FORESCOUT

ARISTA

# Accelerate Zero Trust and Innovation

## Streamline network configuration and group-based segmentation enforcement while fostering new network innovation

"IoT and network-enabled device technologies have introduced potential com-promise of networks and enterprises... Security teams must isolate, secure and control every device on the network, continuously." [1]

*Forrester Research*

The need for digital transformation has resulted in many flat, interconnected networks to support the rapid growth of cyber assets across an organization's digital terrain. The inherent vulnerabilities of these networks and the inability to dynamically adjust security controls puts organizations at risk for widespread threat propagation with damaging consequences. As organizations move to adopt zero trust security practices, progress is often limited due to complicated deployments and costly business disruptions.

Other challenges include:

- DIfficulty establishing and enforcing effective segmentation policies without complete device context
- Disparate, inconsistent policy and network management across multiple network silos and enforcement points
- Inability to dynamically adjust policy enforcement for new or transient cyber assets regardless of when or where connectivity occurs

## Dynamically reduce cyber risk and scale to support innovation

Arista and Forescout have joined forces to provide an integrated solution that helps boost network performance while reducing network administration through the delivery of dynamic network segmentation. The partnership enables you to rapidly enforce zero trust security practices and support innovation without being locked into a single vendor's ecosystem. It can help you:

- Simplify network administration and group-based segmentation policy design and management using real-time device context

1. Mitigating Ransomware With Zero Trust: Bolster Your Defenses With Zero Trust Principles and Techniques, June 8, 2020, Forrester Research

## Arista CloudVision and EOS Innovation

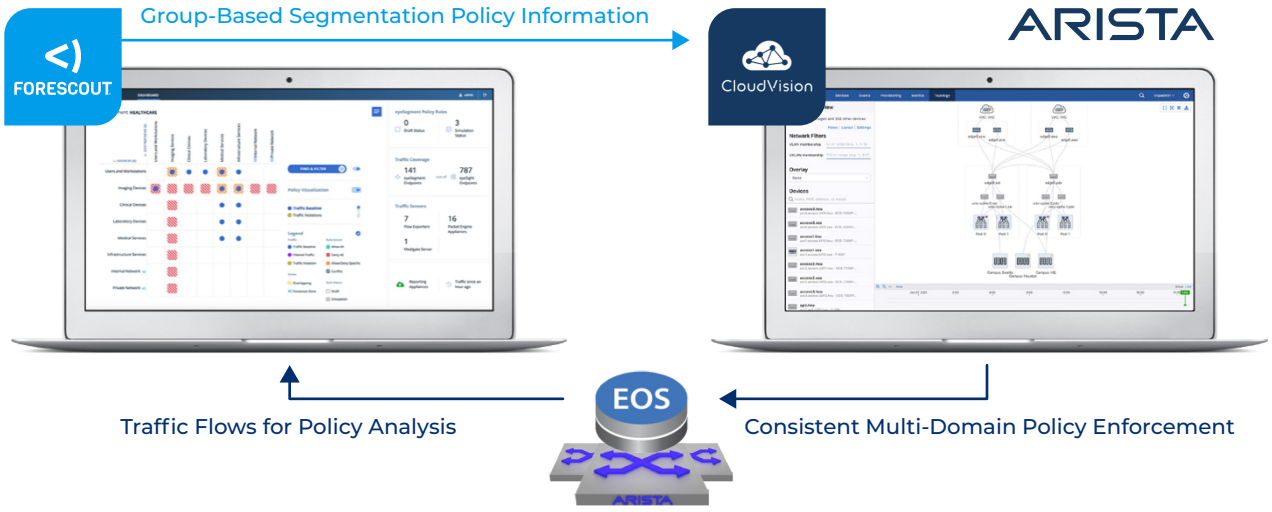
Key advantages of Arista CloudVision and EOS:

- Cloud scale architecture, with unprecedented visibility into appliance performance
- High availability through self-healing resiliency
- Open and programmable to provide automated network workflows
- Flexible consumption models
- Modern, multi-domain network management

- Dynamically reduce attack surface with consistent policy enforcement regardless of when or where devices connect
- Prevent unauthorized communications by monitoring traffic flows among group-based segments
- Increase device and regulatory compliance from endpoint to network
- Operate more efficiently with orchestrated security and network management workflows
- Scale network performance when needed without compromising security controls across multivendor network environments

## Rapidly establish zero trust segmentation with closed-loop workflows

Forescout and Arista have simplified granular enforcement by orchestrating workflows across device identity, logical group creation, group-based segmentation policy design and enforcement. This accelerates zero trust policy deployment while unifying network and security management.




### Forescout Continuum

- Device identification to security group classification
- Policy design/decision point
- Policy compliance monitoring

### Arista

- Network-wide deployment
- Network infrastructure change management & orchestration
- MSS Group enforcement

## SIMPLIFY THE JOURNEY TO ZERO TRUST

# Easily design and enforce business logical group-based segmentation

Forescout Continuum integrates with Arista CloudVision®, the core management platform of Arista's Multi-domain Macro-Segmentation Service® Group (MSS Group) solution architecture. You can use Continuum's device and user context to easily create, simulate, manage and monitor business logical groups as a foundation for segmentation policy design. The integration shares production-ready policy information, including Group ID, member IPs and group communication rules with CloudVision to consistently enforce segmentation policies across campus, data center and cloud network domains via the MSS Group architecture.

Now you can apply real-time context and abstract policy logic from static IP or fixed network segment requirements. As Forescout detects new devices or observes changes in already-connected devices, it automatically assigns those devices to the appropriate segmentation group with its corresponding policy rules, which CloudVision then immediately enforces. Confidence in your zero trust architecture is also enhanced with these unique capabilities:

- Analyze policy-driven traffic flows to ensure group-to-group communications are legitimate and performing as expected
- Highlight simulated and actual traffic violations so you can fine tune policies accordingly
- Manage and track all resulting network configuration changes for analysis and auditing

## ENTERPRISE-SCALE NETWORK SECURITY

# Reduce risk and achieve your network's desired compliance state

Modern networks are under constant strain from both the increasing number and diversity of connected assets, and the threats they face. Network security solutions must be real time and adaptable to first understand and then combat these challenges and threats. Organizations need a force multiplier that can continuously enforce policies for all connected assets across different network vendor environments and domains. This requires automated cybersecurity, with data-powered insights to consistently enforce policy-driven controls – regardless of what, where or when assets connect.

The Forescout Continuum Platform integrates with Arista's wired and wireless campus, data center and cloud network architectures as well as all other major network infrastructure vendors' environments. Forescout provides continuous visibility and automated workflows for network security without requiring major infrastructure upgrades or lengthy deployment cycles. Continuum also lets you:

- Continuously assess the compliance state of all connected cyber assets
- Uniquely classify and score the security risk state of assets
- Automatically contain high-risk or compromised assets with policy-driven network enforcement
- Optimize security and network operations efficiency with orchestrated workflows to mitigate and remediate incidents or threats

## OPTIMIZE INNOVATION

## Embrace digital transformation with network performance and security enhancements without vendor lock-in

Together Arista and Forescout can help you rapidly increase operational efficiency and effectiveness. Arista's performance and management benefits can be easily added where needed while maintaining consistent security controls across the digital terrain with Forescout Continuum. Achieve higher network and security performance, scalability, and value at a lower cost of ownership through:

- Cognitive network management and quality validation via Arista's Extensible Operating System (EOS®) and multi-domain software-defined management platform, CloudVision
- Continuous visibility and centralized policy management via Forescout Continuum to drive consistent security controls across Arista and multivendor network environments
- Business logical and dynamic network segmentation through group-based policy enforcement that leverages real-time device, user and network context — without relying on agents, 802.1X, proprietary tagging methods, network upgrades or vendor lock-in

**Contact us** at alliances@forescout.com to discuss how Forescout and Arista can accelerate your zero trust journey while fostering high-quality network innovations without vendor lock-in.

FORESCOUT®

**Forescout Technologies, Inc.**
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com