Delinea

LIVRE BLANC

La sécurité de l'identité est essentielle pour obtenir et conserver une cyber assurance

Rapport de l'étude sur la cyber assurance 2024

Synthèse

La cyber assurance est un élément essentiel d'un programme de gestion des cyber-risques pour garantir la résilience et la reprise. Maintenant que la cyber assurance est devenue une pratique courante pour tous les types d'organisation, la priorité est de maintenir une couverture même si les facteurs de risque évoluent.

Alors que les cyber incidents ont secoué le secteur, les assureurs se livrent à des évaluations détaillées des risques, et il est de plus en plus difficile pour les responsables de la cybersécurité de démontrer la valeur de leur programme de sécurité et d'obtenir une couverture solide. Les organisations doivent fournir des preuves pertinentes pour s'assurer que leur assurance se poursuit et augmente ou s'ajuste si nécessaire. La collecte d'informations précises et actualisées peut s'avérer incroyablement lourde et fastidieuse pour les organisations complexes et hybrides dont le profil de risque évolue.

Dans cette étude de recherche menée auprès de 300 décideurs, nous analysons comment les entreprises relèvent ces défis pour obtenir et maintenir une cyber assurance. Plus précisément, nous étudions comment les organisations adoptent de nouvelles technologies comme l'intelligence artificielle pour accroître leur efficacité, évoluer rapidement et réduire leurs coûts.

Points clés :

1. **Les lacunes en matière de sécurité de l'identité sont la cause la plus fréquente des cyber incidents qui donnent lieu à des demandes d'indemnisation. Les compromissions d'identité et de privilèges représentent 47 % des attaques qui donnent lieu à des demandes d'indemnisation.**

2. **Les compagnies d'assurance exigent des preuves quant à la sécurité de l'identité avant d'accorder une police. Plus de 40 % des compagnies d'assurance exigent des contrôles d'autorisations/d'accès à moindre privilège avant d'accorder une police d'assurance. Pratiquement l'ensemble (95 %) des entreprises américaines ont dû investir dans des solutions de sécurité de l'identité avant de souscrire une police d'assurance.**

3. **Bien que les coûts globaux de la cyber assurance augmentent, l'IA constitue un levier pour les assurés. La moitié des entreprises américaines utilisent la détection et la surveillance des menaces assistées par l'IA pour réduire leurs primes de cyber assurance.**

Lisez la suite pour évaluer vos propres pratiques en matière de sécurité de l'identité et vos stratégies en matière de cyber assurance. Ce que vous apprendrez vous aidera à préparer votre prochaine évaluation de cyber assurance et à identifier des moyens innovants pour réduire vos efforts et vos coûts.

47 %

Les compromissions d'identité et de privilèges représentent 47 % des attaques qui donnent lieu à des demandes d'indemnisation

Principale conclusion 1

Les lacunes en matière de sécurité de l'identité sont la cause la plus fréquente des cyber incidents qui donnent lieu à des demandes d'indemnisation.

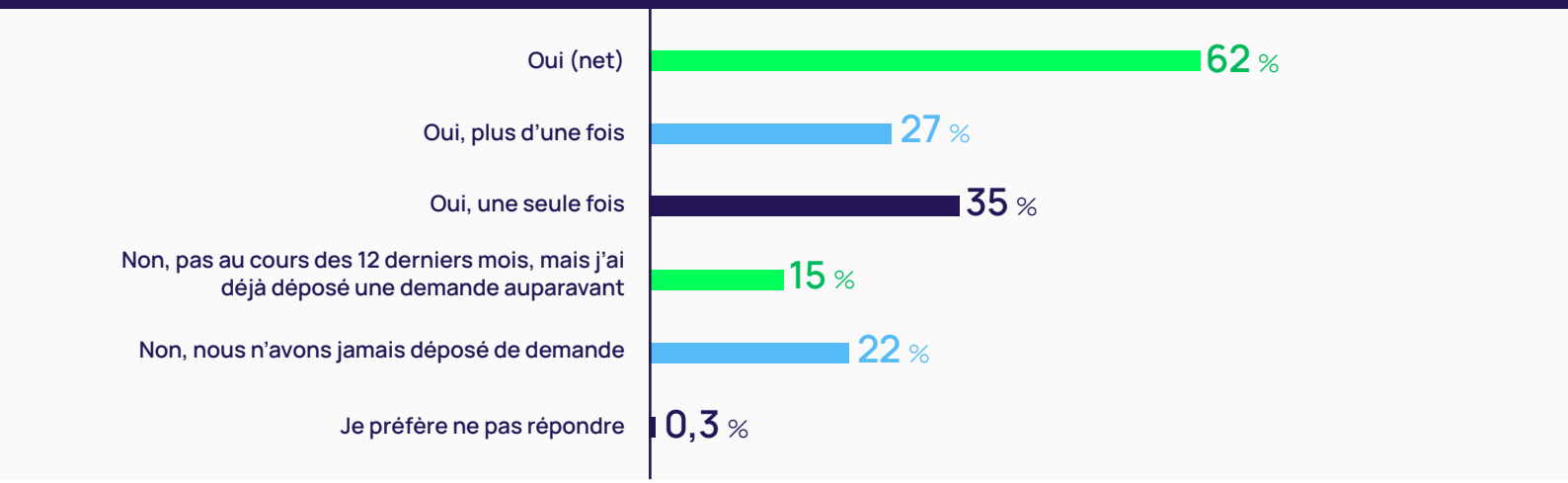
La fréquence des sinistres liés aux cyber assurances reste élevée.

Une fois que les entreprises disposent d'une cyber assurance, elles l'utilisent.

Les données montrent que 77 % des entreprises assurées ont déjà déposé une demande d'indemnisation. Cela concorde avec les résultats de l'enquête de Delinea en 2023, dans laquelle 79 % des répondants ont déclaré avoir déjà utilisé une cyber assurance dans le passé.

Au cours des 12 derniers mois seulement, 62 % des entreprises ont déposé une demande d'indemnisation. L'année a été particulièrement mauvaise pour plus de 27 % des entreprises, qui ont déposé plus d'une demande au cours des 12 mois précédents.

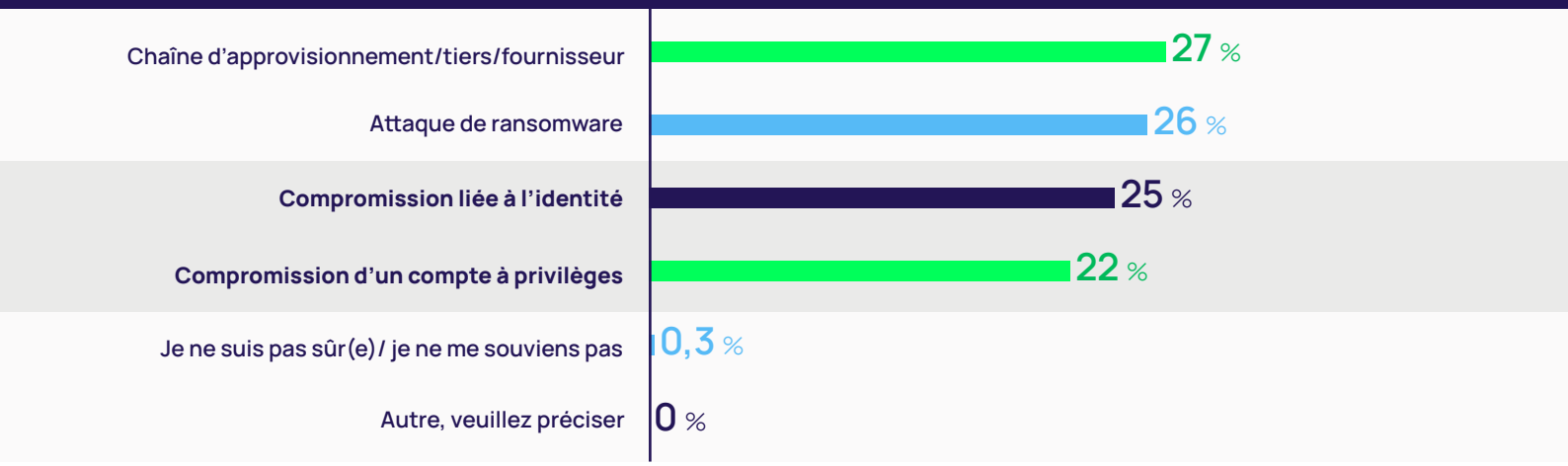
Figure 1 | Votre organisation a-t-elle déposé une demande d'indemnisation au titre de leur cyber assurance au cours des 12 derniers mois ?



Les techniques d'attaque exploitent les identités et les comptes à privilèges.

Lorsqu'on les considère ensemble, deux vecteurs d'attaque liés à l'identité — la compromission d'identité et celle des comptes à privilèges — sont responsables de plus de 47 % des attaques ayant entraîné des demandes d'indemnisation.

Figure 2 | Quelle est la cause du cyber incident lié à la demande d'indemnisation au titre de la cyber assurance ?



De nos jours, la plupart des cyber attaquants n'ont pas besoin de s'introduire dans un système : ils s'y connectent simplement. Les attaques liées à l'identité commencent généralement lorsqu'un attaquant utilise des informations d'identification valides qu'il a volées ou achetées. Il peut utiliser ces informations d'identification pour usurper une identité autorisée ou utiliser un compte à privilèges afin de pouvoir déverrouiller l'accès à des ressources protégées. Selon le niveau d'accès attaché à cette identité ou à ce compte à privilèges, l'attaquant peut être en mesure de télécharger des logiciels malveillants, de manipuler des données, d'arrêter des systèmes, ou plus encore, ce qui peut conduire à une demande d'indemnisation potentielle auprès de l'assureur.

Dans le cadre de la chaîne d'approvisionnement, des tiers tels que les sous-traitants, les fournisseurs et les partenaires ont souvent accès à des données sensibles et à des systèmes informatiques. Par exemple, les équipes d'opérations informatiques externalisent souvent des tâches telles que le dépannage, et les équipes d'ingénierie évoluent généralement en faisant appel à des développeurs externes. Ces utilisateurs peuvent accéder aux ressources à l'aide d'un compte à privilèges partagé ou d'une identité individuelle. Trop souvent, ces types d'utilisateurs opèrent sans surveillance suffisante et l'accès reste en place longtemps après la fin des projets, laissant des vulnérabilités que les acteurs malveillants exploiteront, ce qui entraînera un éventuel dédommagement pour les assureurs.

Les ransomwares s'implantent souvent grâce à l'ingénierie sociale ou au phishing, encourageant les utilisateurs disposant de privilèges locaux à cliquer sur un lien qui télécharge des logiciels malveillants. Une fois qu'ils ont pris pied, un attaquant peut crypter les données et exiger une rançon pour la clé de cryptage, ou exfiltrer les données et menacer de les divulguer à moins qu'une rançon ne soit payée.

Les entreprises souscrivent une couverture de cyber assurance pour répondre à leurs exigences de conformité et assurer la continuité de leurs activités.

Nous avons demandé aux entreprises les raisons pour lesquelles elles ont cherché à souscrire une assurance *au moment où elles l'ont fait*. Les éléments déclencheurs incluent le respect des exigences réglementaires, les directives de la direction générale ou du conseil d'administration ou en réaction à des cyber attaques récentes, soit au sein de leur secteur, soit affectant directement leur organisation.

Les répondants indiquent que les exigences de conformité/réglementaires constituent le *principal motif* de souscription d'une cyber assurance. Il ne s'agit pas ici de dire que les réglementations telles que PCI, HIPAA et d'autres cadres de conformité exigent que les entités couvertes aient une cyber assurance. Il ne s'agit pas non plus de dire que la cyber assurance est une stratégie efficace pour couvrir les amendes liées à la non-conformité, du moins pour la plupart des entreprises ; en réalité, les amendes réglementaires sont l'une des dépenses ***les moins courantes*** que la cyber assurance prend en charge.

Figure 3 A | Quelles étaient vos principales raisons de souscrire une cyber assurance au moment où vous l'avez fait ?

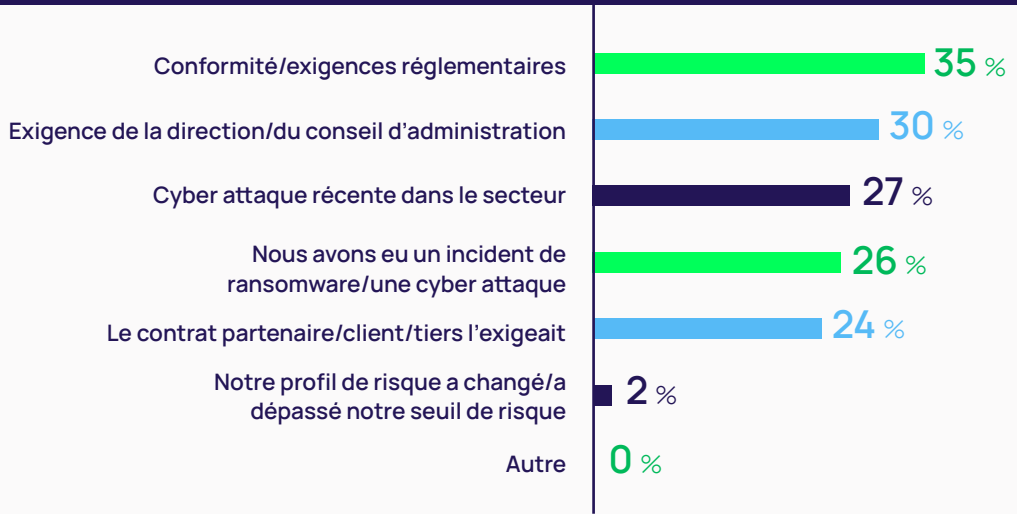
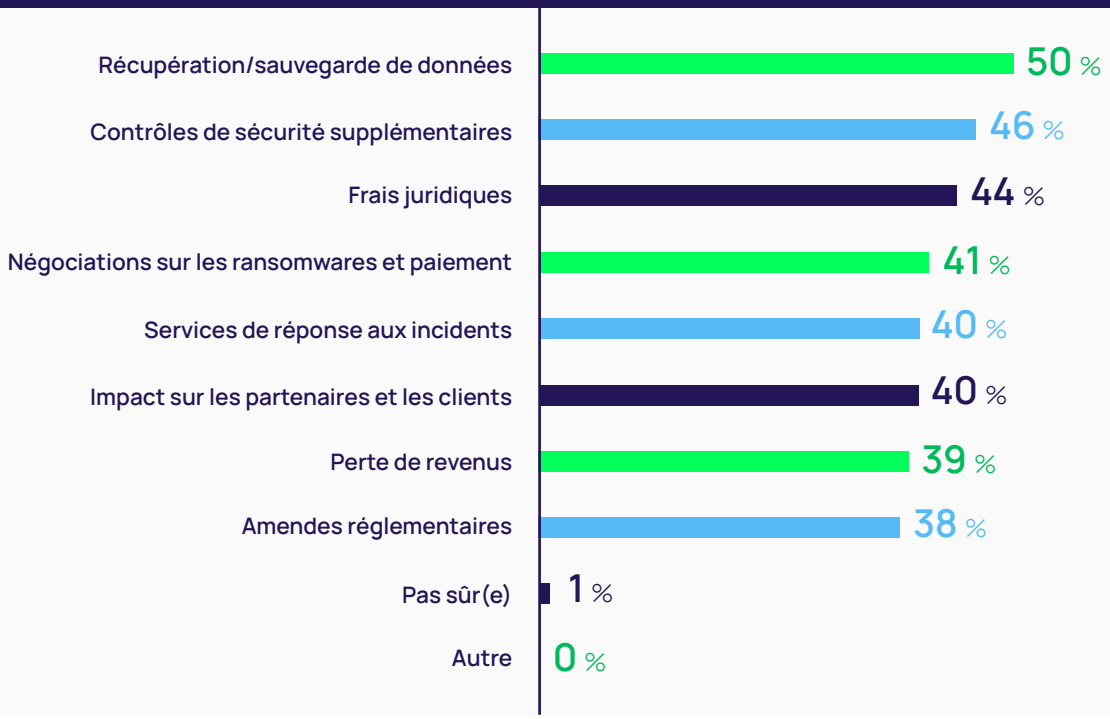


Figure 3 B | Que couvrirait votre police de cyber assurance ?



Il est plus probable que les entreprises régies par des réglementations sectorielles soient confrontées à des amendes sévères en cas de non-conformité en matière de protection des données. Une récupération et une sauvegarde rapides peuvent aider à éviter les amendes et autres coûts associés à une non-conformité à la suite d'une violation de données, car elles vous permettent de récupérer et de sécuriser rapidement les données.

La cyber assurance se concentre fortement sur les services de récupération et de sauvegarde des données, car ils sont essentiels pour réduire les temps d'arrêt et les pertes financières après un cyber incident. En couvrant ces services, les assureurs soutiennent une reprise rapide et la résilience des entreprises, ce qui profite à la fois à l'assuré et à l'assureur.

Considérez également que l'assurance est une stratégie de gestion des risques et non une stratégie de cybersécurité. De nombreuses entreprises utilisent des cadres de conformité ou de cybersécurité comme NIST pour guider leurs programmes de sécurité, même si elles ne sont pas des entités couvertes. Ces cadres exigent des preuves de contrôles de sécurité, tout comme les compagnies d'assurance, car il est prouvé qu'ils réduisent les risques. Si vous mettez en place ces contrôles, vous serez en mesure de satisfaire à la fois les régulateurs et les compagnies d'assurance. Même si vous n'êtes pas soumis à des réglementations pouvant entraîner des amendes, vous ne pouvez pas simplement ignorer cet aspect et espérer réussir votre prochain audit ou évaluation d'assurance.

La moitié des entreprises américaines utilisent la détection et la surveillance des menaces assistées par l'IA pour réduire leurs primes de cyber assurance

Principale conclusion 2

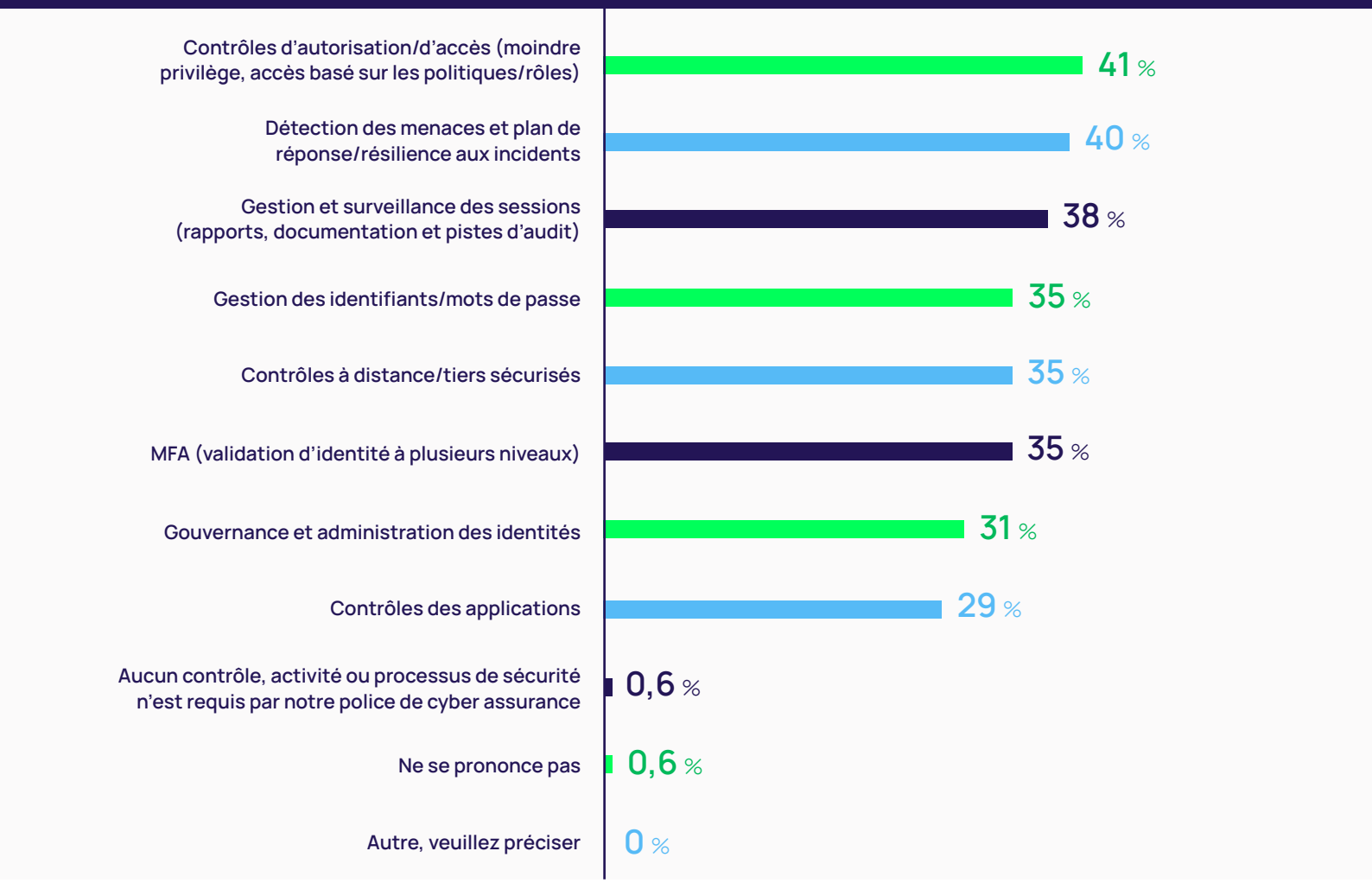
Les compagnies d'assurance exigent des preuves en matière de sécurité de l'identité avant d'accorder une police, 41 % d'entre elles exigeant des contrôles d'autorisation.

Les assureurs ont besoin de contrôles, d'activités et de processus de sécurité de l'identité.

Maintenant qu'elles disposent de davantage de données historiques indiquant la cause des cyber attaques, de nombreuses compagnies d'assurance exigent des assurés qu'ils réduisent la probabilité et l'impact des cyber incidents, atténuant ainsi leurs indemnités potentielles en cas de sinistre. Presque tous les répondants ont une certaine forme d'exigence en matière de sécurité de l'identité imposée par leur compagnie de cyber assurance. La plupart des personnes interrogées affirment que les polices de cyber assurance nécessitent de multiples contrôles de sécurité de l'identité.

Les assureurs demandent généralement aux assurés d'établir des contrôles liés à l'autorisation/à l'accès à moindre privilège, suivis de près par la détection et la réponse aux menaces.

Figure 4 | Quels contrôles, activités et processus de sécurité sont requis par votre police de cyber assurance ?



Ces contrôles sont conformes aux meilleures pratiques du secteur et aux exigences réglementaires. Des contrôles de sécurité efficaces aident non seulement à prévenir les incidents, mais garantissent également que les organisations peuvent réagir rapidement et efficacement, réduisant ainsi les temps d'arrêt et les pertes financières. En exigeant des contrôles de sécurité complets, les assureurs peuvent mieux gérer et prévoir les pertes potentielles, ce qui conduit à des primes plus stables et prévisibles pour les assurés.

Des contrôles de sécurité de l'identité définis requis

Contrôles d'accès/ autorisation

Les contrôles d'accès autorisent les systèmes et les données auxquels une identité peut accéder et ce qu'elle peut faire avec cet accès. Les entreprises gèrent généralement les autorisations via des politiques telles que des contrôles d'accès basés sur les rôles ou des contrôles d'accès basés sur les attributs. Les meilleures pratiques en matière de moindre privilège exigent que les identités ne disposent que des autorisations nécessaires pour exécuter leurs fonctions, uniquement lorsqu'elles en ont besoin.

Contrôles des applications

Les contrôles des applications vous aident à équilibrer les meilleures pratiques en matière de moindre privilège et la productivité des utilisateurs. Les applications de confiance sont ajoutées aux listes d'autorisation pour l'installation ou l'exécution automatiques, tandis que les applications malveillantes connues (malware) sont ajoutées aux listes noires et bloquées. Les applications inconnues peuvent être mises en sandbox jusqu'à ce qu'elles aient été examinées et approuvées.

Gestion des identifiants/mots de passe

Les informations d'identification incluent les noms d'utilisateur, les mots de passe, les tokens et d'autres secrets qui déverrouillent l'accès à vos systèmes et à vos données. Les cyber attaquants recourent à des techniques comme le bourrage d'identifiants et le craquage de mots de passe pour dérober des informations d'identification. Ils peuvent également acheter des informations d'identification auprès de courtiers d'accès initial (access brokers) sur le dark web. Pour éviter le vol, les informations d'identification doivent être difficiles à deviner et toujours sécurisées. Vous pouvez stocker vos informations d'identification dans un coffre-fort crypté répondant à des standards de niveau militaire. La gestion continue des informations d'identification, comme la rotation et l'expiration, garantit que les informations d'identification ont une durée de vie limitée.

Gouvernance et administration des identités

La gouvernance et l'administration des identités contrôlent les autorisations pour les identités tout au long de leur cycle de vie, y compris lorsque les utilisateurs rejoignent, changent de poste ou quittent l'entreprise, et permettent de superviser toutes les identités de votre organisation (humaines et machines), ce qui facilite la démonstration de cette supervision aux auditeurs, aux compagnies proposant des cyber assurances et aux organismes de conformité.

Authentification multi-facteurs (MFA)

L'authentification multi-facteurs vérifie les identités humaines en demandant aux individus de fournir un élément en leur possession (comme un code sur leur téléphone ou une empreinte digitale) ou une information qu'ils connaissent (comme des réponses à des questions de sécurité). Les meilleures pratiques imposent une vérification de l'identité à chaque interaction à haut risque, y compris lors de la connexion initiale et lors de l'élévation des privilèges.

Contrôles à distance/ tiers sécurisés

Ces contrôles permettent aux employés à distance et aux tiers d'accéder en toute sécurité aux ressources exactes dont ils ont besoin pour effectuer leur tâche, tout en étant étroitement surveillés.

Gestion et surveillance des sessions

La gestion et la surveillance continue des sessions détectent les anomalies dans les activités et les événements liés à l'identité, contribuant ainsi à la prévention proactive des incidents et à une réponse rapide. Les pistes d'audit vous aident à identifier des tendances, ce qui permet de mieux anticiper les risques et de faciliter l'analyse approfondie après un incident. De plus, les rapports granulaires vous permettent de suivre les améliorations de votre posture de sécurité de l'identité, de garantir la responsabilité et de fournir la preuve des contrôles effectués aux compagnies de cyber assurance.

Détection des menaces et réponse aux incidents

Une détection efficace des menaces et une réponse aux incidents sont essentielles pour la cyberrésilience et la continuité des activités. Les contrôles comprennent des mécanismes de détection des menaces et un plan de réponse structuré pour atténuer de manière proactive les risques et contenir et corriger les incidents en cours. Cela inclut des redondances pour garantir un minimum ou aucune perturbation en cas d'incident.

L'importance de la sécurité de l'identité est soulignée par les experts en sécurité et en cyber assurance.

CJ Dietzman

Vice-président principal d'Alliant Assurance Service

Lorsque je pense aux attentes des compagnies d'assurance et des souscripteurs, la sécurité de l'identité est devenue un enjeu de taille. La manière dont les compagnies de cyber assurance mesurent le risque est basée sur les incidents, la loi et les demandes d'indemnisation. Lorsque nous procédons à la rétro-ingénierie des cyber attaques, nous constatons souvent des points faibles dans la gestion des identités. Il est essentiel de disposer d'un récit clair sur les contrôles mis en place et d'une vue d'ensemble cohérente sur la manière dont vous atténuez les risques d'accès non autorisé et protégez les identités.

La majorité des incidents de cybersécurité ayant conduit à une demande d'indemnisation trouvent leur origine dans la collecte d'informations d'identification, la compromission interne ou l'accès accordé à un tiers. Ainsi, lors des évaluations pour un renouvellement, ce sont ces aspects qui sont examinés en priorité.

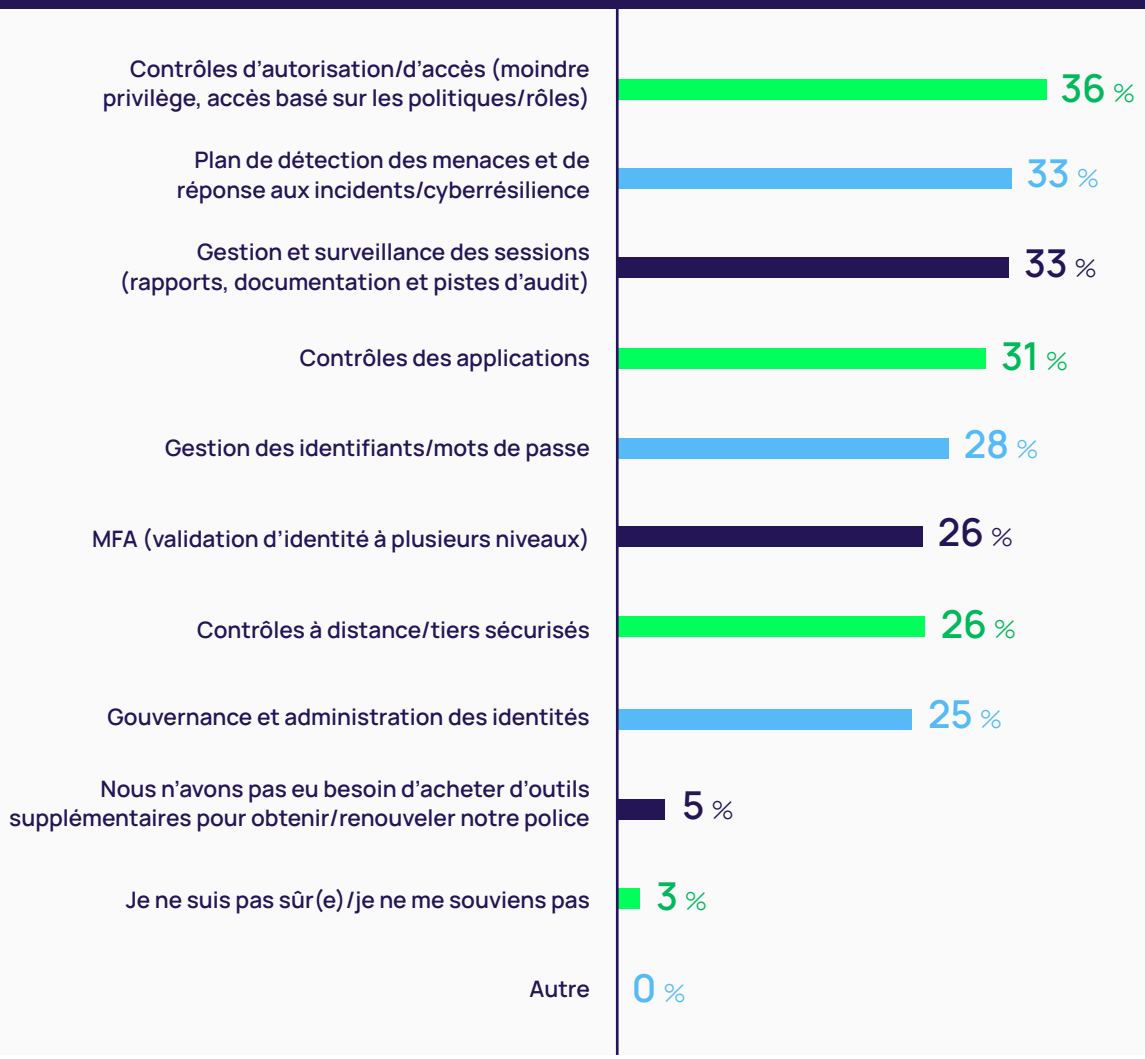
Myrna Soto

PDG d'Apogee Executive Advisors et experte en cybersécurité et gestion des risques

La majorité des entreprises interrogées ont dû investir dans des solutions de sécurité de l'identité avant d'obtenir ou de renouveler leur police.

Pour répondre aux exigences de sécurité mentionnées ci-dessus, les organisations reconnaissent qu'elles ne peuvent pas se contenter de présenter des processus manuels aux compagnies d'assurance et espérer obtenir une police. Au lieu de cela, elles ont dû acheter des solutions de sécurité de l'identité pour les intégrer à leur pile technologique de sécurité.

Figure 5 | Quels outils supplémentaires avez-vous dû acquérir pour obtenir/renouveler votre police ?

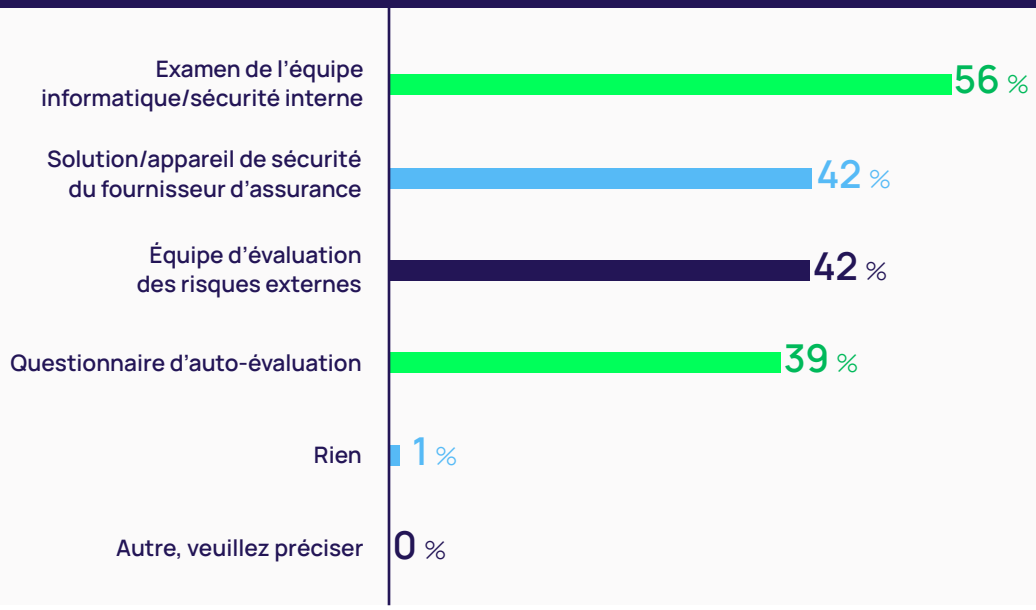


Ces résultats mettent en évidence la diversité des besoins des organisations en matière de sécurité et leurs différents niveaux de préparation en ce qui concerne l'infrastructure de cybersécurité.

Les évaluations examinent la posture de sécurité avant l'octroi des polices d'assurance.

Reflétant la maturité croissante du secteur de la cyber assurance, les assureurs exigent désormais des évaluations détaillées de la posture de sécurité. La plupart des répondants choisissent de réaliser eux-mêmes ces évaluations. D'autres font appel à une équipe d'évaluation des risques tierce pour compléter leurs compétences internes et fournir une vision impartiale de la posture de sécurité d'une entreprise.

Figure 6 | Quels types d'évaluations avez-vous dû effectuer pour obtenir votre police de cyber assurance ?



Que vous réalisiez ces évaluations en interne ou fassiez appel à un prestataire externe, attendez-vous à ce qu'elles mobilisent des membres qualifiés de vos équipes informatiques et de sécurité, les détournant ainsi de leurs tâches quotidiennes et projets stratégiques.

41 %

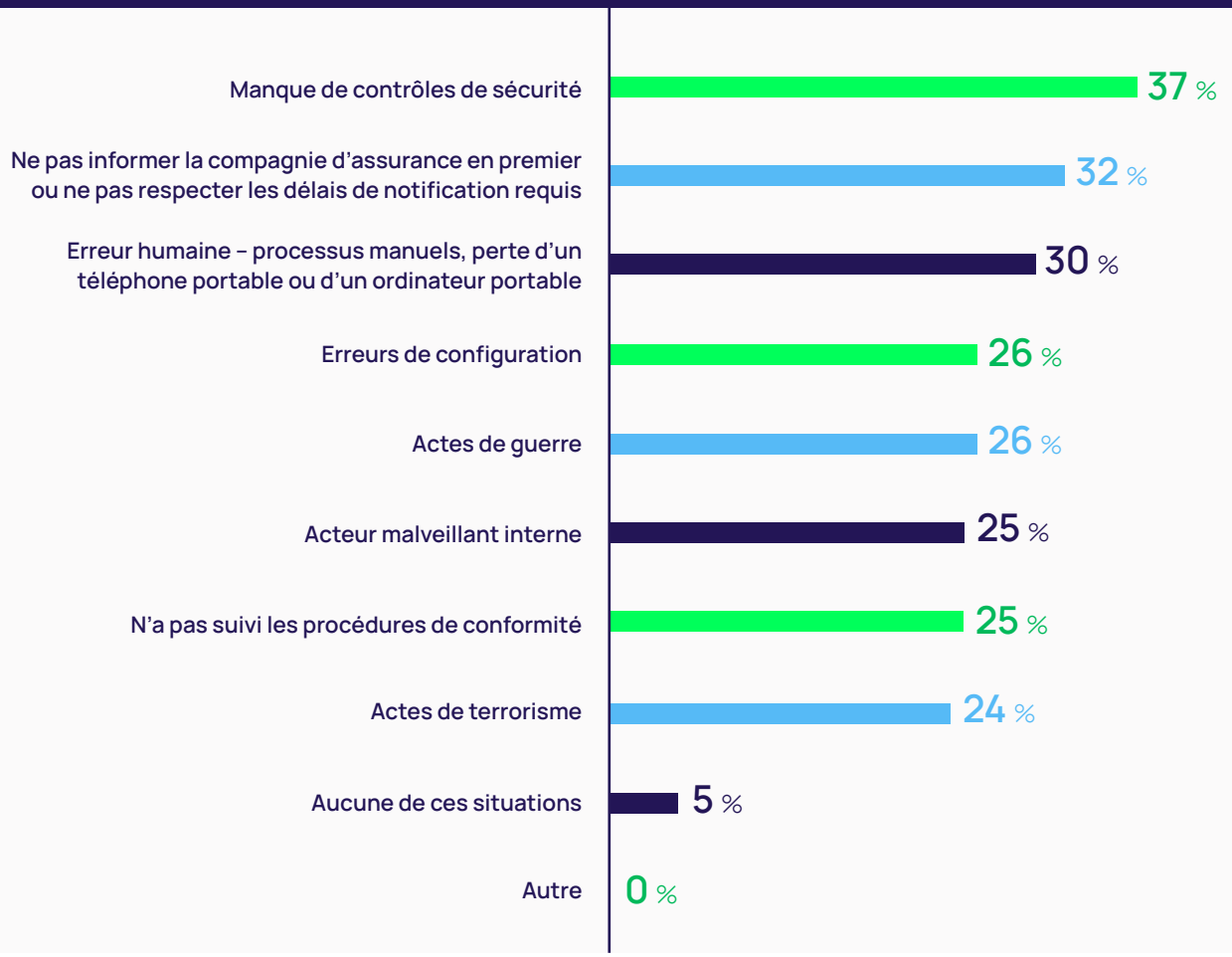
41 % des compagnies d'assurance exigent des contrôles d'autorisations/ d'accès à moindre privilège avant d'accorder une police d'assurance

Les exigences ne s'arrêtent pas après l'octroi des polices. Vous devez maintenir des contrôles de sécurité efficaces si vous souhaitez que les demandes d'indemnisation soient réglées.

Bonne nouvelle : vous avez acquis des solutions de sécurité de l'identité, démontré l'efficacité de vos contrôles et réussi votre évaluation. Votre police d'assurance vous a été accordée !

Cependant, les résultats de cette enquête montrent que si vous ne maintenez pas ces contrôles de sécurité en place et ne les utilisez pas correctement, votre demande d'indemnisation risque d'être refusée. Comme l'ont souligné les répondants, vous devez vous assurer que les contrôles de sécurité sont bien appliqués à votre organisation en pleine évolution, qu'ils sont correctement configurés et fonctionnent comme prévu.

Figure 7 | Dans quelles situations, le cas échéant, votre couverture de cyber assurance pourrait-elle devenir caduque ?



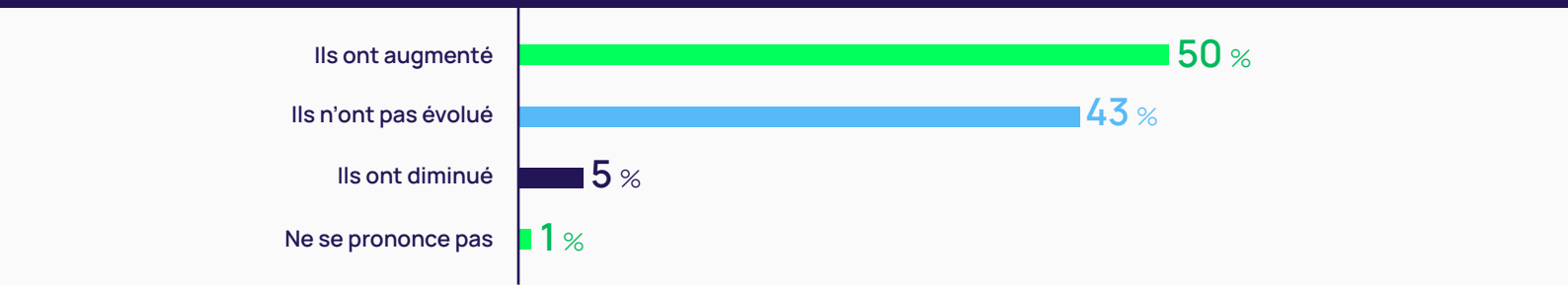
Votre posture de sécurité ne consiste pas à « mettre en place et oublier ». Votre risque évolue constamment à mesure que votre environnement informatique devient plus complexe et que des personnes rejoignent votre organisation, changent de poste et vous quittent. En réalité, les entreprises ne respectent pas toujours les politiques qu'elles présentent fièrement aux compagnies d'assurance lors de leur demande.

Principale conclusion 3

Bien que les coûts globaux de la cyber assurance augmentent, les nouvelles technologies comme l'IA réduisent les primes.

Les coûts d'assurance continuent d'augmenter pour de nombreuses organisations.

Figure 8 | Comment vos coûts de cyber assurance ont-ils évolué, le cas échéant, depuis votre souscription initiale ou votre dernier renouvellement ?



Bien que plus de la moitié des répondants signalent une augmentation, une comparaison d'une année sur l'autre montre que cette augmentation ralentit. L'année dernière, 79 % des entreprises ont déclaré que les coûts d'assurance ont augmenté depuis leur dernière demande ou renouvellement.

Pourquoi cette hausse pour certaines entreprises ?

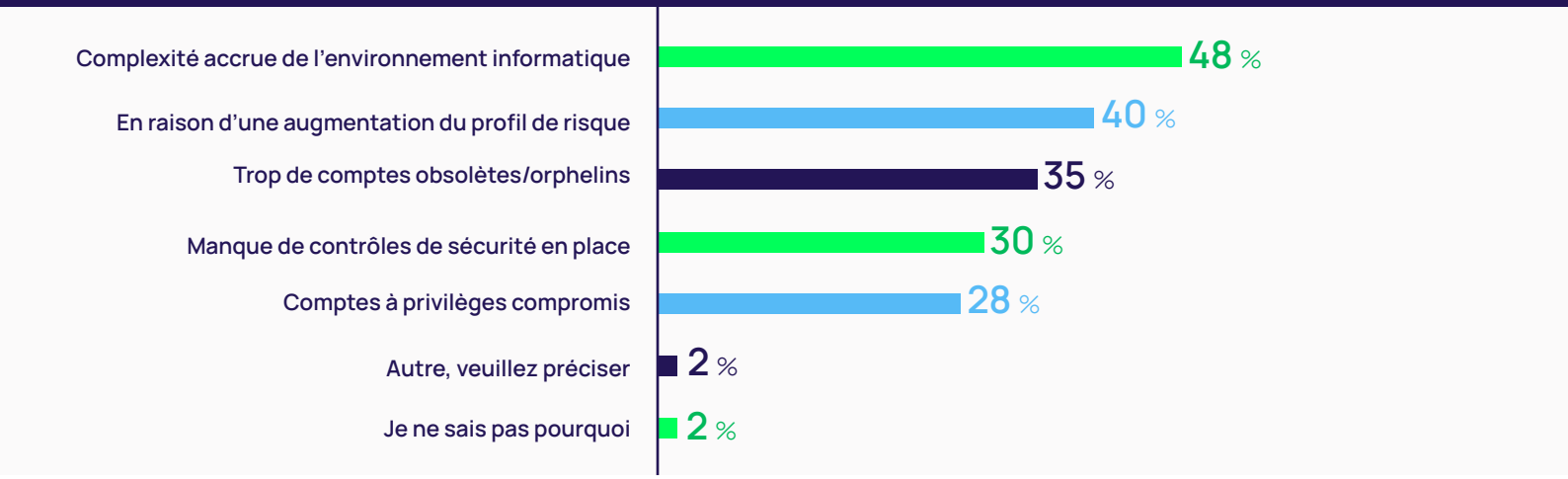
Prenez en compte le coût total des ressources nécessaires pour effectuer les évaluations d'assurance, combler les lacunes et démontrer l'efficacité de la cybersécurité dans un environnement informatique hybride moderne.

Les personnes interrogées identifient la complexité informatique comme l'un des facteurs principaux de la hausse des coûts. À mesure que le nombre d'identités augmente, davantage de ressources sont nécessaires pour accomplir ces tâches. La complexité de l'environnement informatique rend les évaluations de sécurité de la cyber assurance plus difficiles à réaliser, avec des solutions d'audit et de reporting disjointes qui compliquent l'agrégation des détails et la mesure des risques.

L'augmentation des coûts pourrait signifier que les assurés demandent des limites de couverture plus élevées en raison d'un profil de risque accru. Ils reconnaissent l'impact business qu'ils devront assumer en cas de cyber attaque et cherchent à transférer ce risque.

En fonction de la complexité informatique et du profil de risque, les compagnies d'assurance peuvent augmenter les prix pour tous les assurés afin de garantir une liquidité suffisante au cas où plusieurs sinistres surviendraient simultanément.

Figure 9 | Pourquoi les coûts ont-ils augmenté ?



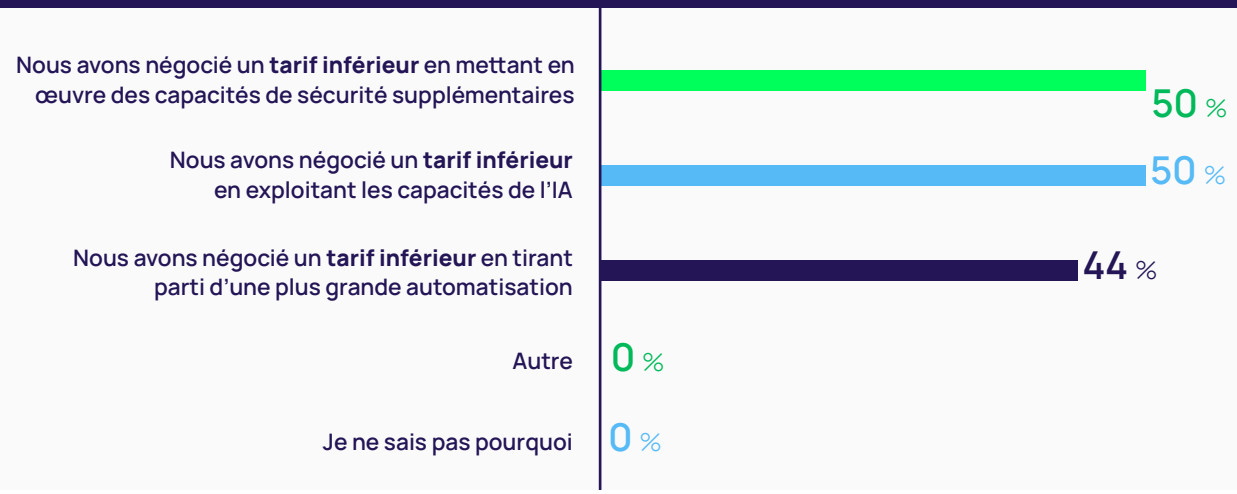
Les solutions de cybersécurité qui évaluent rapidement et de manière exhaustive un environnement informatique complexe et fournissent des rapports basés sur les risques que vous pouvez partager avec les assureurs sont des moyens efficaces de réduire vos coûts de cyber assurance.

L'IA et les contrôles de sécurité ont aidé les entreprises tournées vers l'avenir à réduire leurs tarifs d'assurance.

Tout le monde n'obtient pas le même tarif d'assurance. Votre tarif est déterminé en fonction du risque que la compagnie d'assurance considère comme le vôtre - votre profil de risque. Dans le cas d'une cyber assurance, votre risque est influencé par des facteurs tels que votre pile technologique, vos contrôles de sécurité et votre historique. Si vous êtes en mesure de démontrer une bonne visibilité et des contrôles efficaces réduisant votre niveau de risque, vous pourriez potentiellement obtenir des tarifs plus avantageux et, par conséquent, diminuer vos coûts.

Les résultats de l'enquête montrent que les entreprises avant-gardistes profitent des avantages de l'IA pour négocier des tarifs plus bas et, par conséquent, des coûts plus bas. Toutefois, la majorité d'entre elles doivent encore se concentrer sur l'adoption et la mise en œuvre des fondements d'une solide sécurité de l'identité.

Figure 10 | Pourquoi vos coûts d'assurance ont-ils diminué ?

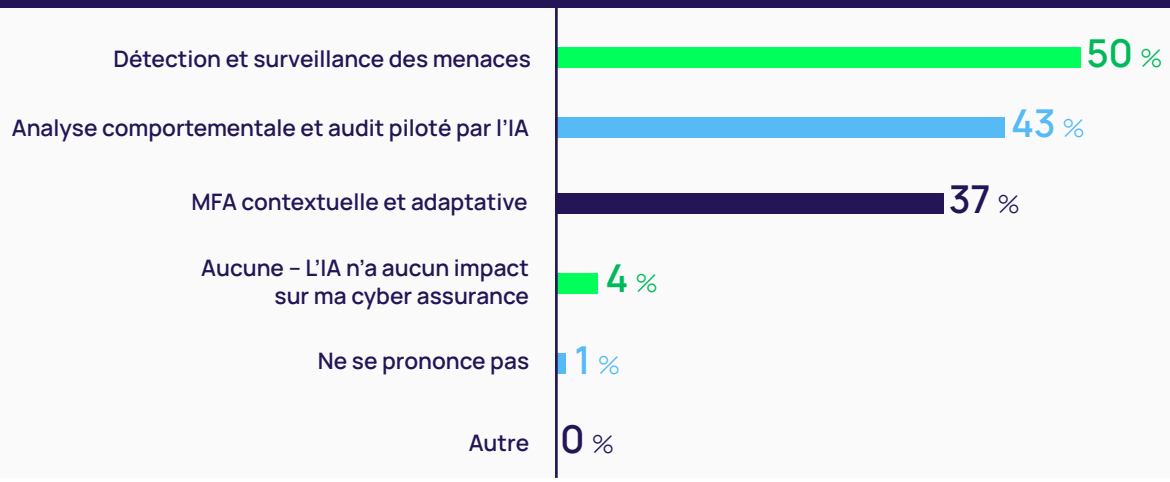


L'intelligence artificielle, notamment pour la détection et la surveillance des menaces, est efficace pour réduire les primes de cyber assurance

Les primes, c'est-à-dire le montant qu'une entreprise paie pour maintenir une police d'assurance active, sont déterminées par plusieurs facteurs, tels que le type d'assurance souscrit, les limites de la police et le montant de la franchise. Plus vous avez confiance en votre posture et vos contrôles de sécurité, mieux vous pourrez sélectionner l'assurance qui vous convient et négocier des primes plus basses.

Les entreprises adoptent l'intelligence artificielle (IA) pour s'assurer que leurs solutions et politiques de cybersécurité fonctionnent efficacement, et pour contenir les incidents en cours. Cela permet de réduire le temps de présence des agents malveillants et le périmètre des attaques, contribuant ainsi à diminuer leur profil de risque.

Figure 11 | Quelles capacités d'IA, le cas échéant, adoptez-vous pour réduire vos primes de cyber assurance ?



Conclusion

Pratiquement l'ensemble des entreprises américaines interrogées ont dû investir dans des solutions de sécurité de l'identité avant de souscrire une police d'assurance

Si l'assurance est un outil essentiel pour la cyberrésilience, vous ne pourrez jamais transférer tous vos risques. La cyber assurance doit fonctionner de concert avec des contrôles et des processus de cybersécurité robustes, raisonnables et défendables.

En particulier, les compagnies d'assurance s'attendent à voir des politiques de sécurité de l'identité et des solutions efficaces avant d'accorder une police. Vous devrez fournir des preuves de l'application des contrôles de sécurité de l'identité et veiller à les maintenir au fur et à mesure que votre surface d'attaque évolue et que votre profil de risque s'accroît.

L'IA aide les organisations à capitaliser sur l'expertise des spécialistes et agit comme un « assistant SOC » pour identifier plus rapidement les menaces liées à l'identité, réduisant ainsi le temps de réponse, limitant l'étendue des attaques et diminuant les risques. D'après les résultats de cette enquête, l'IA est sur le point d'offrir des avantages encore plus importants aux entreprises qui négocient leurs polices avec les compagnies d'assurance.

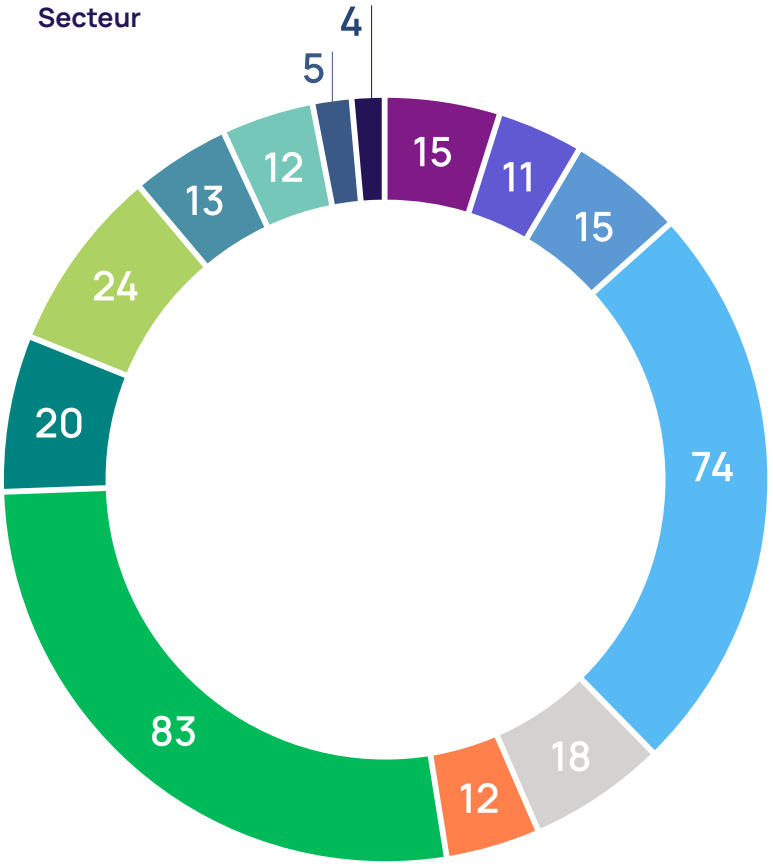
Dans le cadre de leurs évaluations des risques, les souscripteurs voudront savoir comment vous intégrez l'IA dans vos efforts de transformation numérique, y compris le développement de produits, le codage, le développement, les tests d'assurance qualité, etc. Vous devez également vous attendre à des questions qui examinent la manière dont votre équipe de sécurité utilise l'IA pour des éléments tels que la gestion des identités, l'autorisation, la détection et la réponse. Tous les contrôles basés sur l'IA doivent être facilement explicables afin que votre équipe, les auditeurs et les assureurs puissent comprendre comment ils fonctionnent pour réduire les risques.

Méthodologie

Cette enquête en ligne a été menée pour le compte de Delinea par Censuswide, qui, en juin 2024, a interrogé 306 dirigeants ayant une visibilité sur le processus de demande ou de renouvellement de cyber assurance de leur organisation. La même série de questions a été présentée à tous les répondants et les choix de réponses ont été aléatoires. Les résultats n'ont pas été pondérés.

Répartition des 306 répondants par nombre

Secteur

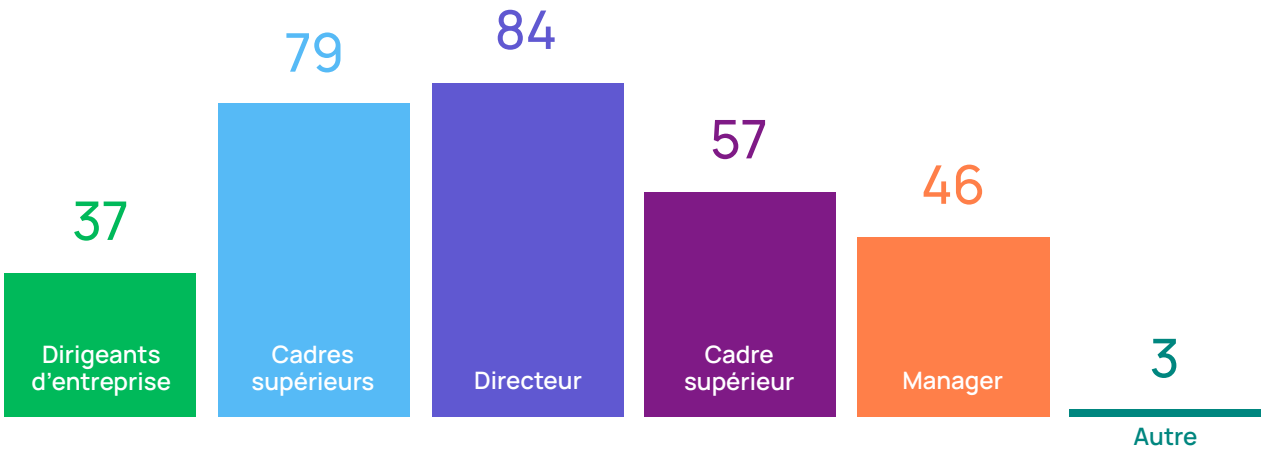


- Architecture, ingénierie et bâtiment
- Arts et culture
- Enseignement
- Finance
- Santé
- RH
- IT et télécoms
- Service juridique
- Conditionnement et services publics
- Commerce de détail, restauration et loisirs
- Ventes, médias et commercialisation
- Voyage et transports
- Autre

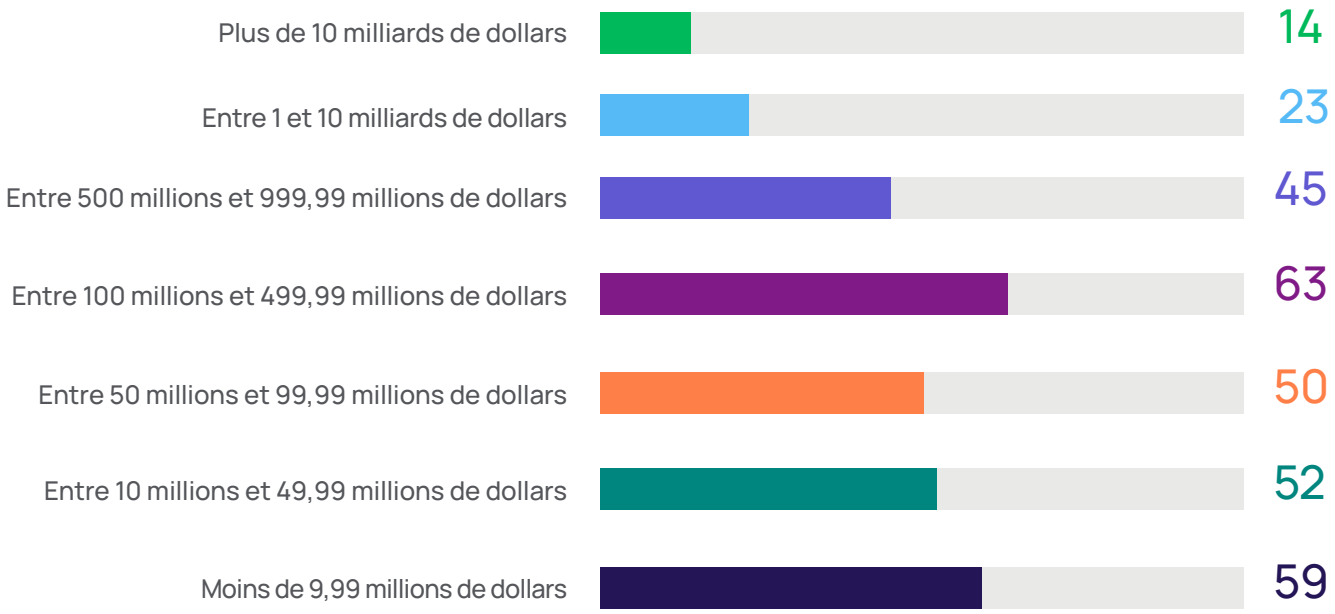
Rôles

Service financier | Juridique | IT | Sécurité/Risque | Conformité

Titres



Taille de l'entreprise



Ressources connexes

WEBINAIRE

The Future of Cyber Insurance: Navigating the Impact of AI on Policy Holders

Consultez des experts en cybersécurité et en assurance pour évaluer le langage des polices d'assurance, afin de bien comprendre votre couverture, les exclusions, et la manière dont votre compagnie vous assistera en cas d'incident.

Voir maintenant (EN)

LIVRE BLANC

Analyse des conditions renforcées en matière de cyber assurance

Ce rapport regroupe les questionnaires des principales compagnies d'assurance et met en évidence les questions courantes. Plus précisément, il examine les exigences de plus en plus strictes des assureurs en matière de sécurité de l'identité, notamment l'authentification multi-facteurs (MFA), la gestion des mots de passe, le contrôle d'accès, l'élévation des privilèges, la gestion des sessions, le moindre privilège et les politiques du Zero Trust.

Télécharger maintenant

PODCAST

Cyber Insurance Trends for Risk Management with Joe Carson of Delinea and Dara Gibson of Optiv

Apprenez à discuter de cyber assurance avec votre conseil d'administration.

Découvrir maintenant (EN)

Delinea

Securing identities at every interaction

Delinea est un pionnier de la sécurisation des identités en proposant une autorisation centralisée qui permet de rendre les organisations plus sûres et de régir de manière intuitive leurs interactions au sein de l'entreprise moderne. Delinea permet aux entreprises d'établir le contexte et l'intelligence tout au long du cycle de vie de l'identité à travers l'infrastructure cloud et traditionnelle, les données et les applications SaaS afin d'éliminer les menaces liées à l'identité. Avec l'autorisation intelligente, Delinea fournit la seule plateforme qui vous permet de découvrir toutes les identités, d'attribuer les niveaux d'accès appropriés, de détecter les irrégularités et de répondre immédiatement aux menaces liées à l'identité en temps réel. Delinea accélère l'adoption par vos équipes en déployant les solutions en quelques semaines, et non en quelques mois, et les rend plus productives en nécessitant 90% de ressources en moins à gérer que le concurrent le plus direct. Avec un temps de fonctionnement garanti de 99,99%, Delinea Platform est la solution de sécurité de l'identité la plus fiable du marché. Pour en savoir plus sur Delinea, consultez nos pages **delinea.com/fr/**, **LinkedIn**, **X** et **YouTube**.