MEDIGATE

cisco

AT A GLANCE

Medigate and Cisco ISE Medical NAC

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, in clinical environments, a NAC requires more detailed IoT and IoMT device information.

First, because many IoT and IoMT devices were not designed to be network-managed, NACs are not able to present the necessary detailed information on many connected devices, resulting in highly limited network visibility. Furthermore, for similar reasons, NACs cannot perform posture enforcement on medical devices, e.g. verifying updated software versions. Accurate identification of such devices requires a specialization that NACs struggle to match.

Second, setting efficient access policies for IoT and IoMT devices through NACs require an intimate understanding of clinical workflows, device functionality, as well as numerous vendors and proprietary protocols. only with such understanding can administrators create the granular policies and access rules needed to protect the network.

Third, while NACs enable preventative actions such as limiting a device's network access, they require clear triggers as to when and why they should take such action. These triggers require detailed device profiling and behavior analytics that NACs alone cannot offer.

Finally, NACs operate actively to support their visibility capacities, which may present challenges in a clinical environment. Actively scanning a device to better identify it could potentially lead to compliance issues with manufacturers' policies.

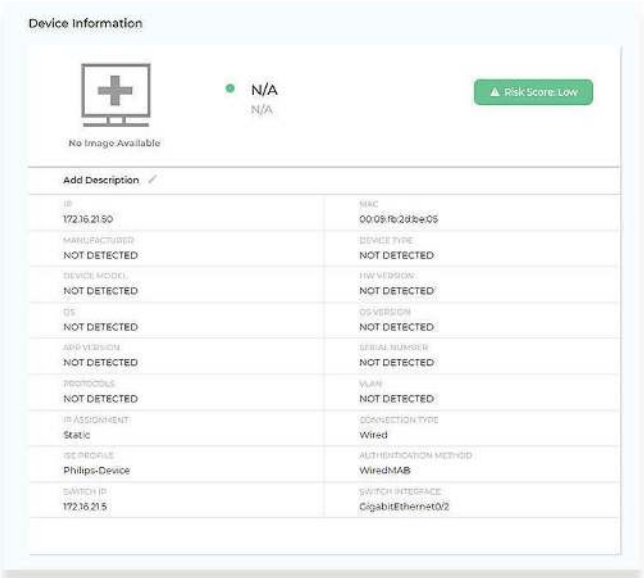
The Solution

Medigate and Cisco have integrated their platforms to provide superior cybersecurity for clinical networks. Organizations can now leverage their existing ISE infrastructure with Medigate's leading identification and profiling capabilities to gain greater visibility into their connected medical devices, benefit from sophisticated network analysis to detect threats, and implement clinically-driven, rule-based policies through the Cisco ISE enforcement mechanisms.

Medigate fuses the knowledge and understanding of medical workflows and device identity and protocols with its networking expertise to provide comprehensive and accurate visibility, contextual anomaly detection, and clinical policy enforcement.

The joint solution combines the strengths of Cisco ISE and Medigate's platform. Cisco ISE provides industry-leading access control capabilities, including granting network visibility of IT devices, enforcing highly customizable access policies and facilitating swift action against unsafe devices. Medigate powers Cisco ISE with its detailed understanding of medical devices and their protocols to create more accurate device profiles, enabling deeper visibility into all connected IoT and IoMT devices and more granular access policies. Additionally, the joint solution utilizes information obtained through the Cisco ISE to detect anomalous behavior out-of-policy or manufacturer-intended workflows. These alerts can drive enforcement activity executed by ISE.

Device information received from Cisco ISE



Updated device information after Medigate's analysis