RAPPORT

La réalité de la confiance dans la cybersécurité en 2026

Une enquête indépendante menée auprès de 5 000 responsables informatiques et cybersécurité

SOPHOS

Introduction

Quand les organisations choisissent un fournisseur de solutions de cybersécurité, elles confient leur résilience opérationnelle critique — c'est-à-dire leur personnel, leurs données et leur chiffre d'affaires — entre les mains de ce fournisseur.

Pourtant, selon une nouvelle étude de Sophos, malgré cette dépendance, la plupart des organisations manquent de confiance envers les fournisseurs sur lesquels elles comptent pour assurer leur sécurité.

Pour mieux appréhender la réalité de la confiance dans la cybersécurité, Sophos a commandé une enquête mondiale indépendante et impartiale auprès de 5 000 responsables informatiques et cybersécurité dans 17 pays. Réalisée par Vanson Bourne, un cabinet d'études spécialisé, cette enquête offre un aperçu concret et statistiquement significatif de la manière dont la confiance s'établit et se perd entre les acheteurs et les fournisseurs de solutions de cybersécurité.

5 000

responsables informatiques et cybersécurité issus de 17 pays ont participé à une enquête indépendante mondiale

Principaux enseignements

La confiance fait défaut : seuls 5 % des responsables informatiques affirment qu'eux-mêmes et leur organisation font pleinement confiance à leurs fournisseurs de solutions de cybersécurité.

Des preuves vérifiées sont un facteur essentiel de confiance : les équipes informatiques et la direction s'accordent à dire que les éléments concrets et vérifiables permettant de mesurer la maturité de la cybersécurité constituent le principal indicateur de fiabilité.

Juger de la fiabilité d'un fournisseur reste un défi : 79 % des organisations ont du mal à évaluer la fiabilité des nouveaux fournisseurs de cybersécurité, tandis que 62 % ont du mal à évaluer celle de leurs fournisseurs actuels. Les personnes interrogées ont cité plusieurs facteurs qui ont entamé leur confiance envers les fournisseurs, le principal étant que les informations fournies par ces derniers n'étaient pas assez factuelles ou détaillées.

Ce manque de confiance a des conséquences : 51 % des personnes interrogées affirment que le manque de confiance suscite la crainte que l'organisation soit plus exposée à un cyber incident majeur.

Praticiens et dirigeants sont souvent en désaccord : 78 % des personnes interrogées indiquent que leur équipe informatique et la direction/le conseil d'administration ont des avis divergents sur la fiabilité des fournisseurs de cybersécurité de leur organisation. Près d'un tiers des entreprises ayant répondu à l'enquête de Sophos indiquent que ce désaccord se produit « souvent ».

La fiabilité est difficile à évaluer

Seuls 5 % des responsables informatiques affirment qu'eux-mêmes et leur organisation font pleinement confiance à leurs fournisseurs de solutions de cybersécurité.

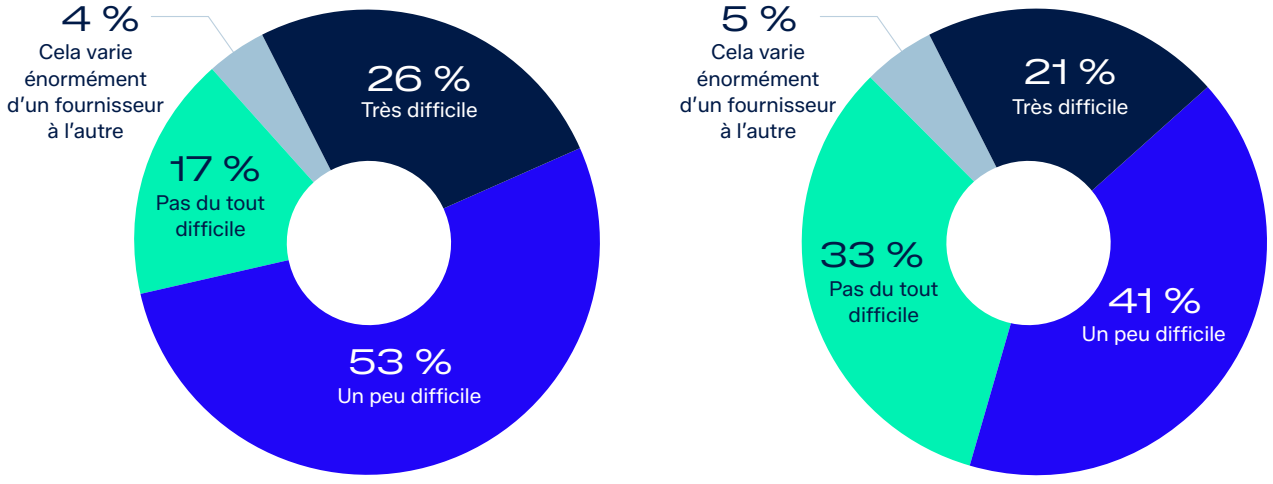
Lorsque vous comptez sur votre fournisseur de cybersécurité pour assurer la sécurité de votre réseau et le bon fonctionnement de vos activités, la confiance est essentielle. Ce sont les fournisseurs de cybersécurité qui protègent votre entreprise 24 h/24 et 7 j/7, même la nuit et le week-end, et lorsque les membres de l'équipe informatique sont en vacances. Pour les propriétaires de petites entreprises, qui n'ont parfois pas de personnel informatique dédié, ces produits ou services de cybersécurité jouent même le rôle d'un véritable collaborateur.

Avant de pouvoir décider à qui faire confiance, les organisations doivent relever un défi encore plus fondamental : évaluer en premier lieu la fiabilité d'un fournisseur donné.

D'après l'enquête, 79 % des personnes interrogées déclarent qu'il est difficile d'évaluer la fiabilité des nouveaux fournisseurs ou partenaires de cybersécurité, ce qui met en évidence une difficulté généralisée à comparer les produits, à vérifier les affirmations et à déterminer si un fournisseur potentiel est réellement en mesure de protéger l'entreprise. 62 % ont également du mal à évaluer la fiabilité des fournisseurs avec lesquels ils travaillent déjà — ce qui montre bien que les problèmes de confiance ne disparaissent pas une fois le contrat signé (figure 1).

79 %

79 % des entreprises interrogées ont déclaré qu'il était difficile d'évaluer la fiabilité des nouveaux fournisseurs ou partenaires de cybersécurité



Évaluer les **nouveaux** fournisseurs et partenaires de cybersécurité

Évaluer les fournisseurs et partenaires de cybersécurité **existants**

Figure 1 : De manière générale, dans quelle mesure est-il difficile, le cas échéant, pour votre organisation d'évaluer la fiabilité des fournisseurs et partenaires en matière de cybersécurité ? n = 5 000

Les obstacles à l'évaluation de la fiabilité

Les personnes interrogées ont identifié plusieurs obstacles entravant la confiance envers les fournisseurs, dont la plupart sont liés à la transparence. Beaucoup ont du mal à interpréter les arguments mis en avant par les fournisseurs, à évaluer les détails techniques ou à trouver les informations dont ils ont besoin pour prendre des décisions en toute confiance.

Près de la moitié (47 %) estime que les informations fournies par les fournisseurs ne sont pas assez factuelles ou détaillées, et 45 % trouvent ces informations difficiles à interpréter ou à comprendre. En outre, 43 % reconnaissent ne pas avoir les compétences ou les connaissances nécessaires pour évaluer efficacement les fournisseurs, 41 % se heurtent à des informations contradictoires et 38 % ont tout simplement du mal à trouver les informations dont ils ont besoin (figure 2).

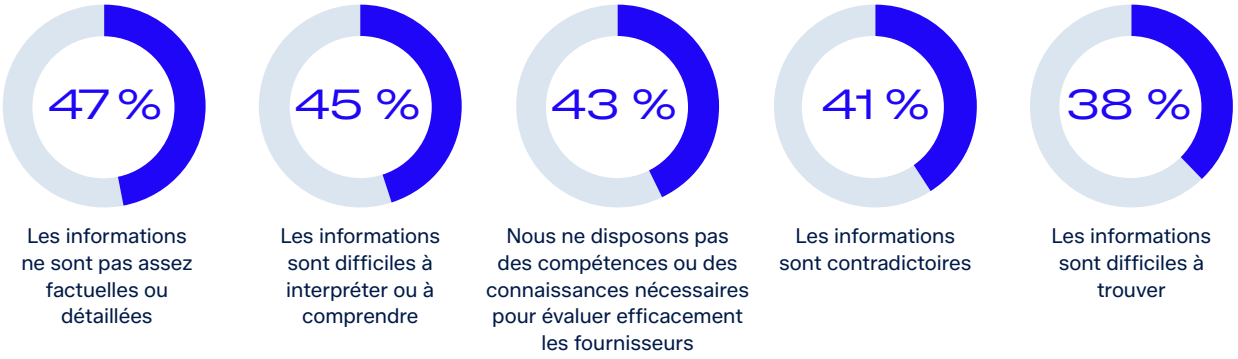


Figure 2 : Pourquoi votre organisation a-t-elle du mal à évaluer la fiabilité des fournisseurs de cybersécurité ? n = 4 483

La principale différence entre les petites entreprises (moins de 250 employés) et les grandes entreprises (plus de 1 000 employés) réside dans le fait que les PME sont bien plus susceptibles de ne pas disposer des compétences ou des connaissances nécessaires pour évaluer efficacement la fiabilité des fournisseurs : les PME ont cité ce problème dans 8 % des cas de plus que les répondants issus des grandes entreprises (figure 3).

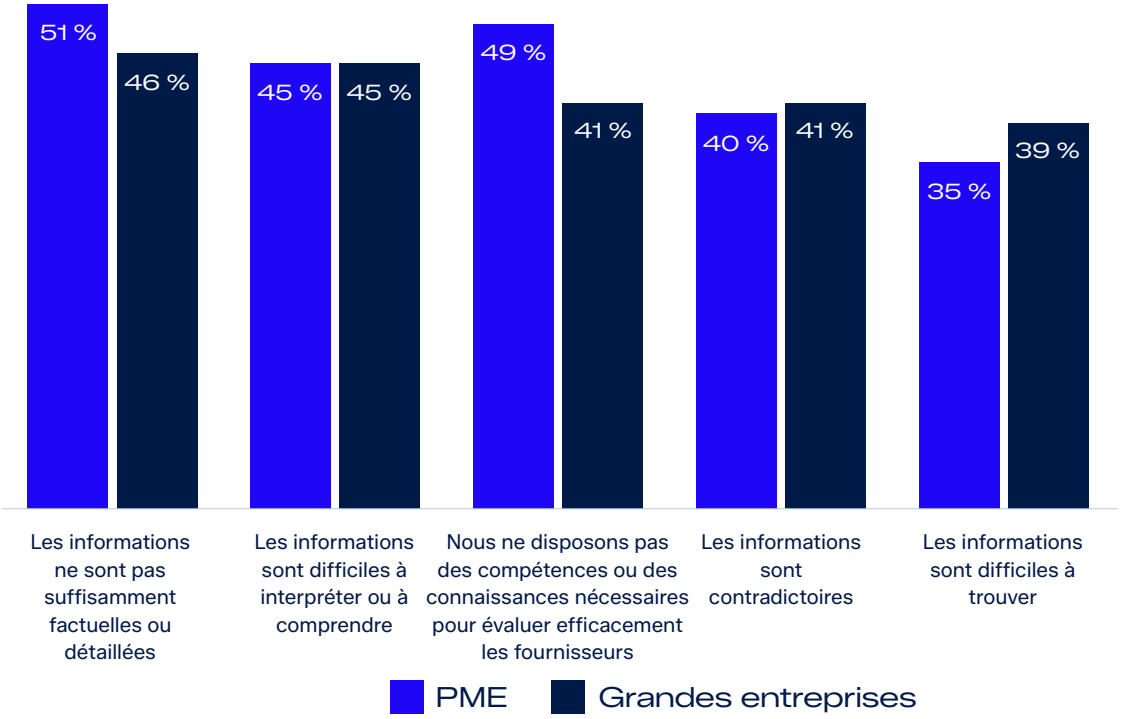


Figure 3 : Pourquoi votre organisation a-t-elle du mal à évaluer la fiabilité des fournisseurs de cybersécurité ? n = 504 (PME), 2 260 (grandes entreprises)

Le manque de confiance a des conséquences

Cette étude montre à quel point le manque de confiance entre un fournisseur et ses clients constitue un problème majeur à plusieurs égards. Interrogés sur les conséquences du manque de confiance totale envers leurs fournisseurs de cybersécurité, les personnes interrogées ont répondu à l'ensemble des questions en mettant en avant un mélange de répercussions tant sur le plan émotionnel qu'opérationnel :

- **51 %** se disent de plus en plus inquiets à l'idée que leur organisation puisse être victime d'un cyber incident grave.
- **45 %** disent que ça les incite davantage à changer de fournisseur — un processus coûteux et perturbateur pour la plupart des organisations.
- **42 %** prévoient un renforcement des exigences en matière de contrôle.
- **41 %** déclarent se sentir moins rassurés quant à leur niveau de cybersécurité.
- **38 %** craignent qu'eux-mêmes ou leur organisation aient fait un mauvais choix de fournisseur.

Ces répercussions viennent s'ajouter aux contraintes opérationnelles qui pèsent déjà sur les équipes informatiques et de cybersécurité.

Des points de vue divergents entre le service informatique et la direction

Un autre défi majeur réside dans le décalage entre les personnes qui utilisent quotidiennement les outils de cybersécurité et celles qui signent les contrats. 78 % des personnes interrogées indiquent que leur équipe informatique et leur direction ou leur conseil d'administration ont des avis divergents sur la fiabilité de leurs fournisseurs de cybersécurité, et près d'un tiers précise que ces désaccords surviennent « souvent » (figure 4).

Les personnes interrogées ont indiqué que la direction reste très impliquée dans les décisions d'achat. Seul 1 % des organisations ont indiqué que le conseil d'administration ou la direction ne jouait aucun rôle dans les décisions d'achat en matière de cybersécurité.

1 %

des organisations interrogées ont déclaré que la direction ne jouait aucun rôle dans les décisions d'achat en matière de cybersécurité.

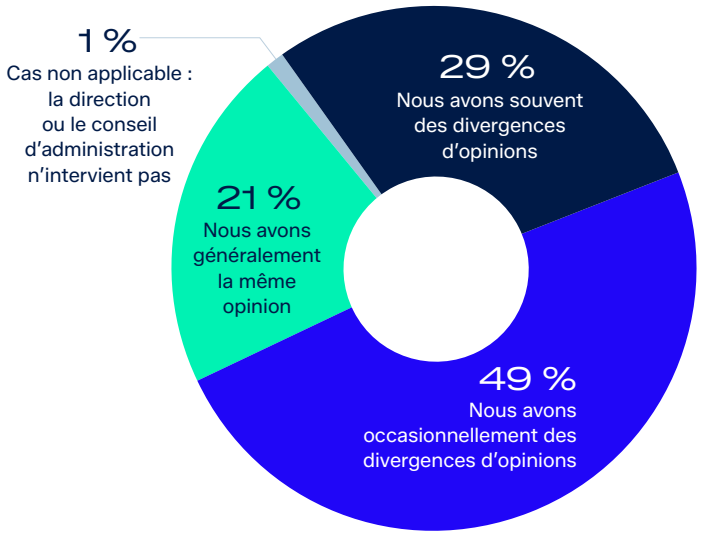


Figure 4 : L'équipe informatique et la direction générale/le conseil d'administration ont-elles des divergences d'opinions quant à la fiabilité des fournisseurs de solutions de cybersécurité de votre organisation ? n = 5 000.

Comment instaurer la confiance dans la cybersécurité

Les personnes interrogées ont indiqué que des pratiques de sécurité transparentes et fondées sur des données factuelles sont essentielles pour instaurer la confiance. Les organisations recherchent des fournisseurs qui inspirent confiance grâce à leur transparence, leur clarté et leurs pratiques de sécurité fondées sur des preuves concrètes et vérifiables.

Tant parmi les cadres supérieurs que parmi les équipes informatiques, les « éléments vérifiables témoignant de la maturité de la cybersécurité » ont été cités comme le principal facteur de confiance envers les fournisseurs de solutions de cybersécurité. Ces preuves comprennent notamment les programmes de Bug Bounty, un Centre de confiance accessible au public, des avis de sécurité détaillant les vulnérabilités de leurs produits (ainsi que leur remédiation), des évaluations réalisées par des tiers et des certifications.

« La transparence et la communication rapide en cas d'incidents et de divulgations » ont également été classées comme le deuxième facteur le plus important pour les membres de la direction et le troisième pour les membres de l'équipe informatique.

Facteurs de confiance envers les fournisseurs de cybersécurité

Facteurs	Dir./ CA	Équipe IT/ cyber	Facteurs d'influence
Facteurs primaires	n° 1	n° 1	Des preuves concrètes qui démontrent la maturité de la cybersécurité. Par ex. : programmes de Bug Bounty, Centre de confiance, avis de sécurité, évaluations par des tiers, certifications
	n° 2	n° 3	Transparence et communication rapide en cas d'incidents et de divulgations
	n° 3	n° 4	Expertise médiatique suite à des cyber incidents majeurs. Par ex. : citations dans la presse, à la télévision
	n° 4	n° 2	Prestation constante de services et de produits de cybersécurité de haute qualité
	n° 5	n° 5	Performance dans des rapports d'analystes. Par ex. : le Magic Quadrant de Gartner
Facteurs secondaires	n° 6	n° 9	Transparence sur les procédures de sécurité internes
	n° 7	n° 7	Performance dans des tests indépendants. Par ex. : MITRE, SE Labs
	n° 8	n° 6	Support réactif et fiable
	n° 9	n° 8	Recommandation de votre revendeur/partenaire de cybersécurité
Facteurs tertiaires	n° 10	n° 13	Qualité des publications de recherche sur les menaces
	n° 11	n° 12	Couverture dans la presse financière et économique
	n° 12	n° 11	Expérience des autres (pairs/clients)
	n° 13	n° 10	Expérience personnelle

Quels sont les facteurs qui influencent ou influenceraient le plus la confiance de la direction ou du conseil d'administration dans un fournisseur de cybersécurité ? Réponses arrivées en tête. Quels sont les facteurs qui influencent ou influenceraient le plus le niveau de confiance de l'équipe informatique/cybersécurité dans un fournisseur de cybersécurité ? Réponses arrivées en tête.

L'engagement de Sophos à gagner la confiance de nos clients et de nos partenaires

Chez Sophos, nous avons conscience que la confiance se mérite et ne s'impose pas. C'est pourquoi nous nous efforçons chaque jour de la gagner en faisant preuve de transparence, d'intégrité et d'un engagement sans faille en faveur de la sécurité et de la confidentialité.

Au cœur de nos efforts se trouve le Sophos Trust Center où nous publions des avis de sécurité, répertorions les vulnérabilités de nos produits et les remédiations, présentons notre posture de conformité et expliquons comment nous protégeons les données de nos clients.

Cette transparence se reflète également dans l'investigation « Pacific Rim » réalisée par Sophos X-Ops, qui a rendu publique une campagne menée pendant cinq ans par des acteurs malveillants basés en Chine et a partagé des informations détaillées sur les tactiques, techniques et procédures (TTP), les indicateurs de compromission (IOC) ainsi que des conseils de défense pour aider les organisations à renforcer leur résilience à travers tout le secteur.

En mettant au jour les activités sophistiquées menées par des États-nations, en collaborant avec les gouvernements et d'autres fournisseurs, et en faisant preuve de franchise tant sur ses points forts que sur ses points faibles, Sophos réaffirme que la confiance se mérite jour après jour grâce à l'honnêteté, à la responsabilité et à un engagement à protéger l'écosystème numérique dans son ensemble.

En savoir plus

Pour en savoir plus sur notre engagement en faveur de la confiance et sur les ressources que nous mettons à disposition pour vous aider à évaluer la fiabilité de Sophos, rendez-vous sur le Centre de confiance ou contactez votre partenaire ou représentant Sophos.

SOPHOS

Pour plus d'informations, consultez le Centre de confiance ou contactez votre partenaire ou représentant Sophos.

Sophos France
Tél. : 01 34 34 80 00
Email : info@sophos.fr