DOCUMENT DES ANALYSTES
Commandité par : Bell

La sécurité infonuagique requiert une approche stratégique qui associe l'adoption de l'infonuagique aux processus de sécurité clés, ainsi qu'aux couches technologiques requises.

L'état de la sécurité infonuagique au Canada : les meilleures pratiques pour de solides résultats

Octobre 2022

Rédigé par : Yogesh Shivhare, directeur de la recherche, Sécurité et infrastructure, IDC

Introduction

L'amélioration des activités commerciales grâce aux services infonuagiques présente des avantages évidents. Toutefois, le parcours permettant de profiter de ces avantages peut se faire au détriment du maintien de la sécurité. En raison de l'évolution constante des technologies de sécurité et des menaces, il existe peu de données sur les mesures prises par les organisations canadiennes pour sécuriser leurs opérations infonuagiques. Alors que l'on pourrait s'attendre à une corrélation entre les résultats en matière de sécurité et l'augmentation de la mise en œuvre des technologies de sécurité, un sondage mené par IDC avec la participation de Bell suggère le contraire. Le sondage a révélé de grandes lacunes dans les approches de sécurité infonuagique au sein des organisations canadiennes : l'adoption de stratégies de sécurité ne suit pas toujours le rythme de l'adoption de l'infonuagique, néanmoins, les organisations continuent d'accélérer les initiatives infonuagiques publiques, hybrides et multiples et, en moyenne, 43 % de leurs données se trouvent désormais dans le nuage public. En outre, les technologies de sécurité seules ne suffisent pas et donnent souvent un faux sentiment de sécurité. Des processus de sécurité appropriés sont essentiels.

EN BREF

STATISTIQUES CLÉS

- 43 % des données des organisations se trouvent désormais dans le nuage.
- Les taux d'adoption de l'infonuagique sont en hausse, mais seulement 52 % des organisations ont été en mesure de se protéger contre une brèche de sécurité.
- Seulement 34 % des organisations ont déployé une gestion de la posture de sécurité infonuagique, laissant les autres exposées à de mauvaises configurations.

POINT CLÉ À RETENIR

Les organisations qui disposent d'importants budgets de sécurité et qui investissent massivement dans les technologies de sécurité peuvent néanmoins voir leur efficacité en matière de sécurité diminuer considérablement si elles n'ont pas mis en place les processus de sécurité adéquats.

Étudier la sécurité infonuagique

Afin de mieux comprendre l'état de la sécurité infonuagique au Canada, Bell a participé à un sondage mené par IDC Canada auprès de plus de 300 moyennes et grandes organisations de divers secteurs et de différentes régions géographiques. Les questions du sondage portaient sur l'adoption de l'infonuagique, les capacités de sécurité et la réussite de l'obtention de résultats solides en matière de sécurité infonuagique. Les résultats sont surprenants, et ils ouvrent une fenêtre sur les meilleures pratiques des organisations qui sont très innovantes en matière d'infonuagique, tout en maintenant une sécurité robuste.

La matrice de l'efficacité de la sécurité infonuagique

À l'aide des résultats du sondage, IDC et Bell ont classé les organisations répondantes dans une matrice de l'efficacité de la sécurité infonuagique (CSEM, en anglais). La CSEM offre aux organisations l'occasion d'apprendre du succès et des erreurs de leurs pairs.

Grâce à notre analyse des résultats de l'étude, les organisations ont été regroupées en quatre catégories distinctes (voir la **figure 1**) en fonction de leur utilisation de l'infonuagique, de leurs compétences, de leurs capacités et de leurs technologies en matière de sécurité, ainsi que de leurs progrès dans la mise en œuvre de processus de sécurité clés.

En raison de sa simplicité et de son omniprésence croissante, nous avons utilisé le cadre de cybersécurité de la NIST comme outil pour communiquer les résultats du sondage dans certains passages du présent document. Si une organisation n'utilise pas le cadre de cybersécurité de la NIST, il existe des processus similaires dans d'autres cadres pour faciliter la comparaison.

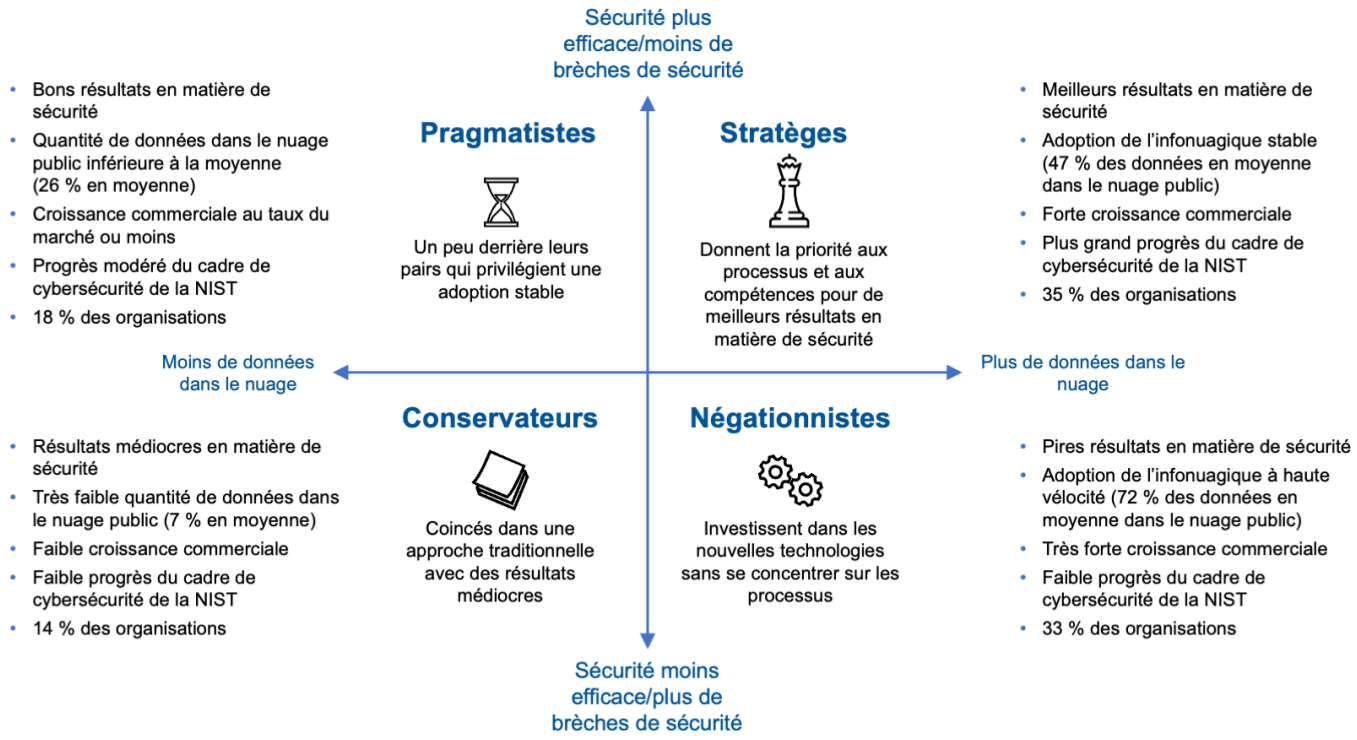
Effectuée en collaboration avec Bell, la recherche a permis de cerner les caractéristiques communes de la façon dont quatre groupes d'organisations abordent la cybersécurité :

- Les **conservateurs** voient généralement les avantages d'une migration vers l'infonuagique, mais ils sont bloqués par des compétences, des processus et des technologies obsolètes. Ils connaissent une croissance commerciale plus lente, une adoption limitée de l'infonuagique et ont une sécurité médiocre. Un déficit technique affecte grandement le succès de leur sécurité.
- Les **négationnistes** font preuve d'une migration rapide vers l'infonuagique et d'une forte croissance de leurs activités, mais ils s'appuient principalement sur les technologies de sécurité pour la protection des données. Ils ont les pires résultats en matière de sécurité parmi les quatre groupes, parce que les processus de sécurité adéquats ne sont pas en place. Ce groupe semble être en déni concernant le fait qu'il doit aller au-delà des technologies de sécurité (dont il achète beaucoup) et se concentrer sur les processus et les personnes.
- Les **pragmatistes** montrent une adoption de l'infonuagique plus lente que la moyenne, mais ils commencent à prendre les bonnes mesures de sécurité. Toutefois, ils ne profitent pas de certains des avantages dont ils pourraient tirer profiter en accélérant leur adoption de l'infonuagique. Parce qu'ils

commencent à faire les bonnes choses du point de vue des processus, ils s'en sortent généralement bien du point de vue des résultats en matière de sécurité.

- Les **stratèges** adoptent une approche mesurée de l'infonuagique, avec une adoption légèrement plus élevée que la moyenne. Ils connaissent une forte croissance commerciale et obtiennent les meilleurs résultats en matière de sécurité. Comme on le voit ci-dessous, il s'agit du groupe que les organisations devraient s'efforcer d'imiter.

Figure 1. Matrice canadienne de l'efficacité de l'utilisation et de la sécurité du nuage



Source : IDC et Bell, 2022

Leçons tirées des stratèges, les responsables de la sécurité

Le groupe situé dans le quadrant supérieur droit de la CSEM est celui des stratèges. Les organisations dans ce groupe ont trouvé le bon équilibre entre la vitesse de l'adoption de l'infonuagique et le temps nécessaire pour la mise en œuvre de processus de sécurité. De plus, elles se concentrent également sur l'amélioration des compétences en matière de sécurité des développeurs, du personnel informatique et du personnel de sécurité. Elles ne s'appuient pas autant sur les solutions technologiques que les négationnistes qui sont moins à l'aise. Elles reconnaissent que l'amélioration de la maturité sur le plan de la sécurité entraîne un investissement continu de ressources et une gestion permanente; il s'agit d'une stratégie et non d'un projet. Elles reconnaissent que le maintien de la sécurité prend du temps et que s'il est planifié correctement, il se fait sans difficulté importante.

Les stratèges adoptent les lignes directrices suivantes pour renforcer l'efficacité de la sécurité de leur nuage :

- **Utilisation de cadres d'application.** Les stratèges ont tendance à adopter des cadres d'application, car ils permettent de s'assurer qu'ils ont couvert l'étendue et la profondeur des exigences du nuage et de sa sécurité. Cela comprend des cadres d'application infonuagiques pour la migration (p. ex., de AWS, Azure, GCP), pour les opérations (p. ex., matrice de contrôle infonuagique de Cloud Security Alliance) et, plus important encore, pour la sécurité (p. ex., NIST, ISO, CIS). L'utilisation d'un cadre d'application permet d'établir l'étendue des capacités de sécurité nécessaires et constitue la base du succès.
- **Concentration sur les processus de sécurité clés.** Il y a d'innombrables contrôles et processus connexes dans les cadres de sécurité qui contribuent à garantir la sécurité infonuagique. Le sondage souligne que l'inventaire continu des services infonuagiques, l'évaluation permanente des configurations du nuage, la gestion des droits et la détection des menaces (incluant la journalisation et la surveillance des services infonuagiques) sont essentiels. Ces processus relèvent en grande partie des fonctions « d'identification » et « de détection » du cadre de cybersécurité de la NIST. Les processus des trois autres fonctions du cadre de cybersécurité de la NIST (à savoir « la protection », « la réponse » et « la reprise ») sont clairement importants, mais l'identification et la détection sont encore plus importantes pour une sécurité infonuagique efficace.
- **Devancer la réalisation des tests et mettre en place des contrôles pour protéger les services actifs.** Les organisations qui sont très avancées sur la voie du DevSecOps (sécurité intégrée dès le début du processus de développement, aussi appelé « réalisation devancée des tests ») ne sont pas nécessairement plus sûres que leurs pairs. La recherche suggère que ce résultat contre-intuitif est dû à la mauvaise exécution des processus au sein des fonctions d'identification et de détection. Contrairement aux négationnistes, les stratèges obtiennent de bons résultats en matière de sécurité à gauche et à droite du déploiement des applications. Ils « protègent les services actifs » en appliquant une sécurité importante à leurs applications en direct.
- **Assurer les compétences en matière de sécurité.** Le personnel qualifié, y compris les architectes infonuagiques, les développeurs natifs du nuage, les opérations et les professionnels de la sécurité sont rares au Canada. Les DPI et les OPSI trouvent souvent difficile de se procurer du personnel avec les compétences nécessaires. La bonne nouvelle est que l'infonuagique permet l'automatisation de certaines tâches de sécurité (p. ex., la gestion de la surface d'attaque, la journalisation, la surveillance, la réponse et la reprise), ce qui permet à des ressources moins qualifiées d'accomplir davantage. Les stratèges sont en avance sur leurs pairs en matière d'automatisation de la sécurité et d'intégration à travers différents outils et environnements infonuagiques, lesquels améliorent leur efficacité en matière de sécurité.
- **Donner la priorité à la protection native de l'infonuagique.** Les charges de travail natives de l'infonuagique nécessitent une sécurité native de l'infonuagique. Une mauvaise configuration des services infonuagiques crée des problèmes de sécurité importants. Les stratèges surveillent les changements dans les configurations du nuage à la fois lors de la mise en place initiale, mais également lorsque des changements surviennent. Les outils et les processus de gestion de la posture de sécurité infonuagique (CSPM) sont essentiels pour détecter les mauvaises configurations et les déviations par

rapport au bon état connu. Étant donné que le nuage comporte un grand nombre de fonctionnalités avec une variété de paramètres et de configurations, les utilisateurs professionnels, le service de TI, les développeurs et d'autres personnes peuvent introduire involontairement de mauvaises modifications. En outre, plus le nombre de services infonuagiques et d'API augmente, plus la probabilité d'une compromission de la sécurité s'accroît. En plus du CSPM, une plateforme de protection des charges de travail en nuage (CWPP) aide à sécuriser les charges de travail natives de l'infonuagique, qu'elles soient optimisées au sein d'un seul fournisseur, d'un environnement hybride ou à travers plusieurs nuages. Elle offre une visibilité sur les vulnérabilités, les comportements anormaux et d'autres protections de sécurité qui vont au-delà des mauvaises configurations.

- **Assurer le contrôle du nuage.** Au-delà du CSPM, il existe des solutions telles que les agents de sécurité d'accès au nuage (CASB) et l'accès réseau à confiance zéro (ZTNA), qui sont importantes pour la découverte/l'inventaire, le contrôle de l'accès, la visibilité et le contrôle des données grâce à la prévention de la perte de données. Elles permettent de contrôler la sécurité bidirectionnelle des données entre l'utilisateur et le nuage. Sans ces solutions, les environnements de nuage public sont sujets aux abus au moyen des TI parallèles et aux menaces externes.

Facteurs à considérer

Pour une majorité d'organisations canadiennes, l'adoption de l'infonuagique est toujours en évolution; ce faisant, une sécurité efficace peut ressembler à une cible mouvante. Voici d'autres lacunes, en plus de celles décrites ci-dessus, où les organisations peuvent échouer à assurer une sécurité infonuagique efficace :

- **Un manque de visibilité et de contrôle :** Le manque de visibilité sur l'ensemble des comptes utilisateurs, des services et du contrôle des changements est un problème qui peut entraîner des brèches de sécurité plus importantes.
- **Une absence de gouvernance infonuagique solide :** Les mauvaises configurations, les erreurs humaines, les contrôles d'accès insuffisants et l'exploitation des vulnérabilités connues découlent souvent d'une absence de gouvernance de la sécurité et du suivi nécessaire pour mesurer continuellement et automatiquement le risque et l'exposition. En outre, une gouvernance adéquate guidera la bonne planification dans les domaines comme la réponse aux incidents et la reprise.
- **Une absence de partage des responsabilités :** Dans un environnement multinuagique avec différents modèles de déploiement (IaaS, PaaS, SaaS), la responsabilité des fournisseurs de services infonuagiques pour les couches de la pile de sécurité varie considérablement. Il est essentiel d'examiner le modèle de responsabilité partagée et de définir clairement les rôles et les responsabilités en matière de sécurisation des données, des API, des services et des informations d'identification des utilisateurs du nuage.

Les stratèges se concentrent sur le personnel et les processus; ils reconnaissent qu'atteindre la maturité de la sécurité est un investissement continu de ressources et une gestion permanente.

- **Un excès de confiance à l'égard de la sécurité traditionnelle :** Les déploiements infonuagiques ne bénéficient pas de la façon dont les défenses complexes sur le site étaient structurées par le passé. Par exemple, la détection, l'investigation et la réponse aux menaces sont différentes dans les environnements infonuagiques. La journalisation et la surveillance de l'ensemble des services infonuagiques sont d'autant plus essentielles, puisque certains contrôles traditionnels sur le site ne s'appliquent pas non plus. Il est important d'identifier et de mettre en place des sources de données de journalisation multinuagiques qui facilitent la collecte et le point d'analyse unique. Les organisations devraient également automatiser dans la mesure du possible (p. ex., pour l'inspection et le triage des alertes, etc.).
- **Des tests contradictoires insuffisants :** Le fait de ne pas étendre l'évaluation des risques et les tests de pénétration de la sécurité aux environnements infonuagiques augmente le risque. Des tests adéquats permettent de hiérarchiser les investissements en matière de sécurité, en plus de minimiser l'exposition immédiate.

Conclusion

Le nuage est essentiel pour la réussite des entreprises. Les choix de sécurité effectués maintenant auront un impact considérable à l'avenir. Les organisations doivent devenir comme les stratèges au sein de la matrice de l'efficacité de la sécurité infonuagique et trouver l'équilibre entre le rythme d'adoption des technologies et l'approche systématique des processus de sécurité et d'amélioration des compétences. Cela permettra d'éviter le piège de l'approche individualiste : un excès de confiance à l'égard des technologies sûres qui a entraîné les pires résultats en matière d'efficacité de la sécurité. En outre, il est essentiel de suivre les cadres de base tels que le cadre de cybersécurité de la NIST et le modèle de capacité infonuagique de Cloud Security Alliance (CSA CCM). Grâce à cet investissement sous-jacent dans les processus et les compétences en matière de sécurité, les organisations peuvent obtenir des résultats solides en matière d'affaires et de sécurité.

Méthodologie

En juillet, avec la participation de Bell, IDC a effectué un sondage auprès de plus de 300 moyennes et grandes organisations de divers secteurs d'activité et de différentes régions géographiques canadiennes, afin de mesurer l'adoption de l'infonuagique, les capacités de sécurité et la mesure dans laquelle les organisations canadiennes réussissent à obtenir de solides résultats en matière de sécurité dans le nuage.

Tous les participants du sondage ont été impliqués dans la stratégie informatique, la budgétisation, les spécifications des exigences techniques ou l'évaluation des fournisseurs et l'autorisation finale d'achat.

Pour organiser ces résultats et aider les organisations à accélérer leurs efforts en matière d'infonuagique et de numérique tout en réduisant la probabilité de brèches de sécurité, Bell et IDC ont élaboré une matrice de l'efficacité de la sécurité infonuagique. La matrice classe les organisations interrogées en quatre groupes distincts, en fonction de leur utilisation du nuage, de leurs capacités de sécurité et de leurs processus de

sécurité, conformément à des cadres populaires tels que le cadre de cybersécurité de la NIST. La répartition des organisations parmi les groupes était la suivante :

- Conservateurs = 14 %
- Négationnistes = 33 %
- Pragmatistes = 18 %
- Stratèges = 35 %

À propos de l'analyste

Yogesh Shivhare [Yogesh Shivhare (idc.com)], directeur de la recherche, Sécurité et infrastructure, IDC

Yogesh Shivhare est directeur de la recherche chez IDC Canada, au sein de l'équipe de recherche des Solutions d'infrastructure et de la sécurité. Il gère la recherche sur la cybersécurité et fournit des données et des analyses sur les tendances industrielles et technologiques qui façonnent le marché canadien de la sécurité.

MESSAGE DU COMMANDITAIRE

Pour en savoir plus sur les solutions de cybersécurité de Bell, visitez www.bell.ca/cybersecurity

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

IDC Custom Solutions