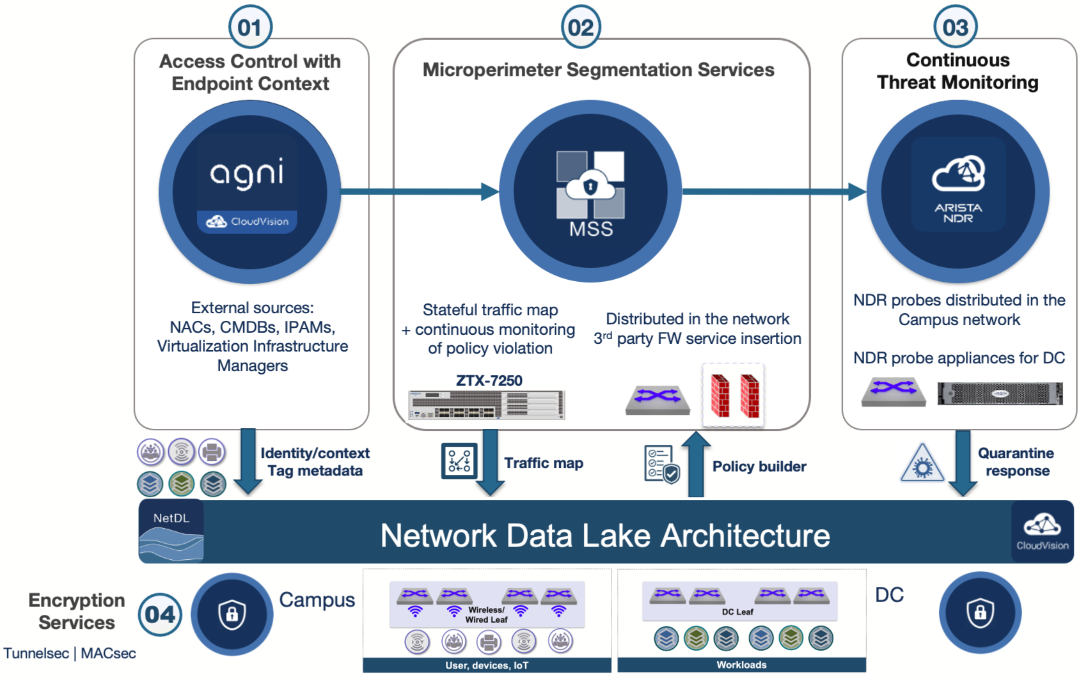
- **Enhance and extend** agent/host-based microsegmentation to the rest of the infrastructure not managed by host Firewalls/agents.
- **Simplify** existing switch-based microsegmentation deployments with an easy-to-deploy consistent solution that adapts to any network overlay and underlay from data center to campus and branch.

Organizations new to microsegmentation that are looking to:

- **Reduce Firewall** spend while extending segmentation to all internal traffic
- **Jumpstart their zero trust initiative** with an easy-to-insert solution in existing brownfield network infrastructure with wired and wireless endpoints and virtualized and bare metal workloads

Conclusion: Arista Zero Trust Networking (ZTN) Services

Arista MSS is one of the cornerstones of Arista ZTN architecture which offers a suite of services to simplify the implementation of zero trust initiatives across the entire Enterprise.


01
Access Control with Endpoint Context
agni
CloudVision
External sources: NACs, CMDBs, IPAMs, Virtualization Infrastructure Managers
02
Microperimeter Segmentation Services
MSS
Stateful traffic map + continuous monitoring of policy violation
ZTX-7250
Distributed in the network
3rd party FW service insertion
03
Continuous Threat Monitoring
ARISTA NDR
NDR probes distributed in the Campus network
NDR probe appliances for DC
Identity/context Tag metadata
Traffic map
Policy builder
Quarantine response
NetDL
Network Data Lake Architecture
CloudVision
Encryption Services
04
Tunnelsec | MACsec
Campus
Wireless/ Wired Leaf
User, devices, IoT
DC Leaf
Workloads
DC

To learn more go to: www.arista.com/en/solutions/security/mss

- Arista CloudVision AGNI for access control
- Arista MSS for identity-aware microperimeter segmentation
- Arista NDR for continuous threat monitoring and quarantine response

Reference:

https://www.arista.com/assets/data/pdf/Whitepapers/Zero-Trust-Maturity-Model-WP.pdf

https://www.arista.com/assets/data/pdf/Whitepapers/MSS-Segmentation-Technical-WP.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