CloudVision

Key Features

- Centralized configuration and policy management
- Cognitive cloud-based network baselining and troubleshooting with root cause analysis engine
- WiFi analytics for business intelligence
- Wireless Intrusion Prevention (WIPS)
- Application Visibility and Control
- Visual packet trace and analysis
- Wireless Access Security
- Client location tracking
- Wired-wireless monitoring
- Multifunctional management of 3rd radio for client emulation and intelligent RF optimization
- API Integration
- Cloud and On-Premises options

Overview

Harnessing the power of the cloud, big data analytics, machine learning and automation, CloudVision WiFi brings the power of intelligence, speed and accuracy to wireless networks. Through root cause analysis and proactive problem resolution options, CloudVision WiFi reduces the mean-time-to-resolve problems, minimizing network troubleshooting effort while reducing total cost of ownership.

Enterprise ready cloud architecture

CloudVision WiFi’s cognitive management plane simplifies configuration, troubleshooting while delivering richer telemetry to network administrators. A centralized management plane remarkably simplifies policy management and provisioning of WiFi networks. A flexible data plane allows wireless access points to provide customizable traffic redirection at the network’s edge. A distributed control plane enables enterprise WiFi features without the scalability issues of older architectures - and an innovative cognition plane with streaming telemetry automates WiFi network monitoring and troubleshooting to optimize the WiFi user experience and minimize the mean time to resolution (MTTR) for network access and performance issues.

Arista Network Design

Simplicity Redefined

Centrally managing a WiFi network has many advantages - it is simple to change a network configuration globally, physically locate a WiFi device, view real-time or historical experience of WiFi users or capture and visualize a packet trace from a remote site.

Mission-critical Reliability

Arista WiFi’s distributed dataplane architecture ensures there is no loss of functionality if connectivity to the management plane is lost. The WiFi network continues to support mission-critical applications and secure airspace at all times. Automated disaster recovery and high-availability ensures users do not experience downtime even in the event of a datacenter- or region-wide incidence.

Federal grade security

The Arista Cloud implements multiple tiers of security—including strong access controls, two-factor authentication, regular vulnerability scanning and management, encryption of data in transit (TLS) and at rest (EBS and S3), and PII data privacy. The security measures certifications are SSAE SOC 2 Type II and FIPS 140-2.
Seamless scalability
With virtually unlimited and elastic availability of storage and compute resources, the Arista cloud eliminates artificial boundaries inherent in controller-based WLAN architectures. Naturally, it enables many innovative, previously unforeseen applications in big data analytics, machine learning and cognitive computing in the context of WiFi.

Flexible Data Plane
The decoupling of data, management and control planes results in tremendous flexibility in data traffic forwarding. Traffic from the Arista APs can be locally routed or tunnelled to a central aggregation, e.g., an Arista switch. APs support VXLAN and EoGRE based tunnelling. The choice of tunnelling protocol depends on the aggregator’s capability to terminate the tunnel using either of the two protocols. This allows enterprises to migrate their existing controller-based WiFi networks to Arista’s controller-less cloud architecture without having to change the design of their underlying campus network. Tunneling of data to a central aggregation point may also be required by certain enterprises for regulatory compliance and by service providers for ease of billing. CV WiFi enables the configuration and monitoring of EoGRE and VXLAN endpoint on WiFi APs. Tunnels can be configured in redundant mode with automatic failover.

Cognitive Management Plane
Arista uses cognitive computing to deliver the best experience possible to WiFi administrators and users

Location Tracking
CloudVision WiFi supports tracking location of any WiFi APs and clients on a floor. It enables visualization of WiFi associations and includes filtering based on client or user information, or connectivity or performance issues. It can be used for mapping of WiFi client connectivity and performance issues in the context of their physical location.

CV WiFi provides information about the wired interface on Arista WiFi Access Points. This includes upstream PoE switch details, DHCP options and VLANs seen by the AP. As this information is gathered from LLDP packets, it is available irrespective of the PoE switch vendor, if it supports LLDP. Information about AP health, in the form of CPU and memory utilization, is also displayed on the UI.

Client Journey™
CloudVision WiFi provides direct and real-time insight into the experience of WiFi clients as they journey on the network. Client Journey tracks when and why clients fail to connect to the network, reporting latencies of network services such as AAA, DHCP, and DNS. Administrators can drill down and access live and historical client connection logs to aid troubleshooting.

Network Baselining
Using machine-learning algorithms on the telemetry it collects, CloudVision WiFi baselines network traffic and automatically detects and highlights anomalies. When necessary it fine-tunes the WiFi network to optimize the user experience and provides recommendations to resolve network problems.

Root Cause Analysis Engine
CloudVision WiFi employs built-in domain expertise and protocol-level intelligence to help administrators maintain the network. In real time, it automatically detects and classifies WiFi clients connection failures and pinpoints the root cause—if it is related to WiFi or to a network service such as DHCP or DNS, a client device or an application. Similarly it automates root cause analysis of poor performance, such as poor coverage, high retry rate and sticky clients.
Single Client Inferencing
WiFi clients may face poor experience due to various reasons. CloudVision WiFi identifies such clients based on RF and application KPIs and then uses the Single Client Inferencing engine for automated root cause analysis of possible problem. This makes it easier to diagnose performance issues of individual clients.

Automatic Packet Capture
CloudVision WiFi preemptively captures packet traces to help diagnose problems. The traces are stored alongside related failures or symptoms to simplify troubleshooting at a later time. Packet traces can be downloaded or directly visualized in Arista Packets, the cloud-based, visual WiFi packet analyzer.

Client Emulation and Network Profiling
CloudVision WiFi employs the 3rd multi-function radio, turning it into a client to run tests and proactively identify problems before users do. This helps validate the network’s readiness for supporting business-critical applications.

Wireless Intrusion Prevention (WIPS)
With the third radio acting as a dedicated wireless intrusion prevention (WIPS) sensor, wireless threats are detected and blocked almost instantly in your network. CloudVision WiFi works with the APs, which are powered by patented techniques such as Marker Packets™, to enable surgical over-the-air intrusion prevention, automatically and accurately creating alerts and classifying wireless threats.

WiFi Analytics
Analytics based on presence and behavior of WiFi devices can provide significant business intelligence, and can inform business functions such as

- marketing research (A/B testing of storefront displays, measure ROI of marketing campaigns, context-based guest engagement)
- operations (staff planning, optimize facility utilization),
- IT (network planning and design based on user density).

The gathered data is based on WiFi device mac addresses collected from probe requests, content analytics and application visibility based on WiFi connections, and engagement analytics based on WiFi users who opt in and choose to share their personal information.

Presence Analytics
Presence analytics provide anonymous, statistical information about the footfall (number of WiFi devices detected), dwell time (duration for which WiFi devices are present) and repeat versus new customers. These trends can be viewed by particular site or aggregated across multiple sites, and across different time periods: intra-day, daily, weekly, monthly and year-over-year.

Intelligent RF Optimizations
Unparalleled visibility in both 2.4 GHz and 5 GHz enables automatic RF optimizations such as band steering, smart steering, auto channel selection or auto transmit power control to maximize WiFi capacity. Real-time application performance is further enhanced with multicast-to-unicast conversion and smart blocking, pruning and optimization of broadcast and multicast traffic.
Engagement analytics
Integration with social networks and third-party loyalty systems can be leveraged to collect demographics and other information from WiFi users who opt in to share their personal details. This in turn can be used to engage with the opt-in WiFi users, e.g., retail business can provide special deals to their loyal customers and convert them into brand ambassadors.

Zone analytics
Zone analytics provide insight into the density and flow of WiFi users by visualizing it on a floor map. This allows administrators to monitor how the various parts of a facility are populated over a period of time. Zones can be demarcated as a region around WiFi APs on a floor map.

Content analytics and application visibility
Web analytics and application visibility based on deep packet inspection can provide insight into WiFi usage pattern and allow you to enforce policies in terms of the type of content or applications that can or cannot be accessed based on the type of WiFi network (e.g., employee vs. guest) and user privileges (e.g., students vs. teachers) and assign the desired quality of service.

Wireless access security and control
With a suite of features to identify users, devices and applications and to control the access and privileges they get on the network, Arista provides a comprehensive solution to enforce context-based policies and protect the network from abuse.

Integration with Google® G Suite
Google G Suite for business or education, can be used to enforce an additional layer of security for WiFi users with Arista’s WiFi integration. No additional hardware, software or license is required. Regardless of whether PSK or 802.1X is being used for authentication, network access control for WiFi users and devices can be enforced based on a users’ Google account privileges and organization unit (OU) membership.

Role Based Control
Role based controls can be enforced on a per SSID basis. Role profiles can be created to match roles configured in the RADIUS server, Google G Suite or both. Rules of precedence can be used to combine settings defined in a role profile and SSID, and enforce policies in terms of role attributes such as VLAN access, firewall rules, application firewall rules, per user bandwidth control and redirection to a captive portal.

APIs and Third-party Integration
With Single Sign-On, powerful Web APIs, and secure tunneling, integrating the Arista Cloud with third-party systems, in-cloud or on-premises, is easy. Both push and pull mechanisms are available. Using custom applications, WiFi analytics can be pulled from the Arista Cloud or configuration and policy changes can be pushed to it. WiFi analytics from the Arista Cloud or directly from the Arista APs can also be pushed to third-party Web services.

Social WiFi
Inbuilt integration with Facebook, Google+, Twitter, LinkedIn, Instagram and Foursquare enables guest on-boarding using social login.

Bonjour® Gateway
Arista APs can be configured as a Bonjour Gateway to allow WiFi clients to discover and access Bonjour services across VLANs. This feature can be enabled on a per SSID basis and works for both static and dynamic VLANs.
Stateful L3-L7 Firewall
Arista APs can enforce SSID-based rules for inbound and outbound traffic based on host or domain name, IP address, port number, protocol, e.g., UDP, TCP, and applications. Leveraging the in-built application visibility engine, rules can be defined to block or allow specific applications, or an entire category of applications, or to mark applications with DSCP for appropriate handling at the network layer.

Mesh Mode
In a wireless mesh network, APs can connect to the network wirelessly eliminating the need to provide a wired network connection to every AP. In such a network, one or more APs connected to the wired network can provide wireless network connectivity to other APs that are not connected to the wired network. Arista WiFi APs can operate in mesh mode where one radio can be configured as a mesh radio while the other radio, or both radios, can be configured to offer WiFi access to clients. The AP connected to wired network is acts as ‘root’ node while the AP(s) connected with the root AP over wireless link are referred to as non-root nodes.

GDPR Compliance
Arista Networks provides General Data Protection Regulation (GDPR) compliant Arista Cloud WiFi to its partners, resellers, and customers in the European Union. The Arista Cloud acts as a GDPR Processor of personal data.

Cloud Integration Point
Whether you are using Arista WIps or transitioning to cloud based WiFi, integrating the Arista cloud WiFi server with your on-premise systems allows you to leverage key advantages of the cloud server while continuing to use your existing infrastructure. It also saves you the time, effort, and cost of installing and maintaining an on-premise Arista WiFi server. A Cloud Integration Point (CIP) is an Arista AP that enables the integration of the Arista WiFi cloud server with existing third-party services on-premises.

The data exchanged between Arista Cloud and an on-premise Cloud Integration Point (CIP) is secured with AES-256 encryption. The CIP contains a firewall that only forwards traffic to the specified local destinations on the defined ports. It also isolates the network with NAT so client connections cannot be established through the CIP.

WiFi controller integration for WIps overlay
Arista Cloud integration with other wireless LAN controllers allow Arista’s WIps solution to fetch information from the controller for WIps classification and tracking the location of devices.

Enterprise Security Management (ESM)
Integration with Enterprise Security Management servers enables Arista Cloud to send events and audit logs to Syslog and ArcSight servers, allowing customers to use their existing logging infrastructure to manage Arista events and logs.
## CloudVision-WiFi System Requirements:

<table>
<thead>
<tr>
<th>Feature/Platform</th>
<th>CloudVision WiFi (Cloud Subscription)</th>
<th>CloudVision WiFi (ESXi on-prem)</th>
<th>CloudVision WiFi (KVM on-prem)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Browser</td>
<td>Safari, Firefox, Chrome, Microsoft Edge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Requirements</td>
<td>NA</td>
<td>Upto a 1000 APs - CPU - <a href="mailto:2vCPUs@2.933Ghz">2vCPUs@2.933Ghz</a> 5866Mhz Reserved RAM - 4096 MB Reserved Hard Disk - 100Gb, Thin Provisioning</td>
<td>Upto a 5000 APs - CPU - <a href="mailto:4vCPUs@2.933Ghz">4vCPUs@2.933Ghz</a> 11732Mhz Reserved RAM - 16384 MB Reserved Hard Disk - 100Gb, Thin Provisioning</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 CPUs RAM - 4096 MB Reserved Hard Disk - 100Gb</td>
</tr>
<tr>
<td>Client Journey</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Application Visibility and Control</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>WIPS</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>RCA Engine</td>
<td>✔</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Baselining</td>
<td>✔</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Packet Capture/ Troubleshooting</td>
<td>✔</td>
<td></td>
<td>Limited</td>
</tr>
<tr>
<td>Network Profiling</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>RF Optimization</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>WiFi Analytics</td>
<td>✔</td>
<td></td>
<td>Limited</td>
</tr>
<tr>
<td>Guest and Captive Portal Management</td>
<td>✔</td>
<td></td>
<td>Limited</td>
</tr>
<tr>
<td>WiFi ACLs</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>RBAC</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Automatic Updates and Upgrades</td>
<td>✔</td>
<td></td>
<td>Customer managed</td>
</tr>
</tbody>
</table>
SKUs Service and Support

Software support for CloudVision-WiFi is included in the CloudVision software subscription license. Hardware support for the CloudVision Physical Appliance requires a corresponding A-Care service contract. Support for each EOS device managed by CloudVision is covered by standard A-Care offerings for each particular device. For more details on A-Care service offerings across all Arista products, see: http://www.arista.com/en/service

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS-COGWIFI-1M</td>
<td>Cognitive Cloud SW Subscription License for 1-Month for 1 x Wireless Access Point</td>
</tr>
<tr>
<td>SS-PREMWIFI-1M</td>
<td>On-premises SW Subscription License for 1-month for 1 x wireless access point. For electronic delivery only; not for sale with DCA-200 appliance</td>
</tr>
<tr>
<td>SS-PREMWIFI-1M-DCA</td>
<td>On-premises SW Subscription License for 1-month for 1 x wireless access point. For sale only with DCA-200 appliance</td>
</tr>
<tr>
<td>SS-PREMWIFI-1M-VM</td>
<td>On-premises SW Subscription License for 1-month for 1 x wireless access point for virtual environment. For electronic delivery only</td>
</tr>
<tr>
<td>DCA-200-CV</td>
<td>1 unit CloudVision Physical Appliance, Model 200 (Includes CVX, CVP and Server). No device licenses.</td>
</tr>
</tbody>
</table>