Arista CloudVision®: Cloud Automation for Everyone
Table of contents

Introduction 3
- Cloud Principles for Enterprise Network Operations 3
- Different Approaches for Different Enterprises 4
- A Single Platform with Universal Applicability 5

Arista CloudVision Overview 6
- Infrastructure Service 6
- Web Portal 7
- Analytics Platform AI/ML 7
- CloudVision’s Advantage 9

CloudVision Architecture 9
- High Availability Clusters 10
- State Streaming 11
- Real-time Telemetry 12
- On-Premises or SaaS 13

CloudVision Applications 14
- Topology View 14
- Events View 15
- Device View 17
- Dashboards View 18
- Cloud Tracer 19

Network Automation 19
- Building the Network 20
- Validating and Deploying the Network 22
- Using Change Controls 23
- Viewing Device Comparisons 24
- Using Network Rollback 25
- Deploying CloudEOS 26
- Risk Management with Compliance Checking 27

CloudVision Integrations 28
- Network API Gateway WiFi Service Integration 28
- CloudVision APIs 29
- ITSM, ITOM and AIOps Integration 29
- DevOps Integration 29
- Device SDK 30
- Overlay Controller Integration 30
- Service Insertion 31

Summary 31
Introduction
In network operations circles, there is an old adage that the network is always guilty, until “proven innocent”. By touching all infrastructure components - compute, storage, virtualization, apps, users, WAN, LAN, etc. - it is clear that the network plays a fundamental role in all IT operations. With such a broad scope, the network is the service that is expected to always work, and when an IT issue happens, the network is almost always suspected to be at fault.

Network operations teams are counted upon to manage availability, security, agility, costs, and risks. To do so, they need processes and tools that enable them to employ efficient and repeatable workflows with continuous visibility and observability. The approach that they take to do their daily jobs has to allow them to control and monitor their networks, make changes without disruption, and deploy new sites quickly and reliably.

However, the traditional approaches to monitoring and managing networks have failed to keep up with today’s cloud networking era. Today’s network operations and engineering teams are challenged across a wide number of areas, including planning, site deployment and upgrades, day-to-day operations, troubleshooting, and compliance management. As human error remains a primary cause of observed network issues, new software-driven approaches are needed to enable automation in network operations and improve both reliability and mean-time-to-innocence.

Cloud Principles for Enterprise Network Operations
Over the past decade, Arista has been delivering cloud networking solutions with a unique software-driven approach to building reliable networks designed around the principles of standardization, simplification, cost-savings, and automation. We coined the term “cloud networking” to characterize the evolved approach and architecture which addresses these principles, while we worked closely with the largest hyper-scale cloud operators on their journeys.

Cloud operators pioneered new principles for scale-out designs and software-first thinking because the scale of operational and technical challenges that they faced in all aspects of their businesses could not be surmounted the old way. These cloud principles modernized networking for hyper-scale networks with simplified designs using standards-based protocols, open scale-out IP fabric designs, and software-driven orchestration to help them scale operations with minimal resources.

Just as hyper-scale cloud operators set an example with network automation to simplify time-consuming and error-prone tasks, and to separate the human factor that made continuous hyper-scale operations risky – these principles can now help enterprise customers with exceptional improvements in reliability, efficiency, and cost savings.

Enterprises that want to embark on this journey to cloud networking are often challenged with breaking away from the traditional network operation models, and will follow some common decision points and success factors to plan their path:
• **Building vs. buying.** While hyper-scale cloud operators drove much of the new technologies and systems that they used to build their infrastructure, most enterprises do not have the time, skillset, or resources to build out their own homegrown cloud automation platform. However, these innovations can drastically improve network operations for everyone. Therefore, enterprises are looking for a modern, consistent NetOps platform that is also turnkey and provides the same benefits.

• **Choosing a modern architecture.** Cloud network operations cannot be built on network management tools that are decades old (e.g. SNMP polling, screen-scraping, manual cut-and-paste configuration). Modern network architectures require a system approach with real-time automation, using open state-streaming APIs for continuous real-time synchronization of network state and configuration, and providing advanced AI/ML analytics to provide instantaneous compliance, visibility, and troubleshooting.

• **Breaking down silos.** Traditional enterprise networks have often been deployed by selecting a different ‘box’ for each “place-in-the-network” (PIN). With each box comes a different operating system, with different design limitations and features, different APIs, and different management apps. The selection of platforms with the greatest commonality, across the widest aperture, provides an alternative to disparate places-in-the-network thinking, as does the selection of standard approaches to management plane communications.

**Different Approaches for Different Enterprises**

As decisions about how to approach network modernization with a software automation model are considered, each customer will have different options to consider. Various approaches exist and are not mutually exclusive. Fundamentally, there are several common approaches to network modernization for the enterprise customer, with the primary approaches summarized as follows:

![Figure 2: Arista Supports a Variety of Approaches to Network Automation](image)

• **Do-It-Yourself (DIY) Automation.** DIY solutions are typically deployed by hyper-scale cloud operators, such as Microsoft or Facebook, who are building massive public infrastructures at scale exceeding 100's-1,000's of times those of the typical large enterprise. For them, automation is fundamental to their business model as a means to remain competitive. With many specialized in-house applications and services designed to account for infrastructure failure, they employ large software teams to automate their entire estate. Arista helps such customers by providing open tools like EOS SDK, Openconfig / gRPC agents, streaming telemetry, and eAPI device programmability. With unrestricted programmability of the EOS Linux software infrastructure, these customers are able to fully integrate EOS-based switches into their broader software orchestration systems.

• **DevOps CI/CD Model.** This model is typically deployed by relatively large service providers or enterprises, as they embark on an automation journey. Their approach includes using automation frameworks – typically also being used by the DevOps compute and platform operations teams – such as Hashicorp Terraform or Red Hat Ansible to automate the provisioning of the network
infrastructure and to drive down OpEx costs. These customers have the resources and skills to write their own custom scripts and are invested in DevOps automation approaches with committed resources. Arista supports these customers by providing open software integration into DevOps frameworks like Terraform, Ansible, Puppet, and Chef, as well as supporting streaming receiver platforms like ELK stack, Prometheus, and others.

- **Turnkey Solution.** There are few tools that exist today to guide customers down a path to successful network automation, and fewer still for customers that do not have the time, skills, or resources to build a custom approach. CloudVision provides a turnkey solution for all customers, allowing customers to provision, manage and observe their infrastructure while still permitting extensibility and customization. CloudVision is designed to help customers of all sizes, in particular small, mid-sized, and large enterprises across every industry who are looking to reduce OpEx by applying the principles and lessons learned by the cloud providers.

**A Single Platform with Universal Applicability**

Arista’s Extensible Operating System (EOS®) and CloudVision® are designed with universality and applicability in mind. Designed around cloud principles, these systems provide a platform based on a software-driven model for turnkey network automation, which normalizes disparate places in the network with a uniform software operating model. With CloudVision, this software approach is not just for the data center or for hyper-scale operators. A common approach for automated provisioning and real-time visibility can now apply to the campus, the hybrid cloud, and the routed interconnect, as well.

Operations teams can implement a single operating model and runbook for:

- Upgrade procedures
- Certification efforts
- Lifecycle management
- Vulnerability management
- Network designs
- Troubleshooting approaches
- Automation techniques
- Feature discrepancies
- Management platforms
- Ecosystem integration
- And more…

With Arista EOS and CloudVision, operators don’t need to re-invent different solutions for each place-in-the-network. In fact, there is a significant benefit of consolidating network operations using a single uniform approach for every place-in-the-cloud (PIC).

**Arista CloudVision Overview**

Arista CloudVision is a next-generation network management platform that communicates with any device running Arista EOS software, whether in a switching or routing role to deliver network-wide automation, telemetry/analytics, and orchestration.
Arista CloudVision Overview

Arista CloudVision is a next-generation network management platform that communicates with any device running Arista EOS software, whether in a switching or routing role to deliver network-wide automation, telemetry/analytics, and orchestration.

As a turnkey solution for network-wide orchestration and workflow automation. CloudVision is designed to also provide SDN (virtualization overlay) integration for:

- Enterprise EVPN
- Routed LAN/WAN
- Cloud-native fabrics and third-party controllers

By orchestrating virtual network overlays and focusing on workflow visibility, automation, and initial or ongoing network provisioning, CloudVision complements modern network designs.

CloudVision is available as a software platform that is deployed as a virtual or physical appliance, or as a managed-service offering called CloudVision as-a-Service. It manages physical Arista switches running in any network, Arista EOS software instances running in the public cloud, containerized EOS routers in a Kubernetes cluster, EOS running on white boxes, and Arista cognitive WiFi access points. Because of this broad scope, CloudVision can provide a single management plane across data centers, hybrid public/private cloud, and campus networks thus helping enterprise IT to break down traditional box-based network silos.

Infrastructure Service

The foundation of CloudVision is an infrastructure service accessed via a web portal, sharing and aggregating the working state of network devices running EOS to provide visibility and central coordination. The CloudVision platform builds on one of Arista’s core strengths - the innovative EOS event-driven state-sharing database design model called NetDB, which holds the entire state for a particular device (e.g., running configuration, neighbor topology, protocol state, tables, monitoring counters, interface/link-state, errors, and events). Leveraging this state-sharing NetDB architecture, Arista EOS devices provide greater resilience and state separation between processes which leads to an overall lower fault rate and better network maintainability.
In CloudVision, NetDB is extended via the infrastructure service to a central CloudVision database through open state-streaming binary APIs, representing the real-time aggregated NetDB database as well as the entire desired state and running state of all the devices across the network.

State from each participating EOS node is registered to CloudVision using the same publish/subscribe architecture of the EOS system database (NetDB). By communicating to each participating switch instance using a high-performance binary API, CloudVision actively synchronizes state relevant to network-wide operational tasks and can provide a unifying point of integration for third-party IT operations, configuration management, deployment and orchestration tools like ServiceNow and Ansible.

**Web Portal**

The CloudVision web-based portal combines the most common operational tasks in a dashboard view decoupled from the underlying hardware. Workflow automation in CloudVision permits operators to execute common deployment and configuration tasks from a single visual touchpoint. The portal includes a turnkey solution for Arista’s Zero Touch Provisioning (ZTP) and extends that from automating initial device provisioning to also include automating ongoing change controls and device replacements over the operational life cycle of the network.

Using the CloudVision web portal, operators can organize devices in logical hierarchies through the use of list or configuration (config) container views for rapid categorization of devices by role, type, or other specification. Configurations can be broken down into more manageable configlets that are built and stored directly on CloudVision, ready for network-wide or group-specific provisioning.

The CloudVision database also keeps historical data, including a history of network state, configuration and software versions. This state can be used for taking a network-wide snapshot for change control verification of the network, helping to simplify the change management process and reduce maintenance window times.

**Analytics Platform AI/ML**

CloudVision also contains a powerful, event-driven, streaming analytics engine that enables you to monitor the state of all managed devices, orchestrate various actions, and gain valuable insights along the way. Conceptually, AI/ML is the application of Artificial Intelligence (AI) techniques to predict outcomes of observed conditions and to take actions accordingly. By configuring devices to stream device-state and telemetry data to CloudVision, the Analytics Engines and CloudVision Apps use Machine Learning (ML) algorithms to provide valuable insights into the entire state of the network, highlighting observed anomalies, and providing real-
CloudVision uses its analytics pipeline to improve network operations with AI/ML algorithms that are implemented in microservices called “Turbines”. Of course, the value of the applied AI/ML technology in these scenarios depends on the quality and timeliness of data that is analyzed, benefiting greatly from the real-time state and telemetry data that is streamed into the CloudVision platform from connected devices.

In practical terms, CloudVision Analytics can dramatically improve operational efficiency, network uptime, and cost savings through better network observability, automated workflows, and orchestration of the network across services. The outcome is enhanced reliability, faster root cause analysis, and faster mean time to innocence.

Some examples of where AI/ML technology is used in CloudVision include:

- **Reachability Anomalies.** Modeling time-series data for reachability and latency baselines, derived from Cloud Tracer telemetry, where alerts are identified based on dynamically learned deviations from a reachability/latency baseline and compared over time.

- **Resource Utilization.** Monitoring resource utilization trends and associated telemetry to make predictive assessments and generate proactive notifications before functional hardware limits such as TCAM allocation are reached.

- **Device Observability.** Using correlation analysis of subtle device state changes such as optical power levels, hash selection, or buffer utilization to identify transient ‘grey failures’ and prevent these hard to pinpoint issues.

The CloudVision Analytics Platform provides a very promising resource for AI NetOps services, such as proactive TAC support and efficient network-wide capacity management. More information on these capabilities is included in descriptions of CloudVision Apps and uses of AI/ML in CloudVision is increasing as more use cases are discovered.
CloudVision’s Advantage
The CloudVision platform is a modern construct – 100% streaming-based, with no legacy polling or MIB limitations – for a more granular and complete centralized view. CloudVision uses the state-streaming design to focus on three key pillars of functionality:

- **Telemetry and Analytics.** Based on this native state-streaming for real-time and historical visibility into network state, incoming telemetry is constantly processed and evaluated with AI/ML capabilities to identify anomalies and provide extensive observability for the entire network.

- **Automated Provisioning and Change Control.** Provides seamless workflows for automated cloud-like network operations, dramatically reducing the possibility of errors and misconfigurations and making operations tasks significantly more efficient.

- **Orchestration.** Acting as a single point of integration for both 3rd party ecosystem partners and non-EOS devices, as well as providing a native API gateway for customer extensibility.

![Figure 7: Three functional pillars in one platform](image)

Arista’s open software-driven cloud networking approach focuses on improving the operator’s experience and improving economics for everyone. With a single operating system and streaming approach across all network platforms and use-cases. Together, Arista EOS and CloudVision dramatically simplify the complexity of a myriad of OS trains that proliferate across a typical network. Built from the ground up as a programmable software platform with exceptional reliability and unique state-streaming architecture, Arista EOS and CloudVision have established themselves as the preferred platform for cloud networking.

CloudVision Architecture
CloudVision was built with the architectural goal of streaming the state of all systems under management in real-time, through an analytics pipeline, and finally into a database for historical retrieval. The common challenge in traditional management systems when trying to build a given application is getting access to the right data in the first place. The CloudVision architecture and design allows a focus on building the most interesting applications on top of a complete dataset. This is incredibly important for any network analytics, where the insights can only be as deep as the underlying dataset allows.
To achieve this goal, CloudVision is built on a modern scale-out cloud-native architecture with end-to-end streaming. It is implemented as microservices orchestrated under Kubernetes but packaged as a turn-key solution so that it is accessible to any customer.

Arista has implemented what others would build for a modern telemetry system in the do-it-yourself model. Below are some examples of the common open-source component choices for building a modern telemetry pipeline, along with the choices implemented in CloudVision:

<table>
<thead>
<tr>
<th>Component</th>
<th>Distributed Key-value Database</th>
<th>Queuing System</th>
<th>Analytics Pipeline</th>
<th>Search Engine</th>
<th>Visualization</th>
<th>Container Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>HBase, Cassandra, Kudu, Druid, etc</td>
<td>Kafka, ActiveMQ, ZeroMQ, RabbitMQ</td>
<td>Spark, Storm, Heron, etc</td>
<td>Elastic, Solr</td>
<td>Kibana, Grafana</td>
<td>Kubernetes, Docker Swarm, Apache Mesos</td>
</tr>
</tbody>
</table>

These components break down into functions as described below and as depicted in figure 8:

- A scale-out database built on top of HBase for historically storing all network state
- An indexing engine built with ElasticSearch for quickly searching through historical state
- A queuing system built with Kafka and gRPC to stream updates between components of the pipeline
- An API Server, providing a single point of access for all applications into the CloudVision database, exposing read, write, and subscribe semantics over a gRPC, WebSocket, and REST interface
- An analytics engine, called CloudVision Turbines, for stream processing applications
- The CloudVision UI for visualizing the underlying network-wide database and analytics insights for network operators

**High Availability Clusters**

CloudVision software is deployed as a virtual or physical appliance, and in a production on-premises cluster uses three redundant servers to achieve high levels of availability. In the cloud version of the service the cluster supports multi-tenancy and can be expanded to as many nodes as required to meet service level objectives.

The CloudVision cluster consists of distributed components such as Zookeeper, Hadoop/HDFS, and HBase. Zookeeper provides consensus and configuration tracking mechanisms across a cluster of redundant systems. The cluster relies upon the underlying Hadoop/HDFS data store for high availability and HBase as a distributed key/value store. Running these services in a reliable fashion on multiple nodes is a proven and open approach used in many big data applications and provides reliability, performance and scale with limited overhead.

The Analytics engine utilizes the high-performance Hbase database to store device-state data, including events. Data is stored in a compressed format without a loss of resolution. Events and device state changes are time-stamped by the device as they occur and...
can be reviewed in a time slider in various application dashboards in CloudVision. Also, changes in device state and correlated events can be generated by the CloudVision platform to take predetermined actions, such as alerting an operator or executing a program or script.

**State Streaming**

Device state is streamed throughout the system end-to-end: from each device, into the CloudVision database, through CloudVision's analytics pipeline, and then to the web UI. There's no polling anywhere in the system. A NetDB State Streaming component called TerminAttr is an agent that runs on Arista EOS-based switches. It streams the time-stamped device-state data to the CloudVision Analytics Engine, which is the back-end data processing component of the platform.

![Figure 9: CloudVision’s Analytics Pipeline](image)

The transport layer between services throughout the system uses “grpc remote procedure call” (gRPC). gRPC is a modern high-performance framework built on top of Google protocol buffers (protobufs) and HTTP2, providing the scale and performance to stream the full network state from each device into the CloudVision analytics pipeline.

The streaming telemetry agent in EOS and the Device SDK are built on top of gNMI, an open-source protocol specification created by the OpenConfig working group. gNMI is used to provide read, write, and subscribe semantics from network devices to the datastore, while OpenConfig provides the standard data models. These methods and data models are the obvious choices for modeling network state in CloudVision and have been supplemented by Arista to represent the complete state of the EOS network where necessary.

In order to provide a network-wide aggregate view the CloudVision Analytics engine serves as a backend repository to collect and process all streamed data, including historical time-stamped data as it is received. The Analytics engine performs a variety of stream processing and data analysis including state correlation, event generation, trend monitoring, anomaly detection, and other analytics.

In addition to providing a historic state database network-wide, the Analytics Engine also offers an API server that allows customers and partners to leverage a single point of integration to third-party or internal tools using streaming and WebSocket-based APIs. CloudVision Telemetry Applications and third-party applications leverage access to the state repository via the API server offering a seamless way to provide read/write access to the state repository.
The streaming telemetry and analytics then feed into the provisioning workflows in CloudVision, where the user can fully automate the rollout network-wide changes, from initial deployment to ongoing change controls.

**Real-time Telemetry**
Along with providing real-time visibility into the state of the network and its attached devices, CloudVision streaming technology provides a modern approach to network telemetry. Unlike legacy management architectures that relied upon periodic SNMP polling, which gathered telemetry and configuration data from the network every few minutes at best, CloudVision streaming delivers a constant feed of real-time telemetry data to the CloudVision Analytics Engine, database and CloudVision applications. All of the data that is collected is stored and can be viewed and further analysed in any time window that the user selects.

Telemetry streaming allows CloudVision to identify network problems virtually instantaneously, and it allows IT operations teams to optimize network performance much more quickly than legacy management using polling ever could. When conditions worsen due to errant configuration changes, intermittent faults, or demanding workloads there is instantaneous visibility throughout the system. Transient problems that might impact users between polling intervals are no longer hidden. Remediation can start within seconds.

For historic troubleshooting situations, like forensic analysis, time-stamped records of the received state and telemetry data can be viewed in many of the CloudVision applications on a time-series continuum with the use of a simple slider mechanism, showing finely granular details at every point in time. This capability allows events and data to be correlated with each other, and with any other observed anomalies that have been reported.

As the variety and volume of metrics that network devices can generate are increasing, and with an explosion of IoT devices and mobile users connecting to enterprise networks, it is imperative that a telemetry based approach to management tools replace legacy monitoring. An enterprise-class telemetry architecture can address issues such as security, scaling, and polling gaps to provide full observability of all aspects of network operations.
On-Premises or SaaS

As previously discussed, the CloudVision platform is available in two different consumption models – either as on-premises software or appliances, and as SaaS-based software delivery. Both models offer the same fundamental capabilities and are based on a common software platform.

CloudVision was initially offered only as an on-premises solution, consisting of either a virtual software appliance (i.e., virtual machine image) or a pre-loaded physical hardware appliance (i.e., an x86 server such as the DCA-250-CV).

CloudVision as-a-Service provides a complementary managed-service consumption model of the same CloudVision software product. Running the same application containers, the CloudVision service delivers the same user workflows, state-streaming, telemetry, analytics, and provisioning capabilities. It gives customers a choice of whether to choose an on-premises or cloud service deployment and to transition from one to the other without having to compromise.

CloudVision as-a-Service is an Arista managed, multi-tenant cloud service deployed in tier one public cloud providers. Its features include the same secure state-streaming and analytics on top of an Arista-managed multi-tenant scale-out Kubernetes architecture. Customers are assigned to a unique organization (tenant) in a specific region. All devices and users of that tenant are exclusively part of the subscribed organization. Organizations are isolated from each other and a user in one organization cannot access any data or device from other organizations. Authentication and authorization in the service are tied to the customer’s identity provider and roles are assigned to users by the customer’s Sysadmin in the same manner as they are in the on-premises model.

By taking advantage of CloudVision’s cloud-native Kubernetes architecture, the as-a-service option can deliver faster mean-time-to-value, virtually unlimited elastic scale, and a richer connected service experience in a highly secure, private, and safe offering backed by Arista’s Site Reliability Engineering (SRE) workforce.

While CloudVision as-a-Service has a number of unique advantages, the choice of on-premises or cloud consumption are left to the user and will provide fundamentally the same capabilities.
The rest of this whitepaper will focus on the various CloudVision functions that can be deployed on-premises or via the cloud service for enterprise use-cases across data center, campus, and hybrid cloud.

CloudVision Applications
The CloudVision platform consists of the previously described core infrastructure and several value-added applications shown as ‘views’ in the web GUI.

- Topology View
- Events View
- Device View
- Dashboards
- Cloud Tracer

Topology View
CloudVision breaks down legacy network silos by providing an end-to-end view across data center, campus, and cloud with a single management plane platform. Topology View is designed to visualize these broad network topologies into a common view.

The Topology View app helps network administrators visualize the network topology to understand how devices are interconnected and quickly identify hotspots in the network based on link level metrics such as bandwidth, discards. CloudVision’s Topology View provides an intuitive approach to mapping the network topology not just based on LLDP neighbors but also backend analytics that automatically calculate device type, neighbor relationships, and common layouts. Using heuristics, CloudVision determines if devices in a topology are Leaf, Spine, or an Endpoint device and presents them in a network design view that relates to their logical interconnection. These layouts can be collapsed and expanded to reduce visual complexity and help network administrators visualize their network in a way that aligns with the network design.
Topology View allows users to overlay metrics on the network topology view. This helps network administrators quickly identify problems such as network congestion and traffic imbalance from the network-wide perspective. Items such as events, bandwidth, error/discard rates, network segments (VLAN and VxLAN), and network paths for traffic flows are displayed as optional layers on the topology. The view allows users to start at a network-wide level and use the overlays to drill down to the problem area for troubleshooting. The timeline can be leveraged in Topology View to view the historical state for segmentation, flow, and link-level metrics.

Events View
Events are created when one or more metrics in the state database reach certain criteria, as defined in the Analytics Engine. Events are categorized similarly to the Syslog model with varying levels of severity that can be used as a filter, and the event store can be searched by keyword. The unique aspect of the event view is the depth of correlated information that is offered, as compared to a typically ‘thin’ Syslog message. For example, a Syslog message for a drop counter only logs the event that the counter has increased a set threshold for an interface. This information is not sufficient to identify the root cause of the discards. In operational practice, not only are other metrics such as traffic rate, buffer utilization required to pinpoint the root cause but also it’s key to have these metrics for the same time window when the discards were incrementing. The CloudVision event view for interface discards provides all pieces of the puzzle and at the same point in time to help the operator identify if the discards were a result of congestion. The correlated view is available for all such events generated for all monitored devices.
As demand on a network increases with the onset of server virtualization, consolidation, IP storage, Hadoop, there will be times of congestion on the network. When there is congestion on the network, Arista switches have a feature called ‘LANZ’ (Latency ANalyZer) which can highlight proactively when there is congestion and the impact of the latency. However, this is box-by-box and not holistic for the network.

CloudVision helps the network operator to monitor health and congestion network-wide and identify hot spots there may be on a specific port or link. This allows the operator to quickly move workloads and workflows to less demanding resources on the network.

CloudVision supports the ability to configure and receive alerts for events generated. Users can get alerted via email, common chat-based services such as Slack or HipChat, and PagerDuty applications. Webhooks are available for custom alerting and monitoring needs that can help integrate the alerts into existing monitoring and incident management systems like centralized log servers, ServiceNow, or any web server-based application that can accept an HTTP POST notification. Webhooks also provide flexibility in taking actions in response to an event, for example, opening an incident ticket for a link down event from a specific device or closing an incident/task for a software upgrade on change of EOS version, triggering configurable actions based on certain event types from critical devices.

Further, alert rules can be configured based on the type of event, severity, and per device to allow users to customize how they receive alerts from various devices. This helps raise visibility for specific events on critical devices and prevents network operators from overlooking important events.
### Device View

This view offers a detailed insight into relevant metrics at a device level that are accessible using CLI commands, such as environmental, system details, interface statistics, MAC addresses, and routing tables. In addition to these metrics, it also includes platform-level details like digital optical monitoring (DOM), hardware route table, ACL table. PoE metric and buffer utilization for every device that SNMP-based legacy tools typically do not provide. The graphical user interface adds an abstraction layer by removing platform level subtleties that are often dependent on chip architecture and are heavily reflected in CLI commands making the outputs hard to interpret for network operators. All user views include a selectable time window at the bottom of the screen allowing users to either monitor the metrics in real-time or leverage the state repository to view the historical state for forensic troubleshooting.

---

**Figure 15: CloudVision’s Device View**

<table>
<thead>
<tr>
<th>Device Overview</th>
<th>System Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System</strong></td>
<td>Hostname: DC-NY-p2r3-Edge1</td>
</tr>
<tr>
<td>Processes</td>
<td>Model: 70805-64</td>
</tr>
<tr>
<td>Storage</td>
<td>Software Version: 4.18.11M</td>
</tr>
<tr>
<td>Log Messages</td>
<td>Uptime: 3 months, 3 days</td>
</tr>
<tr>
<td>Hardware Capacity</td>
<td>Management IP: 95.76.154.231</td>
</tr>
<tr>
<td>Configuration</td>
<td>More...</td>
</tr>
<tr>
<td>Software Image</td>
<td>Device ID: JPK00002</td>
</tr>
<tr>
<td>Snapshots</td>
<td>MAC Address: 75:a5:8c:06:be:2f</td>
</tr>
<tr>
<td>CVE and Bug Exposure</td>
<td>SSH to Device</td>
</tr>
<tr>
<td>Environment</td>
<td></td>
</tr>
<tr>
<td><strong>Tags</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Switching</strong></td>
<td>Streaming Agent Version: 1.5.2</td>
</tr>
<tr>
<td>ARP Table</td>
<td>Streaming Agent Mode: Normal</td>
</tr>
<tr>
<td>NDP Table</td>
<td>Streaming Status: Active</td>
</tr>
<tr>
<td>Bridging Capability</td>
<td>Streaming Latency: 4.516 ms</td>
</tr>
<tr>
<td>MAC Address Table</td>
<td>Provisioning Status: Ready</td>
</tr>
<tr>
<td>VLAG</td>
<td>Compliance Status: 2 bugs</td>
</tr>
<tr>
<td>VXLAN</td>
<td>Interface Counts</td>
</tr>
<tr>
<td><strong>Routing</strong></td>
<td>Ethernet Interfaces: 4</td>
</tr>
<tr>
<td>IPv4 Routing Table</td>
<td>VLAN Interfaces: 5</td>
</tr>
<tr>
<td>IPv6 Routing Table</td>
<td>IP Interfaces: 27</td>
</tr>
<tr>
<td>IPv4 Multicast Table</td>
<td>Port Channels: 2</td>
</tr>
<tr>
<td>BGP</td>
<td></td>
</tr>
<tr>
<td>IGMP</td>
<td></td>
</tr>
</tbody>
</table>

---

*Figure 15: CloudVision’s Device View*
**Dashboards View**

This view highlights the power of a network-wide perspective by allowing the user to choose metrics and correlate them across the network for the same time window. Users can build customized dashboards for monitoring groups of devices or interfaces using built-in and user-created tags. This allows network operators to quickly identify anomalies in device metrics or gauge the exposure of behavior in the network. For example, identifying a sudden surge in the number of routing table entries on one device may warrant a quick check on how many devices saw a surge in route table entries at the same time to see if devices in critical paths could be at risk. This would otherwise be a tedious approach to get the outputs from the CLI on a device-by-device basis. With the metrics view, accessing the output of the CLI command across the network in one consolidated empowers the operator to identify anomalies quickly and decreases time to resolution. This view also aids with tracking compliance, flows, endpoints, top utilized interfaces, errors, and congestion across devices and interfaces in the network using a few clicks versus a manual approach.

*Figure 16: CloudVision’s Dashboards*
Cloud Tracer
While telemetry and visibility are important within the data center, it is even more important when operating in a diverse hybrid cloud environment. Workloads that span public and private clouds need to maintain consistent availability. It is up to the network operator to be aware of any connectivity issues, even on the cloud transit networks that they don’t own themselves.

For this case, CloudVision Cloud Tracer™ App provides a dashboard of reachability information to endpoints throughout an organization’s hybrid cloud network. Using probe-based techniques, each EOS device is able to maintain connectivity information to any endpoint, including packet loss, latency, jitter, HTTP response time, etc. And then that state information is streamed to CloudVision’s central NetDB database for further analysis. The Cloud Tracer app displays the reachability information, based on both real-time as well as historically.

Network Automation
Even today, most network device provisioning, software upgrades, and configuration changes are still being done manually. This not only takes significant amounts of time, but it also leads to complexity and often error-prone operational procedures.

Building on the strength of the telemetry architecture, CloudVision is also a powerful platform for network provisioning. CloudVision Studios provides the tools needed for a fully automated network operations lifecycle, including building the network configurations, deployment, and ongoing operations.
Building the Network

Arista was one of the first in the networking industry to deliver Zero Touch Provisioning (ZTP). ZTP allows the customer to make a switch out of the box, rack it, and automatically provision it with a machine-generated configuration, officially approved image, or script without any human intervention – similar to how an IP Phone configures itself, or how a wireless access point configures itself with no manual intervention.

However, there was no turnkey way to orchestrate the ZTP process using a network-wide view. When network switches are managed, typically a configuration, image, and script are used to provision and manage change controls for that switch. The Provisioning app allows a customer to perform all three actions at the same time in a network-wide view.

To take ZTP a step further, CloudVision allows administrators to not only deploy brand new switches in remote locations without requiring an engineer to manually configure the switch but for replacements as well. Zero Touch Replacement (ZTR), allows a switch that has failed to be reprovisioned, or decommissioned to inherit the configuration and settings of an existing switch without requiring to apply all settings from scratch. Once again, with the flexibility of the EOS single binary image, it makes moving switch settings from one switch to another with ease.

CloudVision Studios brings operational ease to provisioning with built-in point and click workflows that simplify the provisioning of Arista validated network designs ranging from complex EVPN setups to POD deployments for the enterprise campus and datacenter. This prevents administrators from having to manually create each configuration for every switch. Using abstracted network data models, CloudVision studios translates network design to deployment by automating the creation and validation of configuration from day 0 provisioning to ongoing day1 and day2 tasks associated with network maintenance. CloudVision Studios also supports a no-code approach for easy customizations to these workflows and the ability to create new workflows with Studios for the advanced network administrators.
ZTP solutions were first born out of the need for automating the initial deployment of a switch in the infrastructure i.e. a ‘day zero’ process. To obtain OpEx cost reductions of managing the asset during the life cycle of its deployment in the data center, CloudVision is expanding the scope of ‘Zero Touch’ to a broader perspective to help automate ongoing changes over the lifecycle of the network devices. Customers are enabled to use a turnkey portal-based ZTP and ZTR solution to provision the device initially and throughout its lifecycle.
Validating and Deploying the Network

After the device configurations are built, CloudVision Studios can help validate those configurations and deploy the changes to production.

Many customers will build a virtual network environment using virtual machines or containers to simulate a network environment and validate the effects of configuration changes. vEOS-lab and cEOS-lab are software tools that run the exact same EOS software as an Arista switch but in a VM or container format. As such, they provide the same control and management plane experience as an actual physical switch running EOS. So these software options are commonly used to build virtual environments for pre-production validation. Similarly, CloudVision can manage these VM or container-based EOS instances to build the virtual environment and to practice change controls on the virtual estate. CloudVision’s ability to build and operate this virtual environment provides a useful simulation of actual production network changes.

Customers can also integrate CloudVision Studios with 3rd party validation tools, such as Batfish, that can simulate the effect of configuration changes on the network using software modeling. Software modeling can be useful when networks are too large to efficiently simulate, or as an initial test before moving on to a fully simulated environment. These integrations can be made part of the configuration change control in CloudVision to ensure that the proposed changes meet all the predefined tests before executing the change.

Once the configuration is validated and approved, CloudVision can help to roll out the network configuration through integrated network-wide change control workflows.
Using Change Controls

In the context of network maintenance, the change control process brings a controlled and coordinated approach to changes made in the network, while maintaining a documented audit trail and ensuring minimal disruption to network uptime. To ensure minimum service disruption, changes made to the network (configuration change, software upgrade, etc.) are planned at length and heavily scrutinized in the change control process, often requiring lengthy approvals and testing cycles before execution. The change control process in CloudVision comprises the following major steps, diagrammed below. An average change control in enterprise IT can take many hours across several weekends since a series of manual, box-by-box steps are employed and tend to be complicated and error prone. Automating the change control process could reduce this time dramatically, resulting in significant operation savings.

CloudVision’s Change Control workflow provides a facility for an operator to orchestrate these otherwise manual steps into an automated workflow. Individual device tasks are grouped into a change control that allows for scheduling, stage-based sequencing, redundancy modal awareness, pre-snapshot and post-snapsots, and notification processing.

The modal awareness includes specific procedures for upgrades to MLAG switch pairs as well as a mode to upgrade spine switches by bringing them gracefully out of and then back into service through BGP maintenance mode.

Once the change control is built, the operator must go through both a review and approval step before the change control can be executed. In addition, each of these steps is tied into CloudVision’s Roles Based Access Control (RBAC) system so that different authority levels can be applied to each step. A strict non-author review model can also be enforced for change control approvals.

All of these capabilities work together to ensure that the network change control proceeds without impacting the network operation. With this workflow, operators have a tool that can make changes across the entire network without concern for slow manual procedures and typical human errors.
Viewing Device Comparisons

Typically, enterprise customers perform change controls outside production hours and request a change control window. When the change control window starts, the engineer performing the change will perform pre-change control procedures e.g. capturing switch interface status, VLAN status, ip routing status, multicast status, ACLs, QoS configuration, etc. using a number of show commands. These scripts may be run on a single device on a larger set of devices depending on the size of the change. Once the change has been completed, the engineer will most probably run exactly the same scripts again. The reason these scripts are run is to ensure that the delta performed during the change is per expectation. The only way to ensure this delta is accurate is if the engineer were to manually compare the pre-change & post-change status. If the change impacts a large number of devices, it is not manually possible to ensure 100% accuracy and there is a reliance on the sample-based confirmation, which substantially increases the risk of the change. Typically depending on the device or the complexity of the change, verifying the change manually can take an hour per device.

CloudVision’s architecture of real-time state capture provides a better way to identify these state changes because it can identify the changes as they happen in real time. When this data is captured over time, it can be leveraged to track changes in key device metrics or review state before and after configuration changes and to facilitate network wide rollback. Continuous snapshots and Diff Views are key features that leverage the historical state database to automatically track state changes and present comparison views that highlight the changes in device state.

This functionality can be viewed on a per device basis as ‘Historical Comparison’. Historical comparison tracks deviations from an established baseline for key metrics that network operators typically track per device such as CPU utilization, peering status for BGP, MLAG and entry count for MAC, ARP and routing tables. In addition to these device states, users can also capture outputs of CLI commands periodically and review the differences between outputs in a user-friendly rendering that highlights the differences. Continuous snapshots leverage the state repository to automatically track and compare changes in device state which provides a starting point for the network operators trying to identify what’s changed in their network.

This concept of comparing device outputs from different points in time has traditionally formed the basis for identifying changes in the network, and is often the first step in network troubleshooting. This is also often the task that consumes the most time when done using a device-by-device approach. CloudVision’s historical state repository and analytics framework automatically tracks changes from a baseline and summarizes the changes based on key metrics indicative of normal operation. Diff views provide an easy to read view that clearly visualizes the differences between the data sets at the device level, and summarizes the metrics for
layer-2 and layer-3 tables such as ARP, MAC, IPv4 Routing and IPv6 Routing tables. The views offer a user-friendly way to identify exactly what entries were removed and added between the two points in time making it easy for network operators to focus on the changes rather than spending time parsing data trying to identify what has changed over time.

Using Network Rollback

Building on top of the Snapshots, network-wide rollback brings this concept to our maintenance windows for a before and after comparison before the change takes place. All enterprise networks have maintenance windows in order to make changes to adjust to business needs. However, any time a maintenance window or change happens, there may be a need to roll back to a previous configuration for unforeseen reasons. Similar to how with virtualization we have the ability to take a snapshot and rollback to previous dates, Cloudvision now brings this concept to the networking world.

One issue with traditional network operating systems is the inability to easily move between different versions of code, or configuration. Network engineers in the past have used notepad files or spreadsheets in order to accomplish their maintenance windows. CloudVision now allows for an easier approach, leveraging CloudVision’s state database allows for a quicker change between two different states on one, some, or all switches in your network.
Deploying CloudEOS

CloudEOS is Arista's multi-cloud and cloud-native networking solution supporting autonomic operation, delivering an enterprise-class, highly secure and reliable networking experience for the cloud. CloudEOS is the same Arista EOS software image packaged as a virtual machine or a containerized package, and is usually deployed in public cloud and Kubernetes environment interconnect virtual private cloud (VPC), virtual private network (VNET), and Kubernetes POD network.

By integrating Hashicorp Terraform with CloudVision, CloudEOS will be declaratively provisioned and configured in public cloud environments to build out a secure, high performance, and segmented enterprise backbone network in minutes to accelerate enterprise customer’s cloud adoption. Once the network is built, CloudVision’s multi-cloud dashboard allows customers to monitor their cloud network, including VPCs, VNETs, as well as network performance (latency, jitter, packet loss and bandwidth) between and across multiple cloud providers. In CloudVision’s topology view, customers can visualize the cloud deployments to understand how VPCs, VNETs are interconnected, and what segment those resources belong to for compliance reasons.

Figure 24: Topology View Example with CloudEOS Tunnels
Risk Management with Compliance Checking

Arista's Compliance Dashboard provides a comprehensive view of the current state of the infrastructure as it relates to security advisories, NIST Common Vulnerabilities and Exposures, and enterprise-wide security and operational standards. This system is updated in real time as new vulnerabilities are released allowing a clear measurement of environmental risk and the rapid implementation of compensating controls and patches through the CloudVision upgrade workflow. This enables the enterprise to rapidly remediate these exposures while orchestrating the deployment of the non-disruptive patch or software release in a manner that minimizes or altogether eliminates any outage.

Compliance dashboard provides a real-time summary view of image, configuration and security compliance for all managed devices. Compliance tracking for security vulnerabilities provides the user information about potential vulnerabilities and software releases that carry the fix for the same. The dashboard also shows a summary of known high severity software defects (software bugs) that affect managed devices. The assessment uses bug details published on www.arista.com and leverages the network wide database to compute the exposure based not just on hardware and software versions but also real-time state of configuration and operating conditions. CloudVision has the ability to get the latest information on known software defects through updates from arista.com hence allowing customers to leverage this information in making network-wide software upgrade and patch rollout decisions.
CloudVision Integrations

CloudVision’s framework can integrate with 3rd party systems and devices, both northbound and southbound. By leveraging the well-defined APIs, operators further customize CloudVision into existing management infrastructure and other 3rd party management platforms.

CloudVision is the preferred point of integration with other best of breed solutions, including overlay controller integration, flexible compute integration, application services (Layers 4-7) integration, workflow tool integration, telemetry tool integration, and many others. In addition, CloudVision can be customized to integrate with customer-specific scripts and management tools through its open APIs.

Network API Gateway

CloudVision’s approach starts with standardized OpenConfig data models as the basis for CloudVision’s data repository.

![Network API Gateway Diagram](image)

*Figure 26: CloudVision's Network API Gateway Approach*
CloudVision APIs
CloudVision is an extensible platform with a suite of APIs for custom integrations.

To start, CloudVision has a REST based API for configuring/monitoring/managing resources on CloudVision. The API documentation is built into the CloudVision web portal itself (at https://<cloudvision_address>/web/api). As an abstraction, CVPRAC is a Python wrapper for working with the API.

CloudVision APIs can be accessed through gRPC and protobuf, which enables a high speed, efficient, and data model-based communication with CloudVision. These APIs are documented on the Arista Github page, here: https://github.com/aristanetworks/cloudvision-apis

Bi-directional information can also be exchanged with CloudVision through websockets, which is particularly useful for web-based application development.

Arista provides the CloudVision Connector javascript library to facilitate websocket interaction: https://github.com/aristanetworks/cloudvision/tree/trunk/packages/cloudvision-connector

Additionally, CloudVision can send notifications to a number of 3rd party notification receivers when events are triggered. This includes an option for webhooks to trigger notifications to generic applications. Supported notification endpoints include: e-mail, VictorOps, PagerDuty, OpsGenie, Slack, WeChat, Pushover, and Webhook.

ITSM, ITOM and AIOps Integration
CloudVision API Gateway and SDK are an extensible platform with rich APIs that drive all of the CloudVision web portal GUI functionality and provide a platform for integration with IT Service Management (ITSM), and IT Operations Management (ITOM) and Artificial Intelligence for IT Operations (AIOps). They provide the ability to integrate with other orchestration and operations management workflows.

An example of this is with the workflow integration between CloudVision and ServiceNow. CloudVision integrates with ServiceNow to allow task and device related information to flow freely between the two applications. Supported features include ServiceNow Change Request generation and ServiceNow CMDB Management. With this integration, change requests are created in ServiceNow for every task created in CloudVision, and task execution takes place on approval of the change request in ServiceNow. Notes and logs for the change request are seamlessly ported between the applications to provide a complete audit trail. If ServiceNow is used for managing and tracking network devices in its Change Management Database (CMDB), the CloudVision inventory feature supports automatic import and population of switches managed by CloudVision into ServiceNow’s CMDB.

DevOps Integration
When managing network configuration changes in a DevOps environment, a number of tools such as Ansible can be used to drive configuration changes through CloudVision. By interfacing with the CloudVision northbound API, DevOps modules like Ansible allow administrators to generate network configuration changes through CloudVision using their DevOps platform of choice. This enables standard DevOps workflows that manage compute and storage to manage networking, while still gaining all the additional benefits of CloudVision for monitoring, visibility, compliance, and change control.

In addition, CloudVision integration with IPAM tools such as Blue Coat and Infoblox provides programmatic allocation of IP addresses in CloudVision Configlet Builders, pulling information from a single source of truth.
Device SDK

CloudVision focuses on managing and monitoring Arista devices, leveraging the powerful EOS state streaming and eAPI capabilities. However in brownfield deployments operators may have third party devices, which can create monitoring blind spots.

To address these gaps, CloudVision’s Device SDK provides support for monitoring third party devices. Arista has standardized on gRPC and OpenConfig as the interface for all devices into CloudVision. This means that devices natively supporting OpenConfig and gRPC gNMI can integrate into CloudVision for visibility as well. The Device SDK also supports legacy devices that only accept SNMP, or other third party device APIs, by translating into OpenConfig data models prior to streaming to CloudVision.

With the Device SDK, operators can now get end to end visibility of network utilization and errors across a multi-vendor network.

Overlay Controller Integration

Most SDN controllers are focused on the overlay network itself and are not tightly coupled with the underlay network.

CloudVision provides that openness to serve as a central integration point to all 3rd party controllers, such as VMware NSX. CloudVision also provides a more scalable solution as it does not require the controller to talk to every single network device. Instead, the SDN controller simply talks to CloudVision’s central integration point, which will then communicate the overlay information to the rest of the VTEP devices.

In addition to supporting OpenStack integration, CloudVision is fully open to supporting any customized controller that the customer may want to deploy. This provides the customer the choice of not being locked into any single overlay vendor.
Service Insertion
Of the various points of integration, the network firewall service is often the most difficult to design into today’s cloud networks. Considering the myriad of traffic patterns, firewall policy enforcement is dependent on seeing traffic across both virtualized and non-virtualized hosts as well as increasing east-west traffic patterns. The challenge becomes where to place the network service so that it is in the data plane path to make a filtering decision for most – if not all – traffic in a data center.

With Arista’s Macro-Segmentation Services (MSS), these network services can be more efficiently inserted into network designs, regardless of where traffic originates. MSS runs on CloudVision, which sees the entire physical network and serves as a broker point for service insertion by leveraging APIs to the appropriate service device. And MSS doesn’t change the service operations model, as all service enforcement and administration is in the domain of the appropriate service appliance.

MSS integrates with a number of Arista’s security partners, including across physical and virtual security models.

For more information on Macro-Segmentation, see our Solution Brief here.

Summary
Every CIO is driving a spending shift from traditional IT operations to innovations that meet business needs more quickly. The only way to obtain the substantial OpEx cost reductions required to remain competitive is to automate their network environments.

Traditionally, approaches have been shackled in working with closed or limited network operating systems. This seriously restricts the ability of an organization to be agile and flexible as the application requirements change quickly. This also provides an opportunity for network operations teams to be able to manage a network infrastructure network wide any of the historic, error-prone methods (CLI, API, scripts).

Arista CloudVision is built on an innovative network-wide database architecture and is for cloud-like operations. With a focus on simplified provisioning, configuration, image management, troubleshooting, visibility, security and 3rd party integration, CloudVision provides the platform to allow any organization to reduce OpEx costs by running their network based on cloud principles.