Network Segmentation and Clinical Policy Enforcement

THE PROBLEM

A hospital has a typical clinical network, secured by standard security practices. It has many connected medical and Internet of Things (IoT) devices, along with standard IT equipment, organized into VLANs assigned to buildings and floors. It has up-to-date NAC and firewalls in all relevant network locations, and the security team recently implemented a general-purpose IoT solution to properly manage their increasing number of connected devices. The CISO recognizes their current tools are insufficient for containing security threats that may arise from compromised medical devices. In particular, the hospital's ultrasound devices are concerning, in light of recently published operating system vulnerabilities and outdated application versions.

1. **Limited visibility** - While the hospital uses a number of connected medical and IoT devices, many remain unidentified by current security solutions. It is impossible to set security policies or define a dedicated VLAN for ***unidentified*** devices.

2. **No clinical expertise** - The general-purpose security software and policies do not cover all ultrasound devices. The number of detected devices simply does not match the CMMS inventory registries. Even those which are detected can lack essential technical details, such as their serial numbers, manufacturer, model, operating system, and app version.

3. **Geographic segmentation** - Currently, most ultrasound devices are not identified in the network, so out of convenience, the network is segmented into VLANs according to buildings and floors with ultrasound devices spread between them. This is clearly not beneficial for managing them and containing potential threats. Ideally, the ultrasound devices would be set into a single VLAN, or at least included with other radiology devices.

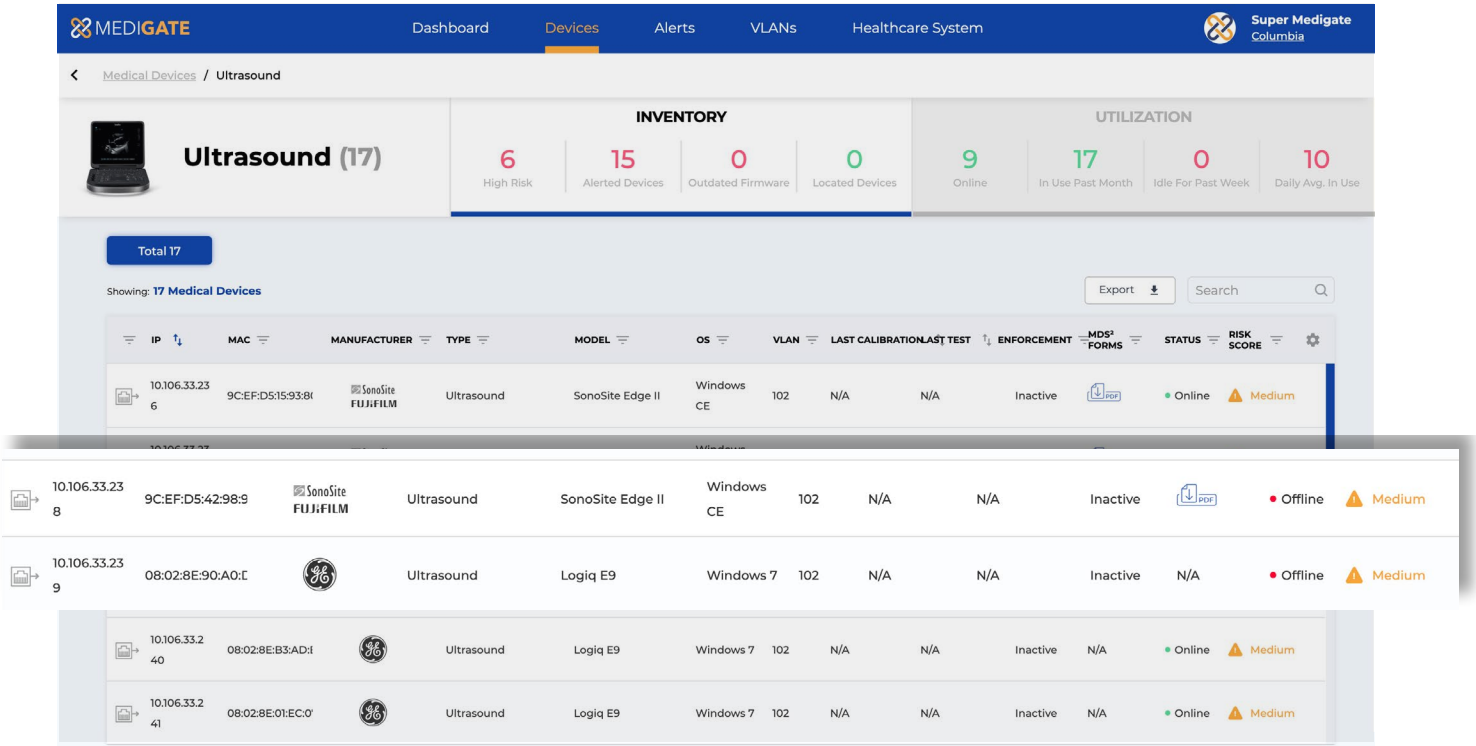
4. **Manual processes** - Due to the lack of visibility and cumbersome integrations between different security platforms, the security team currently spends valuable time and money manually defining NAC and firewall policies. They cannot define precise policies for the ultrasound devices without granular visibility and behavioral profiles.

THE SOLUTION

Installing Medigate in the network addresses these challenges head-on by providing granular visibility into all devices across the hospital, including ultrasound machines. This enables the hospital to quickly and easily contain all ultrasound devices within a dedicated VLAN, and identify out-of-order behavior. Medigate's platform also integrates with the existing NAC and firewalls, leveraging the hospital's infrastructure to enforce the clinical policies now made possible by the detailed device data.

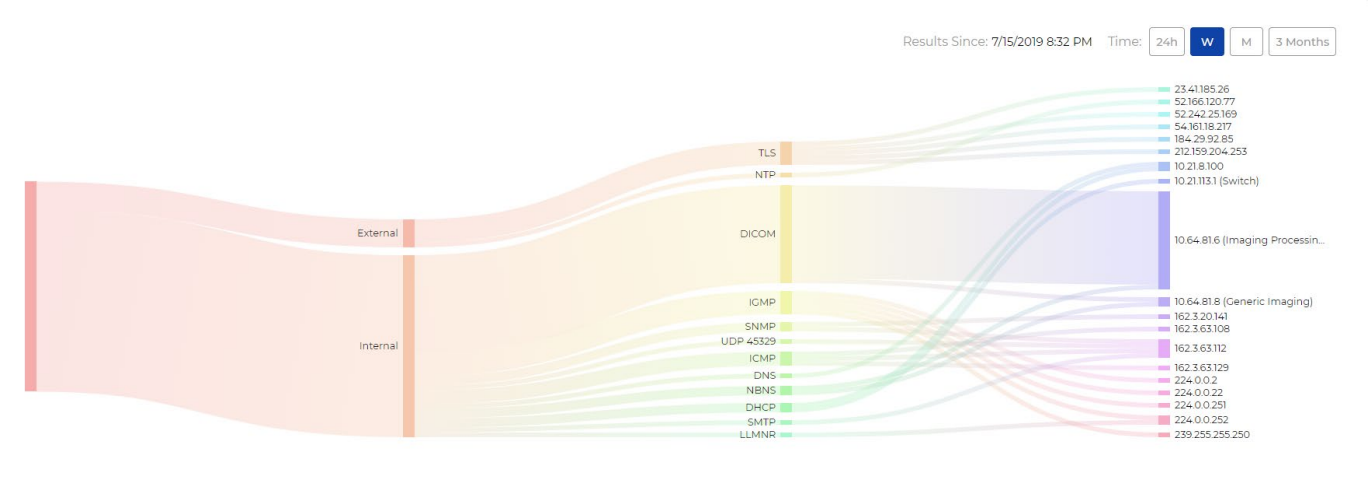
This is how it looks step-by-step:

1. **The hospital can identify 100% of its ultrasound devices with Medigate's DPI capabilities.**
   Medigate uses Deep Packet Inspection (DPI) on passively-collected network traffic to discover all ultrasound devices in the clinical network and obtain granular identifications for each device, including manufacturer, model, OS, app versions, AE title and hardware versions. It also extracts location data from communications in the DICOM protocol and from other IT services in the network. This enables the hospital to identify all ultrasound devices at risk. Medigate's DPI techniques are based on a deep understanding of medical communication protocols and workflows, enabling more effective device discovery then probabilistic approaches, such as those driven by AI or Machine Learning (ML).



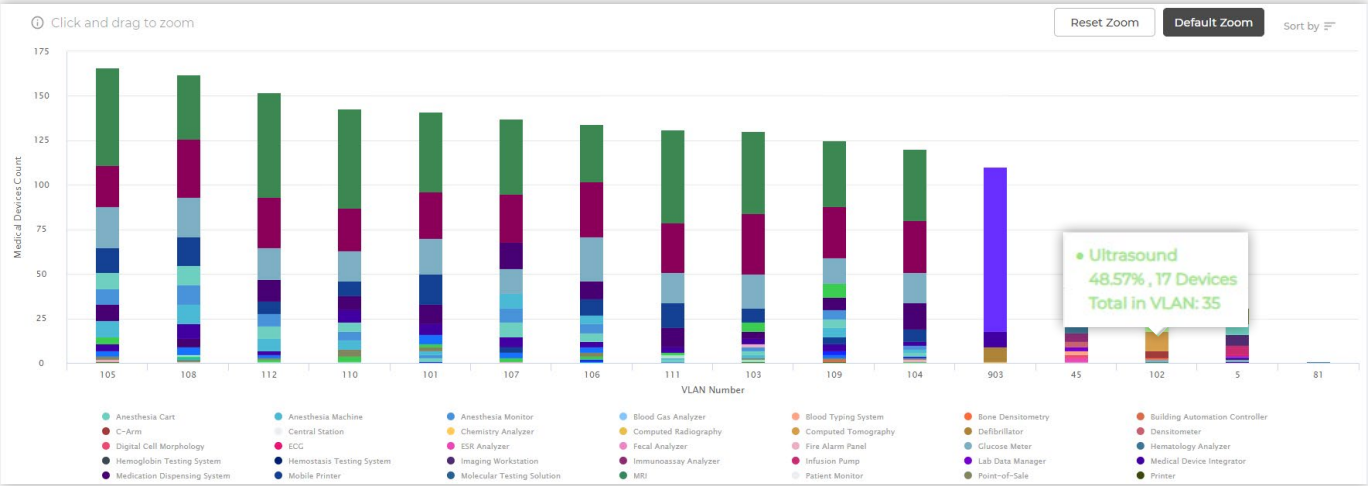
2. The hospital has context around the devices' network communication.

The Medigate platform understands the ultrasound devices' protocols and manufacturer-intended protocols so it can detect malicious or out-of-order behavior, based on the passively-collected network traffic. Medigate maps all internal and external communications of the ultrasound devices, categorizes it by protocol and destination, and marks any suspicious activity.



3. The hospital can create a segmentation plan based on device type or functionality.

After identifying all existing devices and presenting how they are currently organized into VLANs or virtual security groups, the hospital can effectively and efficiently define segmentation policies for all ultrasound devices. In collaboration with Medigate researchers, the security team can now more safely segment the entire network based on device type or functionality.



4. **The hospital can build clinically-driven security policies for NAC and firewall enforcement.** Medigate devises clinically-driven policies in line with the hospital's compliance requirements and best-practice standards to ensure the ultrasound devices cannot compromise the network. Enforcement is done automatically for all ultrasound devices via integration with the hospital's existing NAC and firewalls. Medigate attaches custom tags with the discovered technical attributes to the device, so NACs and firewalls can enforce policies. Without Medigate's precise device identification, it is highly unlikely to enforce a correct and strict policy without affecting the device's functionality. Medigate allows the hospital to leverage their existing policy enforcement infrastructure and make it much more effective in the clinical setting.

		Source	Destination				
	Name	Address	Address	Application	Service	Action	Options
1	Ultrasound devices to PACS allow	Medical Devices - Ultrasound	Servers - PACS	dicom	application-default	Allow	
2	Ultrasound devices general deny	Medical Devices - Ultrasound	Servers - PACS	any	any	Deny	

The hospital's clinical network protection strategy is no longer limited by its general-purpose security solution and manual processes. With Medigate, they now have granular visibility into all devices, contextually-driven anomaly detection, functionally-based segmentation, and automatic, clinically driven rule-based security policies - all integrated seamlessly into their existing security and CMMS platforms. In essence, they have true segmentation made simple.