MEDIGATE

paloalto NETWORKS

Medical Device Cybersecurity App

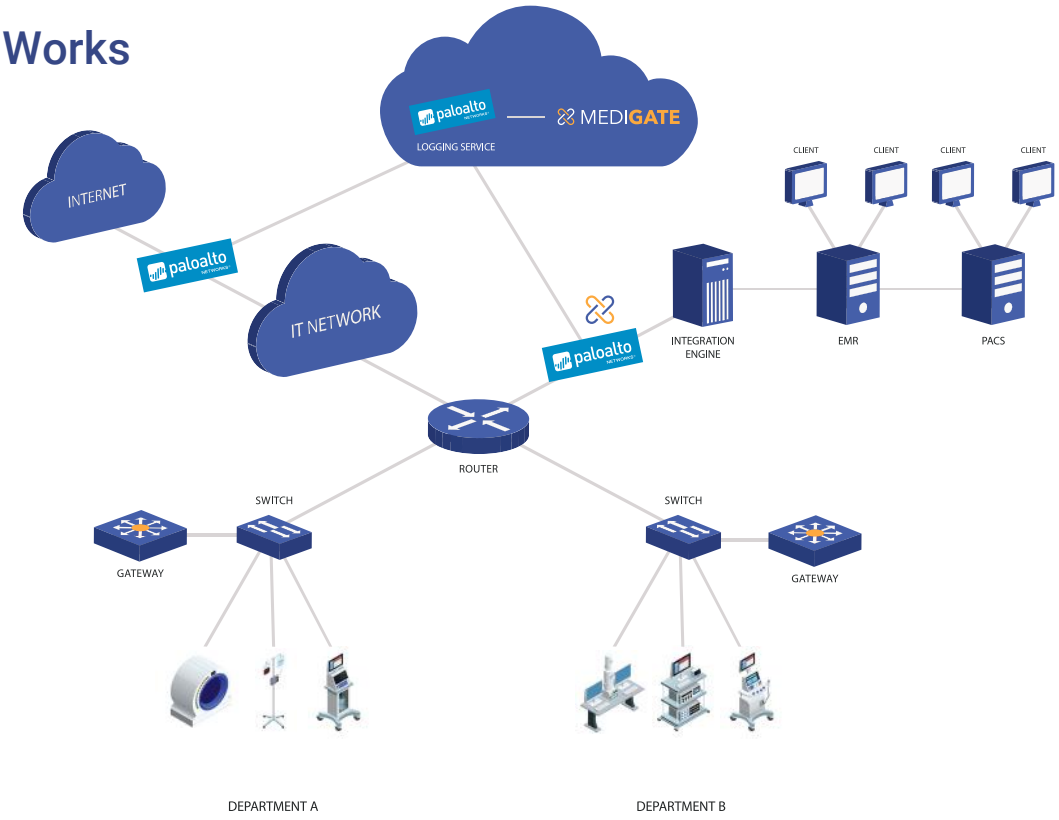
For Palo Alto Networks® Application Framework

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

Medigate's app provides healthcare organizations with full visibility into the medical device inventory connected to their networks, as well as alerts to potential risks. With the capabilities of Medigate's innovative device security platform available via an app for the Palo Alto Networks Application Framework, healthcare organizations benefit from a comprehensive security solution that identifies and secures connected medical devices, while protecting their investment in Palo Alto Networks Next-Generation Firewalls.

The Medigate app utilizes the data provided by the Palo Alto Networks Application Framework to fingerprint medical devices in a clinical environment, safely enable fingerprinted devices via External Dynamic Lists, and correlate data to trigger alerts of suspicious medical device behavior.

How It Works



The process begins with enhanced visibility of all of the medical devices on the network with the custom signature database created for Palo Alto Networks Firewalls by Medigate's platform. Once identified, the devices' communication logs are passed to the Palo Alto Networks Logging Service and onto the Medigate application. Together with the firewall, the Medigate application detects both network and security anomalies, generating alerts for version control, vulnerabilities, security issues, changes, and much more. Finally, MineMeld provides threat intelligence sharing which enables rule-based, research-backed, security policies which allow only approved traffic and forbids any unauthorized communications.

Features & Benefits

Medigate's combined appliance and cloud solution empowers healthcare providers' IT, Security and Biomed personnel through three unique features:

Visibility - Fingerprints connected medical devices using deep packet inspection (DPI) techniques, enabling more informed risk assessment activities and dynamic medical device inventory management.

Detection - Identifies network anomalies and uses 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.

Threat Prevention - Identifies and groups the relevant inter-connected medical devices while allowing enforcement of micro-segmentation security policies within the clinical network. Utilizing reverse engineering of the medical devices' communication protocols, the security platform and Palo Alto Network Firewalls identify and surgically block malicious communication with rules and policies, without affecting the operation and efficacy of the devices.

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 visibility and security for your Internet of Medical Things (IoMT).