Arista CloudVision®: Cloud Automation for Everyone

In network operations circles, there is an old adage that states ‘the network is guilty until proven innocent’. Touching all infrastructure components - compute, storage, virtualization, apps, etc, it is clear that the network plays a fundamental role in IT operations. With that scope, the network is the service that is expected to ‘just work’. And when an IT issue happens, the network is almost always a suspect.

Network operations teams are chartered to manage availability, costs, agility, and risk. To do so, they need processes and tools that give them the workflows and visibility to control and monitor the network. However, the traditional approaches to monitor and manage networks have failed to keep up with today’s cloud networks. The historical ‘box-first’ sales focus has meant that network software and management were distant, under-prioritized components in any vendor’s solution.

As a result, network operations teams are challenged across a number of areas, including troubleshooting, manual operations, and compliance management. As human error remains a primary cause of network issues, new software approaches are available to enable an evolution to automated network operations. In embarking on an automation journey, operators can improve their mean-time-to-innocence.

Figure 1: Challenges for Network Operations
Cloud Principles for Network Operations

Over the better part of the last decade, cloud operators have led the industry with new approaches to scale-out designs and software-first thinking. These cloud principles have modernized cloud networks with simplified designs using standards based protocols and software-driven orchestration to help scale the operations. These cloud operators leverage network automation to simplify the manual, time consuming and resource intensive tasks to bring operations efficiency at scale. And they have driven new principles to improve visibility and reduce troubleshooting efforts.

These cloud principles are here today and can apply to any network. Customers want to embark on this journey to cloud networking operations, but are often challenged with breaking away from the traditional network operation models. The considerations include the following decision points and factors:

1. **Build vs. buy.** Automation for some is done via a build it yourself software model. Most enterprises do not have the time, skill set, or resources to build homegrown automation themselves. Therefore, enterprises are looking for a modern, consistent NetOps platform that is also turnkey. And while there are many network management tools available for purchase, most are lacking true cloud-principles for automation and telemetry.

2. **Modern architecture.** Cloud network operations cannot be built on network management tools that are decades old (e.g. SNMP polling, screen-scraping). Modern architectures including state-streaming APIs, big data repositories, and advanced analytics are needed to truly achieve network automation.

3. **Silo'd operational approaches.** Traditional networks have been deployed by selecting a different ‘box’ for each place in the network. With each box came a different operating system, with different features, different APIs, different management apps, etc. But the cloud principles are based on a software-first model, which normalizes the various network boxes to a uniform software operating model. This software approach is not just for the data center. A common approach for automated provisioning, or real time troubleshooting can apply to the campus, the cloud, and the routed interconnect, as well. Operators don’t need to re-invent different solutions for each. In fact, there is significant benefit of consolidating network ops on a single uniform approach.

![Figure 2: Operational Benefits of a Consistent Operations Model](image-url)
Arista’s Approach to Automation

Arista’s software-first approach focuses on improving the user’s operational experience. With a single operating system across platforms and use-cases, Arista EOS (Extensible Operating System) dramatically simplifies the complexity of a myriad of OS trains that proliferate across a typical network. Built from the ground-up as a programmable software platform, EOS has established itself early-on as a preferred platform for software integration.

There are several approaches to network automation, with the primary approaches summarized as follows:

CloudVision changes that operational model by taking a drastically different approach. It is built on the following four characteristics:

1. **Do-It-Yourself (D.I.Y.) Automation** - D.I.Y. solutions are typically deployed by ‘cloud titans’, such as Microsoft, Facebook, etc who are building massive data center infrastructures. Often cloud titans have a 10x appetite for deploying infrastructure (server, database, network) compared to the largest enterprises. For them data center automation is necessary to their business model as a means to compete in the marketplace. Such large organizations also have different application profiles and their applications are designed to account for infrastructure failure. As a result, cloud titans often employ large software teams to write custom designed scripts to automate their infrastructure. Arista helps such customers by providing them open tools like EOS SDK, Openconfig / gRPC and eAPI with unrestricted access to the Linux infrastructure to be able to fully integrate EOS-based switches into their broader software orchestration system.

2. **DevOps** - This model is typically deployed by large Service Providers or larger Enterprise, as they embark on the automation journey. The approach includes prebuilt 3rd party automation frameworks typically also being used by the compute teams, such as Ansible, Puppet, and Chef to consolidate provisioning tools and apply those frameworks to the network infrastructure to drive down OpEx costs. Such customers are large enough to have resource pools available in order to write custom scripts to achieve some of the automation gains in their environment. They are more invested in the automation approach with committed resources, budget and vision to achieve the OpEx reduction goals. Arista supports these deployments by providing open software integration into these DevOps frameworks like Ansible, Puppet, Chef, as well as streaming platforms like ELK stack, Prometheus, others, to be able to fully customize their network.

3. **Turnkey solution** - There are limited tools which exist in the marketplace today to guide customers down the path to network automation. Arista’s CloudVision provides a turnkey solution allowing customers to be able to provision, manage and gain more visibility into an infrastructure while still allowing the tools for extensibility and customization. This software is designed to help customers of all sizes, in particular the small, mid-sized and large enterprise across every vertical, who are looking to reduce OpEx by applying the lessons-learned and problems solved from network automation of the cloud providers. As mentioned before, other enterprises have the need and desire to embark on an automation journey, but do not have the time, skill set, or resources to do so. This is where CloudVision comes in.
Arista CloudVision Overview

Arista's CloudVision is a turnkey management plane providing a modern approach to automation and telemetry. It is a software product - available as a virtual or physical appliance - for managing any EOS instance - physical Arista switches, vEOS in the public cloud, cEOS in Kubernetes environment, EOS running on white boxes, and access points. Because of this scope, CloudVision is a single management plane across data center, hybrid cloud, and even campus, helping to break down traditional box-based network silo's.

CloudVision builds on one of Arista's core strengths - the innovative EOS state database model, called "NetDB" - extended to a central repository through native state-streaming APIs. NetDB holds the entire state for a particular device (e.g., configuration, topology, protocol state, monitoring counters details, etc) as well as the entire state of all the devices across the network. The system is a modern platform, 100% streaming based - with no legacy polling or MIB limitations - for a more granular and complete centralized view.

• Leveraging this network-wide database - or NetDB - architecture, CloudVision focuses on three key pillars of functionality:
• Telemetry and Analytics, based on this native state-streaming for real-time and historical visibility into network state
• Automated Provisioning and change control workflows for cloud-like network operations
• Orchestration, as a single point for integration with both 3rd party ecosystem partners as well as native APIs for customer extensibility options.

Figure 4: Arista's Places-In-the-Network (PINs) to Places-In-the-Cloud (PICs) Strategy

Figure 5: Three functional pillars in one platform
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 historically 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 a complete dataset. This is incredibly important for any network analytics, where the insights can only be as deep as the underlying dataset.

To achieve this goal, CloudVision is built on a modern scale out database architecture with end-to-end streaming. It is designed as microservices orchestrated under kubernetes, but packaged as a turn-key solution so that it is accessible to any customers.

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

These components break down into functions as described below and as depicted in figure 7:

- 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

![Figure 6: Telemetry System Components](image)

![Figure 7: CloudVision Streaming-based Pipeline](image)
State is streamed throughout the system end-to-end: from each device, into the database, through our analytics pipeline, and then to the UI. There’s no polling anywhere in the system.

CloudVision applications are built on top of the foundation of modern network management APIs, namely gRPC gNMI and OpenConfig. OpenConfig is an industry effort driven by operators to define standard models for network devices, and is the obvious choice for modeling network state in CloudVision for external consumption. OpenConfig is the standardized data-model for device data in CloudVision, supplemented with Arista data models to build the complete state of the network.

The transport layer between services throughout the system, as well as externally to CloudVision, is gRPC. gRPC is a modern high-performance framework built on top of protobufs and HTTP2, providing the scale and performance to stream the full network state from each device and through the CloudVision pipeline. The EOS streaming telemetry agent in EOS and the Device SDK are built on top of gNMI, a standard gRPC Network Management Interface to provide read, write, and subscribe semantics from network devices.

In order to provide a network-wide aggregate view, the CloudVision Analytics Engine, which is part of CloudVision Portal, serves as a backend repository to collect and process the state data. The Analytics engine performs a variety of data analysis including state correlation, event generation, trend monitoring, anomaly detection and other state 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.

CloudVision fits into a broader telemetry framework that allows streaming between 3rd party repositories and UI engines.

The rest of this whitepaper will focus on the various functionality that where CloudVision can be deployed across the enterprise data center, campus, and hybrid cloud use-cases.

Figure 8: CloudVision Open Telemetry Framework
Real-time Telemetry

Today’s spine / leaf network designs provide a solid framework for scale-out network designs but also come with new challenges for network visibility. Without proper visibility, the network operators are driving blind to determine outage causes or capacity planning. Arista EOS has a long history of network telemetry tools, called Tracers, which provide visibility into the devices, the topology, and even the workloads. These tools have been a strong foundation to ensure visibility and reduced mean-time-to-resolution (MTTR) when troubleshooting a spine leaf architecture.

Traditional visibility tools are built on SNMP polling-based approaches that gather state every few minutes, thus only providing a very limited view of the network state. With NetDB, Arista EOS devices store all real-time state in one common database and then aggregate that state from all devices into a network-wide view. By collecting every state change on the network, Arista customers have access to both real-time and historical views of the network in one place and at a level of granularity never before achievable.

To leverage this rich network data, the CloudVision platform provides both the analytics engine and telemetry visualization for this network-wide state. On the backend, a scalable state repository built on open-source HBase runs an analytics engine to track trends, correlate data across devices and layers, and detect anomalies.

Topology App

CloudVision breaks down legacy network silo’s 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. 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 how topologies would be drawn. 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. The topology view provides this broader view and provides direct access to the lower-level interface or device views. Items such as events, bandwidth, error/discard rates, network segments are displayed as optional layers on the topology. The view allows users to further identify and drill down into device interconnect links to view additional metrics in the Metrics View. The timeline can be leveraged in Topology View to view historical state for link level metrics.

Events App

Events are created when one or more metrics in the state database reach a certain criteria, as defined in the Analytics Engine. Events are categorized similar 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 for 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 was 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 was 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 manage the health and congestion network wide and to report any 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 provides 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 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 prevent network operators from overlooking important events.

**Device App**

This view offers a detailed insight into every metric at a device level that is accessible using CLI commands such as environmental, system details, interface statistics, MAC address and routing tables. In addition to these metrics, it also includes platform level details like digital optical monitoring (DOM), hardware route table, ACL table 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 historical state for forensic troubleshooting.
### Metrics App

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. 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 errors and congestion across interfaces in the network using a few clicks versus a manual approach.

*Figure 11: CloudVision’s Device App*

*Figure 12: CloudVision’s Metrics App*
Cloud Tracer App

While telemetry and visibility is important within the datacenter, it is even more important when operating in a diverse hybrid cloud environment. Workloads that span the 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.

![CloudTracer Dashboard](image)

While designed for the hybrid cloud use-case, the Cloud Tracer App can provide reachability across any network type and any network endpoint.

Automated Provisioning

Even today, most network device provisioning, software upgrades, and configuration changes are still being done manually. This not only takes significant amounts of time, 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. A suite of functionality provides the tools needed for a fully automated network operations lifecycle, including building the network configurations, deployment, and on-going operations.

![Full Automation for the NetOps Lifecycle](image)
Deploying the Network

To resolve the above problem, Arista was the first in the networking industry to deliver Zero Touch Provisioning (ZTP). ZTP allows the customer to take 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. CloudVision’s ‘Network Provisioning’ portal process allows the end user to create a logical network design diagram view to ensure devices are being provisioned with a data center leaf/spine topology view or any other network topology view, which represents the final deployment design. With a logical hierarchical inheritance, administrators can assign switches to different containers which in turn have the ability to apply settings like switch configuration, image version, and device labeling.

When network switches are managed, typically a configuration, image and script are used to provision and manage change controls for that switch. The ‘Network Provisioning’ portal allows a customer to perform all three actions at the same time in a network wide view.

To take ZTP to 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 allows the ability for the dynamic creation of configuration via Configlet Builder – a way to enable you to programmable create device configurations, this prevents administrators having to manually create each configuration for every switch. By using a user interface (UI) and Python engine, administrators can create their own form-driven prompts to create configurations for any EOS feature, which can then in turn get applied to switches or a container full of switches.

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.

Deploying vEOS

Virtual EOS (vEOS) is the same Arista EOS software image packaged as a virtual machine. vEOS is commonly used in the public cloud networks as a network stack for interconnecting virtual private cloud environments.

In these environments, the provisioning of a new vEOS instance requires specific cloud-specific credentials. CloudVision is able to store these credentials for multiple cloud platforms (AWS, Microsoft Azure, in particular) and incorporate them into the provisioning process for vEOS. This provides automated workflow for provisioning a new vEOS instances and reduces the manual credential input.

Operate: Snapshots

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 & 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 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 feature is integrated into the Telemetry UI as a result and 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 leverages 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 provides 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.
Operate: 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 comprises of 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- and post-snapshots, and notification processing.

Figure 16: CloudVision ‘Diff Views’ Example

Figure 17: Change Control Orchestration
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.

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.

**Operate: 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 rollback 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 revisions 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.

**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.

Integrating with CloudVision

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 OpenStack integration, overlay controller integration, flexible compute integration, application services (L4-7) 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.

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.

IToM Integration

CloudVision Portal is an extensible platform with rich APIs that drive all of the GUI functionality. This provides the ability to integrate with other orchestration and operations management workflows. An example of this is with the workflow integration between CloudVision Portal and ServiceNow. CloudVision Portal 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 Portal, 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 the Change Management Database (CMDB), the inventory feature supports automatic import and population of switches managed by CloudVision Portal into 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 allow administrators to generate network configuration changes through CloudVision using their DevOps platform of choice. This allows 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.
Figure 20: Third Party Device support visualization
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 a 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.