Arista-Medigate
Securing Your Connected Care Devices

Executive Summary

The broad innovation and adoption of connected care devices across many healthcare departments has created challenges within their IT organizations. Undeniably these connected devices improve patient care as well as being a key cornerstone for artificial intelligence. Yet these devices need guardrails as left unmanaged connected care devices create cybersecurity risks. IT's role is to protect their community from malicious attacks, while not interfering in the care and treatment of patients, especially with devices that can improve care.

As IT departments can no longer mandate or control the adoption of these devices as there are too many to review ahead of time, they require watchdog solutions that can discover, assess and take action in real time as departments attach these devices within the IT network infrastructure. This requires identity management, authorization, and network access control technologies.

Specifically, healthcare IT departments require Endpoint Detection and Response (EDR) solutions coupled with their network infrastructures, where detection, authorization, and mitigation are fully automated as a combined ecosystem. The network performs the remediation actions such as isolating rogue devices, allowing IoT devices to only communicate with their application provider, and/or resolving communication problems related to authentication or other network related issues.

Arista Networks, a premier provider of campus, wireless and network security infrastructures has integrated their network infrastructure and control offerings, with the Claroty's Medigate healthcare endpoint discovery, inventory, detection platform. By coupling Arista and Medigate offerings together, healthcare organizations have an underlying infrastructure where they can securely attach wired and wireless connected care devices to their networks without the risk of security breaches.

Connected Healthcare Devices

Healthcare has become a connected ecosystem where doctors, patients, staff, and suppliers interact across their wired and wireless networks, leveraging data from laptops, ipads, connected healthcare (Extended Internet of Things XIoT) devices, and a growing number of related applications. Many of these devices are forwarding highly sensitive data that need to be secure within well-defined communities of interests. These communities of interest are facilitated by the network, leveraging secure segment technologies (VLANs, VXLANs, VPN tunnels etc.). This connected ecosystem enhances care as medical teams get faster results, with deeper analytics when compared to antiquated "paper" results.

The number of XIoT devices is increasing exponentially based upon bio medical innovations. Much of the adoption is being driven by open networking standards including those that are wireless (Wi-Fi, 5G, Bluetooth, and smart Ethernet "plugs"). Wireless technologies facilitate mobility, especially for hospitals and urgent care facilities where the staff freely moves their devices around, while wired Ethernet is well suited for imaging, and scanning devices where there are dedicated rooms, and fixed devices.

As healthcare organizations serve the public within their buildings, they require networks that can fully isolate the patient and their family connections from the internal provider care network, all running across the same Wi-Fi access points and/or wired Ethernet switches. Communication between these two communities is handled at the firewall, application server, or demarcation edge router. An endpoint detection and response (EDR) solution detects unauthorized devices on the internal healthcare network, whether it is hacked in through an access point, or connected to an open Ethernet port in a room where the CT scanners and MRI machines are located. And the network takes action on preventing the proliferation of an attack beyond the entry point into the network.

If unauthorized device protection is not present, the consequences could be dire, especially where a rogue device could issue commands and prompt an authorized device to act in a malicious way. Malicious activities include data privacy breaches, and in worst case scenarios, ransomware, where the staff becomes locked out of their applications, or data is stolen and they have to "buy" the data back.

Determining which devices are authorized is one of the bigger challenges as most healthcare organizations have 100s of device types that are being used by their staff. These include PCs, laptops, Ipads, mobile phones, scanners, monitors etc across many suppliers and operating systems, coupled with speciality XIoT devices. What separates authorized devices from unauthorized devices is agent, authentication, and network access control, where the user and device are prompted for their network and application credentials, while simultaneously running background checks on the device they are authenticating on.

To keep up with the rate of smart device innovations, healthcare organizations need an authentication, authorization, and inspection solution as they cannot certify every device attached to their networks. In short many connected care devices require a network centric infrastructure solution, where they are authorized as they connect to the network.

Claroty Healthcare Addresses Healthcare Cybersecurity with The Medigate Platform

The Medigate Platform is modeled around the healthcare industry, for assessing and advancing healthcare cybersecurity within Healthcare Delivery Organizations (HDOs). Medigate powers a mature ecosystem and prioritizes the sequencing where devices are discovered, located, profiled, classified, and authorized.

The Medigate Platform can discover all classes of unauthorized devices (rogue, valid yet first time discovered etc) and migrate these over fully authorized categories based upon their asset visibility, coupled with customer inputted policies. To effectively mediate different device states, integration with the network infrastructure is required, as the network offers the control point for controlling communication behaviors.

The Medigate Platform eliminates inaccurate and manual tracking of device attributes by automating the discovery and monitoring process in order to get a complete understanding of device status, changes, and usage–resulting in more efficient and effective management across your healthcare environment.

- Device utilization metrics: Full visibility into XIoT devices and understanding of their overall device utilization, location, and efficiency.
- Comprehensive inventory device management: Identify, track, and automatically assign management of change (MoC) workflow items to specific team members based on group or device ownership.
- Track and maintain device lifecycles: Advanced report creation, scheduling, and automatic run-and-send capabilities enable stakeholder communication through the Medigate Platform.

Below summarizes many of the Medigate Platform capabilities.

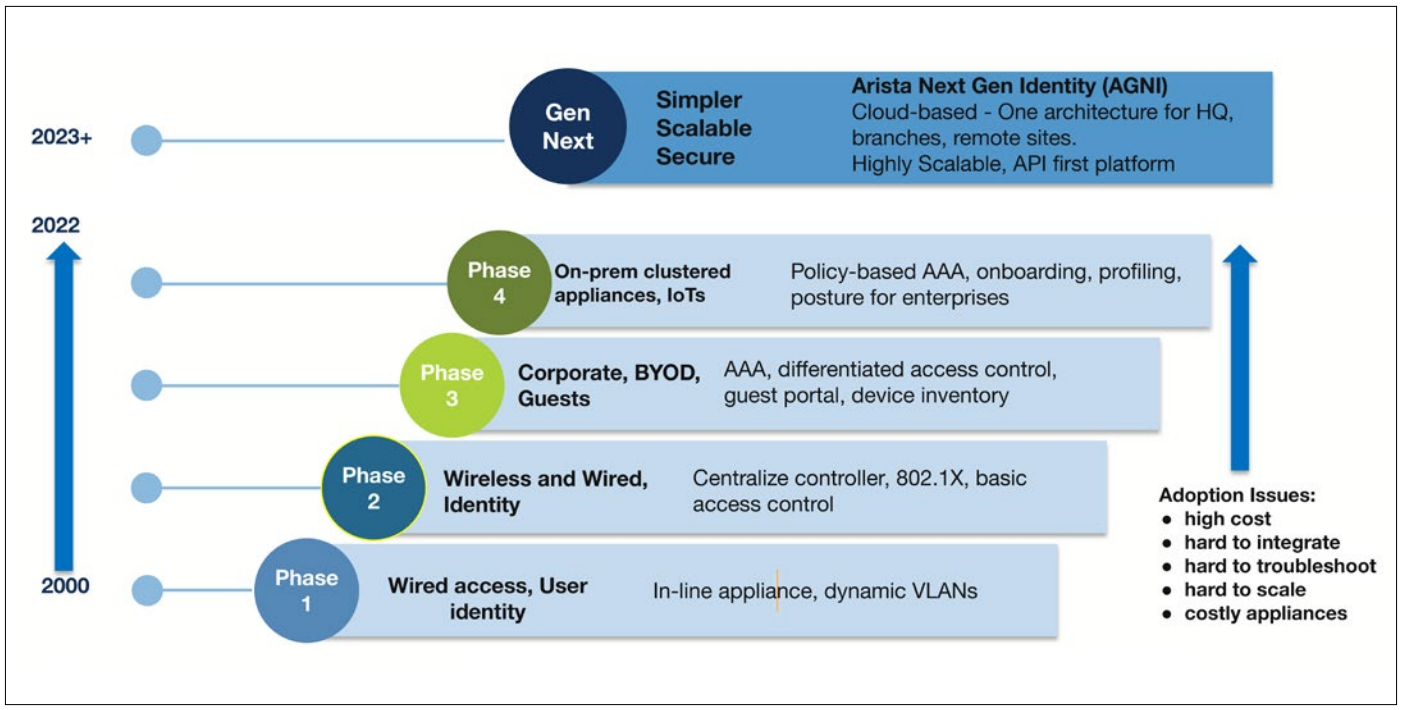
	Medigate Platform Essentials	Medigate Platform Advanced Modules
Visibility & Insights	As the foundation of the Medigate Platform, this functionality provides complete visibility into your device inventory with multiple, distinct discovery methods–backed by the broadest and deepest library of medical device and IoT protocols in the industry. The result is unparalleled accuracy with granular device profiles including information like serial numbers, firmware versions, OS, nested devices, and more.	
Anomaly & Threat Detection	Robust, customizable threat detection engine based on behavioral baselining and anomaly detection with MITRE ATT&CK for ICS alerts mapping	Enhanced threat detection capabilities that include signature-based detection for known threats, custom communication alerts to further monitor and alert on unique device behavior, and additional uses for the MITRE ATT&CK for ICS matrix.
Vulnerability & Risk Management	Comprehensive vulnerability & risk identification and assessment capabilities based on multiple sources of intelligence, proprietary risk profiling, individual MDS² forms, and endpoint management integrations	End-to-end vulnerability & risk management including network-wide recommendation and prioritization features, risk simulation, complete MDS² directory, and vulnerability scanning integrations. This module enables HDOs to take more impactful and efficient risk reduction measures at the network-level.
Network Security Management	Device communication mapping and visualization through a communication matrix and world map view of external connections, setting the foundation for network segmentation and integrations with networking infrastructure.	Provides recommended communication policies that can be customized, monitored, optimized, and enforced through Firewall and NAC integrations. This module is essential for environments looking for a programmatic approach to network security who wish to adhere to Clinical Zero-Trust practices
Clinical Device Efficiency	Operational intelligence on devices including utilization activity, device location and mapping through integrations, and end-of-life information	This module provides users with the ability to monitor, benchmark, and optimize device usage across their healthcare network in order to maximize operational value and achieve increased ROI

Network Access Control

Network Access Control (NAC) solutions, as offered by network infrastructure vendors including Arista control access of both authorized and unauthorized devices and are therefore mission critical for data privacy and security protection. Simply stated, NAC provides authentication & authorization of any device connecting to the network.

NAC is a well known technology, with over 20 years of innovation and maturity. There are many well known standards, protocols and procedures. This drives interoperability where healthcare organizations can deploy complete end-to-end solutions, or choose between different NAC solution offerings depending on their feature and hosting requirements. As of 2023, many healthcare IT teams are leaning towards newer cloud offerings as these eliminate the need for in house appliances, operations teams, and software license agreements. These newer cloud-based NAC solutions interoperate with multi-vendor network infrastructures.

The below shows the evolution of NAC offerings:



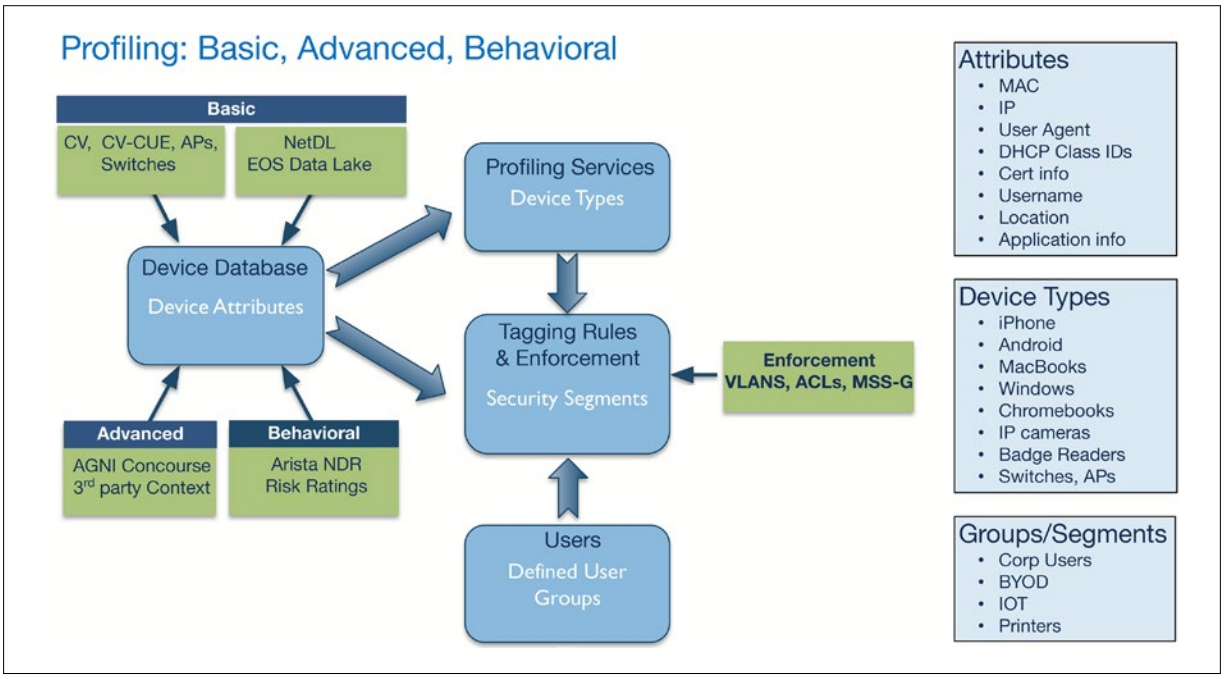
Evolution of NAC Requirements

Most NAC applications provide real-time device information as they interact within the control plane, where endpoints are constantly refreshing their connections. Further, NAC has the ability to apply policies based upon device, user and application profiles. As examples, these policies range from fully trusted devices that have access to secure network segments, to guest services where they can only access public data, to full denial of services for highly suspicious devices. Virtual networks, access control lists, Wi-Fi ssid's, port controls, and firewalls are just several of the ways the network can control endpoints.

Unlike general purpose PCs, laptops, and phones, medical devices (XIot) require specialized identity and authorization intelligence as they have closed operating systems, and specialized hardware that is unique within healthcare. General purpose NAC solutions do not recognize or work with these specialized devices. This results in less NAC control and security mitigation when natively integrating with healthcare devices.

Arista Guardian for Network Identity

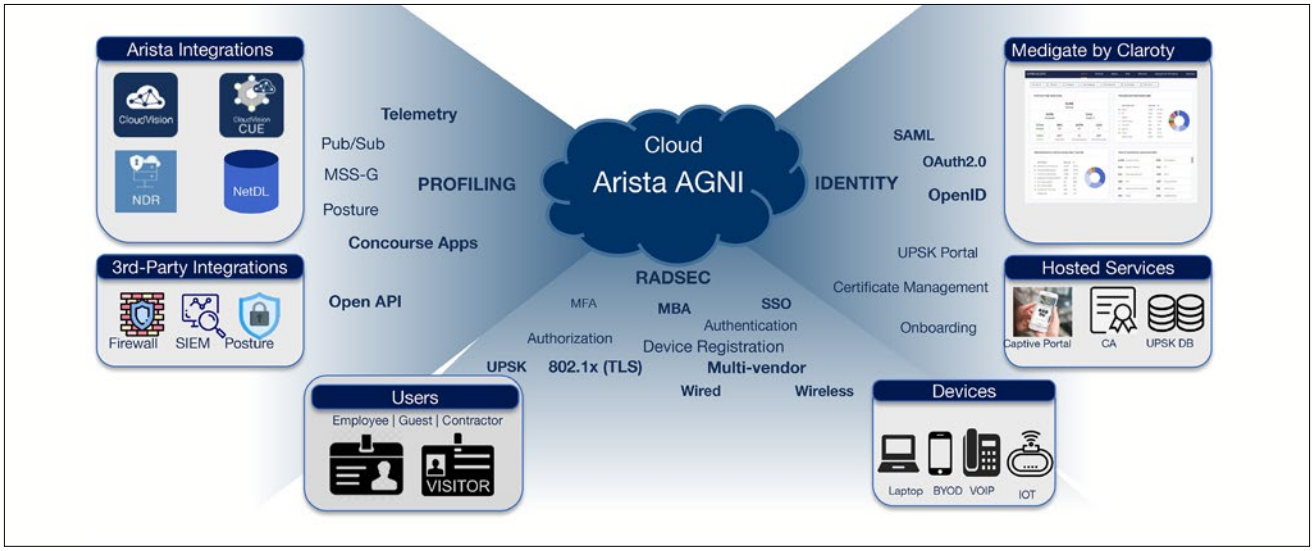
Arista's Guardian for Network Identity (AGNI), next generation cloud offering solution addresses many of the pre 2022 NAC shortcomings with ease of adoption, open ecosystem endpoint identity ecosystem integration, lower cost of ownership, and zero trust network segmentation intelligence. Where many of these pre 2022 NAC offerings were brittle, where the number of trouble tickets they created outweighed the benefits, AGNI focuses on quality, and usability to ensure successful adoption.



AGNI Device Visibility

Arista & Medigate: Proactive Cybersecurity Protection

As healthcare organizations need the combination of an EDR (endpoint) and NAC (network) to fully secure their connected devices, Medigate and Arista have developed an integrated solution. Organizations can now leverage the cloud, by coupling Arista's Guardian Network Identity infrastructure with Medigate's capabilities in determining who is authorized or not. This determination triggers network access control policies including segmentation, access control, and remediation actions.



Arista and Medigate Integration

The joint solution combines the strengths of both the AGNI and Medigate platforms. AGNI provides industry-leading access control capabilities, enforcing highly customizable access policies and facilitating swift action against unsafe devices. Medigate powers AGNI with its detailed understanding of medical devices and their protocols to create more accurate device profiles, enabling deeper visibility into all connected medical devices and more granular access policies.

Additionally, the joint solution utilizes information obtained through AGNI to detect anomalous behavior and trigger alerts that can be converted to active actions in the network, executed by AGNI. AGNI & Medigate together achieves the goal to ensure that security is integrated into the fabric of clinical workflows --not just devices.

Additional Resources

Network Access Control Overview: **NAC**

AGNI Solution Brief: **AGNI Solution Brief**

AGNI Datasheet: **AGNI Datasheet**

Medigate Platform Solution Overview: **Solution Overview**

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

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

Copyright © 2024 Arista Networks, Inc. All rights reserved. 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. February 20, 2024