Key Features

- Centralized configuration and segment policy management
- Simple, Secure and scalable next generation Network Identity solution
- Cloud Native architecture
- Ask AVA - Autonomous Virtual Assistant*
- Microsegmentation with Arista MSS-G and UPSK
- Profiling and Posturing
- Continuous posture check with Arista Awake 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 as other Arista 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 the 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 delivers a substantial reduction in 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. AGNI is tested with Arista, Cisco, and HPE access devices with each release. CloudVision AGNI integrates with network infrastructure devices (wired switches and wireless access points) through a highly secure TLS-based RadSec tunnel. The highly secure and encrypted tunnel offers complete protection to the communications that happen in a distributed network environment. This mechanism offers much greater security to AAA workflows when compared with traditional RADIUS environment workflows, which are not encrypted.

AGNI integrates with Arista products to enable the exchange of important user and client context, secure group segmentation (MSS-G), and authentication 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 facilitates the seamless authentication and authorization workflows that are 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 very 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 • Automated certificates and UPSK provisioning with lifecycle management • Modern, responsive, and intuitive user interface under a single pane of glass • No on-premise equipment
Scalability	• Elastic scaling via Cloud Native microservices architecture • Seamless scaling from tens to thousands to millions • Zero capacity planning required for remote sites, branches, and HQ
Security	• Passwordless (certificate-based) authentication for corporate devices • Secure mTLS and RadSec for data in transport • UPSK and TLS secure auto provisioning • Arista NDR, 3rd-party integrations (via Concourse Apps) • Increased security and compliance
Stability	• Reliable cloud infrastructure with higher SLAs →99.99% availability • One architecture for HQ, branch, and remote sites • Automated tools and alerts to proactively monitor status and identify issues • Resolution to customer issues in real time
Savings	• No hardware or software to procure (no CAPEX) • Reduced spending on compute, storage, and security • Reduced operational costs, maintenance, and upgrades

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, which 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

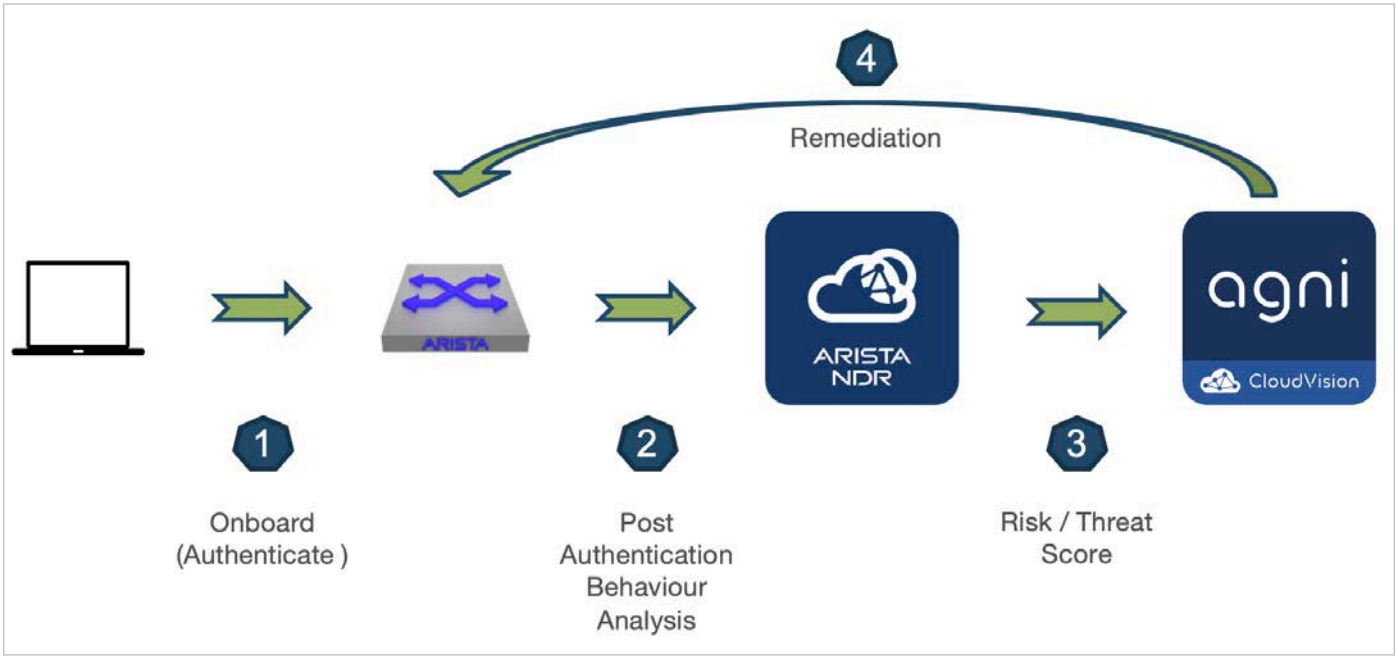
AGNI plays a key role in Zero Trust network architecture by offering profile and posture assessment as well as continuous monitoring of the connected endpoints.

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) solutions from the partner ecosystem. The details acquired assist in pre- and post-admission control.

Behavioral Monitoring and Analytics

Monitoring and analytics are achieved via native integration with the Arista NDR product and external EDR, XDR solutions through the Concourse Application architecture, providing risk ratings of the endpoints and performing policy enforcement on the affected endpoints to ensure network safety.



Client Onboarding

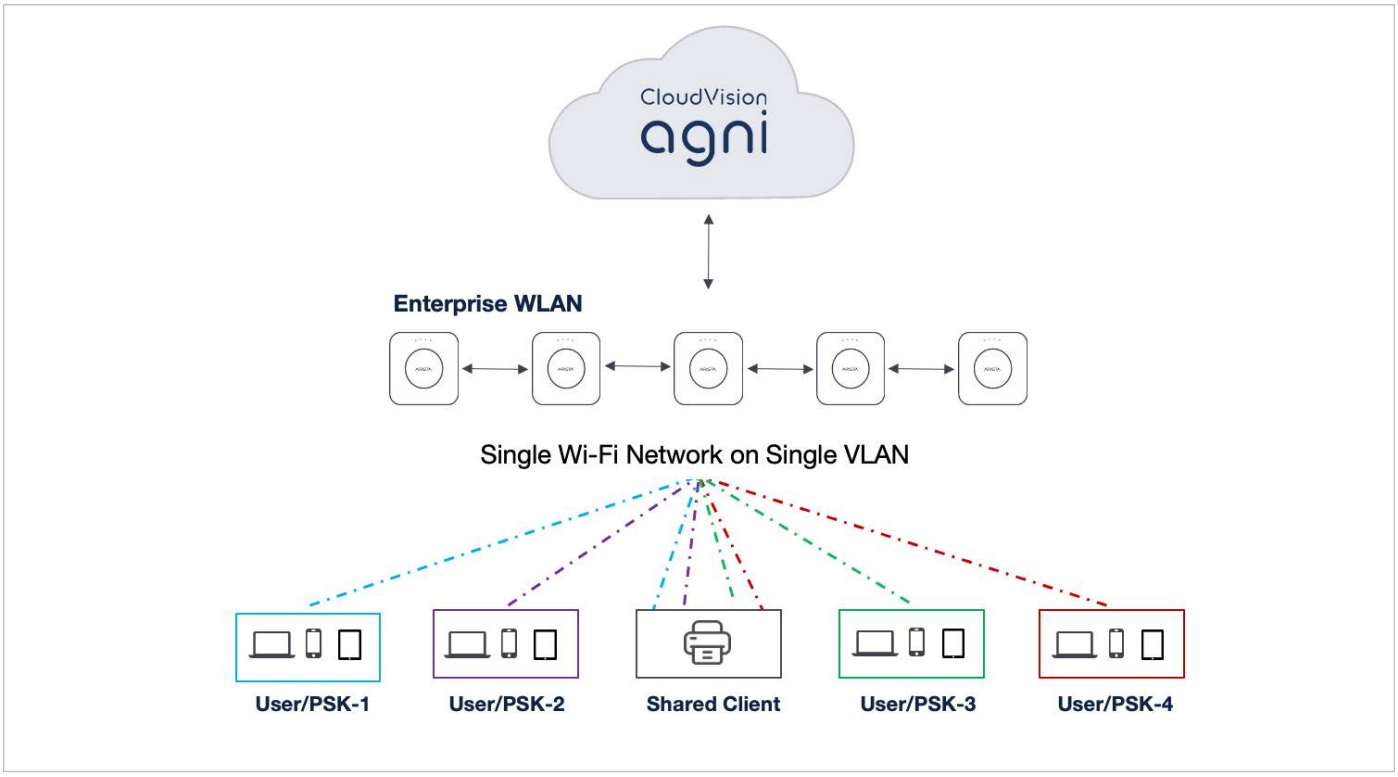
Managed Devices

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 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 requiring any 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 that 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 users' devices. Connection is achieved using secure passphrases that are unique to users or groups of users, and through QR codes.



Security : UPSK- User Private Network

Micro Segmentation

AGNI enables the journey towards Zero Trust architecture by natively integrating with the Arista MSS-G solution. This 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.

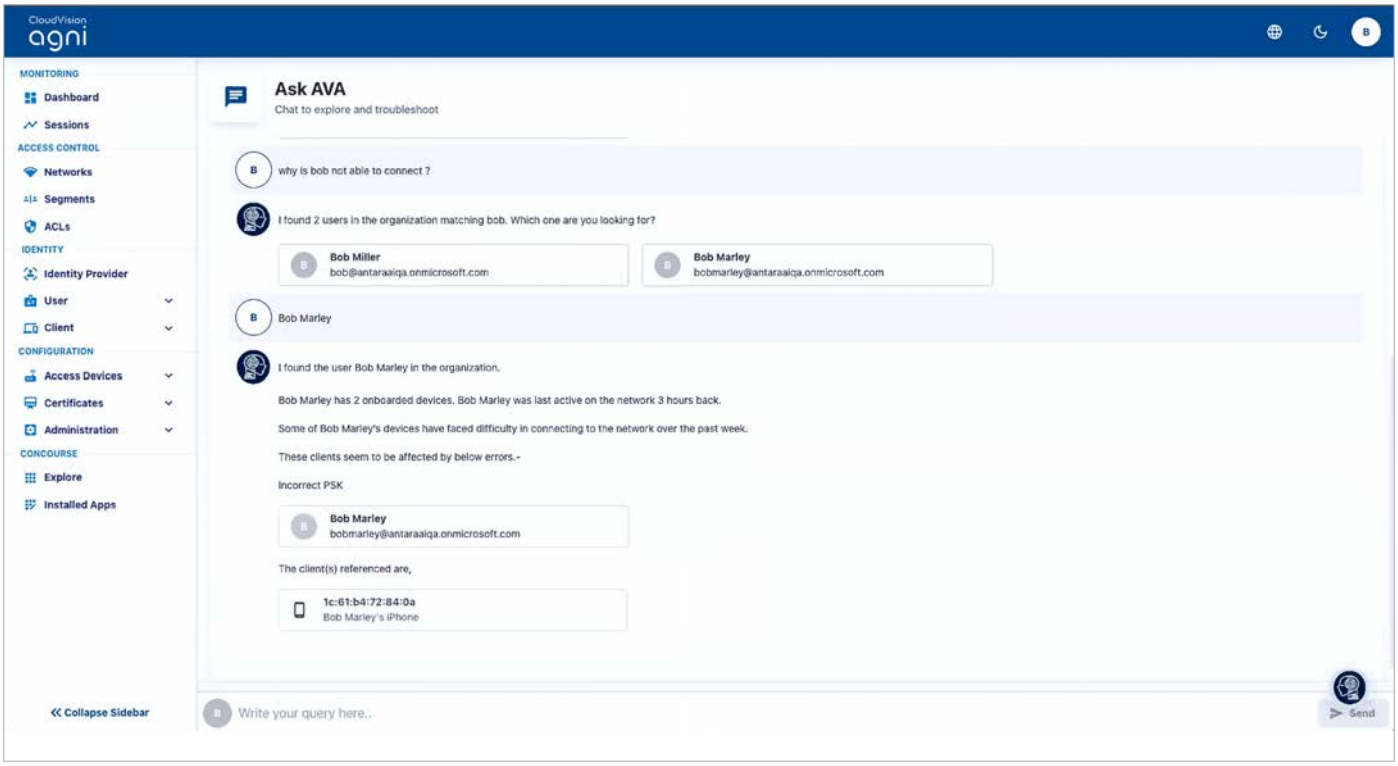
Micro segmentation is extended to wireless clients via the UPSK solution.

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

AGNI offers an autonomous virtual assistant to enable:

- Advanced troubleshooting and context navigation.

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

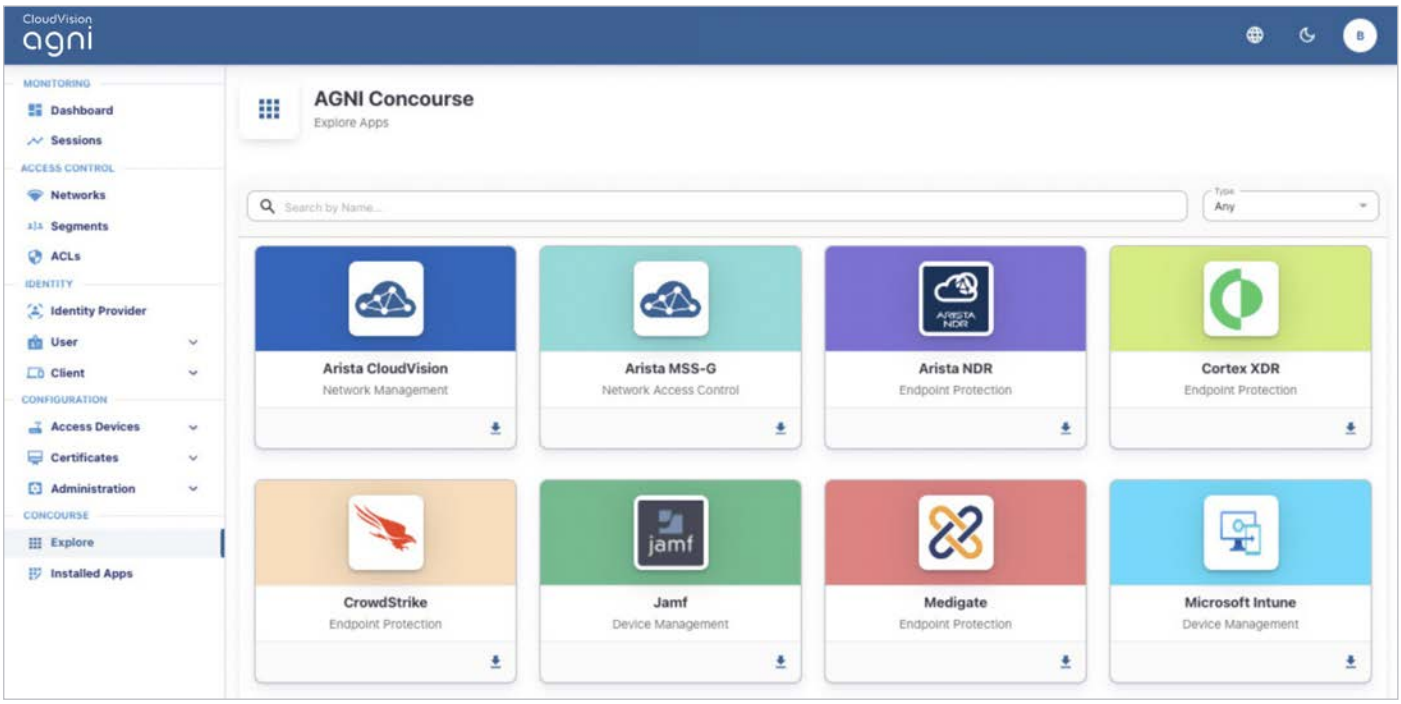


Concourse Applications

AGNI integrates with a wide variety of native and external services to provide enhanced security and visibility to organizations product administration interface.

Concourse App	Category	Description
Arista CVP	Network Management and Device Inventory	Fetches and consumes network switch and access point details comprising location, device identifier, network definitions, and enforcement objects. Builds the inventory of network access devices that can be grouped or used directly in AGNI's access policies.
Arista MSS-G	Network Segmentation and Access Control	Fetches network MSS-G constructs that can be used in access policies.
Arista NDR	Endpoint Security	Facilitates user and device context to enforce granular policy controls. Provides risk and behavioral ratings to enable continuous monitoring of the endpoints

Concourse App	Category	Description
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 of various types of IoT/IoMT devices. Enables segmentation through the endpoint's profiled details.
ServiceNow CMDB	Endpoint Visibility	Fetches profiled information of various types of corporate, IoT devices. Enables segmentation through the endpoint's profiled details.
JAMF	Device Management	Enables onboarding of managed devices and profile configuration. Seamless connection to the network, authenticated and authorized by AGNI.
Microsoft Intune	Device Management	Enables onboarding of managed devices and profile configuration. Seamless connection to the network, authenticated and authorized by AGNI.
Workspace ONE	Device Management	Enables onboarding of managed devices and profile configuration. 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.



Feature	Details
Authentication	• 802.1X • MAC Bypass Authentication (MBA) • UPSK (Unique Pre-shared Key) • Captive Portal
Guest	• Guest book • Host approval • Social plugins • Web form • Clickthrough
Public Key Infrastructure	• Native Certificate Authority (CA) support • External CA integration
Onboarding	• Native support • External MDM services (eg: JAMF, Microsoft Intune)

Identity Providers	• External integrations
	  • Google Workspace
	  • Okta
	  • OneLogin
	  • Microsoft Azure Active Directory
	• Native
	  • Local directory services

Network Vendors	• Native integration with Arista devices • Multi-vendor support • Interoperable with any standards-based implementation
Downloadable Access Control Lists (dACL)	• Cisco dACL • RFC 4849

Enforcement	• Standards-based (Radius attributes)
	• VLANs
	• ACLs
	• DACLs
	• VSAs
	• Arista MSS-G
	• Inbuilt vendor-specific dictionaries
	  • Arista
	  • HPE/Aruba
	  • Cisco
	  • Juniper

TACACS+	• NAS Administration • Exec Authorization • Command Authorization • Web CLI based SSH • Native tool based SSH • Token based password SSH
Eduroam*	• Supports eduroam to onboard visiting students/faculties on the educational institution network using credentials provided by their educational institute • Supports authentication proxy to authenticate clients of visiting students/faculty
Profiling	• Device fingerprinting via standard means (DHCP fingerprinting, User Agent, LLDP) • Posture and profiling via external integrations (e.g., Crowdstrike, Medigate…) • Behavioral profiling via internal and external integrations (e.g., Arista NDR, Cortex XDR)
External Integration	• Refer to Concourse Applications
APIs	• OpenAPI 3.0 compliant

Specification	Details
Deployment	• Public cloud, offered as a service
Connectivity Requirements	• IP connectivity to www.arista.io (port 443)
Protocols	• Client and administrator portals and API services through HTTPs • RadSec with network access devices • OAuth2.0 and OIDC with Cloud Identity Providers
Cloud Identity Providers	• Microsoft Azure Active Directory, Google Workspace, Okta, OneLogin
API	• OpenAPI 3.0

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

SKU	Description
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-10000-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