Vernetzte medizinische Geräte schützen

Medigate – Plattform für die Erkennung und Sicherung von vernetzter Medizintechnik

Medizinische Geräte vom Perfusor über den Patientenmonitor bis zum MRT sind immer öfter vernetzt – man spricht von IoMT (Internet of Medical Things). Doch viele Healthcare-Organisationen verfügen oft nicht einmal über ein komplettes Inventar der vernetzten IoMT-Devices, geschweige denn über detaillierte Kenntnisse von deren Software- und Sicherheitsstatus. Diesem Missstand begegnet das spezialisierte, 2017 von langjährigen Cybersecurity-Experten gegründete und vielfach ausgezeichnete Entwicklerunternehmen Medigate mit seiner gleichnamigen Lösung. Medigate arbeitet auf Basis einer Sensor-Appliance, die für IoMT relevante Informationen aus dem Netzwerkverkehr filtert und zur Analyse weiterleitet. Dies ermöglicht automatisiert eine umfassende Sicherheitsstrategie für den oft schlecht geschützten und nur selten mit Updates versorgten medizintechnischen Gerätepark. Dazu hat Medigate durch eigene Forschung enormes Wissen über die Details der einzelnen Gerätetypen gesammelt, bis hin zu proprietären Protokollen und Firmware-Versionen. Die so gewonnenen Erkenntnisse über die vernetzten Medizingeräte werden auf einer übersichtlichen Web-Konsole in Text und Grafik anschaulich aufbereitet. Medigate ist als offene Plattform konzipiert, versteht sich auf die vorhandenen Geräte und arbeitet mit anderen Cybersecurity-Lösungen und Directory-Services zusammen.

- Erstellt exaktes Inventar aller medizinischen Geräte
- Erkennt Anomalien in der Gerätenutzung und im Datenverkehr
- Unterstützt die Durchsetzung der Sicherheitsrichtlinien
- Verhindert zusammen mit Firewall-Lösungen illegitimen Datenabfluss
- Liefert direkt verwertbare Erkenntnisse über Auslastung der Geräte und weitere Management-Informationen
- Bietet Schnittstellen zu unterschiedlichen Herstellern von NACS, Firewalls, Asset Management, Vulnerability Management, SIEM, IT Monitoring, EMR, IPAM

MEDIGATE by Claroty

Herstellerflyer
Medigate

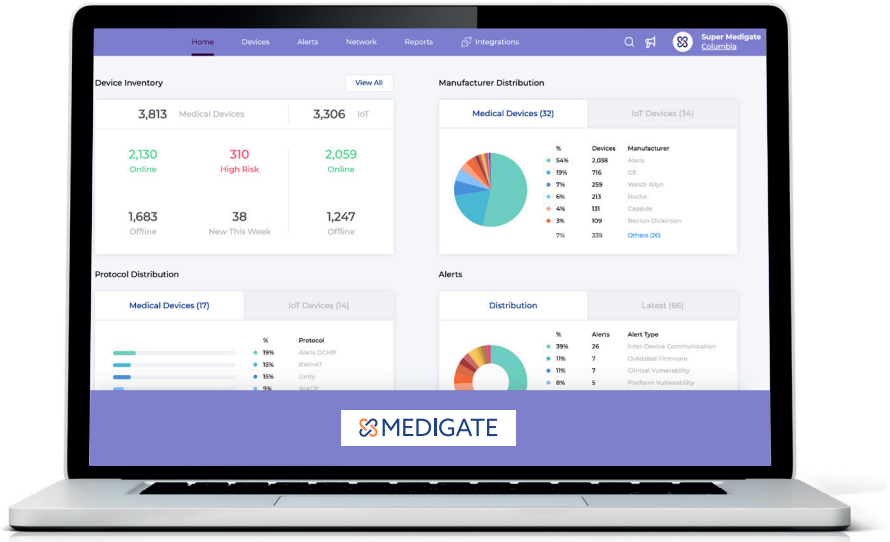
Komplette Visibilität und Sicherheit für den medizinischen Gerätepark

Sichtbarkeit

- Entdeckt und identifiziert jedes vernetzte medizinische Gerät im klinischen Netzwerk
- Basiert auf umfassender Signatur-Datenbank mit «Fingerabdrücken» aller Gerätetypen aufgrund von Deep Packet Inspection
- Erkennt veraltete Firmware/Software-Versionen und Sicherheitslücken
- Informiert über die Auslastung der Geräte
- Präsentiert das Wesentliche auf einen Blick via Web-Konsole
- Bietet Drill-down bis zu den Eigenschaften der einzelnen Geräte

Sicherheit

- Analysiert den IoMT-relevanten Datenstrom
- Kennt die Kommunikationsprotokolle der Geräte – sowohl gängige wie DICOM als auch proprietäre
- Identifiziert atypischen Datenverkehr, anomales Nutzerverhalten und Cyberbedrohungen in Echtzeit
- Verhindert illegitime Datenweitergabe und schützt vor Diebstahl von patientenbezogenen Informationen (PHI Theft)
- Ermöglicht Mikrosegmentation des klinischen Netzwerks und massgeschneiderte Sicherheitsrichtlinien



Integration

- Arbeitet mit bestehenden Firewall-Lösungen zusammen
- Unterstützt Directory-Services wie Active Directory
- Integriert sich mit Maintenance-Management-Systemen (CMMS) und SIEM-Plattformen (Security Information and Event Management)

Komponenten der Plattform

- Sensor-Appliance zum Monitoring des Netzwerkverkehrs
- Cloud-Service oder Analyse-Server On-Premises zur Datenanalyse
- Web-Konsole zur verständlichen Präsentation der Erkenntnisse

BOLL Engineering AG . Jurastrasse 58 / CH-5430 Wettingen / Telefon +41 56 437 60 60 / info@boll.ch / www.boll.ch
BOLL Engineering SA . En Budron H15 / CH-1052 Le Mont-sur-Lausanne / Telefon +41 21 533 01 60 / contact@boll.ch
BOLL Europe GmbH . Ringstrasse 3 / DE-89081 Ulm / Telefon +49 731 85074823 / jwa@boll-europe.com / www.boll-europe.com

BOLL IT Security Distribution