

# Vernetzte medizinische Geräte im Griff

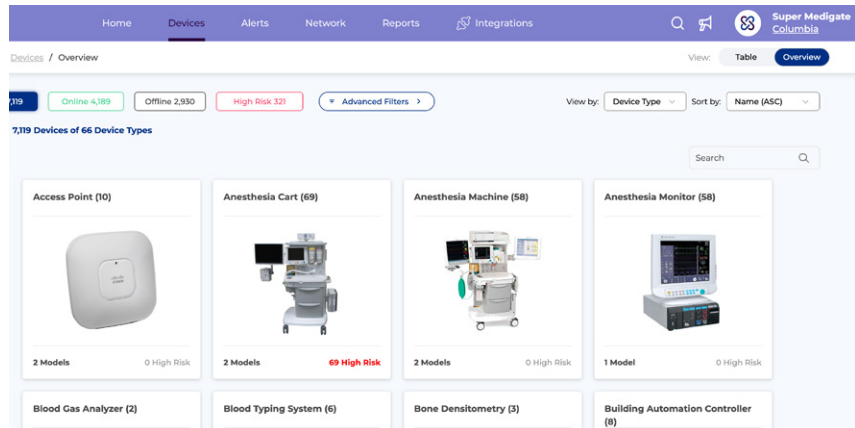
Das Kantonsspital Baselland setzt für Inventarisierung, Überwachung, Schutz und Verwaltung vernetzter medizinischer Geräte auf die innovative Lösung von Medigate.

Immer mehr medizinische Geräte aller Art – vom Patientenmonitor bis zum CT – sind mit den internen Netzwerken der Spitäler oder gar mit dem Internet verbunden. Die Verantwortlichen der Healthcare-Organisationen stehen dabei vor riesigen Herausforderungen. Vielerorts ist nicht bekannt, wie viele und welche vernetzten Geräte vorhanden sind und wo sie genau stehen. Dies ist nicht nur aus Verwaltungssicht ein Problem, sondern steht der Sicherheit und dem Datenschutz diametral entgegen.

Bei manchen Geräten ist die Software womöglich nicht aktuell und es bestehen Sicherheitslücken. Patientendaten können durch Cyberangriffe in unbefugte Hände geraten oder kompromittiert werden. Dies ist kein unrealistisches Szenario: Mehrere Spitäler weltweit wurden bereits von massiven Angriffen in Mitleidenschaft gezogen und Patient Health Information (PHI) zählt bei Hackern zu den gefragtesten Daten überhaupt.

## Lösung für altes Problem gesucht

Das Problem mit der Transparenz im medizinischen Gerätepark und der Sicherheit der IoMT-Devices (Internet of Medical Things) besteht seit dem Aufkommen der ersten medizinischen Geräte mit Netzwerkanschluss. Lange Jahre gab es keine Lösung, die eine übergreifende Sicht auf die IoMT-Landschaft eines Spitals samt all ihren Eigenschaften ermöglichte.



**Medigate ermöglicht automatisiert eine stringente Sicherheitsstrategie für den oft schlecht geschützten und nur selten mit Updates versorgten medizintechnischen Gerätepark.**

Dessen war sich auch das Kantonsspital Baselland (KSBL) bewusst, wie Frank Schilling, Leiter IT Operations und Support am KSBL, schildert: «Wir waren schon lange auf der Suche nach einer Möglichkeit, unsere medizinischen Geräte besser zu verwalten. Welche Geräte sind überhaupt im Netz? Welchen Patch-Stand weisen sie auf? Mit welchen anderen Netzwerkteilnehmern kommunizieren sie und läuft bei der Kommunikation alles ordnungsgemäss? Das sind Fragen, die uns beschäftigen.»

Selbstverständlich führte das KSBL Listen des medizinischen Equipments, aber getrennt

nach Gerätegruppen und durch die Medizininformatiker aufwendig von Hand in Excel-Tabellen zusammengetragen. Je nach Gerätetyp und Abteilung – zum Beispiel Radiologie oder Laborgeräte – waren unterschiedliche Personen für die Erfassung zuständig. Eine automatisierte, stets aktuelle Gesamtübersicht fehlte bisher.

## Medigate tritt in die Lücke

Als langjähriger Kunde von Palo Alto Networks erfuhr das KSBL 2019 von einer Kooperation mit Medigate – und das Interesse war sofort geweckt. «Es gab nun endlich ein Produkt, das sich

## MEDIGATE

### Die Highlights

- Erstellt ein komplettes, 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
- Offene Plattform mit Schnittstellen zu unterschiedlichen Herstellern von NACS, Firewalls, Asset Management, Vulnerability Management, SIEM, IT Monitoring, EMR, IPAM

### Vorteile für das KSBL

- Automatisiertes, vollständiges Inventar ohne manuellen Aufwand
- Sicherheit für die grossen Netzwerke des KSBL
- Unterstützung für zukünftige Digitalisierungsinitiativen



Bild: CandyBox Images / AdobeStock

ganz den Themen Inventar und Sicherheit von IoT-Geräten widmet und die Lücke zwischen IoT und Sicherheit schliesst», erkannte Frank Schilling erleichtert. Mit Unterstützung durch den Partner eternalNet und den Distributor BOLL setzte das IT-Team des KSBL im Herbst 2019 eine Proof-of-Value-Installation der Medigate-Plattform auf. Nach mehrmonatigen Tests mit positiven Erfahrungen entschied sich das Spital im April 2020 definitiv für die Lösung und begann mit der vollständigen Implementierung.

Medigate lieferte zunächst ein komplettes Inventar aller vernetzten Geräte mit detaillierten Informationen zu jedem Device. Dies betrifft nicht nur die Medizintechnik, sondern auch alle anderen IoT-Devices und das IT-Equipment wie PCs, Tablets und Smartphones. Aufgrund des enormen Know-hows von Medigate über die Details medizinischer Geräte bis hin zu proprietären Herstellerprotokollen und Firmware-Versionen liefert die Plattform ein fundiertes Monitoring der medizinischen Gerätelandschaft mit Erkennung anomaler Vorgänge, entsprechende Warnmeldungen sowie aufschlussreiche Analysen, angezeigt auf einer übersichtlichen Webkonsole in Text und Grafik.

Technisch funktioniert die Medigate-Plattform wie folgt: Eine Sensor-Appliance untersucht den Netzwerkverkehr über gespiegelte Switch-Ports, filtert die für IoT relevanten Informationen aus dem Datenstrom und leitet sie an einen Analyseserver weiter. Der Netzwerkverkehr wird also nicht durch Medigate hindurchgeleitet und beeinträchtigt. Es handelt sich um eine rein pas-

sive Überwachung. Im KSBL kommen für Proben und Analysen insgesamt drei Sensor-Appliances zum Einsatz.

**«Medigate hilft uns, die umfangreiche IoT-Landschaft im Griff zu halten. Wir können die Geräte mit unseren Ressourcen optimal und proaktiv managen und so die Sicherheit stark verbessern.»**

*Frank Schilling, Leiter IT Operations und Support, Kantonsspital Baselland*

#### **Zukunftsorientierte Pionierarbeit**

«Die Einführung von Medigate haben wir abgeschlossen», stellt der Leiter IT Operations fest. «Wir wissen nun, was wir haben, und sind daran, weiterführende Massnahmen umzusetzen.» Dazu gehört eine generelle Prüfung, ob alle Geräte in der richtigen Sicherheitszone angemeldet und dort korrekt geschützt sind. Auch der Stand der Firmware-Patches lässt sich für jedes einzelne Gerät leicht ermitteln. «Und wir nehmen genau unter die Lupe, mit wem welche Geräte kommunizieren und ob dabei etwas Verdächtiges passiert.» Es sei wichtig, in solchen Fällen rasch reagieren zu können: «Wir sehen jetzt, ganz im Stil eines Security Operations Center, was genauer untersucht werden muss und wie man Probleme beheben kann.»

Medigate zeigt sich bei Anfragen und Verbesserungsvorschlägen sehr reaktiv, wie Markus

Vögtlin, CEO des KSBL Netzwerk- und Security-Partners eternalNet, feststellt: «Im Lauf des Projekts ergaben sich neue Bedürfnisse, die wir als Feature Request eingereicht haben. Medigate hat immer zugehört, schnell reagiert und unsere Wünsche zeitnah umgesetzt.»

Das Medigate-Projekt am KSBL darf mit Fug und Recht als Pionierleistung bezeichnet werden: Das Kantonsspital Baselland ist das erste Spital in Europa, das auf die Plattform setzt. «Wir legen in der IT-Abteilung höchstes Augenmerk auf die Sicherheit. Dabei verfolgen wir Trends und machen auf publizierte Sicherheitslücken aufmerksam. Der Schutz der Patientendaten ist ein wesentlicher Teil der Security-Strategie», betont Frank Schilling und merkt weiter an: «Medigate ist ein wichtiges Element unserer Digitalisierungsstrategie.»

**Kunde:**  
Kantonsspital Baselland | [www.ksbl.ch](http://www.ksbl.ch)

**Reseller:**  
eternalNet AG | [www.eternalnet.ch](http://www.eternalnet.ch)

**Distributor:**  
BOLL Engineering AG | [www.boll.ch](http://www.boll.ch)

**BOLL**  
IT Security Distribution

Jurastrasse 58  
5430 Wettingen

Tel. 056 437 60 60  
[info@boll.ch](mailto:info@boll.ch)  
[www.boll.ch](http://www.boll.ch)