MEDIGATE

The Medigate App on Cortex

The Medigate app on Cortex™ provides healthcare organizations with accurate and comprehensive device profiling so you can mitigate malicious behaviors and prevent infected medical devices from compromising other systems.

Medigate's unique clinically-contextual device discovery data and anomaly detection, combined with Cortex's enforcement capabilities, gives hospitals the ability to see and secure everything running on their clinical network, instantly. With a few clicks of the mouse, hospitals can turn on the Medigate application from their NGFW and immediately start seeing what's on their network. Devices have never been more secure and implementing and managing them has never been easier.

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 Cortex Data Lake 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, 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.

Automated Rule-Based, Clinically Driven Security Policies

By providing the Medigate App on Cortex, Zero Trust security is attainable today. The painstaking task of procuring and implementing the right infrastructure to support IoT and IoMT security has also been reduced significantly.

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

Contextual Anomaly 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.

Clinical Policy Enforement - 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.