Arista WIPS

World's Top-Ranked Wireless Intrusion Prevention System

Introduction

Wireless LAN (WLAN) infrastructure attacks are one of the most critical and immediate threats to enterprise networks. To make matters worse, the consumerization of Wi-Fi is flooding enterprises with personal Wi-Fi enabled smartphones, tablets and IoT/IIoT devices, which are inadvertently tearing down the network security perimeter; even organizations without an official WLAN are at risk. Arista's WIPS provides enterprises with the most comprehensive and continuous protection against current and emerging wireless threats.

C-230 / C-230E

C-230/C230E

Indoor, 4x4x4 (5GHz) 2x2x2 (2.4 GHz) Wi-Fi6

- Third multi-functional radio
- Internal/External Antenna model

Can operate as:

- Dedicated WIPS sensor, or
- WiFi access point with background scanning

C-260

C-260

Indoor, Dual radio 8x8x8 (5 GHz)
Wi-Fi 6 device that can operate as:

- Dedicated WIPS sensor, or
- WiFi access point with background scanning

Third Multi-functional radio

C-360

C-360
Indoor, Tri-radio 4x4x4 Wi-Fi 6E device that can simultaneously operate as a Wi-Fi 6E access point and a dedicated WIPS sensor,
Fourth Tri- Band Multi-Functional radio

Accurate Location Tracking

Arista WIPS can pinpoint the physical location of any detected Wi Fi device or interference source. As a result security administrators can readily track down such devices and take action.

Both real-time locations (for devices currently active) and historic locations (for devices which may have participated in a security incident in the past) are available. Arista's self-calibrating sensors and sophisticated stochastic models go beyond simplistic RF triangulation to enable accurate location tracking without the need for RF site surveys.

Location-based Policy Management

Arista WIPS simplifies the administration of geographically distributed locations through customizable policies defined on a region-by-region, site-by-site or even floor-by-floor basis. The hierarchical location-based management architecture allows network administrators to manage large number of sites from a single console.

Smart Forensics™

Arista's Smart Forensics simplifies wireless forensics by filtering out useless data and presenting only relevant and accurate forensics information in an easy to understand and actionable format. Smart Forensics summarizes all relevant information without the need for cumbersome trace collection and packet-level analysis.

Simplified Regulatory Compliance

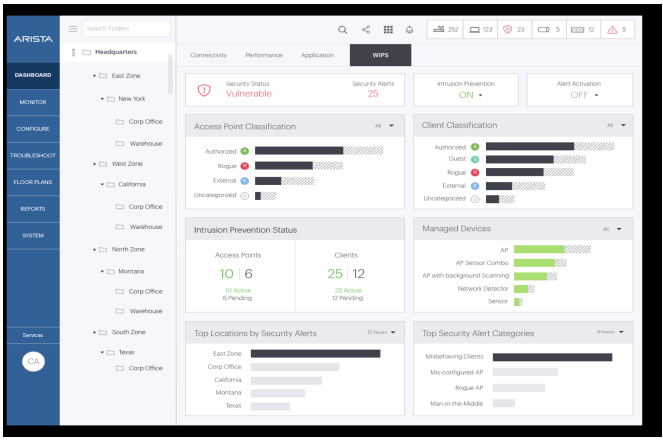
Arista simplifies compliance with regulatory wireless security requirements via automated wireless scanning, consolidated analysis of scan data from multiple locations and ready-touse compliance reporting.

Arista WIPS provides predefined reports that map wireless vulnerabilities to specific data security compliance standards such as DoD Directive 8100.2, PCI DSS, SOX, HIPAA, and GLBA. Network administrators have the option to schedule reports to be automatically generated and delivered to them by email.

Predictive Wireless Performance

Arista WIPS provides 24/7 spectrum analysis capability and alerts administrators of wireless LAN performance problems before they impact end users. It classifies performance issues into various categories such as configuration (e.g. incorrect channel allocation, sub-optimal 802.11n/ac/ax protocol settings), bandwidth (e.g. poor utilization, low average data rate, excessive overhead), and RF (e.g. non Wi-Fi interference, channel crowding).

Remote troubleshooting including remote "live packet capture" from a central console allows network administrators to resolve problems at remote sites quickly without sending IT staff to those locations.



Meets Any Security Need

Arista WIPS can be deployed in different configurations to meet any security need. It can be installed as an overlay security solution on top of your existing WLAN infrastructure or to enforce "No Wi-Fi" policy in highly security sensitive environments where use of Wi-Fi is prohibited. Arista WIPS is also built into Arista Cognitive Wi-Fi™. It can be used in an integrated mode in Arista APs through background scanning.

Integration and Interoperability

With the broadest integration of any WIPS solution, Arista lowers deployment and operational costs by integrating with most major WLAN infrastructure and MDM solutions. This integration creates a seamless workflow and eliminates inefficiencies, making it easier to manage WLAN security and performance.

Arista also interoperates with standard enterprise management and reporting platforms including ArcSight, SNMP and Syslog interfaces provide the flexibility to integrate Arista's wireless events with virtually any centralized event management tools.

Flexible Delivery Models

A variety of deployment and pricing options cater to enterprises of every industry and size. Arista WIPS, offered as a part of Arista's cloud managed platform, can be hosted and managed from Arista's public or private cloud. Enterprises can alternatively choose to host and manage Arista WIPS from a VMware server installed on-premise. Regardless of the deployment model, Arista WIPS sensors can be managed centrally, at any number of geographically distributed sites, from a single HTML5 console.

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