Leitfaden für CISOs
für bessere IoT-Sicherheit im Gesundheitswesen

Zuverlässiger Schutz medizinischer Geräte und sichere Verwaltung von Klinikabläufen in sechs Schritten

Inhalt

Starke Zunahme an IoT-Geräten im Gesundheitswesen

Das IoT leistet neuen Vortrieb im Gesundheitswesen und die Pandemie hat diesen Trend zusätzlich verstärkt.

Das Internet der Dinge (Internet of Things, IoT) bewirkt einschneidende Veränderungen im Gesundheitswesen. Die Nachfrage nach IoT-Geräten für bestimmte Funktionen und Bereiche, wie die Fernüberwachung von Patienten und die Kontaktverfolgung, ist seit Beginn der Pandemie geradezu explosionsartig gestiegen. Doch schon zuvor hatte die IoT-Nutzung im Gesundheitswesen zugenommen.

In den letzten zehn Jahren wurde das IoT immer häufiger für Gesundheitsdienstleistungen eingesetzt. Dazu gehörten unter anderem die Patientenverfolgung und -verwaltung, Ferndiagnosen, die Hygienepflege, die Fernüberwachung und die vorausschauende Instandhaltung medizinischer Geräte.

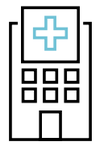
Laut einer Gartner-Analyse von Januar 2020 nutzen 86 Prozent der befragten Gesundheitsdienstleister in den meisten Geschäftsbereichen eine IoT-Lösung.[1] Omdia schätzt, dass 2020 mehr als 250 Millionen medizinische Geräte auf den globalen Markt kamen und bis 2025 weitere 500 Millionen hinzukommen werden.[2]

48 %

der Gesundheitsdienstleister nutzen IoT in umfassenden Bereitstellungen (mehrere Anwendungsfälle und Projekte).[3]

31 %

der Gesundheitsdienstleister nutzen IoT in spezifischen Bereitstellungen (einzelne Anwendungsfälle und Projekte).[4]

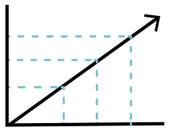


21 Mrd.

IoT-Ausgaben von Gesundheitsdienstleistern im Jahr 2019[5]

54 Mrd.

geschätzte IoT-Ausgaben von Gesundheitsdienstleistern im Jahr 2029[6]



10 %

durchschnittliche jährliche Wachstumsrate (CAGR)[7]

Das Gesundheitswesen hat die Vorteile von IoT erkannt und setzt die neuen Technologien bereits in diversen Bereichen ein. Aber wie gut ist es auf gravierende Sicherheitsprobleme vorbereitet, die dieser Trend nach sich zieht?

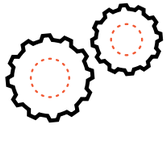
Quellen:

1, 3–4 Gartner Survey Analysis: Healthcare Provider IoT Adoption Is Becoming Mainstream, 2020
2 Omdia, IoT Devices Intelligence, 2020
5–7 Gartner Forecast Analysis: Healthcare Providers IoT Endpoint Electronics and Communications Revenue, Worldwide, 2020

Die Sicherheit ist ein kritischer Schwachpunkt

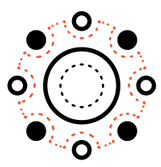
IoMT-Geräte sind erstaunlich schlecht gegen Cyberangriffe geschützt, sodass ein Paradigmenwechsel in Bezug auf die Sicherheitsstrategien notwendig wird.

Das Internet der Dinge revolutioniert zwar das Gesundheitswesen, doch es müssen auch die damit verbundenen Probleme berücksichtigt und behoben werden. Dazu gehört die Sicherheit, die weiterhin eine der größten Hürden für die Einführung von IoT-Geräten ist. Im Gesundheitswesen werden wertvolle Daten verarbeitet. Aus diesem Grund sind die Millionen vernetzten medizinischen Geräte (IoMT), die diese Daten erfassen und speichern, zum strategischen Ziel von Cyberkriminellen geworden. Der Schutz dieser Geräte ist extrem schwierig, sodass sie ähnliche Sicherheitsrisiken darstellen wie die IoT-Geräte.



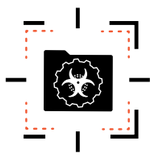
VERALTETE BETRIEBSSYSTEME

IoMT-Geräte nutzen häufig veraltete Betriebssysteme und viele waren nie auf Konnektivität ausgelegt, sodass keine Funktionen zur Bedrohungsabwehr oder Richtliniendurchsetzung integriert sind.



NICHT SEGMENTIERTE NETZWERKE

Die Netzwerke in Krankenhäusern sind oft nicht segmentiert, sodass Angreifer beispielsweise ein IT-Gerät manipulieren und sich dann im Netzwerk ausbreiten und IoT-Geräte infizieren können.



BEREITS VORHANDENE SICHERHEITSLÜCKEN

Medizinische Geräte werden häufig mit Sicherheitslücken ausgeliefert, die sich nur schwer patchen lassen. Obwohl viele dieser Geräte eine lange Betriebsdauer haben, werden sie weder zurückgerufen noch regelmäßig ersetzt.

2020 meldeten Gesundheitsdienstleister 616 Datenlecks mit mindesten 500 betroffenen Datensätzen, wodurch 28.756.445 Patientenakten kompromittiert wurden.[8]

Wussten Sie schon?

41 % der Angriffe nutzen Schwachstellen in IoT-Geräten aus.

57 % der mittelschweren bis schweren Angriffe zielen auf IoMT-Geräte ab.

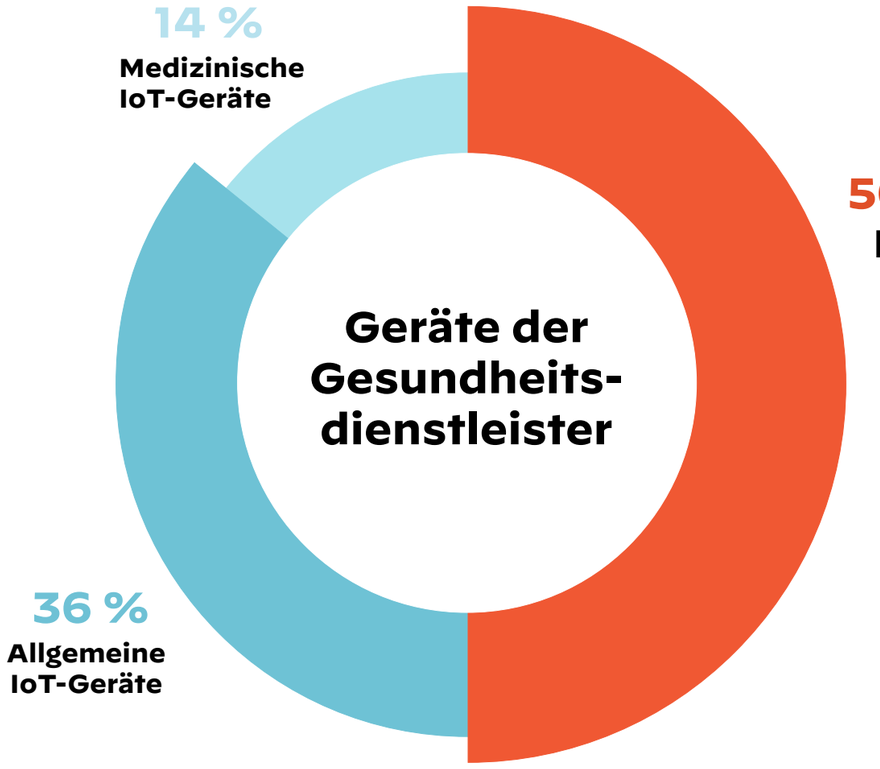
72 % der VLANs im Gesundheitswesen enthalten sowohl IT- als auch IoT- und IoMT-Geräte.

83 % der Bildgebungsgeräte nutzen veraltete, nicht unterstützte Betriebssysteme – 56 % mehr als 2018.

Quelle:
IoT Threat Report 2020 von Unit 42
8 HIPAA Journal, 2021

Die verschiedenen Geräte der Gesundheitsdienstleister

IoMT-Geräte sind erstaunlich schlecht gegen Cyberangriffe geschützt, sodass ein Paradigmenwechsel in Bezug auf die Sicherheitsstrategien notwendig wird.



50 % aller Geräte von Gesundheitsdienstleistern sind nicht verwaltet.

Quelle:
Zingbox, Medical Threat Report, 2019
IoT Threat Report 2020 von Unit 42

Am häufigsten bereitgestellte medizinische IoT-Geräte

46 %
Infusionspumpen

19 %
Medizinische Bildgebungsgeräte

17 %
Systeme zur Patienten-überwachung

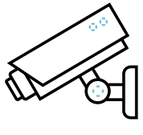
Medizinische IoT-Geräte mit den meisten Sicherheitsproblemen

51 %
Medizinische Bildgebungsgeräte

26 %
Systeme zur Patienten-überwachung

9 %
Gateways für medizinische Geräte

Allgemeine IoT-Geräte mit den meisten Sicherheitsproblemen in allen Unternehmen, einschließlich Gesundheitsdienstleistern



33 %
Überwachungs-kameras

24 %
Drucker

10 %
Geräte für Videospiele

Aktuelle Lösungen bieten nur unzureichenden Schutz für IoT-Geräte im Gesundheitswesen

Da veraltete Sicherheitsmechanismen nicht in der Lage sind, alle Geräte ausreichend zu schützen, nimmt die Arbeitslast für Sicherheits-, Infrastruktur- und Klinikteams zu.

Nutzen Cyberkriminelle eine Sicherheitslücke auf IoMT-Geräten aus, können sie verschiedene Aktionen ausführen, zum Beispiel die Kontrolle über das medizinische Gerät übernehmen, Patientenakten mit sensiblen personenbezogenen, Gesundheits- und Versicherungsdaten stehlen, proprietäre Klinikinformationen stehlen, den Netzwerktraffic verschleiern, die Bereitstellung von Gesundheitsdienstleistungen stören und durch einen Ransomwareangriff Lösegeld erpressen. Zwar kommen immer mehr IoT-Sicherheitslösungen auf den Markt, doch bisher erfüllt keines dieser Angebote den gesamten Anforderungskatalog für den Schutz aller medizinischen Geräte in einem Netzwerk.

Gründe für den unzureichenden Schutz aktueller Lösungen für IoMT- und IoT-Geräte

SIGNATURBASIERTE LÖSUNGEN

zur Identifizierung von Geräten sind nicht präzise genug und können nicht ausreichend skaliert werden, um die Masse an Geräten oder Gerätevarianten zu bewältigen, die jeden Tag eingeführt werden.

NUR ALARM AUSGEBENDE LÖSUNGEN

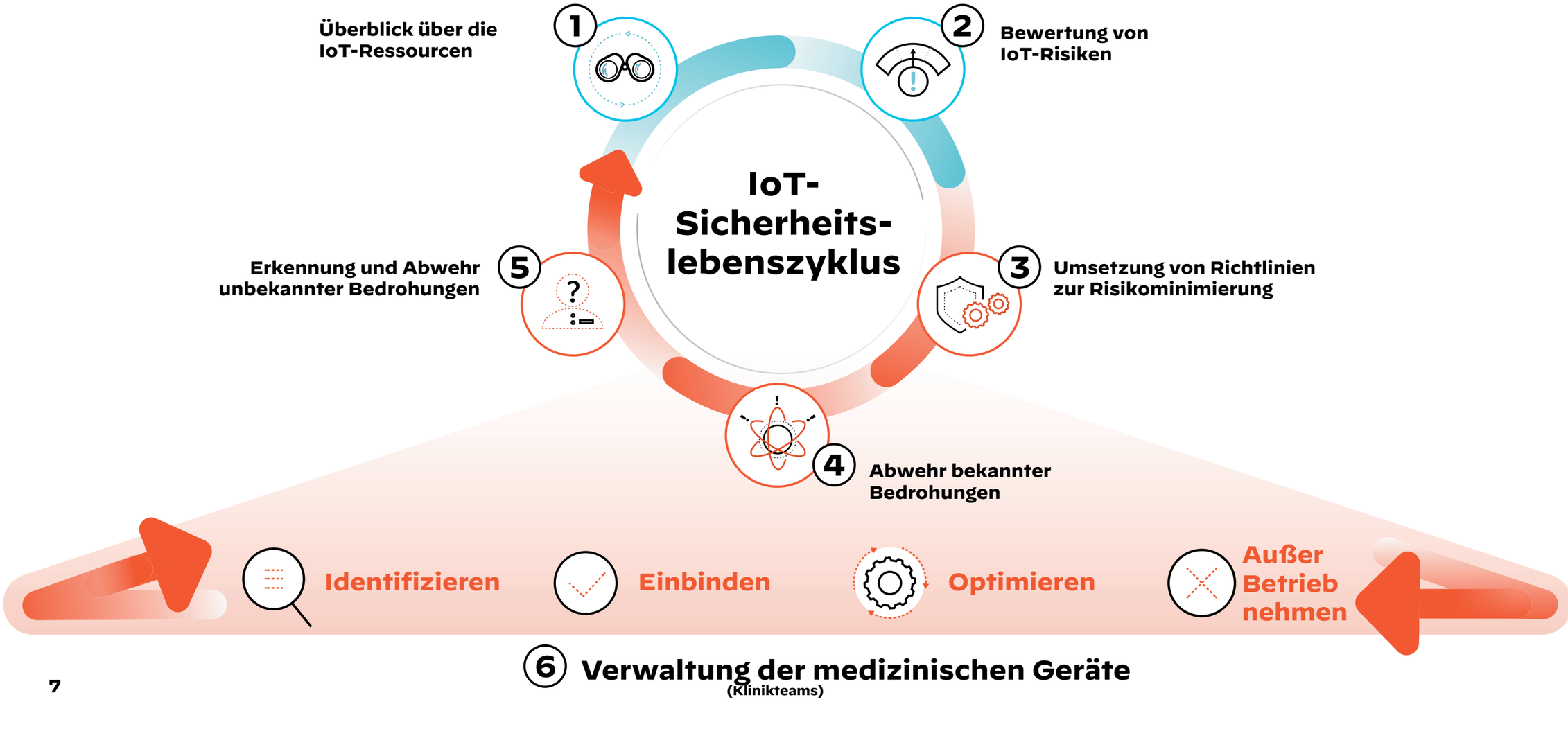
können meist keine Richtlinien empfehlen oder durchsetzen und bieten in der Regel auch keinen Schutz vor bekannten oder unbekannten Bedrohungen für IoMT- oder IoT-Geräte.

PUNKTLÖSUNGEN

sorgen für erhebliche Herausforderungen und einen großen Arbeitsaufwand bei der Bereitstellung, da entweder die Netzwerkinfrastruktur geändert oder neue Netzwerksensoren implementiert werden müssen, um den Datenverkehr zu verarbeiten und die Geräte zu identifizieren.

Ein umfassender Ansatz für den Schutz und die Verwaltung medizinischer Geräte

Medizinische Geräte müssen im Kontext der gesamten Geräteverwaltungsstrategie betrachtet werden, um die Risiken für die Patienten und das Netzwerk zu minimieren. Die ideale Strategie entlastet sowohl Netzwerksicherheits- als auch Klinikteams und deckt Routineaufgaben zum Schutz und zur Verwaltung dieser Geräte ab.



Die Angriffsflächen werden immer größer und die Angriffsvektoren immer komplexer. Verbessern Sie daher jetzt Ihre IoMT-Sicherheit mit einem neuen, effektiven Ansatz.

Zuverlässiger Schutz medizinischer Geräte und sichere Verwaltung von Klinikabläufen in 6 Schritten

1

Umfassender Überblick über alle IoMT-Geräte eines Gesundheitsdienstleisters

Wenn Sie einen umfassenden Überblick über die IoMT-Angriffsfläche haben, können Sie den Sicherheitsstatus besser ermitteln. Damit beginnt Ihr IoT-Sicherheitslebenszyklus. Mithilfe der Geräteerkennung können sich alle Stakeholder, IT-, Sicherheits- und Klinikteams einen umfassenden Überblick über die IoMT-Assets verschaffen. Es wird eine aktuelle IoMT-Bestandsliste erstellt – mit allen Geräten, die Sie kennen, die Sie nicht kannten und die Sie schon vergessen hatten. Die IoMT-Sicherheitslösung sollte dabei auch wichtige Geräteattribute erfassen, um umfassende Kontextinformationen zu jedem medizinischen Gerät zu liefern.

Eine ideale IoMT-Sicherheitslösung sollte folgende Anforderungen erfüllen:

- ✓ Mindestens 90 % der Geräte in sichtbaren Segmenten innerhalb von 48 Stunden erkennen.
- ✓ Neue, bisher unbekannte Geräte mithilfe von ML-gestützter Klassifizierung erkennen und nach Merkmalen wie Hersteller, Marke, Modell, Typ, Betriebssystem, Firmware, Standort, Subnetz, Risikograd, Typ der geschützten Patientendaten (Protected Health Information, PHI) und MDS2 (Manufacturer Disclosure Statement for Medical Device Security) zu kategorisieren.
- ✓ Neu angeschlossene Geräte bereits innerhalb weniger Minuten erkennen, nicht erst nach Stunden oder Wochen.
- ✓ Nicht verwaltete IoMT- und IoT-Geräte von verwalteten IT-Geräten unterscheiden können.
- ✓ Eine Liste aller IT-Geräte erstellen, damit IT- und Sicherheitsteams auch nicht verwaltete IT-Geräte identifizieren können.
- ✓ Lösungen für das Assetmanagement wie CMMS, ITSM und CMDB automatisch mit den detaillierten IoMT-Geräteinformationen aktualisieren.
- ✓ Mehrzwecksensoren nutzen, die sich in die bestehende Infrastruktur integrieren lassen.

2

Proaktive Risikominimierung durch kontinuierliche Risikoüberwachung und -bewertung der IoMT-Geräte

Bei der **Risikobewertung** im Rahmen des IoT-Sicherheitslebenszyklus müssen die IoMT-Geräte fortlaufend aktiv überwacht werden. Um die IoMT-Risiken und die Angriffsfläche proaktiv zu reduzieren, sind Unternehmen auf Funktionen für die Risikoüberwachung, Berichterstellung und Ausgabe von Alarmen in Echtzeit angewiesen. Signaturbasierte Lösungen sind weder präzise noch schnell genug, um diese Assets zu schützen. Nach einer sorgfältigen Risikobewertung können IT-Sicherheitsteams die Geräte kontinuierlich überwachen und die Datenverkehrsmuster kontrollieren, um eine proaktive NAC-Segmentierung durchzuführen und die Angriffsfläche zu verkleinern. Außerdem können die IT-Teams eine Mikrosegmentierung des Netzwerks nach Gerätetypen und -klassen (IoMT, IoT und IT) in Betracht ziehen, um eine Ausbreitung von Bedrohungen im Netzwerk proaktiv zu verhindern.

Eine ideale IoMT-Sicherheitslösung sollte folgende Anforderungen erfüllen:

- Die Integration mehrerer Threat Intelligence Feeds wie CVE, MDS2 und RSSI unterstützen, damit Sicherheitslücken den IoMT-Geräten präzise zugeordnet werden können.
- MDS2-Spezifikationen wie Antivirusfunktionen, Funktionen für elektronisch geschützte Patientendaten (ePHI), FDA-Rückrufe und Anbieterempfehlungen für Patches umfassen.
- Anomalien im IoMT-Geräteverhalten, die die Risikobewertung beeinflussen könnten, in Echtzeit erkennen und melden.
- Den Risikograd für IoT-Geräte und -Gerätekategorien ermitteln.
- Änderungen der Risikograde erfassen und die vollständige Risikoentwicklung für Compliancezwecke protokollieren.
- Integrationen von Systemen für das Schwachstellenmanagement und Systemen der Gerätehersteller unterstützen, um ein zentrales IoMT-Risikomanagement zu ermöglichen und den Sicherheitsteams wichtige Informationen bereitzustellen.

3

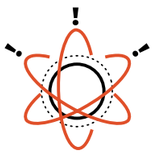
Automatisierte risikobasierte Empfehlung und Durchsetzung von Sicherheitsrichtlinien

Eine effiziente und übersichtliche IoMT-Sicherheitslösung erfordert keine Infrastrukturänderungen oder zusätzlichen Investitionen. IT-Teams können die vorhandenen Next-Generation Firewalls einbeziehen, um eine umfassende und integrierte Sicherheitsinfrastruktur aufzubauen. Die Lösung sollte die Funktionen der Firewall ergänzen und **automatisch Sicherheitsrichtlinien empfehlen und durchsetzen**, die für den Risikograd und das Ausmaß des bei den IoT-Geräten erkannten nicht vertrauenswürdigen Verhaltens angemessen sind. Da Vertrauen im Grunde eine Schwachstelle ist, sollte die IoMT-Lösung einen Zero-Trust-Ansatz verfolgen und Richtlinien nach dem Least-Privilege-Prinzip anwenden. Dadurch werden die Möglichkeiten für Angreifer – ganz gleich, ob sie sich nun innerhalb oder außerhalb Ihrer Organisation befinden – erheblich reduziert und die kritischen IoT-Geräte geschützt.

Eine ideale IoMT-Sicherheitslösung sollte folgende Anforderungen erfüllen:

- Die notwendigen Funktionen bereitstellen, um aus dem normalen IoMT-Geräteverhalten Richtlinien abzuleiten und anschließend nur vertrauenswürdige Verhaltensweisen zuzulassen.
- Die Richtliniendurchsetzung basierend auf der Geräte- und Anwendungserkennung automatisieren.
- Sowohl Zulassungs- als auch Sperrlisten unterstützen.
- Geräte und Anwendungen verfolgen, um Richtlinien im gesamten Netzwerk durchzusetzen.
- Einmal definierte Richtlinien automatisch aktualisieren, damit nicht bei jeder Änderung manuelle Anpassungen nötig sind.
- Integration in NAC und automatische Weitergabe von IoT-Geräteinformationen unterstützen, um Gerätekontrollen und eine kontextbezogene Segmentierung zu erzwingen.

4



Schnelle Abwehr bekannter Bedrohungen

Durch die Vielfalt der IoMT-Geräte wird das Netzwerk zu einer heterogenen Umgebung mit zahlreichen potenziellen Einfallstoren. Um in Phase 4 des IoT-Sicherheitslebenszyklus einen zuverlässigen Sicherheitsstatus zu erreichen, benötigen Sie aussagekräftige Erkenntnisse zur **Erkennung und Abwehr bekannter Bedrohungen** für die IoMT-Geräte, damit Sie schneller auf Bedrohungen reagieren können. Wählen Sie zur Bedrohungsabwehr einen Mechanismus, der komplexe Bedrohungen mittels inhaltsbasierter Signaturen blockiert. Damit sind der Sicherheitsstatus und die Abwehrmaßnahmen für bekannte Bedrohungen immer auf dem neuesten Stand und können in Echtzeit auf Verhaltensanomalien der IoMT-Geräte und auf Schwachstellen im gesamten Netzwerk reagieren. Außerdem werden die Sicherheitsteams nicht mit unnötigen Alarmen überlastet.

Eine ideale IoMT-Sicherheitslösung sollte folgende Anforderungen erfüllen:

- ✓ Die selektive Aktivierung von Schutzmaßnahmen auf Grundlage des Risikograds der IoMT-Gerätegruppe ermöglichen.
- ✓ Bekannte Bedrohungen durch IoMT-Malware, Spyware und Exploits erkennen und abwehren.
- ✓ IoMT-Angriffe über schädliche URLs und Websites abwehren.
- ✓ IoMT-Angriffe abwehren, bei denen DNS für Command-and-Control-Kommunikation oder Datendiebstahl missbraucht wird.
- ✓ Unbekannte, in Datenpaketen eingeschleuste IoMT-Bedrohungen abwehren.

5

Schnelle Erkennung und Abwehr unbekannter Bedrohungen

Mit den alten Ansätzen werden für die **Erkennung und Abwehr unbekannter Bedrohungen** die Bedrohungsdaten isoliert, die jede Organisation erhält und generiert. Dadurch entstehen Silos und die Einrichtung von Abwehrmaßnahmen wird erschwert. Um die Anforderungen des letzten Schritts im IoT-Sicherheitslebenszyklus zu erfüllen, sollte die IoMT-Sicherheitslösung einen neuen Ansatz nutzen, der sich auf eine kollektive Threat Intelligence Engine stützt, die Malware in Echtzeit analysiert und vor Zero-Day-Angriffen auf IoMT-Geräte schützt. Crowdsourcing-Daten aus einer globalen Community stärken nicht nur die kollektive Immunität, sondern sparen IT-Sicherheitsteams auch wertvolle Zeit, da mithilfe der zusammengetragenen IoMT-Identitätsinformationen, Risikobewertungen, Schwachstellendaten und Verhaltensanalysen unbekannte und einzigartige Bedrohungen unmittelbar nach dem Auftreten in Ihrer IoMT-Umgebung untersucht werden können. Dieser letzte Schritt deckt auch potenzielle Bedrohungen auf, die in früheren Phasen übersehen wurden, und sorgt dadurch für kontinuierliche Verbesserungen.

Eine ideale IoMT-Sicherheitslösung sollte folgende Anforderungen erfüllen:

- Verhaltensanomalien auf verschiedenen Ebenen erkennen, das heißt für die Gerätekategorie, den Hersteller/das Modell und schließlich die Geräteinstanz.
- Crowdsourcing-Daten nutzen, die mithilfe von maschinellem Lernen und Bedrohungsmodellen angereichert werden, um unbekannte Bedrohungen oder Angriffe zu erkennen, proaktiv zu melden oder auf sie zu reagieren.
- Integration in SIEM und SOAR mit einem einfachen Playbook-gestützten Ansatz zur Orchestrierung der Maßnahmen für Incident-Response-Einsätze und die Abwehr von Bedrohungen.
- Aktive Untersuchungen von IoT-Sicherheitsteams unterstützen, um neue IoT-Bedrohungen aufzudecken.

6

Wichtige Informationen zu Betriebsabläufen für Klinikteams

Obwohl die meisten medizinischen Geräte nie vollständig ausgelastet werden, weil es teilweise zu viele im Inventar gibt, verursachen sie oft Kapital- und Betriebsausgaben, die zu unnötigen Kosten führen. Da die medizinischen Geräte den Vorgaben der FDA (Food and Drug Administration) unterliegen, müssen alle Software-Updates vom Gerätehersteller überprüft werden, um sicherzustellen, dass das Gerät auch nach den Änderungen für Patienten sicher ist. Klinikteams, die für diese Aspekte verantwortlich sind, benötigen aussagekräftige Betriebsdaten für die Kapitalplanung und vorausschauende Instandhaltung. Außerdem müssen sie wissen, wann das Patching oder ein Software-Upgrade eines Geräts ansteht. Eine IoT-Sicherheitslösung kann sie bei diesen wichtigen Entscheidungen unterstützen. Mithilfe der von der Lösung gelieferten Informationen können Teams Geräte **identifizieren**, je nach Bedarf **einbinden**, die Leistung basierend auf den Nutzungsdaten **optimieren** und sie am Ende gemäß den Compliancevorgaben der Branche sicher **außer Betrieb nehmen**.

Eine ideale IoMT-Sicherheitslösung sollte folgende Anforderungen erfüllen:

- Nutzungsstatistiken für einzelne medizinische Geräte erfassen, die für Entscheidungen bezüglich der Anschaffung neuer Geräte oder des Austauschs älterer Geräte herangezogen werden können.
- Zeiten mit hoher Auslastung ermitteln, damit vorausschauende Wartungsarbeiten und Software-Updates so geplant werden können, dass wichtige medizinische Termine und die Patientenversorgung nicht gestört werden.
- Analysedaten zur Nutzung von Bildgebungsgeräten bereitstellen, einschließlich Angaben zu den einzelnen Benutzern und den Einsatzbereichen, damit sich die benötigten Geräte in der Nähe der jeweiligen Teams befinden.
- Verwaltung von Herstellerhinweisen, FDA-Rückrufen und sonstigen Problemen an einem zentralen Ort, sodass keine manuellen Untersuchungen notwendig sind.
- Inventarsysteme aktualisieren, um kontinuierlich eine Liste der Geräte zu erstellen und alle Abteilungen zu informieren, wenn neue Geräte eingeführt und alte außer Betrieb genommen werden.
- Patientendaten schützen, indem ermittelt wird, wie jedes Gerät Daten nutzt und speichert, und dann Geräte gemäß den HIPAA-Vorgaben eingebunden oder entfernt werden.

IoT Security für das Gesundheitswesen von Palo Alto Networks

Die umfassendste IoT-Sicherheitslösung für das Gesundheitswesen

IoT Security von Palo Alto Networks ist die umfassendste IoT-Sicherheitslösung für das Gesundheitswesen, die mithilfe von ML-gestützten Funktionen einen detaillierten Überblick ermöglicht und Maßnahmen zur Bedrohungsabwehr, Richtliniendurchsetzung und Informationen zu Betriebsabläufen auf einer zentralen Plattform bereitstellt.

Hier finden Sie eine Übersicht aller Vorteile von IoT Security:

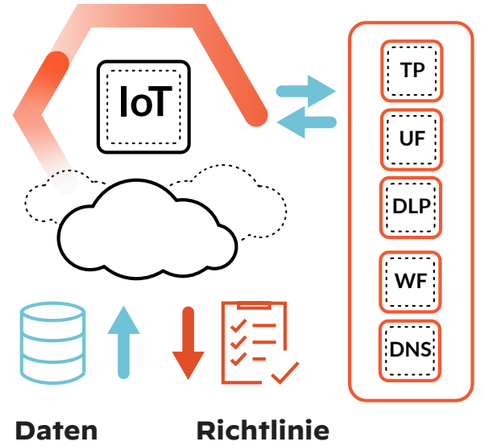
- Es ist die einzige Lösung, die **maschinelles Lernen mit Crowdsourcing** kombiniert, um schnell und präzise alle Geräte zu erfassen – auch bisher unbekannte.

- Außerdem ist es die einzige Lösung mit **integrierten Funktionen zur Bedrohungsabwehr**. Statt sich nur auf Alarme zu verlassen, werden nicht verwaltete Geräte vor allen bekannten und unbekannten Bedrohungen sowie Sicherheitslücken geschützt, da diese gar nicht erst in das Netzwerk gelangen können.

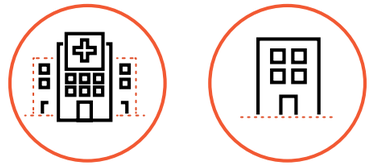
- IoT Security kann auch die Kosten für die Patientenversorgung reduzieren – dank **aussagekräftiger Betriebsdaten** für die Klinikteams und der **automatischen Richtliniendurchsetzung, entweder nativ oder über Integrationen**. Auf diese Weise werden die Netzwerk- und SecOps-Teams entlastet, die Geräte zuverlässig geschützt und die Performance und Verfügbarkeit verbessert.

- Da es sich um eine einzelne Plattform handelt, **ist die Bereitstellung einfach**. Zudem ist keine zusätzliche Infrastruktur erforderlich.

IoT Security von Palo Alto Networks ist die einzige derzeit verfügbare Lösung, die einen maximalen Return on Investment (ROI) und eine bessere Patientenversorgung ermöglicht, da sich die Teams auf der zentralen Plattform einen umfassenden Überblick verschaffen, detaillierte Informationen abrufen und erweiterte Sicherheitsfunktionen für medizinische Geräte nutzen können. **Jedes fünfte Krankenhaus in den USA vertraut auf unsere Sicherheitslösung.**



Flexible Bereitstellungsmöglichkeiten



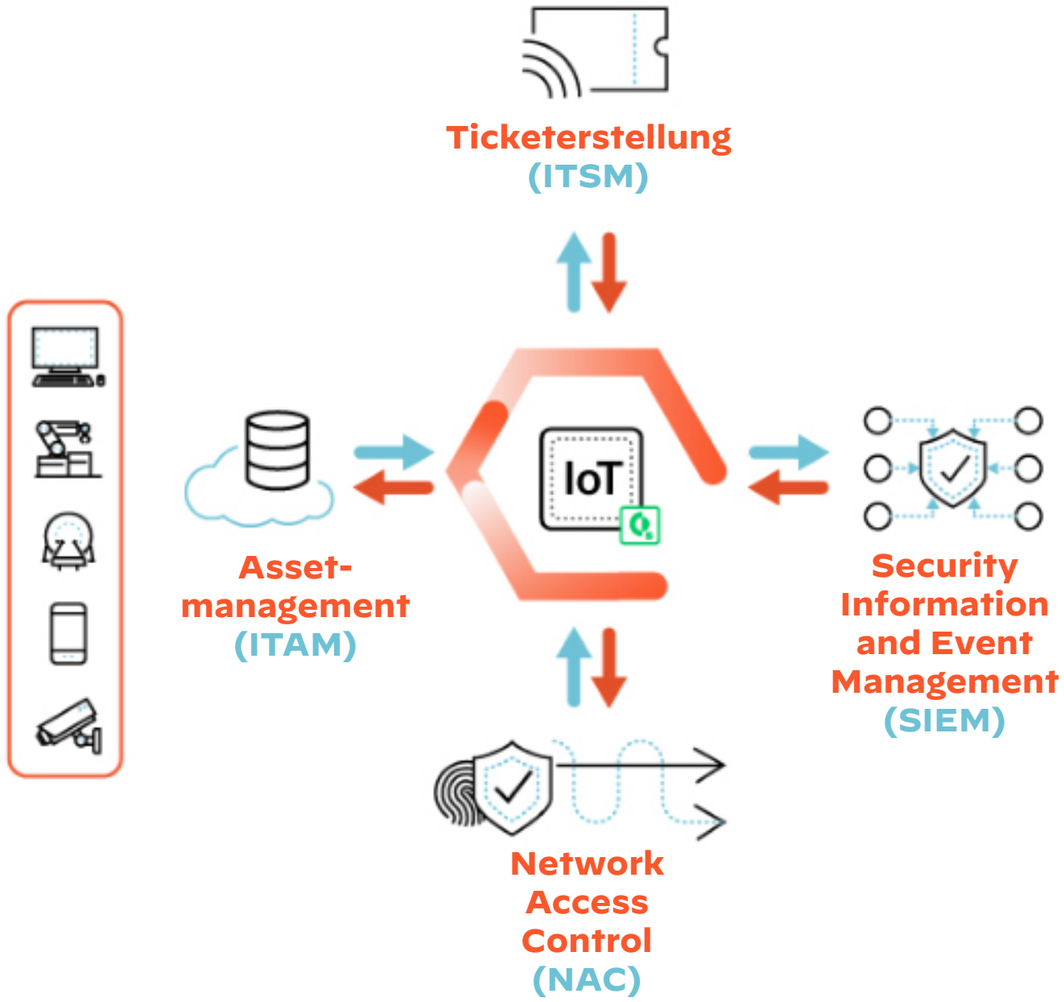
Integration in Lösungen von Drittanbietern

Mit integrierter XSOAR-Technologie

IoT Security lässt sich nahtlos in vorhandene Arbeitsabläufe einbinden, ganz ohne aufwendige API-Integrationen, und entlastet somit die Infrastruktur- und Sicherheitsteams.

Mit den nativen Integrationen in bestehende IT- und Sicherheitsabläufe können Sie die vorhandenen ITSM- (IT Service Management), NAC- (Network Access Control) und SIEM-Lösungen (Security Information and Event Management) sowie andere Anwendungsfälle optimieren.

Dank unserer modularen und anpassbaren Playbook-gestützten Orchestrierung können Sicherheitsteams ineffiziente Abläufe verbessern, präzisere Assetverzeichnisse erstellen, IoMT-Geräte korrekt einbinden, Gerätekontrollen erzwingen und Incident-Response-Maßnahmen automatisieren, ohne diese Integrationen erst selbst entwickeln zu müssen.

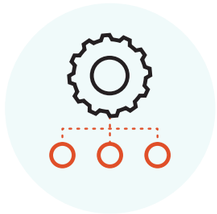


Verwaltung durch das bestehende IT-Sicherheitsteam

Sie brauchen nicht extra ein neues Team zu bilden, sondern können mit dem bestehenden Team neue Infrastrukturen bereitstellen oder vorhandene Abläufe ändern.

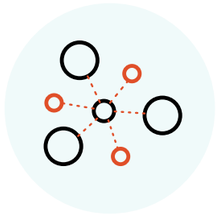
Transparenz und Schutz ohnegleichen

- ML-gestützte IoT-Geräteerkennung
- Automatisierte Risikobewertung
- Native Durchsetzung von Sicherheitsrichtlinien
- Kontextbasierte Netzwerksegmentierung



Einfache Bereitstellung mit flexiblen Optionen

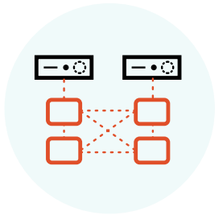
- Hardwarefirewalls
- Softwarefirewalls
- Cloudbasierte Firewalls



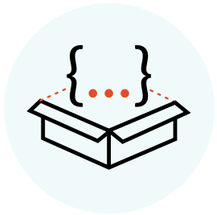
Umfassende Abdeckung von IoT-, IoMT- und IT-Geräten

- Nicht verwaltete IoMT-Geräte
- Nicht verwaltete IoT-Geräte
- Verwaltete IT-Geräte

Nutzung erstklassiger Abwehrmaßnahmen aus anderen Sicherheitsservices



Mühelose Skalierung entsprechend dem Unternehmenswachstum dank einer flexiblen, mandantenfähigen Cloud-Infrastruktur



Automatisierte Arbeitsabläufe mit Playbook-gestützten Integrationen

IoT Security für das Gesundheitswesen

von Palo Alto Networks

Palo Alto Networks hat sich das Ziel gesetzt, zum bevorzugten Cybersicherheitspartner für Unternehmen zu werden und gemeinsam mit ihnen unseren digitalen Lebensstil zu schützen. Palo Alto Networks schützt die Clouds, Netzwerke und Mobilgeräte Zehntausender Unternehmen. Dazu gehen wir durch kontinuierliche Innovation die größten Herausforderungen rund um die Cybersicherheit an, mit denen Unternehmen derzeit konfrontiert sind, und berücksichtigen dabei die neuesten Forschungsergebnisse aus den Bereichen der künstlichen Intelligenz, Analysen, Automatisierung und Orchestrierung.

Palo Alto Networks wurde 2005 gegründet und hat seinen Hauptsitz im kalifornischen Santa Clara. Zur Betreuung unserer Kunden haben wir zudem Niederlassungen auf der ganzen Welt.

Weitere Informationen erhalten Sie unter: 🌐 www.paloaltonetworks.de

Sie möchten mehr erfahren? **Demo ansehen**

Das sagen unsere Kunden

> *IoT Security von Palo Alto Networks ist anwenderfreundlich, in der Cloud verfügbar und einfach zu implementieren. Mit dieser Lösung können wir uns einen umfassenden Überblick über unsere mehr als 4.000 IoT- und medizinischen Geräte verschaffen. Das sind etwa 30 % mehr Geräte als zuvor.*

Miroslav Belote
Chief Information Security Officer
Valley Health System

Valley Health System

www.paloaltonetworks.de

Oval Tower, De Entrée 99–197
1101 HE Amsterdam
Niederlande

Telefon: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600