

IDC MarketScape

IDC MarketScape : marché canadien des services de sécurité 2018 Évaluation des fournisseurs

Kevin Lonergan

David Senf

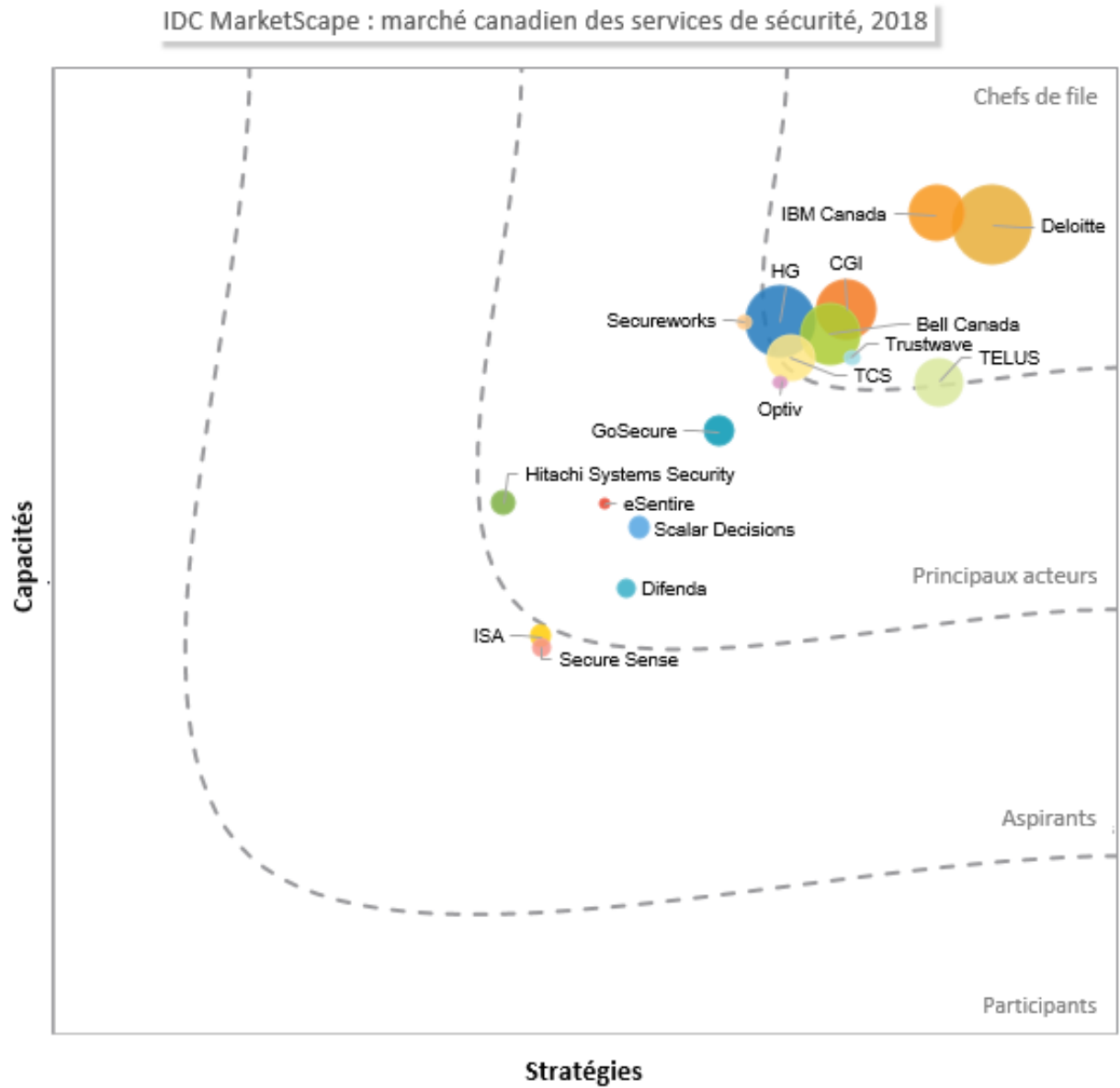
DANS CET EXTRAIT

Le contenu de cet extrait est tiré directement du document IDC MarketScape: Canadian Security Services 2018 Vendor Assessment, par Kevin Lonergan et David Senf (no CA43005218). Les sections suivantes sont intégralement ou partiellement incluses dans cet extrait : Opinion d'IDC, Critères d'inclusion des fournisseurs dans l'évaluation IDC MarketScape, Conseils essentiels à l'intention des acheteurs, Profil sommaire des fournisseurs, Annexe. La figure IDC MarketScape (figure 1) est comprise également dans l'extrait.

FIGURE IDC MARKETSCAPE

FIGURE 1

Évaluation IDC MarketScape des fournisseurs de services de sécurité au Canada



Source : IDC, 2018

Veuillez vous reporter à l'Annexe pour connaître le détail de la méthodologie, de la définition du marché et des critères de notation.

OPINION D'IDC

En utilisant le modèle IDC MarketScape, IDC a comparé 17 fournisseurs de service de sécurité qui exercent des activités et possèdent des clients au Canada. Une entrevue avec chacun des fournisseurs a été faite dans le cadre de ce processus, ainsi qu'avec un ou plusieurs de leurs clients (lorsque nous avons eu accès à ces clients). La majorité des fournisseurs étaient inclus dans l'évaluation de 2017 (IDC MarketScape: Canadian Security Services 2017 Vendor Assessment) (IDC no CA41971017, février 2017). Cette année, cinq fournisseurs de plus ont été évalués. Les participants sont des fournisseurs de solutions de sécurité non diversifiées, des cabinets d'experts-conseils en technologies de l'information, des intégrateurs de systèmes et de grandes multinationales du secteur de la sécurité. L'étude a permis à IDC Canada de déterminer huit chefs de file, sept principaux acteurs et deux aspirants au sein du marché canadien des services de sécurité. Les chefs de file offrent une gamme complète de services pouvant répondre aux besoins des plus petites aux plus grandes entreprises au moyen du plus vaste ensemble de capacités. Toutefois, toutes les solutions des fournisseurs ne constituent pas nécessairement la meilleure option pour toutes les entreprises, car la tarification, les niveaux de service de soutien et d'autres variables sont évalués différemment en fonction des besoins. À titre d'exemple, le budget représente l'obstacle principal à l'amélioration de la sécurité pour les organisations canadiennes et, pour certaines d'entre elles, il peut être tout aussi important, voire plus important, de trouver un fournisseur de services de sécurité qui peut leur offrir une solution à un prix adéquat plutôt qu'une gamme étendue de services. Les fournisseurs classés comme aspirants et comme principaux acteurs peuvent ainsi offrir une solution jugée optimale par certaines organisations. Voici les principaux facteurs de différenciation des fournisseurs de services de sécurité qui exercent des activités au Canada :

- Leur présence canadienne, incluant des partenaires intermédiaires, des centres de gestion de la sécurité (CGS), le nombre de leurs bureaux, du personnel de vente, des ingénieurs en sécurité, des développeurs, des analystes et des équipes de recherche ainsi que leur couverture géographique à travers le Canada.
- La capacité de gérer des dispositifs dans toute la gamme des produits de sécurité (gestion unifiée des menaces [UTM - unified threat management], systèmes de prévention d'intrusion [IPS - intrusion prevention system], gestion de contenu et réseau privé virtuel [RPV]) pour un large éventail de fournisseurs d'équipement et de logiciels.
- L'étendue des services professionnels incluant la stratégie et la planification en matière de sécurité, 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.
- La prise en charge des plateformes de gestion de l'information et des événements de sécurité (SIEM - security information and event management) et la capacité d'en améliorer le rendement.
- Des capacités en matière de sécurité en nuage incluant la sécurité de l'information provenant du nuage et la sécurité à l'intérieur du nuage.
- La prise en charge des solutions de sécurité pour les points d'extrémité, et la réponse aux menaces et les solutions de sécurité de prochaine génération aux points d'extrémité.
- La capacité de participer à des recherches sur la sécurité des TI ou de diriger ces recherches en faisant appel à un partenariat avec un établissement d'enseignement postsecondaire, à leur propre laboratoire ou à un partenariat avec une organisation de sécurité.

- L'utilisation de l'apprentissage automatique et de technologies d'analytique évoluées pour améliorer la qualité et la prestation des services de sécurité.
- Des solutions comportant différentes catégories de service.
- Un portail pour la clientèle et des fonctions de production de rapports.
- La capacité de regrouper les services autres que les services de sécurité/d'offrir un guichet unique.
- La capacité de s'adapter aux exigences des clients en matière de sécurité, tant sur le plan technique que sur celui de la valeur opérationnelle.

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

Pour être inclus dans l'évaluation IDC MarketScape sur les services de sécurité au Canada pour 2018, les fournisseurs devaient répondre aux critères suivants :

- **Avoir une présence au Canada.** Il était possible de satisfaire à ce critère en ayant un centre de gestion de la 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 offerts.** Les fournisseurs doivent offrir un éventail de services de sécurité gérés et professionnels.
- **Revenus associés aux services de sécurité de plus de 2 millions \$ pour l'année 2017.** Les revenus provenant de la revente d'équipement ou de logiciels ne sont pas inclus.

CONSEILS ESSENTIELS À L'INTENTION DES ACHETEURS

L'évaluation des nombreuses capacités actuelles d'un fournisseur de services de sécurité, y compris son adaptation à vos besoins sur le plan des TI et des affaires peut constituer un long processus. Le choix d'un conseiller de confiance exige un contrôle diligent concernant nombre de facteurs. IDC a évalué les critères essentiels dont les organisations doivent tenir compte pour comparer les fournisseurs. Voici les éléments clés dont vous devez tenir compte :

- **Planifiez.** Cela est important pour bien comprendre les besoins de votre organisation en matière de sécurité avant de choisir un fournisseur. Pour vous assurer de classifier adéquatement l'ensemble des actifs de votre réseau, IDC vous recommande d'utiliser les cadres de travail courants de la cybersécurité, comme NIST, ISO 27001/27002 et CIS. Une bonne visibilité de votre réseau vous aidera à choisir les services et le fournisseur appropriés.
- **Faites une mise en correspondance de vos exigences et des capacités du fournisseur.** Les participants à cette étude ont été évalués en fonction de leur capacité à offrir tout service aux entreprises de toutes tailles dans n'importe quel marché vertical. Leurs services peuvent ne pas répondre aux besoins de toutes les organisations. Les fournisseurs de solutions non diversifiées, les télécommunicateurs, les cabinets d'experts-conseils et les autres fournisseurs offrent tous des capacités uniques. Il est important d'évaluer les avantages et les défis liés aux services de chacun.
- **Utilisez les renseignements sur les menaces et l'apprentissage automatique.** Les renseignements sur les menaces et les modèles d'apprentissage automatique sont utilisés pour compléter ou remplacer les solutions traditionnelles de gestion d'information et d'événements de sécurité. L'acheteur doit vérifier si le fournisseur de services de sécurité avec lequel il envisage de travailler possède une feuille de route pour la fourniture de renseignements de pointe sur les menaces (comme l'analyse du comportement des utilisateurs).
- **Vérifiez si des services de sécurité en nuage sont offerts.** La gestion des identités et de l'accès dans le nuage et les capacités de surveillance du nuage deviendront de plus en plus importantes pour les organisations alors que l'adoption des services d'informatique en nuage se poursuit. Cela est particulièrement vrai dans le cas des déploiements de nuages hybrides où l'authentification unique et l'approvisionnement des utilisateurs se compliquent. Le filtrage à l'entrée et à la sortie du trafic, peu importe le type de déploiement utilisé pour l'acheminement en amont ou en aval de vos données, constitue aussi un élément très

important. Les coupe-feu traditionnels, la détection et la prévention d'intrusion, la prévention de la perte des données et d'autres filtres hérités de l'ancien univers des TI continuent d'être pertinents dans le contexte du nuage (en particulier pour les environnements IaaS et PaaS).

- **Déterminez le lieu de résidence des données.** Bien que les lois canadiennes sur l'emplacement de conservation des données (et les règles sur la divulgation imposées par les États-Unis, comme le Patriot Act) touchent uniquement un petit nombre d'organisations et une petite quantité de données, nombreux sont ceux qui sont malgré tout inquiets à l'idée de voir les données traverser la frontière. Mis à part les problèmes de perception des clients, il y a vraisemblablement peu de raisons de se préoccuper de l'endroit où sont conservées les données, mais certains acheteurs souhaiteront savoir à quel emplacement le fournisseur pourra stocker ou envoyer leurs données.
- **Regroupez les services.** Compte tenu de la grande diversité d'entreprises de télécommunications, d'intégrateurs de systèmes et de fournisseurs de produits qui offrent des services de sécurité sur le marché, il est possible de réaliser des économies ou, à tout le moins, de simplifier la gestion des relations grâce au regroupement de multiples services. Les acheteurs devraient consulter plusieurs fournisseurs afin de déterminer s'ils peuvent obtenir une solution de sécurité qu'ils pourraient regrouper avec d'autres produits et services.
- **Évaluez les portails clients.** Les portails clients offrent un aperçu Web pratique de tous les aspects liés à la sécurité sur le réseau ainsi que des « objets » connectés au réseau. Les portails ont évolué et sont devenus plus qu'un simple outil de rapports. Les principales solutions offertes comprennent des éléments visuels interactifs, des tableaux de bord définis par l'utilisateur et des fonctions de production de rapports de vérification et de santé.

PROFILS SOMMAIRES DES FOURNISSEURS

Cette 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. Bien que chacun des fournisseurs ait été évalué en fonction de chacun des critères définis à l'Annexe, la description que nous fournissons ici constitue un résumé des forces et défis de chaque fournisseur.

Bell Canada

Selon l'analyse d'IDC et la perception des acheteurs, Bell Canada est un chef de file IDC MarketScape du marché des services de sécurité au Canada.

Bell Canada exploite trois centres de gestion de la sécurité et de multiples installations où travaillent plus de 300 spécialistes de la sécurité. Bell Canada offre des services de sécurité aux moyennes et grandes entreprises de nombreux marchés verticaux par l'entremise de Bell Marchés Affaires. Bell possède une clientèle importante au pays, en particulier au Canada atlantique, au Québec, en Ontario et au Manitoba.

En tant que plus grand télécommunicateur au Canada, prenant en charge le volume de trafic Internet le plus élevé au pays, Bell détient un avantage concurrentiel grâce à la possibilité de recueillir sur son propre réseau les renseignements sur les menaces. Utilisant les réseaux définis par logiciel et la virtualisation des fonctions réseau, les fournisseurs canadiens de services de communication ont déployé des efforts pour offrir à leurs clients, par l'entremise de leurs réseaux, des fonctions de sécurité liées à la technologie de réseau en tant que service (environnement NaaS). Actuellement, Bell offre la protection DDoS en tant que service, qui bloque les attaques avant qu'elles atteignent l'environnement du client, les empêchant ainsi de saturer les appareils de sécurité installés dans les

locaux du client. Bell travaille à virtualiser une plus grande partie de la gamme des produits de sécurité TI, menant actuellement des projets pilotes en vue d'offrir les fonctions complètes de coupe-feu de prochaine génération. L'entreprise prévoit d'offrir ces services en 2018.

Bell offre une gamme complète de services gérés sur place et de services de surveillance traditionnels. Elle propose aussi des services de gestion d'information et d'événements de sécurité hébergés dans le nuage, ainsi que des solutions de sécurité de messagerie. En outre, Bell offre une vaste gamme de services professionnels de sécurité, exécutés par une équipe comptant plus de 100 conseillers. Les services professionnels comprennent la gestion des risques de sécurité, la stratégie et la conformité, la protection de l'infrastructure et du réseau, la détection évoluée des menaces et la gestion des identités, des données d'authentification et des accès.

Tirant avantage de l'apport de tiers en matière de renseignements sur les menaces et de la visibilité offerte par son propre réseau, Bell offre des renseignements sur les cybermenaces aux clients de ses services Internet d'affaires et de ses services de protection contre les attaques DDoS dans le cadre de leur abonnement. Les renseignements sur les cybermenaces sont recueillis par des analystes de premier plan qui utilisent un moteur de corrélation fondé sur l'apprentissage automatique en vue d'obtenir de l'information de meilleure qualité.

Afin de favoriser le développement de talents dans le domaine de la sécurité au Canada ainsi que son propre recrutement, Bell a annoncé récemment la formation d'un partenariat avec l'Institut canadien sur la cybersécurité de l'Université du Nouveau-Brunswick. L'entreprise cherche activement à établir des ententes similaires avec d'autres établissements universitaires.

Forces

En tant que télécommunicateur, Bell peut offrir un guichet unique pour la connectivité, la communication, l'hébergement et la sécurité TI. Les clients peuvent ainsi simplifier les relations avec les fournisseurs, la facturation et la gestion tout en tirant possiblement avantage de meilleurs prix grâce au regroupement des services. Avec le service de renseignements sur les cybermenaces, il est possible d'améliorer les solutions traditionnelles de gestion de l'information et des événements de sécurité grâce à des modèles d'apprentissage automatique reposant sur des données propres au Canada à l'échelle du télécommunicateur.

Défis

Bell offre des solutions de sécurité d'infrastructure-service (IaaS) et de plateforme-service (PaaS) pour ses propres centres de données, mais n'offre pas encore de services de gestion ou de surveillance de plateformes de tiers, comme AWS et Azure.

ANNEXE

Le marché canadien des services de sécurité maintient sa forte croissance. De tous les marchés des services de sécurité, celui des services gérés offre encore la plus solide performance alors que les organisations canadiennes peinent à trouver du personnel de sécurité qualifié et les budgets nécessaires pour la mise en place d'une solution de sécurité interne adéquate et d'une protection assurée tous les jours, 24 heures sur 24.

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'évaluation 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'un comité d'examen composé 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

Services de sécurité

Les services de sécurité s'appuient sur une intégration globale de toutes les activités nécessaires à la planification, la conception, l'élaboration et la gestion de la sécurité de l'information dans l'ensemble de l'infrastructure de TI de l'entreprise. Ces services peuvent être achetés distinctement ou regroupés avec d'autres services. Dans le cas d'un achat de services de sécurité distincts, le client aura établi une entente avec le fournisseur de services pour l'achat de services principalement axés sur la sécurité, alors que dans le cas d'un achat de services de sécurité groupés, le client aura conclu une entente avec le fournisseur de services pour un projet de services de TI de plus grande envergure dont la sécurité ne constitue qu'une petite composante. Les services de sécurité des TI sont fournis par des intégrateurs de systèmes, des fournisseurs de logiciels/d'équipement, des revendeurs de

technologie ainsi que des spécialistes et des sociétés d'experts-conseils en gestion. Ils sont axés sur la mise en œuvre, la gestion, l'exploitation et la vérification des systèmes de TI pour assurer la sécurité des biens matériels ou des renseignements sensibles. Pour une explication détaillée à propos des services de sécurité, consultez le document IDC's Worldwide Security Services Taxonomy, 2016 (Taxonomie des services de sécurité offerts dans le monde, 2016) (IDC no US41053315, mars 2016).

Critères relatifs aux stratégies et aux 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 pour mesurer le succès de la stratégie : Services de sécurité au Canada

Critère d'évaluation de la stratégie	Définition du sous-critère	Pondération du sous-critère
Stratégie relative à la fonctionnalité et à l'offre		
Offre planifiée de services de sécurité gérés (lancement l'année suivante)	Ajout de services dans l'ensemble des services de sécurité gérés, comme la gestion de l'information et des événements de sécurité, la gestion d'appareils et la surveillance des points d'extrémité afin de combler les écarts existants	15,0
Offre planifiée de services de sécurité professionnels (lancement l'année suivante)	Ajout à l'ensemble des services professionnels (expertise judiciaire, incidence, réponse, conformité, etc.) pour combler les écarts	15,0
Livraison		
Livraison en nuage	Ajout de services pour combler les écarts ou accroître les capacités à offrir une protection de l'information provenant du nuage et la sécurité à l'intérieur du nuage (une pondération supplémentaire est accordée aux organisations qui investissent de façon importante dans ces secteurs)	10,0
Facteurs financiers/financement		
Profit et croissance	Croissance des revenus prévue du fournisseur dans l'ensemble des services de sécurité gérés et des services professionnels en 2018 (une pondération supplémentaire est accordée aux organisations ayant une forte croissance des revenus pour l'année)	10,0
Rythme de la R-D/productivité		
Stratégie de R-D globale	Investissements du fournisseur relatifs à la création de propriété intellectuelle au cours de l'année suivante (lorsque le fournisseur ne fait pas de recherche en interne, les partenariats avec des fournisseurs de premier plan sont pris en considération à la place)	10,0
Croissance		
Croissance géographique	Selon la zone de couverture du fournisseur, plans visant à combler les écarts relatifs aux bureaux, aux installations ou aux CGS dans l'ensemble du Canada	10,0
Croissance de la clientèle	Accroissement de l'évolutivité des services du fournisseur grâce à l'accroissement des ressources d'appoint, à la commercialisation de solutions comportant différentes catégories de service ou à l'amélioration du portail client afin d'accroître la portée ou la convivialité des services	10,0
Stratégie d'affaires		

TABLEAU 1

Indicateurs clés pour mesurer le succès de la stratégie : Services de sécurité au Canada

Critère d'évaluation de la stratégie	Définition du sous-critère	Pondération du sous-critère
Gestion des employés	Plans du fournisseur en vue de travailler plus étroitement avec des établissements universitaires à des fins de recrutement ou de participation à l'éducation communautaire	10,0
Stratégie de pénétration des marchés		
Marketing et vente	Plans du fournisseur en vue d'accroître les ressources d'appoint en vente ou en marketing ou d'intégrer des partenaires intermédiaires	10,0
Total		100,00

Source : IDC, 2018

TABLEAU 2

Indicateurs clés pour mesurer le succès lié aux capacités : Services de sécurité au Canada

Critère d'évaluation des capacités	Définition du sous-critère	Pondération du sous-critère
Capacités en matière de fonctionnalités ou d'offres		
Capacités essentielles	Capacité du fournisseur à servir le marché canadien (une plus grande pondération est accordée pour les CGS, les bureaux et les installations qui sont exploités dans l'ensemble du Canada)	10,0
Degré du nuage	Capacité à offrir une protection de l'information provenant du nuage et la sécurité à l'intérieur du nuage (une plus grande pondération est accordée aux organisations qui offrent une gamme complète de services en nuage et qui peuvent gérer les environnements de nuage public populaires)	10,0
Adaptation aux segments de marché	Échelle de services des fournisseurs capables d'offrir des services aux organisations de toutes tailles (une plus grande pondération est accordée aux fournisseurs qui ont une vaste clientèle et des modèles de solutions comportant différentes catégories de service)	10,0

TABEAU 2

Indicateurs clés pour mesurer le succès lié aux capacités : Services de sécurité au Canada

Critère d'évaluation des capacités	Définition du sous-critère	Pondération du sous-critère
Analyses prédictives	Capacité à offrir des services d'analytique aux fins de la détection des maliciels et de la réponse qui s'impose (une plus grande pondération est accordée aux ajouts personnalisés de services de gestion de l'information et des événements de sécurité, de modèles d'apprentissage automatique et de sources de renseignements sur les menaces)	10,0
Portail clients	Portails ayant évolué pour devenir plus qu'un simple outil de rapports (une plus grande pondération est accordée aux portails présentant des éléments visuels interactifs, des tableaux de bord définis par l'utilisateur et des fonctions de production de rapports de vérification)	10,0
Gamme de services		
Offres de services gérés	Capacité à offrir des services gérés (une plus grande pondération est accordée pour une gamme complète de services de gestion et de surveillance d'appareils dans l'ensemble du réseau et des points d'extrémité, y compris la gestion des identités)	10,0
Services connexes (mise en œuvre, conseil, etc.)	Capacité à offrir des services professionnels (une plus grande pondération est accordée pour une gamme complète de services de gestion et de surveillance d'appareils dans l'ensemble du réseau et des points d'extrémité, y compris la gestion des identités)	10,0
Avantages liés à une gamme de produits et services		
Gamme d'offres interreliées	Capacité à offrir un guichet unique pour les produits, les services ou la connectivité (une plus grande pondération est accordée aux fournisseurs capables de regrouper les services et les solutions pour les clients)	5,0

TABLEAU 2

Indicateurs clés pour mesurer le succès lié aux capacités : Services de sécurité au Canada

Critère d'évaluation des capacités	Définition du sous-critère	Pondération du sous-critère
Stratégie de pénétration des marchés		
Marketing	Utilisation intensive des campagnes de marketing (une plus grande pondération est accordée aux fournisseurs qui utilisent activement la publicité numérique, dont les sites Web sont excellents et qui mènent des campagnes régionales ou nationales/entretiennent des relations communautaires)	5,0
Ventes et distribution	Capacité à vendre dans l'ensemble du Canada (une plus grande pondération est accordée aux fournisseurs qui ont une vaste équipe de vente à l'échelle nationale ou qui font appel à des partenaires intermédiaires)	5,0
Capacités commerciales		
Éducation communautaire	Engagement auprès du milieu de la sécurité (une plus grande pondération est accordée aux fournisseurs qui sont actifs au sein des groupes de sécurité et dans le cadre de conférences sur la sécurité et qui publient des contenus gratuits)	5,0
Gestion des employés	Capacité à recruter de nouveaux talents et à restreindre le roulement du personnel (une plus grande pondération est accordée aux fournisseurs qui collaborent avec des universités dans le cadre de programmes de recrutement ou d'enseignement coopératif et qui offrent des avantages aux employés en vue de les conserver)	5,0
Prestation du service à la clientèle		
Service à la clientèle	Centre de gestion de la sécurité en activité 24 heures sur 24 et 7 jours sur 7; centre d'appels ouvert 24 heures sur 24	5,0
Total		100,0

Source : IDC, 2018

A propos d'IDC

IDC est un acteur majeur de la Recherche, du Conseil et de l'Évènementiel sur les marchés des Technologies de l'Information, des Télécommunications et des Technologies Grand Public. IDC aide les professionnels évoluant sur les marchés IT et les investisseurs à prendre des décisions stratégiques basées sur des données factuelles. Plus de 1100 analystes proposent leur expertise globale, régionale et locale sur les opportunités et les tendances technologies dans plus de 110 pays à travers le monde. Depuis plus de 50 ans, IDC propose des analyses stratégiques pour aider ses clients à atteindre leurs objectifs clés. IDC est une filiale de la société IDG, leader mondial du marché de l'information dédiée aux technologies de l'information.

IDC Canada

33 Yonge St., Suite 420
Toronto, Ontario Canada, M5E 1G4
Twitter: @IDC
idc-community.com
www.idc.com

Avis de droit d'auteur et sur les marques de commerce

Ce document de recherche IDC a été publié dans le cadre d'un service de renseignements continus IDC, offrant de la recherche écrite, des entretiens avec des analystes, des téléconférences d'information et des conférences. Consultez le site www.idc.com pour plus d'information au sujet des abonnements et des services-conseils offerts par IDC. Pour voir une liste des bureaux IDC à l'échelle mondiale, visitez www.idc.com/offices. Veuillez contacter la ligne d'assistance au 800-343-4952, poste 7988 (ou +1-508-988-7988) ou par courriel à sales@idc.com pour des renseignements sur l'application du prix de ce document pour l'achat d'un service IDC ou pour des renseignements sur des reproductions ou des droits de diffusion sur Internet.

Copyright 2018 IDC. Toute reproduction sans autorisation est interdite. Tous droits réservés.

