APOG

01 40 64 93 93

Solution de sécurité informatique

CRÉATION DE SERVICES DE CYBER SÉCURITÉ : FEUILLE DE ROUTE

F-Secure

01 40 64 93 93

Solution de sécurité informatique

Les cyber menaces ne cessent de gagner en complexité. Les entreprises doivent pouvoir compter sur un partenaire capable de les protéger. Le moment est venu d'intégrer à votre offre des services de sécurité managés. Ces derniers constituent désormais un atout indispensable à votre succès.

À l'heure actuelle, les entreprises de toutes tailles et de pratiquement tous les secteurs d'activité font face à des difficultés inédites. Le travail à distance est en pleine expansion et les employés sont désormais actifs en dehors du périmètre de sécurité de leur organisation. Malgré tout, les entreprises s'efforcent d'assurer leur sécurité. Le défi est de taille, à une heure où les cyber criminels élaborent des attaques toujours plus sophistiquées, plus organisées, plus dynamiques.

En intégrant à votre offre des services de cyber sécurité managés, vous pourrez apporter aux entreprises la sécurité et la flexibilité dont elles ont besoin, tout en vous assurant des revenus réguliers. La mise en place de ces services peut exiger certains efforts : ils supposent de nouvelles compétences, des connaissances approfondies et des méthodes de travail différentes. Heureusement, vous n'avez pas à relever ces défis seul : nous pouvons vous aider.

Nous avons élaboré ce guide pour partager avec vous les résultats de notre dernière étude de marché et pour vous présenter les différents aspects à prendre en compte lorsque vous créez une offre de services de cyber sécurité managés. À la fin de ce document, vous trouverez un lien vers un atelier gratuit consacré à la conception de ces services.

LES SERVICES SONT INCONTOURNABLES : POUR VOS CLIENTS, COMME POUR VOUS

Jusqu'à récemment, la cyber sécurité n'était perçue que comme une simple assurance sur l'avenir. Désormais, elle constitue une priorité, non seulement pour les équipes informatiques mais aussi pour les cadres dirigeants qui y voient un outil permettant d'accroître la valeur de l'entreprise. Ils attendent une cyber sécurité plus performante, plus complète. Et, dans le contexte de la pandémie, leur demande s'est faite plus pressante encore.

À l'ère du Covid-19, les cyber menaces évoluent encore plus rapidement. Pour faire face à la multiplication des cyber attaques ciblant les entreprises de toutes tailles et de tous les secteurs, la demande en personnel de sécurité a connu une très nette augmentation[1]. Et de nombreuses organisations éprouvent des difficultés à recruter et à garder auprès d'elles les experts qualifiés dont elles ont besoin pour gérer efficacement leur cyber sécurité. Actuellement, le secteur compte plus de quatre millions de postes vacants, avec très peu d'experts pour les pourvoir. La plupart des entreprises disposent certes d'équipes informatiques travaillant sur la cyber sécurité... mais peu d'entre elles sont capables de détecter les attaques et - plus important encore - d'y répondre. Résultat : le besoin d'un accompagnement à la fois souple et spécialisé devient urgent.

En externalisant une partie ou la totalité de leur cyber sécurité auprès d'un fournisseur de services managés (MSP) ou d'un fournisseur de services de sécurité managés (MSSP), les entreprises peuvent accéder à l'expertise de spécialistes possédant une vision globale des cyber menaces. Ces professionnels s'appuient en effet sur une vaste expérience acquise auprès de nombreux clients, sur divers scénarios d'attaque. Ce choix de l'externalisation constitue, par ailleurs, une option plus rapide et plus abordable que la constitution d'une équipe en interne.

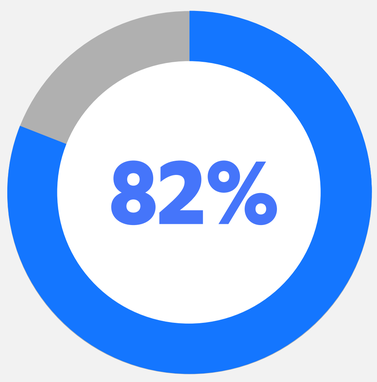
Il n'est donc pas étonnant que, d'après nos dernières recherches, 65 % des moyennes et grandes entreprises externalisent déjà au moins une partie de leurs opérations de sécurité... et que 82 % recherchent un partenaire de sécurité capable de leur fournir toutes les solutions, l'expertise et les services dont elles ont besoin. Selon Gartner, d'ici 2025, les plateformes de protection des endpoints et les solutions de détection et de réponse proposées en SaaS ou services cloud constitueront un choix privilégié pour 75% des nouveaux déploiements[2].

Le passage au cloud, la digitalisation, le souci des réglementations et la pandémie mondiale sont autant de facteurs qui poussent les entreprises à rechercher de nouveaux outils, de nouvelles perspectives et de nouvelles

méthodes de travail. Dans cette perspective, elles acquièrent des solutions issues d'un large éventail de fournisseurs.

Parallèlement, le modèle traditionnel de la cyber sécurité sous licence devient obsolète. Ce système contraint les entreprises à acquérir un nombre de licences correspondant aux pics de consommation, et à réaliser ces investissements en amont. Un tel fonctionnement n'est pas adapté au contexte actuel, marqué par les difficultés liées à la pandémie. Par ailleurs, le concept de licence logicielle ne permet pas de mener facilement un processus continu d'amélioration de la cyber résilience.

Une approche plus souple, basée sur un modèle par abonnement, devient nécessaire. En intégrant des services à votre offre actuelle, vous serez en mesure de répondre aux besoins de vos clients tout en faisant prospérer votre propre entreprise. Cela étant, il est compréhensible que le passage à un modèle de services puisse vous paraître compliqué et fastidieux. Mais vous n'êtes pas seul. F-Secure est là pour vous accompagner.

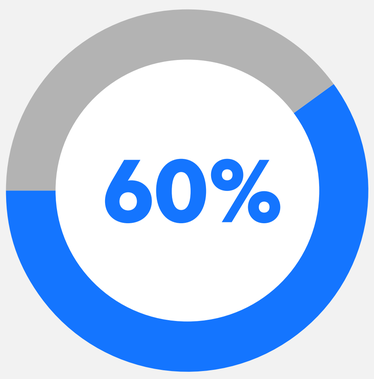


des entreprises recherchent une solution de sécurité tout-en-un.

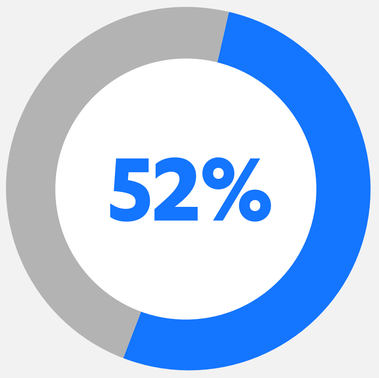
43% préféreraient utiliser un système de sécurité de référence ou un fournisseur de services couvrant la plupart des besoins, tout en conservant, pour certaines fonctions spécifiques, les meilleurs solutions de leur catégorie.

39% souhaiteraient s'appuyer sur un système de sécurité ou sur un fournisseur de services « tout-en-un » couvrant tous leurs besoins en matière de sécurité informatique/réseaux.

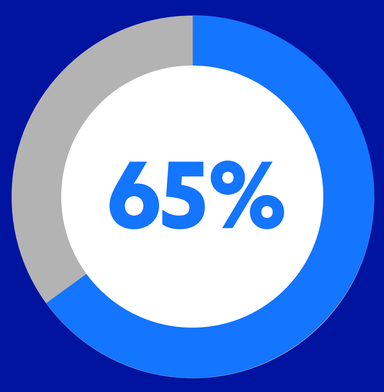
12% préfèrent sélectionner les meilleures solutions de sécurité dans chacune des catégories.



des entreprises considèrent leur fournisseur de services ou leur revendeur comme un partenaire clé en matière de sécurité.



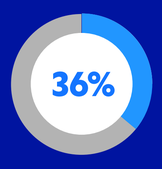
des entreprises disposent d'une équipe interne de sécurité informatique.



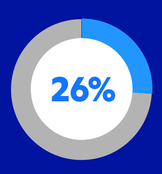
des entreprises recourent à des services rattachés à leurs solutions de sécurité

35% n'utilisent que des produits gérés en interne

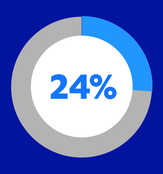
22% n'utilisent que des services managés ou externalisés



invoquent la disponibilité 24h/24 et 7j/7 du service



invoquent la stratégie organisationnelle d'utilisation du service



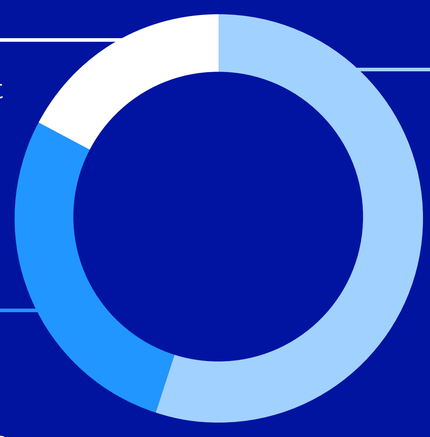
invoquent un manque d'expertise en interne

17%

Nous travaillons directement avec un fournisseur de solutions de sécurité (marque de sécurité) qui nous fournit ses services

28%

Nous travaillons avec un fournisseur de services informatiques managés/MSP



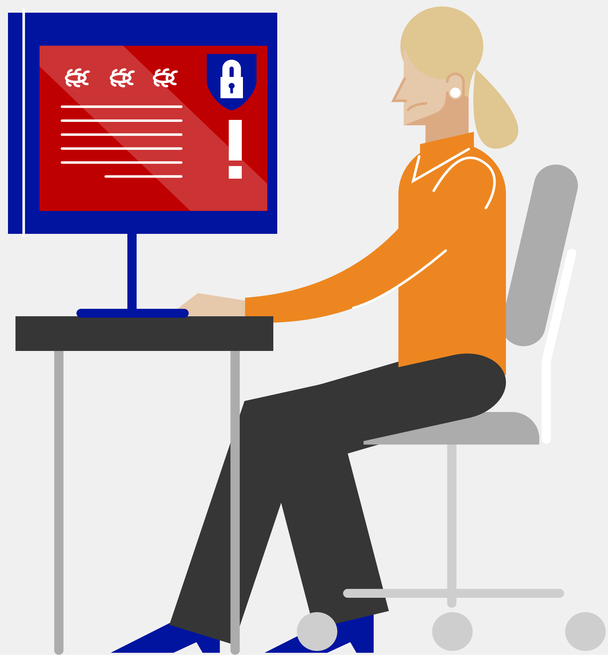
55%

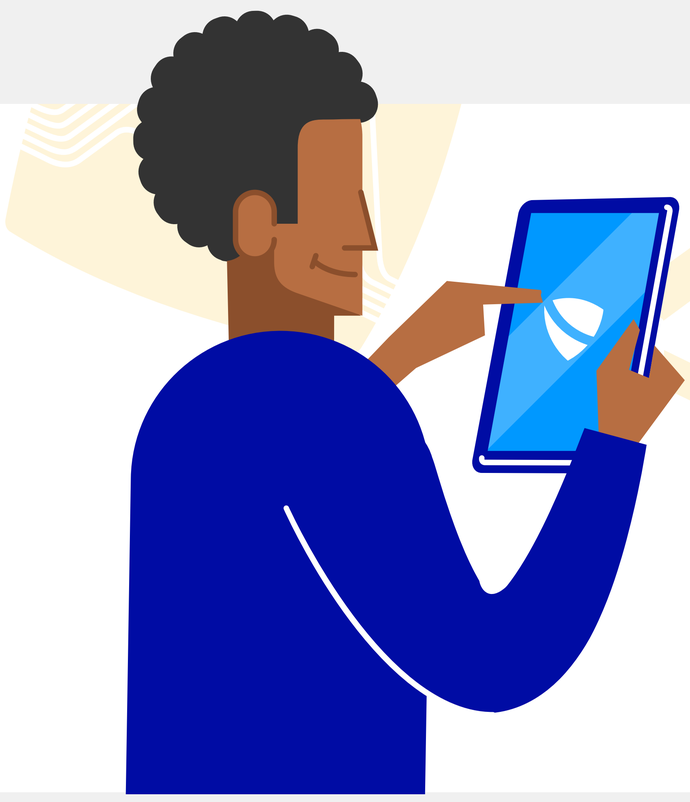
Nous travaillons avec un fournisseur de services de sécurité managés/MSSP

LES 5 INGRÉDIENTS D'UNE OFFRE DE SERVICES DE CYBER SÉCURITÉ RÉUSSIE

1. MATURITÉ DU MARCHÉ ET PRISE DE CONSCIENCE

Actuellement, au moins la moitié des entreprises souhaitent opter pour la cyber sécurité « as-a-service » ou bien acquérir des services en plus des produits déjà en leur possession. Elles entendent ainsi accéder à une expertise spécialisée, à un haut niveau de flexibilité et à la possibilité d'accroître leurs propres compétences. Au moment de choisir leur partenaire, elles ont tendance à rechercher des contrats clairs, des options de produits flexibles, une véritable expertise et la capacité d'adapter ces services à leurs besoins spécifiques. La protection contre les malwares et les ransomwares est essentielle mais les clients veulent également que ces services soient capables de sécuriser leurs solutions cloud et d'assurer une détection-réponse rapide face aux attaques.





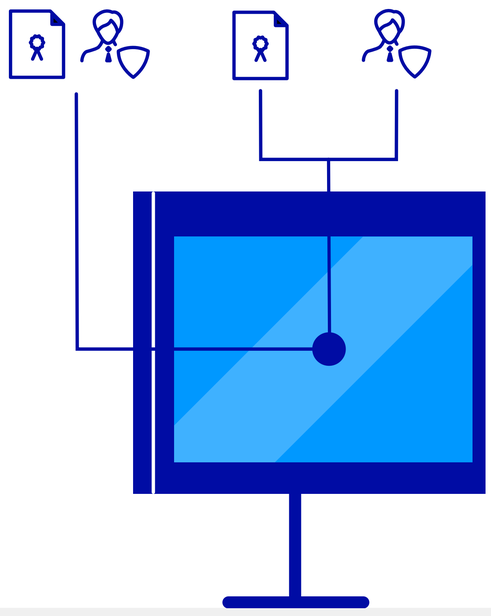
2. DÉFINITION DU SERVICE ET ACCORD DE NIVEAU DE SERVICE (SLA)

Sur le segment du marché mid-market, ces services sont bien souvent proposés sur la base d'une redevance mensuelle. Cet abonnement inclut généralement la détection, le signalement (qu'une attaque ait eu lieu ou non), la maintenance technologique et les mises à jour. La réponse est facturée séparément, en fonction du temps et des actifs concernés, car il est impossible d'anticiper la quantité de travail et de moyens nécessaires à la neutralisation d'une attaque. L'accord de niveau de service (SLA) standard du marché mid-market correspond généralement aux heures de bureau, avec un temps de réponse de deux heures. Les modèles de SLA 24h/24, 7j/7, suscitent toutefois un intérêt croissant, notamment auprès des grandes entreprises.

3. RESSOURCES, COMPÉTENCES, PROCESSUS

Le fonctionnement de tels services suppose de mobiliser des ressources. Si vous disposez à la fois d'un service d'assistance et d'une équipe de sécurité, les collaborateurs du service d'assistance pourront se charger de la sécurité informatique de base et de la détection des faux positifs. Lorsqu'un cas plus complexe sera détecté, ils pourront créer un ticket pour transmettre le dossier à l'équipe de sécurité, dotée d'une expertise plus poussée et d'une meilleure connaissance des produits utilisés. Notre programme de formation destiné aux partenaires repose sur des parcours professionnels spécialisés, pour vous aider à faire de vos employés de véritables experts en sécurité. Pour un SLA correspondant aux heures de bureau, la quantité de ressources nécessaires reste étonnamment faible, même pour la gestion d'environnements de grande envergure. Une équipe de seulement deux experts peut gérer en moyenne 45 000 hôtes touchés par mois. Et si votre équipe a besoin de renfort sous la forme d'analyses approfondies des menaces ou de conseils d'experts, nous sommes là pour vous aider. Face aux cyber incidents les plus délicats, notre solution dispose d'une fonctionnalité unique intégrée appelée « Elevate to F-Secure ». Cette fonction vous permet d'accéder à une analyse professionnelle des méthodes, technologies, itinéraires réseau, origines du trafic et chronologies Broad Context Detection™, avec des conseils d'experts et des directives de réponse supplémentaires en cas d'attaque.

Pour en savoir plus sur la fonction « Elevate to F-Secure », cliquez ici.

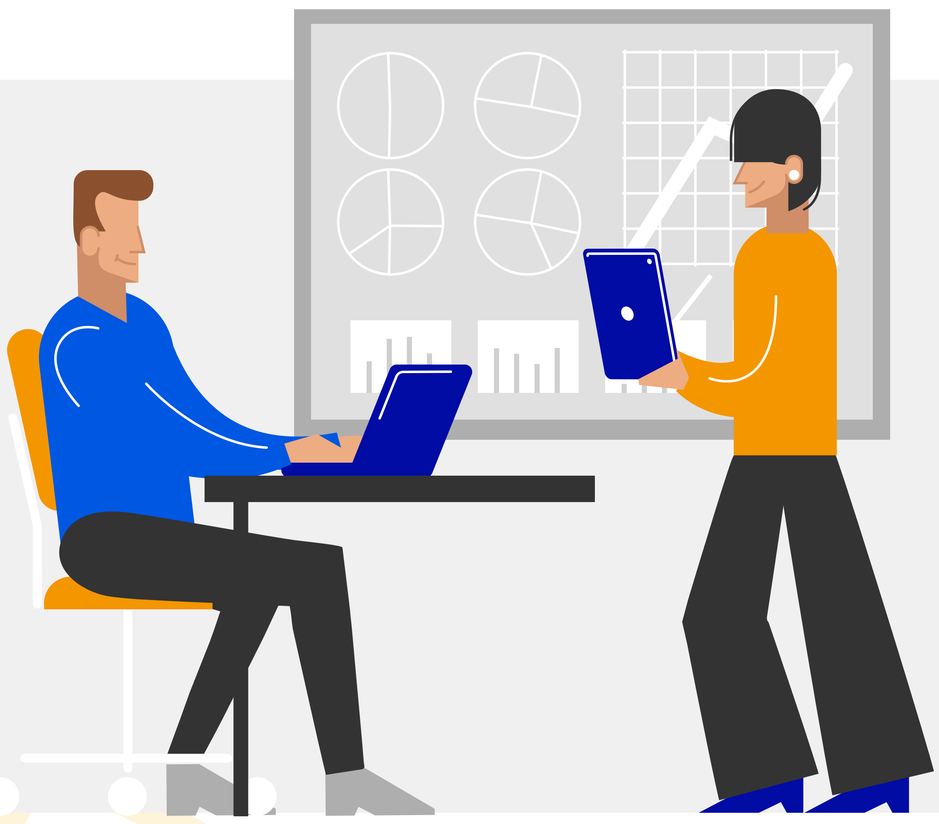


4. MODÈLES TARIFAIRE

Pour faire simple, il existe deux options. La plus courante consiste en une redevance par hôte surveillé, couvrant à la fois l'aspect « licence » et l'aspect « service ». Ce modèle de type SaaS permet au client de comprendre aisément ce à quoi correspondent ses frais mensuels. Le second modèle consiste à séparer les frais de licence et de service. Ce type de formule est plus adapté aux clients souhaitant gérer eux-mêmes leurs solutions et aux partenaires hybrides élaborant des combinaisons de vente de licences et de services.

5. VENTES ET MARKETING

F-Secure est là pour vous aider à élaborer une offre de service réussie. Nous disposons d'informations précieuses sur les tendances du marché et sur les cyber menaces elles-mêmes. Nous pouvons également vous fournir des informations clients, des outils marketing, construire ensemble des plans marketing et des campagnes multi-canaux prêtes à l'emploi pour générer des leads. Nous pouvons également vous accompagner comme co-vendeur ou encore former votre équipe à la vente de services.



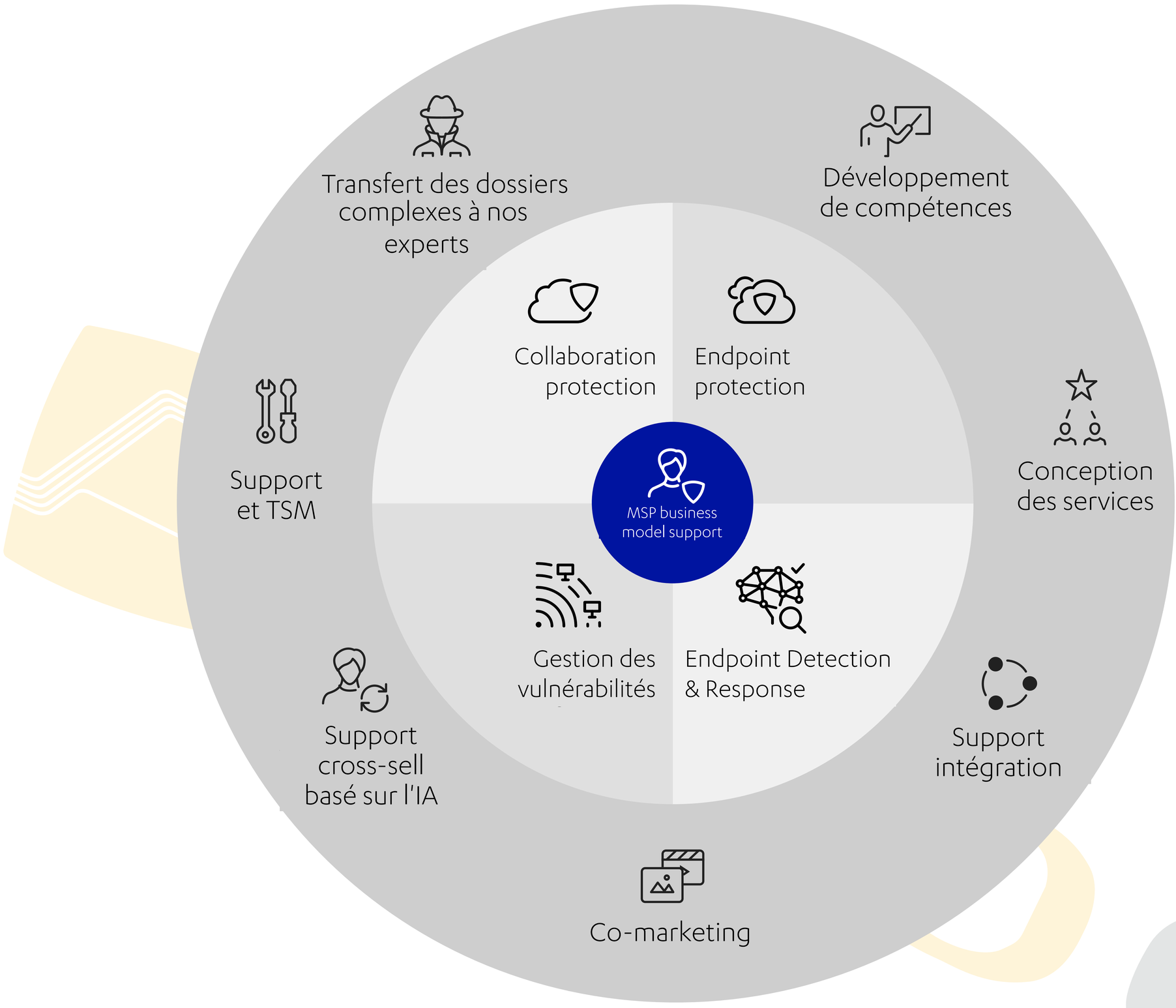
Notre atelier de conception de services vous guidera à travers ces cinq étapes. Ensemble, nous veillerons à élaborer une offre de services correspondant à vos besoins spécifiques. Nous procéderons à une simulation de votre parcours et à une évaluation des résultats attendus à court et long terme. En fonction de votre capacité d'investissement, nous définirons le chemin et le rythme de transformation appropriés à VOTRE ENTREPRISE.

APOG

01 40 64 93 93

Solution de sécurité informatique

Nous vous proposons une offre unique, conçue pour soutenir votre entreprise. Cette offre intègre notre portefeuille de solutions récompensées et des services de support destinés à nos partenaires.



ÉLABORONS ENSEMBLE VOTRE OFFRE DE SERVICES DE CYBER SÉCURITÉ

Nous avons traversé cette année des temps difficiles. Les entreprises ont été contraintes d'optimiser leur activité par tous les moyens possibles et de se recentrer sur leur cœur de métier. Beaucoup d'entre elles ont ainsi procédé à l'externalisation de processus non stratégiques... ce qui constitue une bonne nouvelle pour des entreprises comme la vôtre.

La tendance est nette : une véritable transformation est en cours et le besoin est urgent. Les entreprises souhaitent bénéficier d'un accompagnement sur le plan de la digitalisation, du passage au cloud et surtout de la cyber sécurité. En proposant des services de cyber sécurité, vous pourrez vous positionner comme leur partenaire de confiance et augmenterez leur fidélité. Les revendeurs à même de saisir cette opportunité seront en mesure de se différencier. Les autres, qui n'apportent pas aux entreprises les services et modèles de sécurité dont elles ont besoin, se retrouveront bientôt hors jeu.

Selon l'indice Wells Fargo Small Business 2020, près de 82 % des petits et moyens revendeurs informatiques déclarent que la conquête de nouveaux clients constitue un défi plus grand que la fidélisation des clients existants.

Parallèlement, les marges réalisées sur les licences logicielles et hardware ne cessent de se réduire et les SKU se standardisent. Heureusement, en élargissant votre portefeuille et en proposant de nouveaux services à valeur ajoutée, vous pourrez vous démarquer, pour conquérir de nouveaux clients et consolider votre relation avec votre clientèle existante.

Selon les données dont nous disposons sur le secteur et d'après nos recherches, les MSP et MSSP connaissent une croissance rapide indiscutable. Ce phénomène a notamment été accéléré par la crise du Covid-19. 50 % des MSP affirment qu'ils souhaitent passer d'une offre axée sur les produits informatiques à un catalogue comprenant des services de sécurité managés.

En vous donnant accès aux bonnes technologies, aux bons modèles commerciaux et aux bons services, F-Secure peut vous aider à tirer le meilleur des transformations en cours dans le secteur de la cyber sécurité.

Grâce aux solutions de cyber sécurité modulaires proposées par F-Secure, vous pouvez fournir des produits pertinents, de précieux éclairages et des services permettant à vos clients de rester focalisés sur leur cœur de métier. Ils pourront ainsi avancer en toute sérénité, en sachant que leur cyber sécurité est gérée comme il se doit et que leurs actifs numériques sont protégés par un partenaire de confiance.

En proposant à vos clients des services de cyber sécurité évolutifs, vous pourrez également améliorer votre propre productivité et votre rentabilité. En vous appuyant sur un modèle de cyber sécurité complet intégrant la protection des endpoints, la détection et la réponse, la gestion des vulnérabilités et la protection des collaborations cloud via un portail de gestion unique, vous disposerez d'une visibilité accrue, à la fois sur les endpoints eux-mêmes et sur les environnements informatiques des entreprises dans leur ensemble. Vous serez ainsi en mesure d'optimiser l'utilisation de vos ressources.

Tous les revendeurs ne sont pas des consultants en cyber sécurité. Heureusement, avec F-Secure, la vente de services de cyber sécurité devient un effort commun. L'automatisation de nos produits simplifie la gestion des incidents et, grâce à la fonctionnalité « Elevate to F-Secure », vous pouvez transmettre les dossiers les plus complexes à nos experts pour une analyse et une enquête approfondie. En ciblant le segment de clientèle approprié (les petites et moyennes entreprises), vous pouvez conserver la maîtrise de votre charge de travail. F-Secure vous accompagne dans la conception de services en vous fournissant toutes les clés pour réussir : définition des services, planification des ressources, stratégies de SLA et de tarification, et stratégies de vente et de marketing.

Il est temps d'agir dès maintenant. Les cyber menaces évoluent trop rapidement et les entreprises peinent à suivre. Vos clients recherchent un partenaire de confiance capable de bien comprendre les cyber menaces et de cerner leurs besoins. En élargissant votre offre existante pour y inclure des services de sécurité, vous pourrez devenir ce partenaire, pour aujourd'hui et demain.

F-Secure sera à vos côtés pour vous aider à développer votre activité et à relever les nouveaux défis auxquels vous faites face.

NOTES

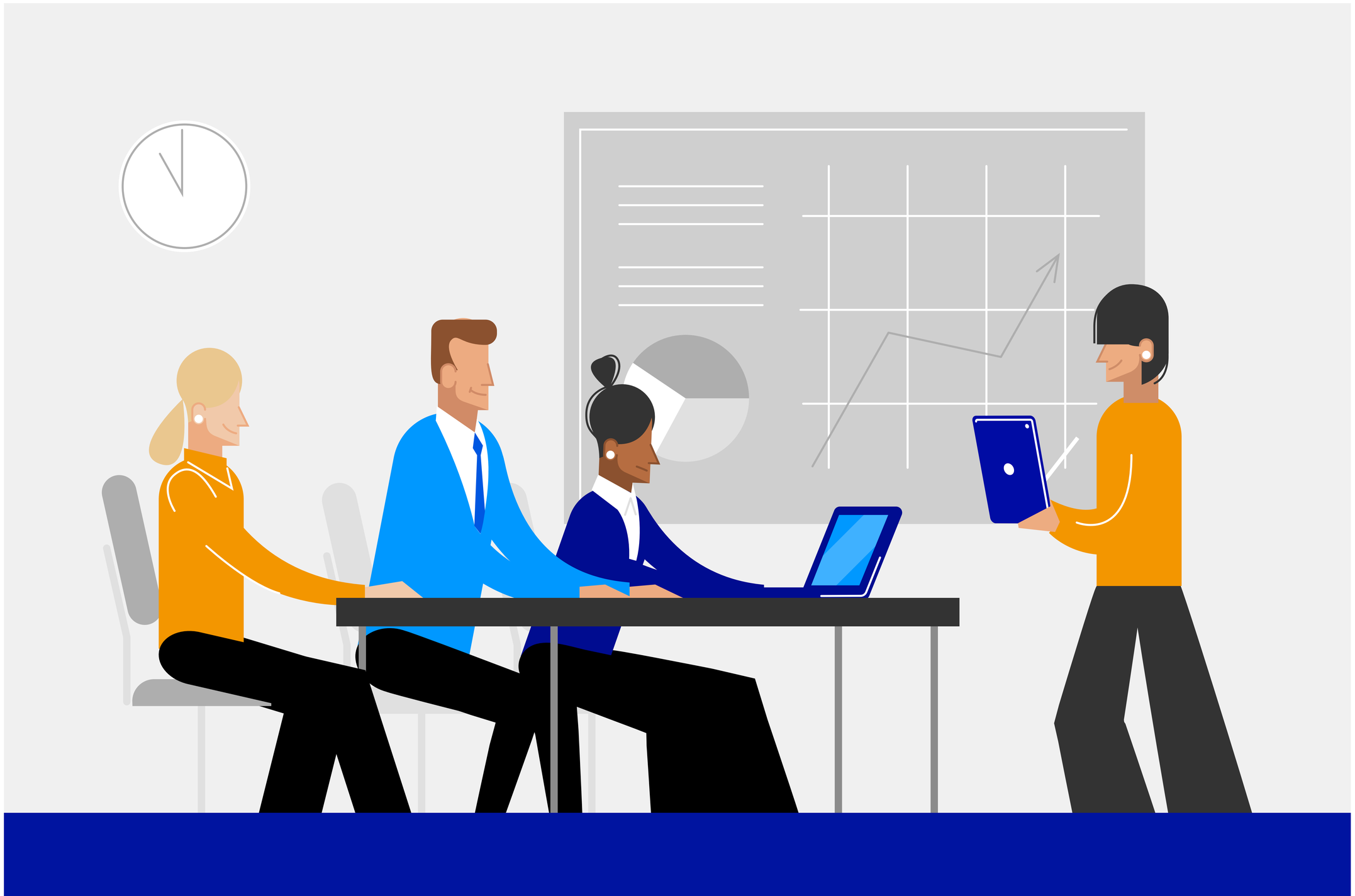
1 Étude de marché B2B F-Secure 2020

2 Gartner Innovation Insight for Cloud Endpoint Protection Platforms, 2019

APOG

01 40 64 93 93

Solution de sécurité informatique



TROIS BONNES RAISONS DE PROPOSER DES SERVICES DE SÉCURITÉ MANAGÉS

1. Répondez à une demande en forte augmentation, dans un contexte de multiplication des cyber menaces.

2. Différenciez-vous et devenez un partenaire de confiance capable de proposer une véritable valeur ajoutée, pour que vos clients puissent, en toutes circonstances, rester opérationnels et en sécurité.

3. Proposez une offre plus évolutive et augmentez votre rentabilité.

Profitez d'un atelier gratuit dédié à la conception de services, pour élaborer sans attendre votre nouvelle offre

RÉSERVER MAINTENANT

À PROPOS DE F-SECURE

Fondée en 1988, F-Secure est une entreprise finlandaise spécialisée dans la cyber sécurité, cotée au NASDAQ OMX Helsinki Ltd.
Depuis plus de trente ans, nous protégeons des dizaines de milliers d'entreprises et des millions de particuliers grâce à notre réseau de partenaires de distribution, et plus de 200 fournisseurs de services.
Des solutions de protection des postes de travail à la détection et réponses aux menaces avancées, nous veillons à ce que nos utilisateurs puissent compter sur une cyber sécurité de haut-niveau.
L'alliance unique de l'expertise humaine, de solutions logicielles et d'intelligence artificielle nous permet d'être reconnu comme un acteur incontournable du marché européen.

f-secure.com/fr_FR/ | **twitter.com/fsecurefrance** | **linkedin.com/company/f-secure-corporation**

F-Secure

APOG

01 40 64 93 93

apog@apog.net

apog.net

Retrouvez-nous sur :