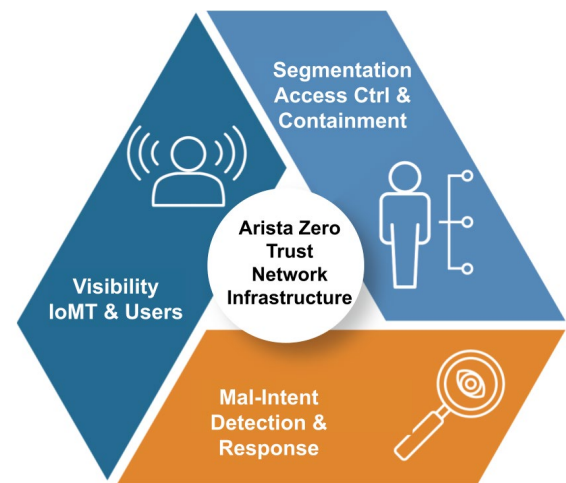


# Tenets of a Healthy Hospital Infrastructure

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 needs to be architected to 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 and need to be controlled. The hospital network needs to be ubiquitous . . . pervasive, readily available, and in unlimited capacity.

In this paper we discuss the four basic tenets all hospital designers must incorporate in their healthy hospital architecture:

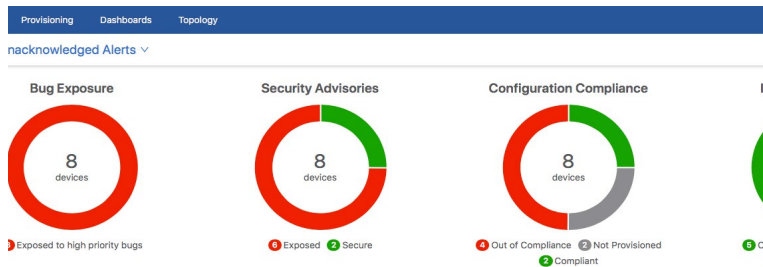
- Visibility of connected IoMT and Users
- Segmentation for Access Control and Containment
- Detection and Response of Mal-Intent
- Arista Infrastructure for Zero Trust Secure Networking

## Visibility of Connected IoMT and Users

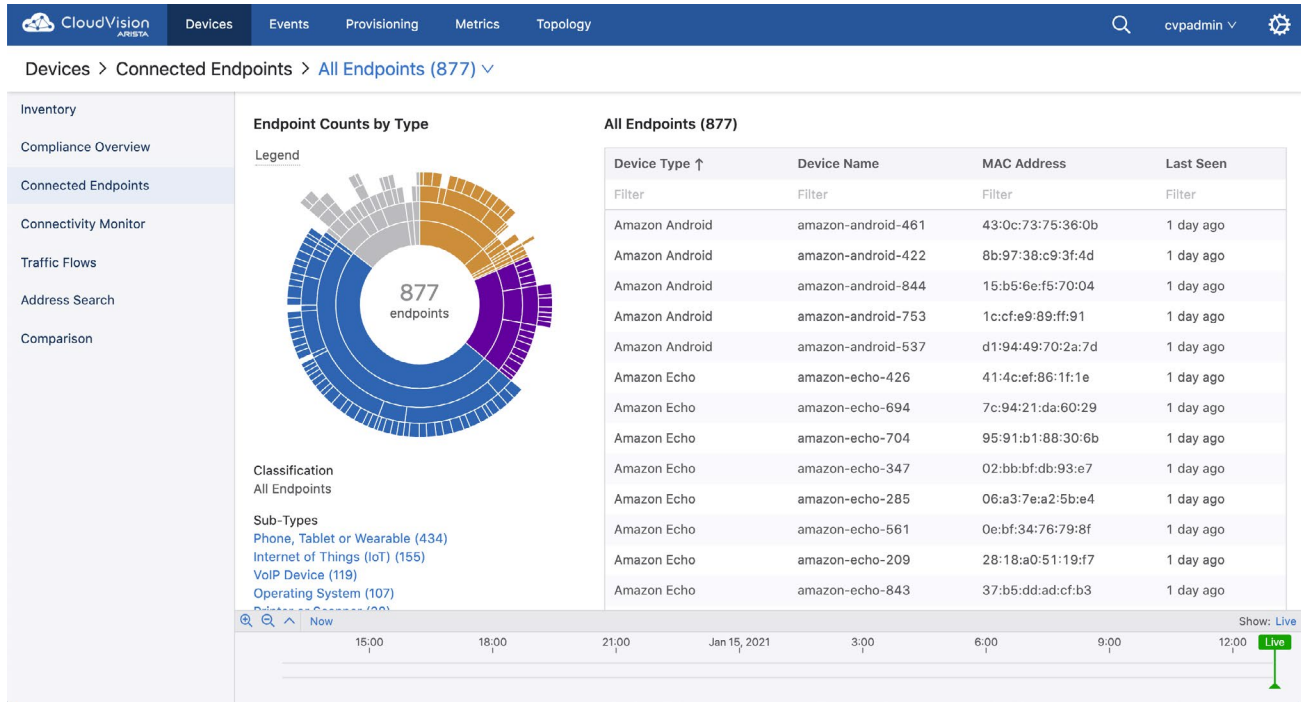
Securing a healthy hospital begins with visibility of all connected resources - IoMT, IoT, users and network infrastructure. Each resource may have state that could include things like software version, location, time/date, observed behavior, device analytics and more. Visibility with network infrastructure 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 is used to build 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, has established strategic partnerships with other vendors and pursues open standards to ensure interoperability.

## Arista CloudVision for Network Infrastructure Visibility

The Arista CloudVision and Awake security platform 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.

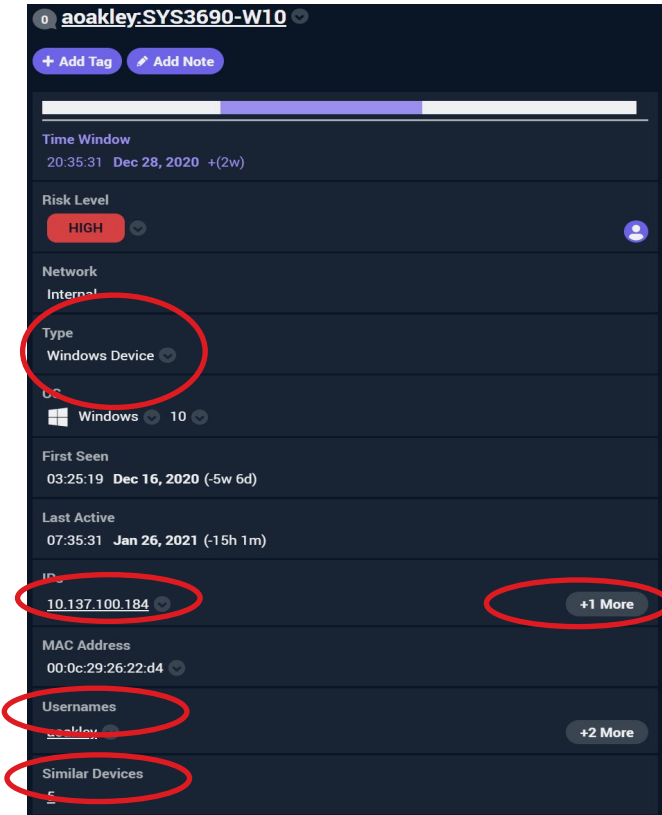


The CloudVision Device Analyzer feature identifies and classifies all connected endpoints. Flow records showing who is talking to whom along with packet data showing the volume of traffic is provided.

### Arista Awake EntityIQ for Visibility

Arista Awake 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 is able to determine the device is a Windows 10 device, used primarily by aakley and has had three different IP addresses in the recent past.

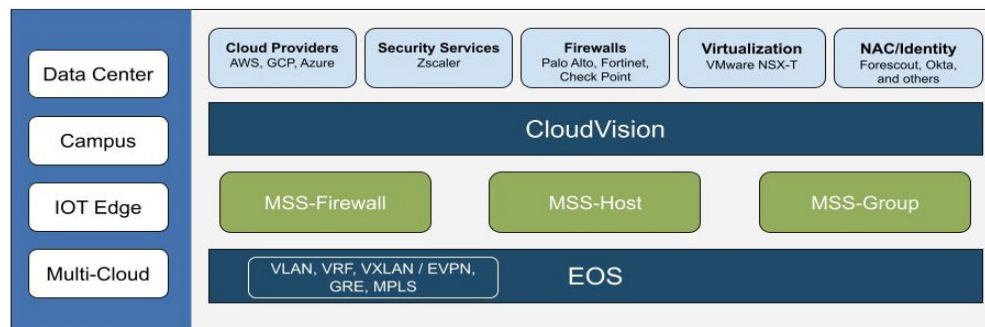


### Third Party Integration for Visibility

CloudVision integrates with all the leading NAC providers. For example, when integrated with Forescout, network visibility is extended to include granular telemetry on IoT 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 for which they are entitled to access. 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

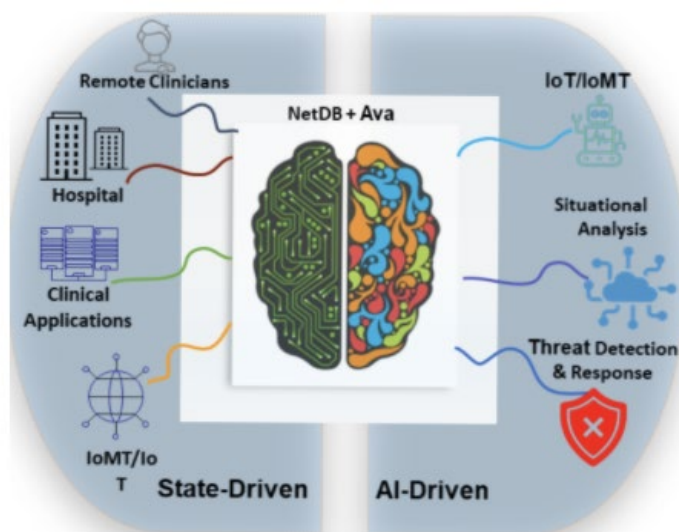
To meet the emerging segmentation requirements mandated by many healthy hospital and campus networks, Arista invented a new approach called MSS-Group (Group Based Macro Segmentation Services). MSS-Group provides several benefits including: segmented groups can be created independent of a device's IP address or subnet, it works with switching equipment from other vendors and is simple to implement and operate. No longer does an administrator need 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 allowed to communicate with each other as that is how malware is sometimes spread. The Arista MSS-Group method was designed to solve such problems.

### 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, more is needed to detect mal-intent. There could be many motivations for mal-intent including malicious inside users seeking financial gain, harvesting of patient private records, or even nation-state chaos. Mechanisms used to exploit the network are highly sophisticated and are no longer restricted to traditional malware direction mechanisms.

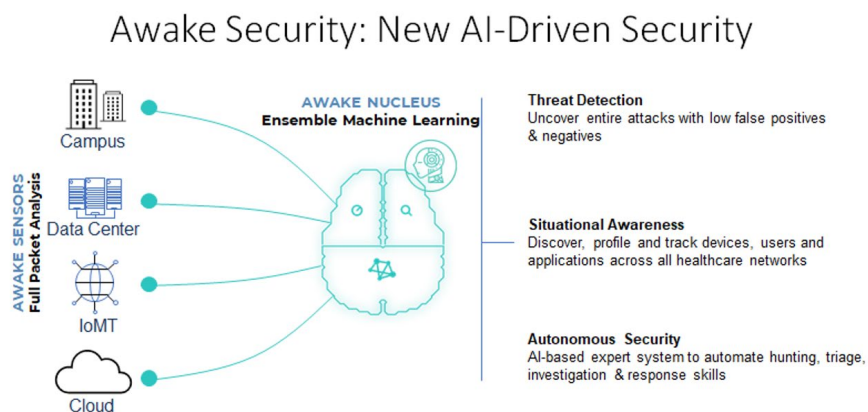
Arista's experience shows that in many organizations, upwards of 50% and sometimes even 70%, devices are unmanaged, meaning they have no endpoint agent, no log export / aggregation. Clearly a security agent cannot be installed on many IoMT devices that go through certification scrutiny for a specific 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's Awake Security Platform is designed precisely to help address these challenges. The Awake Security Platform monitors and analyzes the thousands of IT and IoMT devices that are on today's modern hospital network. Awake 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 Awake solution leverages state of the art AI intelligence technology through a technology called Ava. 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.



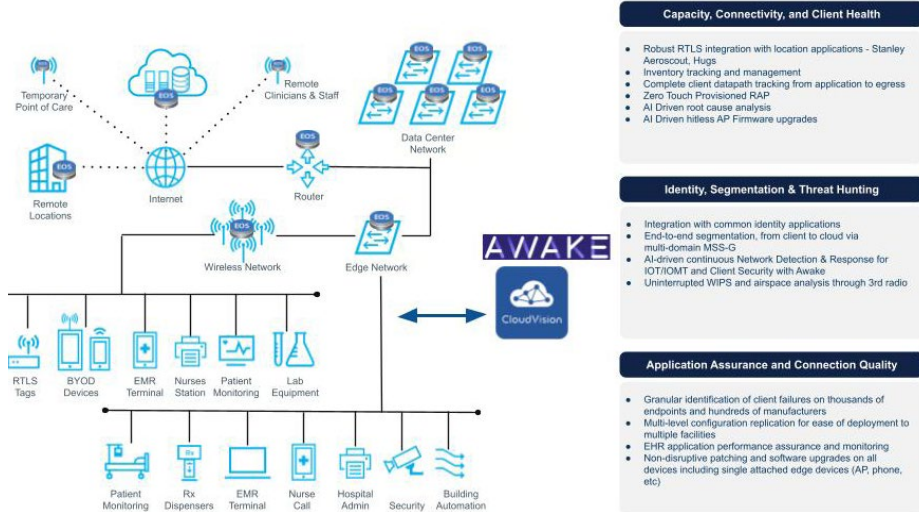
By monitoring the security of all the systems on the hospital networks, not just those with security agents pre-installed, Awake ensures the devices needed by medical staff are available and operating correctly when needed. And by detecting threats and correlating them to potentially impacted devices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

#### Arista Infrastructure for Zero Trust Secure Networking

In 2008 Arista was launched to revolutionize datacenter network architectures by providing a new 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, different 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 greatly reduces the cost of operations.



- Capacity, Connectivity, and Client Health**
  - Robust RTLS integration with location applications - Stanley Aeroscout, Hugs
  - Inventory tracking and management
  - Complete client datapath tracking from application to egress
  - Zero Touch Provisioned RAP
  - AI Driven root cause analysis
  - AI Driven hitless AP Firmware upgrades
- Identify, Segmentation & Threat Hunting**
  - Integration with common identity applications
  - End-to-end segmentation, from client to cloud via multi-domain MSS-C
  - 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 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 a network infrastructure that is always available and of the highest quality. Arista’s quality and architectural approach is designed to meet that need and has been proven by engineers building 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 control access and continuous monitoring for malicious activities of all kinds.

#### 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



Copyright © 2021 Arista Networks, Inc. All rights reserved. CloudVision, and EOS are registered trademarks and Arista Networks is a trademark of Arista Networks, Inc. All other company names are trademarks of their respective holders. Information in this document is subject to change without notice. Certain features may not yet be available. Arista Networks, Inc. assumes no responsibility for any errors that may appear in this document. 08/21