SOPHOS

L'ÉTAT DES RANSOMWARES DANS LES GRANDES ENTREPRISES EN 2025

Résultats d'une enquête indépendante menée auprès de 1733 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. Décembre 2025

Introduction

Nous vous présentons le tout premier rapport Sophos sur l'état des ransomwares dans les grandes entreprises, qui dévoile la réalité des ransomwares pour les organisations de plus de 1000 employés en 2025.

Ce rapport dévoile l'évolution des expériences des grandes entreprises face aux ransomwares (tant les causes que les conséquences) au cours de l'année écoulée. Il met également en lumière les facteurs opérationnels qui ont exposé les grandes entreprises aux attaques et l'impact humain des incidents sur les équipes informatiques et de cybersécurité.

Ce rapport est basé sur les expériences concrètes de 1733 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 :

- Comment les grandes entreprises se retrouvent victimes d'un ransomware.
- Ce qu'il advient des données.
- Le montant de la rançon demandée et le montant payé.
- L'impact économique des ransomwares.
- L'impact humain des ransomwares.

À propos de l'enquête

Ce rapport s'appuie sur les résultats d'une enquête indépendante commandée par Sophos sur les expériences des entreprises face aux ransomwares. L'enquête a été menée par un spécialiste externe entre janvier et mars 2025. Tous les répondants travaillent au moment de l'enquête dans des grandes entreprises comptant entre 1000 et 5000 employés et ont été invités à répondre en se basant sur leur expérience au cours des 12 derniers mois.

Les 1733 grandes entreprises qui ont répondu à l'enquête et contribué à ce rapport sont réparties dans 17 pays, preuve que les résultats de l'enquête reflètent un éventail d'expériences large et varié. Ce rapport établit des comparatifs avec résultats tirés des données 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.

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 et répercussions mentionnées se sont produites en 2024.

Principales découvertes

Comment les grandes entreprises se retrouvent victimes d'un ransomware

- **L'exploitation de vulnérabilités** est la cause première technique la plus fréquemment citée, utilisée dans 29 % des incidents. **Le phishing** et les **identifiants** compromis suivent de près, chacun cité dans 21 % des incidents.
- De multiples facteurs opérationnels contribuent à l'exposition des grandes entreprises aux ransomwares, le plus courant étant une **faille de sécurité inconnue**, cité par 40 % des victimes. Il est suivi de très près par un **manque de personnel/capacités** et un **manque d'expertise**, qui ont joué un rôle dans 39 % des attaques.

Ce qu'il advient des données

- Le taux de chiffrement des données dans les grandes entreprises est à son niveau le plus bas depuis cinq ans : **49 % des attaques se soldent désormais par un chiffrement malveillant**, contre un niveau record de 64 % en 2022.
- 30 % des grandes entreprises dont les données ont été chiffrées ont également subi une exfiltration de données.
- 96 % des grandes entreprises dont les données ont été chiffrées sont parvenues à les récupérer.
- L'utilisation de sauvegardes par les grandes entreprises pour restaurer des données chiffrées est à son plus bas niveau depuis quatre ans, puisqu'elles sont utilisées dans 53 % des incidents.
- **48 % des grandes entreprises victimes d'un ransomware ont payé la rançon** pour récupérer leurs données, ce qui représente l'un des taux les plus bas enregistrés dans l'enquête de cette année.

Rançons : montants demandés et montants payés

- Le montant médian des **rançons demandées** aux grandes entreprises a chuté de 56 % l'année dernière, passant de 2,75 millions de dollars en 2024 à **1,20 million de dollars** cette année. Le principal facteur expliquant ce recul significatif est la baisse de 24 % du nombre de demandes de rançon supérieures à 5 millions de dollars, qui est passé de 38 % des demandes en 2024 à 29 % en 2025. Cependant, il est important de noter que le nombre de demandes comprises entre 1 et 5 millions de dollars a augmenté de 17 %.
- La **rançon moyenne (médiane) payée** par les grandes entreprises a également diminué, atteignant **1 million de dollars** en 2025 contre 1,26 million en 2024. Ce recul s'explique en grande partie par une diminution de 37 % du pourcentage des rançons payées dont le montant est supérieur ou égal à 5 millions de dollars. Il convient toutefois de souligner que des augmentations ont été observées dans presque toutes les tranches de paiements inférieures à 5 millions de dollars.
- La **proportion du montant des demandes de rançons payées** par les grandes entreprises est passée de 95 % en 2024 à 86 % en 2025.
- Lorsque l'on compare le **montant demandé au montant effectivement payé**, on s'aperçoit qu'ils coïncident dans près d'un tiers des cas (31 %). 51 % ont payé moins que la demande initiale, tandis que 18 % ont payé plus.

L'impact économique des ransomwares

- Le **coût moyen de rétablissement après une attaque de ransomware pour les grandes entreprises** a baissé de 41 % au cours de l'année dernière, passant de 3,12 millions de dollars en 2024 à **1,84 million de dollars**.
- Par ailleurs, les grandes entreprises ont tendance à **se remettre plus rapidement d'une attaque** : en 2025, exactement la moitié d'entre elles se sont rétablies après une semaine, contre 36 % l'année précédente.

L'impact humain des ransomwares

Toutes les grandes entreprises dont les données ont été chiffrées ont signalé que cette situation avait eu des répercussions directes sur leur équipe informatique/cybersécurité :

- 40 % des équipes informatique/cybersécurité font état d'une **pression accrue** de la part des cadres supérieurs, tandis que 31 % signalent une **reconnaissance accrue**.
- 39 % ont signalé à la fois une **augmentation continue de la charge de travail** et une **augmentation de l'anxiété ou du stress** à l'égard de futures attaques.
- 37 % ont rapporté un **changement de priorités/objectifs de l'équipe**.
- Plus d'un tiers des personnes interrogées (35 %) ont mentionné à la fois un **sentiment de culpabilité** de ne pas avoir pu empêcher l'attaque et des **changements au sein de l'équipe/de la structure organisationnelle** découlant directement de l'incident.
- 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 peu plus d'un quart des cas (27 %), la **direction de l'équipe a été remplacée** à cause de l'attaque.

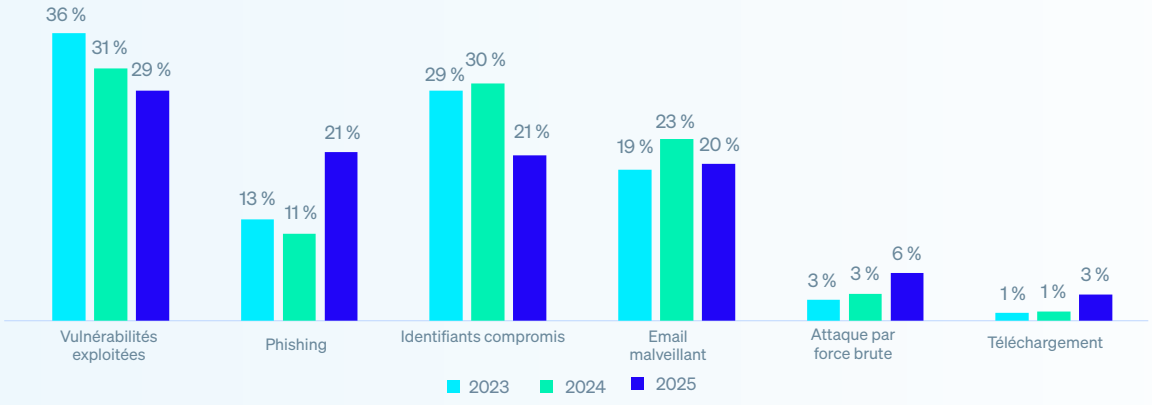
Comment les grandes entreprises se retrouvent victimes d'un ransomware

Les principales causes techniques des attaques dans les grandes entreprises

Pour la troisième année consécutive, les grandes entreprises ont identifié l'**exploitation de vulnérabilités** comme étant la principale cause des attaques de ransomware, présentes dans 29 % des incidents. Les **emails de phishing** arrivent en deuxième position, leur part passant de 11 % en 2024 à 21 % en 2025.

Les attaques basées sur des vols d'identifiants continuent de poser un risque important, bien que ce vecteur d'attaque ait considérablement diminué, passant de 30 % en 2024 à 21 % en 2025. En revanche, les **petites et moyennes entreprises** (celles qui comptent entre 100 et 250 employés) ont cité les attaques basées sur des vols d'identifiants comme la principale cause des attaques de ransomware, responsable de près d'un tiers (30 %) des incidents.

Graphique 1 : Causes premières techniques des attaques de ransomware dans les grandes entreprises, 2023-2025

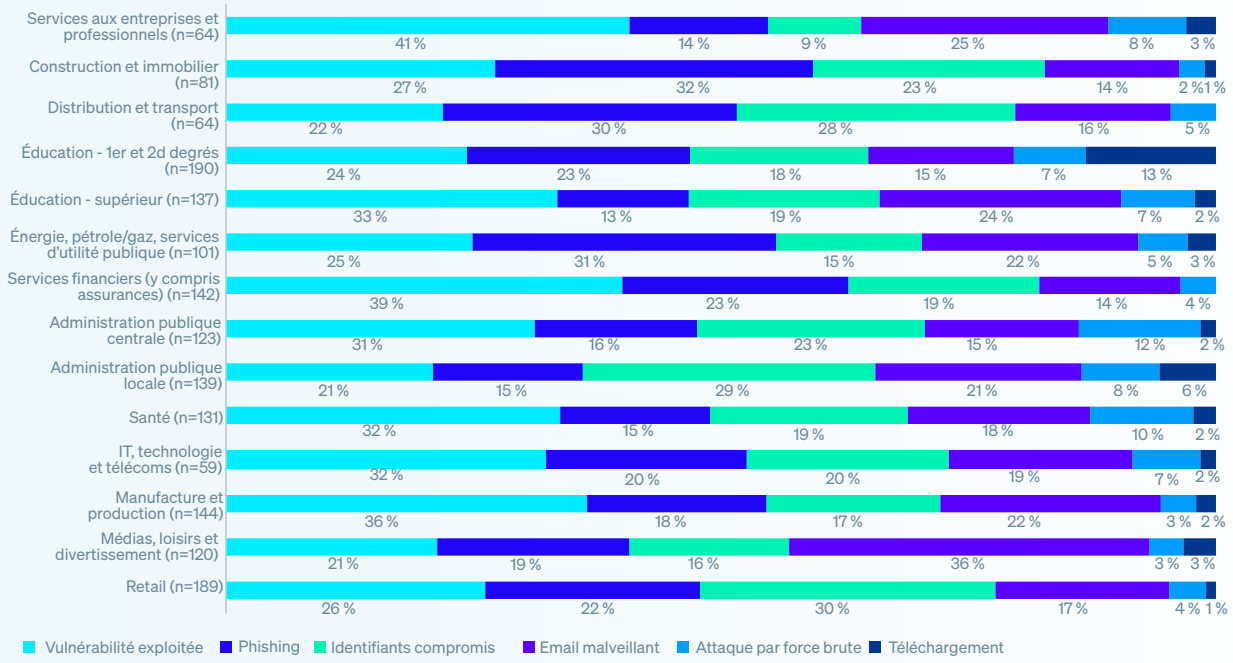


Connaissez-vous la cause première de l'attaque de ransomware dont votre entreprise a été victime au cours de l'année écoulée ? Oui. n=1733 (2025), 1409 (2024), 1045 (2023)

L'enquête révèle que, bien que les causes premières varient d'un secteur à l'autre, les vulnérabilités exploitées constituent un vecteur d'attaque majeur pour les grandes entreprises dans presque tous les secteurs. Exceptions notables :

- **Le phishing** est la cause première la plus fréquemment citée à la fois par les prestataires des secteurs de la **construction et de l'immobilier** (32 %), de la **distribution et des transports** (30 %) et de l'**énergie, du pétrole/gaz et des services d'utilité publique** (31 %).
- Les **identifiants compromis** ont été le vecteur d'attaque le plus observé par les grandes entreprises du **retail**, représentant près d'un tiers des incidents (30 %).

Graphique 2 : Causes premières techniques des attaques de ransomware par secteur

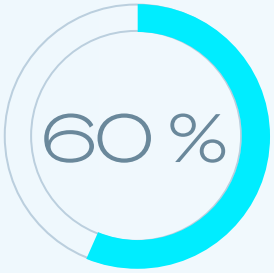


Connaissez-vous la cause première de l'attaque de ransomware dont votre entreprise a été victime au cours de l'année écoulée ? Oui. Chiffres de base dans le graphique.

Les principales causes organisationnelles des incidents dans les grandes entreprises

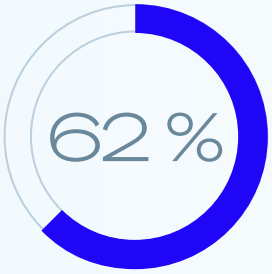
Outre les causes premières techniques des incidents, il est également important de comprendre les facteurs organisationnels qui ont exposé les grandes entreprises à des attaques. Les résultats révèlent que les victimes de ce secteur sont généralement confrontées à de multiples difficultés organisationnelles. En moyenne, les personnes interrogées citent 3 facteurs ayant permis une attaque.

Dans l'ensemble, les causes profondes organisationnelles sont uniformément réparties entre les problèmes de protection, les contraintes en matière de ressources et les failles de sécurité. Cependant, les grandes entreprises ont légèrement plus tendance à évoquer une faille de sécurité (connue ou inconnue) comme facteur principal.



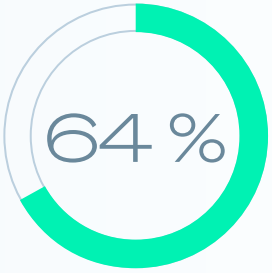
SOLUTION DE PROTECTION MANQUANTE/DE MAUVAISE QUALITÉ

Manque de protection ou solutions de protection de mauvaise qualité qui n'ont pas pu bloquer l'attaque



MANQUE DE PERSONNEL/ COMPÉTENCES

Manque d'expertise humaine (compétences ou capacités) pour détecter et bloquer l'attaque à temps



FAILLE DE SÉCURITÉ (CONNUE/INCONNUE)

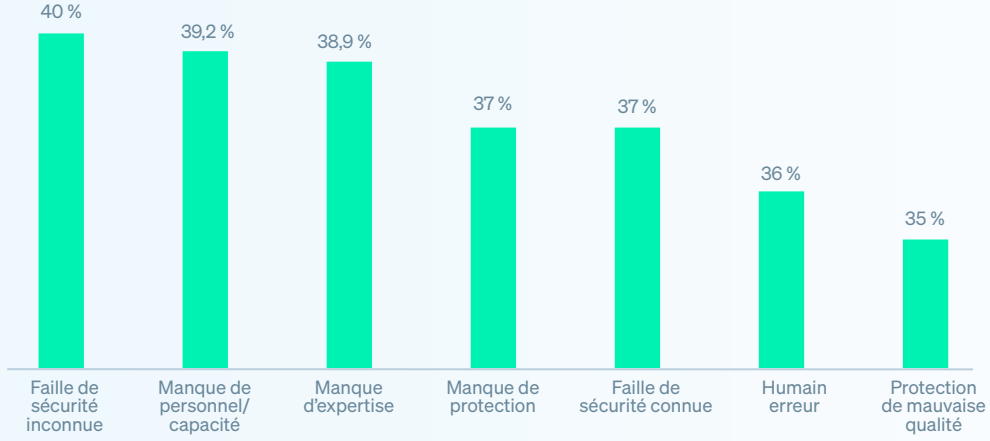
Avaient une faille connue ou inconnue dans leurs défenses

Selon vous, pourquoi votre organisation a-t-elle été victime d'une attaque de ransomware? n=1733. Réponses consolidées.

Les failles de sécurité inconnues (c'est-à-dire les faiblesses dans les défenses dont les répondants n'avaient pas connaissance) sont la raison la plus fréquemment citée, mentionnée par 40 % des entreprises interrogées. Elles sont suivies de près par un **manque de personnel/capacités** (c'est-à-dire un nombre insuffisant d'experts en cybersécurité surveillant les systèmes au moment de l'attaque) et un **manque d'expertise** (c'est-à-dire des compétences ou des connaissances insuffisantes pour détecter et bloquer l'attaque à temps), qui ont été identifiés comme des facteurs contributifs par 39 % des entreprises.

Il est intéressant de noter que les **PME** ont également identifié le **manque de personnel/capacités** comme un facteur commun, 42 % d'entre elles le citant comme l'une des principales raisons pour lesquelles elles ont été victimes d'une attaque, soulignant ainsi que les contraintes en matière de ressources restent un défi courant, quelle que soit la taille de l'organisation.

Graphique 3 : Causes premières opérationnelles des attaques de ransomware dans les grandes entreprises



Selon vous, pourquoi votre organisation a-t-elle été victime d'une attaque de ransomware? n=1733.

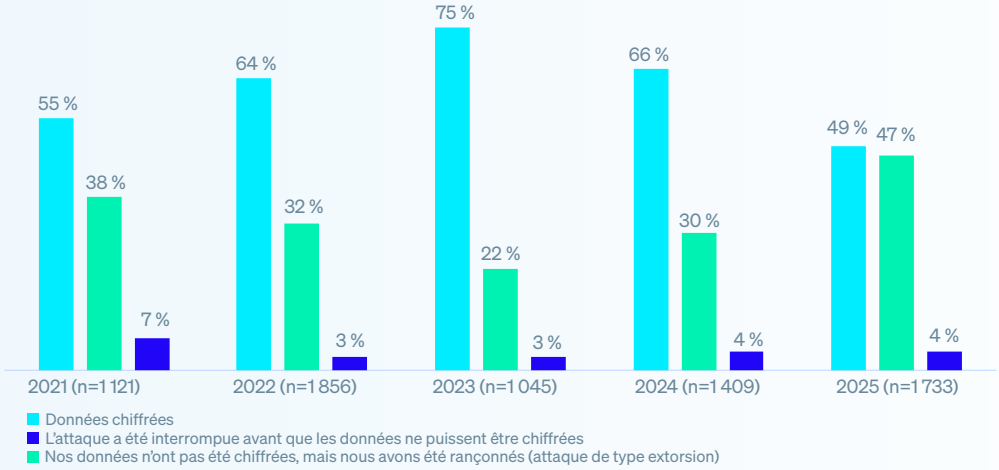
Ce qu'il advient des données

Chiffrement des données dans les grandes entreprises

Il est encourageant de constater que le taux de chiffrement des données dans les grandes entreprises est à son plus bas niveau depuis cinq ans, moins de la moitié (49 %) des attaques ayant entraîné un chiffrement des données, contre 66 % en 2024.

Par ailleurs, le pourcentage d'attaques de ransomware neutralisées avant le chiffrement des données a plus que doublé au cours des deux dernières années, passant de 22 % en 2023 à 47 % en 2025. Ces chiffres suggèrent que les grandes entreprises parviennent de mieux en mieux à détecter et bloquer les attaques avant qu'elles ne causent de graves dommages.

Graphique 4 : Taux de chiffrement des données des attaques de ransomware dans les grandes entreprises, 2021-2025

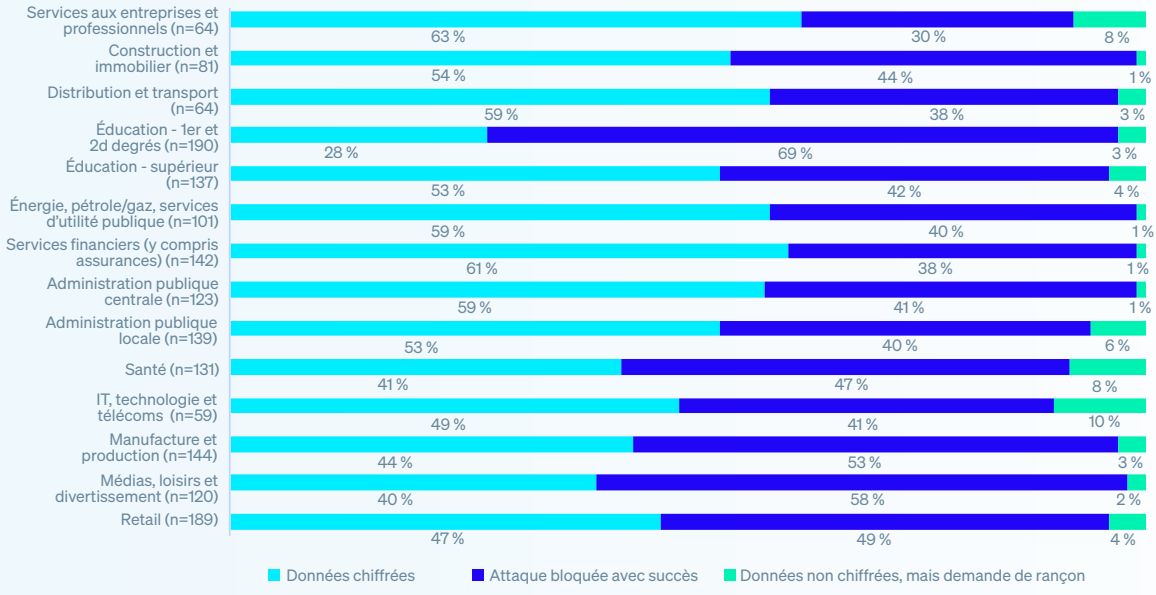


Lors de l'attaque par ransomware, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise? Chiffres de base dans le graphique.

Taux de chiffrement des données par secteur

Les grandes entreprises du secteur des **services aux entreprises et professionnels** sont les plus susceptibles de faire l'objet d'un chiffrement de données (63 %), ce qui indique que les entreprises de ce secteur sont moins efficaces pour détecter et bloquer les attaques avant le chiffrement ou sont moins aptes à bloquer et à annuler les processus de chiffrement malveillant. À l'inverse, les établissements du secteur de l'**enseignement des 1er et 2nd degrés** ont fait état du taux de chiffrement de données le plus faible, à seulement 28 %.

Graphique 5 : Taux de chiffrement des données dans les grandes entreprises, par secteur d'activité



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

Vol de données

Les adversaires ne se contentent pas de chiffrer les données, ils les volent. Parmi les grandes entreprises, 15 % de l'ensemble des victimes de ransomware et 30 % de celles dont les données ont été chiffrées ont aussi subi un vol de données. En ventilant ces données par secteur d'activité, nous constatons que :

- Dans la partie supérieure, 52 % des grandes entreprises du secteur des **médias, des loisirs et du divertissement** ayant été confrontées à un chiffrement des données malveillant ont également subi un vol de données.
- En revanche, seuls 11 % des grandes entreprises du secteur de la **construction et de l'immobilier** ont été confrontées à des vols de données parallèlement au chiffrement.

Attaques de type extorsion

Comme le montre le graphique 4, la proportion de grandes entreprises qui n'ont pas chiffré leurs données, mais qui ont tout de même été victimes d'une demande de rançon est restée stable d'une année sur l'autre, à 4 %. Si l'on considère les différents secteurs d'activité, les entreprises du secteur de **l'informatique, de la technologie et des télécoms** ont été les plus exposées à ce type d'attaque (10 %), tandis que les entreprises des secteurs de la **construction et de l'immobilier, de l'énergie, du pétrole/gaz, des services d'utilité publique, des services financiers et des administrations publiques centrales** ont été les moins touchées, avec seulement 1 % de cas signalés.

Dans l'ensemble, les grandes entreprises du secteur de l'**enseignement des 1er et 2nd degrés** 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'une extorsion). Ce qui signifie que ces prestataires se montrent étonnamment efficaces en matière de détection précoce et d'intervention, malgré des budgets limités.

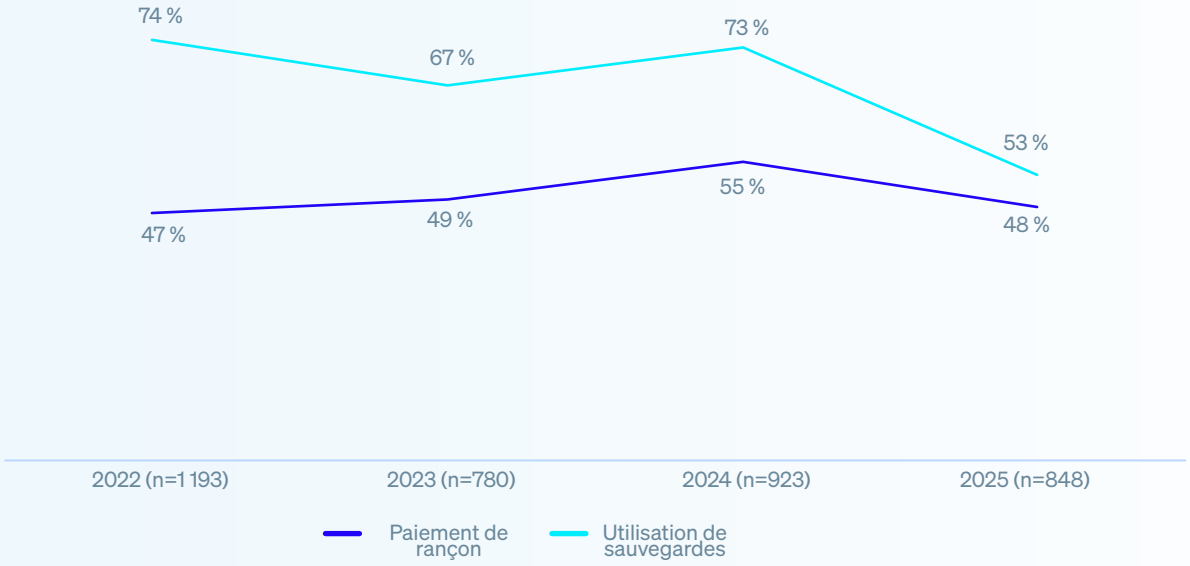
Récupération des données chiffrées dans les grandes entreprises

96 % des grandes entreprises dont les données ont été chiffrées sont parvenues à les récupérer.

En 2025, 48 % des grandes entreprises ont **payé la rançon pour récupérer leurs données** — contre 55 % en 2024. Dans le même temps, l'**utilisation de sauvegardes** a fortement chuté à son plus bas niveau en quatre ans (53 %, contre 73 % en 2024). Collectivement, ces résultats témoignent d'une résistance accrue au rançonnement, ainsi que des faiblesses et sans doute un manque de confiance dans la résilience des sauvegardes.

De plus, le moindre écart entre les grandes entreprises qui paient la rançon en vue de récupérer leurs données et ceux qui utilisent des sauvegardes pour restaurer leurs données suggère une dépendance croissante à l'égard de méthodes de récupération multiples ou alternatives. Pour preuve, nous avons constaté que près d'un tiers (30 %) des grandes entreprises dont les données ont été chiffrées ont déclaré avoir **utilisé d'autres moyens pour restaurer leurs données**. D'autres méthodes pourraient inclure la restauration à partir de clichés instantanés, l'utilisation des fonctionnalités de restauration incluses dans la protection Endpoint ou la récupération des données à partir de systèmes non affectés.

Graphique 6 : Récupération des données chiffrées dans les grandes entreprises, 2021-2025



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.

Rançons

Demandes de rançon dans les grandes entreprises

Le montant médian des rançons demandées aux grandes entreprises a chuté de 56 % l'année dernière, passant de 2,75 millions de dollars en 2024 à 1,20 million de dollars cette année. La baisse des demandes de rançon visant les acteurs de ce secteur résulte en grande partie d'une diminution de 24 % des demandes de 5 millions de dollars ou plus au cours de l'année dernière. Cependant, il est important de noter que le nombre de demandes comprises entre 1 et 5 millions de dollars a augmenté de 17 %, représentant 27 % des demandes, contre 23 % en 2024.

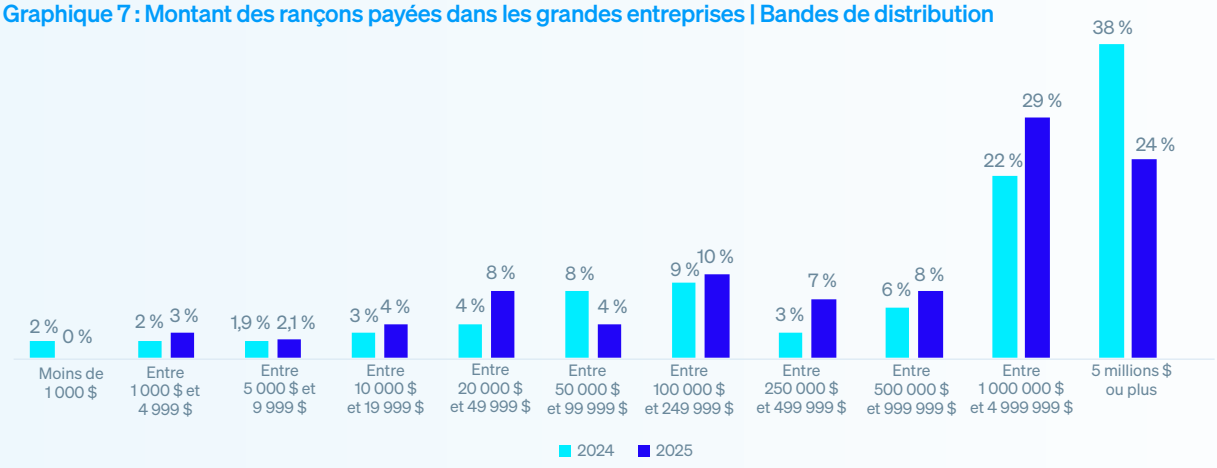
Montants de la rançon payés dans les grandes entreprises

Suivant cette tendance, le montant moyen (médian) des rançons versées par les grandes entreprises a lui aussi diminué, passant de 1,26 million de dollars en 2024 à 1 million de dollars en 2025. Ce résultat s'explique en grande partie par une forte baisse de 37 % des paiements de 5 millions de dollars ou plus au cours de l'année dernière. Toutefois, le rapport révèle des augmentations annuelles dans presque toutes les tranches de paiement inférieures à 5 millions de dollars.

Ces tendances indiquent que les attaquants changent de mode opératoire, en délaissant les demandes de rançon les plus exorbitantes pour cibler les entreprises avec des demandes plus modérées, dont le montant reste préjudiciable, mais plus réaliste à payer.

Les **PME** ont suivi un schéma similaire, bien que la baisse des demandes et des paiements ait été encore plus marquée. Le montant médian des demandes de rançon et des paiements a considérablement diminué, passant respectivement de 2 millions de dollars en 2024 à 126 000 dollars et 200 000 dollars en 2025, ce qui renforce la tendance générale des attaquants à revoir leurs attentes à la baisse pour viser des sommes plus accessibles dans les organisations de toutes tailles.

Graphique 7 : Montant des rançons payées dans les grandes entreprises | Bandes de distribution

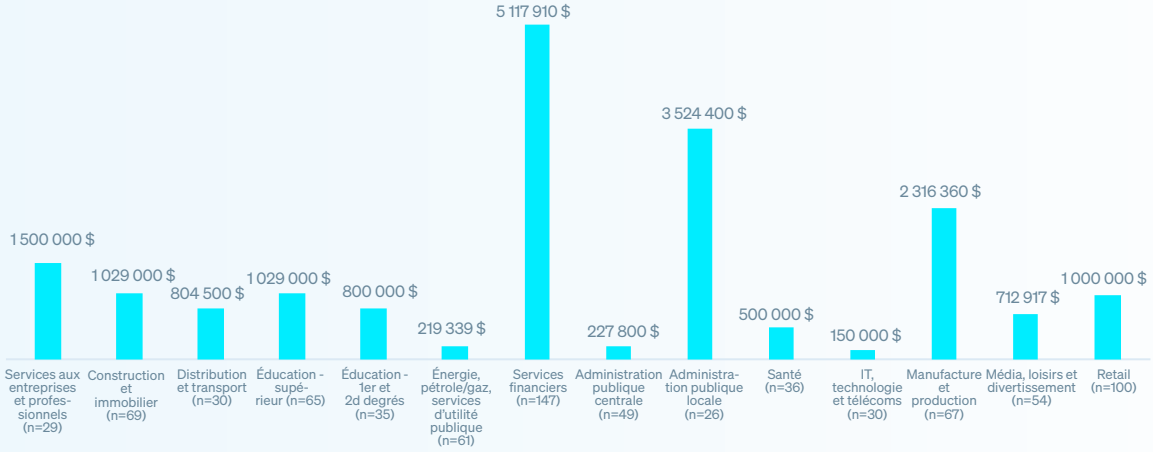


Quel était le montant de la rançon payée aux attaquants ? n=414 (2025), 470 (2024)

Montant des rançons payées par secteur

Les montants payés ont varié considérablement selon les secteurs d'activité, les entreprises du secteur des services financiers ayant payé le montant médian le plus élevé avec 5,1 millions de dollars. Cela peut être dû aux enjeux opérationnels élevés du secteur et à sa faible tolérance aux perturbations, ce qui conforte les attaquants dans l'idée que des paiements plus importants sont plus susceptibles d'être effectués.

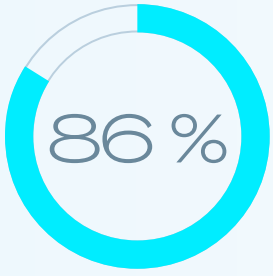
Graphique 8 : Montant des rançons payées par secteur



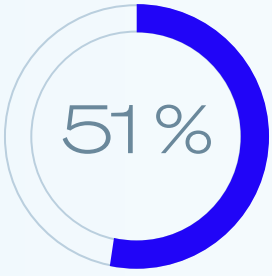
Quel était le montant de la rançon payée aux attaquants ? Chiffres de base dans le graphique. Remarque : lorsque les effectifs de base sont inférieurs à 30, les résultats doivent être considérés comme indicatifs.

Comment le montant des rançons payées par les grandes entreprises diffère-t-il du montant initialement demandé

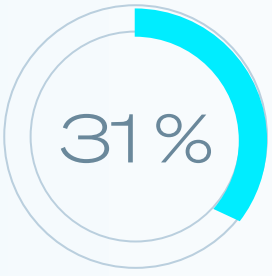
Parmi les grandes entreprises qui ont payé la rançon, 414 ont communiqué à la fois le montant initial demandé et le montant effectivement versé, ce qui révèle qu'elles ont payé en moyenne 86 % du montant initial demandé. Il s'agit là d'une baisse salutaire par rapport aux 95 % enregistrés en 2024. Dans l'ensemble, 51 % ont payé moins que la demande initiale, 18 % ont payé plus et près d'un tiers (31 %) ont payé la somme demandée initialement.



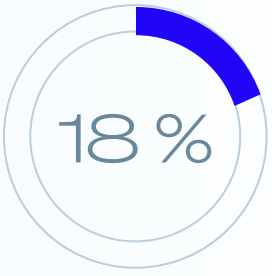
des rançons demandées **ont été payées**, en moyenne



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

Pourquoi la plupart des montants payés par les grandes entreprises diffèrent de la somme initialement demandée

L'enquête a également cherché à comprendre pourquoi certaines grandes entreprises 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.

72 entreprises qui ont **payé davantage** que la demande initiale ont révélé que :

- 61 % : les attaquants étaient convaincus que nous pouvions nous permettre de payer davantage.
- 49 % : les attaquants ont compris que nous constituions une cible de grande valeur.
- 42 % : nos sauvegardes n'ont pas fonctionné ou ont été défaillantes.
- 39 % : les attaquants ont fini par s'énerver et ont augmenté le prix.
- 31 % : nous n'avons pas payé assez rapidement, donc le prix a augmenté.

Les grandes entreprises 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.

214 entreprises ayant **payé moins** que la demande initiale ont expliqué comment elles sont parvenues à réduire leur paiement :

- 49 % : nous avons réussi à négocier un montant inférieur avec les attaquants.
- 46 % : nous avons rapidement payé la rançon, ce qui nous a permis d'obtenir une réduction.
- 45 % : les attaquants ont réduit leur demande pour nous inciter à payer.
- 43 % : les attaquants ont réduit leur demande en raison de pressions externes (par exemple, de la part des médias ou des forces de l'ordre).
- 38 % : 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 dans les grandes entreprises

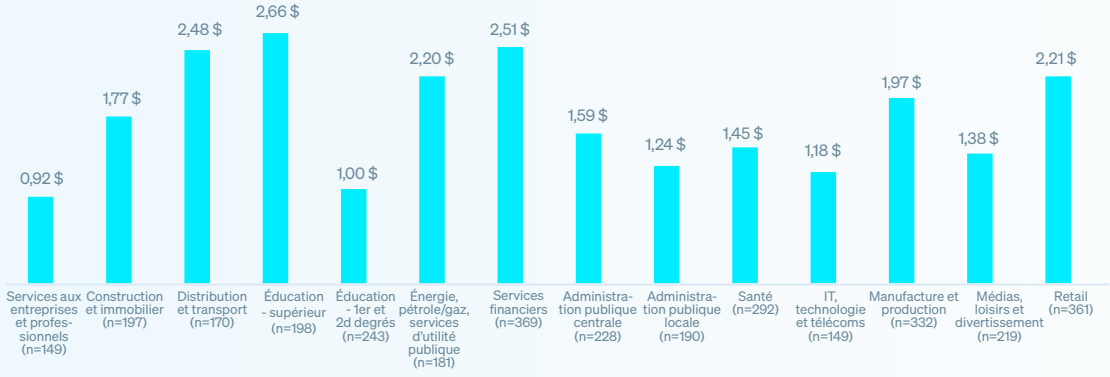
Le coût moyen de rétablissement pour les grandes entreprises après une attaque de ransomware (hors paiement de la rançon) a atteint son niveau le plus bas depuis trois ans, chutant de 41 % au cours de l'année dernière pour s'établir à 1,84 million de dollars, contre 3,12 millions de dollars en 2024. Il est également inférieur de 330 000 dollars par rapport aux 2,17 millions de dollars déclarés en 2023.

2023	2024	2025
2,17 M$	3,12 M$	1,84 M$

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=1733 (2025), 1409 (2024), 1045 (2023)

Lorsque l'on examine la répartition par secteur, les coûts de rétablissement varient considérablement. Les grandes entreprises du **secteur de l'enseignement des 1er et 2nd degrés** sont celles qui ont consenti à payer le plus pour remédier aux incidents, à savoir 2,66 millions de dollars en moyenne. En revanche, les entreprises du secteur des **services aux entreprises et professionnels** ont déclaré le coût le plus bas, soit 0,92 million de dollars. Cette différence reflète probablement en partie le niveau variable de reconstruction de l'infrastructure informatique nécessaire pour se remettre de l'attaque, les établissements d'enseignement utilisant généralement des solutions plus anciennes que les fournisseurs de services du secteur privé.

Graphique 9 : Coût de rétablissement après une attaque de ransomware par secteur d'activité (en million de dollars)

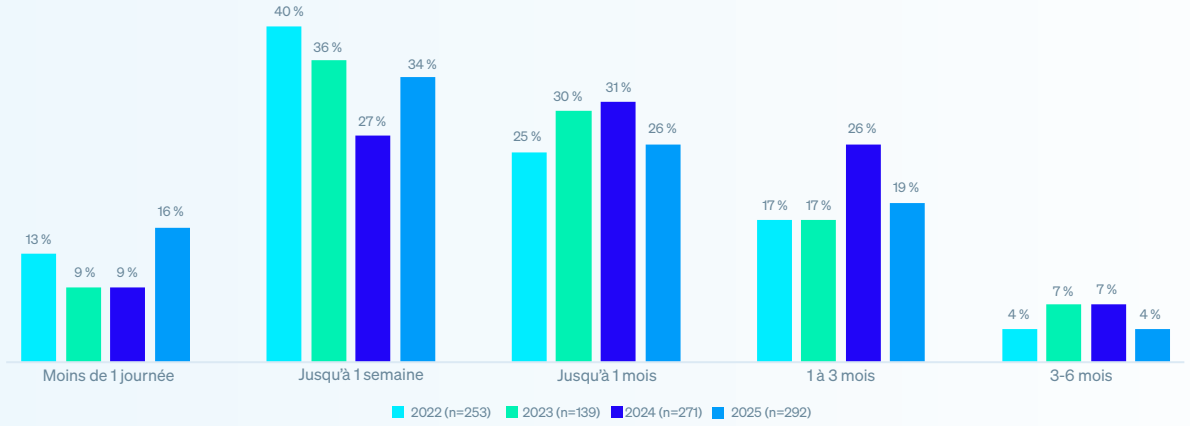


Quel était le coût approximatif payé par votre organisation pour remédier aux conséquences de l'attaque de ransomware la plus significative (en prenant en compte les interruptions de services, le temps passé à résoudre l'incident, les coûts matériels, les pertes d'exploitation, etc.) sans compter les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

Temps de rétablissement dans les grandes entreprises

Selon les données, en 2025, les grandes entreprises se rétablissent plus rapidement après une attaque de ransomware. La moitié a repris ses activités en moins d'une semaine, contre 36 % en 2024. Dans le même temps, la part de ceux qui ont mis entre un et trois mois pour se rétablir a diminué, passant de 26 % en 2024 à 19 %. Dans l'ensemble, 95 % des grandes entreprises victimes ont repris totalement leurs activités en moins de trois mois, ce qui souligne la résilience et les capacités de reprise de plus en plus grandes de l'ensemble du secteur.

Graphique 10 : Temps de rétablissement pour les grandes entreprises après une attaque de ransomware, 2022-2025

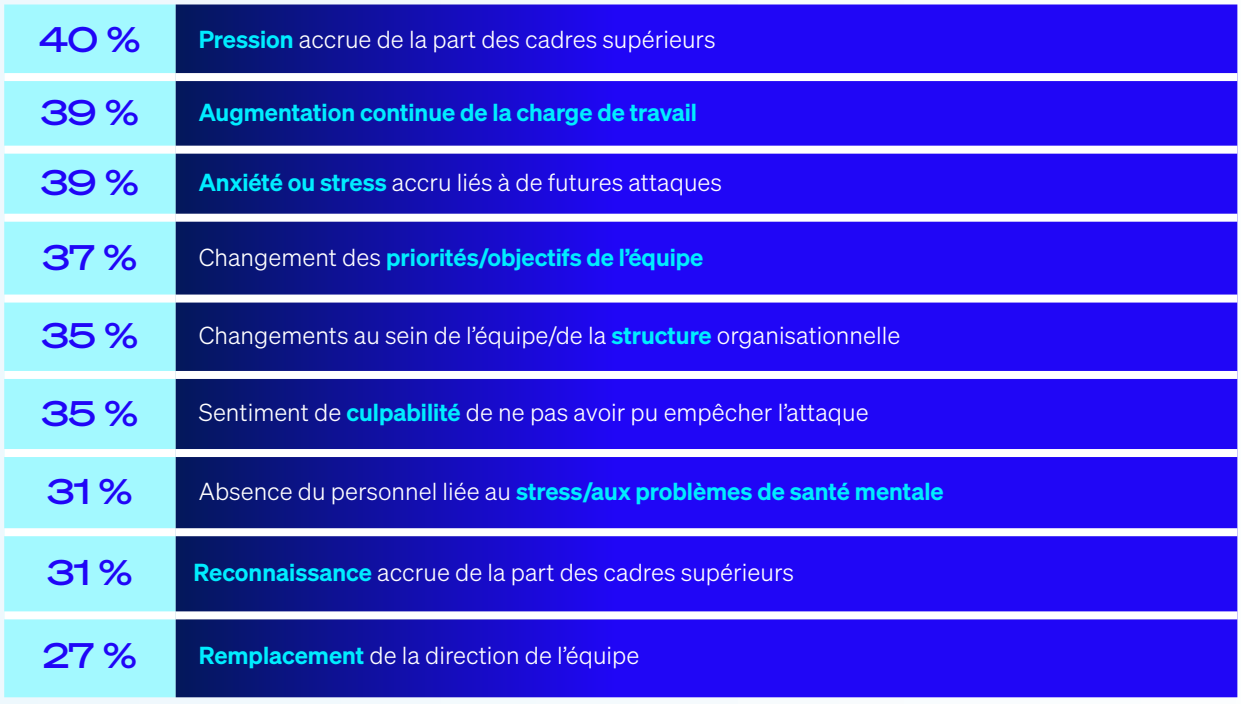


Combien de temps a-t-il fallu à votre organisation pour se rétablir complètement après l'attaque de ransomware? Chiffres de base dans le graphique.

Répercussions humaines des ransomwares

L'enquête montre clairement que le chiffrement des données lors d'une attaque de ransomware a des répercussions importantes pour les équipes informatique/cybersécurité des grandes entreprises, 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=848

Recommandations

Bien que les grandes entreprises se soient adaptées de diverses manières aux ransomwares au cours de l'année dernière, ceux-ci restent une menace importante. Tandis que les adversaires continuent 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.

2025-12-08 WP (MP)

SOPHOS