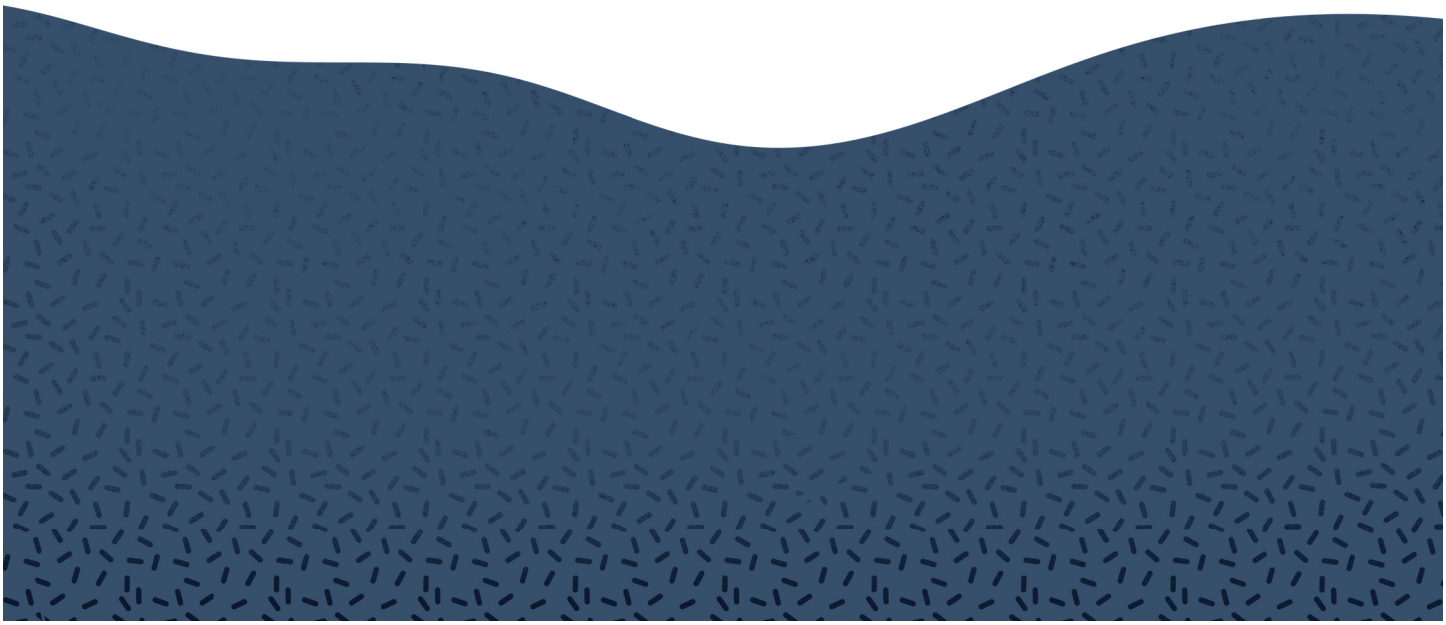
État des lieux de l'ITSM en 2026

Sécurité, IA et complexité croissante : ce que révèlent 1 100 leaders IT et sécurité

by

EASYVISTA®



Introduction

Quand l'IT fonctionne, elle s'intègre naturellement au quotidien, passant presque inaperçue. Mais dès qu'elle se dérègle, c'est toute l'organisation qui ralentit.

Pour comprendre comment les organisations naviguent entre exigences de sécurité, montée en puissance de l'IA, complexité croissante des environnements et ce qu'il faut pour garantir leur continuité, nous avons mené une étude auprès de 1 100 responsables IT et sécurité opérant dans des organisations de plus de 1 000 employés, réparties dans 13 pays.

Cet état des lieux offre une lecture claire et pragmatique de l'ITSM en 2026 : ce que les équipes priorisent, les tensions qu'elles affrontent au quotidien, et les approches qui permettent réellement de gagner en efficacité.

Ce qui ressort est sans ambiguïté : l'IT évolue dans un équilibre permanent entre accélération et automatisation de la prestation de services, entre sécurité renforcée et pression budgétaire.

Les équipes doivent avancer vite, tout en maîtrisant des environnements toujours plus complexes et la pénurie de talents.

L'étude révèle plusieurs enseignements clés sur :

- **L'IA :** comment crée-t-elle de la valeur et où atteint-elle ses limites ?
- **La sécurité :** pourquoi est-elle devenue à la fois un moteur et un frein à la prestation de services ?
- **Différences régionales :** comment les priorités en matière d'ITSM diffèrent-elles en Europe, dans les Amériques et en Asie-Pacifique ?
- **Anticipation :** les axes stratégiques que les responsables IT doivent privilégier pour aborder 2026 avec clarté et confiance

Index

Adoption de l'IA en ITSM : entre maturité et réalisme opérationnel.....4

Pourquoi la sécurité s'impose comme priorité et comme défi majeur 7

Principaux défis de l'ITSM : une lecture régionale.....9

ITSM en 2026 : tendances clés et axes de préparation.....11

I. Adoption de l'IA en ITSM : entre maturité et réalisme opérationnel

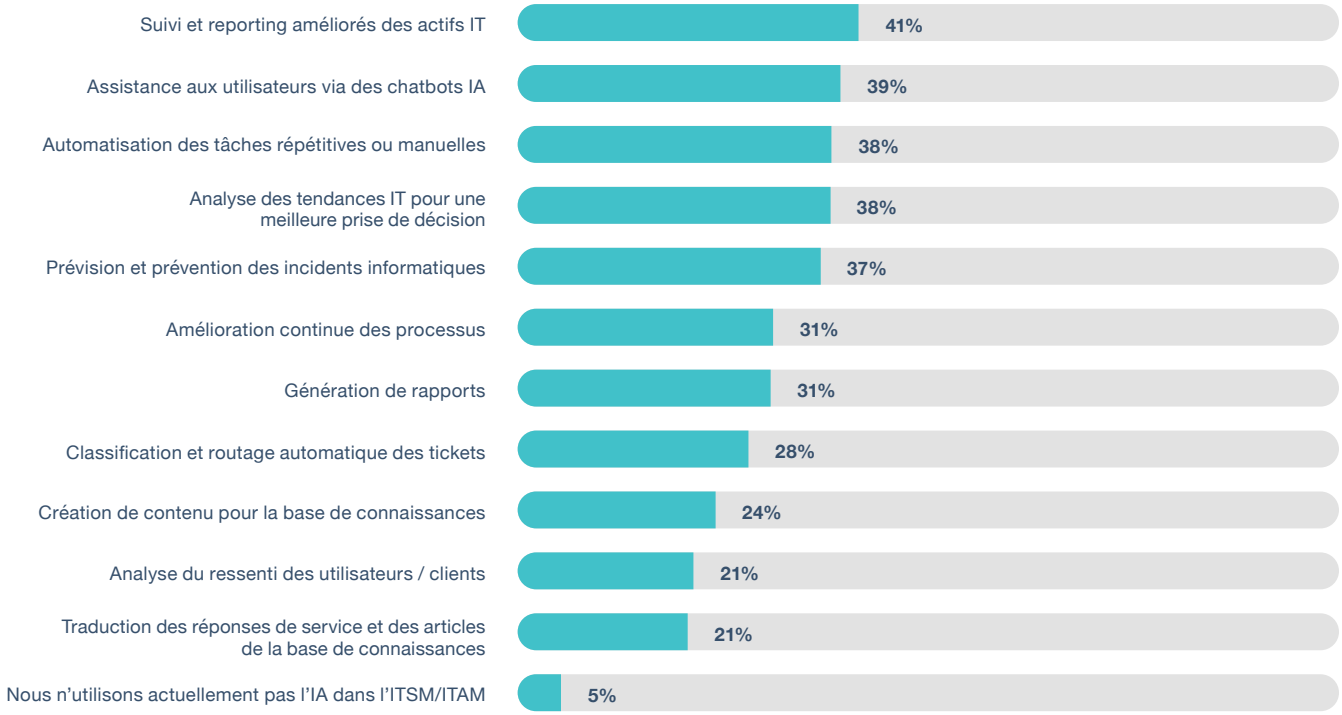
En 2026, l'IA et l'automatisation ne sont plus des expérimentations isolées en ITSM, elles sont devenues des leviers structurants de la performance IT. Plus d'un tiers des organisations (37%) placent désormais l'automatisation des workflows IT parmi leurs priorités majeures, et seules 5% déclarent ne pas utiliser l'IA dans leurs opérations ITSM.

Là où l'IA crée déjà de la valeur

Dans le domaine de l'ITSM, l'automatisation activée par l'IA est principalement utilisée pour :

1. Le suivi et reporting des actifs IT **(41%)**
2. Le support utilisateur via chatbots et assistants virtuels **(39%)**
3. L'automatisation des tâches répétitives **(38%)**
4. L'analyse des tendances IT pour la prise de décision **(38%)**

De quelles manières votre organisation utilise-t-elle l'intelligence artificielle (IA) pour améliorer ses processus ITSM ?



Les résultats de l'étude indiquent que l'IA répond, dans l'ensemble, aux attentes des organisations, et les dépasse même dans plusieurs domaines. Plus de la moitié des participants estiment qu'elle va au-delà de leurs attentes pour la traduction des réponses et des articles de connaissance (55%) ainsi que pour l'automatisation des tâches répétitives (53%). Des niveaux de satisfaction comparables sont observés pour la gestion des actifs IT, la prévention prédictive des incidents et l'analyse de tendances. Le fait que tant de répondants jugent l'IA simplement "conforme aux attentes" révèle une dynamique claire : l'IA renforce la stabilité et la fiabilité des opérations, plutôt qu'elle ne les révolutionne, du moins pour l'instant.

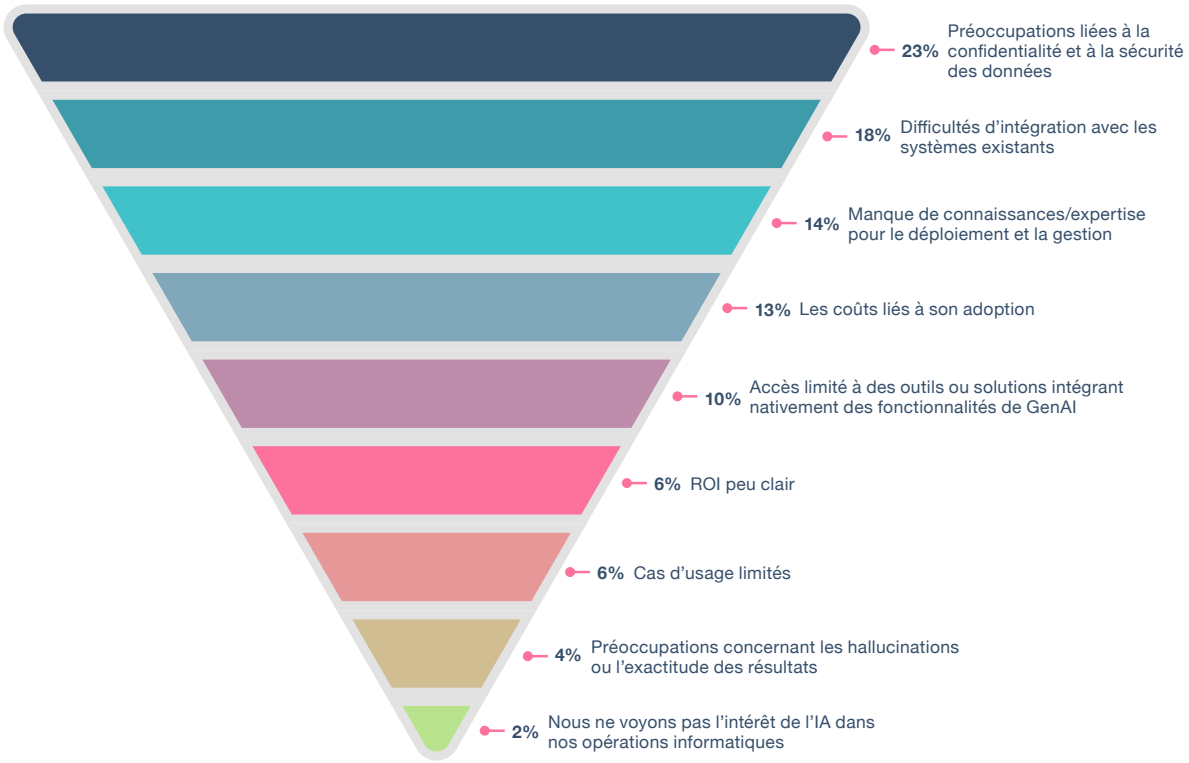
Les véritables freins à l'adoption de l'IA

Contrairement au discours dominant du marché, la précision de l'IA ou le risque d'hallucinations préoccupent très peu les responsables IT (4%). Les véritables obstacles sont d'abord organisationnels et opérationnels :

1. Préoccupations liées à la confidentialité et à la sécurité des données **(23%)**
2. Difficultés d'intégration avec les systèmes existants **(18%)**
3. Manque de compétences internes pour déployer et administrer l'IA **(14%)**
4. Coûts d'utilisation **(13%)**

Ces résultats indiquent que l'adoption de l'IA en ITSM sera déterminée non par la technologie, mais par la maturité organisationnelle : gouvernance des données, intégration aux systèmes existants et fiabilité opérationnelle.

Quel est aujourd'hui le principal obstacle au déploiement de l'IA dans vos opérations informatiques ?



IA et cybersécurité : une trajectoire de maturité parallèle

L'adoption de l'IA est tout aussi avancée dans le domaine de la cybersécurité. Près de quatre organisations sur cinq (79%) déclarent utiliser l'IA dans leurs opérations de sécurité, la plupart d'entre elles s'appuyant sur des solutions commerciales.

- **47%** via des fonctionnalités intégrées aux solutions commerciales (EDR, SIEM, SOAR)
- **42%** via des services ou API externes

Dans le domaine de la réponse aux incidents, l'IA intervient désormais tout au long du cycle de vie, et non plus sur une tâche isolée. Les usages les plus courants incluent :

- La détection et corrélation des menaces **(61%)**
- La rédaction des rapports et analyses post-incident **(49%)**
- Le soutien aux obligations de reporting réglementaire **(42%)**
- La remédiation et résolution des incidents **(41%)**
- L'enrichissement des données d'incident **(38%)**
- Le triage automatisé **(36%)**

Des usages plus avancés sont également déjà bien implantés, comme la cartographie des attaques selon des cadres tels que MITRE ATT&CK (36%) ou l'assistance de type Copilot pour les analystes SOC (35%). Il est important de noter que seulement 1% des répondants déclarent ne pas utiliser l'IA du tout dans la réponse aux incidents.

L'impact global de l'IA sur la cybersécurité est largement positif. 85% constatent une amélioration de la rapidité et de l'efficacité. Mais les responsables restent lucides face aux risques émergents : 74% estiment que l'IA renforcera significativement les capacités des attaquants dans les trois prochaines années. Leur confiance dans la capacité de l'IA à contrer ces menaces est tout aussi élevée, mais pas unanime (74%).

II. Pourquoi la sécurité s'impose comme priorité et comme défi majeur

La sécurité occupe désormais une place centrale dans la prestation des services IT. Près de la moitié des organisations (46%) la placent en tête de leurs priorités pour les douze prochains mois. Paradoxalement, les problématiques de sécurité et de conformité constituent aussi le principal obstacle à une prestation de services efficace (39%). Cette situation crée une tension évidente : la sécurité est indispensable, mais elle absorbe une part croissante du temps, du budget et de l'attention des équipes IT.

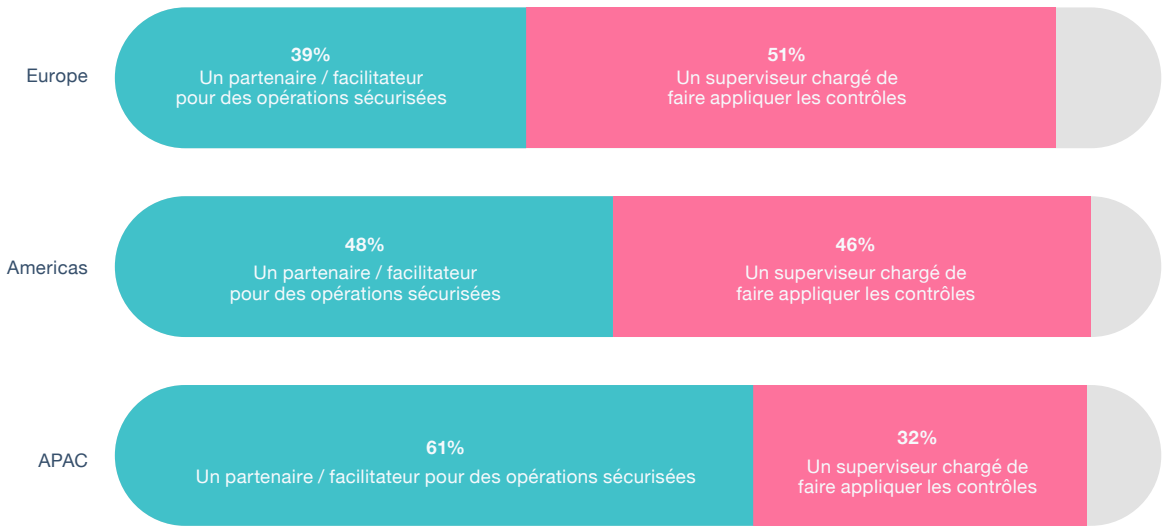
Sécurité et IT : une collaboration réelle, mais encore imparfaite

La majorité des organisations font état d'une collaboration significative entre les équipes informatiques et de sécurité :

- **62%** utilisent des tableaux de bord et outils de supervision partagés
- **55%** disposent de workflows interconnectés entre leurs outils ITSM et SecOps
- **60%** effectuent des revues conjointes après chaque incident de sécurité

Ces pratiques confirment une dynamique positive vers davantage d'alignement. Toutefois, les représentations restent divergentes. Près de la moitié des équipes IT (46 %) continuent de considérer la sécurité avant tout comme un acteur de contrôle plutôt que comme un partenaire opérationnel. Autrement dit, même si les mécanismes de collaboration existent, l'intégration pleine et entière de la sécurité dans les opérations de service reste encore inachevée.

Comment votre service informatique perçoit-il le rôle de l'équipe sécurité au sein de l'organisation ? Perspectives régionales :



La multiplication des outils fragilise l'efficacité des dispositifs de sécurité.

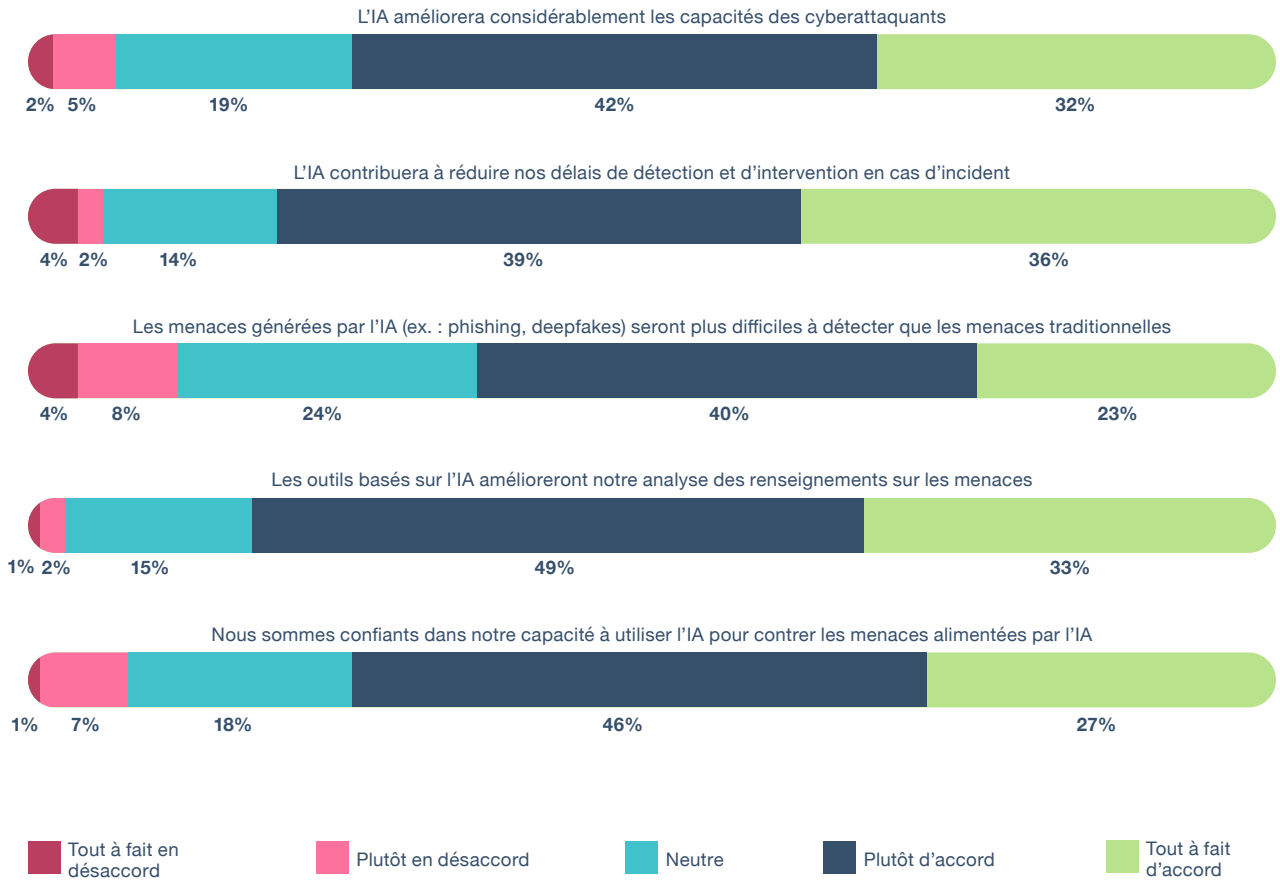
Les responsables sécurité doivent composer avec une complexité croissante :

- **45%** utilisent trop d'outils de sécurité distincts
- **63%** constatent une surcharge opérationnelle liée à cette multiplicité
- **47%** observent un ralentissement des réponses aux incidents

Le diagnostic étant désormais partagé, les organisations s'orientent clairement vers davantage de simplicité. Aujourd'hui, 75% d'entre elles déclarent activement réduire le nombre d'outils utilisés pour limiter la complexité, et 80% jugent que leur environnement est désormais suffisamment intégré.

Pour les responsables IT, la conclusion est nette : la maturité en matière de sécurité ne se construit plus en ajoutant des solutions, mais en resserrant l'architecture. Les progrès viennent de la consolidation. Il s'agit d'orchestrer un ensemble plus limité de plateformes, mieux connectées, et de considérer la sécurité comme un vecteur de résilience opérationnelle, plutôt qu'un ensemble de contraintes supplémentaires.

Selon vous, quel sera l'impact de l'IA sur la cybersécurité au cours des deux prochaines années ?



III. Principaux défis de l'ITSM : une lecture régionale

À l'échelle mondiale, les organisations IT font face à un socle de défis largement communs, même si leur intensité varie selon les régions.

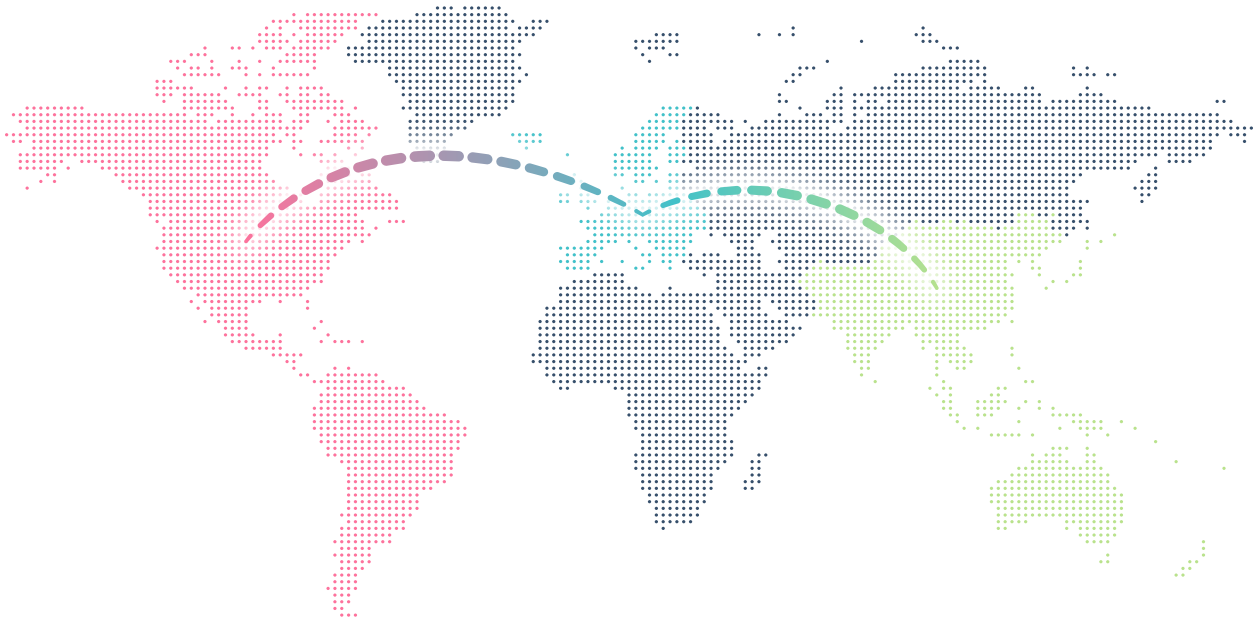
Les entreprises identifient comme obstacles majeurs à une prestation de services IT efficace :

- La garantie de la sécurité et de la conformité **(39%)**
- Les contraintes budgétaires **(38%)**
- La pénurie de compétences IT **(36%)**
- Le manque d'intégration entre les outils **(35%)**
- La lenteur de traitement des demandes et incidents IT **(32%)**

Ces constats dessinent une réalité opérationnelle commune :
les responsables ITSM doivent fournir des services plus rapides et plus fiables, tout en faisant face à une pression croissante, qu'elle soit sécuritaire, budgétaire ou liée aux ressources.

Dans ce contexte, les différences régionales ne traduisent pas des problématiques totalement distinctes, mais plutôt des points de tension spécifiques au sein d'un même ensemble de défis mondiaux.

Amériques, Asie-Pacifique et Europe : comparaison régionale des principaux défis et priorités des entreprises en 2026.



Quels sont les trois principaux obstacles rencontrés par votre organisation pour assurer efficacement la prestation des services informatiques ?

Americas		Europe		APAC	
Sécurité et conformité difficiles à garantir dans les opérations de support	44%	Contraintes budgétaires	38%	Contraintes budgétaires	45%
Manque de personnel informatique qualifié	39%	Manque de personnel informatique qualifié	36%	Sécurité et conformité difficiles à garantir dans les opérations de support	45%
Manque d'intégration entre les outils informatiques	36%	Temps de réponse trop longs aux problèmes informatiques	35%	Manque d'intégration entre les outils informatiques	43%

Quelles sont vos trois principales priorités pour améliorer les opérations informatiques au cours des 12 prochains mois ?

Americas		Europe		APAC	
Renforcer la sécurité informatique	52%	Renforcer la sécurité informatique	43%	Renforcer la sécurité informatique	46%
Automatiser les flux de travail informatiques	35%	Automatiser les flux de travail informatiques	40%	Introduire des outils ou services d'IA pour améliorer l'efficacité	40%
Introduire des outils ou services d'IA pour améliorer l'efficacité	29%	Introduire des outils ou services d'IA pour améliorer l'efficacité	34%	Automatiser les flux de travail informatiques	30%

Europe : pression sur la capacité et la réactivité

En Europe, les contraintes budgétaires et la pénurie de compétences restent structurantes. Mais ce sont surtout les enjeux opérationnels, délais de réponse qui s'allongent, volumes de tickets en hausse, qui pèsent le plus sur les équipes ITSM.

Les environnements ITSM européens sont globalement bien structurés, mais ils se retrouvent de plus en plus sollicités à mesure que la demande dépasse la capacité disponible. Cette pression se traduit directement dans les opérations : un support IT trop lent affecte rapidement la productivité, la qualité de service et, in fine, l'expérience des utilisateurs comme des clients.

Pour les DSI européens, 2026 sera l'année où il faudra réduire l'écart entre ce que l'organisation attend et ce que les équipes peuvent réellement délivrer. L'enjeu ne sera pas d'ajouter de nouveaux outils, mais de renforcer l'efficacité opérationnelle, d'accélérer les temps de réponse et de déployer des modèles de support capables d'absorber la montée en charge.

Amériques : maîtriser le risque à grande échelle

Dans les Amériques, les priorités ITSM sont fortement influencées par les exigences de sécurité et la complexité opérationnelle. Les enjeux liés à la sécurité y apparaissent nettement plus élevés que dans les autres régions, reflet d'une exposition accrue aux menaces et de la taille des environnements à gérer.

À cela s'ajoutent des lacunes d'intégration et une pénurie de compétences qui amplifient les risques et contribuent à la hausse des volumes de tickets comme aux délais de réponse.

Pour les DSI de la région, l'enjeu en 2026 ne sera pas d'adopter davantage d'outils, mais de réduire la complexité : consolider les plateformes, fluidifier les workflows et intégrer la sécurité au cœur même de la prestation des services.

Région APAC : Coûts, intégration et cohérence architecturale

Dans la région APAC, les priorités ITSM reflètent la pression d'une croissance rapide dans un contexte financier et opérationnel contraint. Les tensions budgétaires y sont plus marquées que partout ailleurs, suivies de près par les enjeux de sécurité et par un manque d'intégration entre les outils IT.

Cette combinaison révèle des environnements où l'expansion des plateformes a parfois devancé la cohérence architecturale. Pour les DSI de la région, l'année 2026 sera centrée sur une automatisation maîtrisée, une meilleure intégration et des plateformes capables d'apporter échelle, sécurité et clarté opérationnelle, plutôt que d'ajouter de nouvelles briques technologiques.

IV. ITSM en 2026 : tendances clés et axes de préparation

Les résultats de l'étude font émerger quatre tendances structurantes qui façonneront l'ITSM en 2026, réparties en deux grands domaines :

Domaine I : l'alignement stratégique entre sécurité et ITSM

La sécurité intégrée nativement dans l'ITSM, plutôt qu'ajoutée en surcouche

La sécurité et la gestion des services convergent progressivement autour de workflows, tableaux de bord et indicateurs communs.
Les organisations ont tout intérêt à privilégier des plateformes capables d'assurer une intégration native entre ITSM et SecOps, plutôt que de s'appuyer sur des coordinations manuelles toujours coûteuses et fragiles.

Priorité d'action : standardiser les playbooks, les métriques d'incident et les modes de reporting entre équipes IT et sécurité.

La consolidation des outils comme impératif stratégique

La prolifération des outils est désormais un frein mesurable à la performance. Les organisations accélèrent donc leurs efforts de rationalisation pour retrouver lisibilité et rapidité d'exécution.

La réduction de la complexité n'est plus un exercice d'optimisation budgétaire : c'est un enjeu stratégique pour améliorer l'efficacité opérationnelle et la qualité de service.

Priorité d'action : évaluer les outils de sécurité non pas à l'aune du nombre de fonctionnalités, mais selon la profondeur d'intégration et la couverture du cycle de vie qu'ils offrent.

Domaine II : L'intelligence artificielle au service de l'ITSM

Une IA intégrée, pragmatique et guidée par les cas d'usage

L'adoption de l'IA continuera à progresser, en particulier dans la gestion des actifs, l'analyse des données et la réponse aux incidents. La valeur ne viendra pas de déploiements génériques, mais de cas d'usage bien cadrés, d'une base de données solide et d'une intégration fluide dans les workflows existants. Autrement dit, l'IA sera réellement utile lorsqu'elle soutient les décisions et les opérations, et non lorsqu'elle est déployée pour elle-même.

Priorité d'action : concentrer les investissements IA sur des cas d'usage précis, à forte valeur opérationnelle, capables d'améliorer la prise de décision et les résultats métiers.

IA et automatisation : viser la résilience, pas seulement sur l'efficacité

L'automatisation évolue : il ne s'agit plus seulement de réduire les coûts, mais de prévenir les incidents, d'améliorer les temps de rétablissement et de renforcer la continuité de service.

Priorité d'action : prioriser les automatisations qui améliorent le MTTR, la prévention des incidents et la continuité de service, avant de chercher des gains d'efficacité secondaires.

À propos de l'étude

Ce rapport repose sur une enquête en ligne conduite par EasyVista et OTRS auprès de 1 100 professionnels de l'ITSM et de la sécurité IT, dont près de 300 responsables sécurité. Les répondants exercent au sein d'entreprises de plus de 1 000 salariés, implantées dans 13 pays couvrant six zones majeures : Europe, APAC, États-Unis, Royaume-Uni, Mexique et Brésil. La collecte des données s'est déroulée entre le 11 septembre et le 12 octobre 2025.

Boilerplate

EasyVista est une plateforme ITSM leader qui aide les organisations à simplifier leurs opérations IT, à améliorer la gestion de leurs services et à optimiser leurs processus grâce à l'intelligence artificielle. S'appuyant sur une plateforme unifiée combinant gestion des services, automatisation, monitoring et assistance à distance, EasyVista permet aux équipes IT de gagner en efficacité et d'obtenir des résultats concrets et mesurables. Grâce à une IA directement intégrée aux workflows, les organisations peuvent prioriser plus efficacement, résoudre les incidents en toute confiance et accélérer leur stratégie d'automatisation. Reconnue pour la qualité de l'expérience qu'elle offre, EasyVista a été désignée « Customers' Choice » par Gartner Peer Insights pour l'ITSM, avec une note de 4,9/5 pendant deux années consécutives. Pour en savoir plus, rendez-vous sur https://www.easyvista.com/fr/

EN SAVOIR PLUS

EASYVISTA®