SOTI

UNE PLATEFORME
POUR TOUT CONNECTER

DILEMME NUMÉRIQUE ET SANTÉ :

DÉCRYPTER LES RISQUES ET LES DÉFIS ÉMERGENTS

MOT DE BIENVENUE

Le secteur de la santé est sur le point de connaître une avancée numérique majeure. Les innovations en IA, télésanté, technologie mobile et automatisation ouvrent de nouvelles perspectives pour des soins plus intelligents et mieux connectés. Malgré ces avancées, de nombreuses organisations de santé restent freinées par des systèmes hérités et des inefficacités opérationnelles, limitant leur capacité à adopter pleinement les innovations numériques.

Pour les responsables informatiques, le défi est évident. Les organisations doivent accélérer l'adoption des technologies modernes afin d'améliorer les résultats, de donner plus de moyens au personnel et de fournir des expériences de soins fluides, à la hauteur des attentes des patients.

Les systèmes hérités entraînent des retards dans l'accès aux informations essentielles, ce qui affecte directement la qualité des soins et limite la réactivité des professionnels de santé. Parallèlement, l'IA peut améliorer les diagnostics, rationaliser les flux de travail et anticiper les besoins des patients, à condition d'être soutenue par une infrastructure moderne et performante.

Stephanie Lopinski, vice-présidente, marketing mondial

Le niveau d'intégration des nouvelles technologies et la capacité à exploiter pleinement le potentiel des appareils et applications jouent un rôle essentiel dans l'amélioration des résultats pour les patients et la qualité des soins délivrés. Les organisations doivent prioriser l'intégration des systèmes, l'accès en temps réel aux données et l'abandon des technologies obsolètes afin de tirer pleinement parti de la transformation numérique.

Notre dernière recherche explore l'état actuel des organisations de santé, les défis auxquels elles sont confrontées et les stratégies à adopter pour progresser.

Le rapport 2025 de SOTI met en avant trois thèmes clés :

Intelligence artificielle

L'adoption de l'IA dans le secteur de la santé connaît une croissance rapide, avec **81 %** des organisations mondiales l'utilisant pour les soins aux patients, contre **61 %** en 2024. Ses applications incluent le traitement des données médicales, la mise à jour des dossiers, la personnalisation des traitements et le diagnostic des maladies.

Malgré une adoption croissante, seulement **36 %** des organisations disposent de mesures de sécurité spécifiques à l'IA, ce qui soulève des inquiétudes quant à la confidentialité des données des patients. Ainsi, la modernisation des systèmes est essentielle pour garantir la confidentialité des données des patients.

Le rapport 2025 dresse un tableau clair : la transformation technologique du secteur de la santé progresse, mais de manière inégale. Tant que les systèmes existants ne seront pas modernisés, que la sécurité des données ne sera pas renforcée et que les ressources IT ne seront pas libérées des problèmes récurrents, le secteur peinera à transformer l'adoption de l'IA en une véritable intégration.

Systèmes hérités

Les organisations de santé peinent à intégrer des systèmes interconnectés et des solutions de télésanté, principalement en raison de systèmes hérités obsolètes, difficiles à gérer à distance.

Ces systèmes représentent des risques de sécurité majeurs, **83 %** des organisations ayant signalé des violations de données, des fuites ou des attaques par ransomware depuis 2023. De plus, ils compliquent l'intégration des dossiers médicaux électroniques (DME), affectant **79 %** des organisations.

Par conséquent, lorsque les organisations tentent d'adopter de nouvelles technologies, les difficultés persistent, freinant l'innovation et ayant un impact négatif sur l'expérience des patients. Finalement, les limites imposées par ces systèmes obsolètes influencent directement les résultats des soins aux patients. Il est donc essentiel que les organisations investissent dans des technologies modernes et des systèmes interconnectés afin d'améliorer l'efficacité, la sécurité et la qualité globale des soins.

Gestion des appareils mobiles + Gestion de la mobilité d'entreprise

Les organisations de santé s'appuient de plus en plus sur une large gamme d'appareils mobiles, notamment des ordinateurs portables, smartphones, tablettes, ainsi que des équipements spécialisés comme les lecteurs RFID. La gestion de ces appareils représente un défi majeur, notamment en matière de sécurité et de dépannage à distance, en raison de l'utilisation de solutions de gestion des appareils mobiles (MDM) obsolètes.

Cependant, le contexte actuel exige une évolution au-delà de la gestion traditionnelle des appareils mobiles (MDM) pour adopter une approche globale de la gestion de la mobilité en entreprise (EMM).

À mesure que la technologie médicale progresse, il devient essentiel de privilégier une plateforme intégrée combinant diagnostics avancés, analyse des données et intelligence opérationnelle. Cette approche offre aux organisations la capacité d'anticiper les problèmes, en exploitant les données et les analyses pour orienter la prise de décision et fluidifier les processus opérationnels. En numérisant les processus et en automatisant les tâches administratives, les prestataires de soins peuvent améliorer leur efficacité opérationnelle et offrir une meilleure prise en charge des patients.

Les solutions de gestion des appareils mobiles doivent également intégrer une gestion complète du cycle de vie pour garantir une durabilité optimale et une efficacité à long terme. Les organisations doivent chercher à maximiser la durée de vie de leurs appareils en exploitant des données sur l'état des batteries et les modes d'utilisation afin de développer des stratégies de remplacement plus durables et efficaces. Cette gestion proactive ne se limite pas à préserver l'état des appareils ; elle renforce également la sécurité en réduisant les vulnérabilités et en protégeant les données des patients.

L'ÉVOLUTION DU PAYSAGE DE LA SANTÉ :

PROGRÈS ET AVANCÉES DEPUIS 2020

SOTI mène des recherches sur le secteur de la santé depuis 2020. Au fil de l'évolution de l'enquête, le nombre de pays et de répondants a augmenté. Les tendances observées au cours des cinq dernières années révèlent les points clés suivants :

2020/2021

- Sécurité : **81 %** expriment des inquiétudes quant à la sécurité des dossiers patients
- Problèmes techniques : **63 %** rencontrent des pannes de dispositif ou de système chaque semaine
- Impact de la technologie sur les soins aux patients : **81 %** rencontrent des problèmes avec les systèmes et la technologie lorsqu'ils prodiguent des soins aux patients

475 aides à domicile, infirmiers et autres professionnels de santé répartis dans sept pays à travers le monde

2022

- Sécurité : **73 %** des organisations ont subi une violation ou une fuite de données depuis 2020
- IoT/Télésanté : **98 %** des organisations ont déployé des dispositifs IoT ou de télésanté
- Impact des temps d'arrêt des dispositifs : **53 %** des organisations déclarent subir des pannes régulières, entraînant des retards dans les soins aux patients et une perte moyenne de 3,4 heures par semaine et par employé due aux interruptions

1 300 professionnels de l'informatique travaillant dans des organisations de santé réparties dans huit pays à travers le monde

2023

- Sécurité des données patients : **97 %** des organisations expriment des préoccupations quant à la protection des dossiers médicaux
- Sécurité du réseau : **55 %** des organisations ont subi une fuite de données interne, qu'elle soit accidentelle ou intentionnelle. **53 %** ne parviennent pas à détecter les nouveaux appareils connectés à leur système en raison de technologies obsolètes, ce qui expose leur infrastructure à des vulnérabilités
- Systèmes hérités : **52 %** disent que les systèmes hérités les empêchent de résoudre les problèmes en temps voulu ; **37 %** pensent que ces systèmes les rendent plus vulnérables aux violations de sécurité
- Temps d'arrêt : 3,4 heures perdues en une semaine normale en raison de difficultés techniques ou liées aux systèmes

1 450 professionnels de l'informatique travaillant dans des organisations de santé réparties dans neuf pays à travers le monde

2024

- IA : **85 %** pensent que l'intelligence artificielle pourrait simplifier les tâches, mais seulement 23 % l'utilisent largement à l'heure actuelle
- Sécurité : **71 %** transfèrent leurs données vers des disques durs externes ou des sauvegardes avant de se débarrasser d'anciens appareils. **23 %** considèrent la sécurité des données comme leur principale préoccupation en matière d'informatique
- IoT/Télésanté : **67 %** rencontrent régulièrement des problèmes avec les dispositifs IoT/télésanté, entraînant des retards dans les soins aux patients.
- Systèmes hérités : **63 %** confirment qu'ils utilisent des technologies obsolètes et **45 %** ont subi une violation de données ou une fuite accidentelle de données au cours de l'année écoulée
- Temps d'arrêt : 3,9 heures perdues par employé chaque semaine en raison des interruptions de service

1 450 professionnels de l'IT et décideurs travaillant dans des organisations de santé réparties dans neuf pays à travers le monde

2025

- IA : **81 %** utilisent désormais l'intelligence artificielle pour les soins aux patients, contre 61 % en 2024
- Sécurité : **83 %** ont été confrontés à une fuite accidentelle de données, une violation externe ou une attaque par ransomware DDoS au cours des 12 derniers mois. **30 %** considèrent la sécurité des données comme leur principale préoccupation en matière d'informatique
- IoT/Télésanté : **96 %** rencontrent des difficultés lors de la mise en œuvre des dispositifs médicaux IoT/télésanté
- Systèmes hérités : **45 %** estiment que les infrastructures IT vieillissantes rendent les réseaux plus vulnérables aux attaques
- Gestion des appareils mobiles : **47 %** estiment que les solutions de gestion des appareils mobiles sont essentielles pour le dépannage à distance

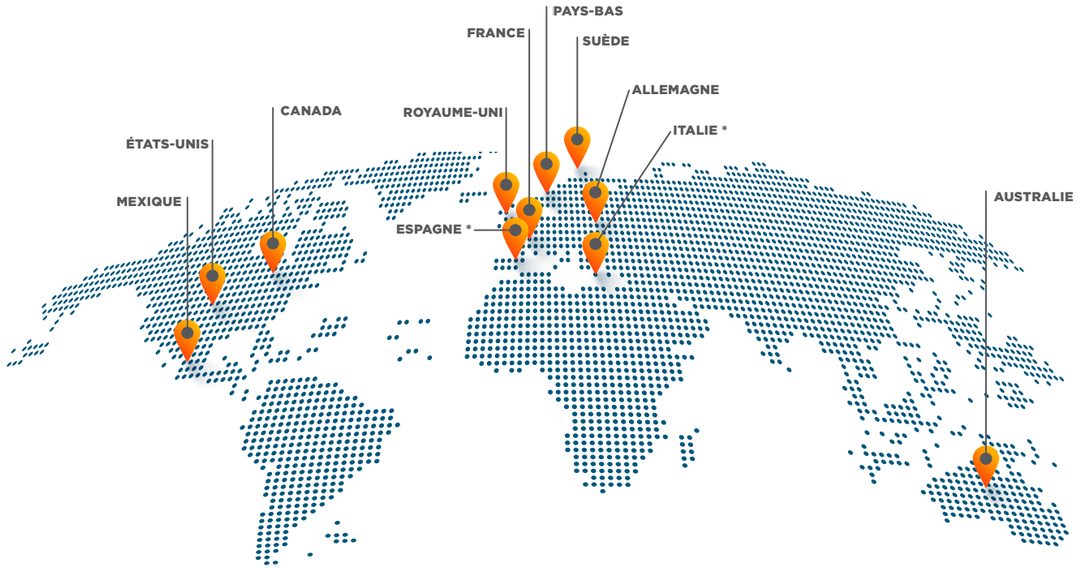
1 750 professionnels de l'IT et décideurs travaillant dans des organisations de santé réparties dans neuf pays à travers le monde

CONTENUS

MÉTHODOLOGIE

Cette année, SOTI a élargi son champ d'étude pour inclure **1 750 répondants répartis dans 11 pays** : États-Unis (200), Canada (150), Mexique (150), Royaume-Uni (200), Allemagne (150), France (150), Suède (150), Pays-Bas (150), Italie* (150), Espagne* (150) et Australie (150). L'enquête a été réalisée entre janvier et mars 2025 par des décideurs informatiques travaillant pour des organisations de santé.

*Nouvelles régions incluses dans le rapport sur les soins de santé de 2025.



RÉPARTITION MONDIALE

Pour ce rapport, les organisations de santé désignent :

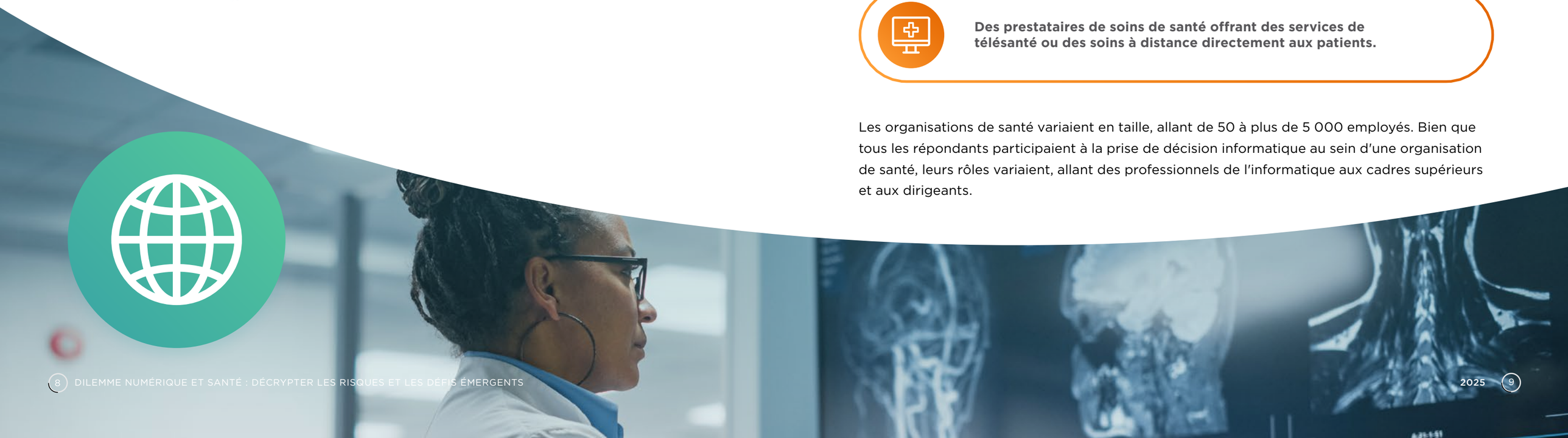
Des hôpitaux offrant des services d'urgence aux patients.

Des cabinets médicaux généraux ou des cliniques regroupant plusieurs spécialistes, tels que des cabinets de médecins ou des médecins traitants.

Des cliniques offrant des services aux patients dans une ou plusieurs spécialités, telles que la santé mentale, la neurologie, la physiothérapie, etc.

Des prestataires de soins de santé offrant des services de télésanté ou des soins à distance directement aux patients.

Les organisations de santé variaient en taille, allant de 50 à plus de 5 000 employés. Bien que tous les répondants participaient à la prise de décision informatique au sein d'une organisation de santé, leurs rôles variaient, allant des professionnels de l'informatique aux cadres supérieurs et aux dirigeants.



RÉSULTATS GLOBAUX

96 %

des organisations rencontrent des difficultés dans la mise en œuvre des dispositifs médicaux IoT/télésanté, l'intégration des systèmes étant le défi le plus important.

83 %

des incidents de sécurité restent élevés, les fuites accidentelles de données, les violations externes et les attaques par ransomware de type DDoS ne montrant aucun signe de ralentissement.

47 %

des décideurs informatiques affirment que les solutions de gestion des appareils mobiles sont essentielles pour le dépannage à distance.

45 %

estiment que les infrastructures IT vieillissantes rendent les réseaux plus vulnérables aux attaques.

81 %

s'inquiètent de la sécurité des données des patients lors de la mise au rebut des appareils mobiles.

81 %

utilisent désormais l'intelligence artificielle d'une manière ou d'une autre pour améliorer l'efficacité et la qualité des soins aux patients, une hausse par rapport à 61 % en 2024.

40 %

des organisations remplacent leurs anciens appareils dès que de nouvelles versions sont disponibles.

30 %

considèrent la sécurité des données comme leur principale préoccupation informatique, par rapport à 23 % en 2024.

AVANCÉE MAJEURE :

L'ESSOR DE L'INTELLIGENCE ARTIFICIELLE DANS LES SOINS AUX PATIENTS

Ces dernières années, le secteur de la santé a connu des avancées transformatrices, notamment grâce à l'intégration des technologies dans les soins aux patients. L'essor de l'intelligence artificielle transforme la manière dont les prestataires de soins de santé dispensent leurs services et interagissent avec les patients.

L'utilisation de l'intelligence artificielle pour améliorer le diagnostic, personnaliser les plans de traitement et optimiser les opérations suscite l'intérêt des organisations de santé à travers le monde. Cette année, notre enquête révèle que l'IA est utilisée dans les soins aux patients par **81 %** des organisations de santé, soit un tiers de plus qu'en 2024 (**61 %**).

La plupart des organisations qui n'utilisent pas encore l'IA pour les soins aux patients envisagent au moins de l'adopter (**16 %** à l'échelle mondiale), tandis que seulement **3 %** des décideurs IT indiquent que leur organisation n'a aucun projet en ce sens.

L'IA est la plus largement utilisée au Royaume-Uni, où **94 %** des décideurs IT déclarent que leur organisation l'emploie pour les soins aux patients, contre **47 %** en 2024. En Australie, **93 %** des décideurs IT déclarent utiliser l'IA, contre **70 %** auparavant.

Pourcentage d'organisations utilisant l'IA pour les soins aux patients en 2025 par rapport à 2024

	2025	2024		2025	2024
Global	**81 %**	**61 %**	France	81 %	45 %
États-Unis	80 %	72 %	Suède	71 %	53 %
Canada	87 %	72 %	Pays-Bas	70 %	43 %
Mexique	82 %	80 %	Italie	74 %	-
Royaume-Uni	94 %	47 %	Espagne	83 %	-
Allemagne	77 %	71 %	Australie	93 %	70 %

IA : ALLÉGER LA CHARGE ADMINISTRATIVE

Bien que le nombre d'organisations utilisant l'IA ait augmenté, son application reste largement inchangée par rapport à l'année dernière. En 2025, l'utilisation la plus courante de l'IA concerne le traitement et/ou l'analyse des données médicales (**60 %** des décideurs IT déclarent que leur organisation l'utilise à cette fin), suivie par la mise à jour des dossiers patients (**59 %**). Un peu moins de la moitié (**46 %**) des organisations utilisent l'IA pour planifier le meilleur parcours de traitement, tandis que **45 %** l'emploient pour personnaliser les soins, et **40 %** l'exploitent pour diagnostiquer des pathologies.

De quelle manière votre organisation utilise-t-elle actuellement l'IA dans les soins aux patients ? (Question posée à ceux qui utilisent l'IA dans les soins aux patients)

Résultats globaux	2025	2024
Pour traiter et/ou analyser les données médicales	60 %	60 %
Pour mettre à jour les dossiers des patients	59 %	56 %
Pour planifier le meilleur parcours de traitement	46 %	47 %
Pour personnaliser les traitements	45 %	44 %
À d'autres fins administratives	45 %	20 %
Pour diagnostiquer les pathologies	40 %	38 %
NET : Mettre à jour les dossiers/autres tâches administratives	79 %	63 %

Cette année, un changement notable est l'augmentation de l'utilisation de l'IA à des fins administratives. En 2024, **20 %** des décideurs IT ont indiqué que l'IA était utilisée à des fins administratives, et en 2025, ce chiffre a grimpé à **45 %**.

En déléguant les tâches fastidieuses à l'IA, le personnel de santé peut se concentrer sur les aspects essentiels des soins aux patients. Si l'on prend en compte les organisations utilisant l'IA pour la mise à jour des dossiers médicaux, on constate qu'au total **79 %** l'exploitent à des fins administratives sous une forme ou une autre.

Le Royaume-Uni et les États-Unis sont les principaux utilisateurs de l'IA pour la personnalisation des traitements (**57 %** et **55 %**, respectivement). Par ailleurs, le Royaume-Uni se démarque dans l'utilisation de l'IA pour le diagnostic des pathologies, avec **52 %** des organisations qui l'exploitent à cette fin. La Suède (**53 %**) et le Canada (**52 %**) sont les pays qui exploitent le plus l'IA à des fins administratives.

Lors de nos recherches l'année dernière, nous avons constaté que plus de la moitié (**57 %**) des professionnels de l'informatique exprimaient des réserves quant à l'utilisation de l'IA dans les soins aux patients, s'inquiétant de la menace qu'elle représentait pour la confidentialité des données des patients. Cette année, nous avons constaté que toutes les organisations ont mis en œuvre au moins quelques mesures de sécurité pour les appareils mobiles. Cependant, seulement **36 %** disposent de mesures de sécurité spécifiques à l'IA. Compte tenu de la forte augmentation de l'utilisation de l'IA au cours de l'année écoulée, il semblerait que ce soit un domaine que davantage d'organisations de santé devraient explorer.

Quelles mesures de sécurité privilégiez-vous pour les appareils mobiles ?

Mises à jour régulières	**51 %**
Former et sensibiliser les employés aux menaces spécifiques et aux meilleures pratiques en matière de sécurité	**45 %**
Garantir la conformité avec la réglementation et les lois sur la protection des données (ex. : RGPD, EHDS)	**45 %**
Limiter l'accès aux données sensibles à certains rôles et responsabilités	**45 %**
Authentification multifacteur	**44 %**
Chiffrement	**42 %**
Réaliser des audits de sécurité réguliers	**42 %**
Mettre en place des mesures de sécurité spécifiques à l'IA	**36 %**
Implémenter l'anonymisation des données	**34 %**
Avoir un plan de réponse aux incidents en place	**33 %**
Suppression à distance	**23 %**

L'année dernière, plus de huit professionnels de l'IT sur dix (**83 %**) ont affirmé que l'IA constitue une stratégie essentielle de réduction des coûts pour les organisations de santé. Cette année, l'utilisation de l'IA dans les soins aux patients a connu une forte hausse. Les systèmes hérités compliquent l'adoption des technologies émergentes, et les défis persistants en matière de sécurité des données affectent l'ensemble du secteur. Pour garantir que l'IA atteigne son plein potentiel en toute sécurité, une gestion rigoureuse des appareils qui l'intègrent est essentielle.

LA PROBLÉMATIQUE :

LES SYSTÈMES HÉRITÉS FREINENT LA VALEUR DES TECHNOLOGIES ÉMERGENTES

L'ADOPTION DE L'IOT ET DE LA TÉLÉSANTÉ EST UNIVERSELLE, MAIS DES PROBLÈMES PERSISTENT

L'intégration des technologies interconnectées transforme le secteur de la santé, notamment grâce à la télésanté, qui relie les appareils et systèmes aussi bien à l'intérieur des établissements de santé qu'à distance. Cette année, presque tous les décideurs informatiques (**99 %**) ont déclaré que leur organisation utilise une forme de dispositifs connectés ou de solutions de télésanté.

Malgré ce fort taux d'adoption, l'efficacité opérationnelle de ces systèmes ne répond pas aux attentes.

Un total significatif de

96 %

des leaders informatiques ont signalé des difficultés avec ces technologies.

L'un des principaux problèmes est le manque d'intégration entre les systèmes utilisés pour les appareils connectés et les applications de télésanté. Ce problème se reflète dans les statistiques suivantes à travers différentes régions.

Les systèmes utilisés pour les dispositifs médicaux IoT/télésanté ne sont pas intégrés :

- **MONDE ENTIER** : 65 %
- **FRANCE** : 60 %
- **ÉTATS-UNIS** : 69 %
- **SUÈDE** : 72 %
- **CANADA** : 71 %
- **PAYS-BAS** : 58 %
- **MEXIQUE** : 66 %
- **ESPAGNE** : 58 %
- **ROYAUME-UNI** : 73 %
- **ITALIE** : 58 %
- **ALLEMAGNE** : 60 %
- **AUSTRALIE** : 53 %

Le défi le plus important auquel **65 %** des organisations sont confrontées cette année est le manque d'intégration entre ces systèmes. Ce problème englobe des défis liés à l'interopérabilité, notamment l'impossibilité d'accéder à l'ensemble des informations de santé d'un patient en un seul endroit (rapporté par **43 %** des répondants) et l'absence de mises à jour automatiques sur tous les systèmes (**40 %**). De plus, **65 %** des décideurs informatiques ont exprimé leur frustration face aux difficultés de leur organisation à fournir des données pertinentes aux bonnes personnes au moment où elles sont le plus nécessaires.

Ces défis sont visibles à l'échelle mondiale, mais ils sont particulièrement marqués en Australie (**77 %**), au Royaume-Uni (**73 %**) et au Canada (**71 %**). Les problèmes d'intégration sont également fréquents parmi les organisations de santé qui exercent dans plusieurs spécialités. Parmi ceux qui rencontrent ces difficultés, **69 %** travaillent dans des cabinets ou cliniques de médecine générale, tandis que **67 %** travaillent dans des cliniques offrant un ou plusieurs services spécialisés. Comparativement, **62 %** des décideurs informatiques dans les hôpitaux offrant des soins de première ligne et les organisations axées sur les services de télésanté ou de soins à distance ont signalé rencontrer des défis similaires en matière d'intégration (**60 %**).

LES SYSTÈMES HÉRITÉS CRÉENT DES PROBLÈMES D'INTÉGRATION ET D'INTEROPÉRABILITÉ

Le pourcentage de décideurs informatiques dont les organisations utilisent une technologie obsolète est passé de **63 %** en 2024 à **55 %** cette année. Pourtant, **97 %** des décideurs informatiques déclarent que leur organisation utilise une technologie héritée. Environ la moitié des utilisateurs de technologies héritées ne les considèrent pas comme obsolètes, mais cela affecte la capacité des organisations à s'adapter facilement aux nouvelles méthodes de travail.

Quatre décideurs informatiques sur dix (**38 %**) affirment que les technologies héritées les empêchent de déployer et de gérer de nouveaux appareils et imprimantes. La même proportion indique qu'elles limitent leur capacité à assurer un support à distance ou à obtenir des informations détaillées sur les problèmes liés aux appareils.

Quel impact les technologies héritées ont-elles sur vos opérations quotidiennes ?

Impossible de déployer et de gérer de nouveaux appareils et imprimantes	**38 %**	39 %	46 %	37 %	47 %	37 %	37 %	31 %	33 %	29 %	36 %	43 %
Impossible de prendre en charge les appareils à distance ou d'obtenir des informations détaillées sur les problèmes rencontrés	**38 %**	38 %	43 %	37 %	53 %	35 %	35 %	38 %	29 %	29 %	33 %	43 %
Trop de temps passé à résoudre des problèmes	**39 %**	38 %	47 %	39 %	41 %	43 %	36 %	43 %	41 %	29 %	33 %	39 %

Avec l'essor des dossiers médicaux électroniques (DME) facilitant le partage fluide des données des patients au sein des organisations de santé, ainsi que l'utilisation croissante des dispositifs de télésanté, l'intégration et l'interopérabilité n'ont jamais été aussi cruciales. Cependant, les résultats de cette année révèlent que les problèmes d'intégration des systèmes causés par les technologies héritées restent un obstacle majeur.

Plus de trois quarts (**79 %**) des décideurs informatiques ont déclaré que l'adoption des DME représente un défi majeur pour leur organisation, et **36 %** attribuent directement ce défi aux systèmes informatiques hérités qu'ils utilisent. L'impact des technologies héritées sur l'adoption et l'intégration des DME est ressenti de manière particulièrement forte au Royaume-Uni (**44 %**), en Australie (**42 %**), ainsi qu'aux États-Unis et au Canada (**41 %** chacun).

L'adoption et l'intégration des DME ont été un défi et ont été affectées par les systèmes informatiques hérités

L'adoption et l'intégration des dossiers médicaux électroniques ont représenté un défi majeur pour notre organisation	**79 %**	74 %	78 %	71 %	92 %	73 %	87 %	66 %	77 %	82 %	84 %	80 %
Les technologies héritées ont freiné l'adoption et l'intégration des dossiers médicaux électroniques	**36 %**	41 %	41 %	35 %	44 %	33 %	31 %	33 %	27 %	27 %	37 %	42 %

Les données suggèrent que l'adaptation humaine est essentielle pour utiliser efficacement les nouvelles technologies. **30 %** des répondants ont indiqué que les systèmes sont modifiés trop fréquemment pour que leur organisation puisse suivre le rythme des changements. **33 %** des répondants ont également indiqué que la formation des utilisateurs aux nouveaux systèmes ralentit les processus et a un impact sur les soins aux patients. Cependant, le principal défi pour assurer le bon fonctionnement des dispositifs médicaux IoT et de télésanté provient des systèmes obsolètes au sein de l'industrie de la santé :

90 % **des organisations demandent davantage d'investissements dans des technologies nouvelles ou améliorées afin d'améliorer la qualité des soins aux patients, et**

89 % **demandent des dispositifs plus interconnectés.**

LES SYSTÈMES HÉRITÉS ENGENDRENT DES RISQUES DE SÉCURITÉ

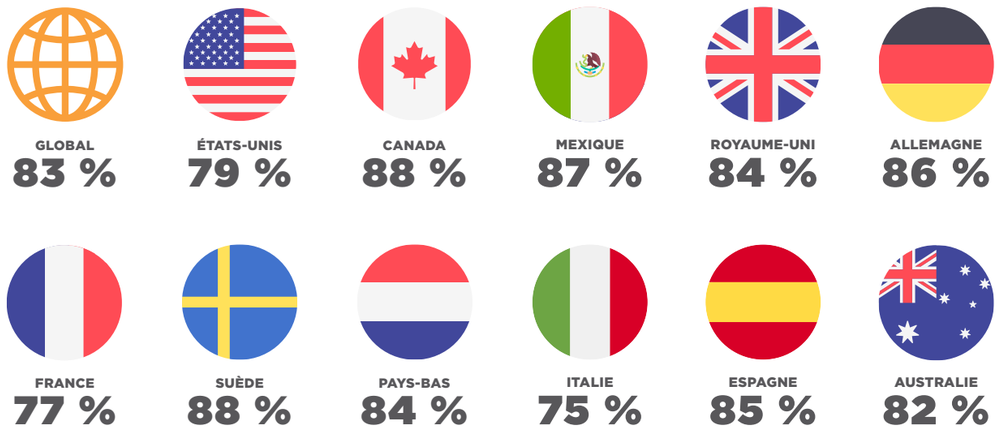
Plus de huit décideurs IT sur dix (83 %)
ont déclaré que leur organisation avait subi au moins une **violation ou fuite de données, ou une attaque par ransomware** depuis 2023.

Cela correspond aux chiffres de 2024 (**85 %**), ce qui montre que ces menaces restent tout aussi répandues et ne sont pas gérées efficacement.

Il peut y avoir peu de changement d'une année à l'autre dans le pourcentage global d'organisations touchées par des incidents, mais près de la moitié ont subi une fuite accidentelle de données (**48 %**, contre **33 %** en 2022). De plus, deux tiers ont été victimes d'une violation de données provenant d'une source externe ou d'une attaque par ransomware (**65 %**, en phase avec 2024, mais en hausse par rapport à **48 %** en 2022 et **52 %** en 2023).

Le seul type d'incident ayant connu un changement significatif cette année est le pourcentage de décideurs IT signalant une fuite de données planifiée par un employé, qui est passé de **34 %** en 2024 à **24 %** en 2025.

A connu un ou plusieurs incidents de sécurité au cours des 12 derniers mois :



Avec la baisse des violations de données impliquant des employés cette année, l'élément humain des préoccupations en matière de sécurité des données pourrait commencer à être maîtrisé. Cependant, les sources technologiques sont encore loin d'être éliminées.

Cette année, près de la moitié des décideurs informatiques (**45 %**) attribuent aux technologies héritées la vulnérabilité des réseaux face aux cyberattaques, en hausse par rapport à **36 %** en 2024.

Il s'agit d'un problème qui touche les organisations à travers le monde, mais dans certains pays, il suscite une inquiétude encore plus grande : plus de la moitié des décideurs informatiques en Suède (**55 %**), en France (**54 %**), en Australie (**53 %**) et au Canada (**51 %**) craignent désormais que leur réseau soit vulnérable aux cyberattaques en raison des technologies héritées qu'ils utilisent.

L'inquiétude liée aux technologies héritées ne cesse de croître d'année en année, avec une augmentation constatée dans chaque pays étudié. Sans une résolution des problèmes liés aux systèmes hérités, les organisations s'exposent de plus en plus aux menaces de sécurité, aux inefficacités opérationnelles et à une qualité des soins compromise.

« Les systèmes IT hérités rendent notre réseau vulnérable aux attaques de sécurité »

	2025	2024		2025	2024
Global	**45 %**	**36 %**	France	**54 %**	**27 %**
États-Unis	44 %	39 %	Suède	55 %	25 %
Canada	51 %	43 %	Pays-Bas	40 %	37 %
Mexique	39 %	35 %	Italie	37 %	-
Royaume-Uni	43 %	40 %	Espagne	41 %	-
Allemagne	45 %	33 %	Australie	53 %	39 %

Quatre professionnels de l'IT sur dix (**38 %**) ne peuvent pas gérer à distance les appareils ni obtenir des informations détaillées sur leurs problèmes, et un sur cinq (**20 %**) a indiqué qu'il ne pouvait pas détecter les nouveaux appareils se connectant au système. Les systèmes IT hérités sont utilisés dans **97 %** des organisations de santé. D'après les résultats de cette année, les problèmes d'intégration, de maintenance et de sécurité persistent.

LES SYSTÈMES HÉRITÉS ALOURDISSENT LA CHARGE DE TRAVAIL DES ÉQUIPES IT

Les pannes fréquentes et les problèmes techniques posent un défi supplémentaire dans l'utilisation des appareils interconnectés et des dispositifs médicaux de télésanté, affectant **59 %** des organisations cette année, contre **52 %** en 2022.

Votre organisation a-t-elle rencontré des problèmes techniques fréquents ou des interruptions de service en utilisant des dispositifs médicaux IoT/télésanté ?

GLOBAL
59 %

ÉTATS-UNIS
62 %

CANADA
73 %

MEXIQUE
52 %

ROYAUME-UNI
64 %

ALLEMAGNE
61 %

FRANCE
53 %

SUÈDE
58 %

PAYS-BAS
48 %

ITALIE
47 %

ESPAGNE
57 %

AUSTRALIE
66 %

Les interruptions techniques dans les environnements de santé peuvent entraîner des perturbations dans les soins aux patients, impactant l'efficacité globale des opérations. Les organisations rencontrent des difficultés liées aux mises à jour et à la maintenance des systèmes, ce qui entraîne des flux de travail inefficaces et une baisse de la qualité des soins de santé.

Ces difficultés sont rencontrées à l'échelle mondiale, mais les problèmes techniques et les interruptions sont nettement plus fréquents dans les pays suivants : Canada (**73 %**), Australie (**66 %**) et Royaume-Uni (**64 %**).

Alors qu'elles se concentrent sur des projets stratégiques, les équipes IT se retrouvent souvent accaparées par des tâches chronophages liées au dépannage de problèmes techniques mineurs, comme la réparation d'imprimantes, les problèmes de connectivité et d'autres demandes de support répétitives. Une grande partie de ce problème est causée par les systèmes IT hérités, et **39 %** des décideurs IT ont indiqué que cela les oblige à passer trop de temps à résoudre des problèmes. Cette inefficacité réduit la capacité à se concentrer sur des initiatives plus stratégiques, qui favorisent le progrès des organisations. Les organisations de santé doivent envisager de mettre en place des solutions permettant d'intégrer les technologies existantes et nouvelles.

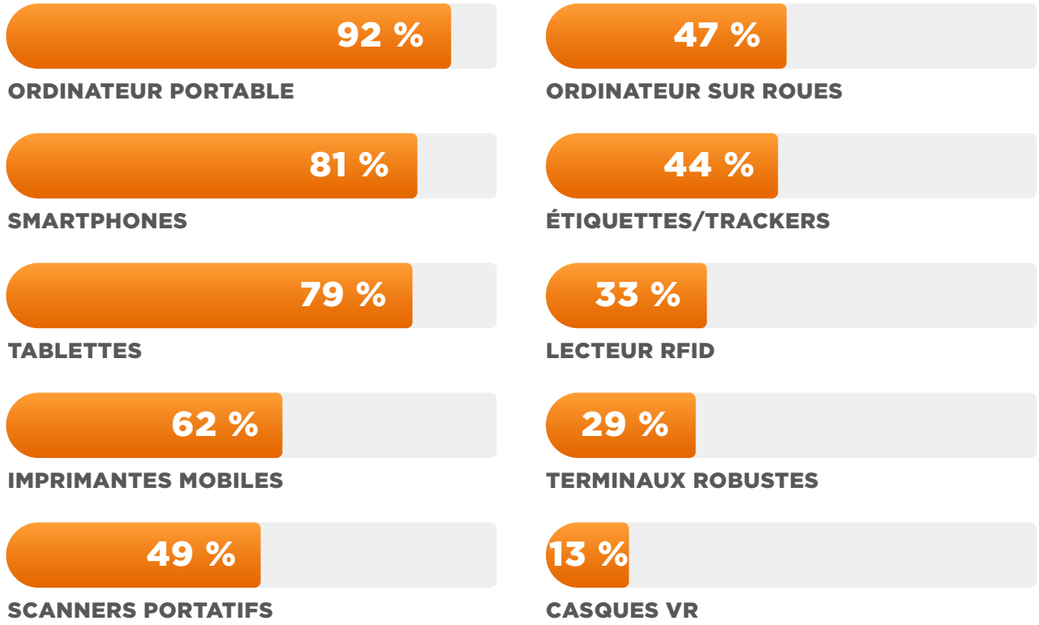
LA VOIE À SUIVRE :

LA GESTION DE LA MOBILITÉ EN ENTREPRISE A REMPLACÉ LA GESTION DES APPAREILS MOBILES

L'intégration croissante de divers appareils mobiles, l'utilisation accrue des imprimantes et la multiplication des applications dans les opérations de santé quotidiennes nécessitent une solution de gestion des appareils robuste.

Quels types d'appareils mobiles sont utilisés dans votre organisation ?

Résultats globaux



Avec une flotte d'appareils aussi diversifiée, les organisations de santé sont confrontées à plusieurs défis, notamment le maintien de la sécurité, le dépannage à distance et la garantie d'un fonctionnement optimal de tous les appareils. Pour les décideurs IT, il est essentiel de garantir une connectivité fluide avec ces appareils. Pour répondre à ces exigences, les organisations de santé doivent aller au-delà de la gestion traditionnelle des appareils mobiles (MDM) et adopter une approche plus globale et intégrée.

LE BESOIN CROISSANT DE SOLUTIONS EMM

Il ne fait aucun doute que la technologie mobile a sa place, puisque **86 %** des décideurs informatiques déclarent qu'elle accélère leur travail. Cependant, le nombre d'appareils en circulation indique qu'il y a beaucoup de dispositifs mobiles à suivre, à entretenir et à gérer, la majorité utilisant un MDM à des fins de sécurité (**90 %**). Cela inclut la gestion des politiques de sécurité, la protection contre les cybermenaces et l'identification des dispositifs non autorisés accédant au réseau, des éléments essentiels pour réduire les vulnérabilités et minimizing le risque de violations.

Quelles fonctionnalités d'une solution MDM sont essentielles pour vos opérations ?

Gestion de la sécurité	63 %
Protection contre les cybermenaces et identification des dispositifs externes accédant au réseau	56 %
Moyens de réduire les vulnérabilités face aux menaces externes et de limiter les opportunités pour les hackers	48 %
Dépannage à distance	47 %
Gestion des applications	47 %
Suivi de terminal	45 %
Conformité et application des stratégies	44 %
Restriction de l'accès aux fonctionnalités des appareils dans certains environnements	38 %
NET : sécurité (gestion de la sécurité ou protection contre les cybermenaces, identification des dispositifs externes accédant au réseau, ou moyens de réduire les vulnérabilités aux menaces externes et limiter les opportunités pour les hackers)	90 %

De nombreuses organisations de santé s'appuient sur des solutions MDM pour la sécurité de base et la gestion des dispositifs, mais cela ne constitue qu'un point de départ. Dans l'environnement de santé actuel, où les enjeux sont élevés et le rythme effréné, un MDM basique ne suffit plus.

Avec la complexité croissante des soins aux patients et le nombre grandissant de dispositifs connectés, les organisations doivent passer de stratégies réactives à des approches proactives qui détectent et préviennent les problèmes avant qu'ils n'affectent la qualité des soins. Cela signifie aller au-delà des bases pour mettre en place une surveillance en temps réel et anticiper les violations de sécurité ainsi que les perturbations opérationnelles.

Les deux tiers (**65 %**) des décideurs informatiques déclarent que leur organisation a subi une violation de données provenant d'une source externe ou une attaque par rançongiciel DDoS au cours des 12 derniers mois. Cela souligne la nécessité de dépasser les fondamentaux et de mettre en place des mesures de sécurité plus avancées et globales.

La sécurité des données reste en tête de la liste des préoccupations informatiques, **30 %** des décideurs informatiques la citant comme une priorité. Le pourcentage de décideurs informatiques la considérant comme leur principale préoccupation continue d'augmenter considérablement, passant de **16 %** en 2023 et **23 %** en 2024. Ajoutons à cela les **13 %** qui ont indiqué que la gestion de la sécurité des appareils partagés était leur principale préoccupation cette année, et nous constatons que près de la moitié (**43** %) mentionnent un problème lié à la sécurité comme la principale inquiétude des équipes informatiques au sein de leur organisation.

Quelle est actuellement la principale préoccupation de votre service informatique ?

Préoccupation liée à la sécurité des données ou gestion de la sécurité des appareils partagés.

	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 %

La sécurité des données est la principale préoccupation de tous les pays cette année, certains enregistrant une hausse particulièrement marquée :

En **France**, un problème lié à la sécurité a été classé comme la principale préoccupation par **25 %** des répondants en 2024 et **51 %** en 2025.

Au **Canada**, ce chiffre est passé de **39 %** l'an dernier à **53 %** cette année.

En **Australie**, ce chiffre a bondi de **39 %** à **53 %**.

En **Allemagn**e, ce chiffre est passé de **24 %** à **41 %**.

La nature des appareils mobiles impose qu'ils soient manipulés par plusieurs utilisateurs. Il n'est donc pas surprenant que la gestion de la sécurité des appareils partagés demeure une préoccupation majeure pour les équipes informatiques. Ajoutez à cela le défi posé par les technologies héritées, qui rendent presque impossible la gestion à distance de ces appareils, et les dispositifs mobiles deviennent alors une arme à double tranchant.

Les fonctionnalités MDM « basiques » ne suffisent plus dans le monde technologique moderne, où des dispositifs et systèmes complexes sont en place. Les capacités historiques du MDM ont atteint leurs limites. Aujourd'hui, le besoin de solutions technologiques avancées est plus crucial que jamais. Les outils EMM modernes offrent aux organisations de santé une visibilité accrue sur l'ensemble de leur écosystème de dispositifs, leur permettant de mieux surveiller les opérations, de renforcer la sécurité des données et de réagir plus rapidement aux menaces émergentes.

PRIORISER LA SÉCURITÉ DES APPAREILS MOBILES : UNE APPROCHE COMPLÈTE

Les organisations donnent la priorité aux mesures visant à garantir la sécurité des appareils mobiles. Certaines organisations adoptent une approche axée sur l'humain, **45 %** d'entre elles formant leurs employés aux menaces de sécurité, aux bonnes pratiques et aux lois sur la protection des données, tandis qu'un nombre similaire restreint l'accès aux données sensibles en fonction des rôles et des responsabilités. Pourtant, seule une organisation sur trois (**33 %**) dispose d'un plan de réponse aux incidents en cas de problème.

La mise en œuvre de mises à jour régulières est la mesure de sécurité la plus adoptée, **51 %** des organisations l'appliquant. Un nombre nettement plus élevé de ceux qui n'ont subi aucun incident de sécurité des données au cours des 12 derniers mois (**60 %**) adoptent cette approche, contre seulement **49 %** parmi ceux qui ont vécu un incident. L'authentification multifacteur est privilégiée par **44 %** des organisations, tandis que le chiffrement est adopté par **42 %**.

Il est évident que toutes les organisations prennent des mesures pour protéger les appareils mobiles, mais peu d'entre elles exploitent pleinement toutes les possibilités à leur disposition.

LE BESOIN DE MEILLEURES STRATÉGIES DE GESTION DES APPAREILS MOBILES

Les solutions MDM obsolètes ne sont pas seulement insuffisantes en matière de sécurité. De nombreuses organisations de santé rencontrent des incohérences dans l'application de ces solutions sur différents appareils, ce qui complique le suivi et le support des dispositifs. Cette incohérence entraîne souvent des remplacements d'appareils inutiles et des inefficacités dans l'ensemble des opérations.

Près de la moitié (**47 %**) des décideurs informatiques considèrent qu'une solution MDM est essentielle pour le dépannage à distance de leur organisation, et **45 %** estiment qu'elle est cruciale pour le suivi des appareils. Toutefois, **38 %** des organisations ne parviennent pas à déployer et gérer facilement de nouveaux dispositifs et imprimantes en raison de systèmes hérités, et **38 %** rencontrent des difficultés pour assurer un support à distance ou obtenir des informations détaillées sur les problèmes des appareils pour la même raison.

La recherche met en évidence la nécessité pour les organisations de santé d'adopter des solutions EMM robustes et centralisées, garantissant la sécurité des appareils et la conformité. Ces solutions devraient également faciliter le dépannage à distance, simplifier la configuration et fournir des informations exploitables.

Les outils avancés qui offrent des analyses et une intelligence opérationnelle sur l'ensemble des appareils permettent aux équipes informatiques d'identifier de manière proactive les problèmes de performance des dispositifs. Ils peuvent également suivre les tendances d'utilisation, offrant aux organisations des informations précieuses pour prendre des décisions éclairées. Cette approche réduit les temps d'arrêt, réduit les inefficacités et améliore la qualité globale des soins.

TECHNOLOGIE MÉDICALE À USAGE UNIQUE

Les préoccupations ne disparaissent pas lorsqu'un appareil mobile n'est plus utilisé, elles ont souvent tendance à s'intensifier. En effet, **81 %** des décideurs informatiques s'inquiètent de la sécurité des données des patients lors de la mise au rebut des appareils.

Les organisations de santé gèrent d'énormes volumes de données sensibles et, sans processus de mise au rebut standardisés, les appareils retirés présentent de sérieux risques de violations de données et de non-conformité réglementaire. Bien que la plupart des organisations prennent des mesures pour protéger les données lors de la mise au rebut des appareils, les incohérences restent élevées, et cette année, huit décideurs informatiques sur dix expriment toujours des préoccupations à ce sujet.

Les mises à niveau fréquentes accentuent le problème. **31** % des organisations remplacent les appareils à la demande des utilisateurs, **40 %** le font lorsque de nouveaux modèles sont disponibles, **41 %** les remplacent en fonction des termes du contrat, et **31 %** lorsque les garanties expirent. Cela soulève d'importantes préoccupations en matière de sécurité et de durabilité.

Pour réduire les risques, les organisations doivent mettre en place des protocoles standardisés, notamment l'effacement des données à distance et une gestion rigoureuse du cycle de vie des appareils, afin d'assurer un suivi et une élimination appropriés. Le personnel devrait également recevoir une formation régulière sur les pratiques de mise au rebut sécurisées. En donnant la priorité à des processus sécurisés et durables, les organisations de santé peuvent mieux protéger les données des patients et respecter les normes de conformité.

Quelle est la stratégie de votre organisation en matière de mise à niveau, de renouvellement et de remplacement des appareils, tels que les smartphones, tablettes, etc. ?

	Nous le faisons à un moment donné en raison de la durée de leur contrat, qu'ils fonctionnent encore ou non	Nous le faisons lorsqu'un modèle plus récent ou plus avancé devient disponible	Nous le faisons lorsque les utilisateurs en font la demande	Nous le faisons lorsque leur garantie expire	Nous le faisons uniquement pour les appareils qui ont cessé de fonctionner
	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 %

Les États-Unis, le Canada et l'Australie ont le pourcentage le plus élevé de remplacement des appareils lorsqu'une nouvelle version est disponible. Il est toutefois important de noter que cette tendance est courante à l'échelle mondiale. Il est essentiel de trouver un équilibre entre la durabilité des appareils et leur performance. Si les appareils ne sont mis au rebut que lorsqu'ils cessent de fonctionner, les équipes IT passeront encore plus de temps à résoudre les petits problèmes.

GESTION DE LA SANTÉ DES BATTERIES : PRÉVENIR PLUTÔT QUE GUÉRIR

Une surveillance inefficace de l'état des batteries peut également être une cause de pannes inattendues des appareils dans le secteur de la santé. Les coûts élevés dus au remplacement prématuré des appareils entraînent souvent des contraintes financières et des préoccupations environnementales liées à la gestion des déchets électroniques. **97 %** des organisations surveillent activement l'état des batteries de leurs appareils, mais seulement **31 %** déclarent ne les contrôler qu'en cas de problème.

Pour **41 %** des organisations, leur stratégie consiste à remplacer les batteries selon un calendrier fixe, indépendamment de leur état de santé. Plus rassurant, la moitié des organisations effectuent des vérifications manuelles régulières, **44 %** utilisent une surveillance automatique de l'état des batteries, et **41 %** disposent d'un système de maintenance prédictive.

En fin de compte, les conclusions suggèrent que, bien que les appareils mobiles offrent des avantages indéniables, leur gestion doit être optimisée : la mise en œuvre de solutions EMM permet d'établir les meilleures pratiques en matière de suivi des appareils, de surveillance de l'état des batteries et de stratégies de remplacement durables. De telles mesures ne permettraient pas seulement de rationaliser les opérations quotidiennes, mais ouvriraient également la voie à des initiatives IT plus stratégiques dans l'ensemble du secteur de la santé.

CONCLUSION

Le secteur de la santé progresse rapidement dans son processus de transformation numérique, mais le chemin reste complexe. Bien que l'utilisation des dispositifs IoT et de télésanté soit répandue, les systèmes hérités obsolètes posent des problèmes tels que la consolidation incomplète des données et des perturbations techniques fréquentes, empêchant ainsi les équipes IT de tirer pleinement parti de leur transformation numérique.

Dans le même temps, les problèmes de sécurité sont devenus la principale préoccupation de **43 %** des décideurs IT, en raison de menaces allant de la gestion des appareils partagés à l'augmentation des violations de données. Bien que les fuites de données intentionnelles des employés aient légèrement diminué, les fuites accidentelles et les attaques externes sophistiquées continuent d'exposer des vulnérabilités. Près de la moitié des responsables IT considèrent que les systèmes hérités sont l'une des principales causes de vulnérabilité des réseaux face aux attaques, ce qui souligne l'urgence de moderniser les technologies fondamentales. Il semble que le problème concerne moins les technologies émergentes elles-mêmes que les systèmes qui les soutiennent.

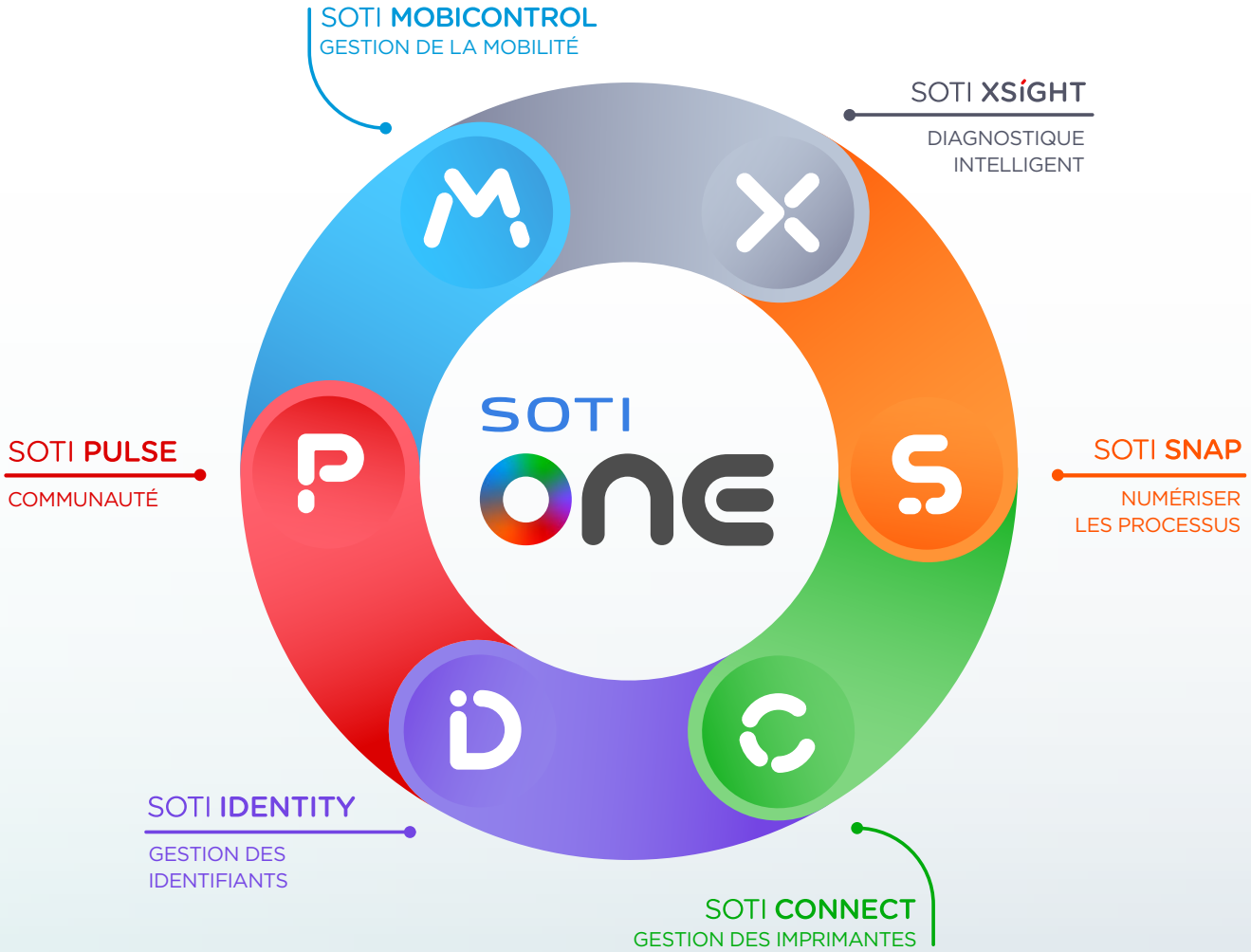
L'adoption de l'IA a fortement progressé à l'échelle mondiale et est utilisée par un tiers d'organisations supplémentaires cette année, avec des régions comme le Royaume-Uni et l'Australie en tête. L'intelligence artificielle est en train de transformer le secteur médical, en étant intégrée à l'analyse des données médicales, la planification des traitements, les soins personnalisés aux patients, et bien plus encore. Une bouée de sauvetage pour un secteur de la santé surchargé, mais la nécessité de surveiller et sécuriser son utilisation ne peut être négligée.

De plus, la gestion des appareils mobiles représente une charge importante pour les ressources IT, et la multiplicité des appareils utilisés complique le suivi efficace ainsi que la gestion à distance. L'insuffisance des solutions MDM existantes et les politiques de remplacement incohérentes accentuent encore la pression, aggravant les préoccupations en matière de sécurité et de durabilité.

En fin de compte, parvenir à une véritable transformation numérique dans le secteur de la santé exige que les organisations prennent du recul et envisagent une vision globale. Ce qu'il faut, c'est une stratégie globale qui associe l'adoption massive des technologies innovantes à des investissements ciblés pour la modernisation et l'intégration des infrastructures IT, ainsi qu'une solution EMM adaptée aux besoins. Cette approche équilibrée permettra aux organisations de sécuriser les données, d'optimiser l'utilisation des appareils mobiles et, en fin de compte, d'améliorer la qualité des soins aux patients.

À PROPOS DE SOTI

SOTI est un innovateur reconnu et un leader du secteur qui simplifie les solutions de mobilité des entreprises en les rendant plus intelligentes, plus rapides et plus fiables. Grâce au portefeuille innovant de solutions de SOTI, les entreprises peuvent faire confiance à SOTI pour améliorer et rationaliser leurs opérations mobiles, maximiser leur retour sur investissement et réduire les temps d'arrêt des appareils. Avec plus de 17 000 clients dans le monde, SOTI a prouvé qu'il était le premier fournisseur de plateforme mobile pour gérer, sécuriser et prendre en charge les appareils critiques de l'entreprise. Grâce au support de classe mondiale de SOTI, les entreprises peuvent donner à la mobilité des possibilités infinies.



POUR EN SAVOIR PLUS :

Pour en savoir plus sur la manière dont SOTI peut aider votre entreprise à réussir, **cliquez ici**.
Pour en savoir plus sur la plateforme SOTI ONE, **cliquez ici**.
Pour savoir comment SOTI peut vous aider dans vos investissements mobiles, contactez-nous dès aujourd'hui à **sales@soti.net**.

SOTI est un innovateur reconnu et un leader de l'industrie pour la simplification de la mobilité d'entreprise des entreprises en les rendant plus intelligentes, plus rapides et plus fiables. SOTI aide les entreprises du monde entier à porter la mobilité vers des possibilités infinies.

soti.fr

© 2025, SOTI Inc. Tous droits réservés. Tous les noms de produits et de sociétés sont des marques™ ou des marques déposées® de leurs propriétaires respectifs. L'utilisation de ces marques ne sous-entend aucune affiliation avec SOTI ou approbation par le titulaire de la marque. Les offres sont susceptibles d'être modifiées ou annulées sans préavis. SOTI se réserve le droit de modifier les produits, services ou prix à tout moment. L'information est fournie « EN L'ÉTAT » sans aucune garantie. Les produits et services sont régis par les conditions générales applicables.

060525