DIGITALE ZWICKMÜHLE IM GESUNDHEITSWESEN:

ZWISCHEN INNOVATIONSDRUCK UND SYSTEMRISIKEN

BEGRÜSSUNGSWORT

Stephanie Lopinski, VP, Global Marketing

Das Gesundheitswesen steht an der Schwelle eines digitalen Durchbruchs. Innovationen in den Bereichen KI, Telemedizin, mobile Technologie und Automatisierung eröffnen neue Möglichkeiten für intelligentere, besser vernetzte Pflegeleistungen. Trotz dieser Fortschritte werden viele Gesundheitsorganisationen durch veraltete Systeme und operative Ineffizienzen ausgebremst.

Für IT-Führungskräfte ist die Aufgabe eindeutig: Organisationen müssen die Einführung moderner Technologien beschleunigen, um bessere Ergebnisse zu erzielen, Mitarbeitende gezielt zu unterstützen und die hohe Versorgungsqualität sicherzustellen, die Patienten heute voraussetzen.

Alte Systeme führen zu Verzögerungen beim Zugriff auf kritische Informationen, was letztlich die Qualität der Versorgung verringert. Unterdessen kann KI die Diagnostik verbessern, Workflows rationalisieren und Patientenbedürfnisse vorhersagen – aber nur, wenn sie von moderner Infrastruktur unterstützt wird.

Der Grad der Integration neuer Technologien und die Fähigkeit, den Nutzen aller Geräte und Anwendungen zu maximieren, spielen eine entscheidende Rolle für die Behandlungsergebnisse der Patienten sowie die Qualität der medizinischen Versorgung. Organisationen müssen die Systemintegration und den Zugriff auf Echtzeitdaten priorisieren und sich von veralteter Technik befreien, um die Vorteile der digitalen Transformation freizusetzen.

Unsere neuesten Untersuchungen befassen sich mit dem aktuellen Stand der Gesundheitsorganisationen, den Herausforderungen, vor denen sie stehen, sowie mit Strategien für Verbesserungen.

SOTIs Bericht des Jahres 2025 hebt drei Hauptthemen hervor:

Künstliche Intelligenz

Die Akzeptanz von KI im Gesundheitswesen nimmt rapide zu, wobei sie von **81 %** der Organisationen weltweit für die Patientenversorgung verwendet wird. Im Jahr 2024 waren es noch **61 %**. Die Anwendungsbereiche umfassen die Verarbeitung medizinischer Daten, die Aktualisierung von Aufzeichnungen, die Personalisierung von Behandlungen und die Diagnose von Krankheiten.

Trotz erhöhter Nutzung verfügen nur **36 %** von Organisationen über KI-spezifische Sicherheitsmaßnahmen, was Bedenken hinsichtlich des Schutzes der Patientendaten hervorruft. Daher ist die Modernisierung der Systeme für die Gewährleistung der Privatsphäre der Patienten von grundlegender Bedeutung.

Der Bericht aus 2025 zeichnet ein klares Bild – der technologische Weg des Gesundheitswesens schreitet voran, aber ungleichmäßig. Solange Altsysteme nicht modernisiert, die Datensicherheit nicht verbessert und IT-Ressourcen nicht von ständigem Troubleshooting entlastet werden, wird die Branche Schwierigkeiten haben, aus bloßer Einführung eine echte Integration zu machen.

Veraltete Systeme

Organisationen im Gesundheitswesen haben Schwierigkeiten, miteinander verbundene Systeme und Lösungen für Telemedizin zu integrieren, vor allem aufgrund veralteter Systeme, die eine Herausforderung für die Remote-Verwaltung darstellen.

Diese Systeme bergen erhebliche Sicherheitsrisiken: **83 %** der Unternehmen melden seit 2023 Datenschutzverletzungen, Datenlecks oder Cyber-Angriffe. Darüber hinaus verkomplizieren sie die Integration von elektronischen Patientenakten (ePA), wovon **79 %** der Organisationen betroffen waren.

Wenn Organisationen versuchen, neue Technologien einzuführen, kommt es daher häufig zu Rückschlägen, die Innovationen verhindern und sich negativ auf die Patientenerfahrung auswirken. Letztendlich beeinflussen die Einschränkungen, die von diesen veralteten Systemen verursacht werden, direkt die Ergebnisse der Patientenbetreuung. Daher ist es für Organisationen von entscheidender Bedeutung, in moderne Technologien und miteinander verbundene Systeme zu investieren, um Effizienz, Sicherheit und die allgemeine Versorgungsqualität zu verbessern.

Mobile Device Management + Enterprise Mobility Management

Gesundheitsorganisationen verlassen sich zunehmend auf eine Reihe mobiler Geräte, darunter Laptops, Smartphones, Tablets und Spezialgeräte wie RFID-Leser. Die Verwaltung dieser Geräte stellt erhebliche Herausforderungen in Bezug auf Sicherheit und Remote-Fehlerbehebung dar, wenn man sich auf veraltete MDM-Lösungen (Mobile Device Management) verlässt.

Die aktuelle Landschaft erfordert jedoch eine Entwicklung über das traditionelle MDM hinaus, um einen umfassenden Ansatz für das Enterprise Mobility Management (EMM) zu bieten.

Im Zuge der Entwicklung der Gesundheitstechnologie muss sich der Fokus auf eine integrierte Plattform verlagern, die fortschrittliche Diagnostik, Daten- und Zustandsanalyse umfasst. Dieser Ansatz ermöglicht es Organisationen, sich proaktiv mit Fragen zu befassen und die Insights zu verwenden, um die Entscheidungsfindung und Arbeitsabläufe zu optimieren. Durch die Digitalisierung von Prozessen und die Automatisierung administrativer Aufgaben können Gesundheitsdienstleister die operative Effizienz steigern und eine bessere Patientenversorgung unterstützen.

Effektive Lösungen für die mobile Verwaltung erfordern auch ein vollständiges Lebenszyklus-Management, um die Nachhaltigkeit zu fördern. Organisationen sollten darauf abzielen, die Lebensdauer ihrer Geräte zu maximieren und Erkenntnisse in Bezug auf Akkuzustand und Verwendungsmuster nutzen, um nachhaltige Ersatzstrategien zu entwickeln. Dieses proaktive Management hilft nicht nur dabei, den Zustand der Geräte zu erhalten, sondern verringert auch Schwachstellen und sichert Patientendaten.

VERÄNDERUNGEN IM GESUNDHEITSWESEN:

FORTSCHRITTE UND WICHTIGE MEILENSTEINE SEIT 2020

SOTI führt seit 2020 Forschungen im Gesundheitswesen durch. Mit der Weiterentwicklung der Umfrage hat sich auch die Anzahl der Länder und der Befragten erhöht. Die Trends der letzten fünf Jahre umfassen die folgenden bemerkenswerten Erkenntnisse:

2020/2021

- Sicherheit: **81 %** haben Bedenken hinsichtlich der Sicherheit von Patientenakten.
- Technische Probleme: **63 %** erleben wöchentlich Geräte- oder Systemausfälle.
- Technische Auswirkungen auf die Patientenversorgung: **81 %** haben während der Patientenbetreuung Probleme mit technischen Systemen.

475 häusliche Pflegekräfte, Krankenpfleger und andere Fachkräfte des Gesundheitswesens in sieben Ländern weltweit

2022

- Sicherheit: **73 %** der Organisationen haben seit 2020 eine Datenverletzung oder ein Leck erlebt.
- IoT/Telemedizin: **98 %** haben die Voraussetzungen für IoT-/Telemedizin-Geräte geschaffen.
- Auswirkungen von Geräteausfällen: **53 %** geben an, dass sie regelmäßig Ausfallzeiten erleben, die zu Verzögerungen bei der Patientenversorgung führen, und dass 3,4 Stunden pro Woche und Mitarbeiter durch Ausfallzeiten verloren gehen.

1.300 IT-Fachleute, die in Gesundheitsorganisationen in acht Ländern weltweit arbeiten

2023

- Sicherheit der Patientendaten: **97 %** haben Bedenken in Bezug auf die Sicherheit von Patientenakten.
- Netzwerksicherheit: **55 %** erlebten entweder ein zufälliges oder geplantes Datenleck aus internen Quellen. **53 %** sind aufgrund veralteter Systeme nicht in der Lage, neue Geräte zu erkennen, die sich mit dem System verbinden, wodurch Schwachstellen entstehen.
- Veraltete Systeme: **52 %** geben an, dass Altsysteme dazu führen, dass sie nicht in der Lage sind, Probleme rechtzeitig zu lösen. **37 %** glauben, dass sie durch Altsysteme anfälliger für Sicherheitsverletzungen sind.
- Ausfallzeiten: In einer normalen Woche gehen 3,4 Stunden aufgrund von Schwierigkeiten mit technischen Systemen verloren.

1.450 IT-Fachleute, die in Gesundheitsorganisationen in neun Ländern weltweit arbeiten

2024

- KI: **85 %** glauben, dass KI helfen könnte, Aufgaben zu vereinfachen, aber derzeit findet nur bei 23 % eine breite Nutzung von KI statt.
- Sicherheit: **71 %** übertragen Daten auf externe Festplatten bzw. erstellen Sicherungskopien, wenn alte Geräte entsorgt werden. **23 %** geben Datensicherheit als ihr oberstes IT-Anliegen an.
- IoT/Telemedizin: **67 %** haben regelmäßig Probleme mit IoT-/Telemedizin-Geräten, was zu Verzögerungen bei der Patientenversorgung führt.
- Veraltete Systeme: **63 %** bestätigen, dass sie veraltete Technologien verwenden, und **45 %** haben im vergangenen Jahr eine Datenverletzung oder ein versehentliches Datenleck erlebt.
- Ausfallzeiten: 3,9 Stunden pro Woche pro Mitarbeiter verloren durch Ausfallzeiten

1.450 IT-Fachleute/Entscheidungsträger, die in Gesundheitsorganisationen in neun Ländern weltweit arbeiten

2025

- KI: **81 %** verwenden jetzt KI für die Patientenversorgung, während es im Jahr 2024 noch 61 % waren.
- Sicherheit: **83 %** haben in den letzten 12 Monaten ein versehentliches Datenleck, einen externen Datenbruch oder einen DDoS-Ransomware-Angriff erlebt. **30 %** geben Datensicherheit als ihr oberstes IT-Anliegen an.
- IoT/Telemedizin: **96 %** stehen vor Herausforderungen bei der Implementierung von IoT-/Telemedizin-Geräten.
- Veraltete Systeme: **45 %** machen Altsysteme dafür verantwortlich, dass Netzwerke anfällig für Angriffe sind.
- Mobile Geräteverwaltung: **47 %** sagen, dass Lösungen zur Verwaltung mobiler Geräte für die Remote-Fehlerbehebung entscheidend sind.

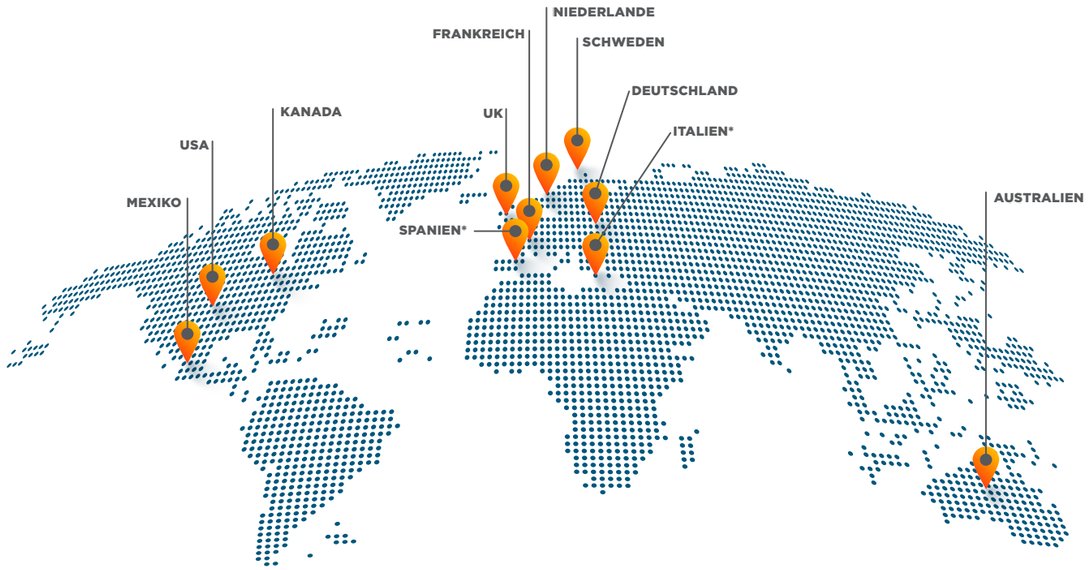
1.750 IT-Fachleute/Entscheidungsträger, in Gesundheitsorganisationen in neun Ländern weltweit arbeiten

INHALTE

METHODIK

In diesem Jahr erweiterte SOTI seinen Forschungsumfang auf **1.750 Teilnehmer in 11 Ländern**: USA (200), Kanada (150), Mexiko (150), UK (200), Deutschland (150), Frankreich (150), Schweden (150), Niederlande (150), Italien* (150), Spanien* (150) und Australien (150). Die Umfrage wurde zwischen Januar und März 2025 von IT-Entscheidungsträgern für Gesundheitsorganisationen abgeschlossen.

*Neue Regionen im Gesundheitsbericht 2025.



GLOBALE AUFSCHLÜSSELUNG

Für diesen Bericht bezieht sich der Begriff „Gesundheitsorganisationen“ auf:

Ein Krankenhaus, das Gesundheitsdienstleistungen direkt für Patienten anbietet.

Eine allgemeine medizinische Praxis/Klinik für viele Fachärzte, z. B. ambulante Chirurgie, Hausarzt, Arztpraxis.

Eine Klinik, die Patienten in einem oder mehreren Spezialgebieten direkt versorgt, z. B. Psychiatrie, Neurologie, Physiotherapie etc.

Ein Gesundheitsdienstleister, der Remote- oder Telemedizin-Dienstleistungen direkt für Patienten anbietet.

Die Größe der Gesundheitsorganisationen rangierte zwischen 50 und 5.000 Mitarbeitern. Obwohl alle Befragten an der IT-Entscheidungsfindung für eine Gesundheitsorganisation beteiligt waren, reichten ihre Rollen von IT-Fachleuten bis hin zu leitenden Managern in der oberen Führungsebene.

GLOBALE ERGEBNISSE

96 %

der Organisationen stehen vor Herausforderungen bei der Implementierung von IoT-/ Telemedizin-Geräten, wobei die Systemintegration die größte darstellt.

83 %

Die Zahl der Sicherheitsvorfälle ist nach wie vor hoch: Unbeabsichtigte Datenlecks, externe Daten-schutzverletzungen und DDoS-Ransomware-Angriffe zeigen keine Anzeichen für ein Nachlassen.

47 %

der IT-Entscheidungsträger sagen, dass Lösungen zur Verwaltung mobiler Geräte für die Remote-Fehlerbehebung entscheidend sind.

45 %

machen Altsysteme dafür verantwortlich, dass Netzwerke anfällig für Angriffe sind.

81 %

haben Bedenken hinsichtlich der Sicherheit von Patientendaten bei der Entsorgung mobiler Geräte.

81 %

nutzen jetzt auf irgendeine Weise KI, um die Effizienz und Wirksamkeit der Patientenversorgung zu verbessern, ein Sprung von 61 % im Jahr 2024.

40 %

der Organisationen ersetzen alte Geräte, wenn neue Versionen verfügbar sind.

30 %

nennen Datensicherheit als ihr oberstes IT-Anliegen, verglichen mit 23 % im Jahr 2024.

DER DURCHBRUCH:

KÜNSTLICHE INTELLIGENZ ERFÄHRT EINEN AUFSCHWUNG BEI DER PATIENTEN-VERSORGUNG

In den letzten Jahren hat die Gesundheitsbranche transformative Fortschritte erlebt, insbesondere durch die Integration von Technologie in die Patientenversorgung. Der Aufstieg der KI verändert die Art und Weise, wie Gesundheitsdienstleister Services erbringen und mit Patienten interagieren.

Die Nutzung von KI zur Verbesserung der Diagnostik, der Personalisierung von Behandlungsplänen und der Rationalisierung von Betriebsabläufen hat die Aufmerksamkeit von Gesundheitsorganisationen weltweit erregt. In diesem Jahr haben wir in unserer Umfrage festgestellt, dass KI in der Patientenversorgung in **81 %** der Gesundheitsorganisationen verwendet wird, ein Drittel mehr als im Jahr 2024 (**61 %**).

Die meisten Organisationen, die zurzeit keine KI für die Patientenversorgung verwenden, erwägen dies zumindest (**16 %** weltweit). Nur **3 %** der IT-Entscheidungsträger geben an, dass ihr Unternehmen nicht in Betracht zieht, KI einzusetzen.

KI wird am häufigsten in Großbritannien eingesetzt, wo **94 %** der IT-Entscheidungsträger sagten, dass ihre Organisation sie für die Patientenversorgung verwendet hat. Im Jahr 2024 waren es nur **47 %**. In Australien sagten **93 %** der Befragten, dass sie KI verwenden, im Vergleich zu **70 %** im Vorjahr.

Prozentsatz der Organisationen, die 2025 KI für die Patientenversorgung verwenden, im Vergleich zu 2024

	2025	2024		2025	2024
	81 %	**61 %**		81 %	45 %
	80 %	72 %		71 %	53 %
	87 %	72 %		70 %	43 %
	82 %	80 %		74 %	-
	94 %	47 %		83 %	-
	77 %	71 %		93 %	70 %

KI: ENTLASTUNG DER VERWALTUNG

Obwohl die Anzahl der Organisationen, die KI nutzen, gestiegen ist, bleibt die Art und Weise der Verwendung dieser Technologie seit dem letzten Jahr weitgehend unverändert. 2025 ist die häufigste Nutzung der KI die Verarbeitung und/oder Analyse medizinischer Daten (**60 %** der IT-Entscheidungsträger sagten, dass ihre Organisation sie für diesen Zweck verwendet), gefolgt von der Aktualisierung von Patientenakten (**59 %**). Knapp die Hälfte (**46 %**) verwenden KI für die Erstellung von Behandlungsplänen, **45 %** für die Personalisierung von Behandlungen, und **40 %** nutzen sie, um Krankheiten zu diagnostizieren.

Auf welcher der folgenden Weisen verwendet Ihre Organisation derzeit KI in der Patientenversorgung? (Frage nur an diejenigen, die KI in der Patientenversorgung verwenden)

Globale Ergebnisse

	2025	2024
Um medizinische Daten zu verarbeiten und/oder zu analysieren	60 %	60 %
Um Patientenakten zu aktualisieren	59 %	56 %
Um den besten Behandlungsweg zu planen	46 %	47 %
Um Behandlungen zu personalisieren	45 %	44 %
Um andere administrative Zwecke zu erfüllen	45 %	20 %
Um Krankheiten zu diagnostizieren	40 %	38 %
NETTO: Um Datensätze zu aktualisieren/ Andere administrative Zwecke	79 %	63 %

Eine wesentliche Änderung in diesem Jahr ist die Zunahme der Verwendung von KI für andere administrative Zwecke. Während 2024 noch **20 %** der IT-Entscheidungsträger angaben, KI dafür zu verwenden, erhöhte sich diese Zahl im Jahr 2025 auf **45 %**.

Durch die Übertragung mühsamer Aufgaben an die KI kann sich das Personal auf wichtige Aspekte der Patientenversorgung konzentrieren. Wenn wir dies zusammen mit Organisationen betrachten, die KI für die Aktualisierung von Krankenakten verwenden, sehen wir, dass **79 %** KI für irgendeine Form von administrativem Zweck verwendet.

Großbritannien und die USA nutzen KI am meisten für die Personalisierung von Behandlungen (**57 %** bzw. **55 %**), wobei Großbritannien bei der Krankheitsdiagnose mittels KI eine Vorreiterrolle spielt (**52 %**). Schweden (**53 %**) und Kanada (**52 %**) meldeten den häufigsten Einsatz der KI für andere administrative Zwecke.

In der Forschung des letzten Jahres fanden wir heraus, dass mehr als die Hälfte (**57 %**) der IT-Fachleute Vorbehalte gegenüber dem Einsatz von KI in der Patientenversorgung hatte. Sie sorgten sich um die Bedrohung, die sie für den Schutz der Patientendaten darstellt. In diesem Jahr haben wir festgestellt, dass alle Organisationen zumindest einige Sicherheitsmaßnahmen für mobile Geräte umgesetzt haben. Jedoch verfügen nur **36 %** über KI-spezifische Sicherheitsmaßnahmen. Angesichts des steilen Anstiegs der KI-Nutzung im letzten Jahr, scheint dies ein Bereich zu sein, den Gesundheitsorganisationen untersuchen sollten.

Welche Sicherheitsmaßnahmen priorisieren Sie für mobile Geräte?

Regelmäßige Updates	**51 %**
Schulung der Mitarbeiter über spezifische Bedrohungen und bewährte Sicherheitsmaßnahmen	**45 %**
Sicherstellung der Einhaltung von Vorschriften und Datenschutzgesetzen (z. B. DSGVO, EHDS)	**45 %**
Einschränkung des Zugriffs auf sensible Daten auf bestimmte Rollen und Verantwortlichkeiten	**45 %**
Multi-Faktor-Authentifizierung	**44 %**
Verschlüsselung	**42 %**
Durchführung regelmäßiger Sicherheits-Audits	**42 %**
Implementierung KI-spezifischer Sicherheitsmaßnahmen	**36 %**
Implementierung von Datenanonymisierung	**34 %**
Vorhandensein eines Reaktionsplans auf Vorfälle	**33 %**
Remote-Löschen	**23 %**

Im vergangenen Jahr sagten mehr als acht von zehn (**83 %**) IT-Fachleuten, dass KI eine wesentliche Kosteneinsparungsstrategie für Gesundheitsorganisationen sei. In diesem Jahr ist der Einsatz in der Patientenversorgung angestiegen. Angesichts der Probleme, die Altsysteme bei der Einführung neuer Technologien darstellen, und der in der gesamten Branche bestehenden Herausforderungen hinsichtlich der Datensicherheit, muss die Verwaltung der Geräte, die diese Technologie nutzen, sorgfältig überwacht werden, um sicherzustellen, dass sie ihr volles Potenzial sicher entfalten kann.

DIE HERAUSFORDERUNG:

ALTSYSTEME MINDERN DEN MEHRWERT NEUER TECHNOLOGIEN

EINFÜHRUNG VON IOT UND TELEMEDIZIN IST UNIVERSELL, ABER ES GIBT NOCH PROBLEME

Die Integration vernetzter Technologien gestaltet die Gesundheitsbranche neu, insbesondere durch die Telemedizin, die Geräte und Systeme sowohl innerhalb der Gesundheitseinrichtungen als auch aus der Ferne verbindet. Fast alle IT-Entscheidungsträger (**99 %**) gaben in diesem Jahr an, dass ihre Unternehmen irgendeine Art von vernetzten Geräten oder Telemedizin-Lösungen nutzen.

Trotz dieses hohen Anteils bleibt die operative Effizienz dieser Systeme hinter den Erwartungen zurück.

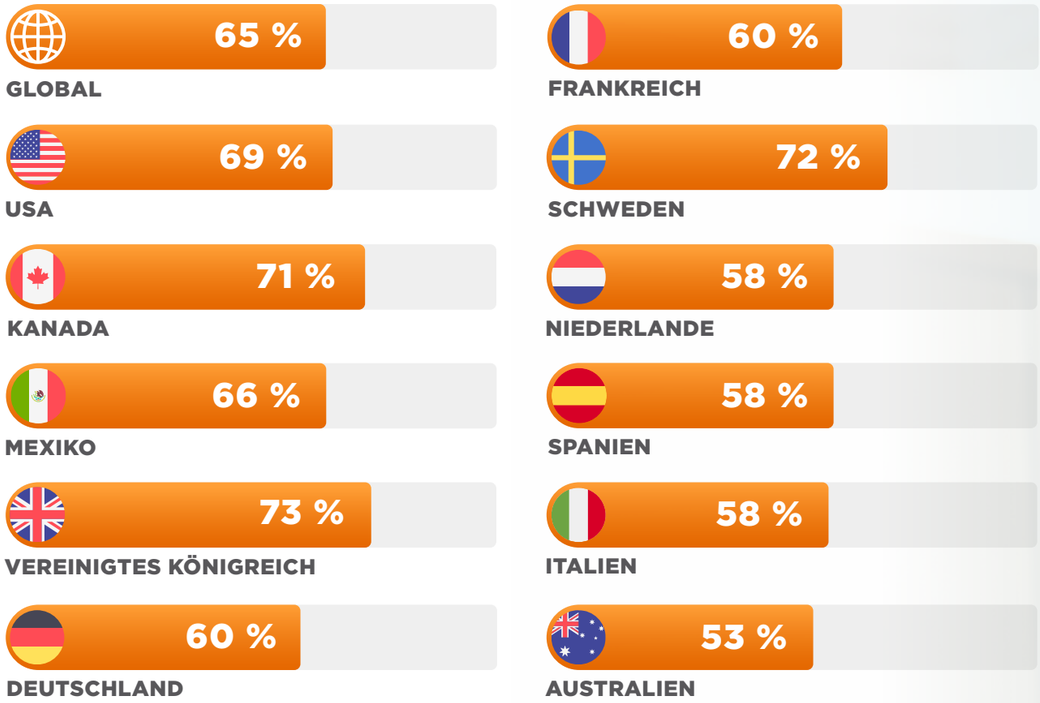
Signifikante

96 %

von IT-Führungskräften berichteten von Herausforderungen mit diesen Technologien.

Eines der Hauptprobleme ist die fehlende Integration zwischen Systemen, die für vernetzte Geräte und Telemedizin-Anwendungen verwendet werden. Dieses Problem spiegelt sich in den folgenden Statistiken verschiedener Regionen wider.

Systeme für IoT-/Telemedizin-Geräte sind nicht integriert:



Die größte Herausforderung für **65 %** der Organisationen in diesem Jahr ist die mangelnde Integration zwischen diesen Systemen. Diese Frage umfasst Herausforderungen der Interoperabilität, wie zum Beispiel die Unfähigkeit, auf die vollständigen Informationen eines Patienten an einem einzigen Ort zuzugreifen (gemeldet von **43 %** der Befragen), sowie das Fehlen automatischer Updates über alle Systeme hinweg (**40 %**). Zusätzlich äußerten **65 %** der IT-Entscheidungsträger Frustration darüber, dass ihre Organisationen Schwierigkeiten haben, den richtigen Personen relevante Daten zur Verfügung zu stellen, wenn diese am dringendsten benötigt werden.

Diese Herausforderungen sind auf globaler Ebene erkennbar, sind aber besonders ausgeprägt in Australien (**77 %**), Großbritannien (**73 %**) und Kanada (**71 %**). Integrationsprobleme sind auch bei den Gesundheitsorganisationen weit verbreitet, die über mehrere Fachgebiete hinweg tätig sind. Unter denen, die diese Schwierigkeiten haben, stammen **69 %** aus allgemeinen Arztpraxen oder Kliniken, während **67 %** aus Kliniken stammen, die eine oder mehrere Spezialdienstleistungen anbieten. Im Vergleich dazu berichteten **62 %** der IT-Entscheidungsträger in Krankenhäusern, die direkte Patientenversorgung anbieten, und **60 %** der Organisationen, die sich auf Remote- oder Telemedizin-Dienste konzentrieren, ähnliche Integrationsprobleme.

ALTSYSTEME ERZEUGEN PROBLEME BEI INTEGRATION UND INTEROPERABILITÄT

Der Prozentsatz der IT-Entscheidungsträger, deren Unternehmen veraltete Technologie verwenden, ist von **63 %** im Jahr 2024 auf **55 %** in diesem Jahr gesunken. Dennoch melden **97 %** der IT-Entscheidungsträger, dass ihre Organisation veraltete Technologie nutzt. Etwa die Hälfte der Anwender von Bestandssystemen hält die Technik nicht für veraltet, aber sie wirkt sich darauf aus, wie leicht sich Unternehmen an neue Arbeitsweisen anpassen können.

Vier von zehn (**38 %**) IT-Entscheidungsträgern sagten, dass veraltete IT sie daran hindere, neue Geräte/Drucker bereitzustellen und zu verwalten. Der gleiche Anteil meinte, dass sie Geräte nicht aus der Ferne unterstützen können oder detaillierte Informationen zu Geräteproblemen erhalten.

Welche Auswirkungen hat veraltete Technologie auf Ihren täglichen Betrieb?

Kann neue Geräte/Drucker nicht bereitstellen und verwalten	**38 %**	39 %	46 %	37 %	47 %	37 %	37 %	31 %	33 %	29 %	36 %	43 %
Kann Geräte nicht aus der Ferne unterstützen/ detaillierte Informationen über Geräteprobleme erhalten	**38 %**	38 %	43 %	37 %	53 %	35 %	35 %	38 %	29 %	29 %	33 %	43 %
Zu viel Zeit für Problembehebung	**39 %**	38 %	47 %	39 %	41 %	43 %	36 %	43 %	41 %	29 %	33 %	39 %

Mit der zunehmenden Verbreitung elektronischer Patientenakten (ePA) und dem wachsenden Einsatz von Telemedizin-Geräten rücken Integration und Interoperabilität stärker denn je in den Fokus von Gesundheitseinrichtungen. Allerdings zeigen die diesjährigen Erkenntnisse, dass Probleme der Systemintegration durch Altsysteme nach wie vor ein Hindernis darstellen.

Mehr als drei Viertel (**79 %**) der IT-Entscheidungsträger gaben an, dass die Einführung von ePAs eine erhebliche Herausforderung für ihr Unternehmen war, und **36 %** führen diese Herausforderung direkt auf ihre veraltete IT zurück. Die Auswirkungen veralteter Technologie auf die Einführung/Integration von ePAs sind am stärksten spürbar in Großbritannien (**44 %**), Australien (**42 %**) sowie den USA und Kanada (jeweils **41 %**).

Die Einführung/Integration von ePAs war eine Herausforderung/ wurde von veralteter IT beeinflusst.

Die Einführung/ Integration von elektronischen Patientenakten war eine große Herausforderung für unsere Organisation	**79 %**	74 %	78 %	71 %	92 %	73 %	87 %	66 %	77 %	82 %	84 %	80 %
Veraltete IT hat die Einführung/ Integration von elektronischen medizinischen Unterlagen beeinflusst	**36 %**	41 %	41 %	35 %	44 %	33 %	31 %	33 %	27 %	27 %	37 %	42 %

Die Daten deuten darauf hin, dass die Anpassung des Menschen für den effektiven Einsatz neuer Technologien unerlässlich ist. **30 %** der Befragten sagten, Systeme werden zu oft geändert, als dass die Organisation mit den Änderungen Schritt halten kann. Weitere **33 %** sagten, dass die Schulung von Benutzern auf neuen Systemen Prozesse verlangsamt und die Patientenbetreuung beeinträchtigt. Die größere Herausforderung für den reibungslosen Betrieb von IoT- und Telemedizin-Geräten liegt jedoch in den veralteten Systemen der Gesundheitsbranche:

90 % **der Organisationen fordern mehr Investitionen in neue oder bessere Technologien zur Verbesserung der Patientenversorgung und**

89 % **für mehr vernetzte Geräte.**

ALTSYSTEME ERZEUGEN SICHERHEITSRISIKEN

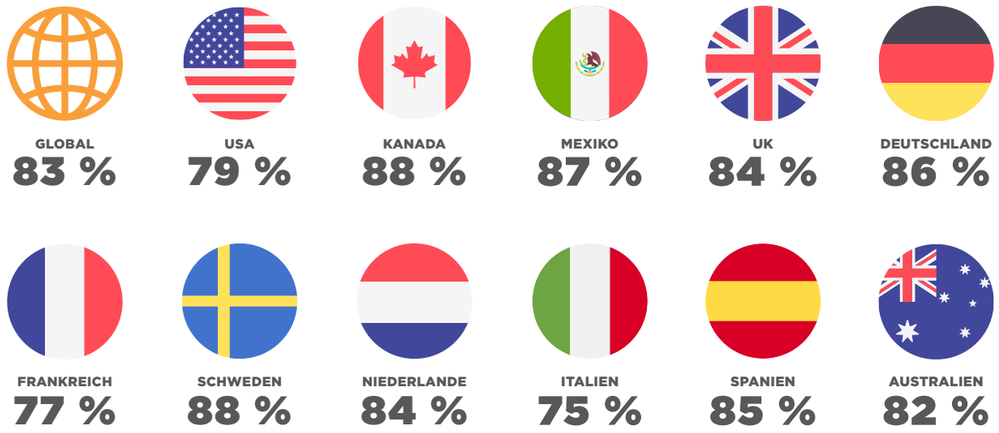
Mehr als acht von zehn (83 %)
IT-Entscheidungsträgern sagten, dass ihre Organisation seit 2023 mindestens einen **Datenbruch/Leck oder Ransomware-Angriff** erlebt habe.

Dies stimmt mit den Zahlen von 2024 überein (**85 %**), was darauf hindeutet, dass diese Bedrohungen genauso weit verbreitet sind und nicht wirksam bekämpft werden.

Der Gesamtprozentsatz der Unternehmen, die von Vorfällen betroffen sind, hat sich im Vergleich zum Vorjahr zwar kaum verändert, aber nun hat fast die Hälfte ein versehentliches Datenleck (**48 %**, im Vergleich zu 2022, als es **33 %** waren) und zwei Drittel haben eine Datenverletzung durch eine externe Quelle oder einen Ransomware-Angriff erlebt (**65 %**, im Einklang mit 2024, aber höher als **48 %** in 2022 und **52 %** in 2023).

Die einzige Kategorie, die in diesem Jahr eine signifikante Veränderung erfahren hat, ist der Prozentsatz der IT-Entscheider, die ein geplantes Datenleck von Mitarbeitern melden. Dieser ist von **34 %** im Jahr 2024 auf **24 %** im Jahr 2025 gesunken.

Einen oder mehrere Sicherheitsvorfälle in den letzten 12 Monaten erfahren:



Da die Zahl geplanter Datenschutzverletzungen durch Mitarbeiter in diesem Jahr voraussichtlich zurückgeht, könnten menschliche Risikofaktoren in der Datensicherheit allmählich eingedämmt werden – technologiebedingte Schwachstellen hingegen bleiben weiterhin eine Herausforderung.

In diesem Jahr gibt fast die Hälfte der IT-Entscheider (**45 %**) der veralteten IT die Schuld daran, dass Netzwerke anfällig für Sicherheitsangriffe sind; im Jahr 2024 waren es noch **36 %**.

Das Problem betrifft Organisationen in der ganzen Welt, aber in einigen Ländern es ist eine größere Herausforderung: Über die Hälfte der IT-Entscheidungsträger in Schweden (**55 %**), Frankreich (**54 %**), Australien (**53 %**) und Kanada (**51 %**) sind nun besorgt, dass ihr Netzwerk wegen der vorhandenen veralteten IT anfällig für Sicherheitsangriffe ist.

Die Bedenken hinsichtlich veralteter IT-Systeme wachsen Jahr für Jahr und erhöhten sich in allen in der Umfrage berücksichtigten Ländern. Werden die Probleme mit Altsystemen nicht behoben, sehen sich Organisationen zunehmend mit Sicherheitsbedrohungen, operativen Ineffizienzen und einer kompromittierten Patientenversorgung konfrontiert.

„Veraltete IT macht unser Netzwerk anfällig für Sicherheitsangriffe“.

	2025	2024		2025	2024
Global	**45 %**	**36 %**	Frankreich	**54 %**	**27 %**
USA	44 %	39 %	Schweden	55 %	25 %
Kanada	51 %	43 %	Niederlande	40 %	37 %
Mexiko	39 %	35 %	Italien	37 %	-
UK	43 %	40 %	Spanien	41 %	-
Deutschland	45 %	33 %	Australien	53 %	39 %

Vier von zehn (**38 %**) können Geräte nicht aus der Ferne unterstützen oder detaillierte Informationen zu Geräteproblemen erhalten. Einer von fünf (**20 %**) sagte, dass keine neuen Geräte erkannt werden können, die sich mit dem System verbinden. Veraltete IT wird in **97 %** der Gesundheitsorganisationen verwendet. Basierend auf den diesjährigen Forschungen bleiben die Probleme mit Integration, Wartung und Sicherheit bestehen.

ALTSYSTEME ERZEUGEN MEHR ARBEIT FÜR IT-TEAMS

Häufige technische Probleme und Ausfallzeiten stellen eine weitere Herausforderung dar, wenn vernetzte Geräte und Telemedizin-Geräte verwendet werden. Dies betrifft **59 %** der Organisationen in diesem Jahr, gegenüber **52 %** im Jahr 2022.

Hat Ihr Unternehmen häufige technische Probleme/Ausfallzeiten mit IoT-/Telemedizin-Geräten erlebt?

GLOBAL	USA	KANADA	MEXIKO	VEREINIGTES KÖNIGREICH	DEUTSCHLAND
59 %	62 %	73 %	52 %	64 %	61 %

FRANKREICH	SCHWEDEN	NIEDERLANDE	ITALIEN	SPANIEN	AUSTRALIEN
53 %	58 %	48 %	47 %	57 %	66 %

Technische Ausfallzeiten im Gesundheitsumfeld können zu Unterbrechungen der Patientenversorgung führen, wodurch die betriebliche Effizienz insgesamt beeinträchtigt wird. Organisationen stehen vor Herausforderungen im Zusammenhang mit Systemaktualisierungen und -wartung, die zu ineffizienten Abläufen und einer Verringerung der Versorgungsqualität führen.

Die Herausforderungen werden weltweit gespürt, aber technische Probleme und Ausfallzeiten treten in den folgenden Ländern deutlich häufiger auf: Kanada (**73 %**), Australien (**66 %**) und Großbritannien (**64 %**).

Während sich IT-Teams auf strategische Projekte konzentrieren, stecken sie oft in zeitraubenden Aufgaben im Zusammenhang mit der Problembehebung von geringfügigen technischen Problemen fest. Dazu gehören zum Beispiel die Reparatur von Druckern, Verbindungsprobleme und andere wiederkehrende Support-Aufgaben. Ein Großteil dieses Problems wird durch veraltete IT verursacht: **39 %** der IT-Entscheidungsträger gaben an, dass dies dazu führt, dass sie zu viel Zeit mit der Behebung von Problemen verbringen. Diese Ineffizienz schmälert die Fähigkeit, sich auf wirkungsvollere Initiativen zu konzentrieren, die organisatorische Verbesserungen vorantreiben. Gesundheitsorganisationen müssen über die Implementierung von Lösungen nachdenken, die zur Integration bestehender und neuer Technologien beitragen können.

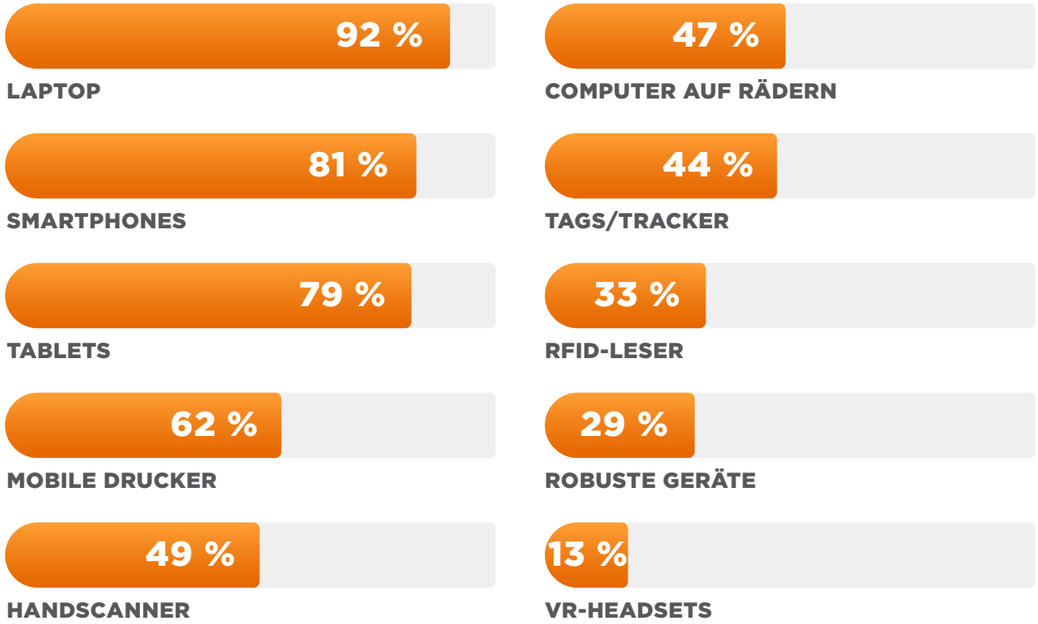
DER WEG IN DIE ZUKUNFT:

ENTERPRISE MOBILITY MANAGEMENT HAT DAS MOBILE DEVICE MANAGEMENT ABGELÖST

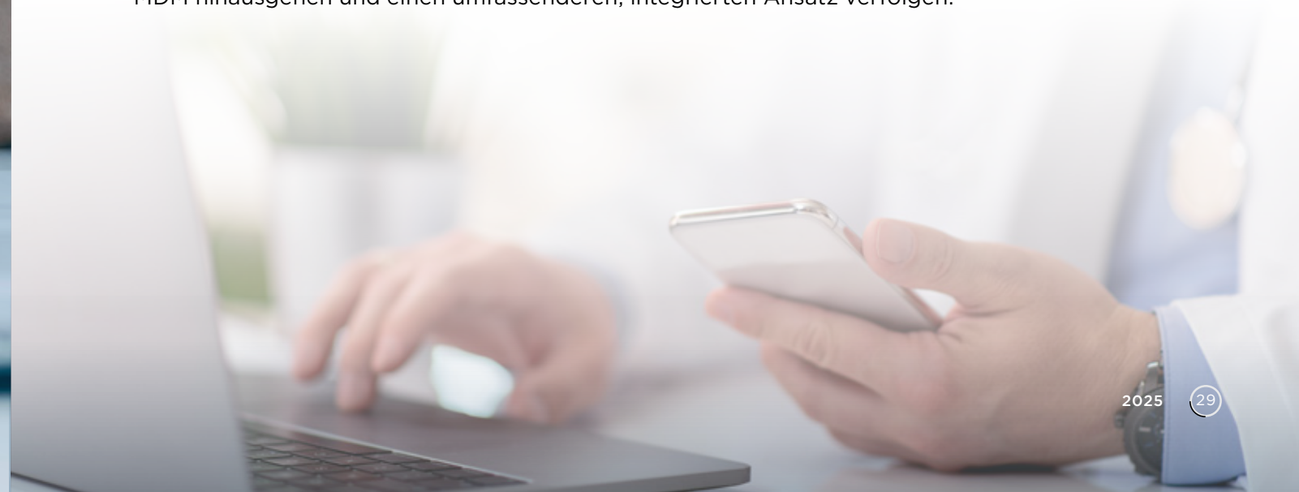
Die zunehmende Integration verschiedener mobiler Geräte, die breitere Verwendung von Druckern und ein breites Anwendungsspektrum im täglichen Gesundheitswesen erfordert eine robuste Lösung für die Geräteverwaltung.

Welche der folgenden Mobilgeräte werden in Ihrem Unternehmen verwendet?

Globale Ergebnisse



Mit einer so vielfältigen Geräteflotte stehen Gesundheitsorganisationen vor der Herausforderung, die Sicherheit zu wahren, Remote-Fehlerbehebung durchzuführen und sicherzustellen, dass alle Geräte optimal funktionieren. Für IT-Entscheidungsträger ist eine nahtlose Verbindung mit diesen Geräten von entscheidender Bedeutung. Um diesen Anforderungen gerecht zu werden, müssen Gesundheitsorganisationen über das traditionelle MDM hinausgehen und einen umfassenderen, integrierten Ansatz verfolgen.



DER WACHSENDE BEDARF AN EMM-LÖSUNGEN

Zweifellos hat mobile Technologie ihre Berechtigung, da **86 %** der IT-Entscheidungsträger sagen, dass sie dadurch ihre Jobs schneller erledigen können. Allerdings deutet die Zahl der im Umlauf befindlichen Geräte darauf hin, dass es viele mobile Geräte zu verfolgen, zu warten und zu verwalten gibt, wobei die Mehrheit MDM aus Sicherheitsgründen verwendet (**90 %**). Dazu gehört die Verwaltung von Sicherheitsrichtlinien, der Schutz vor Cyberbedrohungen und die Identifizierung von unbefugten Geräten, die auf das Netzwerk zugreifen. Das alles ist entscheidend für die Minimierung von Schwachstellen und die Verringerung des Risikos von Verletzungen.

Welche Funktionen einer MDM-Lösung sind für Ihren Betrieb entscheidend?

Sicherheitsverwaltung	63 %
Schutz vor Cyber-Bedrohungen/Identifizierung externer Geräte, die auf das Netzwerk zugreifen	56 %
Methoden zur Reduzierung von Anfälligkeiten für externe Bedrohungen/Reduzierung der Chancen für Hacker	48 %
Remote-Fehlerbehebung	47 %
App-Verwaltung	47 %
Gerätepositionsbestimmung	45 %
Compliance und Durchsetzung von Richtlinien	44 %
Beschränkung des Zugriffs auf Gerätefunktionen in bestimmten Umgebungen	38 %
NETTO: Sicherheitsrelevant (Sicherheitsverwaltung oder Schutz vor Cyberbedrohungen/Identfifizierung externer Geräte, die auf das Netzwerk zugreifen oder Methoden zur Reduzierung von Anfälligkeiten für externe Bedrohungen /Reduzierung der Chancen für Hacker)	90 %

Viele Gesundheitsorganisationen vertrauen auf MDM-Lösungen für grundlegende Sicherheit und Geräteverwaltung, aber das ist nur der Anfang. In der heutigen schnelllebigen Umgebung des Gesundheitswesens, in der viel auf dem Spiel steht, ist ein einfaches MDM nicht mehr ausreichend.

Angesichts der zunehmenden Komplexität der Patientenversorgung und der steigenden Anzahl vernetzter Geräte müssen Unternehmen von reaktiven zu proaktiven Strategien übergehen, die Probleme erkennen und verhindern, bevor sie die Versorgung beeinträchtigen. Das bedeutet, dass über die Grundlagen hinausgegangen und eine Echtzeitüberwachung implementiert werden muss, um Sicherheitsverletzungen und Betriebsstörungen vorzubeugen.

Zwei Drittel (**65 %**) der IT-Entscheidungsträger berichten, dass ihre Organisation in den letzten 12 Monaten einen Datenbruch durch eine externe Quelle oder einen DDoS-Ransomware-Angriff erlitten hat. Dies unterstreicht die Notwendigkeit, über die Grundlagen hinauszugehen und fortschrittlichere und umfassendere Sicherheitsmaßnahmen umzusetzen.

Datensicherheit steht noch immer ganz oben auf der Liste der IT-Bedenken, wobei sie **30 %** der IT-Entscheidungsträger erwähnt wird. Der Prozentsatz, der sie als Hauptsorge nennt, stieg weiterhin deutlich von **16 %** im Jahr 2023 und **23 %** im Jahr 2024. Nimmt man noch die **13 %** hinzu, die angaben, dass die Sicherheitsverwaltung gemeinsam genutzter Geräte ihre größte Sorge in diesem Jahr war, so stellt man fest, dass fast die Hälfte (**43 %**) ein sicherheitsbezogenes Problem als die größte Sorge der IT-Abteilung ihres Unternehmens bezeichnet.

Was ist derzeit die größte Herausforderung für die IT-Abteilung in Ihrer Organisation?

Datensicherheitsbedenken oder die Sicherheitsverwaltung von gemeinsam genutzten Geräten

	2025	2024		2025	2024
	43 %	**35 %**		51 %	25 %
	41 %	43 %		39 %	33 %
	53 %	39 %		31 %	28 %
	43 %	32 %		36 %	-
	39 %	43 %		50 %	-
	41 %	24 %		53 %	39 %

Datensicherheit ist in diesem Jahr die größte Sorge für alle Länder, wobei einige Länder einen besonders starken Anstieg verzeichnen:

In **Frankreich** wurden 2024 Sicherheitsprobleme von **25 %** als Hauptanliegen eingestuft, während es 2025 **51 %** waren,

in **Kanada** stieg es von **39 %** im letzten Jahr und ist jetzt für **53 %**,

in **Australien** sprang es von **39 %** auf **53 %**

und in **Deutschland** von **24 %** auf **41 %**.

Es liegt in der Natur mobiler Geräte, dass sie von mehreren Nutzern verwendet werden. Es überrascht daher nicht, dass die Verwaltung der Sicherheit gemeinsam genutzter Geräte nach wie vor zu den wichtigsten IT-Anliegen gehört. Hinzu kommt die Herausforderung der veralteten Technologie, die die Fernsteuerung dieser Geräte nahezu unmöglich macht. Mobile Geräte werden daher zu einem zweischneidigen Schwert.

„Standardmäßige“ MDM-Funktionen reichen für das moderne Technologieumfeld und all die vorhandenen komplexen Geräte und Systeme nicht mehr aus. Die historischen MDM-Fähigkeiten haben ihre Grenzen erreicht. Heute ist die Notwendigkeit fortschrittlicher Technologielösungen wichtiger denn je. Moderne EMM-Tools verschaffen Organisationen im Gesundheitswesen einen besseren Einblick in ihr gesamtes Geräte-Ökosystem und ermöglichen es ihnen, den Betrieb besser zu überwachen, die Datensicherheit zu verbessern und schneller auf neue Bedrohungen zu reagieren.

DIE SICHERHEIT MOBILER GERÄTE PRIORISIEREN: ALLE BEREICHE ABDECKEN

Organisationen priorisieren Maßnahmen, die sicherstellen, dass mobile Geräte geschützt sind. Einige Unternehmen konzentrieren sich auf einen menschenzentrierten Ansatz: **45 %** schulen ihre Mitarbeiter über Sicherheitsbedrohungen, bewährte Verfahren und Datenschutzgesetze, während eine ähnliche Anzahl den Zugang zu sensiblen Daten auf der Grundlage von Rollen und Verantwortlichkeiten einschränkt. Doch nur ein Drittel (**33 %**) hat einen Plan für die Reaktion auf Vorfälle, sollte etwas schiefgehen.

Die Durchführung regelmäßiger Updates ist die am häufigsten implementierte Sicherheitsmaßnahme und wird von **51 %** der Befragten ergriffen. Deutlich mehr derjenigen, die in den letzten 12 Monaten keinen Datensicherheitsvorfall erlebt haben, (**60 %**) verfolgen diesen Ansatz (im Vergleich zu nur **49 %** derjenigen, die einen Vorfall erlebt haben). Die Mehrfach-Faktor-Authentifizierung wird von **44 %** verwendet; mit Verschlüsselung sind es noch **42 %**.

Es ist offensichtlich, dass alle Organisationen irgendetwas tun, um mobile Geräte zu schützen, aber nur wenige tun alles, was sie können.

DIE NOTWENDIGKEIT FÜR BESSERE STRATEGIEN ZUR VERWALTUNG MOBILER GERÄTE

Sicherheit ist nicht der einzige Aspekt, bei dem veraltete MDM-Lösungen nicht ausreichen. Viele Organisationen des Gesundheitswesens sehen sich mit Unstimmigkeiten bei der Anwendung dieser Lösungen auf verschiedene Geräte konfrontiert, was die Nachverfolgung und Unterstützung von Geräten erschwert. Diese Unstimmigkeiten führen oft zu unnötigen Gerätewechseln und Ineffizienzen im Gesamtbetrieb.

Fast die Hälfte (**47 %**) der IT-Entscheidungsträger gibt an, dass eine MDM-Lösung für ihr Unternehmen entscheidend ist, um Fehler aus der Ferne zu beheben, und **45 %** sagen, dass sie für die Geräteverfolgung entscheidend ist. Aber **38 %** der Unternehmen sind aufgrund von Altsystemen nicht in der Lage, neue Geräte und Drucker einfach zu implementieren und zu verwalten, und **38 %** sind aus demselben Grund nicht in der Lage, Geräte aus der Ferne zu unterstützen oder detaillierte Informationen über Geräteprobleme zu erhalten.

Die Studie unterstreicht die Notwendigkeit für Gesundheitsorganisationen, robuste, zentralisierte EMM-Lösungen einzuführen, die Gerätesicherheit und Compliance gewährleisten. Diese Lösungen sollten auch die Remote-Fehlerbehebung unterstützen, die Konfiguration rationalisieren und relevante Insights liefern.

Erweiterte Tools, die Analytik und Zustandsanalyse auf allen Geräten zur Verfügung stellen, ermöglichen es IT-Teams, Probleme bei der Geräteleistung proaktiv zu identifizieren. Sie können auch Nutzungstrends verfolgen und Organisationen Einblicke geben, um fundierte Entscheidungen zu treffen. Dieser Ansatz reduziert Ausfallzeiten, minimiert Ineffizienzen und verbessert die allgemeine Qualität der Versorgung.

MEDIZINTECHNIK FÜR DEN EINMALGEBRAUCH

Die Bedenken hören nicht auf, wenn ein mobiles Gerät nicht mehr benutzt wird, sondern nehmen oft zu. Tatsächlich sind **81 %** der IT-Entscheidungsträger über die Sicherheit der Patientendaten während der Geräteentsorgung besorgt.

Gesundheitsorganisationen verarbeiten massive Mengen sensibler Daten, und ohne standardisierte Entsorgungsprozesse stellen stillgelegte Geräte ernsthafte Risiken durch Datenverletzungen und Verstöße gegen behördliche Auflagen dar. Obwohl die meisten Unternehmen Maßnahmen zum Schutz von Daten bei der Geräteentsorgung ergreifen, gibt es nach wie vor viele Unstimmigkeiten, und auch in diesem Jahr äußern acht von zehn IT-Entscheidungsträgern Bedenken.

Häufige Upgrades verschlimmern das Problem. **31 %** der Organisationen ersetzen Geräte auf Anfrage des Benutzers, **40 %** tun es, wenn neuere Modelle verfügbar sind, **41 %** ersetzen sie auf der Grundlage von Vertragsbedingungen und **31 %**, wenn Garantien ablaufen. Dies wirft große Bedenken hinsichtlich Sicherheit und Nachhaltigkeit auf.

Um das Risiko zu verringern, müssen Organisationen standardisierte Protokolle implementieren, einschließlich der Remote-Datenlöschung und eines stabilen Lebenszyklus-Managements, um eine ordnungsgemäße Nachverfolgung und Entsorgung sicherzustellen. Das Personal sollte auch regelmäßig über sichere Entsorgungspraktiken unterrichtet werden. Durch die Priorisierung sicherer und nachhaltiger Prozesse können Gesundheitsorganisationen Patientendaten besser schützen und Compliance-Standards erfüllen.

Wie sieht die Richtlinie Ihrer Organisation für Upgrades/ Erneuerung/Ersatz von Geräten wie den oben genannten aus, z. B. Smartphones, Tablets, robuste Geräte usw.?

	Wir machen dies irgendwann in Abhängigkeit von ihrer Vertragslaufzeit, ob sie noch funktionieren oder nicht.	Wir machen dies, wenn ein neueres/ fortschrittlicheres Modell verfügbar ist.	Wir machen dies, wenn Benutzer es anfordern.	Wir machen dies, wenn die Garantie abläuft.	Wir machen dies nur für Geräte, die nicht mehr funktionieren.
	41 %	**40 %**	**31 %**	**31 %**	**5 %**
	38 %	48 %	37 %	38 %	6 %
	41 %	47 %	33 %	32 %	5 %
	50 %	37 %	26 %	30 %	8 %
	49 %	43 %	43 %	49 %	2 %
	45 %	39 %	39 %	25 %	6 %
	34 %	41 %	25 %	23 %	7 %
	39 %	35 %	20 %	31 %	5 %
	37 %	27 %	27 %	25 %	6 %
	39 %	37 %	18 %	31 %	4 %
	41 %	41 %	28 %	21 %	6 %
	40 %	47 %	35 %	29 %	4 %

In den USA, Kanada und Australien meldet der höchste Prozentsatz der Befragten, dass Geräte ersetzt werden, wenn eine neue Version verfügbar ist. Es ist jedoch wichtig, darauf hinzuweisen, dass dies ein allgemeiner Trend ist, der weltweit beobachtet werden kann. Es ist von entscheidender Bedeutung, ein Gleichgewicht zwischen Nachhaltigkeit und Leistung der Geräte zu finden. Werden Geräte erst entsorgt, wenn sie nicht mehr funktionieren, werden IT-Teams noch mehr Zeit damit verbringen, kleine Probleme zu beheben.

VERWALTUNG DES AKKUZUSTANDS – PRÄVENTION IST BESSER ALS HEILUNG

Die ineffiziente Überwachung des Akkuzustands kann auch ein Grund für unerwartete Geräteausfälle im Gesundheitswesen sein. Höhere Kosten aufgrund des vorzeitigen Austauschs von Geräten, die zu finanziellen Zwängen führen, sowie Umweltbedenken hinsichtlich der Entsorgung von Elektroschrott sind weit verbreitet. **97 %** der Organisationen überwacht aktiv den Akkuzustand, aber nur ein Drittel (**31 %**) sagen, dass sie Geräte nur dann überprüfen, wenn Probleme auftreten.

41 % folgen der Richtlinie, Akkus auf Grundlage eines festen Zeitplans zu ersetzen, unabhängig von ihrem Zustand. Etwas beruhigender ist, dass die Hälfte regelmäßige manuelle Kontrollen durchführt, **44 %** eine automatische Überwachung des Akkuzustands einsetzen und **41 %** ein vorausschauendes Wartungssystem eingerichtet haben.

Letztlich deuten die Ergebnisse darauf hin, dass mobile Geräte zwar unbestreitbare Vorteile bieten, Ihre Verwaltung aber optimiert werden muss: EMM-Lösungen sollten eingeführt werden, um bewährte Methoden für die Geräteverfolgung, die Überwachung des Akkuzustands sowie nachhaltige Ersatzstrategien zu etablieren. Diese Schritte würden nicht nur den täglichen Betrieb rationalisieren, sondern auch den Weg für strategischere IT-Initiativen im gesamten Gesundheitswesen ebnen.

SCHLUSS-FOLGERUNG

Der Gesundheitssektor setzt seine digitale Transformationsreise rasant fort, aber der Weg bleibt komplex. Trotz des weit verbreiteten Einsatzes von IoT- und Telemedizin-Geräten bereiten veraltete Systeme Probleme wie unvollständige Datenkonsolidierung und häufige technische Unterbrechungen, die IT-Teams daran hindern, die Vorteile ihrer digitalen Transformation zu nutzen.

Gleichzeitig haben sich sicherheitsrelevante Themen für **43 %** der IT-Entscheider als wichtigstes Anliegen herauskristallisiert, angetrieben durch Bedrohungen, die von der Verwaltung gemeinsam genutzter Geräte bis hin zu zunehmenden Datenschutzverletzungen reichen. Während geplante Datenlecks durch Mitarbeiter leicht zurückgegangen sind, offenbaren versehentliche Lecks und ausgefeilte externe Angriffe weiterhin Schwachstellen. Fast die Hälfte der IT-Führungskräfte nennt Altsysteme als Hauptgrund für die Anfälligkeit von Netzwerken für Angriffe, was die dringende Notwendigkeit unterstreicht, die grundlegenden Technologien zu modernisieren. Es scheint, dass das Problem weniger die sich entwickelnde Technologie selbst ist, sondern die Systeme, die sie unterstützen.

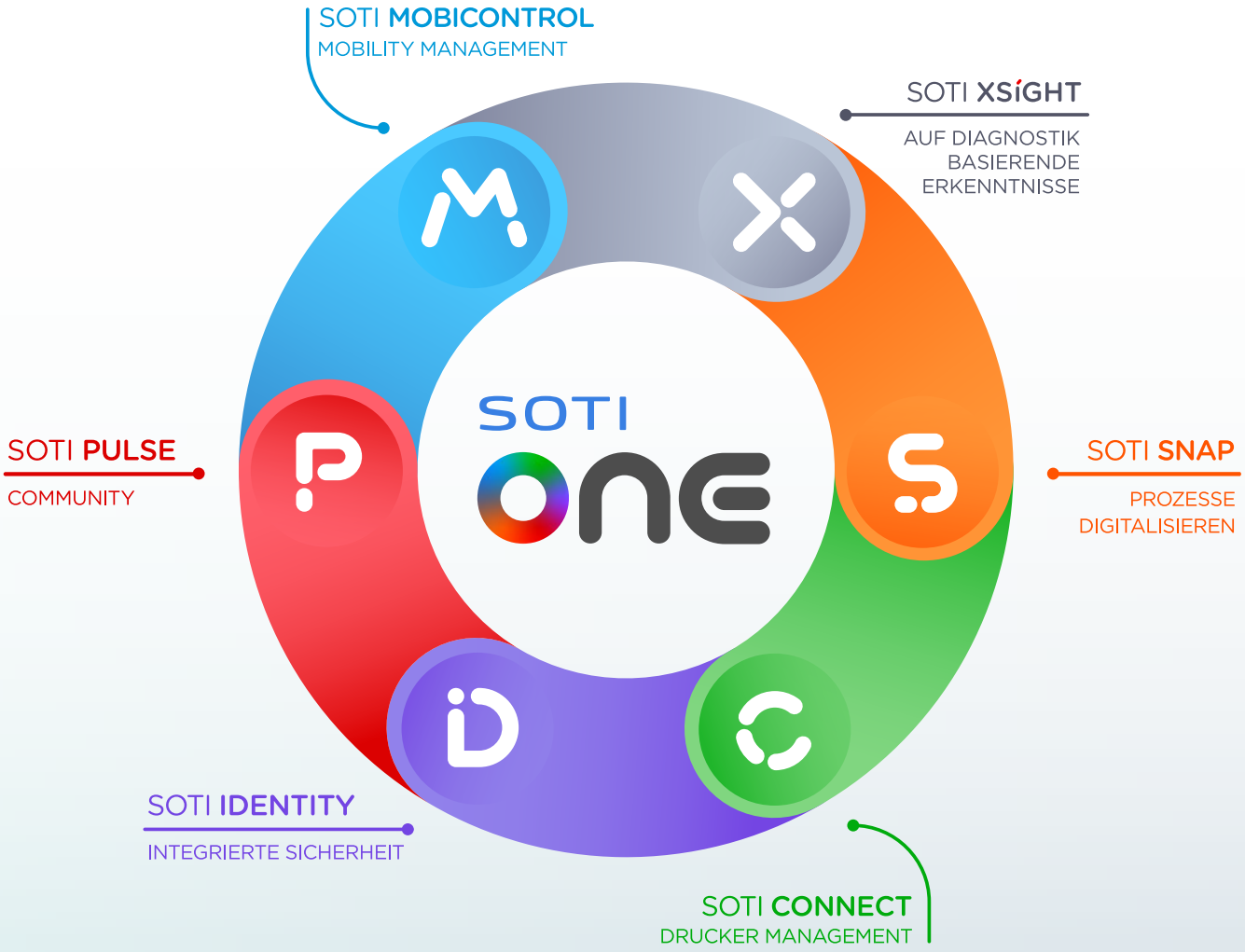
Die Einführung von KI hat weltweit stark zugenommen und wird in diesem Jahr in einem Drittel mehr Unternehmen eingesetzt, wobei Regionen wie Großbritannien und Australien den Weg weisen. KI wird in medizinische Datenanalyse, Behandlungsplanung, personalisierte Patientenbetreuung und darüber hinaus integriert. Ein Rettungsanker für die überlastete Gesundheitsindustrie, aber die Notwendigkeit, ihre Nutzung zu überwachen und für Sicherheit zu sorgen, darf nicht übersehen werden.

Darüber hinaus erweist sich die Verwaltung mobiler Geräte als erhebliche Belastung für die IT-Ressourcen, und die Vielzahl der verwendeten Geräte erschwert eine wirksame Überwachung und Fernverwaltung. Die Unzulänglichkeit bestehender MDM-Lösungen sowie uneinheitliche Ersatzrichtlinien stellen eine zusätzliche Belastung dar und verstärken sowohl die Sicherheits- als auch die Nachhaltigkeitsbedenken.

Letzten Endes erfordert die Verwirklichung einer echten digitalen Transformation im Gesundheitswesen, dass Organisationen einen Schritt zurückgehen und das Gesamtbild betrachten. Benötigt wird eine Strategie, die die weitere breite Einführung innovativer Technologien mit gezielten Investitionen in die Modernisierung und Integration von IT-Infrastrukturen sowie einer zweckmäßigen EMM-Lösung kombiniert. Dieser ausgewogene Ansatz wird es Organisationen ermöglichen, Daten zu sichern, die Nutzung mobiler Geräte zu rationalisieren und letztlich die Patientenversorgung zu verbessern.

ÜBER SOTI

SOTI ist ein innovativer und branchenführender Anbieter intelligenter, schneller, und zuverlässiger Enterprise-Mobility-Lösungen für Unternehmen. Mit dem innovativen Lösungsportfolio von SOTI können Unternehmen ihre mobilen Prozesse rationalisieren, ihren ROI maximieren sowie Geräteausfallzeiten reduzieren. Mit mehr als 17.000 Kunden weltweit hat sich SOTI als zuverlässiger Anbieter mobiler Plattformen für die Verwaltung, Sicherung und Unterstützung geschäftskritischer Geräte bewährt. Mit dem hervorragenden Support von SOTI können Unternehmen die Möglichkeiten ihrer mobilen Geräteflotte voll ausschöpfen.



UM MEHR ZU ERFAHREN:

Für weitere Informationen darüber, wie SOTI Ihrem Geschäft zu größerem Erfolg verhelfen kann, **klicken Sie hier**.
Um mehr über die SOTI ONE Plattform zu erfahren, **klicken Sie hier**.
Um herauszufinden, wie SOTI Ihnen bei Ihren mobilen Investitionen helfen kann, kontaktieren Sie uns noch heute unter **sales@soti.net**.

SOTI ist ein bewährter Anbieter und Branchenführer für die Vereinfachung von geschäftskritischen Mobility-Lösungen, indem er diese intelligenter, schneller und zuverlässiger macht. SOTI unterstützt Unternehmen auf der ganzen Welt dabei, ihre Mobility zu unendlichen Möglichkeiten zu führen.

soti.de

052725