Aligner la cybersécurité sur la dynamique du marché et les besoins des clients

Bell

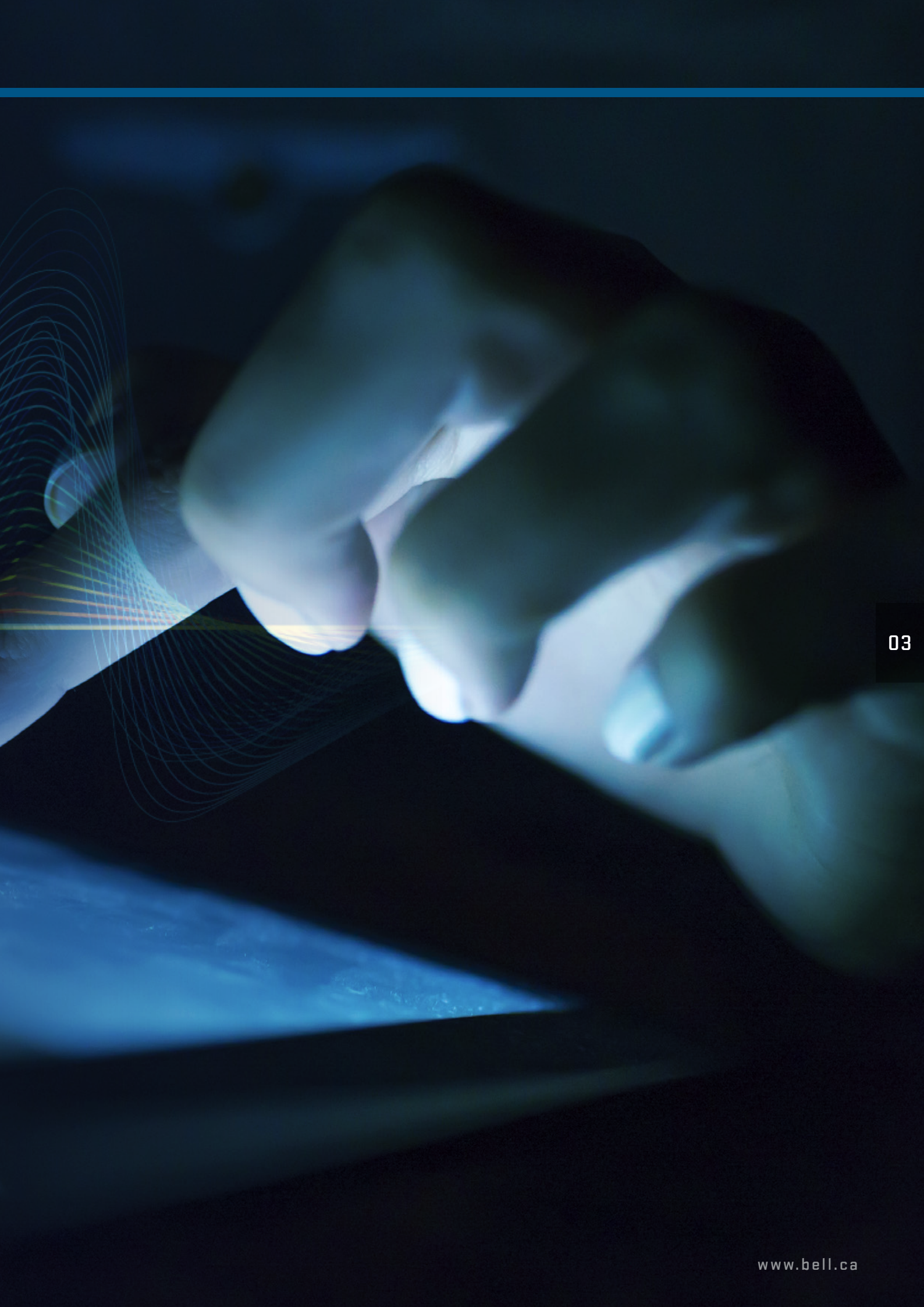
EN ASSOCIATION AVEC

Check Point SOFTWARE TECHNOLOGIES LTD

Akamai

Bell

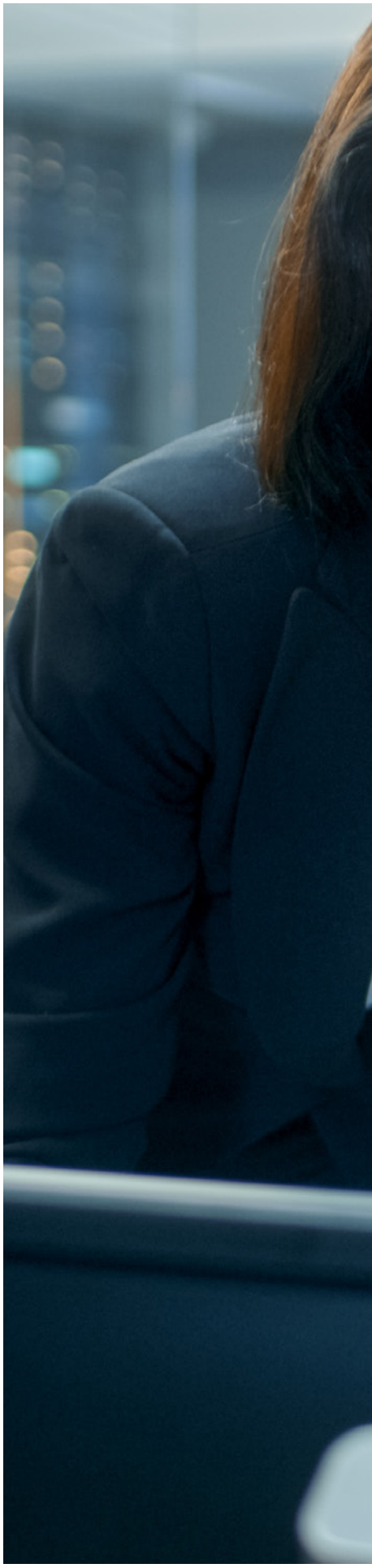
Bell: un leader en matière de cybersécurité constamment à l'affût



Bell est devenu un leader en matière de cybersécurité au Canada, tirant parti d'une mentalité centrée sur le client et d'une forte appréciation des dynamiques du marché.

En tant que réseau de télécommunications le plus important au Canada, Bell est également un leader en matière de cybersécurité au pays. « Nous avons été reconnus comme un leader en matière de cybersécurité par des sociétés telles que IDC (International Data Corporation), et nous accompagnons les clients privés et gouvernementaux à plusieurs niveaux », a déclaré Dominique Gagnon, Directeur général de la pratique de cybersécurité chez Bell. La capacité et la profondeur offertes par le réseau sont combinées à des technologies de pointe et à une stratégie adaptable, tout en demeurant à l'affût du progrès.

Gary Miller, stratège en cybersécurité chez Bell, possédant une longue expérience dans le domaine et une vaste expérience en gestion des affaires, affirme que l'agilité et une stratégie centrée sur le client sont essentielles au succès de Bell. « Ce que nous faisons est orienté par l'écoute de nos clients et en tenant compte de leurs besoins », dit-il.



23,4
milliards $
Revenus (2018)

1880
Année de création

52 790
Nombre d'employés

« Nous avons été reconnus comme un leader en matière de cybersécurité par des sociétés telles que la IDC (International Data Corporation), et nous accompagnons les clients privés et gouvernementaux à plusieurs niveaux »

—

Dominique Gagnon,
Directeur général de la pratique de cybersécurité, Bell

« C'est un processus circulaire, qui nous oblige à être attentif à l'évolution du marché et à l'impact de ces changements sur nos clients. »

En examinant l'évolution de la dynamique du marché, M. Gagnon a constaté cinq tendances majeures qui ont une incidence sur les entreprises canadiennes :

La cybersécurité est une priorité pour les dirigeants et les entreprises canadiennes investissent davantage chaque année dans la cybersécurité. Pourtant, comme le déclare M. Miller, « Le marché des solutions de

CLIQUEZ POUR REGARDER: ‘BELL CYBERSÉCURITÉ’

cybersécurité est chaotique. Tout le monde prétend avoir la solution miracle, et les organisations canadiennes ont besoin de conseils pour les aider à prendre de bonnes décisions. Étant donné que les coûts et les conséquences de ne pas bien faire les choses sont plus importants que jamais, le principal objectif de Bell en matière de sécurité est d’aider nos clients à améliorer leur cybersécurité fondamentale », a-t-il déclaré.

Les approches réactives traditionnelles de la cybersécurité ne suffisent plus, car les cyberattaques deviennent plus sophistiquées, ciblées et persistantes. Au lieu de simplement protéger le périmètre du réseau, M. Gagnon affirme que les menaces modernes nécessitent des protections internes proactives. « Les entreprises reconnaissent qu’elles doivent faire évoluer leur approche et partir du principe que le périmètre a été enfreint. Il s’agit de pouvoir détecter l’attaquant de manière proactive, de déclencher la réponse et de l’exclure. C’est la rapidité avec laquelle vous pouvez y parvenir, et pas seulement votre capacité à les empêcher d’entrer. »


BIENVENUE À LA CYBERSÉCURITÉ DU FUTUR
Check Point Infinity est la première architecture de sécurité consolidée à travers les réseaux, le nuage et les périphériques mobiles, offrant le plus haut niveau de prévention des menaces contre les attaques ciblées, connues et inconnues, afin de vous protéger maintenant et à l'avenir.
PLUS D'INFO
Check Point®
SOFTWARE TECHNOLOGIES LTD

NUAGE • MOBILE • PRÉVENTION DES MENACES

LA COMPLEXITÉ ENGENDRE L'INSÉCURITÉ •

La transformation numérique rapide des entreprises impose des exigences sans cesse croissantes en matière de sécurité. Les opérations informatiques et la sécurité traversent une période de grande perturbation et nous constatons des menaces d'une ampleur sans précédent. Les cyberattaques sont des méga attaques à grande échelle et multi-vecteurs pouvant infliger des dommages importants aux entreprises et à leur réputation.

De plus, la vitesse d'évolution des attaques dépasse le niveau de sécurité déployé par les entreprises; c'est un vrai problème. Le niveau de sécurité déployé par les entreprises ne peut pas être inférieur au niveau des attaques auxquelles elles sont confrontées.

Il existe de nombreuses raisons pour lesquelles les infrastructures de sécurité ont évolué pour être à l'origine du nombre quotidien d'attaques. La plus évidente est que les attaquants ne sont soumis à aucune contrainte : ils peuvent créer et repousser les limites, même imprudemment, dans le développement de techniques nouvelles et avancées. Bien entendu, les entreprises disposent de procédures de contrôle des modifications, de budgets, deconformité et de nombreuses autres contraintes opérationnelles auxquelles elles doivent adhérer, limitant ainsi les progrès en matière de sécurité. Une autre raison est la méthode traditionnelle consistant à utiliser une case à cocher pour créer une infrastructure de sécurité dans laquelle une technologie de sécurité spécifique est déployée pour sedéfendre contre un type d'attaque spécifique ou pour protéger un type d'application spécifique. Cette approche binaire mono-vision, également appelée « meilleure approche », s'est avérée efficace au cours des générations précédentes lorsque les attaques étaient unidimensionnelles, mais les attaques d'aujourd'hui sont tout sauf cela : elles sont multidimensionnelles, multi-étapes, multi-vecteurs et polymorphes.

LES SOLUTIONS D'HIER NE RÉPONDENT PAS AUX DÉFIS D'AUJOURD'HUI •

Malheureusement, alors que les technologies de sécurité prolifèrent et que les clients ont besoin de fonctionnalités informatiques plus avancées pour prendre en charge des capacités telles que l'analyse de données volumineuses, l'hyper-connectivité, la convergence IdO ou l'automatisation, parmi d'autres, les architectures de sécurité efficaces sont très rares. Cela crée de la complexité, augmente les risques et fait monter les coûts.

Prenons, par exemple, le passage généralisé au nuage et l'adoption du Réseau étendu défini par logiciel (SD-WAN). Bien que la connexion directe des succursales à Internet améliore fortement la souplesse et réduit les coûts, elle augmente également considérablement les risques de sécurité.

La numérisation des systèmes opérationnels et industriels augmente la surface d'attaque et le risque de cyberattaques sur les infrastructures critiques et les systèmes de contrôle industriel (SCI). L'ampleur de la croissance dans le domaine de l'IdO présente ses propres risques importants lors de la gestion d'une politique.

DANS QUELLE DIRECTION LE MARCHÉ DE LA CYBERSÉCURITÉ DOIT-IL ALLER? •

Une protection vraiment complète nécessite une nouvelle approche holistique pour évaluer et concevoir la sécurité; cela nécessite une approche structurée qui ne repose pas uniquement sur la détection, mais qui prévient les attaques avant qu'elles ne surviennent. La solution doit combiner une technologie de prévention efficace, une politique de sécurité unifiée et un modèle opérationnel réaliste à mettre en œuvre dans l'environnement informatique actuel, avec un niveau de personnel et de budget raisonnable.

L'objectif est de vaincre toutes les attaques sur tous les vecteurs possibles de manière cohérente et unifiée.

Check Point Infinity est la seule architecture de sécurité qui combine de manière unique plusieurs fonctions de sécurité dans une seule et même solution unifiée de prévention des menaces pour protéger tous vos actifs informatiques - périmètre, centre de données, espace virtuel, nuages, périphériques mobiles et au-delà - contre toutes les attaques connues, auparavant inconnues et les attaques du jour zéro.

L'interface de gestion simple et orientée entreprise réduit la complexité et facilite la mise en place de la sécurité et de la conformité dans le respect des contraintes budgétaires et du personnel. Infinity aide les entreprises à mettre en place une TI agile mais sécurisée, capable de s'adapter et de permettre aux entreprises de s'adapter aux exigences changeantes.

Grâce à la prévention de pointe des menaces, à la gestion de politique orientée entreprise et aux informations sur les menaces basées en nuage, Infinity constitue une base solide pour une stratégie de gestion des risques efficace et durable.

1-800-429-4391
www.checkpoint.com

Check Point®
SOFTWARE TECHNOLOGIES LTD

Alors que les entreprises adoptent de plus en plus d'applications de nuage et hébergent de plus en plus de charges de travail dans le nuage, il est essentiel de s'assurer que des couches de protection sont intégrées. « Nous aidons à décentraliser l'approche de nos clients en matière de sécurité, en facilitant des environnements sécurisés et basés dans le nuage à travers le pays », a déclaré M. Gagnon.

Les entreprises sont également connectées comme jamais auparavant grâce à la convergence de l'Internet

« Notre approche a été d'intégrer différentes capacités technologiques pour offrir à nos clients la meilleure structure de solutions »

Dominique Gagnon,
Directeur général de la pratique de cybersécurité, Bell

des Objets (IdO), à la technologie opérationnelle (TO) et à la prolifération des terminaux. Avec de plus en plus d'applications, d'appareils et de terminaux connectés chaque jour, l'exposition augmente du point de vue de la cybersécurité. « Les organisations subissent de fortes pressions pour que ces nouveaux points de vulnérabilité soient protégés », a-t-il déclaré.

Enfin, les organisations ont reconnu le besoin de mieux contrôler ce qu'elles voient et comment elles le voient. Le défi consiste maintenant à adopter, à gérer et à intégrer des fonctionnalités

PROFIL DE DIRECTION

Dominique Gagnon

Dominique Gagnon est le Directeur général de la pratique de cybersécurité chez Bell et compte plus de 25 ans d'expérience pratique et pédagogique en informatique. Avant son arrivé chez Bell, Dominique occupait le poste de vice-président, Services de consultation chez CGI, en charge des marchés verticaux du gouvernement et du Centre d'excellence canadien en cybersécurité, Ventes, Distribution et Opérations. Dominique possède une expertise en gestion de l'état des profits et pertes, en ingénierie d'affaires, en gestion des engagements stratégiques et en gestion des infrastructures axée sur la cybersécurité. Il a négocié, mis en œuvre et géré de nombreux contrats d'impartition importants et a dirigé des transformations et des transitions pour plusieurs grandes entreprises. Dominique a également servi pendant 12 ans dans les Forces armées canadiennes.

avancées, telles que la détection et l'intervention améliorées et les plates-formes GIES (gestion des incidents et des événements de sécurité), afin d'améliorer la visibilité et le contrôle. Les entreprises ont besoin de la stratégie et du soutien appropriés pour filtrer l'immense quantité de données et d'informations générées par ces solutions avancées, afin d'agir sur les alertes urgentes et de rechercher les menaces de manière proactive.

En tant que l'un des plus importants fournisseurs de solutions technologiques et d'intégration au Canada, Bell est bien équipée pour aider ses clients à évoluer dans cette dynamique de marché, répondant à leurs besoins à tout moment. « Notre approche a été d'intégrer les capacités de différentes technologies afin d'offrir les meilleures solutions à nos clients et de relever les défis que représentent ces 5 tendances », explique M. Gagnon. « Un élément clé est de nous assurer que, dans la mesure du possible, nous ne gaspillons pas les investissements antérieurs de nos clients mais que nous maximisons leur valeur grâce à une intégration efficace. L'objectif est une sécurité simplifiée plutôt qu'une simple sécurité. »

« Nous examinons les métadonnées du trafic réseau et les appliquons à un ensemble de sources de menaces et de modèles de données internes de Bell, afin d'identifier le trafic de menaces potentielles ciblant des secteurs ou des clients particuliers au Canada »

Dominique Gagnon,
Directeur général de la pratique de cybersécurité, Bell

Sécuriser votre stratégie en nuage, sans la complexité

La transformation numérique promet d'accroître l'agilité et l'évolutivité, mais les entreprises d'aujourd'hui sont confrontées à une complexité croissante lorsqu'il est temps de passer au nuage.

Les entreprises doivent gérer plusieurs outils et périphériques, se protéger des menaces plus sophistiquées, surveiller l'activité accrue des robots et offrir des expériences numériques sans faille, le tout avec un budget et des ressources limités.

Comment obtenez-vous tous les avantages du nuage, sans la complexité?

La réponse est Edge.

En exploitant la plateforme Edge Akamai IntelligentMC avec un conseiller en sécurité en nuage comme Bell, vous pouvez adopter la stratégie en nuage qui vous aide le mieux à atteindre vos objectifs commerciaux et à simplifier vos opérations, tout en maintenant la sécurité et les performances.

Découvrez 5 façons de rentabiliser votre stratégie en nuage

Akamai

Intelligent Security Starts at the Edge

« Nous ne parlons pas à nos clients des derniers outils et technologies, nous leur parlons de leurs besoins fondamentaux d'entreprise et de la sécurité qui leur est essentielle »

—

Gary Miller,
Stratège en cybersécurité, Bell

M. Miller précise que cela fournit des couches de protection qui forment un ensemble plus large et plus simple. « Traditionnellement, nous avons toujours parlé de sécurité en profondeur », dit-il. « Nous voyons cette tendance se manifester encore plus aujourd'hui, alors que nous examinons ce que peut fournir une organisation comme Bell. Nous avons une approche de sécurité de bout en bout et nous pouvons intégrer les outils appropriés pour offrir aux clients une visibilité allant de la périphérie jusqu'au coeur de leur réseau d'entreprise. »

PROFIL DE DIRECTION

Gary Miller

Gary Miller est stratège en cybersécurité chez Bell. Depuis plus de 20 ans, Gary aide les gouvernements et les organisations du monde entier à élaborer des stratégies de cybersécurité appropriées et pratiques, pour soutenir leurs objectifs en constante évolution. Gary a occupé des postes de premier dirigeant au sein d'entreprises internationales, notamment dans les fonctions de sécurité d'entreprise et les unités commerciales de cybersécurité. Il a lancé avec succès de nouveaux produits et entreprises en matière de cybersécurité, conseillé les gouvernements sur les stratégies et les politiques nationales en matière de cybersécurité et fait souvent office de conférencier sur les questions stratégiques de cybersécurité.

L'avènement de réseaux virtuels généralisés est également en train de changer le secteur de la cybersécurité. « Les réseaux virtuels offrent aux clients une méthode plus agile et plus sophistiquée de fournir des services réseau. Par ailleurs, chaque fournisseur de télécommunication est affecté par les réseaux virtuels des fournisseurs qui n'ont pas la taille voulue et les technologies nécessaires et qui peuvent réellement laisser leurs clients dans une position vulnérable, » a déclaré M. Gagnon. « Bell adapte sa stratégie pour protéger les déploiements en périphérie de nos services de réseau virtuel, et tirer parti des services en nuage pour prendre en charge une approche plus large et décentralisée de la sécurité. »

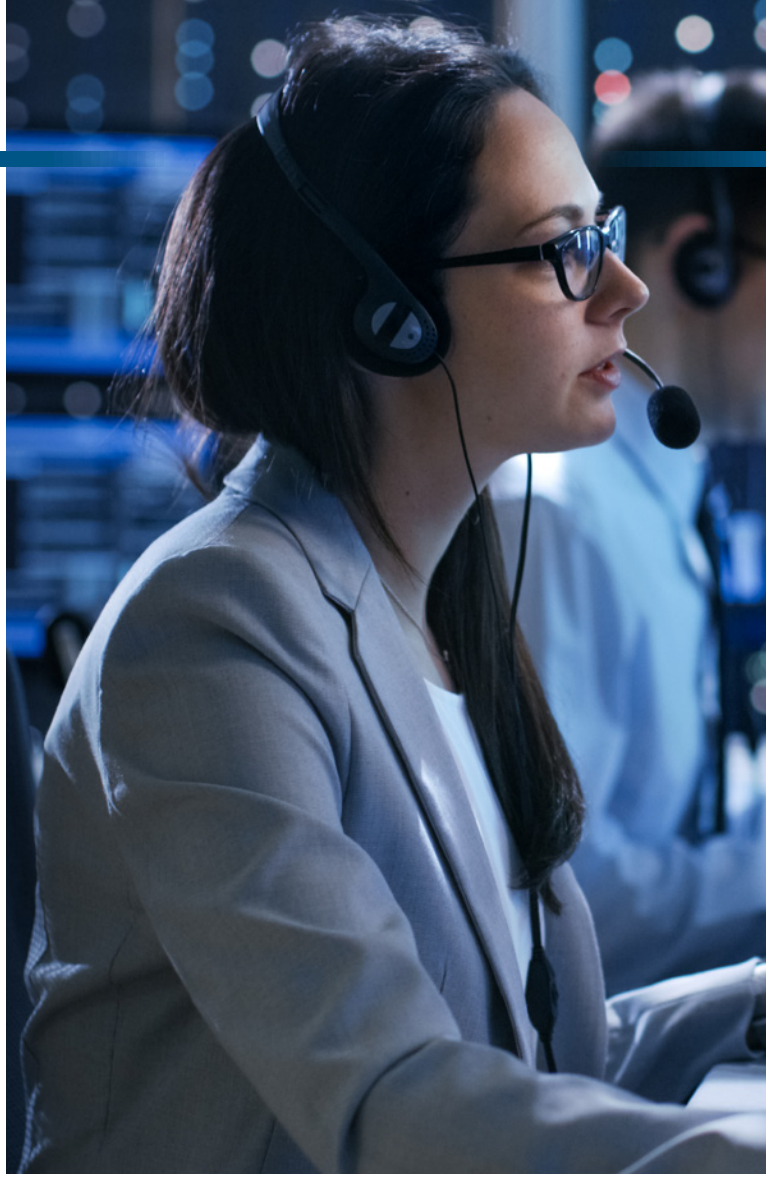
La puissance des solutions de sécurité de Bell est accentuée par des informations basées sur les données. Bell a mis au point une plateforme appelée CTI (Renseignements sur les cybermenaces) qui exploite, avec l'approbation de ses clients, la capacité de son réseau pour créer des informations sur les menaces et les vecteurs

de menaces spécifiques à l'environnement canadien. Le processus, comme l'explique M. Gagnon, ne collecte pas de données, mais reconnaît et évalue les tendances du réseau.

« Nous examinons les métadonnées du trafic réseau et les appliquons à un ensemble de sources de menaces et de modèles de données internes de Bell, afin d'identifier le trafic de menaces potentielles ciblant des secteurs ou des clients particuliers au Canada », a-t-il déclaré. « Ce qui se passe dans le réseau nous donne énormément de renseignements sur les endroits où les problèmes se posent. Nous collaborons avec nos clients pour approfondir leurs jeux de données afin d'obtenir des informations supplémentaires, mais d'une manière générale, nous ne recueillons pas de données transmises, mais uniquement des métadonnées directionnelles, des modèles de trafic, et ainsi de suite ».

Ces opérations existent en dehors de l'environnement réseau des clients, mais Bell déploie des efforts considérables pour offrir ces capacités de détection avancées à ses clients.

« Nous investissons dans l'introduction



des mégadonnées dans l'environnement du client afin qu'il puisse exploiter la technologie et les informations sur les menaces et mieux détecter ce qui se passe au sein de son propre réseau », a déclaré M. Gagnon. « Nous travaillons avec des partenaires d'analyse pour ajouter de telles fonctionnalités à la plate-forme et offrir ces avantages au client. C'est là que se trouve l'avenir. » Pour M. Miller, CTI ajoute une rapidité essentielle au processus de détection des menaces et de réponse, ainsi qu'une capacité de gérer des volumes

PARTENAIRES

Check Point et Akamai :

« Check Point et Akamai sont deux partenaires importants pour Bell. Ce sont des leaders dans leurs domaines respectifs et, grâce à ces partenariats, nous pouvons assurer cette expertise à nos clients », a déclaré Dominique Gagnon, Gérant principale, Service de cybersécurité chez Bell.

« Nous recherchons toujours des entreprises qui sont alignés avec nos objectifs : pour nous aider à clarifier, simplifier et intégrer la gestion de la cybersécurité afin d'assurer la responsabilisation et l'efficacité opérationnelle. Ces deux entreprises sont grandement alignées avec nos objectifs ».

croissants de données. « En réalité, alors que nous passons à la technologie opérationnelle, nous obtenons maintenant plus de données structurées et non structurées. Nous normalisons tous ces ensembles de données très divers et volumineux, appliquons des analyses avancées, une intelligence artificielle et une automatisation pour filtrer à travers cet énorme volume et isolons les éléments les plus critiques et les plus percutants. C'est là où se trouve la valeur des mégadonnées pour l'avenir de la cybersécurité. »

Ultimement, le client est une priorité pour Bell. Qu'il s'agisse de déchiffrer les attentes, de gérer les environnements GIES, de mettre en place des réseaux virtuels ou de renforcer la sécurité interne en plus du contrôle de périmètre, Bell attribue sa profonde compréhension du contexte de la sécurité à son succès en matière de cybersécurité. « Nous sommes très délibérés dans les choix que nous faisons et nous nous engageons continuellement avec nos clients à chaque étape du processus », se réjouit M. Miller. « En mettant la cybersécurité au premier plan, nous avons fondamentalement changé le discours. Nous ne parlons pas à nos clients des derniers outils et technologies, nous leur parlons de leurs besoins fondamentaux d'entreprise et de la sécurité qui leur est essentielle. ■

Bell

www.bell.ca

Bell Canada

Montréal, Canada

T 1 800 668-6878

www.bell.ca