MEDIGATE

cisco Preferred Solution Partner

Medigate and Cisco™ ISE Joint Security Solution

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, in clinical environments, a NAC requires more detailed medical device information.

First, because medical devices are 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.

Second, setting efficient access policies for medical 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 device quarantining, 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.

In addition, NACs also 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

Cisco ISE with Medigate's industry's first and leading dedicated medical device security platform. Medigate fuses the knowledge and understanding of medical workflow and device identity and protocols with its networking expertise to provide full visibility of connected medical devices as well as analyze network traffic to detect anomalous behavior.

Medigate has partnered with Cisco to integrate its dedicated medical devices security platform with the Cisco® Identity Services Engine (ISE) to provide a more comprehensive access control solution for clinical networks. Organizations can now leverage their existing ISE infrastructure with Medigate's capabilities to gain greater visibility into their connected medical devices, benefit from sophisticated behavior analytics to detect threats, and take immediate action through the Cisco ISE enforcement mechanisms.

The joint solution combines the strengths of both the Cisco ISE and Medigate platforms. 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 medical devices and more granular access policies. Additionally, the joint solution utilizes information obtained through the Cisco ISE to detect anomalous behavior and trigger alerts that can be converted to active actions in the network, executed by ISE.

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.

Comparison Matrix

General

Capability	Medigate	Cisco ISE	Joint Solution Benefit
Analyze medical devices' designated protocols and network protocols	Yes	No	Clinical visibility integrated into ISE
Deployment length	Short	Long	Adding Medigate's appliance to an existing Cisco ISE infrastructure is fast and simple.
Deployment complexity	Simple	Complex	
Authenticate corporate devices on the network	No	Yes	A comprehensive suite of network and security management capabilities
Trigger third-party actions (vulnerability scan, mobile device management onboarding, etc.)	No	Yes	A comprehensive suite of network and security management capabilities

Visibility

Capability	Medigate	Cisco ISE	Joint Solution Benefit
Identify connected medical devices and provide detailed device information (make, model, OS, VLAN, port, etc.)	Strong	Weak	Enhancing Cisco ISE device management capabilities with more detailed medical devices identifications
Display medical device application versions and flag patching alerts	Yes	No	Enhancing Cisco ISE device management capabilities with 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	Real-time device status capabilities with accurate device information
Present historical data (network activity, IP history) of device behavior over time	Yes	Yes	Larger depth and breadth of historical data for medical devices

Detection

Capability	Medigate	Cisco ISE	Joint Solution Benefit
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	Ability to prioritize and manage device risks

Prevention

Capability	Medigate	Cisco ISE	Joint Solution Benefit
Facilitates desirable clinic network security practices based on data analysis	Yes	No	Analysis of medical devices activities generates policy settings executed by Cisco ISE.
Enforce access policies for device and user profiles	No	Yes	More accurate and granular policy enforcement
Quarantine devices or limit access to specific VLANs or network resources	No	Yes	Network traffic analysis generates highly accurate alerts of suspicious device activity, handled by Cisco ISE.
Assign devices to specific network zones (ACLs, VLANs, etc.)	No	Yes	Medical device identification facilitates efficient network zone allocation through Cisco ISE
Automates prevention activities initiated by customized alerts (Optional)	No	Yes	Network analysis triggers preventative actions executed by Cisco ISE, by administrator demand.

How It Works

1. Medigate – ISE Integration

a. Medigate's physical appliance is easily deployed in the network.
b. Medigate's appliance is connected to ISE through Cisco pxGrid (Platform Exchange Grid), a platform that allows data sharing and connectivity between ISE and Cisco Security Technical Alliance solutions.
c. Through pxGrid, Medigate's appliance retrieves the relevant session information to populate its database and sets optimized criteria for on-going data collection.

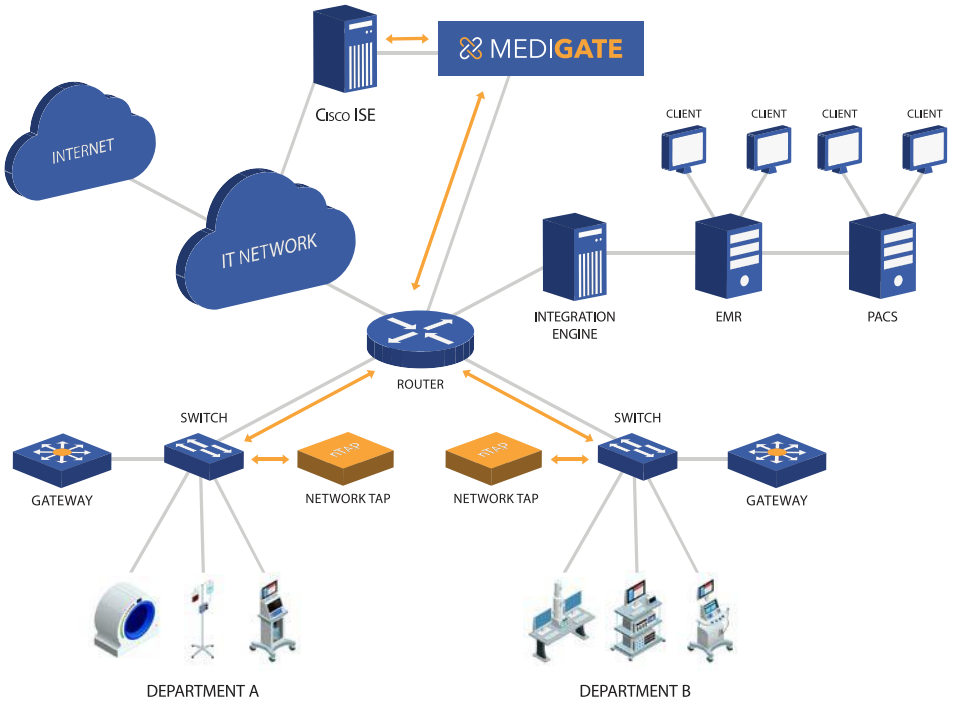
2. Enhanced Network Visibility

a. After collecting network traffic, Medigate discovers and fingerprints connected medical devices using deep packet inspection (DPI) techniques.
b. Medigate's appliance feeds new device identifications into the ISE dashboard, updating its devices inventory with granular device information, thus setting very accurate profiles of devices.
c. Administrators can then create and enforce specific device policies through ISE based on the precise device discovery an identification.

3. Detection and Prevention

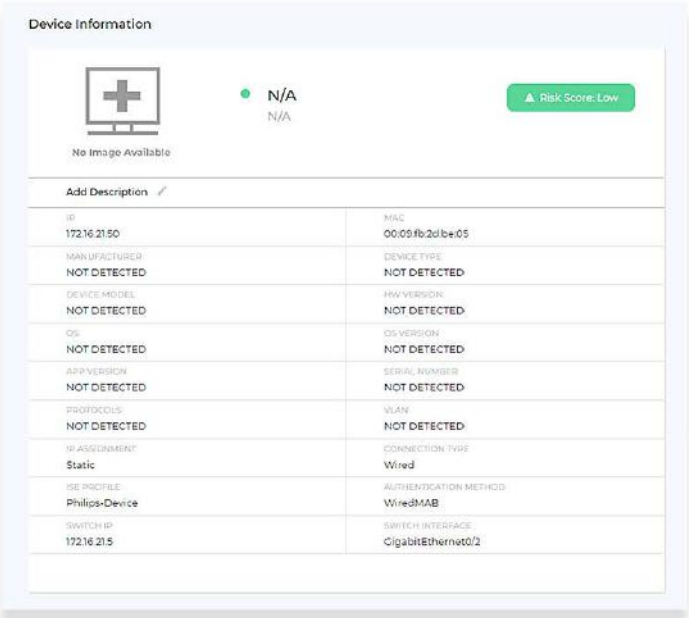
a. Medigate's appliance analyzes network traffic to monitor network behaviors, examining network and device protocols and drawing on clinical understanding of devices' behavior.
b. Medigate's appliance identifies anomalous behaviors and alerts administrators with precise incident information.
c. Administrators can take immediate action against suspicious devices through a variety of ISE mechanisms. Medigate's appliance can also be configured to take automatic action in pre-defined events.

Medigate - Cisco ISE Solution Architecture Example

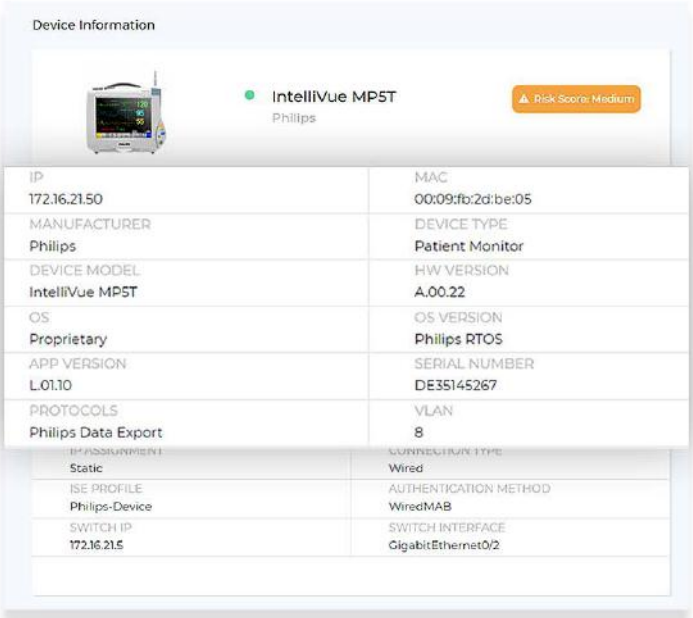


MEDIGATE

Device information received from Cisco ISE



Updated device information after Medigate's analysis



MEDIGATE

contact@medigate.io
www.medigate.io