FORESCOUT

ARISTA

Solution Brief

Forescout and Arista

Reduce costs and manage risks with integrated network access control and intelligent infrastructure

"We like that the Forescout platform is vendor-neutral; it works in our heterogenous environment as is, without having to do any type of upgrades to closet switches or other infrastructure."

— Dale Marroquin
Information Security Officer
Credit Human Credit Union

Challenges

The challenges of securing today's networks continue to evolve as the networks and devices themselves undergo radical change to address new business demands. As organizations scramble to enable digital transformation, maximize operational efficiencies and leverage data from new systems and device types, they must address the reality that multivendor networks are the new normal, especially given the pace of mergers and acquisitions. These networks—and network access—must be effectively managed. What's more, given the relentless pressure of today's sophisticated cyberthreats, innovative solutions must be put in place to address the following challenges:

Enabling and securing IoT and IT devices

- A lack of comprehensive and granular IoT and IT visibility results in network blind spots and makes it extremely difficult to accurately identify and assess devices as well as analyze their compliance and behavior
- Most IoT devices don't support agents/supplicants, so traditional authentication standards such as 802.1X cannot authenticate IoT devices
- The recent exponential growth in numbers of IoT devices greatly increases the attack surface of enterprise networks

Planning and enforcing network segmentation

You can now use the Forescout platform to accelerate the design, planning and deployment of network segmentation across the extended enterprise. New capabilities help you:

- Know and visualize traffic flows
- Design and simulate segmentation policies
- Monitor and respond to enterprise infrastructure controls

Strategic alliances such as the Forescout-Arista partnership can strengthen and further automate seamless segmentation enforcement across multivendor switching infrastructure.

Network management and access control are too complex and expensive

- Disparate architectures, OS images and system configurations are complex and cost-prohibitive to maintain. A single, consistent approach is needed that spans campus wired and wireless, data center and cloud network environments.
- It's difficult to provision the proper level of access based on users and device types (corporate, guest, BYOD, IoT, unauthorized, etc.) while controlling rogue systems
- Proprietary solutions that only work well with a single vendor are unacceptable; an architecture that works well with multiple vendors is required to avoid redundant tasks, network blind spots and the likelihood of human error

Cyber risks are growing and increasingly difficult to manage

- Companies face increased risk of business disruption and theft of intellectual property from malware and ransomware
- Manual control and compliance enforcement methods cannot keep pace with noncompliant, rogue and unknown devices
- Device communication patterns must be continuously monitored to establish normal traffic baselines and detect anomalous behaviors—especially within IoT devices

The Solution

Arista and Forescout have joined forces to reduce cyber risk by providing policy-driven network access control (NAC), cognitive network management and dynamic segmentation across campus, data center and cloud environments. Specifically, this partnership will enable Arista and Forescout customers to boost network performance, increase compliance and better secure heterogeneous networks by:

- Improving visibility and control of devices on wired, wireless and VPN networks
- Increasing security and reducing operating expense
- Accelerating incident response and Zero Trust enforcement

Real-time network access control across network domains

NAC solutions must work seamlessly within multivendor infrastructures. Increasingly, this requires greater levels of technical integration, intelligence sharing and interoperability certification to ensure consistent and automated access control enforcement in today's mixed environments.

With Forescout's device visibility and control platform, you can gain complete situational awareness, automate access control and orchestrate actions across your heterogeneous network environment—without requiring agents, infrastructure upgrades or lengthy deployment cycles. It lets you continuously assess devices and respond to policy violations in real time to:

- Reduce the risk of business disruption from security incidents or breaches
- Help ensure and demonstrate security and regulatory compliance
- Increase security operations productivity

Benefits

- Gain complete endpoint and network traffic visibility and control without relying on agents
- Dynamically control IT and IoT devices across wired and wireless networks
- Improve security posture by keeping noncompliant and compromised devices off Arista and non-Arista networks
- Understand the network state and respond to cyber incidents in real time
- Continuously enforce IT and security compliance enterprise-wide across all wired and wireless devices
- Identify and isolate or block rogue and noncompliant devices
- Incrementally add new network functionality or devices without replacing existing infrastructure
- Increase network performance and security within multivendor environments

Arista's Cognitive Campus Network leverages the Arista Extensible Operating System (EOS®) and CloudVision®, extending the Universal Cloud Network architecture to Cognitive Campus Networks. These critical services use the same binary EOS image and database across Arista's entire product line to:

- Automate deployment, configuration, visibility, troubleshooting and security across wired, wireless and cloud environments
- Simplify management and quality validation across various workloads in the campus and data center
- Deliver higher performance, scalability and value at a lower cost of ownership

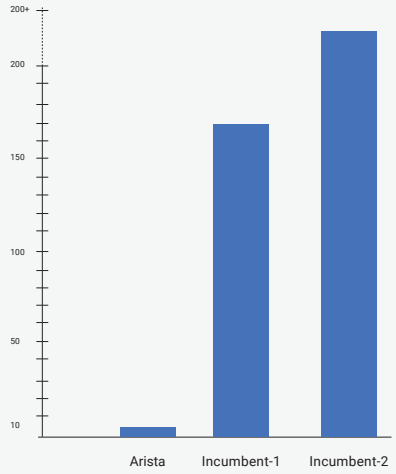
How Quality Affects Customer Success

Quality and customer satisfaction are driving principles within Arista and Forescout, which is reflected by two of the highest Net Promoter Scores in the industry.

Forescout delivers industry-leading customer satisfaction scores in day-to-day operation of the Forescout platform at greater than a 93% cumulative average in 2019 and reported field defect rates of less than 2%.

Commitment to quality has 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.

Total CVEs 2014-2019



Gain in-depth visibility and control of IoT and IT devices

Just one undetected threat can undermine the security and reputation of an organization in minutes. That's why complete visibility of all connected devices at all times is key.

- Discover, classify and assess all IoT and IT devices in real time without requiring agents
- Continuously monitor device hygiene and enforce compliance by automating host and network controls
- Orchestrate information sharing and workflows with third-party security platforms to close security gaps

Scale network performance and access management

Forescout and Arista have a proven track record for enterprise scalability and performance:

- Forescout customers support 2 million devices in a single deployment across IT, OT, campus, data center and cloud environments
- Arista customers support over 20 million ports in total and over 20,000 wireless access points in a single deployment

Increase network security and reduce operating expense

The Arista-Forescout partnership can help you quickly neutralize threats while reducing costs.

- Automate NAC to reduce the attack surface
- Provision appropriate network access based on user role, device type, device ownership and device hygiene—with or without 802.1X
- A single software image across all switches provides consistent features and management providing low operational costs

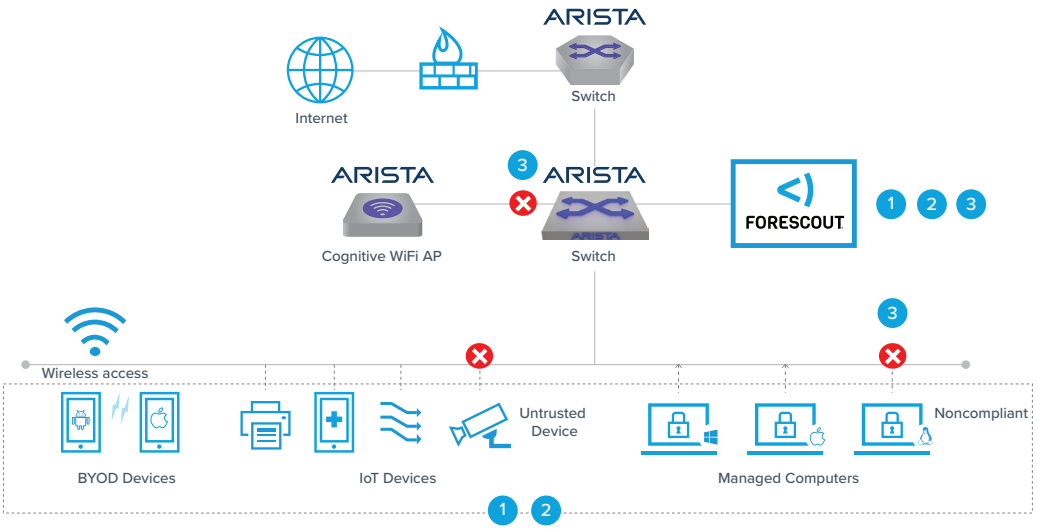
Accelerate incident response

Respond with actionable insights and real agility.

- Quickly identify security incidents such as Mirai, WannaCry and IoT Reaper
- Mitigate threats by automating network response through tight integration with Arista infrastructures (quarantine VLAN, switch block, etc.)
- Minimize lateral threat propagation by dynamically enforcing segmentation to limit device access to only required services

How It Works

Real-Time Network Access Control



1. Forescout discovers and auto-classifies wired and wireless devices by device function, OS, vendor and model—without using agents.
2. Forescout assesses devices to identify vulnerable and noncompliant devices.
3. Based on security polices, Forescout triggers auto-remediation/limits network access by enforcing network controls (VLAN, CoA, switch block, etc.) on Arista network infrastructure.

FORESCOUT

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

To learn more, contact Arista@Forescout.com or visit Forescout.com and Arista.com.