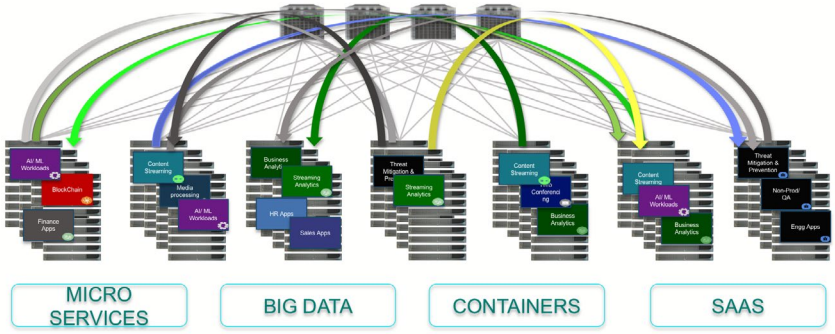
# CloudVision® Macro-Segmentation Service - Firewall

## Inside

Address network-based security and segmentation as a pool of resources, stitch security to applications and transactions, scale on-demand, automate deployment and mitigation, allow transparent application of security policies; do it all seamlessly without introducing gratuitous interdependencies, for both physical and virtualized resources:

- Micro-Segmentation: inserting services in the path of inter-VM traffic by defining policies in an overlay/ virtualization controller for each individual workload — enforced within the hypervisor virtual switch, by application, workload, or other tag.
- Macro-Segmentation™: Segmentation by inserting services between workgroups (intertenant or inter-device) in the physical network by defining inter- segment service policies - defined and enforced via a combination of firewall and Arista cloud networking infrastructure.
- Arista Macro-Segmentation Service (MSS™) Firewall: an extension in Arista EOS® software that utilizes Arista CloudVision® to automate security service insertion for next-generation firewalls

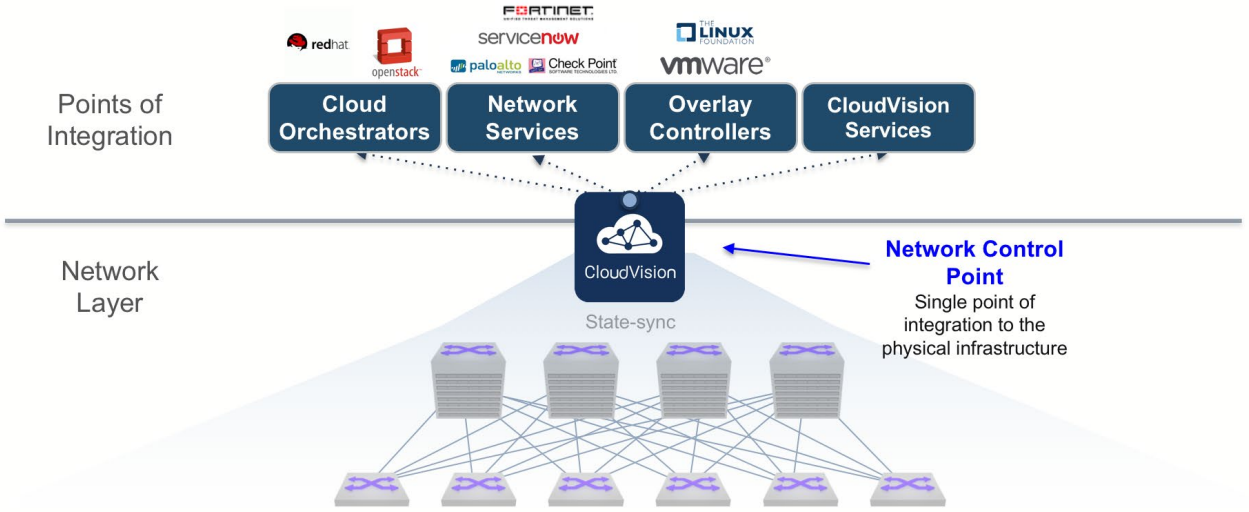
An increase in successful data breaches across all industries, including government agencies, has accelerated the need to re-architect the security framework. With technology transitions driven by SaaS application delivery models, IoT, 5G, AI/ML etc, happening at a rapid pace, Infosec architects are rethinking the way trust perimeters are defined and moving to a zero-trust model. The move to zero trust also means evolving the architecture which has largely remained static and bounded, unable to protect the increasingly virtualized/ containerized data center environments hosting modern applications at scale.




Today's cloud environments need a more flexible approach to deploying security that adapts to constant workload changes, additions, and movements. The capacity of the security solution needs to scale upward to match the broadened attack surface of multi-tenant shared environments. Infrastructures need to offer an unfettered selection of security technology options as opposed to siloed ecosystems of yesterday's solutions that limit flexibility and obstruct freedom of choice.

### Arista Macro-Segmentation Service - Firewall

Arista Networks™ Macro-Segmentation Service (MSS) - Firewall capability for CloudVision® allows next-generation firewalls to be deployed automatically for specific workloads and workflows across modern overlay network virtualization (EVPN) fabrics.




## Platform for Automation and Visibility across the Network

Current security deployment models support embedded security in the virtualization hypervisors to address inter-VM communication and physical firewalls address at-depth protection for north-south traffic leaving the data center.

With east-west traffic dominating the traffic flows, no solution exists yet to dynamically insert advanced security services for this traffic in hybrid data centers utilizing a combination of hypervisors, or containing non-virtualized workloads like big data and storage, or attaching legacy systems to the same networks as new cloud applications.

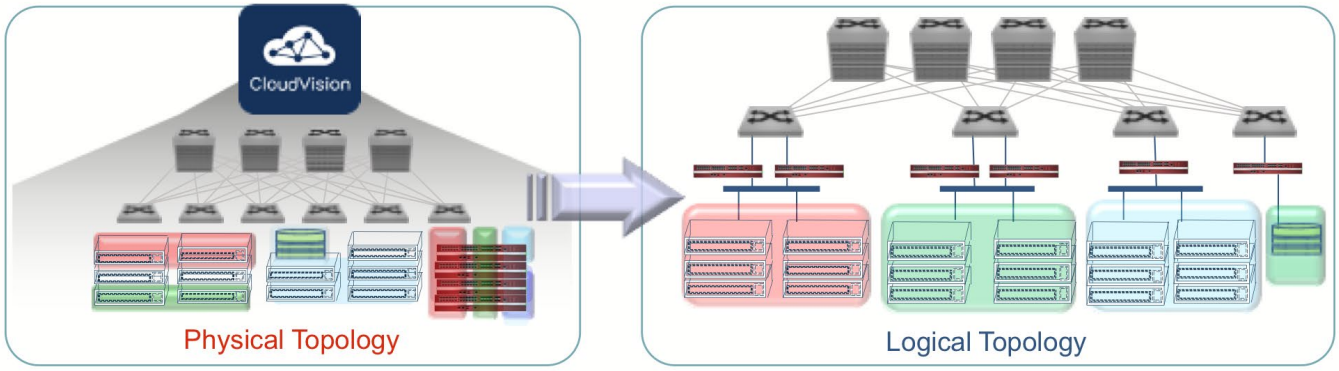
Complicating this situation are the range of design considerations for the cloud data center operator and application users imposed by legacy applications and network architectures. Migrating from legacy network architectures to modern leaf-spine architectures improves network performance, but offers little mitigation for security risks as there is no longer a natural insertion point for firewalls. A more holistic network-wide segmentation approach at the macro- and micro-level is now the mandate to mitigate security threats. This has been addressed in part by the implementation of distributed fine-grain security services within networking and computing hypervisors, often called micro-segmentation. The current compromised security deployment models must change to allow dynamic placement of security services and devices within and around the cloud to protect workloads and data from outside threats as well as from those threats that have already breached the perimeter, while enabling the agility for which the cloud data center was built to begin with.

**Table 1: CloudVision MSS - An open dynamic service for any workload and any application**

| Workload / Workflows | Requirement | Solution |
|---|---|---|
| Ingress-egress from the cloud | Stateful and heuristic protection from external cyber-threats and attacks | High performance next-generation firewalls and security & network monitoring |
| Inter-VM and Intra-Tenant (inside the tenant perimeter) | Isolation of workloads within tenant groups from each other and between tenants | Micro-segmentation of hypervisor workspace and embedded virtual instances of stateful firewalls |
| Extra-VM and intra-tenant (hybrid cloud environment) | For workloads utilizing bare-metal (non virtualized) storage and server resources in combination with hypervisor resident components of micro-segmentation | Strong segmentation of resources within and across the cloud network - a hybrid solution of network + firewall providing control, plus dynamic insertion of stateful next- generation firewalls + advance network monitoring |
| User to application (inside trusted zones) | Segmented access to applications within tenant groups based on privilege levels | Access to resources enforced via strong segmentation of resources in firewalls in combination with AI based network detection and response |

**The Role of Arista Macro-Segmentation Service - Firewall**

Macro-Segmentation Service - Firewall is a complement to fine-grained security services delivered via micro-segmentation, which is implemented in the virtual switch of the physical host on which a VM is running. The delivery of enhanced micro-segmentation security via platforms like VMware NSX is one of the most significant features enabled by network virtualization. Macro-segmentation extends the concept of fine-grained intra-hypervisor security to the rest of the data-center by enabling dynamic insertion of services for physical devices and non-virtualized devices. It is specifically aimed at physical-to-physical (so-called P-to-P) and physical to virtual (P-to-V) workloads.




Macro-segmentation provides a software-driven dynamic and scalable network service to insert security devices into the path of traffic, regardless of whether the service device or workload is physical or virtual, and with complete flexibility on placement of service devices and workloads.

## Arista MSS Firewall - Key Characteristics

MSS Firewall is one of the services enabled by Arista CloudVision. Since CloudVision maintains a network-wide database of all state within the network, it is aware of where every workload is within the network, and it learns in real time about new devices or workloads that are added or removed from the network, or moved across ports or servers.

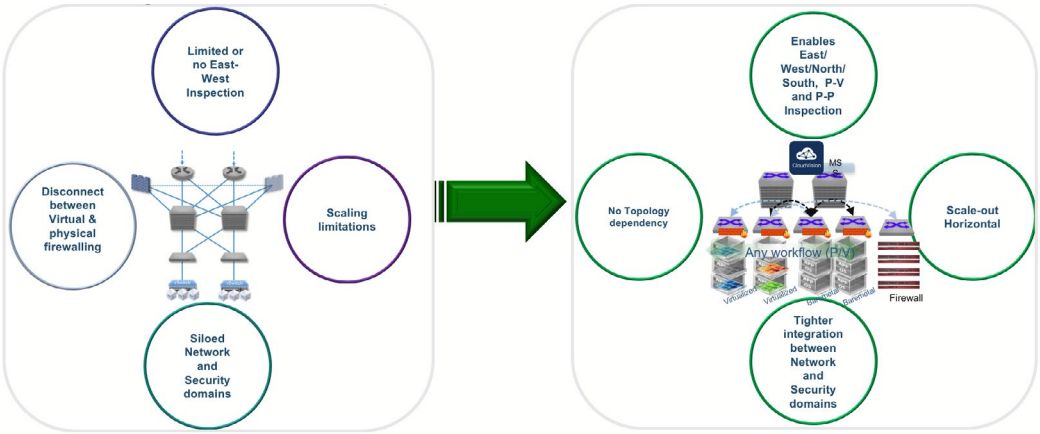
- **Complete flexibility on locality of devices:** Service devices such as firewalls or load balancers can be anywhere in the network on any switch. This allows larger data centers to centralize their security devices in a service rack and insert them in the path between any workloads on-demand or based on a firewall policy. There are no restrictions or limitations on where the service devices are physically attached within the fabric. Likewise, devices to whom services are targeted can be located anywhere in the network with no restrictions or limitations on physical placement.
- **No new frame formats:** There is no requirement for any new frame format, traffic steering or metadata in any new header fields. Macro-Segmentation inserts service devices into the path of traffic without requiring any new frame format, protocol, or anything else that is proprietary. This allows traffic to be monitored by existing tools and ensures that any platform can be easily integrated without modifications.
- **Non-proprietary:** Standards-based forwarding is used to stitch service devices into the path of traffic. To emphasize just how open the approach is, MacroSegmentation can fully function if the network is comprised of devices from multiple vendors.
- **Dynamic:** Hosts can and do move (vMotion and Disaster Recovery), so services and dynamic service insertion should move with them. This is automatically accomplished with Macro-Segmentation and Arista VM Tracer.
- **Enhances next-generation firewalls:** Arista's Macro-Segmentation Service does not try to "own policy" or run a controller-of-controllers that understands every application flow or interaction. Customers prefer to define security policies within the security tool framework, such as the next-generation firewall manager.

**Support for Next Generation Security Platforms: An Open Ecosystem Approach**

By integrating with native APIs provided by the leading next-generation firewalls — native APIs that already exist — macro-segmentation learns which workloads the security policy needs to address or monitor. If the security policy requires a specific logical network topology, then the macro-segmentation service can instantiate that topology into the network. Network can complement the firewall by offloading policies for enforcement, learnt from the firewall, at the edge as the workflows access the network. The automation capabilities of Arista Macro-Segmentation security operate automatically, in real-time, and without any need for a network operator to engage the security administrator (or vice-versa). Furthermore there is no need for the network to be architected in a manner specific to a particular workload. This flexibility is crucial to successful deployment of security in an enterprise private or hybrid cloud.

## Conclusion

Macro-Segmentation Service - Firewall with Arista CloudVision enables flexible deployment of security in the network, without forklift upgrades and without any proprietary lock-ins.




It works in unison with server, storage, and network virtualization solutions from Arista's partners. Macro Segmentation Service complements the intelligence and functionality these provide with enhanced deployment of physical workloads and security services to enable deployment of the complete software defined data center.

**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 & B, 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