IDC MarketScape

IDC MarketScape: Évaluation des fournisseurs de services de sécurité au Canada 2022

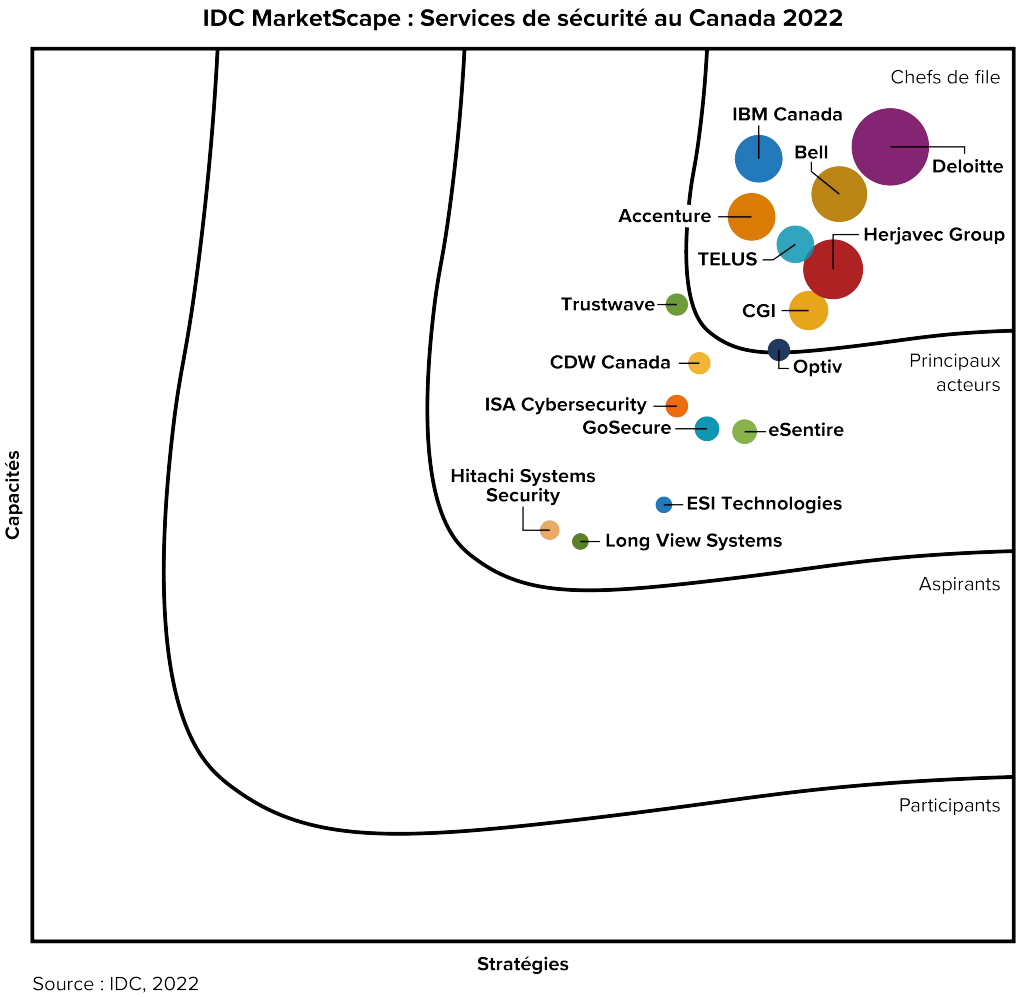
Yogesh Shivhare

CET EXTRAIT DE L'ÉTUDE IDC MARKETSCAPE COMPREND BELL

FIGURE IDC MARKETSCAPE

FIGURE 1

Évaluation des fournisseurs de services de sécurité au Canada de IDC MarketScape



Source : IDC, 2022

March 2022, extrait du document nº CA48060922 d'IDC

Voir l'annexe pour des détails concernant la méthodologie, la définition du marché et les critères de notation.

CONTENU DE CET EXTRAIT

Le contenu de cet extrait est tiré directement du document de IDC MarketScape : Évaluation des fournisseurs de services de sécurité au Canada 2022 de Yogesh Shivhare (document nº CA48060922). Les sections suivantes ont été incluses dans cet extrait, dans leur intégralité ou en partie : Opinion d'IDC, Critères d'inclusion des fournisseurs dans l'évaluation IDC MarketScape, Conseils aux acheteurs de technologie, Profil sommaire des fournisseurs, Annexe et Information supplémentaire. La figure 1 est également incluse.

OPINION D'IDC

Le marché canadien des services de sécurité continue d'évoluer rapidement. Alors que les perturbations technologiques entraînent une numérisation rapide de l'économie canadienne, les organisations doivent repenser l'architecture de l'entreprise, et les événements perturbateurs comme la pandémie de la COVID-19 ne font qu'accélérer cette tendance. Les organisations canadiennes ne cherchent plus que de simples produits de sécurité et services de gestion des politiques ou de la conformité réglementaire auprès de fournisseurs externes de services de sécurité. Bien qu'il s'agisse toujours de fonctions de sécurité très importantes, les organisations recherchent aujourd'hui le soutien de leurs fournisseurs de services de sécurité (SPs) pour assurer une surveillance de la sécurité 24 heures sur 24 et 7 jours sur 7, pour améliorer la détection des menaces nouvelles et avancées, pour améliorer les temps de réponse et pour les aider dans le processus de récupération. En outre, les organisations ont besoin de soutien pour comprendre et gérer le risque lié à la sécurité, concevoir un programme de sécurité à long terme et élever leur maturité sur le plan de la sécurité pour sécuriser leur transformation numérique.

Alors que les organisations intègrent des renseignements et des données de télémétrie provenant de sources multiples telles que le multinuagique, la périphérie, les points d'extrémité, le réseau et l'OT/IdO pour la détection des menaces, elles sont souvent confrontées à des problèmes de surcharge d'alertes et de faux positifs. La pénurie d'experts en cybersécurité répandue au Canada et dans le monde entier fait en sorte qu'il est difficile pour les organisations de donner un sens à tant de données et a motivé les fournisseurs de services de sécurité à investir davantage dans les domaines de l'apprentissage automatique/intelligence artificielle (IA), de l'orchestration de la sécurité, de l'automatisation et de l'analyse. Elle a permis aux fournisseurs de services de sécurité d'offrir des services de sécurité évolutifs qui peuvent être adaptés aux besoins uniques des organisations canadiennes de toutes tailles et de tous les secteurs verticaux de l'industrie.

IDC estime que les domaines suivants feront progresser le marché canadien des services de sécurité, tout en offrant aux fournisseurs la possibilité de différencier leurs offres :

- Un guichet unique – l'étendue et la portée des services de sécurité professionnels ainsi que des services de sécurité gérés (SSG), y compris les services avancés tels que la détection et la réponse gérées (MDR), continueront de se développer parmi les fournisseurs
- L'utilisation de technologies avancées et émergentes qui offriront une plus grande visibilité contre les menaces sophistiquées et permettront une meilleure utilisation des processus automatisés

- La capacité d'offrir un niveau plus élevé d'orchestration, d'automatisation et d'ouverture dans la plateforme centrale
- Des capacités de surveillance, de visibilité et de gestion du nuage qui permettent de mettre en œuvre plusieurs nuages harmonieusement
- Des modèles de déploiement flexibles qui correspondent aux préférences des clients en matière d'adoption et de consommation des services
- Améliorations du portail client, telles qu'une application mobile et des modèles de rapports à présenter aux hauts dirigeants et au conseil d'administration
- Recrutement et rétention de talents de premier ordre dans le domaine de la sécurité

CRITÈRES D'INCLUSION DES FOURNISSEURS DANS L'ÉVALUATION IDC MARKETSCAPE

Pour être inclus dans l'étude IDC MarketScape sur les services de sécurité au Canada pour 2022, les fournisseurs devaient répondre aux critères suivants :

- **Avoir une présence au Canada.** Il était possible de satisfaire à ce critère en ayant un centre des opérations de sécurité canadien, des bureaux au Canada ou du personnel de vente dont les activités consistaient principalement à vendre des services de sécurité au Canada.
- **Services disponibles.** Les fournisseurs devaient offrir un éventail de services de sécurité gérés et professionnels.
- **Revenus associés aux services de sécurité de plus de 10 millions $ pour l'année 2020.** Les revenus pour la revente d'équipement ou de logiciels ne sont pas inclus.

En utilisant son modèle IDC MarketScape, IDC a évalué 16 fournisseurs de services de sécurité qui exploitent des installations et ont des clients au Canada. Ce processus a comporté des entretiens avec 13 fournisseurs et un ou plusieurs clients de ces fournisseurs, tandis que 3 fournisseurs n'ont pas participé activement à cette étude et leur évaluation est basée sur la connaissance qu'IDC a de leurs offres de services de sécurité. La plupart des fournisseurs présentés dans cette étude ont été inclus dans *IDC MarketScape:* Évaluation des fournisseurs de services de sécurité au Canada 2019 (document nº CA44419519, août 2019). À la lumière de cette étude, IDC Canada a identifié sept chefs de file et neuf principaux acteurs IDC MarketScape dans le marché canadien des services de sécurité.

CONSEILS AUX ACHETEURS DE TECHNOLOGIE

L'évaluation des capacités actuelles d'un fournisseur de services de sécurité et de l'harmonisation de sa stratégie par rapport à vos besoins informatiques et opérationnels peut se révéler un long processus. Il est important de bien comprendre les exigences de sécurité de votre organisation avant de sélectionner un fournisseur. IDC recommande de se reporter aux cadres de cybersécurité courants comme ceux qui sont fournis par le NIST (National Institute of Standards and Technology) et le CIS (Center for Internet Security) ou définis en vertu des normes ISO 27001 et 27002 afin de vous assurer que vous avez correctement classé tous les actifs de votre réseau. Une bonne compréhension de votre réseau vous aidera à choisir les bons services auprès du bon fournisseur.

IDC a évalué plusieurs critères essentiels dont les entreprises devraient tenir compte lorsqu'elles comparent des fournisseurs. Voici les principaux éléments à prendre en considération durant votre processus de sélection :

- **L'étendue du portefeuille de SSG.** Il existe un large éventail de fournisseurs offrant des services normalisés ou des services de sécurité gérés fortement personnalisables. Par conséquent, il est important que l'organisation fasse correspondre les différents types d'offres à ses besoins en matière de TI. Dans ce marché, l'acheteur pourrait rechercher des contrôles de sécurité traditionnels tels que les pare-feu, les systèmes de détection des intrusions (identifiants/IPS), la gestion d'informations et des événements de sécurité (SIEM), l'analyse des vulnérabilités et la messagerie sécurisée. Tous les fournisseurs présentés dans ce document offrent ces capacités, mais ces offres se sont également étendues pour inclure des services avancés tels que la gestion des identités et des accès (GIA), les renseignements sur les menaces, l'analyse des applications Web, la détection et la réponse gérées, le SOC géré et la gestion des vulnérabilités/la surveillance du risque. Les fournisseurs de SSG ont également commencé à offrir des services complémentaires tels que la réponse aux incidents (RI), la criminalistique et d'autres capacités de conseil numérique.
- **Capacités de conseil numérique.** Un bon programme de sécurité doit avoir une approche globale, qui comprend l'évaluation du personnel, des processus et des technologies concernés. Les fournisseurs répertoriés dans ce document peuvent aider les acheteurs de technologies à comprendre la maturité actuelle sur le plan de la sécurité, les lacunes et les exigences futures. L'étendue des services professionnels inclut la stratégie et la planification en matière de sécurité, la formation, la conformité et la vérification, l'évaluation et l'élaboration de politiques de sécurité, les tests de pénétration et de vulnérabilité, l'évaluation de l'architecture réseau, la réponse aux intrusions ou aux incidents et l'expertise judiciaire en informatique.
- **Utilisation des renseignements sur les menaces et l'apprentissage automatique.** Les renseignements sur les menaces et les modèles d'apprentissage automatique sont utilisés en complément ou en remplacement des solutions SIEM traditionnelles. Les acheteurs doivent savoir si le fournisseur de services de sécurité avec lequel ils envisagent de travailler possède un plan directeur pour offrir ces capacités avancées.
- **Une plateforme qui offre une visibilité sur les points d'extrémités, le réseau et le nuage.** Un partenaire en matière de sécurité doit être en mesure de démontrer ses capacités d'innovation sur sa plateforme centrale, ainsi que son utilisation des technologies émergentes. Une véritable valeur ajoutée pour l'organisation est la possibilité de choisir un fournisseur capable d'offrir une visibilité complète du cycle de vie de la gestion de la détection et de la réponse.
- **Intégrations des processus d'orchestration et d'automatisation.** Les fournisseurs de services se concentrent davantage sur les outils d'orchestration et d'automatisation, et intègrent ces technologies dans leurs plateformes centrales de prestation. En plus de l'apprentissage automatique et de l'IA avancés, des technologies telles que l'orchestration et l'automatisation aident les fournisseurs de services à améliorer l'efficacité des SOC et les analystes à hiérarchiser, analyser et répondre aux menaces plus rapidement.
- **Renseignements sur les menaces, chasse aux cybermenaces et autres capacités avancées.** Les fournisseurs de services vont au-delà des capacités normales et approfondissent des domaines tels que les renseignements sur les menaces. Les renseignements sur les menaces sont devenus un élément important des services avancés tels que la MDR et sont intégrés aux offres de SSG et de MDR. Certains fournisseurs de services proposent également un usage régulier de la chasse aux cybermenaces, humaine ou automatisée, à partir des flux de renseignements intégrés sur les menaces, et créent des processus et des initiatives d'avenir à partir de ces découvertes.
- **Stratégie de sécurité infonuagique.** L'un des domaines qui continuent à se développer et à s'améliorer est la sécurité infonuagique. La capacité d'un fournisseur à proposer des modèles

infonuagiques flexibles au moyen de services multinuagiques et de travailler dans des environnements pour fournisseurs de services infonuagiques comme Amazon Web Services (AWS), Microsoft et Google est importante selon les besoins de l'organisation. Il est important d'évaluer un fournisseur de services qui aidera et fournira des recommandations pour l'organisation qui passe à ces divers environnements de TI et les utilise.

- **Évaluez les portails clients.** Les portails clients offrent un aperçu Web pratique de toutes les activités liées à la sécurité. Les portails ont évolué pour devenir plus qu'un simple outil de production de rapports, et les solutions populaires incluent de l'information visuelle interactive, des tableaux de bord définis par l'utilisateur, la génération de rapports de vérification et des fonctionnalités de production de rapports sur l'état des systèmes.
- **Expertise et soutien en matière de sécurité.** L'ancienneté de l'équipe de cybersécurité et les ensembles de compétences disponibles deviennent de plus en plus un facteur de différenciation; par ailleurs, la rétention et la formation des talents sont essentielles pour être un fournisseur de sécurité fiable. Les acheteurs doivent choisir un fournisseur qui agira comme un partenaire de confiance et comme une extension de l'équipe des TI. Le fait de savoir que le fournisseur comprend l'environnement informatique et les défis de l'organisation simplifiera la capacité à continuer à faire des recommandations et des ajustements et à fournir des conseils continus tout au long du parcours de sécurité.

PROFIL SOMMAIRE DES FOURNISSEURS

La présente section explique brièvement les principales observations d'IDC qui ont permis d'établir le classement des différents fournisseurs dans le cadre de l'évaluation IDC MarketScape. Alors que chaque fournisseur a été évalué en fonction de chacun des critères présentés dans l'annexe, la description offerte dans cette section constitue un résumé des forces et faiblesses.

Bell

Selon l'analyse d'IDC et la rétroaction des acheteurs, Bell s'est classée dans la catégorie des chefs de file dans la présente évaluation IDC MarketScape 2022 des fournisseurs de services de sécurité au Canada.

Bell offre des services de sécurité au Canada par l'intermédiaire de sa filiale, Bell Marchés Affaires (BMA), et exploite au Canada trois centres des opérations de sécurité (SOC) au niveau commercial, ainsi qu'un SOC au niveau gouvernemental. Le personnel de sécurité, qui compte plus de 700 personnes, est l'une des plus grandes équipes de sécurité au Canada et soutient les clients de BMA tout en sécurisant le réseau de Bell. Bell est présente dans tout le pays et peut servir des clients de taille moyenne et de grande taille dans tous les secteurs verticaux de l'industrie.

Le vaste portefeuille de services de sécurité gérés de Bell comprend des services tels que la sécurité du réseau et du contenu, les services de gestion des menaces (services des SOC, MDR et XDR), les services de gestion des identités et des accès, la sécurité infonuagique et la sécurité de l'IdO. En 2021, Bell a lancé l'ERUSB (Environnement de réponse unifié de sécurité de Bell), un service exploité et entièrement géré par Bell qui combine les dernières technologies SIEM et d'orchestration de la sécurité, d'automatisation et de réponse (SOAR) avec l'expertise de Bell en matière de sécurité, pour offrir à ses clients une surveillance 24 heures sur 24 et 7 jours sur 7, des renseignements sur les menaces, un triage des alertes et une réponse orchestrée et automatisée aux incidents. La gamme de services de SSG de Bell est complétée par un éventail tout aussi large de services de sécurité

professionnels, notamment des services de consultation stratégique, d'évaluation et de test, ainsi que de conception et de mise en œuvre de la sécurité, qui permettent à Bell d'offrir un guichet unique aux organisations qui cherchent à protéger l'ensemble de leur écosystème. Bell schématise ses capacités en matière de sécurité à la maturité des clients sur le plan de la sécurité et s'associe à eux pour la transformer grâce à cinq piliers de sécurité de base : « simplifier et solidifier le cœur », « optimisation des SOC », « services MDR améliorés », « aborder la rapidité du nuage » et « favoriser la convergence à la périphérie de l'IdO/la 5G ». En plus de ces offres de services de sécurité de base, Bell offre également des services de connectivité et de réseautage tels que le SD-WAN, le sans-fil géré, ainsi que le DNS et le VNS avec sécurité intégrée.

Bell fait des investissements importants dans les cas d'utilisation exclusifs de l'IA/l'apprentissage automatique, la sécurité infonuagique, la sécurité de l'IdO et l'automatisation au sein de ses processus de technologie, de soutien aux entreprises et de mobilisation des clients. Cela permet à Bell d'ajouter de nouveaux services, d'améliorer son portefeuille existant et d'améliorer l'expérience client.

Forces

Les clients de Bell citent comme point fort l'évolutivité et la maturité de l'entreprise pour mener à bien des projets importants et complexes. Les vastes partenariats de Bell avec des fournisseurs de technologies de sécurité et des fournisseurs de services infonuagiques permettent à l'entreprise d'offrir des solutions sécurisées intégrées de bout en bout à ses clients.

Faiblesses

Les grandes organisations apportent les avantages de l'envergure et de la maturité; toutefois, Bell doit démontrer aux clients qu'elle est agile et qu'elle peut s'adapter rapidement à la dynamique changeante des projets de sécurité.

Pourquoi choisir Bell

Les organisations devraient envisager Bell si elles cherchent à unifier la gestion de la sécurité à l'échelle de l'entreprise, y compris la connectivité, la sécurité, l'infonuagique, la mobilité et l'IdO.

ANNEXE

Comment interpréter un graphique IDC MarketScape

Pour les besoins de cette analyse, IDC a séparé les indicateurs clés potentiels pour mesurer le succès en deux grandes catégories : les capacités et les stratégies.

Le positionnement sur l'axe des Y tient compte des capacités actuelles du fournisseur et de l'ensemble des services offerts par celui-ci, mais aussi du degré d'harmonisation de ses services par rapport aux besoins des clients. La catégorie des capacités met l'accent sur les capacités de l'entreprise et de ses produits dans le moment présent. Pour cette catégorie, les analystes d'IDC évalueront l'efficacité du fournisseur à développer et à mettre en œuvre des capacités qui lui permettent d'exploiter sur le marché la stratégie qu'il a choisie.

Le positionnement sur l'axe des X, à savoir l'axe des stratégies, est un indicateur du degré d'harmonisation de la stratégie future du fournisseur par rapport aux besoins des clients dans trois à cinq ans. La catégorie des stratégies met l'accent sur les décisions de haut niveau et les hypothèses sur lesquelles elles sont fondées en ce qui a trait aux solutions offertes, aux segments de marché, ainsi qu'aux plans d'affaires et de mise en marché pour les trois à cinq prochaines années.

La taille des différents symboles d'identification du fournisseur dans le graphique IDC MarketScape illustre la part de marché détenue par le fournisseur dans le segment de marché qui fait l'objet de cette évaluation.

Méthodologie utilisée pour l'analyse IDC MarketScape

Les critères de sélection, les facteurs de pondération et la notation des fournisseurs utilisés dans le cadre de l'évaluation IDC MarketScape représentent un jugement d'IDC qui est fondé sur une recherche approfondie au sujet du marché et des différents fournisseurs. Les analystes d'IDC définissent les caractéristiques standard utilisées pour évaluer les fournisseurs en faisant appel à des discussions structurées, des sondages et des entrevues auxquels participent différents chefs de file, intervenants et utilisateurs finals du marché. Les facteurs de pondération du marché s'appuient sur des entrevues auprès d'utilisateurs, des sondages auprès des acheteurs et les recommandations d'experts d'IDC pour chaque marché. Les analystes d'IDC basent les résultats attribués à chaque fournisseur et, à la limite, la position qui lui est attribuée dans l'évaluation IDC MarketScape, sur des sondages détaillés et des entrevues avec les fournisseurs, l'information à caractère public qui est disponible et les expériences des utilisateurs finals, afin d'en arriver à une évaluation précise et uniforme des caractéristiques, comportements et capacités de chaque fournisseur.

Définition du marché

Les services de sécurité s'appuient sur une approche globale de toutes les activités nécessaires à la planification, à la conception, à l'élaboration, à l'amélioration et à la gestion des environnements de sécurité et des programmes exploitation. Ceux-ci peuvent couvrir les processus, les applications et l'infrastructure de TI de l'entreprise. Les services de sécurité peuvent être achetés de manière distincte ou intégrés à d'autres services. Dans le cas d'un achat de services de sécurité distincts (ou, autrement dit, « discret »), le client aura établi une entente avec le fournisseur de services pour l'achat de services entièrement axés sur la sécurité, alors que dans le cas d'un achat de services de sécurité intégrés ou groupés, le client aura établi une entente avec le client pour un projet de services de TI de plus grande envergure dont la sécurité ne constitue qu'une seule composante. Un exemple d'achat de services de sécurité distincts est celui d'un client qui a établi une entente avec un fournisseur de services pour déployer et intégrer une nouvelle technologie de contrôle d'identité et d'accès dans un environnement informatique existant. Un exemple de contrat de services de sécurité intégrés serait celui d'un client qui s'est engagé avec un fournisseur de services à déployer un nouveau système GRC basé sur le nuage et qui doit étendre l'infrastructure de sécurité actuelle pour couvrir les nouveaux systèmes. Pour une explication détaillée à propos des services de sécurité, consultez le document *IDC's Worldwide Services Taxonomy, 2021* (Taxonomie des services à l'échelle mondiale, IDC nº US47191221, mai 2021).

Critères d'évaluation des stratégies et des capacités

Cette section comporte des définitions des facteurs de pondération propres aux marchés ainsi que des valeurs de pondération de ces facteurs (voir les tableaux 1 et 2).

TABLEAU 1

Indicateurs clés de la mesure du succès de la stratégie : Services de sécurité au Canada

Critère d'évaluation de la stratégie	Définition	Pondération (%)
Stratégie relative à la fonctionnalité ou à l'offre	▪ Ajout de services à la gamme des services de sécurité gérés comme la gestion de l'information et des événements de sécurité (SIEM), la gestion des dispositifs, la surveillance des points d'extrémité et les services MDR pour combler les lacunes existantes	24
Livraison	▪ Ajout de services à la gamme des services professionnels comme l'expertise judiciaire en informatique, la réaction aux incidents et la gestion de la conformité pour combler les lacunes ▪ Ajout de services supplémentaires afin de combler les lacunes ou d'ajouter de nouvelles capacités pour offrir des services à partir du nuage ou pour le nuage	15
Cadence des activités de recherche et de développement et productivité	▪ Investissements du fournisseur dans la création de propriété intellectuelle au cours de la prochaine année (si un fournisseur n'effectue pas de recherche en interne, ce sont ses partenariats avec des fournisseurs de premier plan qui seront pris en considération).	12
Croissance	▪ Planifie combler les lacunes en ce qui concerne les bureaux, les installations et/ou les COS situés partout au Canada, selon l'empreinte actuelle du fournisseur ▪ Fournisseur offrant des perspectives de croissance en matière d'expansion des parts de marché, d'acquisition de clients, de croissance des revenus et de financement	27
Stratégie d'affaires	▪ Le fournisseur envisage de travailler plus étroitement avec les établissements universitaires pour le recrutement, pour parrainer des conférences ou pour participer à l'éducation communautaire	10
Stratégie de mise en marché	▪ Le fournisseur envisage d'augmenter ses ressources de vente ou de marketing ou de s'associer à des partenaires intermédiaires.	12
Total		100

Source : IDC, 2022

TABLEAU 2

Indicateurs clés de la mesure de la capacité : Services de sécurité au Canada

Critères d'évaluation de la capacité	Définition	Pondération (%)
Capacités relatives à la fonctionnalité ou à l'offre	▪ Capacité du fournisseur de desservir le marché canadien, notamment les COS, les bureaux et les installations canadiens, répartis à travers le Canada ▪ Capacité d'offrir des services de sécurité à partir du nuage et d'offrir des services pour le nuage ▪ Capacité d'offrir des services évolutifs aux organisations de toutes tailles (les fournisseurs desservent une vaste clientèle et ont des offres de sécurité à plusieurs niveaux.) ▪ Capacité d'offrir aux clients et de tirer parti des services d'analyse de sécurité pour faciliter la détection et l'intervention concernant les menaces (une pondération plus élevée est accordée pour les modules complémentaires SIEM personnalisés, les modèles d'apprentissage automatique et les flux de renseignements sur les menaces). ▪ Capacité d'aider les analystes et les clients en automatisant les flux de travail ▪ Les portails qui ont évolué pour devenir plus qu'un simple outil de production de rapports (une pondération plus élevée est accordée pour les portails offrant de l'information visuelle interactive, des tableaux de bord définis par l'utilisateur et des capacités de génération de rapports de vérification).	51
Gamme de services	▪ Étendue et profondeur des services de sécurité gérés. ▪ Portefeuille de services de sécurité professionnels comprenant la consultation et les services-conseils, les tests de sécurité, la mise en œuvre et l'intégration	20
Avantages du portefeuille de services	▪ Capacité d'offrir des fonctions de guichet unique pour les produits d'informatique, les services et/ou la connectivité avec sécurité intégrée	4
Stratégie de mise en marché	▪ Utilise des campagnes de marketing à grande échelle (une pondération plus élevée est accordée aux fournisseurs qui sont actifs dans la publicité numérique, ont d'excellents sites Web et mènent des campagnes régionales et nationales de marketing et de développement de la conscience communautaire). ▪ Capacité de vendre partout au Canada (une pondération plus élevée est accordée aux fournisseurs ayant une importante force de vente nationale ou qui font appel à des partenaires intermédiaires).	10
Capacités au plan commercial	▪ Implication dans la communauté de la sécurité canadienne (les fournisseurs doivent être actifs dans les groupes et conférences de sécurité et publier de l'information gratuite pour la communauté de la sécurité au Canada). ▪ La capacité de recruter de nouveaux talents et de réduire le roulement du personnel (une pondération plus élevée est accordée pour les organismes qui recrutent du personnel dans les établissements universitaires ou offrent des stages coopératifs à leurs étudiants et qui accordent des avantages sociaux aux employés pour les fidéliser).	10

TABLEAU 2

Indicateurs clés de la mesure de la capacité : Services de sécurité au Canada

Critères d'évaluation de la capacité	Définition	Pondération (%)
Prestation du service à la clientèle	▪ Offre un soutien tous les jours, 24 heures sur 24 et 7 jours sur 7, par l'intermédiaire des COS au Canada et de centres d'appels	5
Total		100

Source : IDC, 2022

INFORMATION SUPPLÉMENTAIRE

Recherches connexes

- *Canadian Cybersecurity Market Outlook, 4Q21: 2020-2025 Security Forecast* (IDC nº CA47049621, novembre 2021)
- *Canadian Cybersecurity Market Snapshot, 4Q21* (IDC nº CA47049421, novembre 2021)
- *IDC's Worldwide Security Services Taxonomy, 2021* (IDC nº US47681721, mai 2021)
- *Brand Perceptions of Managed Security Service Providers in Canada, 2021* (IDC nº CA46282421, mars 2021)

Résumé

Cette étude IDC présente une évaluation des fournisseurs de services de sécurité au Canada par l'intermédiaire du modèle IDC MarketScape. En utilisant son modèle IDC MarketScape, IDC a évalué 16 fournisseurs de services de sécurité qui exploitent des installations et ont des clients au Canada. Ce processus a comporté des entretiens avec 13 fournisseurs et un ou plusieurs clients de chacun de ces fournisseurs, tandis que pour d'autres qui n'ont pas participé activement à cette étude, l'évaluation s'est basée sur la connaissance qu'IDC a de leurs offres de services et de leurs capacités en matière de sécurité. Les fournisseurs ont été évalués en fonction de leurs capacités actuelles et de leurs stratégies futures pour fournir des services aux clients sur le marché canadien.

Yogesh Shivhare, directeur de la recherche, cybersécurité, chez IDC Canada, dit que « Le marché canadien des services de sécurité est très varié et comprend des fournisseurs de services de sécurité non diversifiés et gérés, des fournisseurs de télécommunications, des fournisseurs de technologies de sécurité, des fournisseurs de MDR et des sociétés de conseil en sécurité qui se livrent à une concurrence féroce sur ce marché. Chacun de ces fournisseurs est doté de capacités uniques qui peuvent répondre aux besoins spécifiques et uniques de toutes les organisations canadiennes. Le talent et l'expertise en matière de sécurité, le leadership technologique et la disponibilité de services de sécurité avancés tels que la MDR sont parmi les principaux facteurs de différenciation du marché canadien des services de sécurité. »

À propos d'IDC

International Data Corporation (IDC) est le principal fournisseur mondial en matière d'information commerciale, de services de conseils et d'événements sur les marchés des technologies de l'information, des télécommunications et des technologies grand public. IDC aide les professionnels des TI, les chefs d'entreprise et les membres de la communauté financière à prendre des décisions basées sur des données factuelles pour leurs achats de produits et services technologiques et leurs stratégies d'affaires. Plus de 1 100 analystes d'IDC partagent leur expertise mondiale, régionale et locale au sujet de la technologie, des possibilités et tendances de l'industrie dans plus de 110 pays. Depuis 50 ans, IDC formule des conseils stratégiques pour aider ses clients à atteindre leurs principaux objectifs opérationnels. IDC est une filiale d'IDG, la première société mondiale spécialisée dans la technologie, les médias, les événements et la recherche.

IDC Canada

33, rue Yonge, bureau 902
Toronto (Ontario) Canada, M5E 1G4
Twitter : @IDC
blogs.idc.com
www.idc.com