Arista Guardian for Network Identity (AGNI)

Simple, Scalable, Secure and Cloud Delivered

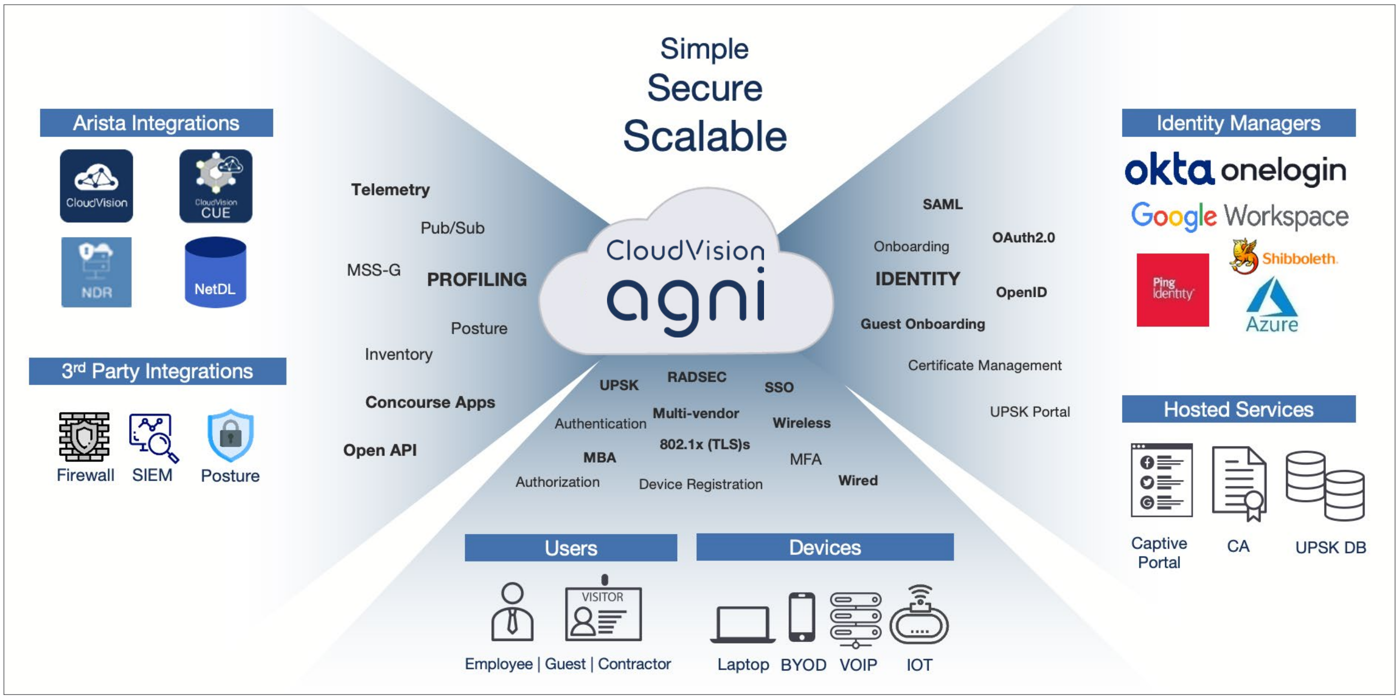
A Modern Access Control Solution for Today's Networks

Never trust, always verify is a foundational principle of modern zero-trust networks. Today, an ever-growing number of corporate and IoT devices, including BYOD, need to be securely onboarded and provisioned with access that are role appropriate. The need for complete visibility and control of your network has become an absolute necessity today more than ever.

CloudVision
agni

Introducing Arista Guardian for Network Identity (AGNI), the next generation cloud-native solution that delivers identity-based network access control. CloudVision AGNI is designed keeping in mind the 5-S fundamentals of network designing — simplicity, scalability, security, stability, and savings (cost-effective). It integrates with all the major Identity and Access Management (IAM) products to support Single Sign-On (SSO). Its intuitive and easy user interface offers managing and monitoring the entire network from a central, single pane of glass.

AGNI brings a fresh and innovative approach to NAC that leverages modern design principles while significantly reducing administrative complexity. It offers a cloud-native solution that seamlessly scales from hundreds of connecting devices to millions from any location—all without requiring additional on-premises equipment or hardware. Keeping in mind the future of security, this solution can also drive users towards a more secure, password-less technology such as digital certificates.

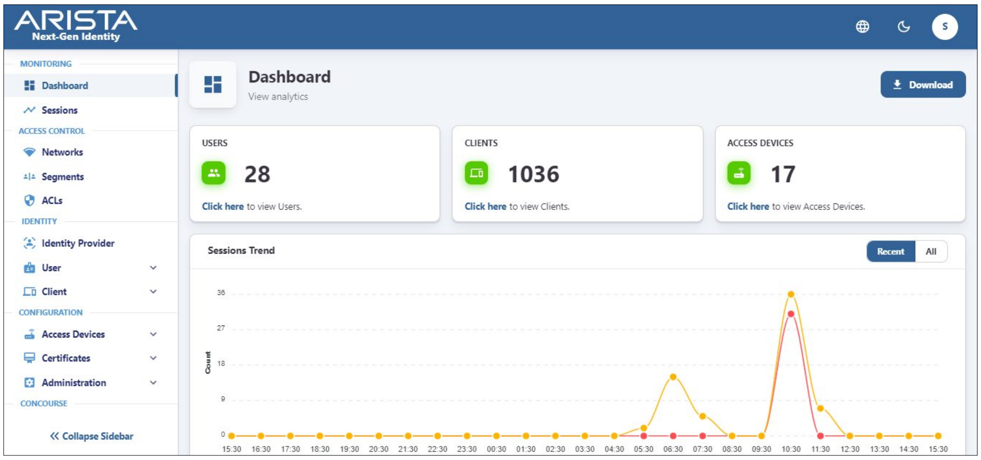


The 5-S Advantage with CloudVision AGNI

Simplicity

CloudVision AGNI is a cloud-native solution that requires no additional on-premises equipment; network designers do not have to deal with hardware boxes, expensive installation services, and frequent upgrades.

CloudVision AGNI streamlines getting corporate and IoT devices, including BYOD, onto the network – wired and wireless – and every connection is secured with a powerful encryption. Devices that use digital certificates or Unique Pre-Shared Keys (U-PSKs) are registered and onboarded through an easy-to-use interface.



USERS
28
Click here to view Users.

CLIENTS
1036
Click here to view Clients.

ACCESS DEVICES
17
Click here to view Access Devices.

Configuration is as easy as a few clicks, with no need for expensive professional services. CloudVision AGNI interfaces with leading SSO/IAM vendors such as Microsoft Azure, Google Workspace, Okta, OneLogin, and Ping over SAML, OpenID Connect, and OAuth 2.0. Importantly, existing NAC deployments can gradually migrate to CloudVision AGNI avoiding expensive forklift upgrades. It natively supports multilevel administration, allowing global administrators to set up multiple zones that can be independently administered (regionally and/or departmentally).

Scalability

CloudVision AGNI is completely built on containerized microservices. These containers are orchestrated via the Kubernetes infrastructure. These containerized and componentized microservices connect and collaborate with each other through well-defined APIs. Most of these services are stateless and can be throttled based on demand, providing the necessary elasticity for scaling. The load change in the number of users, user devices, and/or network devices is dynamically handled in a very efficient and cost-effective manner. For example, when there's an increase in the authentication load, you can scale up just the authentication-related microservice to handle the load, while other microservices remain the same.

CloudVision AGNI is also a SaaS offering with multi-tenant capability built into its architecture. This architectural advantage makes CloudVision AGNI massively scalable, very elastic, more cost-effective, and absolutely maintenance free for customers.

Ease of Management

- No-on premises equipment
- Self-service and frictionless SSO-based onboarding on wired and wireless network
- Automated certificates and U-PSK provisioning/ management
- Intuitive, centralized UI under a single pane of glass
- Easy deployments (hours vs weeks)

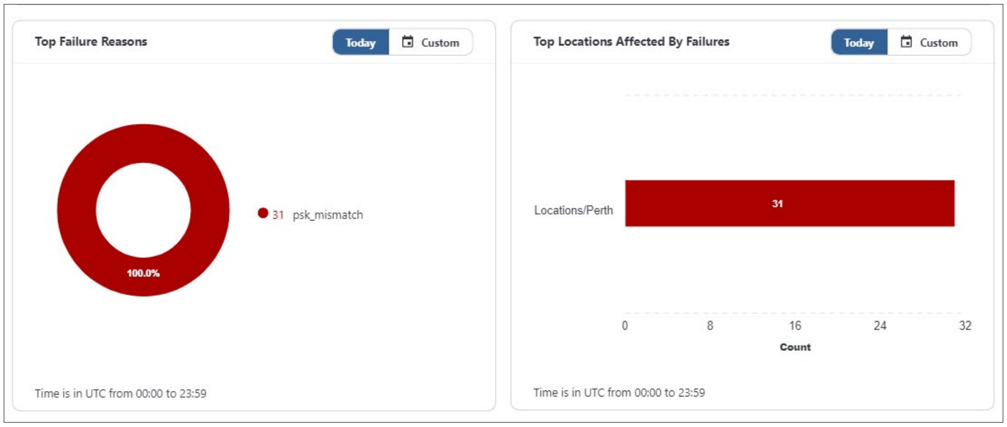
Automatic Scaling

- Cloud-native microservices architecture allows elastic scaling
- Dynamically scales up and down per demand
- Supports thousands to millions of users/ devices
- Plugin integration architecture for context
- One architecture for HQ, branches, remote sites

Security

CloudVision AGNI employs the latest security concepts to further strengthen the NAC security. Some of these include:

- Certificates and other passwordless mechanisms for authentication. CloudVision AGNI recommends digital certificates with 802.1X for user devices and U-PSK passphrase for BYOD and IoT devices.
- Private key generation and storage on the client. This eliminates the possibility of on-the-wire attacks from other products.
- Simple and safe lifecycle management for certificates. It can work with third-party PKI or public PKI issued certificates for identity verification.
- Data protection at all levels. Data in transport is protected with RadSec or HTTPS. All critical network and client information is encrypted and securely stored in the cloud.
- Data privacy between multiple tenants. All data objects are bound to their specific customer or organization.
- GDPR compliant. GDPR requirements for EU businesses and organizations are also natively supported in CloudVision AGNI to meet the EU regulation.


Top Failure Reasons
Today
Custom
100.0%
31 psk_mismatch
Time is in UTC from 00:00 to 23:59
Top Locations Affected By Failures
Today
Custom
Locations/Perth
31
0
8
16
24
32
Count
Time is in UTC from 00:00 to 23:59

Stability

CloudVision AGNI brings continuous identity-based access control services to your workforce – regardless of where they work from. It is built with business continuity in mind; the uptime is more than 99.99%.

Some of the highlights are:

- CloudVision AGNI brings is built on microservices, which are dynamically activated upon detection of hardware faults or capacity constraints. Individual microservices are independent from the hardware platform that could reside anywhere in the cloud.
- Automated tools and alerts to proactively monitor, identify, and resolve customer issues in real-time.
- Customers always get to use the latest version of CloudVision AGNI software.

Security

- Secure wired and wireless network access for all devices
- Passwordless authentication with digital certificates and IAM MFA
- Unique PSK passphrases for non-802.1X
- Secure data transport with RadSec and HTTPS
- Secure all data at rest with AES256 encryption
- Private key never leaves the client

Stable and Always On

- >99.99% available uptime
- Continuous availability with automated cloud-based failover
- No software patch maintenance. Work with the latest and stable image, always
- Single architecture for HQ, branch, and remote

- The network administrators never have to schedule downtime for upgrades.
- The architecture allows access devices to reside at any physical location - corporate headquarters, branch office, or an employee's home.
- One architecture for all locations not only simplifies network planning and monitoring, but also results in a more stable network without the need for complex MPLS/IPSEC tunnels and expensive load balancers

Savings

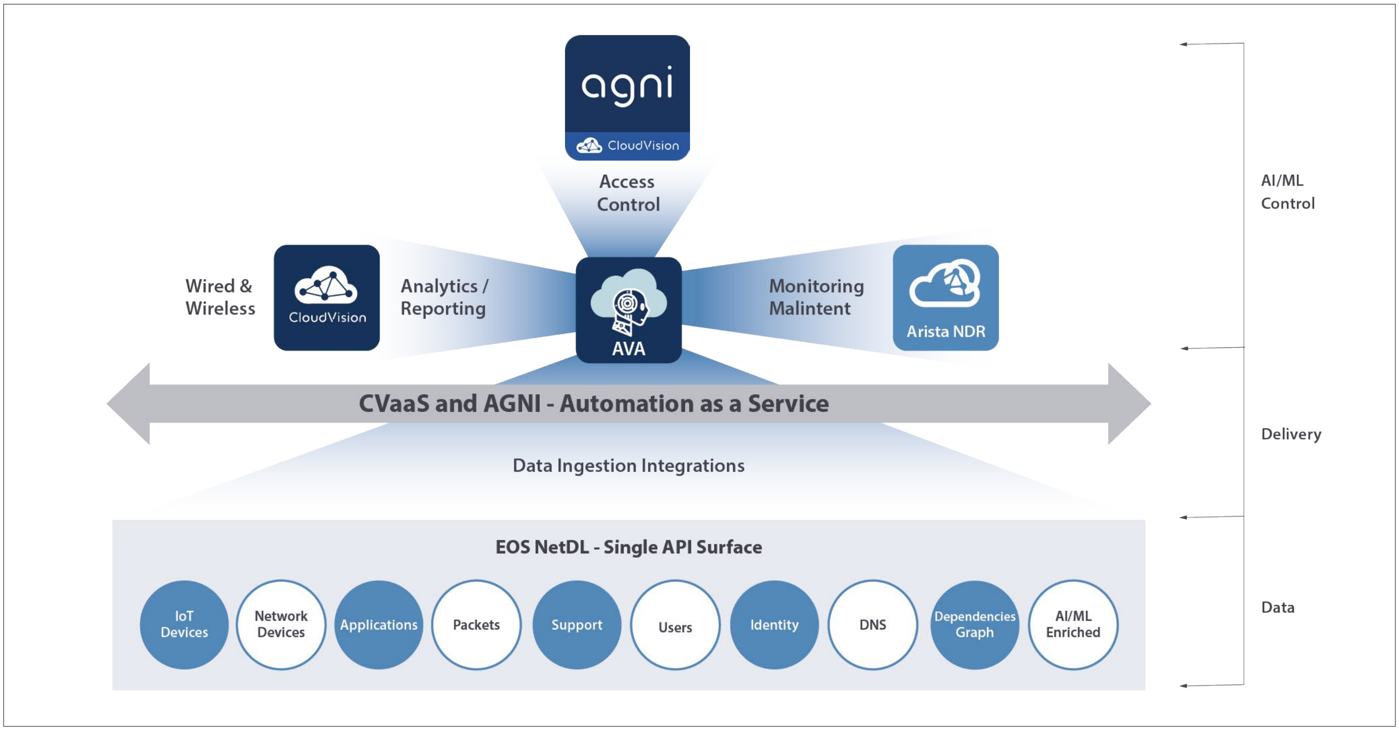
CloudVision AGNI provides the most cost-effective architecture to manage your current NAC security requirements. It also addresses many of the operational shortcomings of on-premises NAC offerings. The pay-as-you-go service with its dynamic auto-scaling features make it very easy for businesses of any size to switch from traditional on-premises NAC to CloudVision AGNI.

- Some of the notable cost saving benefits of CloudVision AGNI are:
- No upfront hardware and software purchases (no CAPEX)
- Reduced spending on compute, storage, and security
- Reductions in operational costs, maintenance costs, and upgrade expenses
- Reduction in operation-oriented personnel

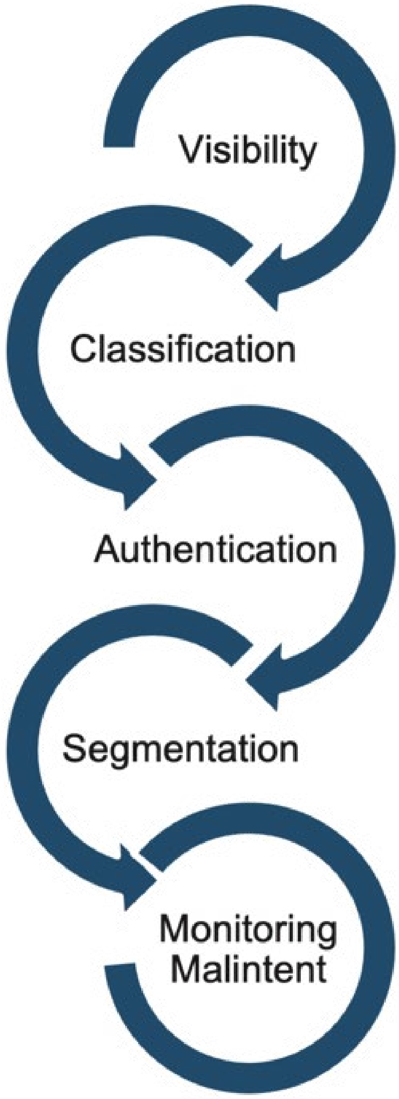
The Arista Advantage

CloudVision AGNI is a foundational component of Arista's Zero Trust security architecture. It tightly integrates with several of Arista's core cloud infrastructure offerings. These offerings include CloudVision Cognitive Unified Edge (CV-CUE) for providing wired and wireless network access control capabilities, and Arista's Network Detection and Response (NDR) for continuous threat monitoring.

Arista's Zero Trust security begins with visibility of all connected devices. As devices enter the network, they are classified and authenticated through digital certificates or unique PSK passphrases. Based on the type of device or the organization the user belongs to, devices are granted access to only the minimum of required resources.



Once a device is allowed onto the network, trust cannot be assumed. Because a device can be infected, or an internal user could be a bad actor, continual monitoring for malintent of all connected devices is the need of the hour. The Arista NDR continually monitors all connected devices for anomalous behavior that suggests malintent. It assigns risk ratings to connected devices and communicates the risk rating to CloudVision AGNI. CloudVision AGNI evaluates the device risk rating and leveraging the administratively-defined policies, it quarantines, restricts, or raises the alerts for the connected devices.



CloudVision AGNI also integrates with Arista CloudVision, Arista Edge Threat Management, and Arista EOS NetDL to provide a comprehensive network security solution.

Now More Than Ever

The need for network security at every level has never been greater. With CloudVision AGNI, you implement an overarching and comprehensive security strategy that includes:

- Zero-trust control that properly manages access to users and devices
- Secure, passwordless authentication, or UPSK-based authentication
- Centralized authentication and authorization for users, devices, and workloads that can reside anywhere - on-premises, cloud, branch office, home office.

CloudVision AGNI is built from the ground up to mitigate the shortcomings of legacy NAC architecture and weak security protocols such as PEAP-MSCHAPv2. It is a future-proof solution for the ever-evolving security requirements and it is a critical component of the overall Arista security solution. Recognizing that modern networks consist of network equipment from many vendors, CloudVision AGNI seamlessly integrates with third-party NAC, CA, switch, and AP solutions.

With CloudVision AGNI, you are assured of simplicity, security, scalability, stability, and savings while managing your network.

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, 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