

ZORGORGANISATIES ONDER DE LOEP:

GECONTROLEERDE RISICO'S EN ONVERWACHTE UITDAGINGEN



WELKOMSTBERICHT

De gezondheidszorg staat op het punt van een digitale revolutie. Innovaties op het gebied van AI, telezorg, mobiele technologie en automatisering bieden nieuwe mogelijkheden voor slimmere, meer verbonden zorg. Ondanks deze vooruitgang blijven veel zorginstellingen stilstaan door verouderde systemen en operationele inefficiënties.

Voor IT-leidinggevend is de uitdaging duidelijk. Instellingen moeten sneller moderne technologieën invoeren om resultaten te verbeteren, medewerkers te ondersteunen en probleemloze zorgervaringen te leveren die patiënten verwachten.

Verouderde systemen leiden tot minder snelle toegang tot cruciale informatie, wat uiteindelijk de kwaliteit van de zorg vermindert. Ondertussen kan AI diagnoses verbeteren, workflows stroomlijnen en behoeften van patiënten voorspellen, maar alleen met de ondersteuning van moderne infrastructuur.

De mate waarin nieuwe technologie is geïntegreerd en de mogelijkheid om alle apparaten en toepassingen optimaal te kunnen gebruiken, spelen een belangrijke rol



Stephanie Lopinski, VP, Global Marketing

bij de invloed op patiëntresultaten en de kwaliteit van geleverde zorg. Instellingen moeten prioriteit geven aan systeemintegratie, toegang tot realtime data en moeten afstand doen van verouderde technologie om te profiteren van de voordelen van digitale transformatie.

In ons meest recente onderzoek onderzoeken we de huidige situatie van zorginstellingen, de problemen waarmee ze worden geconfronteerd en strategieën voor vooruitgang.

Het rapport van SOTI uit 2025 benadrukt drie belangrijke thema's:

Kunstmatige intelligentie

Het gebruik van AI in de gezondheidszorg neemt snel toe, met **81%** van de wereldwijde instellingen die het gebruiken voor patiëntenzorg, vergeleken met **61%** in 2024. AI wordt onder andere gebruikt om medische gegevens te verwerken, gegevens bij te werken, behandelingen te personaliseren en aandoeningen te diagnosticeren.

Ondanks dat AI steeds vaker wordt gebruikt, heeft maar **36%** van de instellingen AI specifieke beveiligingsmaatregelen getroffen, wat de privacy van patiënten in gevaar kan brengen. Daarom is het van fundamenteel belang om systemen te moderniseren om de privacy van patiënten te waarborgen.

Het rapport van 2025 schetst een duidelijk beeld. De technologische ontwikkeling binnen de gezondheidszorg gaat snel, maar niet overal gelijk op. Totdat verouderde systemen zijn vervangen, gegevensbeveiliging wordt verbeterd en IT'ers niet voortdurend problemen op te hoeven lossen, zal de sector moeite blijven houden om implementatie om te zetten in echte integratie.

Verouderde systemen

Zorginstellingen hebben er moeite mee om verbonden systemen en digitale zorgoplossingen te integreren, met name door de verouderde systemen die lastig op afstand te beheren zijn.

Deze systemen leveren aanzienlijke veiligheidsrisico's op, waarbij **83%** van de instellingen sinds 2023 gegevensinbreuk, gegevenslekken of ransomware-aanvallen melden. Daarnaast bemoeilijken ze de integratie van Elektronische Patiëntendossiers (EPD's), waar **79%** van de instellingen mee te maken heeft.

Het resultaat is dat, wanneer instellingen nieuwe technologieën proberen in te voeren, problemen vaak aanhouden, wat innovaties

tegenhoudt en een negatieve invloed heeft op de patiëntervaring. Uiteindelijk beïnvloeden de beperkingen door deze verouderde systemen direct de resultaten van patiëntenzorg, wat het cruciaal maakt voor instellingen om te investeren in moderne technologie en verbonden systemen om de efficiëntie, beveiliging en algemene kwaliteit van zorg te verbeteren.

Mobile Device Management + Enterprise Mobility Management

Zorginstellingen vertrouwen steeds meer op verschillende mobiele apparaten, waaronder laptops, smartphones, tablets en speciale apparatuur zoals RFID-lezers. Het beheren van deze apparaten biedt aanzienlijke uitdagingen op het gebied van beveiliging en probleemoplossing op afstand wanneer u vertrouwt op verouderde oplossingen voor Mobile Device Management (MDM).

Het huidige landschap vraagt echter om een evolutie die verder gaat dan traditionele MDM en omvat een brede benadering voor Enterprise Mobility Management (EMM).

Naarmate de technologie binnen de gezondheidszorg zich ontwikkelt, moet de aandacht gericht worden op een geïntegreerd platform met geavanceerde diagnoses, data-analyses en operationele intelligentie. Met deze benadering kunnen instellingen problemen proactief oplossen en inzichten gebruiken om beslissingen te nemen en workflows te optimaliseren. Door processen te digitaliseren en administratieve taken te automatiseren, kunnen zorgverleners operationele efficiëntie verbeteren en een betere patiëntenzorg ondersteunen.

Voor effectieve oplossingen voor het beheer van mobiele apparaten is ook volledig levenscyclusbeheer vereist om de duurzaamheid te bevorderen. Instellingen moeten zich richten op het maximaliseren van de levensduur van hun apparaten, het gebruiken van inzichten in batterijgebruik en gebruikspatronen om duurzame vervangende strategieën te ontwikkelen. Dit proactieve beheer helpt niet alleen apparaten gezond te houden, maar vermindert ook kwetsbaarheden en beschermt patiëntengegevens.

HET VERANDERENDE LANDSCHAP VAN DE GEZONDHEIDSZORG:

VOORUITGANG EN DOORBRAKEN SINDS 2020

SOTI voert al sinds 2020 onderzoek uit naar de gezondheidszorg. Het onderzoek is steeds uitgebreider geworden en het aantal landen en respondenten ook. Trends in de afgelopen vijf jaar waren met name de opvallende inzichten hieronder:

2020/2021

- Beveiliging: **81%** maakt zich zorgen over de beveiliging van patiëntendossiers
- Technische problemen: **63%** ervaart wekelijks apparaat- of systeemstoringen
- Technische impact op patiëntenzorg: **81%** heeft problemen met systemen en techniek tijdens de zorg voor patiënten

475 thuiszorgmedewerkers, zorgverleners en overige professionals in de gezondheidszorg in zeven landen wereldwijd

2022

- Beveiliging: **73%** van de instellingen heeft sinds 2020 een gegevensinbreuk of gegevenslek meegemaakt
- IoT/telezorg: **98%** heeft mogelijkheden voor medische apparaten voor IoT/telezorg geïmplementeerd
- Impact downtime apparaten: **53%** zegt dat ze regelmatig downtime ervaren wat resulteert in een vertraagde patiëntenzorg en 3,4 uur per week per medewerker die verloren gaan

1300 IT-professionals die in zorginstellingen werken in acht landen wereldwijd

2023

- Beveiliging van patiëntgegevens: **97%** maakt zich zorgen met betrekking tot de beveiliging van patiëntgegevens
- Netwerkbeveiliging: **55%** heeft een toevallige of geplande gegevenslek uit interne bronnen meegemaakt. **53%** kan geen nieuwe apparaten detecteren die verbinding maken met het systeem als gevolg van verouderde systemen, wat leidt tot kwetsbaarheden
- Verouderde systemen: **52%** zegt dat verouderde systemen ervoor zorgen dat ze niet in staat zijn om problemen tijdig op te lossen **37%** gelooft dat verouderde systemen ze kwetsbaarder maakt voor inbreuken op de beveiliging
- Downtime: 3,4 uur verloren tijd is in een normale week als gevolg van technische of systeemproblemen

1450 IT-professionals die in zorginstellingen werken in negen landen wereldwijd

2024

- AI: **85%** denkt dat AI kan helpen om taken te vereenvoudigen, maar momenteel past slechts 23% AI op brede schaal toe
- Beveiliging: **71%** draagt gegevens over naar externe harde schijven/back-ups als ze oude apparaten afdanken. **23%** geeft aan dat gegevensbeveiliging hun grootste IT-probleem is
- IoT/telezorg: **67%** ervaart regelmatig problemen met IoT-/telezorg-apparaten met vertraagde patiëntenzorg tot gevolg.
- Verouderde systemen: **63%** bevestigt dat ze verouderde technologieën gebruiken, en **45%** heeft het afgelopen jaar een gegevensinbreuk of onbedoeld gegevenslek ervaren
- Downtime: 3,9 uur per week per medewerker verloren aan downtime

1450 IT-professionals/besluitvormers die in zorginstellingen werken in negen landen wereldwijd

2025

- AI: **81%** gebruikt momenteel AI voor patiëntenzorg, vergeleken met 61% in 2024
- Beveiliging: **83%** heeft in de afgelopen 12 maanden een onbedoeld gegevenslek, externe gegevensinbreuk of DDoS ransomware-aanval ervaren. **30%** geeft aan dat gegevensbeveiliging hun grootste IT-probleem is
- IoT/telezorg: **96%** ervaart problemen met de implementatie van medische apparaten voor IoT/telezorg
- Verouderde systemen: **45%** geeft verouderde IT de schuld voor de kwetsbaarheid van netwerken voor aanvallen
- Mobile Device Management: **47%** zegt dat oplossingen voor Mobile Device Management cruciaal zijn om op afstand problemen op te lossen

1750 IT-professionals/besluitvormers die in zorginstellingen werken in negen landen wereldwijd

INHOUD

Methodologie

Wereldwijde verdeling

Belangrijkste bevindingen

De doorbraak: Kunstmatige intelligentie tijdens pieken in patiëntenzorg

De uitdaging: Verouderde systemen beperken de waarde van opkomende technologie

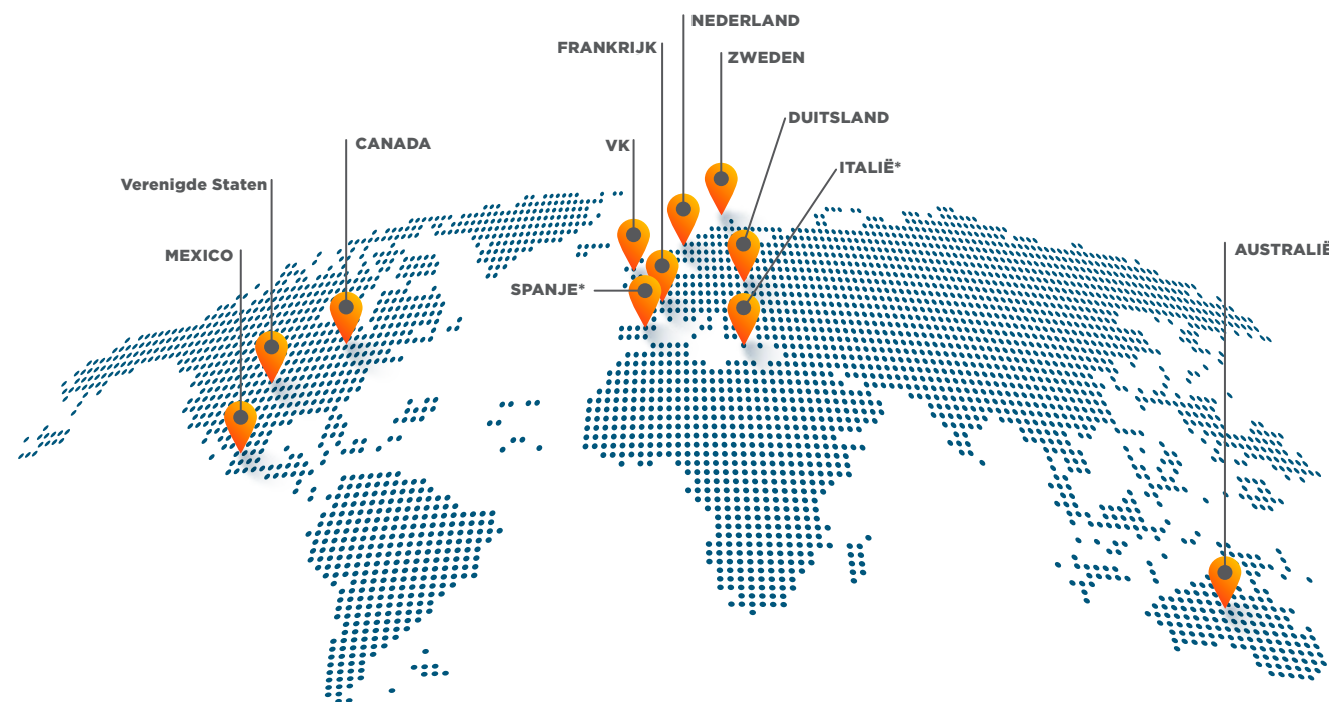
De te volgen koers: Enterprise Mobility Management heeft Mobile Device Management vervangen

Conclusie

METHODOLOGIE

Dit jaar is het onderzoek van SOTI uitgebreid tot **1750 respondenten in 11 landen**: Verenigde Staten (200), Canada (150), Mexico (150), het Verenigd Koninkrijk (200), Duitsland (150), Frankrijk (150), Zweden (150), Nederland (150), Italië* (150), Spanje* (150) en Australië (150). Het onderzoek is uitgevoerd tussen januari en maart 2025 door IT-besluitvormers binnen zorginstellingen.

*Nieuwe landen die zijn toegevoegd aan het 2025 gezondheidszorgrapport.



WERELDWIJDE UITVAL

Voor dit rapport verwijzen zorginstellingen naar:



Een ziekenhuis dat essentiële patiëntenzorg biedt.



Een algemene medische praktijk/kliniek met verschillende specialiteiten, zoals een dokterspraktijk, huisarts, medische praktijk.



Een kliniek die essentiële patiëntenzorg biedt met één of meer specialiteiten, bijvoorbeeld geestelijke gezondheid, neurologie, fysiotherapie, etc.



Een zorgverlener die directe patiëntenzorg of telezorg biedt.

Zorginstellingen met 50 tot meer dan 5000 medewerkers. Hoewel alle respondenten betrokken waren bij IT-besluitvorming voor een zorginstelling, verschilden hun rollen van IT-professionals tot het hoogste managementniveau en het niveau van c-suite.



WERELDWIJDE BEVINDINGEN

96%

van de instellingen ervaart problemen met de implementatie van medische apparaten voor IoT/telezorg waarbij systeemintegratie het grootste probleem is.

83%

van de beveiligingsincidenten blijft hoog, waarbij onbedoeld gegevens lekken, externe datalekken en DDoS ransomware-aanvallen niet lijken af te nemen.

47%

van de IT-besluitvormers zegt dat oplossingen voor Mobile Device Management van cruciaal belang zijn om problemen op te lossen.

45%

geeft verouderde IT de schuld voor de kwetsbaarheid van netwerken voor aanvallen.

81%

maakt zich zorgen over de beveiliging van patiëntgegevens als ze mobiele apparaten afdanken.

81%

gebruikt AI nu op een bepaalde manier om de efficiëntie en effectiviteit van patiëntenzorg te verbeteren, vergeleken met 61% in 2024.

40%

van de instellingen vervangt oude apparaten als er nieuwe versies beschikbaar komen.

30%

zegt dat gegevensbeveiliging hun grootste IT-probleem is, vergeleken met 23% in 2024.



DE DOORBRAAK: KUNSTMATIGE INTELLIGENTIE IN PIEKEN VAN PATIËNTENZORG

In de afgelopen jaren heeft de zorgsector vooruitgang geboekt, met name door technologie te integreren in patiëntenzorg. De opkomst van AI verandert de manier waarop zorgverleners diensten verlenen en communiceren met patiënten.

AI gebruiken om diagnoses te verbeteren, behandelplannen te personaliseren en activiteiten te stroomlijnen heeft wereldwijd de aandacht van zorginstellingen. Uit onze enquête van dit jaar blijkt dat AI wordt gebruikt voor patiëntenzorg in **81%** van de zorginstellingen, een derde meer dan in 2024 (**61%**).

De meeste instellingen die op dit moment geen AI voor patiëntenzorg gebruiken, overwegen het op zijn minst (**16%** wereldwijd), waarbij slechts **3%** van de IT-beleidsmakers zegt dat hun instelling geen plannen heeft om het te gebruiken.

AI wordt het meest gebruikt in het Verenigd Koninkrijk, waar **94%** van de IT-besluitvormers zei dat hun instelling het heeft gebruikt voor patiëntenzorg, vergeleken met **47%** in 2024. In Australië zei **93%** dat ze AI gebruikt, vergeleken met eerder **70%**.

Percentage instellingen dat in 2025 AI voor patiëntenzorg gebruikt
vergeleken met 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: MINDER ADMINISTRATIEVE ROMPSLOMP

Alhoewel het aantal organisaties die AI gebruikt is toegenomen, blijft de manier waarop ze de technologie toepassen grotendeels ongewijzigd sinds vorig jaar. In 2025 werd AI het meest gebruikt voor het verwerken en/of analyseren van medische gegevens (60% van de IT-beleidsmakers zei dat hun instelling AI hiervoor gebruikt), gevolgd door patiëntendossiers bijwerken (59%). Net iets minder dan de helft (46%) gebruik AI om de beste behandeling te plannen, terwijl 45% het gebruikt om behandelingen te personaliseren en 40% het gebruikt om aandoeningen te diagnosticeren.

Op welke van de volgende manieren gebruikt uw instelling momenteel AI voor patiëntenzorg? (Gevraagd aan mensen die AI gebruiken voor patiëntenzorg)

Wereldwijde bevindingen	2025	2024
Om medische gegevens te verwerken of analyseren	60%	60%
Om patiëntendossiers bij te werken	59%	56%
Om de beste behandeling te plannen	46%	47%
Om behandelingen te personaliseren	45%	44%
Om andere administratieve taken uit te voeren	45%	20%
Om aandoeningen te diagnosticeren	40%	38%
NET: Om dossiers bij te werken/overige administratie	79%	63%

Een belangrijke verandering dit jaar is dat AI vaker wordt gebruikt voor overige administratieve doeleinden. In 2024 meldde 20% van de IT-beleidsmakers dat ze AI op deze manier gebruikten en in 2025 nam dit toe tot 45%.

Door tijdrovende taken over te laten aan AI, kunnen zorgverleners zich richten op belangrijke aspecten van patiëntenzorg. Als we dit meenemen naast het feit dat instellingen AI gebruiken om medische dossiers bij te werken, zien we een netto AI-gebruik van 79% voor een of andere vorm van administratieve werkzaamheden.



Het Verenigd Koninkrijk en de VS zijn de grootste gebruikers van AI voor de personalisatie van behandelingen (57% en 55%), en het Verenigd Koninkrijk loopt voorop wat betreft het diagnosticeren van aandoeningen met AI (52%). Zweden (53%) en Canada (52%) gebruiken AI het meest voor andere administratieve doeleinden.

Uit het onderzoek van vorig jaar bleek dat meer dan de helft (57%) van de IT-professionals bedenkingen had over het gebruik van AI in de patiëntenzorg, en zich zorgen maakte over de bedreiging die het vormt voor de privacy van patiënten. Dit jaar bleek dat alle instellingen ten minste een aantal veiligheidsmaatregelen heeft doorgevoerd

voor mobiele apparaten, maar toch heeft maar 36% AI-specifieke beveiligingsmaatregelen genomen. Gezien de enorme toename van het gebruik van AI in het afgelopen jaar, zou dit iets moeten zijn dat meer zorginstellingen zouden moeten onderzoeken.

Welke beveiligingsmaatregelen vindt u het belangrijkst voor mobiele apparaten?

Regelmatige updates	51%
Medewerkers trainen in en op de hoogte brengen van specifieke dreigingen en de beste beveiligingsprocedures	45%
Zorgen dat er aan de wet- en regelgeving voor gegevensbescherming wordt voldaan (zoals de AVG en EHDS)	45%
Toegang tot gevoelige gegevens beperken voor bepaalde functies en verantwoordelijkheden	45%
Multi-factor authenticatie	44%
Encryptie	42%
Regelmatige beveiligingscontroles uitvoeren	42%
AI specifieke beveiligingsmaatregelen nemen	36%
Anonimiseren van gegevens invoeren	34%
Een incidentbestrijdingsplan invoeren	33%
Op afstand opschonen	23%

Vorig jaar zeiden meer dan acht van de tien (83%) IT-professionals dat AI een essentiële kostenbesparende strategie is voor zorginstellingen. Dit jaar is het gebruik in de patiëntenzorg enorm gestegen. Met de problemen die verouderde systemen met zich meebrengen voor het gebruik van opkomende technologie en de uitdagingen op het gebied van gegevensbeveiliging die in de hele sector nog steeds bestaan, moet het beheer van apparaten die het gebruiken zorgvuldig worden gecontroleerd om te zorgen dat alles er op een veilige manier uit kan worden gehaald.



DE UITDAGING: **VEROUDERDE SYSTEMEN BEPERKEN DE WAARDE VAN OPKOMENDE TECHNOLOGIE**

IMPLEMENTATIE VAN IOT EN TELEZORG IS UNIVERSEEL, MAAR ER ZIJN NOG STEEDS PROBLEMEN

De integratie van onderling verbonden technologieën hervormt het zorglandschap, vooral via telezorg, waarbij apparaten en systemen worden verbonden binnen zorgfaciliteiten en op afstand. Dit jaar gaven bijna alle IT-beleidsmakers (**99%**) aan dat hun organisaties op de een of andere manier verbonden apparaten of oplossingen voor telezorg gebruiken.

Ondanks dit hoge gebruik blijft de operationele efficiëntie van deze systemen achter bij de verwachtingen.

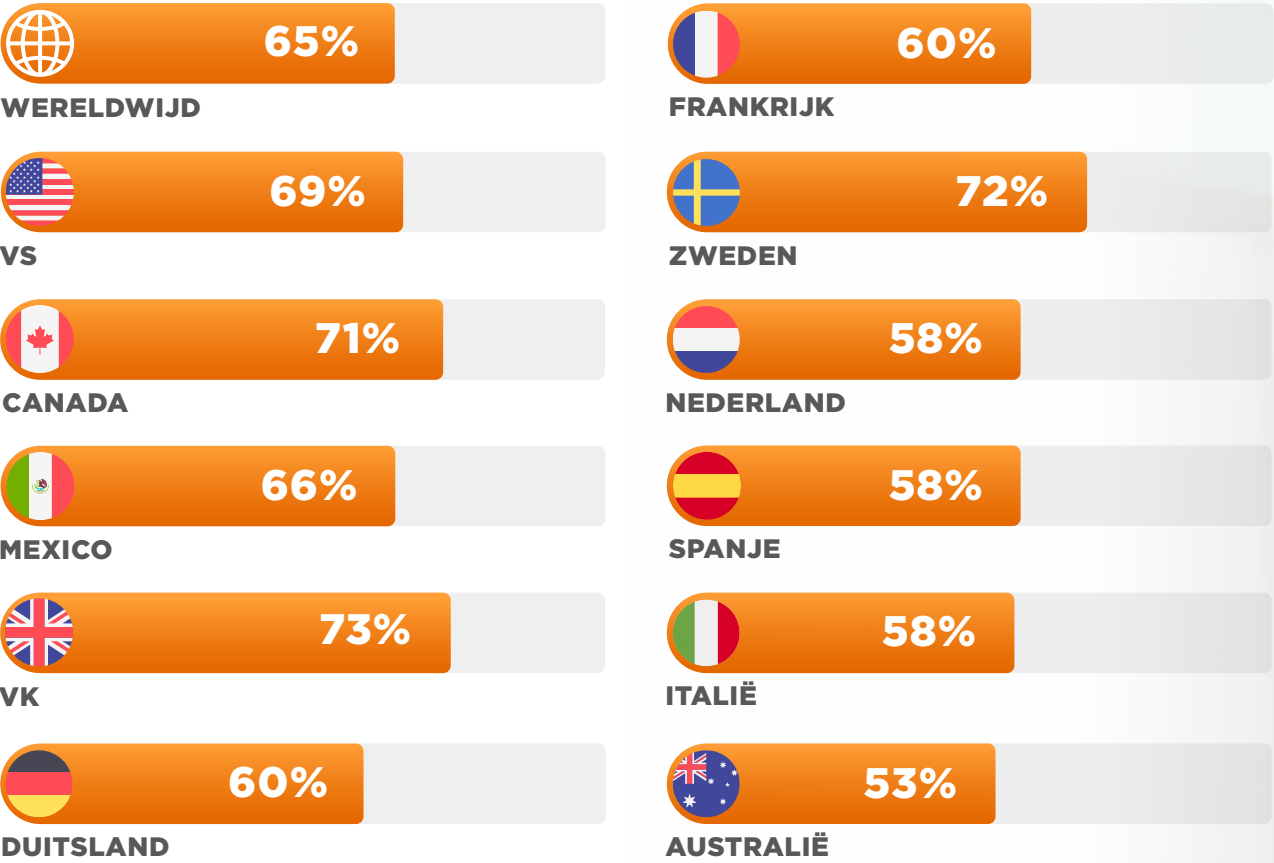
Een significante

96%

van de IT-leidinggevenden meldde dat ze problemen ondervonden met deze technologieën.

Een van de grootste problemen is het gebrek aan integratie tussen systemen die worden gebruikt voor verbonden apparaten en telezorg-applicaties. Dit probleem wordt weergegeven in de volgende statistieken voor verschillende regio's.

Systemen gebruikt voor medische systemen voor IoT/telezorg worden niet geïntegreerd:



De grootste uitdaging dit jaar voor **65%** van de instellingen is het gebrek aan integratie tussen deze systemen. Er zijn problemen met interoperabiliteit zoals niet op één locatie toegang kunnen krijgen tot het volledige medische dossier van een patiënt (aangegeven door **43%** van de respondenten) en het ontbreken van automatische updates tussen alle systemen (**40%**). Bovendien gaf **65%** van de IT-besluitvormers aan dat ze gefrustreerd zijn dat hun instellingen moeite hebben om relevante gegevens te verstrekken aan de juiste mensen wanneer ze deze het hardst nodig hebben.

Deze problemen treden wereldwijd op, maar ze werden vooral gemeld in Australië (**77%**), het Verenigd Koninkrijk (**73%**) en Canada (**71%**). Zorginstellingen met meerdere specialiteiten hebben ook vaak te maken met integratieproblemen. Van de zorginstellingen met deze problemen is **69%** een huisartsenpraktijk of kliniek, terwijl **67%** ervan klinieken zijn met één of meerdere specialisaties. Zo meldde **62%** van de IT-beleidsmakers in ziekenhuizen die essentiële patiëntenzorg bieden en instellingen gericht op externe of telezorg-diensten, dat ze tegen vergelijkbare integratieproblemen aanlopen. (**60%**).

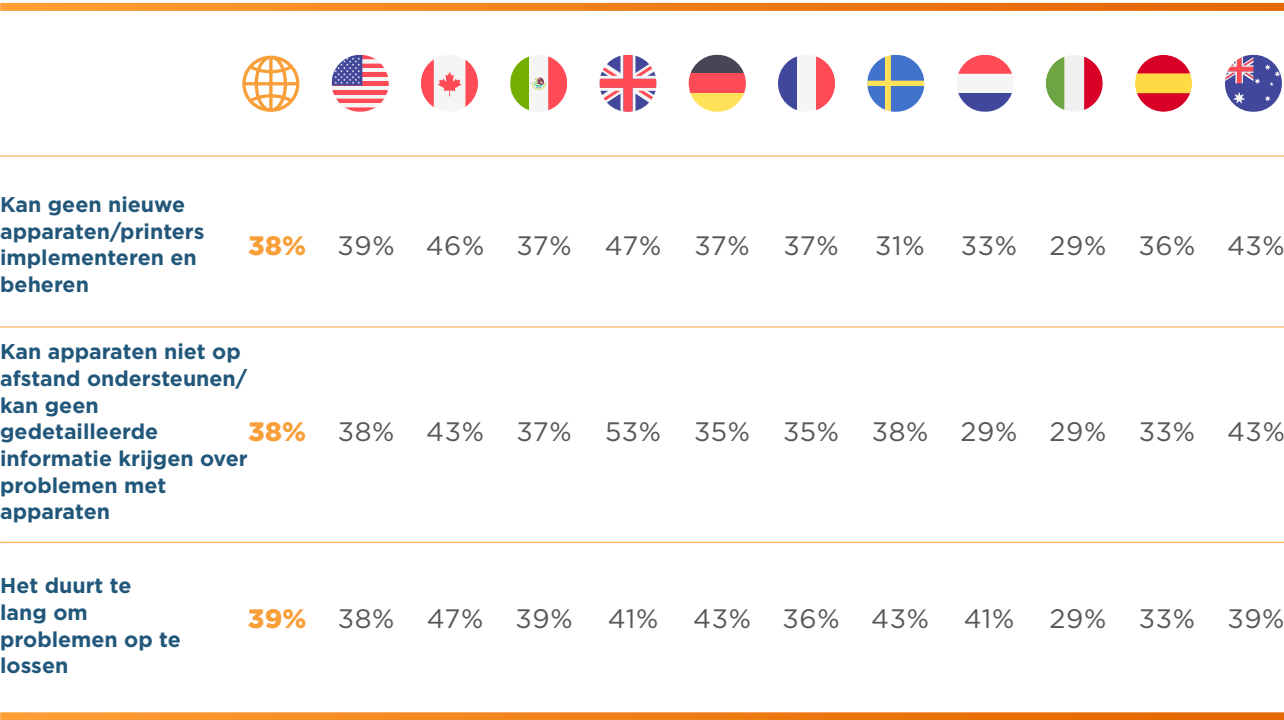


VEROUDERDE SYSTEMEN DIE PROBLEMEN MET INTEGRATIE EN INTEROPERABILITEIT OPLEVEREN

Het percentage IT-besluitvormers waarvan de instellingen verouderde technologie gebruiken, is gedaald van **63%** in 2024 naar **55%** dit jaar. Toch meldt **97%** van de IT-beleidsmakers dat hun organisatie verouderde technologie heeft. Ongeveer de helft van de organisaties die verouderde technologie gebruikt, vindt deze niet overbodig, maar het heeft invloed op hoe eenvoudig organisaties zich aan kunnen passen aan nieuwe werkmethoden.

Vier op de tien (**38%**) IT-beleidsmakers zei dat verouderde IT hen ervan weerhoudt nieuwe apparaten/printers te implementeren en te beheren en hetzelfde percentage zei dat het betekent dat ze apparaten niet op afstand kunnen beheren en geen gedetailleerde informatie krijgen over apparaatgebruik.

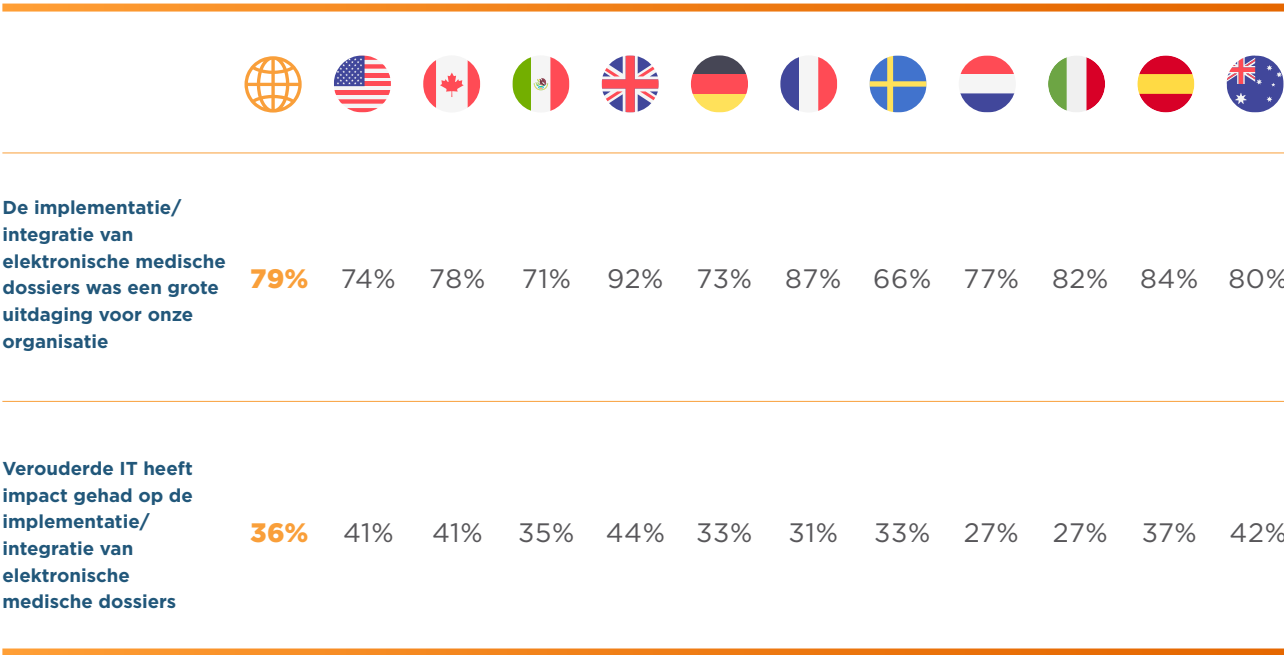
Welke impact heeft verouderde technologie op uw dagelijkse werkzaamheden?



Met de opkomst van elektronische medische patiëntendossiers (EPD's) om probleemloos patiëntengegevens te kunnen delen binnen zorginstellingen en het toenemende gebruik van telezorg-apparaten, zijn integratie en interoperabiliteit belangrijker dan ooit. Uit de resultaten van dit jaar blijkt echter dat problemen met systeemintegratie door verouderde systemen een obstakel blijven.

Meer dan driekwart (**79%**) van de IT-beleidsmakers zei dat de implementatie van EMR's een enorme uitdaging was voor hun organisatie, en **36%** wijt deze problemen rechtstreeks aan de verouderde IT die ze hebben. De impact van verouderde technologie op de implementatie/ integratie van EMR's is het grootst in het Verenigd Koninkrijk (**44%**), Australië (**42%**) en de VS en Canada (allemaal **41%**).

Multi-factor authenticatie



Uit de gegevens blijkt dat menselijke aanpassing essentieel is voor effectief gebruik van nieuwe technologie. **30%** van de respondenten zei dat systemen te vaak worden veranderd en de organisatie deze veranderingen niet bij kan houden. Nog eens **33%** zei dat gebruikers trainen in nieuwe systemen processen vertraagt en van invloed is op patiëntenzorg. Het grote probleem om te zorgen dat medische apparaten voor IoT en telezorg soepel werken, zijn echter verouderde systemen binnen de zorgsector:

90%

van organisaties en dit vraagt om investeringen in nieuwe of betere technologie om patiëntenzorg te verbeteren, en

89%

voor meer verbonden apparaten.

VEROUDERDE SYSTEMEN DIE BEVEILIGINGSRISICO'S OPLEVEREN



Meer dan acht op de tien (83%)

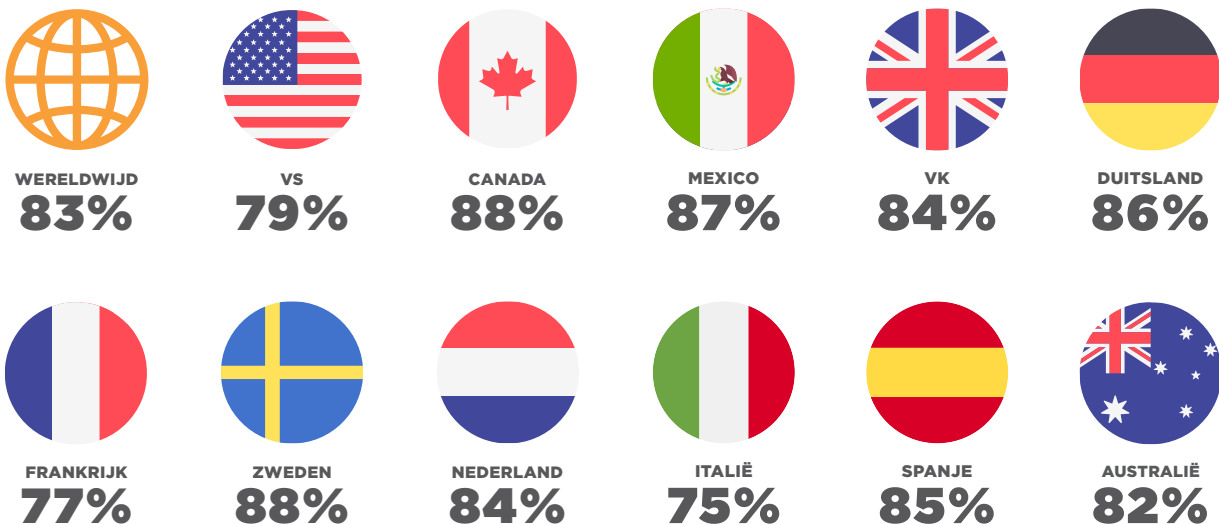
IT-beleidsmakers zei dat hun organisatie met ten minste één gegevensinbreuk/gegevenslek of ransomware-aanval te maken heeft gehad sinds 2023.

Dit komt overeen met de cijfers van 2024 (85%), waaruit blijkt dat deze dreigingen er nog steeds zijn en niet effectief worden beheerd.

De veranderingen in het totale percentage per jaar dat organisaties incidenten ondervinden kunnen klein zijn, maar nu heeft bijna de helft een gegevenslek (48% vergeleken met 2022 toen het 33% was) meegemaakt en ondervond twee derde een gegevenslek van buiten of een ransomware-aanval (65%, vergelijkbaar met 2024 maar 48% in 2022 en 52% in 2023).

Het enige type incident dat dit jaar een significante verandering laat zien is het percentage IT-besluitvormers dat een gepland gegevenslek van medewerkers meldt, die is gedaald van 34% in 2024 naar 24% in 2025.

Heeft de afgelopen 12 maanden één of meer beveiligingsincidenten ondervonden:



Met minder geplande gegevenslekken van medewerkers dit jaar, lijkt het menselijke element van gegevensbeveiliging onder controle, maar de technologische hulpmiddelen zijn absoluut niet onder controle wordt teniet gedaan.

Dit jaar geeft bijna de helft van de IT-beleidsmakers (45%) verouderde IT de schuld voor het kwetsbaar maken van netwerken voor beveiligingsaanvallen, vergeleken met 36% in 2024.

Het is een probleem waar organisaties over de hele wereld mee te maken hebben, maar in sommige landen is het een ernstig probleem: Meer dan de helft van de IT-beleidsmakers in Zweden (55%), Frankrijk (54%), Australië (53%) en Canada (51%) maakt zich nu zorgen dat hun netwerk gevoelig is voor beveiligingsaanvallen vanwege verouderde IT.

De zorgen over verouderde IT nemen ieder jaar toe, aangezien ze in ieder onderzocht land zijn toegenomen. Als problemen met verouderde IT niet worden opgelost, worden organisaties vaker blootgesteld aan beveiligingsdreigingen, operationele inefficiënties en aangetaste patiëntenzorg.

“Verouderde IT maakt ons netwerk kwetsbaar voor beveiligingsaanvallen”

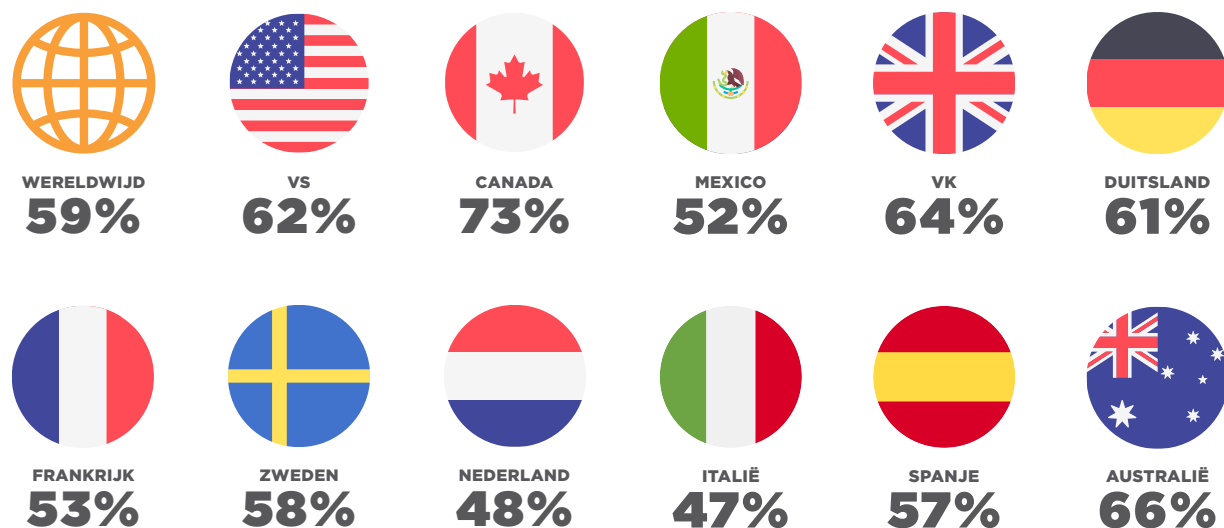
	2025	2024		2025	2024
	45%	36%		54%	27%
	44%	39%		55%	25%
	51%	43%		40%	37%
	39%	35%		37%	-
	43%	40%		41%	-
	45%	33%		53%	39%

Vier op de tien (38%) kan apparaten niet op afstand ondersteunen of gedetailleerde informatie ontvangen over apparaatproblemen, en één op de vijf (20%) zei dat ze geen nieuwe apparaten kunnen detecteren die verbinding maken met het systeem. Er wordt in 97% van de zorginstellingen verouderde IT gebruikt. Op basis van het onderzoek van dit jaar, gaat het door met problemen met integratie, onderhoud en beveiliging.

VEROUDERDE SYSTEMEN ZORGEN VOOR MEER WERK VOOR IT-TEAMS

Regelmatige technische problemen en downtime zijn ook een uitdaging bij het gebruik van verbonden apparaten en medische telezorg-apparaten, wat dit jaar van invloed is op **59%** van de organisaties, vergeleken met **52%** in 2022.

Heeft uw organisatie regelmatig technische problemen/downtime ondervonden tijdens het gebruik van medische apparaten voor IoT/telezorg?



Technische downtime in zorgomgevingen kan leiden tot onderbrekingen van de patiëntenzorg, wat van invloed is op de algemene efficiëntie van activiteiten. Organisaties worden geconfronteerd met uitdagingen met systeemupdates en onderhoud, die leiden tot inefficiënte workflows en een lagere kwaliteit van de zorg.

De uitdagingen worden wereldwijd ervaren en toch worden technische problemen en downtime aanzienlijk meer ervaren in de volgende landen: Canada (**73%**), Australië (**66%**) en het Verenigd Koninkrijk (**64%**).

Terwijl ze zich richten op strategische projecten lopen IT-teams vaak vast door tijdverslindende taken in verband met het oplossen van kleine technische problemen, zoals het repareren van printers, problemen met connectiviteit en andere herhalende ondersteunende taken. Veel van deze problemen worden veroorzaakt door verouderde IT, waarbij **39%** van de IT-beleidsmakers zei dat ze hierdoor te veel tijd besteden aan problemen oplossen. Deze inefficiëntie doet afbreuk aan het vermogen om de aandacht te richten op initiatieven met meer impact die de organisatie verbeteren. Zorginstellingen moeten nadenken over de implementatie van oplossingen die bij kunnen dragen aan de integratie van bestaande en nieuwe technologieën.

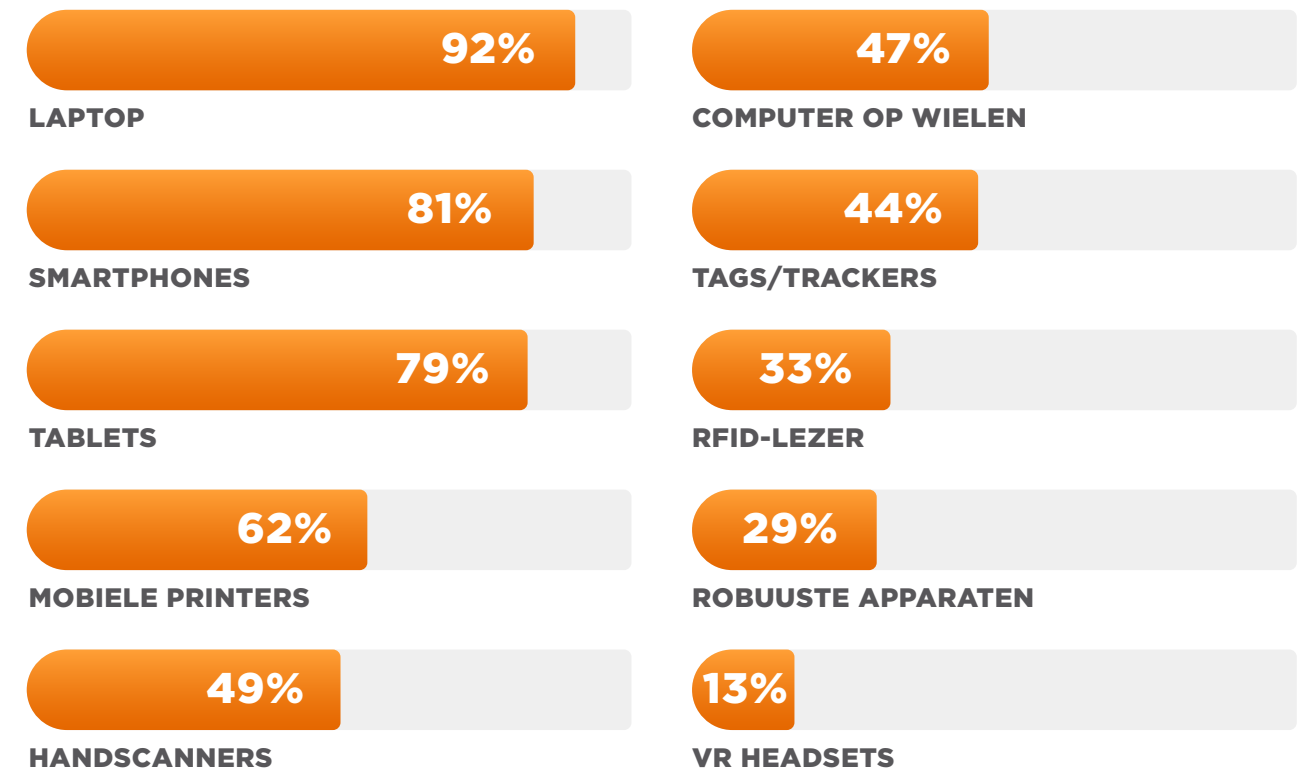


DE TE VOLGEN KOERS: ENTERPRISE MOBILITY MANAGEMENT HEEFT MOBILE DEVICE MANAGEMENT VERVANGEN

De toenemende integratie van verschillende mobiele apparaten, de toename van het gebruik van printers en de verschillende applicaties voor dagelijkse zorg vereist een robuuste oplossing voor apparaatbeheer.

Welke volgende mobiele apparaten worden er binnen uw organisatie gebruikt?

Wereldwijde bevindingen



Met zoveel verschillende apparaten worden zorginstellingen geconfronteerd met de uitdaging om de veiligheid te garanderen, op afstand problemen op te lossen en te zorgen dat alle apparaten optimaal functioneren. Voor IT-beleidsmakers is het cruciaal om deze apparaten probleemloos te kunnen verbinden. Om aan deze vereisten te voldoen, moeten gezondheidsorganisaties verder gaan dan de traditionele MDM en een globalere en meer geïntegreerde benadering hanteren.

DE TOENEMENDE BEHOEFTE AAN EMM-OPLOSSINGEN

Ongetwijfeld is er ruimte voor mobiele technologie, aangezien **86%** van de IT-beleidsmakers zegt dat ze hiermee sneller hun werk kunnen doen. Het aantal dat wordt gebruikt, duidt er echter op dat er veel mobiele apparaten te volgen, onderhouden en beheren zijn, waarbij de meerderheid MDM gebruikt voor beveiliging (**90%**). Dit bestaat onder andere uit het beheer van het beveiligingsbeleid, bescherming tegen cyberdreigingen, en het identificeren van ongeautoriseerde apparaten die op het netwerk komen, allemaal van cruciaal belang om kwetsbaarheden te minimaliseren en de kans op inbreuken te verkleinen.



Welke kenmerken van een MDM-oplossing zijn cruciaal voor uw activiteiten?

Beveiligingsmanagement	63%
Bescherming tegen cyberdreigingen/externe apparaten identificeren die op het netwerk komen	56%
Manieren om kwetsbaarheden te verminderen voor externe dreigingen/de mogelijkheden voor hackers te verkleinen	48%
Probleemoplossing op afstand	47%
App-beheer	47%
Apparaten monitoren	45%
Naleving en beleid uitvoeren	44%
Toegang tot apparaatfuncties in bepaalde omgevingen beperken	38%
NET: Met betrekking tot beveiliging (beveiligingsmanagement of bescherming tegen cyberdreigingen/externe apparaten identificeren die op het netwerk komen of manieren om kwetsbaarheden voor externe dreigingen te verminderen/de mogelijkheden voor hackers te verkleinen)	90%

Veel zorginstellingen vertrouwen op MDM- oplossingen voor standaard beveiliging en apparaatbeheer, maar dat is nu precies de baseline. In de hedendaagse snelle zorgomgeving waarin veel op het spel staat, volstaat standaard MDM niet langer.

Met de toenemende complexiteit van de patiëntenzorg en het toenemende aantal verbonden apparaten, moeten organisaties overstappen van reactieve naar proactieve strategieën die problemen signaleren en voorkomen voordat ze de zorg beïnvloeden. Dit betekent verder gaan dan de basis om realtime monitoring te implementeren en beveiligingsinbreuken en operationele verstoringen een stap voor te blijven.

Twee derde (**65%**) van de IT-besluitvormers meldt dat hun organisatie de afgelopen 12 maanden een gegevenslek van een externe bron of een DDoS ransomware-aanval heeft ervaren. Dit benadrukt de noodzaak om verder te gaan dan de basis en meer geavanceerde en uitgebreide beveiligingsmaatregelen te nemen.



Gegevensbeveiliging staat nog steeds boven aan de lijst met IT-zorgen en **30%** van IT-beleidsmakers vermeldt het. Het percentage dat het vermeldt als hun grootste probleem blijft aanzienlijk stijgen ten opzichte van **16%** in 2023 en **23%** in 2024. Tel dit op bij de **13%** die zei dat het beheer van de veiligheid van gedeelde apparaten dit jaar hun grootste aandachtspunt was, en dan zien we dat bijna de helft (**43%**) een veiligheidsgerelateerd probleem noemt als het grootste probleem waarmee IT binnen hun organisatie wordt geconfronteerd.

Wat is momenteel het belangrijkste aandachtspunt voor IT binnen uw organisatie?

Probleem met de gegevensbeveiliging of de beveiliging van gedeelde apparaten beheeren					
	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%

Gegevensbeveiliging heeft dit jaar prioriteit voor alle landen, waarbij sommige landen een bijzonder sterke stijging ondervinden:

-  in **Frankrijk**, werd een beveiligingsgerelateerd probleem gezien als het grootste probleem door **25%** in 2024 en **51%** in 2025,
-  in **Canada** steeg het van **39%** afgelopen jaar, en nu is het **53%**,
-  in **Australië** is het gestegen van **39%** naar **53%**
-  en in **Duitsland** van **24%** naar **41%**.

De aard van mobiele apparaten vereist dat ze door meerdere gebruikers worden gebruikt. Dan is het geen verrassing dat het beheer van de beveiliging van gedeelde apparaten een belangrijk aandachtspunt is voor IT. Voeg hier de uitdaging van verouderde technologie aan toe, waardoor het bijna onmogelijk wordt om deze apparaten op afstand te beheeren, en mobiele apparaten daardoor als een boemerang werken.

‘Standaard’ MDM-functies volstaan niet langer voor de moderne technologische wereld en alle complexe apparaten en systemen die we gebruiken. De oorspronkelijke mogelijkheden van MDM hebben hun limiet bereikt. Momenteel is de behoefte aan geavanceerde technologie-oplossingen belangrijker dan ooit. Moderne EMM-tools bieden zorginstellingen meer inzicht in hun hele ecosysteem, zodat ze activiteiten beter kunnen monitoren, de gegevensbeveiliging kunnen verbeteren en sneller aanstaande dreigingen kunnen reageren.

PRIORITEIT GEVEN AAN BEVEILIGING VAN MOBIELE APPARATEN: ALLES INDEKKEN

Organisaties geven prioriteit aan maatregelen om de beveiliging van mobiele apparaten te waarborgen. Sommige organisaties richten zich op een benadering waarbij de mens centraal staat, waarbij **45%** medewerkers traint in beveiligingsdreigingen, en wetgeving voor gegevensbescherming, terwijl een vergelijkbaar aantal de toegang tot gevoelige gegevens beperkt op basis van rollen en verantwoordelijkheden. Toch heeft slechts een derde (**33%**) een incidentbestrijdingsplan voor als er iets misgaat.

Regelmatig bijwerken is de meest geïmplementeerde beveiligingsmaatregel, waarbij **51%** dit ook doet. Een aanzienlijk hoger percentage hiervan die de afgelopen 12 maanden geen incident met gegevensbeveiliging heeft meegemaakt (**60%**), hanteert deze benadering (vergeleken met slechts **49%** van zij die wel een incident hebben meegemaakt). Het gebruik van Multi-factor authenticatie heeft prioriteit bij **44%** met encryptie door **42%**.

Het is duidelijk dat alle organisaties iets doen om mobiele apparaten te beveiligen, maar slechts een enkeling doet alles wat er mogelijk is.

DE BEHOEFTE AAN BETERE STRATEGIEËN VOOR MOBILE DEVICE MANAGEMENT

Beveiliging is niet het enige waarin verouderde MDM-oplossingen tekort schieten. Veel zorginstellingen hebben te maken met inconsistenties bij het toepassen van deze oplossingen op verschillende apparaten, wat monitoren en ondersteunen van apparaten lastig maakt. Deze inconsistentie leidt vaak tot onnodige vervanging van apparaten en inefficiënte activiteiten in het algemeen.

Bijna de helft (**47%**) van de IT-beleidsmakers zegt dat een MDM-oplossing cruciaal is voor hun organisatie voor probleemoplossing op afstand en **45%** zegt dat het cruciaal is om apparaten te traceren, maar **38%** van de organisaties kan geen nieuwe apparaten en printers implementeren en beheren vanwege verouderde systemen en **38%** kan vanwege dezelfde reden geen apparaten op afstand ondersteunen of gedetailleerde informatie ontvangen over apparaatproblemen.

Het onderzoek benadrukt de noodzaak dat zorginstellingen robuuste en gecentraliseerde EMM-oplossingen implementeren die apparaatbeveiliging en -naleving garanderen. Deze oplossingen moeten ook probleemoplossing op afstand ondersteunen, de configuratie stroomlijnen en bruikbare inzichten opleveren.

Geavanceerde tools die analyses en operationele informatie tussen alle apparaten bieden, zorgen dat IT-teams de prestatieproblemen van het apparaat proactief kunnen identificeren. Het kan ook gebruikstrends bijhouden en organisaties inzichten bieden om weloverwogen beslissingen te nemen. Deze benadering vermindert vertraging, minimaliseert inefficiëntie en verhoogt de algehele kwaliteit van de zorg.



VERWIJDERBARE MEDISCHE TECHNOLOGIE

Problemen zijn niet zomaar opgelost wanneer een mobiel apparaat niet meer wordt gebruikt, maar worden vaak groter. Sterker nog, **81%** van de IT-beleidsmakers maakt zich zorgen over de beveiliging van patiëntengegevens tijdens de verwijdering van apparaten.

Zorginstellingen verwerken enorme hoeveelheden gevoelige gegevens en zonder gestandaardiseerde verwijderingsprocessen, vormen afgedankte apparaten een ernstig risico op gegevenslekken en niet-naleving van de regelgeving. Hoewel de meeste organisaties stappen ondernemen om gegevens te beschermen bij het verwijderen van apparaten, zijn er nog steeds veel inconsistenties, en dit jaar maken acht van de tien IT-beleidsmakers zich nog steeds zorgen.

Regelmatige updates lossen het probleem op. **31%** van de organisaties vervangt apparaten op verzoek van de gebruiker. **40%** doet dat wanneer er nieuwere modellen beschikbaar zijn. **41%** vervangt ze op basis van contractuele voorwaarden en **31%** als de garantie is verlopen. Dit zorgt voor ernstige problemen met de beveiliging en duurzaamheid.

Om de risico's te beperken, moeten organisaties gestandaardiseerde protocollen implementeren, waaronder ook externe gegevens wissen en een robuust beheer van de levenscyclus, om een goede tractering en verwijdering te waarborgen. Medewerkers moeten ook regelmatig worden getraind in veilige manieren van afdanken. Door prioriteit te geven aan veilige en duurzame processen kunnen zorginstellingen patiëntengegevens beter beschermen en voldoen aan de nalevingsnormen.

Wat is het beleid van uw organisatie voor het upgraden/ vernieuwen/vervangen van apparaten zoals hierboven vermeld, zoals smartphones, tablets, robuuste apparaten etc.?

	We doen dat op enig moment vanwege hun contractduur, of ze nu nog werken of niet	We doen dat wanneer er een nieuwer/geavanceerder model beschikbaar komt	We doen dit als gebruiker er om vragen	We doen dit als de garantie bijna is verlopen	We doen dit alleen voor apparaten die het niet meer doen
	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%

De VS, Canada en Australië hebben het hoogste percentage wat betreft het vervangen van apparaten als er een nieuwe versie beschikbaar komt. Hoewel het belangrijk is om op te vermelden dat dit een algemene wereldwijde trend is. Het is van cruciaal belang om een evenwicht te vinden tussen duurzaamheid en prestaties van apparaten. Als apparaten alleen worden afgedankt als ze niet meer werken, moeten IT-teams nog meer tijd besteden aan kleine problemen oplossen.

GEZONDHEIDSBEHEER VAN ACCU'S – VOORKOMEN IS BETER DAN GENEZEN

Inefficiënte monitoring op de gezondheid van de accu kan ook een reden zijn voor onverwachte apparaatstoringen in de zorgsector. Hogere kosten door voortijdige vervanging van apparaten, wat leidt tot financiële beperkingen en milieuproblemen met betrekking tot het afdanken van elektronisch afval, komen vaak voor. **97%** van de organisaties monitort de accubatterij actief, en toch zegt slechts een derde (**31%**) dat ze alleen controleren wanneer er problemen optreden.

41% vervangt accu's op basis van een vast schema, ongeacht de gezondheid van de batterij. Geruststellend is dat de helft regelmatig handmatige controles uitvoert, **44%** de gezondheid van accu's automatisch monitort en **41%** een voorspelbaar onderhoudssysteem heeft.

Uiteindelijk suggereren de bevindingen dat, ondanks dat mobiele apparaten onmiskenbare voordelen bieden, het beheer ervan moet worden geoptimaliseerd: EMM-oplossingen implementeren om best practices in te voeren voor de tractering van apparaten, gezondheid van accu's monitoren en strategieën voor duurzame vervanging. Dergelijke stappen stroomlijnen niet alleen de dagelijkse activiteiten, maar maken de weg ook vrij voor meer strategische IT-initiatieven in de zorgomgeving.





CONCLUSIE

De zorgsector maakt een snelle digitale transformatie door, maar de complete realisatie hiervan blijft complex. Ondanks het vele gebruik van apparaten voor IoT en telezorg, leveren verouderde systemen problemen op zoals onvolledige gegevensconsolidatie en regelmatige technische storingen, waardoor IT-teams niet de vruchten kunnen plukken van inspanningen op het gebied van digitale transformatie.

Tegelijkertijd zijn beveiligingsproblemen de voornaamste zorg voor **43%** van de IT-beleidsmakers, gevoed door dreigingen op het gebied van het beheer van gedeelde apparaten en toegenomen gegevensinbreuken. Terwijl geplande gegevenslekken door medewerkers iets zijn afgenomen, blijven onbedoelde lekken en geavanceerde externe aanvallen kwetsbaarheden blootleggen. Bijna de helft van de IT-leidinggevenden vinden verouderde systemen de belangrijkste reden waarom netwerken kwetsbaar zijn voor aanvallen, wat de noodzaak onderstreept om fundamentele technologieën te moderniseren. Het lijkt erop dat het probleem niet zozeer gaat om de opkomende technologie zelf, maar meer om de systemen die deze ondersteunen.

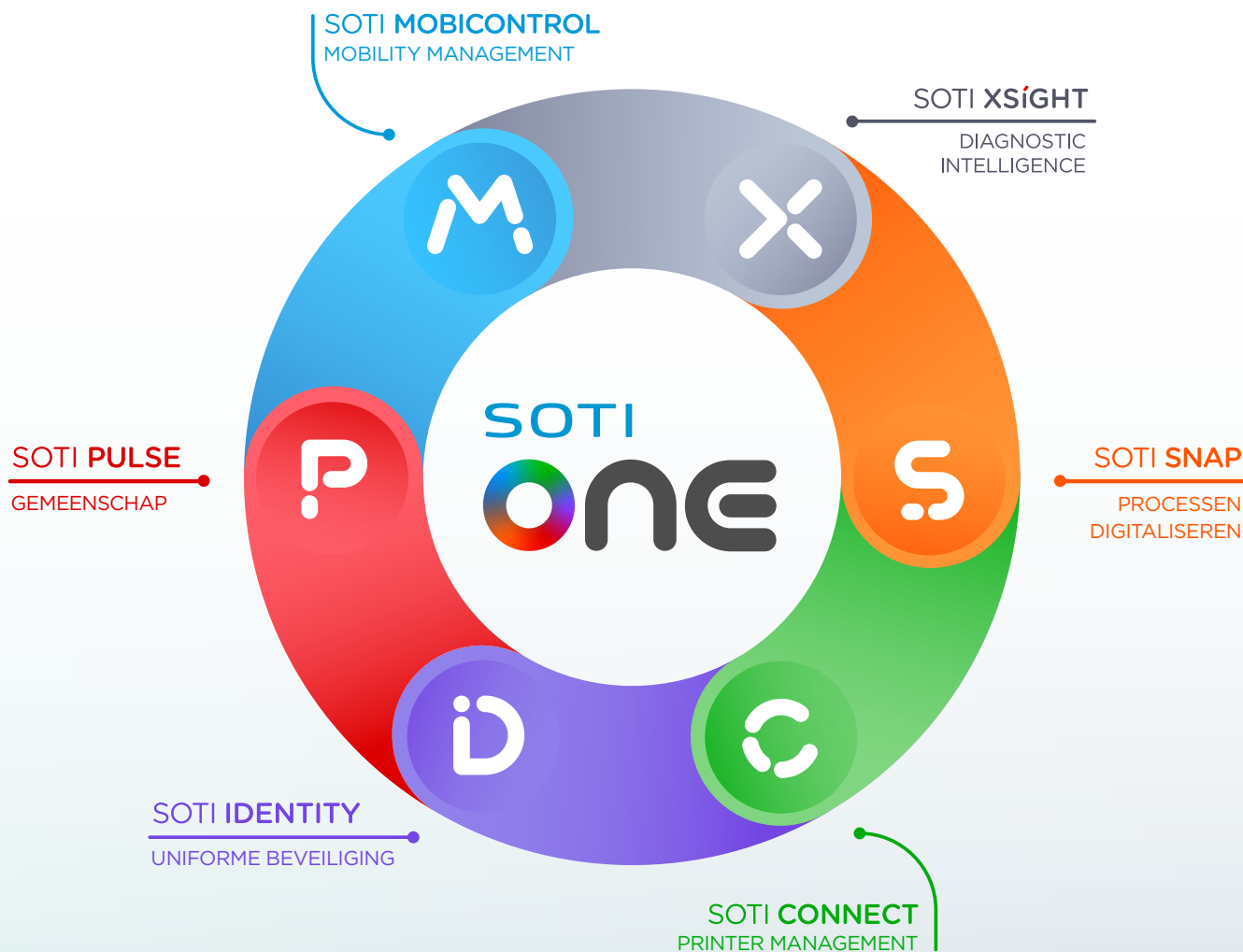
De implementatie van AI is wereldwijd toegenomen en wordt dit jaar door een derde meer organisaties gebruikt, met landen als het Verenigd Koninkrijk en Australië die hierin vooroplopen. AI wordt geïntegreerd in de analyse van medische gegevens, behandelplannen, gepersonaliseerde patiëntenzorg en meer. Een reddingsboei voor de overbelaste zorgsector, maar de noodzaak om het gebruik ervan te monitoren en beveiligen mag niet worden vergeten.

Bovendien blijkt het beheren van mobiele apparaten een aanzienlijke aanslag te zijn op de IT-middelen en de vele gebruikte apparaten in gebruik maakt effectieve monitoring en beheer op afstand moeilijker. De ontoereikendheid van bestaande MDM-oplossingen en inconsistent vervangingsbeleid zorgen voor meer druk, wat beveiligings- en duurzaamheidsproblemen vergroot.

Uiteindelijk is het voor een echte digitale transformatie in de zorg noodzakelijk dat organisaties een stap terug doen en het grotere geheel in ogenschouw nemen. Er is een strategie nodig die de voortdurende wijdverbreide implementatie van innovatieve technologieën combineert met gerichte investeringen in de modernisering en integratie van IT-infrastructuren en een op maat gemaakte EMM-oplossing. Met deze evenwichtige benadering kunnen organisaties gegevens beveiligen, het gebruik van mobiele apparaten stroomlijnen en uiteindelijk patiëntenzorg verbeteren.

OVER SOTI

SOTI is een bewezen innovator en marktleider op het gebied van het beheren en vereenvoudigen van mobiele oplossingen, waardoor ze slimmer, sneller en betrouwbaarder worden. Met SOTI's [innovatieve portfolio van oplossingen en diensten](#) kunnen organisaties erop vertrouwen dat SOTI hun mobiele activiteiten verbetert en stroomlijnt, de ROI maximaliseert en de downtime van apparaten vermindert. Wereldwijd, met meer dan 17.000 klanten, heeft SOTI zichzelf bewezen als de go-to mobile platform provider voor het beheren, beveiligen en ondersteunen van mobiele apparaten van bedrijven. Met SOTI's ondersteuning kunnen bedrijven hun mobiliteit naar eindeloze mogelijkheden brengen.



MEER INFORMATIE:

Voor meer informatie over hoe SOTI uw bedrijf op succes kan voorbereiden, **klikt u hier**.

Voor meer informatie over het SOTI ONE Platform, **klikt u hier**.

Voor meer informatie over hoe SOTI u met uw mobiele investeringen kan helpen, neemt u vandaag nog contact met ons op via **sales@soti.net**.

SOTI is een bewezen vernieuwer en leider binnen de sector voor het vereenvoudigen van mobiliteitsoplossingen door ze slimmer, sneller en betrouwbaarder te maken. SOTI helpt bedrijven over de hele wereld om de eindeloze mogelijkheden van mobiliteit te benutten.

nl.soti.net

© 2025, SOTI Inc. Alle rechten voorbehouden. Alle product- en bedrijfsnamen zijn handelsmerken™ of geregistreerde handelsmerken van hun respectieve eigenaren. Het gebruik van deze handelsmerken duidt op geen enkele verbondenheid aan SOTI of goedkeuring door de houder van het handelsmerk. Aanbiedingen zijn zonder voorafgaande kennisgeving onder voorbehoud van wijzigingen of annulering. SOTI behoudt zich altijd het recht voor om producten, services of prijzen te wijzigen. Informatie wordt zonder enige garantie en "AS IS" aangeboden. Producten en services zijn onderhevig aan de geldende algemene voorwaarden.