Juillet 2025

Étude de marché

Rapport MSP Customer Insight 2025

Ce que les organisations du monde entier exigent de leurs fournisseurs de services managés en matière de cybersécurité

Barracuda®
Your business, secured.

Sommaire

Introduction 3

Résultats clés 5

La clientèle pour les MSP 6

Les MSP permettent aux clients de gérer leur sécurité à mesure qu'ils se développent 8

Les clients auront besoin de plus de soutien en matière d'IA et de sécurité réseau à l'avenir 10

Les clients sont prêts à payer davantage pour des services adaptés 11

Les MSP peuvent perdre des clients s'ils ne peuvent prouver leur expertise 13

Les organisations victimes d'une cyberattaque investissent davantage dans la sécurité et l' externalisation 14

Conclusion 16

Introduction

Ce rapport étudie ce que les organisations du monde entier attendent et exigent de leurs fournisseurs de services managés (MSP) en matière de services de cybersécurité. Il s'appuie sur les résultats d'une nouvelle enquête internationale réalisée auprès des clients MSP et commandée par Vanson Bourne.

Les MSP sont devenus essentiels aux entreprises. La plupart des organisations interrogées externalisent déjà une partie ou la totalité de leurs besoins en cybersécurité à des MSP, tandis que d'autres étudient les possibilités qui s'offrent à elles.

Ce rapport a pour objectif d'aider les MSP à comprendre les besoins actuels et futurs de leurs clients existants, qui sont leurs clients potentiels et où les trouver, et ce qui pousse les clients à se tourner vers un concurrent.

Dans l'ensemble, les résultats montrent que :

- Les MSP permettent aux clients de gérer leur sécurité à mesure qu'ils se développent.
- Au cours des prochaines années, les clients auront particulièrement besoin d'aide pour la mise en place d'applications d'IA/apprentissage automatique et d'une sécurité réseau. Et ils sont prêts à y mettre le prix.

Méthodologie

Barracuda a chargé l'agence d'études de marché indépendante Vanson Bourne de mener une enquête mondiale auprès de 2 000 preneurs de décision de haut niveau en matière de sécurité, occupant des postes informatiques et commerciaux dans des organisations comptant entre 50 et 2 000 employés et issues d'un large éventail de secteurs aux États-Unis, au Royaume-Uni, en France, dans la région DACH (Allemagne, Autriche, Suisse), au Benelux (Belgique, Pays-Bas, Luxembourg), dans les pays nordiques (Danemark, Finlande, Norvège, Suède), en Australie, en Inde et au Japon. Le questionnaire a été soumis en avril et mai 2025.

Introduction

- La plupart des clients MSP envisageront de changer de fournisseur, notamment en raison de préoccupations concernant la capacité du MSP à les aider à remédier à une cyberattaque et à s'en remettre.

Nous espérons que ce rapport aidera les MSP à façonner leurs stratégies futures, à identifier de nouvelles opportunités et à combler leurs lacunes. Barracuda est là pour vous aider à chaque étape du processus. Alors que nous devons faire face aux défis de menaces en constante évolution, veillons ensemble à assurer la cyber-résilience et la protection de nombreuses organisations.

Résultats clés

85 %

des organisations comptant entre 1 000 et 2 000 employés font appel à des MSP pour assurer leur sécurité, contre 61 % de celles qui comptent entre 50 et 100 employés

48 %

des organisations se tournent vers les MSP pour une assistance de sécurité 24 heures sur 24

52 %

des organisations demandent de l'aide aux MSP lorsque le nombre d'outils de sécurité devient ingérable (principale raison invoquée)

51 %

des organisations se tournent vers les MSP pour faire évoluer leurs stratégies de sécurité à mesure qu'elles se développent (deuxième raison la plus citée)

39 %

des organisations pensent qu'elles auront besoin des MSP en ce qui concerne les outils et des applications d'IA et d'apprentissage automatique dans les prochaines années (principale raison citée)

92 %

des organisations sont prêtes à payer davantage pour une assistance à l'intégration d'outils de sécurité

45 %

changeront de MSP si elles ne constatent aucune aptitude, expertise et capacité à les soutenir avec une sécurité 24/7 (principale raison invoquée)

La clientèle pour les MSP

Les cybermenaces continuent d'évoluer, les pirates tirant parti des outils d'intelligence artificielle et des services criminels à louer pour lancer des attaques de plus en plus sophistiquées, et ce, plus rapidement, en plus grand nombre et avec une plus grande précision.

Les professionnels de l'informatique et de la sécurité sont constamment assaillis de telles menaces. Pour assurer la protection de l'organisation et de ses actifs, il est nécessaire de disposer de solutions de sécurité avancées, ainsi que de capacités de surveillance, de gestion et d'atténuation en continu, et d'une compréhension approfondie du paysage des menaces. Peu d'organisations peuvent satisfaire à tous ces besoins en interne.

Constatation clé : 73 % des organisations interrogées externalisent leurs services de sécurité à un MSP

96 % des organisations interrogées envisagent ou font déjà appel à un MSP : 73 % déclarent qu'elles externalisent déjà leurs services de sécurité à un MSP, 18 % comparent actuellement les fournisseurs, et 5 % envisagent la possibilité d'utiliser un MSP.

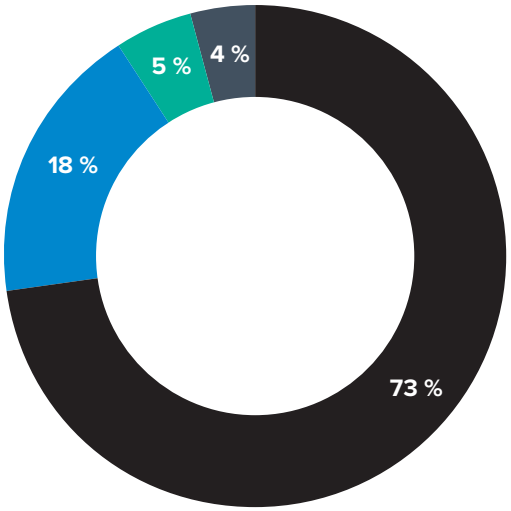

FIGURE 1

Votre organisation externalise-t-elle des activités de sécurité informatique à un fournisseur de services gérés (MSP) ?

n=2 000

- Oui
- Nous comparons actuellement les fournisseurs
- Nous envisageons cette possibilité
- Non

Ces chiffres cachent tout de même quelques différences intéressantes.

Par exemple, les plus grandes organisations interrogées sont plus susceptibles d'utiliser des MSP que les plus petites.

Constatation clé : 85 % des entreprises interrogées comptant entre 1 000 et 2 000 employés font appel à des MSP pour assurer leur sécurité, contre 61 % de celles qui comptent entre 50 et 100 employés

Ce niveau d'engagement des MSP plus élevé peut refléter le fait que les grandes organisations ont une complexité de sécurité accrue et une gamme plus étendue d'outils à gérer.

Par exemple, les grandes organisations interrogées ont tendance à s'inquiéter davantage que les petites concernant la complexité croissante de leur environnement de sécurité (42 %) et de la complexité croissante des cyberattaques (46 %). Pour les plus petites entreprises interrogées, les chiffres correspondants sont de 32 % et 34 %.

Un pourcentage légèrement inquiétant de 10 % des petites organisations interrogées n'ont pas l'intention de faire appel à un MSP pour les aider en matière de cybersécurité. Les petites entreprises disposent généralement de moins de ressources internes dédiées à la protection, ce qui pourrait les rendre encore plus vulnérables aux attaques.

Les secteurs les plus susceptibles de confier la cybersécurité à des MSP sont les administrations locales (84 %) et le secteur de l'éducation (78 %). Il y a un niveau d'engagement plus faible dans les loisirs et le divertissement (60 %), le commerce de détail (65 %) et l'industrie manufacturière (57 %).

Parmi les pays interrogés, les organisations du Royaume-Uni et du Benelux sont les plus susceptibles de faire appel à un MSP (79 % et 81 % respectivement). Les degrés de collaboration les plus bas sont observés dans les pays nordiques (54 %) et au Japon (59 %).

Les MSP permettent aux clients de gérer leur sécurité à mesure qu'ils se développent

Les recherches indiquent que, du point de vue des clients, le partenaire MSP idéal offre à la fois une assistance pratique axée sur les produits et les technologies, et une aide plus stratégique en matière de plans de sécurité et de conformité.

L'examen des deux premiers résultats suggère que les MSP jouent un rôle clé en aidant les organisations à gérer les implications de sécurité relatives à la croissance de l'entreprise.

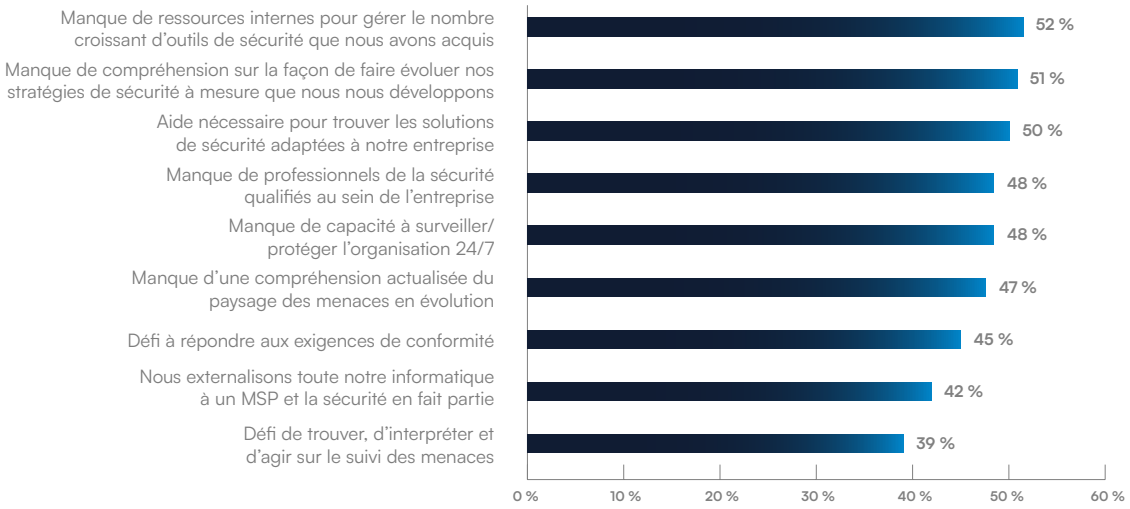

FIGURE 2

Les raisons de sous-traiter la sécurité à un MSP

n=2 000

Constatation clé : 52 % des organisations se tournent vers les MSP pour obtenir de l'aide lorsque le nombre d'outils de sécurité devient ingérable

Le besoin de jongler avec un nombre en constante évolution de produits de sécurité était la raison la plus souvent avancée pour expliquer l'utilisation de MSP. Beaucoup de ces outils proviennent probablement de fournisseurs différents, et la plupart ne s'intègrent pas entre eux.

Ce chiffre atteint 60 % parmi les entreprises du secteur manufacturier interrogées. Les entreprises manufacturières sont susceptibles de posséder un nombre important de systèmes connectés et d'appareils IoT, ce qui augmente la probabilité de prolifération des outils de sécurité.

D'autres résultats de l'étude montrent que le manque d'intégration peut accroître l'exposition et les risques de sécurité, rendant la gestion de la sécurité plus difficile et plus coûteuse, tout comme la détection et l'atténuation des menaces.

Constatation clé : 51 % des organisations se tournent vers les MSP pour faire évoluer leurs stratégies de sécurité à mesure qu'elles se développent

La deuxième raison la plus souvent invoquée pour laquelle les entreprises optent pour un MSP et une assistance de sécurité reflète l'évolution du rôle des fournisseurs de services en tant que conseillers en sécurité : 51 % se tournent vers leur partenaire de service pour les aider à faire évoluer et à mettre à jour leurs stratégies de sécurité à mesure que l'organisation se développe et se transforme. Les organismes d'éducation et de santé étaient particulièrement susceptibles de mentionner cela comme raison pour faire appel à un MSP (tous deux à 55 %).

Les établissements scolaires sont également parmi les plus susceptibles de s'inquiéter de la complexité croissante de leur sécurité informatique (48 % contre 38 % en général), ce qui suggère qu'ils rencontrent des difficultés pour protéger un nombre croissant d'actifs numériques. Opter pour un MSP pour obtenir de l'aide est une étape naturelle pour eux.

Constatation clé : 48 % des organisations se tournent vers les MSP pour une assistance de sécurité 24 heures sur 24

La plupart des organisations reconnaissent que la cybersécurité est une activité continue, et que cela exige des niveaux de personnel et d'investissement que beaucoup d'entre elles n'ont pas en interne. S'appuyer sur un MSP pour vous aider à surveiller et à répondre aux menaces et aux alertes de sécurité 24/7 est un autre facteur clé d'engagement.

De nombreux MSP exploitent désormais, souvent en collaboration avec des fournisseurs de sécurité, un centre d'opérations de sécurité (SOC) géré qui offre une telle couverture experte. Pour bénéficier de la sécurité la plus complète, cela peut être combiné avec une solution de détection et de réponse (XDR) étendue gérée qui peut couvrir l'ensemble de la surface d'attaque, y compris le cloud, les endpoints, emails, applications et réseaux.

Pour de nombreuses organisations interrogées, l'engagement avec les MSP est également étroitement lié au manque de professionnels de la cybersécurité en interne, raison citée par 48 % d'entre elles. La pénurie de compétences semble être un défi universel, car la proportion reste constante, et ce, quelle que soit la taille des entreprises.

Pour 42 % des entreprises interrogées, la sécurité est externalisée à un MSP et intégrée à d'autres services informatiques. Cela représente à la fois une opportunité et un risque pour les MSP, notamment lorsque les clients décident de déplacer leur activité. Pour en savoir plus, consultez la section sur les facteurs décisifs.

Les clients auront besoin de plus de soutien en matière d'IA et de sécurité réseau à l'avenir

Au cours des deux prochaines années, les clients seront très probablement amenés à solliciter l'aide des MSP pour la mise en place d'outils et d'applications d'IA et d'apprentissage automatique. Cela est suivi d'une assistance pour les mises en œuvre d'une sécurité réseau, telles que les mesures zero-trust et les solutions SASE (Secure Access Service Edge).

Constatation clé : 39 % des organisations pensent qu'elles auront besoin des MSP en ce qui concerne les outils et des applications d'IA et d'apprentissage automatique dans les prochaines années

L'IA et la sécurité réseau sont des domaines d'intérêt croissant pour les entreprises, avec une vulnérabilité accrue de la sécurité et une complexité technique. Ils peuvent être difficiles à comprendre, notamment pour les 48 % des organisations en sous-effectif.

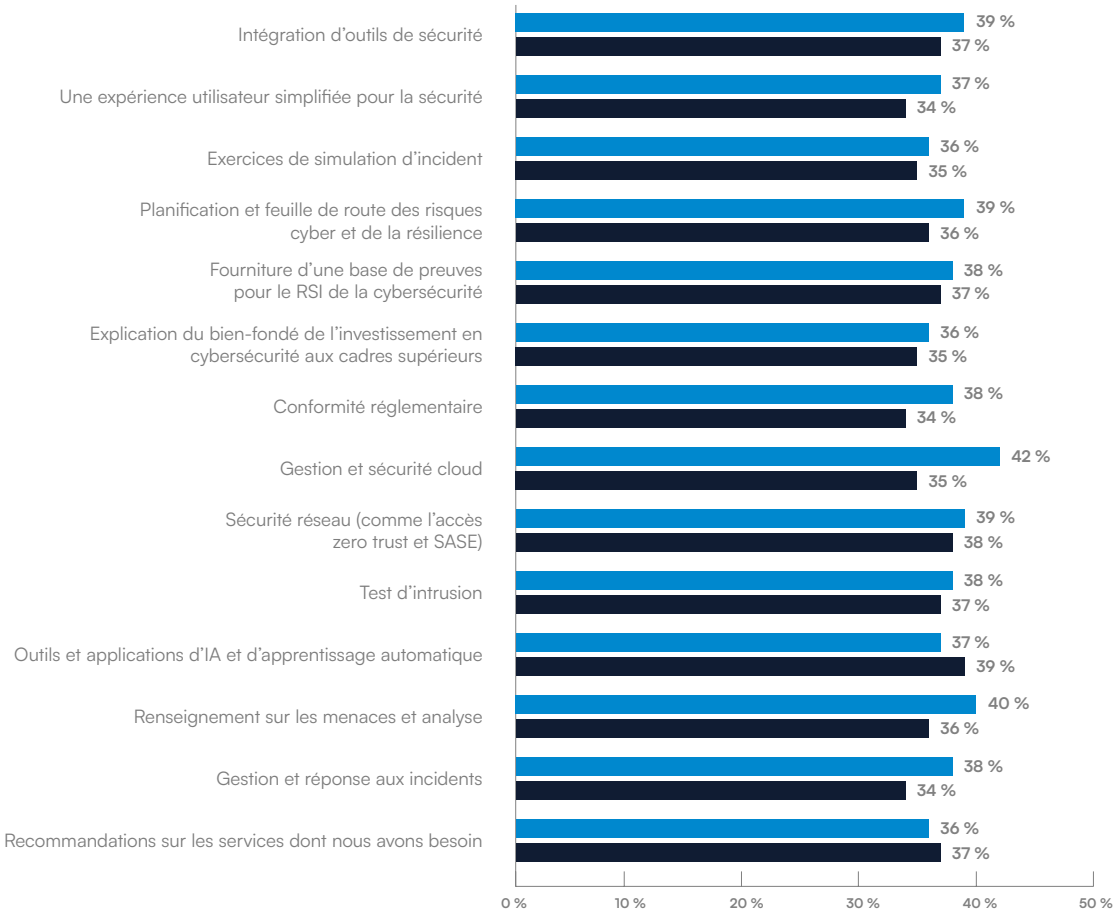

FIGURE 3

Opportunités de sécurité pour les MSP : domaines dans lesquels les organisations auront besoin de l'assistance des fournisseurs de services dans l'année ou les deux années qui suivent

n=2 000

Déjà utilisé par le MSP

Besoin d'assistance prévu

Les résultats soulignent les différents parcours des organisations de tailles variées.

Par exemple, parmi les organisations comptant de 50 à 100 employés, la proportion cherchant une future assistance pour l'IA passe à 44 %, dont 29 % ont déjà opté pour un MSP. Pour les plus grandes organisations, 44 % collaborent avec des MSP en matière d'IA, et 37 % s'attendent à avoir besoin d'assistance au cours des deux prochaines années.

Cela suggère que les grandes organisations comprennent déjà les limites de la gestion de l'IA et de l'apprentissage automatique par elles-mêmes. Par conséquent, elles collaborent activement avec les MSP pour optimiser leur utilisation de l'IA dans l'informatique et la sécurité. Une image similaire, mais avec des différences moindres, est observée pour la sécurité réseau.

Il convient également de noter l'utilisation généralisée et la demande de services stratégiques tels que la planification des risques cyber et de la résilience, la simulation de réponse aux incidents et l'explication du bien-fondé du RSI de la cybersécurité.

Les clients sont prêts à payer davantage pour des services adaptés

L'enquête a révélé que la quasi totalité des clients MSP sont prêts à payer davantage pour les services supplémentaires dont ils auront besoin au cours des deux prochaines années, et qu'environ 70 % sont prêts à payer jusqu'à 10 % ou 25 % de plus.

Constatation clé : 92 % des organisations sont prêtes à payer davantage pour une assistance à l'intégration d'outils de sécurité

Les services pour lesquels ils sont les plus enclins à dépenser davantage incluent les outils et applications d'IA et d'apprentissage automatique, la sécurité cloud et la sécurité réseau. Les résultats restent cohérents quelle que soit la taille de l'entreprise.

Dans l'ensemble, les outils et activités opérationnels s'en sortent mieux en matière de dépenses supplémentaires. Il existe une certaine réticence à investir davantage dans des services « plus souples » tels que la simulation d'incidents, l'explication du bien-fondé de l'investissement en cybersécurité ou les conseils sur les services nécessaires.

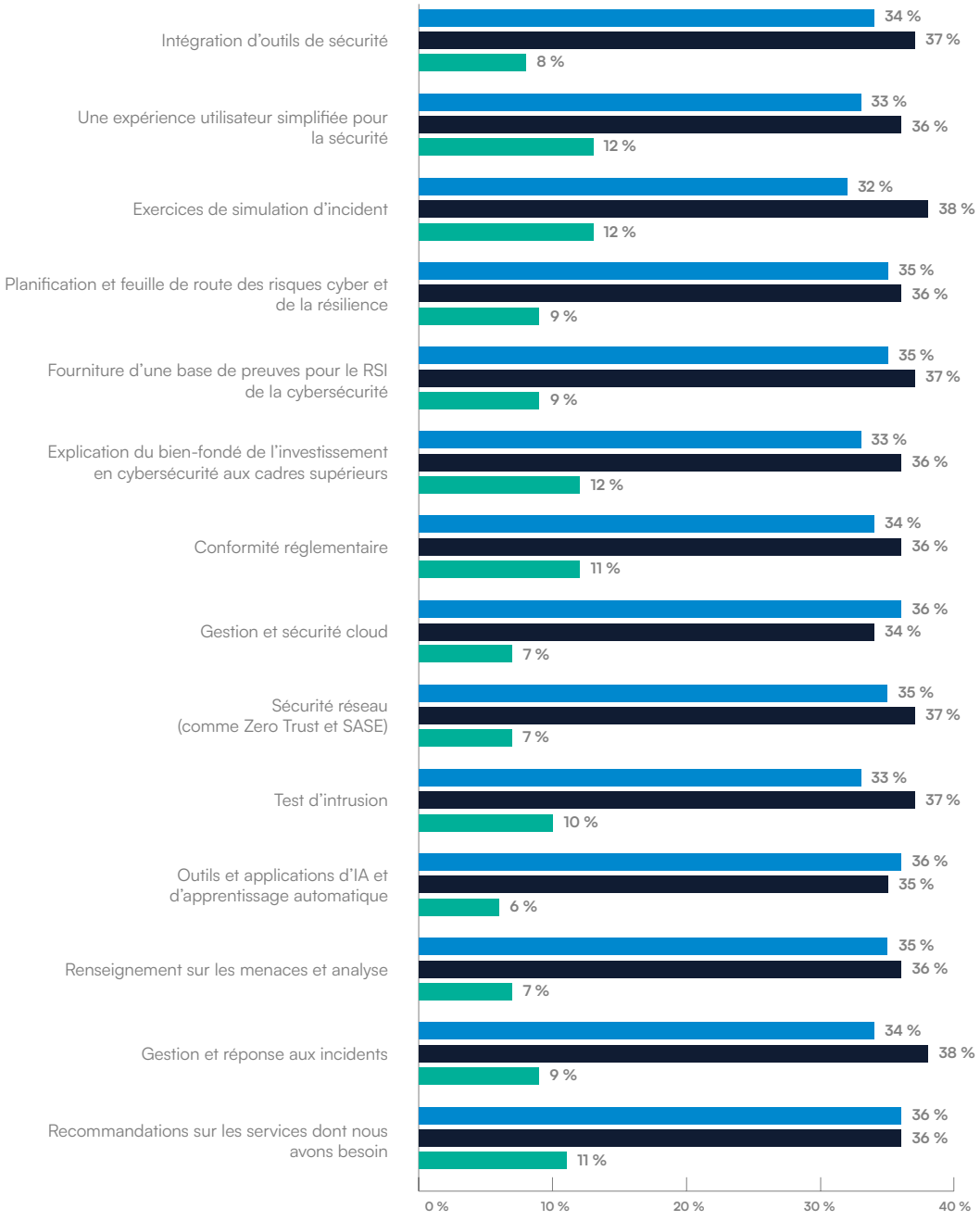

FIGURE 4

Les coûts supplémentaires pour les organisations sont prêts à payer pour ces services auprès des MSP dans les 1 à 2 prochaines années

n=2 000

- Prêts à payer jusqu'à 25 % de plus
- Prêts à payer jusqu'à 10 % de plus
- Je ne suis pas prêt à payer plus pour cela

Cependant, ce que les clients privilégient et ce dans quoi ils sont prêts à investir semble très différent du point de vue d'un incident de sécurité, tel qu'un incident lié à un email ou à une attaque par ransomware. Pour en savoir plus, consultez la section sur l'impact d'une faille de sécurité ci-dessous.

Les MSP risquent de perdre des clients s'ils ne peuvent pas prouver leur expertise

Les résultats montrent que lorsqu'il s'agit de rester fidèle à un partenaire MSP, la loyauté est limitée et dépend de la confiance du client dans l'expertise, la qualité et la stabilité commerciale du fournisseur de services. Seules 2 % des entreprises interrogées ont déclaré qu'elles ne pouvaient pas changer de MSP. Pour tous les autres, il y a des obstacles évidents.

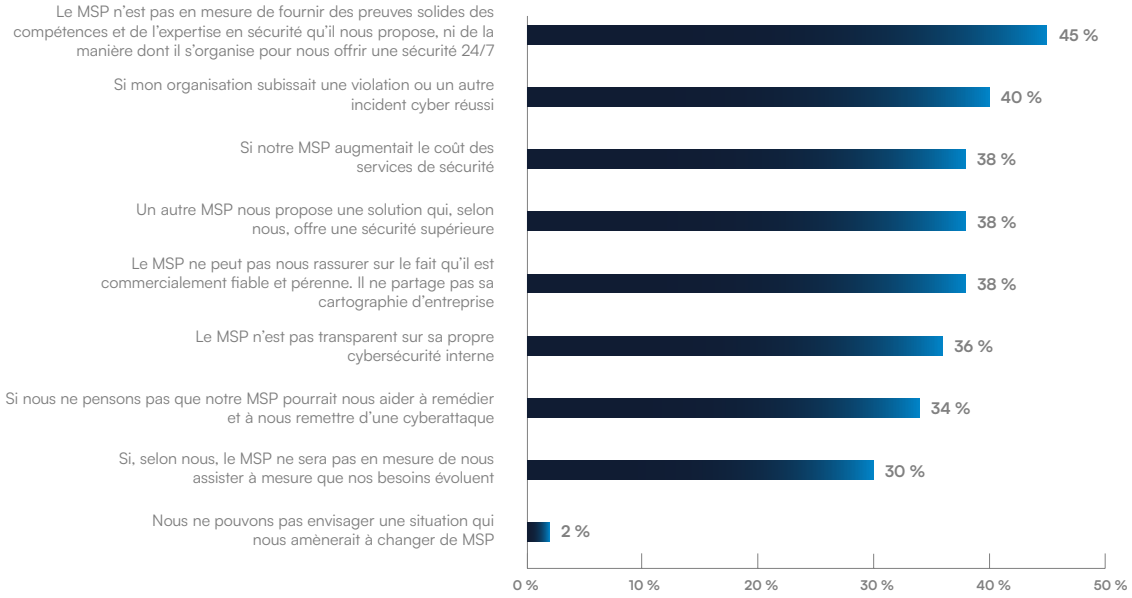

FIGURE 5

Qu'est-ce qui vous pousserait à envisager de changer de MSP pour l'assistance en cybersécurité ?

n=2 000

Une faille de sécurité met clairement à mal les relations professionnelles. Pour plus d'un tiers (38 %) des clients MSP, une augmentation de prix ou une meilleure offre de la part d'un autre MSP les inciterait à changer de fournisseur.

Constatation clé : 45 % des entreprises changeront de MSP si elles ne constatent aucune aptitude, expertise et capacité à les soutenir avec une sécurité 24/7

Pour les MSP concernés, il ne s'agit pas seulement de perdre le secteur de la cybersécurité : 89 % des clients sortants, ayant regroupé leurs services informatiques et de sécurité, supprimeront également ces activités, soit en même temps (46 %), soit plus tard (42 %).

Il convient de mentionner que 38 % des clients MSP déclarent qu'ils changeront de fournisseur si le MSP augmente ses coûts. Outre les conclusions sur la volonté d'investir, cela suggère que les clients

MSP paieront volontiers plus pour les services qu'ils désirent et dont ils ont besoin, mais sont moins à l'aise avec les augmentations de prix imposées arbitrairement par le MSP.

La bonne nouvelle est que les facteurs potentiellement rédhibitoires concernent presque tous les domaines que les MSP peuvent couvrir en investissant dans leur propre résilience de sécurité et commerciale et dans celle de leurs clients, ainsi qu'en renforçant la confiance et la transparence.

Les organisations victimes d'une cyberattaque investissent davantage dans sécurité et externalisation

Une violation de la messagerie ou une attaque par ransomware réussie modifie les priorités de sécurité.

Les différences entre les entreprises qui ont été touchées et celles qui ne l'ont pas été sont claires. Il suffit d'examiner les services pour lesquels elles sont prêtes à payer davantage ainsi que les activités qu'elles ne sont pas en mesure de gérer efficacement en interne. Ces résultats mettent en lumière les domaines dans lesquels les victimes peuvent se sentir particulièrement vulnérables.

Constatation clé : 91 % des victimes d'attaques sont prêtes à payer plus cher pour une expérience utilisateur simplifiée en matière de sécurité, contre 77 % des non-victimes

Par exemple, 91 % des victimes sont prêtes à payer plus pour une expérience utilisateur simplifiée pour la sécurité, contre 77 % de celles qui n'ont pas été touchées. Le chiffre moyen est de 88 %. Cela suggère que pour de nombreuses victimes, une erreur humaine ou une mauvaise configuration, toutes deux facilement déclenchées par des interfaces utilisateur complexes, a pu jouer un rôle dans l'attaque.

Les victimes sont également plus disposées à payer davantage pour des services de cyber-résilience tels que la planification d'une réponse aux incidents, la compréhension de la réglementation et de la conformité, et des recommandations stratégiques relatives aux services de sécurité. Les victimes sont donc prêtes à investir dans des domaines qui les préparent mieux à faire face et à se remettre de futures attaques.

En ce qui concerne les activités menées en interne ou externalisées, la même disparité est observée : les organisations qui n'ont pas été directement affectées par un incident sont plus susceptibles de penser qu'elles peuvent gérer les choses elles-mêmes.

Constatation clé : 81 % des victimes d'attaque prévoient d'externaliser la gestion et la sécurité cloud, contre 73 % des non-victimes

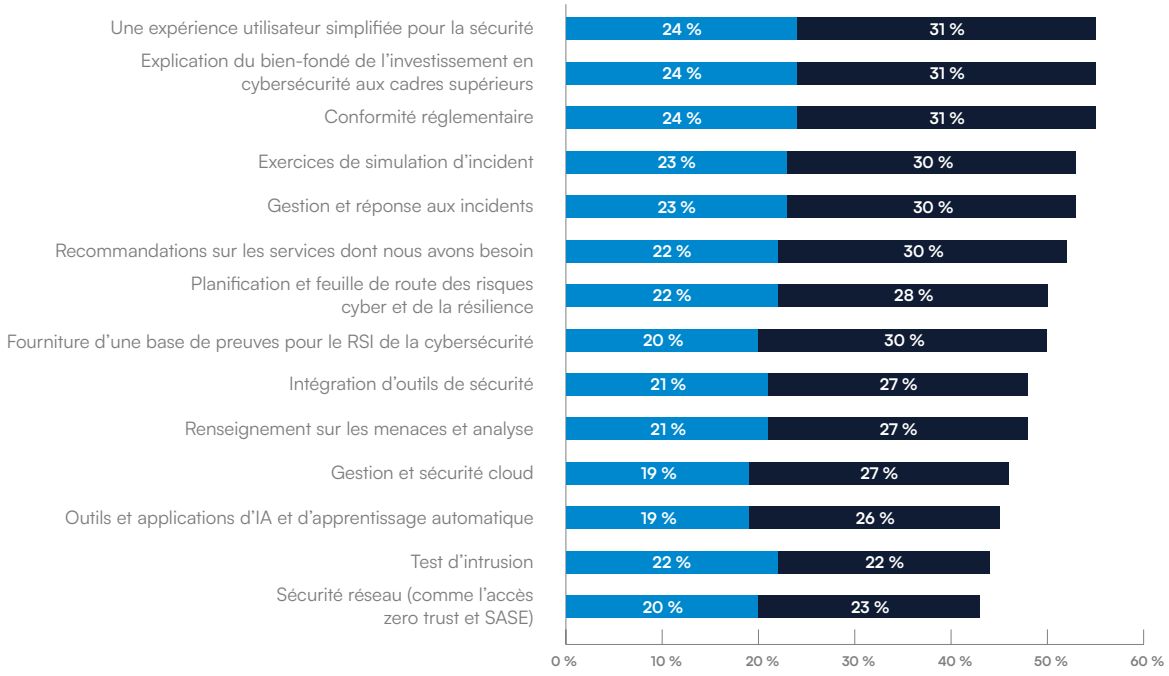

FIGURE 6

Les organisations qui prévoient de gérer chacun des aspects suivants en interne dans l'année ou les deux années qui suivent

n=2 000

- A subi une violation de la messagerie ou une attaque par ransomware réussie au cours de l'année écoulée
- N'a pas subi de violation de la messagerie ni d'attaque par ransomware réussie au cours de l'année écoulée

Conclusion

Les résultats montrent qu'en 2025, les MSP feront face à de nombreuses opportunités prometteuses, mais aussi à certains défis.

Par exemple, de nombreux clients souhaitent obtenir de l'aide pour gérer la prolifération des outils de sécurité. Cependant, aider plusieurs clients à gérer plusieurs produits peut rapidement devenir accablant pour les fournisseurs. Les fournisseurs de sécurité jouent un rôle crucial en aidant les MSP à intégrer les activités de gestion, de réponse et de reporting via des tableaux de bord centralisés et la consolidation des produits. De même, les fournisseurs peuvent aider les MSP à répondre à la demande manifeste de surveillance de sécurité 24/7 avec des SOC gérés.

Ensuite, il est nécessaire de soutenir les clients en matière de conformité et de réglementation, ainsi que dans la mise en œuvre d'outils et d'applications d'IA et d'apprentissage automatique.

En outre, les MSP doivent anticiper les besoins des clients qui souhaitent des services plus proactifs et prédictifs, tels que le suivi des menaces, la planification de la réponse aux incidents, la gestion des risques et le conseil stratégique.

Comme si cela ne suffisait pas, les MSP doivent également veiller à leur propre viabilité commerciale et fournir des preuves de leur expertise et de la fiabilité de leur modèle d'entreprise, sous peine de perdre des clients au profit de leurs concurrents. Cela nécessite un portefeuille de produits avancé et innovant, mais également facile à acheter, à déployer et à utiliser pour vos clients. Les fournisseurs de sécurité doivent également s'engager pleinement dans le partenariat.

Conclusion

Découvrez comment Barracuda peut vous aider

Chez Barracuda, nous nous engageons à 100 % auprès de notre réseau et de nos partenaires pour veiller à leur réussite et à leur développement.

BarracudaONE™

BarracudaONE est une plateforme de cybersécurité basée sur l'IA qui offre des produits intégrés accessibles à partir d'un tableau de bord centralisé afin de maximiser la protection et la cyber-résilience, tout en étant facile à acheter, à déployer et à utiliser.

La plateforme simplifie l'administration des outils de sécurité pour un MSP auprès de tous ses clients, en garantissant que les outils sont correctement configurés, que les alertes sont centralisées et que des rapports sont fournis pour montrer la valeur qu'un MSP apporte à ses clients en matière de sécurité.

BarracudaONE est disponible sans frais supplémentaires pour les MSP, les autres partenaires et les clients utilisant déjà Barracuda Email Protection, Barracuda Cloud-to-Cloud Backup et Barracuda Data Inspector. La plateforme offre une interface centralisée permettant aux MSP et aux partenaires de gérer facilement les solutions et les licences.

Barracuda Managed XDR™

Les MSP, partenaires et utilisateurs finaux peuvent renforcer davantage leur posture de sécurité avec Barracuda Managed XDR, un service 24/7 qui offre une détection et une réponse expertes aux menaces, soutenues par le SOC primé de Barracuda.

Barracuda en quelques mots

Barracuda est une entreprise mondiale de cybersécurité de premier plan qui fournit une protection complète contre les menaces complexes aux entreprises de toutes tailles. Notre plateforme basée sur l'IA sécurise les e-mails, les données, les applications et les réseaux grâce à des solutions innovantes, à un service XDR managé et à un tableau de bord centralisé afin d'optimiser la protection et de renforcer la cyber-résilience. Forte de la confiance de centaines de milliers de professionnels de l'informatique et de fournisseurs de services managés dans le monde entier, Barracuda propose des défenses puissantes, faciles à acheter, à déployer et à utiliser.

À propos de Vanson Bourne

Vanson Bourne est un cabinet indépendant spécialiste des études de marché pour le secteur des technologies. Sa réputation de produire des analyses solides, fiables et basées sur des études est elle-même fondée sur des principes rigoureux ainsi que sur sa capacité à interroger des décisionnaires majeurs qui occupent des fonctions techniques et métier dans tous les secteurs et sur les marchés principaux. Pour plus d'informations, accédez à vansonbourne.com.