



Le modèle MSP en toute simplicité

Pourquoi et comment ajouter
la sécurité à votre portefeuille

Kaspersky
United

Devenir un MSP, ou ajouter la sécurité à votre offre de services, est plus facile que vous ne le pensez

« Avec Kaspersky, nous avons un véritable avantage concurrentiel par rapport aux autres fournisseurs de services informatiques. Nous avons les clients, Kaspersky a les solutions, nous réunissons les deux, et il en résulte un grand succès. »

Erwin Hotting,
Directeur commercial,
Groupe Nemesys

Alors que de nombreux rapports mettent en évidence la croissance rapide à deux chiffres du marché mondial des services informatiques managés, et que la sécurité est le secteur qui connaît la croissance la plus rapide, que pensez-vous des opportunités que cela représente ?

Êtes-vous un revendeur informatique qui envisage de proposer pour la première fois une solution de sécurité par abonnement facile à vendre ? Vous êtes un distributeur à valeur ajoutée (VAR) et souhaitez améliorer votre offre de produits grâce à une sécurité primée à de nombreuses reprises ? Vous êtes un intégrateur de systèmes (SI) à la recherche d'une solution de sécurité en marque blanche à intégrer à vos produits matériels, logiciels, de stockage et de réseau existants ?

Si c'est le cas, il est plus facile que vous ne le pensez de devenir un fournisseur de services managés (MSP) avec Kaspersky.

Que faire si vous êtes un MSP expérimenté, à la recherche d'un partenaire de confiance qui ne vous donnera pas l'impression de recommencer à zéro lorsque vous ajouterez la sécurité à votre offre de services ? Ou d'une entreprise ayant une présence mondiale et l'expertise nécessaire pour vous guider afin de devenir un spécialiste des services de sécurité ?

Dans tous les cas, avec Kaspersky, il vous suffit de remplir un formulaire en ligne, de choisir votre distributeur local, et vous êtes prêt à vous lancer.

Alors, rendons le processus aussi facile que possible.

- Si vous êtes revendeur, VAR ou SI, vous trouverez des réponses simples à vos questions concernant les services managés (y compris la sécurité) dans notre introduction [aux avantages du modèle MSP](#).
- Si vous êtes un MSP expérimenté souhaitant simplement connaître les avantages de notre [programme MSP](#) primé et de notre [sécurité conçue pour les MSP](#), vous pouvez passer directement à ces sections.
- Quelle que soit votre activité, nous espérons que vous trouverez ce guide utile et instructif, et nous sommes déjà impatients de vous compter parmi les membres de notre [famille MSP](#).





MSP : de quoi s'agit-il ?

Si vous êtes nouveau sur le marché, les MSP sont généralement des spécialistes informatiques qui gèrent à distance et de manière proactive un ou plusieurs aspects de l'infrastructure informatique d'un client dans le cadre d'un abonnement.

Profil du client type

Les MSP sont principalement sollicités par les petites et moyennes entreprises (PME) dont les capacités informatiques internes sont limitées et qui considèrent l'offre de services d'un MSP comme le meilleur moyen de bénéficier d'une expertise informatique.

Les grandes entreprises peuvent également faire appel à des MSP, par exemple si elles sont confrontées à des contraintes budgétaires, à des restrictions en matière de recrutement ou si elles ne parviennent tout simplement pas à trouver du personnel qualifié pour compléter leur équipe informatique interne.

Dans les deux cas, le modèle d'abonnement MSP offre aux clients de toutes tailles l'avantage d'avoir accès à des ressources qualifiées et à des coûts d'assistance informatique prévisibles. De plus, comme les MSP adoptent une approche proactive, ils sont en mesure de prévenir l'apparition de problèmes informatiques et la perturbation des opérations commerciales.

Pour répondre à ces besoins, un MSP doit généralement :

- Fournir des services informatiques aux clients en échange d'un abonnement mensuel.
- Servir principalement les clients des PME.
- Fournir des services sur un modèle d'abonnement qui permet aux clients de les comptabiliser sous forme de dépenses d'exploitation (OpEx) plutôt que de dépenses d'investissement (CapEx).
- Permettre de faire évoluer ou de restreindre les licences des clients, sans que ceux-ci aient à s'engager sur des quantités minimales ou des périodes prolongées.
- Utiliser des outils d'automatisation tels que Remote Monitoring and Management (RMM) et Professional Services Automation (PSA), pour simplifier et gérer la prestation de services.

Opportunité du marché MSP

Selon une étude publiée par [Research and Markets](#), le marché mondial des services managés devrait atteindre 731 milliards de dollars d'ici 2030, avec un TCAC de 13,4 %.

En particulier, le segment de la sécurité managée devrait enregistrer le TCAC le plus élevé au cours de la période de prévision, grâce à l'adoption croissante des services de sécurité managés et en raison d'avantages comme la surveillance et la gestion de la sécurité, la gestion des menaces par email, la gestion de la restauration et des sauvegardes, ainsi que la gestion de l'assistance et de la maintenance.

Ces résultats sont amplifiés par les recherches de Kaspersky¹, selon lesquelles les principales raisons de faire appel à des MSP / fournisseurs de services de sécurité managés (MSSP) sont les suivantes : besoin d'expertise spécialisée (52 %), efficacité financière (50 %), respect des exigences de conformité (49 %), efficacité dans la fourniture de solutions de cybersécurité (45 %) et évolutivité (44 %).

¹ Source : Focus sur le marché des MSP en 2021

Qu'est-ce que vous y gagnez ?

Tout le monde veut participer à un marché qui connaît une croissance rapide de plus de 13 %, et l'utilisation de la sécurité comme un moyen d'y parvenir rend la proposition encore plus attrayante. Si vous êtes actuellement un revendeur ou un VAR, quelle différence le passage au statut de MSP pourrait-il faire pour votre entreprise ?

Si vous êtes un **revendeur**, vous vous concentrez probablement sur la recherche et la personnalisation de produits pour répondre aux besoins de projets particuliers, et sur la mise à disposition d'une assistance réactive (dépannage), à laquelle peuvent s'ajouter des services professionnels facturés à l'heure. La marge brute est susceptible de s'élever à environ 50 %, tandis que les chiffres de Kaspersky indiquent que 34 % de vos clients vous feront confiance sur le long terme.

Si vous avez fait évoluer votre activité vers le statut de **VAR**, vous avez probablement consolidé vos outils et fait évoluer vos contrats vers un modèle proactif générant des revenus récurrents. Par conséquent, vous générerez un bénéfice brut d'environ 50 à 75 %, tandis que nos chiffres suggèrent que 53 % de vos clients seront des clients fidèles.

Que se passe-t-il donc si vous faites passer votre entreprise au niveau supérieur en proposant la surveillance, l'automatisation et la sécurité selon un modèle forfaitaire, et en agissant comme un conseiller de confiance et/ou un CIO virtuel ? En tant que **MSP**, vous pourriez augmenter encore plus votre marge brute, et nous prévoyons que 63 % de vos clients seront des clients fidèles.

Vous bénéficierez donc d'une combinaison de revenus récurrents prévisibles, d'une rentabilité plus élevée et, en offrant une plus grande valeur ajoutée, d'une meilleure rétention des clients existants et de la possibilité d'attirer davantage de nouveaux clients. En outre, avec les bons outils, vous serez en mesure d'économiser du temps et des ressources en normalisant et en gérant tous les clients à partir d'une seule console. Alors, comment ne pas y trouver son compte ?

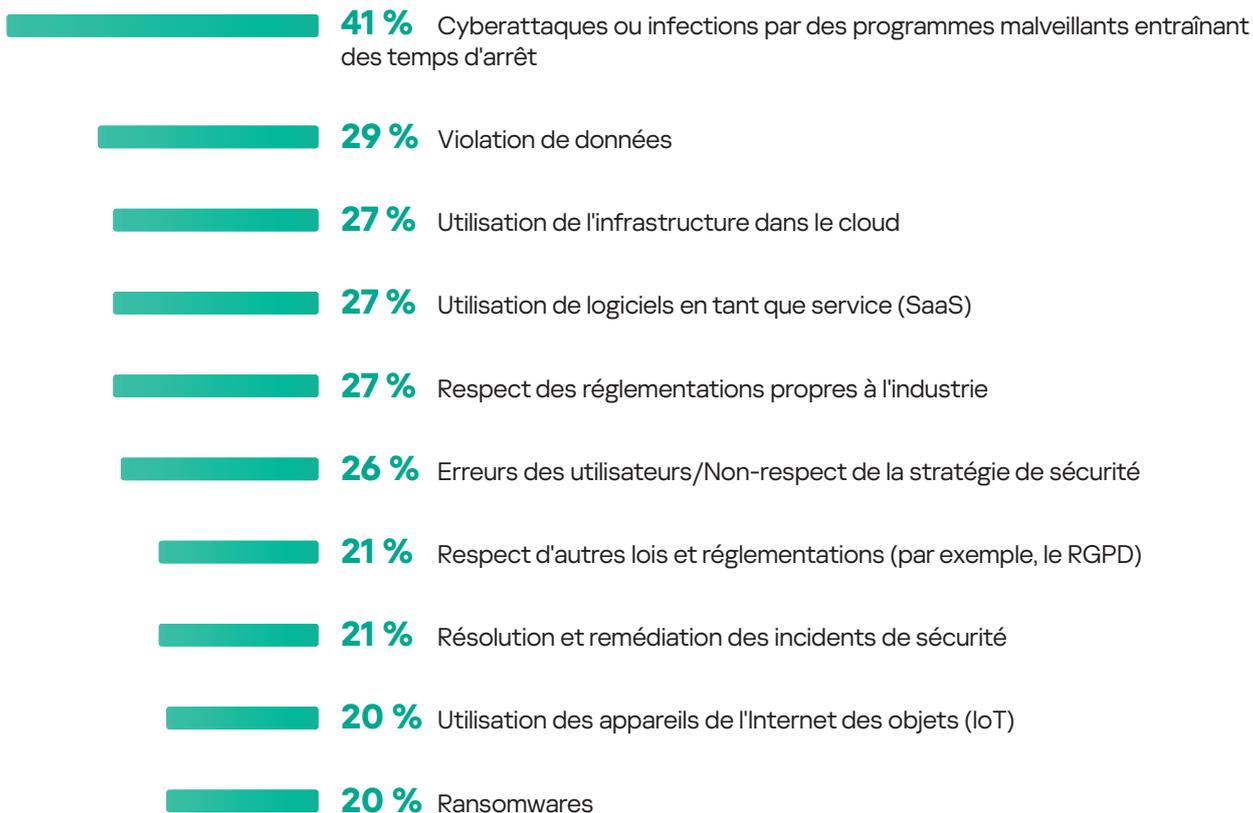


Que recherchent les clients ?

En supposant que ces chiffres soient suffisamment convaincants pour que vous envisagiez de vous lancer dans les services managés, quelles sont les attentes des clients potentiels vis-à-vis d'un MSP ?

Dans notre rapport, [Focus sur le marché des MSP en 2021](#), nous nous sommes entretenus avec une variété de MSP, allant des fournisseurs de services informatiques traditionnels et des grandes entreprises de services informatiques à des MSP et MSSP hautement automatisés.

Lorsque nous leur avons demandé quels étaient les trois principaux défis non résolus en matière de sécurité informatique auxquels leurs clients étaient confrontés, les réponses les plus souvent mentionnées étaient les suivantes :



Cela représente beaucoup de possibilités pour les MSP qui offrent des services de sécurité pour résoudre les problématiques les plus difficiles de leurs clients.



Pourquoi la sécurité correspond au modèle MSP

Cette brève introduction devrait vous permettre de comprendre pourquoi, si vous envisagez de proposer des services managés, la sécurité est un excellent point de départ.

Pour résumer :

- Le marché mondial des services managés devrait atteindre 731 milliards de dollars d'ici 2030, avec un TCAC de 13,4 %.
- La cybersécurité est actuellement le secteur qui connaît la croissance la plus rapide.
- La sécurité est parfaitement adaptée au modèle d'abonnement privilégié par les MSP.
- Les avantages de proposer des services de sécurité en tant que MSP incluent des revenus récurrents prévisibles, une rentabilité plus élevée et, en offrant une plus grande valeur ajoutée, une meilleure rétention des clients et la possibilité d'attirer davantage de nouveaux clients.

Il n'est donc pas surprenant que 93 % des MSP cherchent à étendre leur offre de sécurité informatique².

Maintenant que nous avons aiguisé votre appétit, il ne vous reste plus qu'à identifier un fournisseur disposant d'un programme MSP primé et d'une gamme de produits de sécurité conçue pour les MSP.

Le programme MSP primé de Kaspersky

Dan Driezen
Devis fourni par ESW IT Business
Advisors

Kaspersky a reçu le prix du meilleur programme de partenariat de services managés (MSP) dans le cadre des MSP Innovation Awards Europe de Channel Partner Insight en 2020. En 2020 et 2021, Canalys nous a reconnu 'Champion' en matière de gestion des partenaires dans sa Global Cybersecurity Leadership Matrix. Nous avons donc une connaissance approfondie des défis auxquels sont confrontés les MSP et de la meilleure façon de les relever.

Les défis des MSP

Dans notre rapport [Focus sur le marché des MSP en 2021](#), lorsque nous avons enquêté sur les trois principaux défis des MSP, ceux qui ont été le plus souvent mentionnés sont la concurrence des autres fournisseurs de services (32 %), les clients et utilisateurs exigeants (30 %), la recherche de nouveaux clients (30 %), le maintien de la rentabilité (29 %), et le fait d'attirer et de retenir le personnel (28 %).

Toutefois, si ces défis sont typiques de la plupart des entreprises, les autres défis de la liste sont beaucoup plus spécifiques.

Il s'agit de la complexité des solutions que nous proposons (21 %), des relations avec les fournisseurs / distributeurs (18 %), de la tendance à adopter l'infrastructure dans le cloud (17 %), du maintien de la sécurité des données dans l'infrastructure de plus en plus distribuée de nos clients (15 %), et du trop grand nombre de systèmes / plateformes distincts impliqués pour servir efficacement les clients (14 %).

Parmi les autres besoins généraux des MSP, citons le paiement détaillé avec un budget OpEx (service mensuel), la possibilité d'ajouter ou de supprimer des clients ou de modifier les conditions, la capacité de gérer plusieurs produits à partir d'une seule console multi-clients pour la montée en gamme et la collaboration avec les clients, l'automatisation des processus, de la gestion des licences à l'exploitation des produits, l'intégration avec des outils tels que RMM/PSA, la production de rapports détaillés et l'aide à l'intégration des nouveaux clients (y compris la formation et le marketing).

Que vous soyez un débutant ou un MSP chevronné, toutes ces questions, ces capacités et la manière dont les fournisseurs les abordent valent la peine d'être prises en compte lors du choix de votre partenaire de sécurité.

² Source : Focus sur le marché des MSP en 2021

Ce que les MSP attendent des fournisseurs de sécurité

Pour les aider à faire face aux problèmes décrits ci-dessus, notre rapport a révélé que les trois principaux critères que les MSP recherchent auprès des fournisseurs de logiciels de sécurité informatique sont les suivants :



Comment notre programme MSP répond à ces besoins

L'approche MSP de Kaspersky repose sur trois piliers :

- **Solutions et expertise** : nous fournissons un portefeuille complet avec un support premium et des intégrations avec les principales plateformes RMM et PSA.
- **Licensing simple et flexible** : avec des abonnements mensuels, des remises sur les licences agrégées et une facturation à l'utilisation.
- **Facilité d'accès** : pas d'investissement initial, pas de contrat, pas d'exigences minimales en matière de licence, et des responsables commerciaux dédiés pour vous accompagner tout au long de votre parcours en tant que MSP.

Des possibilités financières et de développement flexibles

- Une tarification par niveau agrégée pour les abonnements mensuels. Plus vous vendez, plus les tarifs baissent.
- Facturation selon le principe du paiement à l'utilisation pour les abonnements mensuels et facturation annuelle pour les abonnements annuels.
- Les statuts partenaires Gold, Silver et Platinum vous permettent de bénéficier de marges toujours plus importantes.
- Profitez de nombreuses opportunités de ventes croisées et de montée en gamme sur l'ensemble des produits Kaspersky.

Les avantages de notre modèle d'abonnement

- Transformez les dépenses d'investissement (CapEx) en dépenses d'exploitation (OpEx) sans engagement ni investissement initial, et en revenus mensuels récurrents prévisibles pour assurer une budgétisation et des prévisions plus précises.
- La gestion flexible des licences vous permet d'évoluer à la hausse ou à la baisse grâce au paiement à l'utilisation, de répondre à la demande des clients et d'ajouter rapidement de nouvelles technologies.
- Un seul code d'activation réduit à jamais les frais d'administration.
- Attirez plus de clients plus rapidement et augmentez leur fidélité en leur permettant de payer uniquement pour les fonctionnalités dont ils ont besoin (pas de frais initiaux), en vous adaptant mieux à leurs demandes (augmentation de la valeur) et en réduisant le taux de résiliation grâce à un engagement continu.

Rentabilité accrue

- Enrichissez votre offre de services grâce à notre portefeuille de solutions.
- Augmentez votre revenu par client grâce à nos nombreuses opportunités de vente croisées et de montée en gamme.
- Profitez de meilleures marges et de remises sur les facturations agrégées (augmentez vos revenus sans effort supplémentaire).

Amélioration de la productivité

- Simplifiez la gestion et les opérations au quotidien grâce aux consoles de produit conçues pour les MSP et à l'intégration avec des solutions tierces.
- Réduisez vos frais de gestion en utilisant un fournisseur de solutions de sécurité unifié.

« Nous sommes conscients qu'une entreprise multinationale comme Kaspersky, leader mondial de la cybersécurité, se soucie réellement de notre activité et souhaite travailler en étroite collaboration avec nous pour nous aider à réussir. »

Brian Oleksiuk
Président et fondateur
Oxygen Technologies

Gestion facile des licences

Vous pouvez commander des licences d'abonnement Kaspersky via la marketplace de votre distributeur ou notre portail LMP (License Management Portal), qui vous permet également de :

- Gérer les clients, les licences, les commandes et les factures via un tableau de bord centralisé.
- Choisir une facturation mensuelle selon le principe du paiement à l'utilisation ou un abonnement annuel, ou un mélange des deux.
- Suivre en temps réel l'utilisation et la consommation des licences.
- Essayer de nouveaux produits et repérer les possibilités de vente incitative mises en évidence par les rapports sur l'utilisation des clients.
- Utiliser le même ensemble d'identifiants sur tous les portails Kaspersky, y compris le portail partenaires, le LMP et les consoles de nos produits.
- Simplifier la commande de licences, la gestion et la création de rapports pour les revendeurs axés sur les abonnements, notamment les fournisseurs de services cloud (CSP), les fournisseurs d'hébergement et les revendeurs SaaS.

Support technique rapide

- Support technique Standard ou Premium pour limiter les interruptions de service.
- Responsable commercial dédié et spécialisé, prêt à vous faire bénéficier de son expertise.
- Vos problèmes les plus critiques résolus en priorité.
- En nous rejoignant, vous bénéficiez du support Premium pour cinq incidents.

Support et formation commerciale

- Processus d'intégration automatisé, rapide et efficace.
- Webinars sur la vente en ligne, la formation technique ou les produits, pour transformer votre équipe en professionnels de la cybersécurité.
- Un large éventail de ressources, y compris des produits dédiés et des documents de marketing, une direction de réflexion et des comparatifs concurrentiels.



Sécurité optimisée pour les MSP

Par où voulez-vous commencer ?

« Il est important pour moi de rester dans le niveau d'élite du programme Kaspersky MSP parce que j'apprécie la possibilité d'avoir un accès anticipé aux nouveaux produits et aux nouvelles idées, de tester les nouvelles technologies et d'être impliqué dans le processus de création et de commentaires. »

Martin Dubreuil

Directeur des services de consultance
B2B Cyber Secure

Les sections ci-dessus devraient vous avoir donné une idée claire des opportunités offertes par le marché des MSP et de la manière dont notre programme MSP primé vous aide à en tirer le meilleur parti. Mais que faire si vous n'avez jamais vendu de solutions de sécurité auparavant ? Par où commencer ?

Admettons que vous fournissez actuellement des services informatiques répondant aux besoins de vos clients en matière de réseau, d'infrastructure, de service d'assistance, de sauvegarde, de reprise après sinistre, etc., et que vous utilisez des outils d'automatisation tiers comme RMM et PSA. Supposons également que vous ne disposez d'aucune expertise interne en matière de sécurité informatique (qu'elle soit technique ou commerciale), que vous êtes à court de ressources (matériel, personnel ou temps) et que vous cherchez donc à ajouter des services de sécurité sans difficulté.

Nos services de sécurité fondamentaux offerts par les MSP vous permettent de vous lancer dans des services simples et prêts à l'emploi, axés sur la sécurité des terminaux, des messageries, de Microsoft Office 365, etc. Ils reposent sur des profils de sécurité par défaut et des pratiques exemplaires, s'intègrent à des outils d'automatisation tiers et vous permettent de fournir des services de sécurité autonomes basés sur des fonctionnalités intégrées avancées.

Non seulement ils sont faciles à commercialiser, à vendre et à gérer, mais ils vous offrent également une base solide pour développer vos propres services de prestation, accroître votre activité et gravir les échelons de notre programme MSP.

Kaspersky Endpoint Security Cloud et Kaspersky Endpoint Security for Business

Notre gamme de produits **la plus testée et la plus récompensée** répond aux besoins des clients B2B, allant des plus petites micro-entreprises aux plus grandes entreprises mondiales. Deux de nos produits sont particulièrement bien adaptés aux besoins des MSP : Kaspersky Endpoint Security Cloud et Kaspersky Endpoint Security for Business. Alors, quelle est la meilleure solution pour vous et vos clients ?

Kaspersky Endpoint Security Cloud

- Tire parti de notre Business Hub natif du cloud pour offrir une sécurité reposant sur le modèle SaaS et ne nécessitant aucun investissement en capital.
- Capable d'être géré par des informaticiens, sa simplicité et l'automatisation des services vous offrent un moyen idéal de vous lancer dans la sécurité informatique.
- Assure la gestion de 5 à 1 000 nœuds, y compris la mise en place de profils de sécurité multi-clients et conformes aux bonnes pratiques.
- Offre une protection de nouvelle génération des terminaux pour les ordinateurs de bureau, les serveurs et les appareils mobiles, des technologies telles que la protection contre les ransomwares et la protection de la messagerie, ainsi que des options telles que la gestion des correctifs, le chiffrement, la découverte du Shadow IT, la protection de Microsoft Office 365, la lutte contre le phishing et les programmes malveillants et bien plus encore.
- Trois niveaux sont disponibles : Cloud, Cloud Plus et Cloud Pro.



Kaspersky Endpoint Security for Business

- Idéal pour les MSP ayant des clients plus importants et des exigences de conformité plus élevées.
- Utilise Kaspersky Security Center pour fournir des options SaaS ou sur site, y compris la gestion avancée, les rapports et les tableaux de bord.
- Multi-location avancée et personnalisation des services, des services de base aux services avancés, y compris la sécurisation des infrastructures hybrides.
- Offre une protection de nouvelle génération des terminaux pour les ordinateurs de bureau, les serveurs et les appareils mobiles, une protection contre les ransomwares et bien plus encore.
- Deux niveaux sont disponibles – Select et Advanced.
- Les intégrations supplémentaires facultatives comprennent la protection des charges de travail dans le cloud (public et privé), la détection et la réponse aux incidents (EDR), la recherche des menaces et la réponse aux incidents managés (MDR).

Rebranding et marque blanche

Ces deux solutions offrent des possibilités de rebranding MSP ou de marque blanche, incluant votre propre logo, nom, schéma de couleurs, etc.

Intégration aux outils RMM et PSA

Afin de s'assurer qu'ils sont conçus pour les MSP, Kaspersky Endpoint Security Cloud et Kaspersky Endpoint Security for Business s'intègrent tous deux aux outils RMM et PSA.

- Les outils RMM permettent l'automatisation, la gestion et le contrôle à distance de l'infrastructure informatique, notamment la gestion des terminaux, la surveillance et les alertes, la gestion des correctifs, l'exécution de scripts, la sauvegarde, la reprise après sinistre et (en option) un antivirus géré. Il n'est donc pas surprenant que 70 % des MSP utilisent des RMM pour automatiser la gestion des terminaux et de l'infrastructure de leurs clients³.
- Les outils PSA permettent aux MSP d'automatiser des activités, comme la gestion des contrats et des ressources, la facturation, le flux de travail des tickets et le service d'assistance, les capacités CRM, les rapports et les analyses.

Les intégrations RMM de Kaspersky comprennent un tableau de bord de sécurité centralisé, le déploiement automatisé d'agents à distance, l'analyse automatique des virus et la mise à jour des bases de données pour des outils comme ConnectWise Automate, N-able N-central et N-able N-sight RMM.

Nos intégrations PSA comprennent la facturation et les rapports automatisés, la création automatique de tickets, la fermeture à la fin des opérations et une facture unique pour tous les services (y compris la sécurité) pour des outils comme ConnectWise Manage®.

³ Source : Focus sur le marché des MSP en 2021

Possibilités d'améliorer et d'élargir vos offres

La gamme de produits Kaspersky couvre tous les domaines, de la sécurité des petites entreprises à la détection et à la réponse étendues (XDR), en passant par la cybersécurité industrielle et la formation automatisée de sensibilisation à la sécurité.

Pour faciliter au maximum le positionnement, la vente et la prise en charge de ces solutions au fur et à mesure que vous progressez en tant que MSP, nous avons adopté une approche de la cybersécurité par étapes.

Il s'agit de préciser quel niveau de sécurité et quelles solutions spécifiques conviennent le mieux à une organisation particulière. Ces étapes fournissent un ensemble de mesures de protection contre les menaces faciles à gérer, se coordonnant en toute transparence entre elles, et offrent une feuille de route de la cybersécurité assurant en douceur la transition d'un niveau de maturité de sécurité informatique vers un autre le moment venu.

Notre approche de la cybersécurité par étapes comprend ce qui suit :

- **Kaspersky Security Foundations** : protection de base essentielle automatisée et basée dans le cloud pour tous les appareils, infrastructures VDI et serveurs hybrides, avant que les organisations progressent en douceur vers...
- **Kaspersky Optimum Security** : pour les organisations qui ont besoin d'une sécurité plus spécialisée contre des menaces très complexes, avant de mettre en œuvre sans effort notre troisième niveau...
- **Kaspersky Expert Security** : pour les entreprises disposant d'équipes de sécurité informatique matures luttant contre les attaques ciblées les plus complexes.

1. Inscrivez-vous sur partners.kaspersky.com
2. Sélectionnez un distributeur dans votre région
3. Commencez à passer vos commandes sur le LMP ou sur la marketplace de votre distributeur
4. Complétez la formation commerciale et technique dédiée aux MSP au cours du délai de grâce de 90 jours

5. Bienvenue à bord !

Vous êtes prêt ?

Si vous êtes un revendeur, un VAR ou un SI, vous cherchez à vendre le plus rapidement et le plus facilement possible. Et si vous êtes un MSP chevronné, l'une des nombreuses tâches que vous maîtrisez mieux que quiconque est la vente et la prestation de services managés. Alors, pourquoi le domaine de la sécurité devrait-il être différent ?

Malgré ce que vous pouvez lire ou entendre, ajouter des solutions de sécurité à votre portefeuille n'est pas difficile. Cet ajout ne doit pas non plus (à moins que vous ne le souhaitiez) vous obliger à vous plonger dans les besoins détaillés de vos clients en matière de sécurité, à participer à des formations ou à passer du temps que vous n'avez pas pour vous tenir au courant des subtilités du portefeuille de produits d'un fournisseur.

En effet, tout partenaire qui fournit des services managés et support client de première ligne peut devenir partenaire MSP Kaspersky. Grâce à nos solutions de sécurité conçues pour les MSP, vous êtes déjà [prêt à vous lancer](mailto:misp@kaspersky.com).

Pour toute question,
veuillez nous contacter
à l'adresse suivante :
misp@kaspersky.com