RAPPORT

L'état des ransomwares 2026

Perspectives de 2 158 responsables informatiques et cybersécurité de 17 pays

SOPHOS

Introduction

Le paysage des ransomwares évolue rapidement avec l'IA. S'il est évident que les organisations qui investissent de manière soutenue dans des défenses de cybersécurité en tirent des bénéfices concrets, les attaques de ransomware continuent toutefois de coûter des millions aux organisations.

Il s'agit de la septième édition du rapport Sophos annuel sur l'état des ransomwares, qui offre de nouvelles données sur les attaques de ransomware de l'année écoulée. Les résultats sont regroupés en différentes sections couvrant :

- Les méthodes d'attaque et de défense
- Le chiffrement et la récupération des données
- Le montant de la rançon demandée et le montant payé
- L'impact commercial et humain

Les données font état de résultats coûteux associés à de réels progrès :

- Les coûts de rétablissement après une attaque de ransomware sont élevés, la facture moyenne s'élevant désormais à 1,7 million de dollars.
- Plus de la moitié des attaques de ransomware (56 %) se soldent encore par un chiffrement de données, avec un taux en hausse par rapport à 2025.
- Cependant, le montant des demandes de rançon et des paiements diminue, et les organisations parviennent à négocier plus efficacement face aux attaquants. Au cours des deux dernières années, le montant médian des demandes a chuté de 65 % et celui des paiements de 62 %.
- Après trois ans à la première place, les vulnérabilités exploitées ne sont plus la cause première des attaques de ransomware (18 %), les attaques par email (phishing 24 % ou emails malveillants 26 %) étant désormais les vecteurs d'attaque les plus courants.

2 158

responsables informatiques et de cybersécurité issus de 17 pays, dont l'organisation a été touchée par un ransomware au cours de l'année écoulée, ont participé à une enquête mondiale et indépendante, qui a servi de base au analyses du rapport de cette année.

À propos de l'enquête

Ce rapport est basé sur les résultats d'une enquête indépendante commandée par Sophos. L'enquête a porté sur l'expérience des organisations face aux attaques de ransomware et aux intrusions basées sur l'identité, en suivant d'une année sur l'autre les taux de paiement des rançons, les coûts de rétablissement, les délais de rétablissement et de nombreux autres indicateurs. Les réponses ont été recueillies de janvier à mars 2026 et sont basées sur les expériences des répondants au cours des 12 mois précédents.

Les participants provenaient de 17 pays, d'un large éventail de secteurs d'activité tant publics que privés, et représentaient un échantillon de la taille des entreprises suivant une courbe en cloche, comprises entre 100 et 5 000 salariés, dont la répartition est restée proportionnellement constante au cours des sept années d'existence de l'enquête. Toutes les données financières sont exprimées en dollars américains.

Aperçu des principales découvertes

- **La compromission de l'identité est le principal mécanisme de distribution des ransomwares**
  - Les emails malveillants (26 %) et le phishing (24 %) sont devenus les principales causes premières des attaques de ransomware.
  - Les vulnérabilités exploitées, la principale cause première des trois dernières années, ont chuté de 14 points de pourcentage au cours de l'année passée pour atteindre 18 %.
  - Deux tiers des victimes de ransomware (67 %) ont confirmé que l'incident de ransomware correspondait également à leur attaque d'identité la plus grave.
- **Les lacunes en matière de protection, de sécurité et de ressources exposent les organisations aux attaques**
  - Les failles de sécurité (connues ou inconnues) ont été les causes premières opérationnelles les plus citées pour la deuxième année consécutive (62 %), suivies par le manque de personnel ou de compétences (58 %) et par une protection de mauvaise qualité ou absente (57 %).
- **Le seul déploiement de l'authentification multifacteur (MFA) ne suffit pas à stopper les ransomwares**
  - La MFA a été déployée dans une certaine mesure dans 97 % des incidents où des identifiants compromis étaient à l'origine des attaques de ransomware.
- **Dans plus de la moitié des incidents, les organisations ne sont pas parvenues à détecter ou à bloquer les attaques de ransomware à temps**
  - Plus de la moitié des attaques de ransomware (56 %) se sont soldées par un chiffrement de données, avec 16 % de cas combinant chiffrement et vol de données.
- **Lorsque les données sont chiffrées, les attaquants ont environ une chance sur deux de percevoir une rançon**
  - 48 % des organisations dont les données ont été chiffrées ont payé la rançon.
  - La moyenne sur quatre ans est désormais de 50 % de rançon payée après un chiffrement.
- **Le montant des demandes de rançon diminue, mais les attaquants ont tendance à demander plus lorsqu'ils parviennent à compromettre un système privilégié dont l'accès est difficile à rétablir**
  - Le montant médian des demandes de rançon est descendu à 698 000 dollars, poursuivant ainsi une tendance à la baisse observée depuis plusieurs années, après avoir atteint une médiane de 1,3 million de dollars dans le rapport 2025 et de 2 millions de dollars dans le rapport 2024.
  - 59 % des demandes de rançon provenant d'attaques ayant commencé par l'exploitation d'une vulnérabilité au niveau du pare-feu s'élèvent à 1 million de dollars ou plus, contre 48 % pour l'ensemble des demandes.
- **Le montant des rançons payées diminue, les victimes réussissant souvent à négocier un montant inférieur à celui initialement demandé**
  - Le montant médian des rançons payées s'élève désormais à 769 000 dollars, une baisse considérable par rapport au million de dollars déclaré l'année dernière.
  - Un peu moins de la moitié (48 %) des paiements s'élevait à 1 million de dollars ou plus, contre 52 % l'année précédente.
  - Près de la moitié (51 %) des organisations ayant payé une rançon ont versé moins que le montant demandé, ce qui correspond étroitement au rapport 2025 (53 %) et est 7 % plus élevé que le rapport 2024 (44 %).
- **Le coût de rétablissement après une attaque de ransomware a augmenté**
  - Le coût moyen de rétablissement après une attaque de ransomware, hors rançon payée, est désormais de 1 700 200 dollars, ce qui représente une augmentation de 11 % par rapport à la moyenne de 1 525 716 dollars du rapport 2025.
- **Le chiffrement des données a presque toujours des répercussions sur les membres de l'équipe IT/cybersécurité**
  - 99 % des victimes de ransomware dont les données ont été chiffrées ont déclaré que l'incident avait affecté leur équipe IT/cybersécurité.
  - Une anxiété ou un stress accrus liés à de futures attaques sont les répercussions les plus courantes (41 %), suivis par une pression accrue exercée par les hauts dirigeants (40 %).
  - Une reconnaissance accrue par les hauts dirigeants (36 %, contre 31 % dans le rapport 2025) est le seul impact qui a augmenté d'une année sur l'autre.

Les méthodes d'attaque et de défense

Causes premières des attaques

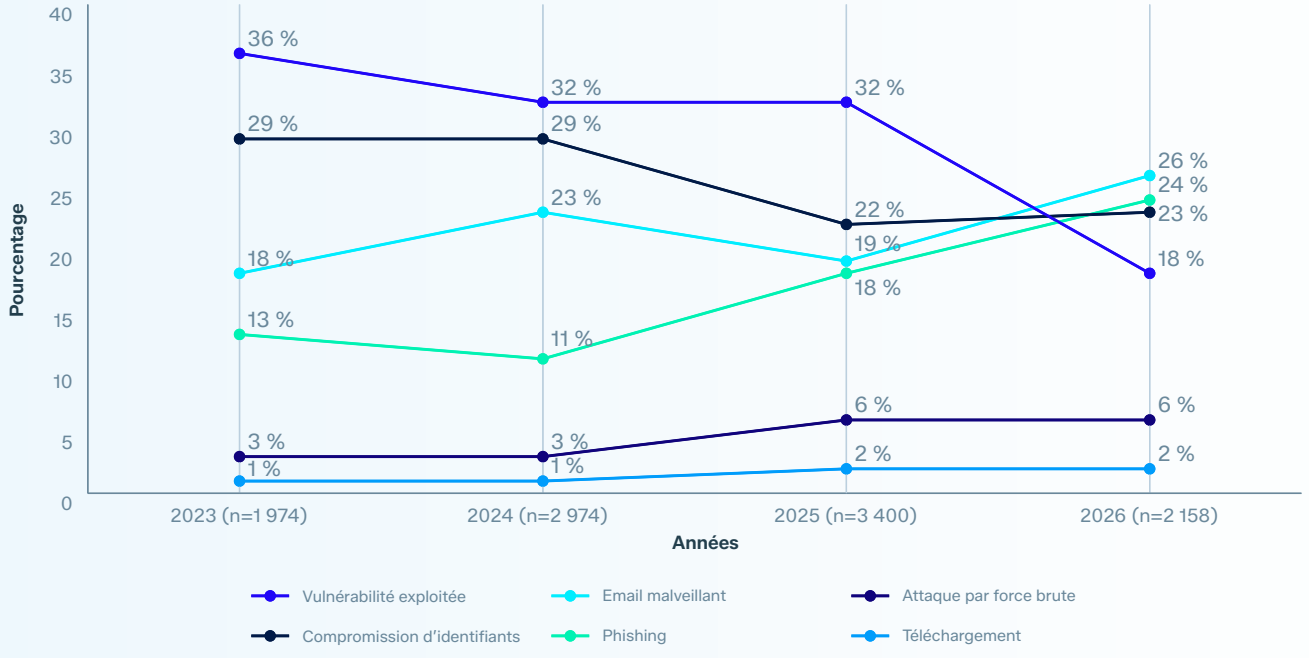
Les principales causes premières techniques des ransomwares ont changé dans le rapport de cette année. Les emails malveillants (26 %) et le phishing (24 %) étaient les deux principales causes premières des attaques de ransomware, représentant la moitié de tous les incidents. Il s'agit d'un changement significatif par rapport aux années précédentes, où les vulnérabilités exploitées étaient régulièrement en tête du classement.

La proportion de vulnérabilités exploitées est passée de 32 % dans le rapport 2025 à 18 % dans le rapport 2026. Toutefois, compte tenu de la rapidité et de l'ampleur des capacités de détection des vulnérabilités offertes par l'IA de pointe, les organisations doivent rester vigilantes face à la possibilité d'une recrudescence des attaques par ransomware dont la cause première serait l'exploitation d'une vulnérabilité au cours de l'année à venir.

Les identifiants compromis restent la troisième cause première la plus fréquente avec 23 %, un chiffre comparable aux années précédentes.

79 % des attaques ont commencé par une approche basée sur l'identité, soit en obtenant des identifiants à des fins malveillantes, soit en exploitant des identifiants déjà compromis. C'est pourquoi la sécurité des identités est un élément essentiel d'une posture de sécurité globale.

Causes premières techniques des attaques de ransomware (2023-2026)



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

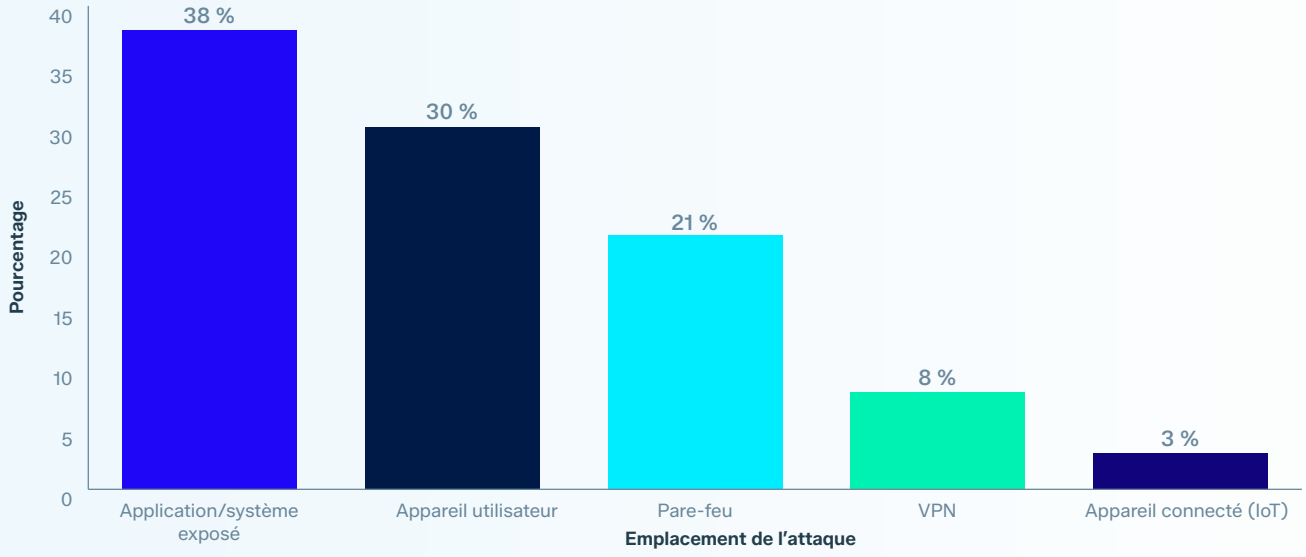
NOUVEAU POINT DE RECHERCHE

Le point de départ des attaques

Cette année, pour la première fois, nous révélons où se situe la cause première dans l'environnement organisationnel. Comprendre par où commencent les attaques est un élément clé pour mettre en place des stratégies de réduction des risques plus éclairées. Parmi les incidents de ransomware qui ont commencé par l'exploitation d'une vulnérabilité, la compromission d'identifiants ou une attaque par force brute, les **applications et systèmes exposés étaient globalement le point d'entrée d'attaque le plus courant (38 %)**, suivis des appareils utilisateur (30 %) et des pare-feu (21 %).

La proéminence des applications exposées s'inscrit dans la tendance générale à l'adoption des environnements cloud et SaaS, où les systèmes connectés à Internet constituent une surface d'attaque importante et en constante augmentation.

Emplacements ciblés par les attaques de ransomware



Vous avez dit que la cause première était une vulnérabilité exploitée, des identifiants compromis ou une attaque par force brute - où cela s'est-il produit dans votre environnement ? n=1 022

En approfondissant, les données révèlent la prévalence des identifiants compromis sur les applications et systèmes exposés, pare-feu, VPN et appareils connectés.

Causes premières les plus courantes pour chaque emplacement

Causes premières	Dans une application ou un système exposé	Dans notre pare-feu	Dans notre VPN	Dans un appareil IoT
Compromission d'identifiants	59 %	41 %	44 %	48 %
Une vulnérabilité exploitée	31 %	33 %	41 %	36 %
Attaque par force brute	10 %	26 %	15 %	16 %

Vous avez dit que la cause première était une vulnérabilité exploitée, des identifiants compromis ou une attaque par force brute - où cela s'est-il passé dans votre environnement ? Sélection des réponses. n=711

Les attaques basées sur des identifiants compromis étaient particulièrement dominantes dans les applications et les systèmes exposés (59 %). Cela souligne combien il est important de sécuriser les ressources et les contrôles d'identité accessibles de l'extérieur.

En réanalysant cette même comparaison de données, on a pu identifier les cibles les plus fréquentes des attaques par identifiants compromis et par force brute.

Le point de départ des attaques de ransomware

Emplacement de l'attaque	Total (%)	Identifiants compromis (%)	Attaque par force brute (%)
Dans une application ou un système exposé	38 %	46 %	30 %
Sur l'appareil d'un utilisateur (sur ou hors réseau, par ex. ordinateur portable, ordinateur de bureau)	30 %	27 %	13 %
Dans notre pare-feu	21 %	18 %	44 %
Dans notre VPN	8 %	7 %	9 %
Dans un appareil IoT	3 %	3 %	4 %

Vous avez dit que la cause première était un identifiant compromis ou une attaque par force brute - où cela s'est-il passé dans votre environnement ? Sélection des réponses. n=628

Différents types d'attaque ciblaient différents emplacements.

- Les attaques basées sur des identifiants compromis se sont concentrées sur les applications et les systèmes exposés (46 %), suivies par les appareils des utilisateurs.
- Les attaques par force brute ciblaient les pare-feu à un taux élevé (44 %), soulignant l'importance des politiques de limitation de débit et de verrouillage des comptes des appareils à la périphérie du réseau.

NOUVEAU POINT DE RECHERCHE

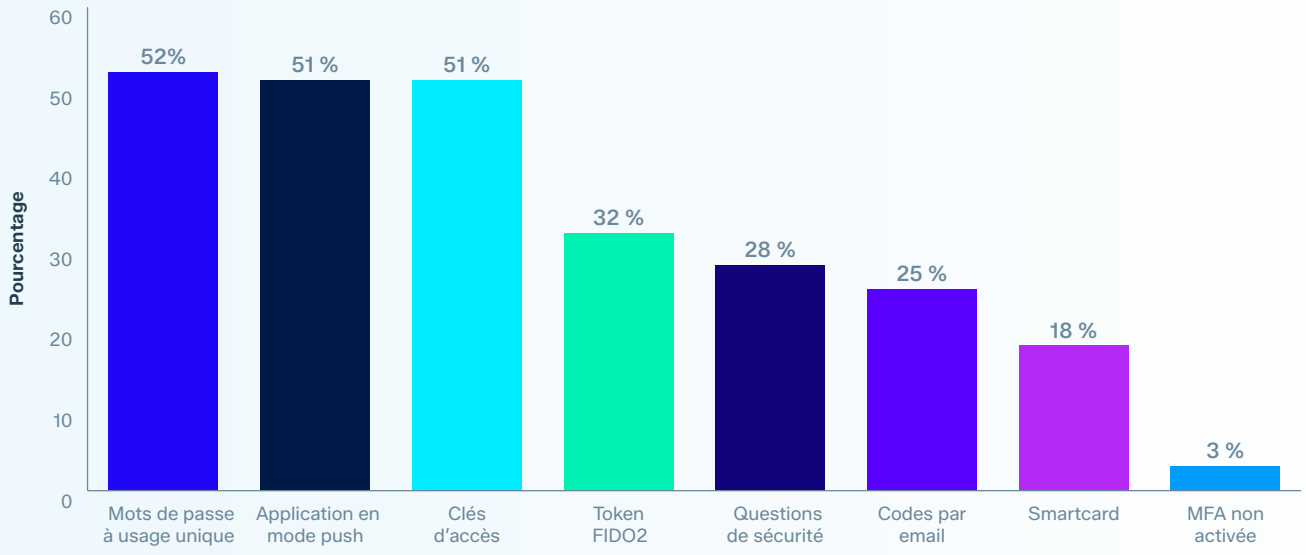
Le rôle de l'authentification multifacteur (MFA)

Le rapport de cette année présente aussi des analyses inédites sur le rôle de l'authentification multifacteur (MFA) dans les attaques par ransomware.

Parmi les organisations ayant subi une attaque de ransomware basée sur des identifiants compromis, **97 % avaient activé une authentification multifacteur sous une forme ou une autre au moment de l'incident**. Les mots de passe à usage unique (52 %), les applications en mode push (51 %) et les clés d'accès (51 %) étaient les méthodes les plus déployées, les répondants déclarant utiliser en moyenne 2,5 méthodes MFA.

Le taux élevé de victimes de ransomware qui avaient déployé une méthode MFA au moment de l'attaque indique qu'elle n'a peut-être pas été complètement déployée sur tous les systèmes concernés, créant ainsi des failles exploitables pour les attaquants. Il suggère également que, bien que la MFA reste un élément essentiel d'une stratégie de cyberdéfense robuste, elle ne suffit pas à elle seule à prévenir les attaques basées sur des identifiants, car les techniques permettant de la contourner ne cessent d'évoluer.

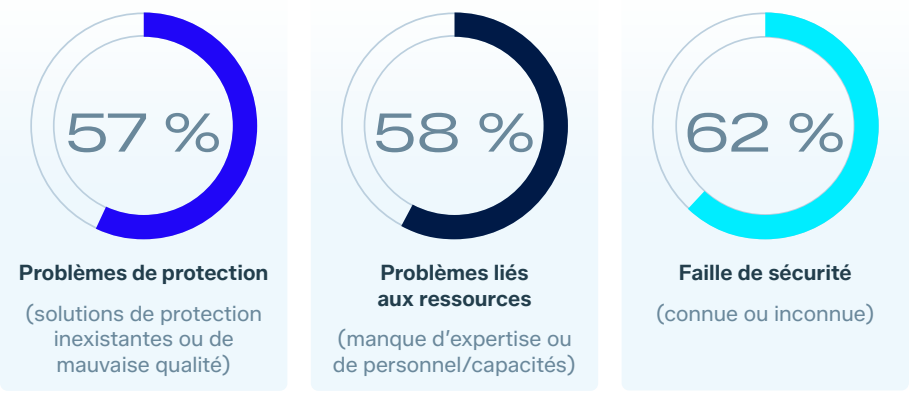
Méthodes MFA activées au moment de l'attaque



Quel type d'authentification multifacteur était activé au moment de l'attaque, le cas échéant ? Base : L'attaque s'est produite en raison d'identifiants compromis. n=503

Les facteurs de vulnérabilité des organisations

Pour la deuxième année, aucun facteur organisationnel dominant n'a exposé les organisations à des attaques, les répondants faisant état d'un large éventail de défis, allant de l'absence ou de la faiblesse de la protection à la pénurie de personnel/de compétences, en passant par des failles dans leur système de sécurité.



Pour la deuxième année consécutive, les failles de sécurité ont été la catégorie la plus citée parmi les causes premières opérationnelles (62 %), suivies par le manque de personnel ou de compétences (58 %) et une protection de mauvaise qualité ou absente (57 %).

Fait encourageant, tous les facteurs individuels (sauf un) ont diminué d'une année sur l'autre, **l'erreur humaine (35 %) étant le seul facteur opérationnel qui ait augmenté au cours de l'année écoulée**.

Comme en 2025, les victimes de ransomware ont signalé de multiples défis organisationnels, avec **2,5 facteurs cités en moyenne**, contre 2,7 auparavant.

35 %

Erreur humaine : la variable constante. Seule cause première opérationnelle des attaques qui n'a pas diminué par rapport au rapport 2025.

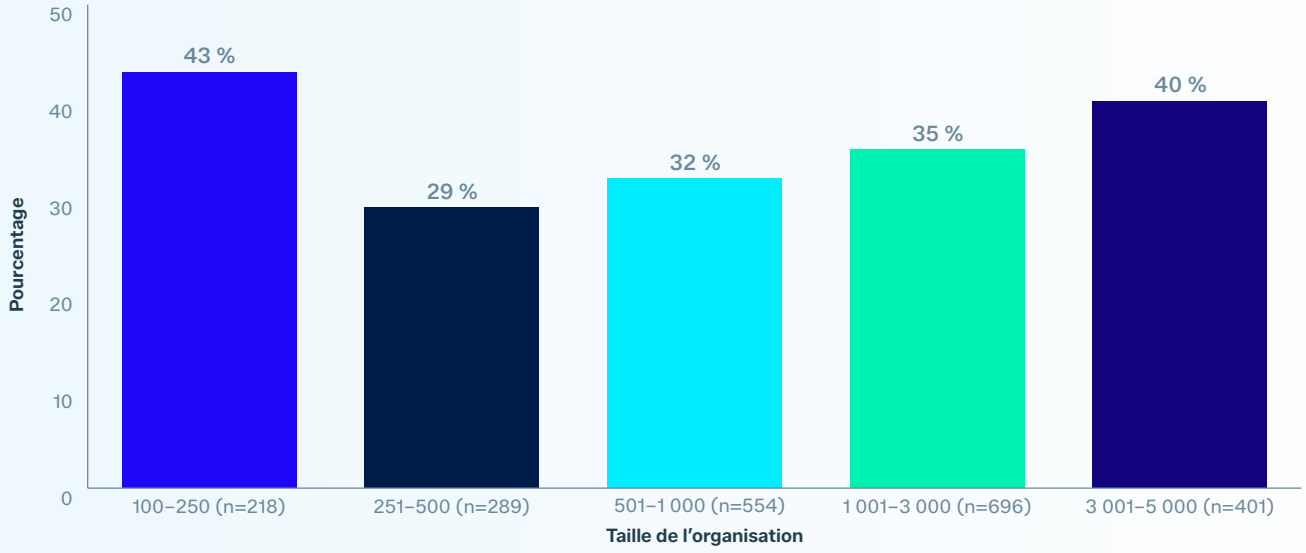
Top 7 des causes premières opérationnelles des attaques de ransomware

Classement	2025	%	Classement	2026	%
1	Manque d'expertise	40,2 %	1	Manque de protection	36,4 %
2	Faille de sécurité inconnue	40,1 %	2	Faille de sécurité inconnue	36,3 %
3	Manque de personnel/ capacité	39,4 %	3	Faille de sécurité connue	36,0 %
4	Manque de protection	39,0 %	4	Manque de personnel/ capacité	35,3 %
5	Faille de sécurité connue	38,2 %	5	Erreur humaine	35,3 %
6	Protection de mauvaise qualité	37,1 %	6	Manque d'expertise	35,1 %
7	Erreur humaine	34,2 %	7	Protection de mauvaise qualité	32,6 %

Selon vous, pourquoi votre organisation a-t-elle été victime d'une attaque de ransomware ? n=3 400 (2025), n=2 158 (2026)

Comme on pouvait s'en douter, le manque de personnel/de capacités a été largement cité par les petites organisations dans la fourchette 100-250. Toutefois, quatre entreprises sur dix comptant entre 3 001 et 5 000 salariés mentionnent également des difficultés liées aux capacités, à un taux qui n'est inférieur que de 3 % à celui des organisations comptant entre 100 et 250 salariés, ce qui montre que la gestion des ressources ne devient pas toujours plus facile à mesure que l'entreprise grandit.

Le manque d'effectifs/de capacité a contribué à ce que l'entreprise soit victime d'un ransomware



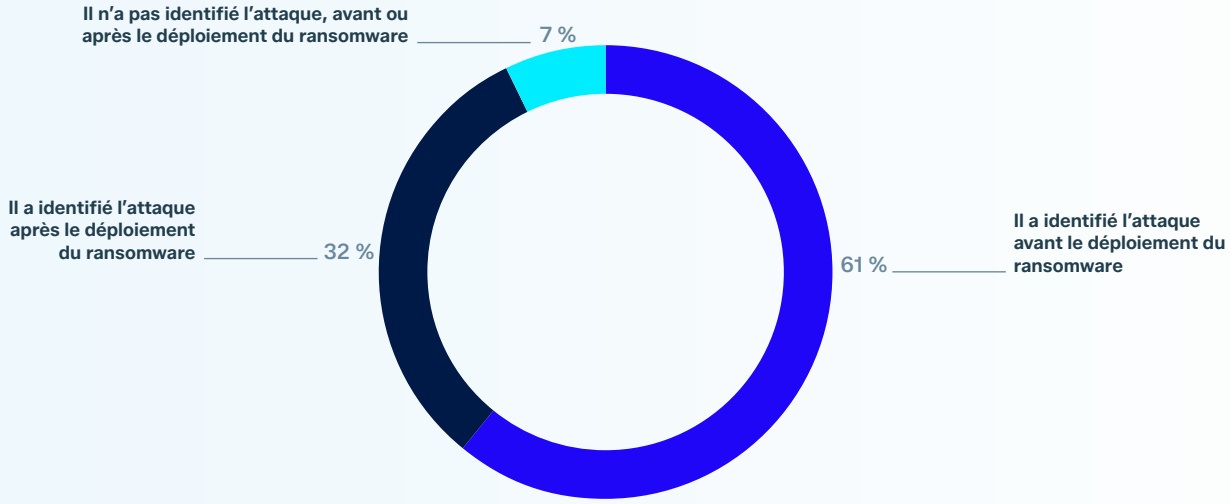
Selon vous, pourquoi votre organisation a-t-elle été victime d'une attaque de ransomware ? Au moment de l'attaque, nous ne disposions pas d'un nombre suffisant d'experts en cybersécurité pour surveiller nos systèmes. Chiffres de base dans le graphique.

NOUVEAU POINT DE RECHERCHE

Le rôle des pare-feu dans les défenses anti-ransomware

61 % des victimes ont déclaré que leur pare-feu avait détecté l'attaque de ransomware avant l'explosion de la charge utile et 32 % l'avaient identifiée après le déploiement du ransomware. Seuls 7 % ont déclaré que leur pare-feu n'avait pas du tout identifié l'attaque.

Votre pare-feu a-t-il joué un rôle dans l'identification de l'attaque ?



Quel rôle votre pare-feu a-t-il joué dans l'identification de l'attaque ? n=2 158

Les 7 % de victimes dont le pare-feu n'a pas détecté l'attaque ont connu les pires résultats en matière de chiffrement : 71 % ont vu leurs données chiffrées, contre 50 % lorsque le pare-feu a détecté l'attaque avant le déploiement du ransomware. La détection après déploiement d'un ransomware — généralement l'identification post-incident des signaux qui ont ensuite été associés à l'attaque de ransomware — correspond à un taux de chiffrement de 65 %.

Les résultats montrent clairement que les pare-feu jouent un rôle clé dans la détection des attaques de ransomware, la télémétrie issue de ces appareils fournissant des signaux précoces précieux de l'activité des adversaires. La télémétrie du pare-feu, lorsqu'elle est combinée avec les informations provenant de l'ensemble de l'environnement de sécurité, par exemple des systèmes de protection Endpoint ou des solutions de sécurité des messageries via un outil XDR ou un service MDR, peut aider les défenseurs à détecter et à bloquer les attaques de ransomware avant que les données ne soient chiffrées.

Impact de l'identification des attaques par le pare-feu sur le taux de chiffrement

	Il a identifié l'attaque avant le déploiement du ransomware	Il a identifié l'attaque après le déploiement du ransomware	Il n'a pas identifié l'attaque, avant ou après le déploiement du ransomware
Les cybercriminels sont parvenus à chiffrer les données	50 %	65 %	71%
Les cybercriminels n'ont pas réussi à chiffrer les données	50 %	35 %	29 %

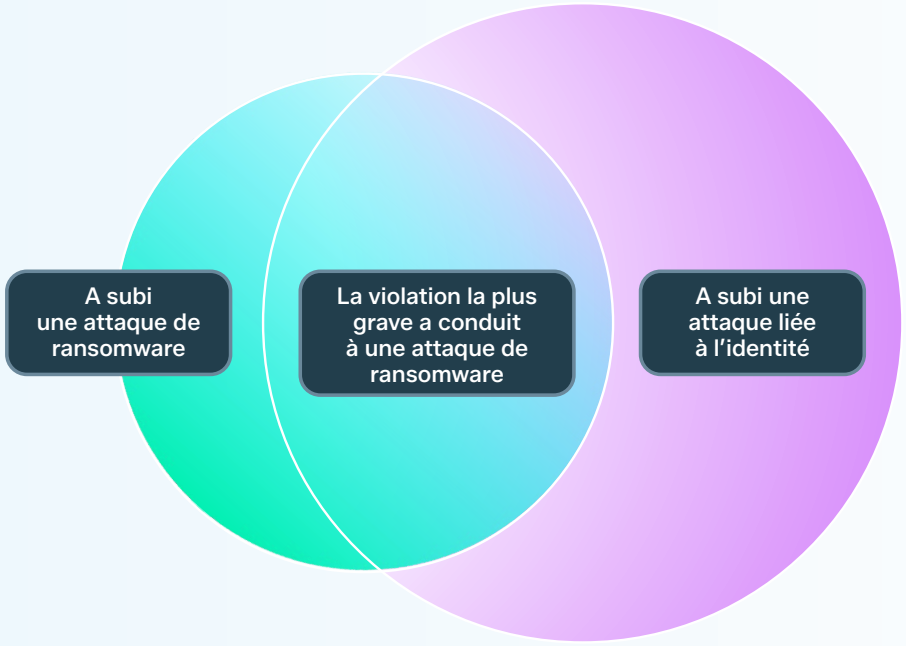
Votre pare-feu a-t-il joué un rôle dans l'identification de l'attaque ? Lors de l'attaque de ransomware, les cybercriminels ont-ils réussi à chiffrer des données de votre organisation ? n=2 158

Les pare-feu occupent une position privilégiée dans l'infrastructure des organisations. Leur compromission expose donc l'entreprise à des conséquences bien plus graves que celles qu'entraînerait la compromission d'autres éléments de l'environnement. En effet, si les attaquants parviennent à exploiter une vulnérabilité du pare-feu, ils obtiennent souvent un accès étendu à l'ensemble de l'entreprise. La différence entre les montants des rançons demandées dans ces différents scénarios vient étayer cet argument : **59 % des demandes de rançon provenant d'attaques ayant commencé par l'exploitation d'une vulnérabilité au niveau du pare-feu s'élèvent à 1 million de dollars ou plus**, contre 48 % de toutes les attaques.

NOUVEAU POINT DE RECHERCHE

Le lien entre usurpation d'identité et ransomwares

L'une des conclusions les plus frappantes de cette enquête est la confirmation du lien direct entre les attaques liées à l'identité et les ransomwares. Parmi les organisations victimes d'un ransomware au cours de l'année écoulée, les deux tiers (67 %) ont confirmé que cet incident correspondait à leur attaque liée à l'identité la plus grave. Même si toutes les attaques n'ont pas donné lieu à un chiffrement des données, ce constat montre que le vol d'identité est l'un des principaux mécanismes utilisés pour propager les ransomwares.



Répartition des données : Au cours de l'année passée, votre organisation a-t-elle été touchée par un ransomware ? (n=5 000) Votre organisation a-t-elle subi des violations de sécurité liées à l'identité au cours des 12 derniers mois ? n=5 000. [Si oui aux deux] Cet incident de ransomware était-il le même que votre attaque liée à l'identité la plus importante ?

Le chiffrement et la récupération des données

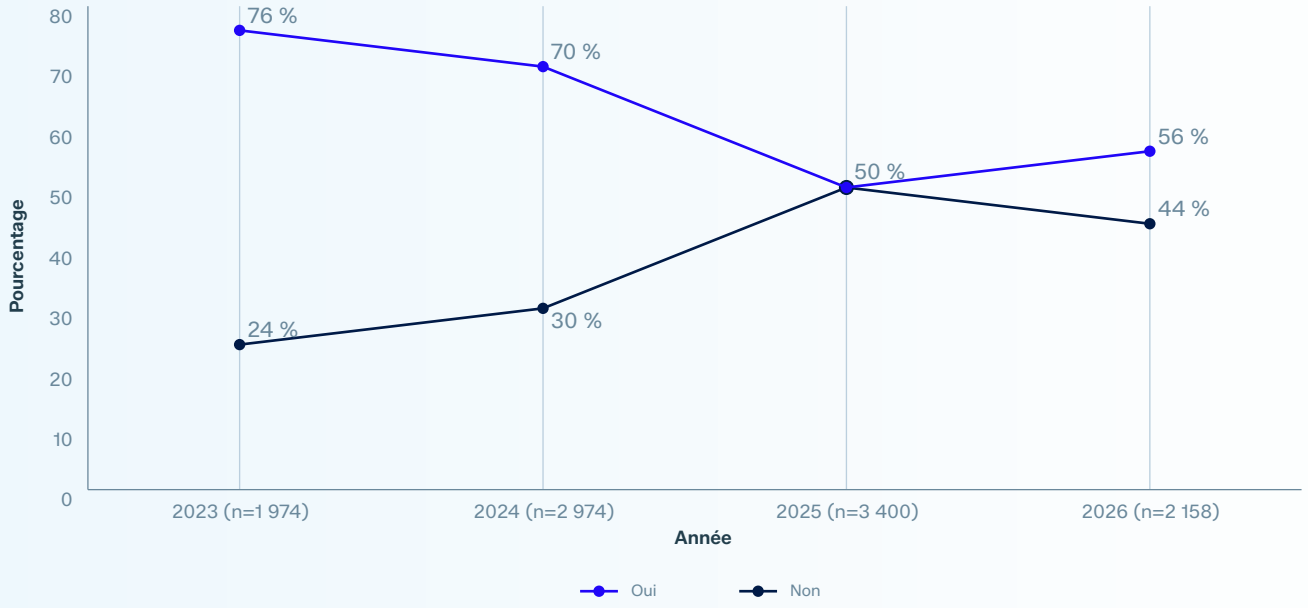
Taux de chiffrement des données

Plus de la moitié des attaques de ransomware (56 %) a abouti au chiffrement de données. Cela inclut 40 % de cas où les données ont été chiffrées uniquement, et 16 % où elles ont été à la fois chiffrées et volées. 41 % des attaques ont été stoppées avant le chiffrement, tandis que 2 % concernaient des attaques sans chiffrement de type extorsion.

+6 %

Augmentation du taux de chiffrement des ransomwares depuis le rapport de l'année dernière.

Des données ont-elles été chiffrées pendant l'attaque ? (Résumé : Oui/non)

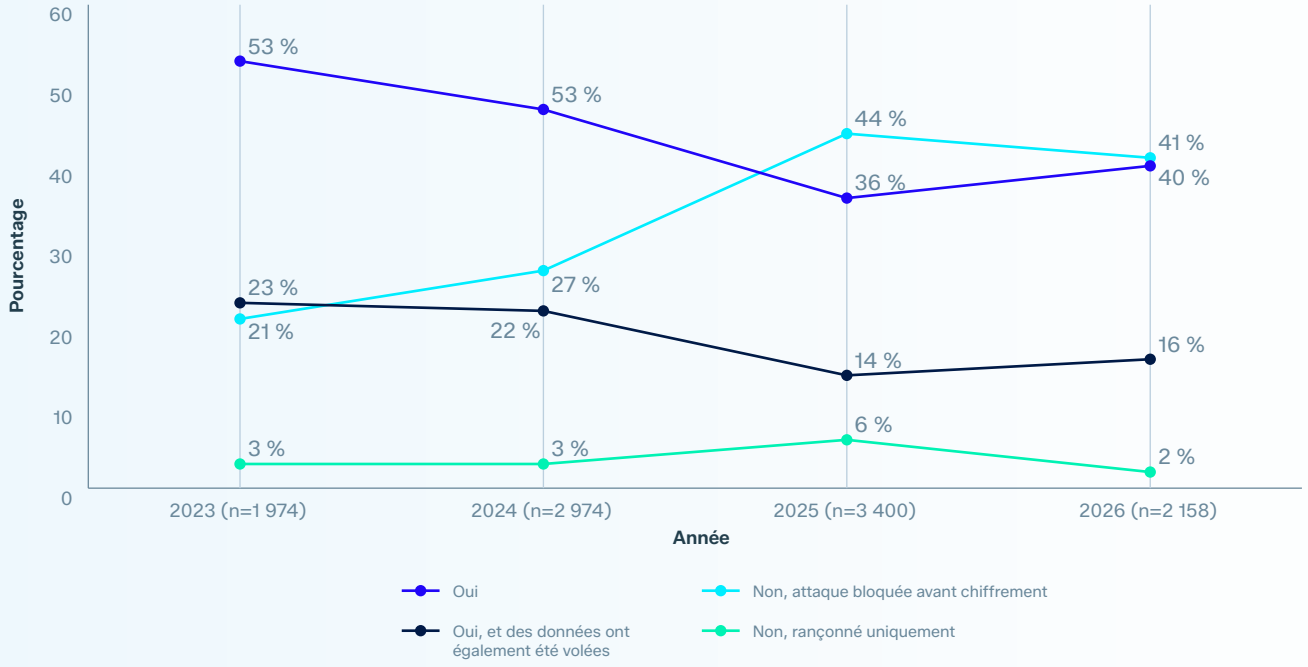


Lors de l'attaque par ransomware, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ? Réponses résumées : Oui / Non. Chiffres de base dans le graphique.

Si le taux de chiffrement reste bien inférieur au pic de 76 % du rapport de 2023, il a légèrement augmenté par rapport au creux de 50 % du rapport 2025. Cette inversion de tendance mérite qu'on s'y attarde : après deux années de recul du succès du chiffrement, les attaquants semblent regagner un peu de terrain.

Les 16 % d'attaques impliquant à la fois chiffrement et vol de données sont particulièrement préoccupants, car ces attaques à double impact donnent aux attaquants de multiples points de levier pour une extorsion.

Des données ont-elles été chiffrées pendant l'attaque ?

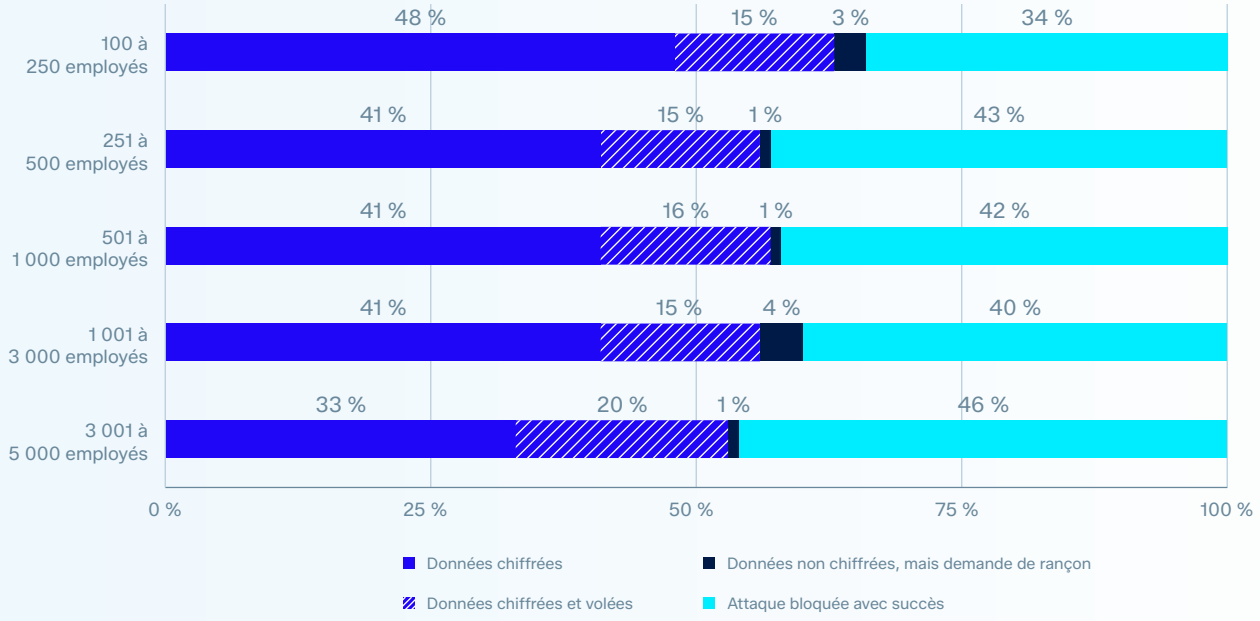


Lors de l'attaque par ransomware, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ? (Liste complète des choix de réponse)
Base : organisations touchées par un ransomware. Chiffres de base dans le graphique.

L'issue des tentatives de chiffrement varie selon la taille de l'entreprise. **Les plus grandes organisations interrogées (3 001 à 5 000 employés) sont les plus susceptibles de stopper les attaques avant le chiffrement ou l'extorsion (46 %)** contre seulement 34 % pour les plus petites organisations (100 à 250 employés).

Cependant, lorsque les attaquants parviennent à chiffrer des données dans les grandes organisations, les victimes sont plus susceptibles de subir également un vol de données. Le taux de « chiffrement et vol » atteint 20 % pour la plus grande tranche de taille contre 15 % pour la plupart des autres. L'exfiltration de données en plus du déploiement d'un ransomware donne aux attaquants une occasion supplémentaire de monétiser l'attaque.

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 des données de votre organisation ? n=2 158

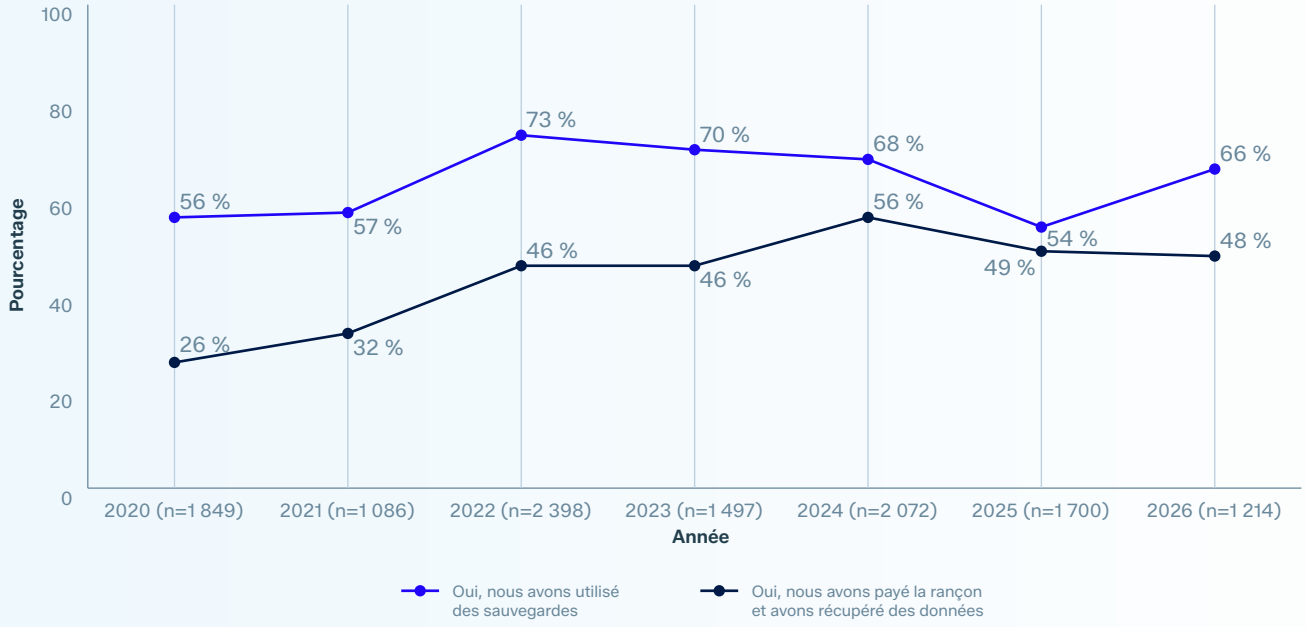
Comment les organisations ont récupéré leurs données chiffrées

La récupération basée sur les sauvegardes a fortement augmenté, atteignant 66 % des attaques avec chiffrement des données, contre 54 % dans le rapport 2025. Ce net rebond suggère que les organisations ont renouvelé leur investissement dans une infrastructure de sauvegarde après le recul observé en 2025, mais aussi qu'elles sont en train de renforcer leur résilience face aux demandes de rançon.

+12 %

Augmentation de l'utilisation des sauvegardes pour se remettre d'une attaque de ransomware entre 2025 et 2026.

Votre organisation est-elle parvenue à récupérer ses données après l'attaque de ransomware ?



Votre organisation est-elle parvenue à récupérer ses données ? Base : organisations dont les données ont été chiffrées. Chiffres de base dans le graphique. Plusieurs réponses sont autorisées. Les pourcentages peuvent donc dépasser 100 %.

La part d'organisations ayant payé la rançon pour récupérer des données est tombée à 48 %, le taux le plus bas des 3 dernières années. Seuls 2 % des organisations ont déclaré ne pas être parvenus à récupérer leurs données, ce qui indique que lorsque les données sont chiffrées, la récupération par un moyen ou un autre est presque universelle.

Montant de la rançon demandée et montant payé

Les demandes de rançon

Le montant médian des demandes de rançon est descendu à 698 000 dollars dans le présent rapport, poursuivant ainsi une tendance à la baisse sur plusieurs années. Cela représente un recul net de 65 % sur les deux dernières années. Le montant moyen des demandes de rançon a également diminué au cours de cette période, passant à 3 126 372 dollars, soit une réduction de 28 % depuis le rapport 2024.

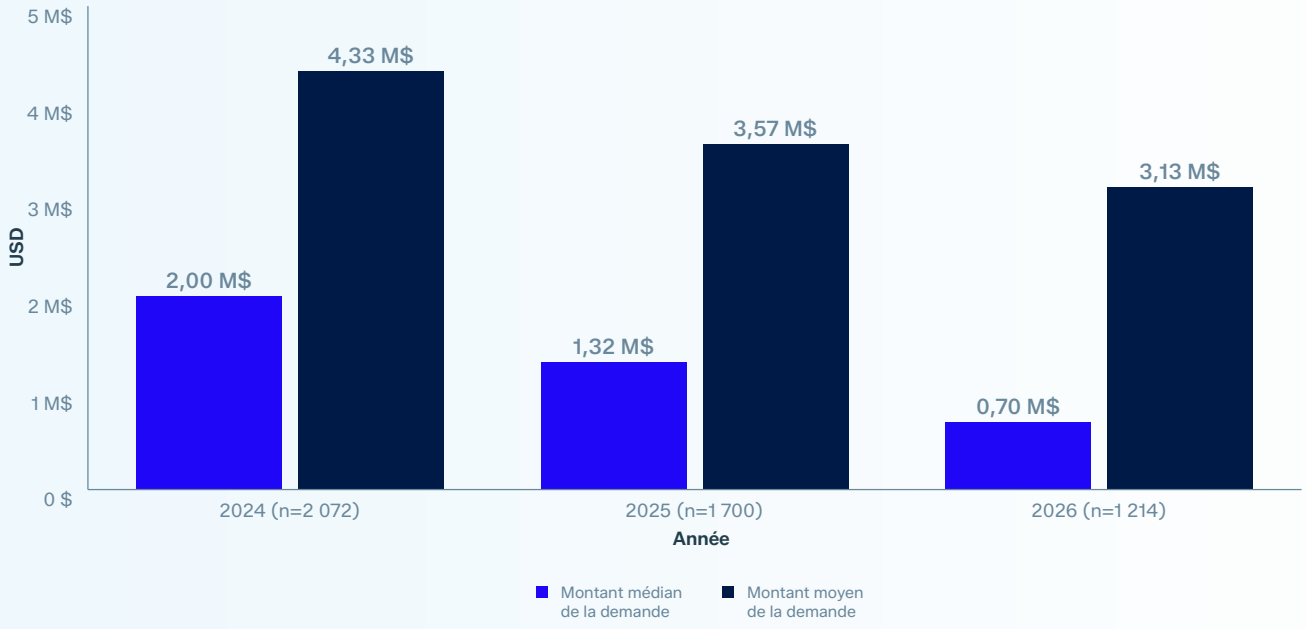
L'écart croissant entre le montant moyen et le montant médian des demandes indique une distribution fortement asymétrique. Un petit nombre de demandes très importantes gonflent la moyenne, tandis qu'une organisation type fait face à une demande légèrement inférieure à 700 000 dollars.

Remarque : les rançons aberrantes de 40 millions de dollars ou plus ont été supprimées de ces données.

698 000 $

Montant médian des demandes de rançons au cours de l'année écoulée.

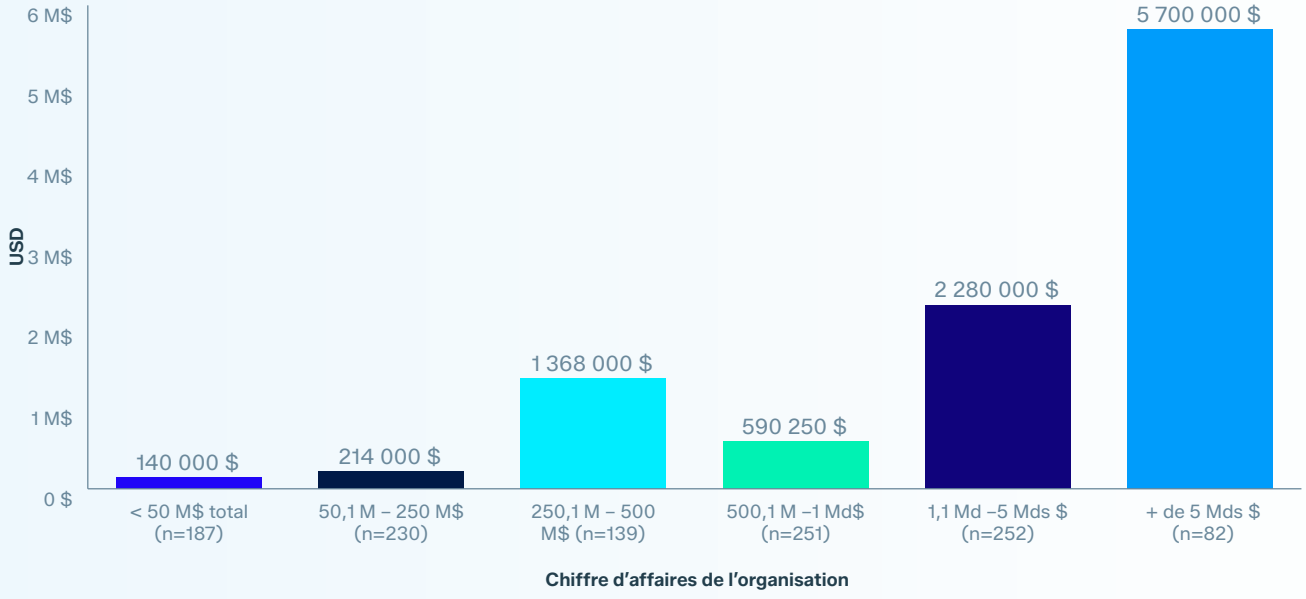
Montants moyen et médian des demandes de rançon



Quel était le montant de la rançon demandée par les attaquants ? Base : organisations dont les données ont été chiffrées. Chiffres de base dans le graphique. Exclut les demandes aberrantes de 40 millions de dollars ou plus.

Le montant des rançons demandées augmente fortement avec le chiffre d'affaires de l'organisation. Les organisations dont le chiffre d'affaires est inférieur à 50 millions de dollars ont fait face à un montant médian d'environ 140 000 dollars, tandis que celles dont le chiffre d'affaires est supérieur à 5 milliards de dollars ont fait face à un montant médian de 5,7 millions de dollars. Cette tendance laisse fortement supposer que les attaquants mènent des opérations de reconnaissance préalable afin d'ajuster leurs demandes en fonction de la capacité de paiement qu'ils estiment chez leurs victimes.

Montant médian des demandes de rançon



Quel était le montant de la rançon demandée ? Base : organisations dont les données ont été chiffrées. Chiffres de base dans le graphique. Exclut les demandes aberrantes de plus de 40 millions de dollars.

Montants des rançons payées

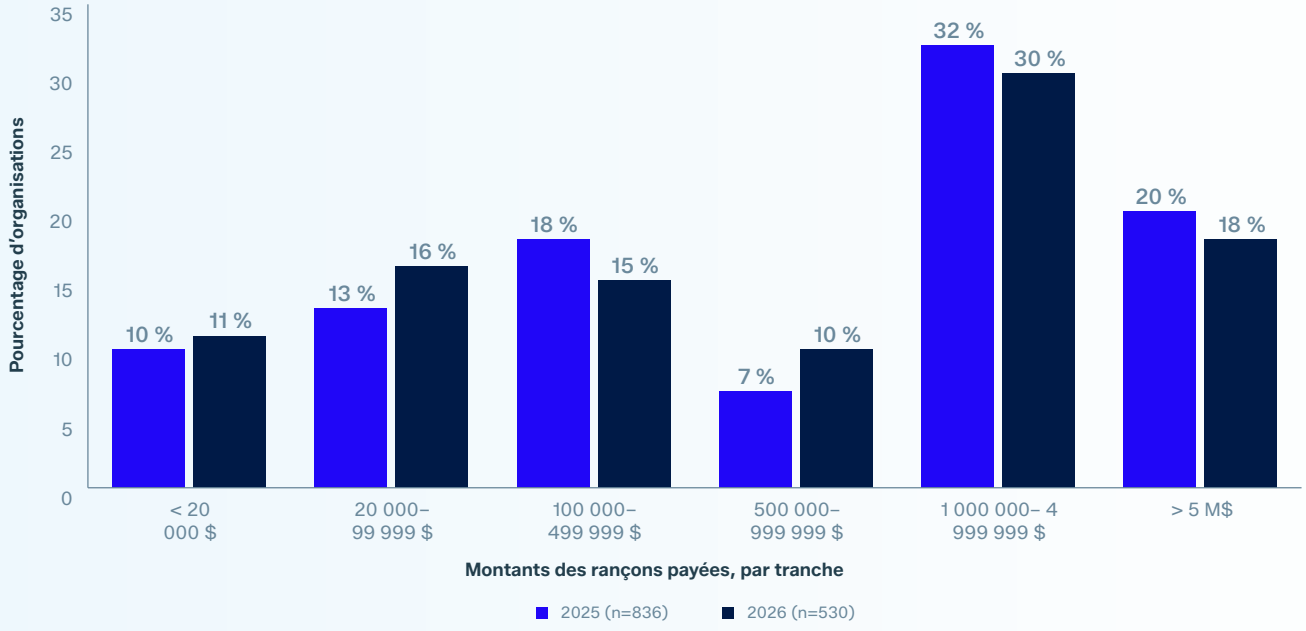
530 organisations ayant payé la rançon nous ont communiqué la somme demandée par l'attaquant, révélant que le montant médian de la rançon était désormais de 769 000 dollars, un chiffre bien inférieur au million de dollars déclaré l'année dernière. Un peu moins de la moitié (48 %) des paiements s'élevait à 1 million de dollars ou plus, contre 52 % l'année précédente.

L'examen de la répartition complète des paiements révèle un glissement manifeste vers le milieu de la fourchette. Les deux tranches les plus élevées (1 à 5 millions de dollars et plus) ont toutes deux connu une baisse comparée au rapport précédent, tandis que les tranches de 20 000 à 99 999 dollars et de 500 000 à 999 999 dollars ont chacune augmenté, ce qui suggère que les attaquants et les victimes s'accordent de plus en plus sur des paiements de niveau faible à moyen.

769 000 $

Montant médian des rançons payées au cours de l'année écoulée.

Montants des rançons payées par tranche

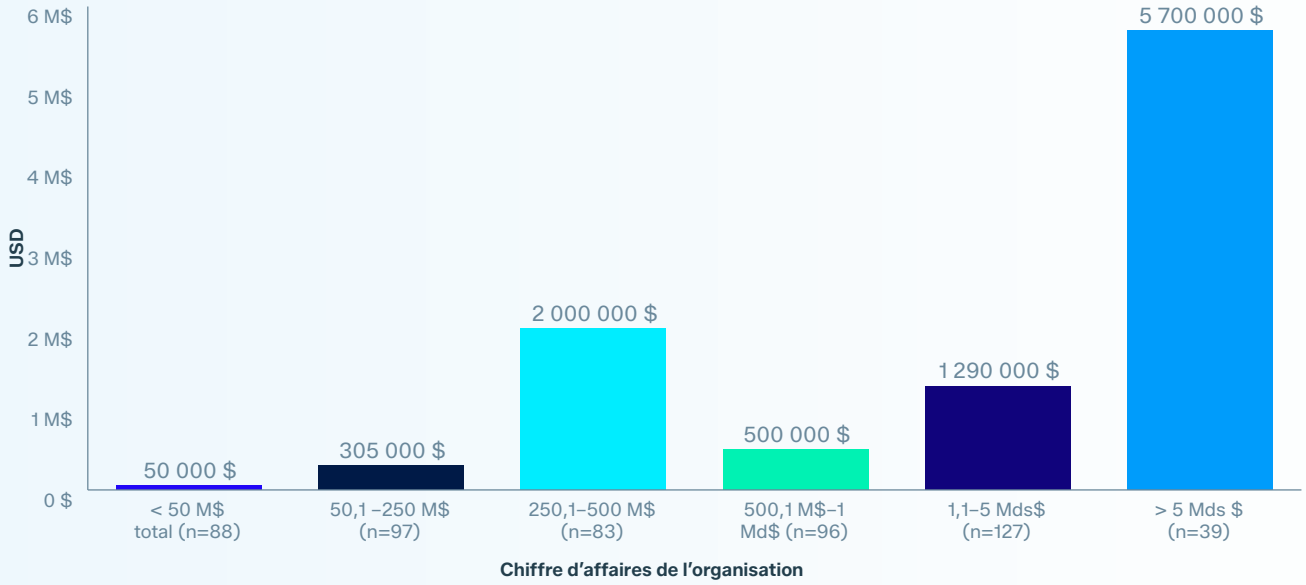


Quel était le montant de la rançon payée aux attaquants ? Chiffres de base dans le graphique.

**L'analyse du montant des rançons payées par niveau de chiffre d'affaires montre un pic dans la tranche 250,1 M$–500 M$, avec un montant médian de 2 M$**. C'est plus que tout autre segment, à l'exception du plus important (> 5 Mds$ de revenus annuels) et quatre fois plus que pour les organisations dont le chiffre d'affaires est compris entre 500,1 M$ et 1 Md$.

Les données liées aux montants des rançons demandées montrent un pic similaire entre 250,1 M$- 500 M$, avec un montant médian de 1,37 million de dollars contre 590 000 dollars dans la tranche supérieure, suggérant que ce segment est particulièrement exposé aux impacts des ransomwares.

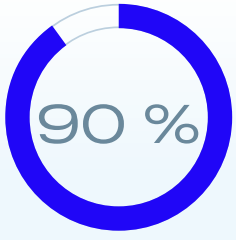
Montant médian de la rançon



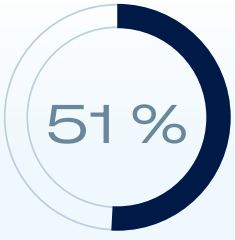
Quel était le montant de la rançon payée aux attaquants ? Base : les organisations ayant payé la rançon. Chiffres de base dans le graphique.

Paiements effectifs vs demandes initiales

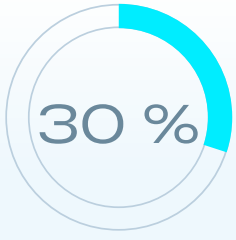
507 organisations ont communiqué à la fois le montant de la rançon demandée et celui de la rançon payée, démontrant leur capacité de négociation avec les attaquants. **Le montant médian payé s'élevait à 90 % de la rançon demandée (moyenne : 85 %)**, un peu plus de la moitié des victimes (51 %) ayant payé moins que la demande initiale, 30 % le montant exact demandé et 18 % davantage. Ces chiffres sont très proches de ceux de l'année dernière, révélant que la relation entre les montants demandés et effectivement payés est restée relativement stable.



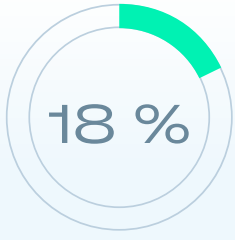
Le pourcentage **médian** du montant de la demande de rançon initiale payée



Paiements **inférieurs** au montant initial demandé



Paiements **équivalant** au montant initial demandé



Paiements **supérieurs** au montant initial demandé

Quel était le montant de la rançon demandée par les attaquants ? Quel était le montant de la rançon payée aux attaquants ? Base : organisations ayant communiqué à la fois le montant demandé et le montant payé. n=507

Comme expliqué ci-dessus, le montant médian des rançons demandées augmentent généralement lorsque l'organisation ciblée a un chiffre d'affaires plus élevé, mais le succès des négociations visant à faire baisser le montant final diffère d'une tranche de chiffre d'affaires à l'autre.

Les organisations de taille moyenne (50 à 250 M$ de CA) sont celles qui parviennent le moins à réduire le montant des rançons, 25 % payant plus que la demande initiale. Les plus grandes organisations (> 5 Mds $ de CA) sont les plus efficaces pour négocier des rançons moins élevées, 11 % payant plus que la demande initiale et 57 % payant moins — le pourcentage le plus élevé toutes cohortes confondues.

Les organisations dont le chiffre d'affaires est supérieur à 500 millions de dollars ont mieux réussi à payer un montant inférieur à la demande de rançon initiale, ce qui indique qu'à des montants plus élevés, les attaquants sont plus disposés à accorder des remises pour des rançons globales plus importantes. Les organisations enregistrant un chiffre d'affaires inférieur à 50 millions de dollars sont elles aussi parvenues, mais dans une moindre mesure, à réduire le montant final de la rançon.

Part de la rançon payée par rapport au montant demandé, par chiffre d'affaires de l'organisation (médiane)

Chiffre d'affaires	Proportion de la rançon payée (médiane)
< 50 millions $	95 %
50,1 - 250 millions $	100 %
250,1 - 500 millions $	100 %
500,1 millions - 1 milliard $	83 %
1,1 - 5 milliards $	83 %
> 5 milliards $	83 %

Quel était le montant de la rançon demandée par les attaquants ? Quel était le montant de la rançon payée aux attaquants ? Base : organisations ayant communiqué à la fois le montant demandé et le montant payé. n=507

Montant de la rançon payée, par secteur

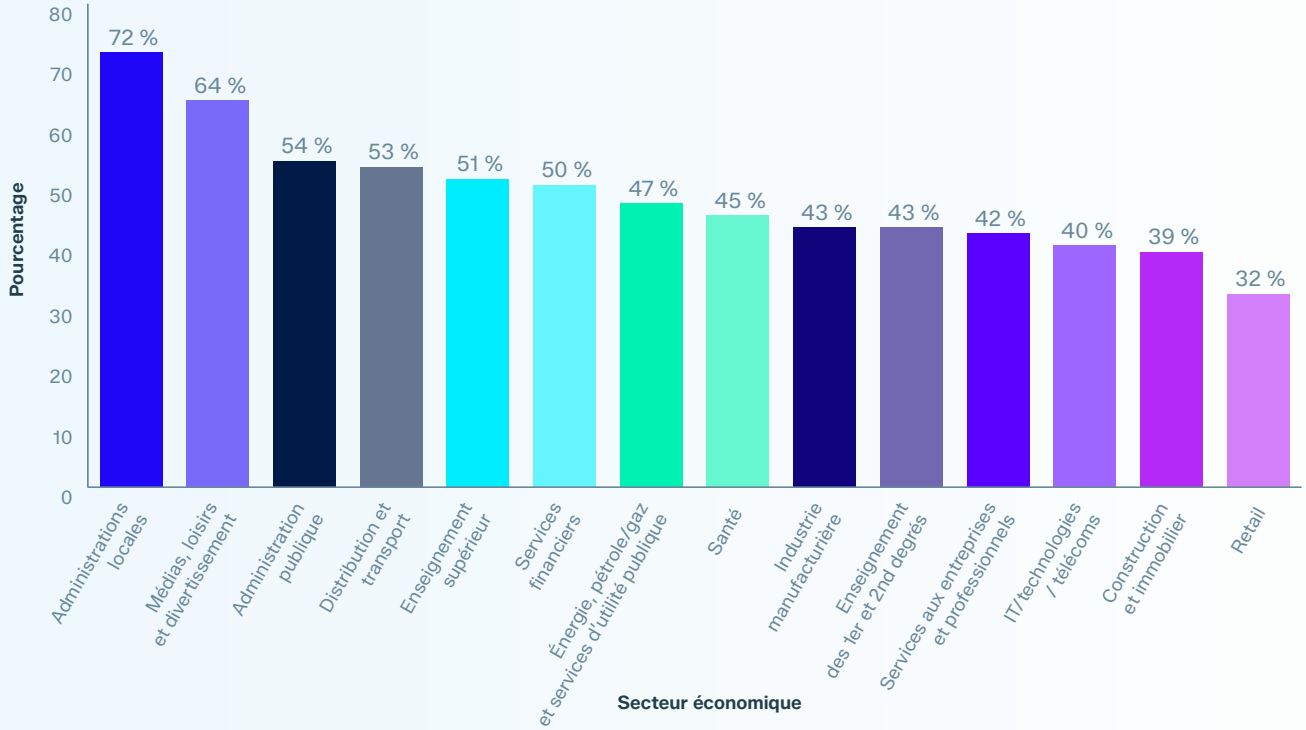
La propension à payer la rançon varie selon le secteur. **Les organisations issues des administrations publiques (72 %) et des médias, loisirs et divertissement (64 %) étaient les plus susceptibles de payer la rançon**, faisant état d'un taux plus de deux fois supérieur à celles appartenant au secteur du retail (32 %).

Les organisations du secteur public et des médias sont souvent soumises à une pression aiguë pour restaurer rapidement des services destinés aux citoyens ou soumis à des délais critiques, alors que les entreprises du retail peuvent être plus enclines à « laisser passer la tempête ».

Retail

est le secteur qui a le moins payé de rançons aux attaquants (32 %).

Pourcentage des organisations ayant payé la rançon, par secteur



Votre organisation est-elle parvenue à récupérer ses données ? Nous avons payé la rançon. Base : organisations dont les données ont été chiffrées. n=1 214

L'impact commercial et humain

Coûts de rétablissement après une attaque de ransomware

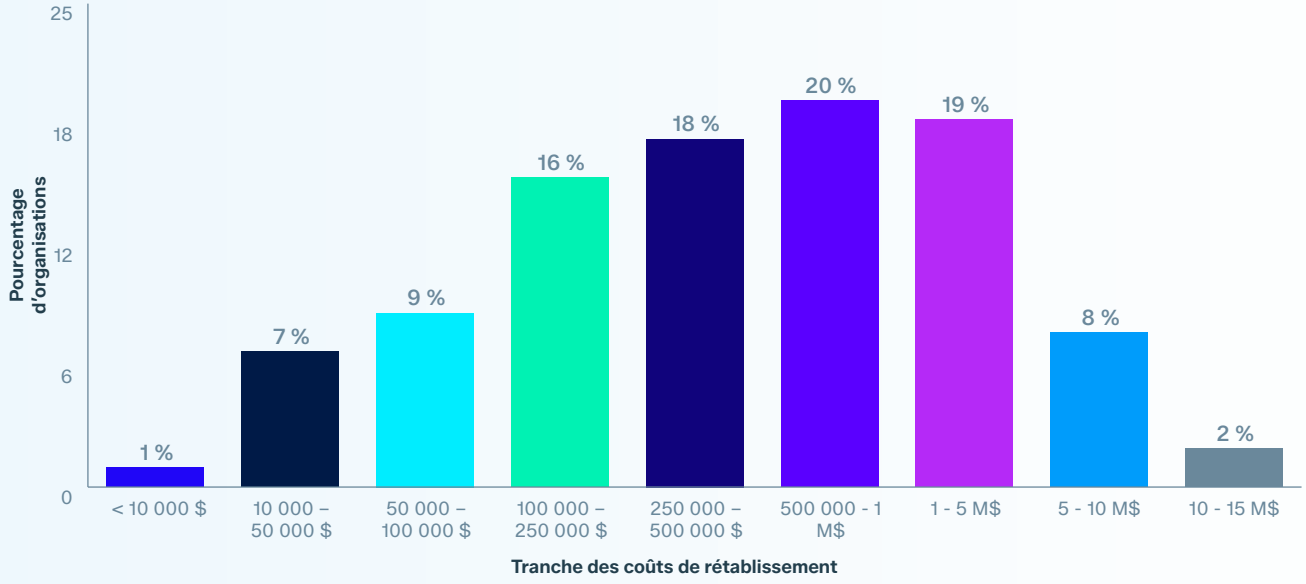
Le coût moyen de rétablissement après une attaque de ransomware, hors montant de la rançon payée, était de 1 700 200 dollars au cours de l'année écoulée. Cela représente une augmentation de 11 % par rapport à la moyenne de 1 525 716 dollars du rapport 2025, mais reste 38 % en dessous du pic de 2 730 684 dollars enregistré dans le rapport 2024. Le coût médian s'élève à 375 000 $, un montant inchangé par rapport à l'enquête précédente.

2024	2025	2026
2,73 millions $	1,53 million $	1,70 million $

Quel a été 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=2 158 (2026), n=3 400 (2025), 2 974 (2024)

Les coûts de rétablissement couvrent un large éventail : 20 % des organisations ont dû régler des factures allant de 500 000 à 1 million de dollars, tandis que 19 % ont dépensé entre 1 et 5 millions de dollars.

Les coûts de rétablissement après une attaque de ransomware



Quel a été le coût approximatif supporté par votre organisation pour remédier aux conséquences de l'attaque de ransomware la plus importante ? n=2 158

Temps de rétablissement

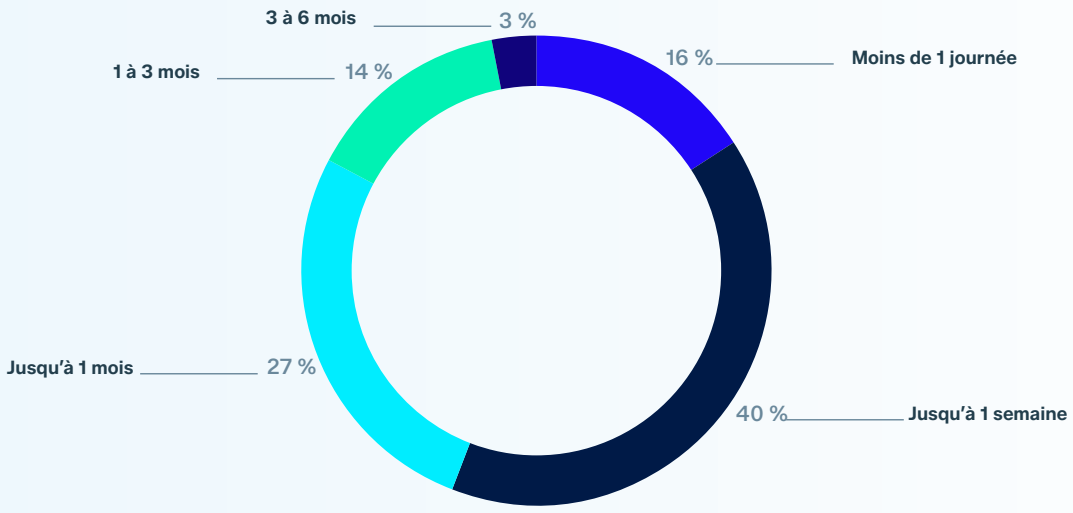
Plus de la moitié des organisations (55 %) se sont rétablies d'un ransomware en une semaine, 16 % en moins d'un jour et 83 % en un mois. Seuls 3 % ont mis plus de trois mois à se rétablir.

Le taux de rétablissement sur une semaine, qui s'élève à 55 %, affiche une hausse de 3 % par rapport à l'année précédente.. Le nombre moyen de semaines nécessaires au rétablissement est resté stable à trois semaines (2026 et 2025), contre cinq semaines dans le rapport 2024.

55 %

Pourcentage d'organisations qui se sont rétablies dans la semaine après l'attaque de ransomware.

Temps nécessaire pour se rétablir



Combien de temps a-t-il fallu à votre organisation pour se rétablir complètement après l'attaque de ransomware ? n=2 158

L'impact humain des ransomwares

Pratiquement toutes les organisations dont les données ont été chiffrées (99 %) ont rapporté des répercussions durables sur leurs équipes informatiques et de cybersécurité. Les impacts les plus cités étaient l'anxiété ou le stress accrus à l'idée de futures attaques (41 %) et la pression accrue exercée par les hauts dirigeants (40 %). Chez plus d'une victime sur cinq (21 %), l'équipe de direction a été remplacée en conséquence directe de l'attaque.

Une reconnaissance accrue par les hauts dirigeants est le seul impact ayant augmenté d'une année sur l'autre, passant de 31 % à 36 %. Toutes les autres répercussions mesurées ont diminué, y compris les changements apportés aux priorités de l'équipe (baisse de sept points), l'augmentation continue de la charge de travail (baisse de sept points) et la restructuration de l'équipe (baisse de cinq points).

21 %

Pourcentage des équipes dirigeantes IT/cybersécurité qui ont été remplacées suite à l'attaque de ransomware.

Comment les ransomwares ont affecté les équipes IT/cybersécurité

Répercussions	2026	Changement par rapport à 2025
Anxiété ou stress accru liés à de futures attaques	41 %	-
Pression accrue de la part des hauts dirigeants	40 %	-
Reconnaissance accrue par les hauts dirigeants	36 %	↑ 5 pp
Changements au sein de l'équipe/ de la structure organisationnelle	32 %	↓ 5 pp
Changement des priorités/objectifs de l'équipe	32 %	↓ 6 pp
Sentiment de culpabilité de ne pas avoir pu empêcher l'attaque	31 %	↓ 3 pp
Augmentation continue de la charge de travail	31 %	↓ 7 pp
Absence du personnel liée au stress/ aux problèmes de santé mentale	29 %	↓ 2 pp
Remplacement de la direction de l'équipe	21 %	↓ 4 pp

Quelles ont été les répercussions de l'attaque de ransomware sur les membres de votre équipe informatique/cybersécurité, le cas échéant ? Base : organisations dont les données ont été chiffrées. n=1 214 (2026), n=1 700 (2025)

L'augmentation de la reconnaissance par les hauts dirigeants peut elle-même contribuer aux tendances opérationnelles positives observées ailleurs dans ce rapport. En effet, une plus grande attention de la part des dirigeants peut se traduire par de meilleures ressources et un meilleur soutien organisationnel pour les programmes de cybersécurité.

Recommandations

Renforcez la sécurité des identités pour vous prémunir contre les ransomwares. Deux tiers des victimes de ransomware ont confirmé que leur incident de ransomware coïncidait avec leur attaque d'identité la plus importante, soulignant le lien étroit entre compromission de l'identité et ransomware. Les organisations doivent accorder la priorité à la détection et à la réponse aux menaces liées aux identités (ITDR), appliquer une authentification multifacteur sur tous les points d'accès et auditer régulièrement les identifiants des identités humaines et non humaines. Comme l'ont montré les résultats de l'enquête (97 % des organisations avaient l'authentification multifacteur activée sous une forme ou une autre au moment de leur attaque), l'authentification multifacteur seule ne suffit pas à bloquer les attaques, et elle doit être activée de manière globale.

Renforcez la protection Endpoint pour les modèles d'IA frontière. L'IA frontière accélère la découverte et l'exploitabilité des vulnérabilités. Il est essentiel de disposer de défenses Endpoint solides qui bloquent automatiquement les attaques basées sur des exploits.

Faites appel à un spécialiste ou à un service MDR Le manque de ressources, de compétences et d'expertise est un enjeu récurrent pour les PME comme pour les grandes entreprises. Les menaces accélérées par l'IA amplifieront la pression sur ces domaines, les professionnels de la sécurité s'efforçant de rester à la pointe de l'évolution rapide des technologies de l'IA. Si vous n'êtes pas en mesure de mettre en place en interne une équipe SecOps fiable, faites appel à un spécialiste externe pour combler ce manque, soit directement auprès d'un fournisseur de solutions MDR assurant une couverture 24/7, soit auprès d'un fournisseur de services managés. Les fournisseurs capables de résoudre plus d'incidents de bout en bout grâce à l'IA et à l'automatisation seront également un multiplicateur de force qui pourra vous aider à combler vos lacunes en matière de compétences et de capacités.

Privilégiez la sécurité des messageries. Le phishing et les emails malveillants représentant désormais la moitié des causes premières des ransomwares dans ce rapport. Les organisations devraient déployer le filtrage avancé des emails, implémenter les protocoles DMARC/DKIM/SPF et investir dans des formations régulières de sensibilisation au phishing. Cette progression des attaques par email suggère que la correction des failles techniques ne suffit pas à elle seule.

Investissez dans une infrastructure de sauvegarde et de restauration. Les organisations ayant maintenu des systèmes de sauvegarde robustes ont récupéré des données chiffrées à un rythme presque record au cours de l'année écoulée. Les sauvegardes doivent être testées régulièrement, stockées hors ligne ou dans des formats immuables, et intégrées dans un plan de réponse aux incidents documenté pouvant être exécuté sous pression.

Maintenez des programmes de gestion de l'exposition. La baisse de 14 points de pourcentage des vulnérabilités exploitées comme cause première est encourageante, mais ces incidents restent un vecteur d'attaque majeur et sont susceptibles d'augmenter à mesure que les modèles d'IA frontière trouveront plus rapidement de nouvelles vulnérabilités. Les organisations vont devoir maintenir des rythmes soutenus d'installation de correctif et se concentrer sur les mesures d'atténuation, notamment la segmentation, l'accès réseau Zero Trust et les déploiements de l'authentification multifacteur/continue.

Réduisez l'exposition à l'aide du pare-feu et tirez parti de sa télémétrie pour détecter les attaques à un stade précoce. Assurez-vous que votre pare-feu reçoive des mises à jour rapides (idéalement automatisées) et minimisez les services connectés à Internet tels que l'accès administrateur et les portails utilisateur. Reliez les pare-feu aux solutions XDR et MDR afin d'utiliser leur télémétrie pour repérer les attaques de ransomware avant que leurs charges utiles ne soient déployées.

Soutenez les équipes de cybersécurité pendant toute la durée de l'attaque. Avec 99 % des équipes affectées déclarant des répercussions, le coût humain des ransomwares est presque universel. Les organisations doivent établir des protocoles clairs de support post-incident et s'assurer que la reconnaissance croissante par les dirigeants se traduit par un investissement soutenu dans les ressources humaines, et pas seulement dans la technologie.

Conclusion

L'état des ransomwares 2026 révèle un paysage de menaces en transition.

Il existe de véritables signes de progrès : les montants des rançons demandées et payées diminuent, la récupération des données basée sur les sauvegardes a atteint des niveaux presque records et les organisations parviennent de mieux en mieux à négocier les conditions lorsqu'elles acceptent de payer. La baisse spectaculaire des attaques par exploitation de vulnérabilités suggère que la découverte basée sur l'IA et l'investissement soutenu dans la gestion des correctifs portent leurs fruits.

Le signal le plus encourageant issu de ces données pourrait être la reconnaissance accrue des équipes de cybersécurité par les dirigeants. Lorsque les dirigeants montrent de l'intérêt, les équipes suivent. Les tendances opérationnelles positives de ce rapport, de l'amélioration de l'utilisation des sauvegardes à de meilleures issues de négociation, peuvent précisément être le reflet de cette dynamique.

Parallèlement, les défis qui restent à relever sont importants. Plus de la moitié des attaques de ransomware parviennent encore à chiffrer des données, les coûts de rétablissement s'élèvent en moyenne à 1,7 million de dollars par incident et l'impact sur les équipes de cybersécurité est presque universel.

Le constat selon lequel deux tiers des victimes de ransomware relient leur incident à une compromission de l'identité **souligne le rôle essentiel que joue la protection de l'identité dans la chaîne de défense anti-ransomware**. Les organisations qui considèrent l'identité comme une couche de sécurité fondamentale, plutôt que comme un élément passant au second plan, sont mieux placées pour empêcher les attaques de réussir.

Les organisations doivent également se préparer à ce qui sera **le grand défi de cybersécurité de la prochaine décennie : les menaces** augmentées par l'IA. Les données du rapport indiquent déjà pourquoi : 62 % des victimes ont cité une faille de sécurité, connue ou inconnue, comme facteur ayant contribué à leur attaque, et 58 % ont évoqué un manque de personnel ou de compétences. Ces deux lacunes deviennent plus lourdes de conséquences à mesure que l'IA accélère la vitesse et l'ampleur des attaques, les adversaires l'utilisant pour identifier plus rapidement les vulnérabilités et orchestrer des attaques sur plusieurs points de contrôle à la vitesse machine.

La tendance qui se dégage des résultats de cette année (de meilleurs résultats obtenus lorsque les pare-feu ont détecté des attaques à un stade précoce à l'essor de la récupération des données basée sur les sauvegardes) va dans le même sens : **lorsque les défenses opèrent ensemble plutôt qu'isolément, les résultats s'améliorent**. Pour faire face aux attaques de l'ère de l'IA, l'enjeu sera moins d'ajouter de nouveaux outils que de connecter ceux déjà en place afin que le contexte, la détection et la réponse puissent évoluer à la vitesse désormais imposée par les menaces.

Les organisations qui s'en sortiront le mieux face aux ransomwares dans les années à venir seront celles qui auront retenu l'attention des dirigeants sur ce problème tout en adoptant des systèmes défensifs intégrés et optimisés par l'IA, investissant non seulement dans la technologie et les processus, mais aussi dans les personnes qui défendent l'entreprise chaque jour contre ces menaces.

Méthodologie

Cette enquête a été réalisée par Vanson Bourne pour le compte de Sophos au premier trimestre 2026. 2 158 décideurs informatiques et de cybersécurité issus d'organisations ayant été touchées par un ransomware au cours des 12 derniers mois ont été interrogés dans 17 pays : Afrique du Sud, Allemagne, Australie, Brésil, Chili, Colombie, Espagne, Émirats arabes unis, États-Unis, France, Italie, Inde, Japon, Mexique, Singapour, Suisse, et Royaume-Uni. Les répondants provenaient d'organisations comptant entre 100 et 5 000 employés, réparties dans 15 secteurs d'activité.

SOPHOS

Apprenez-en plus sur les ransomwares et sur la façon dont Sophos protège votre organisation sur notre site Web.

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

2026-06-09 FR (DD)