# CYBERSÉCURITÉ EN 2022 : PROMOUVOIR LA MATURITÉ DES ORGANISATIONS CANADIENNES

## Protéger la transformation numérique des TI à l'ère des menaces croissantes

Les occasions créées par la modernisation des TI traditionnelles dans un environnement informatique complexe en évolution rapide sont contrebalancées par la nécessité de le protéger contre des menaces toujours plus fréquentes et malicieuses. Les risques de perte de données, de blocage et de perturbation des services sont la priorité pour les chefs d'entreprise au Canada, qui visent à protéger les données des clients, des employés et des partenaires et assurer la continuité des activités.

**Cette étude présente une évaluation de l'état de la sécurité informatique et des enjeux des organisations canadiennes aujourd'hui, et offre des perspectives permettant la progression vers une sécurité musclée.**

# L'évolution rapide des menaces et les contraintes en matière de ressources

**Le nombre de dispositifs branchés a explosé.**
Même le nombre de serveurs, une technologie plutôt mûre, a plus que triplé. À mesure que la surface d'attaque augmente, les nouvelles vulnérabilités et les cyberrisques connexes s'accentuent, comme en témoigne le nombre croissant de cyberattaques.

***Quatre-vingt-dix pour cent des organisations canadiennes interrogées ont indiqué avoir été attaquées au cours de la dernière année.***

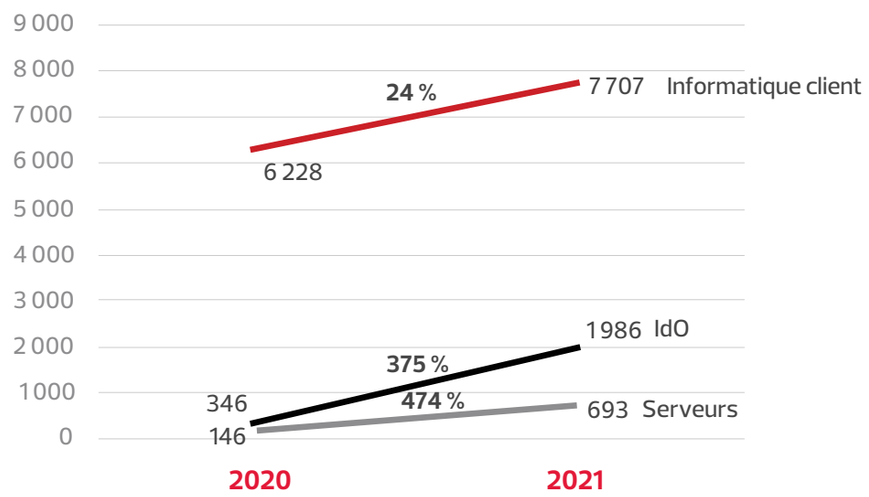
**Quelle que soit la taille, l'industrie ou la région de l'organisation, tout le monde est attaqué.**
Les serveurs du nuage public sont devenus la nouvelle cible. Les cyberattaques évoluent en une industrie bien branchée et organisée, et les attaques sont plus sophistiquées que jamais. Il en faut beaucoup moins qu'auparavant pour compromettre l'infrastructure informatique d'une organisation.

**Les temps d'indisponibilité coûtent cher.**
Les temps d'indisponibilité sont l'une des plus grandes causes de coûts directs liés aux cyberincidents. En effet, les sociétés canadiennes déclarent des temps d'indisponibilité totaux d'une à deux semaines ou plus par catégorie d'attaque.

**Alors que la sécurité est une préoccupation primordiale, de nombreuses organisations canadiennes ont du mal à la financer adéquatement.**
La moitié déclare disposer de budgets qui ne font pas de place pour la modernisation et l'expérimentation des technologies de sécurité les plus récentes. Près du quart (23 %) dispose de budgets insuffisants pour couvrir les opérations de sécurité informatique de base.

**Il y a un écart de compétences en sécurité.**
Cinquante-sept pour cent des organisations signalent des lacunes en matière de dotation ou de compétences de sécurité. L'écart de compétences au sein des équipes de sécurité informatique est un problème considérable, et encore plus complexe que les budgets pour l'effectif.

## Nombre moyen d'appareils informatiques par organisation




L'informatique client comprend les ordinateurs personnels, les portables, les téléphones intelligents et les tablettes.
Source : Enquête sur la sécurité de CDW de 2021 (n = 557) et 2020 (n = 524)

# Un modèle de maturité pour la sécurité informatique

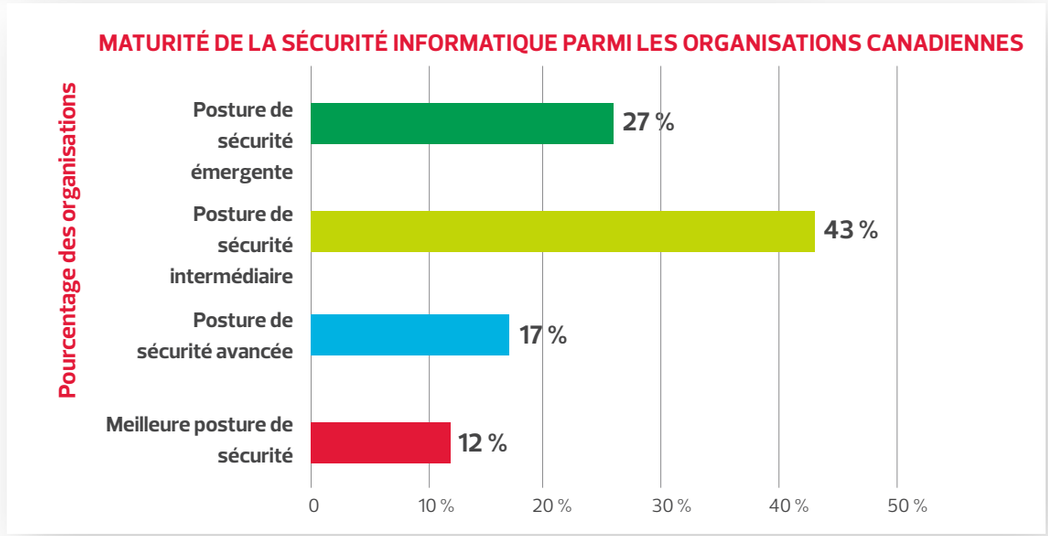
Le chemin vers une sécurité informatique améliorée commence par une évaluation de l'état actuel et l'établissement d'un état final clair et bien défini. CDW a élaboré un modèle pour évaluer les niveaux de maturité de la sécurité informatique d'une organisation selon quatre dimensions, en fonction du sondage de cette année.

| Approche de sécurité | Philosophie de sécurité | Investissements en sécurité | Processus de sécurité |
|---|---|---|---|
| Une équipe de direction (en dehors des TI) qui bâtit une culture de pratiques exemplaires en matière de sécurité<br>**Outillage de la sécurité informatique – dotation en personnel et perfectionnement des compétences**<br>Ampleur des investissements dans les opérations de base, les nouvelles initiatives et les approches expérimentales | Adoption de l'architecture de confiance zéro<br>Intégration des processus et des outils de sécurité informatique<br>**Processus et flux de travail de sécurité informatique reproductibles et cohérents** | Niveau d'investissement (technologies, processus) pour déceler et contrer les menaces à la sécurité informatique internes et externes et le degré des contrôles de la prévention des menaces | **Adoption et optimisation des approches à la fine pointe (vérifications de la gouvernance et de la conformité, évaluations des risques et formation du personnel)**<br>Sauvegarde : sécurité, régularité et authentification |

**Selon ces dimensions, seulement 12 % des sociétés canadiennes ont une posture de sécurité de premier plan.**
Toutes les organisations doivent connaître leur point de départ, leurs forces et leurs faiblesses, ce qui leur permettra d'optimiser leurs processus, leurs investissements et leur culture ainsi que de transformer la sécurité informatique. Elles peuvent toutes, indépendamment de leur taille, mettre en œuvre de vigoureuses pratiques de sécurité informatique.

**Les résultats commerciaux s'en suivent.**
Les organisations affichant la plus grande maturité de la sécurité informatique ont déclaré à la fois des résultats commerciaux supérieurs (revenus, profits, conformité réglementaire, frais d'exploitation, nombre de nouveaux produits et services) et des améliorations commerciales supérieures par rapport à toutes les autres.

Graphique 6



# PRINCIPALES CONSTATATIONS

# Le nuage est le nouveau champ de bataille

- L'infonuagique et toujours au cœur des technologies informatiques modernes.
- Plus de la moitié des organisations canadiennes ont adopté des infrastructures hybrides ou multinuagiques.
- Les attaques sur les services infonuagiques par les criminels, les pirates et les États-nations augmentent.
- Le nuage public représente la cible de prédilection, suivi des applications internes, des réseaux et des applications Web.

**La responsabilité partagée entraîne des complexités.**

La complexité du nuage découle du partage de la responsabilité pour la sécurité entre le fournisseur et l'organisation, et cette responsabilité change selon le modèle de déploiement infonuagique. Les facteurs qui suscitent l'attrait du nuage peuvent aussi compliquer ou restreindre la visibilité et le contrôle, et il faut de nouvelles compétences et de nouveaux ensembles d'outils pour surveiller et sécuriser les environnements informatiques dans le nuage.

Afin de protéger les environnements informatiques dans le nuage, les organisations doivent réaliser les bons investissements pour combler les écarts de gouvernance et de gestion des risques infonuagiques, déployer des contrôles de sécurité pour prévenir les menaces, surveiller et détecter les menaces, et automatiser les réponses.

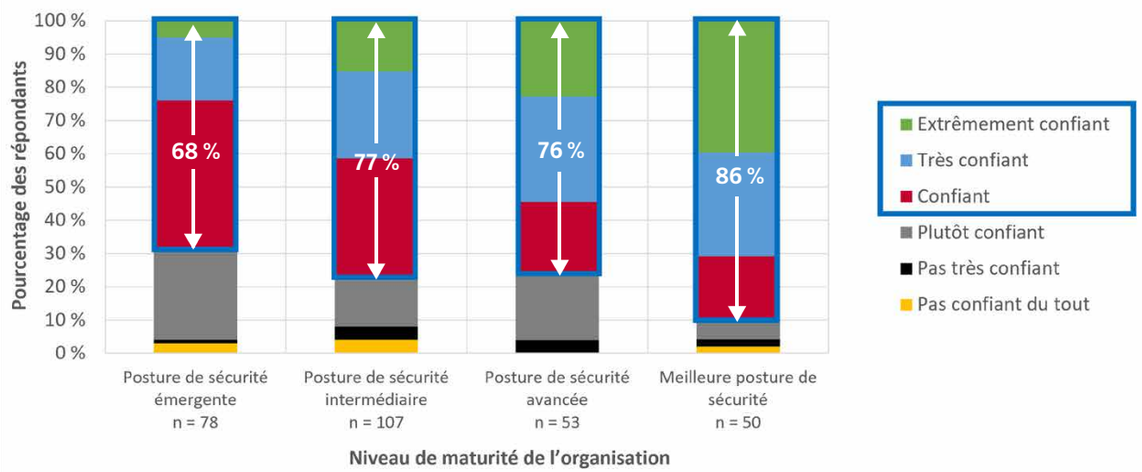
**Ces efforts ont des retombées directes.**

Les organisations affichant une maturité de la sécurité informatique accrue font davantage confiance à leurs efforts de sécurité infonuagique et à la sécurité informatique qui en découle.

## TECHNOLOGIES DE TRANSFORMATION NUMÉRIQUE UTILISÉES PAR LES ORGANISATIONS CANADIENNES

| | |
|---|---|
| Hybride ou multinuagique | 52 % |
| Technologies opérationnelles/IdO | 41 % |
| Informatique en périphérie | 38 % |
| Nuages privés | 35 % |
| Développement et exploitation | 29 % |
| Appareils personnels (BYOD) | 28 % |

## CONFIANCE ENVERS LA SÉCURITÉ INFORMATIQUE DES ENVIRONNEMENTS HYBRIDES ET MULTINUAGIQUES




Source : Enquête sur la sécurité de CDW de 2022 (n = 288)

# Rançongiciels : la menace qui afflige les organisations canadiennes.

**La taille de l'organisation n'importe pas : tout le monde est sur le radar des cyberattaquants.**

Les rançongiciels sont si répandus qu'ils comptent parmi les plus grands risques informatiques planant sur les organisations aujourd'hui. Sans une enquête approfondie, l'analyse des causes profondes et leur élimination, la réinfection par le rançongiciel est possible. Ces portes arrière sont souvent vendues à d'autres groupes d'attaque ou réutilisées par le même groupe pour une autre attaque.

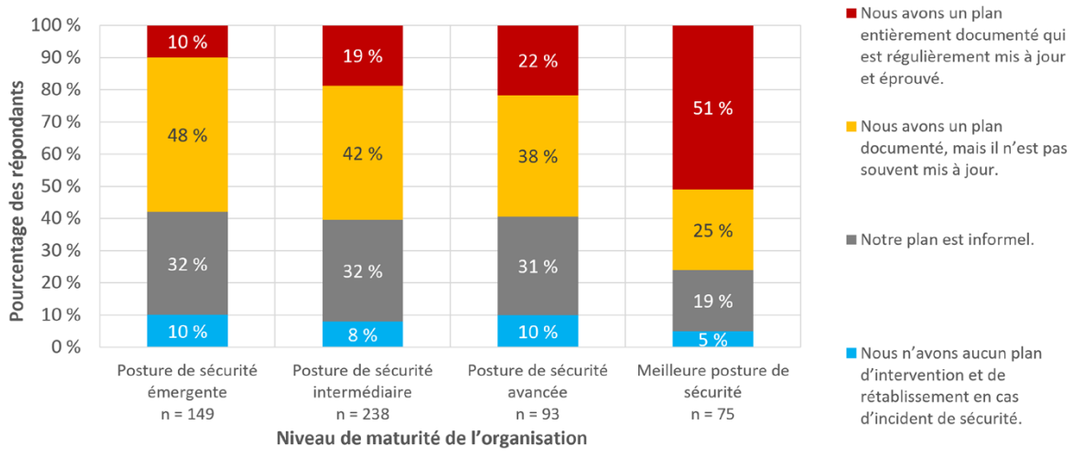
***Soixante-treize pour cent des sociétés canadiennes interrogées ont signalé des attaques d'infiltration des données avec demande de rançon dans la dernière année.***

**Revenir à l'état de confiance grâce à un plan d'intervention et de récupération.**

Un plan d'intervention et de récupération à jour et éprouvé est crucial pour limiter et éradiquer les attaques, analyser les causes profondes, permettre un rétablissement en douceur à partir de copies de sauvegarde et communiquer avec toutes les parties prenantes importantes. On peut ainsi optimiser la récupération après une attaque par rançongiciel ou autre, réduisant le temps d'indisponibilité et les coûts.

Les organisations parvenues à maturité relativement à la sécurité maintiennent un plan d'intervention et de récupération officiel et investissent le temps et les ressources nécessaires pour le mettre à jour et l'éprouver fréquemment.

## PLANS D'INTERVENTION ET DE RÉCUPÉRATION



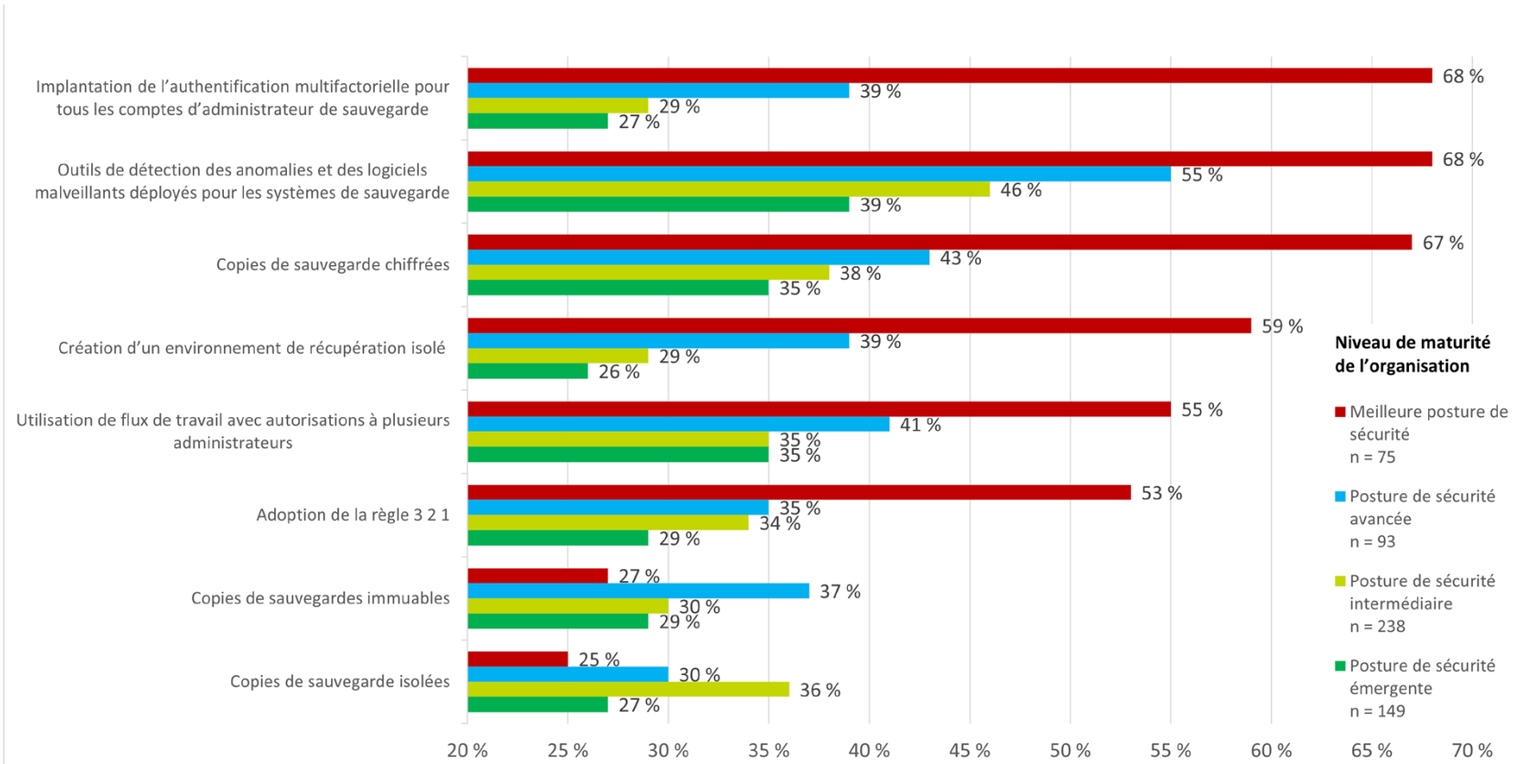

Source : Enquête sur la sécurité de CDW de 2022 (n = 555)

## Les stratégies de sauvegarde et de récupération des organisations canadiennes ne suffisent pas.

- Seulement 36 % des organisations canadiennes ont été en mesure de rétablir complètement leurs données et systèmes à partir de copies de sauvegarde lorsque nécessaire.
- Vingt et un pour cent ont déclaré être carrément incapables de se rétablir.

Les cyberattaques modernes et sophistiquées, notamment par rançongiciel, ciblent de plus en plus les sauvegardes pour mettre de la pression sur les organisations visées. Lors d'incidents de sécurité, il est courant de supprimer ou de compromettre des sauvegardes avant de s'approprier l'environnement de production. Pour les organisations touchées, l'évaluation de la fiabilité des copies de sauvegardes pendant une cyberattaque est l'une des principales causes d'une récupération lente.

### ADOPTION DE MESURES DE SAUVEGARDE



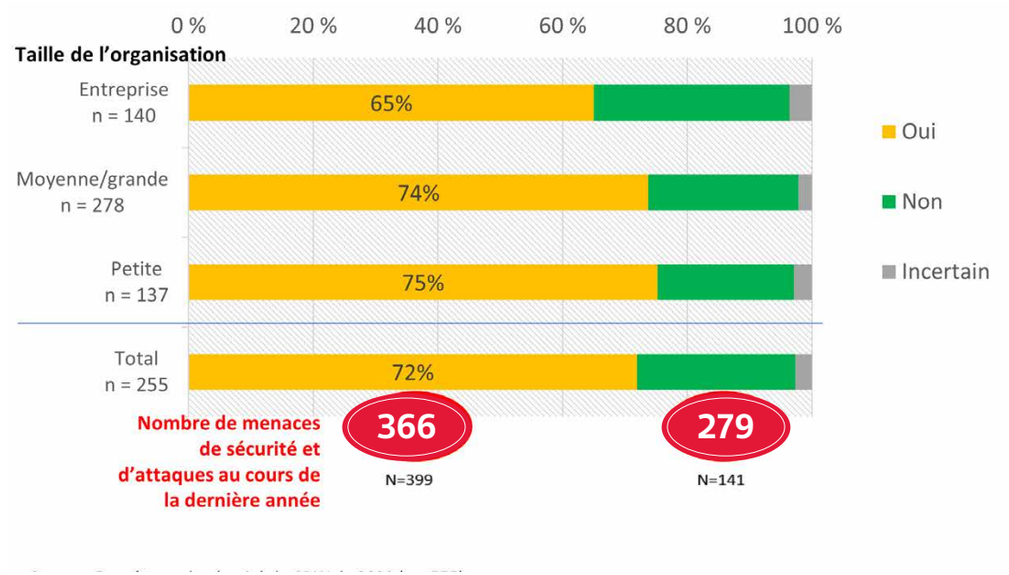

## Apprendre des experts.

Les organisations mûres ont investi dans une variété de mesures pour améliorer leur sécurité, dressant et tenant à jour un solide plan de récupération.

## La surexposition des renseignements permettant l'identification mène à une expansion significative de la surface d'attaque.

Les organisations dont des tiers ont accès à des renseignements personnels permettant l'identification (RPI) ont souffert 31 % plus de cyberattaques en 12 mois comparativement à celles dont les RPI dans leur environnement informatique ne sont pas exposés à des tiers.

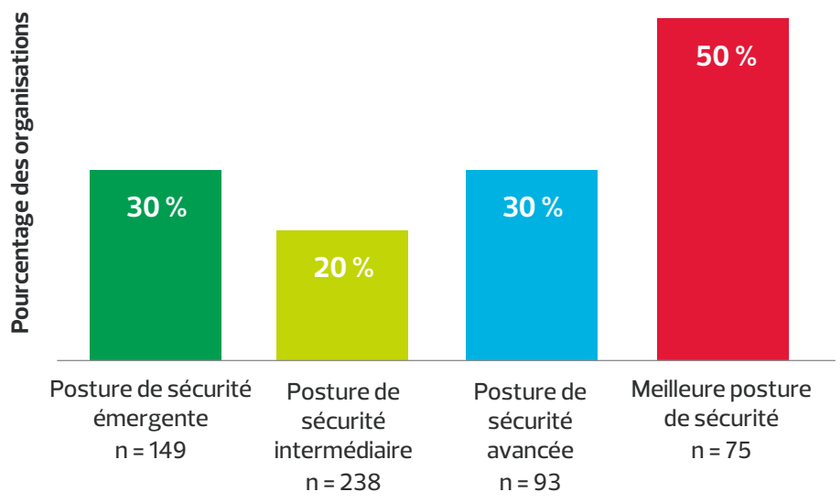
### ACCÈS EXTERNE AUX RPI




Source : Enquête sur la sécurité de CDW de 2022 (n = 555)

***Soixante-douze pour cent des organisations canadiennes interrogées ont indiqué que leurs fournisseurs, partenaires et entrepreneurs ont accès aux RPI contenus dans les systèmes informatiques, les technologies opérationnelles ou les bases de données.***

### ÉVALUATION DES RISQUES DE TIERS EFFECTUÉE




Source : Enquête sur la sécurité de CDW de 2022 (n = 555)

La gestion efficace de l'accès aux RPI est essentielle pour cerner et atténuer les risques se rapportant au recours à des tiers. Un plan de sécurité contenant une évaluation complète des risques de tiers constitue un indicateur d'une maturité élevée sur le plan de la sécurité.

# La confiance zéro devient une architecture de sécurité de prédilection.

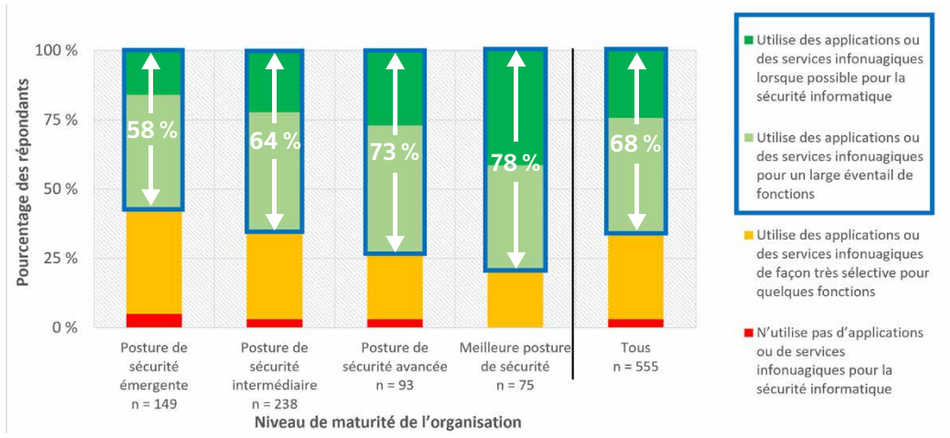
**L'avenir est voué aux effectifs hybrides. Or, qui dit effectif hybride dit surface d'attaque élargie.**

Selon Statistique Canada, en 2020, 40 % des employés se sont retrouvés à travailler à la maison, grimpant jusqu'à 70 % pour les travailleurs de certains secteurs. En 2023, environ 23 % de la main-d'œuvre canadienne travaillera surtout à domicile ou à distance, et on prévoit que ce pourcentage augmentera à 27 % d'ici 2025[1].

**La stratégie de confiance zéro se répand largement.**

- Trente pour cent des organisations canadiennes interrogées ont épousé l'architecture de confiance zéro.
- Quarante pour cent sont en train de la déployer.
- Une seule organisation sur sept (14 %) est indécise ou ne le prévoit pas.
- La catégorie Entreprises ouvre la voie, 93 % des sociétés l'appliquant ou prévoyant le faire au cours de la prochaine année.
- Les organisations qui adoptent de nombreuses technologies de transformation numérique ont toutes choisi une architecture de confiance zéro.

## LES PLANS DE SÉCURITÉ INFONUAGIQUES




Source : Enquête sur la sécurité de CDW de 2022 (n = 555)

**Plus des deux tiers (68 %) de toutes les organisations font confiance à la sécurité informatique dans le nuage.**

Les plus matures affichent un taux d'adoption beaucoup plus élevé de la sécurité infonuagique. Les technologies de pointe telles que l'intelligence artificielle (IA), l'apprentissage machine et les renseignements sur les menaces sont de plus en plus intégrées aux solutions de sécurité.

[1] Prévisions de retour au bureau d'IDC pour le Canada, novembre 2021

# Une culture d'entreprise privilégiant la cybersécurité améliore la maturité

**La cybersécurité n'est plus qu'un problème informatique, mais bien la responsabilité de tout le monde.**

- La participation de la direction en dehors des TI à la création d'une culture où les pratiques exemplaires de sécurité sont ancrées dans l'organisation constitue un facteur déterminant pour l'évaluation du niveau de maturité en matière de sécurité.
- Les chefs d'entreprise doivent comprendre les cyberrisques et leurs répercussions afin de déterminer le niveau optimal de protection, dont les investissements et les ressources.

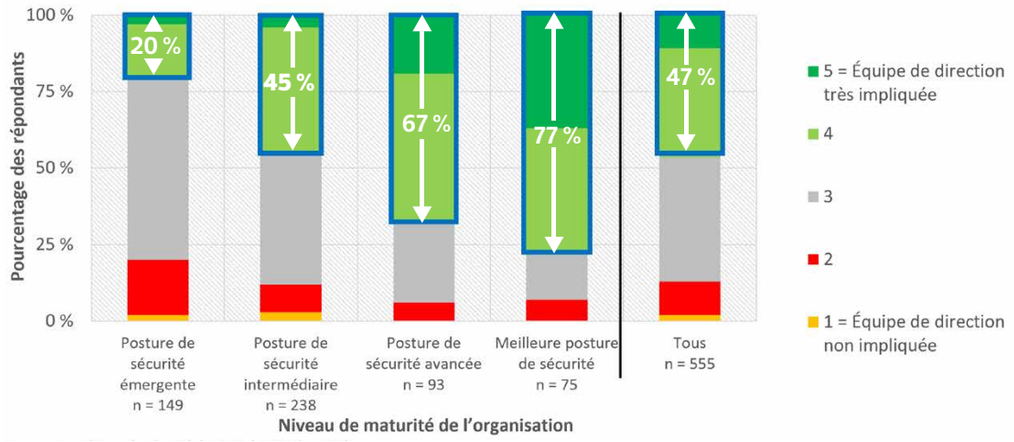
**Offrez de la formation tous les trimestres.**

- Les organisations qui donnent une formation trimestrielle de sensibilisation à la sécurité ont connu moins d'incidents ou d'attaques réussies que celles offrant de la formation à une autre fréquence; même la formation mensuelle n'a pas entraîné moins d'incidents.
- Tout le monde dans l'organisation doit savoir comment aborder les courriels suspects, assurer la sécurité des données d'entreprise ainsi que créer et gérer des mots de passe forts.

**Adoptez le principe de développement, de sécurité et d'exploitation.**

- Le cycle de vie de développement sûr est à la base d'une culture de développement et d'exploitation durable. Le processus de développement, de sécurité et d'exploitation intègre la sécurité aux cycles de développement rapides.
- Parmi les organisations disposant d'un processus de développement et d'exploitation interne, 73 % l'ont adopté ou sont en train de le déployer dans toute l'organisation.
- Près de toutes (90 %) les organisations les plus mûres ont recours au principe de développement, de sécurité et d'exploitation, et plus de la moitié de même les moins mûres y ont recours.

## LA DIRECTION FAVORISE UNE CULTURE DE PRATIQUES DE SÉCURITÉ EXEMPLAIRES




Source : Enquête sur la sécurité de CDW de 2022 (n = 555)

## Recommandations et appels à l'action

**I. Prendre du recul et procéder à une évaluation.**
Il est crucial de prendre le temps d'évaluer les cyberrisques qui planent sur votre organisation ainsi que la capacité de votre programme de sécurité de les atténuer. Cette évaluation doit comprendre les employés, les processus et les technologies pour refléter fidèlement votre état actuel, décrire une vision de votre état futur et dresser une feuille de route pour la concrétiser.

**II. Repenser la sécurité grâce à une architecture de confiance zéro.**
La transformation numérique bouscule la sécurité traditionnelle. À mesure qu'elles évoluent, les organisations canadiennes doivent adapter leur approche pour s'assurer qu'elles ont la résilience nécessaire. Repensez la sécurité en optant pour la zéro confiance, et mettez ainsi l'accent sur la protection de l'infrastructure d'entreprise, des applications et des données en fonction de l'identité et la confiance envers les utilisateurs comme les dispositifs.

**III. Épouser le nuage pour la cybersécurité.**
Le nuage représente un élément d'infrastructure essentiel que votre programme de sécurité protège. Les solutions et les services de sécurité sont fins prêts pour la transformation numérique, et les organisations doivent adopter des plateformes de sécurité infonuagiques. La sécurité conçue et bâtie pour tirer parti des technologies infonuagiques permet aux organisations de répondre aux besoins de leur effectif numérique et de leurs clients.

**IV. Rétablir la confiance envers vos copies de sauvegarde.**
Vu la fréquence et la gravité des incidents de sécurité, il est plus essentiel que jamais de faire confiance à ces copies de sauvegarde. Les organisations doivent hiérarchiser la sécurité de leurs sauvegardes afin d'en garantir l'intégrité et la disponibilité. C'est essentiel pour s'assurer qu'elles peuvent se rétablir à un niveau de confiance indiqué par leurs objectifs de point et de délai de récupération.

**V. Créer une culture de responsables de la sécurité.**
Les organisations doivent faire de la protection des systèmes et des données la responsabilité de tous. On peut y arriver en l'intégrant à une culture organisationnelle qui aborde la sécurité en tant que facteur de différenciation. Communiquez les indicateurs de rendement clés liés à la sécurité et à la protection de la vie privée à la direction ainsi qu'à l'ensemble de l'organisation afin d'accroître la responsabilisation et la sensibilisation.

**Pour connaître les conclusions détaillées et les recommandations de CDW aux chefs des TI et d'entreprise, consultez le rapport complet.**

*L'analyse a montré qu'une maturité accrue de la sécurité porte des fruits. Les organisations canadiennes affichant la plus grande maturité de la sécurité informatique ont déclaré* ***miser sur un plus vaste éventail de résultats commerciaux*** *(revenus, profits, conformité réglementaire, frais d'exploitation, nombre de nouveaux produits et services) et des* ***améliorations commerciales supérieures*** *par rapport à leurs contreparties.*

## À PROPOS DE CDW

CDW Canada est un chef de file parmi les fournisseurs de solutions technologiques pour les entreprises, le gouvernement, le milieu de l'enseignement et celui des soins de santé. CDW Canada aide ses clients à atteindre leurs objectifs en leur livrant des solutions et des services technologiques intégrés qui les aident à s'y retrouver dans un marché des TI de plus en plus complexe et à maximiser le retour de leur investissement en technologie. Ses domaines de spécialisation comprennent les logiciels, le réseautage, les communications unifiées, les centres de traitement des données et les solutions de mobilité. CDW Canada, qui fait partie des 100 meilleurs fournisseurs de solutions au Canada selon Channel Daily News, est une filiale en propriété exclusive de CDW Corporation, qui est située à Vernon Hills, en Illinois, et qui figure au classement Fortune 500. Pour obtenir de plus amples renseignements, visitez le site www.CDW.ca.

## À PROPOS D'IDC CANADA

International Data Corporation (IDC) est le premier fournisseur mondial de renseignements, de services de conseil et d'événements sur le marché de la technologie de l'information, des télécommunications et des technologies grand public. IDC Canada fait partie d'un réseau de plus de 1 100 analystes fournissant une expertise globale, régionale et locale sur les possibilités et tendances en matière de technologie et d'industrie, avec plus d'analystes dédiés à la compréhension du marché canadien que tout autre cabinet de recherche mondial.

Étude indépendante menée par IDC Canada | Publiée en mai 2022