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 WiFi is flooding enterprises with personal WiFi enabled smartphones and tablets, which are inadvertently tearing down the network security perimeter; even organizations without an official WLAN are at risk. Arista WIPS provides enterprises with the most comprehensive and continuous protection against current and emerging wireless threats.

Key Features

- Automatically detects, blocks and locates all types of wireless threats
- Patented Marker Packet™ techniques eliminate false alarms in 'on wire' Rogue AP detection
- Secure BYOD policy enforcement
- Off-line sensor mode for fault-tolerant continuous policy enforcement
- 24/7 Spectrum analysis
- Detects and locates 'non WiFi' interference & RF jamming
- Smart Forensics™ for quick resolution of wireless incidents
- Remote troubleshooting including remote "live packet capture"
- Management options include virtual server or cloud

Unmatched Wireless Protection

Powered by Arista's portfolio of patented wireless intrusion detection and prevention techniques, Arista WIPS provides 24/7 visibility into and complete control over wireless activity in the enterprise airspace.

Automatic device classification

Using Arista's patented Marker Packet™ techniques, Arista WIPS automatically and quickly classifies wireless devices detected in the airspace as Authorized, Rogue and External. As a result it eliminates false alarms and saves security administrators the effort of defining complex rules to identify rogue wireless devices or manually inspecting devices. This contrasts the error-prone device classification integrated into most other WLAN solutions, which rely on slow and inconclusive CAM table lookups and MAC correlation, signatures, or passive wired network sniffing.

Comprehensive Wireless Threat

Arista WIPS provides the most comprehensive protection from all types of wireless threats, including Rogue APs, Soft APs, Honeypots, WiFi DoS, Ad-hoc networks, Client misassociations, and Mobile hotspots. Security administrators are not required to define complex signatures for threat detection, which is the case with other WIDS/WIPS solutions. Arista WIPS takes a fundamentally different approach by focusing on the primary threat vectors and vulnerabilities that form the building blocks for all known and emerging WiFi hacking attacks and tools.

Automatic Threat Prevention

Most wireless IDS/IPS solutions do not encourage automatic over-the-air prevention for fear of disrupting own or neighboring WiFi networks. Because of Arista's accuracy in distinguishing genuine wireless threats from neighboring WiFi devices, Arista customers effectively and confidently use its automatic prevention capability to block any misuse of WiFi or violation of enterprise security policies.

Arista WIPS intelligently chooses from various patented over-the-air and on-wire prevention techniques depending on the type of wireless threat, and is capable of simultaneously blocking multiple threats across multiple channels in 2.4 GHz and 5 GHz frequency bands.

Secure BYOD Policy Enforcement

In today's Bring Your Own Device (BYOD) culture, the omnipresence of smartphones and tablets poses an immediate threat to enterprise networks. Authorized users need only their enterprise login credentials to connect unapproved personal devices to WPA2/802.1x secured WiFi networks and access sensitive enterprise assets. Data leakage on unapproved personal devices, malware and viruses, and "tethering" Soft APs and Mobile hotspots can compromise enterprise data security. Arista WIPS can automatically fingerprint all types of smartphones and tablets, and enforce a secure BYOD policy by blocking unapproved devices from getting onto the enterprise network.

Demo

Want to learn more? An intimate demo is the best way to learn more about Arista and what we can do to bring you the best wireless security platform for every need.

Evaluation

After we show you what Arista WIPS is all about, we want you to see it for yourself. Be sure to contact Arista Sales and ask us about demo units.

Contact us

408-547-5501
sales@arista.com
www.arista.com

Federal agencies can contact:
federal.sales@arista.com

C-120

Dual radio 4x4 802.11ac Wave 2 device

- FIPS and Common Criteria certified for WIPS

Can operate as:

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

The tri-radio variant, C-130, can simultaneously operate as an access point and a dedicated WIPS sensor.

C-100

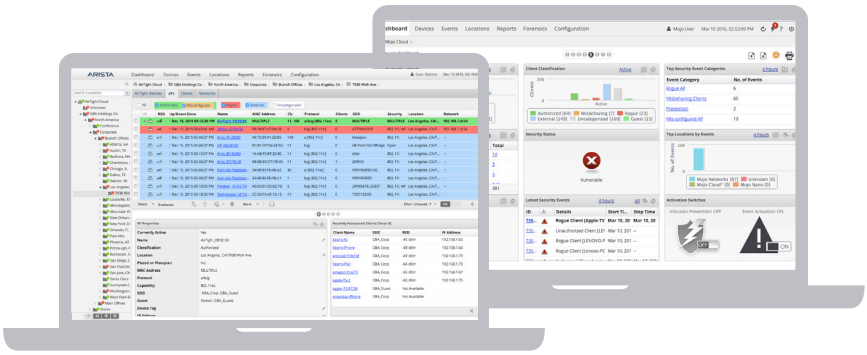
Dual radio 2x2 802.11ac Wave 2 device that can operate as:

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

The tri-radio variant, C-110, can simultaneously operate as a WiFi access point and a dedicated WIPS sensor.

W-118

Tri-radio 2x2 802.11ac Wave 2 wall plate device that can simultaneously operate as a WiFi access point and a dedicated WIPS sensor.



Accurate Location Tracking

Arista WIPS can pinpoint the physical location of any detected WiFi 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 protocol settings), bandwidth (e.g. poor utilization, low average data rate, excessive overhead), and RF (e.g. non WiFi 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 WiFi" policy in highly security sensitive environments where use of WiFi is prohibited. Arista WIPS is also built into Arista Cognitive WiFi™. 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