SOPHOS

# L'état des ransomwares dans le secteur de la santé en 2023

**Résultats d'une enquête indépendante et agnostique menée entre janvier et mars 2023 auprès de 3 000 responsables informatiques/cybersécurité dans 14 pays, dont 233 dans le secteur de la santé.**

*Un livre blanc Sophos. Août 2023*

# Introduction

L'étude annuelle de Sophos porte sur les expériences réelles des responsables informatiques et des responsables cybersécurité face aux ransomwares et illustre la réalité à laquelle les organismes de santé seront confrontés en 2023. Ce rapport révèle les causes premières à l'origine des attaques et met en lumière l'impact des ransomwares sur ce secteur. Il dévoile également l'impact commercial et opérationnel que peut avoir le fait de payer une rançon pour récupérer des données plutôt que d'utiliser des sauvegardes.

## À propos de l'enquête

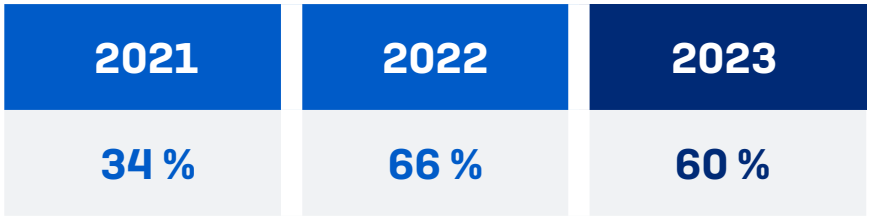
Sophos a commandé une enquête indépendante auprès de 3 000 responsables informatiques/cybersécurité travaillant dans des entreprises de 100 à 5 000 employés, répartis dans 14 pays sur le continent américain, dans la région EMEA et dans la région Asie-Pacifique. 233 participants étaient issus du secteur de la santé. Cette enquête s'est déroulée entre janvier et mars 2023 ; les participants ayant été invités à répondre sur la base de leurs expériences vécues en 2022.

# Taux d'attaques par ransomware dans le secteur de la santé

Notre enquête de 2023 montre que le taux d'attaques par ransomware dans le secteur de la santé est passé de 66 % à 60 % sur les douze derniers mois. Mais malgré cette tendance à la baisse, ce taux représente en réalité presque le double du taux rapporté dans l'enquête de 2021, où 34 % des organismes de santé avaient déclaré avoir été touchés par des ransomwares.

Bien que le secteur ait observé une diminution de la fréquence des attaques, avec près des deux tiers des organismes de santé touchés par un ransomware l'année dernière, il est clair que les adversaires sont capables d'exécuter des attaques à grande échelle de manière systématique, et les ransomwares sont incontestablement le plus grand cyber risque auquel ces organismes sont confrontés aujourd'hui.

Depuis plusieurs années, les cybercriminels développent et perfectionnent le modèle de « ransomware-as-a-service ». Ce modèle abaisse les barrières et facilite l'entrée de cybercriminels potentiels, tout en augmentant la sophistication des attaques en permettant aux adversaires de se spécialiser dans différentes étapes d'une attaque. Pour plus d'informations sur les ransomwares « as-a-service », consultez le Rapport Sophos 2023 sur les menaces.




Au cours de l'année passée, votre organisation a-t-elle été touchée par un ransomware ? Oui. n=233 (2023), 381 (2022), 328 (2021)

Contrairement à la baisse du taux d'attaques par ransomware dans le secteur de la santé, la tendance mondiale tous secteurs confondus reste stable. En effet, aussi bien dans l'enquête de 2023 que dans celle de 2022, 66 % des personnes interrogées ont déclaré que leur organisation avait été victime d'un ransomware l'année précédente.

Sur l'ensemble des secteurs, l'éducation apparaît comme le secteur le plus touché, avec 80 % des établissements du primaire/secondaire et 79 % des établissements du supérieur ayant subi une attaque. Le segment regroupant l'informatique, les technologies et les télécoms a signalé le niveau d'attaque le plus bas (50 %), supposant un meilleur niveau de préparation et de défenses cyber dans ces secteurs.

## Causes premières des attaques de ransomware dans le secteur de la santé

La compromission d'identifiants (32 %) apparaît comme la cause première la plus fréquemment citée par les participants du secteur de la santé, suivie de près par l'exploitation de vulnérabilités (29 %). Les attaques par email (emails malveillants ou phishing) ont été le point de départ de plus d'un tiers des attaques (36 %) dans les organismes de santé, un chiffre supérieur à la moyenne transsectorielle de 30 %.

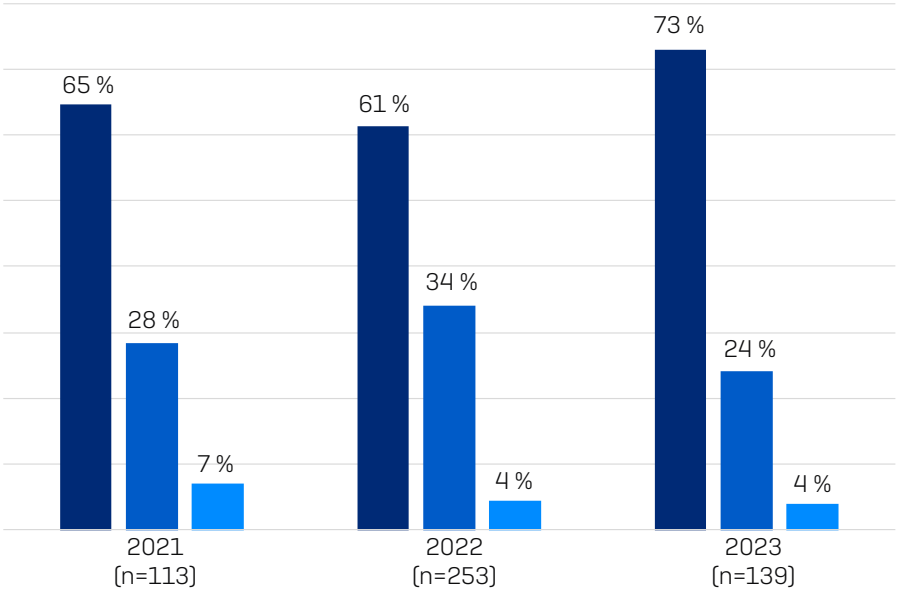
Au niveau mondial et tous secteurs confondus, l'ordre des deux causes premières est inversé, avec l'exploitation des vulnérabilités qui occupe la première place (dans 36 % des attaques), suivie par la compromission d'identifiants (à l'origine de 29 % des attaques).

| | SANTÉ (n=139) | MOYENNE GLOBALE (n=1 974) |
|---|---|---|
| Vulnérabilité exploitée | 29 % | 36 % |
| Identifiants compromis | 32 % | 29 % |
| Email malveillant | 22 % | 18 % |
| Phishing | 14 % | 13 % |
| Attaque par force brute | 1 % | 3 % |
| Téléchargement | 1 % | 1 % |

# Taux de chiffrement des données dans le secteur de la santé

Le secteur de la santé a subi le taux de chiffrement des données le plus élevé des trois dernières années, avec près de trois quarts des organismes de santé (73 %) déclarant que leurs données avaient été chiffrées, contre 61 % dans le rapport 2022 et 65 % dans le rapport 2021. Cela reflète probablement le niveau de compétence toujours plus élevé des adversaires qui continuent d'innover et d'affiner leurs approches.

Dans le secteur, le taux d'attaques basées sur l'extorsion uniquement est resté stable à 4 %, en deçà des 7 % rapportés en 2021.




Oui - Les données ont été chiffrées
Non - L'attaque a été stoppée avant que les données ne soient chiffrées
Non - Les données n'ont pas été chiffrées, mais une rançon nous a été exigée (extorsion).

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

Bien qu'élevé, le taux de chiffrement des données signalé par le secteur de la santé est inférieur à la moyenne transsectorielle, qui elle atteint les 76 %. La fréquence la plus élevée de chiffrement des données (92 %) a été signalée par le secteur des services aux entreprises et des services professionnels.

En plus d'avoir été chiffrées, les données ont également été volées dans plus d'un tiers des attaques (37 %) visant ce secteur. Cette approche dite du « double dip » devient de plus en plus courante, car les adversaires cherchent tous les moyens possibles de monétiser leurs attaques. Ils peuvent menacer de rendre publiques des données volées pour extorquer de l'argent ou même vendre ces données. Le nombre élevé des vols de données accroît l'importance de stopper les attaques le plus tôt possible, avant que les informations ne soient exfiltrées.

**37 %**
des attaques de ransomware touchant le secteur de la santé où des données ont été chiffrées ont aussi volé des données.

Lors de l'attaque par ransomware, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ?
Oui/Oui, et les données ont aussi été volées ; n=101/37

# Taux de récupération des données dans le secteur de la santé

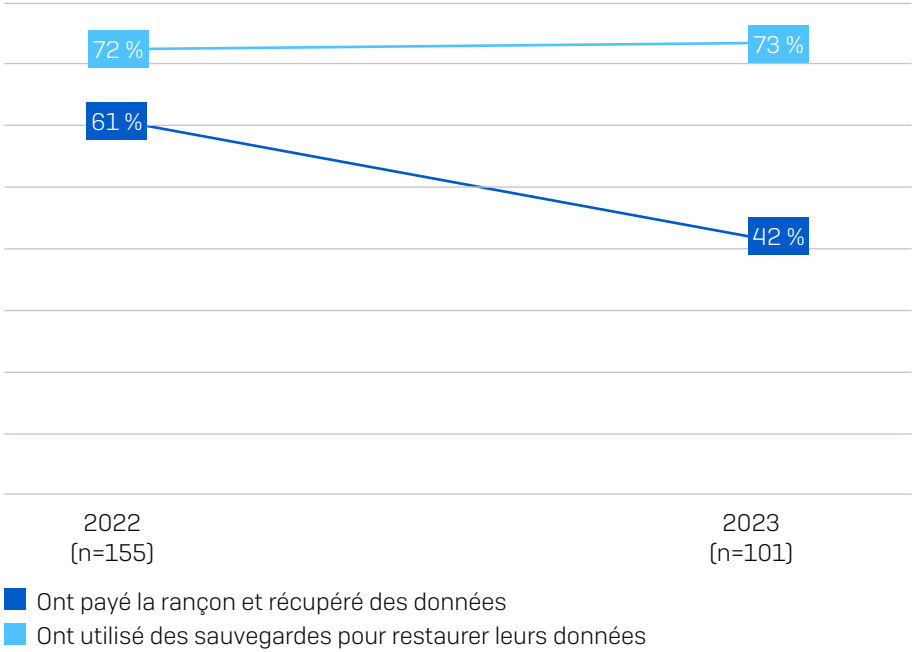
La bonne nouvelle est que tous les organismes de santé (100 %) qui ont vu leurs données chiffrées ont été en mesure de les récupérer, alors que la moyenne transsectorielle est de 97 %.

Ajoutons que 73 % des organismes ayant eu leurs données chiffrées ont utilisé des sauvegardes pour les récupérer, soit une très légère hausse par rapport aux 72 % de 2022. Il est néanmoins encourageant de noter la baisse de la propension à payer la rançon pour récupérer ses données : 42 % des personnes interrogées dans le secteur de la santé ont déclaré avoir payé une rançon pour récupérer leurs données, contre 61 % dans le rapport de l'an dernier.  Et 17 % des participants ont déclaré avoir utilisé plusieurs méthodes pour récupérer leurs données chiffrées.

| | SANTÉ | MOYENNE GLOBALE |
|---|---|---|
| Ont récupéré des données | **100 %** | **97 %** |
| Ont utilisé des sauvegardes pour restaurer des données | **73 %** | **70 %** |
| ont payé la rançon pour récupérer des données | **42 %** | **46 %** |
| ont utilisé d'autres moyens pour récupérer des données | **2 %** | **2 %** |

Votre entreprise a-t-elle récupéré des données ? Oui, nous avons eu recours aux sauvegardes pour restaurer nos données ; Oui, nous avons payé la rançon et récupéré nos données ; Oui, nous avons utilisé d'autres moyens pour récupérer nos données. n=1 497 (tous secteurs) ; n=101 (santé).

Dans le secteur de la santé, le taux de paiement de la rançon est non seulement nettement inférieur à celui de l'année précédente, mais aussi à la moyenne transsectorielle de 46 %. À l'échelle mondiale, le taux de paiement de la rançon est resté stable d'une année sur l'autre, tandis que l'utilisation des sauvegardes est passée de 73 % en 2022 à 70 % en 2023.




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.

# L'impact de l'assurance sur la propension à payer la rançon

Si le taux global de récupération des données atteint les 100 % dans le secteur étudié, les méthodes utilisées varient en fonction de la couverture d'assurance. Les organisations ayant souscrit une cyberassurance à part entière ont rapporté une plus forte propension à payer la rançon que celles bénéficiant de clauses cyber dans le cadre d'une assurance plus globale.

Plus de la moitié des organismes de santé (50 %) qui ont eu des données chiffrées et qui disposaient d'une police d'assurance cyber autonome ont payé la rançon. Ce pourcentage est tombé à 34 % pour les organismes ayant souscrit une police d'assurance globale incluant des clauses cyber.

**Impact de l'assurance sur le paiement de la rançon dans le secteur de la santé**

| Police d'assurance spécifique cyber | Police d'assurance 'classique' avec clause cyber |
|---|---|
| **53 %** ont payé la rançon | **34 %** ont payé la rançon |

Votre entreprise a-t-elle récupéré des données ? Oui, nous avons payé la rançon et avons récupéré des données n= 101 organismes de santé touchés par un ransomware en 2022 ayant eu des données chiffrées (45 avec une police dédiée cyber, 53 avec une police classique avec clause cyber, 10 sans police cyber)

# Montant des rançons payées

Si la propension mondiale, tous secteurs confondus, à payer la rançon reste au même niveau que celle révélée dans notre enquête précédente, les sommes versées ont considérablement augmenté sur les douze derniers mois, passant en moyenne de 812 380 dollars à 1 542 333 dollars. Le paiement médian de la rançon est passé de 76 500 dollars à 400 000 dollars d'une année sur l'autre.

Dans le secteur de la santé, 12 organismes nous ont communiqué les montants exacts versés pour la rançon, la médiane s'élevant à 2,5 millions de dollars, soit 30 000 dollars de plus que 2022.

Neuf organismes ont déclaré avoir payé des rançons d'un million de dollars ou plus, et un seul a payé moins de 100 000 dollars. Malgré le faible nombre de participants, qui signifie que les données du rapport 2023 ne sont pas statistiquement significatives et doivent donc être utilisées avec prudence, les résultats montrent néanmoins que les paiements de rançons dans le secteur de la santé sont en augmentation.

| | 2022 | 2023 |
|---|---|---|
| Moyenne globale | 812 360 $ (moyenne)<br>76 500 $ (médiane) | 1 542 330 $ (moyenne)<br>400 000 $ (médiane) |
| Santé | 196 749 $ (moyenne)<br>30 000 $ (médiane) | 2 884 167 $ (moyenne)<br>2 500 000 $ (médiane) |

Quel était le montant de la rançon payée aux attaquants ? À l'exclusion des réponses « Ne sait pas » et des valeurs aberrantes. Tous secteurs confondus : n=216 (2023)/965 (2022) ; Secteur de la santé : n=12 (2023)/83 (2022).

*La base de participants du secteur de la santé dans l'étude 2023 sans cyberassurance n'est pas assez élevée pour que les résultats puissent être considérés comme indicatifs.

## Coûts de rétablissement

Le montant de la rançon ne représente qu'une partie du coût de rétablissement encouru par l'entreprise après une attaque par ransomware. Sur l'ensemble des secteurs, les entreprises ont estimé le coût de rétablissement après une attaque par ransomware (en excluant le montant des rançons payées) à 1,82 million de dollars en moyenne. C'est une hausse par rapport au montant de 1,4 million de dollars de 2022 (qui englobait les rançons payées) et correspond au montant de 1,85 million de dollars rapporté dans l'enquête de 2021.

Conformément à la tendance mondiale, le coût de rétablissement pour les organismes de santé est passé de 1,85 million de dollars à 2,20 millions de dollars d'une année sur l'autre et représente presque le double des 1,27 million de dollars rapportés par le secteur dans notre enquête de 2021. Cette augmentation est probablement tributaire de la fréquence accrue du chiffrement des données dans les attaques de ransomware.

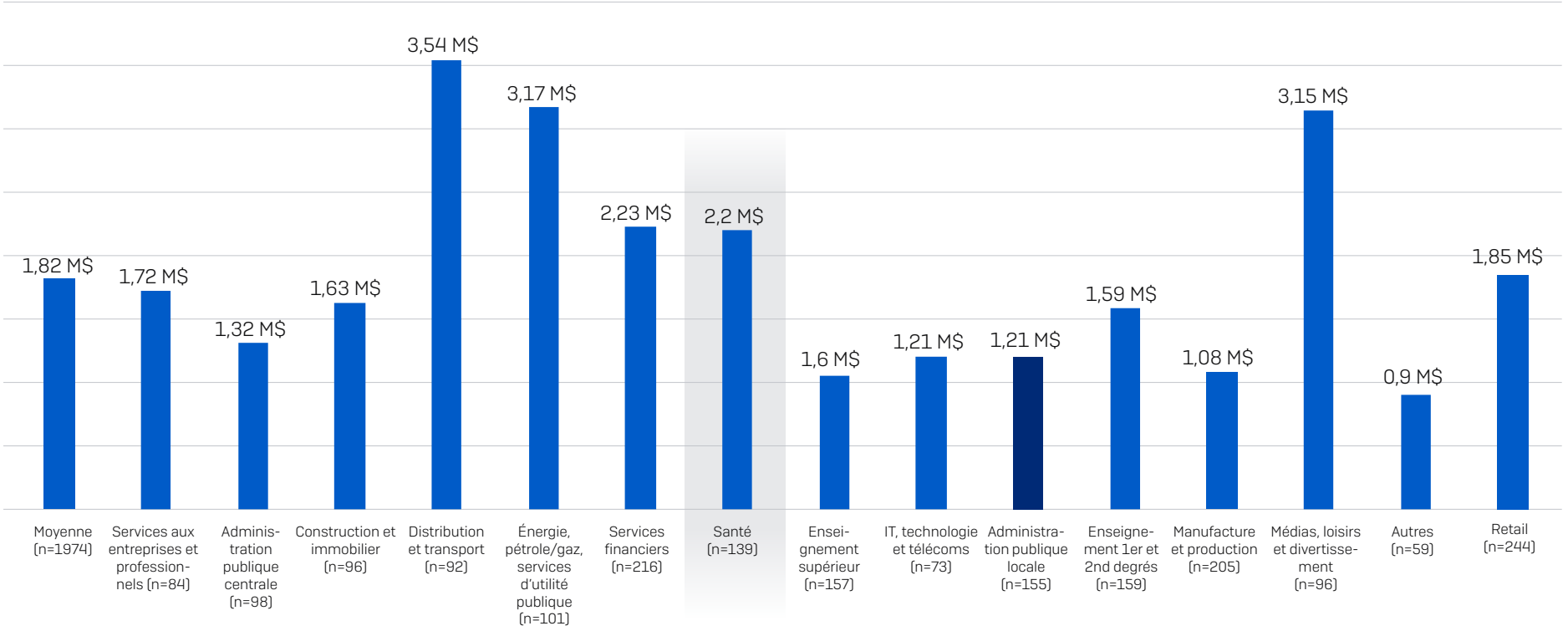
| | 2021 | 2022 | 2023 |
|---|---|---|---|
| Moyenne globale | 1,85 M$ | 1,4 M$ | 1,82 M$ |
| Santé | 1,27 M$ | 1,85 M$ | 2,20 M$ |

Quel était le coût approximatif payé par votre entreprise pour remédier aux conséquences de l'attaque par ransomware la plus significative (en prenant en compte les interruptions de services, le temps passé à la résolution de l'incident, les coûts matériels, les pertes d'exploitation, etc.) ? Tous secteurs confondus : n=1 974 (2023)/3 702 (2022)/2 006 (2021) Secteur de la santé : n=139 (2023)/253 (2022)/113 (2021).

Remarque : dans leur formulation, les questions posées en 2022 et 2021 incluaient également le paiement des rançons.

Les coûts de rétablissement dans le secteur de la santé étaient supérieurs à la moyenne transsectorielle de 1,82 million de dollars. Le secteur de la distribution et des transports a accusé le coût de rétablissement le plus élevé (3,54 millions de dollars), soit presque le double de la moyenne mondiale.

**Coût de rétablissement après l'attaque par ransomware la plus importante (en millions de dollars)**




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

# Coût de rétablissement par méthode de récupération des données

La présente enquête confirme que l'utilisation des sauvegardes est un moyen plus économique pour récupérer ses données chiffrées que le paiement de la rançon.

Tous secteurs confondus, le coût médian de rétablissement pour les entreprises ayant utilisé des sauvegardes est deux fois moins élevé (375 000 dollars) que le coût de celles ayant payé une rançon (750 000 dollars). De même, le coût moyen de rétablissement est inférieur de près d'un million de dollars pour celles ayant utilisé des sauvegardes par rapport à celles ayant payé la rançon.

On observe la même tendance pour le secteur de la santé, où le coût médian de rétablissement pour les organismes ayant utilisé des sauvegardes est moins élevé (2,11 millions de dollars) que le coût de ceux ayant payé une rançon (2,58 millions de dollars).

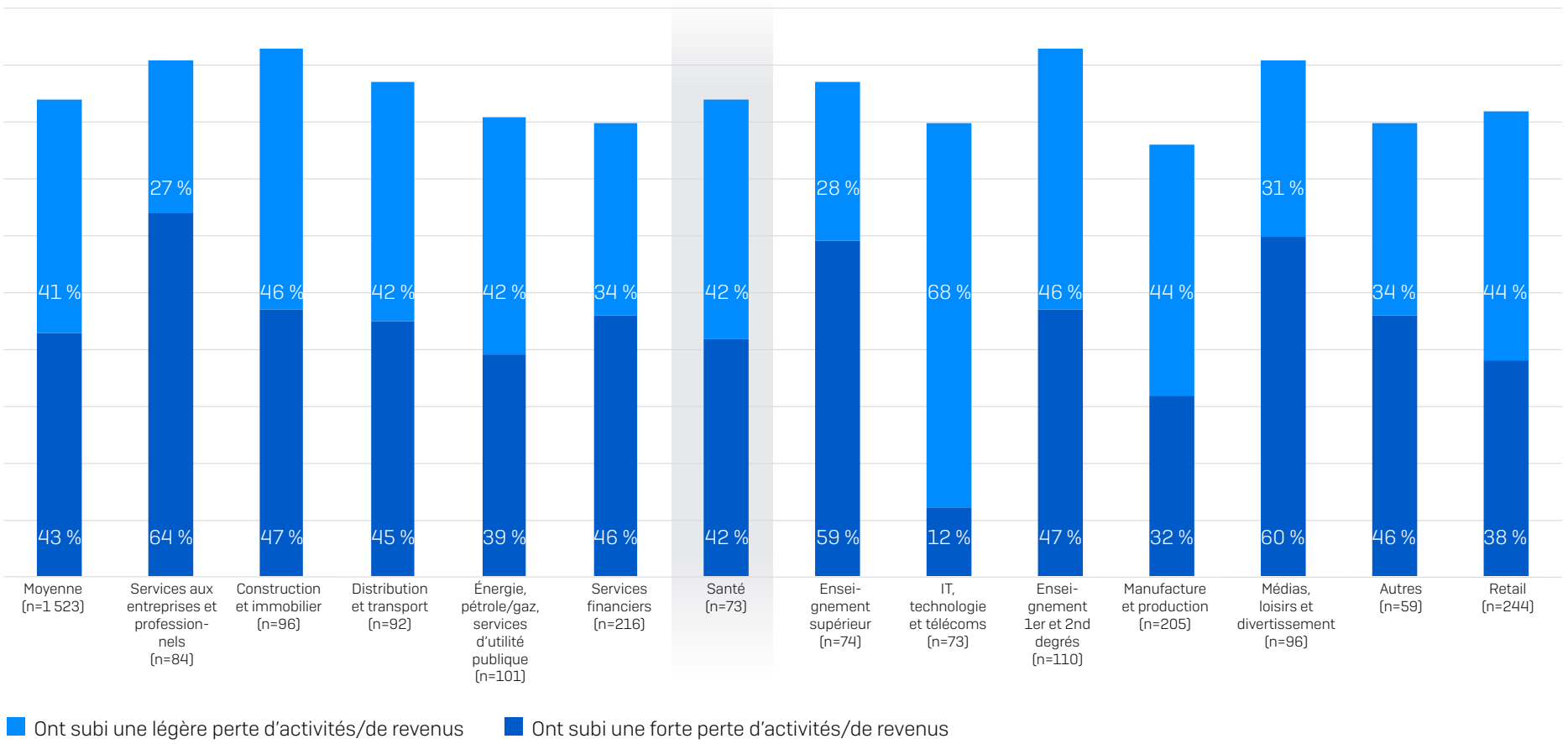
| | Ont payé la rançon et ont récupéré leurs données | Ont utilisé des sauvegardes pour restaurer leurs données |
|---|---|---|
| Moyenne globale | **750 000 $** médiane<br>**2,6 M$** moyenne | **375 000 $** médiane<br>**1,62 M$** moyenne |
| Santé | **750 000 $** médiane<br>**2,58 M$** moyenne | **750 000 $** médiane<br>**2,11 M$** moyenne |

Quel était le coût approximatif payé par votre entreprise pour remédier aux conséquences de l'attaque par ransomware la plus significative (en prenant en compte les interruptions de services, le temps passé à la résolution de l'incident, les coûts matériels, les pertes d'exploitation, etc.) ? Tous secteurs confondus : n=694 ont payé la rançon et ont récupéré des données et n=1 053 ont utilisé des sauvegardes pour restaurer les données.

Santé : n=42 ont payé la rançon et ont récupéré des données et n=74 ont utilisé des sauvegardes pour restaurer les données.

# Impact commercial

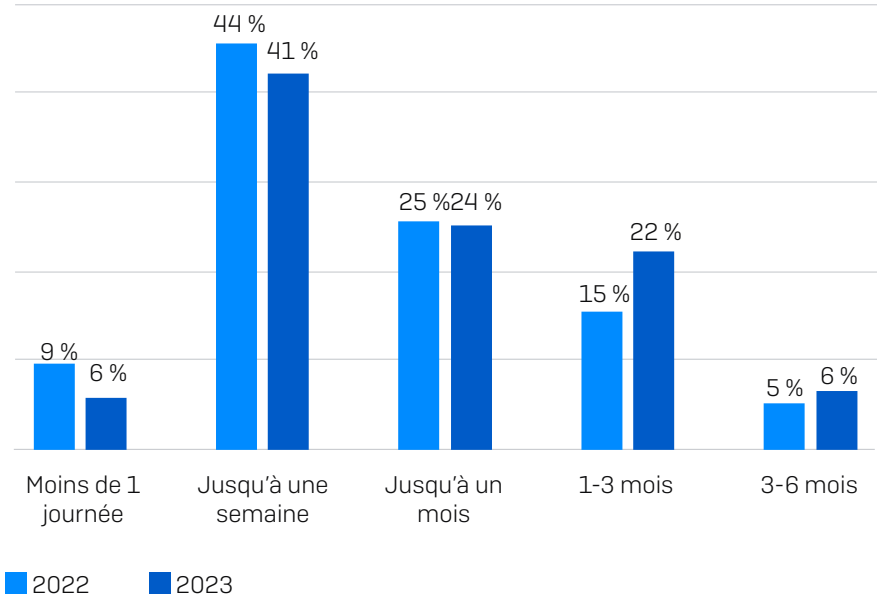
85 % des organismes de santé victimes d'un ransomware ont déclaré que l'attaque avait entraîné une perte d'activité ou de chiffre d'affaires, soit un pourcentage légèrement supérieur à la moyenne mondiale de 84 %. Le secteur de l'enseignement des premier et second degrés (94 %) et celui de la construction et de l'immobilier (93 %) ont déclaré avoir perdu une petite partie de leurs activités/recettes, tandis que les services aux entreprises et les services professionnels sont ceux qui ont perdu la grosse partie de leurs activités/recettes (64 %). À l'inverse, dans le secteur bien préparé regroupant l'informatique, les technologies et les télécoms, seuls 12 % ont déclaré avoir subi une forte perte de revenus.




L'attaque par ransomware a-t-elle entraîné une perte d'activité ou de revenus ? Oui, nous avons subi une forte perte d'activités/de revenus
Oui, nous avons subi une légère perte d'activités/de revenus. Entreprises du secteur privé victimes d'un ransomware, chiffres de base dans le tableau

## Temps de rétablissement

Les organismes de santé mettent plus de temps à se rétablir suite à une attaque de ransomware. En effet, seulement 47 % d'entre eux sont capables de se rétablir en une semaine, contre 54 % dans le rapport de 2022. De plus, le pourcentage d'organismes ayant plus d'un mois à se rétablir a augmenté de 7 % (avec arrondis) à 21 % (avec arrondis) d'une année sur l'autre.



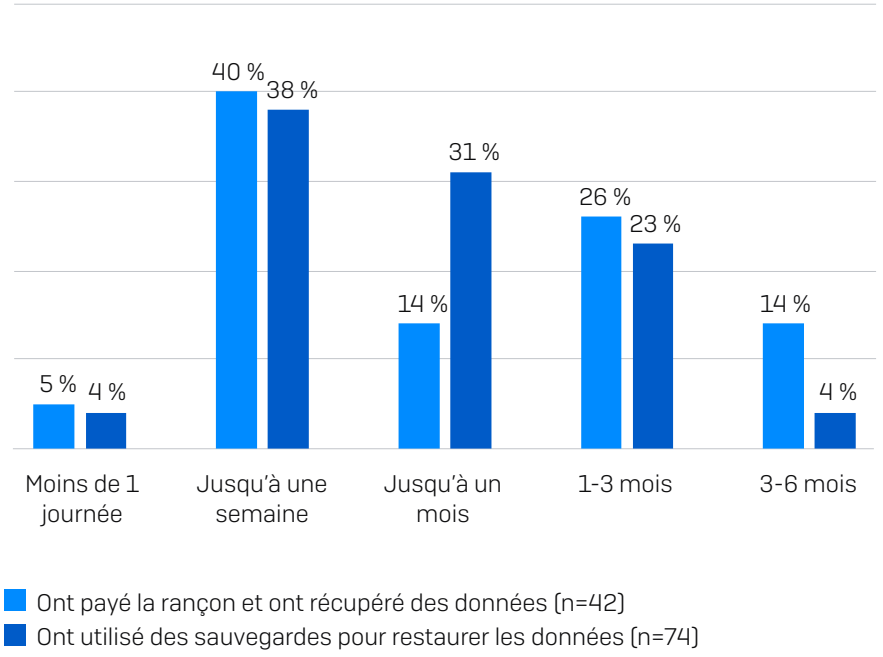

Combien de temps a-t-il fallu à votre organisation pour se rétablir complètement après l'attaque de ransomware ?
139 (en 2023)/253 (en 2022) organismes de santé ayant été touchés par un ransomware.

## Temps de rétablissement par méthode de récupération des données

L'étude a révélé que les organismes de santé utilisant des sauvegardes pour restaurer leurs données se rétablissent plus rapidement que celles ayant payé une rançon.

Un quart des personnes interrogées (arrondi à 27 %) ayant utilisé des sauvegardes ont mis plus d'un mois à récupérer leurs données, alors que 40 % (arrondi) des organismes ayant payé la rançon ont mis plus d'un mois à le faire.

Bien que ces deux options de réponse ne s'excluent pas mutuellement et que certaines organisations interrogées aient à la fois payé la rançon et utilisé des sauvegardes, l'avantage des sauvegardes dans le processus de rétablissement est évident.




Combien de temps a-t-il fallu à votre organisation pour se rétablir complètement après l'attaque de ransomware ?
Entreprises ayant payé la rançon ou utilisé des sauvegardes pour récupérer leurs données. Chiffres de base dans le graphique.

# Conclusion

Les ransomwares restent une menace majeure pour les organismes du secteur de la santé. Bien que le secteur rapporte une baisse du taux de ransomware dans l'enquête de cette année, près des deux tiers (60 %) des personnes interrogées ont été touchées par ce type d'attaque.

Alors que les adversaires continuent de perfectionner leurs tactiques, techniques et procédures d'attaque (TTP), les défenseurs ont du mal à suivre le rythme. Cela se traduit par des niveaux d'attaque et un taux de chiffrement à la hausse : les trois quarts (73 %) des organismes de santé victimes de ransomware ont vu leurs données chiffrées, soit une hausse par rapport aux 61 % de l'année précédente. En outre, 37 % d'entre eux ayant eu leurs données chiffrées ont déclaré qu'elles avaient également été volées.

Fait encourageant, le secteur de la santé a signalé une baisse de la propension à payer la rançon pour la récupération des données chiffrées, diminuant de 61 % en 2022 à 42 % dans le rapport 2023.

Dans le même temps, l'utilisation de sauvegardes dans ce secteur n'a que légèrement augmenté, passant de 72 % à 73 % en une année. La bonne nouvelle est que tous les organismes de santé (100 %) ayant vu leurs données chiffrées ont été en mesure de les récupérer après l'attaque, alors que la moyenne transsectorielle est de 97 %.

Autre point, la posture des organismes en matière d'assurance semble avoir un impact sur la méthode de récupération des données. En effet, alors que 53 % des organismes dont les données ont été chiffrées et qui disposaient d'une police d'assurance cyber autonome ont payé la rançon, ce pourcentage tombe à 34 % pour les organismes ayant souscrit une police d'assurance globale incluant des clauses cyber.

Le coût global de rétablissement pour les organismes du secteur est passé de 1,85 million de dollars à 2,20 millions de dollars d'une année sur l'autre, probablement (et en partie) en raison de l'augmentation du taux de chiffrement suivant les attaques. Il est donc supérieur à la moyenne transsectorielle de 1,82 million de dollars.

Face à la généralisation du modèle de « ransomware-as-a-service », Sophos ne s'attend pas à une diminution des attaques courant 2023.

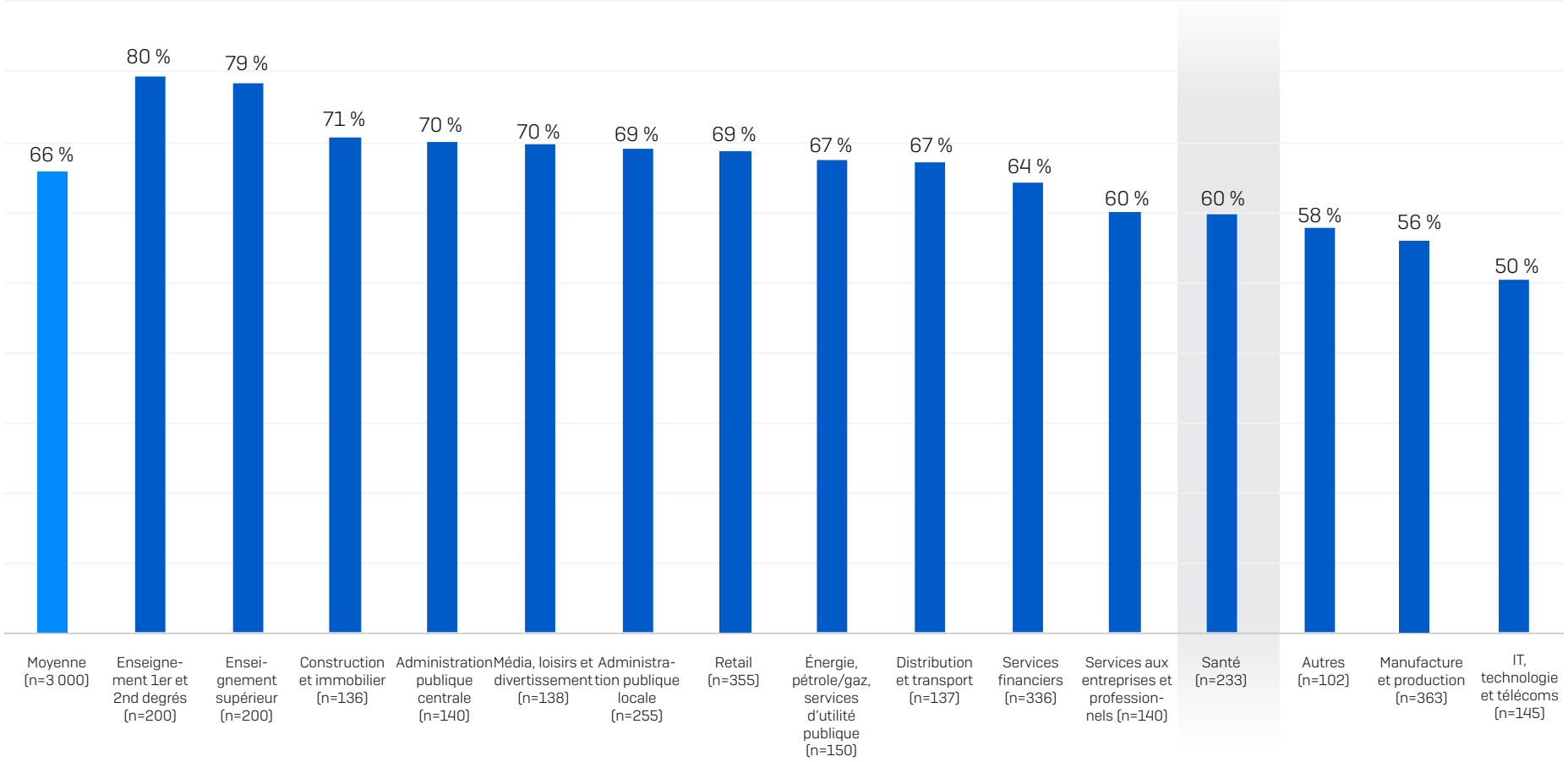
Les entreprises devraient concentrer leurs efforts sur :

- Renforcer davantage leurs boucliers défensifs avec :
  - Des outils de sécurité qui protègent contre les vecteurs d'attaque les plus courants, y compris une protection Endpoint dotée de fortes capacités anti-exploit pour empêcher l'exploitation des vulnérabilités et un accès réseau Zero Trust (ZTNA) pour contrecarrer l'utilisation abusive d'identifiants compromis.
  - Des technologies adaptatives qui répondent automatiquement aux attaques, interrompant les adversaires et donnant aux défenseurs le temps de répondre.
  - Une solution de détection des menaces, d'investigation et de réponse 24/7, assurée en interne ou en partenariat avec un fournisseur de services MDR spécialisé.
- Se préparer aux attaques, notamment en effectuant des sauvegardes régulières, en s'entraînant à récupérer les données à partir des sauvegardes et en maintenant à jour un plan de réponse aux incidents.
- Maintenir une bonne hygiène de sécurité, notamment par l'application des correctifs le plus tôt possible et l'examen régulier de la configuration des outils de sécurité.

# Autres graphiques

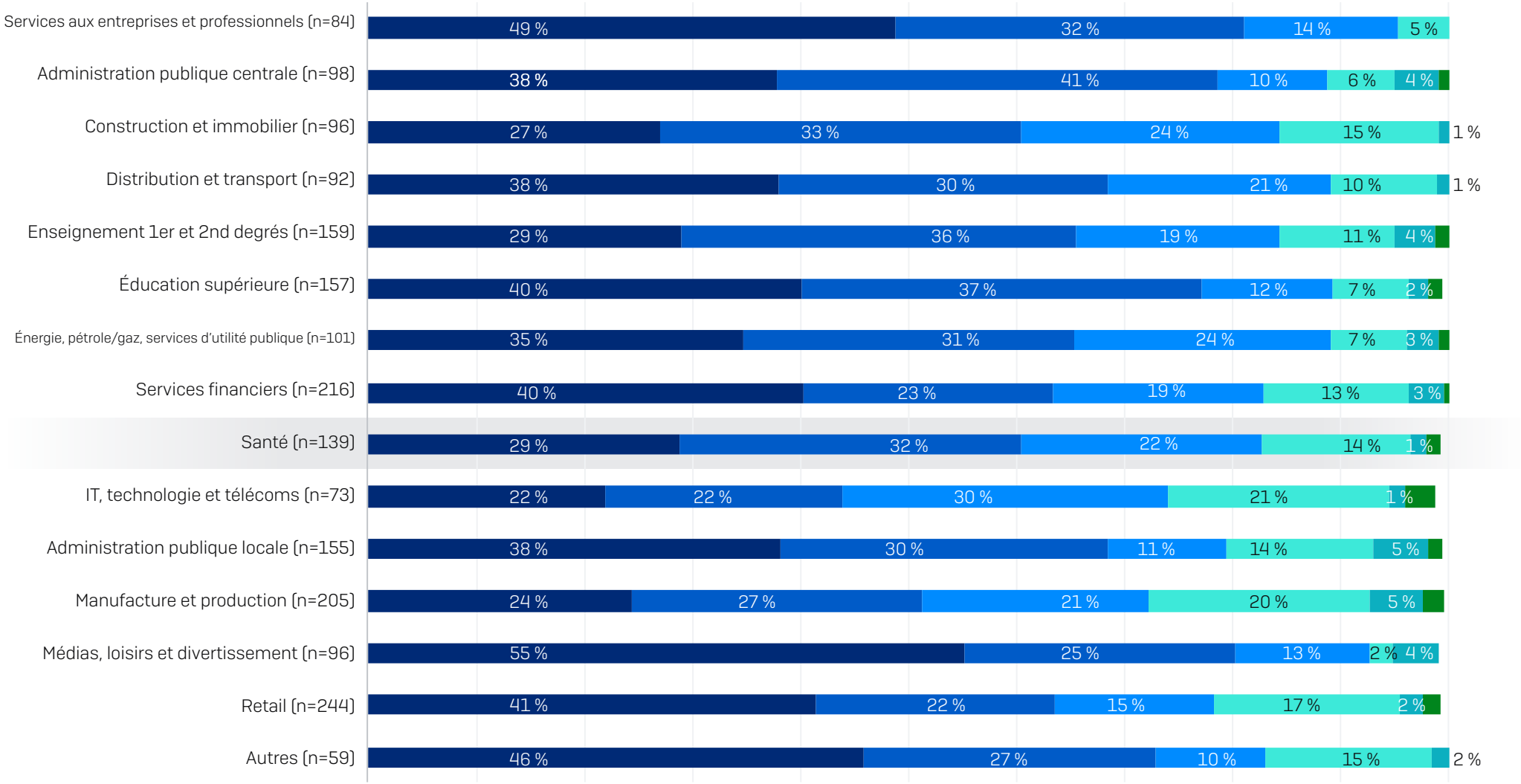
## Attaques de ransomware par secteur

**Pourcentage d'entreprises touchées par un ransomware**



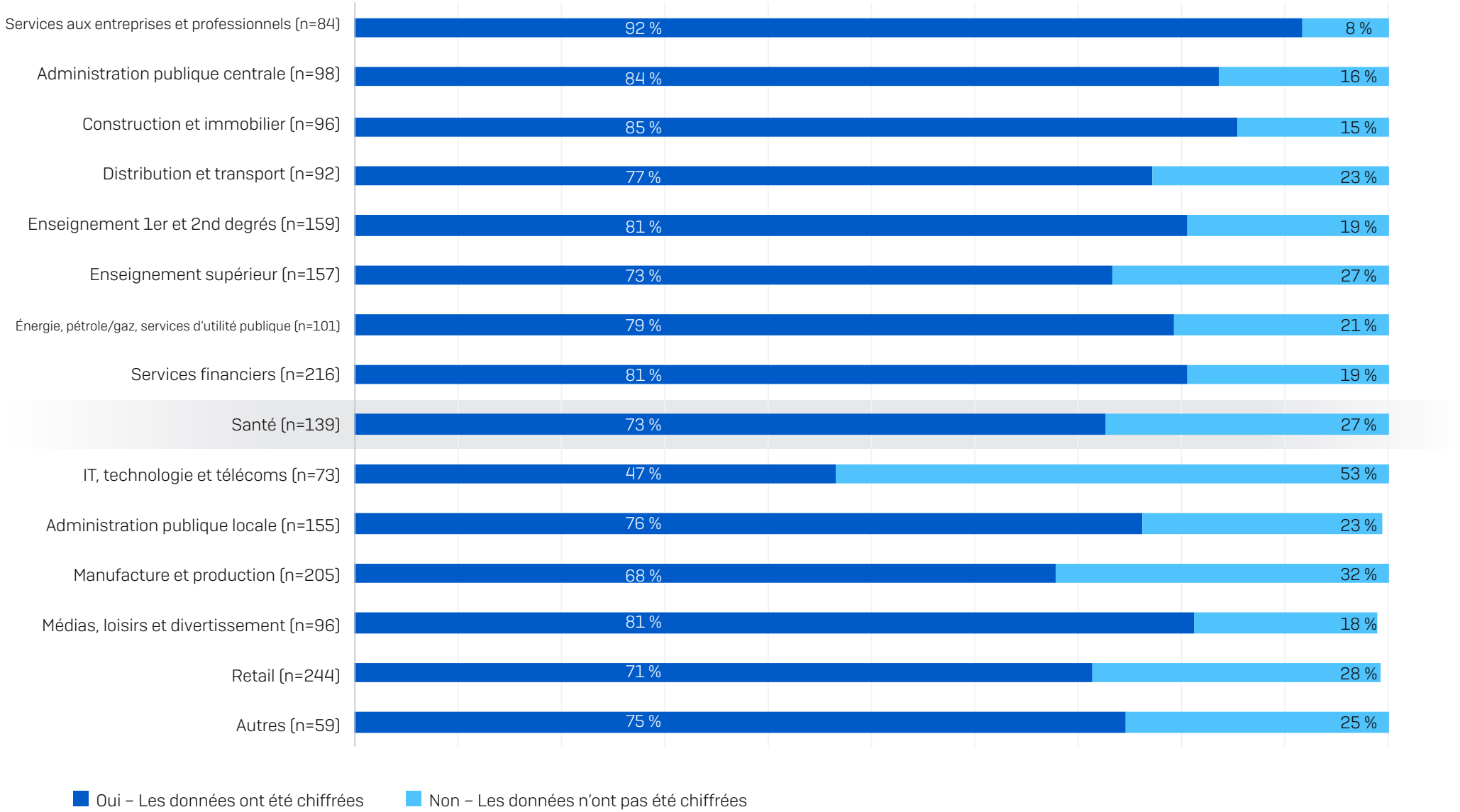

Au cours de l'année passée, votre organisation a-t-elle été touchée par un ransomware ? Chiffres de base dans le graphique.

## Causes premières de l'attaque par secteur



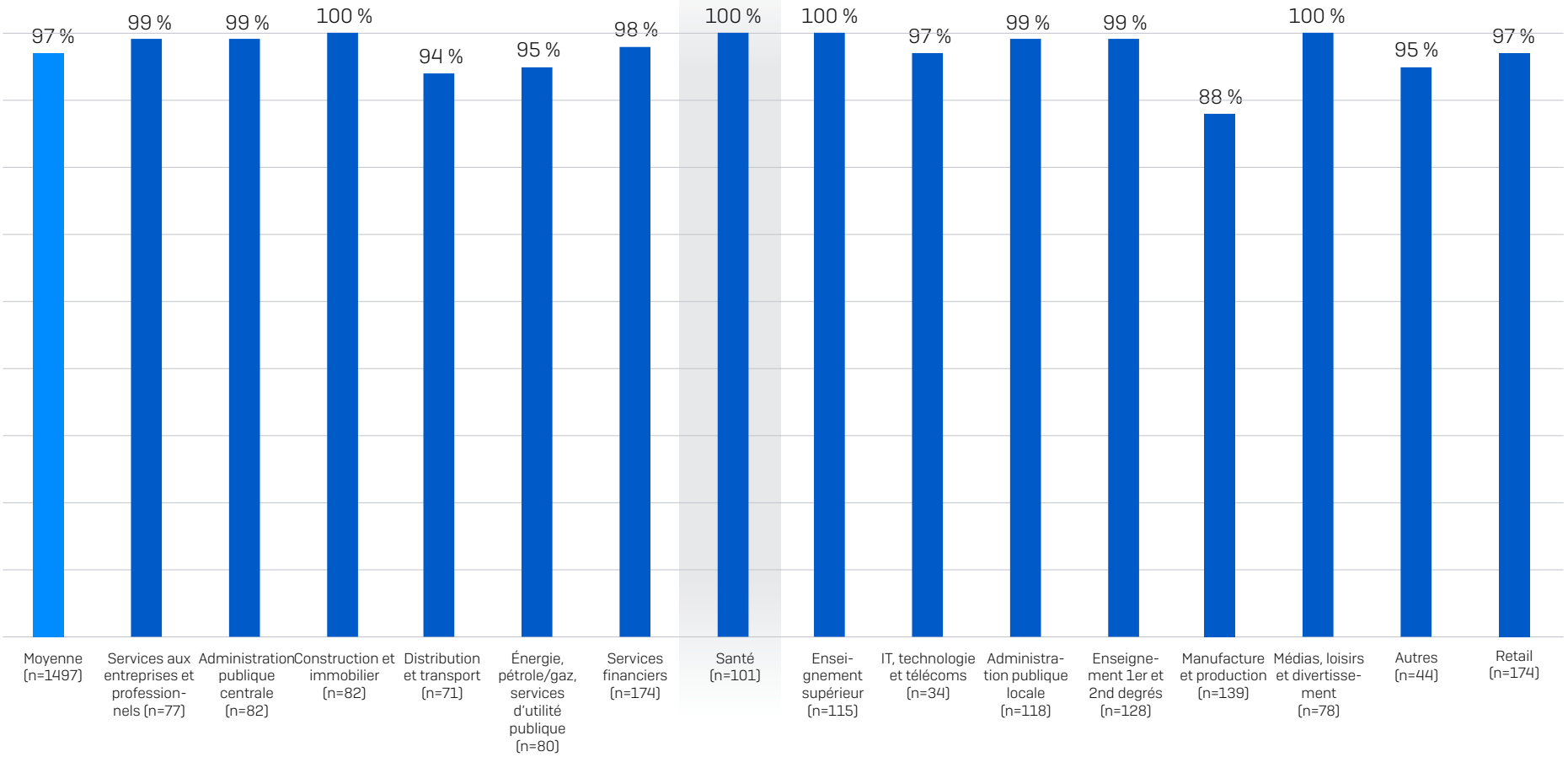

Connaissez-vous la cause première de l'attaque de ransomware dont votre entreprise a été victime au cours de l'année écoulée ? Sélection des options de réponse. Chiffres de base dans le graphique.

## Chiffrement des données par secteur



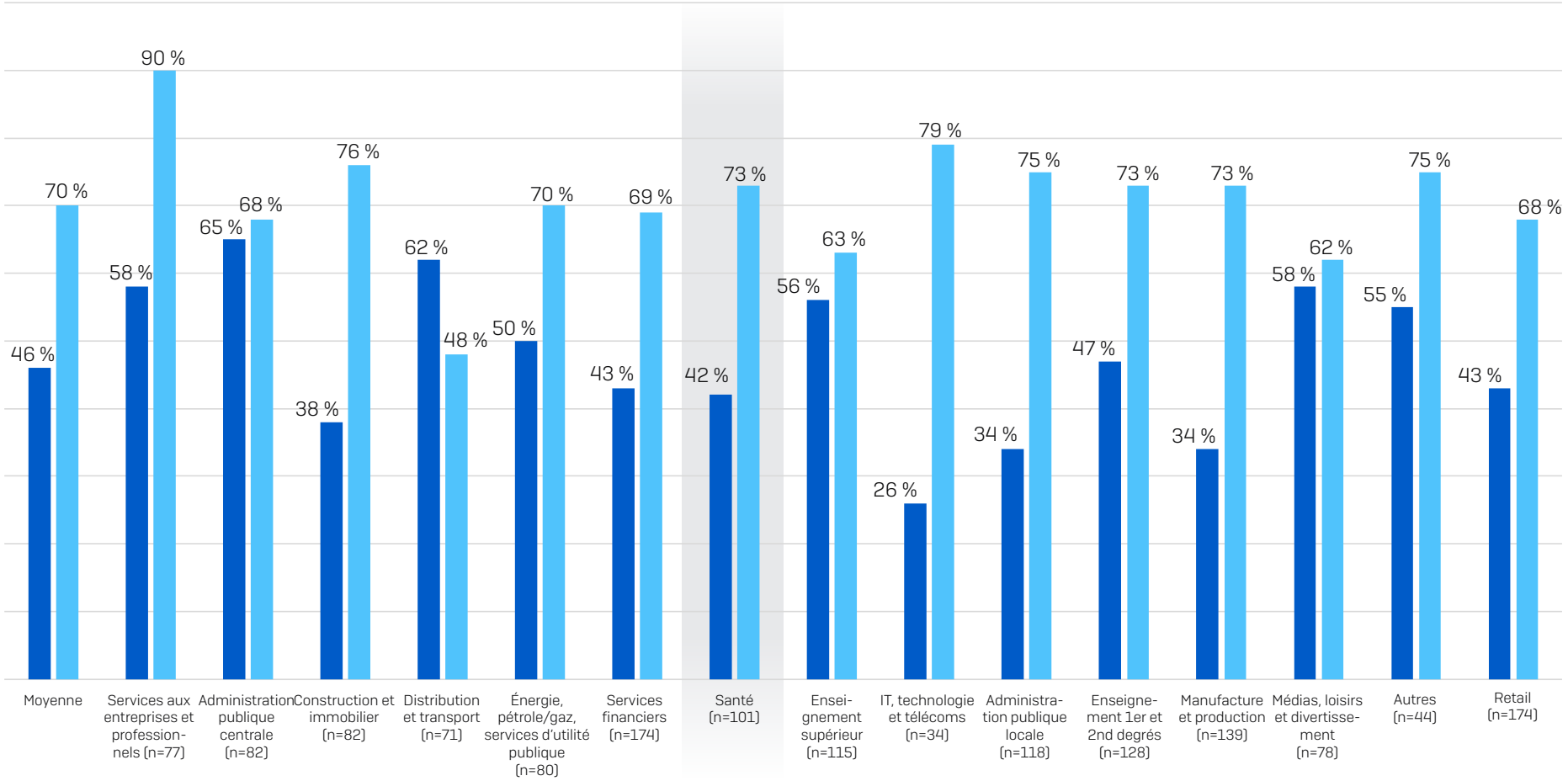

Lors de l'attaque par ransomware, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ? Consolidation des options de réponse. Chiffres de base dans le graphique.

## Taux de récupération des données




Votre entreprise a-t-elle récupéré des données ? n= 1 497 entreprises touchées par un ransomware ayant eu des données chiffrées.

## Paiement de la rançon et utilisation des sauvegardes pour la récupération des données




Votre entreprise a-t-elle récupéré des données ? n= 1 497 entreprises touchées par un ransomware ayant eu des données chiffrées.

# Méthodologie

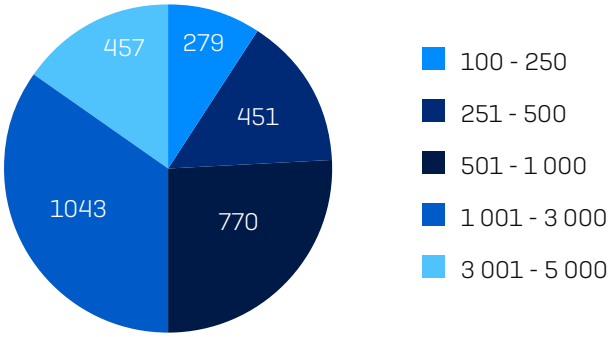
Sophos a commandé une enquête indépendante et agnostique auprès de 3 000 responsables informatiques (RSI) et responsables cybersécurité (RSSI), qui a été réalisée entre janvier et mars 2023. Les personnes interrogées étaient basées dans 14 pays du continent américain, de la région EMEA (Europe, Moyen-Orient, Afrique) et de la région Asie-Pacifique.

Toutes les personnes interrogées provenaient d'entreprises comptant entre 100 et 5 000 employés (50 % : 100-1 000 employés, 50 % : 1 001-5 000 employés). Au sein de la cohorte d'étude, le chiffre d'affaires annuel allait de moins de 10 millions de dollars à plus de 5 milliards de dollars.

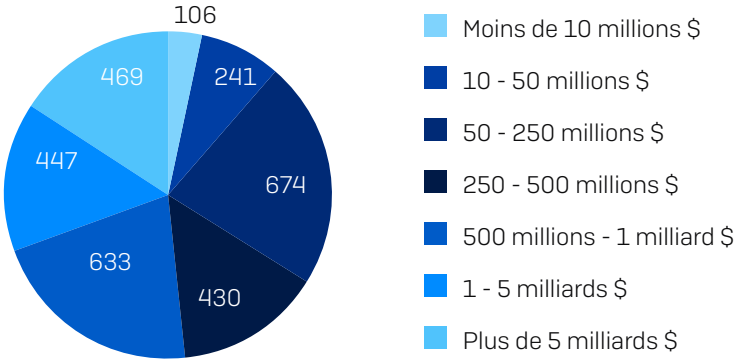
## Répondants par pays

| PAYS | NOMBRE DE RÉPONDANTS | PAYS | NOMBRE DE RÉPONDANTS |
|---|---|---|---|
| États-Unis | 500 | Royaume-Uni | 200 |
| Allemagne | 300 | Afrique du Sud | 200 |
| Inde | 300 | France | 150 |
| Japon | 300 | Espagne | 150 |
| Australie | 200 | Autriche | 100 |
| Brésil | 200 | Singapour | 100 |
| Italie | 200 | Suisse | 100 |

## Répondants selon la taille de l'entreprise (nombre d'employés)




## Répondants selon la taille de l'entreprise (CA annuel)




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.



2023-08-03 (WP-NP)

SOPHOS