# Rapport 2025 sur le coût d'une violation de données

## Les lacunes de contrôle de l'IA

Synthèse

**think** report

IBM

# Synthèse

Bienvenue dans le rapport annuel d'IBM sur le coût d'une violation de données. Cette édition marque les 20 ans de la recherche sur les violations de données. Cette année, nous nous sommes intéressés au changement technologique le plus important depuis une génération : l'adoption de l'IA.

Le rapport 2025 est l'occasion idéale pour commencer à répertorier et quantifier les risques liés à l'IA. Et les résultats observés sont inquiétants : les entreprises semblent faire l'impasse sur la sécurité et la gouvernance de l'IA au profit d'une adoption immédiate. Non gouvernés, ces systèmes sont plus susceptibles de subir des violations, augmentant leurs coûts en cas d'attaque avérée. Surprenant ? Pas vraiment.

Depuis 2005, ce rapport suit l'évolution d'un environnement technologique en constante expansion, ainsi que les menaces qui en découlent. Le Ponemon Institute, notre partenaire de recherche, n'a pas seulement documenté l'émergence de nouvelles menaces et surfaces d'attaque : il a également quantifié ces menaces en des termes financiers que les responsables de la sécurité et des opérations peuvent comprendre et exploiter. Au total, les chercheurs ont analysé plus de 6 485 violations et interrogé plus de 34 652 responsables technologiques, de la sécurité et des opérations impliqués dans la réponse aux incidents de violation de leur entreprise.



Sans surprise, les menaces de sécurité ont évolué au fil des années. Il y a 20 ans, près de la moitié de toutes les violations de données (45 %) étaient dues à la perte ou au vol d'appareils informatiques, comme des ordinateurs portables ou des clés USB, alors que seulement 10 % des violations étaient attribuées aux « systèmes électroniques piratés ». Aujourd'hui, la plupart des violations sont causées par de nombreuses activités malveillantes, des attaques de phishing aux menaces internes.

Il y a 10 ans, les violations découlaient d'une mauvaise configuration du cloud et n'étaient pas considérées comme une menace catégorisée. Aujourd'hui, le cloud et les données sont des cibles de choix, et ce n'est que lors des confinements en période de COVID-19, en 2020, que les attaques par ransomware ont commencé à prendre de l'ampleur. Un an plus tard, ces attaques représentaient un coût de violation moyen de 4,62 millions de dollars… une estimation qui a atteint les 5,08 millions de dollars cette année.

En revanche, ce qui n'a pas changé, c'est le travail de Ponemon. Cette année, l'étude, réalisée de manière indépendante par le Ponemon Institute et commanditée, analysée et publiée par IBM, portait sur 600 entreprises victimes de violations de données survenues entre mars 2023 et février 2025. Ensemble, nous nous sommes concentrés sur des entreprises opérant dans 17 secteurs, dans 16 pays et régions, et sur des violations ayant compromis de 2 960 à 113 620 enregistrements. Afin d'obtenir des informations sur le terrain, les chercheurs du Ponemon Institute ont interrogé 3 470 dirigeants et responsables de la sécurité en lien direct avec les incidents de violation de données au sein de leur entreprise. Parmi elles figuraient des PDG, des cheffes des opérations, des contrôleurs ou des responsables financiers, des informaticiens, des responsables d'unités commerciales et des directrices et directeurs généraux, ainsi que des spécialistes de la gestion des risques et de la cybersécurité.

Les conclusions de l'étude ont été compilées dans un rapport de référence sur lequel les responsables technologiques et de la sécurité peuvent s'appuyer pour renforcer leurs défenses, informer les allocations de ressources et stimuler l'innovation, en particulier concernant la protection et la gouvernance de leurs initiatives d'IA.

En tête d'affiche cette année : le coût global des violations de données a diminué pour la première fois en cinq ans, tombant à 4,44 millions de dollars. En cause ? L'accélération de l'endiguement des violations, soutenu par les défenses alimentées par l'IA. Mais si les défenseurs évoluent plus intelligemment et plus rapidement, il en va de même pour les attaquants. En effet, 16 % des violations impliqueraient des attaques reposant sur l'IA, souvent utilisées pour le phishing et le deepfake. Bien que cette intensification de la course aux armements de l'IA a profité aux entreprises en réduisant les coûts de violation globaux, les États-Unis ne semblent pas vouloir suivre la tendance. En effet, les coûts des violations y ont dépassé les 10 millions de dollars en raison de sanctions réglementaires plus strictes et de l'augmentation des coûts de détection.

Nous avons également constaté que l'adoption de l'IA est plus rapide que son contrôle : 97 % des violations de la sécurité liées à l'IA impliquaient des systèmes d'IA dépourvus de contrôles d'accès adaptés. De même, la plupart des entreprises victimes d'une violation ont indiqué qu'elles n'avaient pas mis en place de politique de gouvernance pour gérer l'IA ou prévenir l'IA fantôme (l'utilisation de l'IA sans contrôle ou autorisation de l'employeur). L'utilisation non autorisée de l'IA fantôme et le manque de gouvernance sont des facteurs qui ont contribué à la hausse des coûts de violation.

## Nouveautés du rapport 2025

Comme chaque année, le rapport sur le coût d'une violation de données s'intéresse aux nouvelles technologies, aux tactiques émergentes et aux événements récents. Cette année, le rapport aborde pour la première fois les éléments suivants :

- État de la sécurité et de la gouvernance de l'IA
- Prévalence et profil de risque de l'IA fantôme
- Types de données ciblées lors d'incidents de sécurité impliquant l'IA
- Durée des interruptions de l'activité des entreprises suite à une violation
- Économies de coûts grâce aux outils de sécurité Quantum
- Coûts des violations associés aux attaques pilotées par l'IA
- Montant des coûts des violations répercutés sur les clients

# Principales conclusions

Les principales conclusions présentées ici sont basées sur l'analyse réalisée par IBM à partir des données de recherche compilées indépendamment par le Ponemon Institute.

## 4,44 millions de dollars

**Coût moyen global d'une violation de données**

Le coût moyen global d'une violation de données est passé de 4,88 millions de dollars en 2024 à 4,44 millions de dollars, soit une baisse de 9 % et un retour aux niveaux de coûts observés en 2023. Ce qui a rendu possible cette baisse ? L'identification et la maîtrise plus rapides des violations, principalement à l'initiative des équipes de sécurité et des services de protection des entreprises, qui s'appuient sur l'IA et l'automatisation. La moyenne globale aurait pu être plus basse si elle ne tenait pas compte des États-Unis, où le coût moyen a augmenté de 9 % pour atteindre les 10,22 millions de dollars : un record absolu, tous territoires confondus. La hausse des amendes réglementaires et des coûts de détection et de remontée aux États-Unis a contribué à cette augmentation.

## 13 %

**Part d'incidents de sécurité liés à l'IA**

Pour l'instant, les incidents de sécurité impliquant l'IA d'une entreprise demeurent limités. En moyenne, 13 % des entreprises ont indiqué avoir été victimes de violations impliquant leurs applications ou modèles d'IA. Toutefois, parmi les entreprises victimes, la quasi-totalité (97 %) n'a pas mis en place de contrôles d'accès par l'IA suffisants. De même, la plupart de ces incidents de sécurité sont survenus sur la chaîne d'approvisionnement d'IA par le biais d'applications, d'API ou de plug-ins compromis. Et ces incidents ont eu des répercussions : ils ont conduit à une compromission de données à grande échelle (60 %) et une perturbation opérationnelle (31 %). D'après les résultats, l'IA devient une cible de très grande valeur.

## 4,92 millions de dollars

**Coût moyen des attaques par initié malveillant**

Pour la deuxième année consécutive, les attaques par initié malveillant ont provoqué les coûts de violation les plus élevés parmi les vecteurs de menace initiaux, représentant en moyenne 4,92 millions de dollars. S'en suivent de près les compromissions des fournisseurs tiers et de la chaîne d'approvisionnement, avec un coût moyen de 4,91 millions de dollars. Parmi les autres vecteurs d'attaque coûteux, on retrouve l'exploitation des vulnérabilités et le phishing. En revanche, le type de vecteur d'attaque le plus fréquent est le phishing (16 %), avec un coût moyen de 4,8 millions de dollars.

## 200 000 dollars

**Coût supplémentaire d'une violation impliquant l'IA fantôme**

Parmi les entreprises ayant participé à l'étude cette année, 20 % ont affirmé avoir été victime d'une violation suite à des incidents de sécurité impliquant l'IA fantôme : des violations ont ajouté 200 321 dollars au coût moyen des violations. En outre, ces incidents ont compromis davantage d'informations personnelles identifiables (65 %) et de données relatives à la propriété intellectuelle (40 %). Ces données étaient le plus souvent stockées sur de nombreux environnements, ce qui permet d'avancer qu'il suffit d'un seul système d'IA non surveillé pour conduire à une exposition généralisée. L'essor rapide de l'IA fantôme a supplanté les pénuries de compétences en matière de sécurité en tant que l'un des trois principaux facteurs de violations coûteuses recensés dans ce rapport.

## 1,9 million de dollars

**Économies réalisées grâce à l'utilisation intensive de l'IA dans la sécurité**

Les équipes de sécurité qui utilisent considérablement l'IA et l'automatisation ont réduit la durée des violations de 80 jours et ont diminué le coût moyen des violations de 1,9 million de dollars par rapport aux entreprises qui n'adoptent pas ces solutions. Près d'un tiers des entreprises expliquent utiliser largement ces outils tout au long du cycle de vie de sécurité, pour la prévention, la détection, l'enquête et la réponse. Toutefois, ce chiffre n'est que légèrement supérieur à celui de l'année passée, suggérant que l'adoption de l'IA est sans doute au point mort. Il montre également que la majorité des entreprises n'utilise pas encore l'IA et l'automatisation et n'en perçoit donc pas les avantages financiers.

## 63 %

**Part des entreprises refusant de payer les demandes de rançon**

En 2025, les entreprises victimes d'une attaque par ransomware ont été plus nombreuses à refuser de payer une rançon (63 %) qu'en 2024 (59 %). En revanche, le coût moyen d'un incident d'extorsion ou de ransomware demeure élevé, surtout lorsqu'il est révélé par l'attaquant (5,08 millions de dollars). Dans le même temps, cette année, 40 % des victimes de ces attaques ont déclaré avoir fait appel aux forces de l'ordre, soit moins que l'année passée (53 %).

## 49 %

**Part des entreprises qui investissent dans la sécurité suite à une violation**

Le nombre d'entreprises prévoyant d'investir dans leur sécurité après avoir été victimes d'une violation a considérablement réduit, atteignant 49 % cette année contre 63 % l'année dernière. Moins de la moitié des entreprises qui prévoient de mettre en place des mesures de sécurité envisagent de se tourner vers des solutions ou des services pilotés par l'IA, comme la détection et la réponse aux menaces, la planification et les tests de réponse aux incidents (RI), ainsi que les outils de sécurité ou de protection des données.

## 63 %

**Part des entreprises ne possédant pas de politique de gouvernance de l'IA**

La majorité des entreprises victimes d'une violation (63 %) ne possède pas de politique de gouvernance de l'IA ou se trouve encore en phase d'élaboration. En outre, même lorsqu'elles disposent d'une politique, moins de la moitié d'entre elles ont mis en place un processus d'approbation des déploiements d'IA, et 62 % ne disposent pas des contrôles d'accès adaptés sur les systèmes d'IA. Parmi les entreprises appliquant des politiques de gouvernance, seule une minorité (34 %) réalise des audits réguliers d'utilisation non autorisée de l'IA. Ces réponses montrent bien que l'IA demeure en grande partie non contrôlée, alors que son adoption, elle, dépasse la sécurité et la gouvernance.

## 1 sur 6

**Nombre de violations impliquant des attaques pilotées par l'IA**

Les attaques peuvent se servir de l'IA générative pour perfectionner et étendre leurs campagnes d'attaques de phishing et d'ingénierie sociale. IBM avait déjà observé la capacité de l'IA générative à réduire de 16 heures à seulement 5 minutes le temps nécessaire pour concevoir un e-mail de phishing convaincant. Cette année, le rapport en montre l'impact : en moyenne, 16 % des violations de données impliquaient des attaquants utilisant l'IA, le plus souvent pour des attaques de phishing générées par l'IA (37 %) et des attaques d'usurpation d'identité par deepfake (35 %).

# Recommandations

Pour aider à prévenir, atténuer et réduire les coûts d'une violation de données, ainsi que pour gouverner les modèles d'IA, les applications et les usages, les experts IBM proposent ces cinq approches fructueuses.

## Fortifier les identités des personnes et des machines

De nombreuses entreprises travaillent avec des contrôles d'accès souples, des comptes possédant trop d'autorisations et peu de visibilité sur les personnes ayant accès aux systèmes critiques. Dans de nombreux cas, on fait appel à différents services et outils pour la gestion des identités et des accès (IAM). L'ensemble de ces facteurs créent des ouvertures que les attaquants exploitent activement, c'est pourquoi il est essentiel de les limiter. De même, les modèles d'IA et les infrastructures se développent rapidement, offrant aux attaquants une nouvelle surface d'attaque de grande valeur.

Fortifier la sécurité des identités grâce à l'IA et à l'automatisation peut renforcer l'IAM sans surcharger les équipes de sécurité qui manquent constamment de mains. En outre, alors que les agents d'IA commencent à jouer un rôle plus important au sein des opérations organisationnelles, la même rigueur doit être appliquée pour la protection de l'identité des agents et des ressources humaines. Tout comme les utilisateurs humains, les agents d'IA se reposent de plus en plus sur les identifiants pour accéder aux systèmes et exécuter des tâches. Il est donc indispensable de mettre en œuvre des contrôles opérationnels robustes ou des services qui y contribuent, tout en assurant la visibilité sur toutes les activités des identités non humaines (NHI). Les entreprises doivent être en mesure de faire la différence entre les NHI utilisant des identifiants gérés (archivés) et ceux utilisant des identifiants non gérés.

Dès que les identifiants sont pris en charge et gérés, il est important de les protéger et d'appliquer une gestion et une gouvernance du cycle de vie adaptées. Cela passe par le provisionnement, la rotation, l'audit, la protection et le déclassement des identifiants, ainsi que par la surveillance du comportement des NHI pour s'assurer qu'ils fonctionnent selon les paramètres prévus. Ce faisant, les entreprises peuvent réduire le risque d'utilisation abusive des identifiants et maintenir un environnement conforme et sécurisé.

Aujourd'hui, de nombreux attaquants se connectent plutôt que de pirater. Pour lutter contre ce problème, il est essentiel de commencer par empêcher les attaquants d'obtenir ces identifiants. L'un des moyens les plus efficaces consiste à s'assurer que tous les utilisateurs humains adoptent des méthodes d'authentification modernes et résistantes au phishing, telles que les clés d'accès. Ces technologies sont conçues pour éliminer les vulnérabilités des mots de passe traditionnels et des codes à usage unique, compliquant l'interception ou l'utilisation abusive des identifiants par les attaquants.



## Renforcer les pratiques de sécurité des données par l'IA

Les entreprises ont désormais dépassé la phase d'expérimentation de l'IA générative et des agents d'IA pour se lancer dans l'innovation en contexte réel, en intégrant la technologie au cœur de leurs activités. Mais la vitesse d'adoption dépasse la sécurité : cette année, le rapport a révélé que 62 % des entreprises ne disposent pas de contrôles d'accès adaptés sur les systèmes d'IA. Et comme les données sont le carburant de l'IA, elles constituent une cible de choix pour les attaquants.

Sécuriser les données d'IA est essentiel, non seulement pour la protection de la vie privée et la conformité, mais aussi pour protéger l'intégrité des données, maintenir la confiance organisationnelle et éviter la compromission des données. Cette approche signifie qu'il faut aller plus loin que les contrôles de surface et mettre en œuvre des principes fondamentaux de sécurité des données : la découverte de données et la classification, ainsi que la protection des données, comme le contrôle d'accès, le chiffrement et la gestion des clés. Elle peut également inclure l'utilisation de services de sécurité des données et de l'IA. Ces mesures ne sont pas propres à la sécurisation de l'IA, mais l'émergence de l'IA en tant que vecteur de menace et d'aide à la sécurité signifie qu'elles sont plus importantes que jamais.

## Relier la sécurité et la gouvernance de l'IA

La sécurité et la gouvernance de l'IA sont deux disciplines complémentaires. Lorsque les entreprises les conservent dans des silos, elles accroissent les risques, la complexité et les coûts. Malheureusement, l'adoption de l'IA dépasse l'adoption de la sécurité et de la gouvernance : cette année, 41 % des entreprises affirment ne pas avoir mis de telles politiques en place, alors que 22 % sont encore en train d'en élaborer.

Les entreprises doivent s'assurer que les responsables de la sécurité des systèmes d'information (RSSI), les responsables de la gestion des risques (CRO) et les responsables de la conformité (CCO), ainsi que leurs équipes, collaborent régulièrement. Investir dans des logiciels et des processus de sécurité et de gouvernance intégrés pour réunir ces parties prenantes interfonctionnelles peut aider l'entreprise à découvrir et à gérer automatiquement l'IA fantôme. De tels investissements peuvent également les aider à :

- Gagner en visibilité sur tous les déploiements d'IA
- Identifier et atténuer les vulnérabilités
- Protéger les prompts et les données découlant d'une utilisation indésirable
- Utiliser des outils d'observabilité pour renforcer la conformité et détecter les anomalies

## Utiliser des outils de sécurité de l'IA et l'automatisation pour avancer plus vite

L'IA aide déjà les attaquants à avancer plus rapidement, en facilitant par exemple la création de deepfakes avec seulement quelques prompts, ou en réduisant le temps nécessaire pour produire un message de phishing réaliste de plusieurs heures à seulement quelques minutes. Alors que les attaquants se tournent vers l'IA pour produire et distribuer des attaques plus adaptatives, les équipes de sécurité doivent également adopter les technologies d'IA. Les équipes de sécurité peuvent utiliser l'IA pour réduire ou prévenir les attaques et leurs impacts commerciaux, en employant de manière proactive des mesures qui améliorent la précision de la détection (traque des menaces) et réduisent le temps de réponse.

Les outils de sécurité et les services de sécurité gérés, y compris ceux alimentés par l'IA et l'automatisation, peuvent soutenir les équipes de sécurité déjà surchargées. Ils sont capables de réduire considérablement le volume d'alertes, d'identifier les données à risque, de repérer plus tôt les failles de sécurité et les menaces, de détecter des violations en cours et de permettre des réponses plus rapides et précises aux attaques.

## Améliorer la résilience

Sur une période suffisamment longue, les violations de données sont inévitables. Elles surviennent, même malgré des mesures de prévention strictes. S'il est important de tenter de bloquer les menaces, les entreprises ne doivent pas en faire leur seule préoccupation : elles doivent également se concentrer sur l'atténuation des dommages une fois l'attaque lancée et la violation survenue, et planifier en conséquence.

Renforcer la résilience signifie être capable de détecter rapidement les problèmes, de les contenir avant qu'ils ne fassent trop de dégâts et de relancer rapidement ses activités avec un minimum de perturbations. Un plan de renforcement de la résilience devrait inclure des tests réguliers des plans de réponse aux incidents et du rétablissement des sauvegardes, la définition claire des rôles et des responsabilités face aux réponses aux crises, même pour les responsables non techniques, et la limitation de l'accès de haut niveau afin de réduire l'ampleur d'un problème potentiel. Une formation en personne ou virtuelle peut s'avérer essentielle pour aider les équipes de sécurité à comprendre leur rôle et à agir en cas de crise. Pour améliorer leur capacité à faire face aux attaques, les entreprises peuvent également participer à des exercices de simulation de crise cyber.

# À propos

## IBM

L'un des principaux fournisseurs mondiaux de cloud hybride, d'IA et de services métier, IBM aide ses clients dans plus de 175 pays à tirer parti des informations issues de leurs données, à rationaliser les processus métier, à réduire leurs coûts et à obtenir un avantage concurrentiel dans leurs secteurs. Ces capacités s'appuient sur l'engagement légendaire d'IBM en faveur de la confiance, de la transparence, de la responsabilité, de l'inclusion et du service. Pour plus d'informations, rendez-vous sur www.ibm.com/fr-fr.

Pour en savoir plus sur l'amélioration de votre posture de sécurité, rendez-vous suribm.com/fr-fr/security.

Participez à la conversation dans la communauté IBM Security.

## Ponemon Institute

Fondé en 2002, le Ponemon Institute est un institut indépendant spécialisé dans la recherche et la formation dont le but est de promouvoir des pratiques responsables de gestion de l'information et de la confidentialité dans le secteur public et privé. 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.

Dans le cadre de ses enquêtes commerciales, le Ponemon Institute respecte strictement la confidentialité des données et des personnes et les règles éthiques propres aux études et ne collecte pas d'informations personnelles identifiables auprès des personnes, ni d'informations identifiant une entreprise. De plus, nous respectons des normes de qualité très strictes qui garantissent qu'aucune question superflue, non pertinente ou inappropriée ne sera posée aux participants. 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
Research Department
1-800-887-3118
research@ponemon.org