Channel Futures™

SAUVEGARDE ET CYBERPROTECTION DANS LE CLOUD

Le moyen le plus facile pour les RVA de stimuler la vente de services

POWERED BY | Acronis

INTRODUCTION

Les technologies de rupture sont la nouvelle norme. La transformation numérique continue de redéfinir pratiquement tous les aspects de l'économie mondiale, sans épargner le segment des revendeurs à valeur ajoutée (RVA). Le Cloud, la multiplication des terminaux, la croissance fulgurante des données, la diversification de l'offre de solutions SaaS (visant désormais les cas d'utilisation les plus divers) et les innovations en matière d'automatisation modifient en profondeur le modèle RVA, jusqu'à remettre en question son rôle et la définition même de ses objectifs commerciaux dans la décennie à venir.

Reconnaissons-le, les RVA les plus dynamiques se sont (lentement) adaptés à ces changements radicaux. Beaucoup ont étoffé leur portefeuille de produits avec des licences récurrentes, des solutions SaaS et une infrastructure Cloud. C'est un pas important dans la bonne direction.

Mais il reste beaucoup à faire dans un monde où les entreprises privilégient résolument la location de services informatiques auprès de fournisseurs experts, plutôt que l'acquisition et l'exploitation de technologies en interne. Les nouvelles startups XaaS (Everything-as-a-Service) se multiplient et réinventent à vitesse vertigineuse les formules de commercialisation. En bref, les RVA n'ont pas le choix : ils doivent évoluer ou périr.

Comme nous allons le démontrer, pour les RVA, le chemin le plus direct vers une réussite et une croissance durables consiste à adopter le modèle Cloud pour la fourniture de services de sauvegarde et de protection des données. Ceux qui auront le plus de chances de prospérer en 2020 et au-delà vont devoir gérer un nombre croissant de services Cloud et exploiter des outils d'automatisation en soutien à leurs clients. De même, ils devront explorer de nouvelles façons d'exploiter au mieux les nombreuses plates-formes qui peuplent l'écosystème technologique — notamment celles qui incluent des fonctions d'automatisation grâce auxquelles les RVA peuvent proposer des services à forte valeur ajoutée. Il existe également de nouvelles plates-formes de services managés qui traitent les détails opérationnels critiques, les mises à jour de sécurité, la gestion de l'infrastructure et les tâches de routine.

Le choix d'une plate-forme de qualité, associée à une sélection soignée de solutions, doit permettre aux RVA d'offrir à leurs clients et partenaires des services managés sans les tensions et les dépenses qui vont généralement de pair avec la création d'un nouveau modèle opérationnel ou d'une nouvelle unité opérationnelle.

L'intérêt commercial des services à forte valeur ajoutée

Des motifs divers mais nécessaires incitent les RVA à élargir leur offre de services récurrents à forte valeur ajoutée et de services managés. Certains sont assez évidents, notamment les impératifs globaux de stabilité et de prévisibilité des activités (grâce à des revenus récurrents plutôt que ponctuels) ou l'amélioration de la rentabilité.

Cependant, les RVA qui ne changent pas de cap et n'offrent que des renouvellements de licence traditionnels, des contrats de support ainsi que des services managés de base apparaissent de plus en plus vulnérables. L'adoption des services Cloud, segment des services informatiques qui connaît la plus forte croissance, protège les RVA contre l'obsolescence. Selon Gartner, le marché mondial des services de Cloud public progressera de 182,4 milliards de dollars en 2018 à 331,2 milliards en 2022[i], à mesure que les entreprises abandonnent les services traditionnels au profit du Cloud dans leur choix de produits et services informatiques[ii].

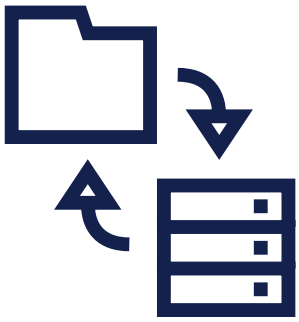
Services informatiques : les 5 services les PLUS/MOINS SOLLICITÉS

par taux de croissance annuel composé (TCAC) (2017-2022)

Source : Gartner. Top Trends Driving Change for IT Services.

Les 5 services plus sollicités	TCAC en % 2017-2022
IaaS	**26,6**
Services d'infrastructure	**14,1**
Mobile (Services managés en milieu professionnel)	**11,3**
Colocation	**11,0**
Hébergement	**10,4**

Les 5 services moins sollicités	TCAC en % 2017-2022
Bureau (Services managés en milieu professionnel)	**-3,5**
Support matériel (Support des terminaux clients)	**-3,4**
Externalisation du centre d'assistance	**-3,2**
Externalisation du centre de données	**-2,5**
Externalisation du réseau d'entreprise	**-2,3**



Les services Cloud managés connaissent eux aussi une croissance exponentielle : le marché mondial devrait atteindre 84,7 milliards de dollars en 2023, soit plus du double des 41,4 milliards recensés en 2018[iii]. Gartner prévoit que les services liés au Cloud tels que le conseil, l'implémentation, la migration et les services managés représenteront 28 % des budgets totaux du Cloud d'ici 2022[iv].

En conclusion, tout RVA qui souhaite améliorer ses statistiques de vente à moyen ou long terme doit étoffer son portefeuille de services Cloud managés. Les clients du monde entier se tournent vers le Cloud et se détournent des RVA qui ne suivent pas le mouvement.

Développer et gérer un portefeuille de services Cloud

Comment un RVA franchit-il le cap ? Les services Cloud managés s'articulent autour de deux éléments clés. Le premier est une **plate-forme** destinée à la gestion des services, à l'intégration des fournisseurs, à l'intégration des clients et à la personnalisation.

La mise au point d'une plate-forme de gestion des services implique un développement logiciel complexe et ardu. C'est pourquoi les RVA (ainsi que les fournisseurs MSP) ont tout intérêt à s'associer à un partenaire technologique qui fournit une solution robuste, testée et prête à l'emploi, telle qu'**Acronis Cyber Cloud**. Une plate-forme optimisée pour les fournisseurs de services permet aux partenaires et aux RVA de formuler et de proposer rapidement des services Cloud, sans pratiquement aucun investissement initial. Les meilleures plates-formes permettent la création de services différenciés, l'ajustement des modèles opérationnels et tarifaires et l'intégration des services Cloud au portefeuille.

Quel que soit le fournisseur, une plate-forme de services Cloud managés doit offrir les fonctionnalités suivantes :

- Architecture multitenant avec partitionnement sécurisé des services pour prendre en charge plusieurs clients
- Possibilité de créer divers packages et offres groupées de services
- Authentification unique (SSO) pour les comptes clients et intégration avec des systèmes SSO externes

- Moteur de règles qui prend en charge des règles d'utilisation et de sécurité personnalisées, p. ex. le contrôle de l'accès basé sur les rôles
- Quotas d'utilisation
- Plusieurs modèles de tarification tels que le paiement à l'utilisation, les abonnements annuels, les capacités réservées, etc.
- Console de gestion unifiée qui prend en charge les environnements multitenant
- Rapports d'utilisation, audits, indicateurs et tableaux de bord complets
- Intégration avec d'autres systèmes, dont le provisionnement des utilisateurs, l'authentification des utilisateurs ou le système IAM, la facturation, le système de support ou de gestion des tickets, le CRM, etc.
- Marque personnalisée (c.-à-d. une offre en marque blanche)
- API REST pour faciliter le développement et l'intégration de services Cloud personnalisés

Le succès des services Cloud managés dépend également d'un **portefeuille de services** bien pensé. Bien sûr, il est possible pour un RVA de continuer à vendre des centaines de solutions provenant de centaines de fournisseurs. Mais il apparaît plus sensé d'opter pour une approche plus simple et rationnelle, en identifiant un petit nombre de fournisseurs qui répondront à tous vos besoins. Plus précisément, des fournisseurs actifs dans des créneaux spécialisés (réseau, protection des données, IaaS, gestion de l'infrastructure, outils de productivité, etc.) et offrant des services stratégiques portant sur des éléments tels que :

- Terminaux (ordinateurs de bureau, ordinateurs portables et terminaux mobiles)
- Services de données Internet et mobiles
- Services VoIP
- Impression
- Messagerie électronique et applications de productivité bureautique (Office 365 ou Google Apps)
- Applications CRM
- Applications financières
- Applications ERP/HCM
- Applications marketing
- Gestion des terminaux (mobiles et ordinateurs de bureau/portables)

Acronis est le couteau suisse de la cyberprotection. Il ne couvrira pas l'intégralité de vos besoins en matière de services Cloud (pas plus que ne le ferait aucun autre fournisseur), mais il en assurera une bonne partie :

- Services de protection des données
- Continuité des activités
- Solutions de sécurité des terminaux (p. ex. protection contre les ransomwares)
- Stockage et partage de fichiers
- Services de certification, de vérification et de signature électronique des fichiers

Quels que soient les secteurs qu'un RVA choisit de servir, Acronis possède des solutions qui apporteront une valeur ajoutée à ses clients.

Protection des données : le socle d'un portefeuille de services Cloud

Se concentrer sur des catégories de produits et services dont le marché potentiel reste étendu constitue toujours une bonne stratégie commerciale. À cet égard, la protection des données en tant que service (DPaaS) correspond parfaitement à cet objectif, IDC prévoyant que le marché connaîtra un taux de croissance annuel composé (TCAC) de 16,2 %, pour atteindre 10,2 milliards de dollars d'ici 2022[v].

Un portefeuille de services de protection des données doit avant tout inclure une solution de **sauvegarde sécurisée** pour les données hébergées sur les serveurs traditionnels et les baies de stockage d'entreprise, ainsi que les machines virtuelles, les environnements de stockage virtuels et les ressources Cloud. Un produit comme **Acronis Cyber Backup Cloud** permet aux RVA de stocker en toute sécurité toutes les données critiques d'une entreprise grâce à un modèle de stockage hybride qui prend en charge à la fois le stockage sur site et dans le Cloud, et qui ne lie pas les clients à un seul emplacement ou environnement.

La **reprise d'activité après sinistre** est un autre composant essentiel d'une offre complète de protection des données d'un RVA. Ces services complètent la solution de sauvegarde en permettant de restaurer rapidement les données et de redémarrer les applications sur une infrastructure secondaire (en général, un site de restauration dans le Cloud).

L'automatisation des processus traditionnellement requise pour un service de reprise d'activité après sinistre sans erreur nécessite souvent un effort de développement important. Les RVA peuvent s'en dispenser en recourant à un produit SaaS tel que **Acronis Cyber Disaster Recovery Cloud**, qui ajoute la reprise d'activité après sinistre à votre portefeuille de services Cloud. Le produit clé en main prend en charge les charges de travail physiques et virtuelles, fournit un éditeur d'interface graphique pour la création d'automatisations et peut tester divers scénarios de récupération sans perturber les systèmes de production.

Ensuite, les services de **synchronisation, partage et stockage de fichiers** offrent les fonctionnalités de partage de fichiers dans le Cloud exigées par les entreprises, alliées à des fonctions complètes de sécurité, de contrôle et de protection des données. Bien que certains services pour particuliers proposent une version pour entreprises, il s'agit généralement de produits isolés dont la compatibilité avec d'autres services professionnels de protection et de sécurité des données n'est pas idéale. Au lieu de cela, les RVA peuvent offrir une solution complète et intégrée en adoptant **Acronis Cyber Files Cloud**, un service personnalisable qui fonctionne avec les systèmes de stockage existants ou l'infrastructure Cloud d'Acronis. Comme les services destinés aux particuliers, il prend en charge les appareils mobiles, les ordinateurs Windows, les Mac et tous les navigateurs Web courants, mais il offre également des fonctions conviviales pour les entreprises, comme l'édition in situ de documents Microsoft Office.

Ensuite, il y a les indispensables pour le bureau paperless telles que **la certification, la vérification et la signature électronique des fichiers**. Ces fonctionnalités offrent un mécanisme sécurisé et incontestable pour l'approbation des documents numériques et la validation de leur authenticité. Un produit SaaS tel que **Acronis Cyber Notary Cloud** permet aux RVA de fournir un service basé sur la blockchain pour la notarisation, la signature électronique et la vérification des fichiers. Il permet aux clients d'authentifier les documents critiques et de répondre aux exigences réglementaires en matière d'intégrité et de transparence des données.

Et dans la perspective d'une stratégie commerciale optimale, soulignons que les services de protection des données sont toujours **le produit le plus facile à vendre pour un fournisseur de technologies.** Plusieurs des grands fournisseurs de services managés du marché ont commencé par proposer des solutions de sauvegarde, de reprise d'activité après sinistre et de sécurité, et se sont développés par la suite.

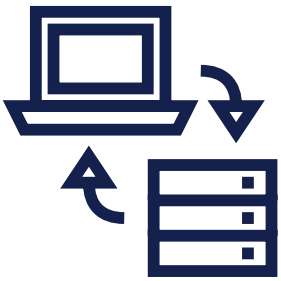
Dépasser le concept de la protection des données pour rester compétitif

Les incidents classiques tels que les pannes de courant et les catastrophes naturelles ne sont pas les seuls dangers auxquels les entreprises sont confrontées au XXIe siècle. Les cybermenaces représentent un danger considérable pour les organisations du monde entier. Selon Accenture[vi], les atteintes à la sécurité numérique ont augmenté de 67 % au cours des cinq dernières années, enregistrant une croissance de 11 % au cours de la dernière année seulement.

C'est une mauvaise nouvelle pour les entreprises, mais un créneau pour les RVA. Dans un monde où la cybercriminalité coûte 2,9 millions de dollars chaque minute[vii], les RVA qui vont au-delà des produits de sauvegarde classiques et offrent des solutions complètes de cyberprotection se dotent d'un avantage concurrentiel. Pour Acronis, la cyberprotection est une nouvelle génération de protection des données qui converge avec la cybersécurité. Elle a pour but de renforcer cinq éléments essentiels : **fiabilité, accessibilité, confidentialité, authenticité et sécurité des données**. Les RVA peuvent proposer des services fiables et différenciés de protection des données en s'appuyant sur ces éléments.

Le premier élément est la **fiabilité**, qui permet de s'assurer que des copies non altérées des données sont toujours disponibles. Le deuxième élément, l'**accessibilité**, permet aux clients et aux utilisateurs mobiles, toujours connectés, d'accéder aux données de l'entreprise où qu'ils se trouvent. La **confidentialité** vise à garantir que les données sensibles et confidentielles sont tenues à l'abri des regards indiscrets de personnes non autorisées (tout en prévoyant les contrôles d'accès nécessaires pour les utilisateurs légitimes). Non moins importante, l'**authenticité** sert à garantir que les données n'ont pas été subrepticement modifiées et que les copies légitimes sont identiques à l'original.

Enfin, les RVA doivent garantir la **sécurité** des données, des systèmes et des utilisateurs contre les acteurs malveillants, qu'il s'agisse de pirates informatiques externes ou d'employés internes malveillants. La sécurité doit couvrir à la fois les données au repos (stockées) et en mouvement (sur le réseau) en utilisant diverses techniques comme le chiffrement, le hachage, les signatures numériques, la surveillance ainsi que la prévention et la remédiation des attaques.



Les RVA et les fournisseurs MSP qui offrent une suite intégrée de services de protection des données sécurisés doivent également intégrer une protection contre les ransomwares. Les ransomwares sont un type de malware qui bloque l'accès aux systèmes informatiques et aux données et ne le rétablit que contre le paiement d'une rançon. Selon les prévisions, ils devraient frapper une entreprise toutes les **14 secondes d'ici la fin de 2019**[viii]. Un rapport de Malwarebytes révèle que les attaques contre les entreprises ont déjà augmenté de 195 % entre le quatrième trimestre 2018 et le premier trimestre 2019[ix].

Acronis Active Protection empêche les ransomwares de chiffrer et verrouiller les fichiers, les sauvegardes et jusqu'au logiciel de sauvegarde lui-même. En surveillant continuellement les accès et modifications aux systèmes, Acronis Active Protection identifie et contrecarre les activités suspectes avant qu'une attaque par ransomware ne fasse des ravages. Et dans le cas où un ransomware parviendrait à franchir les défenses, Acronis Active Protection restaure automatiquement les fichiers chiffrés, épargnant aux fournisseurs de services un temps considérable en restaurations et réduisant les temps d'arrêt. Parce qu'elle est intégrée à Acronis Cyber Backup Cloud, cette technologie réduit instantanément votre exposition aux ransomwares (et celle de vos clients) sans avoir à installer de composants en plus de vos agents de sauvegarde.

Proposer des services de cyberprotection avec Acronis

Acronis Cyber Cloud ne se contente pas de fournir des fonctions de sauvegarde, de reprise d'activité après sinistre, de synchronisation et partage de fichiers, de notarisation de documents et de sécurité des données. Dans un souci d'efficacité, Acronis Cyber Cloud s'intègre également aux principaux outils de back-office des fournisseurs de services managés et de fournisseurs de services Cloud, tels que la gestion des services, les tickets d'assistance, la surveillance et les alertes.

En outre, Acronis Cyber Cloud est la *seule* solution à offrir à la fois des services de cyberprotection à la demande et une plate-forme de provisionnement et de gestion des utilisateurs, assurant ainsi aux revendeurs la liberté de promouvoir leur marque et de contrôler la relation client. Acronis Cyber Cloud fournit également l'accès à l'infrastructure Cloud d'Acronis et la prise en charge des systèmes privés pour la prestation de services.

Feuille de routes partenaire : Comment vendre Acronis Cyber Cloud

En élaborant son portefeuille sur un socle solide de services SaaS provenant d'un éditeur bien établi, un RVA peut offrir des services Cloud avec un **investissement de départ minimal en temps et argent**, ainsi que le soutien d'un partenaire disposant d'une expertise approfondie en matière de protection des données.

En plus des compétences techniques, un fournisseur de services Cloud doit inscrire dans son programme de partenariat une assistance complète sur le plan des ventes et du marketing. Les experts du Programme Partenaires Cloud Acronis assistent les RVA à toutes les étapes du cycle de vie des services : des premiers pas (où Acronis aide le RVA à s'orienter, depuis le lancement du service jusqu'à la tarification et au développement du packaging) à l'intégration du client aux campagnes marketing en cours et au support avant-vente.

Services de protection des données sécurisés : exemples et cas d'utilisation

Les fonctionnalités de protection des données sécurisées offertes par Acronis Cyber Cloud permettent aux RVA de commercialiser une multitude de services Cloud génériques et personnalisés conçus pour répondre aux besoins d'entreprises de tous types et de toutes tailles. Parmi les catégories les plus prisées :

Les **services de protection des données hybrides** à multiples facettes. Ils sont compatibles avec n'importe quelle infrastructure, y compris les baies de stockage ou les serveurs locaux, les systèmes managés par des RVA sur un site de cohébergement ou les ressources de stockage dans le Cloud. Un scénario de déploiement typique utilise un service Cloud pour l'archive principale, avec des copies secondaires optionnelles vers le stockage local. Ce genre de déploiement hybride permet aux RVA de proposer une offre complète de services Cloud et de vente croisée matériel-logiciels pour gérer le stockage local.

La popularité croissante des applications SaaS telles qu'Office 365 est favorable aux services Cloud qui utilisent une solution du type de celle d'Acronis Cyber Backup Cloud. De nombreux RVA proposent une **formule incluant Office 365 et une solution de sauvegarde**. Cette proposition permet à leurs clients d'atteindre leurs objectifs en matière de protection des données et, dans certains cas, leurs exigences de conformité.

Les services de protection des données de type SaaS peuvent être étendus à l'aide de **services de synchronisation et partage de fichiers dans le Cloud** destinés à améliorer la collaboration, tout en bloquant l'exfiltration des données et les accès non autorisés.

Les **services Cloud de reprise d'activité après sinistre** étendent les services d'archivage de données par l'automatisation des processus, ce qui permet de restaurer les activités interrompues sur des sites distants gérés par le fournisseur et évite à l'entreprise de devoir mettre en place une infrastructure redondante et coûteuse. Dans une perspective à long terme, à mesure que les clients adoptent l'infrastructure Cloud pour héberger des applications d'entreprise, les RVA peuvent étendre leurs services à l'utilisation des ressources IaaS comme emplacement dédié à la reprise après sinistre.

Les **services convergents de protection et sécurité des données** s'attaquent au fléau des ransomwares qui retiennent en otage les données importantes d'une entreprise. Qu'il soit possible de verrouiller des données de cette manière illustre bien l'insuffisance des défenses traditionnelles axées sur les malwares et souligne la nécessité de combiner la protection des données et la surveillance de la sécurité selon une approche cohérente et coordonnée. Un grand nombre d'antivirus classiques basés sur les signatures sont désormais impuissants face à ce type de menaces. En revanche, les solutions modernes qui protègent efficacement les données se basent sur des

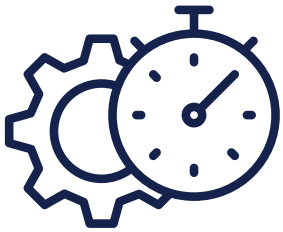
technologies similaires à Acronis Active Protection, qui exploite des modèles d'apprentissage automatique sophistiqués pour détecter et bloquer les ransomwares. Les RVA et fournisseurs de services managés peuvent ainsi offrir des services de sécurité de pointe, tout en confiant la complexité de leur implémentation et de leur gestion à un tiers expert.

Les partenaires et les RVA peuvent également étendre et personnaliser ces services génériques fondamentaux grâce à des fonctionnalités axées sur des secteurs et des clients particuliers. Une plate-forme extensible commercialisée en marque blanche telle que la suite Acronis Cyber Cloud garantit que les partenaires disposent d'un contrôle total sur la marque, les personnalisations et la relation client. Les RVA et les fournisseurs de services managés peuvent étendre les capacités de la suite **Acronis Cyber Cloud** grâce à Acronis Cyber Platform, qui propose une série d'API et de kits de développement logiciel (SDK). De plus, les possibilités d'extension et de personnalisation permettent d'élaborer des offres uniques qui différencient leur marque de la concurrence.

Les domaines les plus prisés pour les services ciblés comprennent **la sauvegarde des postes de travail vers le Cloud** ainsi que **l'archivage à long terme** dans le cadre de services à faible coût de stockage passif dans le Cloud, à des fins de conformité réglementaire.

Autre opportunité importante : le secteur de la **santé**, qui nécessite un stockage et une sauvegarde conformes à des règles strictes (dont la loi HIPAA aux États-Unis). **Un fournisseur de services managés spécialisé dans les services aux dentistes** a utilisé le chiffrement AES-256 intégré d'Acronis Cyber Backup Cloud pour fournir un service conforme à la norme HIPAA et économisé ainsi 30 000 dollars sur son précédent logiciel de sauvegarde. Après avoir adopté Acronis Cyber Backup Cloud, un **important fournisseur de solutions de gestion automatisée de cabinets médicaux et de dossiers médicaux électroniques** a réduit son temps de reprise de 90 %. Et en tirant parti de l'évolutivité des services Cloud, il a multiplié par dix sa base de clients en deux ans seulement.

Autre proposition incontournable : la cyberprotection qui cible **la vente au détail, la logistique et les assurances** — des secteurs caractérisés par un réseau distribué de succursales dont la gestion et la protection centralisées s'avèrent complexes. La plate-forme Acronis fournit les services suivants :



- Cyberprotection centralisée pour toutes les succursales, avec une stratégie de sauvegarde centralisée et une restauration en libre-service.
- Capacités de reprise à distance, y compris la restauration automatisée centralisée à distance.
- Automatisation de la restauration sans personnel informatique.
- Aucun investissement en biens d'équipement requis pour les succursales (tous les services fonctionnant dans le Cloud).
- Administration via une console unique pour les serveurs, les postes de travail et Office 365.

Recommandations et appel à l'action

Les services Cloud de protection des données offrent aux RVA des opportunités incontournables d'accroître leurs revenus récurrents à marge élevée, mais aussi d'impressionner et de fidéliser leurs clients. Le partenariat avec un fournisseur de logiciels établi tel qu'Acronis pour élaborer un portefeuille étoffé de services permet aux RVA de se concentrer sur l'essentiel. Fort des atouts d'Acronis, un RVA peut consacrer son énergie à **la différenciation et la personnalisation** de ses services, ainsi qu'à **l'augmentation de ses marges grâce à la réduction des frais généraux**. Il peut également **protéger les clients contre des menaces nouvelles et évolutives telles que les ransomwares**, **accélérer le rythme de développement et de déploiement de ses services**, et **effectuer des ventes croisées de produits et services connexes**. Avant tout chose, un RVA a la capacité de **construire une marque forte qui favorise la fidélité des clients et réduit le taux d'attrition.**

Contactez l'équipe de vente Acronis pour un entretien personnalisé et une démonstration produit en direct.

CONTACTEZ-NOUS

Sources

[i] Gartner. « Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019 ». Communiqué de presse. 2 avril 2019.

[ii] Gartner. « Top Trends Driving Change for IT Services ». Webinaire. 25 mars 2019.

[iii] IDC. « Worldwide Managed Cloud Services Forecast, 2019–2023: An Extraction View of Technology Outsourcing Services Markets ». Prévision de marché. Septembre 2019.

[iv] Prabha, Anil. « Public Cloud Services Market to Hit $214bn ». TechHQ. 8 avril 2019.

[v] IDC. « Worldwide Data Protection as a Service Forecast, 2018–2022 - Initial Market Sizing ». Prévision de marché. Juillet 2018.

[vi] Accenture. Ninth Annual Cost of Cybercrime Study. 6 mars 2019.

[vii] « Cybercrime Costs Global Economy $2.9m Per Minute ». Infosecurity Magazine. 24 juillet 2019.

[viii] Morgan, Steve. « Global Ransomware Damage Costs Predicted to Hit $11.5 Billion by 2019 ». Cybercrime Magazine. 17 novembre 2017.

[ix] Zamora, Wendy. « Labs Cybercrime Tactics and Techniques Report Finds Businesses Hit with 235 Percent More Threats in Q1 ». MalwareBytes. 25 avril 2019.