Réussir sa posture de cybersécurité au Canada

Renseignements provenant de l'étude auprès de 400 chefs de la sécurité de l'information canadiens

Bell

Table des matières

Introduction et principales constatations

Alors que le nuage, l'IA générative et d'autres avancées technologiques accélèrent les capacités des entreprises (et de ceux qui les menacent), les chefs d'équipes de sécurité sont confrontés à des décisions difficiles.

Il y a de nombreux choix à faire lorsqu'on évalue la variété croissante de produits, de services, de cadres et de normes qui prétendent être essentiels à la réussite d'un programme de sécurité. Nous avons mené un sondage auprès de 402 entreprises canadiennes des secteurs public et privé afin de découvrir comment elles atteignent des résultats clés et pour déterminer les activités susceptibles de susciter des améliorations. Ces résultats, énumérés ici, font l'objet d'une discussion plus approfondie à la page suivante :

- Atteindre ou dépasser les objectifs de conformité;
- Pouvoir se fier à sa posture de sécurité;
- Obtenir les meilleurs tarifs possibles pour la cyberassurance;
- Disposer d'un personnel de sécurité très satisfait;
- Ne pas avoir subi de faille de cybersécurité au cours des 12 derniers mois.

Dans le cadre du sondage, nous avons également posé des questions sur divers facteurs touchant la culture d'entreprise, la gouvernance, l'harmonisation de l'entreprise et les pratiques de sécurité infonuagique. En identifiant les facteurs et les activités qui correspondent à ces résultats, notre objectif est de fournir aux chefs d'équipes de sécurité une perspective éclairée tandis qu'ils font évoluer les stratégies de protection de leur entreprise, en mettant l'accent sur la sécurisation du nuage.

Dans l'ensemble, les principaux facteurs de réussite de la posture de sécurité du nuage sont les suivants : 1) l'intégration des équipes de sécurité et de développement et exploitation; 2) la mise en place d'une politique d'utilisation acceptable des services en nuage; 3) la capacité des équipes de sécurité à répondre aux besoins de l'entreprise et des TI. Nous examinerons ces facteurs, et bien d'autres, dans les pages qui suivent. Voici les principaux éléments à retenir de l'étude que nous examinerons plus en détail dans ce rapport :

Près des deux tiers des entreprises canadiennes ont subi des failles au cours de la dernière année. Près de la moitié se sont produites dans des environnements en nuage.

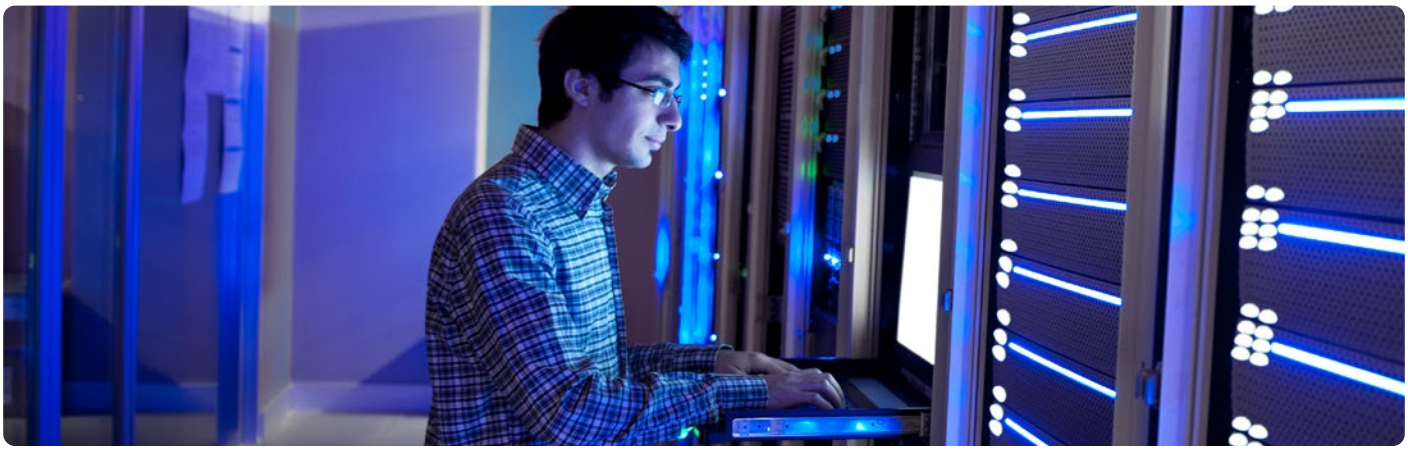
Seulement **1,6 %** des entreprises déclarent avoir obtenu un niveau élevé de succès sur les cinq critères de sécurité que nous avons évalués.

29 facteurs de succès sont associés à des taux de réussite beaucoup plus élevés sur au moins un critère. Dans ce rapport, nous identifions les pôles qui contribuent le plus au succès.

2 Nous identifions deux facteurs qui ont été les plus déterminants pour réduire la probabilité de failles de sécurité.

À propos du sondage

Bell Canada a embauché Maru Group, une firme de sondage professionnelle, pour réaliser un sondage sur un échantillon aléatoire stratifié d'environ 402 professionnels de la sécurité travaillant pour des entreprises au Canada. Les objectifs de réponse ont été fixés de manière à obtenir un équilibre entre les répondants représentant différents secteurs d'activité, provinces et tailles d'entreprise. Les contrôles de qualité ont permis d'éliminer certaines réponses, laissant un échantillon final de 383 répondants pour cette analyse. Vous trouverez les données démographiques de cet échantillon à l'Annexe.



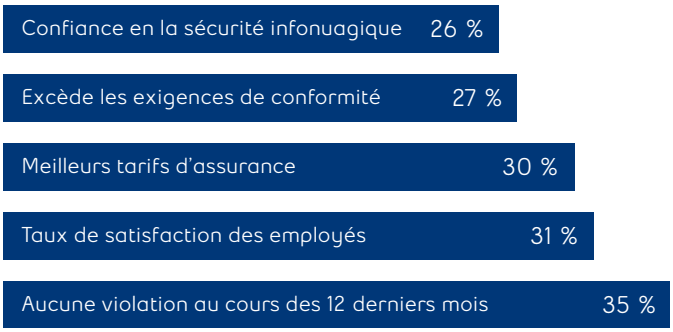
Résultats du programme de sécurité

Ce qui ressort clairement de notre plus récent sondage, ce sont les quelques thèmes communs suivants : si les violations constituent l'indicateur de performance le plus direct de tout programme de sécurité, la plupart des chefs de la sécurité de l'information que nous avons interrogés considèrent que les performances en matière de conformité et la capacité à conserver leur personnel talentueux sont des indicateurs indirects importants.

Lors de l'élaboration de notre sondage, nous avons ajouté une mesure de la confiance globale d'une entreprise dans la sécurité de son nuage ainsi que la perspective indépendante qui accompagne l'évaluation par une cyberassurance. Le sondage posait des questions représentatives permettant d'évaluer le niveau de réussite de l'entreprise sur chacun de ces cinq objectifs.

Ces critères ne constituent pas la référence universelle pour mesurer le succès d'un programme de sécurité, mais ils offrent un bon cadre de mesure pour notre analyse. Voici comment les entreprises ont évalué leur capacité à atteindre chacun de ces résultats. Il convient de noter que de nombreuses entreprises ont fait état d'un niveau élevé de succès sur plusieurs critères, mais que seulement 1,6 % des répondants ont fait état d'un niveau élevé de réussite pour l'ensemble des cinq critères.

Figure 1 : Pourcentage de répondants qui déclarent un niveau élevé de succès, par critère.



- Confiance en matière de sécurité du nuage. 26 % des répondants expriment une grande confiance dans la capacité de leur programme de sécurité à protéger correctement les activités de l'entreprise dans le nuage. Ce taux, le plus bas pour les cinq critères, témoigne de la nature prudente des répondants, en plus des nombreux défis liés à la sécurité dans les environnements en nuage.
- Conformité réglementaire. 27 % des entreprises déclarent dépasser les exigences de conformité et 26 % expriment une grande confiance dans leurs capacités de sécurité infonuagique. La conformité tend à inspirer la confiance, il n'est donc pas surprenant d'obtenir des résultats similaires sur ces critères.
- Cyberassurance. 30 % des répondants affirment que leur entreprise obtient les meilleurs tarifs de cyberassurance. Étant donné que de nombreux assureurs procèdent à des évaluations des risques et à des vérifications préalables pour fixer leurs tarifs, on peut considérer qu'il s'agit d'une évaluation indépendante du niveau de risque que présente chaque entreprise. Il est clair que les entreprises utiliseront d'autres moyens pour valider leur programme de sécurité, mais l'évaluation d'un assureur est une perspective pertinente.
- Satisfaction du personnel. Environ 3 entreprises sur 10 bénéficient d'un taux de satisfaction très élevé des employés chargés de la sécurité. Les résultats plus élevés en matière de satisfaction des employés ont un lien de cause à effet avec la tâche déjà difficile de conserver les talents en sécurité. La réussite au poste, ainsi que la capacité d'innover et d'explorer les technologies et les pratiques les plus récentes, contribue à améliorer la satisfaction des employés.
- Atteintes à la sécurité. Si 35 % des répondants ont déclaré que leur entreprise n'avait pas subi de faille au cours des 12 derniers mois, il convient de noter que certains d'entre eux n'avaient peut-être pas connaissance d'une telle violation. Cette situation ne fait que souligner la conclusion qui en découle : au moins 65 % des entreprises ont connu une faille.

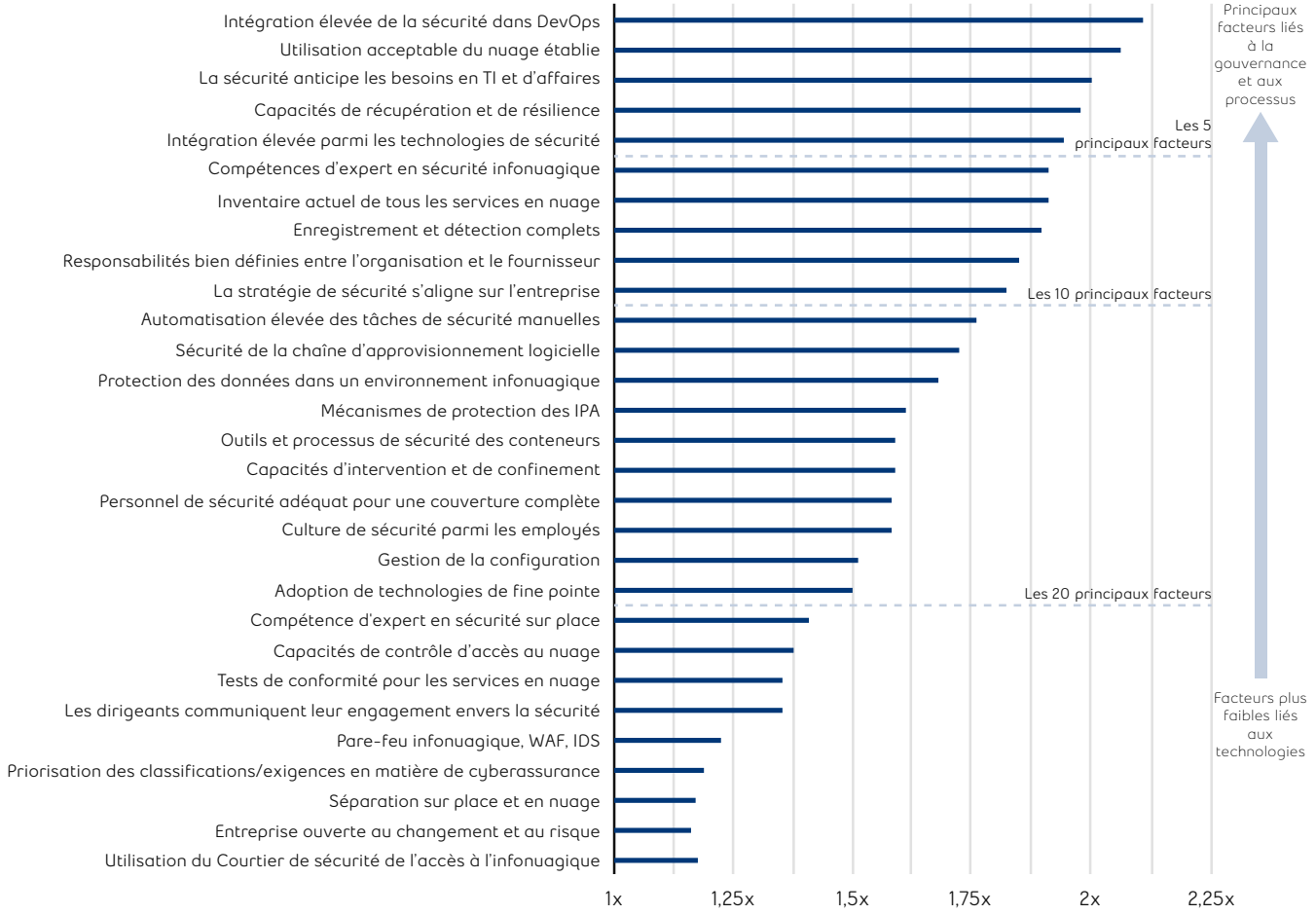
Facteurs de réussite du programme de sécurité

Pour déterminer les facteurs qui sont en corrélation avec les critères de réussite que nous avons choisis, nous avons posé aux répondants de nombreuses questions sur la gouvernance, le personnel de sécurité et les pratiques de sécurité infonuagique de leur entreprise. Les données obtenues nous ont permis non seulement d'établir une corrélation, mais aussi de déterminer dans quelle mesure chaque facteur augmente la probabilité qu'une entreprise s'autoévalue au niveau de réussite le plus élevé pour chaque critère.

En tout, nous avons identifié 29 facteurs en corrélation avec des taux de réussite significativement plus élevés sur au moins un critère. Nous les montrons à la Figure 2, où les chiffres le long de l'axe X représentent l'amélioration moyenne pour chaque facteur sur les cinq critères. **Par exemple : les entreprises qui signalent de solides capacités de reprise après incident et de résilience**

(le 4e facteur le plus élevé) indiquent des taux de réussite deux fois plus élevés que celles qui intègrent moins bien ces facteurs. Nous classerons et mettrons en évidence ces facteurs dans les sections suivantes.

Figure 2 : Facteurs présentant une corrélation positive significative avec au moins un critère de sécurité.



Culture d'entreprise

Dans notre sondage précédent, nous avons appris qu'une dépendance excessive à l'égard de la technologie (au détriment des personnes et de la formation) peut nuire aux résultats. En outre, une mauvaise gouvernance ou une culture de la sécurité inadéquate peuvent nuire même aux meilleurs talents et outils que l'on puisse acheter. Ainsi, avant d'examiner les contrôles techniques, nous commencerons par la gouvernance et la culture.

La Figure 3 énumère les facteurs de gouvernance et de culture que nous avons étudiés en relation avec les cinq critères de notre cadre d'analyse. Les valeurs dans chaque cellule représentent l'augmentation moyenne du taux de réussite sur un critère en corrélation avec ce facteur. **Par exemple : les entreprises qui réussissent le mieux à établir et à appliquer une gouvernance pour l'utilisation acceptable des services en nuage sont deux fois plus susceptibles de déclarer qu'elles dépassent les exigences de conformité**. Les cellules vides du tableau indiquent qu'il n'y a pas d'impact significatif entre le facteur et le critère.

Figure 3 : Augmentation des résultats positifs associés aux facteurs de gouvernance et de culture

		Résultats en matière de sécurité				
		Dépasser de conformité exigences	Haute confiance en matière de sécurité	Faible d'assurance taux	Satisfait de sécurité personnel	Aucune violation
Facteurs d'entrée du programme	Utilisation acceptable du nuage établie	2,4x	2x	2,3x	2,6x	
	Responsabilités bien définies entre l'organisation et le fournisseur	2,1x	2x	2,1x	2,1x	
	La stratégie de sécurité s'aligne sur l'entreprise	2,1x	2,1x	2x	2x	
	Adoption de technologies de fine pointe	2,1x	2,2x		2,1x	
	Culture de sécurité parmi les employés	1,9x		2x	2,1x	
	Les dirigeants communiquent leur engagement envers la sécurité			1,9x	2x	
	Priorisation des classifications/exigences en matière de cyberassurance			2x		
	Entreprise ouverte au changement et au risque					1,9x

Pourquoi les failles sont-elles des observations aberrantes?

Cette situation peut sembler contre-intuitif : le seul facteur de gouvernance qui coïncide avec une réduction significative de la probabilité de signaler une violation est la propension des chefs d'entreprise à accepter le changement et à prendre des risques. En fait, l'ouverture au changement (et au risque calculé) peut se traduire par l'adoption anticipée de nouvelles technologies, l'amélioration du moral des employés et d'autres facteurs.

Établir la responsabilité et l'usage acceptable

L'établissement du niveau de risque pour ce qui constitue ou non un usage acceptable des services en nuage est un facteur général important dans tous les critères. Pour établir des niveaux de risque acceptables, il est essentiel de définir clairement qui est responsable de quel aspect de la gestion du risque. Cette situation concerne la responsabilité interne de l'entreprise, des TI, de la sécurité et d'autres intervenants. Elle est également liée à la responsabilité partagée de la sécurité en nuage dont les spécialistes de la mise à l'échelle assurent la promotion depuis un certain temps. La définition des risques et des responsabilités commence par une bonne gouvernance qui est ensuite mise en œuvre dans de nombreux contrôles de sécurité, y compris la gestion de la configuration en nuage et les contrôles d'accès.

L'harmonisation avec les activités de l'entreprise

Ce n'est pas étonnant : les entreprises qui déclarent harmoniser étroitement leur stratégie d'entreprise et leur stratégie de sécurité sont plus susceptibles d'obtenir de meilleurs résultats dans tous les domaines. Cette situation confère de la crédibilité au rôle récemment créé du responsable de la sécurité de l'information d'entreprise maintenant en place dans certaines grandes entreprises.

En outre, un engagement fort de la direction en faveur des initiatives de sécurité nécessaires à la mise en œuvre de cette stratégie est lié à des taux plus élevés de satisfaction des employés, ainsi qu'à l'obtention des meilleurs tarifs d'assurance (peut-être parce que cet engagement est évident pour les assureurs).

Être ouvert à l'expérimentation

Les entreprises qui déclarent expérimenter et adopter les nouvelles technologies avant les autres ont plus de facilité à satisfaire les auditeurs chargés de vérifier la conformité et le personnel chargé de la sécurité. Ce critère est également associé à des niveaux de confiance plus élevés dans le fait que le programme de sécurité peut correctement protéger les services d'entreprise fonctionnant en nuage. Une culture qui encourage l'expérimentation et les essais peut tirer parti de nouvelles approches natives en nuage pour l'architecture des plateformes et des applications, qui seront sans doute plus sécurisées que les approches traditionnelles (p. ex. vérifications automatisées avant la production et plus grande visibilité et capacité de journalisation des flux de production).

Favoriser une culture de sécurité

Selon les données, une forte culture de la sécurité contribue à stimuler la confiance des entreprises dans les capacités de sécurité du nuage, la satisfaction des employés et la baisse des tarifs d'assurance.

Les deux premiers résultats sont tout à fait logiques : la confiance et la satisfaction sont souvent favorisées par le milieu environnant (tout comme le doute et l'insatisfaction). La corrélation entre la culture et les tarifs d'assurance peut sembler étrange, mais une culture de la sécurité omniprésente est susceptible d'influencer positivement l'évaluation d'un assureur.

Recommandations de Bell

Faites le suivi des mesures importantes

Une bonne gouvernance a besoin du soutien d'une base de mesures saines. L'ensemble des mesures les plus influentes tend à couvrir le plus grand nombre d'actifs. L'élaboration de mesures autour de l'ensemble de vos actifs et de vos expositions est un point de départ naturel.

- Les questions auxquelles vous devez répondre sont les suivantes :
- Quel est mon degré de couverture de la surface d'attaque?
- Comment varie l'exposition?
- Combien de temps faut-il pour résoudre les problèmes?
- À quelle vitesse pouvons-nous réduire les problèmes en suspens?

Échouez rapidement

Créez une culture qui encourage l'apprentissage et l'expérimentation de nouvelles choses. Il faut parfois faire un acte de foi et prendre une direction pour laquelle on ne dispose pas encore de données solides. Pour tirer pleinement parti du nuage, notamment de son architecture flexible, de son développement rapide et de l'automatisation accrue de la sécurité, il faut être ouvert à l'expérimentation dans un cadre bien balisé.

Dans un monde en nuage natif, la gouvernance est plus facilement reflétée dans des logiciels comme la Politique en tant que code pour gérer les risques en temps réel ou limiter les inconvénients de l'expérimentation. Les entreprises qui obtiennent de meilleurs résultats en matière de sécurité indiquent qu'elles acceptent le changement. Par exemple, les entreprises qui utilisent des grands modèles de langage (GML) comme ChatGPT pour les opérations de sécurité en production affichent des résultats de sécurité améliorés.

Facteurs de réussite pour les équipes de sécurité

La Figure 4 présente 20 intersections facteur-critère, dont cinq présentent une amélioration d'au moins 2,5 fois. Pour comparaison, la Figure 2 n'en possède qu'une seule (sur 40). Le personnel est un puissant moteur de résultats positifs.

Figure 4 : Augmentation des résultats positifs associés aux équipes et aux talents

		Résultats en matière de sécurité				
		Dépasser de conformité exigences	Haute confiance en matière de sécurité	Faible d'assurance taux	Satisfait de sécurité personnel	Aucune violation
Facteurs d'entrée du programme	Compétences d'expert en sécurité infonuagique	2,6x	2x	2,6x	2,5x	
	La sécurité anticipe les besoins en TI et d'affaires	2,5x	2,1x	2,2x	2,2x	
	Personnel de sécurité adéquat pour une couverture complète	2,6x			2,3x	
	Compétences d'expert en sécurité sur place		2x		2,1x	

Se faire de nouveaux amis

Dans la dernière section, nous avons vu que les entreprises qui font état d'une approche plus ouverte envers l'adoption des technologies déclarent également qu'il leur est plus facile d'atteindre des résultats élevés sur les critères que nous mesurons. Naturellement, cette situation va de pair avec une collaboration étroite avec les TI et les autres parties prenantes. Les résultats de la Figure 4 corroborent cette approche plus collaborative. Les équipes de sécurité capables de prévoir les besoins de l'entreprise et de l'équipe TI et d'y répondre voient leurs résultats s'améliorer sur quatre des cinq critères.

La collaboration entre l'équipe de sécurité et les autres équipes devient plus importante dans le nuage, où la visibilité des TI et de la sécurité n'est pas toujours évidente. Par exemple, la gestion de la configuration du nuage, la gestion des identités et la sécurité des données sont chacune des domaines où le personnel de sécurité peut ne pas avoir un contrôle total et devoir compter sur la participation rapide d'autres personnes des TI et dans l'ensemble de l'entreprise.

Accroître les effectifs et les connaissances

De nombreuses entreprises confient qu'elles manquent de personnel de sécurité. Qu'il s'agisse de contraintes budgétaires ou de difficultés à pourvoir des postes vacants, il est facile de se sentir dépassé lorsque le personnel est insuffisant. Sans surprise, nous constatons des gains de confiance et de satisfaction parmi les programmes de sécurité qui disposent d'un personnel suffisant pour couvrir les opérations.

Néanmoins, les données attribuent encore plus d'avantages aux équipes de sécurité qui sont hautement qualifiées dans ce qu'elles font. De solides compétences en sécurité du nuage semblent particulièrement efficaces pour améliorer les résultats. Les spécialisations sont importantes et renforcent les capacités globales de protection d'une entreprise, où qu'elle exerce ses activités.

Recommandations de Bell

Allez au-delà des certifications

Les compétences recherchées par les équipes de sécurité couvrent davantage de domaines (p. ex. contrôles natifs en nuage) et s'approfondissent (p. ex. plus de codage). Les compétences techniques traditionnelles et les certifications restent importantes, mais cette étude montre que les connaissances des affaires, les capacités d'intelligence artificielle et de codage ont chacune une influence prépondérante dans les ensembles de compétences indispensables des professionnels de la sécurité. La formation et le recrutement du personnel dans ces domaines sont beaucoup plus importants pour la sécurité en nuage que dans les rôles traditionnels sur place

Élargissez la définition de l'équipe

Pour améliorer la fidélisation du personnel de sécurité, il faut s'efforcer de réduire les frictions qu'il subit en demandant aux autres d'agir (par exemple, corriger les mauvaises configurations, accepter les temps d'arrêt pour les mises à jour, résoudre les problèmes de codage, réduire au minimum les autorisations d'accès, etc.). Cette situation nécessite une entente entre les intervenants d'affaires, les développeurs, les TI et la sécurité sur ce qui constitue un niveau acceptable de risque pour la sécurité, ce qui renvoie à notre section sur la gouvernance et la culture.

Pratiques de sécurité en nuage

Dans cette section, nous décrivons les contrôles techniques et procéduraux qui améliorent de manière mesurable les résultats en matière de sécurité. Après avoir demandé aux répondants d'évaluer la mise en œuvre de diverses pratiques de sécurité en nuage dans leurs entreprises, nous avons ensuite comparé ces réponses aux cinq critères. La Figure 5 présente les meilleures pratiques pour une amélioration globale sur tous les critères.

Figure 5 : Augmentation des résultats positifs associée aux pratiques de sécurité du nuage

Facteurs d'entrée du programme	Résultats en matière de sécurité: Dépasser de conformité exigences	Haute confiance en matière de sécurité	Faible d'assurance taux	Satisfait de sécurité personnel	Aucune violation
Inventaire actuel de tous les services en nuage	2,6x	2x	2,5x	2,5x	
Capacités de récupération et de résilience	2,2x	2x	2,1x	2,6x	
Enregistrement et détection complets	2,2x	1,9x	2,2x	2,2x	
Sécurité de la chaîne d'approvisionnement logicielle	1,9x	2x	1,9x	1,8x	
Protection des données dans un environnement infonuagique	2x		2,3x	2,2x	
Mécanismes de protection des IPA	2,1x		1,8x	2,1x	
Outils et processus de sécurité des conteneurs	2,2x		1,8x	2x	
Capacités d'intervention et de confinement	1,9x		2x	2,1x	
Gestion de la configuration	1,9x		1,8x	1,9x	
Capacités de contrôle d'accès au nuage	2x			1,9x	
Tests de conformité pour les services en nuage	1,9x		2x		
Pare-feu infonuagique, WAF, IDS					2,2x
Séparation sur place et en nuage		1,9x			
Utilisation du Courtier de sécurité de l'accès à l'infonuagique	1,8x				

La liste ci-dessus des pratiques prometteuses pour améliorer la sécurité du nuage est très variée. Nous avons mis en évidence plusieurs thèmes sur différentes pratiques.

Sachez ce que vous protégez

Il y a une raison pour laquelle le cadre de cybersécurité NIST (et de nombreux autres cadres de sécurité) commence par la fonction « Identifier » d'un programme de sécurité. Il est difficile de défendre quelque chose si l'on ne sait pas où il se trouve, comment il est configuré ou si l'on ne sait pas que l'on en dispose. Il est particulièrement important de le faire dans le nuage, où les ressources sont distribuées et éphémères par nature.

Cette constatation appuie nos conclusions selon lesquelles les entreprises disposant d'un répertoire à jour de tous les services en nuage ont enregistré les gains globaux les plus élevés en matière de sécurité. Il est essentiel de savoir ce qui est exécuté ou stocké dans le nuage aujourd'hui pour convaincre les auditeurs, les assureurs ou même votre propre personnel que vous pourrez le protéger de manière adéquate demain. Tous les contrôles de sécurité dépendent de ce point de départ élémentaire, mais difficile à atteindre, qui consiste simplement à savoir quels services sont utilisés et à quoi ils se connectent. Ainsi, la gestion des stocks, la gestion des risques, la gestion des configurations, la gestion de la chaîne d'approvisionnement des logiciels et la gestion de la surface d'attaque sont étroitement liées, et sous-tendent une stratégie globale de sécurité du nuage réussie.

Planifier le succès; bâtir pour l'échec

Le cadre de cybersécurité NIST se termine par « Répondre » et « Rétablir ». Naturellement, l'exécution d'une réponse solide et d'un rétablissement rapide repose en grande partie sur un répertoire à jour des services de nuage, y compris leurs configurations, leurs utilisateurs et leurs données. Les capacités de reprise et de résilience se classent au deuxième rang des facteurs les plus importants pour l'obtention de résultats élevés, tandis que la rapidité de la réaction et du confinement du problème se situe en milieu de peloton.

Pour réagir aux défaillances et rétablir les services, des mécanismes doivent être mis en place pour savoir quand ces défaillances se produisent. Par conséquent, la journalisation et la détection complètes occupent une place importante dans la Figure 5. Bien que notre sondage n'ait pas porté sur ce qui devrait être enregistré et sur les mécanismes de détection les plus efficaces, cette analyse justifie amplement que l'on se pose ces questions au sein d'une entreprise.

Développer des contrôles de protection natifs en nuage

L'architecture et l'administration sont effectuées différemment dans les environnements en nuage. Par conséquent, les protections en nuage ont évolué pour y répondre. Nous en avons la preuve dans la Figure 5, où pas moins de neuf pratiques se rangent sous la bannière de la protection native en nuage.

Ces pratiques vont du portage des contrôles traditionnels sur site vers le nuage (par exemple, les pare-feu), des contrôles pertinents pour l'infrastructure du nuage (par exemple, la sécurisation des API et des conteneurs), et de la prévention de la capacité des adversaires à passer d'une infrastructure sur site compromise vers les environnements du nuage (par exemple, la sécurisation d'« Active Directory »).

Nous voyons également un rappel que les politiques de sécurité du nuage doivent être appliquées (par exemple, par l'entremise d'une passerelle sécurisée d'accès au nuage de la Politique en tant que code, etc.) et que les configurations doivent être continuellement surveillées ou gérées par la mise en place de barrières techniques.

En outre, les entreprises qui développent leurs propres applications de nuage sont encouragées à acquérir une visibilité sur leur chaîne d'approvisionnement en logiciels afin de s'assurer que les bibliothèques tierces vulnérables ne compromettent pas leurs efforts en matière de cybersécurité.

Tirer parti de l'intégration et de l'automatisation

Lors de l'analyse des données sur les pratiques qui sont en corrélation avec les résultats en matière de sécurité, le thème de l'intégration et de l'automatisation est apparu comme particulièrement fort. Nous avons extrait ces données de la Figure 5 pour les mettre en évidence ci-dessous. Par rapport à son prédécesseur, la Figure 6 est nettement plus impressionnante, avec notamment l'effet facteur-résultat le plus fort de l'ensemble des données : l'automatisation poussée des tâches de sécurité est fortement corrélée à l'obtention des meilleurs tarifs d'assurance (et à la validation externe des processus et des contrôles qui l'accompagne).

Figure 6 : Augmentation des résultats positifs associés à l'intégration et à l'automatisation

		Résultats en matière de sécurité				
		Dépasser de conformité exigences	Haute confiance en matière de sécurité	Faible d'assurance taux	Satisfait de sécurité personnel	Aucune violation
Facteurs d'entrée du programme	Intégration élevée de la sécurité dans DevOps	2,6x	2,1x	2,3x	2,6x	
	Intégration élevée parmi les technologies de sécurité	2,5x	2,3x	1,8x	2,2x	
	Automatisation élevée des tâches de sécurité manuelles	1,9x		2,7x	2,2x	

L'automatisation des contrôles de sécurité, comme la gestion de la surface d'attaque, la détection initiale, les éléments des guides des stratégies de réponse et la gestion du contrôle d'accès, est très importante pour la mise à l'échelle des opérations de sécurité.

Recommandations de Bell

Automatisez autant que possible

Il est impossible de le faire sans relever de défis : les contrôles de sécurité critiques du nuage, tels que la gestion de la configuration, peuvent être difficiles à automatiser complètement. Il peut être techniquement simple de détecter et de corriger les mauvaises configurations, mais il faut également veiller à ce que les mesures de sécurité ne causent pas par inadvertance des problèmes de disponibilité pour les parties prenantes de l'entreprise. Nous recommandons de tenir compte de la règle 80/20 selon laquelle la majorité des correctifs devraient être automatiques, mais 20 % nécessiteront une intervention manuelle ou personnelle.

Adoptez des plateformes plutôt que des produits ponctuels

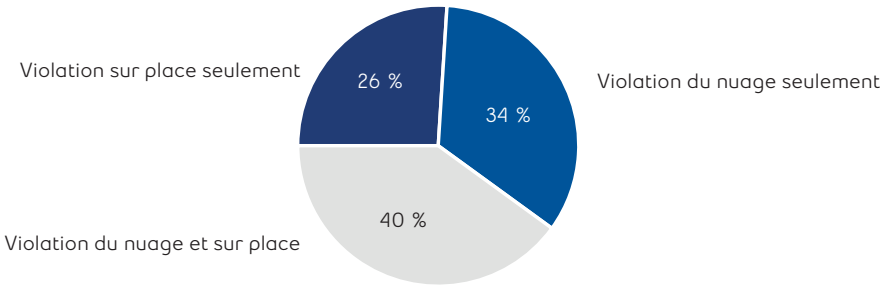
Compte tenu de l'évolution rapide des capacités en nuage, le contrôle du nombre d'outils est un défi, mais a une incidence positive sur les résultats en matière de sécurité. Il est souvent difficile d'essayer d'intégrer rétroactivement des technologies disparates (et les résultats sont souvent moins bons). Le secteur de la sécurité connaît un rythme de consolidation plus rapide dans les PPAIN et le service périphérique d'accès sécurisé, ce qui contribuera à atténuer les défis d'intégration.

Atteintes à la sécurité

D'après les résultats que nous avons communiqués, la majorité des entreprises ont signalé des failles et pourtant très peu des facteurs que nous avons testés sont en corrélation avec une diminution de la probabilité d'une faille. Étant donné que peu de facteurs sont en corrélation avec une réduction mesurable des violations, nous avons décidé d'approfondir ce résultat et d'émettre quelques hypothèses sur les raisons de ce phénomène.

Nous commençons par dévoiler un peu plus le résultat de l'atteinte à la sécurité. Sur nos 383 répondants, 249 ont signalé une faille au cours des 12 derniers mois. Pour les entreprises qui signalent une violation, la réponse la plus fréquente est que ces événements se sont produits à la fois dans des environnements en nuage et sur site (40 %). Pour les autres, les failles dans les infrastructures en nuage (34 %) étaient plus fréquentes que celles sur site (26 %).

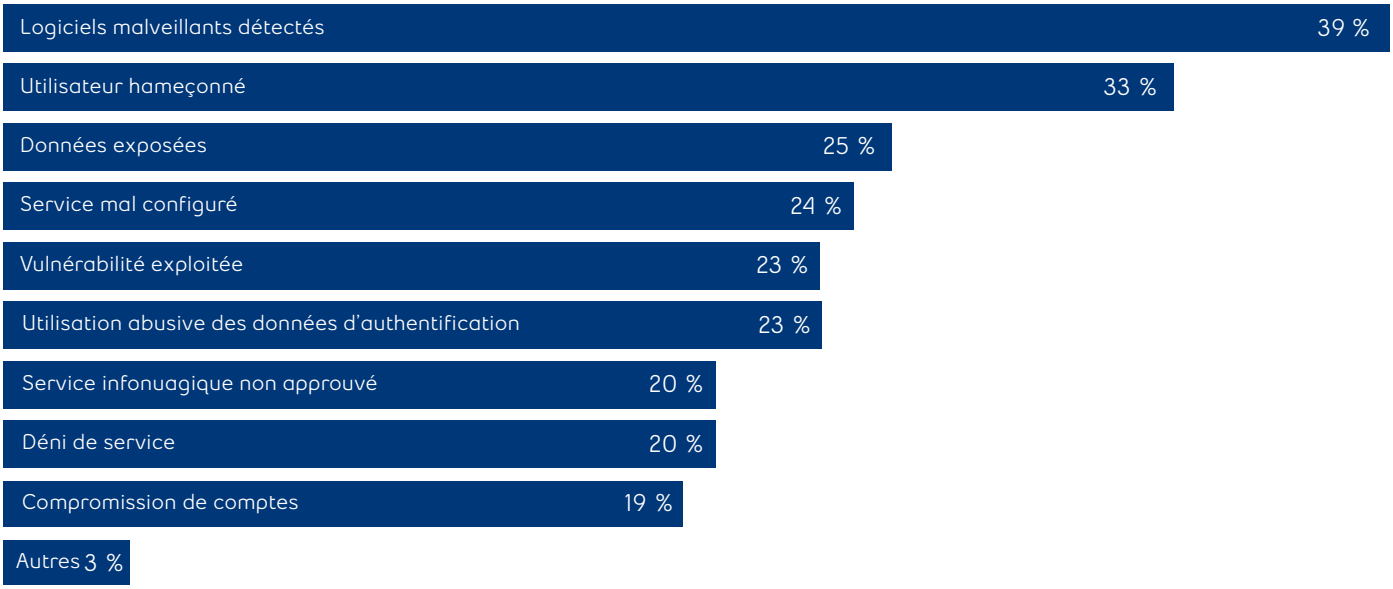
Figure 7 : Proportion d'entreprises qui signalent des failles dans des environnements en nuage et sur place



Principaux incidents

Nous avons interrogé les répondants sur les méthodes et les vecteurs d'attaque utilisés au cours des douze derniers mois, qu'ils aient ou non entraîné des pertes. Il n'est pas surprenant que les logiciels malveillants et l'hameçonnage arrivent en tête dans la Figure 8, chacun contribuant à un tiers ou plus des incidents signalés. Mais les autres ne sont pas loin derrière, nous rappelant que les incidents de sécurité ont rarement une cause ou une étape unique.

Figure 8 : Méthodes et vecteurs d'attaque associés aux incidents de sécurité



Bien qu'il apporte des perspectives intéressantes, ce graphique n'explique pas pourquoi très peu de facteurs sont en corrélation avec un nombre réduit de violations. Nous avons trois hypothèses à ce sujet :

Hypothèse 1 : Les facteurs uniques réduisent rarement les risques d'atteinte à la sécurité.

La plupart des atteintes à la sécurité découlent de multiples attaques menées par des adversaires qui sont souvent très adaptatifs. Par conséquent, il s'ensuit que peu de contrôles individuels ont le pouvoir d'empêcher à eux seuls les failles. Et notre analyse est basée sur l'évaluation de l'effet de chaque facteur individuellement plutôt que par groupes. Les résultats confirment qu'aucune activité isolée n'est particulièrement efficace.

Hypothèse 2 : De nouvelles pratiques ont été mises en œuvre après une violation.

Nous avons demandé aux personnes interrogées si leur entreprise avait subi une faille au cours des 12 derniers mois, mais les questions de l'enquête portaient sur leurs pratiques actuelles. Il est plausible que les entreprises aient subi une violation il y a un an, ce qui les a incitées à apporter des améliorations majeures à leur programme de sécurité. Ce facteur temps pourrait expliquer pourquoi nous n'observons pas de corrélation entre la diminution du nombre de violations et l'amélioration des pratiques.

Hypothèse 3 : La détection d'une infraction ne fait pas toujours partie de l'expérience vécue.

Pour répondre « Oui » à notre question sur l'occurrence d'une violation, les entreprises doivent d'abord avoir été en mesure de détecter qu'une violation s'est produite. En outre, il est facile de comprendre pourquoi si peu de facteurs analysés dans ce rapport sont en corrélation avec une probabilité plus faible de signaler des violations. Nous devrions plutôt nous attendre à l'inverse. De nombreuses pratiques de sécurité devraient ostensiblement améliorer la capacité de l'entreprise à détecter et donc à signaler les violations. Et nous constatons cette corrélation positive entre les facteurs et les violations signalées.

Réflexions/recommandations

Les entreprises dont le budget de sécurité est le plus élevé ne sont pas nécessairement les plus sécurisées. D'autres facteurs identifiés dans cette étude concernant la gouvernance, la culture, le développement des compétences, la fidélisation des employés, l'automatisation, les pratiques de sécurité et la sélection des technologies sont plus importants. Bien que ces facteurs nécessitent un investissement en argent et en temps, il est clair que l'allocation des ressources l'emporte sur la taille du budget total. Utilisez cette étude comme guide pour vous aider à mieux répartir vos ressources limitées afin d'améliorer la sécurité dans le nuage et sur les lieux.

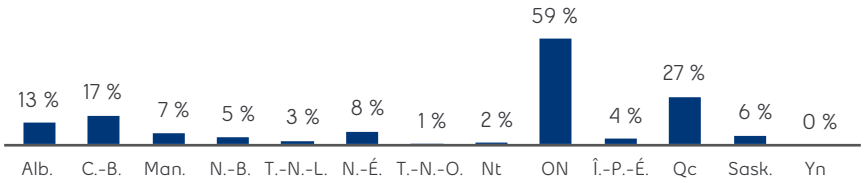
Pour en savoir plus ou pour parler à un spécialiste en cybersécurité, visitez notre site Web.

Bell

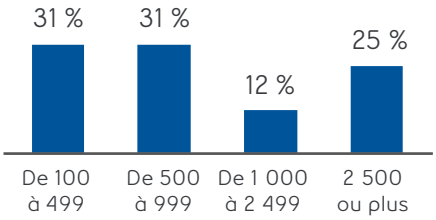
Annexe

Profil des répondants

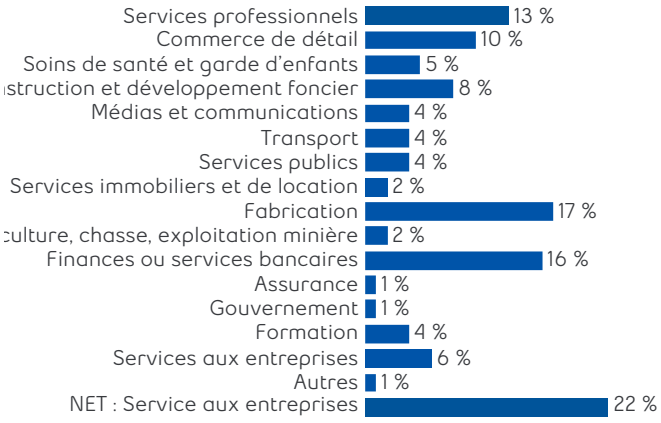
Province d'exploitation



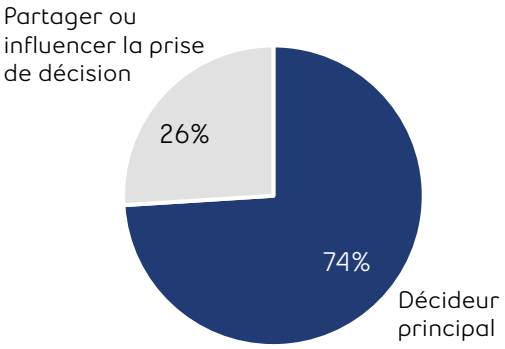
Employés



Industrie



Décideur



Titre professionnel