SOPHOS

Guide Sophos de la cyberassurance

Comment de solides contrôles informatiques peuvent améliorer l'assurabilité et réduire les primes.

Le marché de la cyberassurance ne cesse d'évoluer et les conditions de souscription restent difficiles en raison de l'augmentation du nombre de demandes d'indemnisation et des coûts associés au cours des dernières années. Si la plupart des entreprises disposent déjà d'une cyberassurance, nombre d'entre elles constatent que le niveau de cybersécurité requis pour obtenir une couverture est désormais plus élevé, que les polices sont plus complexes et que les primes ne cessent d'augmenter.

Les assureurs proposent des contrats couvrant les cyber-risques, mais ils se montrent très sélectifs quant aux personnes qu'ils assurent et évitent généralement les demandeurs présentant un risque élevé. En investissant dans des systèmes de cyber-défense robustes, les organisations peuvent réduire leur cyber-risque, et donc améliorer leur assurabilité. En facilitant l'accès à la couverture, en réduisant les primes et en permettant des limites plus élevées, ces mesures de cyberdéfense offrent donc de multiples avantages en matière d'assurance.

Ce guide donne un aperçu de l'état du marché de la cyberassurance et illustre comment la cybersécurité favorise l'accès aux contrats de cyberassurance. Il détaille également les technologies et les services Sophos qui peuvent vous aider à réduire vos cyber-risques et à optimiser votre assurabilité.

Un livre blanc Sophos. Décembre 2023

Éléments fondamentaux

Pourquoi souscrire une cyberassurance

La cyberassurance, également connue sous le nom d'assurance cyber risques ou d'assurance responsabilité civile cybernétique, vous protège contre les conséquences de la cybercriminalité (mais pas contre le crime lui-même). D'une manière générale, la souscription d'une cyberassurance présente quatre avantages principaux :

1. **Gain financier.** L'assurance couvre les coûts liés à un cyberincident.
2. **Gain d'activités.** Pour de nombreuses organisations, une couverture de cyberassurance est de plus en plus souvent une condition préalable à toute activité commerciale.
3. **Gain opérationnel.** En cas d'incident, l'assureur offre un accès immédiat à des experts, notamment des spécialistes en investigations numériques, des avocats spécialisés dans la protection de la vie privée et des chargés de relations publiques.
4. **Tranquillité d'esprit.** En souscrivant une cyberassurance, vous donnez à vos clients, partenaires, fournisseurs et employés l'assurance que vous êtes préparé et couvert en cas de cyberincident.

Principales causes aboutissant à une demande d'indemnisation

Si un grand nombre d'incidents peuvent donner lieu à des demandes d'indemnisations, les causes les plus fréquentes, selon le rapport « Cyber Claims Study 2023 » de NetDiligence sont les suivantes :

1. Un ransomware
2. La compromission de la messagerie professionnelle (Business Email Compromise)
3. Un piratage
4. Un vol de fonds
5. Une erreur humaine[1]

1 Rapport « Cyber Claims Study 2023 » de NetDiligence

Que couvre la cyberassurance

La cyberassurance couvre les frais encourus suite à une cyberattaque. Bien que chaque police d'assurance varie, elle couvre généralement :

- Coûts liés à l'interruption des activités
- Investigations pour identifier la source de l'attaque
- Rançon et spécialistes pour gérer la négociation
- Coûts pour récupérer l'accès ou restaurer vos données à partir de sauvegardes ou d'autres sources
- Frais juridiques
- Services de relations publiques
- Notification des clients ou des organismes de réglementation
- Services de surveillance du crédit pour les personnes affectées

Lorsque vous comparez différentes offres d'assurance et leurs coûts, il convient de noter que les coûts liés à l'interruption des activités (comme la perte de revenus ou les coûts de travail supplémentaires) sont inclus dans certaines polices, mais pas dans d'autres.

En cas de cyber incident, l'assureur intervient et met à disposition des experts pour aider à gérer la situation. Dans le cas d'une attaque par ransomware, il va généralement :

- Nommer un consultant pour vous conseiller sur le traitement et la négociation de la demande de rançon.
- Identifier le moyen le plus économique de restaurer les données (paiement de la rançon, sauvegardes, etc.).
- Faire appel aux experts nécessaires pour traiter le problème.

Couverture de l'assuré et de tiers

De nombreuses polices couvrent les dommages subis par l'assuré (first party) et ceux relevant de la responsabilité civile de l'assuré (third party). La couverture des dommages subis par l'assuré (first party) correspond aux coûts directs associés à la réponse à l'attaque. Cela inclut par exemple les frais juridiques, les frais d'expertise judiciaire, les frais de notification aux clients, les frais de relations publiques, etc. La couverture des tiers (third party) au titre de la responsabilité civile correspond principalement aux coûts associés aux poursuites judiciaires.

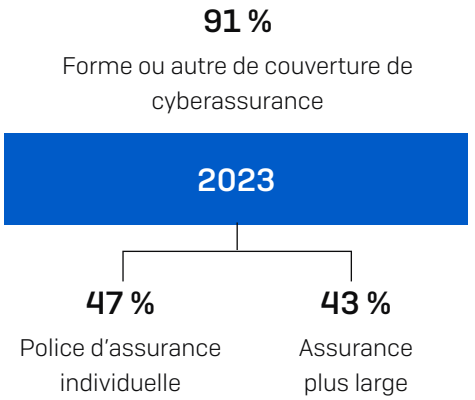
Dans une police d'assurance, il peut y avoir des sous-limites spécifiques à la couverture de l'assuré, et même pour des éléments spécifiques de cette couverture. Par exemple, la couverture de l'assuré peut être limitée à 500 000 €, qui inclut une limite de 50 000 € pour les frais de relations publiques.

La réalité des cyberassurances

La prévalence des cyberassurances

Disposer d'une cyberassurance est devenue la norme : 91 %[2] des organisations étaient couvertes par une forme ou une autre de cyberassurance en 2023, selon une enquête indépendante commandée par Sophos — une augmentation notable par rapport aux 84 % signalés en 2020[3], et en phase avec le chiffre de 92 % en 2022. Parmi les organisations qui ont déclaré être couvertes en 2023, 47 % avaient conclu des contrats de cyberassurances spécifiques, tandis que 43 % englobaient la cybercouverture dans des polices d'assurance commerciale plus larges.

Toutefois, ces chiffres ne donnent pas toute la mesure de la situation. Chaque police est différente et toutes ne couvrent pas les ransomwares, qui sont la principale cause de demande d'indemnisation au titre de la cyberassurance. Près d'une organisation sur dix ayant une couverture cyber en 2022 n'était pas assurée contre les ransomwares, et prenait donc le risque de devoir faire face aux lourdes conséquences, notamment financières, liées à ce type d'attaque.



2 Le rôle critique des cyber-défenses de première ligne lors du recours à la cyberassurance, Sophos.
3 L'état des ransomwares 2021, Sophos

Recours à la cyberassurance par secteur

Au niveau des différents secteurs, l'enquête a révélé que celui de l'enseignement (primaire, secondaire et supérieur) affichait le niveau global de couverture le plus élevé en matière de cyberassurance (96 %), avec une tendance à privilégier une cyberassurance dans le cadre d'une police plus large plutôt qu'une police individuelle.

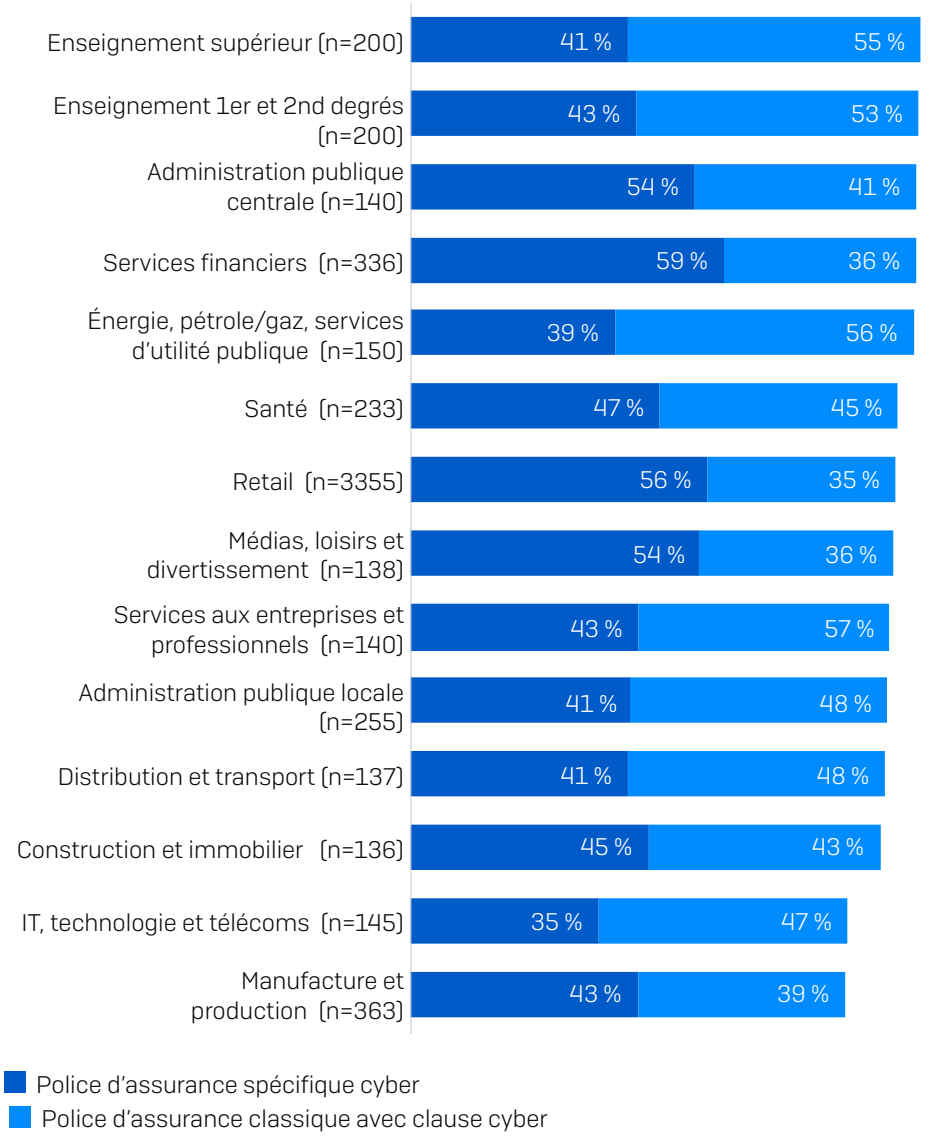
Ce niveau élevé de couverture est compréhensible sachant que ce secteur a signalé le taux le plus élevé d'attaques par ransomware dans notre étude sur l'état des ransomwares 2023 (80 % des établissements d'enseignement supérieur et 79 % des établissements d'enseignement secondaire et primaire ont déclaré avoir été touchés par des ransomwares au cours de l'année précédente). Selon l'enquête, le secteur des services financiers est le plus enclin à se doter d'une cyber-police individuelle (59 %), suivi de près par le secteur du retail (56 %).

Recours à la cyberassurance en fonction du chiffre d'affaires

Sans surprise, le recours à la cyberassurance augmente avec le chiffre d'affaires. 96 % des entreprises avec un chiffre d'affaires annuel supérieur à 5 milliards de dollars disposent déjà d'un type de cyber-couverture, contre 79 % pour celles qui ont un chiffre d'affaires inférieur à 50 millions de dollars.

Les entreprises avec des chiffres d'affaires plus élevés ont également une plus grande propension à être dotée d'une cyber-police individuelle que celles ayant des chiffres d'affaires plus bas : 58 % des entreprises déclarant un chiffre d'affaires annuel supérieur à 5 milliards de dollars ont une police individuelle, contre 34 % pour celles ayant un chiffre d'affaires annuel inférieur à 10 millions de dollars. Dans l'ensemble, notre étude montre que le recours à des polices individuelles augmente de manière constante avec le chiffre d'affaires[4].

Recours à la cyberassurance par secteur, 2023



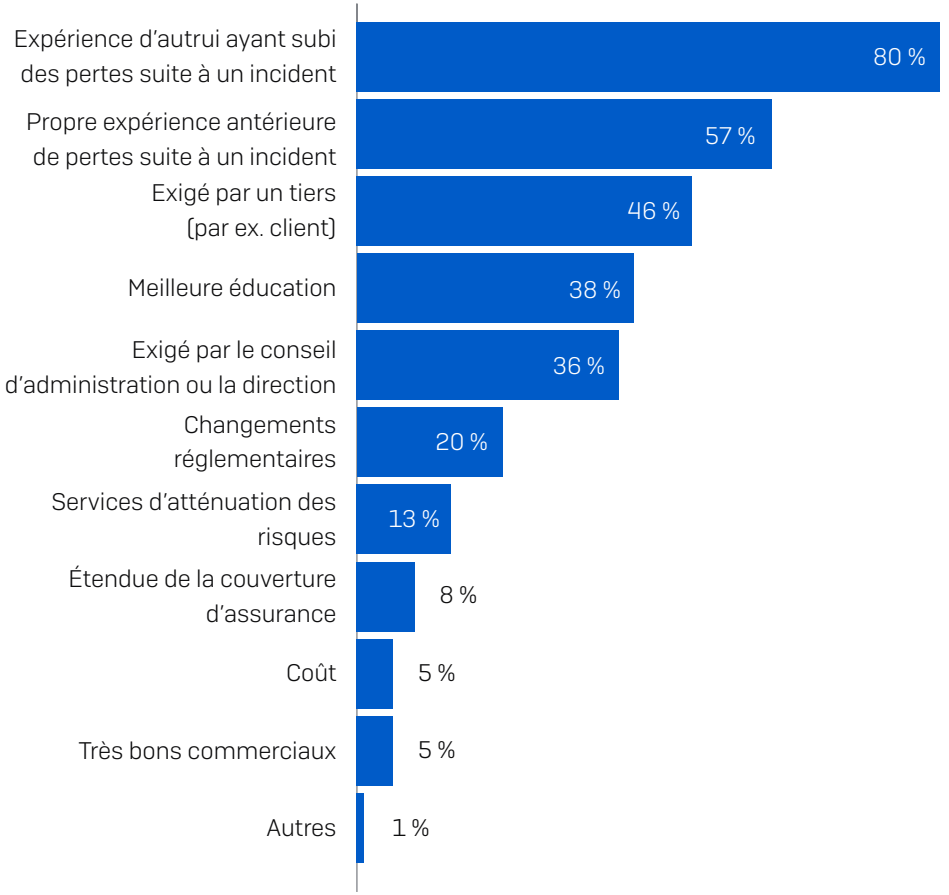
Votre entreprise dispose-t-elle d'une cyberassurance ? Oui, nous avons une police d'assurance spécifique cyber, Oui, nous avons une clause cyber dans notre police d'assurance habituelle (par exemple, une police de responsabilité civile générale). Chiffres de base dans le graphique.

4 Le rôle critique des cyber-défenses de première ligne lors du recours à la cyberassurance, Sophos.

Les cyberattaques sont le moteur de la cyberassurance

Une enquête du cabinet Advisen and PartnerRe auprès de courtiers et de souscripteurs de cyberassurance du monde entier nous permet de mieux comprendre les principaux facteurs de création ou d'augmentation de ventes de cyberassurances. Les deux premiers facteurs poussant les entreprises à souscrire une cyberassurance sont le fait d'apprendre que d'autres entreprises ont subi des pertes à cause d'un cyberincident et le fait d'en être soi-même victime. En troisième position, on retrouve le fait que ce soit « exigé par un tiers ». Face à l'augmentation des attaques de la supply chain, il est de plus en plus souvent demandé aux entreprises de souscrire une cyberassurance avant de conclure un contrat, afin de couvrir le client s'il subit un cyberincident dans le cadre de ce partenariat.

Plus d'une personne sur trois (36 %[5]) cite la demande du conseil d'administration ou de la direction comme l'un des principaux moteurs de l'achat d'une cyberassurance. Cette forte demande de la part des équipes de direction reflète les répercussions que peut avoir un cyberincident majeur sur l'ensemble de l'entreprise. Se protéger contre les conséquences d'une cyberattaque est désormais un problème d'intérêt général, et non plus seulement un problème limité au service informatique.



Cyberassurance : The Market's View – Advisen, PartnerRe

5 Cyberassurance : The Market's View, PartnerRe et Advisen

Le coût des cyberassurances

Comme pour toutes les autres formes d'assurance, le coût dépend de plusieurs facteurs, notamment :

- **Profil démographique :** taille, industrie, secteur, localisation, chiffre d'affaires, etc.
- **Exposition potentielle :** type et volume de données sensibles stockées/collectées/traitées
- **Niveau de cybersécurité :** les défenses de sécurité utilisées par l'entreprise
- **Historique :** les demandes d'indemnisation antérieures entraînent invariablement une hausse des primes
- **Conditions de la police :** couverture/limite de responsabilité, etc.

Il est important de connaitre la distinction entre une police avec franchise et une police avec découvert obligatoire. Dans le cas d'une police avec franchise, la franchise est incluse dans le montant de la garantie. À l'inverse, dans le cas d'une police avec découvert obligatoire, le montant du découvert s'ajoute au plafond de l'assurance.

FRANCHISE	DÉCOUVERT OBLIGATOIRE
Plafond de 100 000 €, Franchise de 10 000 €	Plafond de 100 000 €, Découvert obligatoire de 10 000 €
Vous payez la première tranche de 10 000 €, l'assureur paie 90 000 €.	Vous payez la première tranche de 10 000 €, l'assureur paie 100 000 €.
Couverture totale 100 000 €	**Couverture totale 100 000 €**

Cumul d'assurances

En ce qui concerne les PME, il n'est pas rare qu'elles n'utilisent qu'un seul assureur pour tous leurs besoins en cyberassurance. Quant aux grandes entreprises, il est commun qu'elles cumulent plusieurs assurances, car un seul assureur ne peut pas absorber tous les risques. Les courtiers en assurances construisent de véritables remparts pour des clients individuels, réunissant deux, trois, quatre assureurs ou plus. Le premier assureur absorbe les risques primaires et le reste des assureurs couvre les risques excédentaires.

Comité des approbations

Les organismes de cyberassurance ont souvent des fournisseurs préalablement approuvés, appelés « comité », avec lesquels ils travaillent en cas d'incident. Si l'entreprise victime de l'incident n'a aucune relation existante avec un fournisseur, le cyberassureur l'encouragera, voire exigera, qu'elle travaille avec l'un de ces fournisseurs.

Cela dit, la plupart des assureurs sont également disposés à travailler avec d'autres fournisseurs de bonne réputation, surtout s'il existe une relation préexistante ou des conditions contractuelles. Il s'agira alors d'une approbation « hors comité ». Naturellement, il y a de nombreux avantages financiers et opérationnels à travailler avec un fournisseur qui connaît déjà l'entreprise victime de l'incident et qui est familier avec sa configuration informatique et commerciale.

Si le fournisseur de votre choix ne fait pas partie du comité de votre assureur, vous pouvez tout de même demander à l'utiliser. Il est essentiel de communiquer rapidement avec votre assureur afin que l'équipe de cyberassurance de votre fournisseur de choix puisse s'engager auprès de l'assureur pour obtenir les approbations nécessaires.

Besoins en matière de couverture d'assurance

Lors de la sélection d'une police d'assurance cybersécurité, il est important de choisir le niveau de couverture approprié pour votre entreprise. Vous devez être en mesure de vous rétablir et de maintenir votre entreprise à flot en cas de cyberattaque, tout en maintenant vos primes à un niveau abordable.

Les coûts pour se rétablir après une cyberattaque sont considérables et ne cessent d'augmenter. En 2023, le coût moyen pour remédier à l'impact d'une attaque de ransomware était de 1,82 million de dollars[6], contre 0,76 million de dollars en 2020. Fait intéressant, il s'agit d'une baisse modeste mais positive par rapport aux 1,85 million de dollars de 2021, reflétant probablement le fait qu'avec la multiplication des cas de ransomwares, le préjudice de réputation lié à une attaque a perdu de son importance. Parallèlement, les assureurs sont mieux à même de guider les victimes rapidement et efficacement dans le processus de réponse à l'incident, réduisant les coûts de remédiation.

6 L'état des ransomwares 2023, Sophos

Le marché de la cyberassurance

Les conditions requises pour obtenir une cyberassurance se sont durcies

La cyberassurance était jusqu'à présent un marché « mou », caractérisé par une capacité élevée et des primes faibles. Mais ce marché s'est durci en 2021. Pour la première fois en plus de 15 ans d'existence en tant qu'assurance à part entière, les assureurs voient leur volume d'indemnisation augmenter plus rapidement que leurs revenus des primes : le taux de sinistre du secteur est en hausse régulière depuis 2018 et atteignait 72,8 % en 2020[7]. (Le taux de sinistre correspond au coût de l'assurance divisé par le total des primes reçues. Par exemple, si une entreprise paie 80 € de sinistres pour chaque 160 € de primes perçues, le rapport sinistres-primes sera de 50 %).

Plusieurs facteurs ont contribué à ce durcissement du marché :

- Les cyberattaques ont augmenté à la fois en volume et en complexité —
  - 57 % des responsables informatiques reconnaissent une augmentation du volume des cyberattaques[8]
  - 59 % ont constaté une augmentation de la complexité des cyberattaques[9]
- Comme nous l'avons mentionné, les coûts de rétablissement après une attaque de ransomware ont beaucoup augmenté, avec une moyenne considérable de 1,82 million de dollars en 2023.

L'une des conséquences de ce durcissement du marché est qu'il est désormais beaucoup plus difficile de souscrire à une couverture de cyberassurance. Cette situation a été confirmée par notre enquête menée auprès de 5 600 professionnels de l'informatique début 2022 : 94 % de ceux dotés d'une cyberassurance ont déclaré que le processus d'obtention avait évolué au cours des douze derniers mois :

- 54 % ont déclaré que le niveau de cybersécurité dont elles avaient besoin pour être éligibles était désormais plus élevé.
- 47 % ont déclaré que les politiques étaient désormais plus complexes.
- 40 % ont déclaré que le nombre de compagnies proposant des cyberassurances était en baisse.
- 37 % ont déclaré que le processus prenait plus de temps.
- 34 % ont déclaré que la cyberassurance était plus coûteuse[10].

« Le coût de notre cyberassurance est en hausse et nous devons franchir plus d'obstacles que jamais auparavant. »

Agence de voyages d'affaires

Ce durcissement du marché a suscité des difficultés particulières pour les entités publiques qui sont souvent considérées comme des cibles faciles pour les cybercriminels en raison de leurs défenses plus faibles. Par conséquent, les organismes publics qui voulaient obtenir ou renouveler une couverture ont dû faire face à un nombre réduit de fournisseurs et à des conditions plus difficiles, les prix ayant parfois doublé d'une année sur l'autre.

« Là où [les assureurs] offraient un plafond de 10 millions de dollars, il est maintenant de 5 millions de dollars. »

Jack Kudale, CEO, Cowbell Cyber Inc.

Le deuxième semestre 2023 a été marqué par un certain relâchement du marché de la cyberassurance. Les capacités ont augmenté avec l'arrivée de nouveaux acteurs, mais les assureurs restent très sélectifs quant aux entreprises qu'ils prennent en charge : si les organisations à faible risque profitent d'offres d'assurance améliorées, les entreprises à haut risque continuent de peiner à décrocher une couverture.

Les cyberassurances indemnisent

La bonne nouvelle pour les détenteurs d'un contrat est que les cyberassurances sont toujours efficaces en cas de cyberattaque. Dans l'enquête 'L'état des ransomwares 2022' de Sophos, 98 % des personnes interrogées assurées contre les ransomwares et touchées par un ransomware ont déclaré que leur assureur avait couvert les coûts inhérents à l'attaque. Dans près de trois quarts (73 %) des incidents, l'assureur a pris en charge les frais de nettoyage pour permettre à l'entreprise de reprendre ses activités. Dans 36 % des cas, l'assurance a payé la rançon, et dans 33 % des cas, elle a payé d'autres coûts tels que ceux liés aux temps d'arrêt et aux opportunités perdues.

7 S&P Global, 1er juin 2021
8 L'état des ransomwares 2022, Sophos
9 L'état des ransomwares 2023, Sophos
10 Cyberassurance 2022 : La réalité des experts de l'infosec travaillant en première ligne, Sophos

La cyberassurance, un levier pour améliorer ses défenses

Face au durcissement du marché, la quasi-totalité des entreprises (97 %) ayant souscrit une cyberassurance a dû apporter des modifications à leurs défenses afin d'améliorer leur posture vis-à-vis des assureurs.

- 64 % ont mis en place de nouveaux services/technologies
- 56 % ont augmenté leurs activités de formation/sensibilisation du personnel
- 52 % ont modifié leurs processus/comportements[11].

Mais quelles modifications devriez-vous apporter ?
Comment faire pour améliorer votre posture vis-à-vis des assureurs ?

11 Cyberassurance 2022 : La réalité des experts de l'infosec travaillant en première ligne, Sophos

Une cybersécurité robuste pourra optimiser votre posture face aux assureurs

La cybersécurité et la cyberassurance sont directement liées : 95 % des organisations qui ont souscrit une assurance en 2023 ont déclaré que la qualité de leurs défenses avait une incidence directe sur leur posture vis-à-vis des assureurs[12]. Investir dans des défenses solides permet de bénéficier de multiples avantages en matière d'assurance :

1. Accès simplifié à la couverture

60 % des organisations ayant souscrit une cyberassurance ont déclaré que la qualité de leurs défenses avait une incidence sur leur capacité à obtenir une couverture[13]. Les fournisseurs se concentrent de plus en plus sur la gestion — et la réduction — des risques. Une cybersécurité solide réduit votre cyber risque, ce qui, en retour, fait de vous un candidat plus attrayant pour les fournisseurs de cyberassurance. Bien que les conditions spécifiques de chaque assureur varient, plusieurs contrôles de sécurité sont couramment requis sur le marché :

Authentification multifacteur

L'authentification multifacteur (MFA) est exigée pour l'obtention d'une couverture, les assureurs cherchant à combler les lacunes de sécurité courantes avant d'absorber le risque.

« Le renouvellement de notre cyberassurance est conditionné par l'activation de la MFA pour l'accès à distance. »

Fournisseur de services et d'assistance IT, États-Unis

« Si nous ne nous dotons pas de la MFA d'ici un an, nous allons perdre notre cyberassurance. »

Prestataire de soins de santé, États-Unis

12 Le rôle critique des cyber-défenses de première ligne lors du recours à la cyberassurance, Sophos.
13 Le rôle critique des cyber-défenses de première ligne lors du recours à la cyberassurance, Sophos.

EDR (Endpoint Detection and Response) ou XDR (Extended Detection and Response)

Une protection Endpoint avancée, capable de bloquer automatiquement les menaces, constitue le socle d'une cyberdéfense robuste. Toutefois, comme les cybercriminels ne cessent de faire évoluer leurs méthodes d'attaque en exploitant des outils informatiques légitimes, des identifiants compromis et des vulnérabilités non corrigées, la protection Endpoint n'est désormais plus suffisante à elle seule. Pour stopper les ransomwares avancés et les violations de sécurité (et les demandes d'indemnisation qui en découlent), il est essentiel de surveiller de manière proactive les activités suspectes, d'investiguer et de répondre avant que les acteurs malveillants ne soient en mesure de déployer leurs attaques.

Les technologies EDR et XDR sont des outils conçus pour aider les spécialistes à détecter et à investiguer les compromissions potentielles, et à neutraliser toute cyberattaque avancée avant qu'elle ne cause des dommages. Comme leurs noms l'indiquent, les outils EDR utilisent uniquement les données provenant de la protection Endpoint, tandis que les outils XDR utilisent les sources de données provenant des solutions Endpoint, ainsi que d'autres solutions de sécurité, comme les solutions de pare-feu, de messagerie, Cloud et mobile, afin de fournir une meilleure visibilité et d'accélérer la détection et la réponse. La technologie EDR est souvent une condition pré-requise par les assureurs. De fait, les entreprises qui n'en disposent pas ont généralement du mal à signer un contrat de cyberassurance.

Service MDR (Managed Detection and Response)

Un service MDR est un service entièrement managé 24 h/24 et 7 j/7, fourni par des experts spécialisés dans la détection et la réponse aux cyberattaques que les solutions technologiques ne peuvent à elles seules empêcher. Il offre le plus haut niveau de protection contre les cybermenaces, minimisant les risques et la probabilité de faire une demande d'indemnisation. Bien qu'il s'agisse rarement d'une condition indispensable à l'obtention d'une couverture, les organisations qui font appel à des services MDR sont souvent considérées comme des clients de « première classe » par les assureurs, car elles présentent le niveau de risque le plus faible.

« Le service juridique veut obtenir une assurance contre les ransomwares et [les services MDR] est l'étape dont nous avons besoin pour y parvenir. »

Fournisseur de technologies et de solutions IT, opérant à l'échelle mondiale

Plan de réponse aux incidents

La meilleure façon d'éviter qu'une cyberattaque ne se transforme en une véritable violation de sécurité est de se préparer à l'avance. Souvent, c'est après avoir été victime d'une fuite de données qu'une entreprise se rend compte qu'elle aurait pu éviter beaucoup de frais et de problèmes si elle avait mis en place un plan de réponse aux incidents. Un plan détaillé vous permettant de minimiser l'impact d'un incident réduira votre cyber-risque, ce qui vous rendra plus attrayant aux yeux des assureurs.

2. Réduire les cotisations

62 % des organisations ayant souscrit une cyberassurance ont déclaré que la qualité de leurs défenses avait une incidence sur le coût de leur couverture[14]. De même qu'être doté d'une alarme ou de bonnes serrures réduisent les cotisations de votre assurance habitation, disposer de bonnes cyberdéfenses permet de réduire les coûts de votre cyberassurance. Si les algorithmes de calcul des cotisations des assureurs sont un secret bien gardé, les clients affirment invariablement que la qualité de leur protection a un impact sur leurs cotisations.

« Parce que nous n'avions pas installé de technologie EDR sur 100 % de nos appliances, [le coût de] l'assurance a doublé. »

Société d'hébergement Web, États-Unis

« Grâce à Measured, les clients qui utilisent les produits Sophos MDR ou Sophos Endpoint peuvent économiser jusqu'à 25 % sur leur prime de cyberassurance. »

Measured Insurance, États-Unis

3. Réduire le risque de faire une réclamation

Comme pour d'autres types d'assurance, si vous avez fait une réclamation, vous risquez d'avoir du mal à renouveler votre police. Les entreprises qui ont sollicité des demandes d'indemnisation voient également leurs primes augmenter de manière significative les années suivantes. En minimisant votre risque d'être touché par une cyberattaque grâce à de robustes cyber défenses, vous réduisez la probabilité de devoir faire fonctionner votre police d'assurance, ce qui contribue à réduire les primes de votre contrat.

4. Réduire le risque de non-indemnisation

Une mauvaise hygiène en matière de sécurité informatique peut vous empêcher de recevoir une indemnisation après un incident. Si l'assureur estime que vous avez « laissé la porte ouverte » par des pratiques faibles, il peut avoir des raisons de ne pas payer. En éliminant ces lacunes, vous vous assurez que, si le pire se produit, la compagnie d'assurance interviendra.

« Nous ne payons pas pour les réclamations, pertes, violations, investigations sur la protection de la vie privée ou menaces dues à l'utilisation de logiciels ou de systèmes obsolètes ou non pris en charge. »

Termes de la police Hiscox Cyberclear™, Royaume-Uni, juin 2021.

5. Minimiser l'impact et le coût des éventuels incidents

Une réponse rapide et appropriée à une cyberattaque peut considérablement en réduire l'impact et le coût. Mettre en place un plan de réponse aux incidents de malwares et pouvoir faire appel à des experts en réponse aux incidents sont deux éléments qui vous aideront à minimiser les retombées d'une attaque.

14 Le rôle critique des cyber-défenses de première ligne lors du recours à la cyberassurance, Sophos.

Comment Sophos peut vous aider

Optimisez vos cyberdéfenses

Sophos permet aux entreprises de mettre en place la plupart des cybercontrôles de plus en plus exigés par les assureurs pour leur accorder une couverture d'assurance et leur permettre d'accéder aux meilleurs tarifs et conditions de police. Cette protection est rendue possible grâce aux renseignements sur les menaces et à l'expertise en cybersécurité de Sophos X-Ops.

Sophos Endpoint Detection and Response (EDR)

Sophos EDR associe l'approche robuste de prévention de Sophos Endpoint à de puissantes fonctionnalités de détection et de réponse qui permettent aux analystes de sécurité et aux administrateurs informatiques de chasser, d'investiguer et de répondre aux activités suspectes aussi bien sur les postes que sur les serveurs. Les détections sont analysées et priorisées par l'IA, pour vous aider à définir où consacrer votre temps et votre énergie. Les opérateurs ont la possibilité d'accéder à distance aux appareils afin d'investiguer les problèmes, d'installer et de désinstaller des logiciels, d'arrêter les processus actifs, d'exécuter des scripts ou des programmes, d'éditer des fichiers de configuration, etc.

Sophos Extended Detection and Response (XDR)

Plus les défenseurs pourront voir, plus vite ils pourront agir. Sophos XDR exploite la télémétrie de vos solutions de sécurité Sophos et non Sophos existantes pour vous permettre de détecter, d'investiguer et de répondre aux activités suspectes dans l'ensemble de votre environnement de sécurité.

- **Détection :** Les détections alimentées par l'IA offrent une visibilité instantanée des activités suspectes sur toutes les surfaces d'attaque clé, et notre fonctionnalité de recherche simple sans SQL vous permet de chasser très rapidement les menaces.
- **Investigation :** Les dossiers créés automatiquement et les détections priorisées permettent de se concentrer sur les aspects les plus importants. De plus, notre interface utilisateur conçue par des analystes vous fournit les informations et les outils dont vous avez besoin pour mener à bien vos investigations en toute simplicité.
- **Réponse :** Des outils complets de gestion des dossiers et des actions de réponse vous permettent de collaborer avec les membres de l'équipe et de neutraliser rapidement les attaques.

Sophos Managed Detection and Response (MDR)

Sophos MDR est le service MDR le plus fiable sur le marché, sécurisant plus de sociétés que tout autre fournisseur. Sophos MDR vous offre une protection ultime grâce à la détection, l'investigation et la réponse aux menaces 24/7, fournies par une équipe d'experts sous la forme d'un service entièrement managé. Avec un temps moyen de résolution des incidents de seulement 38 minutes, Sophos MDR minimise considérablement le risque d'un cyber incident majeur et optimise votre posture vis-à-vis des assureurs.

Réduire le risque de faire une réclamation

Sophos vous offre une protection de premier ordre contre les ransomwares, les piratages malveillants et autres menaces avancées. Nos solutions vous aident à minimiser le risque de subir un cyberincident majeur, réduisant ainsi la probabilité d'avoir à faire jouer votre assurance et contribuant à maintenir les primes à un niveau bas à l'avenir.

« Nous ne pouvons pas bloquer tout ce qui entre, c'est pourquoi nous comptons sur Sophos. »

Canucks de Vancouver, Canada

Validation de Sophos par les clients et les analystes

Les solutions Sophos sont largement reconnues par les clients, la communauté des analystes et les testeurs indépendants, notamment :

Sophos Managed Detection and Response (MDR)

- Nommé Gartner® Customers' Choice™ 2023 dans la catégorie Services MDR (Managed Detection and Response) avec une note client de 4,8/5 sur Gartner Peer Insights.
- Nommé Overall Leader pour la catégorie MDR (Managed Detection and Response) dans les rapports G2 Grid® Fall 2023.
- Considéré comme faisant partie des meilleures solutions (Top Performer) par 2022 MITRE Engenuity ATT&CK Evaluation dans la catégorie Managed Services.

Sophos Extended Detection and Response (XDR)

- Nommé Overall Leader pour la catégorie XDR dans les rapports G2 Grid® Fall 2023.
- Considéré comme faisant partie des meilleurs prestataires dans les évaluations MITRE Engenuity ATT&CK 2023 (Turla)
- Reconnu comme Overall Leader N° 1 dans Omdia Universe pour la catégorie Comprehensive Extended Detection and Response (XDR).

Sophos Endpoint Detection and Response (EDR)

- Nommé Leader par le Gartner® Magic Quadrant™ 2022 dans la catégorie Endpoint Protection Platforms pour la 13ème année consécutive.
- Nommé Gartner® Customers' Choice™ 2023 dans la catégorie Endpoint Protection Platforms pour la deuxième année consécutive, avec une note client de 4,8/5 sur Gartner Peer Insights.
- Nommé Overall Leader pour la catégorie Endpoint Protection Suites et EDR dans les rapports G2 Grid® Fall 2023 Meilleur prestataire dans les évaluations MITRE Engenuity ATT&CK de 2023 (Turla)
- Notes AAA et scores de protection totale de 100 % dans le rapport de SE Labs sur la sécurité Endpoint du troisième trimestre 2023, dans les catégories Entreprise et SMB.

Pour en savoir plus sur les solutions Sophos, cliquez ici

Sophos fournit des solutions de cybersécurité de pointe aux entreprises de toutes tailles, les protégeant en temps réel contre les menaces avancées telles que les malwares, les ransomwares et le phishing. Grâce à des fonctionnalités Next-Gen éprouvées, les données de votre entreprise sont sécurisées efficacement par des produits alimentés par l'intelligence artificielle et le Machine Learning.

2023-12-06 (WP-NP)

SOPHOS