Cyber-assurance 2026 : guide choix de police et éligibilité PME

Tout ce qu'une PME doit savoir sur la cyber-assurance en 2026 : couvertures, exclusions, critères d'éligibilité, comparatif assureurs et coûts indicatifs en...

En 2026, souscrire une cyberpolice n'est plus un luxe réservé aux grandes entreprises : c'est une nécessité stratégique pour toute PME qui manipule des données clients ou dépend de systèmes informatiques pour fonctionner. Le marché français de la cyber-assurance a dépassé 1,1 milliard d'euros de primes en 2025 selon l'AMRAE, porté par l'explosion des sinistres ransomware, la montée en puissance de NIS 2 et les exigences croissantes des donneurs d'ordres. Pourtant, beaucoup de dirigeants de TPE/PME restent perdus face à la complexité des polices, aux exclusions de plus en plus nombreuses et aux questionnaires de souscription techniques qui ressemblent à des audits de sécurité. Ce guide vous explique en termes clairs ce que couvre (et ne couvre plus) une police cyber en 2026, comment vous y préparer, quel budget prévoir selon la taille de votre entreprise, et quel lien existe entre conformité NIS 2 et obtention d'une prime compétitive.

À RETENIR

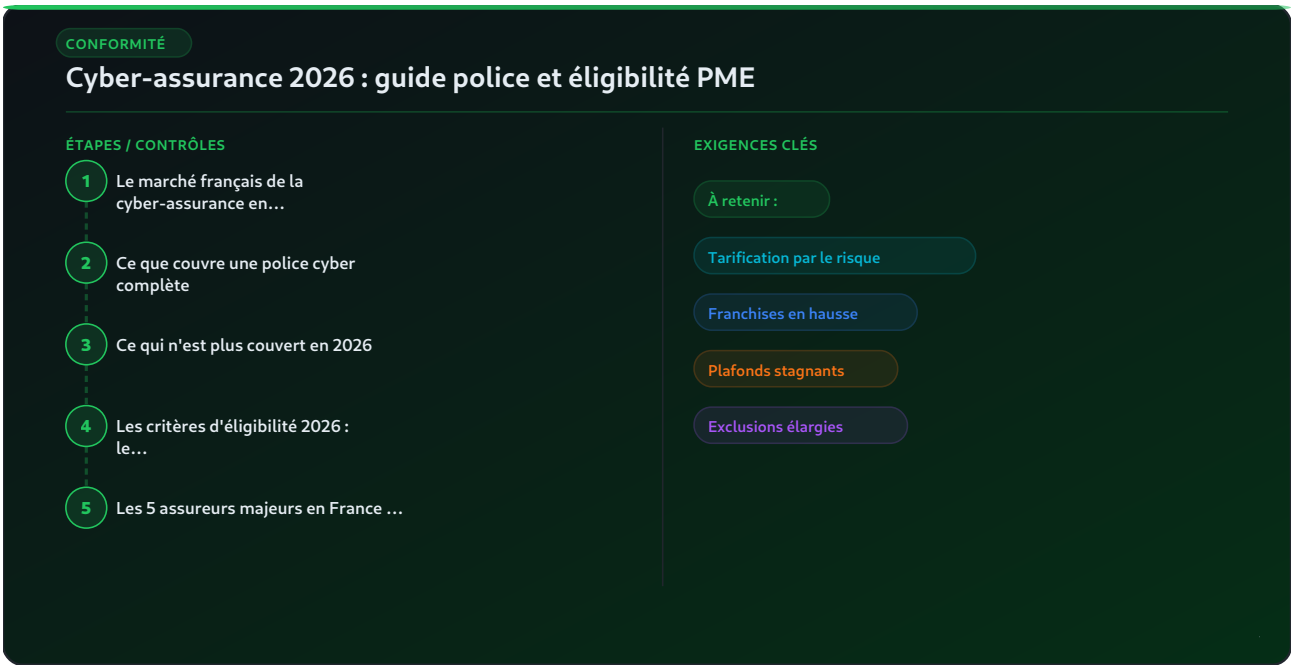
À retenir :

Le marché cyber-assurance France dépasse 1,1 Md€ de primes en 2025 ; les franchises augmentent et les exclusions se durcissent (guerre, État-nation, infrastructure obsolète).

Les 5 critères éliminatoires 2026 : MFA sur accès distants, EDR déployé, sauvegardes offline testées, patch management formalisé, formation phishing annuelle.

La conformité NIS 2 est devenue un argument de négociation pour obtenir une prime réduite de 10 à 25 % chez certains assureurs.

Une PME de 50 salariés peut s'attendre à payer 5 000 à 15 000 € par an selon son secteur et son niveau de maturité cyber.



Le marché français de la cyber-assurance en 2026

Le marché cyber-assurance en France est l'un des plus dynamiques d'Europe. L'AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise) recense une croissance de 18 % des primes entre 2023 et 2025, avec une sinistralité qui reste élevée : 1 entreprise sur 5 déclare au moins un incident cyber significatif chaque année. La réassurance reste tendue après les sinistres massifs liés aux ransomwares qui ont frappé collectivités, hôpitaux et ETI industrielles.

Les grandes tendances 2026 sur le marché :

Tarification par le risque : les questionnaires de souscription se sont sophistiqués — un assureur peut désormais interroger votre configuration réseau via un scan externe passif avant de vous proposer un devis.

Franchises en hausse : pour les PME industrielles et de santé, les franchises minimales sont passées de 5 000 à 20 000 € chez certains assureurs.

Plafonds stagnants : les plafonds de garantie n'ont pas suivi l'inflation des coûts de remédiation — un ransomware sévère peut coûter 200 000 à 500 000 € pour une PME, alors que les plafonds proposés débutent à 100 000 €.

Exclusions élargies : les exclusions liées aux conflits État-nation, aux sanctions OFAC et aux infrastructures non patchées se sont durcies post-NotPetya et post-conflit Ukraine.

Ce que couvre une police cyber complète

Une cyberpolice complète se décompose généralement en trois grandes familles de garanties.

> ⚡ **Retour terrain**
>
> Dans mes missions de conformité, j'observe que les entreprises sous-estiment systématiquement le délai de mise en œuvre des mesures techniques. Les mesures organisationnelles (politiques, procédures) s'écrivent en semaines ; les mesures techniques (segmentation réseau, chiffrement, MFA) se déploient en mois. Pour un plan de mise en conformité réaliste, je multiplie toujours les estimations initiales des équipes IT par 2,5 — et je n'ai jamais eu à réduire ce coefficient.

Couvertures « first party » (dommages propres)

Business Interruption (BI) : perte d'exploitation liée à l'indisponibilité des systèmes — souvent la garantie la plus coûteuse en sinistre. Vérifiez le délai de carence (souvent 8 à 12 heures) et la période d'indemnisation maximale.

Frais de remédiation : forensique numérique, reconstruction des systèmes, restauration des données, frais de crise (communication, relations presse).

Rançon (cyber extorsion) : paiement de rançon négocié avec l'aide d'un spécialiste de négociation mandaté par l'assureur. Attention : certains assureurs exigent leur pré-accord avant tout paiement.

Notification des victimes : frais de notification RGPD des personnes dont les données ont été compromises, frais de surveillance crédit pour les victimes.

Couvertures « third party » (responsabilité civile)

Responsabilité civile envers des tiers dont les données ont été exposées.

Frais de défense et de représentation légale en cas de plainte ou enquête CNIL.

Dommages-intérêts accordés à des tiers suite à une cyberattaque dont votre système est le vecteur.

Assistance en cas de crise

La plupart des polices cyber modernes incluent une **cellule de crise 24/7** : un numéro à appeler en cas d'incident, qui déclenche l'intervention d'une équipe de réponse à incident (DFIR), d'avocats spécialisés et de communicants. Ce service a souvent plus de valeur que les garanties financières elles-mêmes pour une PME qui n'a pas d'équipe sécurité interne.

Ce qui n'est plus couvert en 2026

Les exclusions se sont considérablement durcies après des sinistres systémiques. Il est crucial de lire attentivement les clauses d'exclusion avant de signer.

Exclusion guerre et actes État-nation

Depuis l'arrêt Merck vs ACE American (2023) aux États-Unis et les précédents NotPetya, la clause de guerre (war exclusion) a été retravaillée par les assureurs. En 2026, la plupart des polices excluent explicitement les attaques attribuées à un État ou à un groupe étatique, y compris dans des zones de conflit indirect. Cette exclusion est floue en pratique car l'attribution est rarement certaine — lisez attentivement si votre police inclut une clause de « silent war ».

Infrastructure obsolète et non-patchée

Si votre environnement fait tourner des OS en fin de vie (Windows Server 2008, Windows 7) ou des applications sans mise à jour de sécurité depuis plus de 6 mois, les assureurs peuvent refuser le sinistre en invoquant le défaut de précautions élémentaires. C'est une exclusion de plus en plus fréquemment appliquée.

Faute délibérée ou complicité interne

Une cyberattaque facilitée par un acte délibéré d'un dirigeant ou d'un employé (ex. : installation volontaire d'un malware) n'est pas couverte.

Amendes réglementaires

Les amendes RGPD prononcées par la CNIL et les sanctions pénales ne sont généralement pas couverts. Certaines polices couvrent les frais de défense mais pas l'amende elle-même.

Les critères d'éligibilité 2026 : le questionnaire type

Le questionnaire de souscription d'une cyberpolice en 2026 ressemble à un mini-audit de sécurité. Voici les 5 questions éliminatoires communes à tous les assureurs majeurs :

1. MFA sur les accès distants

L'authentification multi-facteurs (MFA) sur les accès VPN, Remote Desktop Protocol (RDP) et les portails cloud (Microsoft 365, Google Workspace) est devenu un prérequis absolu. Un assureur refusera systématiquement ou appliquera une surprime de 30 à 50 % si le MFA n'est pas déployé sur ces accès. La raison : 80 % des ransomwares entrent via des accès distants compromis.

2. EDR déployé sur les postes et serveurs

Un antivirus traditionnel ne suffit plus. Les assureurs demandent explicitement la présence d'un EDR (Endpoint Detection and Response) tel que SentinelOne, CrowdStrike Falcon, Microsoft Defender for Endpoint ou un équivalent. Certains assureurs imposent leur propre EDR via un partenariat.

3. Sauvegardes offline testées

Les sauvegardes doivent être isolées du réseau principal (offline ou immutable), conservées sur 3 supports différents (règle 3-2-1), et testées avec une restauration complète au moins une fois par an. Le test de restauration est crucial : un assureur peut demander la preuve d'un test récent.

4. Patch management formalisé

Un processus documenté de gestion des correctifs avec une fenêtre de déploiement définie (ex. : correctifs critiques sous 72h) et une liste des systèmes couverts est requis. Les systèmes legacy hors scope doivent être explicitement listés avec un plan de migration ou de compensations.

5. Formation phishing annuelle

Les collaborateurs doivent avoir reçu une formation anti-phishing dans les 12 derniers mois, avec des simulations de phishing pour mesurer la sensibilisation. Un taux de clic sur les simulations supérieur à 20 % est souvent un signal négatif pour les souscripteurs.

Les 5 assureurs majeurs en France : comparatif

Le marché français est dominé par cinq acteurs qui concentrent 70 % des primes cyber pour les PME/ETI :

AXA XL : leader historique, offre cyber complète, cellule de crise AXA CERT, forte présence PME industrie. Critères d'entrée élevés.

Allianz Commercial : produit « AllianzCyber » avec accès à la plateforme Eagle Eye pour la détection de vulnérabilités. Bon rapport couverture/prime pour les ETI.

AIG (Lexington Insurance) : spécialiste historique cyber, ancienne référence du marché. Polices très détaillées avec couverture rançon étendue. Plus sélectif post-2022.

Hiscox France : très actif sur le segment PME (<50 salariés), questionnaire simplifié en ligne, souscription rapide. Couvertures plafonnées à 1M€ pour les petites structures.

Beazley : spécialiste London Market, reconnu pour sa réactivité en sinistre, couvertures étendues pour professions de santé et secteur financier. Tarification agressive pour les dossiers bien préparés.

Comment préparer un dossier de souscription solide

Un dossier bien préparé peut réduire votre prime de 15 à 25 %. Voici les pièces généralement demandées :

Organigramme IT et liste des applications critiques.

Schéma réseau simplifié (segmentation, présence DMZ, VPN).

Politique de sauvegarde documentée avec preuve de test de restauration.

Liste des OS et applications avec versions et dates de dernière mise à jour.

Rapport de test de phishing récent (moins de 6 mois).

Politique MFA documentée (quels accès, quelle solution).

Liste des prestataires IT tiers avec accès à votre SI (MSSP, infogérance).

Plan de réponse à incident ou contact DFIR prestataire. Notre article sur le plan de réponse à incident (modèle gratuit) peut vous aider à formaliser ce document.

Franchises et plafonds : tendances 2026

Pour une PME entre 10 et 50 salariés, les franchises pratiquées en 2026 varient de 2 500 € (secteurs peu risqués, bonne maturité cyber) à 25 000 € (secteurs santé, industrie, organismes critiques). Les franchises relatives (pourcentage du sinistre) ont fait leur apparition dans certaines polices — lisez attentivement.

Les plafonds de garantie pour les PME se situent typiquement entre 250 000 € et 2 millions €. Pour les secteurs très exposés (e-commerce, santé, collectivités), certains assureurs plafonnent désormais la garantie ransomware séparément de la garantie BI globale. Vérifiez que les sous-limites ne vident pas l'essentiel de votre couverture.

NIS 2 et cyber-assurance : le lien vertueux

La directive NIS 2, transposée en droit français fin 2024, impose des obligations de sécurité aux entités essentielles et importantes. Pour les assureurs, la conformité NIS 2 est devenue un signal de maturité cyber équivalent à la certification ISO 27001. Certains assureurs proposent explicitement des réductions de prime (10 à 25 %) pour les entreprises NIS 2 conformes ou certifiées ISO 27001.

Inversement, si votre entreprise est soumise à NIS 2 et subit un incident sans avoir mis en œuvre les mesures minimales (article 21 de NIS 2 : gestion des risques, sauvegardes, MFA, chiffrement, formation), votre assureur pourrait invoquer le défaut de précautions élémentaires pour réduire ou refuser l'indemnisation. Notre article détaillé sur l'ISO 27001 explore comment le cadre de management de la sécurité renforce votre dossier de souscription cyber.

Processus de déclaration de sinistre : ce qu'il faut faire dans les 72h

En cas d'incident cyber couvert, les premières heures sont critiques. Voici la chronologie recommandée :

H+0 à H+4 : isoler les systèmes compromis, appeler le numéro de crise 24/7 de votre assureur. Ne payez aucune rançon sans accord préalable de l'assureur.

H+4 à H+24 : déclaration formelle à votre courtier et à l'assureur par écrit (email + lettre recommandée). Documentez l'heure de découverte, les systèmes touchés, les premières actions prises.

H+24 à H+72 : si des données personnelles sont compromises, notification obligatoire à la CNIL sous 72h (article 33 RGPD). L'assureur mandate généralement un cabinet DFIR pour l'investigation. Conservez toutes les preuves numériques (logs, disques forensiques).

H+72 et au-delà : notification individuelle des victimes si risque élevé pour leurs droits et libertés (article 34 RGPD).

Notre guide sur l'incident response playbook ransomware détaille les étapes techniques de réponse à une attaque ransomware qui s'articulent avec ce processus de déclaration.

Coûts indicatifs selon la taille de l'entreprise

Ces fourchettes sont indicatives pour 2026 et varient fortement selon le secteur d'activité, la surface d'exposition (e-commerce vs cabinet de conseil) et la maturité cyber démontrée :

TPE / 5-10 salariés : 800 € à 3 000 €/an — plafond 100K-250K€.

PME / 50 salariés : 5 000 € à 15 000 €/an — plafond 500K-1M€.

ETI / 500 salariés : 50 000 € à 150 000 €/an — plafond 2M-10M€.

Secteurs sensibles (santé, industrie critique, collectivités) : surprime de 30 à 80 % par rapport aux tarifs standards.

Pour affiner votre estimation, un courtier spécialisé cyber (Marsh, WTW, Verlingue, Veritas) peut vous obtenir 3 à 5 devis comparatifs. Notre article sur l'audit de cybersécurité PME vous aidera à mesurer et documenter votre maturité cyber avant d'approcher les assureurs.

FAQ — Questions fréquentes

Une police cyber couvre-t-elle systématiquement le paiement d'une rançon ?

Pas automatiquement. La couverture de la rançon (cyber extorsion) est une garantie distincte qui doit être explicitement incluse dans votre contrat. De plus, la quasi-totalité des assureurs exigent une autorisation préalable avant tout paiement et mandatent un négociateur spécialisé pour réduire le montant demandé. Certains assureurs, face à la pression réglementaire et éthique (financement du crime organisé), ont commencé à limiter ou exclure cette garantie pour certains secteurs. Vérifiez ce point précisément dans votre police et comprenez la procédure à suivre en cas de demande de rançon. Pour comprendre le cadre technique d'un incident ransomware, consultez notre article sur le playbook de réponse à incident ransomware.

Ma prime augmentera-t-elle forcément après un sinistre ?

Dans la grande majorité des cas, oui. Un sinistre déclaré entraîne une révision à la hausse de la prime lors du renouvellement, avec des hausses pouvant aller de 20 à 100 % selon la gravité du sinistre et les actions correctives mises en place. L'assureur évaluera les mesures de remédiation (EDR renforcé, formation, segmentation réseau) avant de proposer les conditions de renouvellement. Certains assureurs peuvent ne pas renouveler le contrat après un sinistre grave. C'est pourquoi prévenir un incident en investissant dans la sécurité est économiquement plus rationnel que de compter uniquement sur l'assurance — l'assurance couvre l'aléa résiduel, pas le risque évitable.

Une PME peut-elle s'auto-assurer plutôt que souscrire une cyberpolice ?

L'auto-assurance (constituer une réserve financière interne plutôt que de payer des primes) n'est envisageable que pour des entreprises avec une trésorerie très solide et une excellente maturité cyber. Pour une PME classique, un incident ransomware de grande ampleur peut représenter 6 à 18 mois de trésorerie : reconstruction IT, perte d'exploitation, frais juridiques, notification RGPD. L'auto-assurance expose la pérennité de l'entreprise. En revanche, un niveau d'investissement élevé dans la sécurité préventive (réduire la probabilité d'incident) combiné à une franchise élevée (réduire la prime) est une stratégie cohérente pour les entreprises avec une maturité cyber avancée. L'audit de cybersécurité PME et les ressources de l'ANSSI peuvent vous guider dans cette démarche préventive. Pour une vision plus large du marché, l'AMRAE publie chaque année une étude sur la sinistralité cyber en France.

Pour aller plus loin : Mise en œuvre pratique

La conformité réglementaire nécessite une approche structurée et documentée. Ces ressources complémentaires permettent d'approfondir les points techniques et juridiques abordés dans cet article.

Outils d'auto-évaluation

ANSSI — Outil d'évaluation cybersécurité — Le Diagnostic de Cybersécurité de l'ANSSI permet d'évaluer le niveau de maturité de votre organisation sur 5 domaines clés. Gratuit et disponible sur diagnostic.ssi.gouv.fr.

ENISA — Outil d'auto-évaluation NIS2 — Questionnaire structuré pour identifier les exigences applicables à votre secteur et votre taille d'organisation.

Logiciels GRC — Des solutions comme Vanta, Drata ou TrustCloud automatisent la collecte de preuves de conformité et accélèrent les processus d'audit.

Documentation à produire en priorité

Politique de Sécurité du Système d'Information (PSSI) — document fondateur

Registre des activités de traitement (RGPD, article 30)

Analyse d'impact relative à la protection des données (AIPD/DPIA)

Plan de continuité d'activité (PCA) et plan de reprise d'activité (PRA)

Procédure de gestion des incidents de sécurité (notification ANSSI/CNIL)

Accompagnement et conseil

La mise en conformité implique souvent une assistance externe pour les organisations ne disposant pas d'expertise interne. Les RSSI externalisés ou les consultants spécialisés en conformité peuvent accélérer significativement le processus, notamment pour la préparation aux audits de certification ISO 27001 ou pour la mise en conformité NIS 2 avec un délai contraint.

Bonnes pratiques et recommandations complémentaires

Au-delà des techniques et outils présentés dans cet article, plusieurs principes transverses guident les professionnels de la cybersécurité dans leur approche quotidienne. La défense en profondeur (*defense-in-depth*) reste le principe fondateur : aucune mesure de sécurité unique n'est suffisante, et la multiplication des couches de protection — même imparfaites individuellement — crée une résilience globale supérieure à la somme de ses parties.

Veille et mise à jour continue

La cybersécurité est un domaine où l'obsolescence est rapide. Une technique ou un outil efficace en 2024 peut être contourné en 2026. Les équipes sécurité maintiennent leur efficacité en s'appuyant sur des sources de veille fiables : bulletins CERT-FR et ANSSI, advisories des éditeurs (Microsoft MSRC, Google Project Zero, Cisco Talos), recherches académiques

(USENIX Security, IEEE S&P, CCS), et publications de la communauté (threat intel reports des grands éditeurs, articles de blog de chercheurs reconnus).

Documentation et partage de connaissances

La capitalisation des connaissances est un enjeu organisationnel critique dans les équipes de sécurité. Les runbooks d'investigation, les post-mortems d'incidents, les procédures de réponse documentées, et les bases de connaissance internes permettent de maintenir la cohérence des pratiques indépendamment des rotations d'équipe et de réduire le temps de résolution des incidents récurrents. L'utilisation d'un wiki sécurisé (Confluence, Notion avec contrôles d'accès stricts) pour centraliser ces connaissances est une pratique adoptée par la majorité des équipes SOC matures. La documentation proactive, rédigée juste après les incidents pendant que les détails sont frais, est systématiquement plus précise et utile que la documentation rédigée après coup.

Synthèse et feuille de route conformité

La conformité réglementaire est un processus continu, non un projet ponctuel. Les organisations qui abordent ISO 27001, NIS 2, RGPD ou HDS comme des certifications à obtenir une fois pour toutes échouent systématiquement lors des audits de renouvellement. La clé du succès est l'intégration des exigences réglementaires dans les processus opérationnels quotidiens, non leur traitement comme des obligations externes.

En pratique, les organisations matures en matière de conformité fonctionnent avec un SMSI vivant : des revues de direction trimestrielles, un audit interne annuel, des exercices de gestion de crise bi-annuels, et une veille réglementaire hebdomadaire. Le coût de la conformité maintenue en continu est significativement inférieur au coût d'une remise à niveau précipitée avant un audit ou une notification de violation. Les amendes CNIL, les pénalités NIS 2, et les pertes de contrats liées à une non-conformité documentée représentent des risques financiers et réputationnels mesurables que la gouvernance de direction doit intégrer dans l'analyse des risques métier.

