SOPHOS

L'ÉTAT DES RANSOMWARES 2025

Résultats d'une enquête indépendante menée auprès de 3 400 responsables IT et cybersécurité dans 17 pays, dont les organisations ont été touchées par un ransomware au cours de l'année écoulée.

Un livre blanc Sophos. Juin 2025

Introduction

Bienvenue dans la sixième édition du rapport annuel de Sophos qui dresse un état des lieux des ransomwares en 2025.

Ce rapport détaille l'évolution de l'expérience des organisations face aux ransomwares (tant les causes que les répercussions) au cours des 12 derniers mois. Il met également en lumière des aspects jusqu'alors inexplorés, notamment les facteurs opérationnels qui ont exposé les organisations aux attaques et l'impact humain des incidents sur l'équipe informatique/cybersécurité.

Ce rapport est basé sur les expériences concrètes de 3 400 responsables IT/cybersécurité issus de 17 pays dont les organisations ont été touchées par un ransomware au cours de l'année passée. Il fournit des perspectives inédites sur :

- Les raisons pour lesquelles les organisations sont victimes de ransomwares.
- Ce qu'il advient des données.
- Les rançons : les montants demandés et les montants effectivement payés.
- L'impact économique des ransomwares.

Remarque sur les dates mentionnées

Pour faciliter la comparaison des données entre nos enquêtes annuelles, le nom du rapport correspond à l'année au cours de laquelle l'enquête a été menée, dans le cas présent, 2025. Nous sommes conscients que les entreprises interrogées ont fait part de leurs expériences vécues au cours de l'année précédente, aussi nombre des attaques mentionnées se sont produites en 2024.

À propos de l'enquête

Ce rapport s'appuie sur les résultats d'une enquête indépendante sur les expériences des entreprises face aux ransomwares, commandée par Sophos et menée par un spécialiste indépendant entre janvier et mars 2025. Tous les répondants travaillent au moment de l'enquête dans des organisations comptant entre 100 et 5 000 employés et ont été invités à répondre en se basant sur leur expérience au cours des 12 derniers mois.

Les participants provenaient de 17 pays et d'un large éventail de secteurs d'activité, ce qui garantit que les résultats de l'enquête reflètent la diversité des expériences rencontrées dans les secteurs public et privé. Ce rapport établit des comparatifs avec les conclusions de nos rapports précédents, ce qui permet d'effectuer des comparaisons d'une année sur l'autre. Toutes les données financières sont exprimées en dollars américains.

Principales découvertes

Pourquoi les organisations sont-elles victimes de ransomwares

- Pour la troisième année consécutive, les victimes ont identifié l'**exploitation de vulnérabilités** comme la principale cause technique la plus courante des attaques, présentes dans 32 % des incidents.
- De multiples facteurs opérationnels contribuent à l'exposition des organisations aux ransomwares, le plus courant étant le **manque d'expertise**, cité par 40,2 % des victimes. Viennent ensuite, peu après, les **failles de sécurité dont l'organisation n'avait pas conscience**, qui ont contribué à 40,1 % des attaques. En troisième position, on trouve le **manque de personnel/de capacités**, qui, pour sa part, a été déterminant dans 39,4 % des attaques.

Ce qu'il advient des données

- Le **chiffrement des données** est à son niveau le plus bas depuis six ans, 50 % des attaques se soldant désormais par un chiffrement malveillant, contre 70 % en 2024.
- 28 % des entreprises dont les données ont été chiffrées ont également fait l'objet d'une **exfiltration des données**.
- 97 % des données chiffrées ont pu être récupérées.
- L'utilisation de **sauvegardes** pour restaurer des données chiffrées est à son plus bas niveau depuis six ans, puisqu'elle n'est utilisée que dans 54 % des incidents.
- 49 % des victimes ont **payé la rançon** pour récupérer leurs données. Ce chiffre, en légère baisse par rapport aux 56 % enregistrés l'année dernière, représente néanmoins le deuxième taux de paiement de rançon le plus élevé depuis six ans.

Les rançons : montants demandés et montants payés

- Le montant médian des **rançons demandées** est passé de 2 millions de dollars en 2024 à 1 324 439 dollars en 2025, soit une baisse d'un tiers (34 %).
- Quant au montant médian des **rançons payées**, il a diminué de 50 % l'année dernière, passant de 2 millions de dollars en 2024 à 1 million de dollars en 2025. Le principal facteur à l'origine de cette diminution est la baisse du nombre des rançons supérieures à 5 millions de dollars, qui est passé de 31 % des paiements en 2024 à 20 % en 2025.
- Lorsqu'on compare le **montant demandé au montant effectivement payé**, on s'aperçoit qu'ils coïncident dans seulement 29 % des cas, selon les déclarations des entreprises interrogées. 53 % ont payé moins que la demande initiale, tandis que 18 % ont payé plus.

L'impact économique des ransomwares

- En excluant le montant des rançons versées, le **coût de rétablissement** après une attaque de ransomware a baissé en moyenne de 44 % au cours de l'année dernière, passant de 2,73 millions de dollars en 2024 à 1,53 million de dollars.
- Par ailleurs, les entreprises ont tendance à **se rétablir plus rapidement**, 53 % d'entre elles se sont entièrement rétablie après une semaine, contre 35 % en 2024.

L'impact humain des ransomwares

- Toutes les organisations dont les données ont été chiffrées ont signalé que cette situation avait eu des **répercussions directes** sur leur équipe informatique/cybersécurité :
  - 41 % des équipes informatiques/cybersécurité déclarent éprouver **davantage d'anxiété ou de stress** à l'idée de futures attaques.
  - Un tiers (34 %) ont déclaré que les membres de l'équipe avaient éprouvé un **sentiment de culpabilité** de ne pas avoir pu empêcher l'attaque à temps.
  - 40 % des répondants font état d'une **pression accrue** de la part des cadres supérieurs, mais 31 % signalent une **reconnaissance accrue**.
  - 31 % des équipes ont enregistré des **arrêts de travail** liés au stress ou à des problèmes de santé mentale consécutifs à l'attaque.
  - Dans un quart des cas, la **direction de l'équipe a été remplacée** en conséquence de l'attaque.

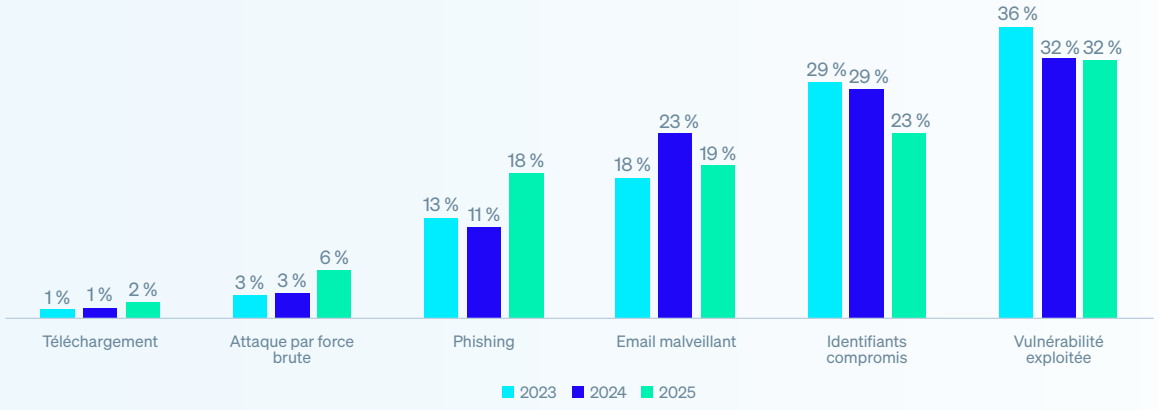
Pourquoi les organisations sont-elles victimes de ransomware

Les principales causes techniques

Pour la troisième année consécutive, les victimes ont identifié l'**exploitation de vulnérabilités** comme la cause principale des attaques par ransomware, méthode utilisée dans 32 % des attaques.

La **compromission des identifiants** reste le deuxième vecteur d'attaque le plus courant, même si la proportion d'attaques utilisant cette approche a baissé de 29 % en 2024 à 23 % en 2025. Les emails représentent toujours un vecteur d'attaque majeur : 19 % des victimes déclarent que des **emails malveillants** étaient à l'origine de l'attaque et près de 18 % citent quant à eux le **phishing**, qui montre un bond notable par rapport aux 11 % déclarés l'année dernière.

Graphique 1 : Causes premières techniques des attaques de ransomware 2023-2025

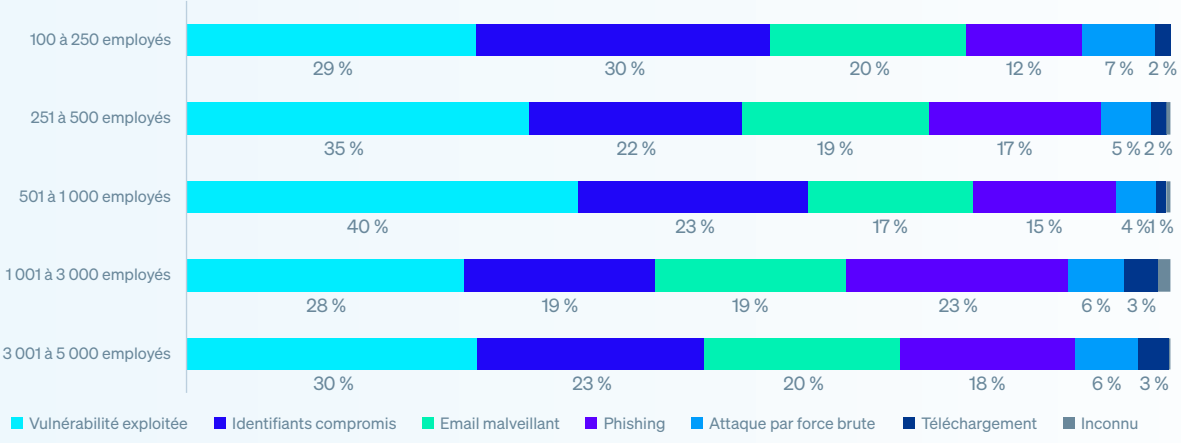


Connaissez-vous la cause première de l'attaque de ransomware dont votre entreprise a été victime au cours de l'année écoulée ? Oui. n=3 400 (2025), 2 974 (2024), 1 974 (2023).

Le rapport met en évidence certaines différences dans les vecteurs d'attaque en fonction de la taille des entreprises :

- Les **identifiants compromis** ont été la cause première la plus fréquente dans le segment des entreprises employant entre 100 et 250 personnes, utilisés dans 30 % des attaques.
- 40 % des attaques menées contre les entreprises comptant entre 501 et 1 000 employés ont commencé par une VULNÉRABILITÉ EXPLOITÉE.
- Environ un quart (23 %) des attaques visant des organisations de 1 001 à 3 000 employés ont commencé par un EMAIL DE PHISHING.

Graphique 2 : Causes premières techniques des attaques de ransomware en fonction de la taille de l'organisation

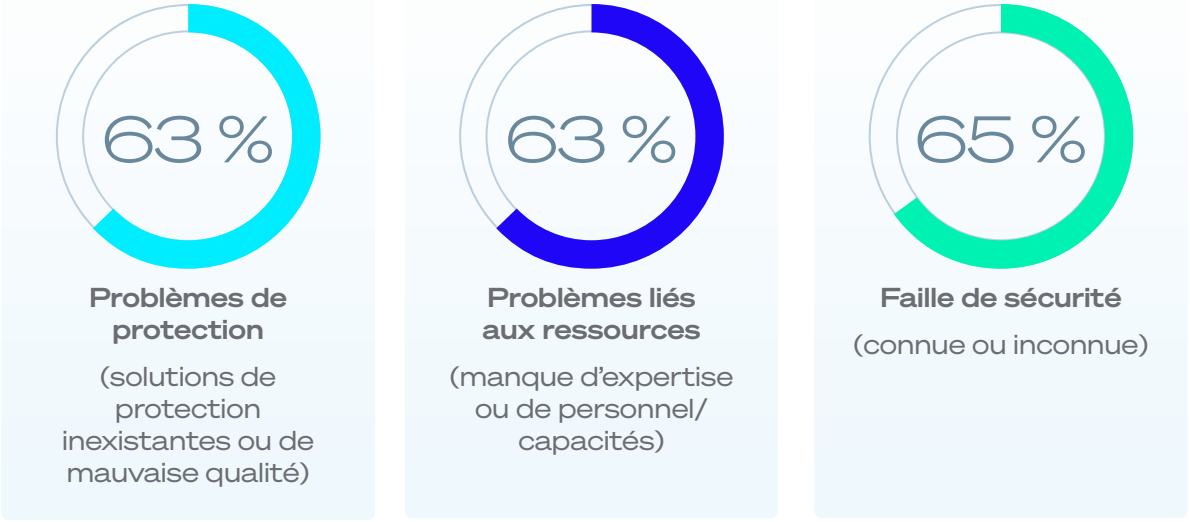


Connaissez-vous la cause première de l'attaque de ransomware dont votre entreprise a été victime au cours de l'année écoulée ? Oui. n=3 400

Les causes premières opérationnelles

Le rapport de cette année se penche pour la première fois sur les facteurs organisationnels qui ont exposé les entreprises à des attaques. Les résultats révèlent que les victimes sont généralement confrontées à de multiples difficultés opérationnelles. En moyenne, les personnes interrogées citent 2,7 facteurs ayant contribué à la survenue de leur attaque.

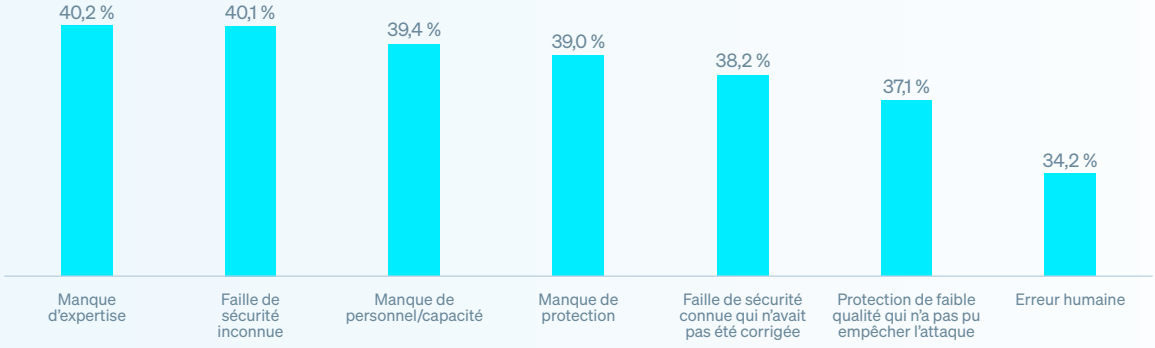
Dans l'ensemble, il n'y a pas de source unique particulière, les causes premières d'ordre organisationnel étant très uniformément réparties entre les problèmes de protection, les problèmes de ressources et les failles de sécurité.



Selon vous, pourquoi votre organisation a été victime d'une attaque de ransomware ? n=3 400

Le **manque d'expertise** (c'est-à-dire le fait de ne pas disposer des compétences ou des connaissances nécessaires pour détecter et stopper l'attaque à temps) est la raison opérationnelle la plus fréquemment citée, mise en avant par 40,2 % des personnes interrogées. Viennent ensuite, tout près derrière, les **failles de sécurité dont l'organisation n'avait pas conscience**, qui ont contribué à 40,1 % des attaques. Le **manque de personnel/de capacités** (c'est-à-dire le fait de ne pas disposer d'un nombre suffisant d'experts en cybersécurité chargés de surveiller les systèmes au moment de l'attaque) arrive en troisième position et est à l'origine de 39,4 % des attaques.

Graphique 3 : Causes premières opérationnelles des attaques de ransomware

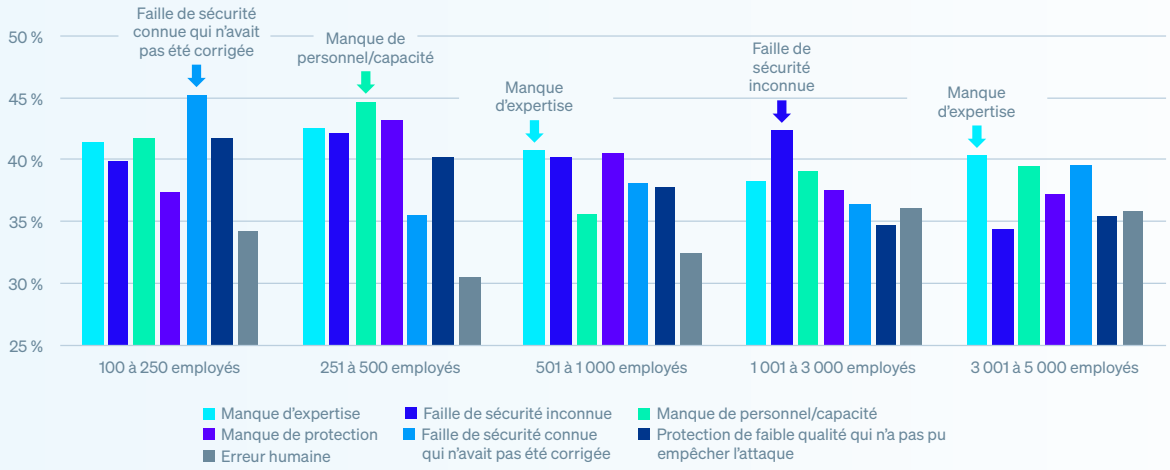


Selon vous, pourquoi votre organisation a-t-elle été victime d'une attaque de ransomware ? n=3 400

Les causes premières opérationnelles par taille d'entreprise

Les causes d'ordre organisationnel les plus courantes qui expliquent pourquoi les entreprises sont victimes d'une attaque de ransomware varient en fonction de la taille de l'organisation, reflétant les différents défis auxquels elles sont confrontées. Dans les cinq segments de taille d'entreprise pris en compte dans ce rapport, quatre défis différents figuraient en tête des facteurs ayant contribué à la survenue de ces attaques, comme le montre le graphique ci-dessous.

Graphique 4 : Causes premières opérationnelles des attaques de ransomware en fonction de la taille de l'organisation



Selon vous, pourquoi votre organisation a-t-elle été victime d'une attaque de ransomware ? n=3 400 Répartition selon la taille de l'organisation (nombre d'employés)

Les causes premières opérationnelles par secteur

De même, la cause opérationnelle la plus courante varie également en fonction du secteur, ce qui témoigne des différents défis auxquels les entreprises doivent faire face. Il convient de noter qu'aucun secteur n'a signalé l'erreur humaine comme étant la raison la plus courante à l'origine de leur vulnérabilité.

Graphique 5 : Causes premières opérationnelles des attaques de ransomware par secteur

MANQUE D'EXPERTISE	FAILLE DE SÉCURITÉ INCONNUE	MANQUE DE PERSONNEL/CAPACITÉ	MANQUE DE PROTECTION	FAILLE DE SÉCURITÉ CONNUE	PROTECTION DE MAUVAISE QUALITÉ
Nous ne disposions ni des compétences ni des connaissances nécessaires pour détecter et stopper l'attaque à temps.	Nous avions une faille dans nos défenses dont nous n'étions pas conscients.	Au moment de l'attaque, nous ne disposions pas d'un nombre suffisant d'experts en cybersécurité pour surveiller nos systèmes.	Nous ne disposions pas des produits et services de cybersécurité nécessaires.	Nos défenses présentaient des vulnérabilités dont nous étions conscients, mais que nous n'avions pas corrigées.	Nos produits et services de cybersécurité n'ont pas été en mesure d'arrêter l'attaque.
Énergie, pétrole/gaz, services d'utilité publique (43 %)	Enseignement supérieur (18 ans et plus) (49 %)	Enseignement des 1er et 2nd degrés (42 %)*	Services financiers, dont assurances (44 %)*	Administration publique centrale (45 %)	Médias, loisirs et divertissement (41 %)
Enseignement des 1er et 2nd degrés (42 %)*	Services aux entreprises (46 %)	Santé (42 %)	Administration publique locale (40 %)	Informatique, technologie et télécoms (42 %)	Distribution et transport (41 %)
Manufacture et production (42 %)	Retail 46 %			Construction et immobilier (41 %)*	
Construction et immobilier (41 %)*	Services financiers, dont assurances (44 %)*				

* indique la cause première conjointe des attaques.

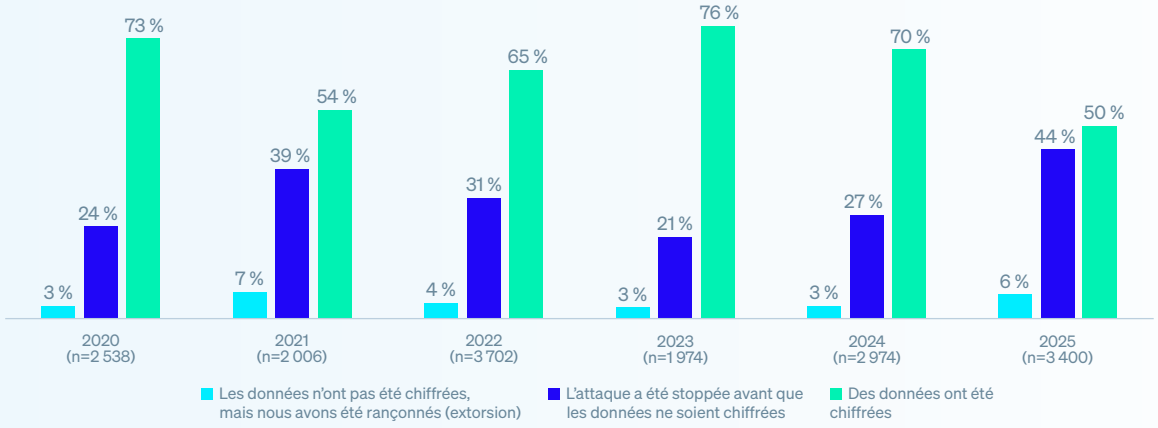
Selon vous, pourquoi votre organisation a-t-elle été victime d'une attaque de ransomware ? n=3 400 Répartition par secteur d'activité

Ce qu'il advient des données

Chiffrement des données

Fait encourageant, le taux de chiffrement des données est à son plus bas niveau depuis six ans, 50 % des attaques ayant abouti à un chiffrement indésiré. Au cours de l'année dernière, le pourcentage d'attaques ayant entraîné un chiffrement des données a considérablement diminué, passant de 70 % dans notre enquête de 2024 à 50 % en 2025. Une tendance qui laisse penser que les entreprises sont désormais mieux aptes à contrer les attaques avant même que la charge virale chiffrée ne soit déployée.

Graphique 6 : Taux de chiffrement des données dans les attaques de ransomware 2020-2025



Lors de l'attaque par ransomware, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ? Chiffres de base dans le graphique.

Les plus grandes organisations interrogées étaient les plus susceptibles d'avoir leurs données chiffrées : 65 % des attaques contre des organisations comptant entre 3 001 et 5 000 employés ont entraîné un chiffrement des données, soit le taux de chiffrement le plus élevé parmi toutes les cohortes, toutes tailles confondues. Ces résultats semblent indiquer que les grandes entreprises sont moins aptes à détecter et à stopper l'attaque avant le chiffrement, ou à bloquer et à annuler le chiffrement malveillant que les petites organisations.

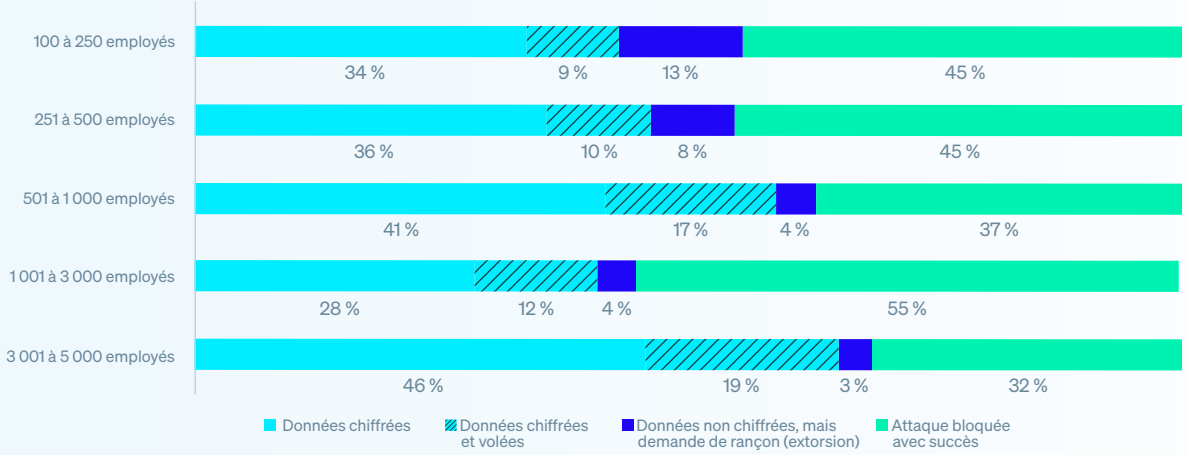
Vol de données

Les adversaires ne se contentent pas de chiffrer les données, ils les volent également. 14 % de l'ensemble des victimes de ransomware et 28 % de celles dont les données ont été chiffrées ont aussi subi un vol de données. En ventilant ces résultats par taille d'entreprise, nous constatons que les petites organisations ont près de 40 % moins de risques de se faire voler leurs données que les grandes.

- 22 % des organisations comptant entre 100 et 500 employés dont les données ont été chiffrées ont aussi été victimes d'un vol de données.
- 30 % des organisations comptant entre 501 et 5 000 employés dont les données ont été chiffrées ont aussi été victimes d'un vol de données.

S'il est possible que les petites entreprises soient plus à même de prévenir le vol de données que les grandes, cet écart tient probablement au fait que les attaquants sont plus susceptibles de tenter d'exfiltrer des données dans les grandes entreprises ou que les petites entreprises sont moins à même d'identifier un vol de données.

Graphique 7 : Taux de chiffrement des données dans les attaques de ransomware, par taille d'organisation



Lors de l'attaque de ransomware, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ? n=3 400

Attaques de type extorsion

Comme le montre le graphique 6, le pourcentage d'organisations qui n'ont pas subi de chiffrement de leurs données, mais qui ont tout de même été victimes d'une demande de rançon (extorsion) a doublé au cours de l'année dernière, atteignant 6 % des attaques en 2025 contre seulement 3 % en 2024. Les petites entreprises ont plus de chances d'être victimes d'une attaque de ransomware sans chiffrement des données (une attaque de type extorsion) que les grandes entreprises :

- 13 % des victimes comptant entre 100 et 250 employés ont essuyé une attaque de type extorsion.
- 3 % des victimes comptant entre 3 001 et 5 000 employés ont essuyé une attaque de type extorsion.

Dans l'ensemble, les organisations comptant entre 1 001 et 3 000 employés sont celles qui sont les plus aptes à gérer avec succès les effets d'une attaque de ransomware (c'est-à-dire à empêcher le chiffrement des données, à prévenir l'exfiltration de données et à éviter d'être victimes d'extorsion). Ces organisations pourraient bien se trouver dans une situation avantageuse, en ce sens qu'elles sont suffisamment grandes pour disposer d'outils et d'une expertise de haut niveau en matière de cybersécurité, sans pour autant être soumises au degré de complexité organisationnelle inhérent aux grandes entreprises.

Récupération des données chiffrées

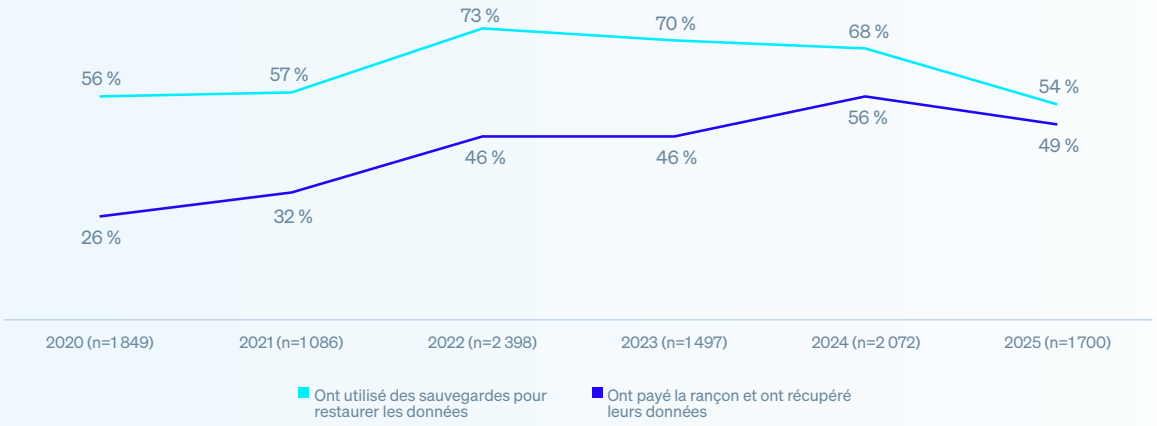
97 % des organisations dont les données ont été chiffrées sont parvenues à les récupérer.

Un peu plus de la moitié (54 %) ont pu restaurer leurs données à l'aide de sauvegardes — un chiffre en baisse pour la troisième année consécutive. Dans l'ensemble, le taux de récupération des données à partir de sauvegardes est à son plus bas niveau depuis six ans.

Un peu moins de la moitié (49 %) des entreprises ont récupéré leurs données après avoir payé la rançon. Ce chiffre, en légère baisse par rapport aux 56 % relevés l'année précédente, demeure néanmoins le deuxième taux de paiement de rançon le plus élevé depuis six ans.

29 % des entreprises ayant fait l'objet d'un chiffrement de leurs données ont déclaré avoir utilisé « d'autres moyens » pour les restaurer. Cela inclut probablement l'utilisation de clés de déchiffrement qui avaient déjà été rendues publiques.

Graphique 8 : Récupération des données via des sauvegardes et montant des rançons payées, 2020-2025



Votre entreprise a-t-elle récupéré des données ? Oui, nous avons payé la rançon et avons récupéré des données ; Oui, nous avons utilisé des sauvegardes pour restaurer les données. Chiffres de base dans le graphique.

Les rançons

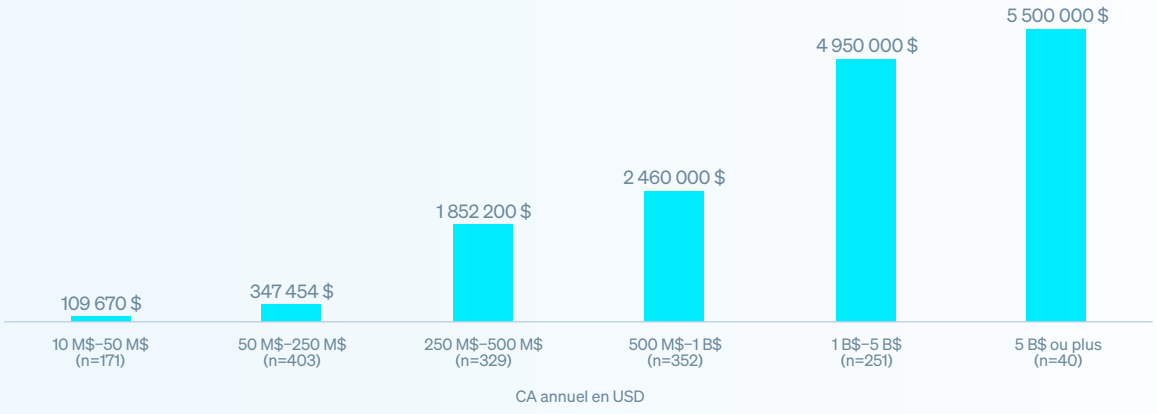
Les demandes de rançon

La demande moyenne (médiane) de rançon a diminué d'un tiers (34 %) au cours de l'année dernière, passant de 2 millions de dollars en 2024 à 1 324 439 dollars. Cette baisse s'explique en grande partie par une diminution du nombre de demandes de rançon de 5 millions de dollars ou plus, qui a diminué de 30 % à 24 %. Une bonne nouvelle, donc, mais il est important de garder à l'esprit que 57 % des demandes de rançon s'élevaient à 1 million de dollars ou plus.

Les demandes de rançon augmentent en fonction du chiffre d'affaires de l'entreprise, ce qui suggère que les adversaires « fixent le prix » de leurs demandes de rançon en fonction de la capacité de paiement perçue de leurs victimes :

- 109 670 dollars : montant médian des demandes de rançon pour les entreprises dont le chiffre d'affaires annuel est compris entre 10 et 50 millions de dollars.
- 5 500 000 $: montant médian des demandes de rançon pour les entreprises dont le chiffre d'affaires annuel est supérieur à 5 milliards de dollars.

Graphique 9 : Montant des rançons demandées, par chiffre d'affaires annuel des entreprises



Quel était le montant de la rançon demandée par les attaquants ? Chiffres de base dans le graphique.

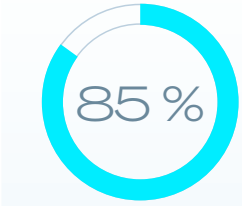
Montants des rançons payées

En ce qui concerne le montant médian des rançons payées, il a chuté de 50 % au cours de l'année dernière, passant de 2 millions de dollars en 2024 à 1 million de dollars en 2025. Comme pour les demandes de rançon, le principal facteur à l'origine de la baisse du montant médian des rançons payées est la réduction du nombre de rançons s'élevant à 5 millions de dollars ou plus, qui est passé de 31 % en 2024 à 20 % en 2025.

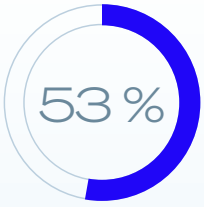
Ainsi, la réduction des montants demandés et payés observée au cours de l'année dernière est d'autant plus encourageante que ce sont les paiements qui ont connu la plus forte baisse. Cela dit, un million de dollars reste une somme très importante, qui aura des conséquences majeures pour la plupart des organisations.

Qu'en est-il de la différence entre les montants initialement demandés et les montants réellement payés ?

Parmi les organisations qui ont payé la rançon, 826 ont communiqué à la fois le montant initial demandé et le montant effectivement versé. Cela nous a permis de déterminer qu'elles ont payé en moyenne 85 % du montant initial demandé. Dans l'ensemble, 53 % ont payé moins que la demande initiale, 18 % ont payé plus et 29 % ont payé la somme demandée initialement.

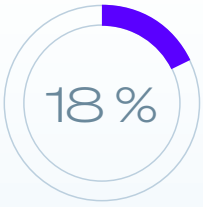


des rançons demandées **ont été payées**, en moyenne.



des paiements étaient **inférieurs** au montant initial de la rançon demandée.

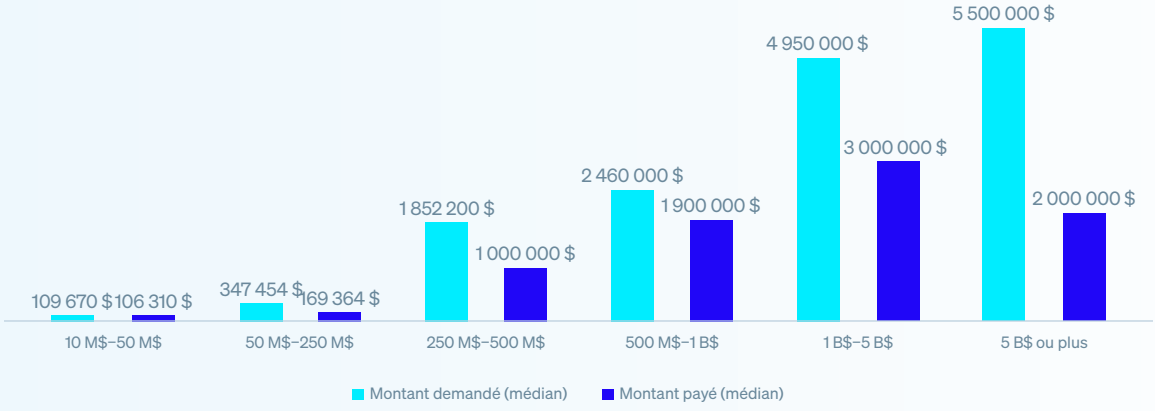
des paiements **correspondaient** au montant initial demandé.



des paiements étaient **supérieurs** au montant initial de la rançon demandée.

En ventilant les données par chiffre d'affaires annuel, il apparaît que toutes les cohortes ont payé, en moyenne, un montant inférieur à la demande initiale. Cependant, ce sont les organisations générant les chiffres d'affaires les plus importants (5 milliards de dollars ou plus par an) qui ont enregistré la plus forte baisse, leur paiement moyen réel (2 millions de dollars) ne représentant que 36 % de la demande initiale (5,5 millions de dollars), hors valeurs aberrantes. Inversement, les organisations dont le chiffre d'affaires annuel se situe entre 10 et 50 millions de dollars ont déclaré la plus faible diminution, leur paiement médian s'établissant à 97 % de la demande médiane.

Graphique 10 : Montant demandé VS montant payé, par chiffre d'affaires annuel des entreprises



Quel était le montant de la rançon demandée par les attaquants ? Quel était le montant de la rançon payée aux attaquants ? (n=1 552/836)

Pourquoi la plupart des montants payés diffèrent de la somme initialement demandée

Cette année, pour la première fois, nous avons cherché à comprendre pourquoi certaines organisations paient plus que la somme initialement demandée et d'autres moins. Ce que nous avons découvert met en lumière un aspect important à prendre en compte lors d'une attaque de ransomware.

151 organisations qui ont **payé davantage** que la demande initiale ont révélé que :

- 50 % : les attaquants étaient convaincus que nous pouvions nous permettre de payer davantage.
- 48 % : les attaquants ont compris que nous constituions une cible de grande valeur.
- 38 % : les attaquants ont fini par s'énerver et ont augmenté le prix.
- 38 % : nos sauvegardes n'ont pas fonctionné ou ont été défaillantes.
- 32 % : nous n'avons pas payé assez rapidement, donc le prix a augmenté.

Les organisations ont généralement cité deux facteurs justifiant leur décision de payer davantage, révélant ainsi les multiples difficultés auxquelles les victimes se heurtent lorsqu'elles tentent de récupérer leurs données.

445 organisations ayant payé moins que la demande initiale ont expliqué comment elles sont parvenues à réduire leur paiement :

- 47 % : nous avons réussi à négocier un montant inférieur avec les attaquants.
- 45 % : les attaquants ont réduit leur demande en raison de pressions externes (par exemple, de la part des médias ou des forces de l'ordre).
- 45 % : les attaquants ont réduit leur demande pour nous inciter à payer.
- 43 % : nous avons rapidement payé la rançon, ce qui nous a permis d'obtenir une réduction.
- 40 % : une partie tierce a réussi à négocier un montant inférieur avec les attaquants.

Cette cohorte a également cité, en moyenne, deux facteurs explicatifs du montant moins élevé de la rançon versée, soulignant davantage la situation complexe et multiforme à laquelle sont confrontées les victimes de ransomware.

Répercussions économiques des ransomwares

Coûts de rétablissement

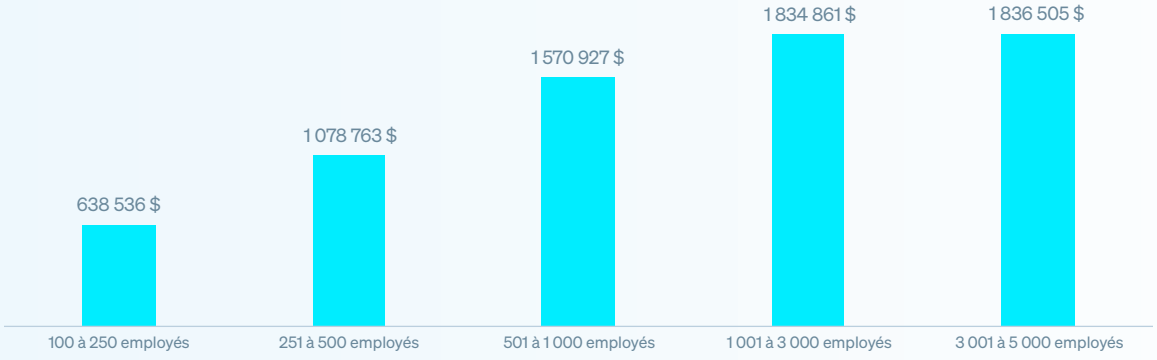
Le coût moyen de remédiation d'une attaque de ransomware (hors paiement de la rançon) a baissé de 44 % au cours de l'année dernière, passant de 2,73 millions de dollars en 2024 à 1,53 million de dollars. Il est également inférieur de plus de 300 000 dollars au montant déclaré en 2023.

2023	2024	2025
1,82 Million $	2,83 Millions $	1,53 Million $

Quel était le coût approximatif payé par votre organisation pour remédier aux conséquences de l'attaque de ransomware la plus significative (en prenant en compte les interruptions de services, le temps passé à résoudre l'incident, les coûts matériels, les pertes d'exploitation, etc.) sans compter les montants versés pour la rançon ? n=3 400 (2025), 2 974 (2024), 1 974 (2023)

Les coûts de rétablissement tendent à croître en fonction de la taille de l'organisation jusqu'à atteindre un plateau pour les organisations comptant entre 1 000 et 5 000 employés. Les entreprises comptant entre 100 et 250 employés font état d'un coût moyen de rétablissement de 638 536 dollars, tandis que celles comptant entre 1 000 et 5 000 employés ont engagé 1,83 million de dollars.

Graphique 11 : Coût de rétablissement après une attaque de ransomware, en fonction de la taille de l'entreprise

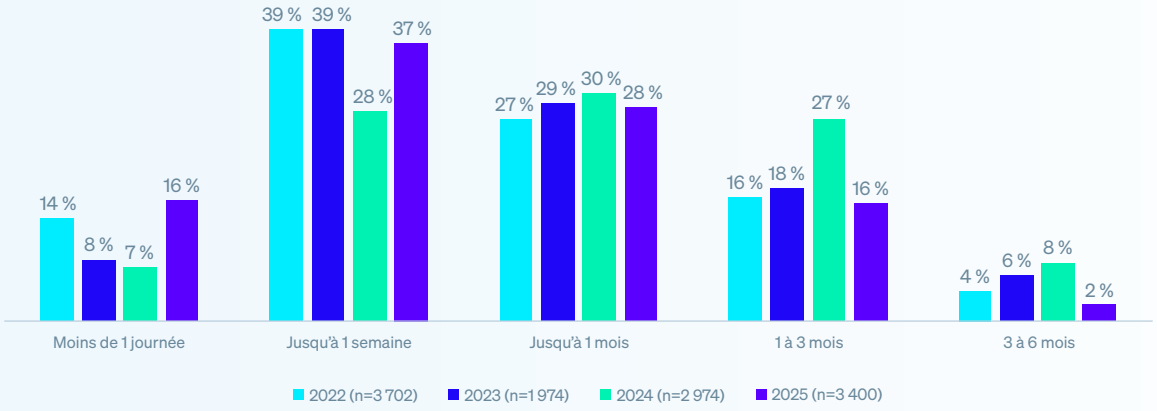


Quel était le coût approximatif payé par votre entreprise pour remédier aux conséquences de l'attaque de ransomware la plus significative (en prenant en compte les interruptions de services, le temps passé à résoudre l'incident, les coûts matériels, les pertes d'exploitation, etc.) sans compter les montants versés pour la rançon ? n=3 400

Temps de rétablissement

Les données révèlent que les organisations mettent moins de temps à se remettre des attaques, 16 % d'entre elles se sont entièrement rétablies en une journée, contre 7 % en 2024 et 8 % en 2023. Plus de la moitié (53 %) des organisations se sont rétablies en moins d'une semaine, un bond significatif par rapport aux 35 % enregistrés en 2024. Dans l'ensemble, presque toutes les victimes (97 %) étaient complètement rétablies trois mois après l'attaque. Cette accélération du processus de rétablissement pourrait indiquer que les organisations ont investi dans la préparation aux cyber incidents et dans la mise en place de dispositifs de rétablissement au cours de l'année écoulée.

Graphique 12 : Temps de rétablissement après une attaque de ransomware, 2022-2025



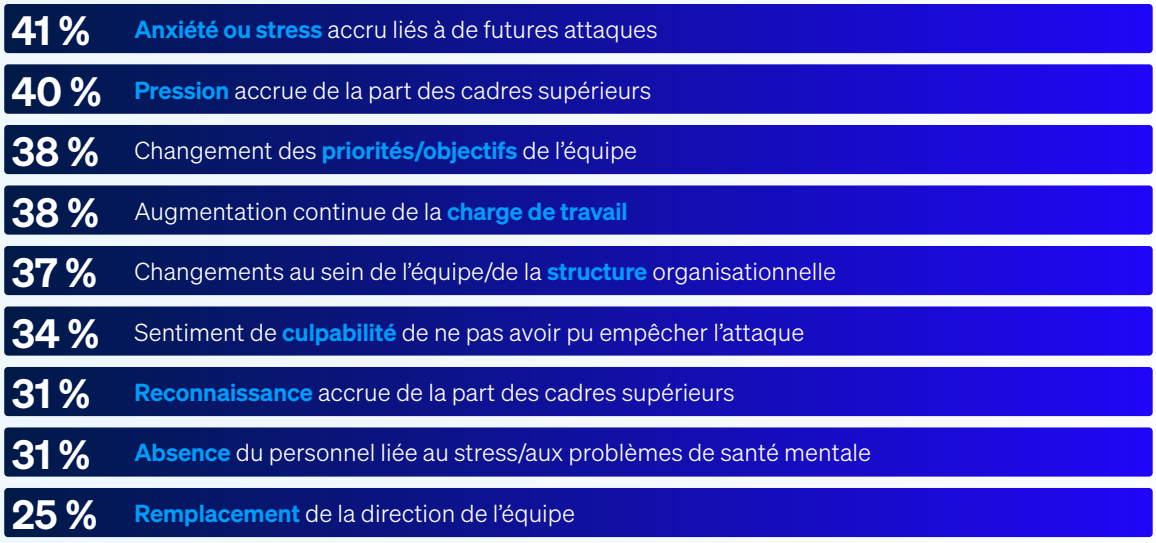
Combien de temps a-t-il fallu à votre organisation pour se rétablir complètement après l'attaque de ransomware ? Chiffres de base dans le graphique.

Sans grande surprise, les organisations ayant subi un chiffrement de données ont généralement mis plus de temps à se remettre que celles qui sont parvenues à stopper le chiffrement : 9 % des entreprises dont les données ont été chiffrées ont pu les récupérer intégralement en une journée, alors que ce chiffre s'élève à 24 % pour les organisations dont les attaquants n'ont pas réussi à chiffrer les données.

Répercussions humaines des ransomwares

L'enquête montre clairement que le chiffrement des données lors d'une attaque de ransomware a des répercussions importantes pour l'équipe informatique/cybersécurité, puisque tous les répondants ont déclaré que leur équipe avait été affectée d'une manière ou d'une autre.

Graphique 13 : Les conséquences du chiffrement des données pour les équipes informatiques et de cybersécurité



Quelles ont été les répercussions de l'attaque de ransomware sur les membres de votre équipe informatique/cybersécurité, le cas échéant ? n=1 700

Recommandations

Même si les expériences des organisations en matière de ransomware ont changé à plusieurs égards au cours de l'année dernière, ce type de menace reste très préoccupant pour toutes les organisations. Tandis que les adversaires continuent de multiplier et de faire évoluer leurs attaques, il est essentiel que les défenseurs ne soient pas pris de vitesse et que leurs cyberdéfenses évoluent au même rythme que les ransomwares et autres menaces. Nous vous invitons à tirer parti des informations contenues dans ce rapport pour renforcer vos défenses, améliorer vos capacités de réponse aux menaces et limiter l'impact des ransomwares sur votre entreprise et vos équipes. Concentrez-vous sur ces quatre domaines clés pour garder une longueur d'avance sur les attaquants :

- **Prévention**. La meilleure défense contre les ransomwares est celle qui empêche toute tentative d'attaque, car les adversaires ne parviennent pas à pénétrer dans votre organisation. Prenez des mesures pour éliminer les causes techniques et opérationnelles mises en évidence dans ce rapport.
- **Protection**. Il est impératif de disposer d'outils de sécurité de base performants. Les systèmes endpoint (dont les serveurs) sont la cible principale des auteurs de ransomwares, c'est pourquoi il faut vous assurer que ceux-ci sont bien protégés, y compris par une protection anti-ransomware dédiée pour bloquer et annuler tout processus de chiffrement malveillant.
- **Détection et réponse**. Pour assurer une issue plus favorable, il est essentiel de stopper une attaque le plus tôt possible. Un service de détection et de réponse aux menaces fonctionnant 24 heures sur 24 constitue désormais une couche de défense essentielle. Si vous ne disposez pas des ressources ou des spécialistes nécessaires pour mettre en place cette solution en interne, envisagez de faire appel à un fournisseur de services MDR (Managed Detection and Response) de confiance.
- **Planification et préparation**. En disposant d'un plan de réponse aux incidents que vous savez parfaitement mettre en œuvre, vous améliorerez considérablement vos résultats si le pire se produit et que vous êtes victime d'une attaque de grande ampleur. Assurez-vous de réaliser des sauvegardes qualitatives et de vous entraîner régulièrement à effectuer des restaurations de données à partir de ces sauvegardes afin d'accélérer le processus de récupération en cas de problème.

Pour découvrir comment Sophos peut vous aider à optimiser vos défenses contre les ransomwares, contactez un conseiller ou visitez le site www.sophos.fr

Apprenez-en plus sur les ransomwares et sur la façon dont Sophos peut vous aider à protéger votre organisation.

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.

© Copyright 2025. Sophos Ltd. Tous droits réservés.
Immatriculée en Angleterre et au Pays de Galles N° 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Royaume-Uni.
Sophos est la marque déposée de Sophos Ltd. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

2025-06-26 WP (DD)

SOPHOS