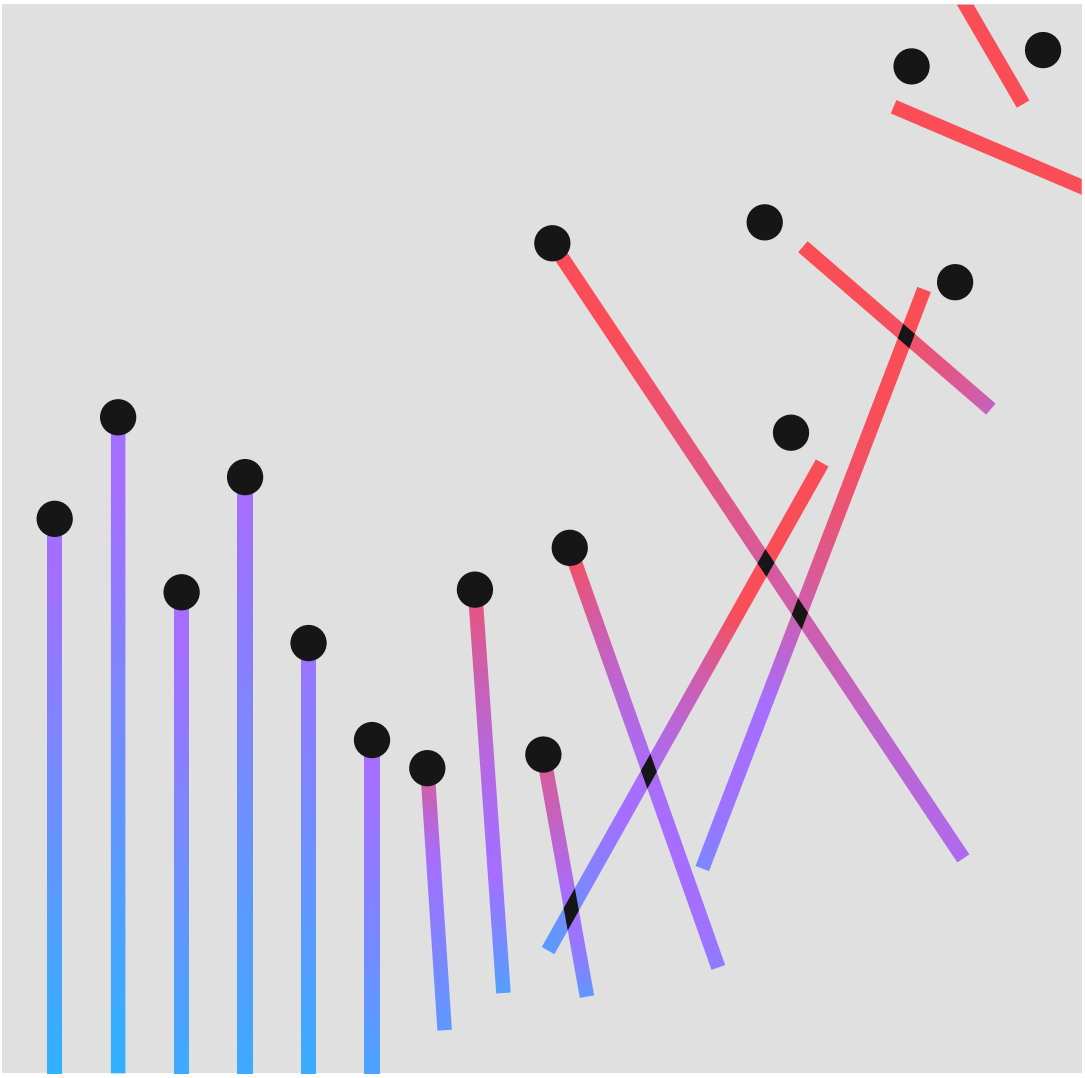
IBM **Security**

Rapport 2022 sur le coût d'une violation de données



Sommaire

Synthèse

Le Rapport sur le coût d'une violation de données offre aux responsables de l'informatique, de la gestion des risques et de la sécurité une perspective sur les facteurs susceptibles d'accroître ou de réduire les coûts croissants d'une violation de données.

Actuellement dans sa 17e année, cette étude est réalisée par le Ponemon Institute et commanditée, analysée et publiée par IBM Security®. Elle porte sur 550 entreprises victimes de violations de données survenues entre mars 2021 et mars 2022. Les violations se sont produites dans 17 pays et à travers 17 secteurs d'activité différents.

Nous avons réalisé plus de 3 600 entretiens avec des employés d'entreprises ayant été victimes de violations de données. Au cours des entretiens, nous avons posé des questions en vue de déterminer les coûts subis par les entreprises pour les différentes activités se rapportant directement à la réponse immédiate et à long terme aux violations de données.

Comme dans les rapports précédents, les données de cette année donnent un aperçu de l'impact de dizaines de facteurs sur les coûts qui continuent de grimper après une violation de données. En outre, le rapport examine les causes profondes, les conséquences à court et à long terme des violations de données, et les facteurs et les technologies qui ont permis aux entreprises de limiter les pertes.

Concrètement, l'étude révèle pour la première fois les informations suivantes :

83 %

des entreprises ont été victimes de plus d'une violation de données.

60 %

des violations ont entraîné des hausses de prix répercutées sur les clients.

79 %

des entreprises d'infrastructures critiques n'ont pas déployé d'architecture Zero Trust.

19 %

des violations se sont produites en raison d'un partenaire commercial compromis.

45 %

des violations se sont produites dans le cloud.

Nouveautés du rapport pour 2022

Chaque année, nous visons à nous appuyer sur les études passées pour suivre l'évolution de la technologie et des événements. Nous essayons également de dresser un tableau plus pertinent des risques et des stratégies de sécurisation des données et de réponse à une violation, de l'intelligence artificielle (IA) au Zero Trust. Couvrant les principales technologies utilisées par les entreprises au cours de l'année passée, l'édition 2022 présente des données nouvelles concernant les éléments suivants :

- Détection et réponse étendues (XDR ou Extended Detection and Response)
- Utilisation de techniques de quantification des risques
- Impacts des technologies individuelles qui contribuent à un cadre de sécurité Zero Trust, telles que la gestion des identités et des accès (IAM) et l'authentification multifacteur (MFA)

En outre, le rapport offre une vision plus large de certains des principaux contributeurs à l'augmentation des coûts d'une violation de données. Pour la première fois, le rapport examine les effets des compromissions de la chaîne d'approvisionnement et le déficit de compétences en sécurité.

Il se penche sur les domaines vulnérables sur le plan de la sécurité, qui vont du cloud aux infrastructures critiques. De même, il s'intéresse plus en détail à l'impact des ransomwares et des attaques destructrices, et au phénomène du télétravail qui continue d'être une réalité pour de nombreuses entreprises après le pic de la pandémie de COVID-19.

Alors que les entreprises sont confrontées à des violations et des coûts qui ne cessent d'augmenter, ce rapport peut servir d'outil pour aider vos équipes à mieux gérer les risques et à limiter les pertes potentielles.
Le rapport comporte cinq sections principales :

- La synthèse, avec les principales conclusions et les nouveautés de l'édition 2022
- L'analyse approfondie des résultats, y compris les coûts des violations par région et secteur d'activité
- Les recommandations de sécurité des experts d'IBM Security sur la base des résultats du rapport
- Les données sur les entreprises et les définitions des secteurs d'activité
- La méthodologie de l'étude, y compris la façon dont les coûts ont été calculés

IBM Security et le Ponemon Institute sont heureux de vous présenter les résultats du Rapport 2022 sur le coût d'une violation de données.

Principales conclusions

Les principales conclusions présentées ici sont basées sur l'analyse réalisée par IBM Security à partir des données compilées par le Ponemon Institute.[1]

4,35 millions USD

Coût total moyen d'une violation de données

Le coût d'une violation de données s'élevait en moyenne à 4,35 millions USD en 2022, un niveau record. Ce chiffre représente une augmentation de 2,6 % par rapport à l'année précédente, lorsque le coût moyen d'une violation était de 4,24 millions USD. En outre, il représente une augmentation de 12,7 % par rapport au coût moyen en 2020, à savoir 3,86 millions USD.

83 %

Pourcentage d'entreprises ayant été victimes de plus d'une violation

Quatre-vingt-trois pour cent des entreprises étudiées ont subi plus d'une violation de données, et seulement 17 % ont déclaré qu'il s'agissait de leur première violation. Soixante pour cent des entreprises étudiées ont déclaré avoir augmenté le prix de leurs services ou produits en raison d'une violation de données.

4,82 millions USD

Coût moyen d'une violation de données affectant une infrastructure critique

Le coût moyen d'une violation de données pour les entreprises d'infrastructures critiques étudiées s'élevait à 4,82 millions USD, soit 1 million USD de plus que le coût moyen pour les entreprises d'autres secteurs. Les entreprises d'infrastructures critiques étaient issues des secteurs des services financiers, de l'industrie, de la technologie, de l'énergie, des transports, des communications, de la santé, de l'éducation et du secteur public. Vingt-huit pour cent ont subi une attaque destructrice ou été victimes d'un ransomware, tandis que 17 % ont subi une violation en raison d'un partenaire commercial compromis.

3,05 millions USD

Économies moyennes associées au déploiement complet de l'IA et de l'automatisation pour la sécurité

Les violations dans les entreprises ayant déployé des solutions complètes d'IA et d'automatisation pour la sécurité coûtent 3,05 millions USD de moins que les violations dans les entreprises n'ayant pas mis en œuvre de telles solutions. Cette différence de 65,2 % dans le coût moyen d'une violation (à savoir 3,15 millions USD avec déploiement complet contre 6,2 millions USD sans déploiement) représentait la plus grande économie constatée dans l'étude. En moyenne, le délai pour identifier et neutraliser la violation, appelé « cycle de vie de la violation », dans les entreprises disposant de solutions complètes d'IA et d'automatisation pour la sécurité était 74 jours plus court que dans les entreprises ne disposant pas de telles solutions, à savoir 249 contre 323 jours. L'utilisation de l'IA et de l'automatisation pour la sécurité a augmenté de près d'un cinquième en deux ans, passant de 59 % en 2020 à 70 % en 2022.

1. Les montants dans ce rapport sont exprimés en dollars américains (USD).

4,54 millions USD

Coût moyen d'une attaque par ransomware, sans compter le coût de la rançon elle-même

Les attaques par ransomware représentaient 11 % des attaques étudiées, en hausse par rapport à 2021 où elles représentaient 7,8 % des violations, soit un taux de croissance de 41 %. Le coût moyen d'une attaque par ransomware a légèrement diminué, passant de 4,62 millions USD en 2021 à 4,54 millions USD en 2022. Ce coût était légèrement supérieur au coût total moyen global d'une violation de données, à savoir 4,35 millions USD.

19 %

Fréquence des violations causées par des identifiants volés ou compromis

L'utilisation d'identifiants volés ou compromis reste la cause la plus fréquente des violations de données. Les identifiants volés ou compromis étaient le principal vecteur d'attaque dans 19 % des violations recensées dans l'étude de 2022, contre 20 % en 2021. Les violations causées par des identifiants volés ou compromis ont coûté en moyenne 4,5 millions USD. Elles comptaient le cycle de vie le plus long : 243 jours pour identifier la violation et 84 jours supplémentaires pour la neutraliser. Deuxième cause la plus fréquente de violation, l'hameçonnage représentait 16 % des violations. Avec un coût moyen par violation de 4,91 millions USD, son coût était également le plus élevé.

59 %

Pourcentage d'entreprises n'ayant pas opté pour l'approche Zero Trust

Seulement 41 % des entreprises étudiées ont déclaré avoir déployé une architecture de sécurité Zero Trust. Pour les 59 % restants qui n'ont pas adopté le Zero Trust, le coût d'une violation est en moyenne 1 million USD plus élevé. Parmi les entreprises d'infrastructures critiques, un pourcentage encore plus élevé, soit 79 %, n'a pas adopté le Zero Trust. En moyenne, le coût d'une violation pour ces entreprises s'élevait à 5,4 millions USD, soit plus de 1 million USD de plus que la moyenne mondiale.

1 million USD

Écart de coût moyen entre une violation où le télétravail a joué un rôle et une violation où il n'a pas été un facteur

Lorsque le télétravail était un facteur à l'origine de la violation, les coûts étaient en moyenne supérieurs de près de 1 million USD à ceux des violations où le télétravail n'était pas un facteur, à savoir 4,99 contre 4,02 millions USD. En moyenne, les violations liées au télétravail coûtent environ 600 000 USD de plus que la moyenne mondiale.

45 %

Pourcentage des violations survenues dans le cloud

Quarante-cinq pour cent des violations étudiées se sont produites dans le cloud. Pourtant, les violations qui se sont produites dans un environnement de cloud hybride ont coûté en moyenne 3,8 millions USD, contre 4,24 millions USD pour les violations dans les clouds privés et 5,02 millions USD pour les violations dans les clouds publics. L'écart de coût était de 27,6 % entre les violations dans un cloud hybride et les violations dans un cloud public. Les entreprises dotées d'un modèle de cloud hybride avaient également des cycles de vie de violations plus courts que celles ayant seulement adopté un modèle de cloud public ou privé.

2,66 millions USD

Économies moyennes associées à une équipe de réponse aux incidents (RI) et à un plan de RI testé régulièrement

Près des trois quarts des entreprises étudiées ont déclaré avoir un plan de RI et 63 % d'entre elles ont affirmé qu'elles le testaient régulièrement. Le fait d'avoir une équipe de RI et un plan de RI qui a été régulièrement testé a permis de réaliser d'importantes économies. En moyenne, les coûts de violations étaient inférieurs de 2,66 millions USD dans les entreprises disposant d'une équipe de RI qui ont testé leur plan de RI par rapport à celles n'ayant pas d'équipe de RI et ne testant pas leur plan de RI. La différence entre 3,26 millions USD et 5,92 millions USD représente une économie de 58 %.

29 jours

Réduction du temps de réponse pour les entreprises qui disposent de technologies de détection et de réponse étendues (XDR)

Les technologies XDR ont été mises en œuvre par 44 % des entreprises. Celles-ci ont constaté des avantages considérables en termes de temps de réponse. Elles ont raccourci le cycle de vie des violations d'environ un mois, en moyenne, par rapport aux entreprises ne disposant pas de technologies XDR. Plus précisément, celles disposant de technologies XDR ont mis 275 jours pour identifier et neutraliser une violation, contre 304 jours pour celles ne disposant pas de telles technologies. Ce chiffre représente une différence de 10 % dans les temps de réponse.

12 ans

Années consécutives durant lesquelles le secteur de la santé a connu le coût moyen d'une violation le plus élevé

Les coûts des violations affectant le secteur de la santé ont atteint un nouveau record. Le coût moyen d'une violation dans ce secteur a augmenté de près de 1 million USD pour atteindre 10,1 millions USD. Au cours des 12 dernières années, le secteur de la santé a affiché les coûts de violations les plus élevés, ceux-ci ayant augmenté de 41,6 % depuis le rapport de 2020. Le secteur des finances arrivait en deuxième position, avec des coûts de 5,97 millions USD en moyenne, suivi du secteur pharmaceutique (5,01 millions USD), du secteur technologique (4,97 millions USD) et du secteur de l'énergie (4,72 millions USD).

9,44 millions USD

Coût moyen d'une violation aux États-Unis, le plus élevé de tous les pays

Les cinq pays et régions affichant les plus hauts coûts moyens d'une violation de données sont les États-Unis (9,44 millions USD), le Moyen-Orient (7,46 millions USD), le Canada (5,64 millions USD), le Royaume-Uni (5,05 millions USD) et l'Allemagne (4,85 millions USD). Les États-Unis sont en tête de liste depuis 12 ans d'affilée. Entre-temps, le Brésil affichait le taux de croissance le plus rapide par rapport à l'année précédente, soit une augmentation de 27,8 %, passant de 1,08 à 1,38 million USD.

Conclusions détaillées

Dans cette section, nous présentons les conclusions détaillées de ce rapport, en 16 thèmes. Les thèmes sont présentés dans l'ordre suivant :

- Faits marquants à l'échelle mondiale
- Cycle de vie d'une violation de données
- Vecteurs d'attaque initiaux
- Principaux facteurs de coût
- IA et automatisation pour la sécurité
- Technologies XDR
- Réponse aux incidents
- Quantification des risques
- Zero Trust
- Ransomwares et attaques destructrices
- Attaques de la chaîne d'approvisionnement
- Infrastructures critiques
- Violations dans le cloud et modèle de cloud
- Télétravail
- Déficit de compétences
- Violations massives

4,35 millions USD

Coût total moyen global d'une violation de données

Coût total moyen d'une violation de données

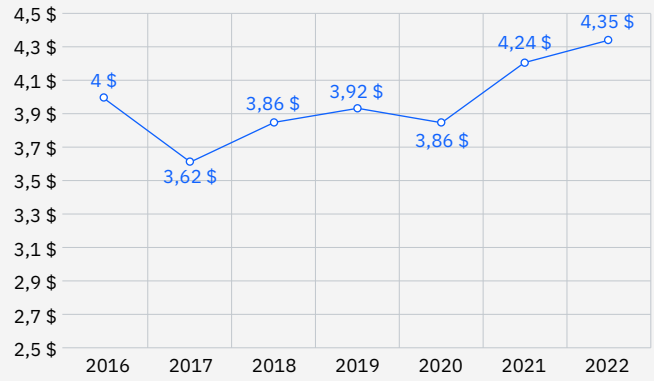


Figure 1 : exprimé en millions USD

Coût moyen par enregistrement d'une violation de données

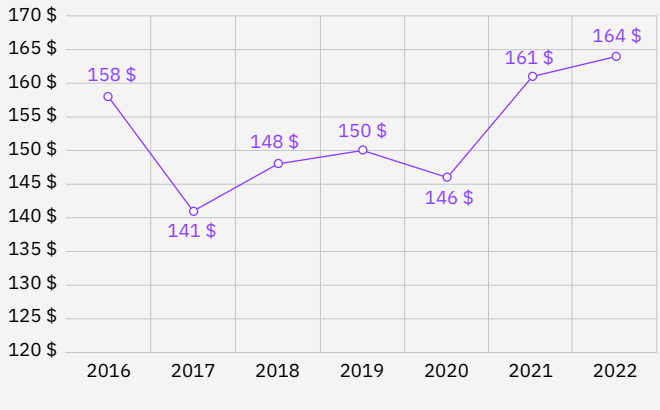


Figure 2 : exprimé en USD

Faits marquants à l'échelle mondiale

Le Rapport sur le coût d'une violation de données a une portée mondiale, et comprend des données provenant de 17 pays et de 17 secteurs d'activité. Dans cette section, nous nous penchons sur plusieurs mesures clés se rapportant à la moyenne mondiale, et nous comparons les coûts entre les pays et les secteurs d'activité.

Figure 1 : le coût moyen d'une violation de données a atteint un niveau record en 2022.
Le coût total moyen mondial d'une violation de données a augmenté de 0,11 million USD pour atteindre 4,35 millions USD en 2022, soit le coût le plus élevé de l'histoire de ce rapport. L'augmentation de 4,24 millions USD dans le rapport de 2021 à 4,35 millions USD dans le rapport de 2022 représente une augmentation de 2,6 %. Au cours des deux dernières années, le coût total moyen a augmenté de 12,7 %. Il s'élevait à 3,86 millions USD en 2020.

Figure 2 : le coût par enregistrement d'une violation de données a atteint son plus haut niveau en sept ans.
Le coût global par enregistrement en 2022 était de 164 USD, soit une augmentation de 1,9 % par rapport à 161 USD en 2021. Par rapport à 146 USD en 2020, cela constitue une augmentation de 12,3 %. Cette étude porte sur les violations représentant entre 2 200 et 102 000 enregistrements. L'utilisation du coût par enregistrement pour calculer le coût des violations supérieures à 102 000 enregistrements n'est pas cohérente avec cette étude. Pour plus d'informations, consultez la section « Méthodologie de l'étude ».

Coût moyen d'une violation de données par pays ou région

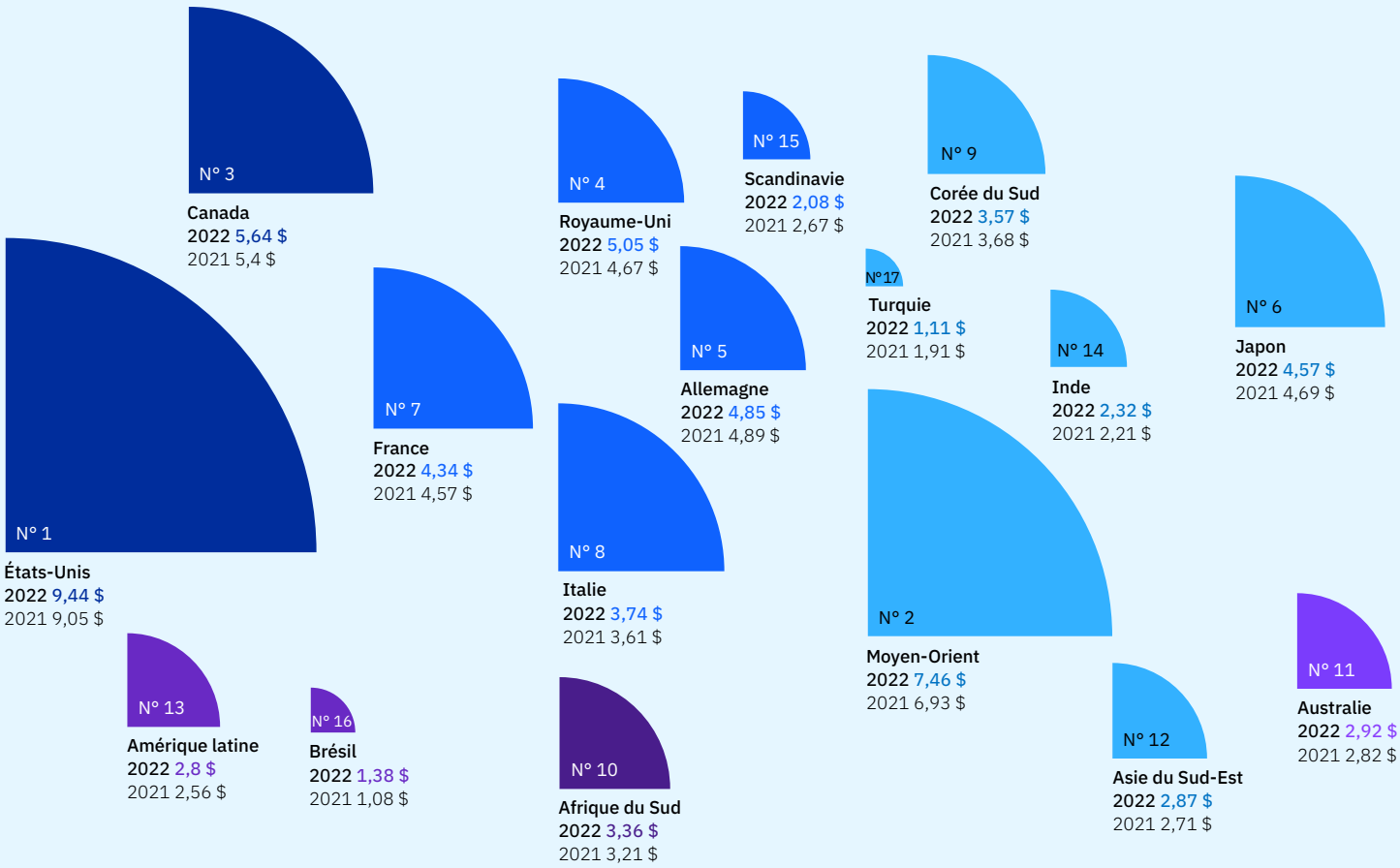


Figure 3 : exprimé en millions USD

Figure 3 : les États-Unis affichaient le coût total moyen d'une violation de données le plus élevé pour la 12e année consécutive. Les cinq pays ou régions affichant les plus hauts coûts moyens d'une violation de données sont les suivants :

1. États-Unis : 9,44 millions USD
2. Moyen-Orient : 7,46 millions USD
3. Canada : 5,64 millions USD
4. Royaume-Uni : 5,05 millions USD
5. Allemagne : 4,85 millions USD

Les États-Unis ont enregistré le coût total moyen le plus élevé d'une violation de données, soit 9,44 millions USD. Cela représente une augmentation de 0,39 millions USD ou 4,3 % par rapport à 2021, où ce coût s'élevait à 9,05 millions USD. Comme l'année dernière, la région Moyen-Orient affichait le deuxième coût total moyen le plus élevé, passant de 6,93 millions USD en 2021 à 7,46 millions USD en 2022. Cela représente une augmentation de 7,6 %, soit 0,53 million USD. Avec un coût total moyen de 5,64 millions USD, soit une augmentation de 0,24 million USD ou 4,4 %, le Canada arrivait une fois de plus en troisième position. Le Royaume-Uni s'est hissé de la huitième à la quatrième place, devançant ainsi l'Allemagne, le Japon et la France parmi les 17 pays ou régions dans le classement. Le coût total moyen d'une violation au Royaume-Uni est passé de 4,67 à 5,05 millions USD, soit une augmentation de 0,38 million USD ou 8,1 %.

Six des 17 pays ou régions étudiés, à savoir l'Allemagne, le Japon, la France, la Corée du Sud, la Scandinavie et la Turquie, ont enregistré une diminution du coût total moyen d'une violation de données. Le Brésil, qui occupait la 16e place du classement avec 1,38 million USD, a connu la plus forte augmentation, soit 0,3 million USD ou 27,8 %. La Turquie, en 17e place, a connu la plus forte baisse, passant de 1,91 à 1,11 million USD, soit une baisse de 0,8 million USD ou 42 %. Les importantes fluctuations des valeurs des devises, comme cela s'est produit en Turquie, peuvent jouer un rôle dans les variations de coûts d'une année à l'autre.

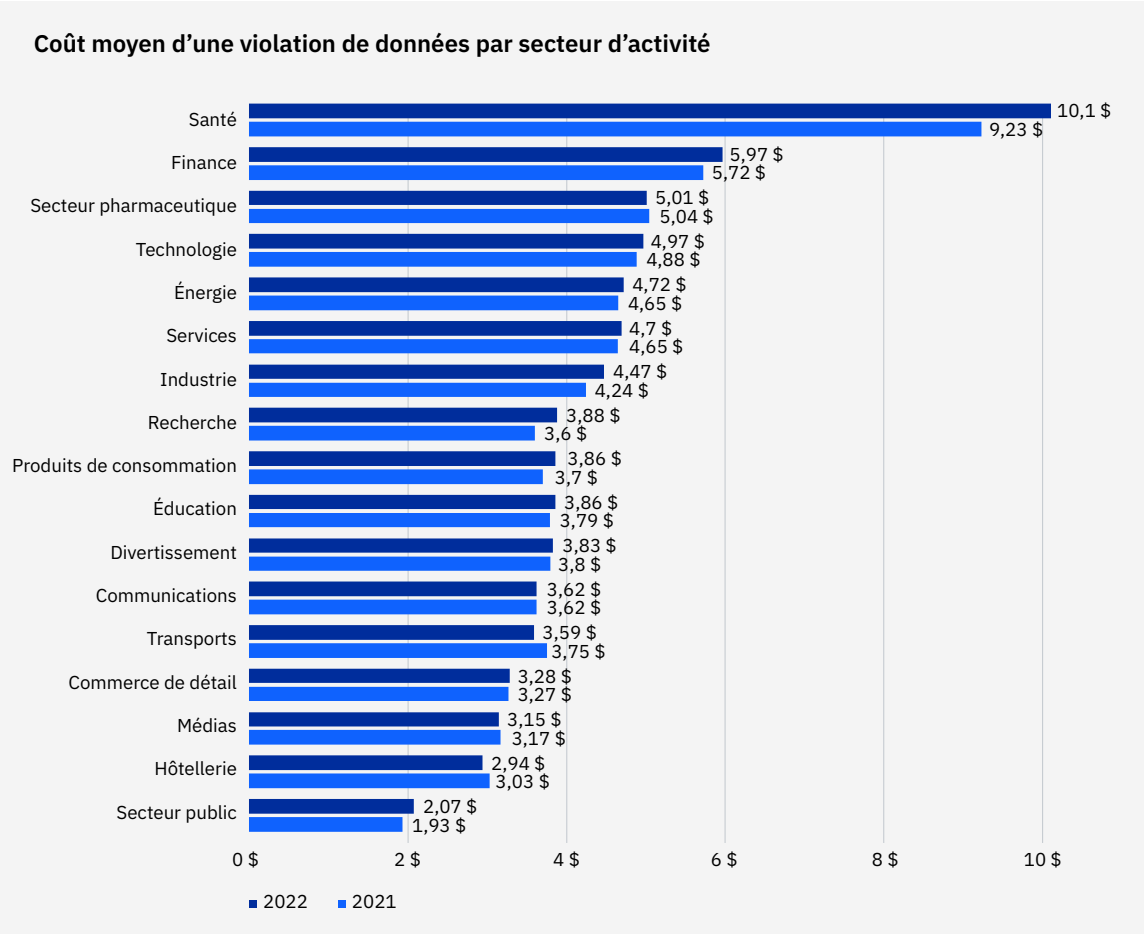


Figure 4 : exprimé en millions USD

Figure 4 : au cours des 12 dernières années, le secteur de la santé a affiché les coûts de violations les plus élevés. Le coût total moyen d'une violation dans ce secteur est passé de 9,23 millions USD en 2021 à 10,10 millions USD en 2022, soit une augmentation de 0,87 million USD ou 9,4 %. Le secteur de la santé est l'un des secteurs les plus réglementés et est considéré comme « infrastructure essentielle » par le gouvernement américain.

Le secteur de la santé est l'un des secteurs les plus réglementés et est considéré comme « infrastructure essentielle » par le gouvernement américain.

Comparé au classement du rapport de 2021, les cinq principaux secteurs en termes de coûts restaient inchangés. Après le secteur de la santé viennent les secteurs financier, pharmaceutique, des technologies et de l'énergie. Le secteur financier est passé de 5,72 millions USD en 2021 à 5,97 millions USD en 2022, soit une augmentation de 0,25 million USD ou 4,4 %. Dans le secteur industriel, composé d'entreprises de produits chimiques, d'ingénierie et de fabrication, le coût total moyen est passé de 4,24 millions USD en 2021 à 4,47 millions USD en 2022, soit une augmentation de 0,23 million USD ou 5,4 %. Le coût total moyen a légèrement diminué dans quatre secteurs : les produits pharmaceutiques, les transports, les médias et l'hôtellerie.

Figure 5 : pour la première fois en six ans, les coûts de détection et d'escalade ont dépassé les coûts de pertes d'affaires, qui était la première des quatre grandes catégories de coûts d'une violation de données.
Parmi les quatre catégories de coûts, à savoir les pertes d'affaires, la détection et l'escalade, la notification et la riposte post-violation, la détection et l'escalade ont représenté la plus grande proportion des coûts d'une violation de données en 2022. Les coûts de détection et d'escalade sont passés de 1,24 million USD en 2021 à 1,44 million USD en 2022, soit une augmentation de 0,2 million USD ou 16,1 %. Les coûts de détection et d'escalade couvrent les activités qui permettent à une entreprise de détecter une violation. Ces coûts comprennent la recherche criminalistique et l'investigation, les services d'évaluation et d'audit, la gestion des crises, et les communications destinées aux cadres et au conseil d'administration.

Pour la première fois depuis au moins six ans, les coûts de pertes d'affaires, qui s'élevaient à 1,42 million USD en 2022, ne représentaient pas la plus grande part des coûts des violations de données. Les coûts de pertes d'affaires ont baissé de 10,7 % par rapport à 2021, où ils s'élevaient à 1,59 million USD. Les coûts de pertes d'affaires comprennent les actions visant à minimiser la perte de clients, la perturbation des activités et les pertes de revenus. Ces coûts comprennent les interruptions d'activité et les pertes de revenus dues aux temps d'arrêt du système ; les coûts liés à la perte de clients existants et à l'acquisition de nouveaux clients ; et les pertes liées à l'atteinte à la réputation et à la bonne volonté.

Les coûts liés à la notification et à la riposte post-violation ont peu changé entre 2021 et 2022. Consulter la rubrique « Mode de calcul des coûts d'une violation de données » dans la section « Méthodologie de l'étude » pour découvrir les définitions de chacune des quatre catégories de coûts.

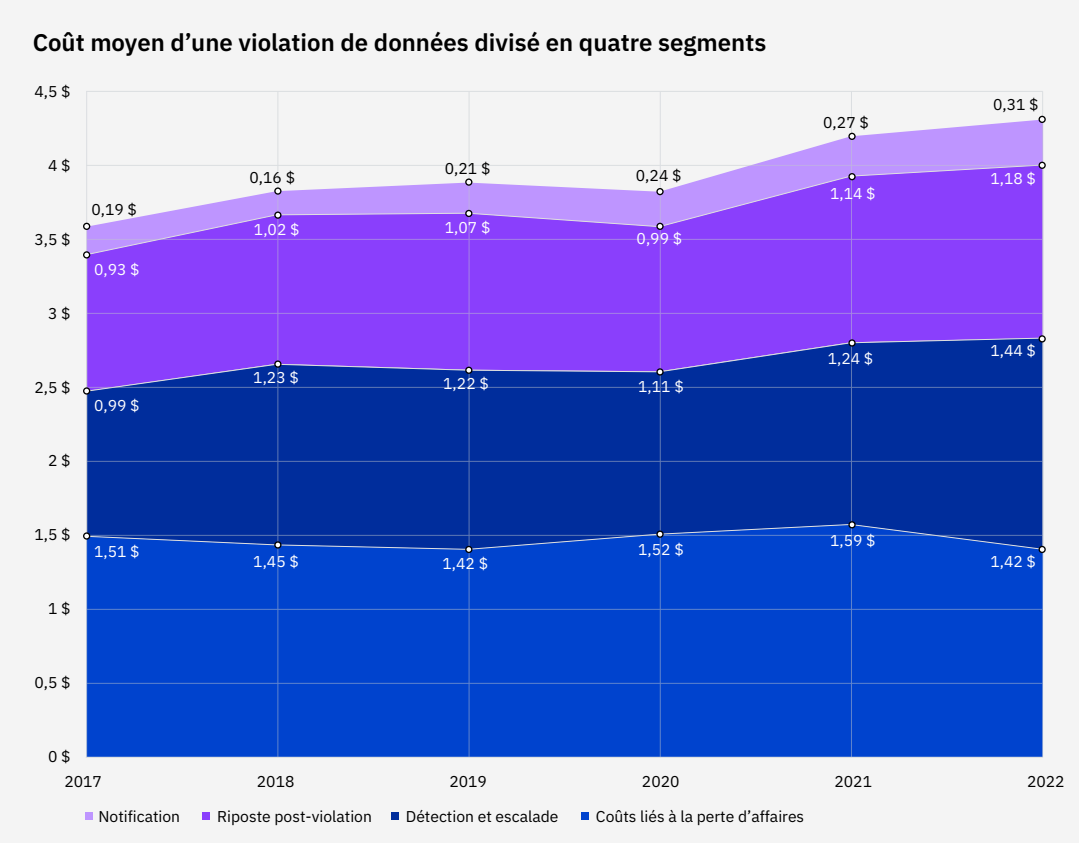


Figure 5 : exprimé en millions USD

S’agissait-il de votre première violation de données ?

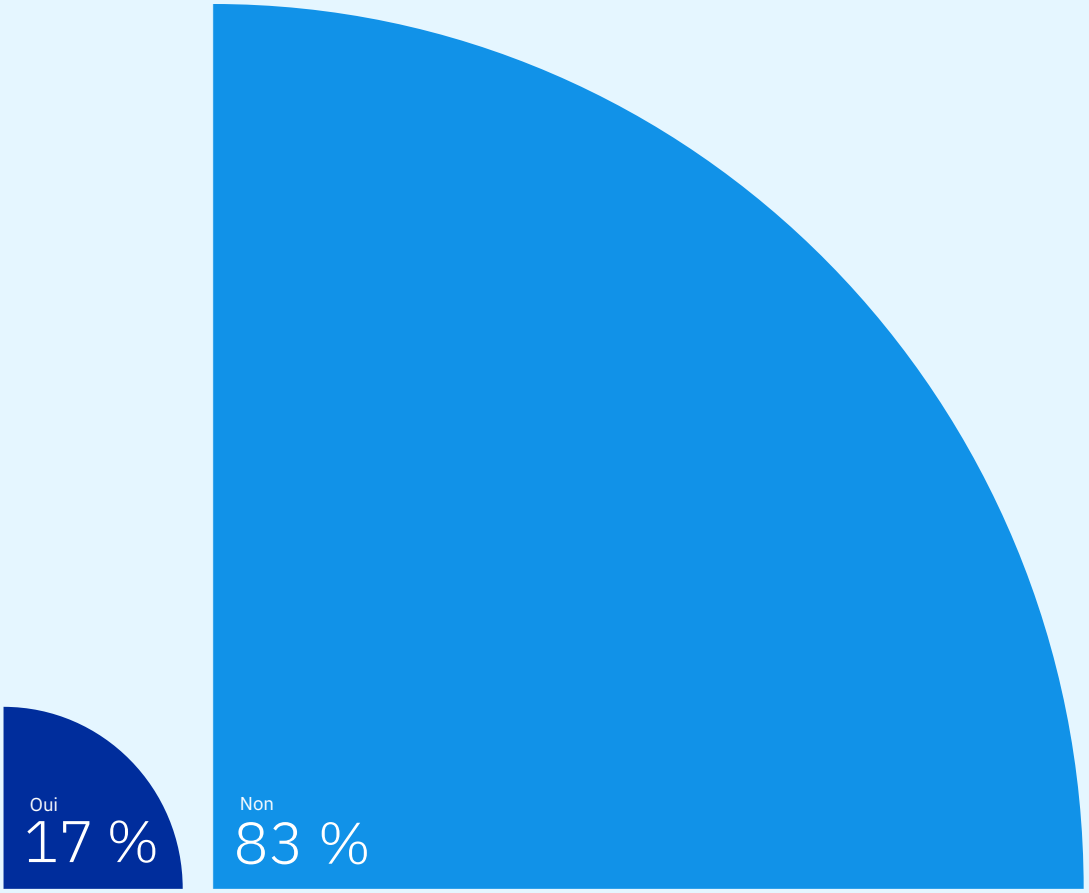


Figure 6

Figure 6 : la plupart des entreprises participant à l’étude ont subi plus d’une violation de données.
Sur les 550 entreprises étudiées, seulement 17 % ont déclaré qu’il s’agissait de leur première violation de données. Quatre-vingt-trois pour cent ont déclaré qu’il ne s’agissait pas de leur première violation de données. Étant donné que les équipes de sécurité traitent de plus en plus d’incidents chaque année et compte tenu de l’impact du télétravail sur la sécurité, il est probable que la récurrence des violations augmente.

Figure 7 : la majorité des entreprises participant à l’étude ont déclaré avoir augmenté le prix de leurs produits et services suite à une violation de données.
60 % ont répondu qu’ils avaient augmenté leurs prix, contre 40 % affirmant le contraire.

La violation de données a-t-elle conduit votre entreprise à augmenter le prix de ses produits et services ?

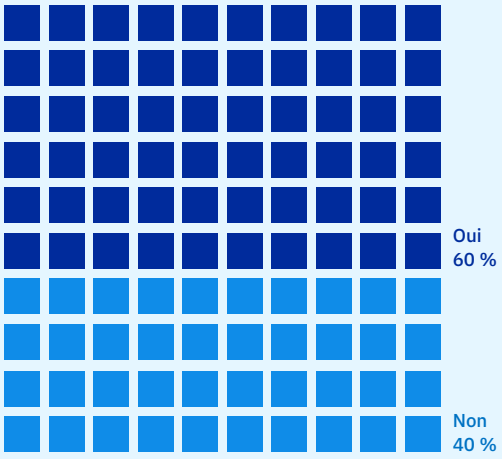


Figure 7

277 jours

Délai moyen pour identifier et neutraliser une violation de données

Cycle de vie d’une violation de données

On appelle « cycle de vie d’une violation de données » le temps écoulé entre la détection initiale de la violation et sa neutralisation. Le délai pour identifier une violation correspond au temps nécessaire pour détecter qu’un incident s’est produit. Le délai pour neutraliser une violation correspond au temps pris par l’entreprise pour résoudre une situation lorsqu’elle a été détectée et, en définitive, restaurer le service. Ces mesures peuvent être utilisées pour déterminer l’efficacité des processus de réponse et de neutralisation des incidents dans une entreprise.

Figure 8 : le délai moyen pour identifier et neutraliser une violation de données est passé de 287 jours en 2021 à 277 jours en 2022, soit une diminution de 10 jours ou 3,5 %.
En 2022, il a fallu en moyenne 207 jours pour identifier une violation et 70 jours pour la neutraliser. En 2021, il a fallu en moyenne 212 jours pour identifier une violation et 75 jours pour la neutraliser. Selon la moyenne de 277 jours en 2022, si une violation se produit le 1er janvier, il faudrait attendre le 4 octobre de la même année pour l’identifier et la neutraliser. Cette moyenne de 277 jours est conforme à la moyenne des sept dernières années, avec une différence maximale de 11 % entre le total le plus bas (257 jours en 2017) et le total le plus élevé (287 jours en 2021).

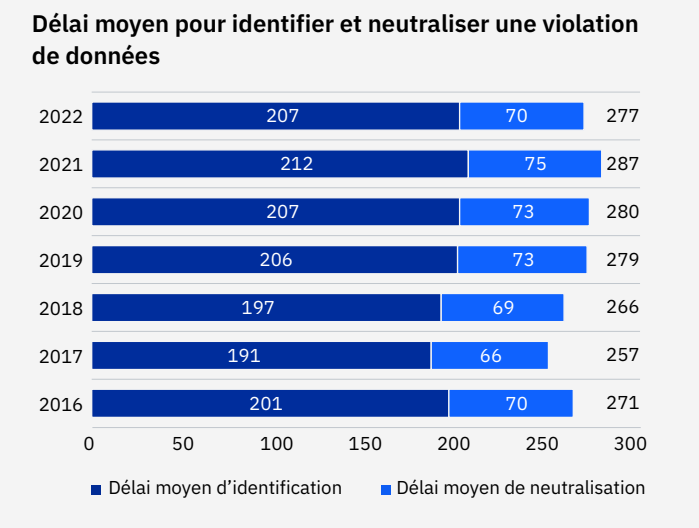


Figure 8 : exprimé en jours

Figure 9 : un cycle de vie plus court continue d'être associé à des coûts plus faibles.
Un cycle de vie d'une violation de données inférieur à 200 jours a été associé à un coût moyen de 3,74 millions USD en 2022, contre 4,86 millions USD pour les violations dont le cycle de vie est supérieur à 200 jours. Cette différence représente une économie moyenne de 1,12 million USD, ou 26,5 %, pour les violations dont le cycle de vie est inférieur à 200 jours.

L'écart de coût entre un cycle de vie supérieur à 200 jours et un cycle de vie inférieur à 200 jours était plus faible en 2022 qu'en 2021, où il était de 1,26 million USD. L'écart de coût en 2022 (1,12 million USD) est le même qu'en 2020. L'écart de coût a légèrement augmenté au cours des sept dernières années, tout comme le coût moyen d'une violation de données. L'écart de coût de 1,26 million USD en 2021 était le plus important des sept dernières années.

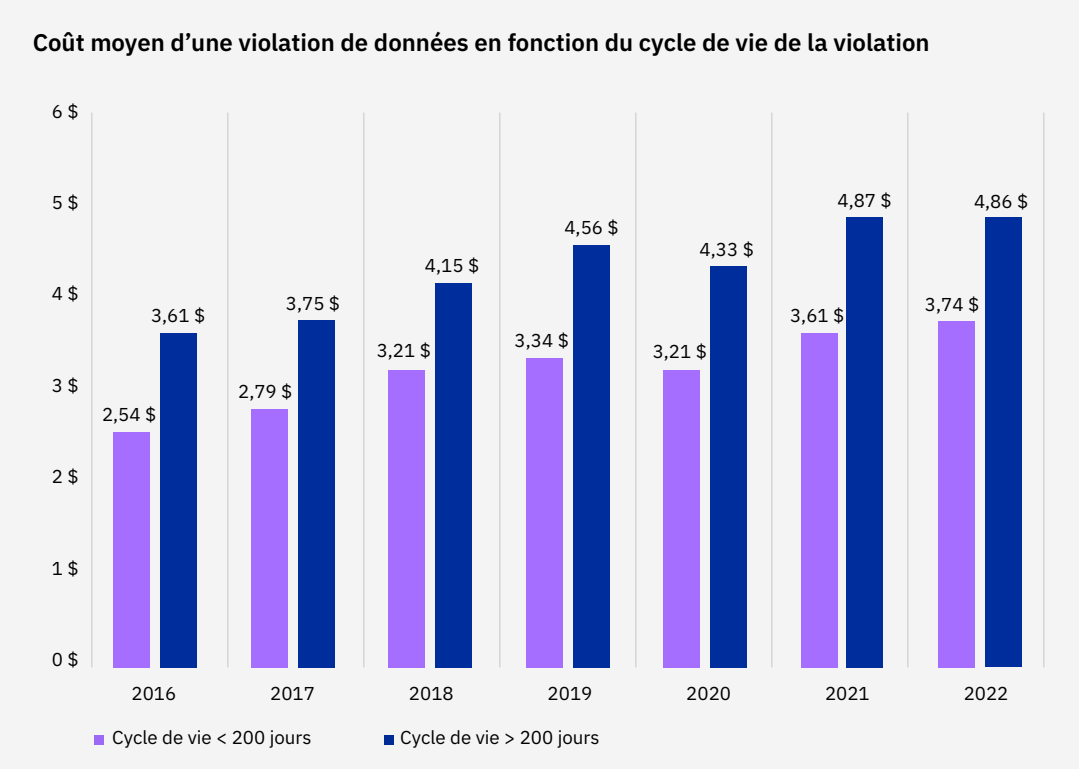


Figure 9 : exprimé en millions USD. La somme des jours pour identifier la violation et des jours pour la neutraliser est égale au cycle de vie de la violation

Temps écoulé	Pourcentage du coût total		
	Moyenne pour 2022	Faible	Élevée
1re année	52 %	66 %	45 %
2e année	29 %	26 %	31 %
Après la 2e année	19 %	8 %	24 %

Figure 10a

Figures 10a et 10b : les violations de données dans les secteurs où la protection des données est très réglementée, à savoir les secteurs de la santé, des finances, de l'énergie, des produits pharmaceutiques et de l'éducation, ont eu tendance à entraîner des coûts au cours des années suivant la violation. La différence entre les environnements très et peu réglementés était particulièrement prononcée deux ans ou plus après la violation de données. On parle ici de coûts à long terme (« longtail costs » en anglais). Dans les secteurs très réglementés, en moyenne 24 % des coûts d'une violation de données ont été subis plus de deux ans après la violation, comparé à une moyenne de 8 % dans les environnements peu réglementés.

Dans le cas de ces derniers, les coûts des violations de données ont eu tendance à s'accumuler au cours des trois à six premiers mois (à savoir 24 % en moyenne du total des coûts). Dans la moyenne globale en 2022, 52 % des coûts ont été subis au cours des 12 premiers mois, 29 % au cours des 12 mois suivants et 19 % plus de deux ans après la violation. Pour les secteurs très réglementés, 45 % des coûts ont été subis la première année, 31 % la deuxième année et 24 % plus de deux ans après.

D'après notre analyse des secteurs très réglementés, nous avons conclu que les coûts réglementaires et juridiques peuvent avoir contribué à des coûts plus élevés dans les années qui ont suivi une violation.

Remarque : cette analyse comprenait un sous-ensemble de 218 entreprises disposant de données historiques sur des violations antérieures.

Répartition moyenne dans le temps des coûts d'une violation de données dans les environnements à faible vs forte réglementation des données

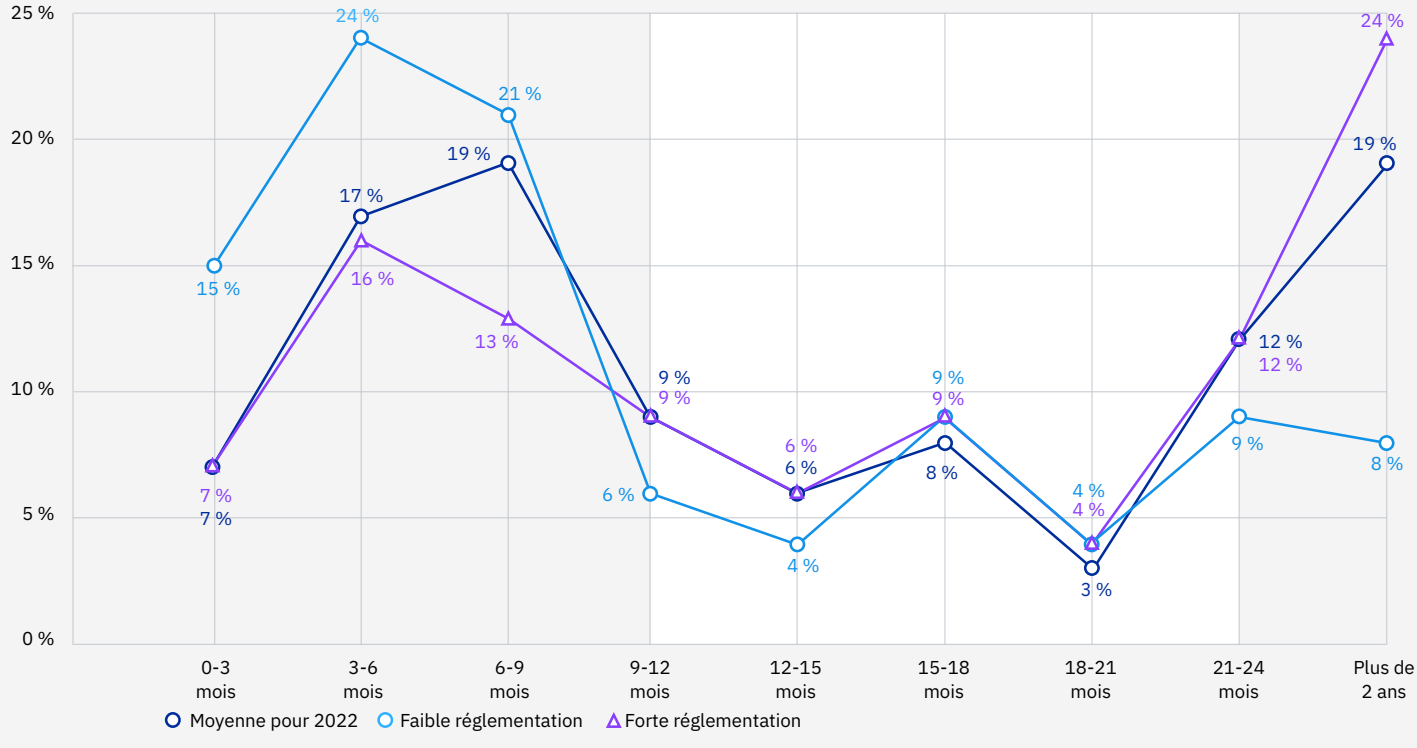


Figure 10b : pourcentage des coûts totaux accumulés à intervalles de trois mois

4,91 millions USD

Coût moyen d'une violation de données avec l'hameçonnage comme vecteur d'attaque initial

Vecteurs d'attaque initiaux

Cette section examine la prévalence des vecteurs d'attaque initiaux et les coûts associés. Dans notre étude, les violations sont réparties selon 10 vecteurs d'attaque initiaux, allant de la perte accidentelle de données et de la configuration incorrecte du cloud au hameçonnage, en passant par les menaces d'initié (ou internes) et les identifiants volés ou compromis. Cette section compare également le temps moyen nécessaire pour identifier et neutraliser les violations en fonction de leur vecteur d'attaque initial.

Figure 11 : les identifiants volés ou compromis étaient responsables de 19 % des violations étudiées en 2022, constituant le vecteur d'attaque initial le plus courant, pour un coût moyen de 4,5 millions USD.
En 2022, les vecteurs d'attaque initiaux les plus courants étaient les identifiants compromis (19 % des violations), l'hameçonnage (16 %), la configuration incorrecte du cloud (15 %) et les vulnérabilités dans les logiciels tiers (13 %). Les quatre principaux vecteurs d'attaque initiaux apparaissaient dans le même ordre dans le rapport de 2021.

En 2022, selon la moyenne, le vecteur d'attaque initial le plus coûteux était l'hameçonnage, avec 4,91 millions USD. Il était suivi des e-mails professionnels compromis, avec 4,89 millions USD, soit 6 % des violations ; les vulnérabilités dans les logiciels tiers, avec 4,55 millions USD ; et les identifiants compromis, avec 4,5 millions USD.

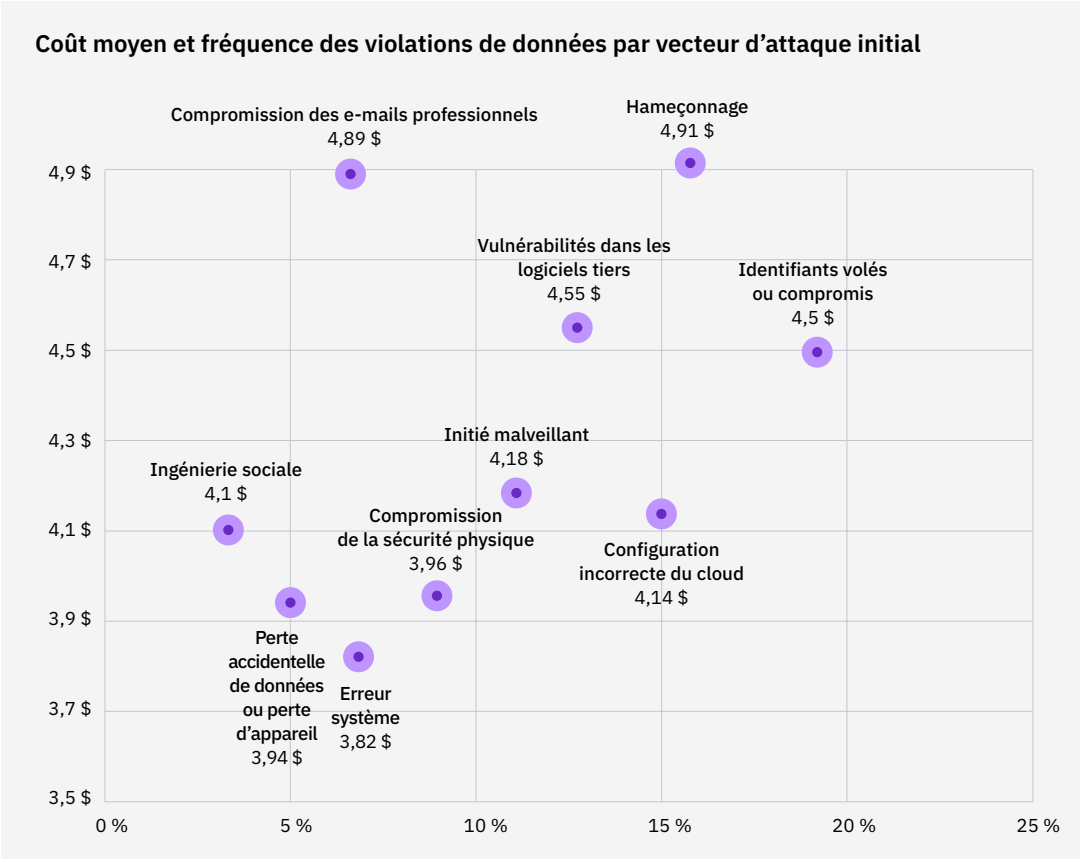


Figure 11 : exprimé en millions USD

Figure 12 : les vecteurs d'attaque avec des délais moyens d'identification et de neutralisation plus longs, tels que l'hameçonnage ou les e-mails professionnels compromis, figuraient également parmi les types de violations les plus coûteux.
Les identifiants volés ou compromis constituaient le vecteur d'attaque initial ayant le délai moyen d'identification et de neutralisation le plus long, soit 327 jours. Ce délai est supérieur de 16,6 % au délai total moyen pour identifier et neutraliser une violation de données. Les identifiants compromis étaient également le vecteur d'attaque initial le plus courant (19 %) à l'origine des violations recensées dans l'étude.

En termes de délai d'identification et de neutralisation, les violations causées par des e-mails professionnels compromis arrivaient en seconde place, avec un délai moyen de 308 jours. Les e-mails professionnels compromis constituaient également le deuxième vecteur d'attaque initial le plus coûteux, les violations de ce type coûtant en moyenne 4,89 millions USD. Avec un délai moyen d'identification et de neutralisation de 295 jours, les violations causées par l'hameçonnage arrivaient en troisième position, pour le coût par vecteur d'attaque initial le plus élevé, soit 4,91 millions USD. Avec un délai moyen d'identification et de neutralisation supérieur à la moyenne mondiale, soit 284 jours contre 277 jours, les vulnérabilités dans les logiciels tiers occupaient la quatrième place.

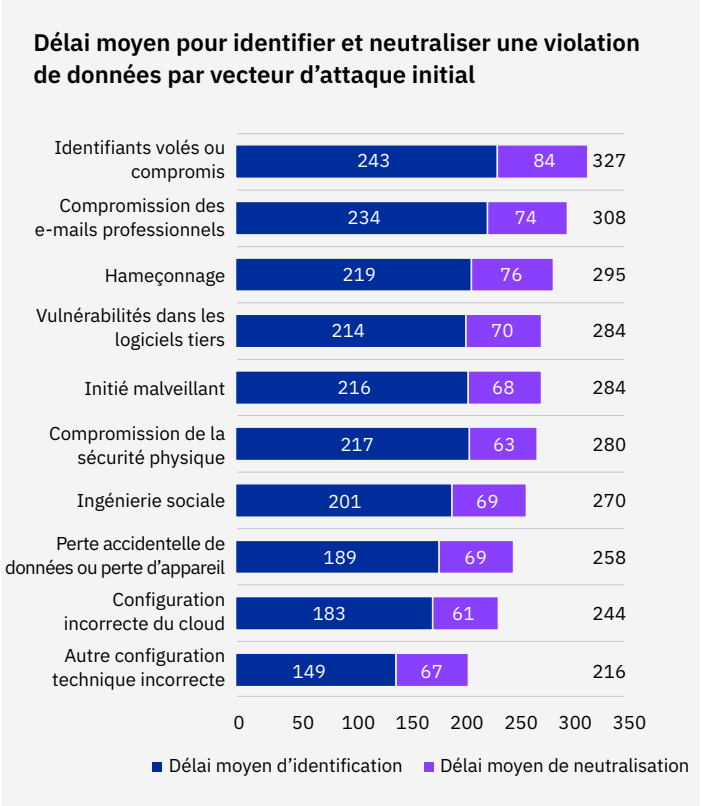


Figure 12 : exprimé en jours

5,57 millions USD

Coût moyen d’une violation pour les entreprises présentant un niveau élevé de manquements à la conformité

Principaux facteurs de coût

Cette section passe en revue une multitude de facteurs qui influent sur le coût d’une violation de données, y compris les différents types de technologies et de pratiques de sécurité. Nous analysons 28 facteurs de coût particuliers et examinons leur impact sur le coût moyen d’une violation de données. Nous étudions comment ces 28 facteurs ont été associés soit à des coûts de violation inférieurs à la moyenne en raison de leurs propriétés d’atténuation des coûts soit, dans le cas contraire, à un coût supérieur à la moyenne en raison de leurs propriétés d’amplification des coûts.

Cette année, les facteurs de coût suivants figurent pour la première fois dans le rapport : la gestion des identités et des accès (IAM) ; les technologies XDR ; l’authentification multifacteur (MFA) ; et les équipes de gestion de crise.

Ces facteurs de coût ne sont pas additifs. Ajouter plusieurs facteurs de coût ensemble pour calculer le coût d’une violation n’est donc pas cohérent avec cette étude.

La Figure 13 montre l'impact de 28 facteurs sur le coût moyen d'une violation de données.
Le graphique illustre l'écart de coût moyen dans les entreprises où ces facteurs sont présents par rapport au coût moyen d'une violation de données de 4,35 millions USD. Le graphique est divisé entre les facteurs associés à un coût de violation inférieur à la moyenne, qui sont des atténuateurs de coûts, et les facteurs associés à un coût de violation supérieur à la moyenne, ou amplificateurs de coût.

Les plateformes d'IA, une approche DevSecOps et la présence d'une équipe de réponse aux incidents (RI) étaient les trois facteurs associés à la plus forte diminution des coûts par rapport au coût moyen d'une violation. Par exemple, dans les entreprises dotées de plateformes d'IA, le coût moyen d'une violation était inférieur de 300 075 USD au coût moyen d'une violation de données de 4,35 millions USD, soit environ 4,05 millions USD.

D'autre part, la complexité du système de sécurité, la migration vers le cloud et les manquements à la conformité étaient les trois facteurs associés à la plus forte augmentation nette du coût moyen. Par exemple, les violations dans les entreprises dotées d'un système de sécurité complexe ont coûté en moyenne 290 655 USD de plus que le coût moyen d'une violation de données de 4,35 millions USD, soit environ 4,64 millions USD.

Pour la première fois, l'étude a mesuré l'impact des quatre nouveaux facteurs de coût suivants : la gestion des identités et des accès (IAM) ; les technologies XDR ; l'authentification multifacteur (MFA) ; et les équipes de gestion de crise. Chacun de ces facteurs était associé à des coûts de violation inférieurs à la moyenne, avec l'IAM en tête.

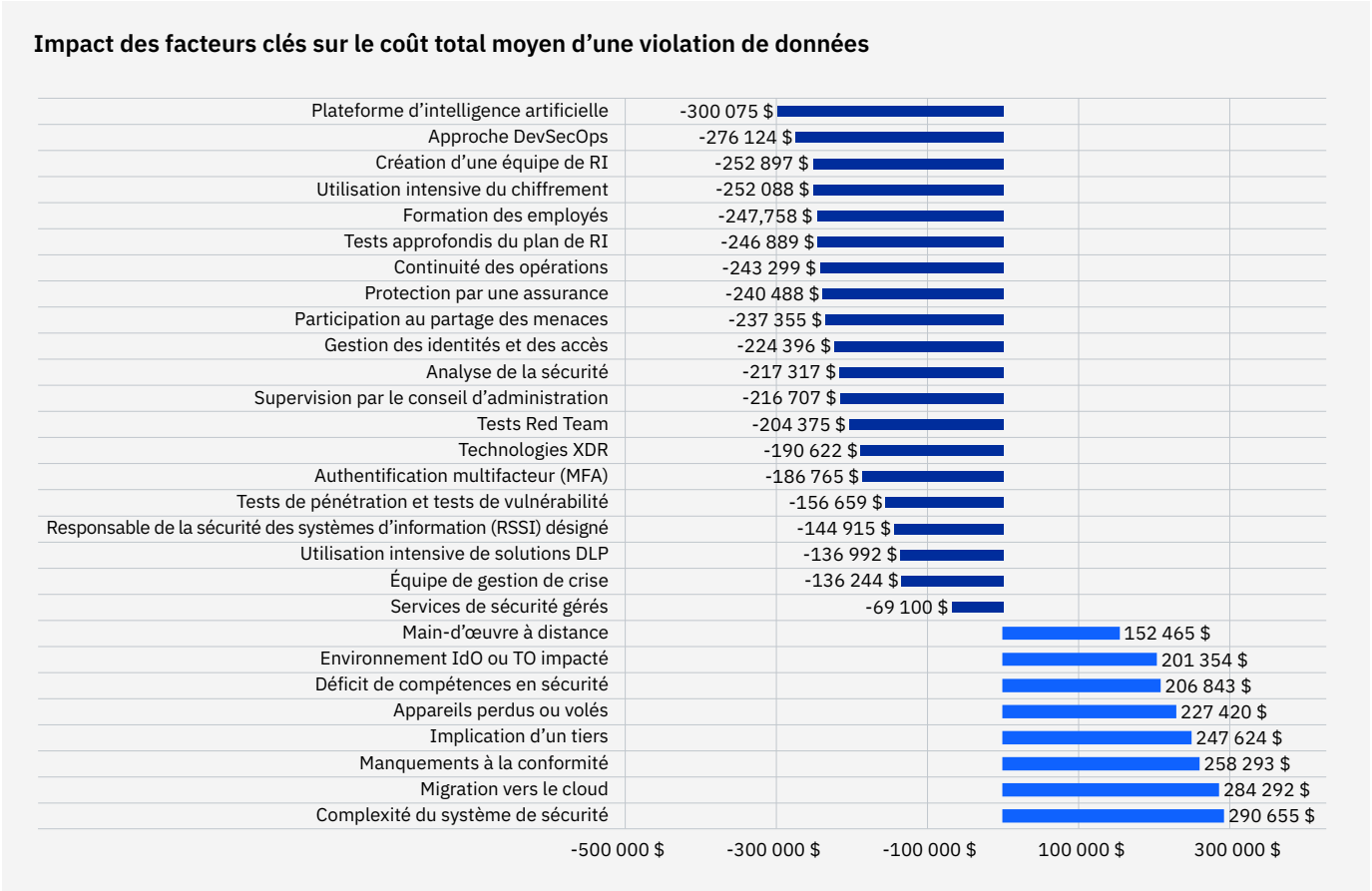


Figure 13 : exprimé en USD

Coût moyen d'une violation de données pour les entreprises présentant un niveau élevé vs un niveau faible de trois facteurs d'amplification des coûts

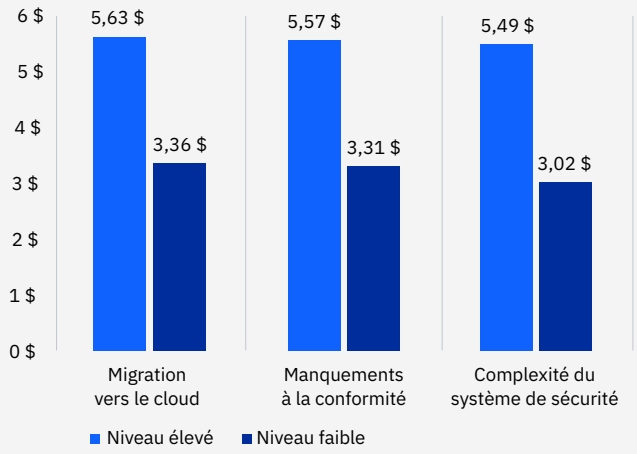


Figure 14 : exprimé en millions USD

Coût moyen d'une violation de données pour les entreprises présentant un niveau élevé vs un niveau faible de trois facteurs d'atténuation des coûts

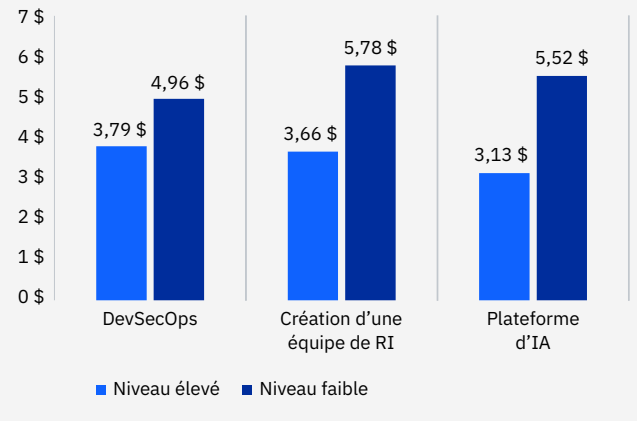


Figure 15 : exprimé en millions USD

La Figure 14 examine les trois facteurs de coût – sur les 28 évalués – qui ont le plus fort potentiel d'amplification du coût moyen d'une violation de données.
Ce graphique compare les entreprises où le facteur de coût occupe une place importante et celles où il est négligeable. En termes de complexité du système de sécurité, il y avait une différence de 2,47 millions USD, ou 58 %, entre les entreprises où ce facteur de coût occupait une place importante et celles où il était négligeable. Pour ce qui est de la migration vers le cloud, cette différence était de 2,27 millions USD, soit 50,5 %. En ce qui concerne les manquements à la conformité, une différence de 2,26 millions USD, soit 50,9 %, a été relevée. Ces données ont montré que lorsque ces facteurs de coût occupaient une place importante, cela engendrait un coût largement supérieur au coût moyen d'une violation de données. Les entreprises pour lesquelles la migration vers le cloud constituait un facteur de coût important affichaient un coût moyen de 5,63 millions USD, soit 1,28 million USD de plus que le coût moyen d'une violation de données, à savoir une différence de 25,7 %.

La Figure 15 examine les trois facteurs de coût – sur les 28 évalués – qui ont le plus fort potentiel d'atténuation du coût moyen d'une violation de données.
Ce graphique compare les entreprises où le facteur de coût occupe une place importante et celles où il est négligeable. Dans les entreprises utilisant de manière intensive les plateformes de sécurité basées sur l'IA, le coût moyen d'une violation était de 2,39 millions USD, soit 55,3 % de moins que pour les entreprises utilisant peu les plateformes d'IA. Dans les entreprises utilisant de manière intensive leur équipe de RI, le coût moyen d'une violation était de 2,12 millions USD, soit 44,9 % de moins que pour les entreprises qui l'utilisent peu. Dans les entreprises utilisant de manière intensive l'approche DevSecOps, le coût moyen d'une violation était de 1,17 million USD, soit 26,7 % de moins que pour les entreprises qui l'utilisent peu. Les entreprises dans lesquelles ces facteurs de coût occupaient une place importante affichaient un coût nettement inférieur au coût moyen d'une violation de données. Dans les entreprises utilisant de manière intensive les plateformes d'IA, le coût moyen d'une violation était de 3,13 millions USD, soit 1,22 million USD de moins que le coût moyen global d'une violation de données, à savoir une différence de 32,6 %.

3,05 millions USD

Économies moyennes grâce à l'IA et à l'automatisation pour la sécurité entièrement déployées par rapport à l'absence d'IA et d'automatisation pour la sécurité

IA et automatisation pour la sécurité

Pour la cinquième fois, nous avons examiné la relation entre le coût des violations de données et l'IA et l'automatisation pour la sécurité. Dans ce contexte, l'IA et l'automatisation pour la sécurité font référence aux technologies de sécurité qui renforcent ou remplacent l'intervention humaine dans l'identification et la neutralisation des incidents et des tentatives d'intrusion. Ces technologies s'appuient sur l'IA, l'apprentissage automatique, l'analyse et l'orchestration automatisée de la sécurité.

À l'autre extrémité du spectre se trouvent des processus manuels, souvent effectués à l'aide de dizaines d'outils et systèmes complexes et non intégrés, sans partage des données.

Figure 16 : le pourcentage des entreprises ayant déployé entièrement ou partiellement l'IA et l'automatisation pour la sécurité a augmenté de cinq points, passant de 65 à 70 % entre 2021 et 2022.
Le déploiement complet de l'IA et de l'automatisation pour la sécurité a augmenté de six points, passant de 25 à 31 % entre 2021 et 2022, et de 10 points, à savoir 21 à 31 %, entre 2020 et 2022. Le pourcentage d'entreprises n'ayant pas déployé l'IA et l'automatisation pour la sécurité est passé de 41 % en 2020 et 35 % en 2021 à 30 % en 2022, soit une différence de 11 points.

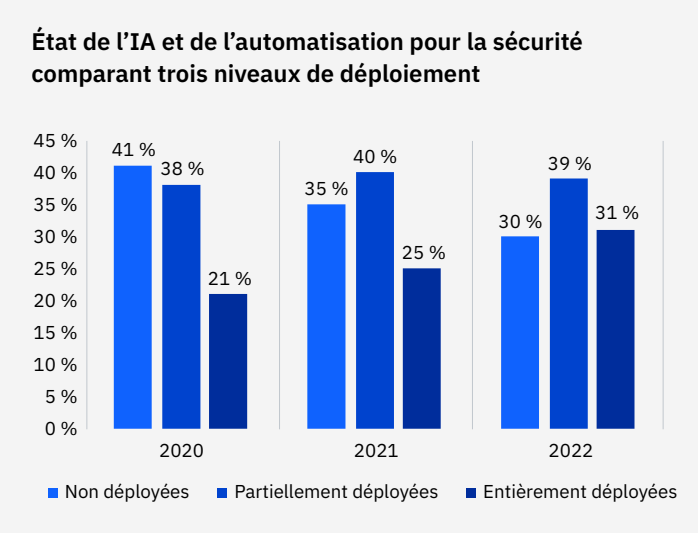


Figure 16 : pourcentage d'entreprises par niveau de déploiement

Figure 17 : le déploiement complet de l'IA et de l'automatisation pour la sécurité était associé à des coûts moyens de violation inférieurs de 3,05 millions USD aux coûts moyens sans déploiement, soit une différence de 65,2 %, ce qui représente la plus grande économie constatée dans l'étude.
Le coût total moyen d'une violation de données s'élevait à 3,15 millions USD dans les entreprises disposant d'une IA et d'une automatisation pour la sécurité entièrement déployées, contre 6,2 millions USD dans les entreprises n'ayant pas déployé l'IA et l'automatisation pour la sécurité. L'écart entre ces coûts moyens était plus faible en 2022 qu'en 2021, où il se chiffrait à 3,81 millions USD et 3,58 millions USD, respectivement.

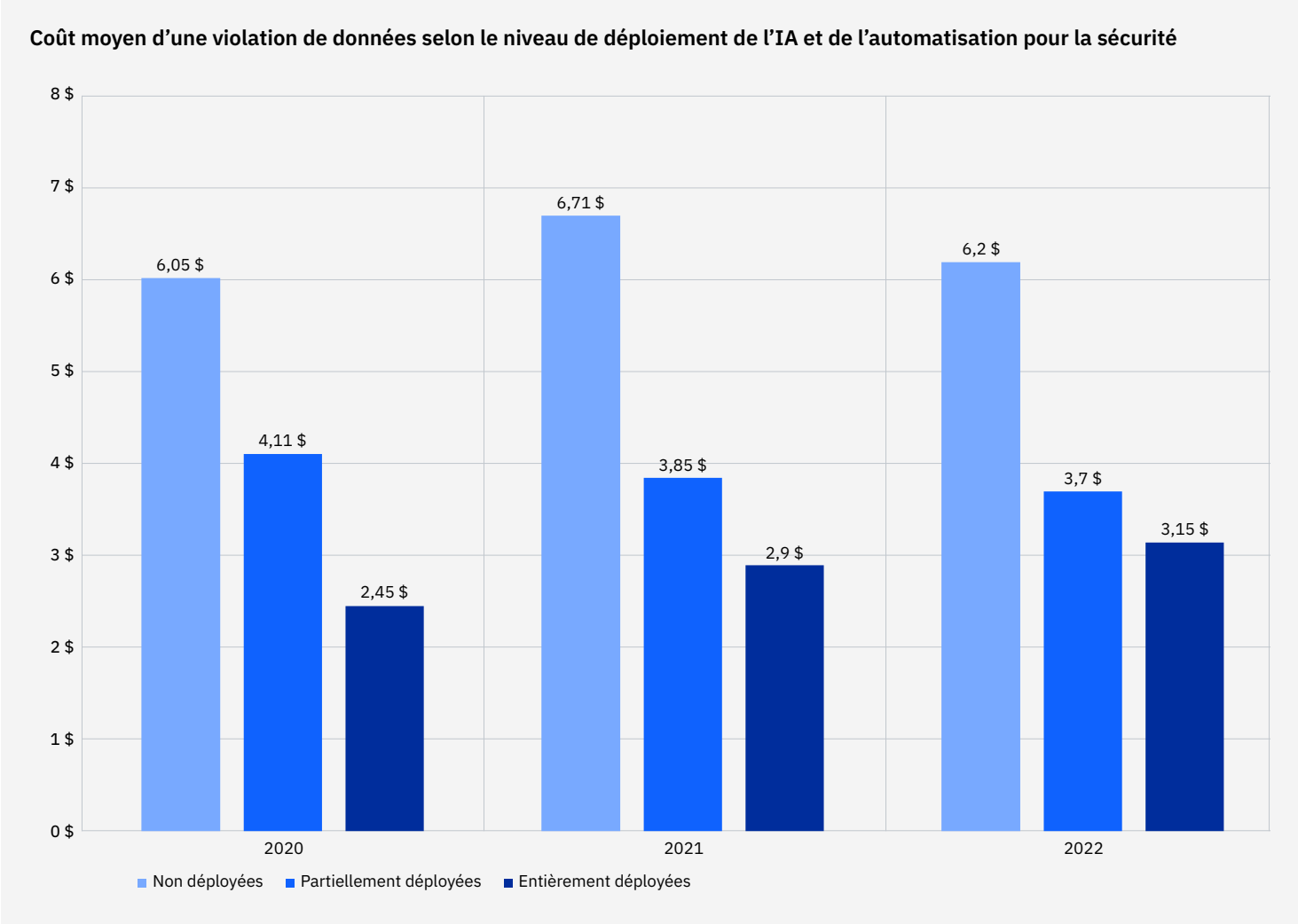


Figure 17 : exprimé en millions USD

Délai moyen pour identifier et neutraliser une violation de données selon le niveau de déploiement de l'IA et de l'automatisation pour la sécurité

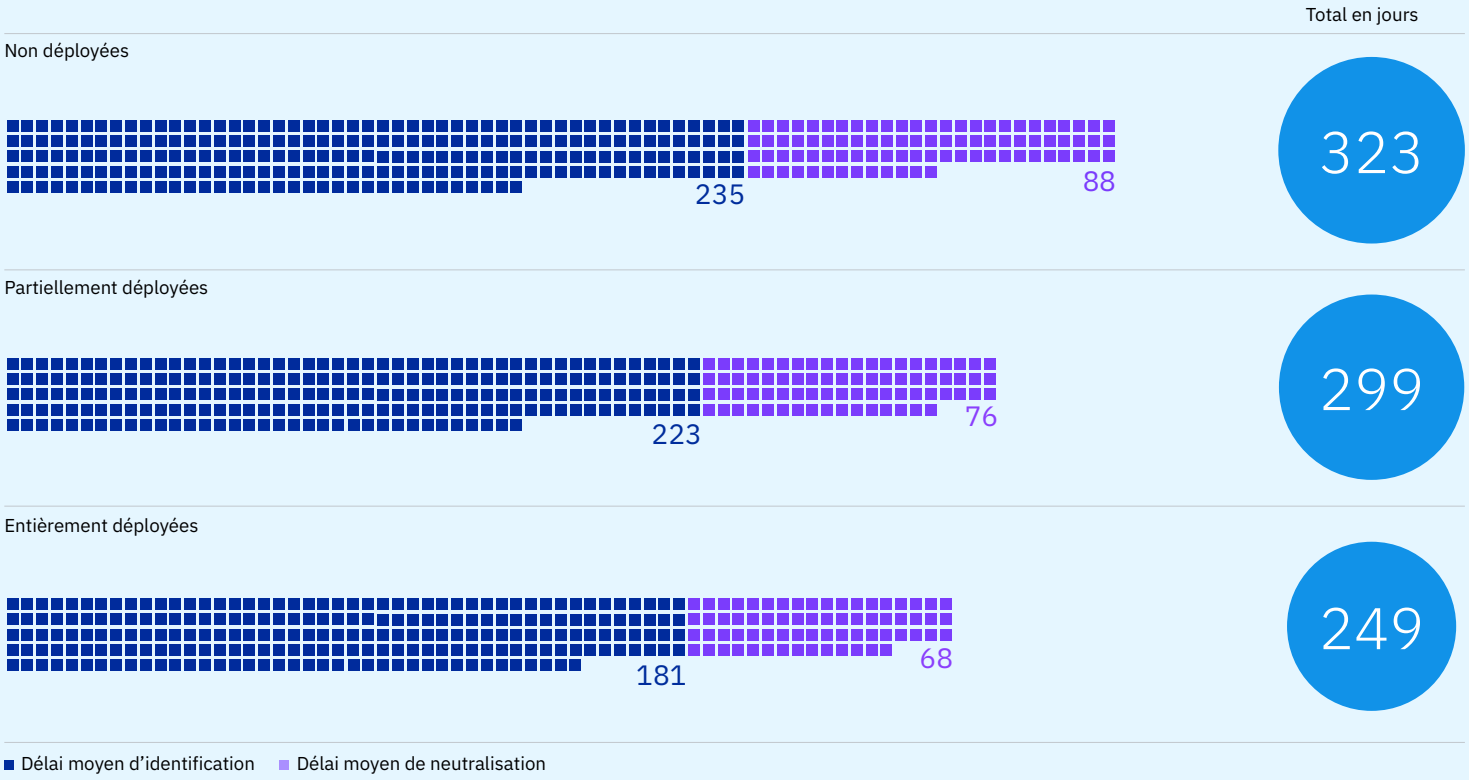


Figure 18 : exprimé en jours

Figure 18 : les entreprises disposant d'une IA et d'une automatisation pour la sécurité entièrement déployées ont été en mesure de détecter et de neutraliser une violation beaucoup plus rapidement que les entreprises n'ayant pas déployé l'IA et l'automatisation pour la sécurité.
Il leur a fallu en moyenne 181 jours pour identifier et 68 jours pour neutraliser une violation de données, pour un cycle de vie total de 249 jours. Les entreprises n'ayant pas déployé l'IA et l'automatisation pour la sécurité ont mis en moyenne 235 jours pour identifier et 88 jours pour neutraliser une violation, pour un cycle de vie total de 323 jours, soit 74 jours de plus que celles disposant d'une IA et d'une automatisation pour la sécurité entièrement déployées. Le délai moyen pour identifier et neutraliser une violation était de 299 jours au total avec l'IA et l'automatisation pour la sécurité partiellement déployées.

29 jours

Les entreprises utilisant des technologies XDR ont identifié et neutralisé les violations 29 jours plus tôt que celles n'en utilisant pas

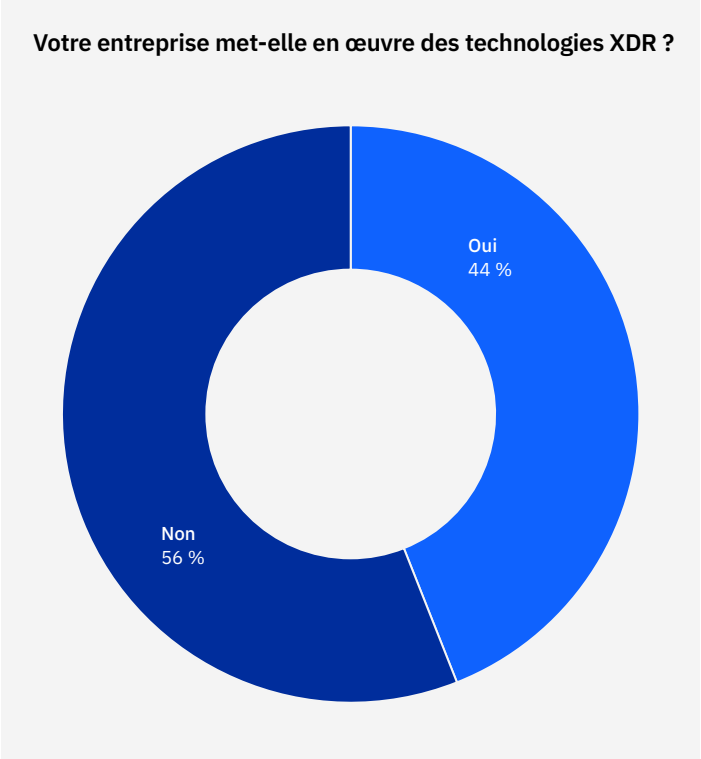


Figure 19

Technologies XDR

Pour la première fois, l'étude a examiné les effets des technologies XDR sur le coût d'une violation de données. Cette section examine la prévalence des technologies XDR dans les entreprises étudiées, ainsi que leur impact sur le coût total moyen et le délai moyen pour neutraliser les violations de données.

Concrètement, les technologies XDR ont eu un impact sur le coût moyen d'une violation et ont permis de réaliser des économies de 9,2 %. Même si ces économies semblent modestes à première vue, le véritable impact réside dans le temps économisé lors d'une violation grâce aux technologies XDR, à savoir près d'un mois. Un délai plus long pour identifier et neutraliser une violation peut entraîner un coût global supérieur et avoir des conséquences plus graves.

Figure 19 : les dispositifs XDR étaient couramment utilisés, mais pas encore par la majorité des entreprises.
Selon l'enquête menée auprès de 550 entreprises, 44 % mettent en œuvre des technologies XDR, contre 56 %.

Figure 20 : l'utilisation des technologies XDR était associée à un coût de violation de données inférieur à la moyenne.
Les entreprises ayant mis en œuvre des technologies XDR affichaient un coût moyen de violation de données de 4,15 millions USD, contre 4,55 millions USD pour les autres. Ce coût était supérieur à la moyenne mondiale et dépassait de 0,4 million USD le coût moyen d'une violation dans les entreprises mettant en œuvre des technologies XDR, soit une différence de 9,2 %.

Figure 21 : le délai moyen d'identification et de neutralisation d'une violation de données était nettement inférieur avec les technologies XDR.
En moyenne, il a fallu aux entreprises ayant déployé des technologies XDR 275 jours pour identifier et neutraliser une violation, contre 304 jours dans les entreprises ne l'ayant pas fait, soit 29 jours de moins. Cela représente une différence de 10 % dans le délai moyen pour identifier et neutraliser une violation.

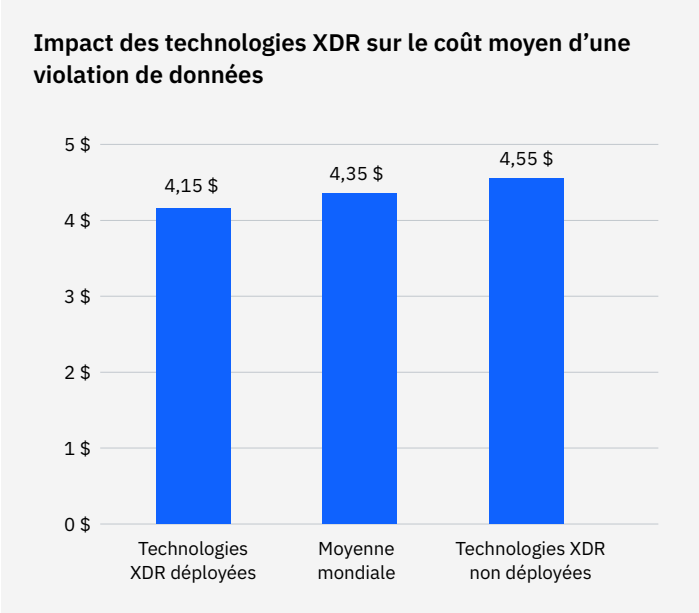


Figure 20 : exprimé en millions USD

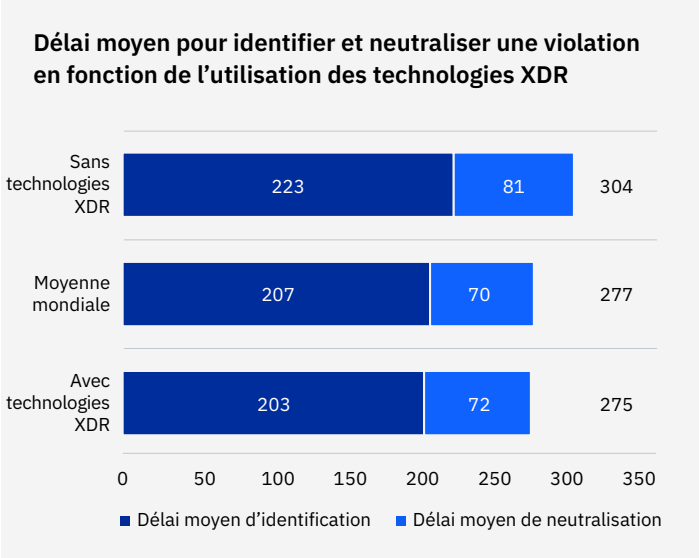


Figure 21 : exprimé en jours

2,66 millions USD

Économies moyennes sur les coûts d'une violation dans les entreprises dont l'équipe de RI a testé son plan de RI vs celles qui n'ont pas d'équipe de RI et qui n'ont pas testé leur plan de RI

Réponse aux incidents

Au cours des années précédentes, cette étude a montré que l'utilisation d'équipes de RI et les tests du plan de RI réduisaient considérablement le coût moyen d'une violation de données. Dans l'analyse de cette année, nous nous sommes de nouveau penchés sur l'impact des équipes, des dispositifs et des processus de RI sur le coût d'une violation.

Figure 22 : la majorité des entreprises ayant pris part à l'étude disposaient de plans de RI et les testaient régulièrement. Près des trois quarts des entreprises étudiées ont déclaré avoir un plan de RI, 73 % affirmant qu'elles avaient un plan de RI contre 27 % déclarant qu'elles n'en avaient pas. Parmi les entreprises ayant un plan de RI, 63 % ont déclaré qu'elles testaient régulièrement leur plan de RI, contre 37 % déclarant ne pas le tester régulièrement.

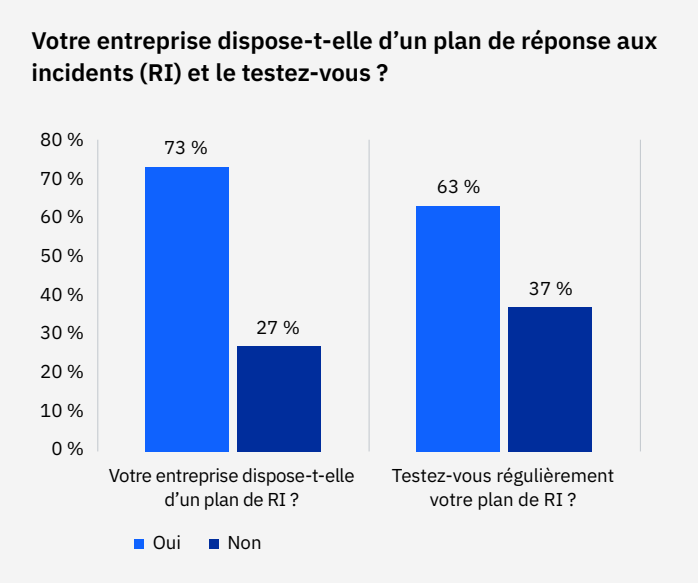


Figure 22

Coût moyen d'une violation de données avec une équipe de réponse aux incidents (RI) et un plan de RI testé

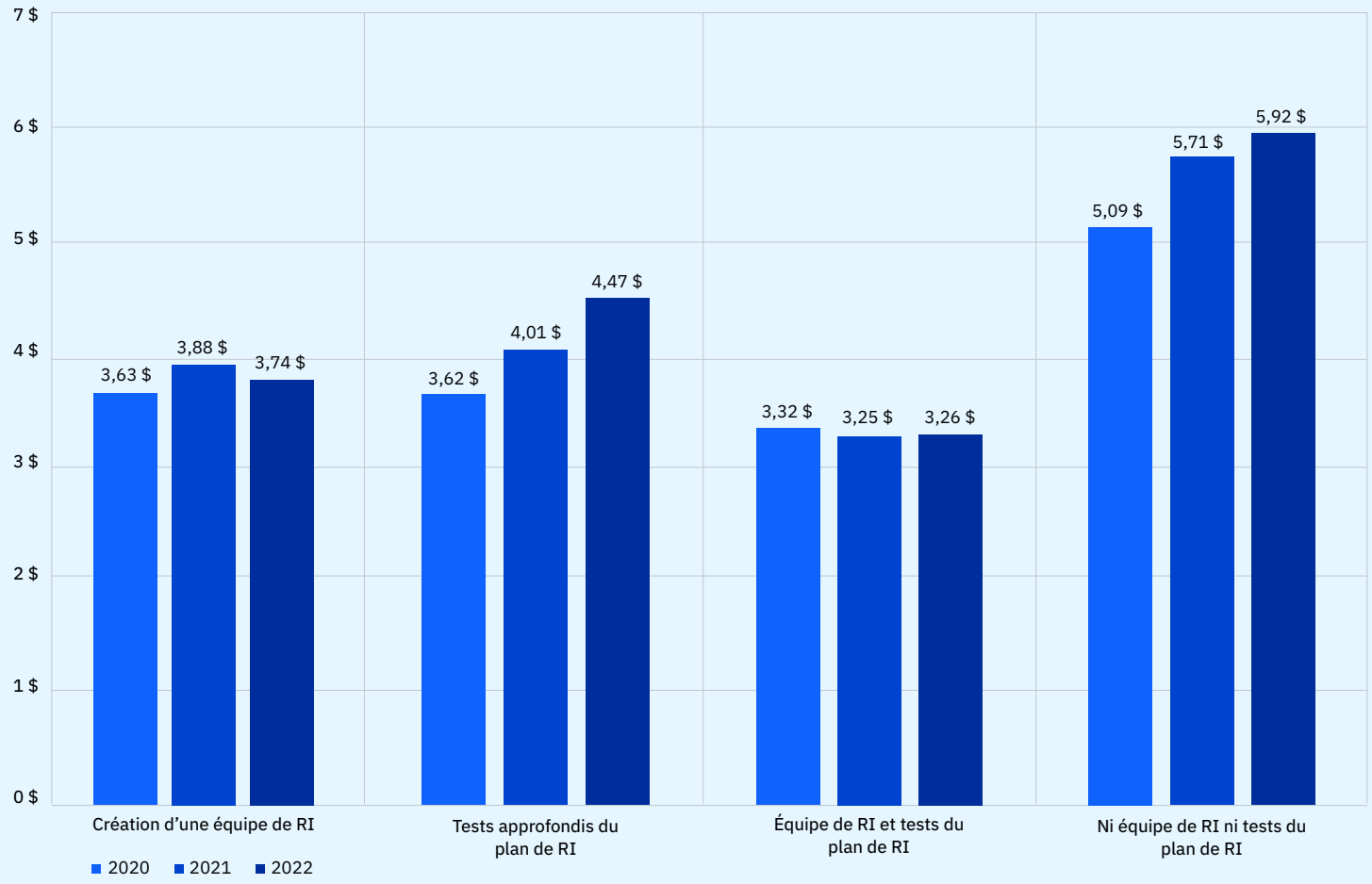


Figure 23 : exprimé en millions USD

Figure 23 : les équipes de RI et les tests approfondis du plan de RI ont continué d'atténuer les coûts des violations de données en 2022.
L'écart entre le coût moyen d'une violation de données dans les entreprises disposant d'une équipe de RI et testant leur plan de RI et le coût moyen dans les autres entreprises a continué de croître entre le rapport 2020 et le rapport 2022. Les violations dans les entreprises dotées de capacités de RI ont entraîné un coût moyen de 3,26 millions USD en 2022, contre 5,92 millions USD dans les entreprises sans dispositif de RI. Cela représentait une différence de 2,66 millions USD, soit 58 %. Ces économies étaient en augmentation par rapport à 2021, lorsque les entreprises dotées de capacités de RI ont économisé 2,46 millions USD, et à 2020, lorsque l'écart de coût se chiffrait à 1,77 million USD. Ce constat indique une efficacité croissante des dispositifs de RI en termes de réduction des coûts.

2,1 millions USD

Économies sur les coûts d'une violation de données dans les entreprises qui utilisent des techniques de quantification des risques vs celles qui n'en utilisent pas

Votre entreprise utilise-t-elle des techniques de quantification des risques pour hiérarchiser les risques, les menaces et les impacts ?

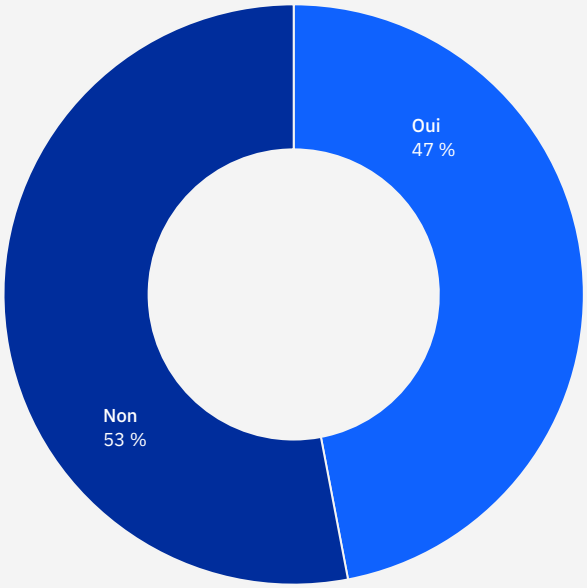


Figure 24

Quantification des risques

La quantification des risques examine les impacts, notamment l'impact financier, et la disponibilité et l'intégrité des données. La quantification des risques peut mettre en évidence les types de pertes financières par impact, notamment : la perte de productivité ; le coût de la réponse ou de la reprise ; l'impact sur la réputation ; et les amendes et les jugements.

Les responsables de la sécurité des systèmes d'information (RSSI), les responsables de la gestion des risques et les équipes de sécurité peuvent utiliser les études comparatives, telles que le Rapport sur le coût d'une violation de données, pour déduire les tendances générales et les moyennes de coûts dans leur secteur ou leur zone géographique. Cependant, l'utilisation de données propres à l'entreprise, plutôt que des moyennes sectorielles, peut mettre en lumière les lacunes de sécurité potentielles et montrer comment réduire le risque global en quantifiant le risque de sécurité en termes financiers.

Cette section porte sur les entreprises qui utilisent des techniques de quantification des risques pour hiérarchiser les risques, les menaces et les impacts, et examine l'impact des techniques de quantification des risques sur le coût moyen.

Figure 24 : moins de la moitié des entreprises interrogées, soit 47 %, ont déclaré qu'elles utilisaient des techniques de quantification des risques pour hiérarchiser les risques, les menaces et les impacts.
En parallèle, sur les 550 entreprises étudiées, 53 % n'utilisent pas de technique de quantification des risques pour hiérarchiser les risques, les menaces et les impacts.

Figure 25 : la quantification des risques a eu un effet considérable sur les coûts des violations de données, permettant d'économiser jusqu'à 2,1 millions USD en moyenne.
Dans les entreprises ayant utilisé des techniques de quantification des risques pour hiérarchiser les risques, les menaces et les impacts, le coût moyen d'une violation était de 3,3 millions USD. Cela représente une économie de 2,1 millions USD (48,3 %) par rapport au coût moyen de 5,4 millions USD dans les entreprises n'utilisant pas de telles techniques. La quantification des risques était associée à des coûts de violation inférieurs de plus de 1 million USD à la moyenne mondiale de 4,35 millions USD.

Impact des techniques de quantification des risques sur le coût moyen d'une violation de données

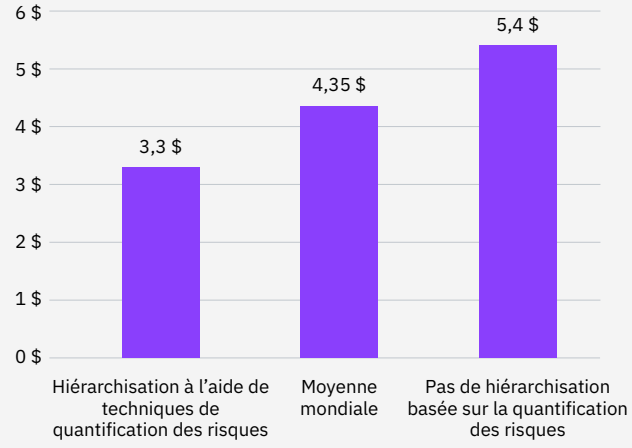


Figure 25 : exprimé en millions USD

1,51 million USD

Économies moyennes sur les coûts d'une violation associées à un déploiement Zero Trust mature vs un déploiement non mature

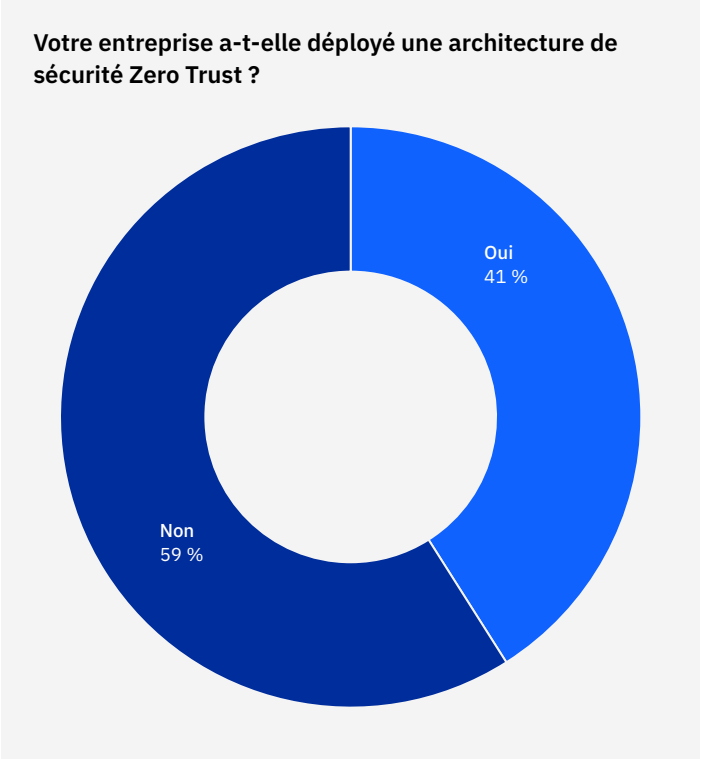


Figure 26

Zero Trust

Cette année, l'étude a examiné pour la deuxième fois la prévalence et l'impact financier des violations de données en cas de déploiement d'un cadre de sécurité Zero Trust. L'approche Zero Trust repose sur l'hypothèse que les identités des utilisateurs ou le réseau lui-même peuvent déjà être compromis, et s'appuie plutôt sur l'IA et l'analyse pour valider en permanence les connexions entre les utilisateurs, les données et les ressources. Comme le montrent les données figurant dans cette section, le Zero Trust a un impact positif net sur les coûts des violations de données.

Figure 26 : dans l'étude de 2022, 41 % des entreprises ont déclaré avoir déployé une architecture de sécurité Zero Trust, contre 59 % ayant déclaré ne pas l'avoir fait.
Dans le rapport de 2021, 35 % déclaraient avoir partiellement ou entièrement déployé une architecture Zero Trust.

Figure 27 : les entreprises ayant déployé une architecture Zero Trust ont économisé près de 1 million USD en coûts moyens de violation par rapport aux autres.
Dans les entreprises ayant déployé une architecture Zero Trust, le coût moyen d'une violation de données était de 4,15 millions USD, contre 5,1 millions USD dans les entreprises ne l'ayant pas fait. Cela représente une différence de 0,95 million USD, et une économie de 20,5 % pour les entreprises ayant déployé une architecture Zero Trust.

Figure 28 : un déploiement Zero Trust mature était associé à des coûts de violation plus de 1,5 million USD inférieurs aux coûts dans les entreprises venant de l'adopter.
Dans les entreprises où le déploiement du Zero Trust était arrivé à maturité, et où il était appliqué de manière systématique dans tous les domaines, le coût moyen d'une violation de données était de 3,45 millions USD. À mi-parcours, lorsque le Zero Trust était appliqué dans de nombreux domaines, le coût moyen d'une violation de données était de 3,96 millions USD. Au début du parcours d'adoption, dans les entreprises qui commençaient à mettre en œuvre quelques pratiques, le coût moyen d'une violation de données était de 4,96 millions USD. Ce coût était supérieur de 1,51 million USD à celui des violations dans les entreprises avec un déploiement mature, soit une différence de 35,9 %.

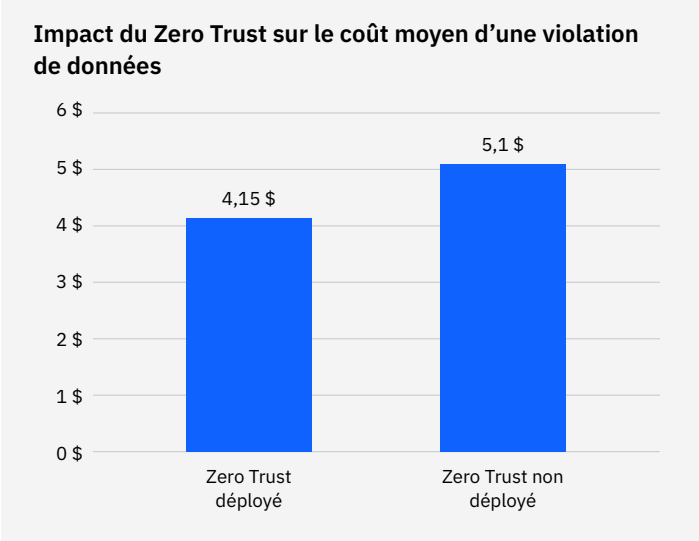


Figure 27 : exprimé en millions USD

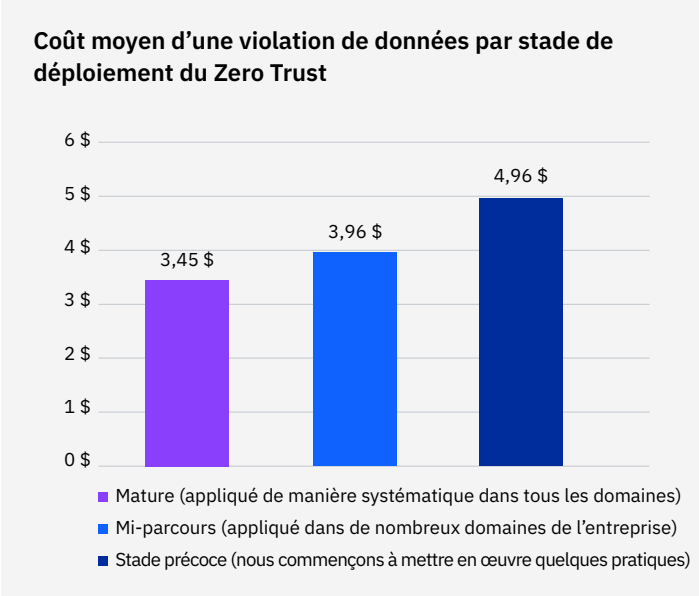


Figure 28 : exprimé en millions USD

49 jours

Il a fallu 49 jours de plus que la moyenne pour identifier et neutraliser les attaques par ransomware.

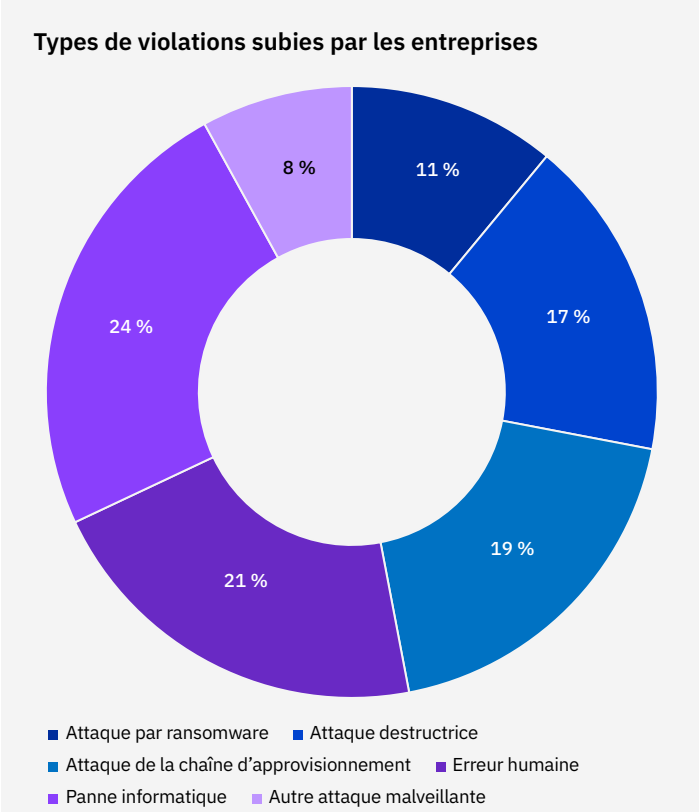


Figure 29

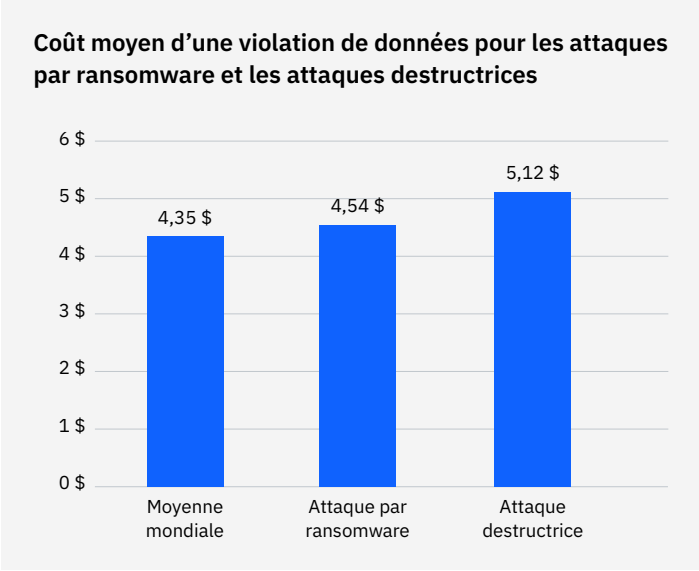


Figure 30 : exprimé en millions USD

Ransomwares et attaques destructrices

Cette année, nous avons examiné pour la deuxième fois les coûts associés aux ransomwares. Nous avons également ajouté les violations liées aux logiciels malveillants. Par rapport à l'année dernière, les coûts des attaques par ransomware ont légèrement diminué, passant de 4,62 à 4,54 millions USD. Cependant, la fréquence des attaques par ransomware a augmenté. Elles représentaient 7,8 % des violations dans l'étude de 2021 et 11 % dans l'étude de 2022.

Cette année, nous avons examiné le cycle de vie de ces violations, ainsi que l'impact du paiement d'une rançon sur le coût hors rançon d'une violation. Remarque : cette étude n'inclut pas le coût de la rançon elle-même dans le calcul du coût d'une attaque par ransomware.

Figure 29 : les ransomwares étaient responsables de 11 % des violations, et les attaques destructrices de 17 % d'entre elles. Dix-neuf pour cent des violations ont été causées par des attaques de la chaîne d'approvisionnement en raison d'un partenaire commercial compromis. Vingt-et-un pour cent des violations étaient dues à des erreurs humaines, à savoir des actions négligentes involontaires d'employés ou de sous-traitants.

Les pannes informatiques, causées par une perturbation ou une défaillance des systèmes informatiques ayant entraîné une perte de données, étaient responsables de 24 % des violations. Elles comprenaient les erreurs dans le code source ou un processus défaillant, tel qu'une erreur de communication automatisée. Les 8 % restants étaient dus à d'autres types d'attaques malveillantes.

Figure 30 : le coût moyen d'une attaque par ransomware – sans compter le coût de la rançon elle-même – était de 4,54 millions USD, légèrement supérieur au coût total moyen global d'une violation de données, à savoir 4,35 millions USD. Le coût moyen d'une attaque destructrice ou de type wiper (effaceur) était de 5,12 millions USD, soit 0,77 million USD de plus que la moyenne globale, ou une différence de 16,3 %.

Figure 31 : le délai moyen d'identification et de neutralisation d'une attaque par ransomware ou d'une attaque destructrice était nettement supérieur à la moyenne.
Il fallait 237 jours pour identifier une attaque par ransomware et 89 jours pour la neutraliser, soit un cycle de vie total de 326 jours. Il fallait 233 jours pour identifier une attaque destructrice et 91 jours pour la neutraliser, soit un cycle de vie total de 324 jours. Par rapport au cycle de vie moyen global de 277 jours, les entreprises ont mis 49 jours de plus pour identifier et neutraliser une attaque par ransomware, soit une différence de 16,3 %. En outre, les entreprises ont mis 47 jours de plus pour identifier et neutraliser une attaque destructrice, soit une différence de 15,6 %.

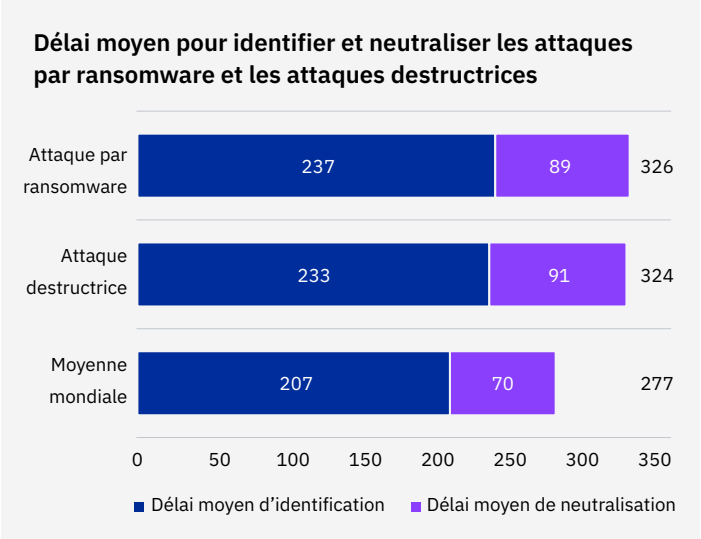


Figure 31 : exprimé en jours

Figure 32 : le coût moyen d'une attaque par ransomware était plus élevé pour les entreprises qui n'ont pas payé la rançon.
Le coût de la rançon n'a pas été inclus dans le calcul du coût d'une attaque par ransomware. Le coût d'une attaque par ransomware était basé sur les activités, telles que la détection de l'attaque, et sur les pertes d'affaires dues aux temps d'arrêt du système. Pour les entreprises n'ayant pas payé la rançon, le coût moyen de l'attaque était de 5,12 millions USD. Pour celles l'ayant payée, il était de 4,49 millions USD. Cela représente une différence de 0,63 million USD, soit 13,1 %.

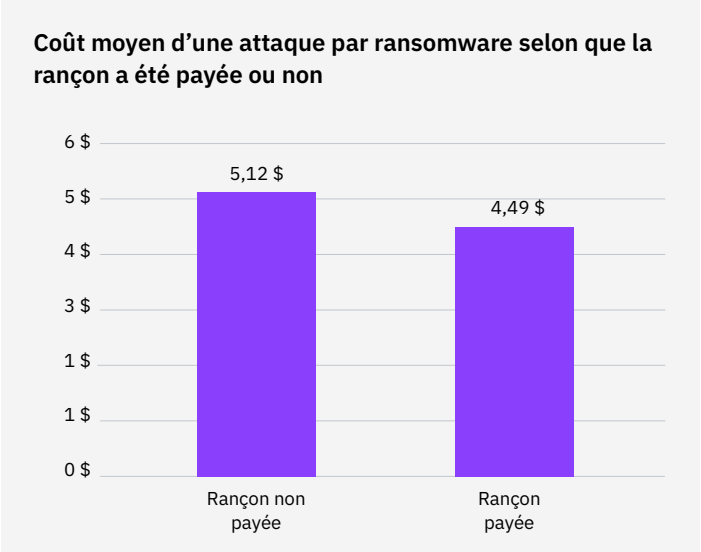


Figure 32 : exprimé en millions USD. Le coût de la rançon n'est pas inclus dans ce calcul.

26 jours

Comparé à la moyenne mondiale, il a fallu 26 jours de plus en moyenne pour identifier et neutraliser une violation de la chaîne d'approvisionnement

Votre entreprise a-t-elle été victime d'une violation en raison d'une compromission de la chaîne d'approvisionnement ?

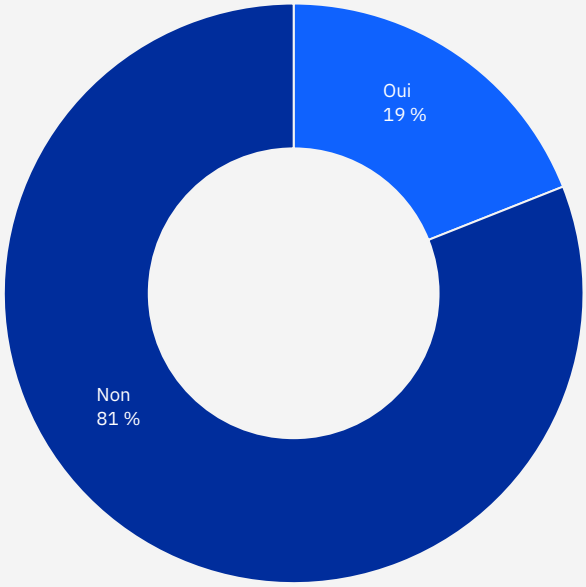


Figure 33

Coût moyen d'une violation de données par compromission de la chaîne d'approvisionnement

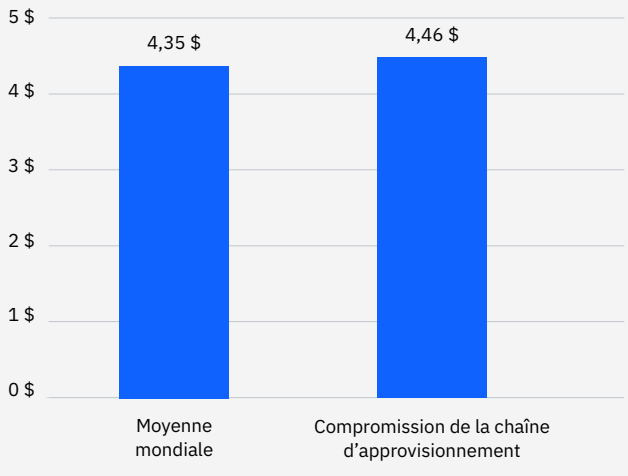


Figure 34 : exprimé en millions USD

Attaques de la chaîne d'approvisionnement

Les chaînes d'approvisionnement ayant été victimes ces dernières années de plusieurs attaques importantes, nous avons examiné pour la première fois dans ce rapport les violations de données dans le contexte des attaques de chaîne d'approvisionnement. Une compromission de chaîne d'approvisionnement est une violation qui résulte d'un partenaire commercial compromis, tel qu'un fournisseur. Comme le révèle l'étude, près d'un cinquième des violations ont été causées par une compromission de la chaîne d'approvisionnement, et ces compromissions ont amplifié les coûts et les cycles de vie des violations.

Figure 33 : environ un cinquième des violations étudiées résultaient d'une compromission de la chaîne d'approvisionnement.
19 % des entreprises ont répondu « Oui », affirmant qu'elles avaient subi une violation suite à une compromission de la chaîne d'approvisionnement, contre 81 % ayant répondu « Non ».

Figure 34 : le coût total moyen d'une compromission de la chaîne d'approvisionnement était de 4,46 millions USD.
Ce coût était supérieur au coût moyen global d'une violation de données (4,35 millions USD), soit une différence de 0,11 million USD ou 2,5 %.

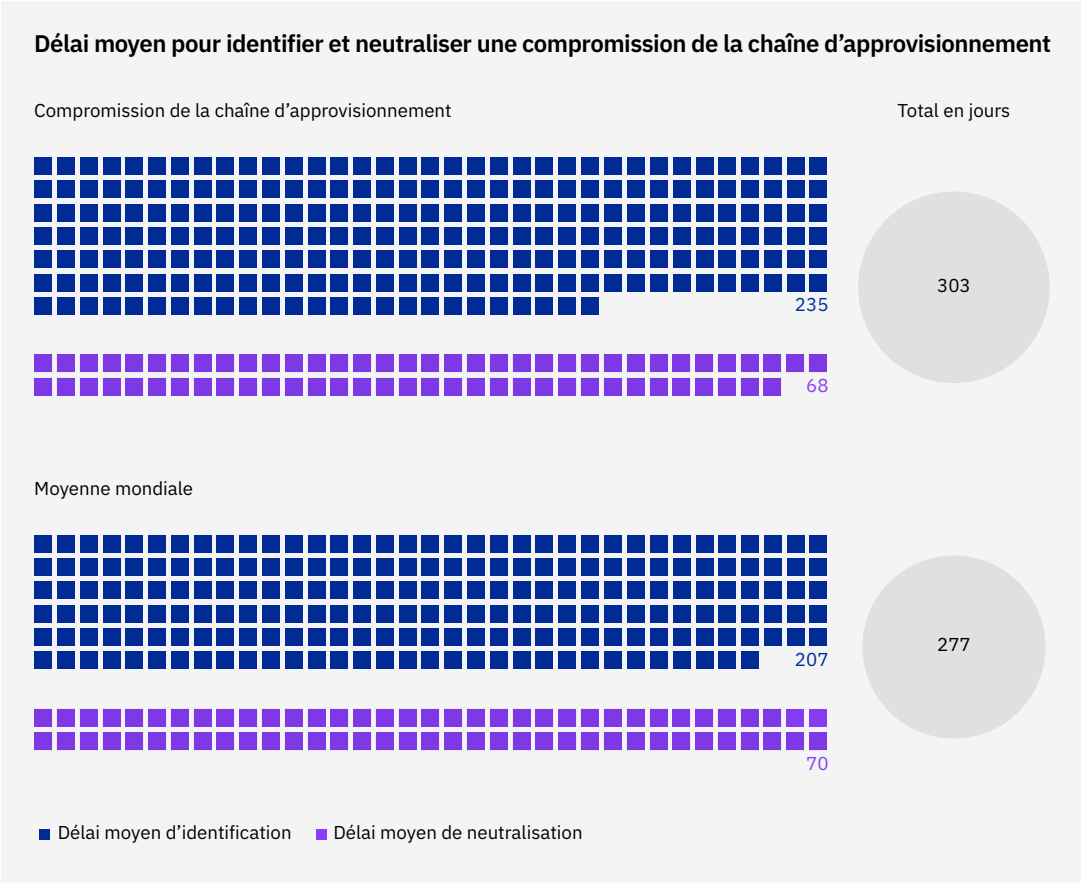


Figure 35 : exprimé en jours

Figure 35 : le cycle de vie d'une compromission de la chaîne d'approvisionnement était plus long que la moyenne mondiale. En moyenne, il a fallu aux entreprises 235 jours pour identifier une compromission de la chaîne d'approvisionnement et 68 jours pour la neutraliser, soit un cycle de vie total de 303 jours. Le cycle de vie moyen était 26 jours plus long que le cycle de vie moyen global de 277 jours, soit une différence de 9 %.

79 %

Pourcentage des secteurs d’infrastructures critiques n’ayant pas adopté une approche de sécurité Zero Trust

Infrastructures critiques

Pour la première fois dans ce rapport, nous avons étudié le coût et la neutralisation des violations de données dans les secteurs d’infrastructures critiques. Sur la base de la classification de la Cybersecurity and Infrastructure Security Agency (CISA) des États-Unis, les secteurs d’infrastructures critiques pris en compte dans cette étude comprenaient les services financiers, l’industrie, la technologie, l’énergie, les transports, les communications, les soins de santé, l’éducation et le secteur public.

Cette étude a révélé en particulier que dans les secteurs d’infrastructures critiques, les approches de sécurité Zero Trust étaient nettement moins présentes que dans la moyenne mondiale. Les coûts de violation de données étaient nettement plus élevés que la moyenne dans les secteurs d’infrastructures critiques ne disposant pas de stratégie de sécurité Zero Trust.

Figure 36 : les attaques par ransomware et les attaques destructrices ont été responsables de plus d’un quart des violations dans les secteurs d’infrastructures critiques.
Les attaques par ransomware représentaient 12 % des violations d’infrastructures critiques, tandis que les attaques destructrices étaient à l’origine de 16 % des violations, ce qui représente un total de 28 %. Les attaques de la chaîne d’approvisionnement, où un partenaire commercial tiers était le vecteur d’attaque, représentaient 17 % des violations dans ces secteurs. Dans le même temps, les violations causées par des erreurs humaines ou des pannes informatiques représentaient respectivement 22 % et 25 % des violations. Les 8 % restants étaient dus à d’autres types d’attaques malveillantes.

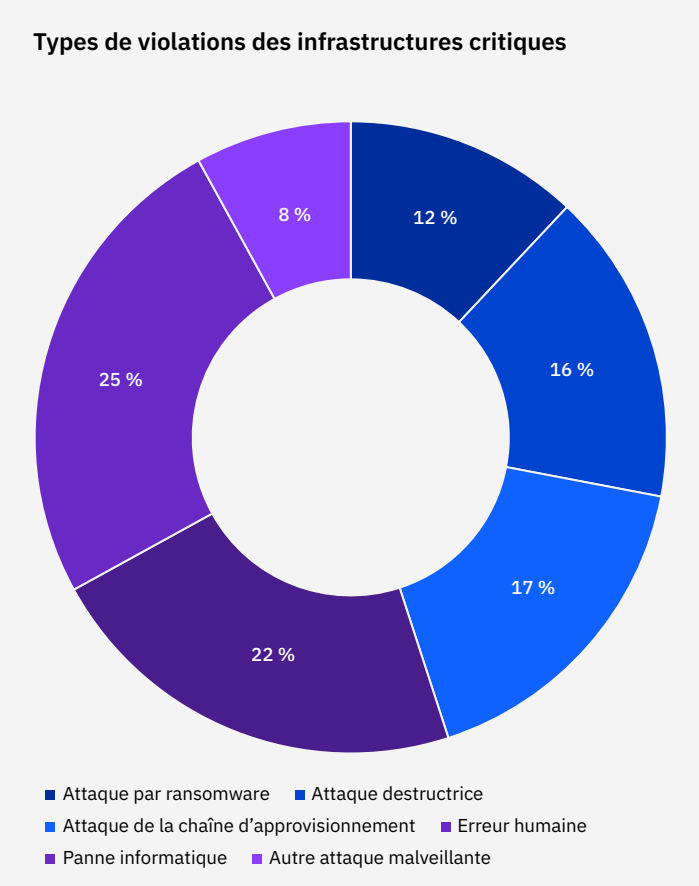


Figure 36

Figure 37 : le coût moyen d'une violation de données dans les entreprises d'infrastructures critiques était de 4,82 millions USD.
Dans les entreprises d'infrastructures critiques, le coût moyen d'une violation de données dépassait de 0,99 million USD les 3,83 millions USD relevé dans les entreprises des secteurs d'infrastructure non critiques, soit une différence de 22,9 %. Les secteurs d'infrastructure non critiques comprenaient les entreprises des secteurs des produits pharmaceutiques, des services, du divertissement, des biens de consommation, des médias, de l'hôtellerie, de la vente au détail et de la recherche.

Figure 38 : les secteurs d'infrastructures critiques ont identifié et neutralisé les violations de données plus rapidement que les autres secteurs.
Dans les secteurs d'infrastructures critiques, le cycle de vie d'une violation de données était inférieur à la moyenne mondiale et au cycle de vie dans les secteurs d'infrastructures non critiques. Le délai moyen d'identification était de 204 jours, contre 211 jours dans les autres secteurs. Le délai moyen de neutralisation était de 69 jours, contre 71 jours dans les autres secteurs. La moyenne combinée de 273 jours pour identifier et neutraliser une violation dans les entreprises d'infrastructures critiques était inférieure de quatre jours à la moyenne mondiale de 277 jours. De plus, la moyenne combinée pour les secteurs d'infrastructures critiques était inférieure de neuf jours à la moyenne de 282 jours pour les autres secteurs.

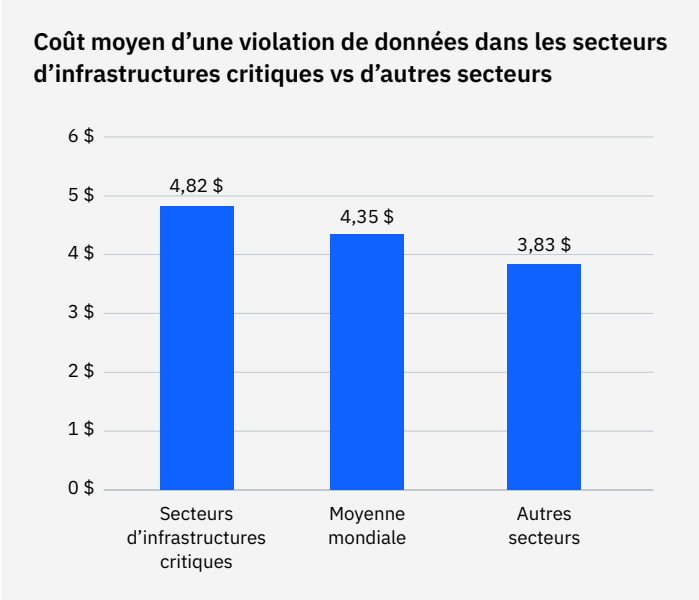


Figure 37 : exprimé en millions USD

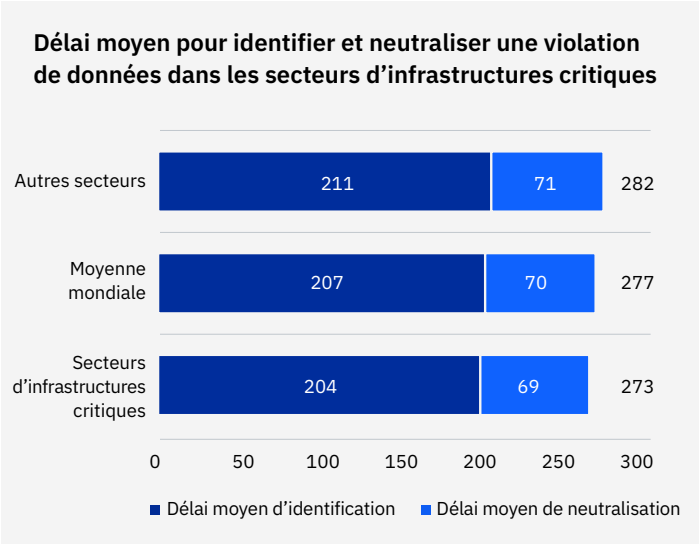


Figure 38 : exprimé en jours

Figure 39 : seulement un cinquième des entreprises d'infrastructures critiques avaient déployé une approche de sécurité Zero Trust, soit deux fois moins que la moyenne mondiale.
Vingt-et-un pour cent des entreprises d'infrastructures critiques avaient déployé une approche Zero Trust, contre 79 % ne l'ayant pas fait. À titre de comparaison, en moyenne, 41 % des entreprises dans le monde ont adopté une stratégie Zero Trust.

Figure 40 : dans les entreprises d'infrastructures critiques ayant mis en œuvre une approche de sécurité Zero Trust, le coût moyen d'une violation de données était de 4,23 millions USD.
Dans celles ne l'ayant pas fait, le coût moyen s'élevait à 5,4 millions USD. Cela équivaut à une différence de 1,17 million USD, soit 24,3 % de plus que dans les entreprises ayant mis en œuvre une stratégie Zero Trust.

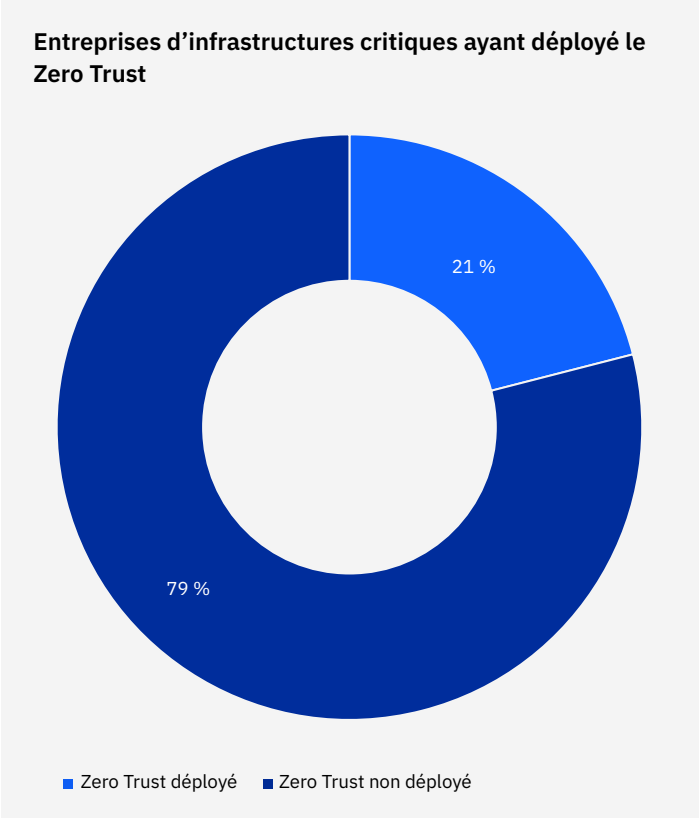


Figure 39

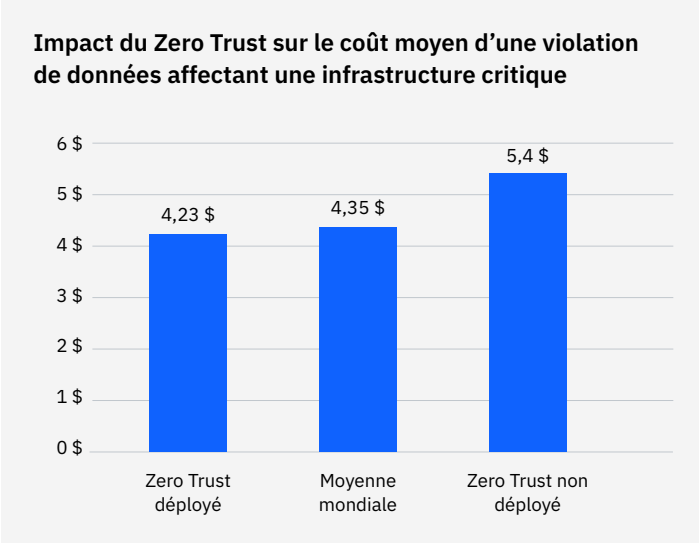


Figure 40 : exprimé en millions USD

43 %

Pourcentage des entreprises qui n'avaient pas commencé ou qui commençaient seulement d'appliquer des pratiques de sécurité pour protéger leurs environnements cloud

Violations dans le cloud et modèle de cloud

Cette année, nous avons examiné pour la deuxième fois l'impact du modèle de cloud et de la maturité de la sécurité cloud sur le coût d'une violation de données. L'étude a révélé que 45 % des violations se sont produites dans le cloud, mais que celles survenues dans un cloud public coûtent beaucoup plus cher que celles survenues dans un cloud hybride. Cependant, notre analyse montre que les entreprises ont besoin d'une posture de sécurité cloud mature, quel que soit le modèle de cloud.

Figure 41 : un grand nombre de participants à l'étude avaient un modèle d'exploitation informatique hybride, 45 % indiquant qu'ils avaient un modèle de cloud hybride.
Dans le même temps, 28 % ont déclaré que leur modèle informatique était entièrement sur site et 27 % que leur modèle informatique était entièrement basé sur le cloud.

Figure 42 : près de la moitié des entreprises ont subi une violation de données dans le cloud.
Quarante-cinq pour cent ont déclaré que la violation de données s'était produite dans le cloud, contre 55 % affirmant qu'elle ne s'était pas produite dans le cloud.

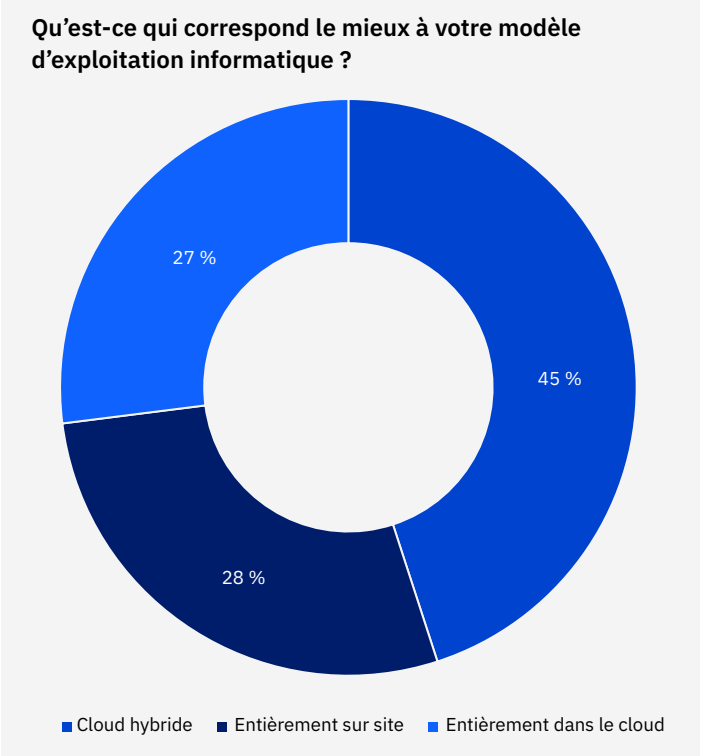


Figure 41

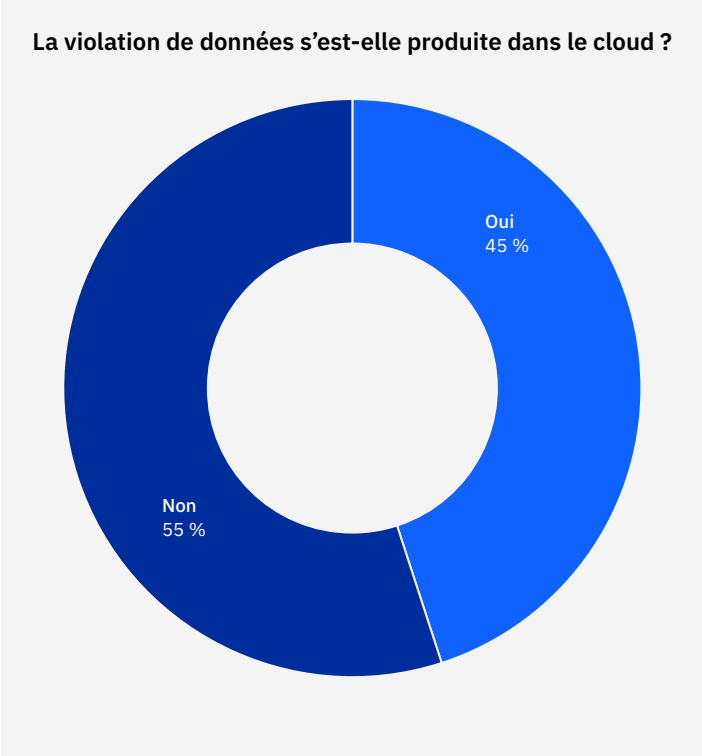


Figure 42

État de maturité de la sécurité dans l'environnement cloud

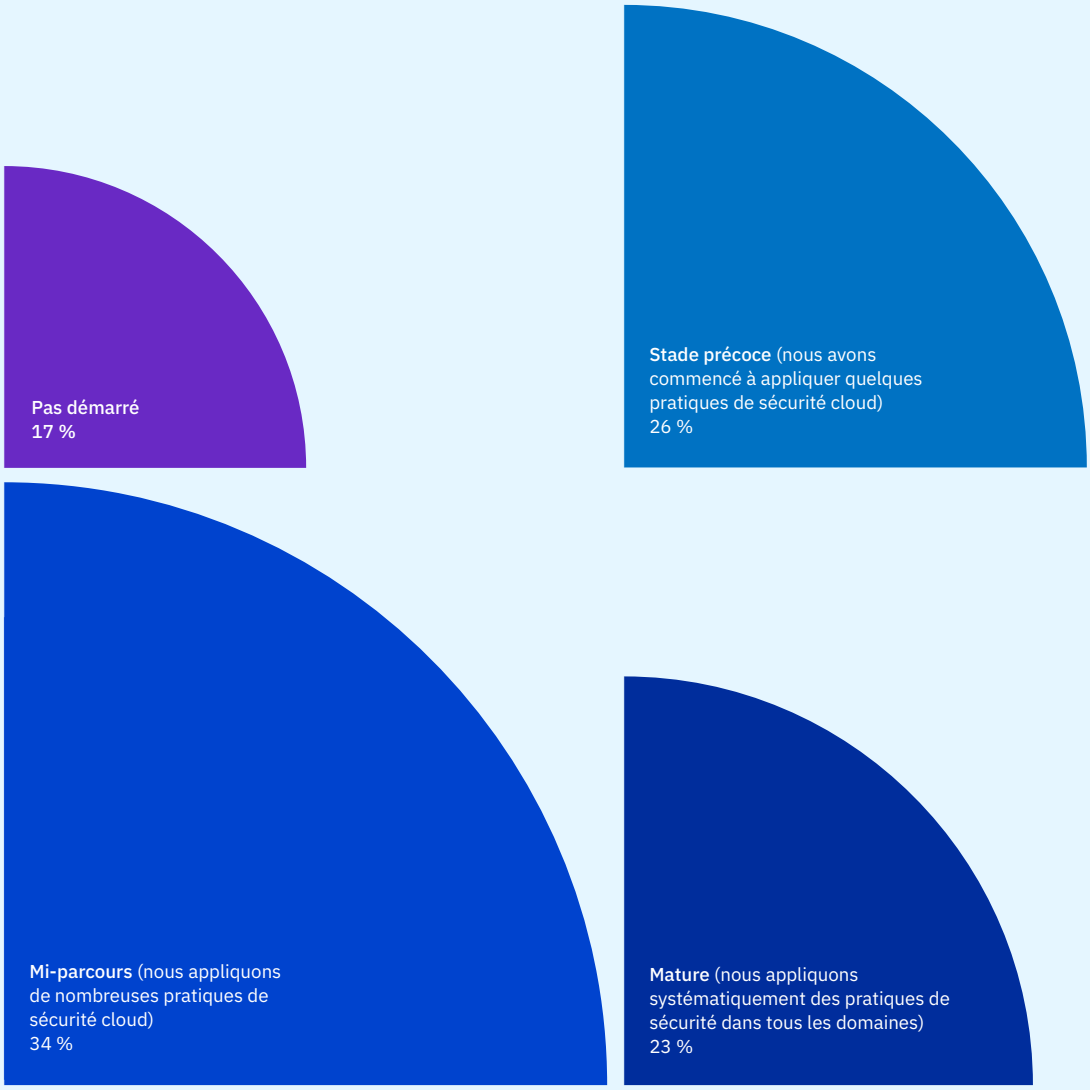


Figure 43

Figure 43 : près de la moitié (43 %) des entreprises n'avaient pas commencé ou commençaient seulement à mettre en œuvre des mesures pour sécuriser leurs environnements cloud. Dans le même temps, 34 % étaient à mi-parcours et appliquaient de nombreuses pratiques de sécurité cloud, et 23 % avaient atteint le stade de la maturité et appliquaient des pratiques de sécurité de manière systématique dans tous les domaines. Vingt-six pour cent des entreprises ont déclaré qu'elles en étaient à un stade précoce, ce qui signifie qu'elles avaient commencé à appliquer quelques pratiques de sécurité cloud. Enfin, 17 % des entreprises ont déclaré qu'elles n'avaient pas entamé leur parcours de sécurisation du cloud.

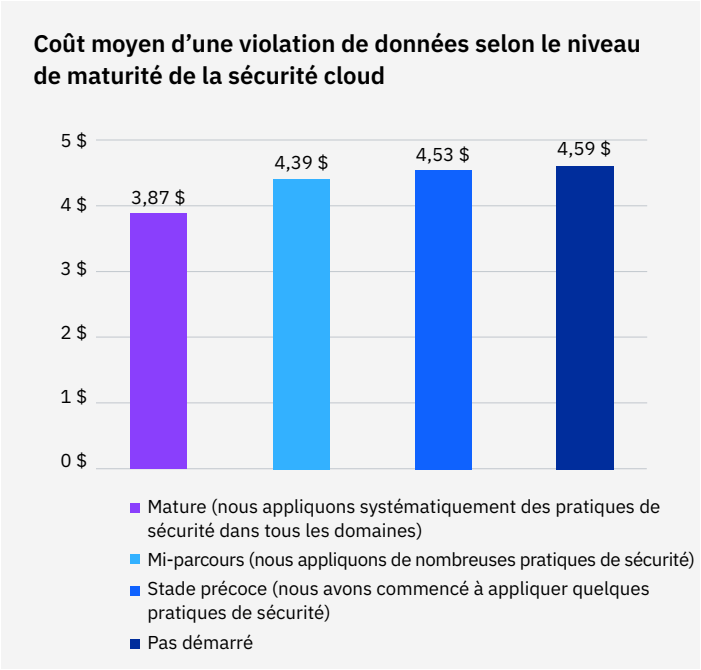


Figure 44 : exprimé en millions USD

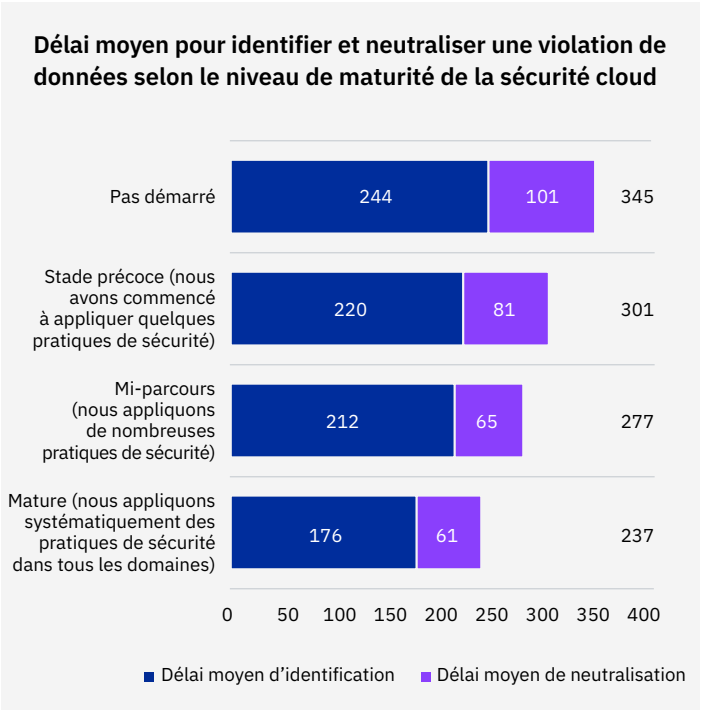


Figure 45 : exprimé en jours

Figure 44 : dans les entreprises dotées d'une sécurité cloud mature, le coût d'une violation de données était inférieur à la moyenne.
Il était en moyenne inférieur de 0,66 million USD au coût dans les entreprises aux premiers stades de la sécurisation de leurs environnements cloud. Les violations dans les entreprises ayant une sécurité cloud mature coûtent en moyenne 3,87 millions USD, contre 4,39 millions USD dans les entreprises à mi-parcours, 4,53 millions USD dans les entreprises à un stade précoce et 4,59 millions USD dans les entreprises n'ayant pas encore entamé leurs parcours. L'écart de coût entre le stade mature et le stade précoce représentait une économie de 15,7 % pour les entreprises ayant une sécurité cloud mature. Remarque : les coûts des violations dans cette étude comprennent tout type de violation, pas seulement les violations survenues dans le cloud.

Figure 45 : les entreprises au stade mature de sécurisation de leurs environnements cloud ont pu identifier et neutraliser les violations de données beaucoup plus rapidement que les entreprises à un stade précoce.
En moyenne, il a fallu aux entreprises au stade mature 176 jours pour identifier et 61 jours pour neutraliser une violation, soit 237 jours au total. Ce cycle de vie était inférieur de 40 jours à la moyenne mondiale de 277 jours et de 64 jours au cycle de vie dans les entreprises au stade précoce, soit plus de deux mois, ou une différence de 23,8 %. Les entreprises qui n'avaient pas entamé leur parcours de sécurisation du cloud ont mis beaucoup plus de temps à identifier et à neutraliser les violations. La moyenne pour ces entreprises était de 345 jours, soit plus de 100 jours de plus que les entreprises au stade mature. Pour les entreprises à mi-parcours, le délai moyen pour identifier et neutraliser une violation de données était de 277 jours, soit le même temps que la moyenne mondiale.

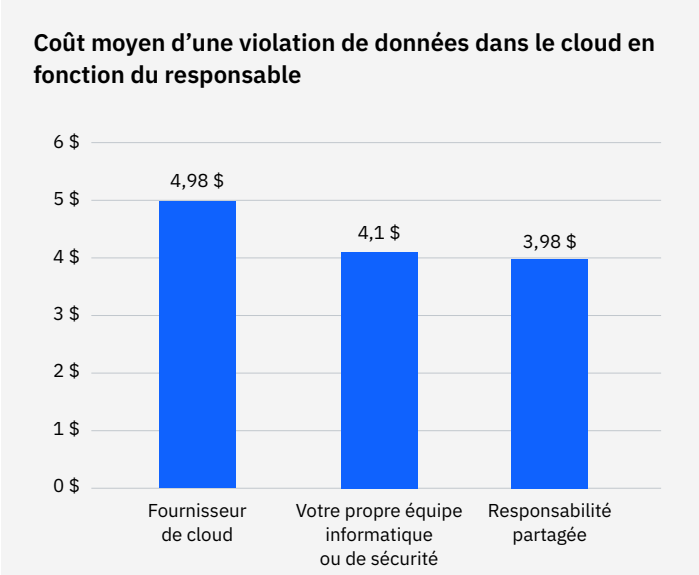


Figure 46 : exprimé en millions USD

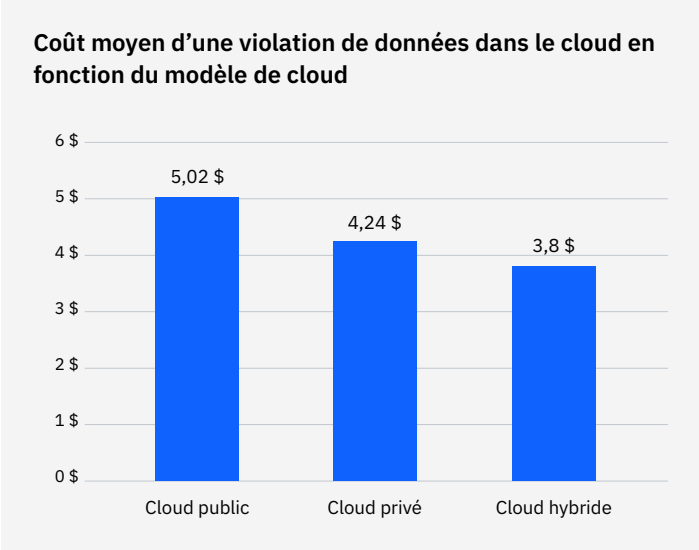


Figure 47 : exprimé en millions USD

Figure 46 : les violations relevant de la responsabilité du fournisseur cloud s'accompagnaient du coût total moyen le plus élevé.
Le coût total moyen des violations qui relevaient de la responsabilité du fournisseur cloud était de 4,98 millions USD. Les violations relevant de la responsabilité de l'équipe informatique ou de sécurité de l'entreprise ont coûté en moyenne 4,1 millions USD. Les violations qui relevaient de la responsabilité partagée du fournisseur cloud et de l'équipe informatique ou de sécurité de l'entreprise ont coûté en moyenne 3,98 millions USD. Ce coût moyen est inférieur de 1 million USD à celui des violations imputables au fournisseur cloud, soit une différence de 22,3 %.

Figure 47 : les violations dans le cloud public étaient les plus coûteuses.
Les violations dans un cloud public coûtent en moyenne 5,02 millions USD, tandis que les violations dans un cloud privé coûtent en moyenne 4,24 millions USD. Dans un cloud hybride, les violations coûtent en moyenne 3,8 millions USD, soit environ 1,2 million USD de moins que les violations dans un cloud public, pour une différence de 27,7 %.

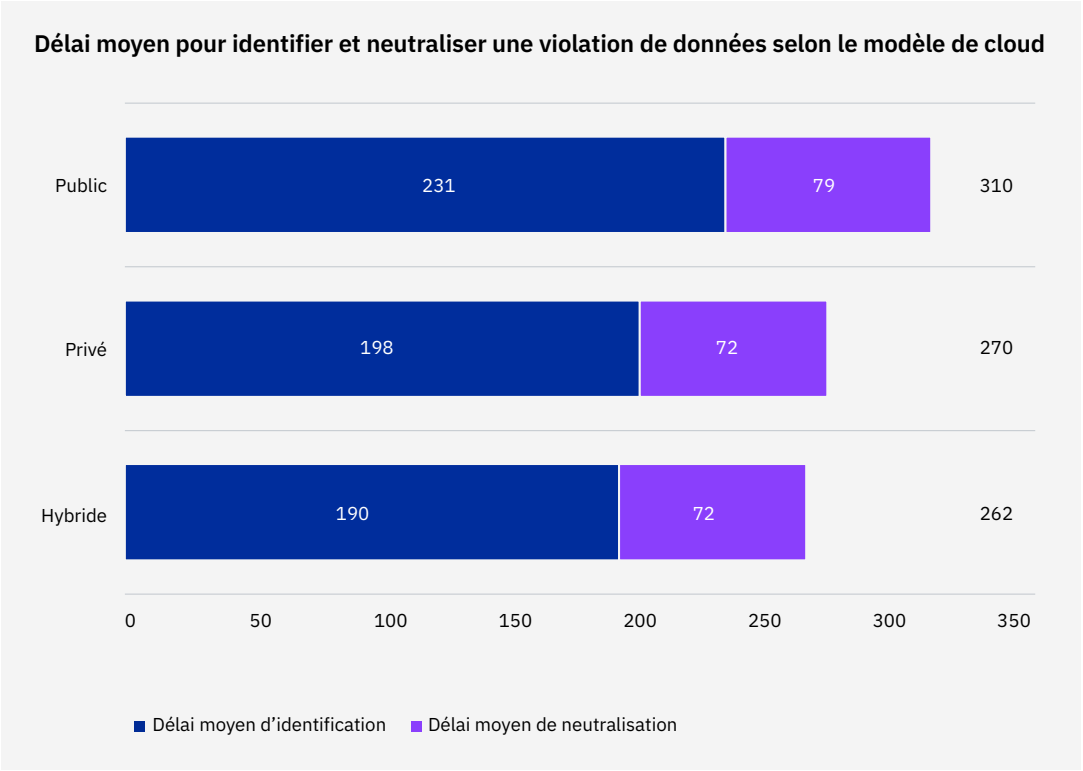


Figure 48 : exprimé en jours

Figure 48 : en moyenne, les entreprises ayant adopté un modèle de cloud hybride ont pu identifier et neutraliser une violation beaucoup plus rapidement que celles ayant adopté les modèles de cloud public ou privé.
Le délai moyen pour identifier et neutraliser une violation avec un modèle de cloud hybride était de 262 jours. Ce cycle de vie était inférieur de 15 jours à la moyenne mondiale de 277 jours et de 8 jours au cycle pour le cloud privé. Dans les entreprises ayant adopté un modèle de cloud public, il a fallu en moyenne 310 jours pour identifier et neutraliser une violation. Ce cycle de vie était 48 jours plus long que pour le cloud hybride, soit une différence de 16,8 %. Remarque : compte tenu de la variété de mise en œuvre du cloud hybride, cette analyse intègre les violations survenues dans le cloud, mais également les violations sur site.

1 million USD

Lorsque le télétravail était un facteur à l'origine d'une violation, le coût de celle-ci était supérieur d'environ 1 million USD par rapport aux violations où le télétravail n'était pas un facteur.

Coût moyen d'une violation de données en fonction de la part des employés travaillant à distance

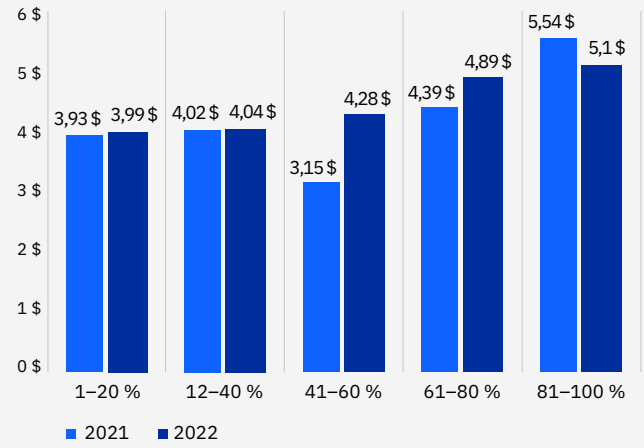


Figure 49 : exprimé en millions USD

Coût moyen d'une violation de données lorsque le télétravail était un facteur à l'origine de la violation

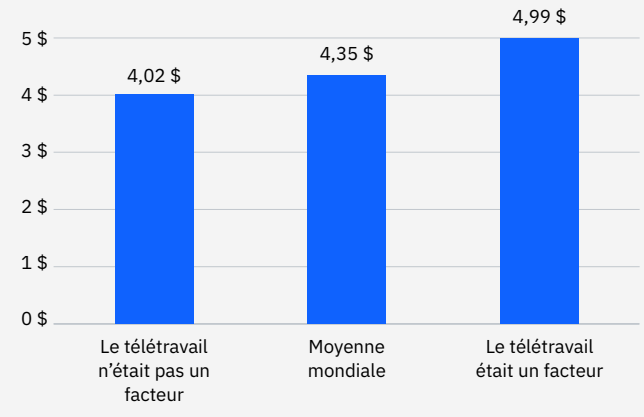


Figure 50 : exprimé en millions USD

Télétravail

C'est la troisième fois que ce rapport est publié depuis le début de la pandémie de COVID-19. Dans le contexte de la pandémie, nous avons examiné pour la première fois l'an dernier les répercussions du télétravail sur les coûts des violations de données. Le télétravail a eu des effets considérables sur le coût d'une violation lorsqu'il était un facteur à l'origine de la violation, par exemple un télétravailleur dont les identifiants auraient été volés. L'étude a également révélé que les coûts des violations étaient les plus élevés pour les entreprises dont la plupart des employés étaient en télétravail.

Figure 49 : il existait une forte corrélation entre le télétravail et le coût d'une violation de données et, lorsqu'un plus grand nombre d'employés étaient en télétravail, les coûts des violations de données étaient plus élevés.
Dans les entreprises ayant la plus forte proportion (entre 81 % et 100 %) de télétravailleurs, le coût moyen d'une violation de données était de 5,1 millions USD. Cela représente une légère baisse dans cette catégorie par rapport à l'an dernier. Dans les entreprises ayant la plus faible proportion (moins de 20 %) de télétravailleurs, le coût moyen d'une violation de données était de 3,99 millions USD. La différence entre la proportion la plus forte et la plus faible était de 1,11 million USD, soit une différence de 24,4 %.

Figure 50 : le coût total moyen d'une violation de données était supérieur de près de 1 million USD lorsque le télétravail était un facteur à l'origine de la violation.
Dans les entreprises ayant indiqué que le télétravail était un facteur à l'origine de la violation, le coût moyen d'une violation de données était de 4,99 millions USD. En revanche, le coût moyen d'une violation de données était de 4,02 millions USD lorsque le télétravail n'était pas un facteur à l'origine de la violation, soit une différence de 0,97 million USD ou 21,5 %. Lorsque le télétravail était un facteur, le coût était également de 0,64 million USD supérieur à la moyenne mondiale, soit une différence de 13,7 %.

550 000 USD

Économies moyennes sur les coûts d'une violation de données dans une entreprise dotée d'effectifs suffisants vs une entreprise dont les effectifs sont insuffisants

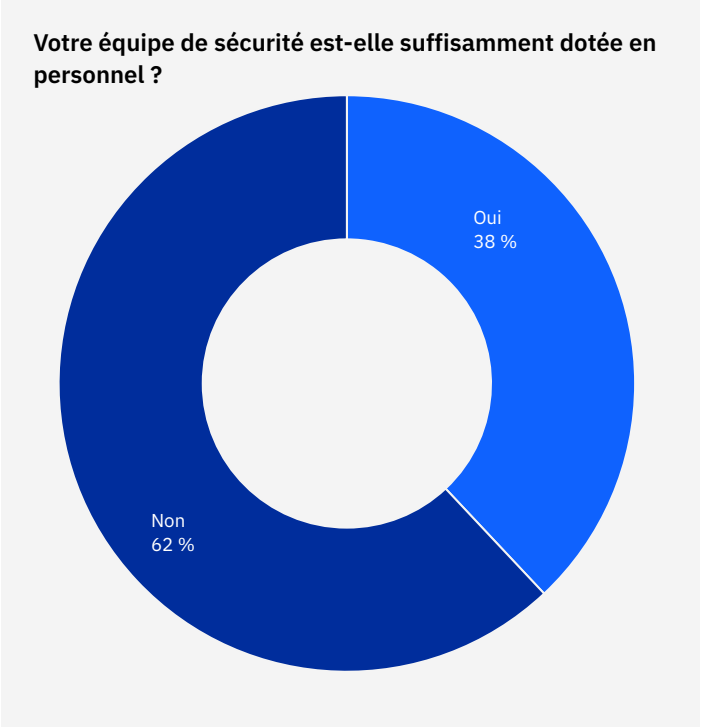


Figure 51

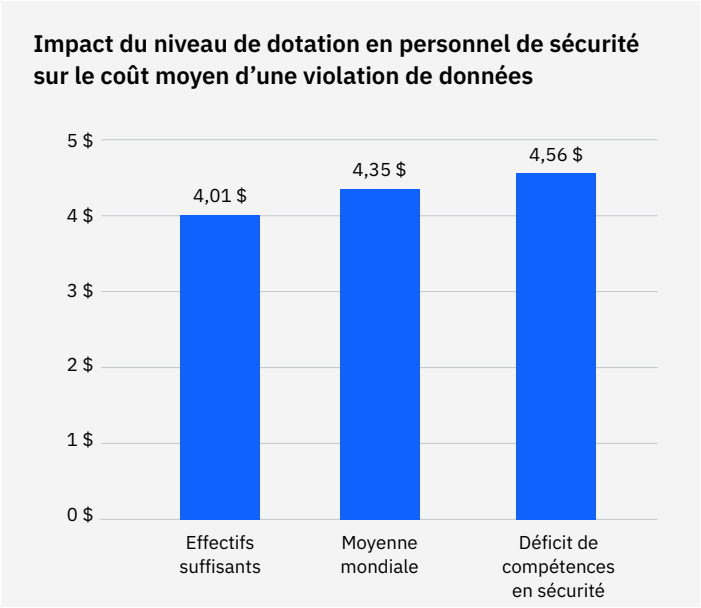


Figure 52 : exprimé en millions USD

Déficit de compétences

De nombreuses entreprises ont eu du mal à pourvoir les postes au sein de leurs équipes de sécurité. Celles ayant déclaré qu'elles disposaient de suffisamment de personnel ont réalisé des économies considérables en termes de coûts de violation de données, par rapport à celles qui affirmaient le contraire. Pour la première fois dans ce rapport, nous avons examiné de plus près le déficit de compétences dans le domaine de la sécurité.

Figure 51 : les entreprises participant à l'étude ont fait état d'un déficit de compétences en sécurité.
Seulement un peu plus d'un tiers des entreprises disposaient d'équipes de sécurité suffisamment dotées en personnel. En effet, seulement 38 % des entreprises ont déclaré que leurs équipes de sécurité étaient suffisamment dotées en personnel pour répondre à leurs besoins en matière de gestion de la sécurité, tandis que 62 % ont déclaré qu'elles n'étaient pas suffisamment dotées en personnel.

Figure 52 : dans les entreprises ayant déclaré que leur équipe de sécurité n'était pas suffisamment dotée en personnel, le coût d'une violation de données était supérieur à la moyenne.
Dans les entreprises dont l'équipe de sécurité était suffisamment dotée en personnel, le coût moyen d'une violation de données était inférieur à la moyenne. Le coût moyen d'une violation de données dans les entreprises suffisamment dotées en personnel était de 4,01 millions USD. En revanche, il était de 4,56 millions USD dans les entreprises dont l'équipe de sécurité n'était pas suffisamment dotée en personnel, soit une différence de 0,55 million USD ou 12,8 %.

387 millions USD

Coût total moyen des violations représentant entre 50 et 60 millions d'enregistrements

Violations massives

Pour la plupart des entreprises, une violation massive (plus de 1 million d'enregistrements compromis) n'est pas une expérience normale. Mais les violations massives ont un impact démesuré sur les consommateurs et les entreprises.

Cette étude comprenait 13 entreprises ayant subi une violation de données impliquant la perte ou le vol de 1 à 60 millions d'enregistrements. La méthodologie utilisée pour étudier les violations massives était différente de celle utilisée pour étudier les 550 autres violations, chacune d'elles ne comptant pas plus de 102 000 dossiers perdus. Pour une explication complète de la méthodologie de l'étude, consultez la rubrique « FAQ sur les violations de données » figurant à la fin de ce rapport.

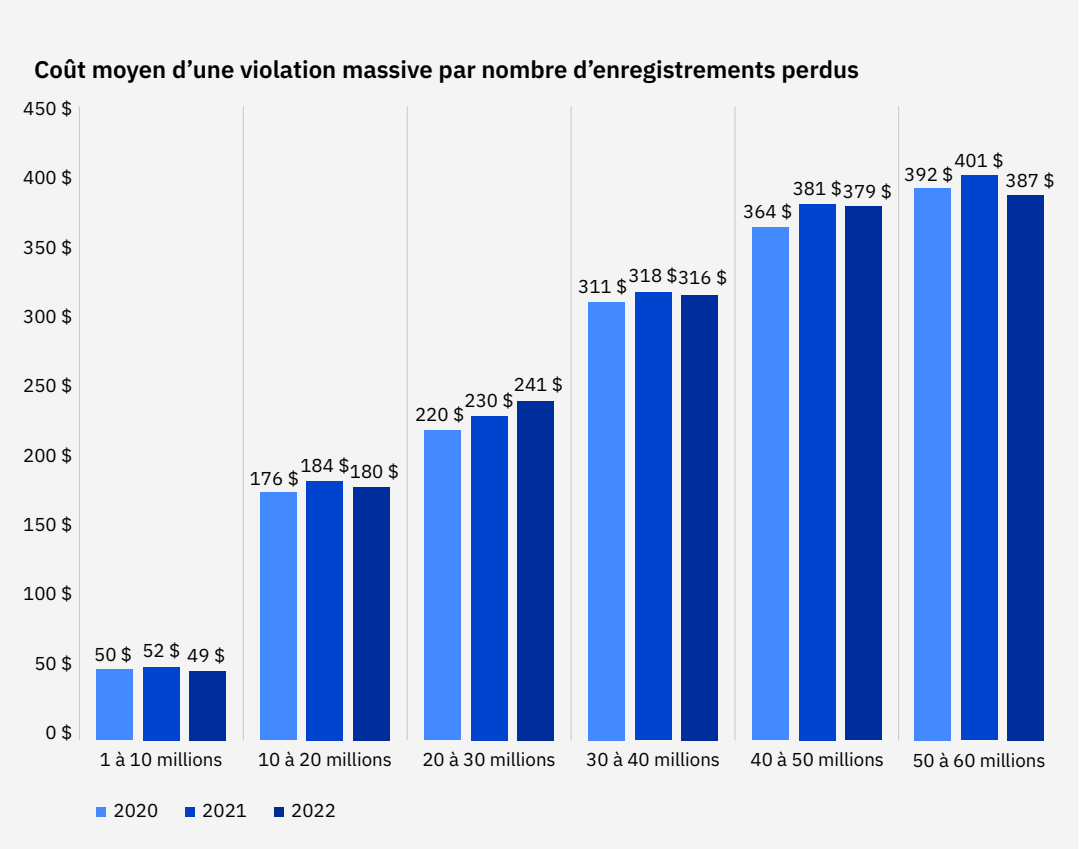


Figure 53 : exprimé en millions USD

Figure 53 : en 2022, le coût moyen d'une violation massive a légèrement diminué.
Par rapport à 2021, les coûts des violations massives ont diminué dans six des sept niveaux de violation. Le coût des violations massives les plus grandes, à savoir celles qui touchent entre 50 et 60 millions d'enregistrements, est passé de 401 millions USD en 2021 à 387 millions USD, soit une baisse de 14 millions USD ou 3,6 %. Le niveau de 20 à 30 millions d'enregistrements est le seul où la moyenne a augmenté par rapport à l'année dernière. Dans ce groupe, le coût total moyen d'une violation massive est passé de 230 à 241 millions USD, soit une augmentation de 11 millions USD ou 4,8 %.

Recommandations pour minimiser l’impact financier d’une violation de données

Dans cette section, IBM Security décrit les mesures que les entreprises peuvent prendre pour réduire les coûts financiers et les conséquences sur la réputation d’une violation de données. Ces recommandations comprennent des stratégies de sécurité efficaces qui ont été adoptées par les entreprises étudiées.

Adoptez un modèle de sécurité Zero Trust pour prévenir tout accès non autorisé aux données sensibles.
Les résultats de l’étude montrent que, même si seulement 41 % des entreprises ont mis en œuvre une approche de sécurité Zero Trust, elles pourraient économiser 1,5 million USD en coûts de violations avec un déploiement mature. Alors que les entreprises intègrent le télétravail et les environnements multicloud hybrides, une stratégie Zero Trust peut protéger les données et les ressources en limitant leur accessibilité et en exigeant du contexte.

Les outils de sécurité capables de partager des données entre des systèmes disparates et de centraliser les opérations de sécurité des données peuvent aider les équipes de sécurité à détecter les incidents dans des environnements multicloud hybrides complexes. Vous pouvez obtenir des analyses plus approfondies, atténuer les risques et accélérer la réponse grâce à une plateforme de sécurité ouverte qui peut faire progresser votre stratégie Zero Trust. Dans le même temps, vous pouvez utiliser vos investissements existants tout en laissant vos données là où elles se trouvent, aidant ainsi votre équipe à devenir plus efficace et à mieux collaborer.

Protégez les données sensibles dans les environnements cloud à l'aide de règles et du chiffrement.
Étant donné que la quantité et la valeur des données hébergées dans les environnements cloud augmentent sans cesse, les entreprises doivent prendre des mesures pour protéger leurs bases de données hébergées dans le cloud. La mise en œuvre de pratiques de sécurité cloud matures était associée à une réduction des coûts de violations de 720 000 USD. Utilisez le schéma de classification des données et les programmes de rétention pour gagner en visibilité et réduire le volume d'informations sensibles vulnérables à une violation. Protégez les informations sensibles à l'aide du chiffrement des données et du chiffrement entièrement homomorphe. L'utilisation d'un cadre interne pour les audits, l'évaluation des risques dans l'ensemble de l'entreprise et le suivi de la conformité aux exigences de gouvernance peuvent vous permettre de mieux détecter une violation de données et d'intensifier vos efforts de neutralisation.

Investissez dans l'orchestration, l'automatisation et la réponse aux incidents de sécurité (SOAR) et dans les technologies XDR pour améliorer les temps de détection et de réponse.
Avec l'IA et l'automatisation pour la sécurité, les capacités XDR peuvent contribuer à grandement réduire les coûts moyens des violations de données et les cycles de vie des violations. Selon l'étude, les entreprises ayant déployé des solutions XDR ont raccourci le cycle de vie des violations de 29 jours en moyenne par rapport à celles qui ne l'ont pas fait, ce qui se traduit par une économie de 400 000 USD. Les technologies SOAR, les logiciels de gestion des informations et des événements de sécurité (SIEM), les services gérés de détection et de réponse et les technologies XDR peuvent aider votre entreprise à accélérer la réponse aux incidents grâce à l'automatisation, à la normalisation des processus et à l'intégration avec vos outils de sécurité existants.

Utilisez des outils permettant de protéger et de surveiller les terminaux et les télétravailleurs.
L'étude a montré que lorsque le télétravail est à l'origine d'une violation, celle-ci coûte près de 1 million USD de plus que lorsqu'il n'est pas un facteur. Les produits et services de gestion unifiée des terminaux (UEM), de détection et de réponse des terminaux (EDR) et de gestion des identités et des accès (IAM) peuvent offrir aux équipes de sécurité une visibilité plus poussée sur les activités suspectes. Cette surveillance couvre les dispositifs personnels (BYOD, Bring your own device) et les ordinateurs portables, ordinateurs de bureau, tablettes, appareils mobiles et les dispositifs IdO de l'entreprise, y compris les terminaux auxquels l'entreprise n'a pas accès physiquement. L'UEM, l'EDR et l'IAM accélèrent l'investigation et le temps de réponse pour isoler et contenir les dommages lorsque le télétravail est en cause.

Créez et testez des manuels de réponse aux incidents pour renforcer votre cyber-résilience.
La création d'une équipe de réponse aux incidents (RI) et des tests approfondis du plan de RI sont deux des moyens les plus efficaces pour réduire le coût d'une violation de données. Les violations survenues dans les entreprises disposant d'une équipe de RI qui teste régulièrement son plan ont coûté 2,66 millions USD de moins que celles survenues dans les entreprises sans équipe de RI ou qui ne testaient pas leur plan de RI. Les entreprises peuvent réagir rapidement pour contenir les retombées d'une violation en élaborant un manuel détaillé pour les cyberincidents. Testez régulièrement ce plan par le biais d'exercices de simulation ou exécutez un scénario de violation dans un environnement simulé tel qu'un cyber-range.

Les exercices de simulation d'adversaire, également appelés exercices « Red Team », peuvent améliorer l'efficacité des équipes de RI en découvrant les voies et techniques d'attaque qui pourraient leur échapper et en identifiant les lacunes dans leur dispositif de détection et de réponse. Une solution de gestion de la surface d'attaque peut aider les entreprises à améliorer leur posture de sécurité en localisant des points d'exposition auparavant inconnus grâce à la simulation d'une expérience d'attaque authentique.

Les pratiques de sécurité recommandées le sont à titre éducatif et les résultats ne sont pas garantis.

Données sur les entreprises

L’étude de cette année portait sur 550 entreprises de différentes tailles, zones géographiques et secteurs d’activité. Vous découvrirez dans cette section la répartition des entreprises étudiées par zone géographique et par secteur d’activité, et les définitions utilisées pour classer les entreprises par secteur d’activité.

17 ans

Les États-Unis sont le pays qui figure dans l'étude depuis le plus longtemps, à savoir 17 ans.

Répartition géographique

L'étude de 2022 a été menée dans 17 pays ou régions.

L'étude globale, en un coup d'œil

Pays	Échantillon de 2022	Pourcentage	Nombre d'années dans l'étude	Devise
États-Unis	64	12 %	17	USD
Inde	49	9 %	11	INR
Royaume-Uni	43	8 %	15	GBP
Brésil	43	8 %	10	BRL
Allemagne	38	7 %	14	EUR
Japon	35	6 %	11	JPY
France	33	6 %	13	EUR
Moyen-Orient[1]	31	6 %	9	SAR
Corée du Sud	30	5 %	5	KRW
Australie	26	5 %	13	AUD
Canada	25	5 %	8	CAD
Italie	24	4 %	11	EUR
Asie du Sud-Est[2]	23	4 %	6	SGD
Amérique latine[3]	23	4 %	3	MXN
Afrique du Sud	21	4 %	7	ZAR
Scandinavie[4]	20	4 %	4	NOK
Turquie	20	4 %	5	TRY
Total	**550**	**100 %**		

1. L'échantillon Moyen-Orient regroupe des sociétés situées en Arabie saoudite et aux Émirats arabes Unis.
2. L'échantillon Asie du Sud-Est regroupe des sociétés situées à Singapour, en Indonésie, aux Philippines, en Malaisie, en Thaïlande et au Vietnam
3. L'échantillon Amérique latine regroupe des sociétés situées au Mexique, en Argentine, au Chili et en Colombie
4. L'échantillon Scandinavie regroupe des sociétés situées au Danemark, en Suède, en Norvège et en Finlande.

Figure 54

Les secteurs les plus représentés dans l'échantillon étaient les suivants.

16 % Finance

12 % Services

12 % Industrie

11 % Technologie

Répartition sectorielle

Cette année, l'étude portait sur 17 secteurs d'activité, les mêmes que ceux inclus dans plusieurs études antérieures.

Répartition de l'échantillon par secteur d'activité

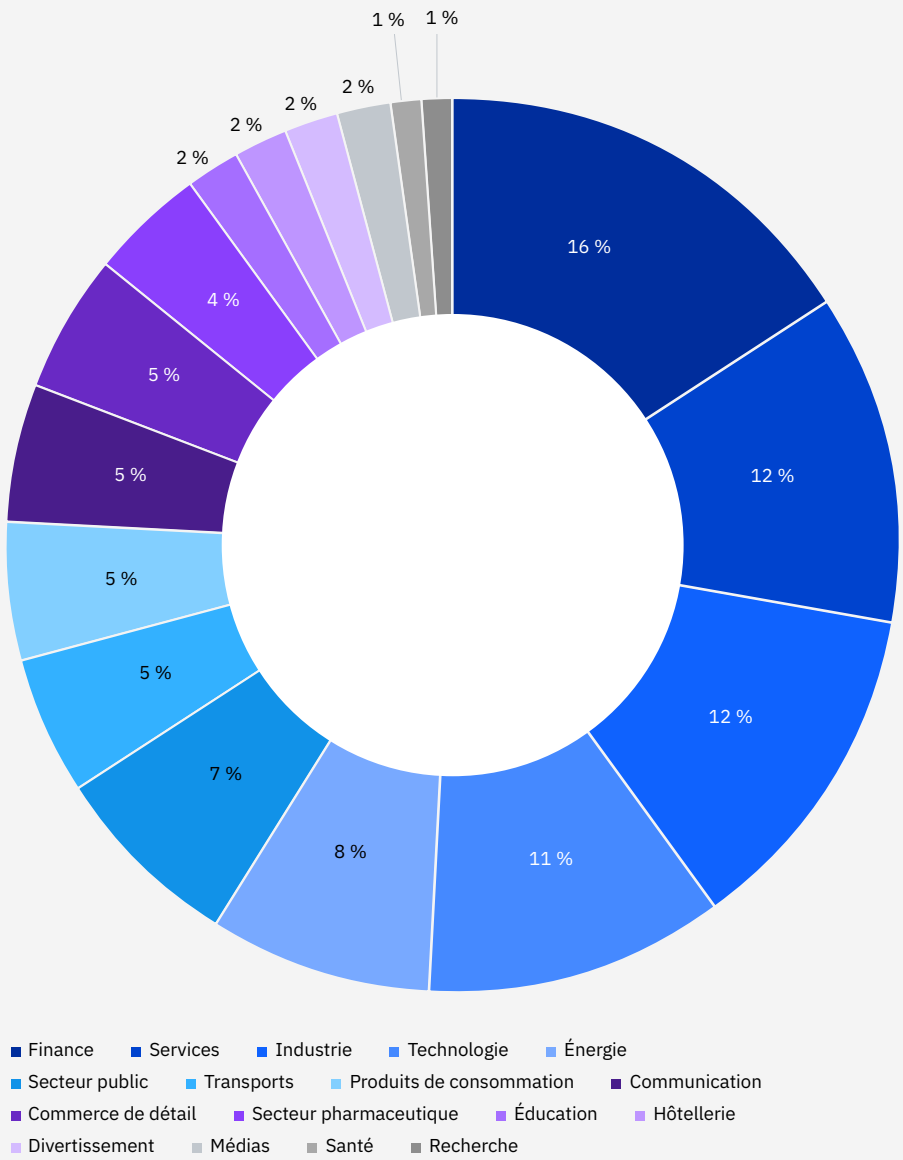


Figure 55

Définitions des secteurs d’activité

Santé
Hôpitaux, cliniques

Finance
Banques, assurances, sociétés d’investissement

Énergie
Sociétés pétrolières et gazières, services publics, producteurs et fournisseurs d’énergies alternatives

Secteur pharmaceutique
Produits pharmaceutiques, sciences de la vie et biomédicales

Industrie
Entreprises de traitement chimique, d’ingénierie et de fabrication

Technologie
Sociétés de logiciels et de matériel

Éducation
Universités et établissements d’enseignement supérieur publics et privés, entreprises de formation et de développement

Services
Services professionnels tels que les cabinets d’avocats, comptables et de conseil

Divertissement
Production de films, sports, jeux et casinos

Transports
Compagnies aériennes, chemins de fer, transport routier et entreprises de livraison

Communication
Journaux, maisons d’édition, agences de relations publiques et de publicité

Produits de consommation
Fabricants et distributeurs de produits de consommation

Médias
Télévision, satellite, médias sociaux, Internet

Hôtellerie
Hôtels, chaînes de restaurants, compagnies de croisière.

Commerce de détail
Magasins physiques et commerce électronique

Recherche
Études de marché, groupes de réflexion, recherche et développement

Secteur public
Organismes gouvernementaux, régionaux et locaux et organisations non gouvernementales (ONG)

Méthodologie de l’étude

Pour préserver la confidentialité, l’outil de comparaison n’a capturé aucune information spécifique aux entreprises. Les méthodes de collecte des données ne comprenaient pas d’informations comptables à proprement parler. Les participants devaient plutôt fournir des estimations des coûts directs en inscrivant une variable de plage sur une ligne numérique. Les participants devaient sélectionner un point situé entre la limite supérieure et inférieure d’une plage pour chaque catégorie de coût.

La valeur numérique obtenue avec cette ligne, et non une estimation chiffrée précise correspondant à chaque catégorie de coût présentée, a permis de préserver la confidentialité et a garanti un taux de réponse plus important. L’outil de comparaison demandait aussi aux répondants de fournir une seconde estimation des coûts indirects et des coûts d’opportunité, et ce séparément.

Pour conserver une taille gérable pour le processus de benchmarking, nous nous en sommes tenus aux centres de coûts que nous avons jugés essentiels pour mesurer les coûts d’une violation de données. Suite à des entretiens avec des spécialistes, nous avons finalisé un jeu fixe de domaines de coûts. Une fois la collecte terminée, nous avons soumis de nouveau les outils à un examen minutieux pour être certains qu’ils étaient complets et homogènes.

La portée des postes des coûts des violations de données était limitée à des catégories de coût connues, s’appliquant à une large palette d’opérations métiers appelées à gérer des informations personnelles. Nous avons jugé qu’une étude privilégiant les processus métiers, et non les activités de protection des données ou de conformité à la confidentialité, donnerait des résultats de meilleure qualité.

Dans cette étude, nous avons utilisé la méthode ABC (Activity Based Costing, ou évaluation des coûts par activité). Elle permet d'identifier les activités et leur affecte un coût en fonction de leur utilisation réelle.

Mode de calcul des coûts d'une violation de données

Pour calculer le coût moyen d'une violation des données, les violations de très petite et de très grande taille ont été exclues de l'étude. Les violations de données prises en compte dans l'étude de 2022 allaient de 2 200 à 102 000 enregistrements compromis. Pour analyser les coûts des violations massives, nous avons utilisé une méthode distincte. Une explication détaillée de celle-ci est fournie dans la rubrique « FAQ sur les violations de données » qui figure dans le rapport.

Dans cette étude, nous avons utilisé la méthode ABC (Activity Based Costing, ou évaluation des coûts par activité). Elle permet d'identifier les activités et leur affecte un coût en fonction de leur utilisation réelle. Quatre activités liées aux processus entraînent une gamme de dépenses associées à la violation de données : la détection et l'escalade, la notification, la riposte post-violation et la perte d'affaires.

Détection et escalade
Activités qui permettent à une entreprise de détecter raisonnablement une violation, notamment :
- La recherche criminalistique et l'investigation
- Les services d'évaluation et d'audit
- La gestion des crises
- Les communications destinées aux cadres et au conseil d'administration

Notification
Activités qui permettent à l'entreprise d'avertir les victimes de la violation, les autorités de protection des données et autres tiers, notamment :
- E-mails, lettres, appels sortants ou avis général aux personnes concernées
- Détermination des exigences réglementaires
- Communication avec les organismes de réglementation
- Implication de spécialistes externes

Riposte post-violation
Activités visant à aider les victimes d'une violation à communiquer avec l'entreprise et activités de réparation auprès des victimes et des organismes de réglementation, notamment :
- Centre d'assistance et communications entrantes
- Services de surveillance des rapports de crédit et de protection des identités
- Création de nouveaux comptes ou délivrance de nouvelles cartes de crédit
- Frais juridiques
- Remises sur les produits
- Amendes pour infraction aux réglementations

Pertes d'affaires
Activités qui tentent de minimiser la perte de clients, les perturbations des opérations et les pertes de revenus, notamment :
- Interruption des activités et pertes de revenus dues aux temps d'arrêt du système
- Coût de la perte de clients et de l'acquisition de nouveaux clients
- Pertes liées à l'atteinte à la réputation et à la bonne volonté

FAQ sur les violations de données

Qu'est-ce qu'une violation de données ?
Une violation de données est définie comme un événement lors duquel le nom et le dossier médical d'une personne, un dossier financier ou une carte de paiement sont potentiellement mis en danger. Ces enregistrements peuvent être au format électronique ou papier. Les violations prises en compte dans l'étude allaient de 2 200 à 102 000 enregistrements compromis.

Qu'est-ce qu'un enregistrement compromis ?
Un enregistrement est une information qui identifie la personne physique ou la personne dont les informations ont été perdues ou volées lors d'une violation de données. Il peut s'agir de données contenant le nom d'une personne, d'informations de carte de crédit et autres informations identifiant la personne, ou d'un dossier médical comportant le nom du titulaire de la police et ses informations de paiement.

Comment collectez-vous les données ?
Nos analystes ont recueilli des données qualitatives approfondies au moyen de plus de 3 600 entretiens distincts avec des employés de 550 entreprises ayant subi une violation de données entre mars 2021 et mars 2022. Parmi les personnes interrogées figuraient des professionnels de l'informatique, de la conformité et de la sécurité de l'information qui avaient une bonne connaissance de la violation subie par leur entreprise et des coûts associés à la résolution de celle-ci. Pour des raisons de confidentialité, nous n'avons pas recueilli d'informations spécifiques aux entreprises.

Comment calculez-vous le coût moyen d'une violation de données ?
Nous avons recueilli les dépenses directes et indirectes engagées par l'entreprise. Les dépenses directes comprenaient l'embauche d'experts en investigation, l'externalisation du centre d'assistance et la fourniture d'abonnements gratuits pour la surveillance du crédit et de remises pour les futurs produits et services. Les coûts indirects comprenaient les enquêtes et les communications internes, ainsi que la valeur extrapolée des pertes de clients ou de la baisse des taux d'acquisition de clients.

Cette étude tient uniquement compte des événements directement liés à l'expérience de violation de données. Des réglementations telles que le Règlement général sur la protection des données (RGPD) et le California Consumer Privacy Act (CCPA) peuvent encourager les entreprises à investir davantage dans leurs technologies de gouvernance de la cybersécurité. Cependant, de telles activités n'ont pas eu d'incidence directe sur le coût d'une violation de données dans le cadre de cette étude.

Par souci de cohérence avec les années précédentes, nous avons utilisé la même méthode de conversion des devises plutôt que d'ajuster les coûts comptables.

En quoi l'étude comparative diffère-t-elle de la recherche par sondage ?
Dans notre rapport sur le coût d'une violation de données, l'entreprise était l'unité d'analyse. Dans la recherche par sondage, l'unité d'analyse est l'individu. Nous avons recruté 550 entreprises pour participer à cette étude.

Le coût moyen par enregistrement peut-il être utilisé pour calculer le coût des violations représentant des millions d'enregistrements perdus ou volés ?
Dans notre étude, le coût moyen d'une violation de données ne s'applique pas aux violations de données catastrophiques ou massives, telles que celles dont ont été victimes Equifax, Capital One ou Facebook. Ces événements ne sont pas typiques des violations subies par de nombreuses entreprises. Pour tirer des conclusions utiles afin de comprendre les comportements en matière de coûts de violations de données, nous avons ciblé les violations de données qui ne dépassaient pas 102 000 enregistrements.

L'utilisation du coût par enregistrement pour calculer le coût des violations impliquant des millions d'enregistrements n'est pas cohérente avec cette étude. Cependant, l'étude utilise un cadre de simulation pour mesurer l'impact financier d'une violation massive représentant 1 million d'enregistrements ou plus, sur la base d'un échantillon de 13 violations de cette taille.

Pourquoi avez-vous utilisé des méthodes de simulation pour estimer le coût d'une violation massive ?
L'échantillon de 13 entreprises ayant subi une violation massive était trop petit pour effectuer une analyse statistiquement significative à l'aide de la méthode ABC. Pour remédier à ce problème, nous avons utilisé la simulation Monte-Carlo pour estimer une gamme de résultats possibles, à savoir des résultats aléatoires obtenus à l'aide d'essais répétés.

Au total, nous avons réalisé plus de 150 000 essais. La moyenne générale de toutes les moyennes constituait le résultat le plus probable pour chaque niveau de violation, allant de 1 à 60 millions d'enregistrements compromis.

Le suivi porte-t-il chaque année sur les mêmes entreprises ?
Chaque année, l'étude porte sur un échantillon différent d'entreprises. Pour garantir la cohérence avec les rapports précédents, nous recrutons des entreprises présentant des caractéristiques similaires, telles que le secteur d'activité de l'entreprise, l'effectif, l'empreinte géographique et la taille de la violation de données. Depuis le début de cette étude en 2005, nous avons étudié les expériences de violation de données de 5 027 entreprises.

L’outil utilisé n’a capturé aucune information permettant d’identifier les entreprises.

Limites de l’étude

Notre étude utilise une méthode confidentielle de comparaison développée par nos soins et qui s’est révélée concluante dans nos études antérieures. Cependant, certaines restrictions inhérentes à cette étude comparative doivent être examinées avec attention avant de tirer des conclusions à partir des résultats présentés.

Résultats non statistiques
Notre étude s’appuie sur un échantillon représentatif et non statistique d’entreprises du monde entier. Ces données ne peuvent donner lieu à des inférences statistiques, des marges d’erreur ou des intervalles de confiance car nos méthodes d’échantillonnage ne sont pas scientifiques.

Non-réponse
Nous n’avons pas testé le taux de non-réponse et il est donc toujours possible que les coûts sous-jacents des violations de données présentent des différences importantes dans les sociétés n’ayant pas participé.

Biais d’échantillonnage
Notre échantillonnage résultant d’un choix délibéré, la qualité des résultats est influencée par le fait que cet échantillonnage est représentatif des sociétés étudiées. Nous pensons que cet échantillonnage privilégie les sociétés ayant mis en place des programmes plus matures de confidentialité ou de sécurité de l’information.

Informations relatives aux entreprises
L’outil utilisé n’a capturé aucune information permettant d’identifier les entreprises. Les individus ont utilisé des variables de réponse catégoriques pour communiquer des informations démographiques sur l’entreprise et le secteur d’activité.

Facteurs non mesurés
Nous avons décidé d’omettre certaines variables de nos analyses, telles que les tendances majeures et les caractéristiques organisationnelles. Il n’est pas possible de déterminer dans quelle mesure les variables omises peuvent expliquer les résultats de l’étude.

Résultats des coûts extrapolés
Bien que certains contrôles puissent être intégrés au processus de comparaison, il est toujours possible que les répondants n’aient pas fourni des réponses exactes ou véridiques. En outre, l’utilisation des méthodes d’extrapolation des coûts et non de données de coût réelles peut introduire accidentellement un biais et des inexactitudes.

Conversions monétaires
La conversion des devises locales en dollars américains a entraîné la diminution des estimations moyennes du coût total dans d’autres pays. Par souci de cohérence avec les années précédentes, nous avons décidé de continuer à utiliser la même méthode comptable plutôt que d’ajuster le coût.

À propos du Ponemon Institute et d'IBM Security

Ponemon Institute

Le Ponemon Institute est un institut indépendant spécialisé dans la recherche et la formation, dans le but de promouvoir des pratiques responsables de gestion de l'information et de la confidentialité dans le secteur public et privé. Le Ponemon Institute se consacre à la recherche et à l'éducation indépendantes pour proposer des pratiques de gestion responsable de la vie privée et des informations à destination du gouvernement et des entreprises. Notre mission est de réaliser des études empiriques de haute qualité portant sur des questions critiques affectant la gestion et la sécurité des informations sensibles sur les personnes et les entreprises.

Le Ponemon Institute respecte des normes strictes en matière de confidentialité des données, de vie privée et de recherche éthique, et ne recueille aucune information qui permettrait d'identifier les personnes ou les entreprises participant à ses études. De plus, nos normes de qualité strictes sont la garantie qu'aucune question superflue, non pertinente ou inappropriée ne sera posée aux participants.

IBM Security

IBM Security propose l'un des portefeuilles de produits et services de sécurité d'entreprise les plus avancés et les plus intégrés. Ce portefeuille, soutenu par l'équipe de recherche IBM Security X-Force® de renommée mondiale, fournit des solutions de sécurité pour aider les entreprises à intégrer la sécurité au sein de leurs activités afin de prospérer en dépit d'un environnement imprévisible.

IBM dirige des opérations de recherche, de développement et de prestation dans le domaine de la sécurité qui figurent parmi les plus vastes et les plus complètes du marché. IBM surveille plus de 4 700 milliards d'événements par mois dans plus de 130 pays et détient plus de 10 000 brevets de sécurité. Pour en savoir plus, rendez-vous sur ibm.com/fr-fr/security. Prenez part à la conversation dans la communauté IBM Security.

Si vous avez des questions ou des commentaires au sujet de ce rapport, y compris pour obtenir la permission de citer ou de reproduire son contenu, veuillez nous contacter par courrier, téléphone ou e-mail aux coordonnées suivantes :

Ponemon Institute LLC
À l'attention de : Research Department
2308 US 31 North
Traverse City
Michigan 49686, États-Unis

1.800.887.3118
research@ponemon.org

Passez à l'étape suivante

Solutions de sécurité Zero Trust
Assurez la sécurité de chaque utilisateur, de chaque appareil et de chaque connexion.
En savoir plus

Gestion des identités et des accès
Connectez chaque utilisateur, API et appareil à toutes les applications en toute sécurité.
En savoir plus

Sécurité des données
Découvrez, classez et protégez les données sensibles de l'entreprise.
En savoir plus

Orchestration, automatisation et réponse aux incidents de sécurité
Accélérez la réponse aux incidents grâce à l'orchestration et à l'automatisation.
En savoir plus

Gestion des informations et des événements de sécurité
Gagnez en visibilité pour détecter, enquêter et répondre aux menaces.
En savoir plus

Sécurité cloud
Intégrez la sécurité dans votre parcours vers le multicloud hybride.
En savoir plus

Sécurité des terminaux
Protégez les appareils, les utilisateurs et l'entreprise contre les attaques sophistiquées.
En savoir plus

Services de cybersécurité
Réduisez les risques grâce aux services de conseil, de cloud et de sécurité gérés.
En savoir plus

Réponse aux incidents et renseignements sur les menaces
Gérez et répondez de manière proactive aux menaces à la sécurité.
En savoir plus

Programmez une consultation individuelle avec un expert IBM Security X-Force
Réservez

Compagnie IBM France
17 avenue de l'Europe
92275 Bois-Colombes Cedex

Produit aux
États-Unis d'Amérique
Juillet 2022