Why NACS Alone Are Not Enough

Clinical networks, like any other mission-critical network, require high security standards. Network Access Control (NAC) products are a central part of a comprehensive security solution, ensuring authorized access to network resources by users and devices. Like in many other industries, healthcare organizations need to manage authorization levels for users and devices, control authentication processes and manage use of network resources. NACs provide real-time information about connected endpoints, and the ability to set dedicated access policies and take action against suspicious devices and activities.

However, clinical environments need more security.

First, because medical devices are inherently not designed to be network-managed, NACs are not able to present detailed information on many connected devices, resulting in highly limited network visibility. Further, for a similar reason, NACs cannot perform posture enforcement on medical devices, e.g. verifying updated software versions.

Second, setting efficient access policies for medical devices through NACs require an intimate understanding of clinical workflows, device functionality, numerous vendors and proprietary protocols. Only such understanding can allow administrators to create granular policies and access rules.

Third, while NACs enable preventative actions such as device quarantining, it requires clear triggers as to when and why take such action. These triggers require detailed device profiling and behavior analytics that NACs alone cannot offer.

On top of their limited security capabilities, NACs also operate actively to support their visibility capacities, which may be hazardous in a clinical environment. NACs may actively scan a device to identify it better, potentially leading to compliance issues with manufacturers' policies. In contrast, Medigate's device discovery and identification process yields more information while remaining entirely passive.

The Solution

Medigate provides the industry's first and leading dedicated medical device security platform. Only Medigate fuses the knowledge and understanding of medical workflow and device identity and protocols with the expertise to address today's cybersecurity threats to provide full visibility of connected medical devices and analyze network traffic to detect anomalous behavior.

Use Case: False NAC Identifications

NACs identify the connected device's vendor based primarily on the MAC address of their network adapters. However, many medical devices vendors use network adapters produced by a different vendor. Consequently, they are falsely identified by NACs according to their network adapter vendor, rather than their true vendor. In contrast, Medigate's appliance analyzes each device's communication protocol using DPI techniques, yielding more accurate and more informative device identifications, integrated into the ISE dashboard.

Medigate's platform performs three primary roles:

Visibility

Superior visibility and discovery throughout the clinical network by fingerprinting all connected medical devices to the level of make and model using deep packet inspection (DPI) techniques, allowing dynamic medical device inventory management. This knowledge base is then leveraged to calculate a device's risk score, integrated with medical devices standards and clinical parameters, to inform risk assessment activities.

Detection

Identifying network anomalies specific to the healthcare sector and using them to provide real-time alerts about cyberattacks and pertinent network events. This contextual approach meticulously analyses network communication and medical workflow patterns to ensure highly credible identification of attacks in real time while minimizing instances of false positives.

Prevention

Leveraging the intelligence gathered by the visibility and detection layers in conjunction with existing traditional security solutions enables to actively prevent security threats posed by medical devices. Medigate's platform can allow organizations gain more from their NAC solutions by enforcing more accurate and granular access policies, respond to highly accurate alerts of suspicious device behavior and facilitate more efficient network zone allocation (ACLs, VLANs, etc.).

Forescout CounterACT Comparison Matrix

General

Capability	Medigate	Forescout CounterACT	Medigate Added Value
Analyze a medical device's designated protocols and network protocols	Yes	No	Medically-based threat detection
Deployment time	Short	Long	Adding Medigate's appliance to an existing Forescout infrastructure is fast and simple.
Deployment complexity	Simple	Complex	

Visibility

Capability	Medigate	Forescout CounterACT	Medigate Added Value
Analyze a medical device's designated protocols and network protocols	Yes	No	Medically-based threat detection
Identify connected medical devices and provide detailed device information (make, model, OS, VLAN, port, etc.)	Strong	Weak	More detailed medical devices identifications
Display medical device application versions and flag patching alerts	Yes	No	More detailed medical devices identifications
Identify connected IT devices and display standard IT application versions and flag patching alerts	No	Yes	Manage both standard IT and medical devices
Discover medical devices behind serial adapter or gateway	Yes	No	Enhanced device network discovery capabilities
Present granular real-time medical device inventory status	Strong	Weak	More detailed medical devices identifications
Present historical data (network activity, IP history) of device behavior over time	Yes	Yes	A larger variety and granularity of historical data for medical devices

MEDIGATE

Detection

Capability	Medigate	Forescout CounterACT	Medigate Added Value
Network-based anomaly detection	Yes	No	Network detection abilities yielding a comprehensive security solution
Clinically-based anomaly detection	Yes	No	Ability to detect deviations from devices' intended use, e.g. protocol usage, network connections, and external communications
Present historical alerts data for security review	Yes	No	Ability to track devices' behavior over time
Generate dedicated medical devices risk score based on medical devices standards, clinical parameters and more	Yes	No	Enhanced understanding of device risks contributing to more informed security processes

Prevention

Capability	Medigate	Forescout CounterACT	Medigate Added Value
Facilitates desirable security practices based on network analysis	Yes	No	Informative medical device identification and anomaly detection enables improved security practices.
Enforce access policies for device and user profiles	No	Yes	More accurate and granular access policies
Quarantine devices or limit access to specific VLANs or network resources	No	Yes	Network traffic analysis generates highly accurate alerts of suspicious device activity
Assign devices to specific network zones (ACLs, VLANs, etc.)	No	Yes	Medical device identification facilitates more efficient network zone allocation

MEDIGATE

contact@medigate.io
www.medigate.io