Product Highlights

Simplified Operations

- Standard networking, no custom protocols or hardware for microperimeter tagging
- Fit into multi-vendor wired-wireless network infrastructure
- No endpoint software
- CloudVision centralized policy management
- Single EOS across Campus, Branch and Datacenter

Dynamic Management Of Microperimeters

- Integration with external NAC solutions for Campus endpoints microperimeter tags
- Integrations with CMDB, IPAMs and Virtualization Systems (e.g. VMware vCenter) for datacenter workloads microperimeter tags

Zero Trust Policy Planning

- Build a traffic map all the communications among endpoints
- Generate zero trust policies based on the traffic map to explicitly allow the observed trusted traffic

Microperimeter enforcement

- Microperimeter enforcement in the network at wire speed with Campus and Datacenter switches
- Endpoints and workloads can map to more than one microperimeter
- Maximize TCAM rule compression with advanced EOS Tagging engine

Redirect to third party Firewalls for L4-7 Stateful Inspection

- Option to redirect traffic between microperimeters to existing zone based Firewall for L4-7 stateful inspection

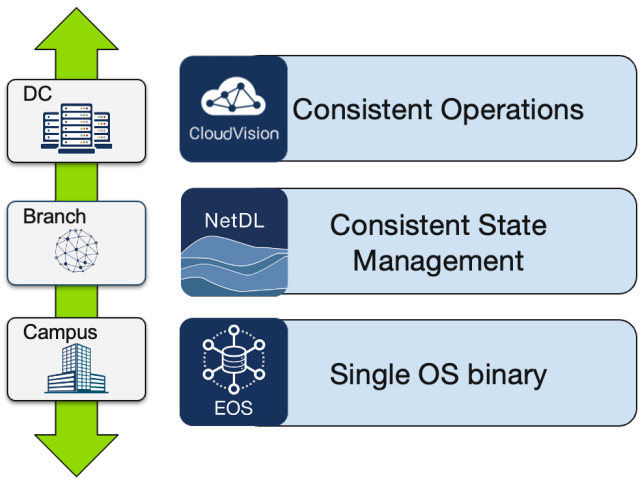
Continuous Policy Monitoring

- Monitor policy violations
- Gain flow visibility into dropped traffic with ZTX-7250S or vZTX appliance

Introducing Arista Multi-Domain Segmentation Services (MSS)

Arista Networks has defined the only *multi-domain microperimeter segmentation (MSS) architecture* designed to maximize operational simplification and overcome all the limitations of legacy microsegmentation solutions based on switches or host-based Firewalls:

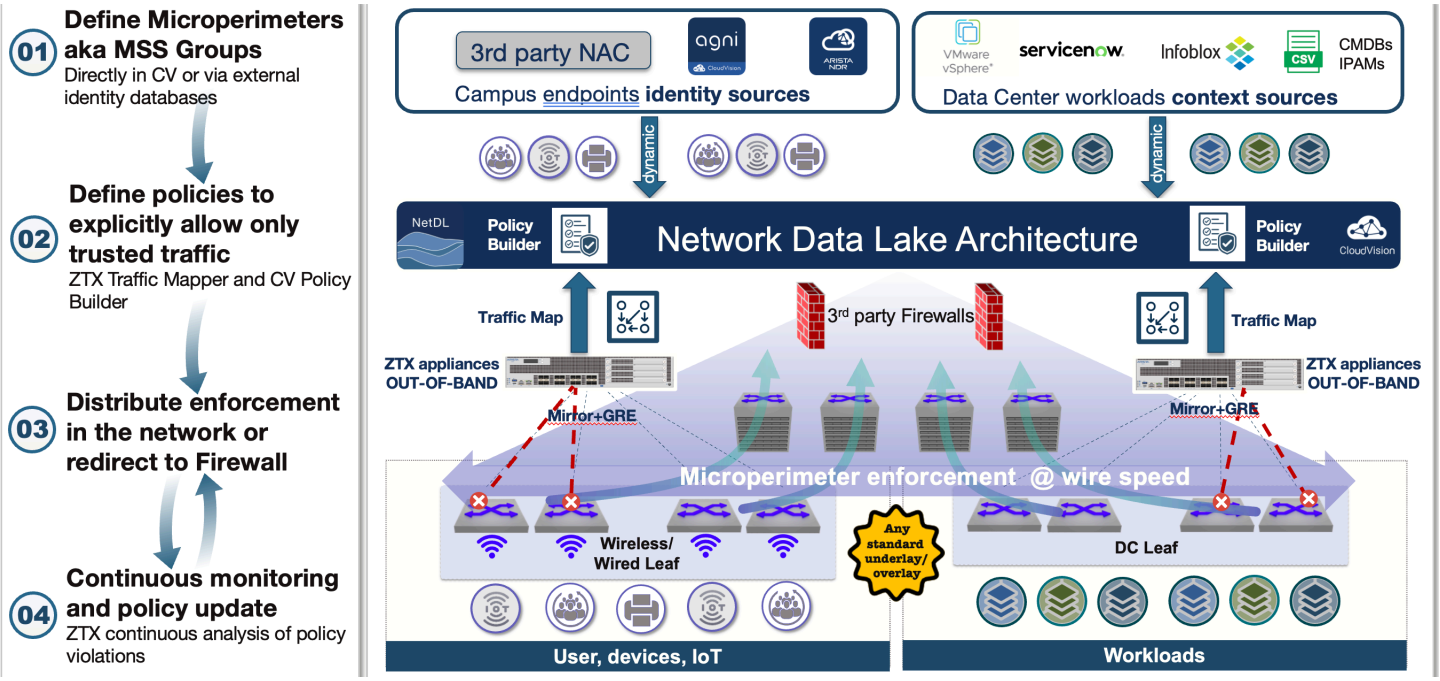
- **One operational model for Campus, Branch and Datacenter:**
  Predicated on a single EOS binary, common across all switching platforms, and a single Arista CloudVision™ policy orchestration platform.
- **Abstracted from the network:**
  Works with any standard overlay and underlay w/o proprietary encapsulations
  Microperimeter tagging independent from the network
  Simple brownfield insertion in a multivendor wired/wireless network
- **Agentless:**
  Since MSS does not require any software agents on endpoints and workloads, it seamlessly extends microperimeter segmentation from Campus, branch, factory, IoT endpoints all the way to virtualized and bare metal workloads in the data center.
- **Simplify the management of zero trust microperimeters:**
  CloudVision integration with many external Campus endpoint and Datacenter workload identity sources can manage dynamically endpoints and their microperimeters.
- **Simplify the deployment of zero trust policies:**
  The ZTX appliance (ZTX-7250S or vZTX) maps all the traffic sessions and CloudVision Policy Builder generates a set of zero trust rules based on the observed traffic map. Once policies are deployed, the ZTX appliance can continuously monitor traffic violating policies and stream the flow information to CloudVision for monitoring and rule update purposes.



Consistent Operation Across Multi-domains

Arista MSS Services

Arista MSS offers four core functionalities to implement a complete microperimeter segmentation solution.



1. **Define Microperimeters (aka MSS Groups):**
   The first step in planning a microsegmentation strategy consists of binding endpoints, workloads and even networks to specific microperimeters tags. CloudVision MSS automates the management of microperimeters, by connecting to external sources and importing dynamically endpoints and workload group tags. CloudVision Network Data Lake can connect to a variety of external sources like NAC systems, CMDBs or virtualization infrastructure management solutions such as vSphere.

2. **Define policies to explicitly allow only trusted traffic:**
   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 necessary to have full visibility into the traffic sessions currently in the network. MSS provides a service to map all the communications among microperimeters and provide a set of recommended rules to explicitly permit trusted communications based on the observed traffic map.
   To create the traffic map, MSS leverages the Arista ZTX appliance (ZTX-7250S or vZTX) to monitor all the traffic sessions and export them to CloudVision, which then generates the zero trust rules with the CloudVision MSS Policy Builder.

3. **Distribute enforcement in the network or redirect to Firewall:**
   CloudVision MSS distributes the rules and objects to the EOS powered network switches to either enable wire speed distributed enforcement of the MSS policies in the network, or redirect the traffic to a 3rd party firewall for stateful L4-7 inspection. EOS switch based enforcement is based on an advanced "tagging" engine that optimizes hardware utilization and maximizes scalability. Because the labels are internal to a switch, and never go into the network, the MSS technology can seamlessly insert into any multi-vendor network.

4. **Continuous monitoring and policy update:**
   Once the zero trust policies are deployed, MSS offers the ability to monitor any policy violations and detect the specific flows dropped in the network. This enables the administrator to update the zero trust policies, when valid, yet new, services are being denied, or monitor specific endpoints violating traffic rules.

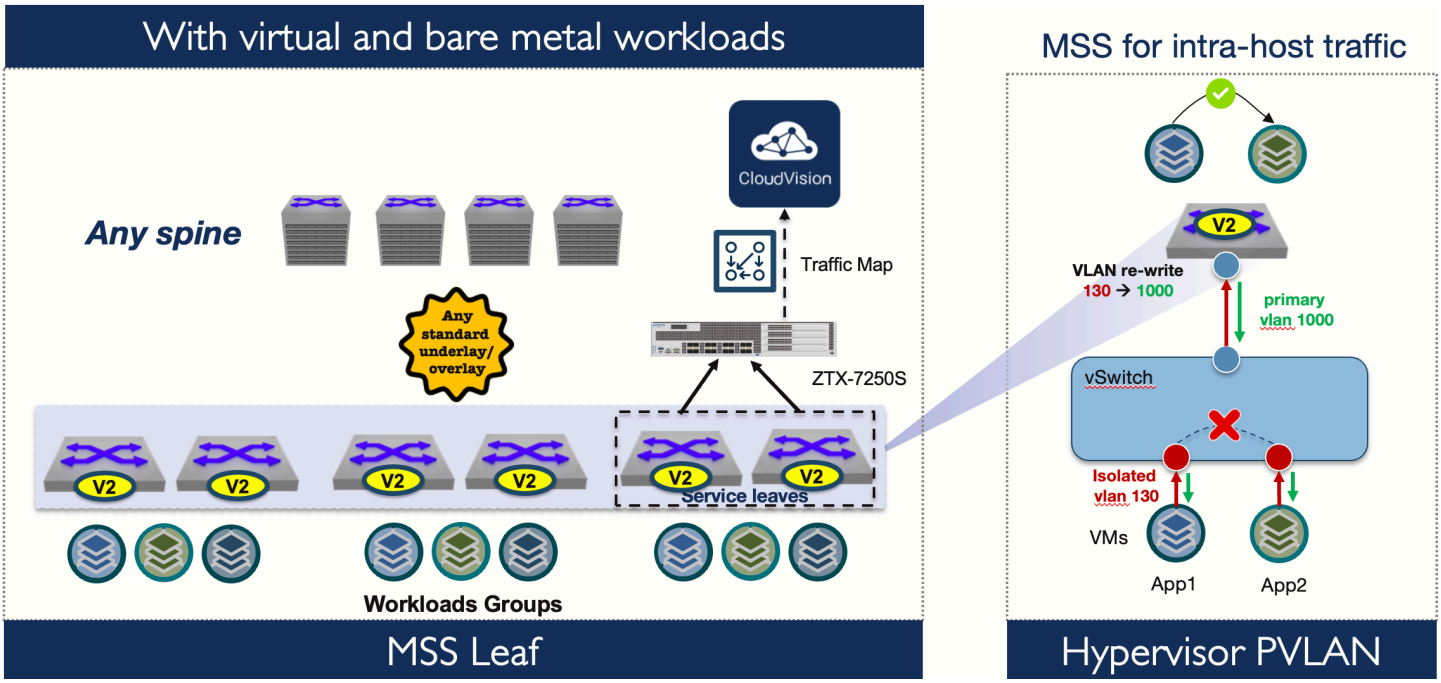
   MSS rules support a "drop+monitor" action, which programs the switches to drop the packets and at the same time create a copy of each dropped packet and mirror it to the ZTX appliance. The appliance analyzes each mirrored packet and records flows metadata (including source, destination, and L4 service) which is then streamed to the CloudVision Policy Builder which generates an updated policy recommendation.

Datacenter Deployment Model

In the datacenter MSS is deployed on the leaf switches for both the intra-rack and inter-rack security.
The MSS solution is composed of:

- A V2 license required on the leaf switches. The network topology can be based on any standard underlay and overlay and the spine switches can be from a third party vendor.
- CloudVision for policy orchestration and monitoring and to integrate with external workload identity sources.
- The ZTX appliance (ZTX-7250S or vZTX) for traffic mapping to generate the zero trust policy recommendations and detect flows violating the policies.

In virtualized environments, it is also necessary to extend microsegmentation rules to traffic between VMs on the same host. This traffic is normally bridged by the host virtual switch and never reaches the leaf switches. To enable MSS on the leaf switches to control the inter-VM traffic on the same host, it is possible to force all the VM-to-VM traffic to be directed to the leaf switch where MSS rules can be enforced before the traffic is forwarded back to the destination VM.
This requires a combination of Private VLAN(PVLAN) configuration on the vSwitch, along with configuring VLAN translation & disabling source port filtering on the leaf switches (to allow broadcast and ARP traffic between the VMs).



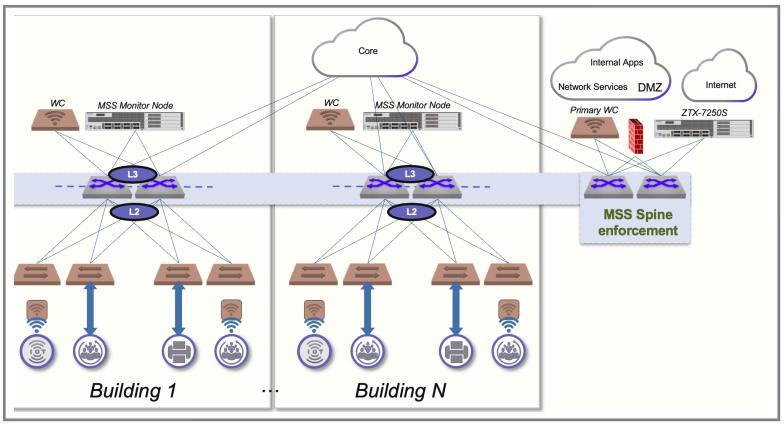
Campus Deployment Models

In Campus and Branch the goal is to enforce MSS rules for traffic from both wired and wireless endpoints. The versatility of the MSS architecture allows organizations to insert microsegmentation in any standard network with a mix of third party wireless access points and switches. Below are a few examples illustrating the flexibility of the MSS architecture, which enables enforcement either at the "MSS leaf" or at the "MSS spine":

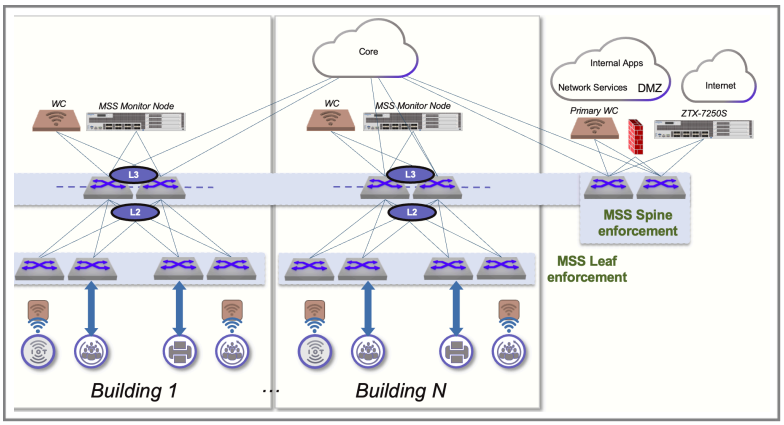
- "MSS Spine" enforcement for both third party wireless (tunneled traffic terminated to a controller) and wired traffic
- "MSS Spine" enforcement for third party wireless (tunneled) and "MSS Leaf" for wired traffic
- "MSS Spine" enforcement for Arista wireless (tunneled) and "MSS Leaf" for wired traffic

The MSS solution is composed of:

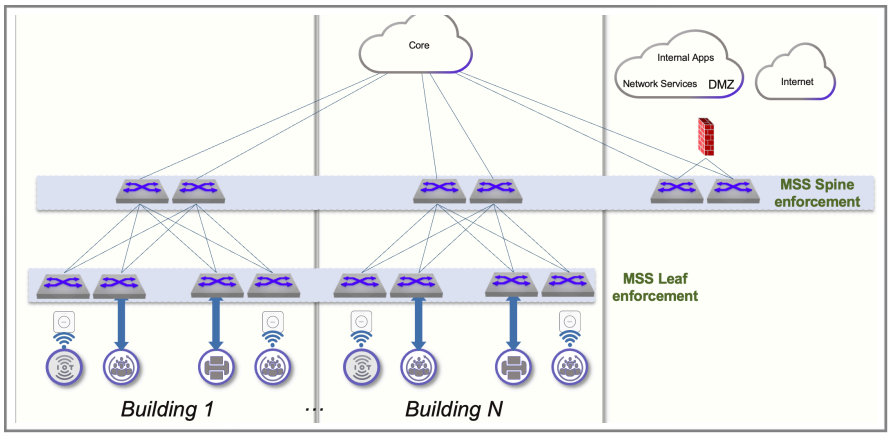
- A V2 license required on the "MSS Spine" and "MSS Leaf" switches. The network topology can be based on any standard underlay and overlay and the spine switches can be from a third party vendor.
- CloudVision for policy orchestration and monitoring and to integrate with external endpoint identity sources.
- The ZTX appliance (ZTX-7250S or vZTX) for traffic mapping to generate the zero trust policy recommendations and detect flows violating the policies.



MSS insertion with 3rd party wifi and wired access



MSS insertion with 3rd party wifi and Arista wired access



MSS with Arista wifi (tunneled) and wired access

Licensing Requirements

- EOS V2 add-on license on all the switches where MSS rules are enforced
- CloudVision Premier license
  (See https://www.arista.com/assets/data/pdf/Software-Licensing-Framework.pdf for details on Arista's software licensing)

MSS Minimum Software Versions

- EOS : 4.33.2F
- CloudVision (on-prem): 2024.3.0
- CloudVision (as-a-service)

MSS Switch Platforms Series

- DCS-7280R3/R3A
- DCS-7050X3
- CCS-720DP (excluding 720DP-24S)
- CCD-720DT (excluding 720DT-24S)
- CCS-720DF
- CCS-720XP (excluding 720XP-96ZC2*, 720XP-48TXH-2C-S*)
- CCS-722XPM (excluding 722XPM-48ZY8*)
- DCS-7010TX

* On Roadmap

CloudVision Dynamic Microperimeter Data sources

- Arista CloudVision AGNI
- VMware vSphere
- ServiceNow
- Infoblox
- Generic CMDB via csv

(No additional Arista license required on CloudVision or any of the above systems to enable MSS)

MSS Enforcement Features (EOS)

- MSS policies per VRF
- Multiple tags per endpoint/network
- Hybrid rules with tags and IP prefixes
- TCP and UDP L4 ports filtering
- ICMP filtering
- L4 ports tag summarization - 7280R3 only
- Enforcement actions:
  - Forward (explicitly allow traffic) or Drop (deny)
  - Monitor (forward and mirror a copy to ZTX appliance)
  - Drop+Monitor
  - Redirect to 3rd party Gateway/Firewall*

* On Roadmap for 7280R3/R3A, 720XP-96ZC2, 720XP-48TXH, 722XPM-48ZY8

CloudVision MSS Orchestration and Monitoring

- MSS Manager (rules, groups management)
- MSS Policy Builder (for policy recommendation, requires MSS Traffic Mapper ZTX-7250S or vZTX*)
- MSS Policy Monitor

* Roadmap

MSS Scalability Matrix

Platform Series*	Max Rules (unidir.)	Max IPv4 prefixes	Max HW prefix labels
7280R3/R3A	12,000	7,500	64K source, 64K dest
7280R3K/R3AK	12,000	~ 250,000 (Number varies by model type)	64K source, 64K dest
7050X3	~ 2,650 (Number varies by model type)	72K Host, 8K LPM	1K
720DP-24ZS/48ZS, 720DF, 720XP	3,500	32K Host, 4K LPM	1K
722XPM, 720DP/DT-48S, 7010TX	5,500	15K Host, 2K LPM	1K

(*) For individual switch models scale, refer to respective hardware platform data sheets. Maximum values dependent on shared resources in some cases. The number varies by model type.

Headquarters
5453 Great America Parkway
Santa Clara, California 95054
408-547-5500

Support
support@arista.com
408-547-5502
866-476-0000

Sales
sales@arista.com
408-547-5501
866-497-0000

Service and Support

Support services including next business day and 4-hour advance hardware replacement are available. For service depot locations, please see: http://www.arista.com/en/service

www.arista.com

ARISTA