

HEALTHCARE'S DIGITAL DILEMMA:

CALCULATED RISKS AND HIDDEN CHALLENGES EXPOSED



WELCOME NOTE

Healthcare is on the cusp of a digital breakthrough. Innovations in AI, telehealth, mobile technology and automation are opening new possibilities for smarter, more connected care. Despite these advancements, many healthcare organizations remain held back by legacy systems and operational inefficiencies.

For IT leaders, the challenge is clear. Organizations need to accelerate the adoption of modern technologies to improve outcomes, empower staff and deliver seamless care experiences that patients expect.

Legacy systems cause delays in accessing critical information, which ultimately reduces the quality of care. Meanwhile, AI can enhance diagnostics, streamline workflows, and predict patient needs, but only when supported by modern infrastructure.

The extent to which new technology is integrated and the ability to maximize the



Stephanie Lopinski, VP, Global Marketing

benefits of all devices and applications play a key role in influencing patient outcomes and the quality of healthcare delivery. Organizations must prioritize system integration, real-time data access and moving away from outdated technology to unlock the benefits of digital transformation.

Our latest research examines the current state of healthcare organizations, the challenges they face, and strategies for advancement.

SOTI's 2025 report highlights three key themes:

Artificial Intelligence

AI adoption in healthcare is growing rapidly, with **81%** of global organizations using it for patient care, up from **61%** in 2024. Its applications include processing medical data, updating records, personalizing treatments, and diagnosing conditions.

Despite increased usage, only **36%** of organizations have AI-specific security measures, raising concerns about patient privacy. Thus, modernizing systems is fundamental to ensuring patient privacy.

The 2025 report paints a clear picture — healthcare's technological journey is progressing, but unevenly. Until legacy systems are addressed, data security is strengthened, and IT resources are freed from constant troubleshooting, the industry will struggle to turn adoption into true integration.

Legacy Systems

Healthcare organizations struggle to integrate interconnected systems and telehealth solutions, primarily due to outdated legacy systems that are challenging to manage remotely.

These systems present significant security risks, with **83%** of organizations reporting data breaches, leaks, or ransomware attacks since 2023. Additionally, they complicate the integration of Electronic Medical Records (EMRs), impacting **79%** of organizations.

As a result, when organizations attempt to adopt new technologies, setbacks often persist, hindering innovation and negatively affecting the patient experience.

Ultimately, the limitations imposed by these outdated systems directly influence patient care outcomes, making it crucial for organizations to invest in modern technology and interconnected systems to enhance efficiency, security, and overall quality of care.

Mobile Device Management + Enterprise Mobility Management

Healthcare organizations are increasingly relying on a range of mobile devices, including laptops, smartphones, tablets, and specialized equipment such as RFID readers. Managing these devices presents significant challenges in security and remote troubleshooting when relying on outdated Mobile Device Management (MDM) solutions.

However, the current landscape necessitates an evolution beyond traditional MDM to encompass a comprehensive Enterprise Mobility Management (EMM) approach.

As healthcare technology evolves, the focus must shift toward an integrated platform that includes advanced diagnostics, data analytics, and operational intelligence. This approach enables organizations to proactively address issues, leveraging insights to inform decision-making and optimize workflows. By digitizing processes and automating administrative tasks, healthcare providers can enhance operational efficiency and support better patient care.

Effective mobile management solutions also require full lifecycle management to promote sustainability. Organizations should aim to maximize the lifespan of their devices, utilizing insights into battery health and usage patterns to develop sustainable replacement strategies. This proactive management not only helps maintain device health but also reduces vulnerabilities and safeguards patient data.

HEALTHCARE'S CHANGING LANDSCAPE:

PROGRESS AND BREAKTHROUGHS SINCE 2020

SOTI has been conducting healthcare research since 2020. As the survey has evolved, so has the number of countries and respondents. Trends over the past five years include notable insights below:

2020/2021

- Security: **81%** have concerns about the security of patient records
- Tech Issues: **63%** experience device or system failure on a weekly basis
- Tech impacts on patient care: **81%** have issues with systems and tech while out caring for patients

475 homecare workers, nurses and other healthcare professionals across seven countries worldwide

2022

- Security: **73%** of organizations have experienced a data breach or leak since 2020
- IoT/Telehealth: **98%** have implemented IoT/telehealth medical device capabilities
- Device Downtime Impacts: **53%** say they experience regular downtime that results in delays to patient care and 3.4 hours per week per employee lost to downtime

1,300 IT professionals working in healthcare organizations in eight countries worldwide

2023

- Patient Data Security: **97%** have a concern relating to the security of patient data records
- Network Security: **55%** experienced either an accidental or planned data leak from internal sources, **53%** are unable to detect new devices connecting to the system due to outdated systems, leading to vulnerabilities
- Legacy Systems: **52%** say legacy systems result in them being unable to resolve issues in a timely way **37%** believe legacy systems are leaving them more vulnerable to security breaches
- Downtime: 3.4 hours lost is in a normal week due to technical or system difficulties

1,450 IT professionals working in healthcare organizations in nine countries worldwide

2024

- AI: **85%** believe AI could help simplify tasks, but only 23% are currently using AI widely at present
- Security: **71%** are transferring data to external hard drives/backup when disposing of old devices. **23%** list data security as their top IT concern
- IoT/Telehealth: **67%** experience regular problems with IoT/telehealth devices leading to patient care delays.
- Legacy Systems: **63%** confirm they are using outdated technologies, and **45%** have experienced a data breach or accidental data leak in the past year
- Downtime: 3.9 hours per week per employee lost to downtime

1,450 IT professionals/decision makers working in healthcare organizations in nine countries worldwide

2025

- AI: **81%** now use AI for patient care up from 61% in 2024
- Security: **83%** have experienced an accidental data leak, external data breach or DDoS ransomware attack in the past 12 months. **30%** list data security as their top IT concern
- IoT/Telehealth: **96%** experience challenges implementing IoT/telehealth medical devices
- Legacy Systems: **45%** blame legacy IT for making networks vulnerable to attack
- Mobile Device Management: **47%** say mobile device management solutions are critical for remote troubleshooting

1,750 IT professionals/decision makers working in healthcare organizations in nine countries worldwide

CONTENTS

Methodology

Global Breakdown

Key Findings

The Breakthrough: Artificial Intelligence in Patient Care Surges

The Challenge: Legacy Systems Limit the Value of Emerging Technology

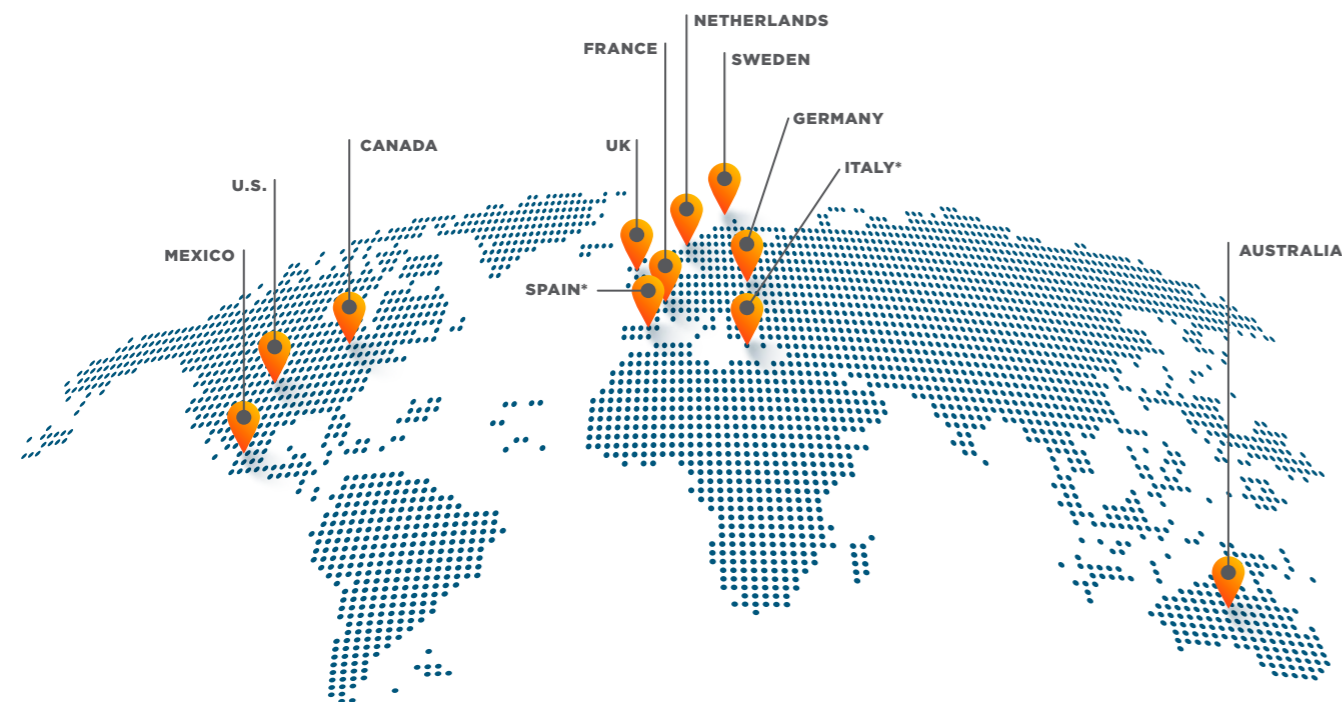
The Way Forward: Enterprise Mobility Management Has Replaced Mobile Device Management

Conclusion

METHODOLOGY

This year, SOTI's research extended its scope to cover **1,750 respondents across 11 countries**: U.S. (200), Canada (150), Mexico (150), UK (200), Germany (150), France (150), Sweden (150), Netherlands (150), Italy* (150), Spain* (150) and Australia (150). The survey was completed between January and March 2025 by IT decision makers for healthcare organizations.

*New regions included in the 2025 healthcare report.



GLOBAL BREAKDOWN

For this report, healthcare organizations refer to:



A hospital providing frontline patient services.



A general medical practice/clinic across many specialists, e.g., doctors' surgery, family doctor, medical practice.



A clinic providing frontline patient services across one or more specialties, e.g., mental health, neurology, physiotherapy, etc.



A healthcare provider providing direct-to-patient remote or telehealth patient services.

The healthcare organizations ranged in size from 50 to over 5,000 employees. Although all respondents were involved in IT decision making for a healthcare organization, their roles ranged from IT professionals to senior management and C-suite levels.



GLOBAL FINDINGS

96%

of organizations experience challenges implementing IoT/telehealth medical devices with systems integration being the greatest.

83%

of security incidents remain high with accidental data leaks, external data breaches and DDoS ransomware attacks showing no signs of abating.

47%

of IT decision makers say Mobile Device Management solutions are critical for remote troubleshooting.

45%

blame legacy IT for making networks vulnerable to attack.

81%

have concerns about the security of patient data when disposing of mobile devices.

81%

now use AI in some way to improve the efficiency and effectiveness of patient care, a jump from 61% in 2024.

40%

of organizations replace old devices when new versions become available.

30%

list data security as their top IT concern, up from 23% in 2024.



THE BREAKTHROUGH: ARTIFICIAL INTELLIGENCE IN PATIENT CARE SURGES













In recent years, the healthcare industry has witnessed transformative advancements, particularly with the integration of technology into patient care. The rise of AI is reshaping how healthcare providers deliver services and interact with patients.

Leveraging AI to enhance diagnostics, personalize treatment plans, and streamline operations has captured the attention of healthcare organizations worldwide. This year, our survey found that AI is being used in patient care in **81%** of healthcare organizations, a third more organizations than in 2024 (**61%**).

Most organizations that are not currently using AI for patient care are at least considering it (**16%** globally), with only **3%** of IT decision makers saying their organization has no plans to use it.

AI is most widely used in the UK, where **94%** of IT decision makers said their organization used it for patient care, up from **47%** in 2024. In Australia, **93%** said using AI, up from **70%**.

Percentage of organizations using AI for patient care 2025 versus 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%

AI: EASING THE ADMINISTRATIVE BURDEN

Although the number of organizations using AI has increased, how they are applying the technology remains largely unchanged since last year. In 2025, the most common use of AI is for processing and/or analyzing medical data (60% of IT decision makers said their organization uses it for this purpose), followed by updating patient records (59%). Just under half (46%) use AI to plan the best course of treatment, while 45% use it to personalize treatments, and 40% use it to diagnose conditions.

In which of the following ways does your organization currently use AI in patient care? (Asked to those using AI in patient care)

Global Findings	2025	2024
To process and/or analyze medical data	60%	60%
To update patient records	59%	56%
To plan the best course of treatment	46%	47%
To personalize treatments	45%	44%
To fulfill other administrative purposes	45%	20%
To diagnose conditions	40%	38%
NET: To update records/other admin	79%	63%

A significant change this year is the increase in AI being used for other administrative purposes. In 2024, 20% of IT decision makers reported AI being used in this way, and in 2025, this increased to 45%.

By delegating tedious tasks to AI, healthcare staff can focus on important patient care aspects at hand. If we consider this alongside organizations using AI for updating medical records, we see that a net of 79% use AI for some form of administrative purpose.





The UK and the U.S. are the top users of AI for the personalization of treatments (57% and 55%, respectively), whereas the UK leads the way when it comes to diagnosing conditions with AI (52%). Sweden (53%) and Canada (52%) reported the greatest use of AI for other administrative purposes.

In last year's research, we found that over half (57%) of IT professionals had some reservations about the use of AI in patient care, worrying about the threat it posed to patient privacy. This year we found that all organizations have implemented at least some security measures for mobile devices, yet only 36% have AI-specific security measures in place. Given the steep rise in AI usage over the past year, this would seem to be an area more healthcare organizations should investigate.

What security measures do you prioritize for mobile devices?



Last year, over eight in ten (83%) IT professionals said AI is an essential cost-saving strategy for healthcare organizations. This year, the use in patient care has surged. With the issues that legacy systems present to the take-up of emerging technology and the data security challenges that persist across the industry, the management of devices using it needs careful monitoring to ensure it can reach its full potential safely.

IOT AND TELEHEALTH ADOPTION IS UNIVERSAL, BUT ISSUES PERSIST

The integration of interconnected technologies is reshaping the healthcare landscape, particularly through telehealth, which connects devices and systems both within healthcare facilities and remotely. This year, nearly all IT decision makers (**99%**) indicated that their organizations utilize some form of connected devices or telehealth solutions.

Despite this high level of adoption, the operational efficiency of these systems falls short of expectations.

THE CHALLENGE:
**LEGACY SYSTEMS
LIMIT THE VALUE OF
EMERGING
TECHNOLOGY**

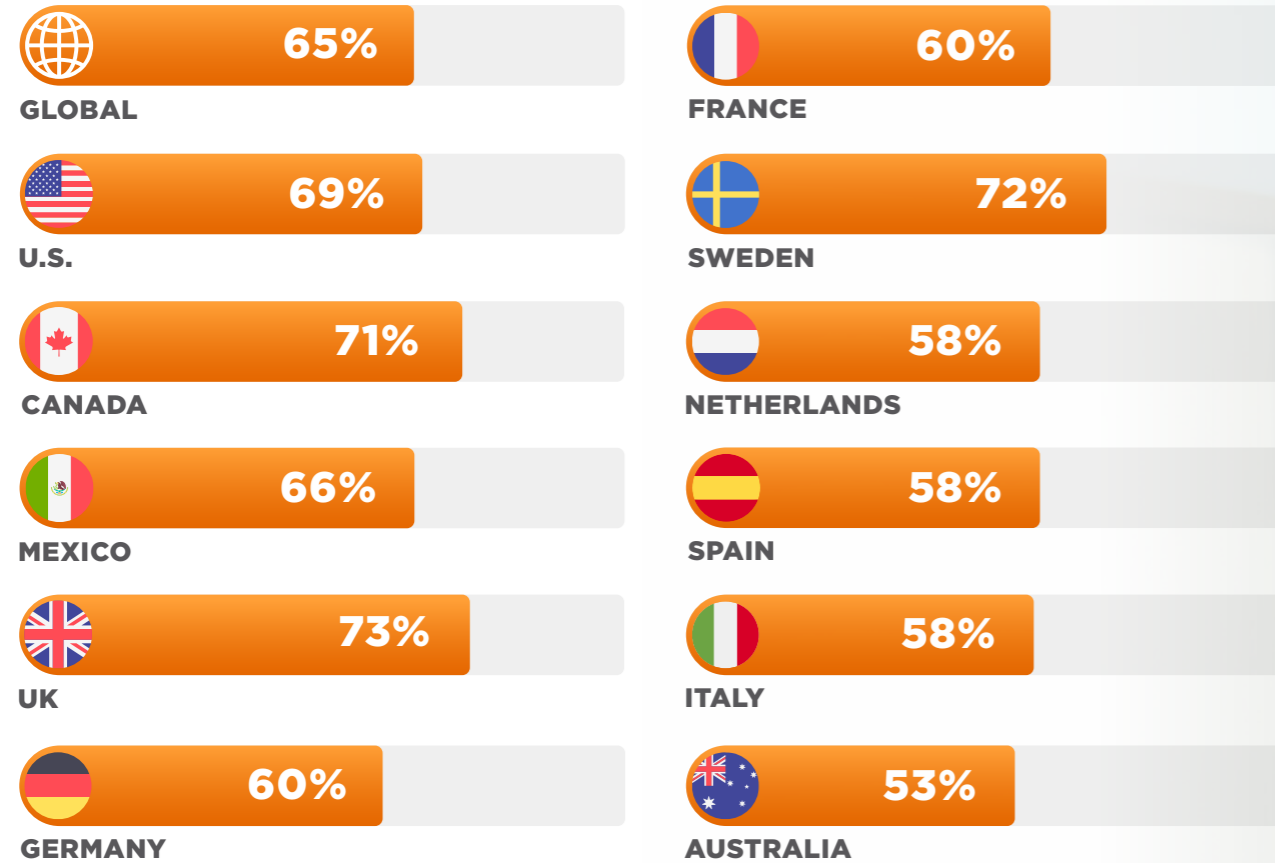
A significant

96%

of IT leaders reported facing challenges with these technologies.

One of the primary issues is the lack of integration among systems used for connected devices and telehealth applications. This problem is reflected in the following statistics across various regions.

Systems used for IoT/Telehealth medical devices are not integrated:



The most significant challenge faced by **65%** of organizations this year is the lack of integration between these systems. This issue encompasses interoperability challenges, such as the inability to access a patient's complete health information in a single location (reported by **43%** of respondents) and the lack of automatic updates across all systems (**40%**). Additionally, **65%** of IT decision makers expressed frustration that their organizations struggle to provide relevant data to the right individuals when it is needed most.

These challenges are evident on a global scale, but they are particularly pronounced in Australia (**77%**), the UK (**73%**), and Canada (**71%**). Integration issues are also common among healthcare organizations that operate across multiple specialties. Among those experiencing these difficulties, **69%** are from general medical practices or clinics, while **67%** are from clinics offering one or more specialty services. Comparatively, **62%** of IT decision makers in hospitals providing frontline care and organizations focused on remote or telehealth services reported encountering similar integration challenges (**60%**).



LEGACY SYSTEMS CREATING INTEGRATION AND INTEROPERABILITY ISSUES

The percentage of IT decision makers whose organizations use outdated technology dropped from **63%** in 2024 to **55%** this year. Yet, **97%** of IT decision makers report that their organization has legacy technology. Around half of those using legacy technology don't consider it obsolete, but it is impacting how easily organizations can adapt to new ways of working.

Four in ten (**38%**) IT decision makers said that legacy IT prevents them from deploying and managing new devices/printers and the same proportion said it means they cannot support devices remotely or get detailed information on device issues.

What impact does legacy technology have on your day-to-day operations?



Cannot deploy & manage new devices/printers 38% 39% 46% 37% 47% 37% 37% 31% 33% 29% 36% 43%

Cannot support devices remotely/get detailed info on device issues 38% 38% 43% 37% 53% 35% 35% 38% 29% 29% 33% 43%

Too much time fixing issues 39% 38% 47% 39% 41% 43% 36% 43% 41% 29% 33% 39%

With the rise of Electronic Medical Records (EMRs) to enable the seamless sharing of patient data within healthcare organizations and the growing use of telehealth devices, integration and interoperability have never been more critical. However, this year's findings reveal that system integration issues caused by legacy systems remain a roadblock.

Over three-quarters (**79%**) of IT decision makers said that the adoption of EMRs has been a significant challenge for their organization, and **36%** attribute this challenge directly to the legacy IT they have in place. The impact of legacy technology on the adoption/integration of EMRs is felt most severely in the UK (**44%**), Australia (**42%**), and the U.S. and Canada (each **41%**).

The adoption/integration of EMRs has been a challenge/has been impacted by legacy IT



The adoption/integration of Electronic Medical Records has been a significant challenge for our organization 79% 74% 78% 71% 92% 73% 87% 66% 77% 82% 84% 80%

Legacy IT has impacted the adoption/integration of Electronic Medical Records 36% 41% 41% 35% 44% 33% 31% 33% 27% 27% 37% 42%

The data suggests that human adaptation is essential for effectively using new technology. **30%** of respondents said systems are changed too frequently for the organization to keep up with the changes. An additional **33%** said that training users on new systems slow processes and impacts patient care. However, the bigger challenge in getting IoT and telehealth medical devices to work smoothly comes from outdated systems within the healthcare industry:

90%

of organizations call for more investment in new or better technology to improve patient care, and

89%

for more interconnected devices.

LEGACY SYSTEMS CREATING SECURITY RISKS



More than eight in ten (83%)

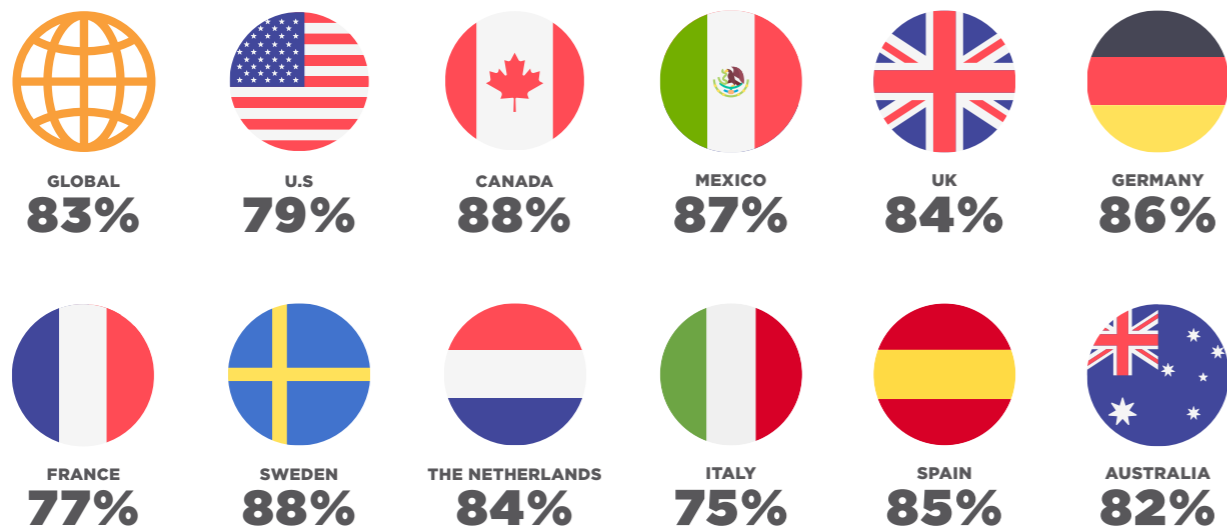
IT decision makers said their organization had experienced at least one **data breach/leak or ransomware attack** since 2023.

This is consistent with 2024 figures (85%), indicating that these threats remain just as prevalent and are not being effectively managed.

There may be little year-over-year change in the overall percentage of organizations experiencing incidents, but now almost half experienced an accidental data leak (48% compared to 2022 when it was 33%) and two-thirds experienced a data breach from an outside source or a ransomware attack (65%, in line with 2024 but up from 48% in 2022 and 52% in 2023).

The only type of incident to see a significant change this year is the percentage of IT decision makers reporting a planned employee data leak, which has fallen from 34% in 2024 to 24% in 2025.

Experienced one or more security incident in the past 12 months:



With planned employee data breaches falling this year, the human element of data security concerns may start to come under control, but the technology-driven sources are far from being wiped out.

This year, almost half of IT decision makers (45%) blame legacy IT for making networks vulnerable to security attacks, up from 36% in 2024.

It is an issue affecting organizations across the world, but in some countries, it is a greater concern: over half of IT decision makers in Sweden (55%), France (54%), Australia (53%) and Canada (51%) are now worried their network is susceptible to security attacks because of the legacy IT they have in place.

The concern with legacy IT is growing year-over-year, as it has increased in every country surveyed. Without addressing legacy system issues, organizations face increasing exposure to security threats, operational inefficiencies and compromised patient care.

“Legacy IT makes our network vulnerable to security attacks”

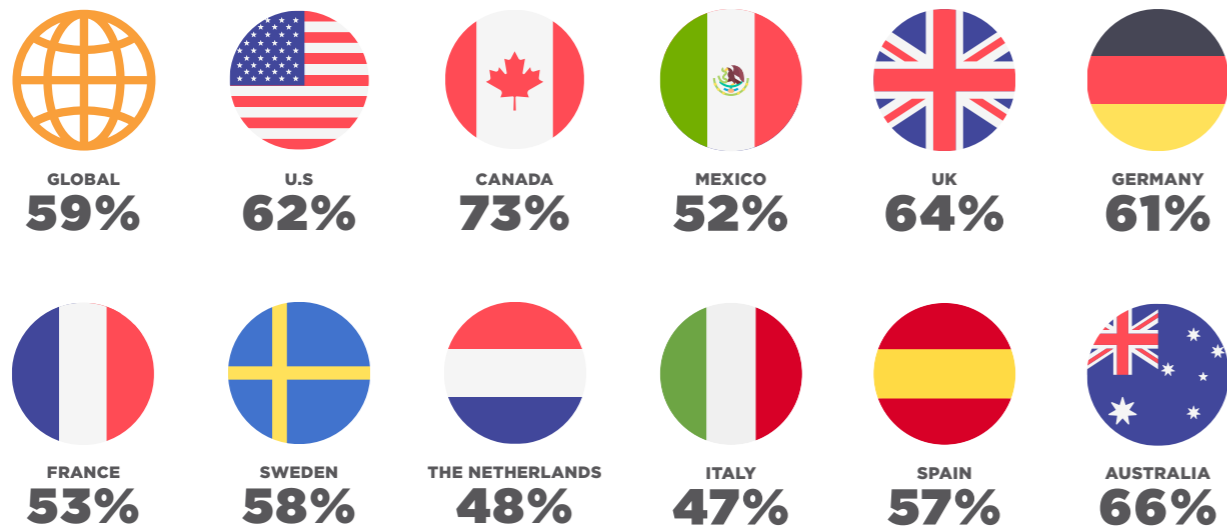
	2025	2024		2025	2024
	45%	36%		54%	27%
	44%	39%		55%	25%
	51%	43%		40%	37%
	39%	35%		37%	-
	43%	40%		41%	-
	45%	33%		53%	39%

Four in ten (38%) can't support devices remotely or get detailed information on device issues, and one in five (20%) said they cannot detect new devices connecting to the system. Legacy IT is in use in 97% of healthcare organizations. Based on this year's research, it continues with integration, maintenance and security issues.

LEGACY SYSTEMS CREATING MORE WORK FOR IT TEAMS

Frequent technical issues and downtime present a further challenge when using interconnected devices and telehealth medical devices, one that affects **59%** of organizations this year, up from **52%** in 2022.

Has your organization experienced frequent technical issues/downtime using IoT/Telehealth medical devices?



Technical downtime in healthcare settings can lead to interruptions in patient care, affecting the overall efficiency of operations. Organizations face challenges related to system updates and maintenance, which lead to inefficient workflows and a decrease in healthcare quality.

The challenges are experienced globally, yet technical issues and downtime are experienced significantly more in the following countries: Canada (**73%**), Australia (**66%**), and UK (**64%**).

While focusing on strategic projects, IT teams often find themselves bogged down by time-consuming tasks related to troubleshooting minor technical issues, such as fixing printers, connectivity issues, and other repetitive support tasks. Much of this problem is caused by legacy IT with **39%** of IT decision makers said this led them to spend too much time fixing issues. This inefficiency detracts from the ability to focus on more impactful initiatives that drive organizational improvements. Healthcare organizations must consider implementing solutions that can help integrate existing and new technologies.

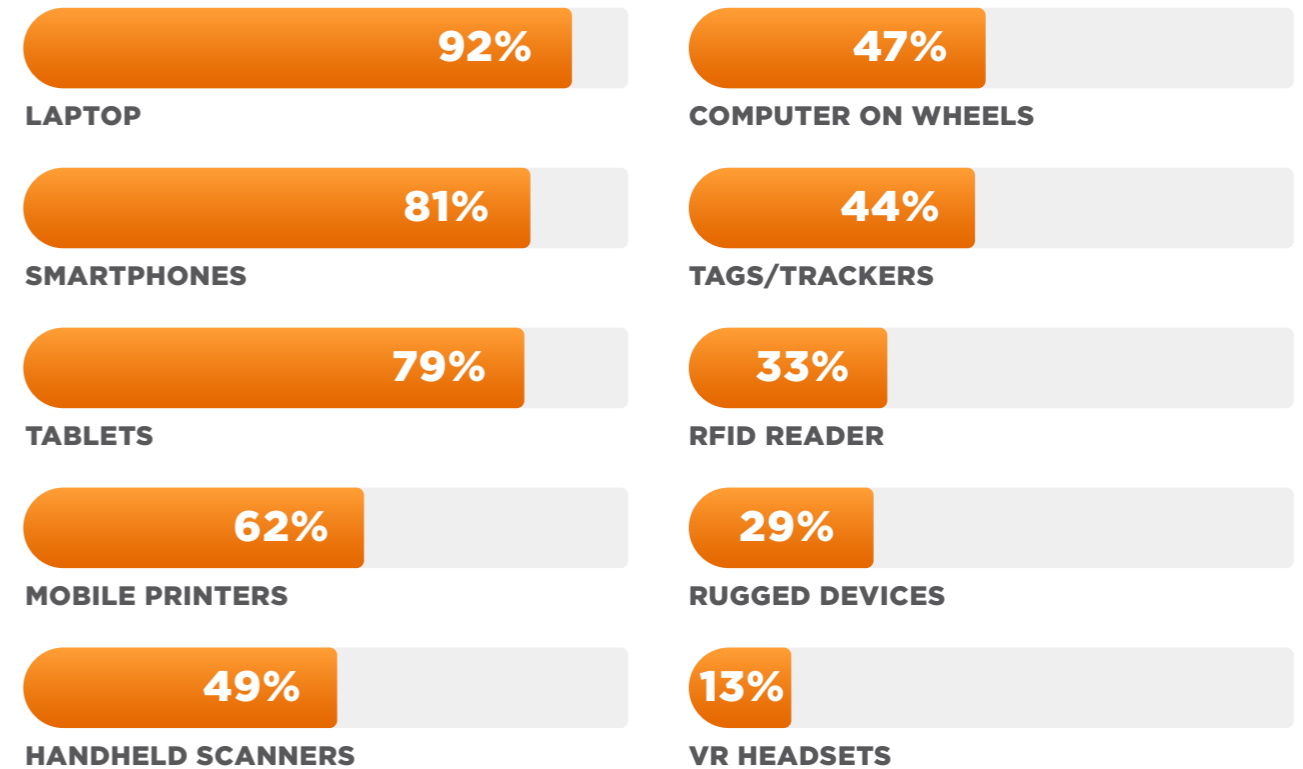


THE WAY FORWARD: ENTERPRISE MOBILITY MANAGEMENT HAS REPLACED MOBILE DEVICE MANAGEMENT

The increasing integration of various mobile devices, broader usage of printers and wide range of applications into everyday healthcare operations demands a robust device management solution.

Which of the following types of mobile devices are used in your organization?

Global Findings



With such a diverse fleet of devices, healthcare organizations face the challenge of maintaining security, conducting remote troubleshooting, and ensuring that all devices function optimally. For IT decision makers, it is crucial to have seamless connectivity with these devices. To meet these demands, healthcare organizations must move beyond traditional MDM and adopt a more comprehensive, integrated approach.

THE GROWING NEED FOR EMM SOLUTIONS

Undoubtedly, there is a place for mobile technology as **86%** of IT decision makers say it makes their jobs faster. However, the number in circulation suggests there are a lot of mobile devices to track, maintain and manage, with the majority using MDM for security purposes (**90%**). This includes managing security policies, protecting against cyberthreats, and identifying unauthorized devices accessing the network, all critical to minimizing vulnerabilities and reducing the risk of breaches.



What features of an MDM solution are critical for your operations?



Many healthcare organizations rely on MDM solutions for basic security and device management, but that's just the baseline. In today's high-stakes, fast-paced healthcare environment, basic MDM is no longer enough.

With the growing complexity of patient care and the increasing number of connected devices, organizations must shift from reactive to proactive strategies that detect and prevent issues before they impact care. This means going beyond the fundamentals to implement real-time monitoring and stay ahead of security breaches and operational disruptions.













Two-thirds (**65%**) of IT decision makers report that their organization experienced a data breach from an outside source or a DDoS ransomware attack in the past 12 months. This highlights the need to move beyond the basics and implement more advanced and comprehensive security measures.







Data security still tops the list of IT concerns, with **30%** of IT decision makers mentioning it. The percentage listing it as their top concern continues to increase significantly from **16%** in 2023 and **23%** in 2024. Add to this the **13%** who said that managing the security of shared devices was their top concern this year, and we see almost half (**43%**) name a security-related issue as the top worry faced by IT within their organization.

What is currently the biggest area of concern for IT within your organization?

Data security concern or managing the security of shared devices

	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%

Data security is the top concern for all countries this year, with some countries experiencing a particularly sharp increase:

-  in **France**, a security related issue was rated the top concern by **25%** in 2024 and **51%** in 2025,
-  in **Canada** it rose from **39%** last year, and is now for **53%**,
-  in **Australia** it jumped from **39%** to **53%**
-  and in **Germany** from **24%** to **41%**.

The nature of mobile devices necessitates that they be handled by multiple users. It is no surprise, then, that managing the security of shared devices remains a top IT concern. Add to this the challenge of legacy technology making it nearly impossible to manage these devices remotely, and mobile devices therefore become a double-edged sword.

'Basic' MDM features are no longer enough for the modern tech world and all the complex devices and systems that are in place. The historic MDM capabilities have reached their limits. Today, the need for advanced technology solutions is more critical than ever. Modern EMM tools give healthcare organizations greater visibility into their entire device ecosystem, enabling them to better monitor operations, strengthen data security, and respond faster to emerging threats.

PRIORITIZING MOBILE DEVICE SECURITY: COVERING ALL BASES

Organizations are prioritizing measures to ensure mobile devices are secure. Some organizations focus on a human-centric approach with **45%** training employees on security threats, best practices, and data protection laws, while a similar number restrict access to sensitive data based on roles and responsibilities. Yet only a third (**33%**) have an incident response plan in place should something go wrong.

Undertaking regular updates is the most implemented security measure, with **51%** doing so. Significantly more of those who had experienced no data security incident in the past 12 months (**60%**) employ this approach (compared with only **49%** of those who had experienced an incident). The use of multi-factor authentication is prioritized by **44%** with encryption by **42%**.

It's clear that all organizations are doing something to protect mobile devices, but few are doing everything they can.



THE NEED FOR BETTER MOBILE DEVICE MANAGEMENT STRATEGIES

Security isn't the only place where outdated MDM solutions are falling short. Many healthcare organizations face inconsistencies in applying these solutions across various devices, which complicates device tracking and support. This inconsistency often leads to unnecessary device replacements and inefficiencies in overall operations.

Nearly half (**47%**) of IT decision makers say an MDM solution is critical for their organization to remote troubleshoot and **45%** say it is critical for device tracking, but **38%** of organizations are not able to deploy and manage new devices and printers easily due to legacy systems and **38%** are unable to support devices remotely or get detailed information on device issues for the same reason.

The research highlights the need for healthcare organizations to adopt robust, centralized EMM solutions that ensure device security and compliance. These solutions should also support remote troubleshooting, streamline configuration, and deliver actionable insights.

Advanced tools that provide analytics and operational intelligence across all devices enable IT teams to proactively identify device performance issues. It can also track usage trends, providing organizations with insights to help make informed decisions. This approach reduces downtime, minimizes inefficiencies, and enhances the overall quality of care.

DISPOSABLE MEDICAL TECHNOLOGY

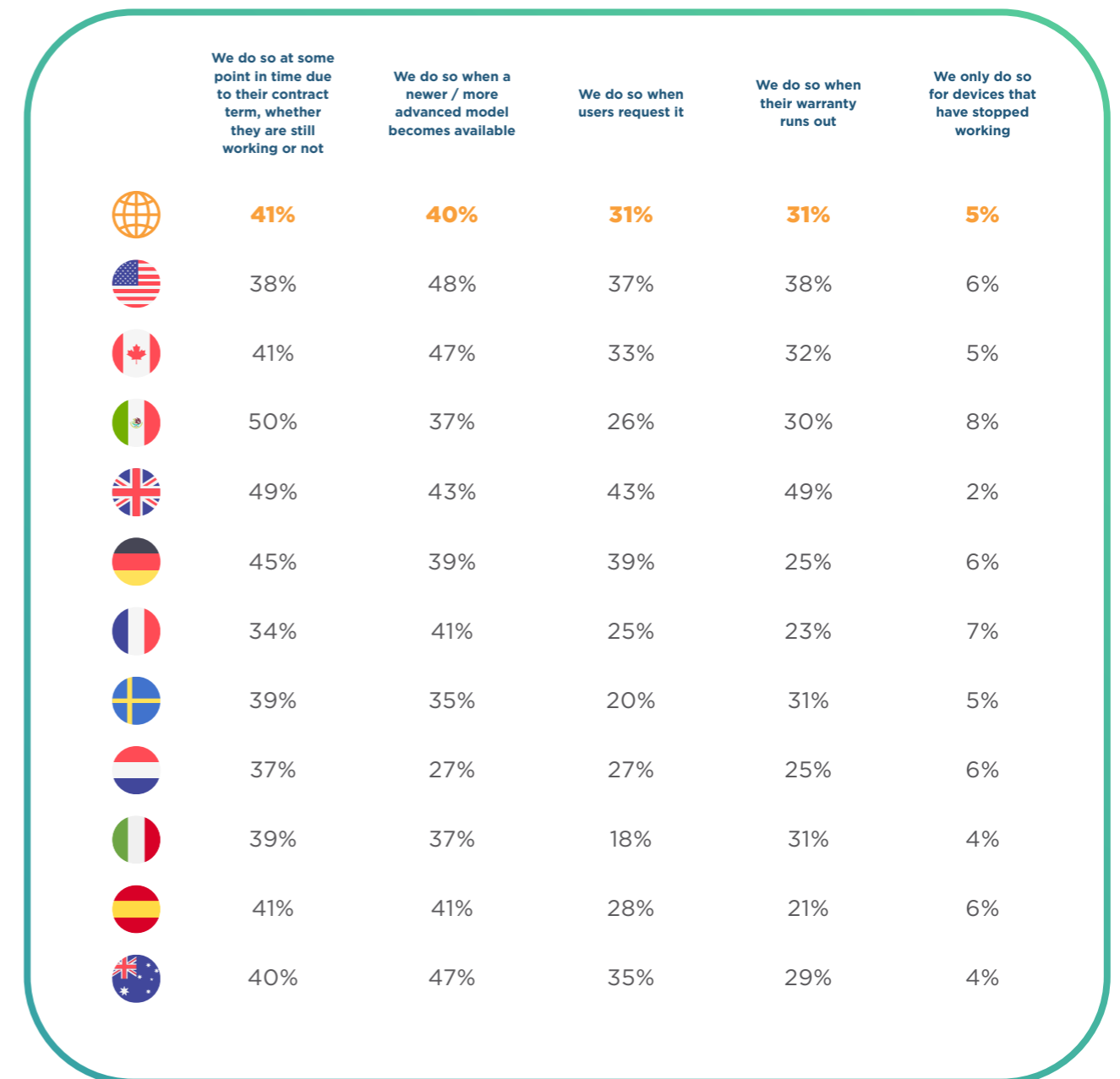
Concerns do not end when a mobile device is no longer in use, they often increase. In fact, **81%** of IT decision makers are concerned about the security of patient data during device disposal.

Healthcare organizations handle massive volumes of sensitive data, and without standardized disposal processes, retired devices pose serious risks of data breaches and regulatory non-compliance. While most organizations take steps to protect data when disposing of devices, inconsistencies remain high, and this year, eight in ten IT decision makers still express concern.

Frequent upgrades compound the issue. **31%** of organizations replace devices upon user request, **40%** do so when newer models are available, **41%** replace them based on contract terms, and **31%** when warranties expire. This raises major security and sustainability concerns.

To reduce risk, organizations must implement standardized protocols, including remote data wipe and robust lifecycle management to ensure proper tracking and disposal. Staff should also receive regular training on secure disposal practices. By prioritizing secure and sustainable processes, healthcare organizations can better protect patient data and meet compliance standards.

What is your organization's policy for upgrading/renewing/replacing devices such as the ones mentioned above, e.g., smartphones, tablets, rugged devices etc.?



The U.S., Canada and Australia have the highest percentage of replacing devices when a new version becomes available. Although it is important to note that this is a common trend seen globally. It is crucial to find a balance between device sustainability and performance. If devices are only disposed of when they stop working, IT teams will spend even more time fixing the little issues.

BATTERY HEALTH MANAGEMENT - PREVENTION BETTER THAN CURE

Inefficient monitoring of battery health can also be a reason for the unexpected device failures in the healthcare sector. Higher costs due to premature device replacements, leading to financial constraints and environmental concerns regarding e-waste disposal are common. **97%** of organizations actively monitor device battery health, yet only one third (**31%**) say they check only when issues arise.

For **41%**, their policy is to replace batteries on a fixed schedule, regardless of battery health. More reassuringly, half conduct regular manual checks, **44%** use automatic battery health monitoring and **41%** have a predictive maintenance system in place.

Ultimately, the findings suggest that while mobile devices offer undeniable benefits, their management must be optimized: implementing EMM solutions to establish best practices for device tracking, battery health monitoring, and sustainable replacement strategies. Such steps would not only streamline daily operations but also pave the way for more strategic IT initiatives across the healthcare landscape.





CONCLUSION

The healthcare sector is rapidly advancing its digital transformation journey, yet the path remains complex. Despite the widespread use of IoT and telehealth devices, outdated legacy systems present issues such as incomplete data consolidation and frequent technical disruptions, preventing IT teams from reaping the benefits of their digital transformation journey.

At the same time, security related issues have emerged as the foremost concern for **43%** of IT decision makers, driven by threats ranging from the management of shared devices to increasing data breaches. While planned employee data leaks have slightly decreased, accidental leaks and sophisticated external attacks continue to expose vulnerabilities. Nearly half of IT leaders attribute legacy systems as a primary reason for making networks vulnerable to attacks, underscoring the urgent need to modernize foundational technologies. It seems the issue is less about the emerging technology itself and more about the systems that support it.

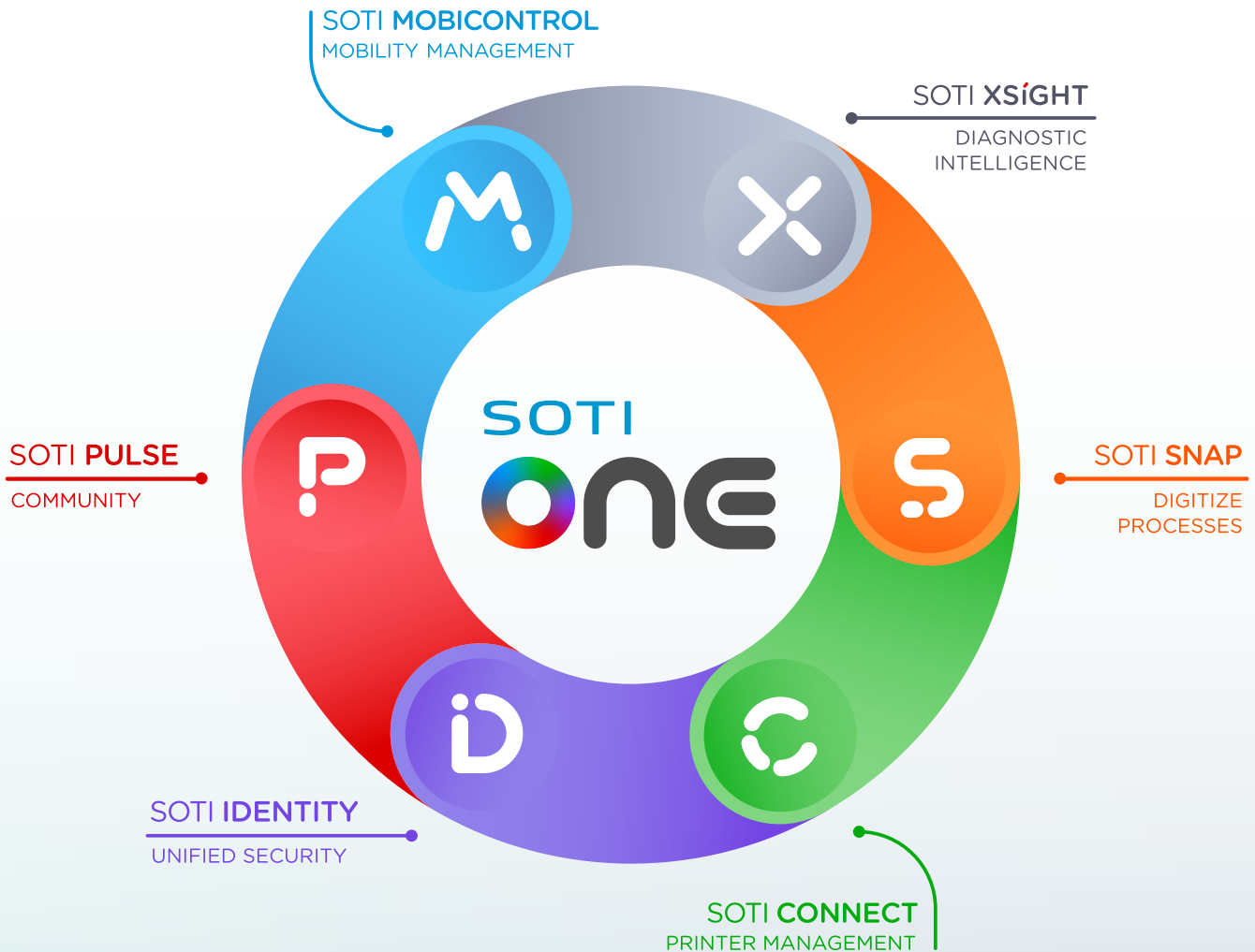
AI adoption has surged globally and is used in a third more organizations this year, with regions such as the UK and Australia leading the way. AI is being integrated into medical data analysis, treatment planning, personalized patient care and beyond. A lifeline for the overburdened healthcare industry, but the need to monitor and secure its usage cannot be overlooked.

Moreover, managing mobile devices is proving to be a significant drain on IT resources and the multitude of devices in use complicates effective monitoring and remote management. The insufficiency of existing MDM solutions and inconsistent replacement policies add further strain, heightening both security and sustainability concerns.

Ultimately, achieving true digital transformation in healthcare demands that organizations step back and consider the bigger picture. What is needed is a strategy that combines the continued widespread adoption of innovative technologies with targeted investments in modernizing and integrating IT infrastructures and a fit-for-purpose EMM solution. This balanced approach will enable organizations to secure data, streamline mobile device use, and ultimately enhance patient care.

ABOUT SOTI

SOTI is a proven innovator and industry leader for simplifying business mobility solutions by making them smarter, faster and more reliable. With SOTI's [innovative portfolio of solutions](#), organizations can trust SOTI to elevate and streamline their mobile operations, maximize their ROI and reduce device downtime. Globally, with over 17,000 customers, SOTI has proven itself to be the go-to mobile platform provider to manage, secure and support business-critical devices. With SOTI's world-class support, enterprises can take mobility to endless possibilities.



TO LEARN MORE:

For additional information on how SOTI can set your business up for success, [click here](#).

To learn more about the SOTI ONE Platform, [click here](#).

To find out how SOTI can help with your mobile investments, contact us today at sales@soti.net.

SOTI is a proven innovator and industry leader for simplifying business mobility solutions by making them smarter, faster and more reliable. SOTI helps businesses around the world take mobility to endless possibilities.

soti.net

© 2025, SOTI Inc. All Rights Reserved. All product and company names are trademarks™ or registered® trademarks of their respective owners. The use of these trademarks does not imply any affiliation with SOTI or endorsement by the trademark holder. Offers subject to change or cancellation without notice. SOTI reserves the right to modify products, services, or pricing at any time. Information is provided "AS IS" without any warranty. Products and services are governed by applicable terms and conditions.