Medigate and Palo Alto Networks® Integration

A Superior Security Solution for Connected Medical Devices

Medigate and Palo Alto Networks have teamed together to deliver a best-in-class solution that addresses the security risks generated by connecting medical devices to clinical networks.

Features

- Fingerprint connected medical devices with granular detail
- Tag devices to easily set rule-based security policies
- Automated rule-based, clinically-driven security policies

Benefits

- Identify and manage connected medical devices security
- Mitigate security flaws and reduce risk of successful cyberattack
- Prevent infected medical devices from compromising other systems

Securing medical devices is a multi-faceted problem which is why it has proven difficult for the industry to solve.

Protecting the Invisible:

Securing medical devices requires detailed knowledge of each manufacturer and their proprietary protocols, and a comprehensive understanding of medical workflows. Without such knowledge, a security solution cannot accurately identify a device and indicate an out-of-scope activity. The diversity of device types, manufacturers, operating systems, software versions and protocols render standard NAC or firewall solutions inefficient and make achieving full visibility a true challenge. Moreover, many medical devices were not designed to be network-managed and cannot be secured by end-point security solutions, further handicapping traditional security solutions' ability to identify and secure them.

Managing the Undetected:

Equally challenging to fingerprinting connected medical devices, is the clinical domain expertise needed to detect devices' suspicious behavior. Only a deep understanding of both clinically valid workflows and medical device protocols, stemming from meticulous research of device communications, can result in efficient detection of suspicious network behavior of medical devices. Without clinical expertise, security solutions cannot prioritize risks and contribute to providers' risk management plans.

Informed Protection:

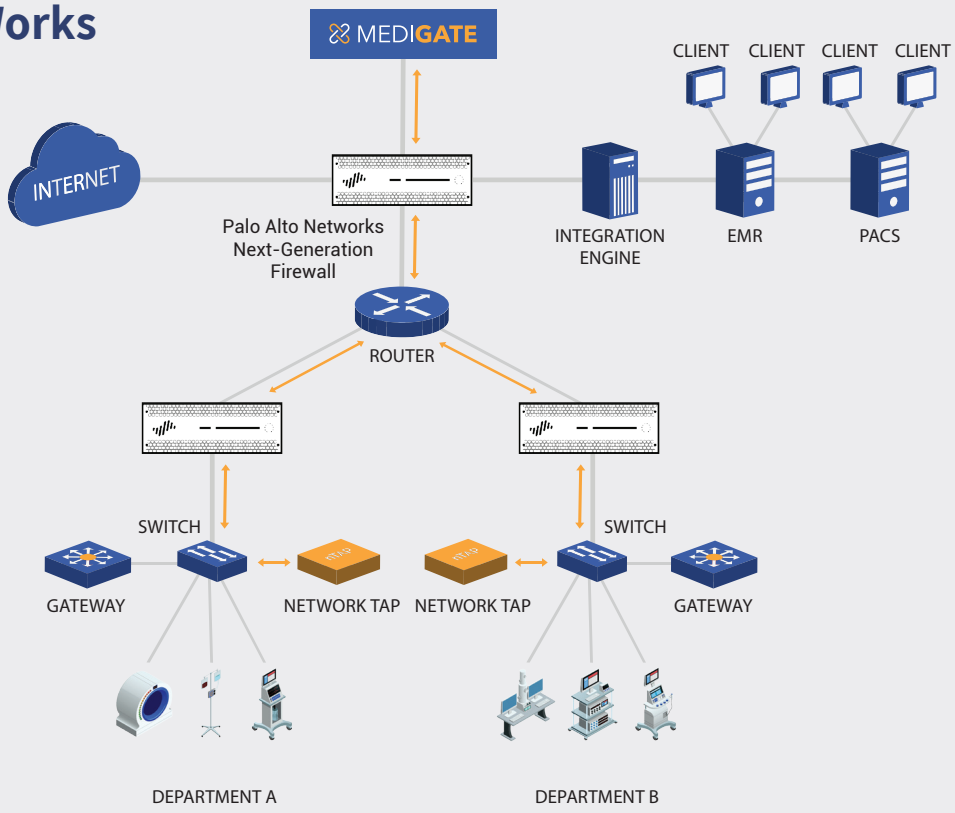
Hospitals rely on firewalls, NACs and generic IoT security solutions to protect their networks. These security solutions are indeed a necessity, but unfortunately, insufficient on their own in dealing with the complexity and diversity of medical devices. By integrating these existing IoT security products with a dedicated medical device security platform that enriching them with accurate device identification and clinical anomaly detection, providers can achieve a well-rounded protection strategy for their networks.

Taking Action Through Integration

Medigate's Medical Device Security Platform and Palo Alto Networks Next-Generation Security Platform share user, device and application information to protect medical devices by only allowing communications designated in the scope defined in the manufacturer's protocol. Coupling Medigate's innovative security solution for the Internet of Medical Things (IoMT) and Palo Alto Networks' proven Next-Generation Firewall (NGFW) capabilities provides healthcare delivery organizations with comprehensive clinical network cybersecurity while leveraging their Palo Alto Networks firewall investment.

Medigate's physical appliance is easily installed and integrated onsite with Palo Alto Networks Next-Generation Firewalls. It then analyzes network traffic, identifies connected medical devices and enriches the Palo Alto Networks firewall to enable efficient, clinically-informed security policies.

How It Works



The process begins with enhanced visibility of all medical devices on the network. Once identified, Medigate's platform matches every device's IP with tags based on its type, vendor and model. It then transfers the tag-to-IP matching to the firewall through Palo Alto Networks API.

> **Medigate's accurate tagging and classification then enable the creation of rule-based, clinically-driven security policies, which only allows approved traffic.**

Additionally, Medigate's platform detects both network and security anomalies, generating alerts for version control, vulnerabilities, security issues, changes, and much more.

Leveraging Medigate's knowledge of clinical domain applications and Palo Alto Networks unparalleled traffic control ability, the integrated solution can automatically create detailed, zero-trust policies based on network communications

The tagging mechanism opens a whole new domain of security policy management capabilities for healthcare providers.

> **Previously, firewall rules had to rely on network zones and IP addresses and ranges. Tagging devices based on functionality and vendor adds new levels of granularity, enabling far more specific policies.**

Furthermore, Medigate monitors changes in devices' network properties such as IP addresses and software versions and incorporates them to update tags continuously.

Medigate's unparalleled clinical domain expertise can be applied by Palo Alto Networks Next Generation Security Platform in four ways:

1

Zone Restriction

Authorize and block access between network zones tailored to device types (e.g. restrict medical device access to Internet zone).

2

Tag-to-Tag Restriction

Authorize connections between specific devices, such as an MRI device and its dedicated imaging server, while blocking all communication out of manufacturer scope.

3

Port Restriction

Leverage Medigate's clinical domain expertise to control a device's authorized ports and enforce only vendor-approved communications.

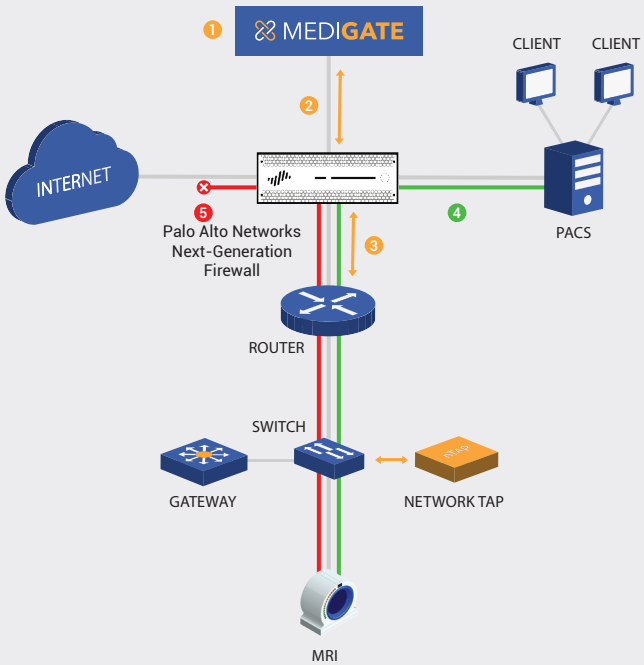
4

Protocol Restriction

Reach the deepest level of network traffic inspection, authorizing only proprietary device protocols and block threatening communication methods.

For example, providers can deny the access of a device tagged as an MRI to the Internet or other network zones in their clinical network. They may also allow it to communicate only with its dedicated imaging server. Moreover, the Port and Protocol Restriction features allows to control not only with which devices the MRI could communicate, but ensure it communicates only in pre-defined ports and proprietary protocols set by the manufacturer. As such, the MRI could communicate with its imaging server in DICOM protocol, while SMB packets will be intercepted.

Exemplary Enforcement Policy Set-up



1. Medigate identifies connected medical devices.
2. Medigate adds type and vendor tags to each device and sends the information to PAN firewall.
3. A security policy is set in the firewall automatically by Medigate to allow the MRI to communicate only with the PACS. Additionally, rules are added to deny communication to the internet.
4. The MRI successfully manages to connect to the PACS.
5. A forbidden connection attempt from the MRI to the internet is blocked.

A Security Solution for Today's Healthcare Cyberthreats

Understanding what's on the network is first step to protecting it. To secure clinical networks require special understanding of medical workflow and unique consideration for identifying, detecting and preventing attacks on medical devices specifically. Medigate's Medical Device Security Platform integrated with Palo Alto Networks Next-Generation Security Platform provides the most effective approach. With integrated core security capabilities and flexible segmentation based on application identification (via App-ID) and user identification (via User-ID), healthcare organizations can support their ever-expanding internet of medical things, effectively mitigate many of the threats facing their devices, all while maintaining the high quality of care patients expect.

Next Step

Contact your local Palo Alto Networks or Medigate sales representative to schedule a demo today and discover how the joint solution can provide a new level of security for your IoMT.

MEDIGATE

paloalto NETWORKS®

About Medigate

Medigate provides the industry's first and leading dedicated medical device security platform, enabling providers to deliver secure, connected care. Only Medigate fuses the knowledge and understanding of medical workflow and device identity and protocols with the reality of today's cybersecurity threats. With Medigate, you can more safely operate all medical devices on your network, enabling you to deploy existing and new devices to patients while ensuring their privacy and safety.

About Palo Alto Networks

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and mobile devices.