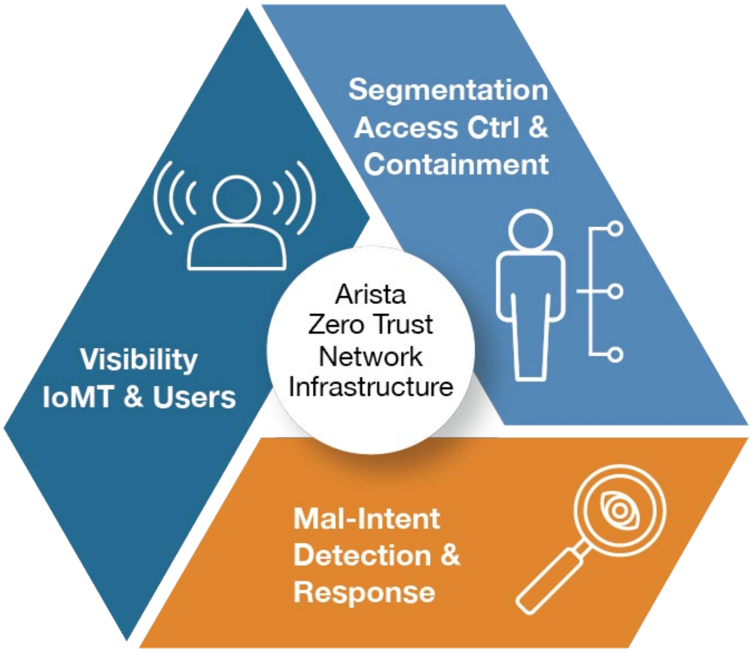
Tenets of a Healthy Hospital Infrastructure

Today more than ever the security of patient data needs to be a fundamental consideration when building a healthy hospital.   Traditional designs and architecture are no longer adequate as evidenced by numerous recent outbreaks of ransomware, theft of patient information and tampering of medical diagnostic equipment. A healthy hospital infrastructure must provide visibility of all assets and users, data containment through segmentation and continuous monitoring of mal-intent. For good reason the high cost of healthcare is top of mind globally, therefore a healthy hospital network architecture needs to not only consider security but operational cost and simplicity as well.

Hospitals' reliance on connected digital technology has created an Internet of Medical Things (IoMT). IoMT includes nurses' stations, building automation systems, medical devices, security systems, televisions, telephones and more; all of which are connected to the hospital network. Users, applications and supply chain partners and contractors all have network access that needs to be controlled. The hospital network needs to be ubiquitous: pervasive, resilient, readily available, and in unlimited capacity.



In this paper we discuss the three basic tenets for a healthy hospital architecture:

- Visibility of connected IoMT and Users
- Segmentation for Access Control and Containment
- Detection and Response of Mal-Intent

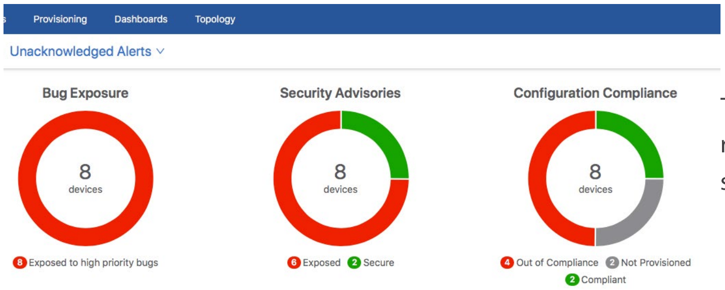
We will also discuss how Arista's zero trust network strategy can help healthcare organizations achieve those tenets.

Visibility of Connected IoMT and Users

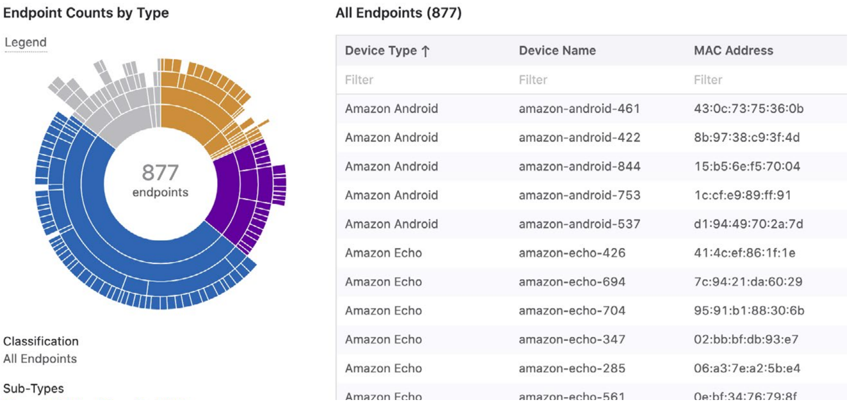
Securing a healthy hospital begins with visibility of all connected resources - IoMT, IoT, users and network infrastructure. Each resource may have state that could include things like software version, location, time/date, observed behavior, device analytics and more. Visibility with network infrastructure such as switches and routers is also needed to ensure that network equipment is not being compromised by known software defects or vulnerabilities identified by industry standard PSIRT (Product Security Incident Response Team) reporting. Security begins with visibility because visibility of resources drives enforcement policies that regulate with what a device or user is or is not allowed to communicate. And as will be discussed later, visibility of all connected resources is the foundation for identifying mal-intent which could be the result of malware or a malicious user. To understand all connected resources, Arista provides a variety of visibility technologies and has also established strategic partnerships with other vendors via open standards to ensure interoperability.

Arista CloudVision for Network Infrastructure Visibility

Arista CloudVision and Arista NDR provide a wealth of visibility information to understand connected resources.



The CloudVision compliance dashboard provides centralized reporting of all Arista switches that are vulnerable to PSIRTs or susceptible to known software defects.



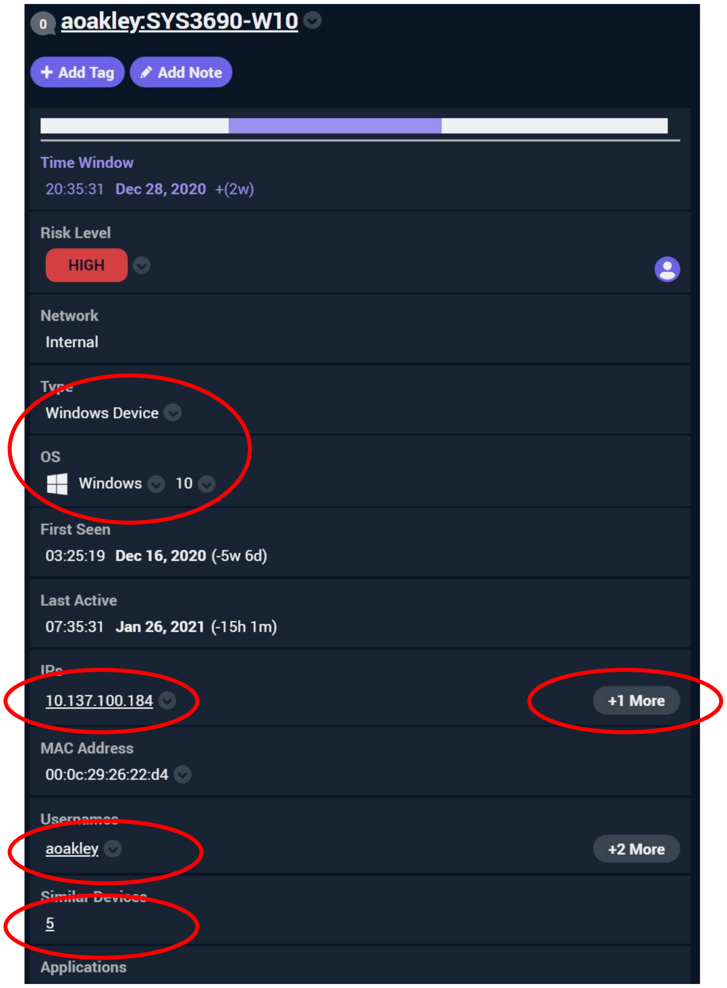
All Endpoints (877)

Device Type ↑	Device Name	MAC Address
Filter	Filter	Filter
Amazon Android	amazon-android-461	43:0c:73:75:36:0b
Amazon Android	amazon-android-422	8b:97:38:c9:3f:4d
Amazon Android	amazon-android-844	15:b5:6e:f5:70:04
Amazon Android	amazon-android-753	1c:cf:e9:89:ff:91
Amazon Android	amazon-android-537	d1:94:49:70:2a:7d
Amazon Echo	amazon-echo-426	41:4c:ef:86:1f:1e
Amazon Echo	amazon-echo-694	7c:94:21:da:60:29
Amazon Echo	amazon-echo-704	95:91:b1:88:30:6b
Amazon Echo	amazon-echo-347	02:bb:bf:db:93:e7
Amazon Echo	amazon-echo-285	06:a3:7e:a2:5b:e4
Amazon Echo	amazon-echo-561	0e:bf:34:76:79:8f

The CloudVision Device Analyzer feature identifies and classifies all connected endpoints. It also provides flow records showing who is talking to whom along with packet data showing the volume of traffic.

Arista EntityIQ for Visibility

Arista EntityIQ provides behavioral device identification via an AI-based security knowledge graph that identifies, profiles and tracks devices, users and applications on an enterprise network. Devices are grouped into peer groups based on common behaviors and tracked as they move across the network and beyond, even as IP addresses change. As shown in the screenshot below, EntityIQ has in fact tracked this device even as those IP addresses have changed.



0 aoakley:SYS3690-W10

+ Add Tag
Add Note

Time Window
20:35:31 Dec 28, 2020 +(2w)

Risk Level
HIGH

Network
Internal

Type
Windows Device

OS
Windows 10

First Seen
03:25:19 Dec 16, 2020 (-5w 6d)

Last Active
07:35:31 Jan 26, 2021 (-15h 1m)

IPs
10.137.100.184
+1 More

MAC Address
00:0c:29:26:22:d4

Usernames
aoakley
+2 More

Similar Devices
5

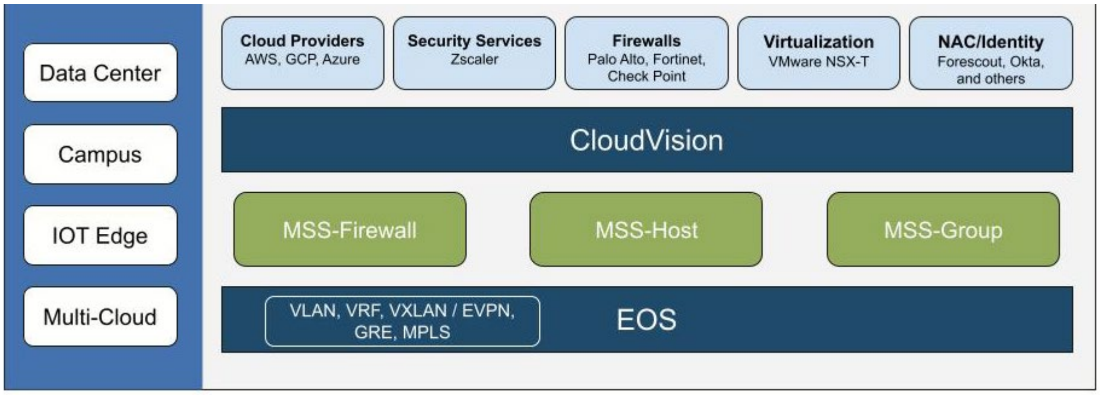
Applications

Third Party Integration for Visibility

CloudVision integrates with all the leading NAC providers. For example, when integrated with Forescout, network visibility extends to include granular telemetry on IoMT devices.

Segmentation for Access Control and Containment

The second aspect of securing a healthy hospital involves implementing access controls to ensure that devices and users only have access to resources that are necessary to deliver the relevant business outcomes. Network segmentation is not only important to regulate access control but to also contain an outbreak to a limited set of devices should an outbreak occur. Arista supports a variety of segmentation controls. Legacy methods such as ACLs, VLANs and VRFs are widely used today, but many modern hospitals require a more granular and dynamic segmentation approach.



MSS-Group

To meet the emerging segmentation requirements mandated by many healthy hospital and campus networks, Arista invented an innovative approach called MSS-Group (Group Based Macro Segmentation Services). MSS-Group provides several benefits including:

- Segmented groups can be created independent of a device's IP address or subnet.
- The solution works with switching equipment from other vendors and is simple to implement and operate.
- The administrator need not worry about scalability issues associated with ACLs, re-IPing a portion of the network to add a new VLAN , proprietary tagging solutions that only work with a single manufacturer or overlay networks that add complexity.

For example, a smart bed should only be able to communicate with the nurses station and physician network. A security surveillance camera should only communicate with the video recorder equipment and the Security team. Security cameras should not even be permitted to communicate with each other as that is often how malware spreads. Arista MSS-Group method provides a solution to these challenges.

Detection and Response of Mal-Intent

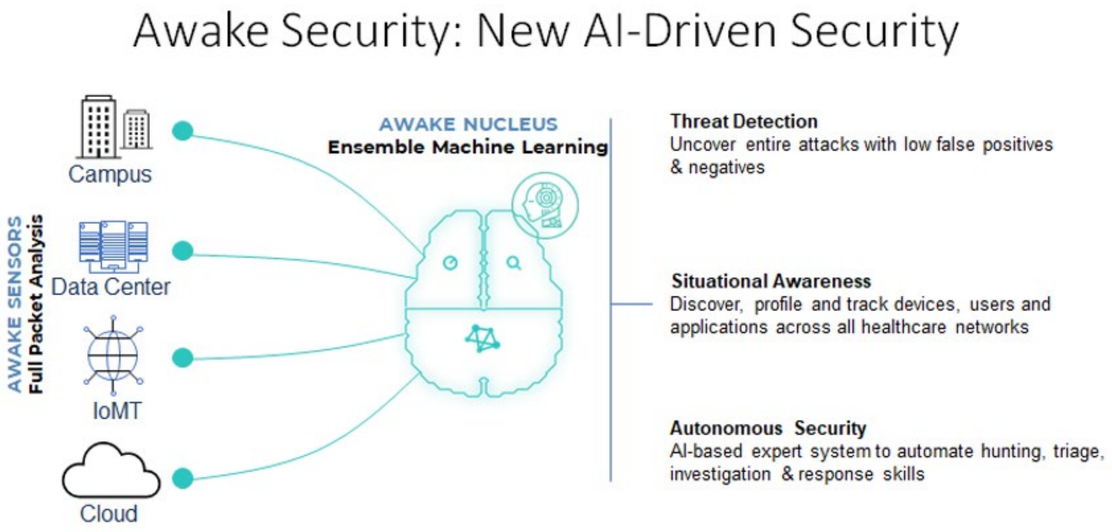
Data protection within hospitals has become increasingly more complicated to address in recent years. While granularly segmenting devices by groups is important to implement access control policies and to contain outbreaks should they occur, detecting mal intent demands more. There could be many motivations for mal-intent including malicious inside users seeking financial gain, harvesting of patient private records,   or even nation-state-driven chaos.   Mechanisms used to exploit the network are highly sophisticated and are therefore no longer discoverable by traditional malware detection mechanisms.

Arista's experience shows that in many organizations, upwards of 50% and sometimes even 70% of devices are unmanaged, meaning they have no endpoint agent, no log export / aggregation. Clearly a security agent cannot be installed on many IoMT devices that go through certification scrutiny for a specific OS and version of software. Such devices are locked down and adding an agent is not permitted even if technically possible. Another trend we see is that the attacks have evolved where more than 50% of breaches show no trace of malware, yet most existing security tools tend to focus on identifying malware. Attackers are subverting credentials from legitimate users, contractors and applications to then operate as an "insider". Their activity simply blends in with all the "business-justified" activity that is typical for a "normal" healthcare facility. Finally, the increasing use of encryption is impacting the efficacy of traditional network security tools. Gartner estimates upwards of 70% of malicious behavior now hides behind encrypted protocols like TLS / SSL.

Arista NDR helps address these challenges. The platform monitors and analyzes the thousands of IT and IoMT devices that are on today's modern hospital network. Arista uses an artificial intelligence-driven approach to uncover malicious intent whether originating from trusted insiders or external attackers. This approach can mitigate attacks ranging from ransomware to supply chain threats as well as those specifically targeting medical devices.

The Arista solution leverages state of the art AI intelligence technology through a technology called AVA (autonomous virtual assist). AVA augments the existing security team by connecting the dots across time, identifying the devices involved and the behaviors observed. AVA focuses on identifying the underlying condition rather than individual symptoms, thereby saving human analysts from the manual and painstaking effort of triage and diagnosis based on individual and often meaningless security alerts. Instead, AVA provides a decision support system that automatically uncovers the entire scope of an attack along with investigation and remediation options on a single screen.

By monitoring the security of all the systems on the hospital networks, not just those with security agents pre-installed, Arista NDR ensures the devices needed by medical staff are available and operating correctly when needed. And by detecting threats and correlating them to potentially impacted devices in real time, security teams can mitigate the risk and the worst impacts.



Threat Detection
Uncover entire attacks with low false positives & negatives

Situational Awareness
Discover, profile and track devices, users and applications across all healthcare networks

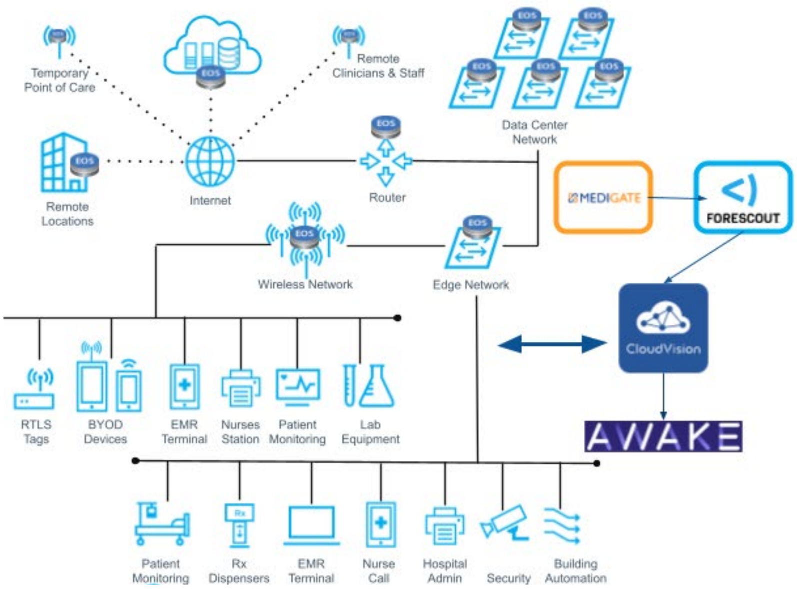
Autonomous Security
AI-based expert system to automate hunting, triage, investigation & response skills

Arista Infrastructure for Zero Trust Secure Networking

In 2008 Arista was launched to revolutionize datacenter network architectures by providing a novel approach to how networks were built. Cloud titans such as Microsoft, Facebook and Google were building large cloud-based networks that required a new level of scale, quality and manageability which was not available from legacy vendors; Arista was founded to meet these requirements. Arista's top priorities continue to be quality, availability, manageability and performance. Delivering a quality, self-healing architecture across a highly agile network is a fundamental requirement for the healthy hospitals. Legacy architectures that merely provide simple redundancy are no longer sufficient for the cloud titan nor is it sufficient for the healthy hospital.

Network availability starts with software. The Arista EOS, Extensible Operating System, software is a single binary that is used on all Arista switches. Other vendors have different software images for each family of products. Each family of products may have a different management system, distinct set of features and even different architectures for redundancy and connectivity. With Arista, all switches use the same binary, are managed by the same management system and have the same baseline feature sets.

Arista leverages EOS to build a single Universal Healthcare Network that spans the hospital to the remote clinics. The fabric includes patients (guests), physicians, administrators, contractors and devices of all kinds. The Universal Healthcare Network provides a single common fabric enabling greater efficiency and availability across the entire infrastructure with security controls that ensure access policy and confidentiality is maintained. It is based on open standards giving administrators the ultimate freedom to choose the best product to meet the hospital's needs. Because Arista uses the same image on all switches, the hospital network administrator only needs to certify a single image of code and can leverage the same design principles at all places in their network. This reduces the cost of operations.



Capacity, Connectivity, and Client Health

- Robust RTLS integration with location applications
- Inventory tracking and management
- Complete client datapath tracking from application to egress
- CBRS support (future)
- Wi-Fi 6e (Future)
- Zero Touch Provisioned RAP
- AI Driven root cause analysis
- AI Driven hitless AP Firmware upgrades

Modern Security Model - Identity, Segmentation & Threat Hunting

- Integration with common identity applications
- End-to-end segmentation, from client to cloud via multi-domain MSS-G
- AI-driven continuous Network Detection & Response for IOT/IOMT and Client Security with Awake
- Uninterrupted WIPS and airspace analysis through 3rd radio

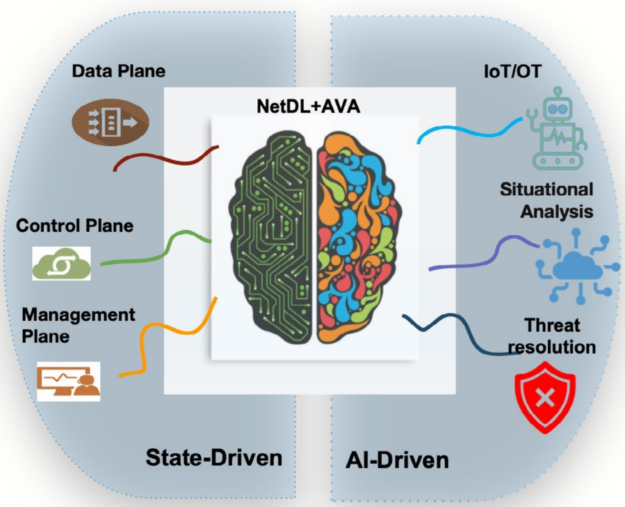
Application Assurance and Connection Quality

- Granular identification of client failures on thousands of endpoints and hundreds of manufacturers
- Multi-level configuration replication for ease of deployment to multiple facilities
- EHR (Epic, Cerner, etc.) application performance assurance and monitoring
- Non-disruptive patching and software upgrades on all devices including single attached edge devices (AP, phone, etc)

The Universal Healthcare Network is managed by a common management solution, Arista CloudVision. The CloudVision solution provides common management and non-disruptive patching. Non disruptive upgrades are a fundamental requirement for an always on network. With CloudVision, new features and patches can be consistently applied from the non-redundant edge switches to redundant spine switches without service disruption. As mentioned earlier, CloudVision provides a wealth of monitoring information to understand connected endpoints, traffic patterns and network telemetry needed for operations and troubleshooting . A healthy hospital must begin with network infrastructure that is always available, resilient and of the highest quality. Arista's quality and architectural approach meets that need and has proved itself in some of the world's largest networks.

Conclusion

The foundation of a healthy hospital is its ability to ensure smooth operations enabling it to deliver quality care; a healthy hospital must provide patient and hospital data security and protect IoMT devices from unauthorized access. Due to the growth of connected IoMT devices that exchange data, hospitals are more than ever susceptible to malicious activities that jeopardizes the patients' health care and privacy. To address this industry problem, a new approach to how hospital networks are built is needed. The new approach needs to provide a reliable and secure infrastructure, visibility into all connected devices, segmentation to control access and continuous monitoring for malicious activities of all kinds. Arista's state and AI-driven approach to a healthy hospital network enables organizations to deliver highly reliable and resilient services that ultimately improve outcomes for patients and healthcare professionals.



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