FORESCOUT
Active Defense for the Enterprise of Things™

ARISTA

Accelerate Zero Trust and Innovation

Streamline network access control and group-based segmentation enforcement while fostering new network innovation

The need for digital transformation has resulted in many flat, interconnected networks to support the rapid growth of Enterprise of Things (EoT) connected devices. The inherent vulnerabilities of these networks and the inability to dynamically adjust security controls puts organizations at risk for extensive threat propagation and damaging consequences. As organizations scramble to increase security with a Zero Trust architecture, progress is often limited due to complicated deployments and costly business disruptions.
Other challenges include:

- Lack of device context makes it difficult to establish and enforce effective segmentation policies
- Disparate, inconsistent policy and network management across multiple domains
- Inability to dynamically adjust policy enforcement for new or changed devices regardless of when or where connectivity occurs

> **"IoT and network-enabled device technologies have introduced potential compromise of networks and enterprises…Security teams must isolate, secure, and control every device on the network, continuously."[1]**
>
> **FORRESTER RESEARCH**
> **JUNE 2020**

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 and dynamically deliver network access control (NAC) and granular segmentation. The partnership enables you to rapidly achieve Zero Trust and support innovation without vendor lock-in. It can help you:

- **Simplify network access control and group-based segmentation** policy design and management using real-time EoT device context

- **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 where needed without compromising security controls** across multivendor network environments

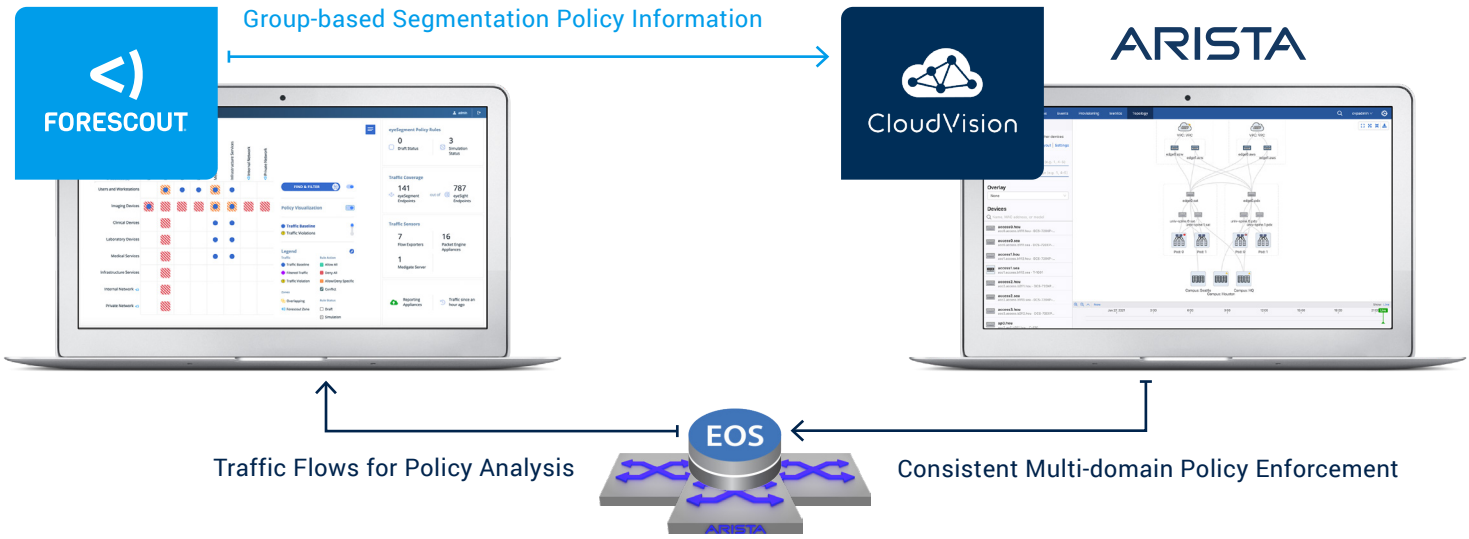
Rapidly establish Zero Trust segmentation with closed-loop workflows

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

SECURE & INNOVATE YOUR NETWORK WITH EASE

This unified solution from Forescout and Arista lets you:

- Enable non-disruptive and dynamic group-based segmentation
- Accelerate Zero Trust segmentation projects with confidence
- Reduce the risk of business disruption
- Reduce operational cost
- Rapidly adapt to compliance and regulatory requirements
- Scale network performance without compromising security



FORESCOUT

- 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 ZERO TRUST

Easily design and enforce group-based segmentation

Forescout eyeSegment integrates with Arista CloudVision®, the core management platform of Arista's Multi-domain Macro-Segmentation Service® Group (MSS Group) solution architecture. You can utilize eyeSegment's device and user context to easily create, simulate, manage and monitor group-based segmentation policies. The integration shares production-ready eyeSegment 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 eyeSegment group with its corresponding policy rules, which CloudVision then immediately enforces. Confidence in your Zero Trust deployment is also enhanced with these unique capabilities:

- eyeSegment lets you analyze policy-driven traffic flows to ensure group-to-group communications are legitimate and performing as expected
- eyeSegment highlights simulated and actual traffic violations so you can fine tune policies accordingly
- CloudVision manages and tracks all resulting network configuration changes for analysis and auditing

ENTERPRISE-SCALE NAC

Reduce risk and increase compliance with multi-domain NAC

Modern NAC solutions must continuously enforce policies for all connected devices across different network vendor environments and domains. This requires centralized policy management with exceptional levels of interoperability to consistently enforce policy-driven controls -- regardless of what, where or when devices connect. The Forescout 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 policy-driven access control without requiring agents, 802.1X, major infrastructure upgrades or lengthy deployment cycles. Forescout also lets you:

- Continuously assess devices for compliance or compromise
- Automatically contain threats with policy-driven network actions
- Optimize security and network operations efficiency with orchestrated workflows to mitigate and remediate incidents

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 performance and management benefits can be easily added where needed while maintaining consistent security controls enterprise-wide through Forescout. You can more easily 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 Enterprise of Things visibility and centralized policy management via Forescout to drive consistent security controls across Arista and multivendor network environments
- Dynamic NAC and segmentation policy enforcement based on real-time device and user profiles — without relying on agents, 802.1X, proprietary tagging methods, network upgrades or vendor lock-in

HOW QUALITY AFFECTS CUSTOMER SUCCESS

Quality and customer satisfaction are also driving principles for Arista and Forescout, which is reflected by two of the highest Net Promoter Scores in the industry. Commitment to quality has also allowed Arista to drive down Common Vulnerabilities and Exposures (CVEs). In fact, Arista has the lowest Technical Assistance Center calls per 100 switches in the industry.

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.

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

Don't just see it. Secure it.™

Contact us today to actively defend your Enterprise of Things.

www.Forescout.com alliances@forescout.com www.Arista.com

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com and Arista.com