# Arista Cognitive Campus Network

Enterprises are adapting to new hybrid workspace paradigms as workforces demonstrate continued or improved productivity. At the same time, campus administrators are retooling for the revised security, support and collaboration challenges inherent in the diffuse workforce. Furthermore, campus IoT device deployments are exploding in the distributed workforce; increasing workforce productivity.

While price/performance improvements of campus switched LAN and Wi-Fi technologies remains an important criteria for infrastructure upgrades, there is a new emphasis on telemetry, automated provisioning, troubleshooting, and remediation that offload and streamline day to day management activities from burdened NetOp and SecOp teams. Additionally, there are requirements for declarative management that's workspace oriented, to allow a more diverse group of net admins, including front line workers, to realize point and click, zero-touch deployments and maintenance of campus and edge workspace networks.

When planning new deployments, network administrators look for standards-based solutions that leverage their infrastructure, applications, knowledge, and experience, to help reduce TCO. Key decision criteria include: reliability, ease of maintainability, and a simplified, comprehensive, administrative experience that streamlines deployments. Furthermore, administrators look for automation tools that deliver predictable, repeatable and successful outcomes in the management of their evolving network campus and edge workspaces.

Arista's Cognitive Campus delivers a comprehensive feature set needed to fulfill the networking challenges encountered in increasingly dispersed workspaces. As workers require constant access to their corporate and cloud resources, Arista's Cognitive Campus workspaces fulfills constant availability requirements, with hitless upgrading and patching, lossless failover, and proactive remediation of client connection issues. The Cognitive Management Plane (CMP) in EOS is the foundation for enhanced visibility, feeding its telemetry to Arista's comprehensive, data-driven architecture: The Network data Lake (NetDL). This dataset is used for provisioning, compliance and fault remediation. Arista's Cognitive Campus Architecture delivers the telemetry, analytics, automated provisioning, problem detection and compliance systems, and a broad ecosystem of third party solutions that ensures the cost effective and reliable operation of enterprise campus and edge workspaces.

## Extending Cloud Grade Principles to the Campus

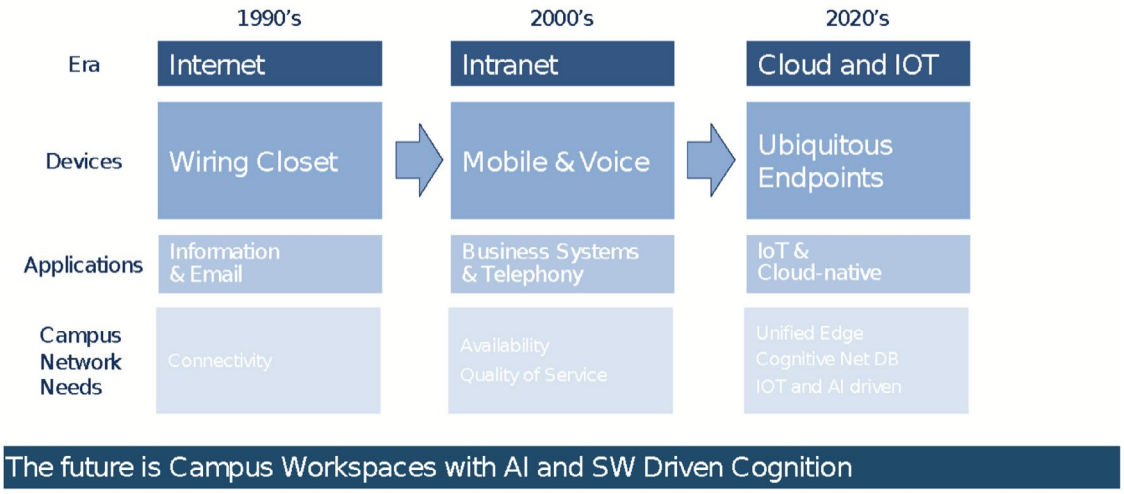



*Figure 1: Evolution of the Cognitive Campus Network*

Cloud computing economics continue to drive innovations in the provisioning, operation and monetization of enterprise networks. Many cloud grade principals have become best practices within data centers and are now being 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 common deployment and configuration tasks), rich real time telemetry for security mitigation, proactive remediation, location services, and specialized applications (e.g. location for asset tracking) for compliance to regulatory and other industry standards.

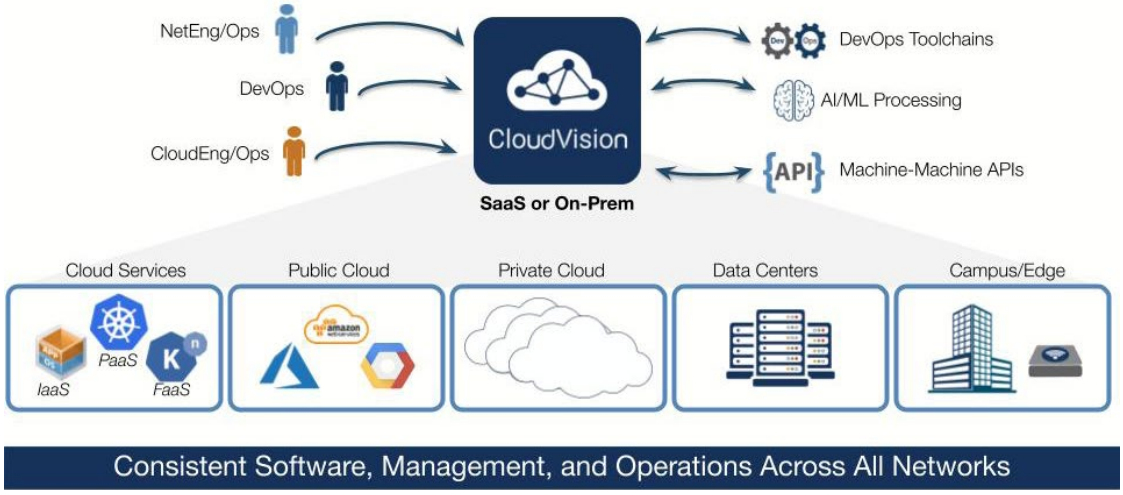



*Figure 2: Cognitive Universal Campus Edge Network*

The goal of the cognitive campus is to ensure the workforce remains productive while administrators adapt to hybrid workspace models; ensuring quality of experience and leveraging machine intelligence to streamline monitoring, troubleshooting, and compliance remediation. The cognitive campus builds on a reliable, consistent, cost-effective network that also supports scalability for small and large enterprises alike. It delivers quality and consistency to help administrators avoid the pitfalls of inefficient legacy architectures that are brittle, costly to deploy and maintain, and are plagued with disparate OS feature sets and management tools.

## Innovations in Campus Technologies

Campus architects shouldn't settle for table stakes services like VoIP, QoS, RADIUS, or 802.1X in hybrid workspaces. They should expect state of the art behavioral Network Access Control (NAC), SSO availability, and segmentation capabilities that improve the existing infrastructure. These authentication services should also serve workers wishing to leverage remote home/office use cases. Of equal consideration are embedded security options such as MACsec encryption and Wireless Intrusion Protection services (WIPs) that serve important roles for securing the campus edge. Finally, customizable telemetry and in-band network detection and response (NDR) sensors offer threat hunting and visibility across all appliances in campus workspaces, complementing today's security solutions.

The price, performance and operational benefits of new generation campus edge platforms should be open and standards based so it will work in brownfield environments and not require a proprietary, end-to-end, forklift refresh. New architectures should utilize wirespeed, cloud grade technologies 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.

Price and performance efficiencies can be obtained by collapsing legacy access-aggregation-core topologies to an elegant two tier campus leaf-spine or spline as shown in Figure 3.

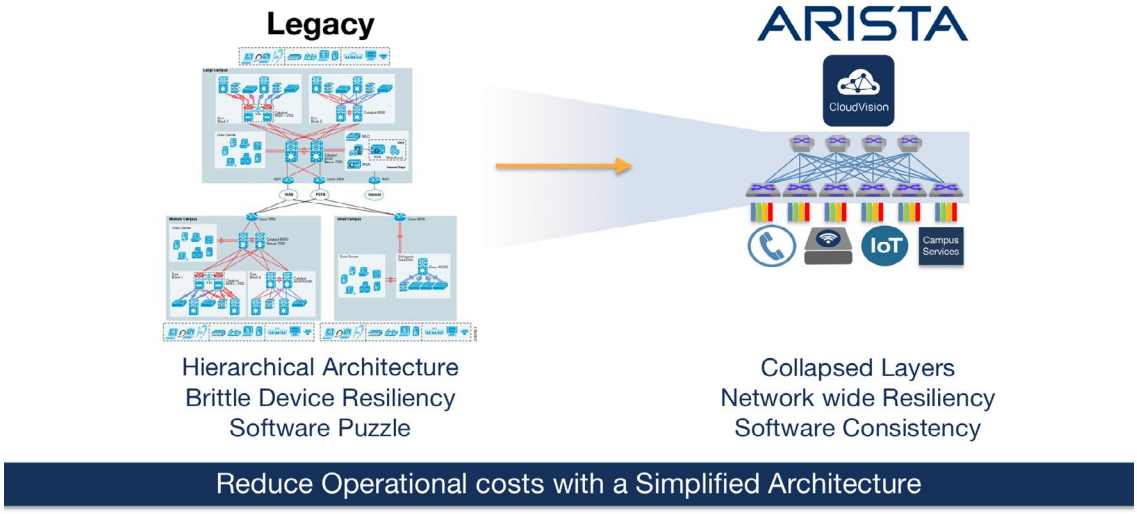
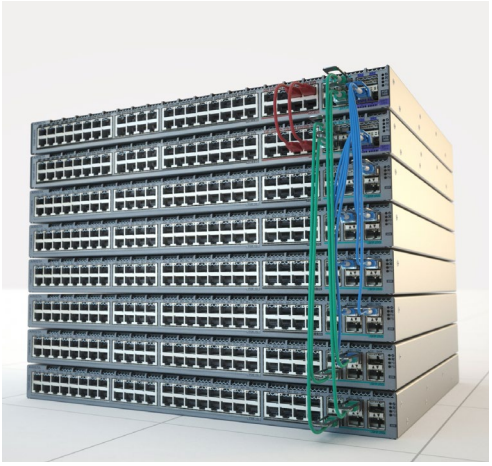



*Figure 3: Three Tiered Layers versus Single Tier Campus Leaf Spine or Spline™*

Collapsing the mid-tier aggregation and core layers reduces equipment count and costs while increasing reliability. Next generation, active-active, dynamically load sharing paths enhance spine to leaf bandwidth utilization, improving both performance and reliability. This removes the "reliability or performance" compromise of active-passive control plane architectures.

New cloud campus spine and leaf architectures enable hitless maintenance and advanced reliability features that prevent network degradation and failure. Finally, open L2, L3, virtual overlay, and segmentation 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.

### Reliability of Cognitive Wired PoE

Until recently, the only innovations one could point to in PoE systems came through increased power: moving from 15W 802.3af, to 30W 802.3at and the latest upgrades of up to 90W using type 4 802.3bt. Arista drove additional innovations to improve both the reliability and efficiency of wired and wireless systems. Following are the capabilities of Cognitive PoE:

**Continuous PoE**

Continuous PoE expands on reliable power distribution, not only in cases of FRU failure(power redundancy), but also in cases involving system patching and maintenance. Continuous PoE ensures power even when the system is rebooted or encounters any form of software issue. Administrators can also utilize port prioritization so campus switches can degrade gracefully in case of power starvation. Essential services, like badge readers, or security cameras would have priority over non-essential IP phones or similar non-critical devices.

**Concurrent PoE**

Concurrent PoE is designed for use cases where common power is required across all switched ports. Only the most power efficient switches coupled with high density power sources can fulfill this requirement.

**Dynamic PoE**

Dynamic PoE allows switches to measure the difference between the power requested and what is actually used. The excess unused power can therefore be reallocated to other devices thereby extending the switch's power budget and economy.

### Real-Time Telemetry for the Enterprise

Campus architects must also evaluate state of the art, real time monitoring services that can deliver more information, more efficiently. The symptomatic telemetry gaps of SNMP polling systems can't keep pace with the real time demands of workforce collaboration and conferencing apps. 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.

**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 |

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. These services should use standard publish/subscribe oriented APIs, like OpenConfig's gNMI/gRPC protocols, for flexibility. Campus networking systems must be able to glean and report on the thousands of user and application flows in the enterprise, detailing throughput, payload, latency and congestion, to name a few. Therefore, the telemetry services must be customizable with the ability to filter and capture well known, and to be defined, traffic types. Monitoring systems should thoughtfully present telemetry data in easy to use and customizable formats, allowing all levels of administrators to easily identify and troubleshoot service issues. Lastly, administrators should expect no compromise in reliability, performance or manageability.

### Wireless Mobility Services Improving Reliability, Scale, and Location

In the post pandemic era WiFi's ubiquitous mobility is a requirement. Workers' expectations of continuous connectivity can be foiled by radio integrity, resource overloading or system faults. Cognitive WiFi systems should monitor the workspace spectrum to discover, notify and even adjust radio configurations to ensure continuous access to the workforce. Dynamic resource management services should assist with day one provisioning and validation, yet be ready to cognitively reconfigure due to future environmental changes and service impacts.

WiFi's scaling potential also opens possibilities for private multi-tenancy use cases in enterprises. Similar to ad-hoc networks, Unique Pre-Shared Key (PSK) networks offer flexible virtual workspaces where users can collaborate privately, use resources personally, and segment themselves from other workers. Supporting private WiFi workspaces should be supported, leveraging industry standards alongside guest portal registration services that help provision and segment workgroups.

Locating mobile workers and business critical IoT assets is another natural extension of WiFi services. Various options exist for providing RF location services in the enterprise: WiFI based triangulation, Bluetooth Low Energy (BLE) beacons and various bespoke RF based systems. All provide location services and open APIs that support wayfinding, locating, footfall monitoring and asset tracking use cases, to name a few. What's most important is the WiFi architecture supports a large ecosystem of partner solutions so the workforce can pick best of breed options for their needs.

### Arista's Cognitive Campus Workspaces

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, wireless infrastructure and secure edge platforms, telemetry and analytics, and a single Image EOS that supports an ecosystem of solutions from industry leading partners as shown in Figure 4.

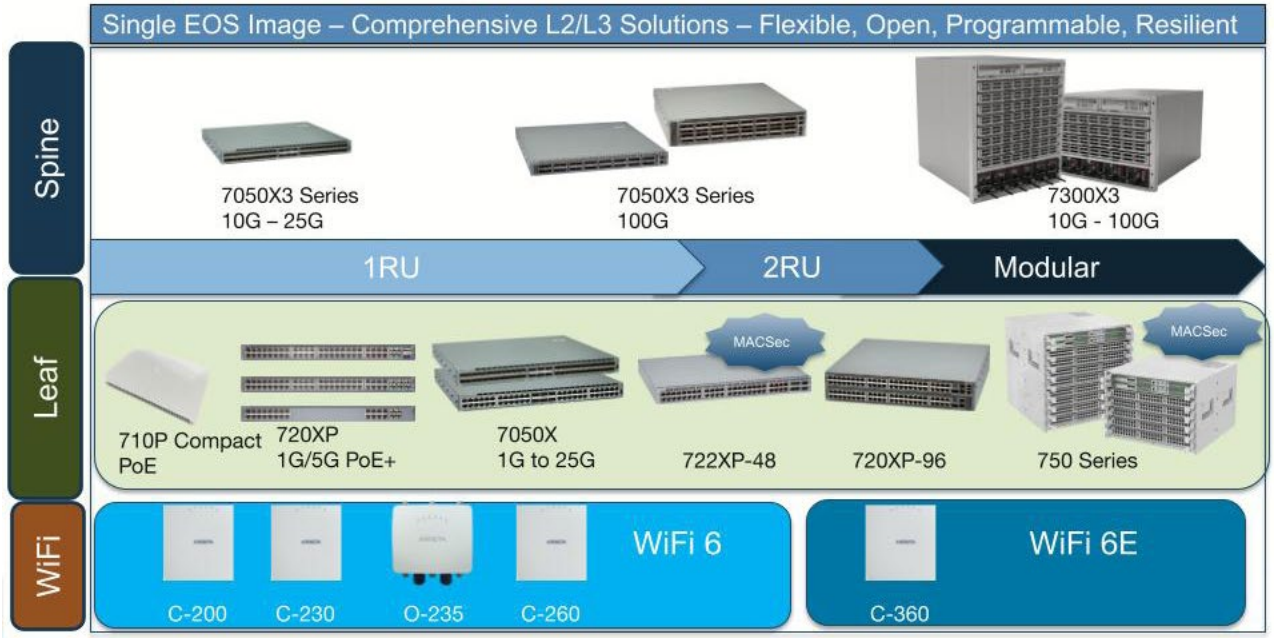



*Figure 4: Arista Cognitive Campus - Cognitive Wi-Fi, PoE leaf, threat management & Spline Platforms, EOS and Cognitive Unified Edge based on CloudVision*

### Edge as a Service for Smaller Enterprises: The Cognitive Unified Edge

Managing IT budget expenditures is business critical, however, smaller enterprises must consolidate; fulfilling multiple campus requirements with multi-tasking staff and dissimilar technologies. While designing and administering smaller enterprise nets may sometimes not be as technically difficult as those of larger enterprises, integrating networking services to deliver an optimal yet secure user experience is challenging.

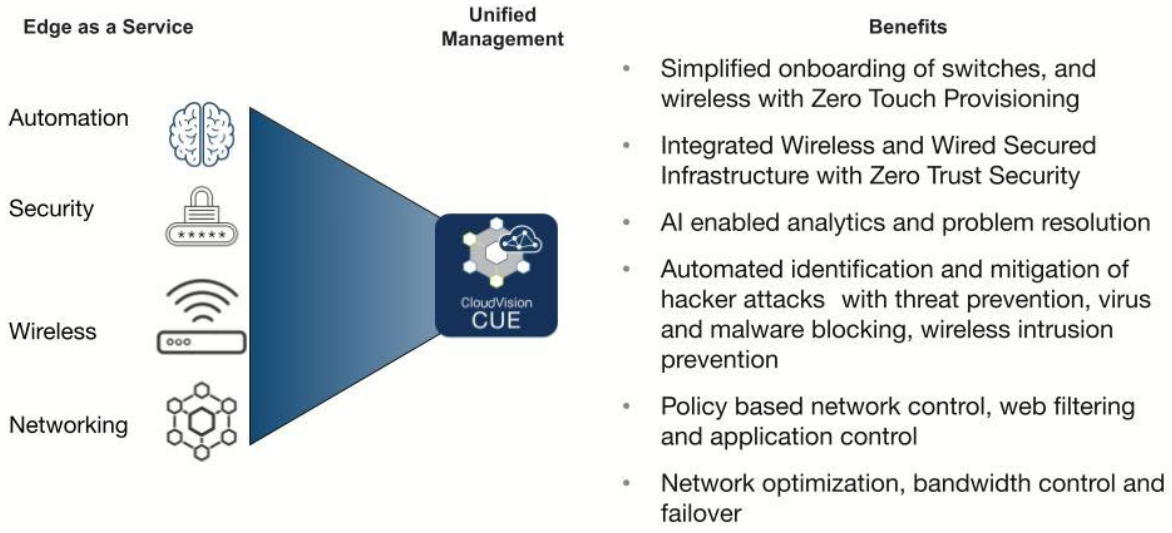



*Figure 5: Cognitive Unified Edge Management Architecture*

Arista's solution for providing a managed, cognitive unified edge for smaller enterprises is built upon its field-proven EOS, NetDL's comprehensive dataset and the automation and machine intelligence capabilities integral to CloudVision. This cloud-based management service uses streamlined user interface, built to facilitate declarative deployments of LAN, WiFi and edge security services, while retaining configuration and troubleshooting capabilities to accommodate most every contingency. CUE is an integral part of Arista's multi-modal CloudVision platform, giving customers seamless access to all the features and capabilities of Arista's extensive product portfolio to accommodate their evolving needs.

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 Wired Switches**

   Arista continues expanding its portfolio of cognitive, secure, high performance and high density PoE connectivity, 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. Cognitive 802.3af-t/bt power services deliver up to 90W, with speed options ranging from 10Mbps - 1Gbps, and 100M - 10Gbps (including MGig) over UTP, to support a variety of campus workloads. High speed SFP and QSFP uplinks support speeds from 1Gbps to 100Gbps which offer flexibility and scalability in network designs. All Arista campus platforms run Arista's common binary EOS, providing a comprehensive, open standard, layer 2, 3, and overlay feature set including MLAG, 802.1Q, EVPN/VXLAN virtualization, and

Macro-segmentation services, to name a few. 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, the 720XP, 722XP, and 750XP series share the same silicon architecture, and are designed to provide scale-up capacities with dynamic traffic load balancing, and real time flow monitoring of all campus workloads. 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 switching also provides real-time Flow tracker telemetry. Supporting CloudVision and flexible IPFIX APIs, Flow tracker allows administrators to capture an unlimited variety of key performance indicators and traffic flows in real time. Administrators can focus on infrastructure, device, application and user data for security, 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 6.

| | |
|---|---|
| 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 6: Key Attributes of Cognitive Campus Platforms*

Finally, Arista's campus portfolio accommodates a variety of layer 2 and 3 and overlay 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 networking processors in the 720XP/750XP series 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 720XP/750XP 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 802.1Q, EVPN and Arista's innovative MacroSegmentation services for Groups (MSS-G) with support from CloudVision. EVPN and MSS-G are friendly to brownfield infrastructures to support graceful additions or migrations. Finally, CloudVision can extend segmentation orchestration to data center and cloud based workloads.

### 3. Cognitive Unified Edge: (CUE) for WiFi

Arista's distributed data plane architecture for WiFi embeds manageability, telemetry and 802.1Q plus 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 AP-C360 series of 4X4 WiFi 6E capable APs, complements the 802.11ax C200 series APs, expanding networking capacity by utilizing the 6GHz band (where allowed). These 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, certain AP models offer optional third scanning radios for dedicated WIPs services, as well as BLE and Zigbee. Arista WiFi supports locationing solutions based on BLE, WiFi as well as custom solutions from partners like Aeroscout™.

As enterprises adapt to hybrid workspace deployments, 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 tunneling services, Arista Wi-Fi APs interoperate with leading VPN concentrator solutions to extend campus services under the enterprise's existing security infrastructure. CUE's Zero Touch Provisioning (ZTP) services simplify 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 CUE 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.

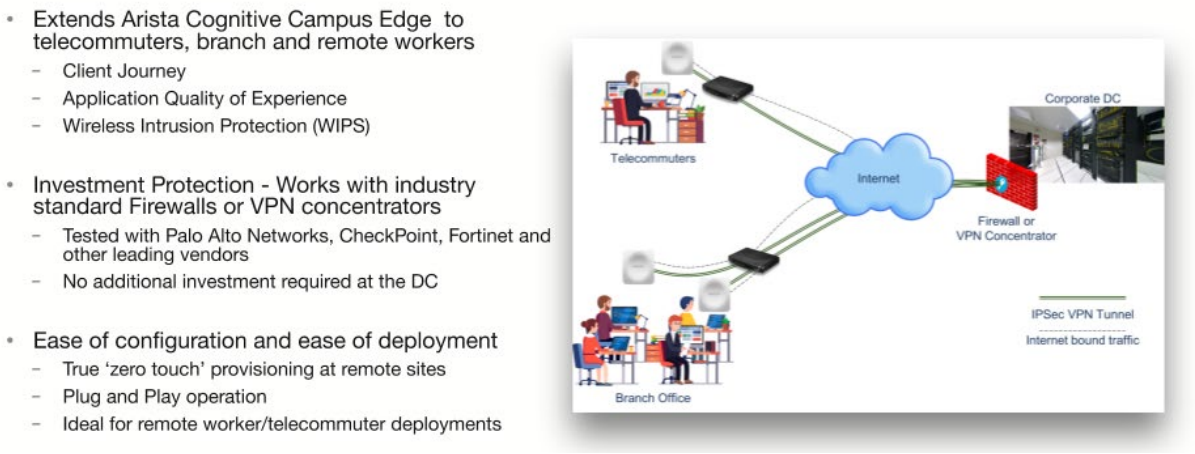



*Figure 7: Extending CUE across Distributed Campus Workspaces*

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

The CUE Wi-Fi manager, available as an on premise or in cloud service, helps optimize the workforce's quality of experience. CUE 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:
  CUE 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.

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

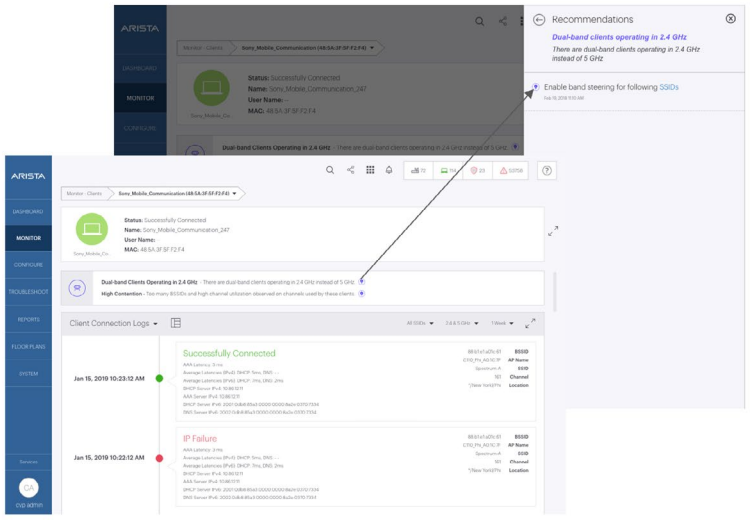



*Figure 8: Client Inference Problem Resolution*

- Site specific Inference based troubleshooting:
  The focus of CUE's inference tools can be expanded from individual devices, to AP, and site level views, to address issues impacting user groups or workloads. The Arista Virtual Assistant (AVA) AI 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. CUE 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
  - CUE 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

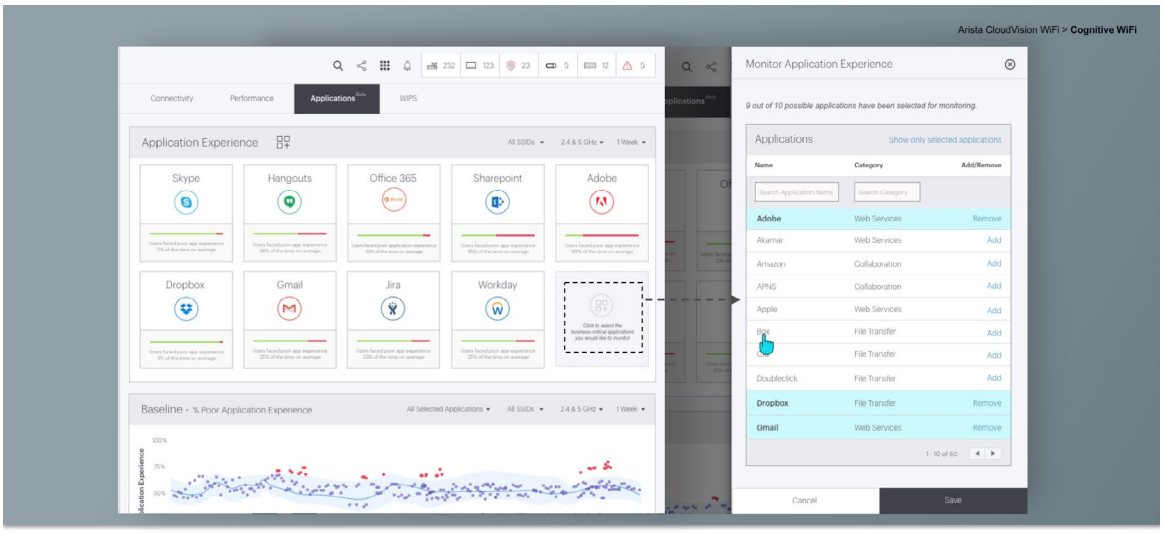
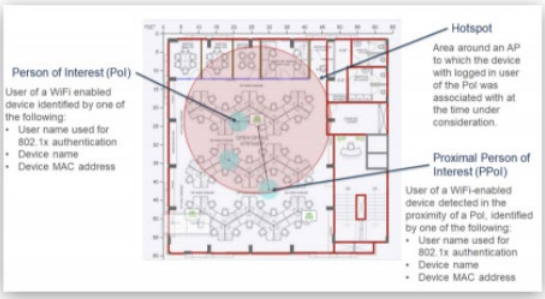


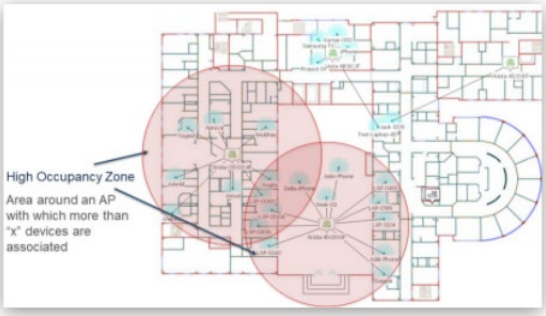

*Figure 9: Application Quality of Experience for Business Critical Applications*

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

### Client Location Monitoring

CUE collects a multitude of real-time client telemetry used to improve and ensure user and application Quality of Experience. CUE's AI 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.




CUE is now leveraging this rich, real time data, with a feature called P-tracer. P-Tracer runs Wi-Fi telemetry through a policy engine to physically track clients connected to any CUE 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. Finally, P-Tracer's information can be leveraged for a variety of location services, tracking key workers and assets to fulfill security and compliance needs.

- 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
- CUE'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.

CUE's tools streamlines and automates provisioning, securing, troubleshooting and ensuring client Quality of Experience throughout all workspaces in the distributed campus enterprise.

## 4. Cognitive Arista EOS

Arista's transformational Extensible Operating System (EOS) provides a common software foundation for the cognitive campus network. EOS brings all its 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.

Core to Arista's EOS architecture is the Cognitive Management Platform (CMP) that supports open standard configuration and monitoring APIs to support industry leading DevOps and monitoring solutions. Unlike legacy polling or inter-processor communication (IPC) schemes, The CMP is purpose-built to share all state in real time.

The CMP in Arista EOS, feeds Arista's Enterprise-wide Network DataLake or NetDL. NetDL provides a single source of network data 'truth' and a common sensor/collector architecture that enables forensics and analytics for threat hunting, network packet brokers, network detection and response, network performance monitoring, and application performance monitoring. By collaborating with a variety of industry leaders, Arista is able to deliver powerful production customer benefits. These data-driven network models can be transformed into insights that deliver actionable operational outcomes.

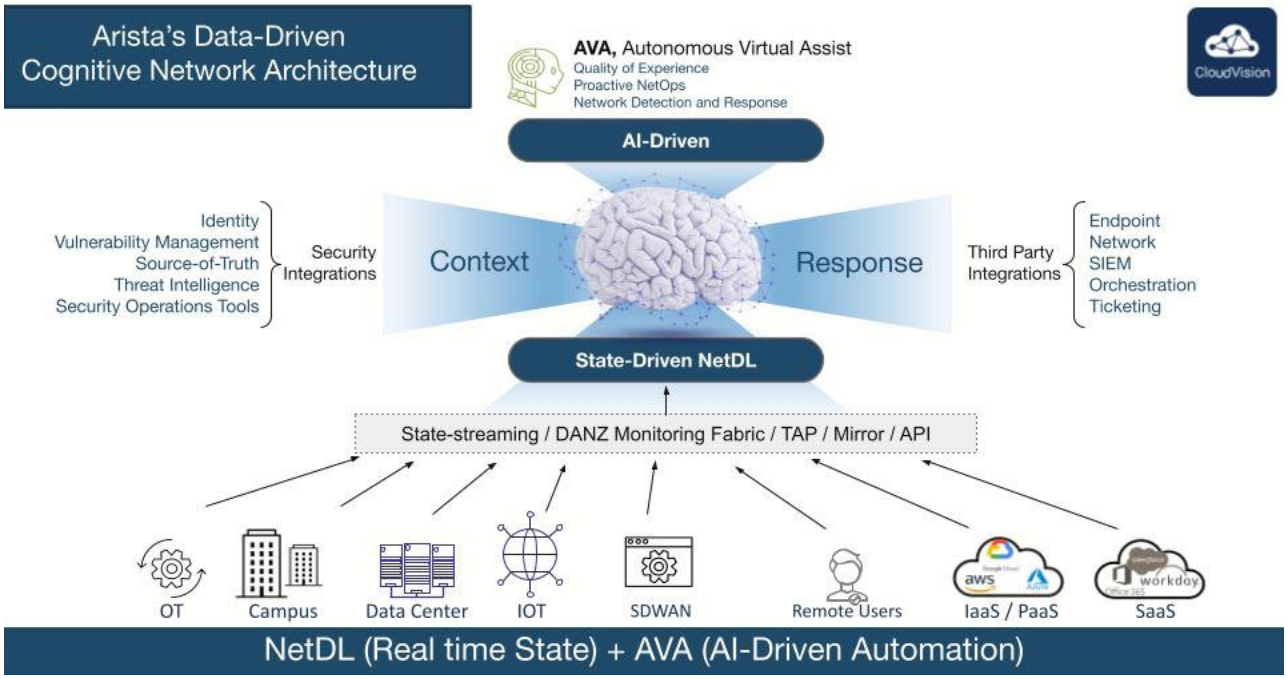



*Figure 10: Open Architecture Supports Best of Breed Solutions*

## 5. Cognitive Unified Edge (CUE) Arista's Management Architecture for Commercial Enterprise

While a common enterprise EOS coupled with NetDL's rich dataset offers administrators the foundation for automating provisioning, troubleshooting and remediation, the management platform must provide both flexibility and economy, fitting the needs, scaling and budget of the campus enterprise. For over eight years, Arista has been developing its CloudVision management architecture to fulfill use cases ranging from sophisticated data center overlay networks to small enterprise workspace deployments. The CloudVision platform (CVP) is deployable either on-premises, or as CloudVision as a Service (CVaaS). Enterprises can select whichever option that best suits their sys-admin, cloud budget and data privacy requirements. Finally, flexible subscription models for CVP and CVaaS help optimize the IT administration budget.

Mid-size and distributed branch enterprises have the additional challenge of leveraging their multi-functional staff to manage their workspace LAN, WiFi and secure edge network. To help reduce administrative load, the management solution must be easy to use and comprehensive, supporting declarative and assisted provisioning to ensure proper configuration of security and segmentation functions, to name a few. It must be easy to deploy: plug and play to lighten deployment workloads, coupled with cloud based services to eliminate management overhead.

Arista's Cognitive Unified Edge (CUE) as a service, builds upon Arista's Zero Touch Provisioning (ZTP) capabilities, Cloud Vision network as a service foundation, and embeds cognitive edge threat management capabilities to quickly deploy and manage secure edge networks in branch and smaller workspaces. "Edge As A service" integrates security, WiFi and LAN switch deployment as a streamlined automation and troubleshooting service. Leveraging Arista's total management architecture. CV CUE retains the troubleshooting and automation capabilities of CloudVision while allowing easy migration to CVaaS platforms for client-to-cloud networks. Arista's CUE, cloud scale reliability and TCO benefits is an important step for branch and mid-sized enterprises.

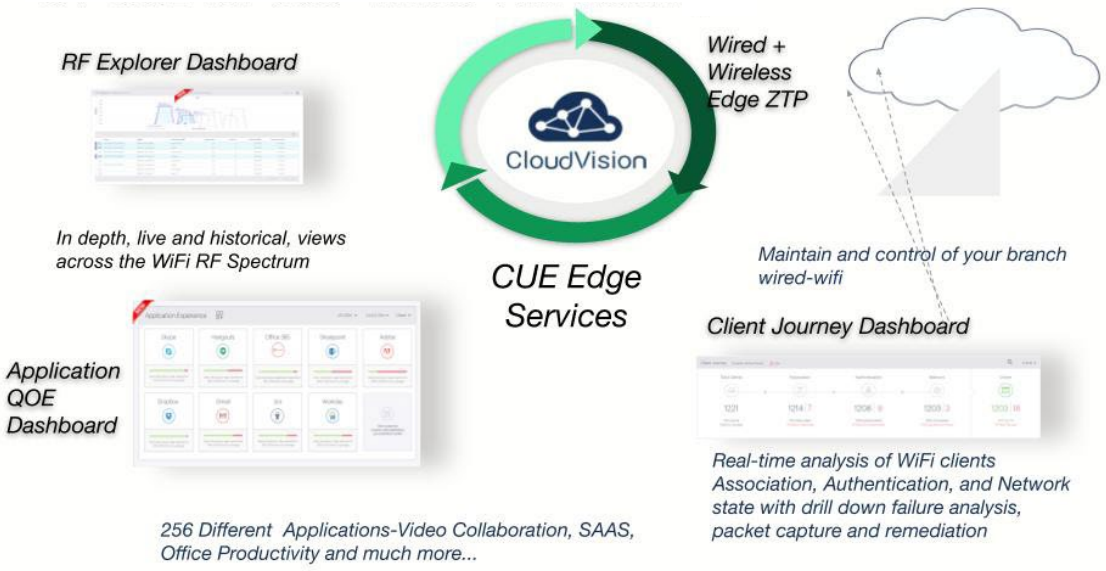



*Figure 11: AI/ML Predictive Alerting*

**6. Streamlined, Declarative Provisioning with CloudVision for "Network as a Service"**

Most IT managers face the dilemma of fixed budget and staffing for campus NetOps, while 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 look to point and click provisioning tools and automation systems to lighten and distribute campus networking workloads.

Arista has worked with its customers to develop enhancements to its CloudVision management system to simplify day 0 through day N provisioning workflows in the campus. Using a combination of scripting automation and declarative point and click provisioning, CloudVision Studios 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.

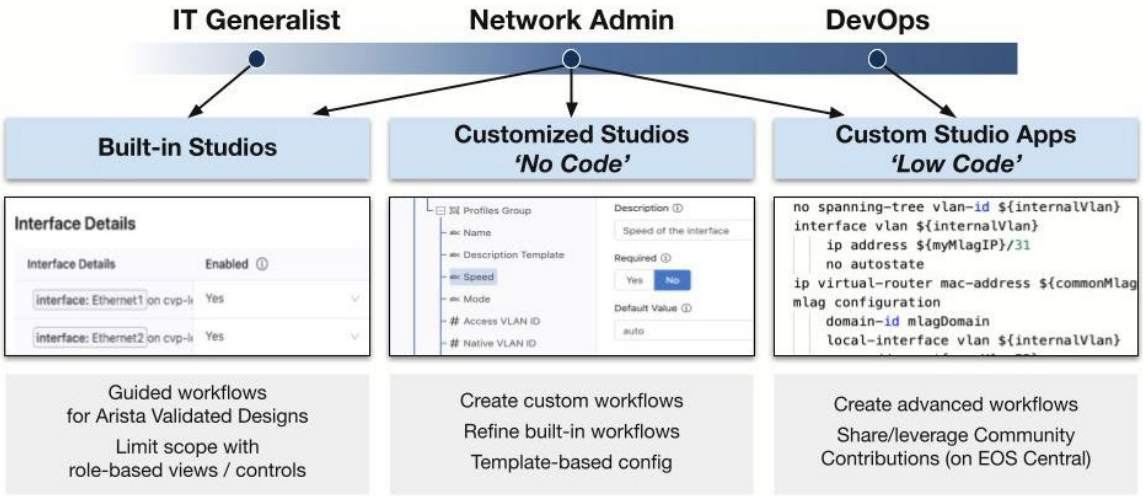



*Figure 12: Customizable Point and Click Provisioning Workflow*

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.

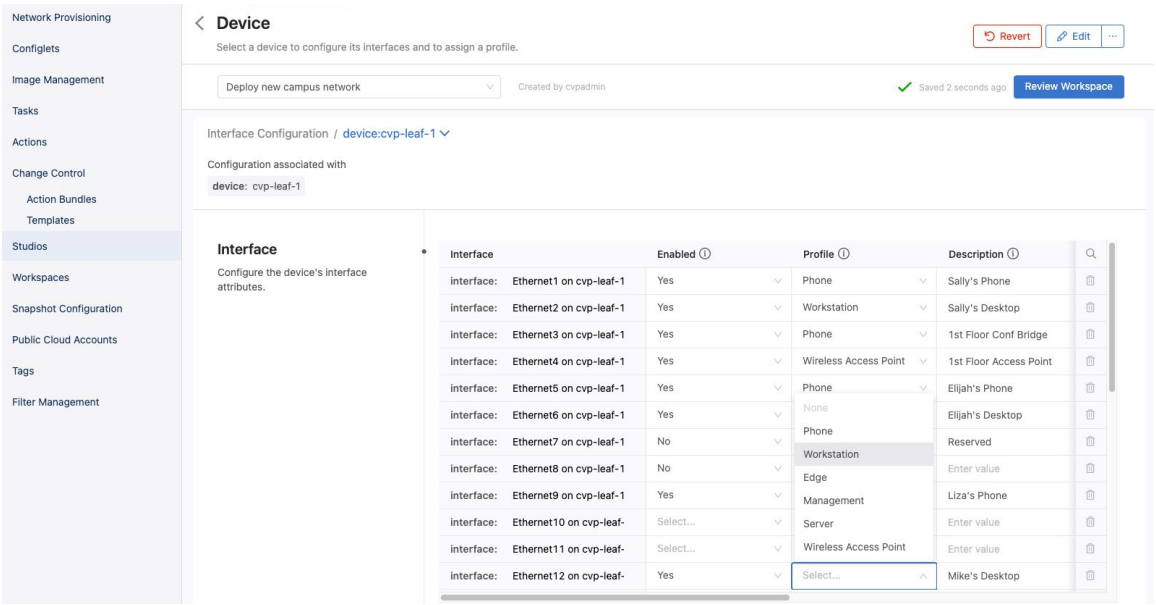



*Figure 13: Studios Declarative Provisioning Model*

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

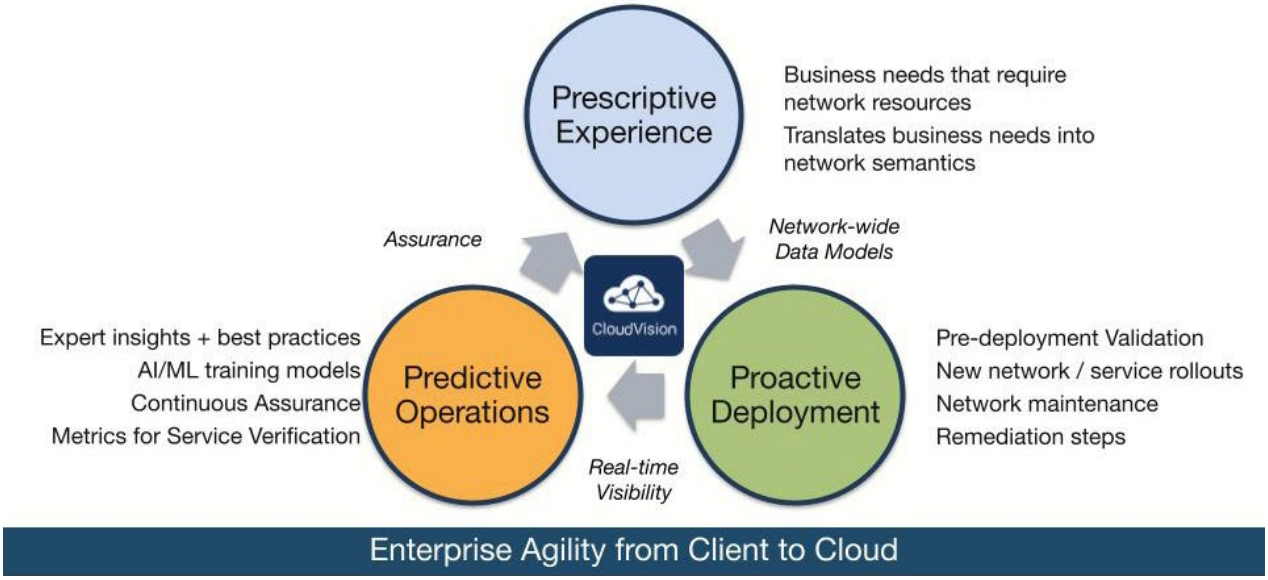



*Figure 14: Extending and Ensuring Outcomes in Campus Workspaces*

**7. AI Driven Threat Detection and Response: Arista NDR**

The explosive proliferation of client and IoT devices in the enterprise correlates to an increased and often unmonitored attack surface and elevated 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 patterns in traffic that signal a data probe or ransomware attack.

Arista's Network Detection and Response(NDR), is the only advanced network detection and response solution that provides the InfoSec team with answers to threats, rather than alerts lacking context. NDR combines artificial intelligence with human expertise. Arista NDR 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 Arista NDR can also be embedded in Arista Campus switches. These AVA sensors deeply analyze millions of network sessions to autonomously discover, profile and classify every device, user and application across any network. Using a multi-dimensional machine learning approach, NDR 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, Arista NDR compares entity behaviors to the peer group and the rest of the organization and brings together secure threat hunting in the campus for malware, IOT and disparate devices.

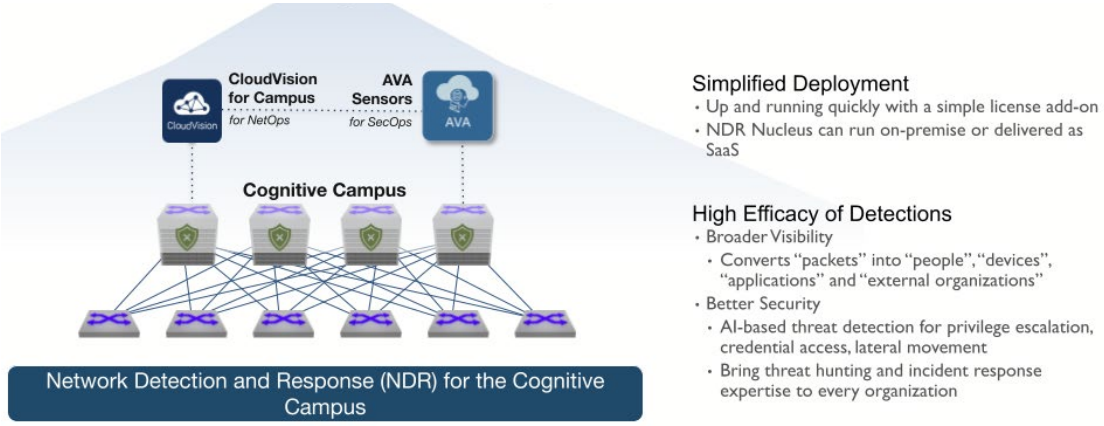



*Figure 15: AVA Sensors for Campus Threat Hunting*

Arista NDR monitoring sensors can be deployed in high traffic areas or run as a process on Arista campus switches. NDR Sensors are deployed locally ensuring that sensitive data does not leave your network. Sensors send summarized metadata to the NDR Nucleus which can be deployed on premises or in the NDR cloud. NDR Nucleus leverages Arista'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. Arista NDR leverages EntityIQ to Analyze all devices through Adversarial modeling. Arista NDR provides pre-configured adversarial models which can be customized by administrators through an easy to use AMI interface. Finally, Arista's Ava expert system automates the investigation and remediation process.

### Cognitive Campus: Client to Cloud Use Cases

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

- Deploying and managing an edge or small enterprise network
- Enhanced client to cloud automation
- Monitoring the distributed campus workforce
- Flow tracking to pinpoint hotspots
- Improved security from audit to segmentation

Here are a few examples:

1. **CUE in the Commercial Enterprise Network**

   Fast and fault-free provisioning of the edge or small enterprise network relies on simple, validated network topologies and corresponding provisioning tools that allow workers to securely connect WiFi users, and wired appliances to the public/private internet. Arista's CUE architecture leverages its campus switching, WiFi and secure edge solutions to fulfill this requirement. Arista's 710P series compact switches, coupled with the AP-C200/300 series access points, can be quickly deployed in workspace environments using common office wiring and power.

   The 710P switches are compact, aesthetic, and fanless, allowing convenient deployment from wiring closets to open plan workspaces. 1G and MGig PoE networking ports simplify connection of WiFi devices or other UTP appliances while also providing up to 60W power as needed. SFP+ uplink modules offer extensive options for connecting to various fiber backbones. MGig PoE passthrough (PD) connections allow the switches to be powered by a PoE enabled office net. Arista's foundational EOS provides EVPN overlay, MSS segmentation and real time monitoring support which includes NDR sensors for security analysis.

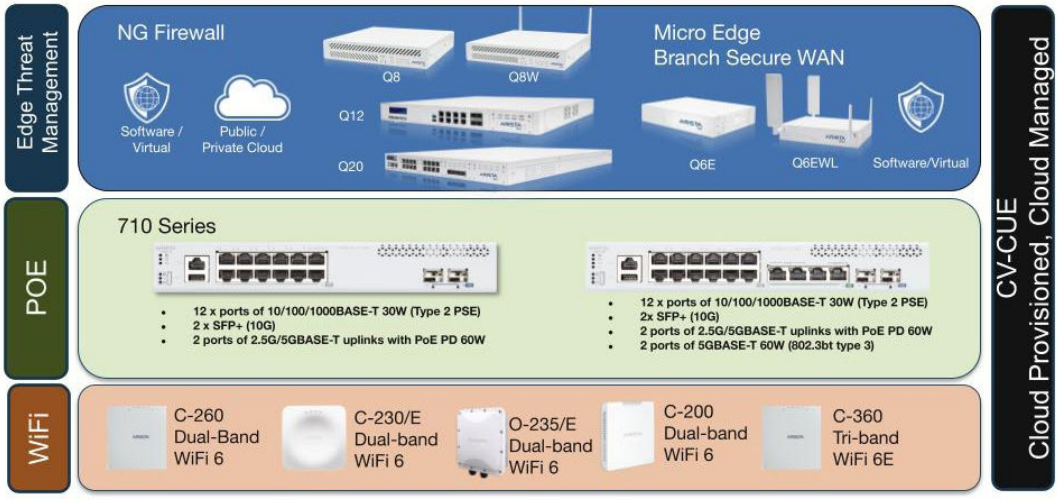



*Figure 16: Arista's Commercial Enterprise Portfolio*

Arista's AP-C200 series WiFi 6 and the C300 series 6E capable access points provide high performance, easy to deploy, cognitively managed wireless connectivity. PoE power support and a wide variety of ceiling mount options simplify deployment. Once powered, access points automatically connect to the cloud based CUE platform to receive its configuration and deliver cognitively managed WiFi.

Arista's edge threat security platforms are simple to administer, delivering cognitively managed security for small enterprises and remote offices. The Q series edge platforms economically deliver up to 1Gbps throughput with:

- Cognitive backhaul WAN prioritization across public and private internets including an optional LTE backhaul.
- Cognitive security profile provisioning and deployment templates that streamlines single or multi-site deployments.

All of Arista's small enterprise and edge workspace solutions are supported through CUE, coordinating network provisioning, monitoring and remediation. Using Arista's simplified provisioning templates, even novice administrators can quickly deploy and secure small enterprise workspaces. CUE's cognitive monitoring and troubleshooting tools simplify troubleshooting and remediation, ensuring the smooth and productive operation of the small enterprise.

**2. CUE in the Commercial Enterprise Network**

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 17 below.

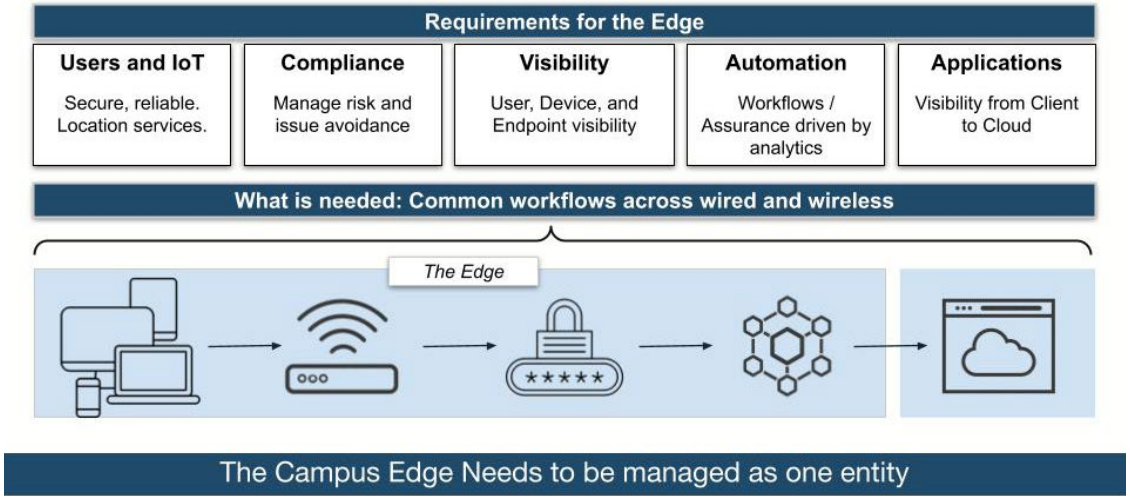



*Figure 17: Prudent Automation Steps From Client to Cloud.*

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 and CUE'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.

3. **Connecting and Monitoring the Distributed Workforce**

Arista Wi-Fi supports 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.

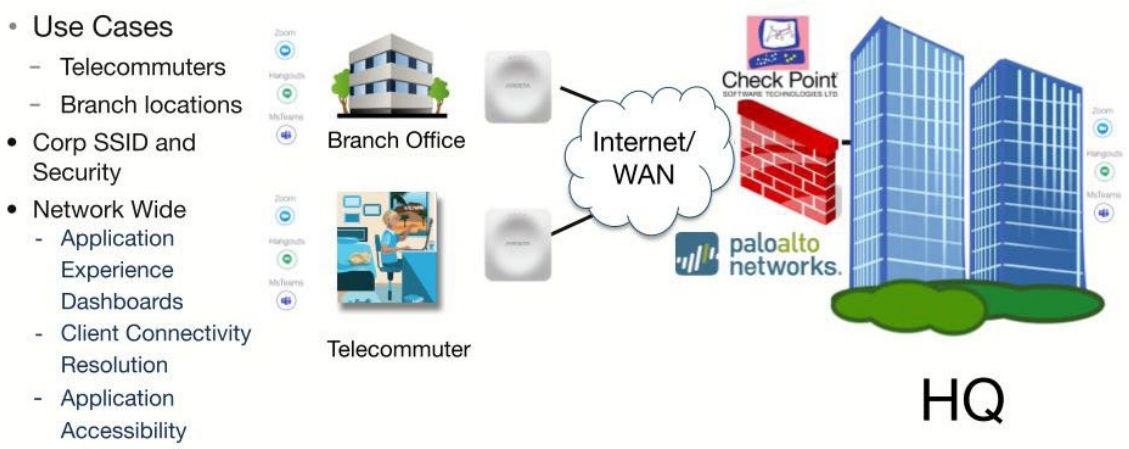



*Figure 18: Remote Connectivity Leveraging Existing VPN Concentrators*

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 CUE to track movements of key workers and assets in campus offices as seen in Figure 19.

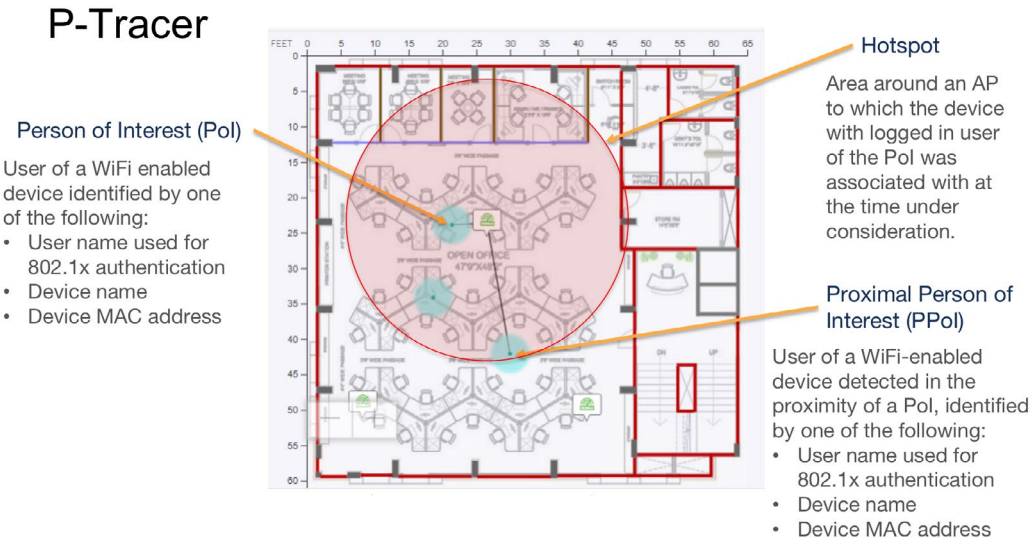



*Figure 19: Workforce/Asset Tracking and Reporting*

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

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

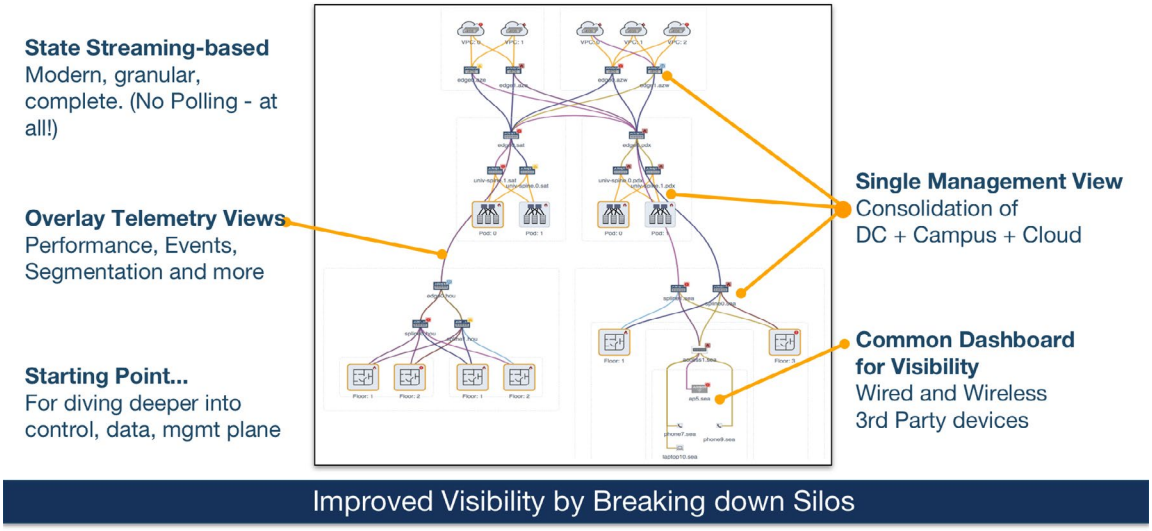



*Figure 20: CloudVision Telemetry Visualization from Client to Cloud*

Campus LAN and Wi-Fi platforms deliver real-time user and IoT device flow tracking and 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 worker devices, security systems, and facilities appliances.

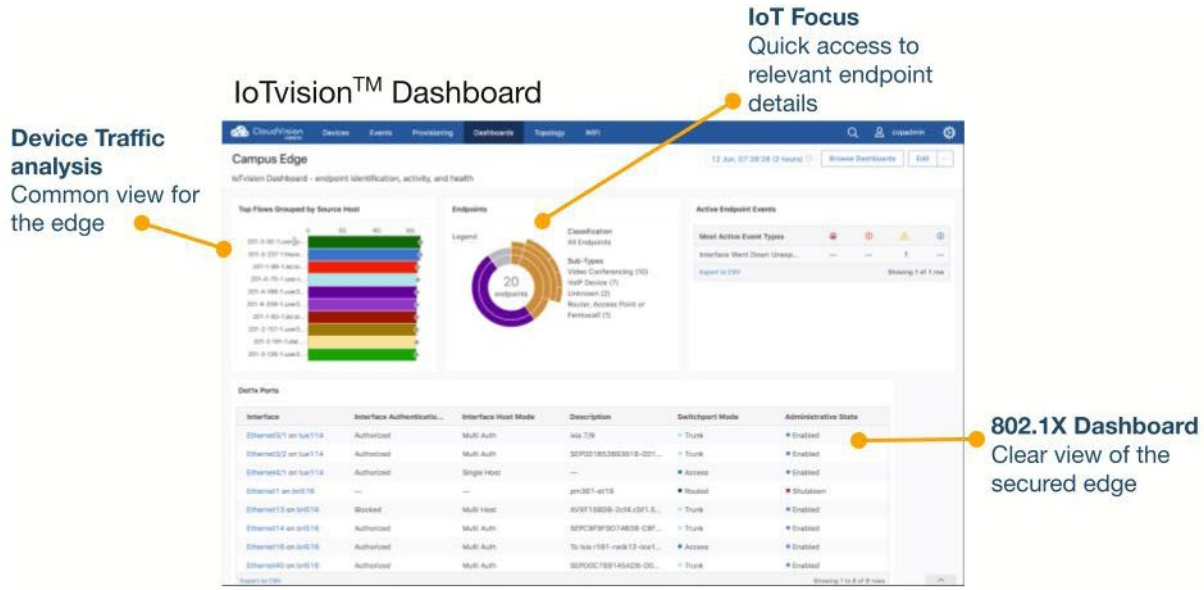



*Figure 21: Expanding Monitoring and Visibility to Campus IoT Devices*

## 5. 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 pin-point segmentation, CloudVision provides Macro Segmentation Services for Groups(MSS-G). Using existing switch resources, inter-device communications can be segmented into atomic granularity, using CloudVision's studios tools or solutions available from Arista's ecosystem partners. Using these segmentation options, 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.

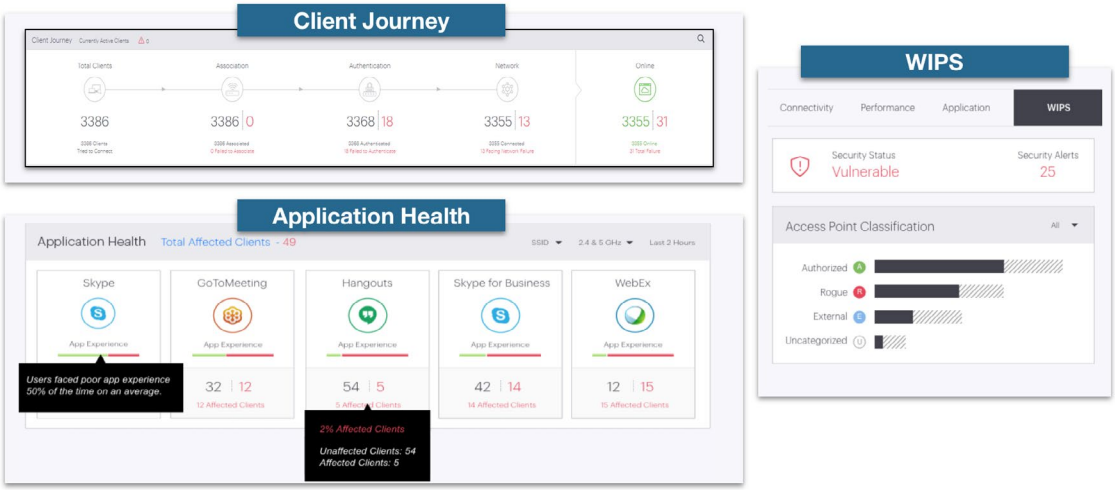



*Figure 22: Key Attributes of Cognitive Wi-Fi Including Intrusion Detection/Prevention*

In addition, the Arista NDR network sensor, deployed on Arista campus switches, provides ongoing security monitoring allowing Arista Virtual Assistants (AVA) to detect and report actionable threats. InfoSec operators can then respond through integrations with a variety of partners, including endpoint security and firewall providers.

## Summary

Embracing the new model of hybrid campus workspaces requires thoughtful assessment throughout the enterprise. Increasing dependency on workforce collaboration and meeting tools, coupled with the growing adoption of IoT devices 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 as a service from edge to network, leverages telemetry from NetDL to deliver the next level of performance, reliability, security and automated management for network administrators and the distributed workforce.

The contrast between other's intent-based networking, implying hope or hype, versus Arista's pragmatic cognitive-driven actions, is clear. Arista's portfolio of cognitive campus LAN, Wi-Fi and secure edge platforms, using EOS, and managed by CloudVision, allows IT managers to implement an adaptive and cognitive campus architecture that will meet the enterprise's 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