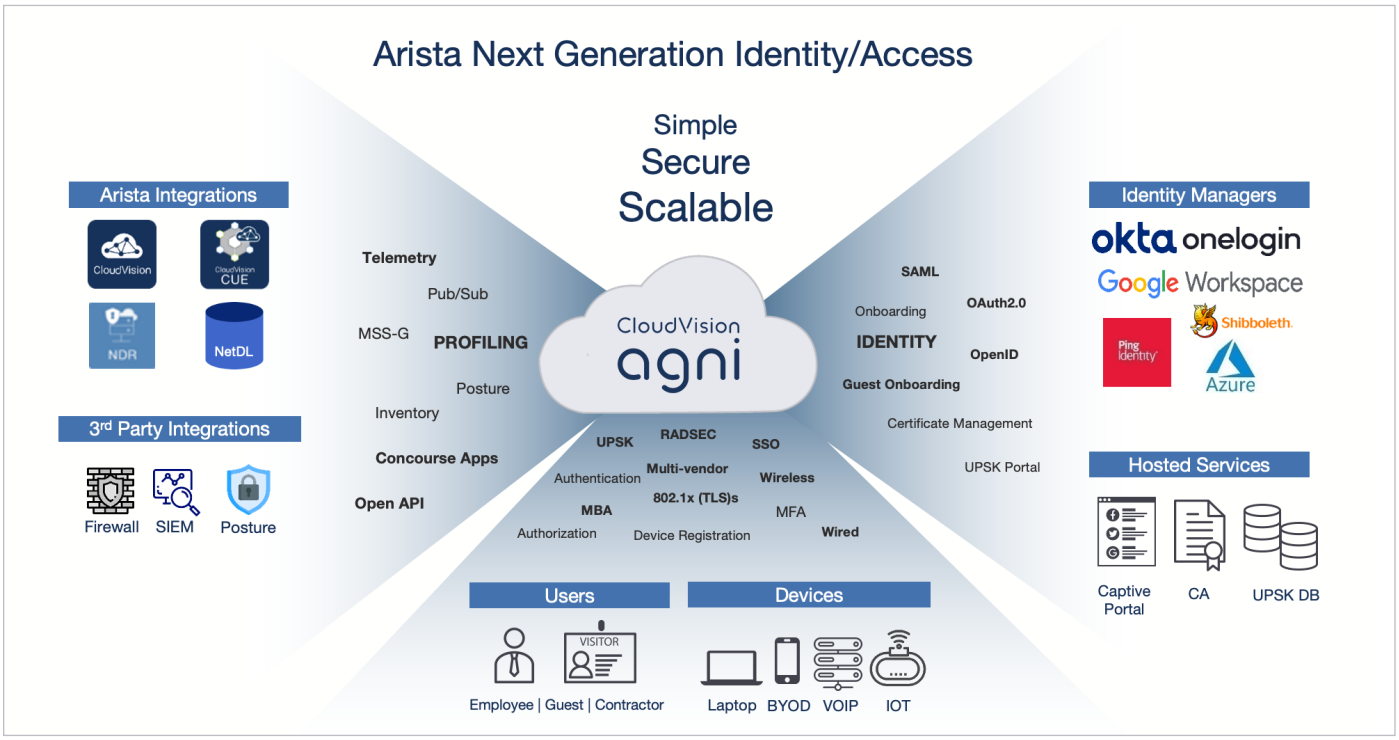
## Key Features

- Centralized configuration and segment policy management
- Simple, Secure, and Scalable next-generation Network Identity solution
- Cloud Native architecture
- Ask Autonomous Virtual Assistant (AVA)
- Microsegmentation with Arista MSS and UPSK
- Profiling and Posturing
- Continuous posture check with Arista NDR solution
- Multi-Vendor Support
- Publisher/Subscriber APIs for 3rd party integration

### Overview

Arista has been at the forefront of the cloud networking revolution, leveraging a software-driven approach based on Cloud Native principles, open standards-based designs, and native programmability to deliver consistent, reliable software solutions. Arista Guardian for Network Identity (CloudVision AGNI) has adopted a similar architectural approach to other products to deliver a state-of-the-art solution for managing network identity. CloudVision AGNI embraces modern design principles, Cloud Native microservices architecture, and Machine Learning/Artificial Intelligence (ML/AI) technologies to significantly simplify administrative tasks and reduce complexities. It offers a comprehensive range of features to meet the requirements of modern networks, including support for scaling, operational simplicity, stability, and zero-trust security.

CloudVision AGNI substantially reduces the total cost of ownership, making it a very cost-effective choice for businesses of all sizes. With its cutting-edge features and advanced technology, CloudVision AGNI is the ideal choice for businesses looking to enhance their network security infrastructure.




**CloudVision AGNI Platform**

AGNI delivers network identity as a service to any standards-based wired and wireless infrastructure. CloudVision AGNI integrates with network infrastructure devices (wired switches and wireless access points) through a highly secure TLS-based RadSec tunnel. This highly secure and encrypted tunnel offers complete protection to communications in a distributed network environment. This mechanism offers much greater security to AAA workflows than the traditional RADIUS environment workflows. Radius is also supported in the on-premises deployment model.

AGNI integrates with Arista products to exchange user and client context, secure micro-segmentation, and authenticate telemetry data. Additionally, AGNI can fetch advanced profiling, posture, and network inventory data to provide comprehensive policy management and insights into network security. The platform's API-first approach enables seamless integration with third-party solutions, allowing for the exchange of user and client context, authentication telemetry, and endpoint protection status. AGNI utilizes its Concourse application plug-in architecture to achieve these integrations.

AGNI natively integrates with leading cloud identity providers (IDPs) through Open Authorization (OAuth2.0) and OpenID Connect (OIDC). This integration facilitates the seamless authentication and authorization workflows needed to support modern use cases.

AGNI provides comprehensive support for Public Key Infrastructure (PKI) and enables onboarding for sophisticated 802.1X use cases by providing complete lifecycle management of client certificates. Organizations can feel confident with the secure enrollment procedure as the private key of the client never leaves the client premises. AGNI offers Arista's Unique PSK (UPSK) solutions to enable secure authentication mechanisms for BYOD, IoT/IoMT, and gaming devices. AGNI extends its feature set to accommodate a wide range of client devices with its support for Captive Portal and MBA authentications.

| Benefit | Details |
|---|---|
| Simplicity | • Self-service and frictionless SSO-based onboarding.<br>• Automated certificates and UPSK provisioning with lifecycle management.<br>• Modern, responsive, and intuitive user interface under a single pane of glass. |
| Scalability | • Elastic scaling via Cloud Native microservices architecture.<br>• Seamless scaling from tens to thousands to millions for cloud deployment model.<br>• Scales upto 256K devices in On-Premises deployment model.<br>• Zero capacity planning required for remote sites, branches, and HQ. |
| Security | • Password-less (certificate-based) authentication for corporate devices.<br>• Secure mTLS and RadSec for data in transport.<br>• UPSK and TLS secure auto-provisioning.<br>• Arista NDR, 3rd-party integrations (via Concourse Apps.)<br>• Increased security and compliance. |
| Stability | • Reliable cloud infrastructure with higher SLAs ⟶ 99.99% availability.<br>• One architecture for HQ, branch, and remote sites.<br>• Continuous service monitoring and upgrades delivered as a service for the on-premises deployment model.<br>• Automated tools and alerts to proactively monitor status and identify issues.<br>• Resolution of customer issues in real-time. |


CloudVision agni

## CloudVision AGNI provides the following features:

### Access Control Policies and Enforcements

AGNI offers simplified access control policies through its network and segment constructs. These constructs enable organizations to authorize users and clients based on a wide range of attributes, including network attributes, group memberships, location, client profile, and posture, among others. These policies can be uniformly defined for a variety of use cases on both wired and wireless infrastructures.

### Profiling and Posture Assessment

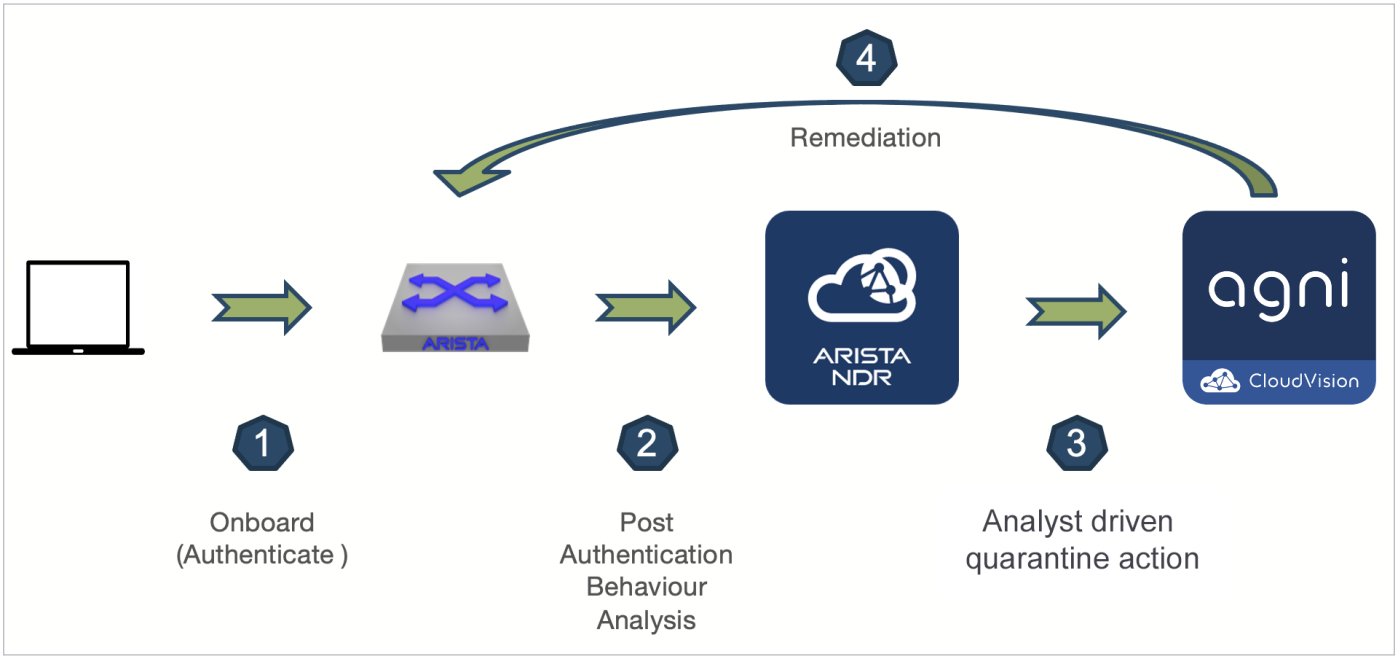
AGNI plays a key role in Zero Trust network architecture by offering profile and posture assessment and continuous monitoring of the connected endpoints through device finger printing and behavioral monitoring and analytics..

#### Device Fingerprinting

Profiling and posture are managed via external integrations through Concourse Application architecture. AGNI builds the client posture status by interacting with Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Inventory Management solutions from the partner ecosystem. The details acquired assist in pre- and post-admission control.

#### Behavioural Monitoring and Analytics

Monitoring and analytics are achieved via native integration with the Arista NDR product and external EDR and XDR solutions through the Concourse Application architecture. This provides risk ratings for the endpoints and enforces policy on the affected endpoints to ensure network safety.



## Client Onboarding

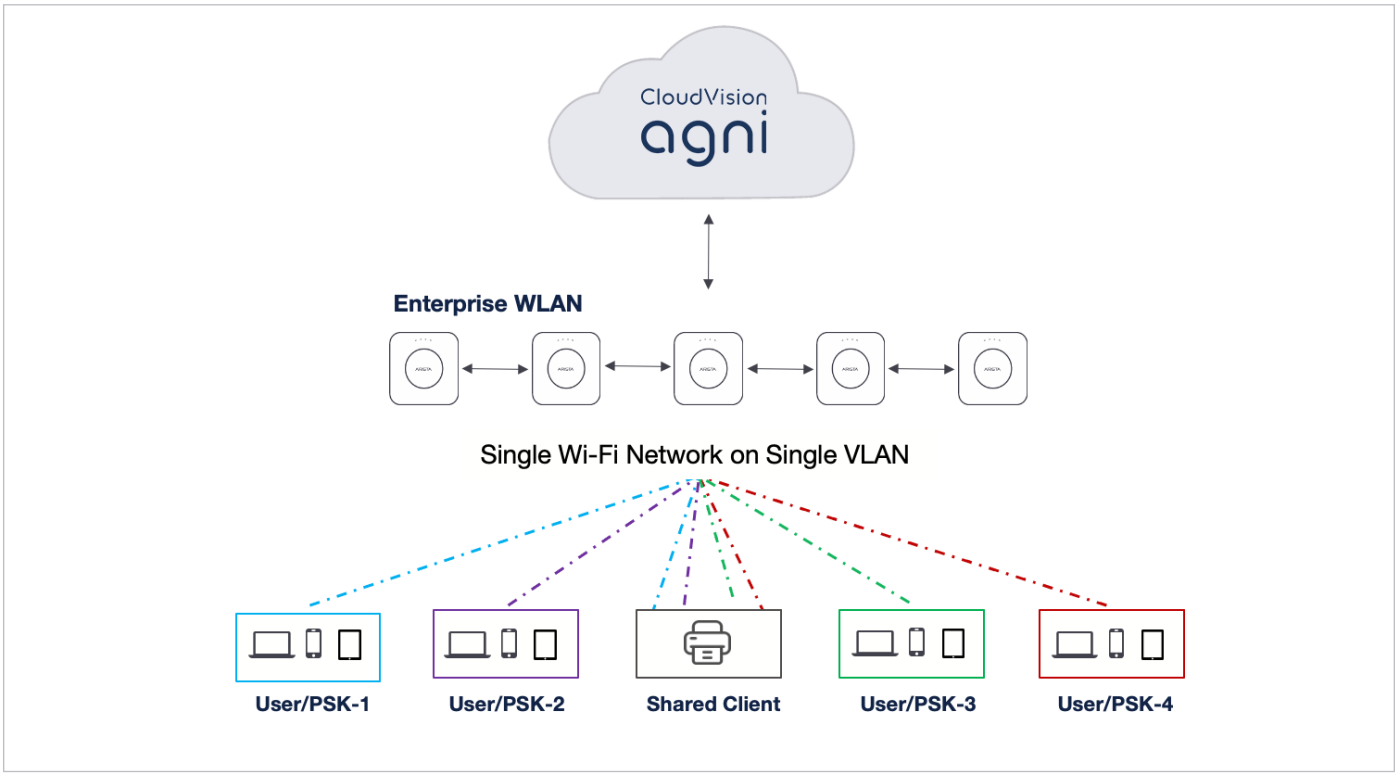
### Managed Devices

AGNI provides native onboarding of clients in a secure 802.1X network for a wide range of client devices through its native PKI. Secure onboarding is enabled through the Simple Certificate Enrollment Protocol (SCEP) and the Enrollment over Secure Transport (EST) protocol. AGNI offers:

- Complete lifecycle management of certificates along with management and visibility.
- Seamless integration with external PKI systems without additional onboarding to authenticate the client endpoints.
- Integration with external MDM solutions to extend onboarding functionality.

### BYOD & IoT/IoMT Devices

AGNI provides lifecycle management of UPSK passphrases, which can either be created by individual users (through the Client persona) to manage their devices or by an administrator (via the Admin persona) to manage the end user's devices. Connection is achieved using secure passphrases that are unique to users or groups of users and QR codes.




**Security : UPSK- User Private Network**

## Multi-Domain Segmentation

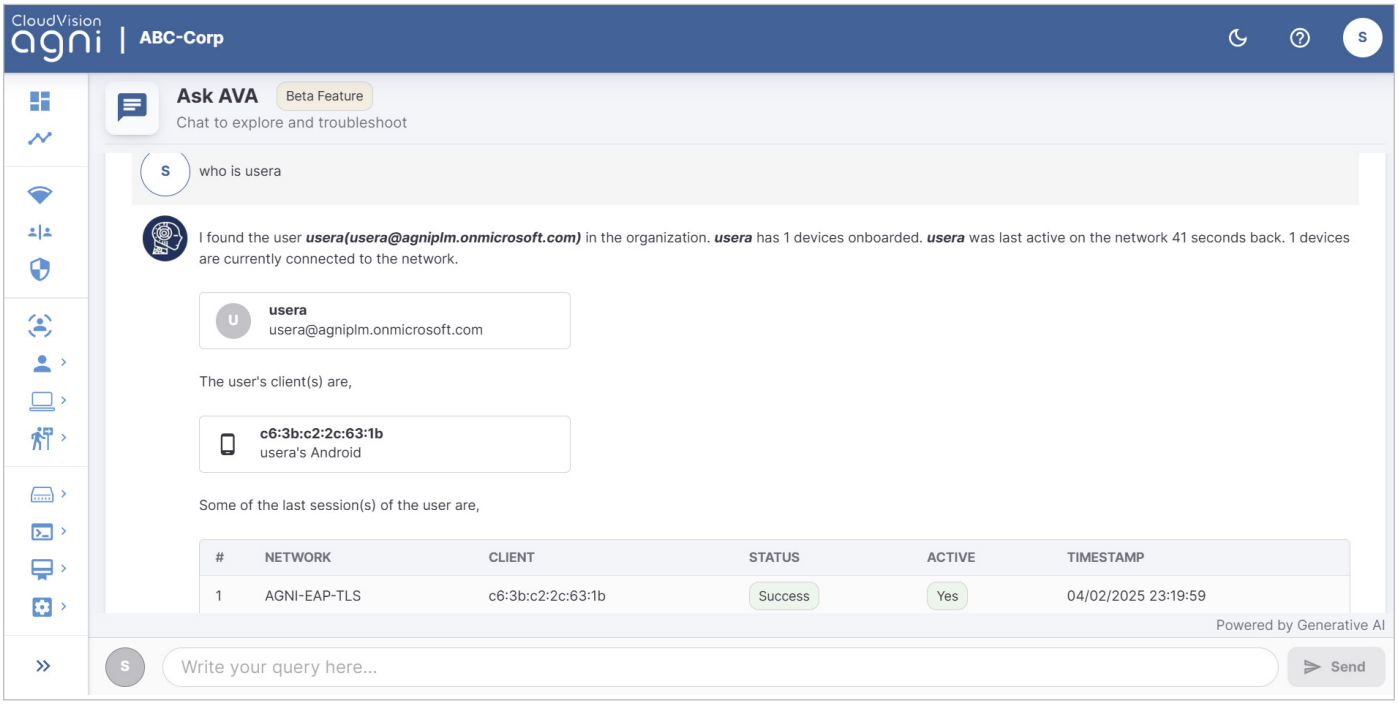
AGNI enables the journey towards Zero Trust architecture by natively integrating with the Arista MSS solution. This integration allows granular segmentation policies to enforce client connection based on various combinations of user and client-group membership, device profile and posture status, and network attributes.

## Ask AVA-Autonomous Virtual Assistant (ML/AI)

AGNI (Cloud deployment model) offers an autonomous virtual assistant to enable:

- Advanced troubleshooting and context navigation.

Using a well-trained AI/ML engine, AGNI system offers a chat-like service that enables natural language interactions with an administrator. The system guides the administrator by providing answers through context and navigational options within the product administration interface.




## Concourse Applications

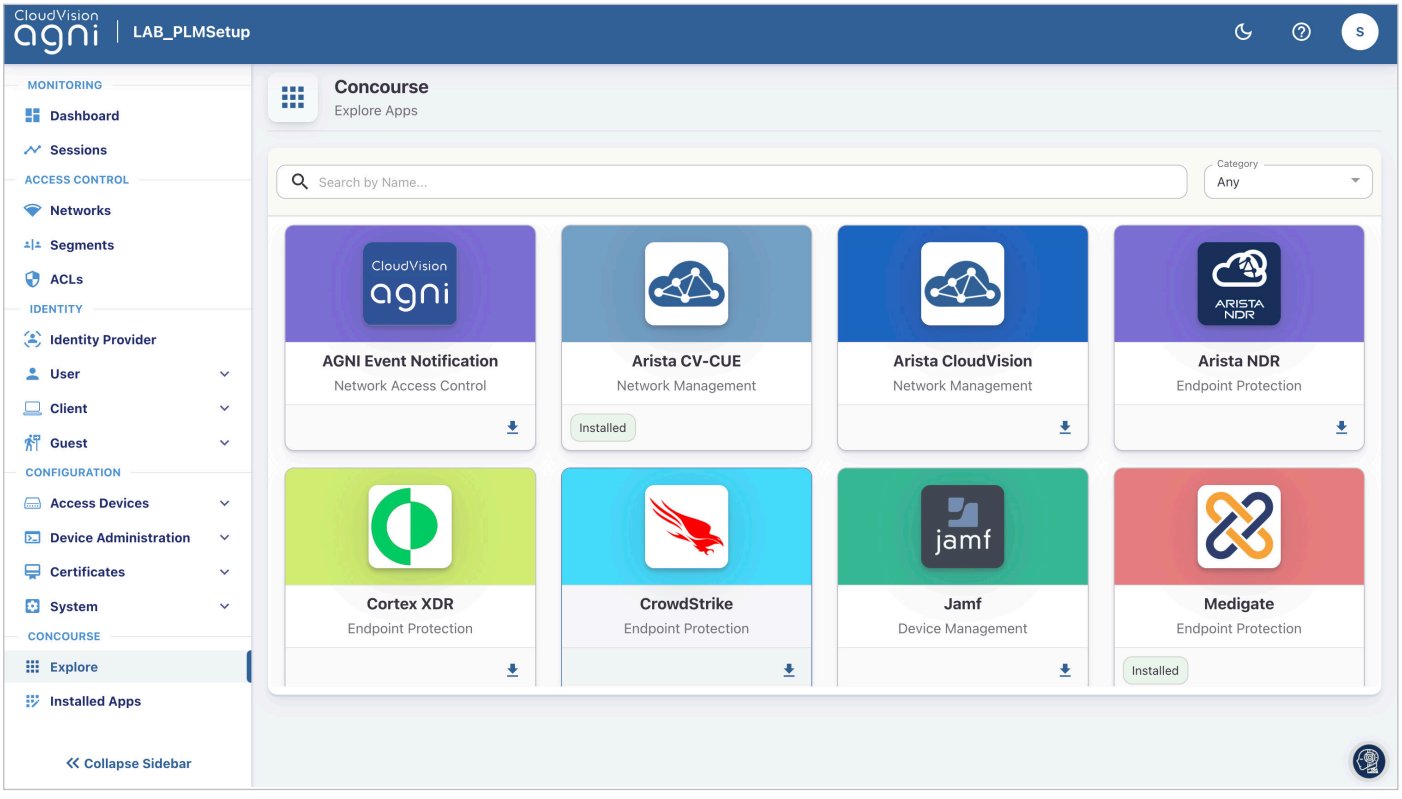
AGNI integrates with a wide variety of native and external services to enhance the security and visibility of the organization's product administration interface.

| Concourse App | Category | Description |
|---|---|---|
| Arista CVaaS/CV-CUE * | Network Management and Device Inventory | Fetches and consumes network switch and access point details such as location, device MAC, and IP address. Builds the inventory of network access devices that can be grouped or used directly in AGNI's access policies. |
| AGNI Event Notification | Network Segmentation and Access Control | Streams user and client connection events to the CloudVision platform that enables MSS Manager to manage group-based network policies. |
| Arista NDR | Endpoint Security | Facilitates user and device context to enforce granular policy controls. Provides risk and behavioral ratings to enable continuous monitoring and advanced profiling of endpoints. |

** On-Premises CV-CUE/CVP supported with On-Premises deployment model.*

| Concourse App | Category | Description |
|---|---|---|
| Palo Alto Cortex XDR | Endpoint Security | Fetches risk and behavioral details to enforce network security. |
| CrowdStrike | Endpoint Security | Facilitates user and device context to enforce granular policy controls. Provides Containment Status, Minutes Since Last Seen, Sensor Status, and Sensor Version to enable continuous monitoring of the endpoints. |
| Medigate | Endpoint Visibility | Fetches profiled information on various types of IoT/IoMT devices. Enables segmentation through the endpoint's profiled details.<br>Fetches risk details of endpoints to enforce network security. |
| ServiceNow CMDB | Endpoint Visibility | Fetches profiled information on various types of corporate IoT devices. Enables segmentation through the endpoint's profiled details. |
| Palo Alto Firewall* | Endpoint Visibility | Facilitates user and device context to enforce granular policy controls on the firewall. AGNI sends the user context to the firewall and the firewall creates the policies and applies them to the interface. |
| JAMF | Device Management | Enables onboarding of managed devices and provides a seamless connection to the network, authenticated and authorized by AGNI. |
| Microsoft Intune | Device Management | Enables onboarding of managed devices and posturing of endpoints. Provides seamless connection to the network, authenticated and authorized by AGNI. |
| Workspace ONE | Device Management | Enables onboarding of managed devices and posturing of endpoints. It provides a seamless connection to the network, authenticated and authorized by AGNI. |
| Splunk | SIEM | Publishes authentication telemetry for monitoring, reporting, and troubleshooting. |
| Sumo Logic | SIEM | Publishes authentication telemetry for monitoring, reporting, and troubleshooting. |

** Supported with AGNI (Cloud deployment model) only.*



| Feature | Details |
|---|---|
| Authentication | • 802.1X<br>• MAC Bypass Authentication (MBA)<br>• UPSK (Unique Pre-shared Key)<br>• Captive Portal |
| Guest | • Guestbook<br>• Host approval<br>• UPSK with Guest<br>• Self-registration.<br>• Clickthrough<br>• Support for Captcha<br>• SMS Gateway Support to send user credentials<br>• Email Template Support to send user credentials |
| Public Key Infrastructure | • Native Certificate Authority (CA) support<br>• External CA integration |
| Onboarding | • Native support (Applications for Android, Chromebook, and Windows OS devices), Apple iOS onboarding<br>• External MDM services (eg: JAMF, Microsoft Intune) |
| Identity Providers | • External integrations<br>  • Google Workspace<br>  • Okta<br>  • OneLogin<br>  • ADFS<br>  • Microsoft Azure Active Directory<br>• Native<br>  • Local directory services |
| Network Vendors | • Native integration with Arista devices<br>• Multi-vendor support<br>• Interoperable with any standards-based implementation |
| Downloadable Access Control Lists (dACL) | • Cisco dACL<br>• RFC 4849 |
| Enforcement | • Standards-based (Radius attributes)<br>• VLANs<br>• ACLs<br>• DACLs<br>• VSAs<br>• Inbuilt vendor-specific dictionaries<br>  • Arista<br>  • HPE/Aruba<br>  • Cisco<br>  • Juniper<br>  • Microsoft |
| Profiling | • Device fingerprinting via standard means (DHCP fingerprinting, User Agent, LLDP)<br>• Posturing Via external integrations (e.g., Cortex XDR, Crowdstrike, Intune, Medigate, WorkSpace ONE)<br>• Behavioral profiling via internal and external integrations (e.g., Arista NDR, ServiceNow CMDB, Medigate) |
| Device Administration | • TACACS+<br>  • NAS Administration<br>  • Exec Authorization<br>  • Command Authorization<br>  • Web CLI-based SSH<br>  • Native tool-based SSH<br>  • Token-based password SSH<br>• RADIUS<br>  • NAS Administration<br>  • Web CLI-based SSH<br>  • Native tool-based SSH<br>  • Token-based password SSH |
| Eduroam* | • Supports Eduroam in onboarding visiting students/faculty on the educational institution network using credentials provided by their educational institutes.<br>• Supports authentication proxy to authenticate clients of visiting students/faculty. |
| External Integration | • Refer to Concourse Applications |
| APIs | • OpenAPI 3.0 compliant |

## CloudVision AGNI Deployment Models

The following table describes the deployment models for CloudVision AGNI

**For AGNI (Cloud deployment model)**

| AGNI as a Service | Details |
|---|---|
| Deployment | • Public cloud, offered as a service |
| Connectivity Requirements (UI Access) | • IP connectivity to www.arista.io (port 443) |
| Connectivity for RadSec | • 2083 |
| Protocols | • Client and administrator portals and API services through HTTPS<br>• RadSec with network access devices<br>• OAuth2.0 and OIDC with Cloud Identity Providers |
| Cloud Identity Providers | • Microsoft Azure Active Directory, Google Workspace, Okta, OneLogin |
| API | • OpenAPI 3.0 |

**For AGNI (On-Premises deployment model)**

| CloudVision AGNI Physical Appliance | Details |
|---|---|
| Deployment | • On-Premises with 32k endpoint scale per appliance.<br>• Can go up to 500K endpoint scale with cluster architecture. |
| Physical Appliance Platform Specifications<br>Specifications for DCA-AGNI-100 | CPUs: Intel(R) Xeon(R) Silver 4310 CPU @ 2.10GHz, 12 core, 24 thread<br>DRAM: 64 GB<br>Hard Drives: Four SSDs with 894.25GiB each<br>Network Interfaces: 6 Integrated 1 Gigabit Network Connection<br>Power Supply: Dual power supply. Input wattage 927W and Output wattage 800W<br>Dimensions (HxWxD): 3 feet * 2 feet * 1 feet<br>Weight: ~100 lbs<br>Remote management: iDRAC Enterprise controller |
| Physical Appliance Software Version Requirements. | DCA-AGNI-100 supports software applications for CV AGNI on-premises solution. For software recommendations, please refer to the appliance release notes. |

## CloudVision AGNI Ordering Information

CloudVision AGNI is delivered as a service and as a ***"pay-as-you-go"*** model. Software support for CV-AGNI is included in the CV-AGNI software subscription license.

CV-AGNI provides a simplified software subscription model that includes all the listed features in a single SKU. The subscription is based on the average concurrently active end user/IOT devices over a 7-day period.

- A CloudVision AGNI license (SKUs starting with 'SS-CV') includes all available CloudVision functionality except for ASK AVA.
- A CloudVision license (SKUs starting with 'SS-CVS') for CloudVision as-a-Service includes all available functionality except for native Radius communication support.

| Product SKU | Description |
|---|---|
| **On-Premises Appliance SKU** | |
| DCA-AGNI-100 | 1 unit CloudVision AGNI Physical Appliance, Model 100(Includes CV-AGNI Server software). No CV-AGNI device licenses. |
| SVC-DCA-AGNI-100-NB | 1 Month NBD Hardware Replacement/Same Day Ship for DCA-AGNI-100 Appliance |
| **On-Premise Software subscription SKU** | |
| SS-CV-AGNI-500-D-1M | CloudVision AGNI SW Subscription License for 1-Month for 500 devices. |
| SS-CV-AGNI-1000-D-1M | CloudVision AGNI SW Subscription License for 1-Month for 1000 devices. |
| SS-CV-AGNI-5000-D-1M | CloudVision AGNI SW Subscription License for 1-Month for 5000 devices. |
| SS-CV-AGNI-10K-D-1M | CloudVision AGNI SW Subscription License for 1-Month for 10000 devices. |
| SS-CV-AGNI-30K-D-1M | CloudVision AGNI SW Subscription License for 1-Month for 30000 devices. |
| **Cloud software subscription SKU** | |
| SS-CVS-AGNI-100-D-1M | CloudVision AGNI Cloud Service SW Subscription License for 1-Month for 100 devices. |
| SS-CVS-AGNI-500-D-1M | CloudVision AGNI Cloud Service SW Subscription License for 1-Month for 500 devices. |
| SS-CVS-AGNI-1000-D-1M | CloudVision AGNI Cloud Service SW Subscription License for 1-Month for 1000 devices. |
| SS-CVS-AGNI-5000-D-1M | CloudVision AGNI Cloud Service SW Subscription License for 1-Month for 5000 devices. |
| SS-CVS-AGNI-10k-D-1M | CloudVision AGNI Cloud Service SW Subscription License for 1-Month for 10000 devices. |

## Services and Support

Software support for CloudVision AGNI is included in the CloudVision AGNI subscription license. For more details about the service and support across all Arista products, see: http://www.arista.com/en/service.

### Headquarters

5453 Great America Parkway
Santa Clara, California 95054
408-547-5500

### Support

support@arista.com
408-547-5502
866-476-0000

### Sales

sales@arista.com
408-547-5501
866-497-0000

www.arista.com