RAPPORT

# L'état des ransomwares dans le secteur de l'éducation en 2026

Résultats d'une enquête indépendante menée auprès de 226 responsables IT et cybersécurité du secteur de l'éducation dans 17 pays, dont les organisations ont été touchées par un ransomware au cours de l'année écoulée.

SOPHOS

# Introduction

Bienvenue dans la sixième édition du rapport annuel sur l'état du ransomware dans l'éducation de Sophos, qui révèle la réalité du ransomware pour les fournisseurs d'enseignement des 1er et 2nd degrés (incluant notamment les écoles primaires et secondaires — généralement pour les élèves de moins de 18 ans) et de l'enseignement supérieur (universités, collèges et établissements équivalents — généralement pour les étudiants de plus de 18 ans) en 2026.

Le rapport de cette année jette également un nouvel éclairage sur des domaines jusque-là inexplorés, notamment l'origine des attaques dans l'environnement, le rôle défensif de l'authentification multifacteur (MFA) et des pare-feu, et le lien entre les attaques liées aux identités et le ransomware.

S'appuyant sur les expériences réelles de 226 responsables informatiques et de cybersécurité du secteur de l'éducation, dont 131 issus de l'enseignement des 1er et 2nd degrés et 95 d'établissements d'enseignement supérieur, ce rapport offre des perspectives uniques sur :

- 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

**Remarque :** Tout au long de ce rapport, « enquête globale » fait référence aux résultats des répondants de tous secteurs confondus. Les 226 participants du secteur de l'éducation font partie d'une cohorte plus large de 2158 participants répartis sur 15 secteurs industriels.

## 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, comprise entre 100 et 5 000 salariés, dont la répartition est restée proportionnellement constante au cours des six années d'existence de l'enquête. Toutes les données financières sont exprimées en dollars américains.

# Principales découvertes

- **Les attaques liées aux identités, en particulier par email, étaient nombreuses dans les secteurs de l'éducation.**
  - 77 % des victimes de l'enseignement supérieur et 71 % de celles de l'enseignement des 1er et 2nd degrés ont confirmé que leur attaque de ransomware était également leur attaque d'identité la plus importante, toutes deux supérieures au taux global de 67 % (tous secteurs confondus).
  - Les emails malveillants étaient la principale cause première technique des attaques de ransomware dans l'enseignement des 1er et 2nd degrés (31 %) et dans l'enseignement supérieur (29 %).
  - Les approches basées sur l'identité (emails malveillants, phishing, identifiants compromis ou force brute) ont déclenché 85 % des attaques dans l'ensemble du secteur de l'éducation, soit un taux supérieur à celui de 79 % dans tous les secteurs.
- **Les faiblesses opérationnelles dans le secteur de l'éducation étaient plus élevées que l'enquête globale (tous secteurs confondus).**
  - L'écart déterminant dans l'enseignement supérieur était l'expertise : 53 % ont déclaré ne pas avoir les compétences nécessaires pour détecter et stopper l'attaque à temps, contre 35 % pour l'enquête globale.
  - Les principales causes premières opérationnelles de l'enseignement des 1er et 2nd degrés étaient les erreurs humaines (52 %), le manque de protection (47 %), les failles de sécurité inconnues (42 %) et le manque de personnel ou de capacités (41 %).
- **Le chiffrement des données lié aux attaques de ransomware a fortement augmenté dans l'enseignement des 1er et 2nd degrés.**
  - Le taux de chiffrement des données dans l'enseignement des 1er et 2nd degrés a plus que doublé, passant de 29 % en 2025 à 61 % en 2026.
  - 58 % des attaques du secteur de l'éducation ont abouti au chiffrement des données, un chiffre proche du taux global de 56 %.
- **Les établissements d'enseignement comptaient beaucoup sur les sauvegardes pour restaurer les données.**
  - 77 % des établissements d'enseignement des 1er et 2nd degrés ont restauré des données chiffrées à partir de sauvegardes, un chiffre supérieur au taux global de 66 % de l'enquête.
  - 69 % des établissements d'enseignement supérieur ont également restauré leurs données à l'aide de sauvegardes.
- **Les établissements d'enseignement ont payé moins que le taux global, mais ont enregistré un nombre plus élevé de paiements de rançon supérieurs à 5 millions de dollars.**
  - Le montant médian des demandes de rançon dans le secteur de l'enseignement était plus élevé que celui de l'enquête globale, s'élevant à 775 200 dollars (contre 698 000 dollars), tandis que le paiement médian de rançon était inférieur, atteignant 515 000 dollars (contre 769 000 dollars au total).
  - Le montant médian des demandes de rançon dans le secteur de l'éducation a diminué deux années consécutives, tandis que les paiements ont augmenté de 15 000 dollars entre le rapport 2025 et 2026.
  - Les établissements d'enseignement ont été plus susceptibles de payer 5 millions de dollars ou plus (23 % contre 16 % dans l'enquête globale).
- **La récupération a coûté plus cher et a pris plus de temps dans l'éducation.**
  - Les coûts moyens de rétablissement dans l'éducation ont atteint 2,26 millions de dollars, un chiffre supérieur à celui de l'enquête globale de 1,7 million de dollars.
  - Le coût de rétablissement de l'éducation est passé de 1,66 million de dollars dans le rapport 2025 à 2,26 millions de dollars, le coût de rétablissement de l'enseignement supérieur augmentant de plus d'un million de dollars.
  - 26 % des établissements d'enseignement ont eu besoin d'un à trois mois pour se remettre complètement d'une attaque de ransomware, soit environ le double des 14 % de tous les secteurs.
  - Les établissements d'enseignement des 1er et 2nd degrés ont enregistré la plus forte proportion de rétablissements longs : 31 % ont mis un mois ou plus à se remettre sur pied, plus que tout autre secteur.
- **Le coût humain des équipes de sécurité s'est alourdi.**
  - 53 % des équipes de l'enseignement supérieur ont signalé une pression accrue de la part des cadres supérieurs, contre 40 % tous secteurs confondus.
  - Environ 39 % des équipes éducatives ont signalé une absence du personnel en raison de stress ou de problèmes de santé mentale, contre 29 % tous secteurs confondus.

# Les méthodes d'attaque et de défense

## Causes premières des attaques

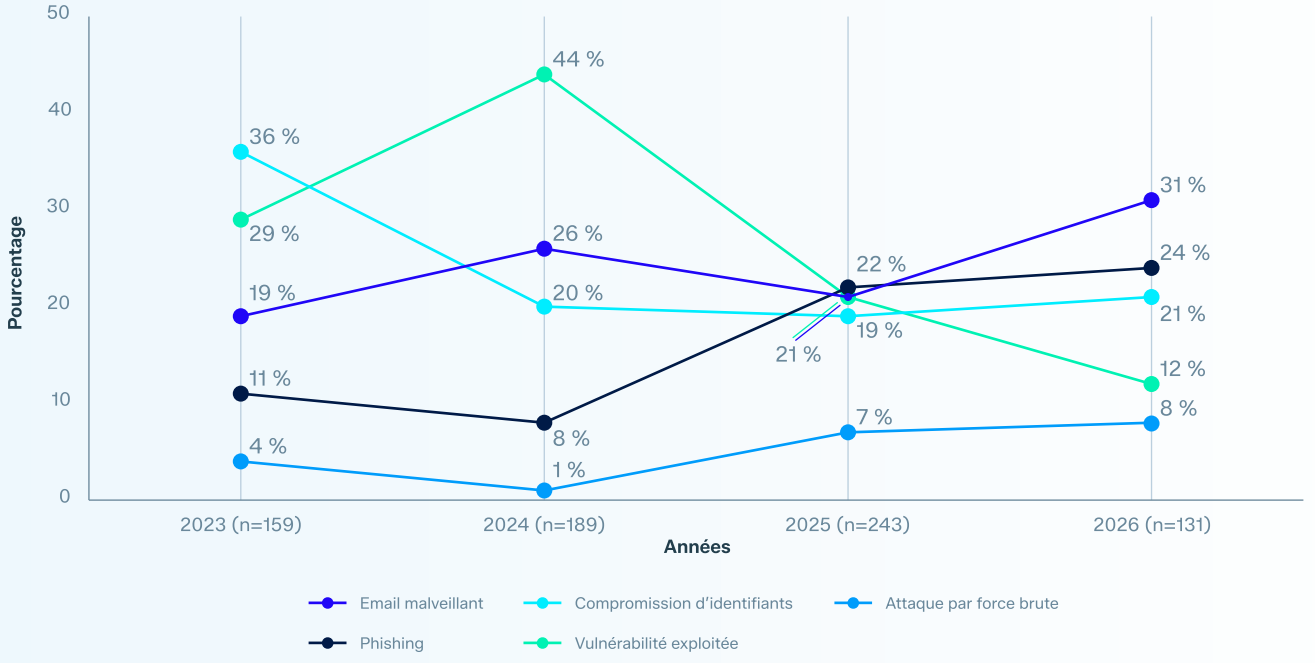
Les données de cette année sur l'éducation reflètent le même changement observé dans tous les secteurs : les attaques basées sur l'identité se multiplient.

Les emails malveillants étaient la cause technique principale la plus fréquente dans l'enseignement des 1er et 2nd degrés (31 %), suivis par le phishing (24 %) et les identifiants compromis (21 %). Les vulnérabilités exploitées sont tombées à 12 %, ce qui va dans le sens de la baisse générale de l'enquête globale (tous secteurs confondus) à 18 %.

**85 %**

La proportion d'attaques ciblant des établissements d'enseignement qui ont commencé par une approche basée sur l'identité (emails malveillants, phishing, identifiants compromis ou force brute), supérieure au taux global de 79 %.

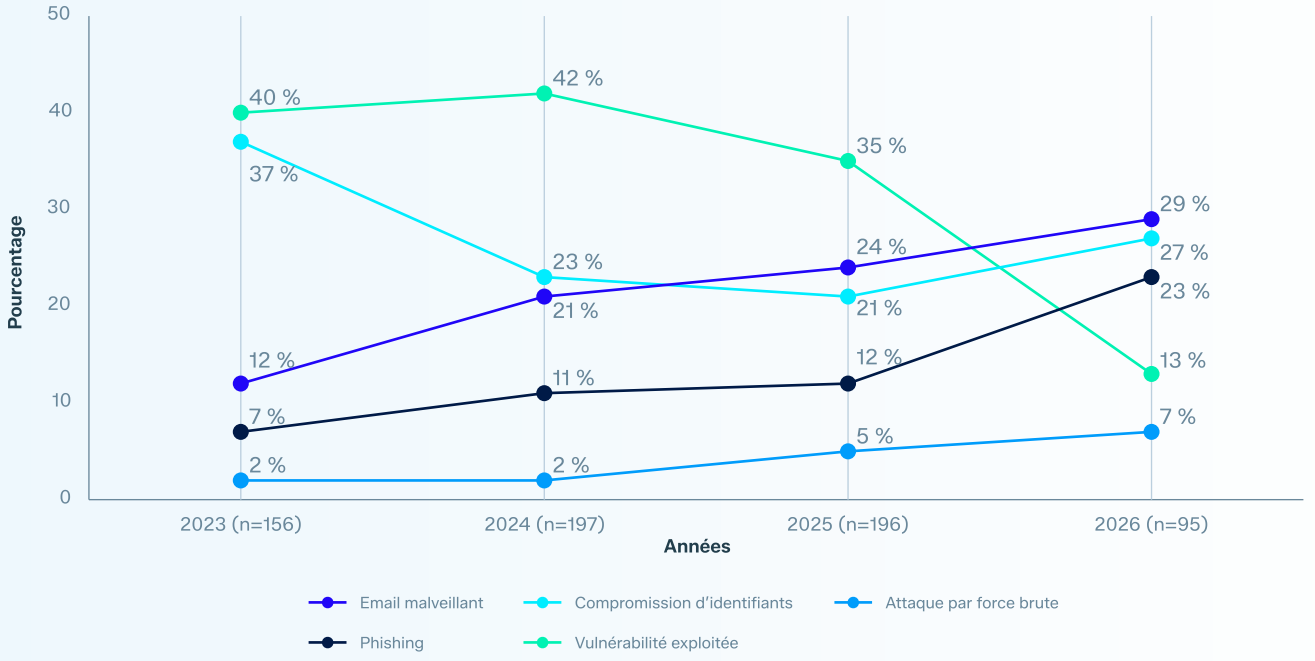
### Causes premières techniques des attaques de ransomware 2023–2026: Enseignement 1er et 2nd degrés




*Connaissez-vous la cause première de l'attaque de ransomware dont votre entreprise a été victime au cours de l'année écoulée ? Téléchargements et « Je ne sais pas » exclus du graphique pour plus de clarté visuelle. La somme des pourcentages peut ne pas être égale à 100 %. Chiffres de base dans le graphique.*

Les établissements d'enseignement supérieur ont également signalé une baisse des vulnérabilités exploitées. Ce vecteur d'attaque est tombé à 13 % dans le rapport 2026, contre 35 % en 2025. **Emails malveillants (29 %) et identifiants compromis (27 %) sont presque les causes principales conjointes**, le phishing arrivant juste derrière (23 %). Les secteurs de l'enseignement des 1er et 2nd degrés et de l'enseignement supérieur signalent les attaques par email comme causes principales, ce qui est cohérent avec l'enquête globale, où les emails malveillants (26 %) et le phishing (24 %) représentent ensemble la moitié des incidents.

## Causes premières techniques des attaques de ransomware 2023–2026: Enseignement supérieur

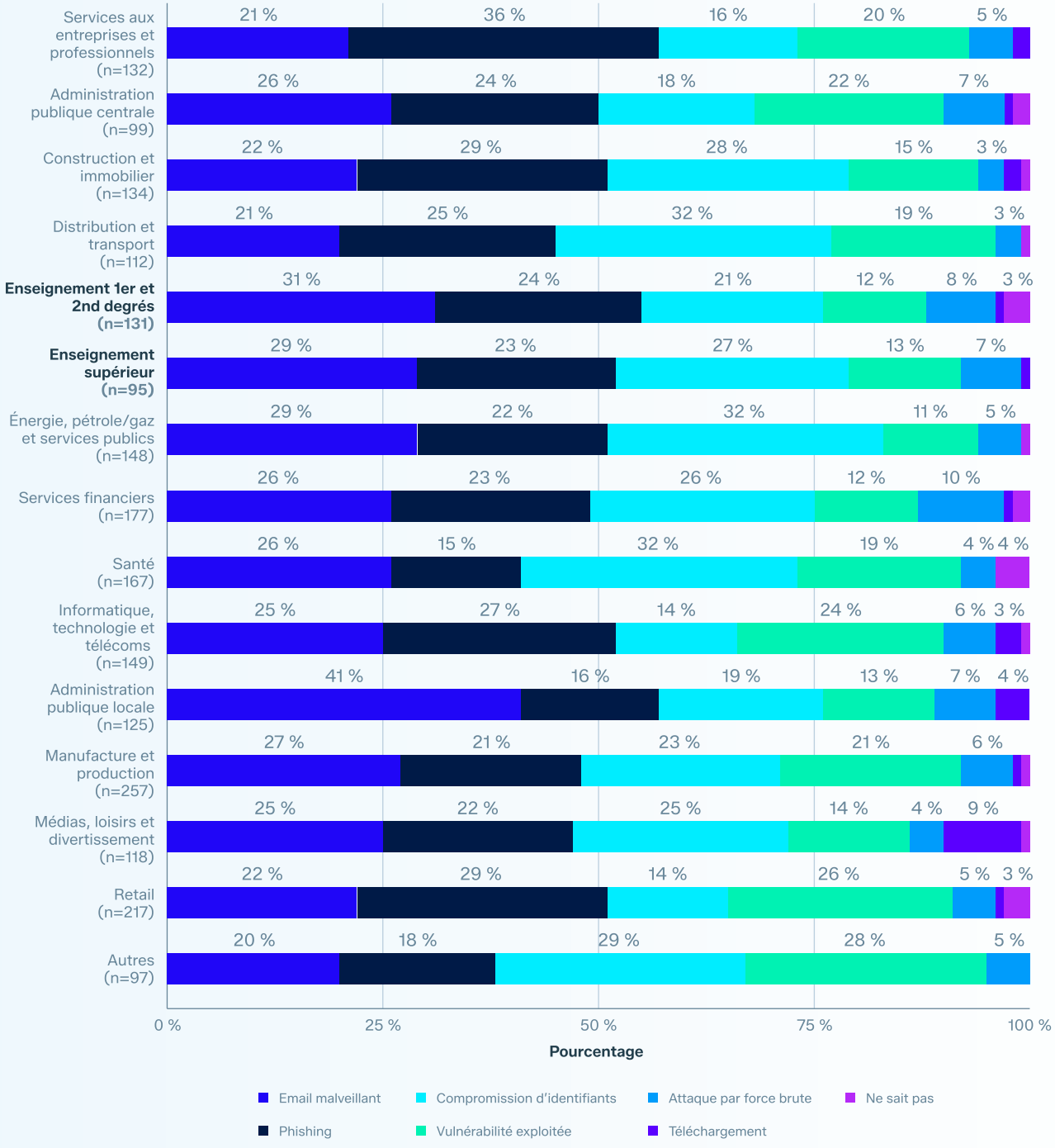



*Connaissez-vous la cause première de l'attaque de ransomware dont votre entreprise a été victime au cours de l'année écoulée ? Téléchargements et « Je ne sais pas » exclus du graphique pour plus de clarté visuelle. La somme des pourcentages peut ne pas être égale à 100 %. Chiffres de base dans le graphique.*

Pris dans leur ensemble, les vecteurs **basés sur l'identité (emails malveillants, phishing, compromission d'identifiants et attaques par force brute) représentaient 85 % des attaques contre les établissements d'enseignement, soit un pourcentage supérieur au taux global** d'enquête de 79 %. L'enseignement supérieur était le plus élevé avec 86 %, suivi de l'enseignement des 1er et 2nd degrés, à 84 %. En d'autres termes, environ six attaques sur sept contre le secteur de l'éducation ont commencé par une approche basée sur l'identité, renforçant ainsi pourquoi la sécurité des identités est au cœur des défenses du secteur.

Le secteur de l'éducation reflète la tendance intersectorielle plus large : davantage d'attaques transmises par email et moins de signalements de vulnérabilités exploitées. Cependant, les experts Sophos s'attendent à ce que les exploits augmentent à nouveau, car les organisations peinent à suivre le rythme des correctifs des vulnérabilités détectées par l'IA frontière.

## Cause première technique par secteur (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.*

## Les facteurs de vulnérabilité des organisations

Les établissements d'enseignement ont cité un large éventail de défis liés à la protection, aux ressources et aux failles de sécurité. Parmi les trois catégories consolidées, les problèmes de ressources (manque de personnel ou de compétences) ont été cités par 63 % des établissements d'enseignement, suivis par les problèmes de protection (62 %) et les failles de sécurité (62 %).


*Selon vous, pourquoi votre organisation a-t-elle été victime d'une attaque de ransomware ? n=226 Réponses consolidées.*

**L'enseignement combiné a rapporté un taux plus élevé par rapport à l'enquête globale sur presque toutes les causes premières opérationnelles**, les failles de sécurité connues étant la seule exception. Séparer l'enseignement des 1er et 2nd degrés et l'enseignement supérieur révèle deux faiblesses différentes.

**La principale faiblesse des entreprises de l'enseignement supérieur était l'expertise**. 53 % ont déclaré ne pas avoir les compétences ou les connaissances nécessaires pour détecter et stopper l'attaque à temps, contre 35 % pour l'enquête globale, soit un écart de 18 points de pourcentage et son plus grand.

**Les faiblesses de l'enseignement des 1er et 2nd degrés se sont regroupées autour de la capacité et des outils**. L'erreur humaine a été citée par 52 % des établissements de l'enseignement des 1er et 2nd degrés (contre 35 % tous secteurs confondus), le manque de protection par 47 % des établissements et le manque de personnel ou de capacité par 41 % des établissements.

**53 %**

La part des victimes de l'enseignement supérieur qui ont déclaré ne pas avoir les compétences ou les connaissances nécessaires pour détecter et stopper l'attaque à temps, soit 18 points de plus que l'enquête globale et leur principale faiblesse.

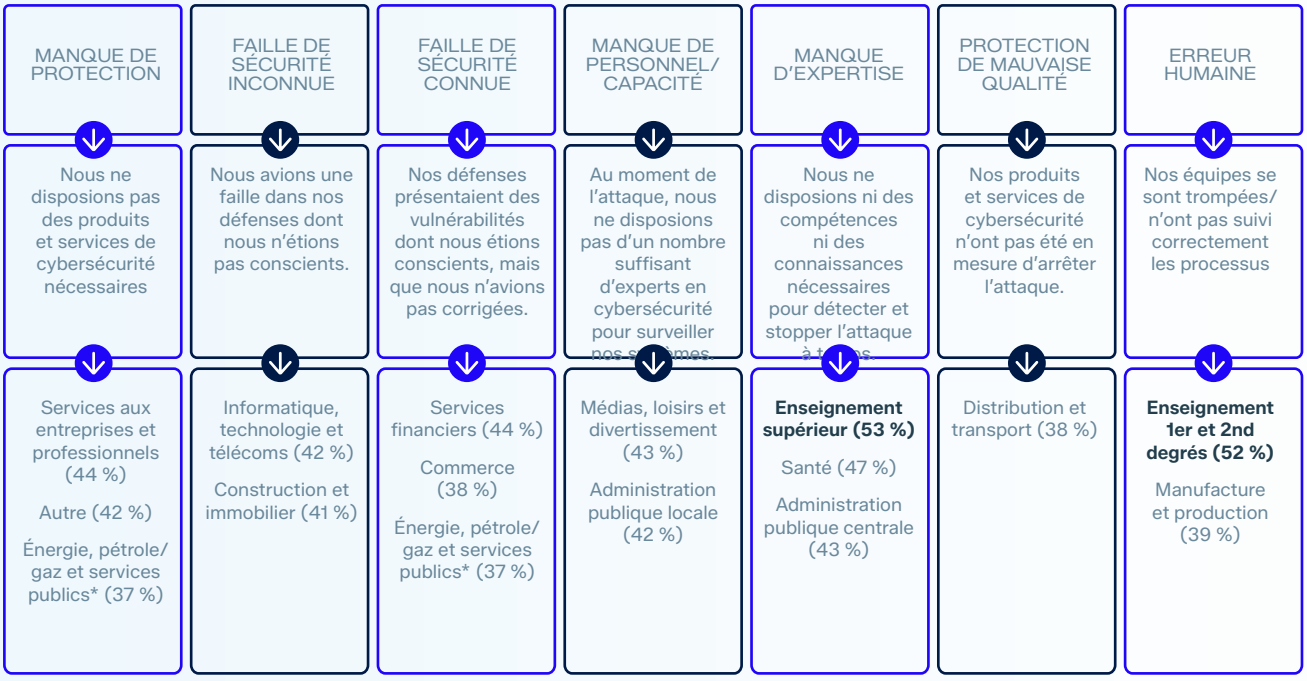
## Causes premières opérationnelles : Enseignement des 1er et 2nd degrés et supérieur vs tous les secteurs

| Cause première opérationnelle | Enseignement 1er et 2nd degrés (n=131) | Enseignement supérieur (n=95) | Tous secteurs (n=2 158) |
|---|---|---|---|
| Manque de protection | 47 % | 36 % | 36 % |
| Faille de sécurité inconnue | 42 % | 38 % | 36 % |
| Faille de sécurité connue | 33 % | 35 % | 36 % |
| Manque de personnel/ capacité | 41 % | 37 % | 35 % |
| Erreur humaine | 52% | 36 % | 35 % |
| Manque d'expertise | 33 % | 53 % | 35 % |
| Protection de mauvaise qualité | 38 % | 39 % | 33 % |

*Selon vous, pourquoi votre organisation a-t-elle été victime d'une attaque de ransomware ? Plusieurs réponses autorisées. Chiffres de base dans le graphique.*

Par rapport à d'autres secteurs, celui de l'éducation a davantage souffert d'un manque de protection et d'expertise. Le tableau ci-dessous montre les secteurs placés dans la colonne de la cause première opérationnelle qu'ils ont le plus citée.

## Causes premières opérationnelles des attaques de ransomware par secteur




*Selon vous, pourquoi votre organisation a-t-elle été victime d'une attaque de ransomware ? Plusieurs réponses autorisées. Les secteurs concernés par plusieurs causes sont marqués d'un astérisque (*). n=2 158.*

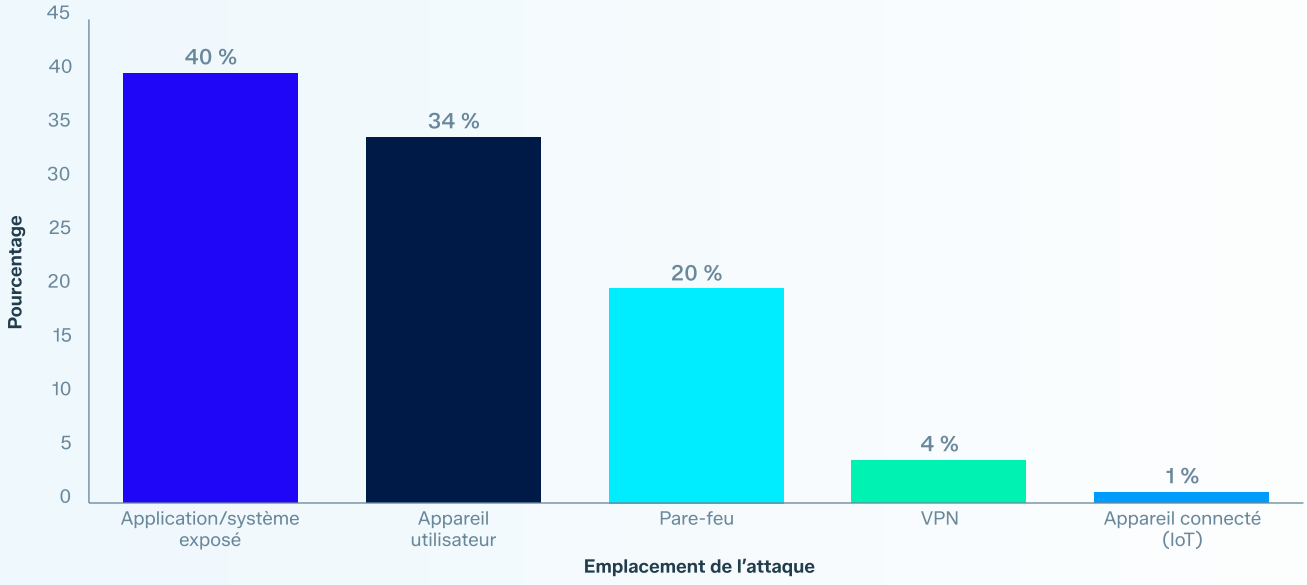
**NOUVEAU POINT DE RECHERCHE**

## Le point de départ des attaques

De nouvelles recherches menées cette année ajoutent une question sur le point de départ des attaques dans l'environnement, en particulier parmi les incidents qui ont commencé par l'exploitation d'une vulnérabilité, des identifiants compromis ou une attaque par force brute.

Dans le secteur de l'éducation, les applications et systèmes exposés étaient le point d'entrée le plus courant (40 %), suivis des appareils utilisateurs (34 %) et des pare-feu (20 %). Ces chiffres suivent de près l'enquête globale (respectivement 38 %, 30 % et 21 %), de sorte que le secteur de l'éducation ne montre aucune divergence significative à cet égard.

### Le point de départ des attaques de ransomware : Enseignement combiné




*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 ? Enseignement supérieur et enseignement des 1er et 2nd degrés combinés. n=99.*

**NOUVEAU POINT DE RECHERCHE**

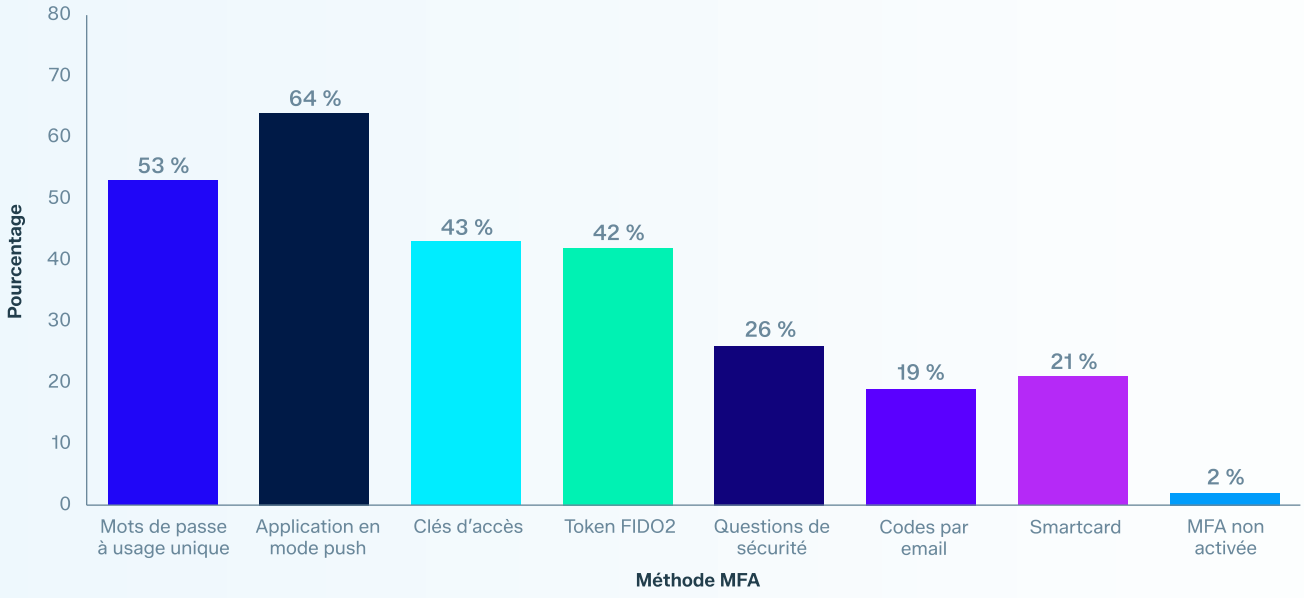
## Le rôle de l'authentification multifacteur (MFA)

Nous avons également examiné les méthodes d'authentification multifacteur en place au moment de l'attaque parmi les établissements d'enseignement dont l'attaque a commencé avec des identifiants compromis. Presque toutes les victimes du secteur de l'éducation avaient activé une forme ou une autre d'authentification multifacteur (98 %), faisant écho au résultat global de l'enquête (97 %) selon lequel l'authentification multifacteur était présente dans la plupart des attaques basées sur des identifiants.

Cependant, parmi les établissements d'enseignement interrogés sur l'authentification multifacteur, 81 % ont fait l'objet d'un chiffrement de données malgré l'activation de l'authentification multifacteur. Cela suggère que soit l'authentification multifacteur n'a pas été déployée de manière complète sur tous les systèmes critiques, soit les attaquants ont trouvé des moyens de contourner les protections de l'authentification multifacteur, soit les vecteurs d'attaque ne reposaient pas uniquement sur la compromission des identifiants.

Les applications en mode push (64 %) et les mots de passe à usage unique (53 %) étaient les méthodes les plus couramment déployées pour l'éducation.

### Méthodes MFA activées au moment de l'attaque : Enseignement combiné



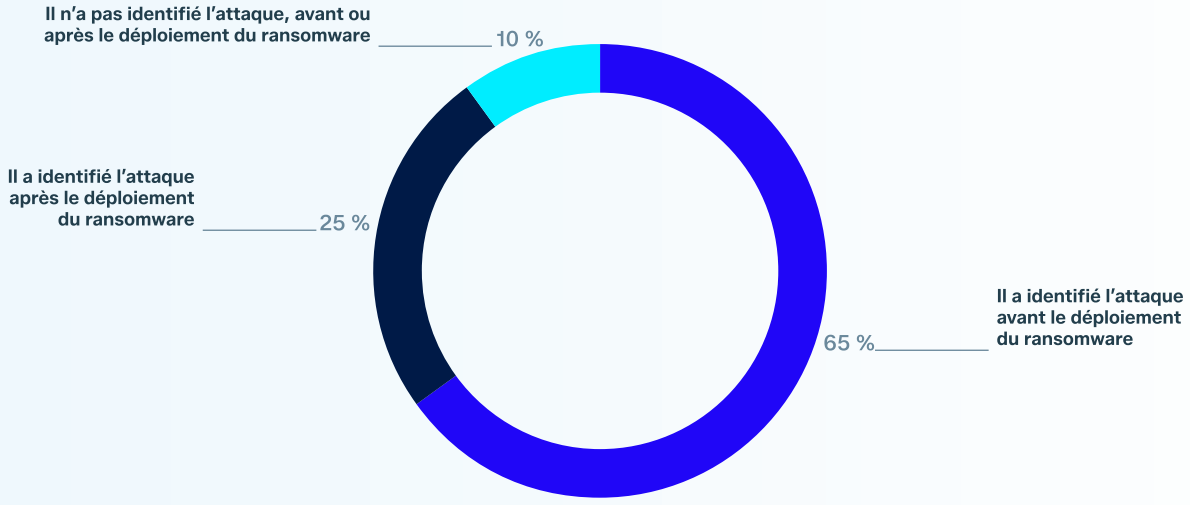

*Quel type d'authentification multifacteur était activé au moment de l'attaque, le cas échéant ? Plusieurs réponses autorisées.*
*Base : L'attaque s'est produite en raison d'identifiants compromis. Enseignement supérieur et enseignement des 1er et 2nd degrés combinés. n=53.*

**NOUVEAU POINT DE RECHERCHE**

## Le rôle des pare-feu

Pour l'éducation, les pare-feu ont identifié la plupart des attaques, mais ils n'ont pas toujours aidé à les bloquer. 65 % des fournisseurs ont déclaré que leur pare-feu avait identifié l'attaque avant le déploiement du ransomware, 25 % qu'il avait identifié l'attaque après coup et 10 % qu'il n'avait pas identifié l'attaque du tout. Ces chiffres reflètent ceux de l'enquête globale (61 %, 32 % et 7 %) avec un léger changement vers les deux extrémités du spectre.

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




*Votre pare-feu a-t-il joué un rôle dans l'identification de l'attaque ? Enseignement supérieur et enseignement des 1er et 2nd degrés combinés. n=226.*

**Parmi ces cas de détection précoce, les victimes du secteur de l'éducation ont tout de même vu leurs données chiffrées 51 % du temps.**

Les pare-feu collectent de bonnes données pour identifier les attaques, mais les attaques ne sont toujours pas stoppées au même rythme qu'elles le sont. Les pare-feu enregistrent souvent les données nécessaires pour détecter et bloquer une attaque, mais il se peut qu'ils ne se connectent pas suffisamment aux autres systèmes pour reconnaître la menace et y répondre à temps.

**NOUVEAU POINT DE RECHERCHE**

## Le lien entre usurpation d'identité et ransomwares

L'une des conclusions les plus claires de l'enquête est le lien direct entre les attaques liées aux identités et les ransomwares. Tous secteurs confondus, deux tiers des victimes de ransomware (67 %) ont confirmé que l'incident était le même que leur attaque d'identité la plus importante. Cependant, le secteur de l'éducation se situe au-dessus de cette barre : 71 % dans l'enseignement des 1er et 2nd degrés et 77 % dans l'enseignement supérieur (73 % dans l'enseignement combiné).

Bien que toutes les attaques n'aient pas abouti au chiffrement des données, le constat montre un fort chevauchement entre les attaques liées aux identités et les ransomwares dans le secteur de l'éducation.

### L'attaque de ransomware était également leur attaque liée à l'identité la plus grave


*Votre organisation a-t-elle subi une attaque de ransomware qui était également une attaque d'identité ? Organisations touchées par un ransomware Bases dans les graphiques.*

**73 %**

La proportion de victimes du secteur de l'éducation dont l'incident de ransomware a été le même que leur attaque d'identité la plus importante, soit plus que le taux global de 67 %.

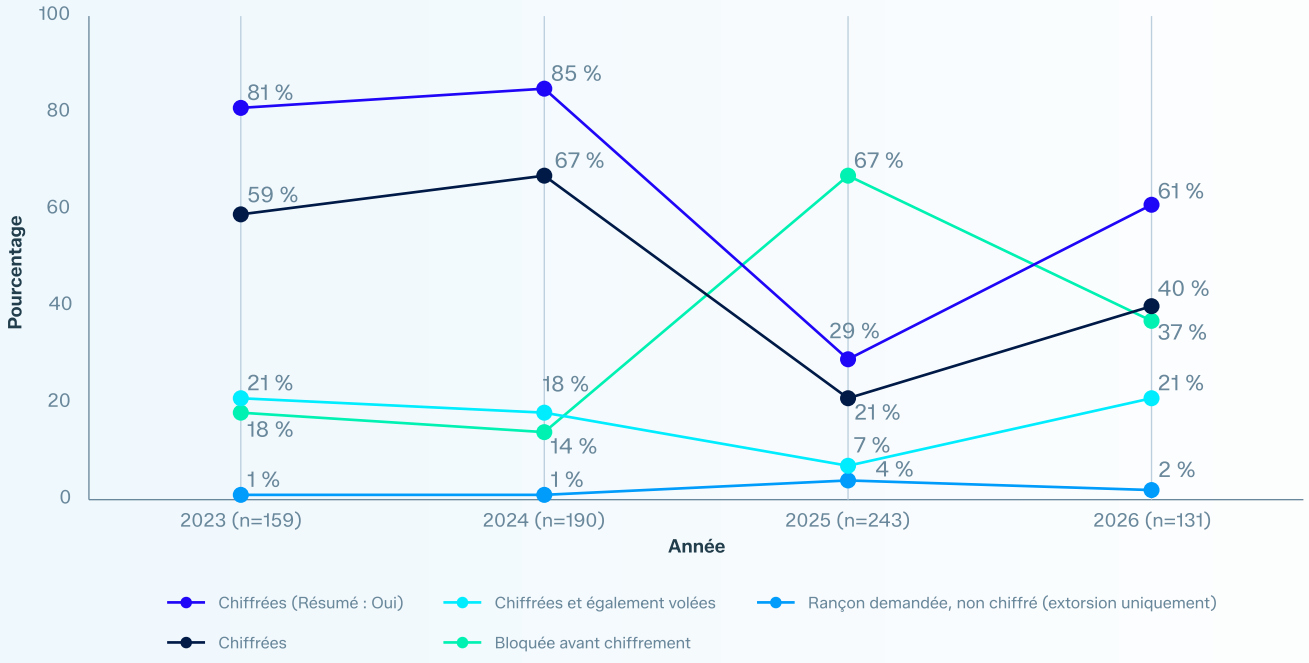
# Le chiffrement et la récupération des données

## Taux de chiffrement des données

Les résultats du rapport 2025 sur l'état des ransomwares dans l'éducation ont montré des résultats très positifs pour l'enseignement des 1er et 2nd degrés. Malheureusement, le rapport de cette année montre que l'enseignement des 1er et 2nd degrés recule pour se rapprocher de sa tendance antérieure.

Après que le taux de chiffrement dans l'enseignement des 1er et 2nd degrés soit tombé à 29 % dans le rapport 2025, le plus bas de tous les secteurs cette année-là, **la part des attaques contre l'enseignement des 1er et 2nd degrés qui ont réussi à chiffrer des données a plus que doublé pour atteindre 61 % en 2026** (supérieure au taux global d'enquête de 56 %). Seulement 37 % des attaques ont été stoppées avant chiffrement dans l'enseignement des 1er et 2nd degrés cette année, contre 67 % dans le rapport de l'an dernier.

### Taux de chiffrement des données dans le temps : Enseignement 1er et 2nd degrés

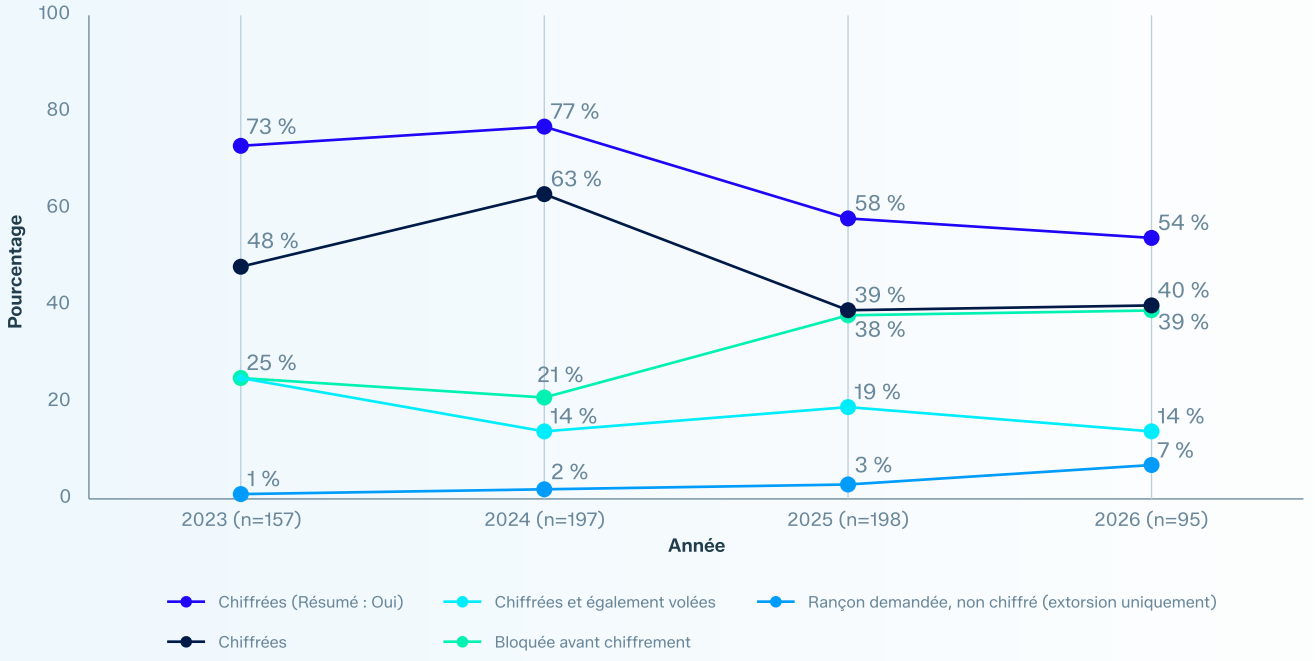



*Lors de l'attaque par ransomware, les cybercriminels ont-ils réussi à chiffrer les données de votre organisation ? Chiffres de base dans le graphique. La ligne « Chiffré (Résumé : Oui) » de ce graphique correspond à la somme des réponses « Chiffrement » et « Chiffrement et vol de données ».*

La double extorsion (où les données sont à la fois chiffrées et volées) a repris dans l'enseignement des 1er et 2nd degrés, passant de 7 % en 2025 à 21 % en 2026, ce qui est conforme à ses niveaux d'avant-2025. Ces attaques donnent aux attaquants un second moyen de pression. Les attaques par extorsion uniquement **(demandées à rançon sans chiffrement)** ont légèrement diminué, passant de 4 % à 2 % dans l'enseignement des 1er et 2nd degrés.

**L'enseignement supérieur est plus stable. Son taux de chiffrement a légèrement diminué pour atteindre 54 % en 2026, contre 58 % en 2025,** ce qui le maintient proche de l'enquête globale.

## Taux de chiffrement des données dans le temps : Enseignement supérieur




*Lors de l'attaque par ransomware, les cybercriminels ont-ils réussi à chiffrer les données de votre organisation ? Chiffres de base dans le graphique. La ligne « Chiffré (Résumé : Oui) » de ce graphique correspond à la somme des réponses « Chiffrement » et « Chiffrement et vol de données ».*

Dans l'enseignement supérieur, les attaques par extorsion seule ont atteint 7 %, contre 3 % en 2025, ce qui mérite d'être observé, même pour une faible part.

Les données 2026 replacent également le secteur de l'éducation dans sa tendance de long terme. En 2023 et 2024, le taux de chiffrement des données dans l'enseignement des 1er et 2nd degrés était supérieur à celui de l'enseignement supérieur ; 2025 a été l'exception, avec une chute temporaire du taux observé dans l'enseignement des 1er et 2nd degrés. Le taux de chiffrement de 61 % enregistré cette année dans l'enseignement des 1er et 2nd degrés contre 54 % dans l'enseignement supérieur replace la secteur dans sa tendance à long terme.

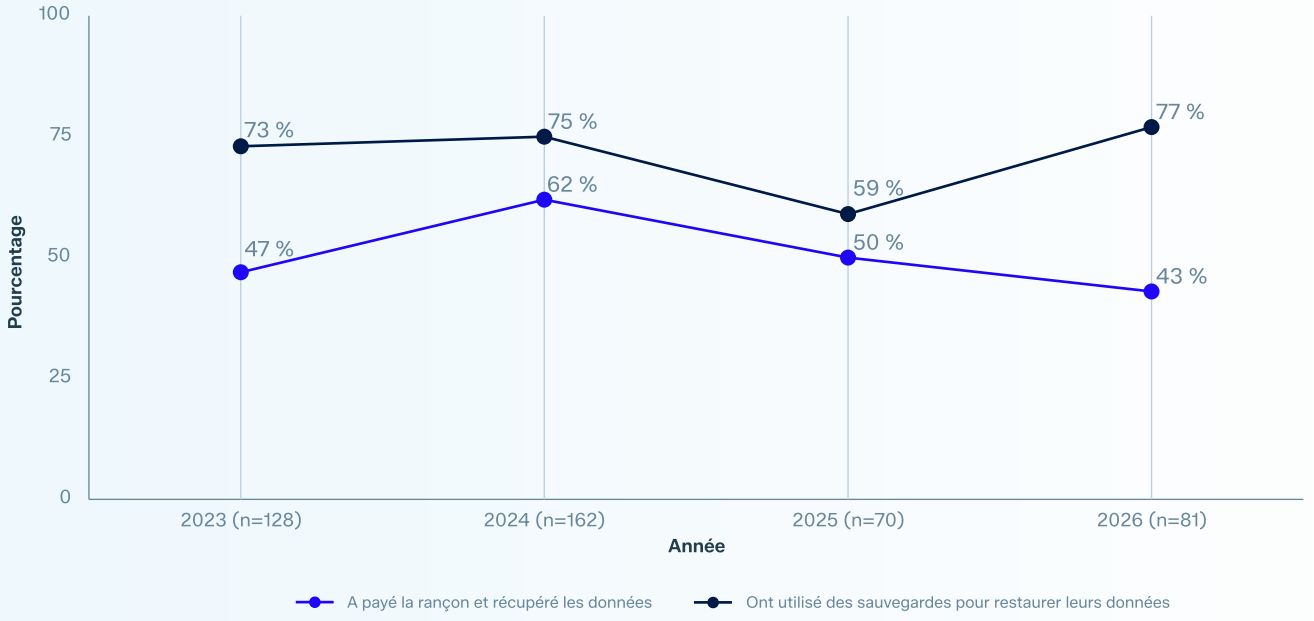
## Comment les organisations ont récupéré leurs données chiffrées

Les sauvegardes étaient le levier de rétablissement le plus puissant de l'éducation en 2026. Après avoir connu un repli en 2025 (59 % dans l'enseignement des 1er et 2nd degrés et 47 % dans l'enseignement supérieur), la restauration basée sur les sauvegardes a rebondi cette année. **77 % des établissements d'enseignement des 1er et 2nd degrés et 69 % des établissements d'enseignement supérieur ont restauré leurs données à partir de sauvegardes**, deux taux supérieurs aux 66 % de l'enquête globale. Ce rebond suggère que l'éducation a renouvelé son investissement dans l'infrastructure de sauvegarde et reconstruit sa résilience face aux demandes de rançon.

**77 %**

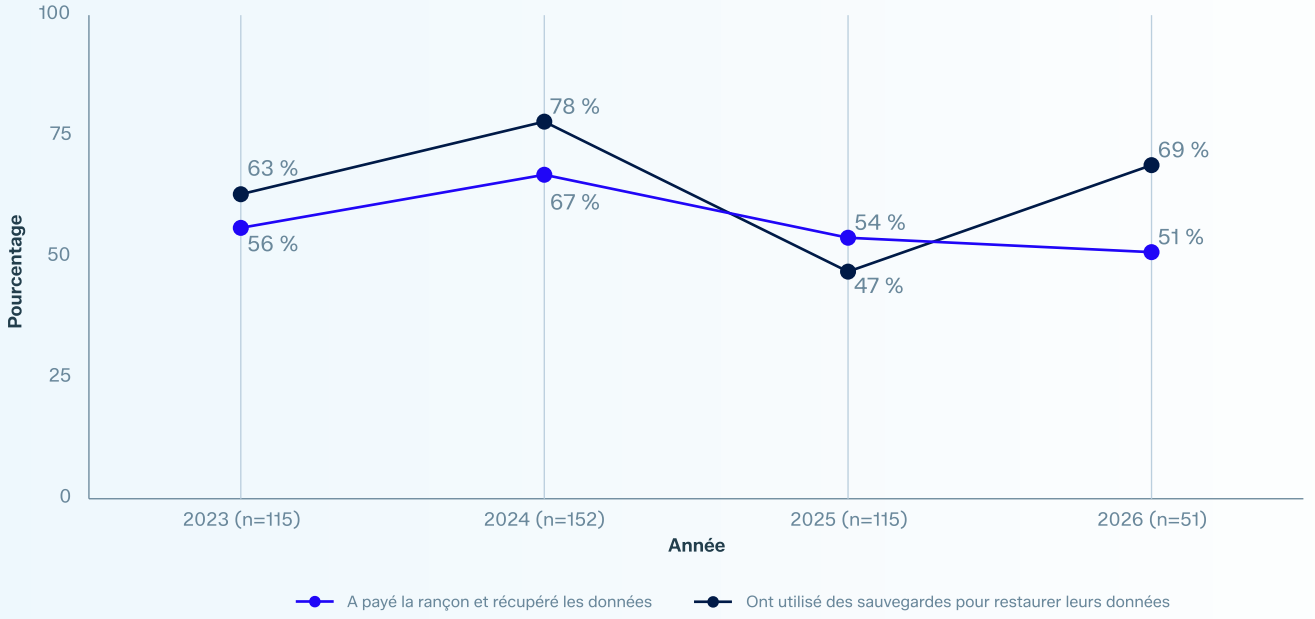
La part des établissements d'enseignement des 1er et 2nd degrés qui ont restauré des données chiffrées à partir de sauvegardes en 2026, soit plus que le taux global de 66 % de l'enquête.

### Méthodes de récupération des données au fil du temps : Enseignement 1er et 2nd degrés




*Votre organisation est-elle parvenue à récupérer ses données ? Plusieurs réponses autorisées. Chiffres de base dans le graphique.*

## Méthodes de récupération des données au fil du temps : Enseignement supérieur




*Votre organisation est-elle parvenue à récupérer ses données ? Plusieurs réponses autorisées. Chiffres de base dans le graphique.*

Dans le même temps, les établissements d'enseignement paient moins fréquemment les rançons. **La part des établissements ayant payé la rançon et récupéré des données a diminué pour deux années consécutives**, passant de 62 % (2024) à 50 % (2025) à 43 % (2026) dans l'enseignement des 1er et 2nd degrés, et de 67 % à 54 % à 51 % respectivement dans l'enseignement supérieur.

Avec l'augmentation des restaurations de sauvegardes et la baisse des restaurations basées sur le paiement, le secteur de l'éducation se rétablit davantage grâce à ses propres capacités qu'à la coopération des attaquants.

# Montant de la rançon demandée et montant payé

## Les demandes de rançon

L'éducation a fait face à des demandes de rançon plus importantes que d'autres secteurs dans l'ensemble de l'enquête. Le montant médian des rançons demandées à un établissement d'enseignement était de 775 200 dollars, un chiffre supérieur au montant médian de 698 000 dollars tous secteurs confondus. La répartition était également fortement orientée vers des montants élevés : **la moitié des demandes de rançon (50 %) s'élevaient à 1 million de dollars ou plus, et un quart (25 %) à 5 millions de dollars ou plus**, contre 46 % et 23 % respectivement dans l'échantillon de tous les secteurs.

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

### Montant médian des demandes de rançon

| | 2025 | 2026 |
|---|---|---|
| Éducation | 0,98 M$ (n=185) | 0,78 M$ (n=132) |
| Tous les secteurs | 1,32 M$ (n=1 700) | 0,70 M$ (n=1 214) |

*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.*

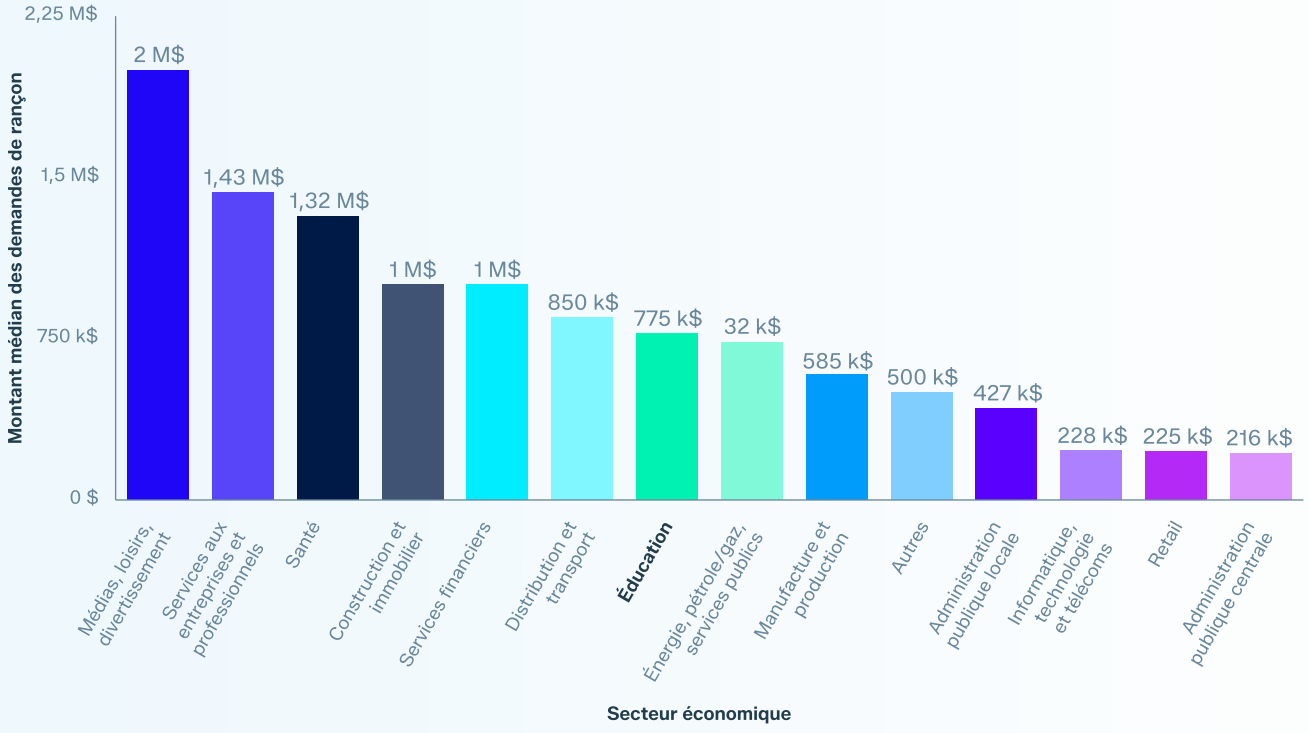
Comparé aux autres secteurs, celui de l'éducation se situe dans la moyenne. Dans l'éducation, les demandes de rançon médianes sont inférieures à celles des secteurs affichant les montants les plus élevés, tels que les médias, les loisirs et le divertissement (2 millions de dollars) et les services aux entreprises et professionnels (1,43 million de dollars), mais bien supérieures aux secteurs où les montants demandés sont plus faibles comme l'administration centrale (216 500 dollars) et le commerce de détail (225 000 dollars).

**$775 200**

Montant médian des rançons demandées aux établissements d'enseignement—supérieur au montant médian de 698 000 $ de l'enquête globale.

La moitié des demandes de rançon pour l'éducation s'élevaient à 1 million de dollars ou plus.

## Montant médian des demandes de rançon par secteur




*Quel était le montant de la rançon demandée par les attaquants ? Base : organisations dont les données ont été chiffrées. (n=1 141)*

Les tendances d'une année sur l'autre sont bonnes et mauvaises. La demande médiane faite aux établissements de l'enseignement combiné est passée de 976 000 dollars en 2025 à 775 200 dollars en 2026. Cette baisse est due en grande partie à l'enseignement des 1er et 2nd degrés, où la demande médiane est passée de 1,03 million de dollars à 737 600 dollars, tandis que l'enseignement supérieur est allé à l'encontre de cette tendance, sa demande médiane passant de 697 086 dollars à 889 200 dollars.

## Montants des rançons payées

Les rançons les plus élevées demandées aux établissement d'enseignement ne se sont pas soldées par des paiements plus élevés. **Bien que les demandes aient été plus élevées, le montant médian des rançons payées par les établissements d'enseignement était inférieur à celui des autres secteurs de l'ensemble de l'enquête**. Le montant médian de la rançon payée par un établissement d'enseignement était de 515 000 dollars, ce qui est inférieur au montant médian de l'enquête globale (769 000 dollars).

**Les paiements de l'éducation se situaient globalement en dehors de la tranche supérieure, mais comprenaient une part importante de paiements de 5 millions de dollars ou plus**. 39 % des paiements effectués par les établissements d'enseignement atteignaient 1 million de dollars ou plus, ce qui est inférieur aux 44 % de l'enquête globale. En revanche, 23 % atteignaient 5 millions de dollars ou plus, un chiffre supérieur au taux de l'enquête globale (16 %). En clair, lorsque les établissements du secteur de l'éducation paient, les montants sont généralement inférieurs à ceux observés dans les autres secteurs, mais une minorité non négligeable consent à verser des sommes très élevées.

### Montant médian de la rançon

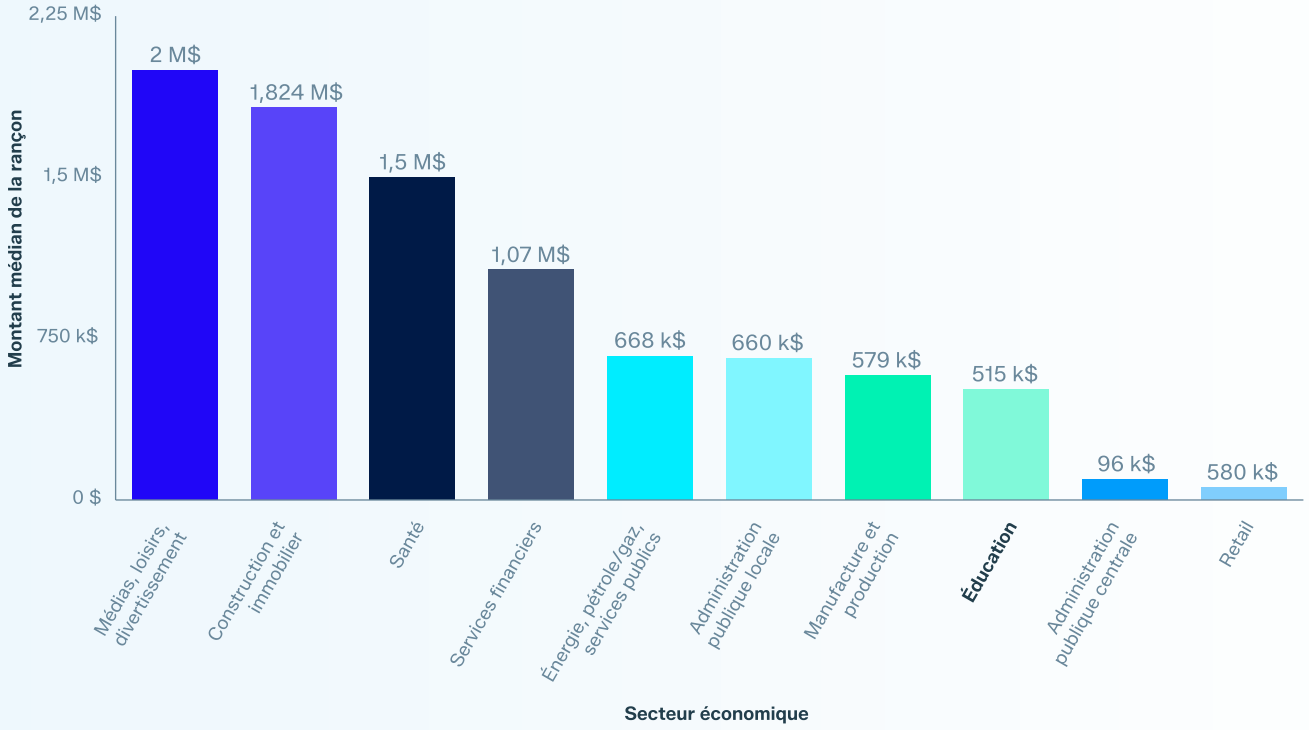
| | 2025 | 2026 |
|---|---|---|
| Éducation | 0,50 M$ (n=100) | 0,52 M$ (n=62) |
| Tous les secteurs | 1,00 M$ (n=847) | 0,77 M$ (n=587) |

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

**515 000 $**

Le montant médian des rançons payées par les établissements d'enseignement était inférieur à la médiane de 769 000 dollars de l'enquête globale, malgré des demandes de rançon plus élevées.

## Montant médian de la rançon payée, par secteur




*Quel était le montant approximatif de la rançon payée aux attaquants ? Base : organisations ayant payé la rançon. n=587. Exclut les secteurs comptant moins de 30 répondants à cette question.*

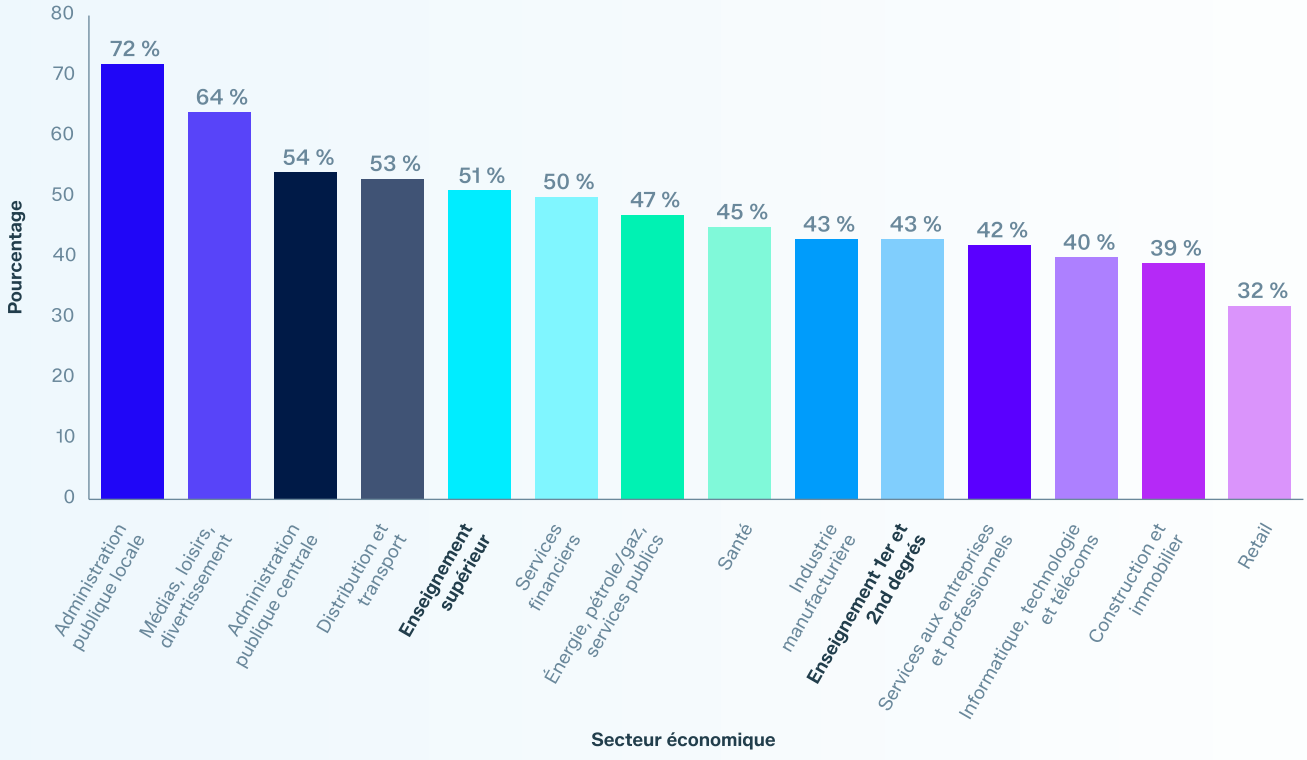
Les tendances d'une année sur l'autre étaient également contrastées pour le paiement des rançons. Le paiement médian de l'éducation combinée est essentiellement stable, passant légèrement de 500 000 dollars en 2025 à 515 000 dollars en 2026. Le paiement médian de l'enseignement des 1er et 2nd degrés a fortement diminué au cours de la même période, passant de 800 000 dollars à 320 000 dollars. La légère hausse enregistrée au niveau combiné est donc due à l'enseignement supérieur.

Étant donné que moins de 30 établissements d'enseignement supérieur ont déclaré un montant de paiement cette année (n=27), nous ne pouvons pas afficher de tendance distincte fiable pour les paiements de l'enseignement supérieur, nous recommandons donc d'utiliser les tendances combinées des paiements de l'enseignement.

## Pourcentage des organisations ayant payé la rançon, par secteur

La propension à payer les rançons diffère entre les deux segments de l'éducation. Dans l'enseignement supérieur, 51 % des victimes ont versé la rançon, soit plus que les 48 % relevés dans l'enquête globale. Dans l'enseignement des 1er et 2nd degrés, cette part tombait à 43 %, signe d'une moindre propension à payer la

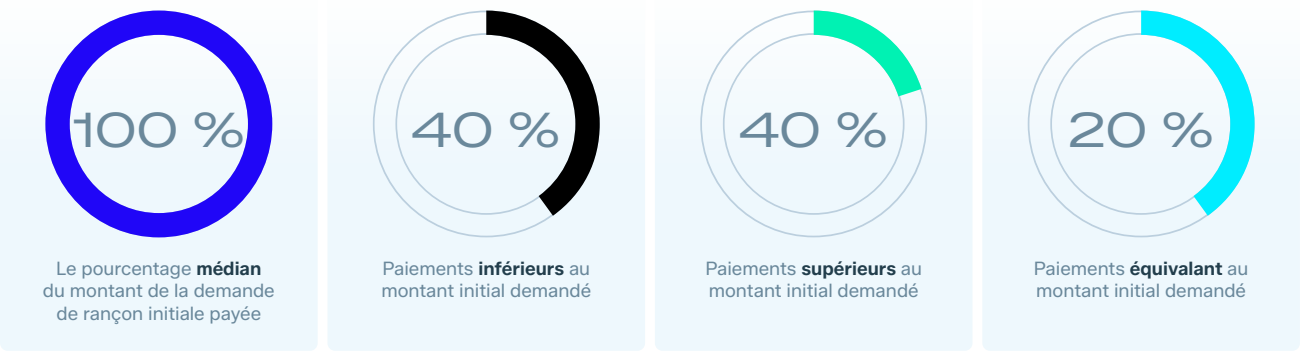
### Pourcentage des organisations ayant payé la rançon par secteur




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

## Paiements effectifs vs demandes initiales

Parmi les établissements d'enseignement qui ont payé la rançon, 40 % ont payé moins que la demande initiale, 40 % ont versé davantage et 20 % ont réglé la somme demandée. L'établissement moyen a payé 100 % du montant demandé, contre 82 % en 2025. Ainsi, alors qu'une part substantielle des établissements négociaient leur paiement à la baisse, une part égale a fini par payer plus que la somme exigée au départ.




*Concernant le montant de la rançon payée, était-il inférieur, identique ou supérieur au montant initial de la rançon demandée ? Hors valeurs aberrantes. Enseignement supérieur et enseignement des 1er et 2nd degrés combinés. n=58.*

# L'impact commercial et humain

## Coûts de rétablissement après une attaque de ransomware

Le secteur de l'éducation a dû engager des dépenses de rétablissement supérieures à la moyenne. **Le coût moyen de rectification d'une attaque de ransomware, hors rançon payée, était de 2,46 millions de dollars dans l'enseignement des 1er et 2nd degrés et de 1,99 million de dollars dans l'enseignement supérieur**, tous deux supérieurs à la moyenne globale de 1,7 million de dollars de l'enquête.

Pour la deuxième année de suite, l'enseignement des 1er et 2nd degrés est le segment qui a dû faire face aux coûts de rétablissement les plus élevés. Son coût moyen de rétablissement est passé de 2,28 millions de dollars en 2025 à 2,46 millions de dollars en 2026, ce qui en fait le secteur de l'éducation le plus cher et bien supérieur à l'enquête globale (1,7 million de dollars).

### Coût moyen de rétablissement

| | 2025 | 2026 |
|---|---|---|
| Enseignement 1er et 2nd degrés | 2,28 M$ (n=243) | 2,46 M$ (n=131) |
| Enseignement supérieur | 0,90 M$ (n=198) | 1,99 M$ (n=95) |
| **Tous les secteurs** | 1,53 M$ (n=3 400) | 1,70 M$ (n=2 158) |

*Quel a été le coût approximatif supporté par votre organisation pour remédier aux conséquences de l'attaque de ransomware la plus importante ? Moyenne, hors rançon payée. Chiffres de base dans le graphique.*

**C'est dans l'enseignement supérieur que l'écart s'est le plus creusé. Son coût moyen de rétablissement a plus que doublé, passant de 0,90 million de dollars en 2025 à 1,99 million de dollars en 2026**. Dans le rapport 2025, l'enseignement supérieur avait enregistré l'un des coûts de rétablissement les plus bas de tous les autres secteurs. Cette année, il a augmenté pour se rapprocher du niveau de l'enseignement des 1er et 2nd degrés. Les deux réductions dans le secteur de l'éducation dépassent désormais la moyenne globale de l'enquête, qui elle-même a légèrement augmenté, passant de 1,53 million de dollars à 1,7 million de dollars.

**1,09 M$**

L'augmentation des coûts moyens de rétablissement après une attaque de ransomware dans l'enseignement supérieur de 2025 à 2026.

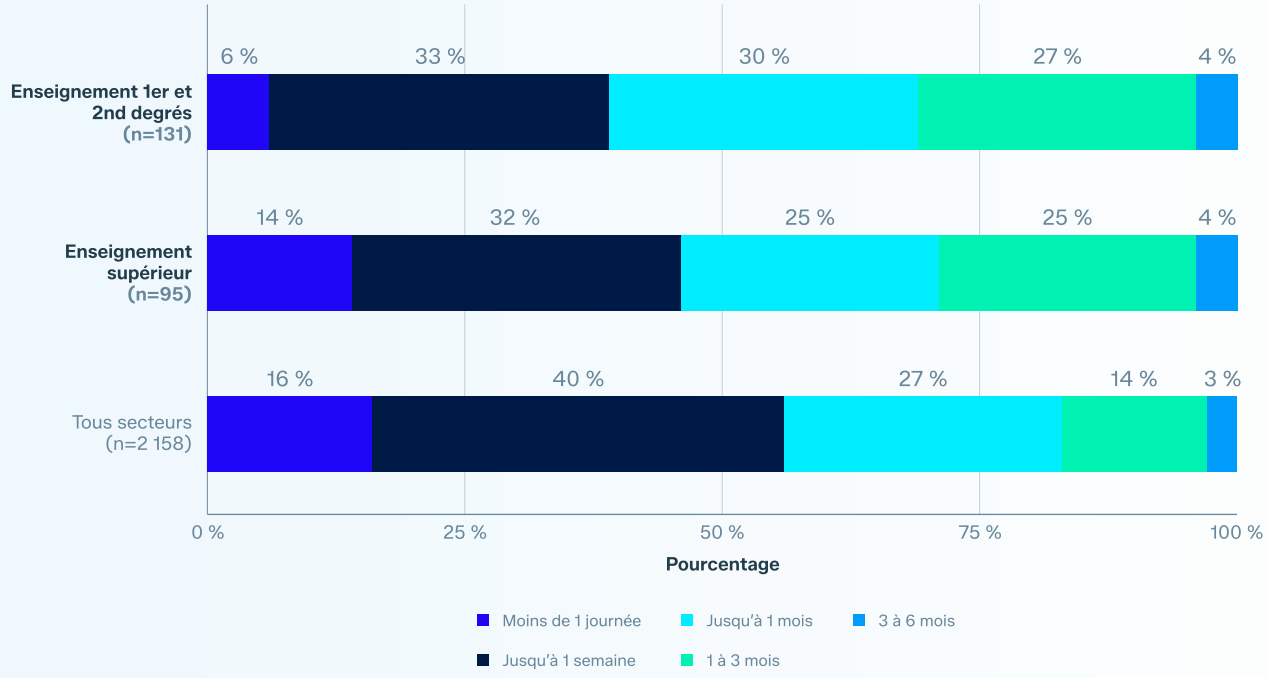
## Temps de rétablissement

Les établissements d'enseignement ont non seulement payé plus cher pour se rétablir, mais ils ont également mis plus de temps à le faire. C'est sur la tranche d'un à trois mois que l'écart est le plus marqué : 27 % des établissements d'enseignement des 1er et 2nd degrés et 25 % des établissements d'enseignement supérieur ont eu besoin de ce temps pour se rétablir complètement, contre seulement 14 % dans l'enquête globale. **Les établissements d'enseignement étaient presque deux fois plus susceptibles de devoir composer avec des délais de rétablissement d'un mois ou plus**.

**31 %**

Proportion d'établissements d'enseignement des 1er et 2nd degrés qui ont eu besoin d'au moins un mois pour se rétablir, plus que tout autre secteur.

### Temps nécessaire pour se rétablir d'un ransomware




*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.*

La tranche des délais de rétablissement les plus courts confirme le même constat, en miroir. Seuls 6 % des établissements d'enseignement des 1er et 2nd degrés se sont rétablis en moins d'une journée, contre 16 % pour l'enquête globale et 14 % pour l'enseignement supérieur.

**Aucun secteur n'a enregistré une plus grande part de rétablissements longs que l'enseignement des 1er et 2nd degrés**, où 31 % des établissements ont eu besoin d'au moins un mois pour rebondir complètement.

## L'impact humain des ransomwares

Le coût humain pour les personnels de l'éducation dépasse celui relevé dans l'enquête globale, avec des ressentis différents dans chaque segment du secteur. Pour le personnel de l'enseignement supérieur, la pression déterminante est venue d'en haut : 53 % des équipes ont signalé une pression accrue de la part des cadres supérieurs, soit 13 points de plus que le taux de l'enquête globale de 40 %. Les changements apportés à l'équipe ou à la structure organisationnelle sont également plus fréquents dans l'enseignement supérieur (43 % contre 32 % tous secteurs confondus).

Pour les établissement d'enseignement des 1er et 2nd degrés, les effets se sont principalement concentrés sur la reconnaissance et la charge de travail. Près de la moitié des équipes de l'enseignement des 1er et 2nd degrés (49 %) ont signalé une reconnaissance accrue de la part des cadres supérieurs, ce qui est supérieur au taux global d'enquête de 36 %. La reconnaissance peut être positive, mais l'augmentation de la charge de travail ne l'est pas. 43 % des équipes de ce segment de secteur ont mentionné une augmentation continue de la charge de travail, contre 31 % dans tous les autres secteurs. Cette attention accrue a été à double tranchant : plus de reconnaissance, mais aussi une charge plus lourde et plus soutenue.

**53 %**

Le pourcentage d'équipes informatiques et de sécurité de l'enseignement supérieur qui ont été confrontées à une pression accrue de la part des cadres supérieurs après une attaque, contre 40 % dans l'ensemble de l'enquête.

### L'impact humain des ransomwares

| Répercussion | Enseignement 1er et 2nd degrés (n=81) | Enseignement supérieur (n=51) | Tous secteurs (n=1 214) |
|---|---|---|---|
| Anxiété ou stress accru liés à de futures attaques | 40 % | 33 % | 41 % |
| Pression accrue de la part des hauts dirigeants | 48 % | 53 % | 40 % |
| Reconnaissance accrue par les hauts dirigeants | 49 % | 29 % | 36 % |
| Changements au sein de l'équipe/de la structure organisationnelle | 33 % | 43 % | 32 % |
| Changement des priorités/ objectifs de l'équipe | 33 % | 35 % | 32 % |
| Sentiment de culpabilité de ne pas avoir pu empêcher l'attaque | 31 % | 25 % | 31 % |
| Augmentation continue de la charge de travail | 43 % | 31 % | 31 % |
| Absence du personnel liée au stress/aux problèmes de santé mentale | 40 % | 39 % | 29 % |
| Remplacement de la direction de l'équipe | 27 % | 29 % | 21 % |

*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. Chiffres de base dans le graphique.*

**Quel que soit le segment, le bien-être du personnel a été impacté. 39 % des équipes de l'enseignement supérieur et 40 % de celles de l'enseignement des 1er et 2nd degrés ont signalé une absence du personnel pour cause de stress ou de problèmes de santé mentale**, ce qui est bien supérieur au taux global d'enquête de 29 %.

Le taux de rotation des dirigeants a également été plus élevé, avec 29 % des équipes de l'enseignement supérieur et 27 % de l'enseignement des 1er et 2nd degrés ayant vu leur leadership remplacé après l'attaque, contre 21 % dans l'ensemble.

# Recommandations

**Renforcez la sécurité des identités pour vous prémunir contre les ransomwares.** 73 % des victimes de ransomware du secteur de l'éducation ont confirmé que leur incident de ransomware coïncidait avec leur attaque d'identité la plus importante, ce qui est supérieur aux 67 % de l'enquête globale, soulignant le lien étroit entre compromission de l'identité et ransomware dans ce secteur. Les établissements d'enseignement doivent prioriser la détection et 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.

**Activez l'authentification multifacteur (MFA) complète, en particulier l'authentification multifacteur résistante au phishing**. L'enquête a montré que 98 % des organisations du secteur de l'éducation ayant des identifiants compromis avaient activé l'authentification multifacteur d'une manière ou d'une autre au moment de leur attaque, mais que leurs taux de chiffrement restaient élevés. L'authentification multifacteur seule ne suffit pas à bloquer les attaques : elle doit être soit activée de façon globale, et non laissée active uniquement pour les applications SaaS qui l'imposent, mais désactivée pour les connexions VPN, les consoles d'administration du pare-feu et les applications héritées.

**Renforcez la protection Endpoint pour les modèles d'IA frontière**. Même si les rapports d'exploitation de vulnérabilités ont diminué dans ce rapport, les experts de Sophos s'attendent à ce que les exploits augmentent à nouveau, car les organisations peinent à suivre le rythme des correctifs pour les vulnérabilités détectées par l'IA frontière. 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 capacités, de compétences et d'expertise est un problème permanent dans l'ensemble de l'éducation, et particulièrement dans l'enseignement supérieur, où le manque d'expertise interne s'est révélé être une faiblesse majeure. Les menaces liées à l'IA renforceront encore la pression sur ces domaines, alors que les équipes de sécurité tentent de rester à jour face à l'évolution rapide des technologies de l'IA. Si vous n'êtes pas en mesure de mettre en place en interne une équipe d'opérations de sécurité fiable, faites appel à un spécialiste externe pour combler ce manque, soit directement auprès d'un fournisseur MDR assurant une couverture 24/7, soit auprès d'un fournisseur de services managés. Les fournisseurs qui résolvent plus d'incidents de bout en bout grâce à l'IA et à l'automatisation agissent comme un multiplicateur de force qui aide à combler les lacunes en matière de compétences et de capacités.

**Investissez dans une infrastructure de sauvegarde et de restauration**. Les sauvegardes étaient la principale voie de récupération tant pour l'enseignement des 1er et 2nd degrés que pour l'enseignement supérieur (77 % et 69 %, tous deux supérieurs aux chiffres de l'enquête globale). 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**. Les vulnérabilités exploitées restent un vecteur d'attaque majeur et sont susceptibles de s'accroître à mesure que les modèles d'IA frontière trouvent plus rapidement de nouvelles faiblesses. Les établissements d'enseignement 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 via le pare-feu et exploitez la télémétrie du pare-feu pour détecter les attaques à un stade précoce**. Les données de 2026 ont montré que les pare-feu sont efficaces pour repérer les signes d'un ransomware, 65 % d'entre eux disposant de suffisamment de données pour identifier une attaque avant que le ransomware ne soit déclenché. Mais même dans ces cas de détection précoce, les victimes du secteur de l'éducation ont tout de même vu leurs données chiffrées 51 % du temps, car le pare-feu ne peut souvent pas confirmer ou stopper une attaque sans télémétrie provenant d'autres points de contrôle. 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. Connectez les pare-feu à XDR et MDR afin que la télémétrie des pare-feu aide à détecter les attaques de ransomware avant le déploiement des charges utiles. La solution : un système de cybersécurité dans lequel les contrôles partagent les signaux.

**Actions recommandées en un coup d'œil :**

1. Segmentation pour ralentir les attaquants
2. ZTNA pour remplacer les VPN hérités et contenir les exploits des applis
3. Détection et réponse aux menaces liées aux identités (ITDR) pour renforcer l'infrastructure d'identité
4. MFA résistante au phishing considérée comme objectif plutôt que comme point de départ
5. Application rigoureuse des correctifs sur les appareils connectés à Internet
6. Détection et réponse 24/7

# Conclusion

L'état des ransomware dans le secteur de l'enseignement en 2026 révèle un paysage de menaces en pleine transition.

**Des signes de progrès sont visibles** : les demandes de rançon diminuent, la récupération basée sur des sauvegardes a atteint des niveaux presque records et les paiements de rançon par les établissements d'enseignement sont faibles par rapport à d'autres secteurs.

Parallèlement, les défis qui restent à relever sont importants. Plus de la moitié des attaques de ransomware contre l'éducation parviennent encore à chiffrer les données, les coûts moyens de rétablissement s'élèvent à 2,26 millions de dollars par incident (soit un montant supérieur à celui de l'enquête globale) et l'enseignement des 1er et 2nd degrés a enregistré la plus grande part de rétablissements d'une durée d'un mois ou plus.

C'est au niveau de l'identité que se concentre l'exposition dans le secteur de l'enseignement. Une plus grande part des organisations d'enseignement ont confirmé que leur incident de ransomware était le même événement que leur attaque d'identité la plus importante par rapport à l'enquête globale. Dans un secteur où la récupération est déjà plus lente et plus coûteuse, ce lien étroit fait de l'infrastructure d'identité le levier d'investissement le plus prometteur.

Les organisations d'enseignement 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 organisations d'enseignement ont cité une faille de sécurité, connue ou inconnue, comme facteur ayant contribué à leur attaque, et 63 % 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.

Les données de cette année sur les causes racines livrent également un enseignement plus profond. Les causes racines déclarées tendent à se répartir de façon plus équilibrée : tous secteurs confondus, éducation comprise, aucun vecteur d'attaque ne domine. C'est pourquoi il est risqué de concentrer trop étroitement les défenses sur une seule cause racine, les attaquants parviennent désormais à leurs fins par le biais de plusieurs vecteurs.

Les résultats de cette année, en particulier le faible impact de la détection des pare-feux et de l'authentification multifacteur sur les résultats, vont dans le même sens : lorsque les défenses fonctionnent en isolement, vous n'êtes pas protégé. 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 d'enseignement qui s'en sortiront le mieux face au ransomware 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'organisation chaque jour contre ces menaces.

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



2026-09-12 FR (DD)