

RAPPORT

MSP PERSPECTIVES 2026

Perspectives de 800 MSP sur les défis et les opportunités qui façonnent l'avenir des services de cybersécurité.

SEPTEMBRE 2026



Résumé

La cybersécurité est confrontée à une crise de leadership. Il n'y a qu'un responsable de la sécurité des systèmes d'information (RSSI) pour 10 000 organisations dans le monde¹, laissant la grande majorité sans la gouvernance et la stratégie dédiées dont elles ont besoin pour être sécurisées de manière vérifiable. Pour aggraver le problème, le nombre d'incidents ne cesse de croître, les dépenses de sécurité augmentent et la confiance des dirigeants reste faible. Les organisations investissent peut-être plus que jamais, mais beaucoup ont encore du mal à répondre à des questions fondamentales sur leurs risques, leur résilience et les résultats de leurs investissements.

Cette lacune représente une opportunité majeure pour les fournisseurs de services managés (MSP) et autres experts channel : aller au-delà de la prestation pour devenir de véritables référents cyber de confiance. Les résultats de l'étude présentée dans ce rapport montrent que les clients se tournent de plus en plus vers leurs partenaires pour obtenir des conseils couvrant l'ensemble de leur programme de cybersécurité, de l'implémentation technique à la gestion complète. Les partenaires qui apporteront de la clarté à la complexité, en aidant leurs clients à voir où ils en sont, comment ils s'améliorent et où les risques demeurent, seront les mieux placés pour combler ce vide de leadership.

Cependant, pour assurer un leadership en matière de cybersécurité à grande échelle, la simple expertise ne suffit pas. Comme illustré en page 19, les **MSP estiment qu'ils pourraient faire gagner plus de la moitié du temps** à leur équipe si les activités de sécurité et de conformité étaient gérées depuis une plateforme unique et unifiée. Cela souligne l'importance cruciale de l'efficacité opérationnelle. Pour répondre à la demande croissante des clients, les prestataires ont besoin d'un modèle qui rende leurs efforts reproductibles, évolutifs et mesurables sur l'ensemble de leur clientèle.



Scott Barlow
VP, Chief Evangelist
Sophos

¹ <https://www.sophos.com/fr-fr/resources/report/2026-ciso-report>

Introduction

Le rapport MSP Perspectives 2026 de Sophos fournit des informations sur trois domaines stratégiques de l'activité des MSP :

- L'essor du cyber leadership assuré par les MSP
- La conformité au cœur de la prestation de services des MSP
- L'opérationnalisation de la sécurité et de la conformité à grande échelle

Les résultats sont basés sur une enquête indépendante, menée auprès de 800 MSP situés aux États-Unis (200), au Royaume-Uni (100), en Allemagne (100), en France (100), à Singapour (100), en Australie (100) et au Brésil (100). Les répondants sont des décideurs MSP, cadres dirigeants ou membres du conseil d'administration.

L'enquête commandée par Sophos a été réalisée par l'institut de recherche Vanson Bourne en avril 2026.

800

MSP

7

Domaines de conformité clés

7

Pays

Aperçu des principales découvertes

1. Les MSP sont devenus de facto les RSSI de leurs clients

- **88 %** des MSP déclarent qu'au moins **20 %** de leurs clients se tournent vers eux pour agir en tant que RSSI.
- **84 %** des MSP s'attendent à ce que la demande de services de RSSI augmente au cours des 12 prochains mois.

2. Les services de conformité sont très répandus, sans pour autant avoir atteint un niveau de maturité élevé.

- **99 %** des MSP fournissent des services de conformité.
- **6 %** fournissent une gamme complète de services de conformité, ce qui laisse une marge de croissance.

3. La conformité stimule l'investissement en matière de sécurité

- **50 %** des décisions d'achat des clients sont influencées par les exigences de conformité.
- Cette influence est un facteur majeur dans **33 %** des décisions d'achat en moyenne.

4. La transition vers une conformité continue reste progressive

- **62 %** des MSP sont « très confiants » dans leur capacité à surveiller, gérer et documenter en continu la conformité de multiples clients.
- **33 %** se déclarent « totalement confiants », ce qui souligne que beaucoup pourraient bénéficier d'une amélioration de leurs pratiques.

5. La fourniture basée sur des outils est la norme

- **53 %** des MSP utilisent plusieurs outils ou plateformes pour gérer de manière centralisée la conformité à la cybersécurité ou les activités de type RSSI.
- **36 %** s'appuient sur un seul outil, ce qui implique que les MSP et leurs clients évoluent dans un environnement complexe, fragmenté et potentiellement incomplet.

6. Les rapports de sécurité deviennent automatisés

- **86 %** des MSP utilisent un processus entièrement ou semi-automatisé pour produire des rapports consolidés sur la posture de sécurité.
- **55 %** nécessitent encore une intervention manuelle pour consolider les différentes activités, ce qui suggère que la plupart des processus de reporting ne sont que partiellement automatisés.

7. Des gains d'efficacité significatifs restent inexploités

- Les MSP pourraient gagner **53 %** de temps s'ils pouvaient gérer la posture de sécurité et la conformité de leurs clients, ainsi que le reporting, depuis une plateforme unique et unifiée.
- **81 %** des MSP estiment que cela leur permettrait de réduire de plus de **30 %** le temps qu'ils consacrent actuellement à ces activités.

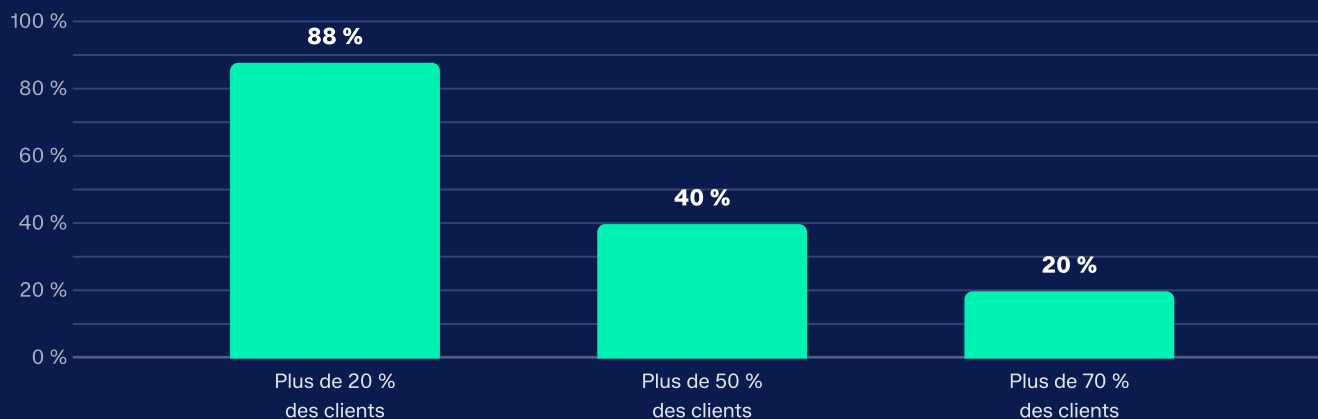
Partie 1 : L'essor du leadership en matière de cybersécurité assuré par les MSP

1. Les MSP sont devenus de facto les RSSI de leurs clients

Les organisations sont confrontées à une pression croissante due à l'évolution du paysage des menaces, aux attaques optimisées par l'IA, à l'expansion des réglementations et à la pénurie de compétences en sécurité. Beaucoup ne disposent pas non plus du leadership interne nécessaire pour relever ces défis à l'aide d'un programme de cybersécurité coordonné plutôt qu'à une gestion technologique seule. En réponse, les MSP montent dans la chaîne de valeur, évoluant de fournisseurs d'outils tactiques à partenaires de conseil stratégique.

Les données du rapport montrent que ce changement est déjà bien engagé. En moyenne, les MSP estiment que **46 % de leurs clients** comptent désormais sur eux pour ce type de leadership. Cette dépendance est très répandue : **88 % des MSP** font office de RSSI pour plus de **20 %** de leur clientèle, **40 %** pour plus de la moitié et **20 %** pour plus de **70 %**.

Dépendance des clients aux services RSSI fournis par le MSP



*approximativement, pour quelle proportion de vos clients votre organisation assure-t-elle le rôle de RSSI, le cas échéant ? (n=800)

88 %

des MSP exercent des fonctions de RSSI auprès de plus de 20 % de leurs clients.

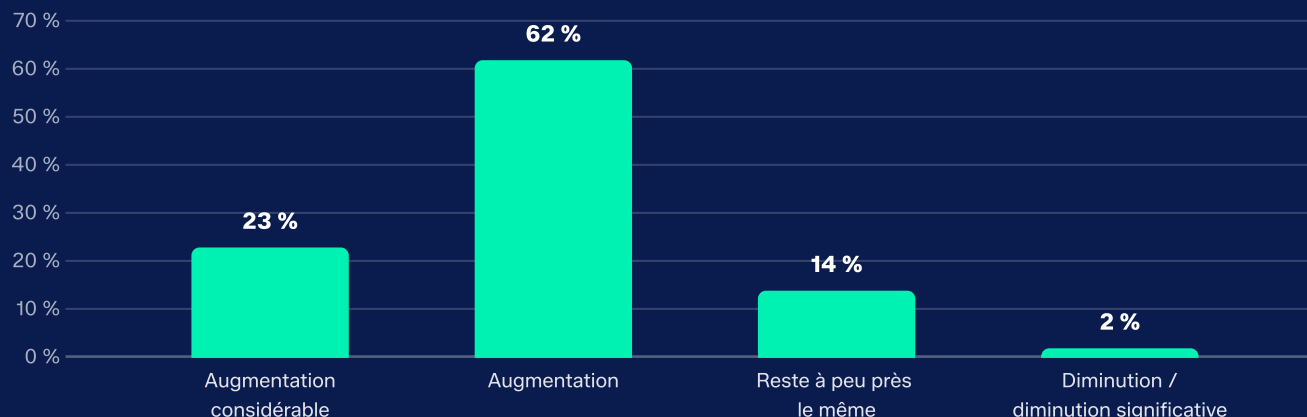
46 %

des clients des MSP, en moyenne, se tournent vers leur MSP pour agir en cette qualité.

La demande pour des services RSSI fournis par les MSP est appelée à augmenter

Cette opportunité pour les MSP ne fait que croître. **84 %** s'attendent à ce que la demande de services RSSI augmente au cours des 12 prochains mois, **23 %** d'entre-eux prévoyant même une croissance significative. Seuls **2 %** s'attendent à une diminution.

Évolution estimée de la demande de services RSSI



Comment pensez-vous que cela changera au cours des 12 prochains mois, le cas échéant ? (n=800)

Les limites traditionnelles du rôle de MSP changent rapidement, reflétant les défis auxquels sont confrontées les organisations qui ne disposent pas de l'expertise, des ressources ou des fonds nécessaires pour s'adjoindre les services d'un responsable de la sécurité dédié en interne. Les clients attendent désormais de leur MSP des conseils stratégiques en cybersécurité de niveau RSSI, ainsi qu'un accompagnement en matière de gestion des risques et de gouvernance, au-delà de la simple gestion technologique quotidienne. Les fournisseurs capables de combler ce vide et de s'imposer comme références sont bien placés pour répondre à une demande croissante.

84 %

des MSP s'attendent à ce que la demande de services de type RSSI augmente au cours des 12 prochains mois.

23 %

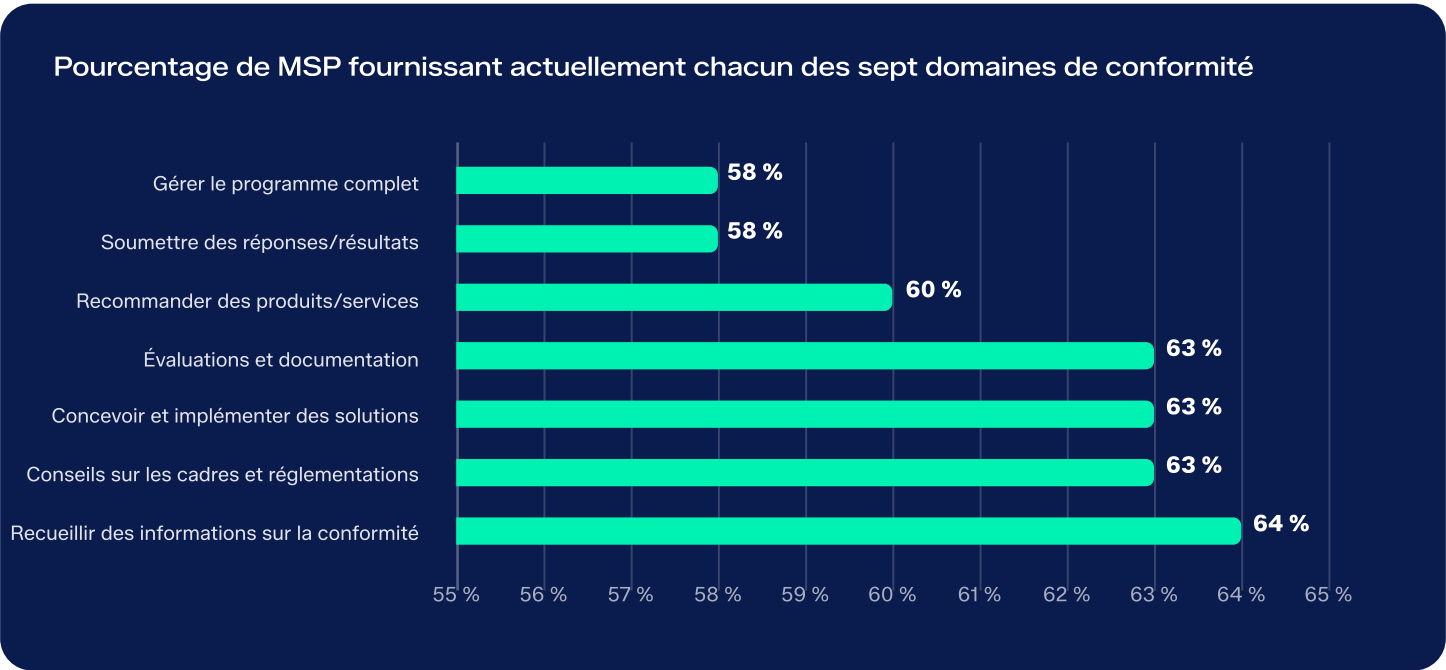
s'attendent à ce qu'elle augmente de manière significative.

Partie 2 : La conformité au cœur de la prestation de services des MSP

1. Les services de conformité sont très répandus, sans pour autant avoir atteint un niveau de maturité élevé.

La conformité en matière de cybersécurité fait désormais partie intégrante de la proposition de valeur des MSP, entraînée par l'augmentation des réglementations et des lois qui exigent une gestion des programmes de cybersécurité dédiée et continue. Les MSP sont extrêmement bien placés pour le faire.

Sur les sept activités de conformité mesurées, l'offre de services reste systématiquement solide. Pour chaque domaine de service répertorié, **58 % à 64 % des MSP** déclarent déjà fournir cette fonctionnalité spécifique aux clients.



Parmi les propositions suivantes, laquelle décrit le mieux l'implication de votre organisation dans la conformité des clients en matière de cybersécurité aujourd'hui et à l'avenir ? (n=800)

99 %

des MSP fournissent un certain niveau de service de conformité.

58 %

assurent la gestion complète du programme.

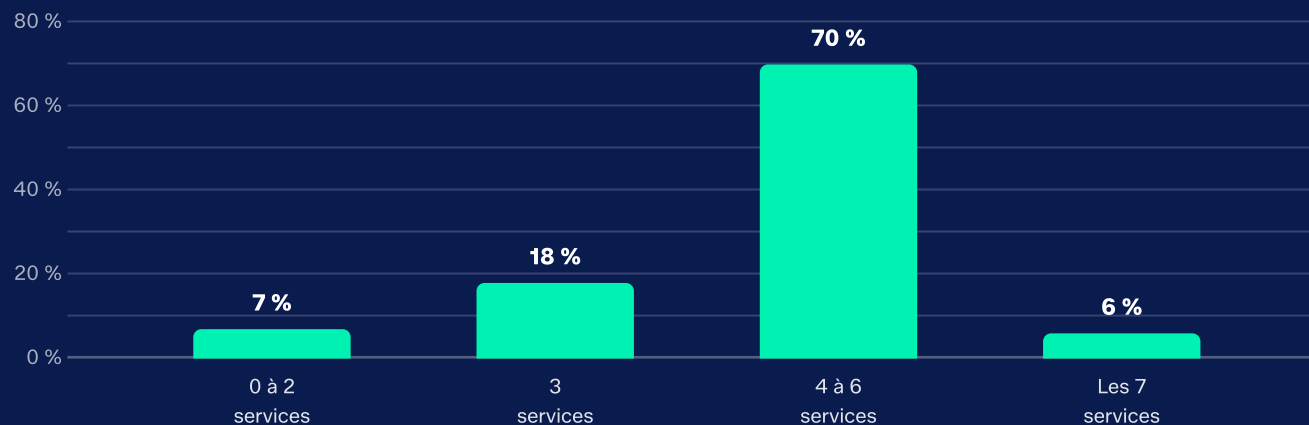
6 %

fournissent un ensemble complet de services de conformité.

Peu de MSP offrent l'intégralité de la suite de services de conformité

Bien que des services de conformité individuels soient largement proposés, la plupart des MSP ne sont pas en mesure d'assurer le cycle de vie complet de la conformité : **70 %** offrent entre quatre et six des sept activités mesurées, tandis que seulement **6 %** fournissent les sept activités. Cela suggère que de nombreux MSP doivent encore élargir leur offre et connecter ces capacités dans un programme de conformité de bout en bout qui offre la supervision complète dont les clients ont besoin.

Profondeur des services de conformité offerts



Parmi les propositions suivantes, laquelle décrit le mieux l'implication de votre organisation dans la conformité des clients en matière de cybersécurité aujourd'hui et à l'avenir ? (n=800)

De nombreux MSP assurant la gestion des programmes de conformité n'offrent pas tous les services d'assistance

En s'intéressant plus particulièrement aux MSP qui gèrent le programme de conformité complet de leurs clients, on constate une lacune similaire. Sur les **58 % de MSP** qui le font, seuls **10 %** fournissent également les six autres services. Des chiffres qui suggèrent que de nombreux MSP assument des responsabilités au niveau du programme avant de mettre en place une offre complète de services de conformité. En pratique, la gestion d'un programme de conformité peut consister à coordonner des activités menées par les clients ou par des spécialistes tiers, plutôt qu'à fournir directement chaque service. Par conséquent, la surveillance des programmes et la prestation des services ne vont pas toujours de pair.

Nombre de services de conformité fournis par les MSP offrant une gestion complète du programme



* Parmi les propositions suivantes, laquelle décrit le mieux l'implication de votre organisation dans la conformité des clients en matière de cybersécurité aujourd'hui et à l'avenir ? Les MSP assurant la gestion complète du programme de conformité (n=465)

Les MSP prévoient de développer leur offre de conformité

La bonne nouvelle est que la demande pour ces capacités est susceptible d'entraîner une nouvelle expansion. De nombreux MSP qui ne fournissent pas actuellement de services de conformité prévoient de les intégrer à l'avenir. La croissance la plus forte est attendue dans la gestion complète des programmes de conformité : au-delà des 58 % qui offrent déjà cette capacité, 40 % supplémentaires prévoient de l'ajouter. Cela suggère que la gestion des programmes devient rapidement une composante standard des offres de conformité des MSP.

SERVICE	ACTUELLEMENT PROPOSÉ	PROJET DE MISE EN PLACE	TOTAL
Recommander des produits/services Conseiller sur les outils et services de sécurité qui soutiennent les objectifs de conformité.	60 %	38 %	99 %
Concevoir et implémenter des solutions Configurez et déployez des contrôles de sécurité pour répondre efficacement aux exigences de conformité.	63 %	37 %	100 %
Cadres et réglementations Identifiez les réglementations, normes et cadres applicables affectant la conformité des clients.	63 %	36 %	99 %
Recueillir des informations sur la conformité Fournir les preuves dont les clients ont besoin pour satisfaire à leurs obligations de conformité.	64 %	35 %	99 %
Évaluations et documentation Effectuer des évaluations et créer une documentation démontrant l'état de conformité et les lacunes.	63 %	36 %	98 %
Soumettre des réponses/résultats Préparer et soumettre les réponses aux audits, les questionnaires et les preuves de conformité.	58 %	40 %	98 %
Gérer le programme complet Superviser les activités de conformité en cours, la collecte de preuves, l'élaboration de rapports et la gouvernance.	58 %	40 %	99 %

Les pourcentages sont arrondis.

Parmi les propositions suivantes, laquelle décrit le mieux l'implication de votre organisation dans la conformité des clients en matière de cybersécurité aujourd'hui et à l'avenir ? Exclut « Ne sait pas » (n=800)

Les services de conformité sont un domaine de croissance pour les MSP de toutes tailles

La maturité de l'offre de conformité des MSP n'est pas définie par leur taille. Bien que les MSP de plus de 51 employés soient les plus susceptibles de fournir les sept services de conformité mesurés **(10 %)**, les petits MSP restent compétitifs. Ceux comptant jusqu'à cinq employés sont plus susceptibles de fournir quatre à six des sept services **(77 %)** que tout autre groupe et déclarent le nombre moyen le plus élevé de services fournis.

L'adoption de la gestion complète du programme est également relativement constante, allant de **54 % à 62 %**. Ces données suggèrent que la conformité devient un facteur de croissance pour les MSP de toutes tailles, ce qui fait évoluer la concurrence : l'accent n'est plus mis sur la disponibilité des services, mais sur la rapidité de prestation, l'étendue de l'offre et la maturité.

TAILLE DU MSP	0-2 SERVICES	3 SERVICES	4-6 SERVICES	LES SEPT SERVICES	NB MOYEN DE SERVICES	GESTION COMPLÈTE DU PROGRAMME
1-5 employés	5 %	11 %	77 %	7 %	5	62 %
6-25 employés	8 %	25 %	65 %	2 %	4	54 %
26-50 employés	8 %	17 %	70 %	6 %	4	59 %
Plus de 51 employés	5 %	17 %	69 %	10 %	4	59 %

Les pourcentages sont arrondis.

Parmi les propositions suivantes, laquelle décrit le mieux l'implication de votre organisation dans la conformité des clients en matière de cybersécurité aujourd'hui et à l'avenir ? Exclut « Ne sait pas » (n=800)

Les MSP ont réalisé des progrès significatifs dans la mise en place de pratiques de conformité : la quasi-totalité des fournisseurs offre désormais au moins un service de conformité et la majorité propose plusieurs fonctionnalités couvrant l'ensemble du cycle de vie de la conformité. La gestion complète des programmes est en train de se généraliser et est en passe de devenir une offre presque universelle, reflétant la demande croissante des clients pour un soutien continu en matière de conformité.

Toutefois, il ne faut pas confondre l'étendue du service avec la maturité. De nombreux MSP ont élargi leur offre au-delà des simples services de conseil, mais rares sont ceux qui disposent aujourd'hui d'une offre de conformité véritablement complète. La plupart continuent de fonctionner avec des piles de service partielles. Même parmi ceux assurant la gestion complète du programme, seule une petite minorité fournit l'ensemble des services de soutien en matière de conformité.

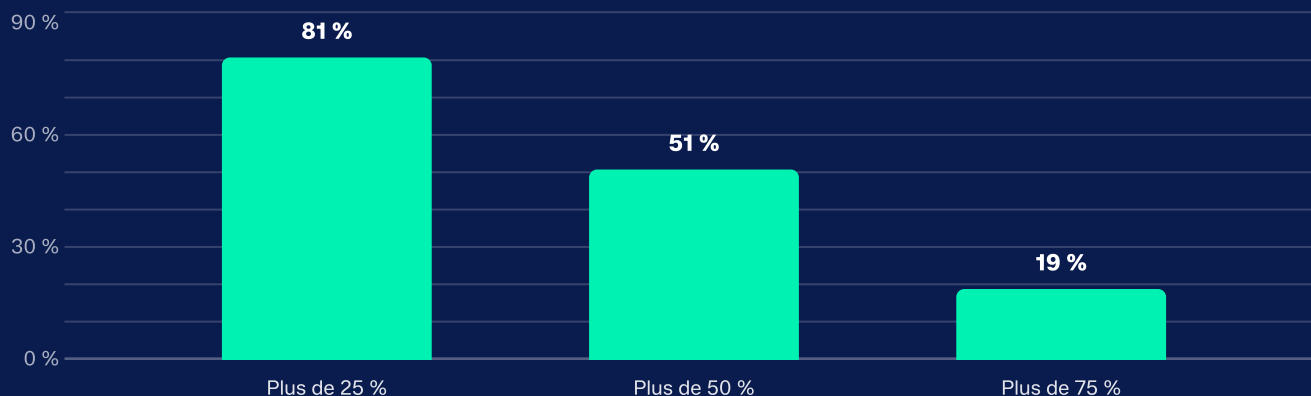
À mesure que les services de conformité deviennent plus largement disponibles, l'avantage concurrentiel dépendra de plus en plus de la rapidité, de la profondeur, de la qualité et de la fluidité de la prestation plutôt que de la fourniture seule. **Les MSP capables de relier les services de conseil, d'implémentation, de documentation, de reporting et de gestion de programme dans une pratique de conformité cohérente seront les mieux placés pour se différencier en tant que leaders du marché.**

2. La conformité stimule l'investissement en matière de sécurité

La conformité est désormais un moteur important des investissements de cybersécurité. Les MSP affirment que la conformité influence en moyenne **50 %** des achats de cybersécurité des clients, avec **33 %** des décisions « lourdes » ou « décisives ». Cette influence est très répandue : **81 % des MSP** déclarent que la conformité affecte au moins **25 %** des achats des clients, et **51 %** déclarent qu'elle en influence au moins la moitié. En d'autres termes, la conformité n'est plus seulement une obligation de reporting et façonne activement la manière dont les clients priorisent les dépenses de sécurité.

L'opportunité est maintenant de rendre cette influence plus stratégique. Seuls **9 %** des MSP déclarent que la conformité influence « fortement » ou « de manière décisive » une majorité significative (**75 %**) des achats de cybersécurité des clients. Cela laisse la possibilité aux MSP d'utiliser la conformité comme une passerelle vers un accompagnement plus stratégique, des services plus approfondis et des programmes de cybersécurité mieux structurés.

Pourcentage des achats de clients influencés par la conformité



Quel pourcentage des décisions d'achat de vos clients en matière de cybersécurité est influencé, au moins en partie, par les exigences réglementaires de conformité, le cas échéant ? (n=800)

50 %

des décisions d'achat des clients sont influencées par les exigences de conformité.

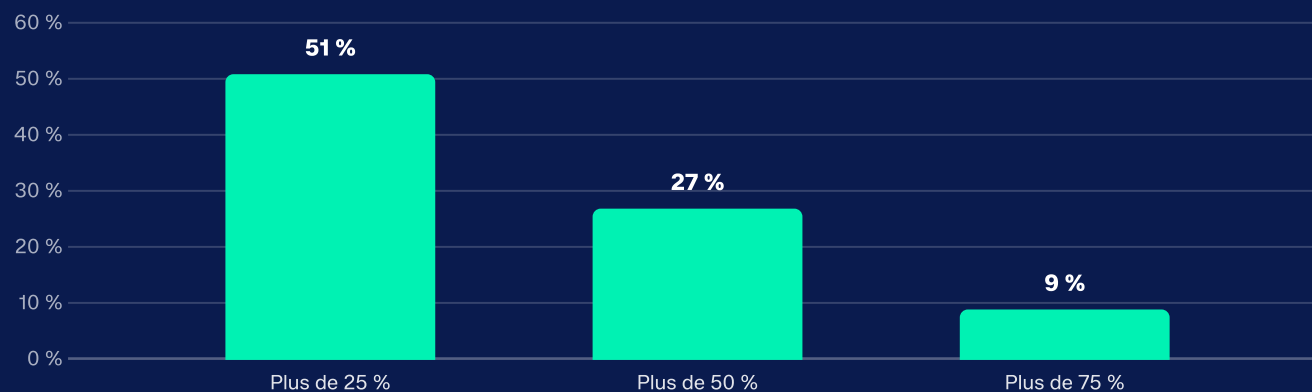
33 %

de ces décisions sont fortement influencées par les exigences de conformité réglementaires.

Les MSP peuvent utiliser la conformité des clients pour éclairer leurs conversations stratégiques

Dans l'ensemble, ces résultats montrent que la conformité est en train de passer du statut d'obligation réglementaire à celui de facteur clé de la stratégie d'entreprise. Elle a déjà un impact manifeste sur les investissements des clients en matière de cybersécurité. Cependant, peu de MSP en ont fait une voie lucrative dans des conversations plus larges sur la cybersécurité. Cela leur offre la possibilité de combler cette lacune et de transformer la demande de conformité en relations de conseil plus approfondies et en services stratégiques à plus forte valeur ajoutée.

Pourcentage des achats des clients influencés « fortement » ou « de manière décisive » par la conformité

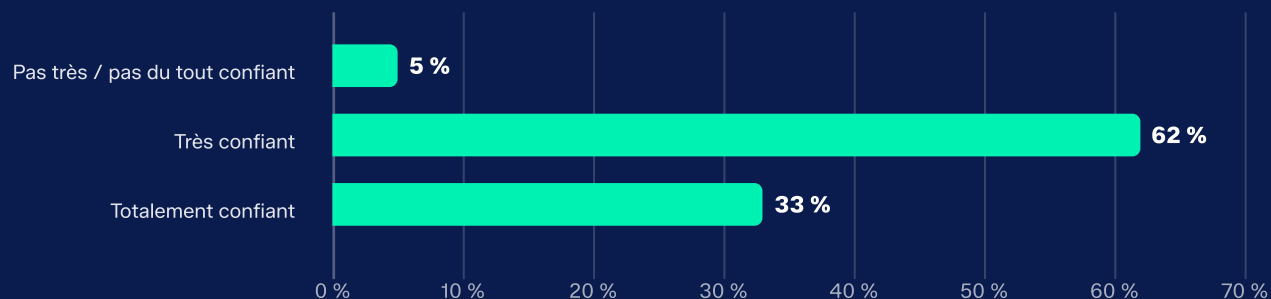


Quel pourcentage des décisions d'achat de vos clients en matière de cybersécurité est fortement ou de manière décisive influencé par les exigences réglementaires en matière de conformité ? (n=800)

3. La transition vers une conformité continue reste progressive

Les MSP adoptent de plus en plus une approche continue de la gestion de la conformité. Les niveaux de confiance suggèrent que la plupart des fournisseurs pensent être bien équipés pour soutenir les clients alors que la conformité évolue, passant d'audits périodiques à une surveillance et une gouvernance continues. Dans l'ensemble, **95 % des MSP** se déclarent « très » ou « totalement » confiants dans leur capacité à surveiller, à gouverner et à documenter en continu la conformité de multiples clients.

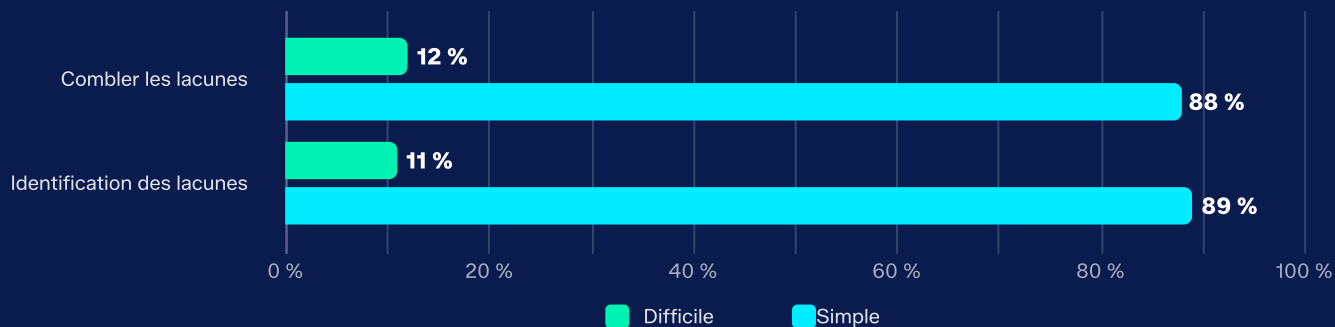
Confiance du MSP dans la gestion continue de la conformité



Dans quelle mesure êtes-vous confiant dans la capacité actuelle de votre organisation à surveiller, gérer et documenter en continu les exigences de conformité de plusieurs clients, le cas échéant ? (n=800)

Ce niveau de confiance se retrouve aussi dans la manière dont les MSP sont équipés pour identifier et remédier aux écarts de conformité et de contrôle chez leurs clients, seule une petite minorité signalant des difficultés dans les deux domaines.

Facilité pour le MSP à identifier et à combler les lacunes en matière de conformité et de contrôle



Dans quelle mesure est-il facile ou difficile pour votre entreprise d'identifier et de remédier aux lacunes de conformité ou de contrôle pour vos clients aujourd'hui ? (n=800)

62 %

des MSP sont « très confiants » dans leur capacité à surveiller, gérer et documenter en continu la conformité de multiples clients.

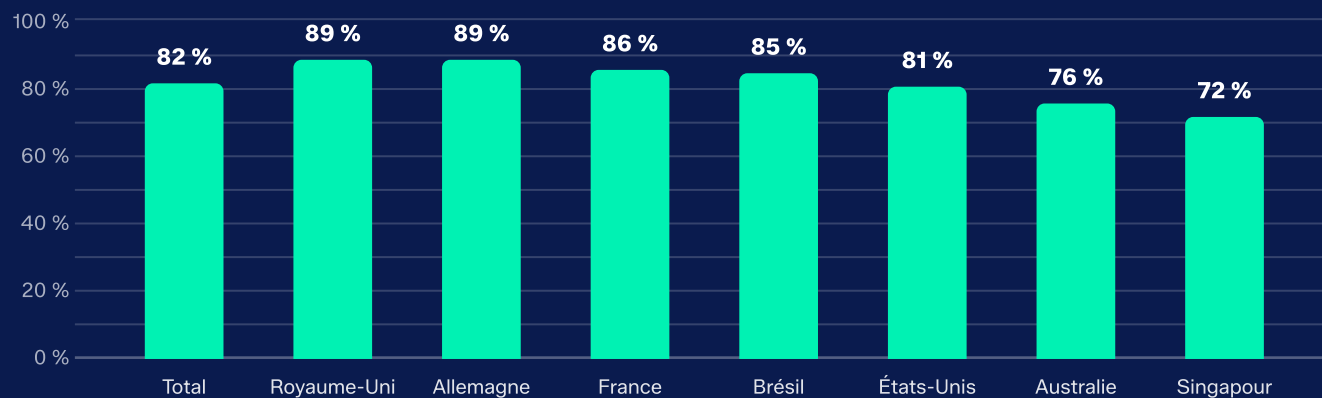
33 %

sont « totalement confiants » dans leur capacité.

La confiance dans la gestion des lacunes en matière de conformité et de contrôle varie selon les pays

Bien que la gestion des lacunes en matière de conformité et de contrôle soit une capacité bien établie pour la plupart des MSP, la confiance varie selon les pays. Les MSP du Royaume-Uni et d'Allemagne sont les plus nombreux à déclarer pouvoir à la fois identifier et remédier facilement à ces problèmes (**89 %**), contre **81 %** aux États-Unis, **76 %** en Australie et **72 %** à Singapour. Ces différences suggèrent que si de nombreux fournisseurs ont mis en place des processus opérationnels, le défi pratique consistant à maintenir la conformité et à réduire les risques est plus grand sur certains marchés que sur d'autres.

La facilité à identifier et à remédier aux lacunes de conformité varie selon les pays



Dans quelle mesure est-il facile ou difficile pour votre entreprise d'identifier et de remédier aux lacunes de conformité ou de contrôle pour vos clients aujourd'hui ? (n=800)

Les MSP de toutes tailles sont confiants dans leur capacité à gérer en continu la conformité des clients

Les niveaux de confiance sont remarquablement constants chez les MSP de toutes tailles. Les fournisseurs de plus petite taille rapportent la confiance globale la plus élevée, avec **98 % des MSP** de 1 à 5 employés se disant « totalement » ou « très » confiants dans leur capacité à gérer une conformité continue, contre **92 %** des MSP de 51 employés ou plus. La confiance totale reste beaucoup plus faible dans toutes les tranches de taille, allant de **30 % à 36 %**. L'écart entre une confiance élevée et une certitude totale suggère que, bien que des capacités de conformité continues soient établies dans la communauté des MSP, de nombreux fournisseurs gagneraient à améliorer leur modèle actuel.

CONFIANCE DANS LA GESTION CONTINUE DE LA CONFORMITÉ	TOTAL	1-5 EMPLOYÉS	6-25 EMPLOYÉS	26-50 EMPLOYÉS	>51 EMPLOYÉS
Totalement confiant	33 %	36 %	34 %	30 %	31 %
Très confiant	62 %	62 %	62 %	65 %	60 %
Pas très confiant	4 %	2 %	4 %	5 %	7 %
Pas du tout confiant	0 %	0 %	0 %	1 %	1 %
Totalement ou très	95 %	98 %	96 %	95 %	92 %

^a Dans quelle mesure êtes-vous confiant dans la capacité actuelle de votre organisation à surveiller, gérer et documenter en continu les exigences de conformité de multiples clients, le cas échéant ? (n=800)

La cyber-résilience exige de pouvoir démontrer la conformité en continu, plutôt que de s'appuyer sur des contrôles périodiques. Pour les clients, cela signifie clairement que les contrôles fonctionnent, que des lacunes sont mises en évidence et que des améliorations sont apportées au fil du temps. Le niveau de confiance des MSP montre que cette capacité est clairement en train de se développer, mais l'absence de certitude totale met en lumière à la fois des opportunités et des risques. Les fournisseurs capables de combler cette lacune en fournissant des services de conformité cohérents, évolutifs et reproductibles seront fortement positionnés pour développer des services de gouvernance à plus forte valeur ajoutée. Ceux qui ne le peuvent pas peuvent avoir du mal à fournir le niveau d'assurance dont les clients ont besoin, à l'heure où les menaces, les réglementations et les risques commerciaux continuent de s'intensifier.

Partie 3 : Opérationnalisation de la sécurité et de la conformité à grande échelle

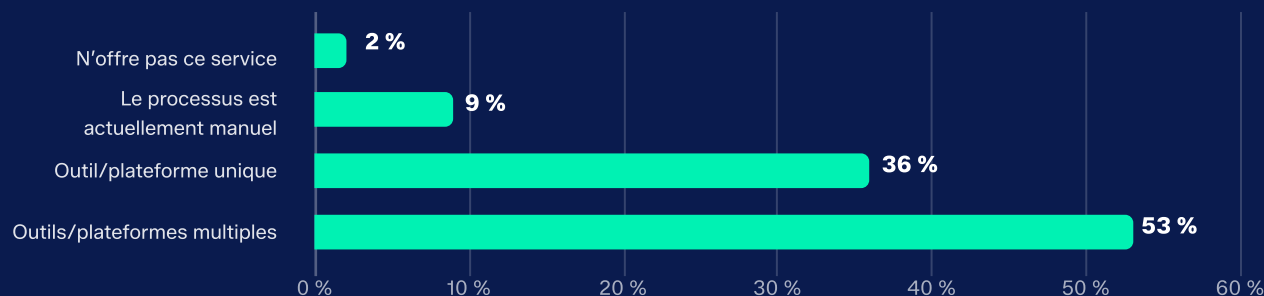
1. La fourniture basée sur des outils est la norme

À mesure que les MSP élargissent leur rôle en matière de conformité à la cybersécurité et de services de conseil stratégique, la prestation basée sur des outils est devenue une pratique courante. **89 % des MSP** utilisent désormais un ou plusieurs outils ou plateformes pour gérer de manière centralisée les activités de conformité ou de type RSSI sur l'ensemble de leur clientèle. Seuls **9 %** continuent de s'appuyer sur des processus entièrement manuels, tandis que **2 %** ne proposent pas du tout ces services.

L'adoption de ces technologies opérationnelles n'a pas conduit à une consolidation généralisée. Les MSP sont plus nombreux à utiliser plusieurs outils ou plateformes (**53 %**) qu'une seule solution (**36 %**), suggérant ainsi que beaucoup fournissent ces services via un ensemble de plateformes spécialisées plutôt qu'un système unique et unifié.

Cela reflète potentiellement la complexité croissante de la gestion à grande échelle des exigences de conformité, des évaluations du risque, du reporting, des activités de gouvernance et de la communication avec les clients. Cela met également en évidence un défi courant : de nombreux outils ne permettent pas d'alimenter en données une plateforme centrale de reporting, ce qui oblige à consolider manuellement les activités dans un rapport unique destiné au client. Les résultats suggèrent un intérêt croissant pour des approches plus unifiées en matière de gestion et de reporting sur les programmes de conformité.

Approche par plateforme pour la prestation d'activités de conformité/RSSI



Quelle approche votre organisation utilise-t-elle actuellement pour mettre en œuvre des activités de conformité à la cybersécurité ou de type RSSI sur l'ensemble de votre clientèle ? (n=800)

53 %

des MSP utilisent plusieurs outils ou plateformes pour gérer de manière centralisée la conformité en matière de cybersécurité ou des activités type RSSI.

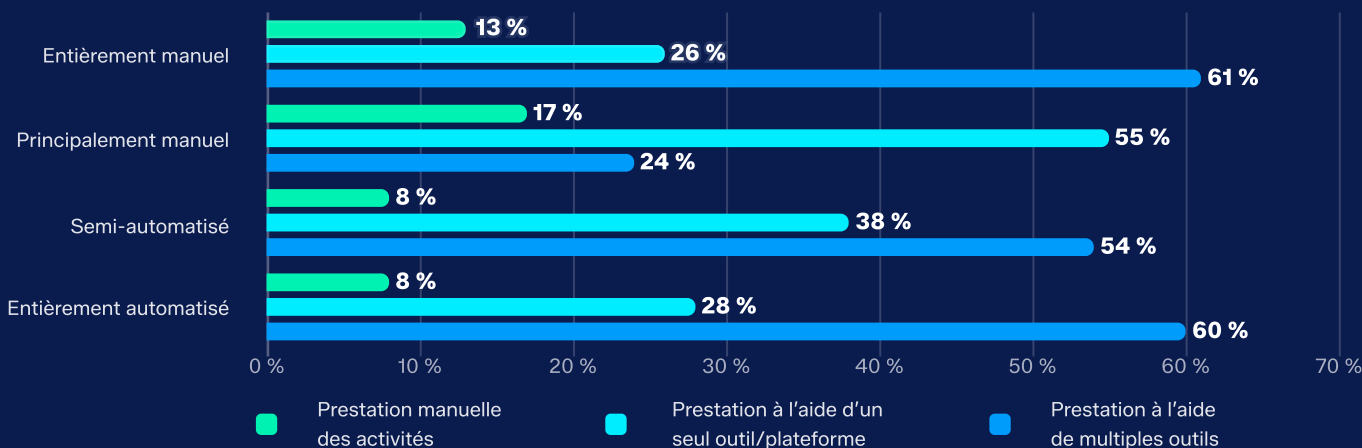
36 %

des MSP ne s'appuient que sur un seul outil ou plateforme

2. Les rapports de sécurité deviennent automatisés

La plupart des MSP ont délaissé les processus de reporting entièrement manuels, **86 %** d'entre eux utilisant des méthodes entièrement automatisées ou semi-automatisées pour produire des rapports consolidés sur la posture de sécurité. Toutefois, l'automatisation complète n'est pas normalisée. Seuls **31 % des MSP** peuvent générer des rapports rapidement grâce à un processus entièrement automatisé, tandis que **55 %** comptent encore sur un effort manuel pour combiner les données, ajouter du contexte et finaliser les rapports.

Niveau d'automatisation du reporting selon l'approche de prestation



Quelle approche votre organisation utilise-t-elle actuellement pour mettre en œuvre des activités de conformité à la cybersécurité ou de type RSSI sur l'ensemble de votre base de clients, VS dans quelle mesure automatise-t-elle la production de rapports consolidés présentant leur situation, les risques et les recommandations en matière de cybersécurité ? (n=800)

Cela montre qu'une stratégie de plateforme ne garantit pas, à elle seule, un niveau élevé de maturité en matière d'automatisation. Les MSP, quel que soit leur niveau d'automatisation, utilisent plusieurs outils, ce qui peut s'expliquer par la fragmentation des processus ou la présence de flux de travail plus automatisés sur un ensemble d'outils plus large. Quoi qu'il en soit, le besoin d'automatisation et la valeur qu'elle peut créer pour les MSP sont largement répandus.

86 %

des MSP utilisent un processus entièrement ou semi-automatisé pour produire des rapports consolidés sur la posture de sécurité.

31 %

peuvent générer des rapports rapidement grâce à l'automatisation.

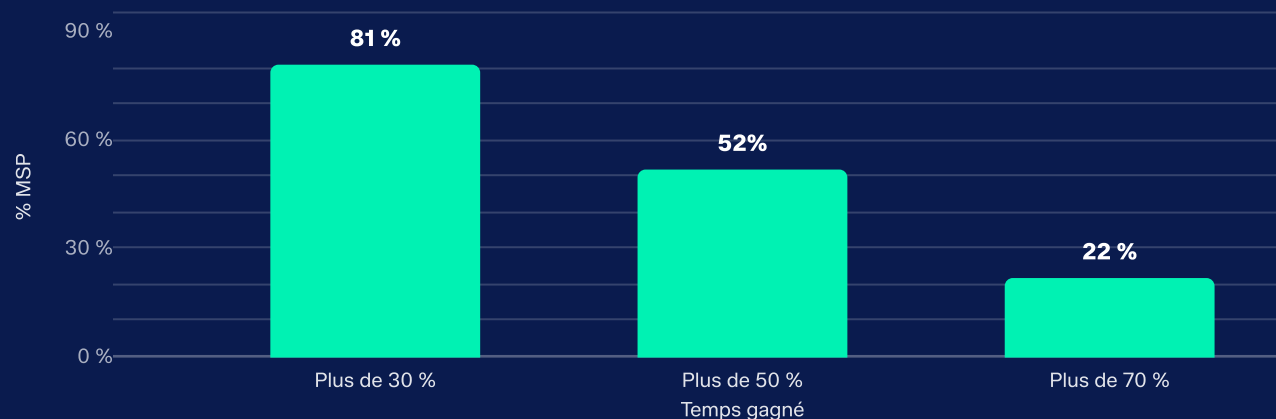
55 %

nécessitent encore quelques efforts manuels pour consolider les activités.

3. Des gains d'efficacité significatifs restent inexploités

La consolidation des plateformes pourrait permettre aux MSP de réaliser des gains d'efficacité substantiels. En moyenne, les MSP estiment qu'une plateforme unique et entièrement unifiée pourrait réduire de **53 %** le temps que leurs équipes consacrent à la gestion et à l'établissement de rapports sur la posture de sécurité et la conformité des clients. Dans l'ensemble, **81 % des MSP** anticipent un gain de temps de plus de **30 %**, 52 % de plus de 50 % et 22 % de plus de 70 %.

Gain de temps estimé grâce à une plateforme unifiée



Quelle proportion du temps de votre équipe pourrait être économisée si toute posture de sécurité et de gestion et reporting de la conformité des clients était gérée depuis une plateforme unique et entièrement unifiée ? (n=800)

Les économies perçues sont particulièrement élevées chez les MSP qui offrent déjà une gestion complète du programme de conformité. **84 % des MSP** offrant ce service déclarent qu'ils pourraient réaliser plus de **30 %** de gains de temps, contre **64 %** chez les MSP qui n'offrent ni ne prévoient d'offrir le service. Cela suggère que ceux qui gèrent des activités de conformité plus complètes ou intégrées sont aussi ceux qui pourraient avoir le plus à gagner de la consolidation des plateformes.

Ces résultats mettent en évidence la charge opérationnelle à laquelle de nombreux MSP restent confrontés lorsqu'ils doivent gérer le reporting, la conformité et les services de conseil à travers plusieurs plateformes et flux de travail. À mesure qu'augmente la demande de services à forte valeur ajoutée, tels que la gestion de la conformité et les conseils traditionnellement donnés par les RSSI, il devient essentiel d'identifier des moyens de réorganiser la gestion des programmes de cybersécurité à grande échelle.

Les résultats suggèrent que les MSP accordent une grande importance à l'utilisation d'un modèle unifié pour combiner l'ensemble du programme de conformité, aidant ainsi leurs équipes à consacrer moins de temps à la consolidation des informations et plus de temps à la fourniture de résultats stratégiques à leurs clients.

53 %

de temps potentiellement gagné pour les MSP si la posture de sécurité et les activités de gestion de la conformité et de reporting des clients étaient gérées depuis une plateforme unique et unifiée.

81 %

des MSP déclarent qu'une approche unifiée permettrait à leur équipe de gagner plus de 30 % de leur temps.

22 %

disent qu'ils gagneraient plus de 70 % de ce temps.

Conclusion

Le paysage des MSP est en pleine mutation. Les clients attendent de plus en plus de leurs fournisseurs qu'ils assurent un leadership stratégique en matière de cybersécurité, en parallèle de la gestion des technologies. Les MSP répondent à cette évolution en élargissant leur offre à la gestion de la conformité, aux services de conseil en cybersécurité et à d'autres fonctions relevant traditionnellement du RSSI. Avec **84 % des MSP interrogés s'attendant à ce que la demande de services relevant traditionnellement du RSSI augmente au cours de l'année prochaine**, ces services à forte valeur ajoutée représentent une opportunité croissante pour la croissance et la différenciation des activités.

Dans le même temps, la gestion à grande échelle de la posture de sécurité, de la conformité et du reporting client reste un défi opérationnel. Alors que la plupart des MSP ont adopté des plateformes et des processus automatisés, beaucoup s'appuient encore sur de multiples outils et des interventions manuelles pour fournir ces services. À bien des égards, cela reflète la complexité à laquelle sont confrontés les RSSI et les équipes de sécurité, les MSP devant composer avec les mêmes problèmes qu'ils cherchent à résoudre chez leurs clients.

Les MSP capables d'assurer de manière fiable et efficace un leadership évolutif en matière de cybersécurité, une gestion continue des programmes et des résultats mesurables en matière de sécurité seront les mieux placés pour renforcer les relations avec les clients, accroître les ventes et capitaliser sur la prochaine frontière d'opportunités.

Sophos CISO Advantage

[Sophos CISO Advantage](#) offre aux MSP l'opportunité d'assumer un rôle de leader dans un autre type de conversation sur la cybersécurité : une conversation axée sur les résultats, les risques commerciaux, la mise en conformité progressive et l'amélioration mesurable.

Fourni depuis [Sophos Fusion](#), le système de cybersécurité IA-natif de Sophos, cette solution transforme le rôle de RSSI que la plupart des MSP jouent déjà en un service structuré, évolutif et facturable de gestion des programmes de cybersécurité.

Les processus d'évaluation, de reporting et d'élaboration de feuilles de route, accélérés par l'IA agentique, offrent à ces partenaires essentiels un moyen reproductible de fournir, à l'ensemble de leur clientèle, des analyses prêtes à être présentées aux dirigeants, des preuves étayées par des référentiels et des plans d'action priorités.

Cela permet aussi d'ouvrir de nouvelles opportunités de revenus récurrents, de croissance et de fidélisation des clients à partir des engagements déjà en place. Chaque évaluation met en évidence des failles de sécurité et chaque faille donne lieu à l'établissement d'une feuille de route d'amélioration, pour que les MSP soient en position de fournir les solutions appropriées.

Sophos CISO Advantage répond à une demande que la communauté de la cybersécurité met en avant depuis des années. En adoptant cette solution de manière précoce, les MSP sont en mesure d'assumer pleinement le rôle de leader que leurs clients attendent d'eux.

Pour en savoir plus sur Sophos CISO Advantage, les MSP peuvent visiter le [Portail Partenaires](#).

Vous souhaitez devenir partenaire
Sophos ? **Inscrivez-vous ici.**

Sophos France

Tél. : 01 34 34 80 00

Email : info@sophos.fr