vmware®

Canada

Rapport VMware sur les perspectives de sécurité au Canada

2021

Introduction

Cette étude a été menée dans le but de comprendre les défis et les problèmes auxquels sont confrontées les entreprises canadiennes face à la recrudescence des cyberattaques. Elle identifie les tendances en matière de piratage et d'actes malveillants, ainsi que l'impact financier et les risques de fuites de données survenues au cours de la dernière année qui fut une année sans précédent. L'étude se penche sur les objectifs des entreprises canadiennes en matière de sécurisation des nouvelles technologies et d'adoption d'une stratégie de sécurité axée sur l'infonuagique, ainsi que sur la complexité de l'environnement actuel entourant la gestion de la cybersécurité.

En consultant ce rapport, vous découvrirez comment les experts en cybersécurité prévoient de s'adapter aux défis de sécurité que créent le télétravail et une équipe dispersée géographiquement. Vous découvrirez également comment les mécanismes de défense évoluent pour que la sécurité fasse partie intégrante de l'infrastructure et des opérations.

Synthèse de la direction :

Avant-propos

APERÇU DU PAYSAGE DE LA CYBERSÉCURITÉ AU CANADA

Rick McElroy, stratège principal en cybersécurité, Unité commerciale de sécurité de VMware

Tout est différent… et pourtant similaire.

Les experts en cybersécurité qui ont contribué à la quatrième édition de notre Rapport sur les perspectives de sécurité au Canada se trouvent dans une position très différente de celle qu'ils occupaient lorsqu'ils ont répondu de 2020. Après une année de transformation qui fut la plus importante et la plus rapide des modes de travail de notre histoire, les équipes de sécurité président désormais un écosystème plus distribué et hétérogène que jamais.

Les programmes de transformation numérique ont progressé rapidement pendant que les cyberattaques se multipliaient pour atteindre nos salons, nos cuisines, nos réseaux domestiques et nos appareils personnels. La main-d'œuvre à distance se comporte très différemment de la main-d'œuvre au bureau, ayant accès au réseau à des heures imprévisibles alors que les travailleurs s'efforcent de rester productifs tout en s'occupant de leur famille et en respectant les directives gouvernementales. Conséquemment, le trafic du réseau a changé de manière irrémédiable. Les responsables de la défense informatique doivent adapter les systèmes de surveillance et les points de déclenchement, au risque de laisser la possibilité aux auteurs de cybermenaces d'utiliser des comportements atypiques pour masquer des tentatives d'infiltration.

Dans ce contexte de constante mouvance, certaines choses demeurent inchangées : la cybercriminalité est un secteur qui n'a pas été perturbé par la COVID-19.

La fréquence des attaques est élevée et leur sophistication continue d'évoluer ; les brèches en sont le résultat inévitable.

Plus des trois quarts (77 %) des 251 répondants à notre enquête ont déclaré que le nombre d'attaques auxquelles ils ont été confrontés a augmenté au cours de l'année écoulée et, parmi eux, 78 % ont spécifié que les attaques avaient augmenté en raison de l'augmentation du nombre d'employés travaillant à domicile. Soixante-dix-neuf pour cent (79 %) ont déclaré que les attaques étaient devenues plus sophistiquées.

Les RSSI doivent jongler avec plusieurs angles morts

Le volume des cyberattaques a augmenté, mais le passage rapide au télétravail ne permet pas encore aux entreprises d'avoir une vue d'ensemble. Le comportement irrégulier des employés, l'utilisation d'appareils personnels et des réseaux domestiques réduisent la visibilité, créant des angles morts et des coins sombres où les attaques ne sont pas détectées. En conséquence :

78 %

ont déclaré que les attaques ont augmenté en raison du télétravail.

2

brèches en moyenne par organisation et par an.

88 %

ont déclaré avoir subi une brèche substantielle.

Le résultat ? Le nombre de brèches est important. Les personnes interrogées qui ont subi une cyberattaque ont déclaré **en moyenne deux brèches par an**. Il ne s'agissait pas non plus d'incidents mineurs ; dans près de neuf cas sur dix, la brèche était un incident important nécessitant un signalement aux autorités réglementaires ou l'implication d'une équipe d'intervention en cas d'incidents.

Il est clair que les équipes de sécurité sont sous pression et que la complaisance n'est pas de mise : 56 % des responsables de la sécurité des systèmes d'information (RSSI) canadiens interrogés craignent que leur organisation subisse une brèche matérielle importante au cours de l'année à venir.

Les failles d’exploitation et les vulnérabilités des systèmes, les applications tierces, les rançongiciels et les technologies obsolètes sont les principales causes d’une brèche de sécurité

Lorsque nous avons demandé quelles étaient les causes des brèches, les trois vecteurs les plus courants ont permis de dresser un tableau des menaces externes et des faiblesses internes. Les vulnérabilités du système d’exploitation sont la cause la plus fréquente, à l’origine de 19,5 % des brèches, suivies de près par les applications tierces, les rançongiciels et les systèmes de sécurité obsolètes.

Le passage rapide au télétravail a exposé les organisations qui ont négligé les pratiques exemplaires en sécurité et n'ont pas mis en œuvre l'authentification multifacteur, et ce, alors que l'entreprise étendue subit une pression croissante du fait que les tiers présentent un risque important de brèche.

En plus de ces menaces, la recrudescence rapide des rançongiciels a ajouté une pression supplémentaire non souhaitée. Les attaques en plusieurs étapes impliquant l'intrusion, la persistance du problème, le vol de données et l'extorsion font monter la pression alors que les pirates tirent parti des perturbations auxquelles sont confrontés les travailleurs à distance. Dans la plupart des attaques de rançongiciels, le courriel continue d'être utilisé comme le vecteur d'attaque le plus courant pour obtenir un premier accès.

Recrudescence des rançongiciels

Les rançongiciels reviennent en tête des causes de brèches alors que les pirates lancent des campagnes sophistiquées et lucratives en plusieurs étapes.

13 % **de toutes les brèches ont été causées par un rançongiciel.**

Appréhension du développement et de la consommation d'applications

Selon les RSSI interrogés, les applications tierces sont souvent à l'origine de brèches et 64 % d'entre eux affirment que leur capacité d'innovation en tant qu'entreprise en dépend. Il n'est donc pas surprenant que les équipes de sécurité s'efforcent d'affiner leur approche de la consommation et du développement de ces applications.

Cinquante-huit pour cent (58 %) des personnes interrogées sont en accord[1] avec l'idée qu'elles ont besoin d'une meilleure visibilité des données et les applications afin de prévenir les attaques et un nombre similaire de répondants conviennent qu'une meilleure sécurité contextuelle est nécessaire pour suivre la sécurité des données tout au long du cycle de vie des applications. L'impact de la COVID-19 est reconnu puisque plus de la moitié (58 %) des personnes interrogées conviennent qu'elles doivent revoir les processus de sécurité différemment de ce qui était fait par le passé en raison de l'élargissement de la surface d'attaque.

Les applications figurent également en tête de liste comme points les plus vulnérables du parcours des données, mais elles sont loin d'être le seul sujet de préoccupation.

Les charges de travail augmentent de manière significative et constituent une source de vulnérabilité apparente.

12 % des personnes interrogées ont déclaré que les charges de travail constituaient le point de rupture le plus vulnérable dans le parcours des données au sein de leur organisation, notant que ce n'était pas le cas il y a 12 mois.

1. En accord correspond à la combinaison des options « Fortement d'accord » et « Assez d'accord » au questionnaire.

De plus, 1 % des répondants ont déclaré que les charges de travail étaient le point le plus vulnérable depuis plus de 12 mois. Les équipes reconnaissent que les antivirus traditionnels ne parviennent pas à sécuriser les charges de travail des serveurs et que les erreurs de configuration constituent un risque de brèche important. Cette situation est souvent due à un manque de connaissances entre les équipes de sécurité et les équipes d'infrastructure. En effet, les équipes de sécurité ne savent pas comment les charges de travail de production sont censées se comporter alors que les équipes d'infrastructure n'ont pas l'expertise requise pour reconnaître le comportement des pirates. Cette année, nous prévoyons que les organisations chercheront à combler ces lacunes et à renforcer les défenses des charges de travail dans le nuage.

En ce qui concerne l'infonuagique, notre étude révèle qu'un changement inexorable est en cours. Quatre-vingt-quinze pour cent (95 %) des RSSI que nous avons interrogés ont déjà eu recours à une stratégie axée essentiellement sur l'infonuagique, ou prévoient de le faire très prochainement. Il s'agit d'un changement considérable qui démontre que les organisations accélèrent leur feuille de route en matière de sécurité infonuagique en réponse aux défis reliés à la COVID-19. Il s'agit peut-être d'un chemin qu'elles empruntaient déjà, mais les organisations mettent le pied sur l'accélérateur en reconnaissant l'impératif d'une sécurité complète pour un monde axé sur l'infonuagique.

Nous espérons que vous trouverez notre quatrième **Rapport VMware sur les perspectives de sécurité au Canada** révélateur et instructif.

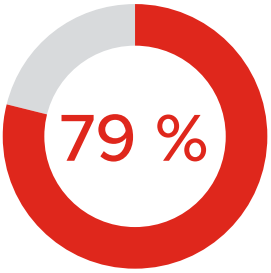
Principaux résultats

La fréquence des attaques et le risque de brèche demeurent élevés

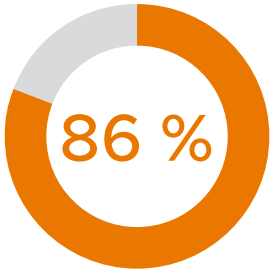
La fréquence des attaques est élevée, leur sophistication ne cesse de croître et les brèches en sont le résultat inévitable.

77 % ont déclaré que le volume des attaques avait augmenté au cours des 12 derniers mois, de 62 % en moyenne pour l'ensemble des organisations concernées.

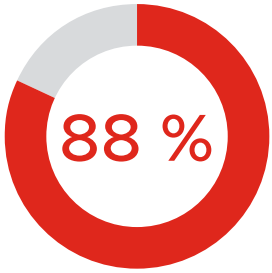
78 % de ceux ayant subi une cyberattaque ont déclaré que les attaques ont augmenté en raison de l'accroissement du nombre de personnes travaillant à domicile.



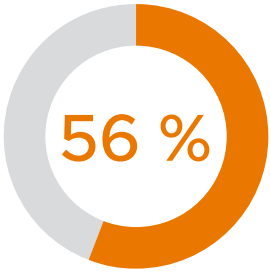
de ceux ayant subi une cyberattaque ont déclaré que les attaques étaient plus sophistiquées.



d'entre eux ont subi une brèche au cours des 12 derniers mois, et ceux qui ont été victimes d'une brèche en ont subi deux en moyenne au cours de cette période.



ont déclaré que les brèches qu'ils ont subies étaient substantielles.



craignent une brèche substantielle au cours des douze prochains mois.

Les vulnérabilités des systèmes d'exploitation, les applications tierces, les rançongiciels et les technologies de sécurité obsolètes sont les principales préoccupations des RSSI

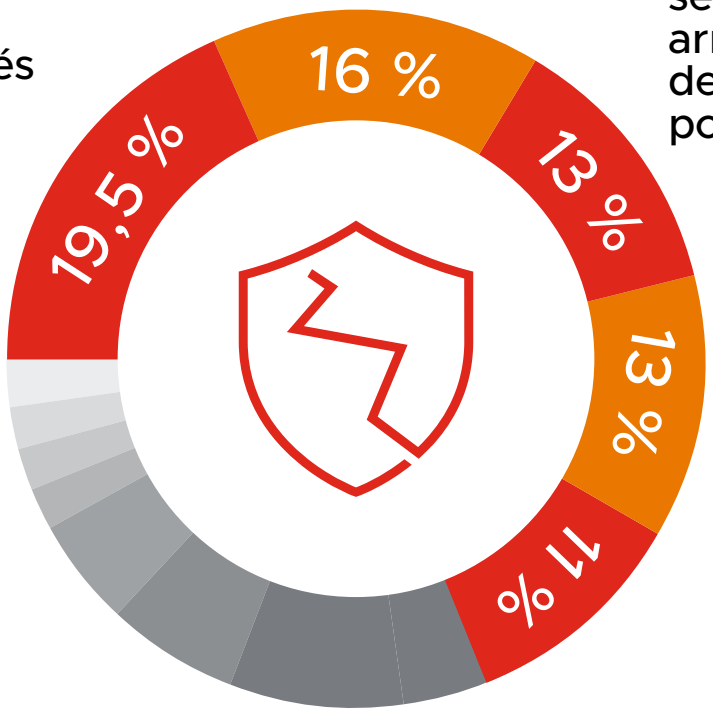
Les principaux vecteurs à l'origine des brèches permettent de dresser un tableau des menaces externes et des faiblesses internes.

Principales causes de brèches pour ceux ayant subi une cyberattaque :

Les applications tierces arrivent en seconde position avec 16 %

Les vulnérabilités des systèmes d'exploitation arrivent en tête avec 19,5 %

Les rançongiciels et les technologies de sécurité obsolètes arrivent tous deux en troisième position avec 13 %



Le « island hopping » complète le top 5 avec 11 %

Les applications sont en tête de liste des points les plus vulnérables du parcours des données, mais elles sont loin d'être le seul sujet de préoccupation.

L’expansion des surfaces d’attaque amène les dirigeants à repenser leur approche traditionnelle de la sécurité

La bonne nouvelle, c’est que l’on reconnaît l’existence d’un changement fondamental en matière de sécurité dans une ère numérique hautement connectée, où le travail est effectué à distance.

58 % reconnaissent qu’ils doivent envisager la sécurité différemment de ce qu’ils faisaient auparavant, car la surface d’attaque s’est étendue.

67 % reconnaissent qu’ils ont besoin d’une meilleure sécurité contextuelle pour être en mesure de suivre les données tout au long de leur cycle de vie.

58 % reconnaissent qu’ils ont besoin d’une meilleure vue d’ensemble sur les données et les applications afin de prévenir les attaques.

La simplification, la consolidation et le passage à l'infonuagique sont au programme pour 2021

Les RSSI interrogés semblent suivre la voie de la consolidation technologique et de l'adoption d'une approche plus intrinsèque de la sécurité alors que 36 % disent augmenter leur budget de sécurité pour atteindre ces objectifs.

↗ 29,5 % ont mis à jour leur technologie de sécurité pour atténuer le risque.

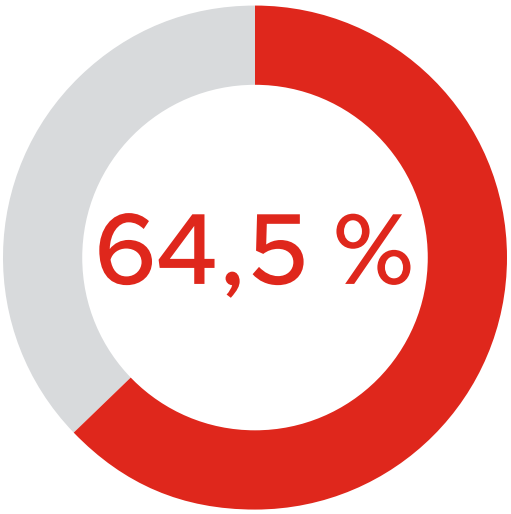
↗ 34 % intègrent davantage de sécurité au sein de leur infrastructure et leurs applications et réduisent le nombre de solutions ponctuelles.

↗ 31,5 % ont mis à jour leur politique et leur approche de la sécurité pour atténuer les risques.

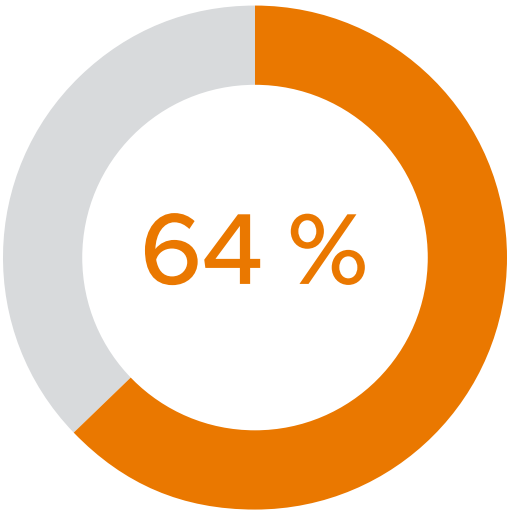
95 % ont adopté ou prévoient d'adopter une stratégie de sécurité axée sur l'infonuagique.

L'IA est la prochaine frontière de l'innovation commerciale, mais les problèmes de sécurité entravent-ils le progrès ?

Alors que les entreprises cherchent à obtenir un avantage pour offrir des services à la clientèle et des expériences numériques plus compétitifs, la prochaine frontière de l'innovation commerciale se trouve à être l'intelligence artificielle.

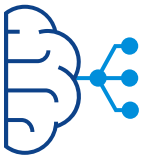


Pourtant, 64,5 % des répondants canadiens reconnaissent que les problèmes de sécurité les empêchent d'adopter des applications basées sur l'IA et l'apprentissage automatique pour améliorer ces services.



Et 64 % des personnes interrogées reconnaissent que leur capacité à innover dépend de leur capacité à créer des applications et à les mettre entre les mains des employés et des clients de manière plus sûre.

L'IA est la prochaine frontière de l'innovation commerciale, mais les problèmes de sécurité entravent-ils le progrès ?



De nombreuses personnes interrogées craignent de ne pas être en mesure de répondre à l'opportunité numérique.

60 % s'accordent à dire que le secteur des solutions de sécurité est trop complexe pour les inciter à modifier leur politique de sécurité, même s'ils sont conscients que la sécurité informatique actuelle ne fonctionne pas.

63 % reconnaissent que leur conseil d'administration ou leur équipe de direction se sentent de plus en plus inquiets lors de la mise en marché de nouvelles applications ou de nouveaux services, en raison de la menace croissante et des dommages causés par les brèches ou les attaques de données.

61 % reconnaissent qu'ils aimeraient utiliser davantage d'IA et d'apprentissage automatique dans leurs applications pour améliorer la sécurité et les services.

58 % reconnaissent qu'ils ont besoin d'une meilleure visibilité des données et des applications afin de prévenir les attaques.

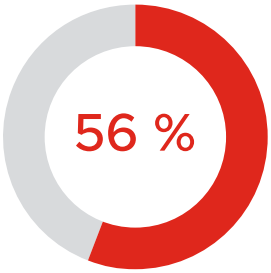
Assurer l'image et la réputation de l'entreprise - l'urgence de changer est-elle plus importante ?

L'image de marque et la réputation restent le Saint Graal des entreprises et sont facilement impactées. Cependant, l'impact des brèches de sécurité sur la réputation est plus important que l'impact financier.

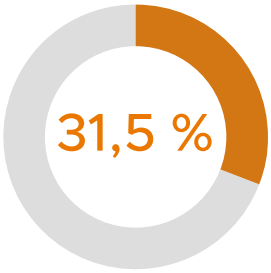
↗ 79 % de ceux ayant subi une cyberattaque mentionnent que leur réputation a en quelque sorte été impactée négativement contre 47 % en juin 2020.

↗ 88 % des répondants ont dû se rapporter aux organismes réglementaires ou engager un cabinet de RI pour surmonter les problèmes de réputation causés par des brèches substantielles au cours des 12 derniers mois.

Il y a une reconnaissance mitigée parmi les répondants par rapport à la gravité de ces brèches et certains ne ressentent pas l'urgence d'un changement, et ce, malgré l'augmentation des menaces.



craignent de subir une brèche substantielle au cours de l'année à venir.



ont mis à jour leur politique et leur approche en matière de sécurité pour atténuer le risque.

Résultats complets de l'enquête

Avez-vous constaté une augmentation des cyberattaques contre votre entreprise au cours des 12 derniers mois ? Si oui, de combien ?

Soixante-dix-sept pour cent (77 %) des RSSI interrogés ont déclaré avoir subi une augmentation du nombre de cyberattaques contre leur organisation au cours des 12 derniers mois, l'augmentation moyenne étant de 62 %. Le pourcentage d'augmentation du nombre d'attaques atteint 96 % dans le secteur des services financiers et l'augmentation moyenne est de 69 %. Il est intéressant de noter que, même si le secteur de la fabrication et de l'ingénierie compte moins de répondants ayant subi une augmentation du nombre d'attaques (59 %), l'augmentation moyenne est élevée (86 %).

Les entreprises qui se situaient dans la catégorie 5 001-10 000 employés ont connu la plus forte augmentation des attaques (67 %), se trouvant ainsi dans la catégorie 51-100 % d'augmentation.

Quarante-trois pour cent (43 %) des personnes interrogées comptant entre 31 et 40 personnes dans leur équipe informatique ont signalé une augmentation de 51 à 100 % du volume des cyberattaques.

Le nombre de cyberattaques typiques sur votre système a-t-il changé en raison de l'augmentation du nombre d'employés travaillant à domicile dû à la pandémie de COVID-19 ?

Soixante-dix-huit pour cent (78 %) des personnes interrogées ayant subi des cyberattaques ont déclaré avoir constaté une augmentation de la fréquence en raison de l'augmentation du nombre d'employés travaillant à domicile.

Quatre-vingt-huit pour cent (88 %) des personnes interrogées dans le secteur des services financiers ont constaté une augmentation des attaques reliées au télétravail, avec une hausse moyenne de 33 %, alors que, étonnamment, 19 % des personnes interrogées dans le secteur des soins de santé ont déclaré que le nombre d'attaques était demeuré stable et 14 % ont affirmé que les attaques avaient diminué.

Quatre-vingt-dix-huit pour cent (98 %) des entreprises appartenant à la catégorie 5 001-10 000 employés ont connu une augmentation. Cinquante et un pour cent (51 %) des personnes interrogées comptant entre 31 et 40 personnes dans leur équipe informatique ont déclaré que les attaques avaient augmenté de 25 à 49 %.

Les cyberattaques contre votre entreprise sont-elles devenues plus ou moins sophistiquées au cours des 12 derniers mois ?

En ce qui concerne la sophistication des attaques, 79 % des RSSI interrogés ayant subi une cyberattaque ont vu les attaques devenir plus sophistiquées. Ce chiffre est légèrement inférieur à celui du rapport de juin 2020 au sein duquel 86 % avaient signalé une sophistication accrue des attaques.

> 79 % des RSSI interrogés ayant subi une cyberattaque ont vu les attaques devenir plus sophistiquées.

Toutefois, 46 % de ceux ayant subi une cyberattaque déclarent que les attaques auxquelles ils sont confrontés sont nettement ou modérément plus sophistiquées, ce qui indique qu'il existe un noyau de personnes mal intentionnées qui développent et améliorent leurs techniques d'attaque.

Il semble que ces personnes dirigent leurs techniques vers le secteur des services financiers, où 90 % des RSSI ont fait état d'une sophistication accrue et près des deux tiers (67 %) ont déclaré que les attaques étaient devenues modérément ou considérablement plus complexes.

Les adversaires dirigent également leurs attaques plus sophistiquées vers les grandes entreprises, un pourcentage plus élevé affirmant que les attaques sont devenues nettement plus sophistiquées. Cela s'explique par le fait que plus l'entreprise est grande, plus les données qu'elle détient sont précieuses et volumineuses, ce qui signifie que les cybercriminels ont davantage de possibilités de rentabiliser leur travail.

Quel a été le type de cyberattaque le plus fréquent que votre entreprise a connu au cours des 12 derniers mois ?

L'environnement de cyberattaque potentielle au Canada est diversifié, peu de répondants subissent la même combinaison de types d'attaque et aucun type d'attaque ne prédomine. Cette réalité souligne les défis auxquels les RSSI canadiens sont confrontés. Ceux-ci doivent élaborer des réponses stratégiques et des tactiques à une très grande variété de types d'attaque et de techniques diverses.

Les applications tierces arrivent en tête du classement avec 11 % des personnes interrogées ayant été victimes de ce type d'attaque. Ce nombre passe à 18 % pour les répondants œuvrant dans le secteur public. Les rançongiciels étaient également l'un des principaux types d'attaques pour 9 % des répondants, passant à 17 % pour les répondants du secteur de la santé. Suivi de près par Google Drive et le « process hallowing » à la fois avec 8 %.

Dans le rapport de juin 2020, les attaques des applications sur le Web ont dominé, 21 % des répondants étant le plus souvent confrontés à ce type d'attaque.

À quelle fréquence votre entreprise a-t-elle été victime d'une cyberattaque au cours des 12 derniers mois ?

Près de neuf RSSI sur dix (86 %) ayant participé à notre recherche ont déclaré que leur organisation avait subi une brèche de données à la suite d'une cyberattaque au cours de l'année écoulée. Ce nombre est en baisse puisque 100 % des répondants avaient déclaré avoir été victimes d'une brèche en juin 2020.

Cependant, le nombre moyen de brèches subies par chaque organisation est passé de 1,10, en juin 2020, à 2 au sein de ce rapport. De plus, 10 % des répondants ont déclaré que leur organisation a été victime d'une attaque entre cinq et dix fois.

Le secteur public a subi le plus faible nombre moyen de brèches, à 1,18. Les secteurs notables, dont la fréquence des infractions est supérieure à la moyenne, sont les voyages et les transports (3,89), le commerce de détail (3,38) et les services professionnels (3,40).

La fréquence des brèches est la plus faible au sein des organisations de 5 001 à 10 000 employés, chacune ne subissant que 1,32 attaque en moyenne et avec 86 % déclarant avoir été victime d'une attaque une fois.

Quelle a été la cause principale de ces brèches ?

Pour 19,5 % des RSSI interrogés ayant subi des brèches de sécurité à la suite d'une cyberattaque, la vulnérabilité du système d'exploitation était le principal coupable. Pour 16 %, une brèche était due à des applications tierces et 13 % à un rançongiciel. Alors que 9 % des organisations ayant subi des brèches de données ont découvert que leurs processus n'étaient pas aussi puissants qu'ils le pensaient. Les technologies de sécurité obsolètes (13 %) et le « island hopping » (11 %) sont venus s'ajouter à ce problème. La tension exercée par le passage soudain au télétravail a clairement mis en évidence les domaines dans lesquels les politiques et la technologie n'ont pas su suivre le rythme de l'évolution de l'environnement.

Moins fréquents, mais toujours significatifs, 8 % des brèches ont été attribuées à des attaques d'applications Web et 4,5 % via leur chaîne d'approvisionnement. Encore une fois, cette diversité de brèches de données met en évidence les nombreux fronts sur lesquels les RSSI canadiens doivent défendre leur organisation.

Les rançongiciels étaient un problème particulier pour les organisations de services financiers, soit à l'origine de 22 % des brèches de données. Le « island hopping » était relativement élevé au sein de tous les secteurs : 16 % des organismes de services financiers et 11 % des répondants gouvernementaux affirmant qu'il s'agissait d'une cause principale. De plus, 31 % des établissements de santé ont également signalé que les rançongiciels étaient l'une des principales causes de brèches, tandis que les organisations du secteur gouvernemental ont signalé un pourcentage beaucoup plus élevé que la moyenne (36 %) d'attaques de vulnérabilité de leur système d'exploitation.

Les entreprises comptant entre 5 001 et 10 000 employés étaient particulièrement vulnérables aux brèches causées par des vulnérabilités de leur système d'exploitation, avec 35 % des brèches causées de cette manière. Et ceux dont la taille de l'équipe informatique est comprise entre 21 et 30 employés ont connu un pourcentage élevé de brèches dues à des vulnérabilités du système d'exploitation (25 %).

Quel pourcentage des brèches par cyberattaque au cours des 12 derniers mois considérez-vous comme une brèche substantielle (c'est-à-dire que vous avez dû les divulguer aux organismes réglementaires, contacter une équipe de réponse aux incidents, etc.) ?

Lorsqu'une brèche se produit, c'est une affaire sérieuse. Quatre-vingt-huit (88 %) ont dû se rapporter aux organismes réglementaires ou engager un cabinet de RI pour surmonter les problèmes causés par les brèches.

88 % des organisations ont subi une brèche importante.

Près de la moitié (45 %) des personnes interrogées ayant subi une cyberattaque ont déclaré qu'entre 21 % et 30 % étaient des brèches substantielles, et 16 % de plus ont déclaré qu'entre 31 % à 40 % des brèches étaient substantielles.

Étonnamment, les répondants du secteur des services financiers avaient un nombre moyen inférieur à la moyenne de brèches substantielles signalées (21 %), 47 % déclarant que seulement 10 % à 20 % des brèches étaient importantes. Les répondants du secteur des aliments et des boissons ont rapporté des chiffres élevés, soit 67 % admettant que 21 % à 30 % des infractions devaient être divulguées aux organismes réglementaires.

Quelles ont été les conséquences de ces brèches d'un point de vue financier et réputationnel pour votre entreprise ?

Seuls 5,5 % des victimes d'une cyberattaque ont déclaré avoir subi un impact financier négatif en raison d'une brèche de données subie par leur organisation. Ce nombre est inférieur à la moyenne mondiale de 24 %.

Le pourcentage déclarant l'absence d'un impact financier à la suite d'une brèche a légèrement diminué, passant de 62 %, en juin 2020, à 54 % au sein de ce rapport. À noter que 34 % des répondants ont indiqué ne pas savoir si un impact financier était à signifier ou non.

Dans l'ensemble, l'effet sur la réputation des marques ressort comme étant plus important avec 79 % des personnes interrogées ayant subi une cyberattaque qui ont déclaré que leur marque avait été affectée négativement par une brèche de données, contre 47 % dans le rapport de juin 2020. De plus, 6 % ont déclaré que les impacts étaient graves.

Seulement 17 % ont déclaré que leur réputation n'avait pas été impactée lors d'une brèche.

Soixante-trois pour cent (63 %) des répondants en provenance du domaine des services financiers ont déclaré qu'il n'y avait pas d'impact financier négatif, comparativement aux 18 % ayant déclaré qu'il n'y avait pas d'impact négatif sur la réputation.

Dans quelle mesure craignez-vous des brèches importantes qui, selon vous, pourraient affecter votre organisation au cours des 12 prochains mois ?

Il existe un facteur de peur significatif associé au potentiel de brèches importantes au cours de l'année à venir. Cinquante-six pour cent (56 %) ont très ou assez peur qu'une brèche frappe leur entreprise.

Le secteur des services financiers est plus préoccupé avec 71 % des répondants déclarant craindre une brèche.

Les petites organisations, quant à elles, étaient plus susceptibles de mentionner qu'elles ne croient pas être à risque d'être affectées par une brèche substantielle.

Comment abordez-vous ce problème (la probabilité de brèches), le cas échéant ?

Interrogés sur leurs plans pour atténuer le risque de brèche, les répondants accordaient la priorité à la simplification et à la consolidation des solutions de sécurité, tout en rendant la sécurité intrinsèque. Il était également important de mettre à jour la technologie et les politiques, et d'y consacrer un budget.

Trente-quatre pour cent (34 %) des répondants ont déclaré qu'ils prévoyaient **intégrer plus de sécurité au sein de leur infrastructure et de leurs applications et de réduire le nombre de solutions ponctuelles**.

Trente-trois pour cent (33 %) des répondants ont déclaré avoir **adapté la sécurité pour atténuer les risques**, en utilisant les actifs existants. En particulier, les organisations du secteur public sont plus susceptibles que d'autres à envisager d'adapter la technologie (43 %). De plus, 29,5 % des répondants ont déclaré avoir **mis à jour leur technologie de sécurité pour atténuer le risque**.

34 % déclaré qu'ils prévoyaient intégrer plus de sécurité au sein de leur infrastructure et de leurs applications et de réduire le nombre de solutions ponctuelles.

Les répondants ont déclaré à 31,5 % avoir mis à jour leur politique de sécurité et leur approche pour atténuer les risques. Il s'agit d'une tactique importante étant donné les changements importants du paysage de la sécurité au cours de la dernière année. Ce sont 39 % des organismes gouvernementaux qui ont adopté cette approche.

Trente-six pour cent (36 %) ont augmenté leur budget de sécurité. Plus particulièrement, 53 % des organisations reliées au domaine des services financiers ont augmenté leur budget.

Dans quelle mesure êtes-vous en accord ou en désaccord avec les déclarations suivantes relatives au développement et à l'utilisation d'applications au sein de votre organisation ?

Interrogés sur l'évolution de la façon dont ils envisagent les défis de sécurité liés au développement et à la consommation d'applications dans leur organisation, nos répondants ont offert un aperçu des problèmes auxquels ils sont confrontés.

La visibilité est une préoccupation notable avec 58 % des répondants qui conviennent avoir **besoin d'une meilleure vue d'ensemble sur leurs données et applications afin de prévenir les attaques**.

Cinquante-huit pour cent (58 %) des répondants canadiens ont convenu que les changements à l'environnement des attaques provoqués par la COVID-19 nécessitent une refonte de leur sécurité, reconnaissant qu'ils doivent revoir leur sécurité différemment de ce qu'ils ont fait auparavant puisque le nombre d'attaques augmente.

Soixante-sept pour cent (67 %) déclarent avoir **besoin d'une meilleure sécurité contextuelle pour suivre les données/la sécurité tout au long de leur cycle de vie**. Cela indique un environnement prédominant dans lequel la sécurité a tendance à être centrée sur les menaces et à être réactive. Les responsables informatiques reconnaissent que les environnements dynamiques nécessitent une approche centrée sur le contexte.

Les RSSI canadiens interrogés ne se font aucune illusion quant à la nature critique de la sécurité des applications pour leur entreprise. Près de 64 % d'entre eux ont convenu que leur capacité à innover en tant qu'entreprise dépend **de leur capacité à créer, gérer et distribuer des applications de manière plus sécurisée**.

Soixante-et-un pour cent (61 %) des répondants se sentent **confiants dans la mise en marché de nouvelles applications sachant qu'elles seront sécurisées**.

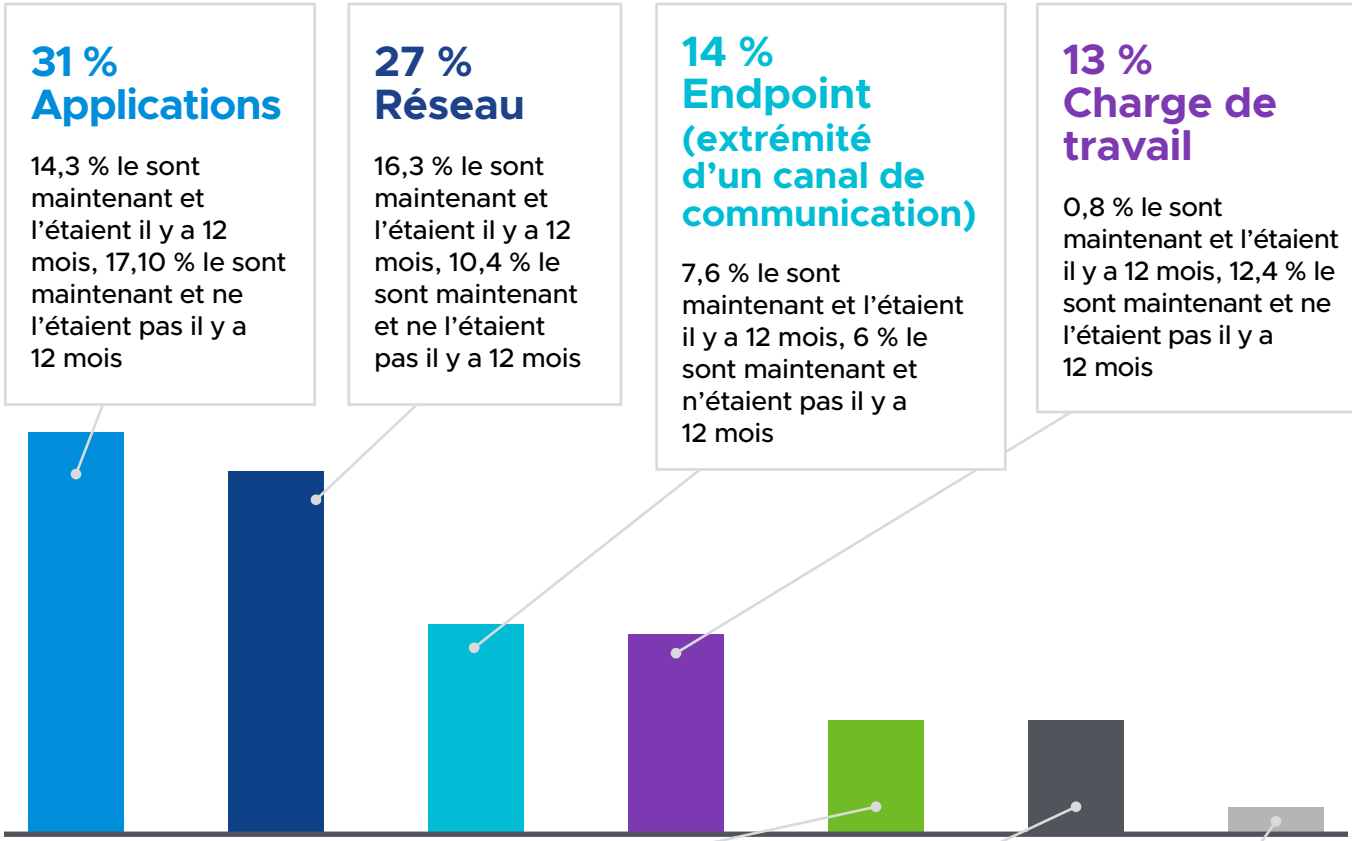
Interrogés sur leur vision de l'IA dans le développement d'applications sécurisées, les répondants entrent en conflit sur certains points. En ce sens, 64,5 % conviennent que les **problèmes de sécurité nuisent à l'adoption d'applications basées sur l'intelligence artificielle/l'apprentissage automatique pour améliorer les services**, tandis que 61 % conviennent qu'ils aimeraient **utiliser plus d'IA et d'apprentissage automatique au sein de leurs applications afin d'améliorer la sécurité et les services**.

Plus de la moitié des répondants (60 %) ont convenu qu'il y a **trop de complexité sur le marché des solutions de sécurité pour les inciter à changer de politique de sécurité, et ce**, même sachant que la sécurité informatique actuelle ne fonctionne pas – et ils indiquent que les fournisseurs ont du travail à faire pour simplifier leur proposition dans une approche intégrée.

Enfin, 63 % ont convenu que la sécurité des applications retenait l'attention du conseil d'administration et que leur **conseil d'administration/équipe de direction se sentait de plus en plus inquiet lorsque les organisations adoptent de nouvelles applications/services en raison de la menace croissante et des dommages causés par les brèches/attaques de données**.

Selon vous, quel est le point de brèche le plus vulnérable sur le parcours des données au sein de votre infrastructure de sécurité et celui-ci a-t-il changé au cours des 12 derniers mois ?

Les applications ont été désignées comme le point de brèche le plus vulnérable du parcours des données et il est clair que cela est préoccupant depuis quelque temps. Ce qui est le plus intéressant, c'est que les charges de travail augmentent considérablement en tant que source de vulnérabilité perçue. Il est probable que les organisations se concentrent davantage sur la lutte contre ce risque au cours de l'année à venir.



31 %
Applications

14,3 % le sont maintenant et l'étaient il y a 12 mois, 17,10 % le sont maintenant et ne l'étaient pas il y a 12 mois

27 %
Réseau

16,3 % le sont maintenant et l'étaient il y a 12 mois, 10,4 % le sont maintenant et ne l'étaient pas il y a 12 mois

14 %
Endpoint (extrémité d'un canal de communication)

7,6 % le sont maintenant et l'étaient il y a 12 mois, 6 % le sont maintenant et n'étaient pas il y a 12 mois

13 %
Charge de travail

0,8 % le sont maintenant et l'étaient il y a 12 mois, 12,4 % le sont maintenant et ne l'étaient pas il y a 12 mois

6 %
Nuage

4,4 % le sont maintenant et l'étaient il y a 12 mois, 2,0 % le sont maintenant et ne l'étaient pas il y a 12 mois

6 %
En périphérie de réseau

3,2 % le sont maintenant et l'étaient il y a 12 mois, 2,8 % le sont maintenant et ne l'étaient pas il y a 12 mois

1 %
Conteneurs

1,2 % le sont maintenant et 0 l'étaient il y a 12 mois

Comment les organisations ont-elles fait face aux défis de la transition vers le télétravail ?

Nous avons demandé aux RSSI interrogés d'évaluer leur succès en lien avec la transition de la main-d'œuvre vers le télétravail et si une approche axée sur la sécurité aurait contribué à une transition plus efficace.

Trente-neuf pour cent (39 %) des répondants conviennent qu'ils ont été en mesure de rendre leur personnel opérationnel à distance et que la sécurité n'a pas été un obstacle. Ceci témoigne du travail des équipes de sécurité qui ont été plus que jamais au cœur des opérations.

Les répondants reconnaissent qu'on peut faire mieux, avec 52 % qui estiment qu'une approche axée sur la sécurité aurait augmenté leur capacité à permettre aux employés de travailler à partir d'emplacements alternatifs et de rester productifs. Cela a également été confirmé au sein de recherches antérieures de VMware (en anglais seulement) qui ont révélé que l'incapacité de mettre en œuvre l'authentification multifacteur était la principale préoccupation des professionnels de l'informatique dans leur réponse au passage en mode télétravail. Maintenant que le profil de la sécurité s'est amélioré, il devrait être plus facile pour les RSSI d'obtenir le soutien du conseil d'administration pour une approche axée sur la sécurité.

Utilisez-vous ou prévoyez-vous utiliser une stratégie de sécurité axée sur l'infonuagique ?

95 % utilisent déjà ou prévoient d'adopter une approche infonuagique pour protéger l'organisation.

La majorité des répondants (95 %) ont déclaré qu'ils prévoyaient passer à une stratégie de sécurité axée sur l'infonuagique dans les plus brefs délais. De même que si ce n'est pas encore mis en place, cette stratégie est fermement inscrite sur la feuille de route.

Dans l'ensemble, 25 % déclarent utiliser une approche basée sur l'infonuagique depuis plus d'un an, tandis que 39 % déclarent avoir utilisé l'infonuagique depuis moins de 12 mois. Un autre 31 % envisagent de le devenir au cours de la prochaine année ou ils feront le changement plus loin sur la piste.

La maturité des processus de sécurité axée sur l'infonuagique est élevée parmi les organismes gouvernementaux, où 27,5 % d'entre eux sont sur l'infonuagique depuis plus de 12 mois, alors que 57 % des organisations de services financiers sont sur l'infonuagique depuis moins de 12 mois.

Perspectives clés et actions

Notre quatrième Rapport sur les perspectives de sécurité au Canada révèle que les principaux experts en cybersécurité et les organisations qu'ils servent continuent de faire face à des menaces sophistiquées à volume élevé. Celles-ci sont exacerbées par le télétravail et, bien que la plupart des organisations aient réussi à faire la transition vers le télétravail, les RSSI reconnaissent qu'une approche axée sur la sécurité aurait facilité la transition.

Sans aucun doute, la COVID-19 a considérablement changé l'environnement de cybersécurité et continuera d'influencer la stratégie de sécurité. Pour sa part, le secteur de la cybersécurité doit se concentrer à fournir des solutions qui réduisent la complexité opérationnelle tout en protégeant de manière robuste les environnements de travail dispersés qui deviendront une normalité pour la plupart des organisations.

L'analyse des réponses à l'enquête révèle des domaines importants pour la cybersécurité au cours de l'année à venir.

Accorder la priorité à l'amélioration de la visibilité

Les organisations ont un problème de visibilité résultant du passage rapide au télétravail. La véritable ampleur des attaques est difficile à discerner puisque les responsables de la cyberdéfense ne peuvent pas toujours facilement savoir où les appareils mobiles personnels et les réseaux domestiques ont été greffés sur l'écosystème de l'entreprise. Nous pouvons ajouter à cela les défis de la surveillance des applications et des fournisseurs tiers ainsi que le nombre d'angles morts qui augmente.

En termes simples, les défenseurs ne savent pas ce qu'ils ne savent pas et les entreprises sont exposées en retour. Cette compréhension contextuelle limitée du risque désavantage les responsables de la cyberdéfense lorsqu'ils protègent la surface d'attaques potentielles. Les organisations doivent donner la priorité à l'amélioration de la visibilité sur tous les terminaux et les charges de travail pour sécuriser l'environnement de télétravail. Une intelligence situationnelle solide qui donne un contexte aux menaces aidera ces professionnels à prioriser et à corriger les risques en toute confiance.

Répondre à la résurgence des rançongiciels

Les cyberattaques ont continué de gagner en sophistication et les rançongiciels ne font pas exception. Les pirates obtiennent un accès non détecté aux réseaux, exfiltrent des données et établissent des portes dérobées, avant de lancer des demandes de rançon ou de monétiser directement les données volées. Pour éviter d'être victime d'attaques répétées, les entreprises doivent combiner une protection avancée contre les rançongiciels avec une correction post-attaque robuste qui détecte la présence continue d'adversaires au sein de leur environnement.

Continuer à lutter contre les technologies de sécurité héritées inefficaces et les faiblesses des processus

Les faiblesses obsolètes de la sécurité et des processus continuent de présenter des risques importants pour les organisations, et le passage au télétravail les a encore plus exposées. Alors que nous sortons de la phase de réponse immédiate et que nous commençons à voir l'avenir se dessiner à long terme, les organisations doivent identifier les changements critiques des processus et de la technologie nécessaires pour aider les personnes qui travaillent à distance ou de manière hybride à travailler en toute sécurité et à réduire les risques.

Fournir une sécurité en tant que service distribué

Il fut un temps où les équipes de sécurité sécurisaient les postes de travail appartenant à l'entreprise pour les employés travaillant sur le campus, se connectant aux applications d'entreprise exécutées sur des serveurs dans un centre de données appartenant à l'entreprise. Le monde est un endroit plus compliqué aujourd'hui avec des travailleurs à distance se connectant à des applications exécutées sur une infrastructure qui peut ou non être gérée, détenue ou contrôlée par l'entreprise. Avec autant de nouvelles surfaces et différents types d'environnements à défendre, la sécurité ne peut être fournie comme une litanie de produits ponctuels et de points d'étranglement du réseau. Au lieu de cela, les contrôles des points de terminaison et du réseau doivent être fournis en tant que service distribué. Cela signifie fournir une sécurité qui suit les actifs protégés, quel que soit le type d'environnement dont vous disposez.

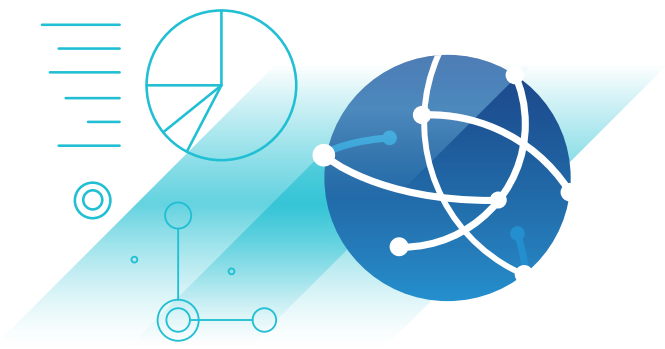
Adopter une approche intrinsèque de la sécurité axée sur l'infonuagique

Le plus grand changement découvert par nos recherches est le passage à une stratégie de sécurité axée sur l'infonuagique. Il est difficile de surestimer l'ampleur du changement qui s'est produit en si peu de temps; très peu de RSSI avant 2020 qualifiaient leur stratégie de sécurité comme étant axée sur l'infonuagique. C'est le résultat logique du fait que les organisations doivent réagir aux pratiques de travail hautement distribuées causées par la COVID-19.

Passer à l'infonuagique n'est pas le remède à la sécurité. Tous les « nuages » ne sont pas égaux et les contrôles doivent être vérifiés par les consommateurs, car si des adversaires souhaitent attaquer à grande échelle, le « nuage » est l'endroit idéal pour le faire. À mesure que ce changement prend de l'ampleur, l'investissement dans la sécurité du « nuage » public sera essentiel. Lorsque vous passez à un « nuage » public, vous vous déplacez dans un environnement très difficile où la sécurité dépend non seulement de vos propres actions, mais de celles de vos utilisateurs. Vous pouvez peut-être sécuriser vos propres ressources, mais vous n'avez aucun contrôle sur ceux qui partagent cet environnement avec vous. Les organisations doivent donner la priorité à la sécurisation des charges de travail sur le « nuage » à chaque étape du cycle de vie de la sécurité alors que le grand virage vers le nuage se poursuit.

Finalement, le Rapport VMware sur les perspectives de sécurité au Canada montre une industrie qui se concentre sur les succès de l'année écoulée et sur la réponse à l'évolution de l'environnement des menaces. Les RSSI ont un sens aigu de la direction à prendre et des outils dont ils ont besoin pour garder une longueur d'avance sur les pirates.

Méthodologie



VMware a commandé une enquête d'opinion, réalisée par un organisme de recherche indépendant, Opinion Matters, en décembre 2020. 251 DSI (ou CIO), directeurs de la technologie (ou CTO) et responsables de la sécurité des systèmes d'information (ou RSSI) canadiens ont été sondés auprès d'entreprises de divers secteurs, dont les suivants : les finances, les soins de santé, le gouvernement et les autorités locales, le commerce de détail, le domaine manufacturier et l'ingénierie, l'alimentation et les boissons, les services publics, les services professionnels de même que les médias et le divertissement. Il s'agit du quatrième Rapport sur les perspectives de sécurité au Canada de VMware. Il s'appuie sur l'enquête précédente réalisée en juin 2020. Cette enquête est partie intégrante d'un projet de recherche mondial à travers **14 pays**, incluant : l'Australie, le Canada, l'Arabie saoudite, le Moyen-Orient, le Royaume-Uni, les pays nordiques, l'Allemagne, l'Espagne, l'Italie, le Japon, Singapour et les États-Unis.

À propos de VMware

Partout dans le monde, la technologie VMware fait fonctionner les infrastructures numériques les plus complexes. Les solutions propriétaires de Cloud, de modernisation des apps, de réseau, de sécurité et d'espaces de travail numériques aident les clients à déployer n'importe quelle application sur tout type de Cloud, quel que soit le terminal. Basée à Palo Alto, en Californie, l'entreprise VMware s'engage à œuvrer pour le bien, grâce à des innovations technologiques révolutionnaires ou son impact à l'échelle mondiale. Pour plus d'informations, rendez-vous sur vmware.com/ca-fr/company.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com
 Item No: 863494aq-sec-insgt-rprt-fr-ca-uslet 6/21