Arista Cognitive Campus Network

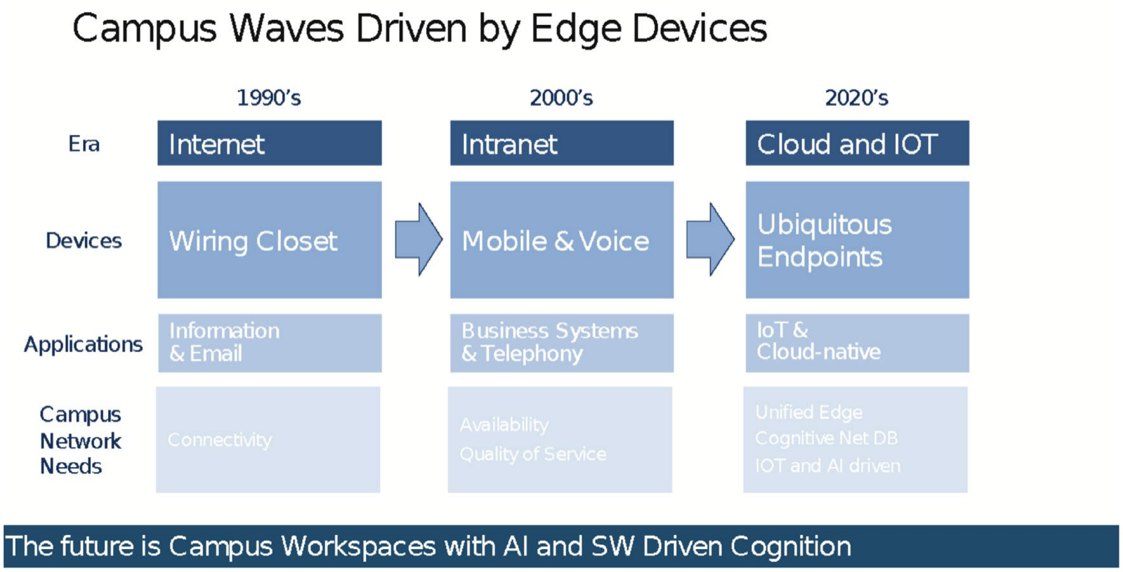
The recent global upheaval has forced an unexpected sea-change upon corporate business workflows and campus networks. Workers and network administrators not only have to embrace a new model of the diffused campus workspace, but also adapt to the revised security, support and collaboration challenges imposed by social distancing, contact tracing and an amplified reliance of collaboration tools that are evermore business critical. Furthermore, campus IoT device deployments are exploding, as more use cases are becoming commonplace in the distributed workforce; amplifying workforce productivity, and providing better monitoring of workloads, workers and physical workspaces.

While the relentless price/performance improvements of campus switched LAN and Wi-Fi technologies remains an important criteria for infrastructure upgrades, there is a new emphasis on automation, telemetry, and decision support analytics to offload and streamline day to day management activities from overly burdened NetOp and SecOp teams. Additionally, there are requirements for automated deployment, declarative configuration management, and simplified remediation, that allow a more diverse group of net admins to realize point and click, zero touch campus network deployments and maintenance.

Network administrators look for standards based solutions delivering high quality, ease of maintainability and a simplified administrative experience to facilitate templatized deployments, and help administrators build on industry best practices and their networking experience. Furthermore, as enterprises continue to drive operational efficiencies with new use cases, leveraging net based apps and specialized IoT devices, administrators look more to automation systems and tools to fulfill the business imperatives of predictable, repeatable and successful outcomes in the management of their ever growing network campus workspace.

Arista's Cognitive Campus Architecture delivers a comprehensive set of capabilities needed to fulfill the communications challenges of workers coping with increasingly dispersed workspaces. As workers require constant access to their corporate and cloud resources, Arista's Cognitive Campus Workspaces meets constant availability requirements, with hitless upgrading and patching, lossless failover, and proactive remediation of client connection issues.

Arista’s enhanced visibility, based on secure, real time state streaming, is coupled with highly scalable SaaS or premise based NetDB data repositories, open API’s, auto remediation turbines, and machine learning assistance, to form an enterprise wide Cognitive Management Plane (CMP) which is vital for managing all wired/wireless workspace infrastructure. Arista’s Cognitive Campus Architecture delivers the telemetry, analytics, automation, decision support systems and open API code points that gives administrators unparalleled visibility, network analytics and additional best of breed monitoring solutions from an ecosystem of partners that ensures the smooth operation and growth of today’s remote and office workspaces.



Campus Waves Driven by Edge Devices

	1990’s	2000’s	2020’s
Era	Internet	Intranet	Cloud and IOT
Devices	Wiring Closet	Mobile & Voice	Ubiquitous Endpoints
Applications	Information & Email	Business Systems & Telephony	IoT & Cloud-native
Campus Network Needs	Connectivity	Availability Quality of Service	Unified Edge Cognitive Net DB IOT and AI driven

The future is Campus Workspaces with AI and SW Driven Cognition

Figure 1:Evolution of the Cognitive Campus Network

Extending Cloud Grade Principles to the Campus

Today’s era of cloud computing is radically changing how networks are provisioned, operated and monetized. Many of the cloud grade principals that have become best practices within data centers and now being evaluated and implemented across campus workspaces. These principles include more efficient leaf/spine architectures, a highly programmable API driven network operating system, declarative provisioning and change management workflows (for automating many of the mundane deployment and configuration tasks), rich real time telemetry for security mitigation, proactive remediation, location services, and specialized applications (contact tracing) for compliance to regulatory and other industry standards.

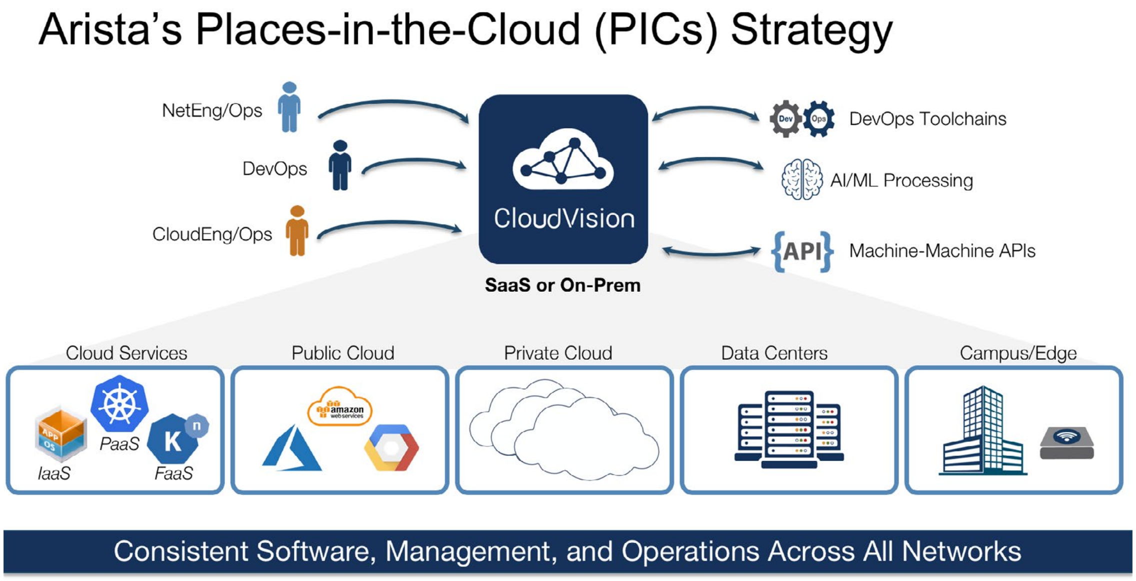
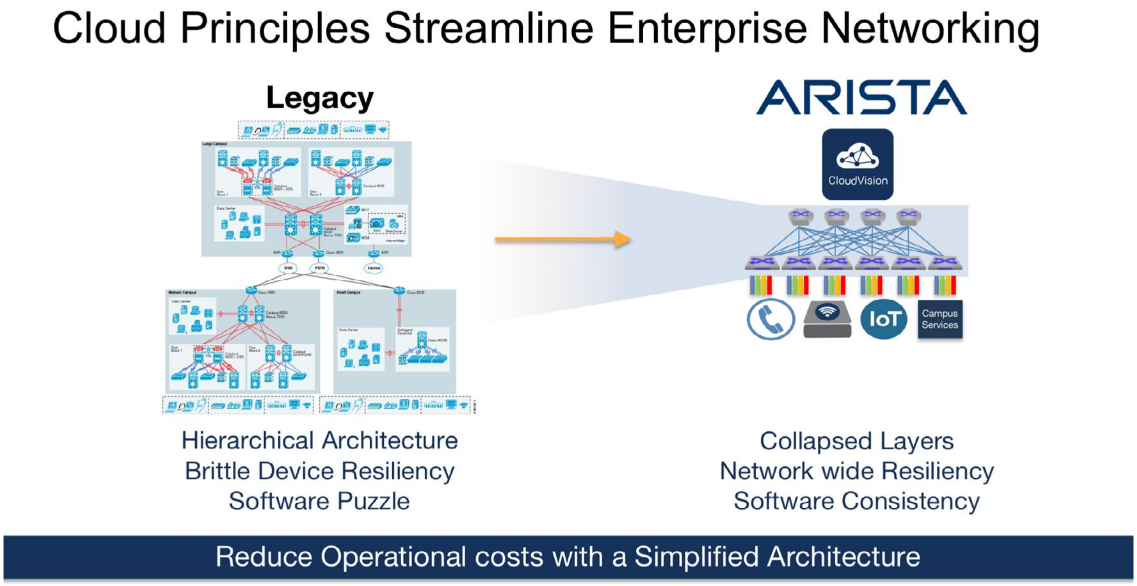


Figure 2: Universal Cloud Network

While the performance requirements of a remote office worker differ from a web server handling 1000's of transactions per minute, the need for security, reliability, traffic visibility and analytics, Quality of Experience, and problem mitigation are common. As a result, campus networks need to evolve much like data center networks have over the past 10 years.

The goal of the cognitive campus is to help the workforce remain productive while adapting to the changing environment: fulfill campus quality of experience through improved visibility of key performance indicators, leveraging machine intelligence to troubleshoot and automate compliance remediation. Finally, the cognitive campus builds on a reliable, consistent architecture that is open and leverages other leading solutions. It delivers quality and consistency to help administrators avoid the pitfalls of inefficient legacy architectures that are brittle, costly to deploy and maintained, and are plagued with disparate OS feature sets and management tools. Cost and performance efficiencies can be obtained by collapsing legacy access-aggregation-core topologies to a campus leaf-spine or spline as shown in Figure 3.



Cloud Principles Streamline Enterprise Networking

Legacy

ARISTA

Hierarchical Architecture
Brittle Device Resiliency
Software Puzzle

Collapsed Layers
Network wide Resiliency
Software Consistency

Reduce Operational costs with a Simplified Architecture

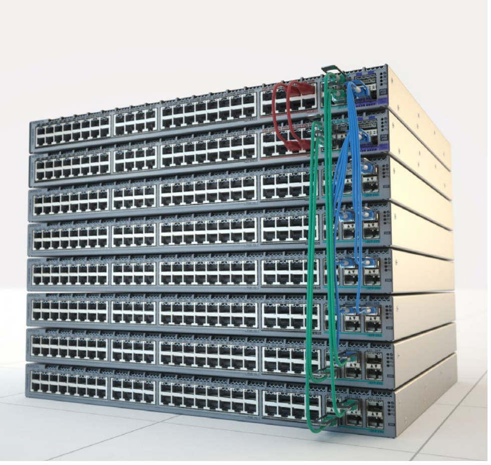
Figure 3: Three Tiered Layers versus Single Tier Campus Leaf Spine or Spline^{TM}

Campus architects should also expect table stakes services like VoIP, QoS, RADIUS, or 802.1X, and newer business critical services like remote access, SAML/SSO, behavioral segmentation and AI/ML troubleshooting, should work with brownfield environments and not require a forklift refresh or proprietary end to end implementations. New architectures should be able to embrace best of breed ecosystems to enhance security, monitoring and segmentation.

Campus designers should look to their data center peers for the automation, telemetry, and AI capabilities of the data center that simplify provisioning, compliance, rich visualization and machine assisted troubleshooting while also automating compliance and segmentation. At the same time, modern provisioning workflows must be adaptable to allow administrators to simplify common tasks to allow delegation to IT generalists. Lastly, campus administrators should look to the price/performance benefits of cloud grade platforms that marry cost effective, open standards systems supporting 10/25/40/50/100G Spline uplinks to evolving 10/100M, 1G, 2.5-5MGig, 10GBase-T and Wi-Fi 6/6E access technologies.

Collapsing the mid-tier aggregation and core layers reduces equipment count and costs while increasing reliability. Next generation, active-active, dynamically load sharing paths improve spine to leaf bandwidth utilization, improving both performance and reliability. This obsoletes the "reliability or performance" compromise of active-passive control plane architectures. New cloud campus spines and leaf architectures enable hitless maintenance and advanced reliability features that prevent network degradation and failure. Finally, open L2, L3 and virtual overlay feature sets are scalable, interoperable, and dynamically reconfigurable, giving network designers the flexibility to accommodate workload variety and graceful evolution. Examples range from reconfigurable route scale to supporting open standards based EVPN-VXLAN in the campus, letting managers integrate with, and transcend the limitations of 802.1q 4K VLANs to the possibility of 16 million VNIs (Virtual Network Interfaces) to accommodate device and workload proliferation.

MLAG Aggregation



In the 1990's, proprietary stacking architectures were developed to simplify expansion and management of grouped campus wiring closet switches. However these stacking schemes have not aged well, showing compromised reliability and elevated CapEX/OpEX due to complicated, proprietary hardware architectures and costly cabling accessories, brittle software life cycle management and underwhelming performance from oversubscribed daisy chained network devices.

Arista's EOS MLAG uses industry standard LACP-LAG with dynamic load balancing to deliver active/active connectivity to stacked switches by leveraging standard, economical Ethernet from 1G-100G. Field validated in thousands of data centers, MLAG is simpler, more reliable, standards based, and interoperable with other LAG capable devices. Maintenance and expansion is hitless, while monitoring and software lifecycle management is simplified through Arista's CloudVision Management platform, or other industry standard DevOps tools.

Cloudscale, Real-Time Telemetry for the Enterprise

Today's business critical applications rely on a hybrid wired and wireless distributed campus infrastructure. This is also the case for the exploding variety of IoT devices such as cameras, monitors, sensors, security devices and other user critical appliances. The scope of the enterprise campus is evolving too, incorporating branch, remote and home workspaces. Therefore, to maintain service levels and ensure user productivity and application performance, campus administrators require management systems that simplify repetitive or common tasks, allowing administrators with varying experience to confidently remediate or update the campus infrastructure. These management systems must also monitor the collective infrastructure to facilitate troubleshooting, compliance and remediation of the entire campus net. The management architecture's utility must adapt to a broad set of infrastructure expertise, while its management scope must be comprehensive, incorporating as much of campus workspaces as possible to deliver better visibility for administrators and their tools.

Campus architects must also evaluate state of the art, real time monitoring services that can deliver more information, more efficiently. Real time monitoring, coupled with AI/ML performance analytics that track workspace infrastructure, workgroups, applications and users, helps the operations team maintain SLAs, spot or even anticipate potential problems, and rationalize infrastructure investment. To achieve these goals, campus infrastructure platforms must deliver comprehensive state streaming telemetry, beyond bytes and drops, to include throughput and latency data at the client, workgroup, and application level. Campus networking systems must be able to glean and report on the thousands of user and application flows in the enterprise, detailing throughput, duration, latency and congestion, to name a few. Lastly, administrators should expect no compromise in reliability, performance or manageability.

Of course, innovations in telemetry must be matched with advances in monitoring systems. Even at five second intervals, polling schemes, like SNMP, are too slow and limited in the new world of the distributed cloud and campus. In contrast to legacy schemes, cognitive cloud-based telemetry combines real-time streaming with big data analytics as shown in Table 1. Open architectures such as OpenConfig use standard APIs, like gRPC/gNMI to deliver a wealth of streaming information quickly and efficiently. Publish-subscribe exchange models are inherently more efficient and adaptable because only information updates are shared. The shared data model is also more advanced, providing both data definition or keys, along with data values. Combined, this architecture greatly increases visibility, while reducing telemetry processing and network load.

Table 1: Legacy vs Modern Telemetry

Traditional / Legacy Approach	Campus Telemetry Requirements
Polling Approach (1-15 min)	Real-time Streaming
State scope limited to MIB definition	Complete state history
Per-Switch Per Device	Network-wide scope
Static, discrete events. Manually correlated	Dynamic event correlation

While many networking companies understand the value of telemetry and analytics, few have architected analytics to create, stream and process networking data effectively.

Arista's Cognitive Campus Network

Arista's vision and framework for the Cognitive Campus Network leverages cloud capabilities and state of the art merchant silicon to deliver critical services that automate deployment, configuration, visibility troubleshooting and security. The Arista Cognitive Campus delivers spline, leaf and wireless infrastructure platforms, telemetry and analytics, and a single Image EOS that supports an ecosystem of solutions from industry leading partners as shown in Figure 4.

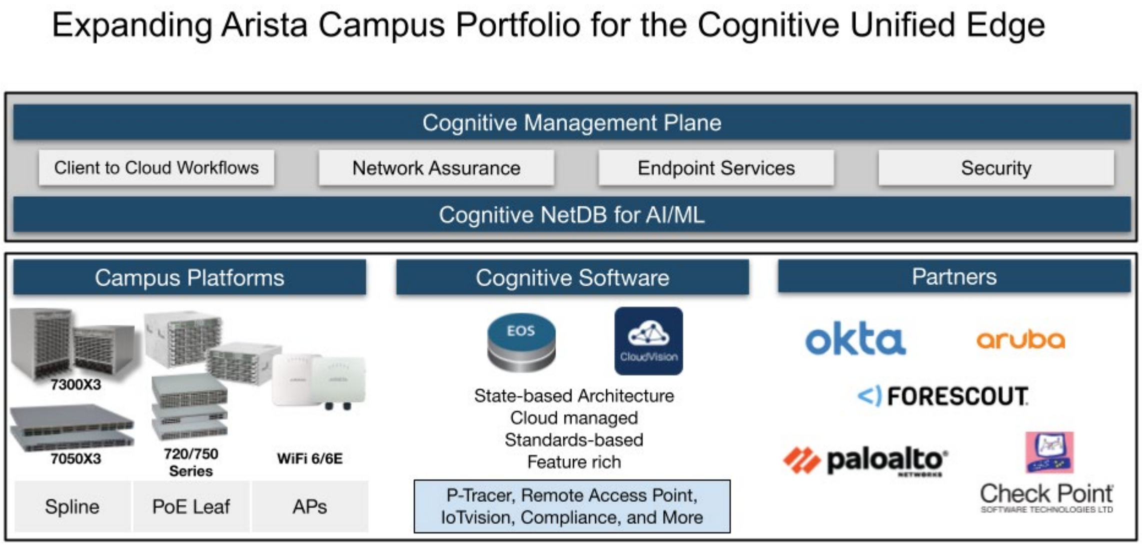


Figure 4: Arista Cognitive Campus - Cognitive Wi-Fi, PoE Leaf, & Spline Platforms, EOS and Cognitive Management Plane based on CloudVision

1. **Splines for Collapsed Campus Fabric**

   Arista has uniquely extended cloud grade capabilities to the campus with the modular 7300X3 and fixed 7050X3 platforms. These spline platforms are designed to provide a suite of cognitive features and actions for high availability and simplicity. Self healing, hitless upgrades and live patching are cognitive actions that avoid impact on the infrastructure. Arista's Smart System Upgrade (SSU) feature enables switch operating software to be completely upgraded while the platform continues to process campus traffic.

   The X3 series switches provide a variety of connectivity options: 1-10G, multi-rate 10/25G SFP+, 40G, 50G and 100G QSFP. These platforms support dynamic load balancing and buffer allocation available to all networked ports to help avoid data loss from link faults, congestion or micro-bursts. The splines work with all devices that support static or dynamic port aggregation to preserve and enhance the installed base investment.

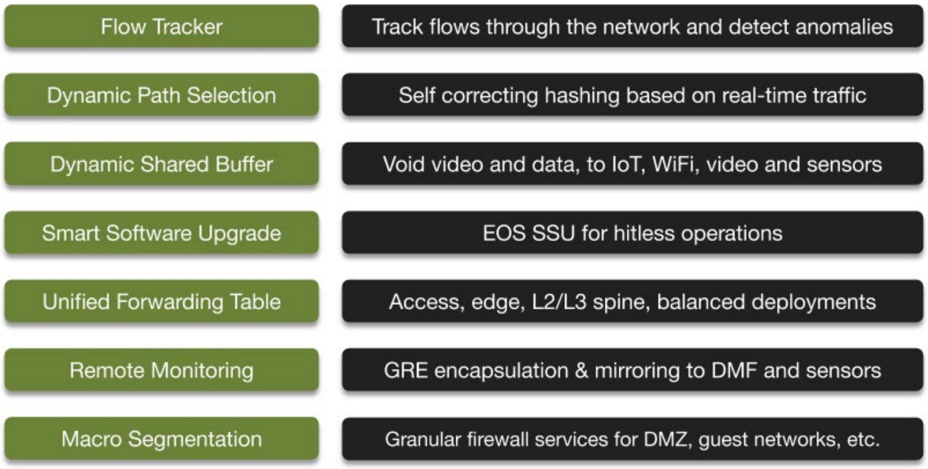
2. **Cognitive Leaf POE Switches**

   With the release of the CCS 750 series modular switches, Arista expands its offering of cognitive, secure, high performance and high density PoE connectivity in the wiring closet, delivering 10M through 10G connectivity, MACsec security, segmentation and power options for all campus user workloads. The suite of platforms delivers a variety of connection options for user desktops, POE appliances and IoT devices. Managed 802.3af-t/bt power services deliver up to 60W, with speed options ranging from 10Mbps - 1Gbps, and 100M - 10Gbps (including MGig) over UTP, to support a variety of campus workloads. Modular SFP and QSFP uplinks support speeds from 1Gbps to 100Gbps which offer flexibility in network architecture and scalability. As with all Arista platforms, the 750 Series runs Arista's common binary EOS, providing a comprehensive set of layer 2 and layer 3 open standard features including MLAG, 802.1Q, EVPN/VXLAN virtualization, and table stakes QoS and segmentation services. Arista EOS supports standards based 802.1X and RADIUS access control and LLDP device identification services to automate admission and segmentation of appliances, users, and applications in the campus.

The 7050X3 and 7300X3 Spline and the CCS 720 and 750 series share the same silicon architecture, and are designed to provide scale up networks with dynamic traffic load balancing, and real time flow monitoring of all campus workloads.

The campus dynamic load balancing makes forwarding decisions based on the rates of existing flows in addition to the traditional static 5-tuple hash. Therefore, new flows are balanced to the least utilized link and are re-ordered as stale flows age out. this performance optimizing feature interoperates with all devices that support link aggregation to ensure trouble free interoperability and migration.

Arista's campus switches also provide real time flow tracker telemetry. Supporting CloudVision and IPFIX APIs, flow tracker allows administrators to capture thousands of key performance indicators in real time for infrastructure, device, application and user data for SLA monitoring and troubleshooting use cases. The combined telemetry of the campus leaf and spline helps administrators better understand the proliferation of mobile, diverse and bursty traffic generated by campus users and devices. Salient EOS features and their benefits enhancing the cognitive campus are listed below in Figure 5.



Flow Tracker	Track flows through the network and detect anomalies
Dynamic Path Selection	Self correcting hashing based on real-time traffic
Dynamic Shared Buffer	Void video and data, to IoT, WiFi, video and sensors
Smart Software Upgrade	EOS SSU for hitless operations
Unified Forwarding Table	Access, edge, L2/L3 spine, balanced deployments
Remote Monitoring	GRE encapsulation & mirroring to DMF and sensors
Macro Segmentation	Granular firewall services for DMZ, guest networks, etc.

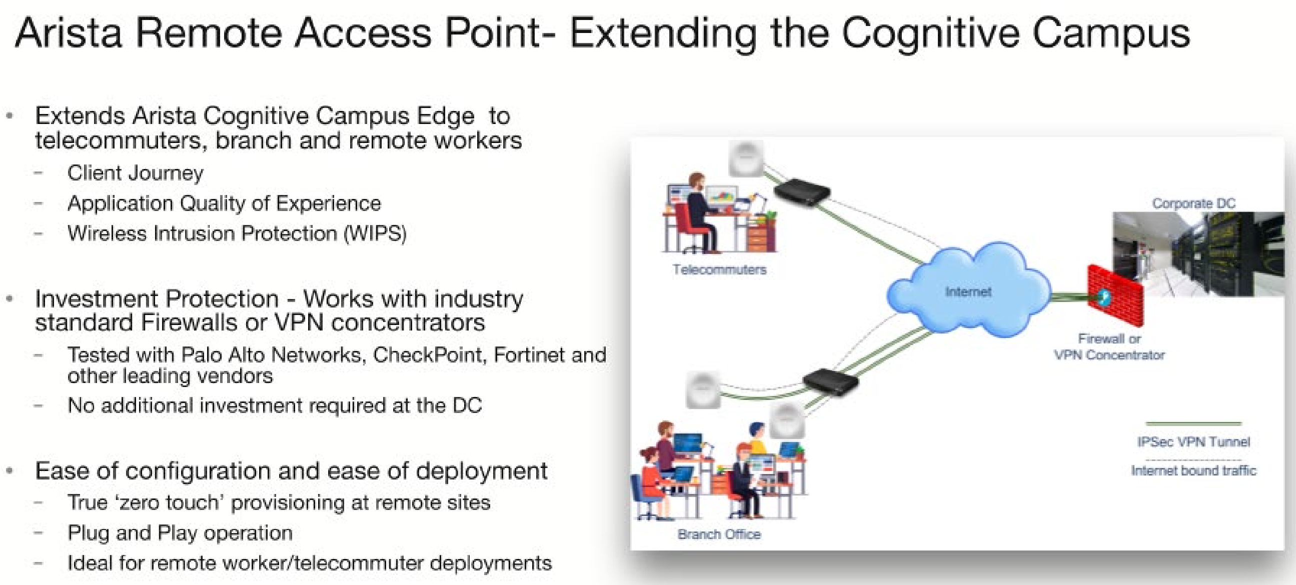
Figure 5 : Key Attributes of Cognitive Campus Splines and EOS

Finally, Arista's campus platforms accommodate a variety of layer 2 and 3 scaling demands with the help of its dynamically configurable Unified Forwarding Table (UFT). Unlike other static architectures with fixed L2 MAC and L3 routing tables, the X3/XP platforms let administrators select from multiple profiles optimized for either L2 MAC addressing, L3 host addressing or IPV4-6 route table scale. This simplifies design considerations because a common platform can be optimized for various campus use cases. Consistent with other Arista platforms, the X3 series supports wire speed L2 VLAN, L3 routing and L2 over L3 VXLAN that transcends 4K vlans to more than 16.7 million industry standard VXLAN virtual networks. Campus-wide dynamic segmentation of workgroups is accomplished through .1Q and EVPN services facilitated with CloudVision automation. CloudVision can extend segmentation orchestration to data center and cloud based workloads.

3. Cognitive Wi-Fi Edge

Arista's distributed data plane architecture for Wi-Fi embeds manageability, telemetry and .1Q or overlay VXLAN segmentation within the access points. This controller-less architecture continues to evolve with Arista's expanding family of Wi-Fi 6E, cognitive access points. The new AP360 series of 4X4 6E capable APs, expand 802.11ax networking capacity by utilizing the 6GHz band (where allowed). These new APs are backwards compatible with Wi-Fi 5-6, supporting upstream/downstream MU-MIMO and OFDMA communications, improving performance and user density compared to legacy Wi-Fi architectures. Finally, this flagship Wi-Fi platform also has a third scanning WIPs radio, with BLE and Zigbee.

As enterprises cope with the impact of social distancing, campus net admins are tasked to extend accessibility of business critical IT functions to workers without compromising their security profile. Arista's cognitive Wi-Fi solution now offers standard VPN overlay features in its APs to extend the campus network to branch, remote or home workspaces. Leveraging IPSEC tunnelling services, Arista Wi-Fi APs interoperate with leading VPN concentrator solutions to extend campus services under the enterprise's existing security infrastructure. CloudVision Wi-Fi's Zero Touch Provisioning (ZTP) services simplifies remote office AP deployment, allowing administrators to drop ship APs to their distributed workforce who simply plug the device into their home network. Fully managed by CloudVision Wi-Fi and with AP support for optional tunneled Ethernet connectivity, Arista's remote access solution fulfills the need for administrators to connect their socially distant workforce.



Arista Remote Access Point- Extending the Cognitive Campus

- Extends Arista Cognitive Campus Edge to telecommuters, branch and remote workers
  - Client Journey
  - Application Quality of Experience
  - Wireless Intrusion Protection (WIPS)
- Investment Protection - Works with industry standard Firewalls or VPN concentrators
  - Tested with Palo Alto Networks, CheckPoint, Fortinet and other leading vendors
  - No additional investment required at the DC
- Ease of configuration and ease of deployment
  - True 'zero touch' provisioning at remote sites
  - Plug and Play operation
  - Ideal for remote worker/telecommuter deployments

Figure 6: Extending Cognitive Wi-Fi across Distributed Campus Workspaces

Arista's expanded family of Wi-Fi6 platforms delivers the highest performance, utility and security to the wireless campus edge. Combining location and scanning radios with AI/ML heuristics in Arista's CloudVision Wi-Fi Manager gives network administrators new capabilities in mobile client monitoring and location.

CloudVision's Wi-Fi manager, available as an on prem or in cloud service, helps optimize the workforce's quality of experience. CVP Wi-Fi facilitates network and application performance monitoring and remediation, provides tools for location and segmentation, and finally secures and monitors campus airwaves.

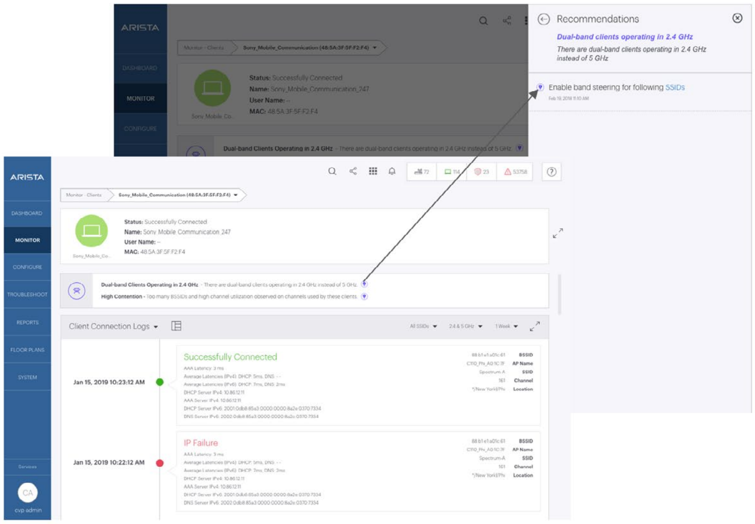
These features include:

Client Journey:

- Connection troubleshooting dashboard to streamline identification of campus users connectivity problems. The dashboard simplifies access troubleshooting including Wi-Fi association, authentication and address allocation, to name a few.
- Inference based Wi-Fi client problem diagnosis
  CloudVision Wi-Fi leverages AI/ML heuristics applied to individual client sessions to analyze and diagnose probable causes of degraded Wi-Fi client experience. As illustrated in Figure 7, the cloud based inference robot offers troubleshooting tips and possible remediation steps to administrators, reducing troubleshooting complexity and downtime while improving operations staff and client productivity.

Cognitive WiFi - Automated Client Issue RCA

- Machine Learning for automatic client connectivity and Performance Issues
- Automatically identifies root causes and provides remediation recommendations



Recommendations

Dual-band clients operating in 2.4 GHz

There are dual-band clients operating in 2.4 GHz instead of 5 GHz

Enable band steering for following SSIDs

Feb 19, 2018 11:10 AM

Status: Successfully Connected
Name: Sony Mobile Communication 247
User Name: --
MAC: 48.5A.3F.5F.F2.F4

Dual-band Clients Operating in 2.4 GHz - There are dual-band clients operating in 2.4 GHz instead of 5 GHz.

High Contention - Too many BSSIDs and high channel utilization observed on channels used by these clients.

Jan 15, 2019 10:23:12 AM

Successfully Connected
AAA Latency: 3 ms
Average Latencies (IPv4): DHCP: 5ms, DNS: - -
Average Latencies (IPv6): DHCP: 7ms, DNS: 2ms
DHCP Server IPv4: 10.86.12.11
AAA Server IPv4: 10.86.12.11
DHCP Server IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
DNS Server IPv6: 2002:0db8:85a3:0000:0000:8a2e:0370:7334

88:b1:e1:a0:1c:61	BSSID
C110_Phi_A0:1C:7F	AP Name
Spectrum-A	SSID
161	Channel
*/New York/Phi	Location

Jan 15, 2019 10:22:12 AM

IP Failure
AAA Latency: 3 ms
Average Latencies (IPv4): DHCP: 5ms, DNS: - -
Average Latencies (IPv6): DHCP: 7ms, DNS: 2ms
DHCP Server IPv4: 10.86.12.11
AAA Server IPv4: 10.86.12.11
DHCP Server IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
DNS Server IPv6: 2002:0db8:85a3:0000:0000:8a2e:0370:7334

88:b1:e1:a0:1c:61	BSSID
C110_Phi_A0:1C:7F	AP Name
Spectrum-A	SSID
161	Channel
*/New York/Phi	Location

Figure 7: Client Inference Problem Resolution

- Site specific Inference based troubleshooting

  The focus of CloudVision Wi-Fi's inference tools can be expanded from individual devices, to AP, and site level views, to address issues impacting user groups or workloads. The inference robot can be trained to an AP, floor or location to help assess problems that may be common to users, applications or a site. Power settings, channelization, interference and infrastructure deployment are among the factors evaluated for remediation recommendations.

- Client and Infrastructure Location Services

  A properly instrumented Wi-Fi infrastructure offers both administrators and clients the ability to locate assets and resources in the cognitive campus network. Arista wireless platforms utilize Wi-Fi and BLE technologies to locate and facilitate mapping of client and infrastructure devices in the campus. CloudVision Wi-Fi discovers and facilitates placement of devices in the mapped campus. Administrators can refine their view of the cognitive Wi-Fi network using a variety of filters/views aimed to identify:

  › Slow or intermittent clients

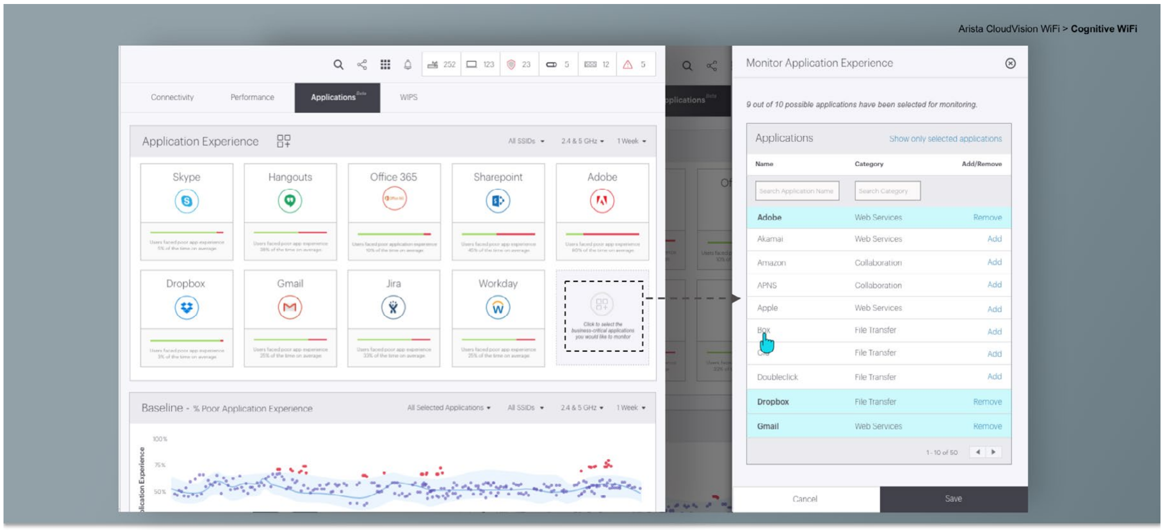
  › Clients exhibiting weak signals, high error or retry rates

  › Clients not meeting Quality of Experience (QoE) expectations for key applications.

  › Clients that are failing to connect.

  › Expanded applications monitoring for user Quality of Experience

  › CloudVision Wi-Fi can now monitor collaboration tools like Microsoft teams and Zoom, in addition to Webex, Skype, GotoMeeting and hangouts. With this expanded capability, administrators can ensure the productivity of users' collaborative applications



Users faced poor app experience 5% of the time on average

Users faced poor app experience 38% of the time on average

Users faced poor application experience 10% of the time on average

Users faced poor app experience 45% of the time on average

Users faced poor app experience 80% of the time on average

Users faced poor app experience 3% of the time on average

Users faced poor app experience 25% of the time on average

Users faced poor app experience 33% of the time on average

Users faced poor app experience 25% of the time on average

Click to select the business-critical applications you would like to monitor

Monitor Application Experience

9 out of 10 possible applications have been selected for monitoring.

Applications — Show only selected applications

Name	Category	Add/Remove
Search Application Name	Search Category	
Adobe	Web Services	Remove
Akamai	Web Services	Add
Amazon	Collaboration	Add
APNS	Collaboration	Add
Apple	Web Services	Add
Box	File Transfer	Add
Cis	File Transfer	Add
Doubleclick	File Transfer	Add
Dropbox	File Transfer	Remove
Gmail	Web Services	Remove

1 - 10 of 50

Cancel Save

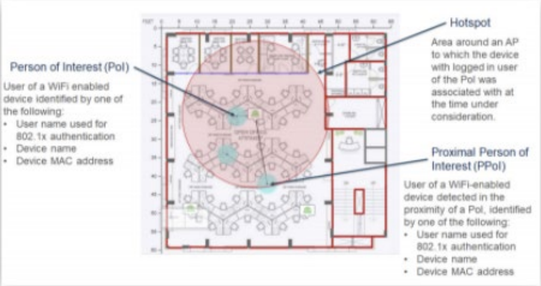
Figure 8: Application Quality of Experience for Business Critical Applications

Finally, Arista leverages Wi-Fi location services to provide enhanced location capabilities to help organizations cope with workforce location monitoring requirements.

Client Location Monitoring

Arista's Cognitive Wi-Fi Management plane collects a multitude of real time client telemetry used to improve and ensure user and application Quality of Experience. CloudVision's inference engines sifts through the accumulated database of RF signal data, mac addresses, machine names, connection times and durations, roaming states, 802.1X authentication and a myriad of other Layer-2 through Layer-4 network data to provide context relevant troubleshooting assistance and KPI trend reporting that's helpful to NetOps administrators.

CloudVision Wi-Fi is now leveraging this rich real time data with a new feature called P-tracer. P-Tracer runs Wi-Fi telemetry through a policy engine to physically track clients connected to any CloudVision Wi-Fi managed access point. P-Tracer identifies AP's where connection densities exceed pre-defined thresholds. Moreover, P-Tracer provides the time of stay duration per AP's. While P-Tracer's information can be leveraged for a variety of location services, it can also help organizations develop reporting for tracking essential workers in the enterprise. P-Tracer helps enterprises measure compliance with social distancing protocols and enables them to provide mandated contact tracing reporting to health agencies.



Person of Interest (PoI)

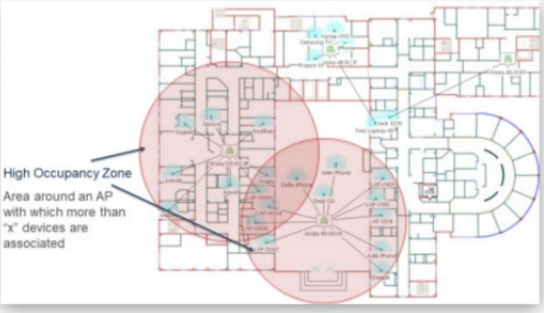
User of a WiFi enabled device identified by one of the following:
- User name used for 802.1x authentication
- Device name
- Device MAC address

Hotspot

Area around an AP to which the device with logged in user of the PoI was associated with at the time under consideration.

Proximal Person of Interest (PPoI)

User of a WiFi-enabled device detected in the proximity of a PoI, identified by one of the following:
- User name used for 802.1x authentication
- Device name
- Device MAC address



High Occupancy Zone

Area around an AP with which more than "x" devices are associated

- Wi-Fi Tracers:
  - › Wireless Intrusion Prevention System to protect against rogue devices
  - › Application and Internet reachability tools to diagnose connectivity problems
  - › Wi-Fi airwave health scanning tools that don't compromise Wi-Fi resources
  - › Extended testing and troubleshooting incorporating guest and BYOD web portals
- CloudVision Wi-Fi's connection troubleshooting dashboard now has enhancements to diagnose typical problems with web provisioning portals. Portal accessibility and functionality are new additions to the client journey suite of diagnostic tools, extending analysis from the airwaves to association, registration, network services and finally quality of Wi-Fi experience.

Utilizing the comprehensive telemetry derived from the Cognitive Management Plane, Arista's CloudVision Wi-Fi tools streamlines and automates provisioning, securing, troubleshooting and ensuring client Quality of Experience throughout all segments of the distributed campus enterprise.

4. Cognitive Arista EOS

Arista EOS provides a common software foundation for the cognitive campus network. The transformational Extensible Operating System (EOS) brings its baseline advantages to the campus with cloud grade control, monitoring, virtualization, scale and reliability. Arista's unique self-healing architecture isolates software defects, supports live patching and redefines hitless upgrade and rollback.The same binary EOS image is used across Arista's entire product line: from campus to cloud. Doing so ensures that EOS quality and reliability is consistently validated across the thousands of Arista customer data center, cloud and campus networks.

Open standard APIs in EOS support industry leading DevOps, monitoring solutions. Core to Arista's EOS architecture is NetDB: the network-wide, state-driven, publish-subscribe-notify database. Unlike legacy polling or inter-processor communication (IPC) schemes, NetDB is purpose-built to share all state in real time. Streaming of real-time data is complete and efficient, communicating thousands of state changes at sub-second intervals to monitoring platforms using open JSON over HTTP. Implementing dynamic JSON dictionaries means NetDB can dynamically evolve, sharing new, additional key/value information to monitoring tools.

5. Cognitive Management Plane

There is a striking contrast between the maturity and robustness that has evolved in networking data and control planes, and the lack thereof in the corresponding management plane. Arista's CloudVision incorporates our cornerstone Cognitive Management Plane (CMP) to automate deployments, simplify infrastructure, user and application monitoring, anticipate errors, and avoid outages across all Arista platforms in real time. CloudVision harnesses the capabilities of cloud computing, big data, and machine learning, collecting and archiving all network state over time.

CloudVision's Cognitive Management Plane ingests all streaming state from all EOS campus, cloud and data center platforms, while its open APIs allow data sharing with CloudVision and other applications, either custom developed or from third parties. This allows administrators the flexibility to use best-of-breed tools for data-driven actions and analysis. The Cognitive Management Plane's API conveys commands as well as telemetry data, allowing configuration management tools to control the campus infrastructure. Together with NetDB's schema and native OpenConfig APIs, Arista's CMP fulfills customer's requirements for standards, openness and flexibility with flexible management and actions as depicted in Figure 9.

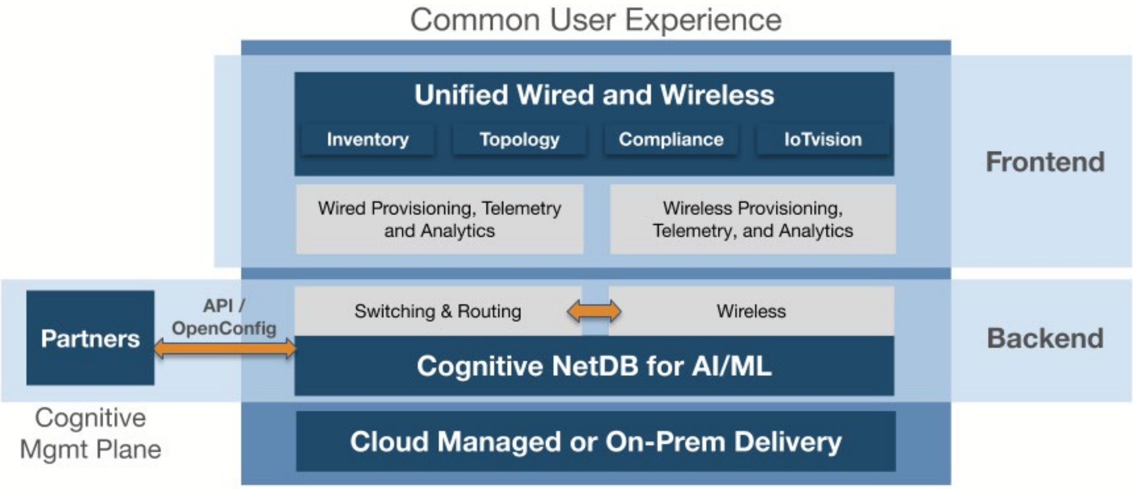
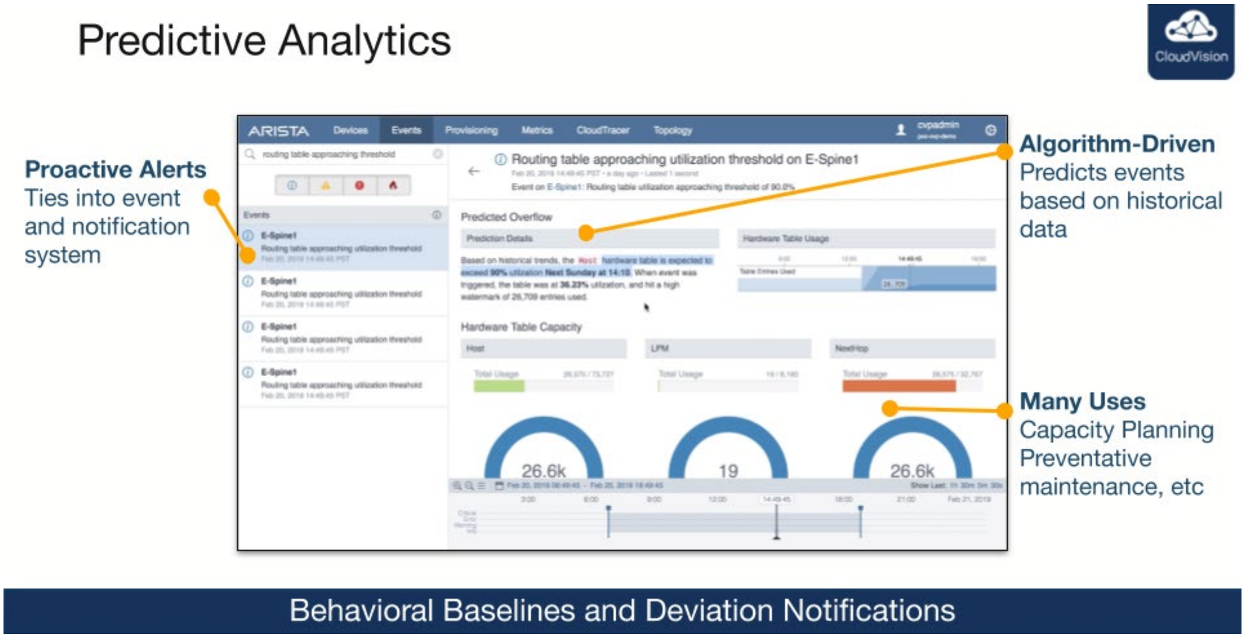

Common User Experience
Unified Wired and Wireless
Inventory
Topology
Compliance
IoTvision
Wired Provisioning, Telemetry and Analytics
Wireless Provisioning, Telemetry, and Analytics
Frontend
Partners
API / OpenConfig
Switching & Routing
Wireless
Cognitive NetDB for AI/ML
Backend
Cognitive Mgmt Plane
Cloud Managed or On-Prem Delivery

Figure 9: Cognitive Management Plane, a repository to drive network analysis and actions

The Cognitive Management Plane supports a growing list of analytics options. Based on real-time state streaming (NetDB) and open source tools including Hbase and Kafka, these streaming processors, called turbines, simplify, timestamp and correlate streaming state. Turbines help visualization and other machine processes better identify and make network-state actionable. Turbines that monitor software compliance, resource utilization and FRU health, not only track parameters for signs of degradation, they anticipate and alert operators of expected failure points, and support behavioral network actions that help network operators improve overall reliability.



Predictive Analytics

Proactive Alerts
Ties into event and notification system

Algorithm-Driven
Predicts events based on historical data

Many Uses
Capacity Planning
Preventative maintenance, etc

Routing table approaching utilization threshold on E-Spine1

Event on E-Spine1: Routing table utilization approaching threshold of 90.0%

Predicted Overflow

Prediction Details

Based on historical trends, the Host hardware table is expected to exceed 90% utilization Next Sunday at 14:10. When event was triggered, the table was at 36.23% utilization, and hit a high watermark of 26,709 entries used.

Hardware Table Capacity

Behavioral Baselines and Deviation Notifications

Figure 10: AI/ML Predictive Alerting

Arista's CMP also collects rich telemetry of IoT appliance, user, and application state through standard IPFIX and accelerated SFlow streaming. This real time data opens new use cases for administrators including:

- Identifying and inventorying campus devices, users and applications
- Monitoring key application and IoT SLAs, such as VoIP or security camera applications
- Identifying critical workflows and segmenting the network to protect them
- Automatically capture device or user rogue behavior and quarantine them

Pervasive Analytics in the Campus

Some workforce environments require complete and thorough data capture of network traffic to comply with organizational or regulatory requirements. Arista's DANZ Monitoring Fabric (DMF) analytics nodes deliver a scalable solution for collecting and analyzing standard data streams including Netflow (V5 and 9), sFlow and IPFIX.

DANZ Monitoring Fabric

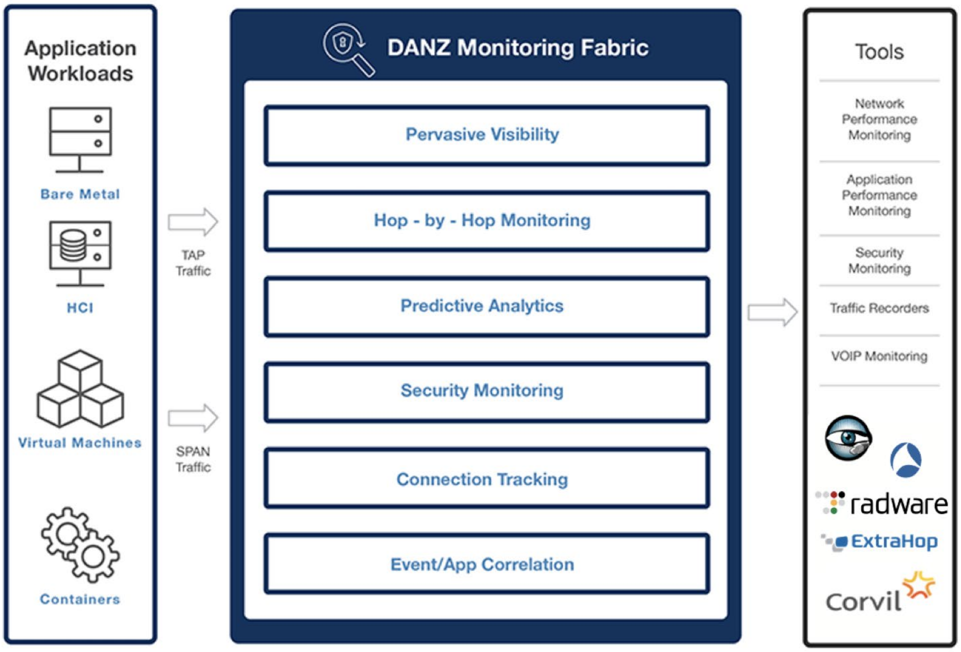


Figure 11: Architecture for Predictive, App-Aware, Pervasive Analytics

DMF analytics nodes can scale to meet the telemetry requirements of any sized enterprise. Providing forensic analytics and machine learning capabilities, the DMF analytics platform fulfills requirements for network data aggregation, archival and analytics. DMF analytics is part of Arista's comprehensive traffic acquisition, packet brokering, archival and processing solution for enterprise network analytics. InfoSec officers can additionally use DMF service and recorder nodes as a core of their zero trust security architecture: sampling or mirroring critical traffic flows to the tool farm for real time or forensic traffic analysis.

AI Driven Threat Detection and Response: Awake

The explosive proliferation of client and IoT devices in the enterprise correlates to an increased and often unmonitored attack surface and the corresponding risks of malicious attacks. Infosec managers have no other option but to leverage AI/ML systems that can aggregate enterprise scale data flows and constantly hunt for traffic patterns that signal a data probe or ransomware attack.

The Awake Security Platform, Arista's newest security investment, is the only advanced network detection and response solution that provides the SecOp team with answers, rather than alerts that lack context. By combining artificial intelligence with human expertise, Awake autonomously models and hunts for both insider and external attacker behaviors while providing triage, digital forensics, and incident response support across the distributed enterprise network.

The Awake Security Platform deeply analyzes billions of network sessions to autonomously discover, profile and classify every device, user and application across any network. Using a multi-dimensional machine learning approach, Awake then models complex adversarial behaviors and connects the dots across entities, time, protocols and attack stages. Unlike legacy network detection and response tools that rely primarily on unsupervised learning to spot anomalies from "normal" baselines, Awake compares entity behaviors to the peer group and the rest of the organization. This enables the platform to deliver threat detections with low false positives and negatives, and additionally provides the context and decision support data necessary for triage, incident response and remediation. Independent testing proves out these differentiators and shows Awake is more than twice as accurate and produces almost 1500% less operational overhead than other NDR systems.

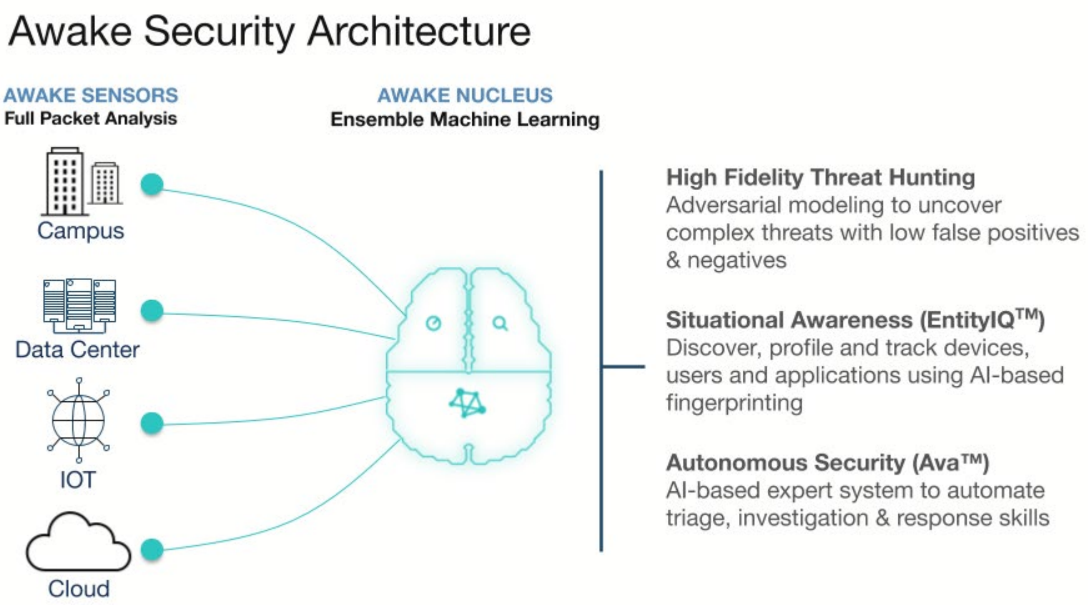

Awake Security Architecture
AWAKE SENSORS
Full Packet Analysis
AWAKE NUCLEUS
Ensemble Machine Learning
Campus
Data Center
IOT
Cloud
High Fidelity Threat Hunting
Adversarial modeling to uncover complex threats with low false positives & negatives
Situational Awareness (EntityIQ™)
Discover, profile and track devices, users and applications using AI-based fingerprinting
Autonomous Security (Ava™)
AI-based expert system to automate triage, investigation & response skills

Figure 12: Ensemble Machine Learning for Threat Hunting, Awareness and Response

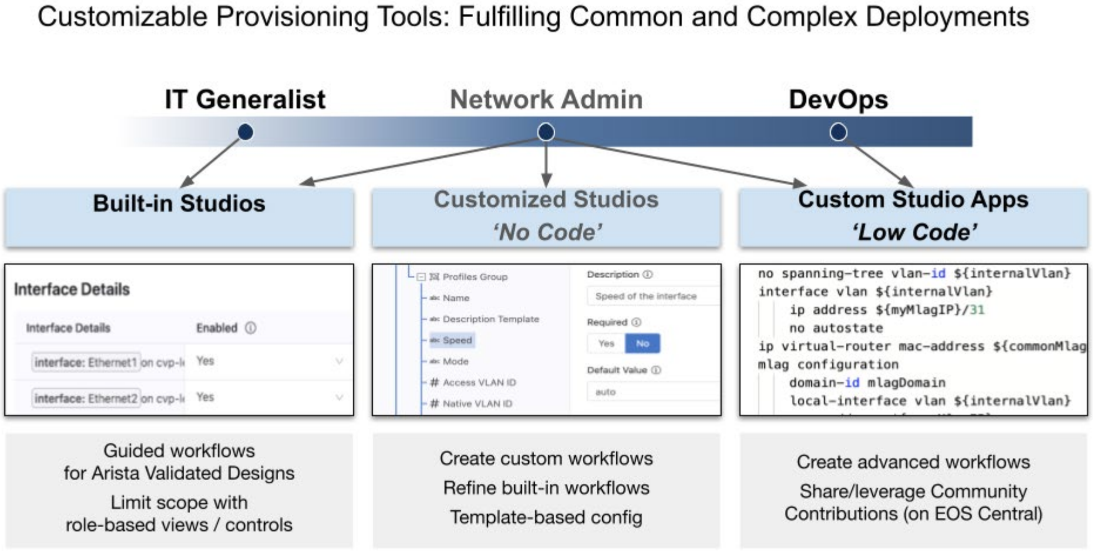
Awake monitoring sensors consume mirrored packets from either the DMF monitoring fabric or directly from infrastructure devices. Awake Sensors are deployed locally ensuring that sensitive data does not leave your network. Sensors send summarized metadata to the Awake Nucleus which can be deployed on premises or in the Awake cloud. The Awake Nucleus leverages Awake's EntityIQ technology to build a graph of network connected devices and their networked relationship.

EntityIQ does this by analyzing device communications, leveraging AI to glean devices from traffic flow data. Awake leverages EntityIQ to Analyze all devices through Adversarial modeling. Awake provides pre-configured adversarial models which can be customized by administrators through an easy to use AMI interface. Finally Awake's Ava expert system automates the investigation and remediation process.

Simple, Streamlined, Declarative Provisioning and Remediation with CloudVision

Most IT managers face the dilemma that while both budget and staffing for campus NetOps remains fixed, the campus network's importance, complexity, and size continues to grow. Compounding this problem is the scarcity of campus networking professionals in the field. For this reason, IT managers are looking at provisioning tools and automation systems to lighten and distribute campus networking workloads. However, most alternatives have been disappointing, requiring costly forklift upgrades.

On the other hand, Arista has worked with its customers to develop enhancements to its CloudVision management system that simplifies day 0 through day N provisioning workflows. Using a combination of scripting automation and declarative point a click provisioning, the new CloudVision Studios enhancement allows networking specialists to create declarative, point and click workflows for common tasks so that IT generalists can lend a hand in the daily maintenance of enterprise campus workspaces.



Customizable Provisioning Tools: Fulfilling Common and Complex Deployments

IT Generalist | Network Admin | DevOps

Built-in Studios

Customized Studios
'No Code'

Custom Studio Apps
'Low Code'

```
no spanning-tree vlan-id ${internalVlan}
interface vlan ${internalVlan}
    ip address ${myMlagIP}/31
    no autostate
ip virtual-router mac-address ${commonMlag
mlag configuration
    domain-id mlagDomain
    local-interface vlan ${internalVlan}
```

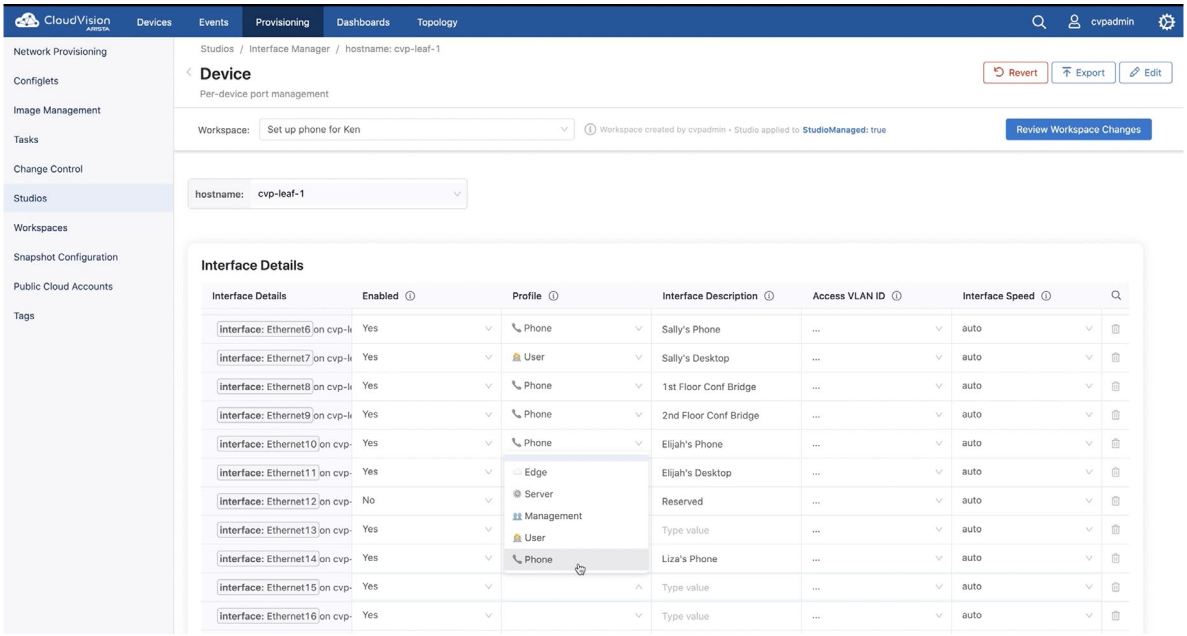
Guided workflows
for Arista Validated Designs
Limit scope with
role-based views / controls

Create custom workflows
Refine built-in workflows
Template-based config

Create advanced workflows
Share/leverage Community
Contributions (on EOS Central)

Figure 13: Standard Point and Click Provisioning Workflow

Networking specialists can deploy pre-built maintenance workflows, such as user, or ip phone port configurations, to the NetOps staff, allowing them to make small work of typical provisioning activities. CloudVision Studios provides a forms builder workspace that lets dev-ops and NetOps specialists customize existing workflows or create entirely new processes for use by the whole NetOps staff. These workflows integrate into CloudVision's existing change management system to ensure compliance to change management procedures while also leveraging CloudVision's automated remediation tools.



Device

Per-device port management

Workspace: Set up phone for Ken

Workspace created by cvpadmin • Studio applied to StudioManaged: true

hostname: cvp-leaf-1

Interface Details

Interface Details	Enabled	Profile	Interface Description	Access VLAN ID	Interface Speed
interface: Ethernet6 on cvp-l	Yes	Phone	Sally's Phone	...	auto
interface: Ethernet7 on cvp-l	Yes	User	Sally's Desktop	...	auto
interface: Ethernet8 on cvp-l	Yes	Phone	1st Floor Conf Bridge	...	auto
interface: Ethernet9 on cvp-l	Yes	Phone	2nd Floor Conf Bridge	...	auto
interface: Ethernet10 on cvp-	Yes	Phone	Elijah's Phone	...	auto
interface: Ethernet11 on cvp-	Yes		Elijah's Desktop	...	auto
interface: Ethernet12 on cvp-	No		Reserved	...	auto
interface: Ethernet13 on cvp-	Yes		Type value	...	auto
interface: Ethernet14 on cvp-	Yes		Liza's Phone	...	auto
interface: Ethernet15 on cvp-	Yes		Type value	...	auto
interface: Ethernet16 on cvp-	Yes		Type value	...	auto

Figure 14: Studios Declarative Provisioning Model

CloudVision Studios allows campus staff to codify the expertise of the enterprise's NetOps specialists, maintain and customize workflows using standard tools, and lastly, all the greater IT staff to utilize these workflows to streamline management of the enterprise net.

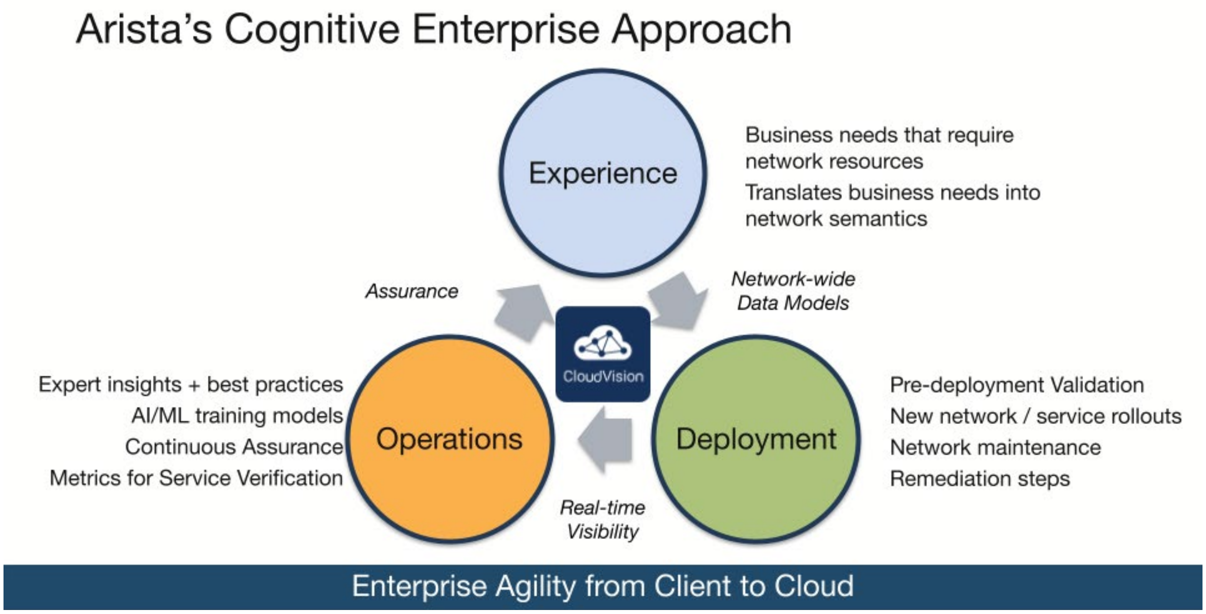

Arista's Cognitive Enterprise Approach
Experience
Business needs that require network resources
Translates business needs into network semantics
Assurance
Network-wide Data Models
CloudVision
Expert insights + best practices
AI/ML training models
Continuous Assurance
Metrics for Service Verification
Operations
Deployment
Pre-deployment Validation
New network / service rollouts
Network maintenance
Remediation steps
Real-time Visibility
Enterprise Agility from Client to Cloud

Figure 15: Extending and Ensuring Outcomes in Campus Workspaces

Cognitive NetDB for CloudVision

In addition to CloudVision's native capabilities, the platform's open architecture allows administrators to integrate expanded functions like threat detection and network access control services from a partner ecosystem of industry leaders and tech innovators.

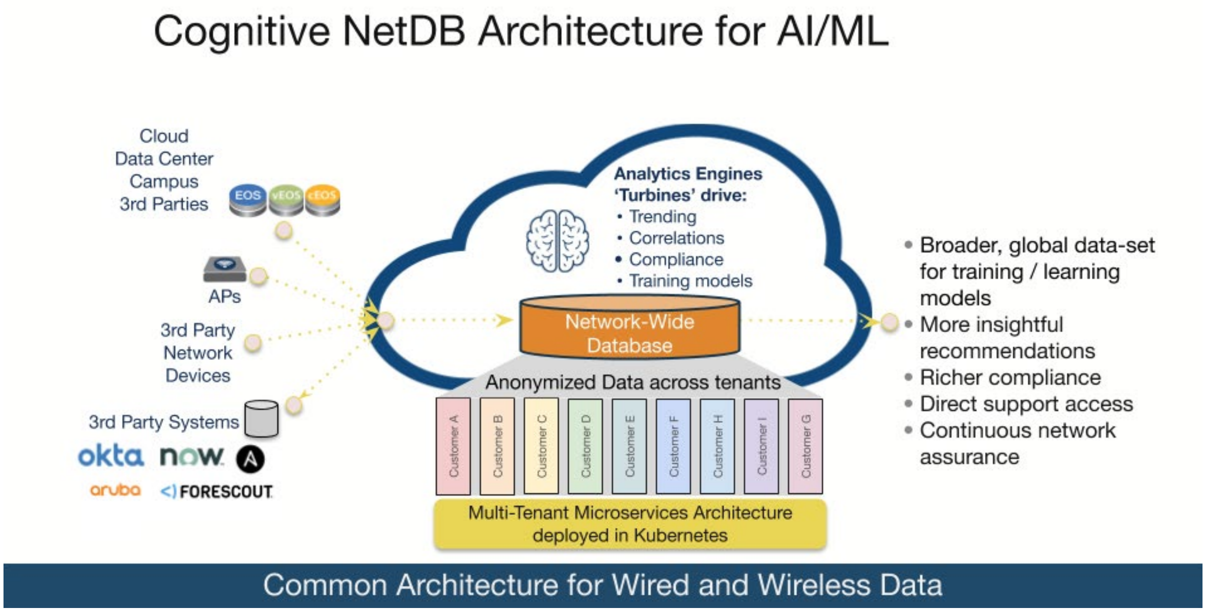

Cognitive NetDB Architecture for AI/ML
Cloud
Data Center
Campus
3rd Parties
EOS
vEOS
cEOS
APs
3rd Party Network Devices
3rd Party Systems
okta
now
aruba
FORESCOUT
Analytics Engines 'Turbines' drive:
• Trending
• Correlations
• Compliance
• Training models
Network-Wide Database
Anonymized Data across tenants
Customer A
Customer B
Customer C
Customer D
Customer E
Customer F
Customer H
Customer I
Customer G
Multi-Tenant Microservices Architecture deployed in Kubernetes
• Broader, global data-set for training / learning models
• More insightful recommendations
• Richer compliance
• Direct support access
• Continuous network assurance
Common Architecture for Wired and Wireless Data

Figure 16: Open Architecture Supports Best of Breed Solutions

Together with CloudVision's suite of configuration management, automation, monitoring and analytics tools, network administrators now have the means to simplify design, automate deployment, streamline monitoring of infrastructure and workloads, anticipate problems and avoid outages. CloudVision can be deployed on premises or as a cloud based service to better fit the organization's operational and budgeting requirements.

Key features of the powerful cognitive management plane include:

- Network view: Arista CloudVision fully supports all Arista products using streaming telemetry but can also ingest standard SNMP MIBs to facilitate data collection from legacy management planes. CloudVision Turbines catalog data in the Hadoop time series database and present actionable information in various device or topology views.
- State history: Operators can see all state of any device from any point in time. Historical visibility is a big help in debugging transient or intermittent issues.
- Machine learning: CMP supports machine learning algorithms to automatically identify alerts that are important for likely root causes of anomalous behavior.
- Multi-vendor scalability. Third parties can provide their own CMP and offer their unique benefits to customers. Multiple CMP clusters can be replicated and distributed to better serve organizational or geographic domains.
- Templatized provisioning with customizable configuration screens: CVP's extensive programmability allows administrators to tailor "day 0" provisioning and "day n" change management to the organization's unique workflow. Network architects can create custom provisioning workflows, leverage existing templates from Arista's Github library of tools, or commission bespoke workflows through Arista's EOS+ services team or its ecosystem partners.
- Configuration and image archiving with change control/automated bug remediation: CVP AI/ML turbines leverage archived configuration and image data sets with Arista's online bug database to correlate potentially impactful bugs against running configurations. CVP compliance manager then alerts administrators of vulnerabilities and suggests actionable remedies.
- In-service roll-out: Because the management plane is independent from the managed devices control plane, CloudVision can be maintained independent of the physical infrastructure. The management plane doesn't affect applications; hence, management plane upgrades are low risk, and new features can be deployed frequently.
- High availability: CMP clusters co-ingest state from the same set of devices, such that if a node in the cluster fails, the cluster continues to manage devices.
- Cross-cluster awareness: Through state export, an application can run in one cluster based on state in other clusters.
- Programmable extensibility: The Cognitive Management Plane (CMP) provides a rich set of telemetry APIs that allow users and Arista's partner ecosystem providers to extend CloudVision's capabilities or leverage CloudVision's Netdb to enhance third party applications.

Cognitive Campus: Client to Cloud Use Cases

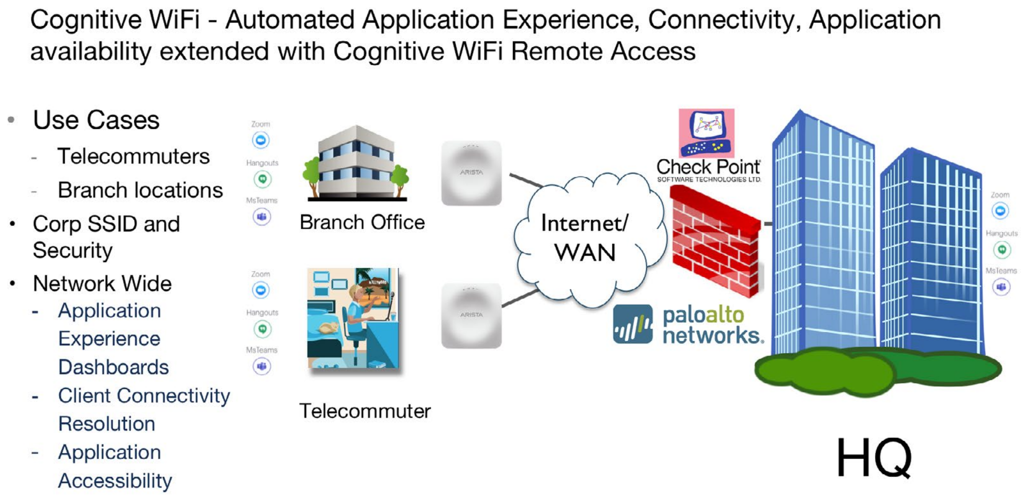
As campus networks transform to support the latest frontier, many examples and use cases are emerging:

- Monitoring the distributed campus workforce
- Flow tracking to pinpoint hotspots
- Improved security from audit to segmentation
- Enhanced client to cloud automation

Here are a few examples:

1. Connecting and Monitoring the Distributed Workforce

Wi-Fi access points support standard IPSEC tunneling features that allow remote workers to securely connect into the campus network and have complete access to enterprise resources. This gives workgroups, like customer service teams, secure and simplified access to critical CRM and knowledge based systems allowing them to work safely and remotely.



Cognitive WiFi - Automated Application Experience, Connectivity, Application availability extended with Cognitive WiFi Remote Access

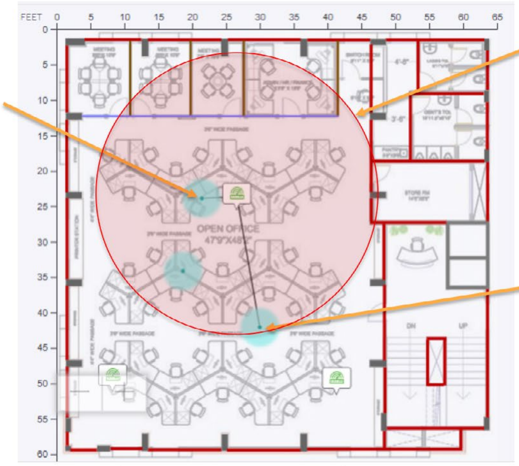
- Use Cases
  - Telecommuters
  - Branch locations
- Corp SSID and Security
- Network Wide
  - Application Experience Dashboards
  - Client Connectivity Resolution
  - Application Accessibility

Figure 17: Remote Connectivity Leveraging Existing VPN Concentrators

Arista's Zero Touch Provisioning (ZTP), simplifies deployments, letting administrators templatize configurations that include Wi-Fi and VPN security provisioning and credentials that are downloaded when the AP is connected to the internet. Provisioning is simplified and automatic: APs are shipped to the remote workforce who then plug and play.

Arista's innovative P-tracer leverages Wi-Fi telemetry collected by the Cognitive Management Plane to track movements of essential workers in campus offices as seen in Figure 18.

P-Tracer



Person of Interest (PoI)

User of a WiFi enabled device identified by one of the following:

- User name used for 802.1x authentication
- Device name
- Device MAC address

Hotspot

Area around an AP to which the device with logged in user of the PoI was associated with at the time under consideration.

Proximal Person of Interest (PPoI)

User of a WiFi-enabled device detected in the proximity of a PoI, identified by one of the following:

- User name used for 802.1x authentication
- Device name
- Device MAC address

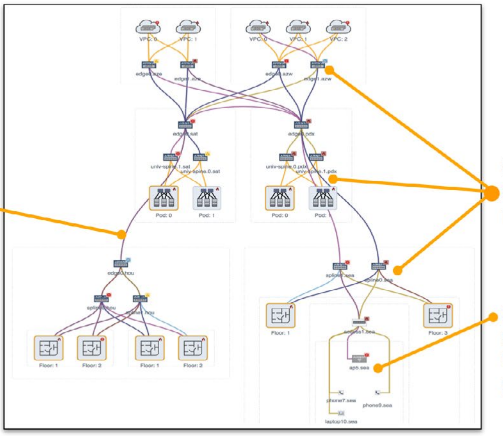
Figure 18: Essential Worker Tracking and Reporting

Worker location is saved in CloudVision's database to allow organizations to audit social distancing compliance and provide regulatory contact reporting if needed.

2. **Cognitive Use Case - Intelligent Monitoring**

Topology View: Client-to-Cloud Visibility

CloudVision



State Streaming-based
Modern, granular, complete. (No Polling - at all!)

Overlay Telemetry Views
Performance, Events, Segmentation and more

Starting Point…
For diving deeper into control, data, mgmt plane

Single Management View
Consolidation of DC + Campus + Cloud

Common Dashboard for Visibility
Wired and Wireless
3rd Party devices

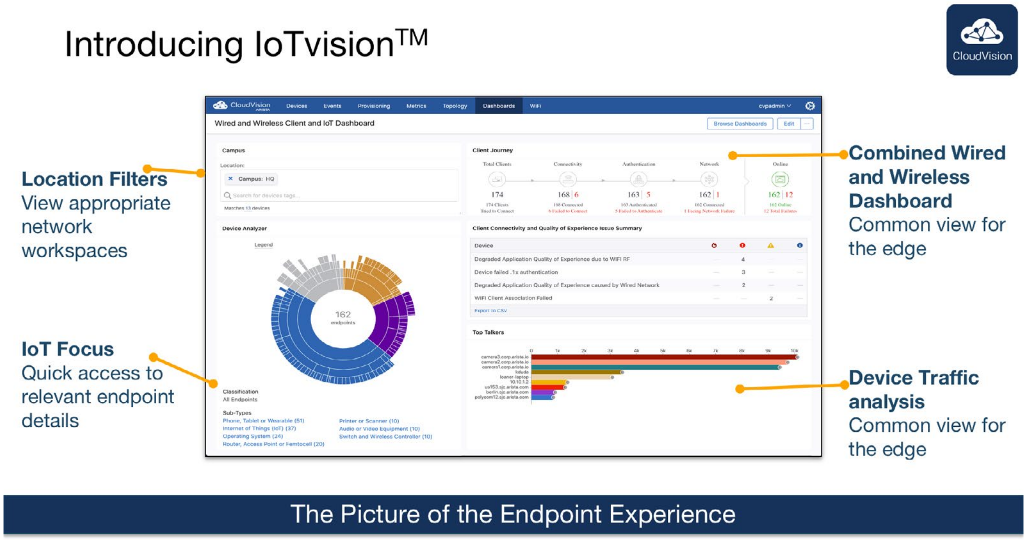
Improved Visibility by Breaking down Silos

Figure 19: CloudVision Telemetry Visualization from Client to Cloud

Campus LAN and Wi-Fi platforms deliver real-time user and IoT appliance flow tracking alongside real-time network state telemetry so administrators can monitor key performance indicators and maintain service levels in the cognitive campus network. Device Analyzer and IoTvision visualize port connections and correlate network, application and IoT/user flow data to identify and rectify performance or security issues. Administrators can use timestamped data to pinpoint and correct network hotspots before applications are adversely impacted or users even notice.

IoTvision: An evolution of CloudVision's device analyzer, IoTvision extends visibility, classification and monitoring to all networked IoT devices: wired or Wi-Fi. CloudVision's analytics turbines sift through flowtracker and SFlow session telemetry to identify, locate and correlate all kinds of appliances including sensors, security and monitoring devices, common office and other specialized appliances. IoT tracer's database functions let administrators catalog appliances using a variety of search criteria allowing administrators to locate devices, review their communications sessions, identify MAC/IP details and more signatures when possible.

IoTvision is a key asset for administrators who need to know the status and interaction of business critical user, security and environmental appliances.



Introducing IoTvision™

Location Filters View appropriate network workspaces

IoT Focus Quick access to relevant endpoint details

Combined Wired and Wireless Dashboard Common view for the edge

Device Traffic analysis Common view for the edge

The Picture of the Endpoint Experience

CloudVision
Wired and Wireless Client and IoT Dashboard
Campus
Client Journey
Device Analyzer
Client Connectivity and Quality of Experience Issue Summary
Top Talkers
162 endpoints

Figure 20: Expanding Monitoring and Visibility to Campus IoT Devices

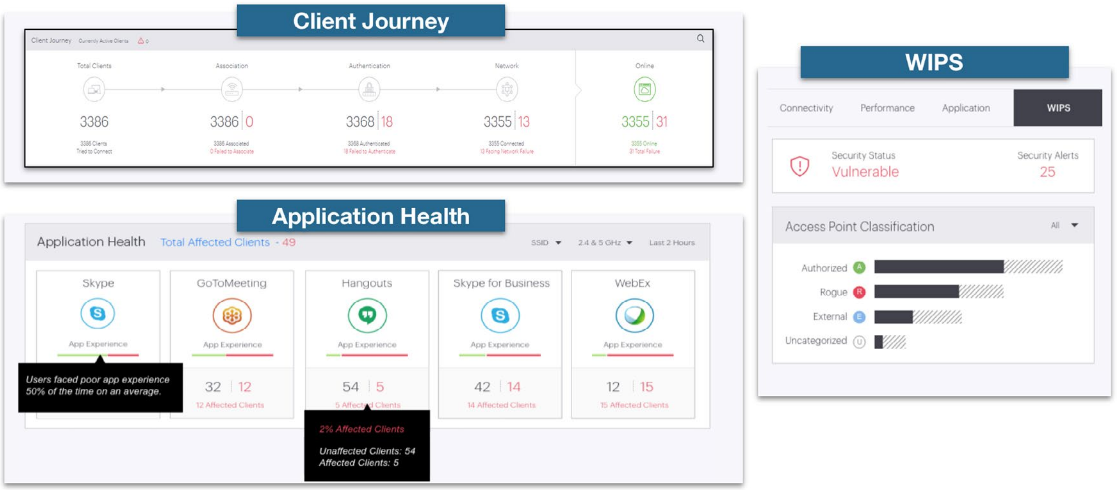
3. Cognitive Use Case - Comprehensive Campus Security: from Authentication to Segmentation to WIPS

Campus security officers are constantly balancing security requirements alongside worker productivity. Organizations' workflows also affect optimal security solutions. To optimize the balance of security and accessibility, campus administrators and infosec personnel must look for campus networking solutions that support a large ecosystem of segmentation partners that offer a variety of credential, single sign-on or IoT-centric behavioral authentication systems.

Unlike complex, proprietary segmentation schemes, open, standards-based 802.1q and VXLAN-based EVPN segmentation services can be combined to secure critical workloads or isolate suspect workflows across a campus-wide, multi-vendor environment. For outlier workflows, CloudVision provides traffic steering and segmentation capabilities in its Macro Segmentation Services (MSS) feature set or through Arista's ecosystem partners. The campus is dynamically configured to enforce security policy with no impact to other workloads. This simplifies campus network administration, and helps automate security enforcement using standard traffic segmentation technologies.

The ease of Wi-Fi accessibility poses a continuous security challenge to campus administrators. To ensure the security of the campus airwaves, cognitive Wi-Fi systems must automate security scans, provide constant coverage and produce actionable threat assessments. Arista's Cognitive Wireless Intrusion Protection Services (WIPS) provides a comprehensive architecture. Starting with dedicated scanning resources at the edge, telemetry is fed to Arista's Cognitive WIPs turbines which constantly log, process and synthesize performance and threat assessments to ensure the security and availability of the campus Wi-Fi.

Cognitive WiFi: Using AI for a Better User Experience



Client Journey

Client Journey Currently Active Clients △ 0

Total Clients	Association	Authentication	Network	Online
3386	3386 | 0	3368 | 18	3355 | 13	3355 | 31
3386 Clients Tried to Connect	3386 Associated 0 Failed to Associate	3368 Authenticated 18 Failed to Authenticate	3355 Connected 13 Facing Network Failure	3355 Online 31 Total Failure

Application Health

Application Health Total Affected Clients - 49 SSID ▾ 2.4 & 5 GHz ▾ Last 2 Hours

Skype	GoToMeeting	Hangouts	Skype for Business	WebEx
App Experience	App Experience	App Experience	App Experience	App Experience
	32 | 12	54 | 5	42 | 14	12 | 15
	12 Affected Clients	5 Affected Clients	14 Affected Clients	15 Affected Clients

Users faced poor app experience 50% of the time on an average.

2% Affected Clients

Unaffected Clients: 54
Affected Clients: 5

WIPS

Connectivity Performance Application WIPS

Security Status Vulnerable Security Alerts 25

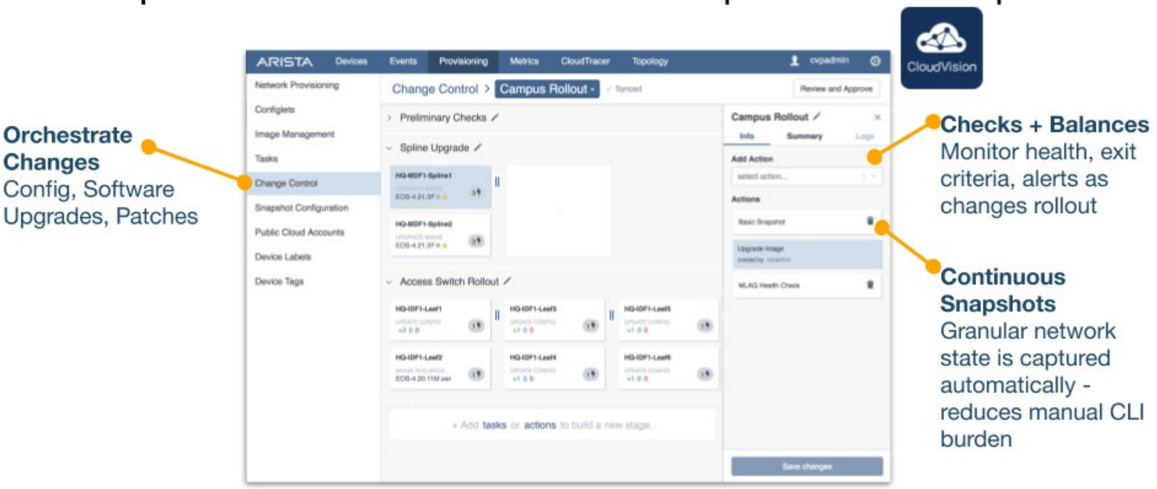
Access Point Classification All ▾

Figure 21: Key Attributes of Cognitive Wi-Fi Including Intrusion Detection/Prevention

In addition, the Awake Security Platform, when deployed, can provide ongoing security monitoring, detect threats and then respond through integrations with a variety of partners including endpoint security and firewall providers.

4. **Cognitive Use Case: Compliance, Audit Control, and Predictive Analytics**

Campus Use-case: Automated NetOps for the Campus



Orchestrate Changes
Config, Software Upgrades, Patches

Checks + Balances
Monitor health, exit criteria, alerts as changes rollout

Continuous Snapshots
Granular network state is captured automatically - reduces manual CLI burden

Maintenance windows from Weekends to Hours

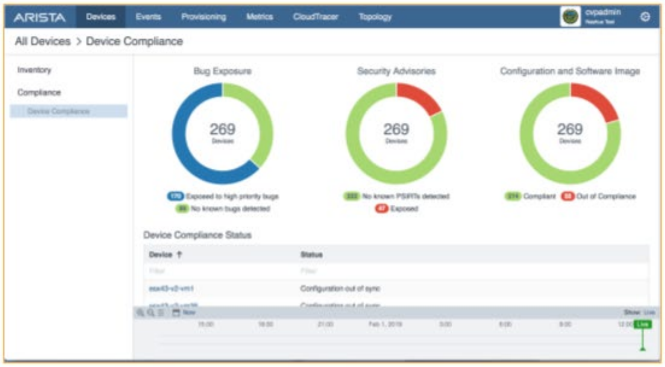
Figure 22: Compliance and Remediation Simplified and Automated

DevOps solutions have proven their worth in countless data centers for both server and network administration. When used to manage uniform software platforms, DevOps systems have a proven record of reducing errors while improving deployment time.

Yet even in DevOps, there are opportunities for data analytics to further reduce TCO. Databases of system configurations can be checked against bug databases to identify and warn administrators of possible vulnerabilities before they become outages. Cognitive compliance checking is better when configurations and operating systems are uniform and consistent, particularly in a sprawling campus. CloudVision's compliance dashboard helps perform cognitive audits.

Systems configurations and running OS images are compared against Arista's bug tracker database to identify possible compliance issues as depicted in Figure 20. This forewarns administrators of potential vulnerabilities and offers remediation options before a catastrophic incident. CloudVision's proactive visibility of pre- and post-differentials for VLANs, MAC or route metric adds additional and valuable audit control.

Compliance Dashboard



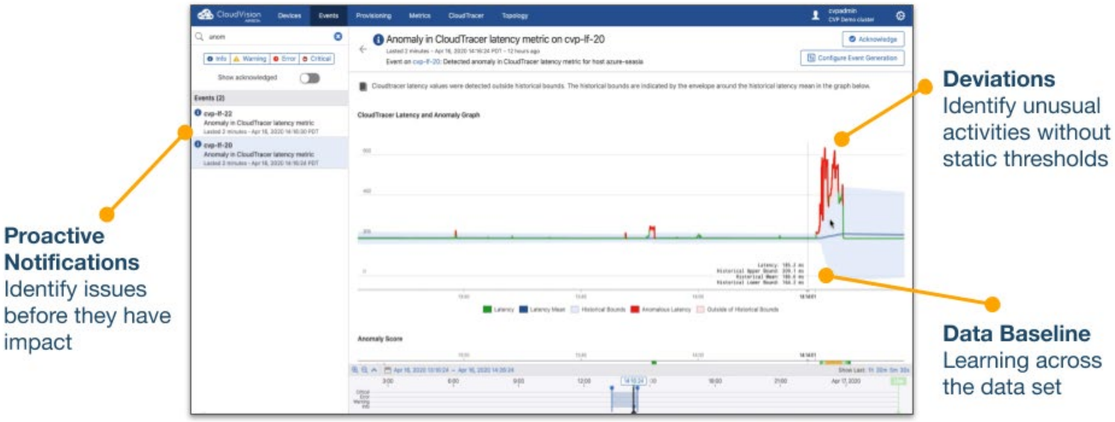
- Continuous checks for Config and Image drift
- Alerts for new Security Advisories and track scope of exposure
- Ongoing assessment of known bugs and potential impact to EOS estate
- Dashboard for aggregated view across entire inventory

Figure 23: Cognitive Checking Simplifies Compliance Decisions

Predictive Analytics:

The quality and actionability of all analytics systems are deeply dependent on the telemetry it consumes. That is why CloudVision's Event Monitoring can detect anomalies before they become failures and alert administrators of the need for corrective actions.

New in CV: Predictive Analytics with AI/ML



Proactive Notifications
Identify issues before they have impact

Deviations
Identify unusual activities without static thresholds

Data Baseline
Learning across the data set

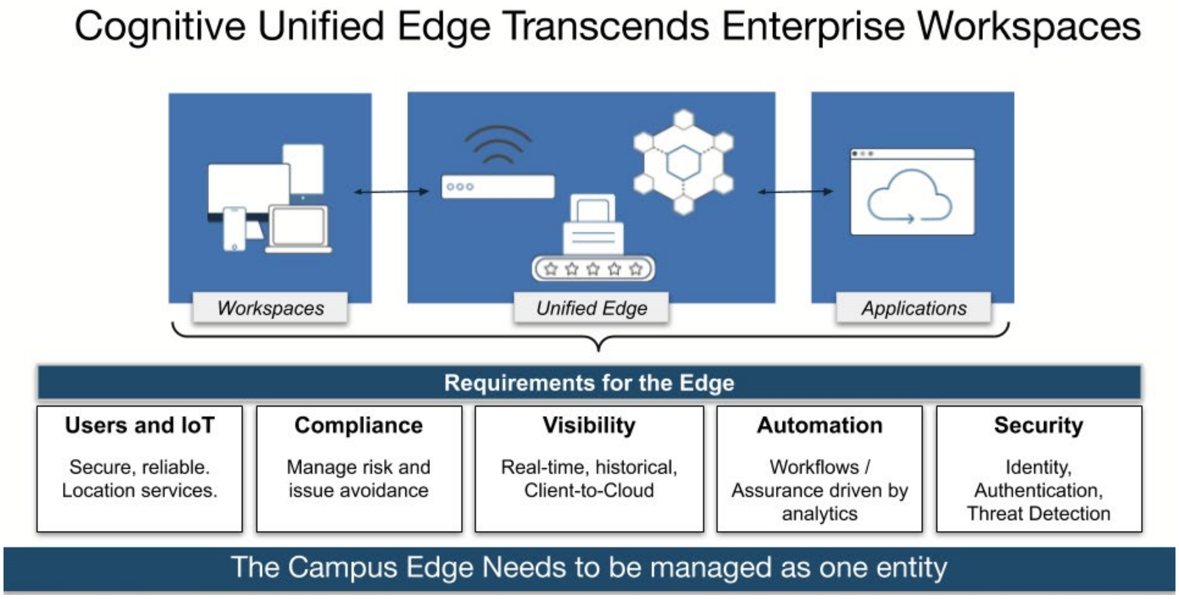
Figure 24: Real Time Telemetry Coupled With Analytics Helps Prevent Service Disruptions

The scope of CloudVision's predictive analytics is comprehensive since NetDB consumes all state within EOS. Real time telemetry improves both the analytic fidelity of AI/ML turbines and the timeliness of alarms generated. CVP provides webhooks and easy to use APIs so notifications can be passed to Network Operator's preferred alerting system.

5. **Cognitive Use Case: Zero Touch Provisioning (ZTP) in the Campus**

There is an ever-increasing frustration with the inconsistencies of legacy campus networks. Campus administrators struggle to manage user's traffic from computers and smartphones, and are additionally faced with mission critical IoT traffic from badge readers, security cameras and environmental controllers, just to name a few. The challenge of securing and protecting information is paramount, but extreme measures may degrade or outright break legitimate applications. Lastly, the complexities of maintaining heterogeneous legacy infrastructure can be its own full-time job as managers must certify discrete platform images for different parts of their multi-tiered network.

Extending cloud networking principles, Arista Cognitive Campus Architecture is designed to address users' and administrators' needs with automated end-to-end configuration builder and orchestration services that are consistent across the entire campus edge as shown in Figure 22 below.


Cognitive Unified Edge Transcends Enterprise Workspaces
Workspaces
Unified Edge
Applications
Requirements for the Edge

Users and IoT	Compliance	Visibility	Automation	Security
Secure, reliable. Location services.	Manage risk and issue avoidance	Real-time, historical, Client-to-Cloud	Workflows / Assurance driven by analytics	Identity, Authentication, Threat Detection

The Campus Edge Needs to be managed as one entity

Figure 25: Prudent Automation Steps From Client to Cloud.

Arista ZTP works in conjunction with CloudVision templates to rapidly on-board new infrastructure and clients, while simplifying QoS, user, guest and IoT segmentation policy across the enterprise Wi-Fi and Wired LAN. Provisioning templates and automation scripts help simplify the definition and deployment of the underlying fabric and overlay workgroup segments across distributed enterprise workspaces. Coupled with CloudVision's Integrated Wi-Fi and Wired LAN topology view, administrators enjoy rich visibility of the entire campus network to simplify troubleshooting.

CloudVision's unique compliance management tool is invaluable for mission critical deployments. It automatically pushes and validates segmentation configurations against the campus infrastructure, ensuring end-end dataplane consistency that can be leveraged by popular NAC solutions.

Solving Productivity Challenges in the Diffused Campus

The sea-change of new campus use cases stemming from social distancing requires thoughtful assessment throughout the enterprise. Increasing dependency on workforce collaboration and meeting tools, coupled with the need to distribute employees while investing in tools for tracking essential workers has dramatically increased the list of business critical applications requiring assurance. Designs must evolve from brittle complexity to uniform networking systems that can adapt to these evolutions while simultaneously lowering TCO. Arista's expanded campus platform portfolio, running its universal EOS and managed with CloudVision, leverages telemetry innovations of the Cognitive Management Plane to deliver the next level of performance, reliability, security and automation for the distributed workforce and network administrators.

The contrast between other's intent-based networking, implying hope or hype, versus Arista's pragmatic cognitive-driven actions, is clear. With Arista's cloud grade EOS, CVP and cognitive campus LAN and Wi-Fi platforms, network leaders and IT managers can implement an adaptive and cognitive campus architecture to ensure they can meet their current and future challenges.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office
1390 Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062