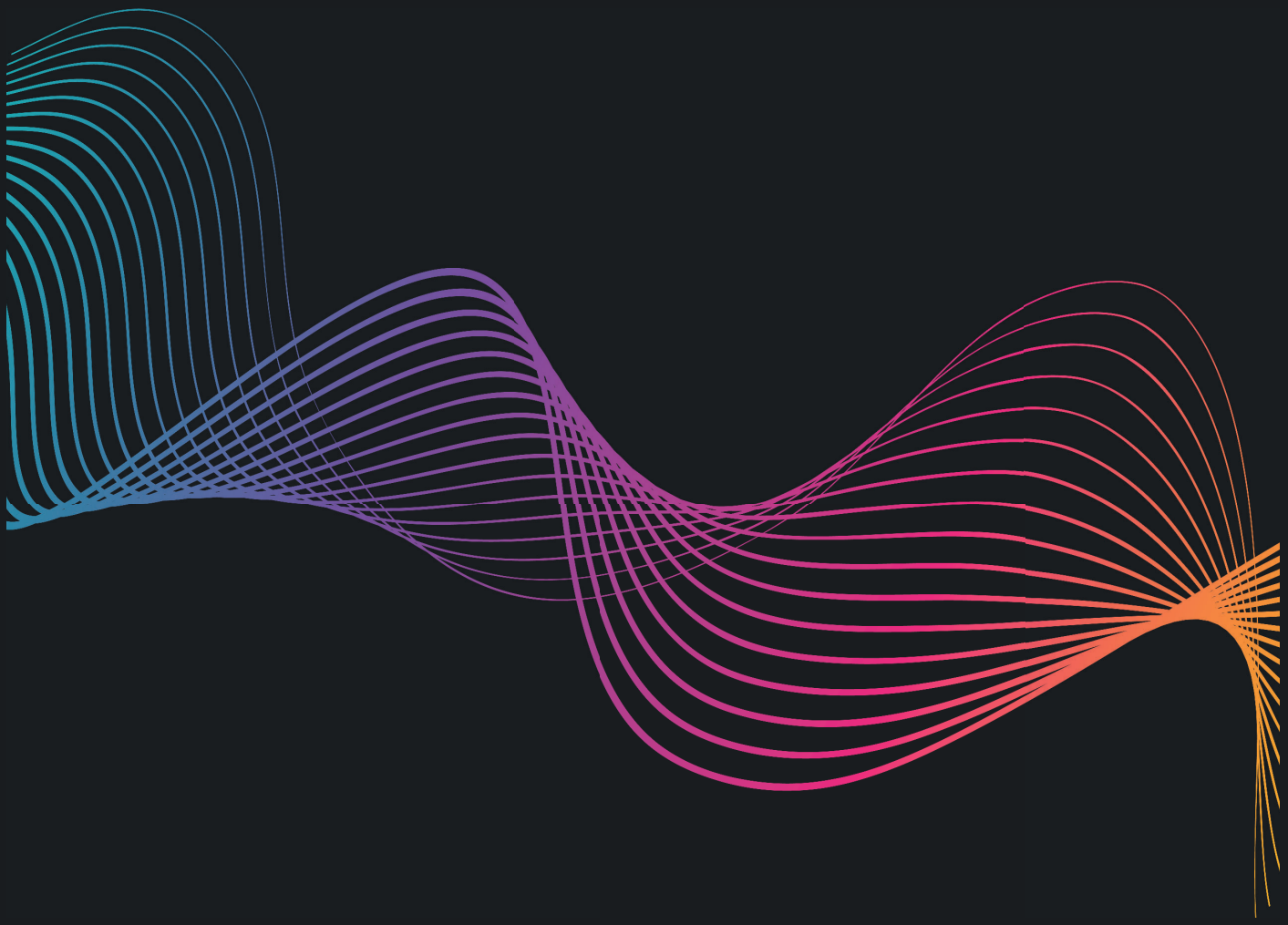
WHITEPAPER

omniIT
INNOVATIVE TECHNOLOGY

OPERATIVER GESUNDHEITSWERT



1.Einführung

In den heutigen vernetzten Unternehmen des Gesundheitswesens haben Geräte, die als Internet of Things (IoT), Internet of Medical Things (IoMT) und Sicherheit für medizinische Geräte klassifiziert sind, die Sicherheitsbranche hinsichtlich der Abdeckung dominiert. Allerdings sind nicht alle medizinischen Geräte hinsichtlich ihres Risikoprofils gleich. Betrachten Sie die folgenden Ökosysteme in Krankenhausumgebungen:

- Geräte, die direkt für die Patientenversorgung eingesetzt werden (z. B. Infusionspumpen, Patientenmonitore)
- Hilfsgeräte zur Unterstützung der Pflege (z. B. Labor, Radiologie, sterile Verarbeitung)
- Betriebstechnologien mit kritischen Auswirkungen (z. B. Rohrpostsysteme, Wasser- und Sauerstoffmanagement, HVAC)
- Kontrollsysteme mit großen Auswirkungen auf den Betrieb (z. B. physische Sicherheit, Alarme, Aufzugskontrollsysteme)

All dies ist ein wesentlicher Bestandteil der „Sicherung der Patientenreise“, doch als Branche haben wir uns schwer getan, den operativen Nutzen von Investitionen in Sicherheitstechnologien nachzuweisen, die Mechanismen zur Verbesserung der klinischen Sicherheit und Qualität bieten.

Armis ist eine Technologieplattform, die Organisationen des Gesundheitswesens dabei unterstützt, einen grundlegenden Ansatz zur Nutzung der Transparenz im Ökosystem der medizinischen Geräte zu verfolgen, um das Risiko der Informationssicherheit einzugrenzen und gleichzeitig die Effizienz der Arbeitsabläufe bei der Pflege zu verbessern und die Auswirkungen auf das Betriebsbudget zu reduzieren.

Um dies zu verdeutlichen, haben wir Anwendungsfälle zusammengestellt, die zeigen, welchen Wert unsere Kunden durch die Investition in die Armis-Plattform für Gerätesicherheit erzielt haben.

2.Klinischer Wert

Inventarverwaltung und -verfolgung

- Erkennen, klassifizieren und verfolgen Sie alle medizinischen Geräte im Bestand
- Identifizierung und Lokalisierung von medizinischen Geräten, die offline sind, um die Kapazität der Patientenversorgung zu erhöhen
- Alarmierung von medizinischen Geräten beim Verlassen der Krankenhausumgebung
- Überwachung des Netzwerkverhaltens auf Frühindikatoren für Fehlfunktionen medizinischer Geräte

Nutzung, die die klinische Wirksamkeit wie Wartezeiten und Patientenzufriedenheit beeinflusst

- Identifizierung von zu wenig und zu viel genutzten medizinischen Geräten, um die Patientenversorgung zu rationalisieren
- Verbessern Sie die Überwachung von Ausfallzeiten und Betriebsproblemen bei den umsatzstärksten Geräten

Verbesserungen bei Sicherheit und Qualität

- Identifizierung von Geräten mit FDA-Rückrufen, die zu Verletzungen oder zum Tod von Patienten führen können

3.Operativer Wert

Kostenmanagement

- Nutzungsberichte und Metriken als Grundlage für Kaufentscheidungen (Leasing oder Kauf)
- Unterstützung des Krankenhausbetriebs bei Finanzprognosen

4.Cybersicherheit und Kontinuität des BetriebsTest Data Management)

Einhaltung der Vorschriften

Audit und Einhaltung von Vorschriften

- Vereinfachte vierteljährliche Berichterstattung für gesetzliche Anforderungen und Rahmenwerke - NIS, PCI-DSS, HIPAA, NIST CSF, FDA
- Erstellung dynamischer Dashboards in Echtzeit, um nicht konforme Geräte zu identifizieren

Schutz der Privatsphäre der Patienten

- Meldung der unverschlüsselten Übermittlung von PHI an interne und nicht genehmigte externe Empfänger

- Erstellung von Sicherheitsrichtlinien für die Exfiltration von Daten

Einhaltung von Sicherheitsrichtlinien und -kontrollen (Sicherheitslückenanalyse)

- Berichte identifizieren Assets, bei denen Sicherheitskontrollen des Unternehmens fehlen, z. B. fehlender Endpunktschutz-Agent, Patching-/Asset-Management-Agent (SCCM). Erhöht die Sicherheitslage und den Schutz vor Cyber-Bedrohungen.

- Durchsetzung des Programms zum Management von Schwachstellen durch verbesserte und regelmäßige Terminplanung

5.Sicherheitsarchitektur und Betrieb

Management von Bedrohungen und Schwachstellen

- Schwachstellenmanagement bei medizinischen Geräten - Identifizierung, Patching-Informationen und Verfolgung der Behebung von Schwachstellen

- Kontextabhängige Risikobewertung in Echtzeit nach Gerätetyp, Rolle, Verhalten und Schwachstellen

Wir sind omniIT

Wir aktivieren Ihre digitale DNA!

Als IT-Dienstleister mit umfassenden Serviceleistungen integriert unser Angebot Themengebiete wie IT-Sicherheit, IT-Infrastruktur, Software-Entwicklung sowie Beratungsprojekte und Managed IT-Services.

Nutzen Sie uns als verlängerten Arm, um Ihre Ziele zeitnah und mit den erwarteten Ergebnissen zu erreichen.

Unser Team setzt sich für den Erfolg nationaler und internationaler Unternehmen – egal ob KMUs oder Konzerne – aus der Technologie, Automobil, Finanz oder Telekommunikationsbranche ein. Wir agieren stets transparent und kommunizieren auf Augenhöhe.

omniIT GmbH
Georg-Hallmaier-Str. 6
81369 München
Telefon +49 89 998 24192 0
E-Mail: info@omniit.de
Web: www.omniit.de
Geschäftsführer: Patryk Wlodarczyk, Marek Chroust

Autoren

Ronny Schubhart
Chief Operations Officer

Ronny Schubhart ist ein anerkannter IT-Sicherheitsexperte, der das gesamte Technologiespektrum abdeckt und die Verknüpfung zur Geschäftsrelevanz von IT-Sicherheit herstellt. Nach seinem Studium der Informatik an der FH Leipzig hat er internationale Erfahrung bei renommierten Unternehmen unter anderem in Italien, Libyen und den USA gesammelt und sich in der komplexen IT-Sicherheit für Finanzdienstleister spezialisiert.