Primary Network Considerations within Healthcare Organizations

All healthcare organizations depend on their networks for their day to day operations. This includes clinician access to EPIC, sending scanned images to doctors remotely, tracking the movement of patients within their care rooms, ensuring data privacy, wayfinding through the hallways, providing guest access to the internet, and/or connecting the explosion of endpoint devices to their intelligent applications. The network has become much more than a way to push data from the bedside PC to a bunch of servers.

Arista, as a network pioneer within many of the largest cloud infrastructures has applied many of their modernization technologies within healthcare, for improving the overall reliability, security, and explosion of specialty medical devices that depend upon the network. Arista has worked directly with many of the top healthcare organizations around the globe in improving their networks.

This solution guide focuses on seven of the more compelling challenges healthcare organizations are faced with today, and the solutions offered by Arista in addressing these.

Below lists several of the many healthcare organizations Arista has provided networking solutions for.

Arista Healthcare Customers and Partners

Challenge: Ensuring Data Privacy with Older Imaging Equipment

Most healthcare organizations have millions of dollars invested in older imaging and scanner devices. They cannot afford to replace these with newer ones that offer data transfer encryption technologies. These older devices send patient data in clear text across the network. This data can be easily snooped by a number of listening devices. These listening devices gain access via taps, open Ethernet ports, and phishing their way through the wireless network into the switch infrastructure. Patient privacy is therefore at risk, which is a HIPAA regulatory violation.

The most common and well known approach for addressing this challenge is to create virtual networks within the campus network, and to leverage a zero trust model, where nothing is trusted and everything attached is identified, classified and associated. Specifically to secure any device attached to the network, into a virtual network, and to protect these networks from the outside.

Many healthcare organizations are not leveraging virtual networking technologies as this requires sophisticated switching and routing configurations, and switch port settings for identifying, classifying and associating endpoints (MRI machines as an example). Unprotected switch ports within imaging departments can lead to security breaches. These ports need to be protected. Given this, many healthcare organizations shut off unoccupied switch ports. These unused ports become wasted, as many nurses and doctors have a need for these ports as they move equipment around but cannot use them.

Arista Solution: Identity Driven Marco-Segmentation Services

As part of Arista's Zero Trust security architecture, Arista offers Macro-Segmentation Services (MSS-G) in which a number of virtual network technologies can be implemented for creating virtual networks. Virtual networks isolate users, traffic, and data into secure groups, all within the same physical infrastructure. Technologies leveraged include VLANs, VXLANS, VPN's, VRF's, MACsec and custom routing groups. Customers can choose the best virtual networks technologies from this list, based on their topology designs, traffic forwarding modes, and levels of security. Several of these technologies can be layered together for enhanced campus edge security. And these technologies are enabled non disruptively.

These tunneling, encryption, and packet header technologies are easily configured centrally, from CloudVision®, with visibility and pro-active troubleshooting to ensure there are no misconfigurations. Healthcare organizations can quickly add new virtual networks, with CloudVision policy templates, that are automatically configured. This cloud approach eliminates misconfigurations as compared to legacy switch platforms that require as required command line changes per box.

Further, Arista's zero trust security architecture includes endpoint identity management, where any endpoint device attached to a switch port, including scanners, MRI machines, PC's, Access Points, and IoT devices are identified, classified and authorized before forwarding any data packets across the network. Traffic from every endpoint authorized onto the network, are tagged with unique virtual network identifiers. Other endpoints including those that access the upstream applications with the same identifiers can communicate with these endpoints. This secures the traffic, i/e patient data into secure groups.
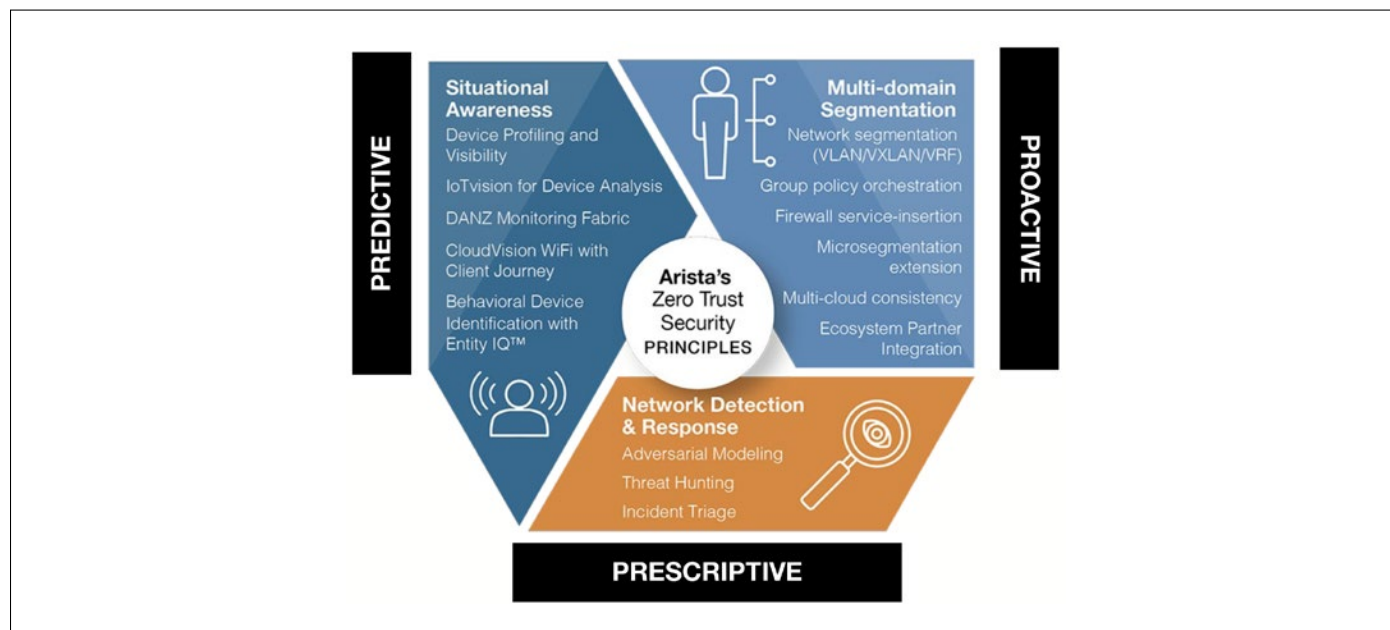
Arista's Modern Zero Trust Networking Security Principles

Arista's EOS®(Extensible Operating System) endpoint identity management is open where Arista switches can integrate with 3rd party identity platforms including Cisco's Identity Services Engine, Aruba's Clearpass Policy Manager, Forescout's EyeSight Platform, the Okta Cloud Identity Platform. These platforms verify the identity of endpoints connected to the network and provide identity information back to Arista switches for customizing the switch port settings and tagging the inbound traffic.

Finally, for healthcare providers implementing zero trust switch port security for the first time, who do not have an endpoint identity platform, Arista offers a next generation, cloud based endpoint identity management platform, known as CloudVision Arista Guardian Network Identity (CV AGNITM). This platform eliminates the need for on premise appliances, complex licensing, proprietary controllers, costly appliance clusters, and software revision management as the offering is 100% multi-tenant cloud based.

Arista Next Generation Identity/Access

Arista manages the cloud back end with highly reputable cloud providers. This cloud offering is analogous to EHRS platforms that are becoming cloud based. (https://binariks.com/blog/epic-cloud-healthcare/). Removing the headache of managing appliances, and secondary application functions frees your networking team in working more closely with your care staff and their speciality medical device needs.

Challenges: Managing Smart Device Chaos

Healthcare is experiencing an explosion of smart devices and applications (network attached). Speciality devices and smart applications that operate on PC's, laptops, tablets, smartphones, and wearables have become commonplace. All of these are attached to the network with a growing percentage being wireless. Wi-Fi is the preferred in building wireless technology as it is the most advanced with regards to security, coverage, throughput, location and mass market adoption. Commonly referred to as endpoints, all healthcare providers should be managing, tracking and monitoring these devices, for a multiplicity of reasons including the following:

1.   Authorized versus unauthorized endpoints: This is important as unauthorized devices are potential security risks. These risks include unauthorized devices that are snooping traffic on the network. This can lead to data breaches and ransom attacks as they gain vulnerability intelligence. Preventing access into the protected networks is critical here.

2.   Asset tracking: As many expensive assets are shared and therefore mobile, including crash carts, IV pumps, ventilators, nurses in particular need to quickly locate these as needed. Additionally, wearable Wi-Fi tags are being introduced for tracking patients and other critical people assets. As all of these mobile devices are attached to the network, where the network is fixed; these mobile devices can be easily tracked and located by triangulating their network connections.

3.   Correlated Troubleshooting: All mobile Wi-Fi endpoints connected into the network require a number of networking services to successfully communicate. These services include SSID, IP address and DNS name assignments, Wi-Fi handshakes, and security certificates (authentication). Additional services may also be applied including quality of service and other priority settings. While 99% of the time these services work, and are completely transparent to the staff using these devices, when there are connectivity issues it is hard to troubleshoot the root cause. As many of these devices are required in critical situations it is imperative to quickly pinpoint the problem and take corrective action.

4. Signal Integrity: One of the unintended outcomes in the adoption of these speciality medical devices, where everything is wireless and mobile, is ending up with congested airwaves, where every device is contending for a clear channel to communicate on. (more on this later). This is a wireless network problem where the endpoints depend on the access points to sort through this congestion. This requires real time congestion management.
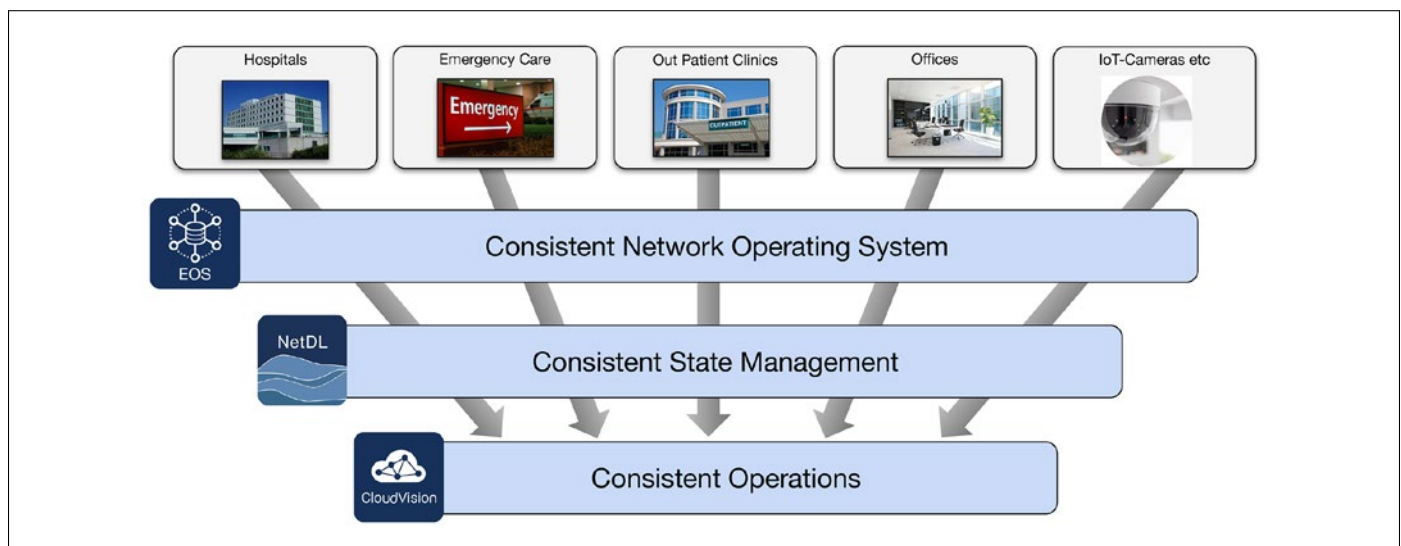
Arista Solution: Cognitive Campus

Managing, troubleshooting and protecting wireless networks, where smart medical devices in this hyper adoption mode requires computer driven machine intelligence as the network staff cannot keep up. This intelligence is commonly referred to machine learning, coupled with artificial intelligence, where sophisticated software observes, learns and acts upon network operation information for pinpointing issues, tracking devices, and mitigating problems including security threats. Network intelligence requires real time telemetry from multiple sources, and a comprehensive correlation engine for getting to the root cause.

Arista offers this machine driven, artificial intelligence, referred to as the Cognitive Campus, specifically for wired and wireless campus networks. While many other vendors market artificial intelligence with their wireless and wired network offerings, they tend to black box the capabilities here, where it sounds compelling yet misses the mark when solving many of the aforementioned issues. Arista Cognitive Campus AI technologies are based upon real world problems with well documented, and proven outcomes. Further, Arista's Cognitive Campus offerings are 100% cloud based where all of the back end intelligence sits within the cloud, thus eliminating the need for on premise controllers and appliances.

Arista's Cognitive Campus intelligence assists in all stages of deployment including the following:

- Initial installation, where default configurations are automatically loaded

- Collecting real time telemetry data in a single repository

- Acting upon this telemetry data with automated tuning, calibrations, and best channel handshakes

- Pro-active troubleshooting and reporting where endpoints are tracked, and reported on, including unauthorized device security reports

- Root cause connectivity dashboards, and signal integrities especially when there are Wi-Fi channel capacity/congestion issues.

All of these Cognitive Campus operations capabilities are integrated together where there are common dashboards that offer 360 degree visibility. Wireless intrusion detection and prevention, root cause analytics, automated tuning within given wireless spectrums, interferences, quality of service, and security settings are all embodied in the same platform. And there is a rich AI engine running in the background that is sifting through volumes of telemetry data in making informed decisions in which the network team can act upon.

Arista Cognitive Campus Consistency Across All Sites

Challenges: Around the Clock Patient Care with Limited Staffing

While tightly watching every patient is an age-old problem, technology advancements in Lidar (Light Detection and Ranging) sensors, which can be categorized as specialty IoT devices, address many of the challenges here. Lidar sensors scan, analyze, normalize, and alert on physical environments in which actions need to be taken. This includes knowing when a patient has fallen, someone forgetting to wash their hands, a hallway being blocked, or someone agitated, as well as myriad other activities.

Fundamentally Lidar measures motion, via light and motion technologies. Motion data is characterized within an AI driven database where abnormal events are flagged and alerted on. These alerts can be integrated into the nurses, doctor, and administration contact management system, where personnel can take action if there is an emergency condition. This technology elevates patient care as there are now human-like monitor systems that learn about the environment and can in real time detect problems.

Hallway Passages

Patient Care

Supply Room Checks

LIDAR Use Cases

Processing Lidar data requires an integrated computing cluster that is networked with each Lidar sensor. Each sensor streams 3 Gbps data in real time data, from the patient care room, and from other critical locations, to this intelligent back-end. While the cost to transfer this data is minuscule when averaged over a 5 to 7 year network infrastructure period, it does require a network upgrade within most patient care sites, as most sites have at most 1 Gbps switching infrastructures where these sensors would be placed. These upgrades require a transition to 5/10/100 Gbps switching infrastructures.

As healthcare organizations look towards the future, where they are retrofitting, and/or constructing patient care floors and rooms with Lidar sensors, as well as upgrading their Wi-Fi technologies to the latest multi gigabit uplink standards, they should be considering wired Ethernet ports to each room that offers multi- gigabit speeds. This includes Category 6 and optical wiring drops, and switching platforms that offer low latency, high performance multi-gigabit per port switching.

Arista Solution: Arista Cognitive Campus Wired and Wireless Network Infrastructures

Arista leads the market with many of the most advanced multi-gigabit campus switching platforms including the modular 7508 chassis, and several fixed 720, and 722 single and dual rack unit (RU) platforms. Moreover Arista offers the 710 platform for small density areas where there are no cooling, and/or equipment racks available. The 710 is fanless and has flexible mounting options. It is fully managed as are these other chassis.

These platforms embrace simplicity whereby one common operating system, management platform, and open automation interfaces lower staffing costs while accelerating time to value, well beyond traditional offerings from legacy market share leaders. These platforms address the current and future needs of patient care use cases, whereby the demands continue to expand including multi-gigabit port capacity, real time streaming data feeds, coupled with data security, and around the clock availability (zero downtime).
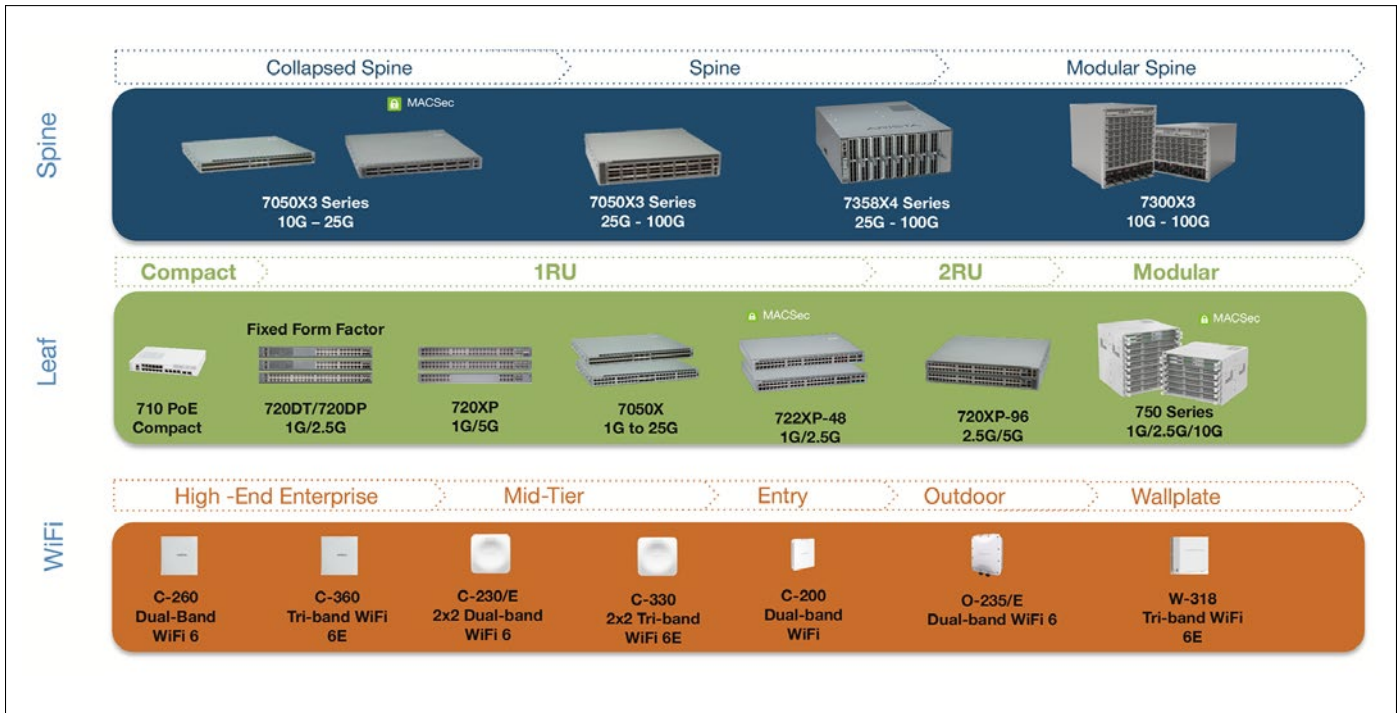
Cognitive Campus Platform Portfolio

Further, these platforms redefine the backbone of the network, where multi-tier, single points of failure, and spanning tree shortcomings are eliminated, while providing integrated wireless Access Point visibility, troubleshooting, and cognitive intelligence.

Arista switching platforms are the future for healthcare organizations looking towards the future of Lidar, IoT, data protection, Wi-Fi 6, 6E (and beyond), real time video, managed cameras, which serves a multiplicity of users including doctors, nurses, patients, guests, and the administration staff.

Challenges: Wireless Network Reliability-Managing Congested Airwaves

All healthcare providers are leveraging wireless communication to its fullest extent, as this technology offers the mobility they need with connections to intelligent data sources. Every month healthcare providers will bring in a new smart device type that is mobile, typically Wi-Fi or Bluetooth. And as stated, the networking teams are typically not involved in the adoption decision as the

Baptist Healthcare Replaces Cisco Campus Infrastructure with Arista Networking Platforms

As Baptist Health looked toward the future across six hospitals, 75 outpatient sites, and three stand-alone emergency departments they needed to reduce the number of Cisco platforms, network operating systems, and management tools. Their current Cisco deployments were too costly and complex for quickly resolving problems, and or addressing future use cases and site expansions.

Baptist Health chose Arista for both their wired and wireless networking infrastructures as Arista has a proven track record specific to one operating system and one operations management platform (CloudVision). These software infrastructure products work across all of their data center, campus, edge routing and cloud networking switches.

Further Arista has tightly integrated their enterprise class Wi-Fi 6 and 6E Access Points in with their wired infrastructure products for common discovery, visibility, upgrading, and troubleshooting operations management. And Arista meets their future requirements as Baptist Health is expanding their number of specialty devices including electroencephalograms and robotic supply carts with asset tracking authentication management.

For more information read the TechTarget article published May 03, 2023. Baptist Health leaves Cisco for Arista

primary focus is whether these devices will solve patient care issues. The network staff have to enable these devices to just work, while ensuring security, stable connectivity, and being able to track them.

The problem here is in the sharing of the same air space as these devices use the same radio frequencies to communicate on, whether Zigbee, Wi-Fi and/or Bluetooth. This leads to crowded airwaves, often on the same radio frequencies, with the most common being 2.4 Ghz. One of the primary functions of the Access Points, is to balance this load in picking the best clear channel within the radio spectrum the endpoints are using. Behind the scenes the access points in real time are managing topology meshes, roaming events, traffic priorities, switch port uplinks. drop offs, channel selection, intrusion detection, password authentication and a myriad of other functions. These capabilities separate enterprise class Wi-Fi access points from consumer grade.

For too long these enterprise grade access points have had nerd knobs to help address the above yet they require a technician that understands radio waves to tune them. Or they have to bring in a professional services company once a year to re-tune their Access Points.

Arista Solution: Cognitive Campus for Wi-Fi 6 and 6E Access Points

As another machine learning, artificial intelligence function within Arista's Wi-Fi product line, Arista access points offer self tuning, self healing, auto channel selection, hitless upgrading, and integrated wireless intrusion protection, for managing congested airwaves, where 7x24 reliability is a requirement. Moreover, this intelligence is easily programmed via highly graphic, visual interfaces where recommendations are provided on how to tune the Access Points based on the client activities within each floor. There are floor maps, and radio coverage maps for helping non Wi-Fi experts understand coverage.

Much of the Intellectual property running in the background is based on multi-radio access point management where tri radios are leveraged for dataplane, telemetry and intrusion detection functions. These radio's are abstracted into a set of policies. All radio tuning is done behind the scenes within the cognitive management plane. This multi-radio cognitive management plane intelligence has been a core focus of Arista.
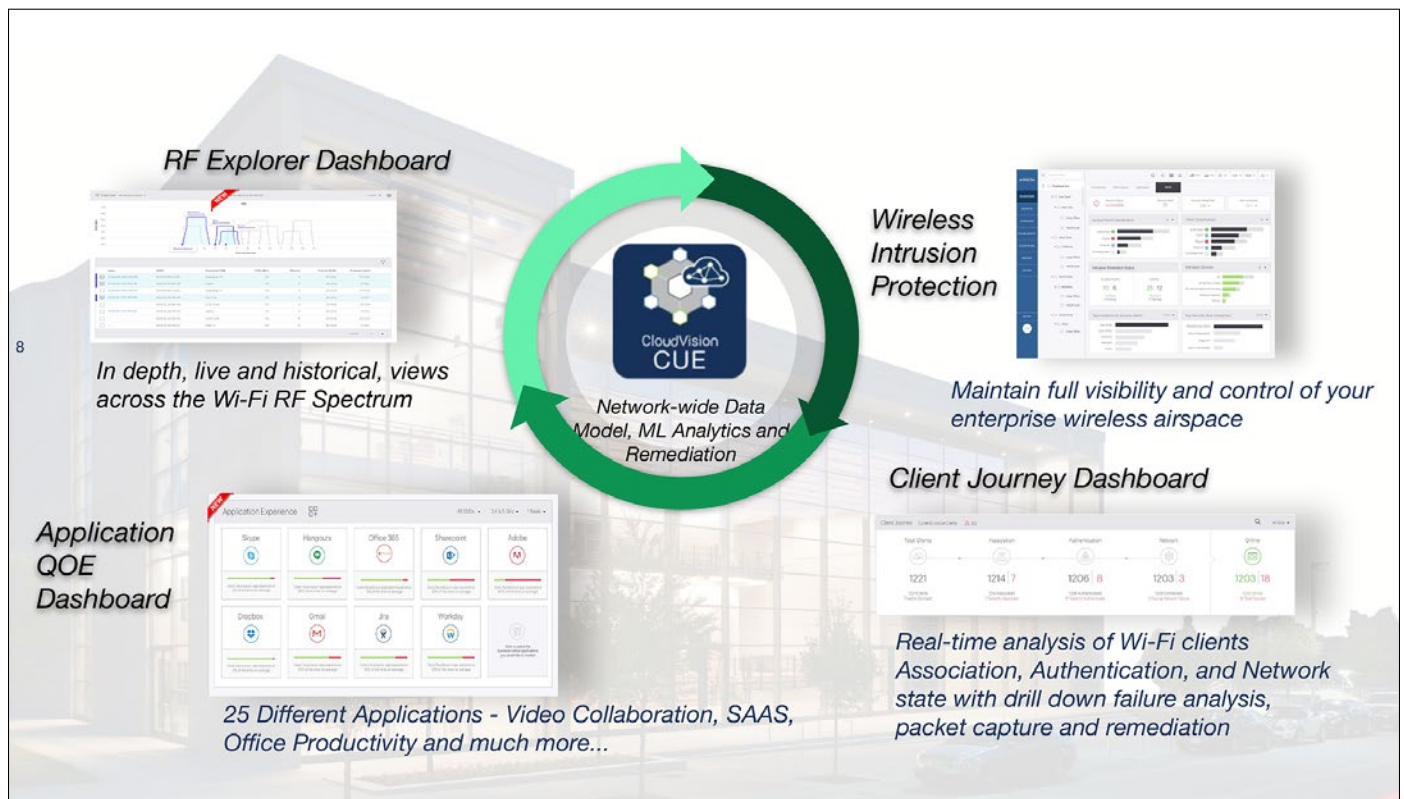
Wireless 360° Visibility and Security

More recently Arista has released Wi-Fi 6E access points, specifically for healthcare providers where the 2.4 and 5 Ghz radio spectrums are over saturated. Wi-Fi 6E access points provide communications across the 6 Ghz unlicensed spectrum while offering backwards compatibility to AC technologies. This new 6 Ghz unlicensed spectrum is significant not only because there are few users today, but also because it offers wider channels. These wider channels offer 10x times the performance in many cases and future proof this spectrum as more and more devices and networks run on 6 Ghz. All of Arista's Wi-Fi 6 and Wi-Fi 6E access points leverage Arista's Cognitive management plane technologies including the AI driven cloud hosted back-end.

C-360	C-330	W-318
• 6/5 GHz: 4x4:4 • 5 GHz: 4x4:4 • 2.4 GHz: 4x4:4 • Wi-Fi 6E 2x2:2 multi-function radio	• 6 GHz: 2x2:2 • 5 GHz: 2x2:2 • 2.4 GHz: 2x2:2 • Wi-Fi 6E 2x2:2 multi-function radio	• 6 GHz: 2x2:2 • 5 GHz: 2x2:2 • 2.4 GHz: 2x2:2
• Dual 10 GigE with power failover (802.3bt PD)	• Dual 2.5 GigE with power failover (802.3at PD)	• 2.5G WAN Port (802.3bt PoE PD) • 3x 1G LAN Ports (one port with 802.3af PoE PSE)
• Full feature Wi-Fi 6E AP • Software configurable Wi-Fi 6 Dual 5GHz or Tri-band Wi-Fi 6E • 2x2:2 Wi-Fi 6E multifunction radio • Integrated BLE / Zigbee • TPM	• Full feature Wi-Fi 6E AP • 2x2:2 Wi-Fi 6E multifunction radio • Integrated BLE / Zigbee • Internal antennas • Full feature set using 802.3at • TPM	• Wi-Fi 6E wall plate AP • Integrated BLE • Internal antennas • 802.3at operation without PSE • TPM

Cognitive Campus Platform Portfolio

Finally, for healthcare organizations looking to upgrade a select floor within their hospitals or other care facilities, Arista access points are fully interoperable with 3rd party PoE switching platforms as Arista Access Points are industry standards based. Customers can easily manage the Arista Access Points without having to install any appliances, controllers or gateway technologies. This is an easy way to migrate over to Arista's Cognitive Campus products.

Challenges: Zero Down Time Network Design and Operations
Healthcare providers depend on their networks, 7x24. Unfortunately there are outages, whether planned or unplanned. These outages can be minor where a room, floor, or an individual application is impacted or major where the entire network is down. For critical care facilities none of these outages are good.

There are many factors involved in designing and operating zero down time networks. Many advancements have been made in the last 10 years, based upon cloud designs, where networking has become far more reliable. Healthcare providers who have the opportunity to upgrade their networks, should consider operational best practices as this significantly reduces the total cost of ownership, while improving uptime.

Arista Solution: Unified Cloud Networking with Hitless Software Upgrading
Zero time network design and hiltless operations management is foundational across all Arista infrastructure products. Starting with topology designs, Arista has led the industry in simple yet highly redundant scale out switching topologies where there are no single points of failure logically or physically. Arista's leaf/spine topologies, leveraging multi-link aggregation and failover protocols, has taken the complexity out of complicated multi-tier legacy backbones, with far better utilization when there is redundant bandwidth. This is embodied in Arista Universal Cloud Networking design principles. Any link, port, or switch failure, can be immediately acted upon where traffic is redirected within milliseconds with close to zero packet drops.

Equally important, Arista platforms, both wired and wireless, can be upgraded with new software releases, and security patches without taking down the network. 99% percent of all Arista switch operating system updates are hitless. Moreover, the switch EOShas been developed on open Linux, where modules and patches are applied in specific areas without impacting the running state of the modules and functions. Arista has greatly reduced the amount of security updates by a factor of 10 compared to other vendors by having the lowest software defect rates within the networking industry. This minimizes upgrades in general.

Arista wireless Access Points are intelligent where they can re-direct clients to neighbor access points, without any drop in communication when needing to upgrade an access point. Clients are automatically re-connected when the upgrade is complete. All of these upgrades are done through Arista's multi-function, CloudVision operations management platform.

Challenge: Threat Detection and Prevention

Healthcare provider networks are private, public and semi private. This equates to networks that handle patient records, monitoring data, smart device programming data, accounting records, insurance communications, guest networks, and facilities mgmt IoT data. Further, these networks are now connected to third party clouds, including many suppliers that are beginning to offer managed services, for example Johnson Controls with their HVAC systems.

While this document provides recommendations on virtual segments, and endpoint authorizations, as part of the zero trust security approach, security threats still occur, especially by very creative smart hackers. The network cannot control all security issues as endpoints can be turned into unsuspecting hotspots, even those that are authorized devices.

This is especially true with IoT devices, where they have very thin network interface stacks and often use GNU General Public License (open Linux) without fully vetting these stacks from a security perspective. Similarly unsuspecting receptionists, or even doctors can make a wrong click on something within their browser and download a worm that becomes a security hack. These devices are easily compromised.

The challenge for most healthcare organizations is that they do not have dedicated security operations teams where they can monitor malicious activities around the clock. Nor are they experts with regards to every device on the network and ensuring these devices have secure interfaces; nor are they aware of how devices should be communicating on the network and whether they are engaged in malicious activities based upon traffic patterns.

Arista Solution: Network Detection and Response

Arista offers an industry leading threat detection and response platform, better known as NDR for detecting and mitigating unwanted network behaviors. Arista's NDR platform is tightly integrated within Arista switches, as smart sensors run natively on every switch port. NDR has patented behavioral analytics where the endpoint and application traffic is observed, analyzed and acted upon. This goes well beyond whether a new device detected is authorized or not.


Securing Healthcare Networks
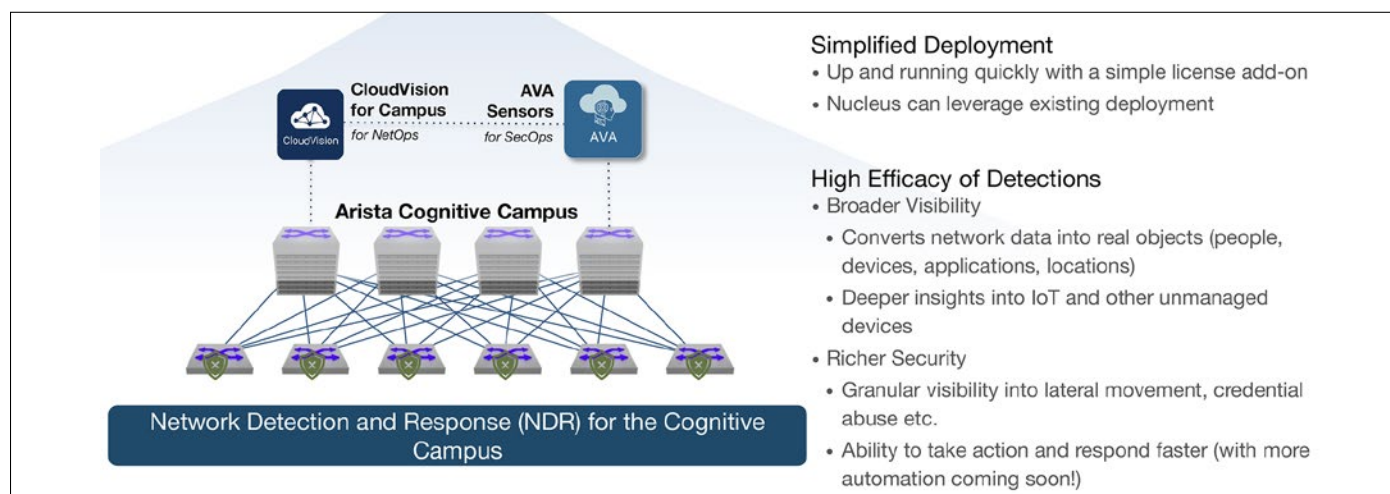
NDR profiles every endpoint based upon what should be normal behaviors versus abnormal behaviors. These behaviors can be observed and learned, and/or customers can create their own behavioral profiles. Moreover, NDR includes predefined profiles for well known device and application types. And NDR easily scales as the smart sensors run distributed at the edge within Arista wiring closet switches.

Going one step further, NDR provides proactive response and remediation, where issues flagged are proactively reported. Customers can also add automation where NDR can make requests to quarantine bad actors. NDR is easily managed by teams without deep security backgrounds. NDR is fully cloud based and does not require on premise appliances. NDR can be purchased as packaged offering or as a service or as a service that can be converted to packaged product.

Challenge: Increasing Efficiency while Improving Patient Care and Safeguarding Inventory

Healthcare institutions invest heavily in advanced medical equipment and costly inventory that needs to be easily and accurately tracked within a facility. If healthcare professionals are spending time searching for equipment, it can be a time consuming and frustrating task. Tracking services could not only help staff quickly locate these items, the data can be used to determine how often and where equipment is needed and make adjustments to improve more efficient use of these resources.

In addition to tracking equipment, every room in a facility should be used to its full potential. Having the data on when and how often a space is being utilized improves the efficient use of valuable facility resources.
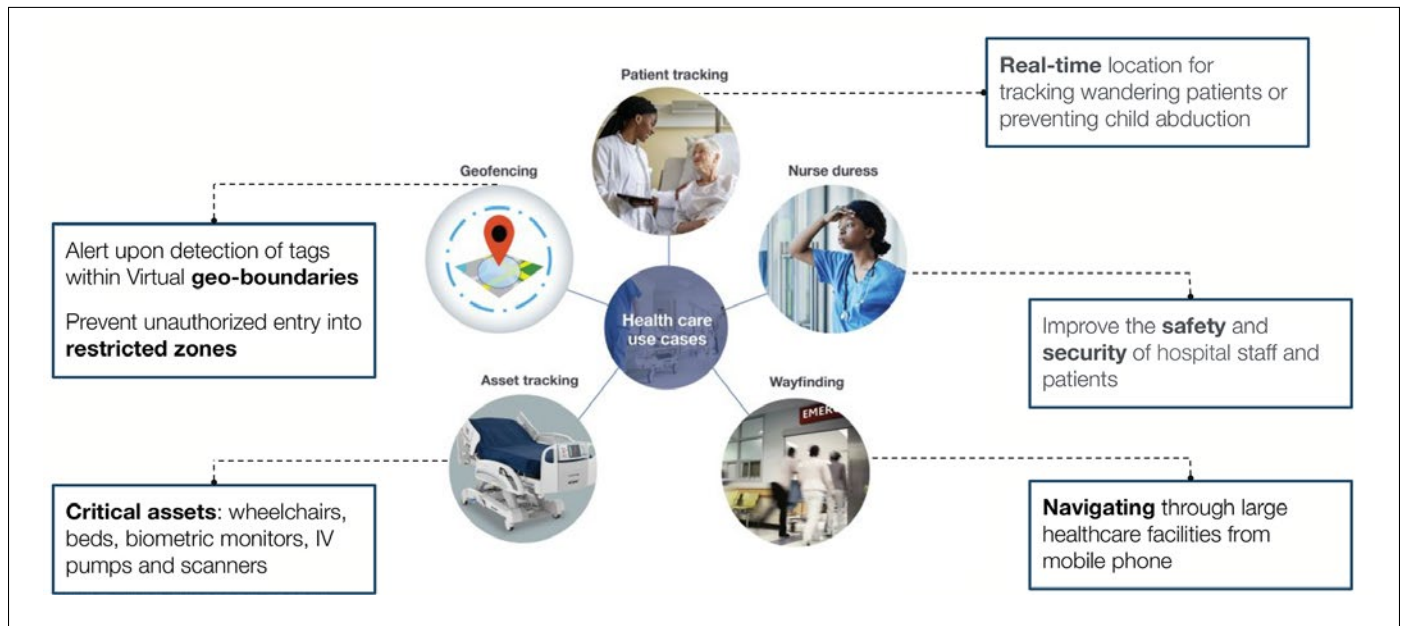

Locationing: Use Cases in Healthcare

Arista Solution: Location and Tracking Services

Arista's Wi-Fi solution integrates with multiple third-party technology service providers delivering location and tracking services for healthcare facilities. Location and tracking services can provide many benefits to healthcare institutions including better utilization and tracking of these shared resources.

These tracking services are provided by leveraging the Wi-Fi infrastructure to relay in real time the location information of a tracked device. The devices tracked can be small beacons attached to equipment or an app on a mobile phone. Wayfinding services can provide turn by turn directions on a mobile phone to help a patient quickly find the location in a complex building. The same wayfinding service can help healthcare professionals find equipment or assets they need to quickly provide services to patients.

Additionally, space analytics of room occupancy data can help in designing optimum scheduling of operating/diagnostic procedures and reduces the amount of idle time between procedures. Thereby, maximizing the efficiency of facilities. Arista Access Points provide granular (less than 10 meters) location centric telemetry data. This telemetry information enables these 3rd party location and asset tracking applications.
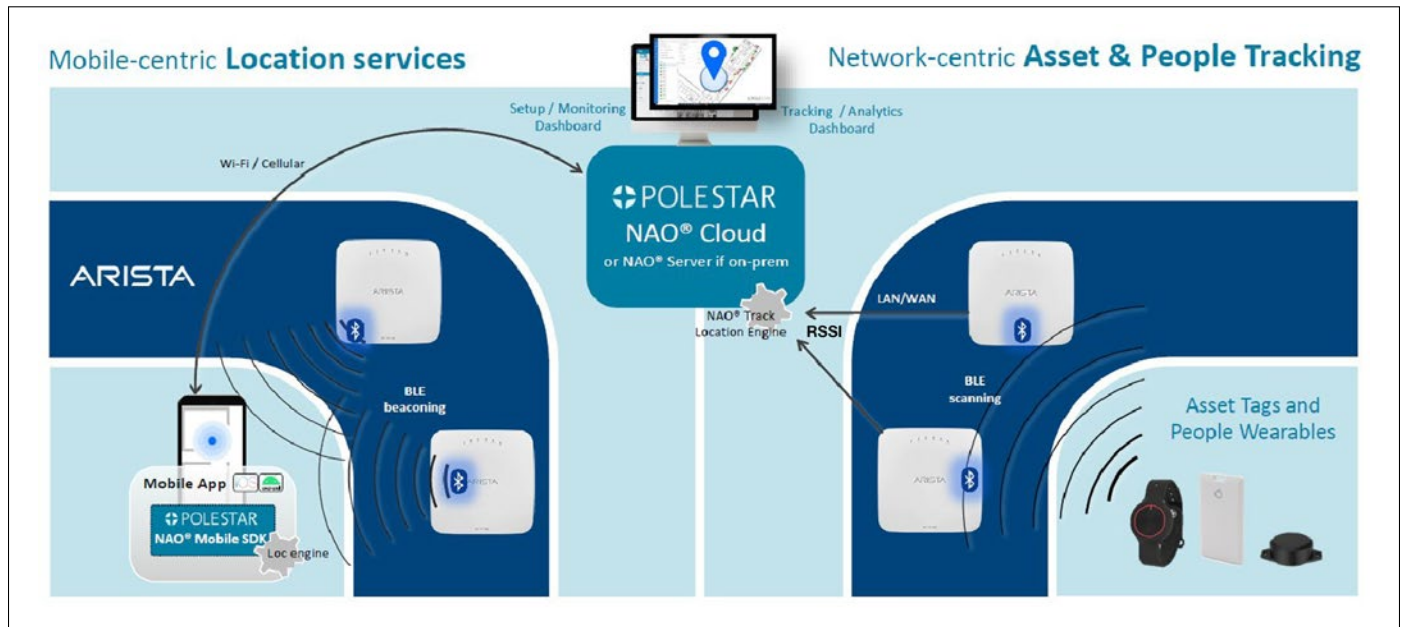
Locationing: Arista - Pole Star Technology Stack

Summary

Healthcare organizations have huge IT challenges in front of them as the explosion of smart patient care devices and applications will continue to accelerate at unprecedented rates. Networking technologies are the number one enabler of these IT driven ecosystems as everything is interconnected with data exchange, data sharing and data streaming interfaces. Healthcare organizations require an open yet highly secure network, one that is borderless yet protected.

Bandwidth remains the primary driver of healthcare networks, yet needs to be based upon cloud principles for all software functions. This requires a more unified approach that includes automated service activation, hitless upgrading, proactive security detection and prevention, and smart segmentation. Arista has developed a unified approach based upon cloud networking principles that overcomes the limitations of legacy approaches. Healthcare organizations need to migrate from these legacy networks to cloud infrastructures as they address their bandwidth, connectivity and mobility needs.