think report

Rapport 2026 sur le coût d'une violation de données

Le point de bascule de l'IA

IBM

Synthèse

Bienvenue dans la 21e édition annuelle du rapport sur le coût d'une violation de données. Les modèles d'IA de pointe ont radicalement transformé le paysage des cybermenaces.

L'annonce, en avril 2026, d'un modèle de pointe ayant réussi à détecter des milliers de vulnérabilités très critiques (dont certaines dans tous les principaux systèmes d'exploitation et navigateurs web) constitue un signal d'alerte pour les équipes de sécurité.

Entre les mains de cybercriminels, ces outils réduiront drastiquement le délai entre la découverte d'une vulnérabilité et son exploitation. Les cybercriminels abandonnent la vitesse humaine au profit de la vitesse machine. Ils le font déjà avec l'IA générative, qui a réduit le temps, le coût et l'expertise nécessaires pour lancer des attaques, poussant les entreprises vers une perturbation continue de leur activité.

Le rapport sur le coût d'une violation de données de cette année montre que les fissures dans le mur s'étendent. Les attaques pilotées par l'IA ont augmenté de 56 % par rapport à l'étude de l'an dernier. Les conséquences financières n'ont rien d'anodin. Les attaques pilotées par l'IA ont ajouté en moyenne 1 million USD au coût de chaque violation, les outils d'IA permettant aux cybercriminels d'accroître leur vitesse et leur échelle d'action. Cette rapidité redéfinit l'économie des violations, et pas dans le bon sens.

Le coût moyen mondial d'une violation de données a augmenté de 12 %, pour atteindre près de 5 millions USD. Cette hausse s'explique en grande partie par les coûts liés à la détection, à l'escalade et à la perte d'activité. L'IA et l'automatisation restent parmi les moyens les plus efficaces de réduire l'impact d'une violation de données. Elles aident les équipes de sécurité à agir à la vitesse de la machine et permettent d'économiser en moyenne 1,93 million USD. Cependant, l'adoption de ces outils tout au long du cycle de vie de la sécurité demeure inégale.

Nous avions signalé pour la première fois l'an dernier cette course à l'armement IA croissante entre cybercriminels et équipes de défense, lorsque le coût moyen mondial d'une violation avait diminué pour la première fois depuis la pandémie. Les équipes de sécurité semblaient reprendre l'avantage. Mais le rapport de cette année montre qu'elles perdent du terrain sur certains indicateurs clés.

Si 50 % des entreprises victimes d'une violation nous ont indiqué avoir déployé des agents pour la chasse aux menaces, la réponse et le confinement, seules 18 % les ont utilisés pour l'analyse et la gestion des vulnérabilités : précisément le domaine que ciblent les capacités de pointe. En réponse aux nouvelles menaces issues des modèles d'IA de pointe, 85 % des entreprises victimes d'une violation ont déclaré prévoir d'augmenter leurs dépenses en outils de sécurité et de gouvernance, à travers tout un éventail de solutions et de services. Cette hausse sera importante à mesure que les agents d'IA se multiplieront au sein des entreprises, ce qui nécessitera de mettre l'accent sur la sécurisation des identités non humaines (NHI) dans les workflows d'IA. Les recherches de cette année montrent que moins de la moitié des entreprises sécurisent ces identités.

Dans le même temps, les cybercriminels n'utilisent pas seulement l'IA : ils la ciblent. Parmi les quelque 20 % d'entreprises ayant signalé une violation liée à l'IA, nous avons constaté que les incidents de sécurité relevaient moins du choix du modèle que de la sécurité du modèle et de son environnement. Des taux d'incidents de sécurité similaires ont été observés entre les déploiements open source et ceux reposant sur des fournisseurs tiers. Les causes profondes de ces incidents étaient souvent structurelles : compromission d'API connectées, d'applications et mauvaises configurations cloud, ce qui indique des défaillances de gouvernance, et non un risque inhérent au modèle.

Point positif : les entreprises reconnaissent la nécessité de renforcer la sécurité de l'IA. Plus de la moitié déclarent prévoir d'investir dans des outils de sécurité et de gouvernance de l'IA après une violation, soit une hausse de 88 % par rapport à l'an dernier, en réaction aux préoccupations suscitées par les menaces liées aux modèles d'IA de pointe. Ce regain d'attention porté à la sécurité est une bonne nouvelle. La souveraineté de l'IA, c'est-à-dire le maintien du contrôle sur l'endroit où les systèmes d'IA s'exécutent, la manière dont les données sont traitées et les personnes ou entités qui y ont accès, est devenue une exigence de sécurité critique. Sans elle, les entreprises élargissent leur surface d'attaque et créent des dépendances susceptibles de retarder la détection et le confinement.

Les recherches de cette année, menées par le Ponemon Institute et sponsorisées, analysées et publiées par IBM, ont porté sur 602 entreprises touchées par des violations de données entre mars 2025 et février 2026. (Les années mentionnées dans ce rapport correspondent à l'année de publication du rapport, et pas nécessairement à l'année de la violation.) Ensemble, nous avons étudié des entreprises issues de 17 secteurs, réparties dans 16 pays et régions, ainsi que des violations ayant compromis entre 2 590 et 115 380 enregistrements.

Ponemon a interrogé 3 558 responsables de la sécurité et dirigeants d'entreprise ayant une connaissance directe des incidents de violation survenus dans leur entreprise. Ces dirigeants comprenaient des PDG, des RSSI, des directeurs des opérations, des contrôleurs ou des directeurs financiers, des professionnels de l'informatique, des responsables d'unités commerciales et des directeurs généraux, ainsi que des spécialistes de la gestion des risques et de la cybersécurité.

Les constats et analyses du rapport de cette année peuvent aider les responsables métier, technologiques, sécurité et risques à renforcer leurs défenses, éclairer l'allocation des ressources et stimuler l'innovation. Pour progresser face aux nouvelles menaces rendues possibles par l'IA de pointe, il est utile que les dirigeants comprennent le point de départ des équipes de sécurité. Que font bien les équipes des centres des opérations de sécurité (SOC), et quels domaines doivent être améliorés ? Le rapport sur le coût d'une violation de données de cette année dresse ce tableau avec une grande précision.

Nouveautés du rapport 2026

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. Pour la première fois, les recherches de cette année ont exploré les points suivants :

- Domaines d'utilisation de l'IA agentique dans le SOC
- Types de contrôles utilisés pour sécuriser les identités non humaines
- Prévalence des technologies de chiffrement pour sécuriser les données
- Prévalence des projets de cryptographie post-quantique
- Types de contrôles destinés à sécuriser la cryptographie
- Réduction du coût des violations grâce à l'utilisation d'outils de gestion du cycle de vie des secrets

Principaux enseignements

4,99 millions USD

Coût moyen global d'une violation de données

Le coût moyen mondial d'une violation de données a augmenté de 12 % par rapport à l'an dernier, atteignant un record de 4,99 millions USD. Autrement dit, cela représente un coût de 1 100 USD par heure. Deux catégories de coûts (détection et escalade, ainsi que perte d'activité) ont représenté la majorité des coûts dans le rapport de cette année, soit 63 %. Ces coûts couvrent aussi bien la gestion de crise que les interruptions d'activité et l'attrition client. Aux États-Unis, où les amendes réglementaires et autres coûts pour les entreprises sont plus élevés, le coût moyen d'une violation de données a dépassé celui de tous les autres pays et régions étudiés, atteignant un record de 11,5 millions USD. C'est plus du double de la moyenne mondiale, et une hausse de 13 % par rapport à l'an dernier.

56 %

Augmentation des attaques générées par l'IA

Les cybercriminels instrumentalisent de plus en plus l'IA, en l'utilisant pour automatiser le cycle de vie des attaques, industrialiser leurs opérations et affiner la sophistication de leurs méthodes. Les recherches de cette année en montrent l'impact : plus d'une entreprise sur quatre ayant subi une attaque malveillante a déclaré qu'elle était pilotée par l'IA, soit une hausse de 56 % par rapport à l'an dernier. L'usurpation d'identité par deepfake IA et les logiciels malveillants dopés à l'IA ont représenté les volumes les plus élevés parmi ces incidents. Conséquence financière : les attaques pilotées par l'IA ont ajouté en moyenne 1 million USD au coût de chaque violation.

6 millions USD

Coût moyen des attaques par inversion de modèle d'IA

Les cybercriminels n'utilisent pas seulement l'IA comme un outil : ils ciblent aussi les modèles et applications d'IA sur lesquels les entreprises s'appuient de plus en plus. Les types d'incidents de sécurité les plus coûteux impliquant le modèle ou les applications d'IA d'une entreprise ont été les attaques par inversion de modèle et par injection de prompt, qui ont entraîné des pertes moyennes de respectivement 6,07 millions USD et 5,89 millions USD. Ces types d'attaques illustrent la difficulté croissante à protéger les données d'entraînement, à contrôler le comportement des modèles et à sécuriser les résultats sensibles. Contrairement aux exploits traditionnels qui compromettent des systèmes, ces attaques comportementales fragilisent la manière dont les modèles d'IA raisonnent et répondent, élargissant ainsi le périmètre de résolution au-delà de la seule reprise technique, pour inclure la confiance et la gouvernance.

92 %

Part des entreprises ayant signalé une violation liée à l'IA et ne disposant pas de contrôles d'accès appropriés pour l'IA

Parmi les entreprises ayant subi une violation liée à l'IA, l'immense majorité, soit 92 %, ne disposait pas de contrôles d'accès appropriés pour l'IA. Et ce, alors même que les entreprises indiquent que la gestion des identités et des accès compte parmi les leviers les plus efficaces pour réduire les coûts des violations de manière générale. Alors que les systèmes d'IA se développent et s'intègrent plus profondément aux workflows des entreprises, les contrôles d'identité et d'accès n'ont pas suivi le rythme. Dans le rapport de cette année, seules 40 % des entreprises ont déclaré utiliser des contrôles d'accès sur les modèles et données d'IA. Le résultat est prévisible : davantage de voies d'attaque, un impact financier plus élevé et des incidents causés par des lacunes élémentaires d'application des règles, qui ne nécessitent même pas de sophistication particulière de la part des cybercriminels.

41 %

Part des attaques par ransomware qui incluaient des menaces contre la réputation de la marque

Les incidents de ransomware parmi les entreprises victimes d'une violation ont légèrement augmenté cette année par rapport à l'an dernier (passant de 34 % à 39 %), les cybercriminels utilisant l'IA pour générer des logiciels malveillants et élargissant leurs méthodes d'extorsion. Si la perturbation des opérations par chiffrement reste une tactique clé (citée dans 23 % des cas), les cybercriminels se tournent vers des méthodes de pression à plus fort impact. Menacer la réputation de la marque est désormais la tactique la plus courante, citée par 41 % des entreprises victimes d'une violation ayant subi un incident de ransomware. Cette évolution traduit un glissement d'une perturbation purement technique vers des stratégies d'extorsion multicouches ciblant la confiance, la perception publique et l'impact à long terme sur l'entreprise.

6,29 millions USD

Coût moyen d'une violation dans le secteur des services financiers

Les secteurs critiques subissent de plein fouet les attaques pilotées par l'IA, représentant 62 % de toutes les violations liées à l'IA étudiées. Les deux secteurs les plus ciblés ont été les services financiers et l'énergie, où les coûts moyens d'une violation ont atteint respectivement 6,29 millions USD et 5,2 millions USD. Cette tendance ciblée est préoccupante. La concentration des attaques pilotées par l'IA dans ces deux secteurs interdépendants crée un risque systémique. Les perturbations touchant une entreprise peuvent entraîner des répercussions plus larges sur les finances des consommateurs, les systèmes économiques et les réseaux électriques. Point positif : ces deux secteurs ont de l'expérience dans l'identification et le confinement des violations, avec des durées moyennes de violation environ quatre semaines plus courtes que la moyenne mondiale.

85 %

Part des entreprises prévoyant d'augmenter leurs dépenses de sécurité en réponse aux menaces des modèles d'IA de pointe

Initialement, 64 % des entreprises déclaraient qu'elles augmenteraient leurs dépenses de sécurité après avoir subi une violation. Après avoir pris connaissance des nouvelles menaces émanant des modèles d'IA de pointe, ce chiffre a fortement augmenté pour atteindre 85 %. Ces nouvelles menaces ont également conduit les entreprises à repenser l'utilisation des agents d'IA dans la sécurité. Trois quarts d'entre elles ont indiqué qu'elles déploieraient davantage d'agents pour le triage des alertes, la gestion des vulnérabilités, ainsi que les analyses et les tests d'intrusion.

1,93 million USD

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

Les équipes de sécurité qui utilisent largement l'IA et l'automatisation ont réduit la durée de leurs violations de 65 jours et abaissé leurs coûts moyens de 1,93 million USD par rapport à celles qui n'utilisent pas ces solutions. Ces économies renforcent l'idée que les opérations de sécurité modernes doivent fonctionner à la vitesse de la machine. Cependant, seules environ un tiers des entreprises victimes d'une violation (36 %) ont déclaré utiliser largement ces outils tout au long du cycle de vie de la sécurité, de la prévention à la détection, en passant par l'investigation et la réponse. Leur utilisation en prévention reste en retrait par rapport aux workflows de détection et d'investigation.

50 %

Part des entreprises déployant des agents d'IA dans leur SOC

Si l'IA et l'automatisation restent parmi les moyens les plus efficaces de réduire l'impact des violations, leur adoption tout au long du cycle de vie de la sécurité demeure inégale. Elles sont le plus souvent utilisées pour la détection et l'investigation, tandis que leur usage en prévention reste en retrait. L'adoption de l'IA agentique suit le même schéma irrégulier. Parmi la moitié des entreprises victimes d'une violation déclarant déployer des agents dans leurs opérations de sécurité, plus de 50 % les consacrent à la chasse aux menaces, à la réponse et au confinement. Seules 18 % utilisent des agents d'IA pour l'analyse et la gestion des vulnérabilités, une application qui pourrait contribuer à réduire l'exposition en amont et potentiellement atténuer l'impact des menaces liées aux IA de pointe.

Recommandations

Alors que les modèles d'IA de pointe réduisent considérablement le délai entre la découverte d'une vulnérabilité et son exploitation (faisant passer les attaques de la vitesse humaine à la vitesse machine) le coût du retard se mesurera en minutes, et non en mois.

Les défaillances liées aux retards de détection, aux lacunes de confinement, aux mouvements latéraux, aux abus d'identifiants et à la lenteur décisionnelle sont désormais exponentiellement plus dommageables et coûteuses pour les entreprises.
Les recherches de cette année le confirment.

Pour aider à prévenir, atténuer et réduire les coûts d'une violation de données, et se préparer à l'ère de la sécurité à vitesse machine, les experts IBM recommandent les quatre approches efficaces suivantes.

Faire fonctionner la sécurité à la nouvelle vitesse de l'attaque

D'ici deux ans, les experts s'attendent à ce que l'IA favorise les cybercriminels par rapport aux équipes de défense à hauteur de 31,7 %.[1] Cette projection met en évidence la menace croissante que représentent les attaques pilotées par l'IA et la nécessité d'accélérer la sécurité. Cette vitesse peut être obtenue grâce à l'utilisation de l'IA et des agents. Si la plupart des entreprises n'appliquent l'IA qu'à des domaines limités des opérations de sécurité, le plus souvent la détection des menaces, elles devraient étendre son usage de manière globale à tous les aspects des opérations de sécurité.

Un bon point de départ consiste à appliquer l'IA agentique à la gestion des vulnérabilités. Ce domaine est devenu une cible facile en raison des capacités des modèles d'IA de pointe à identifier des vulnérabilités critiques dans les principaux systèmes d'exploitation et navigateurs web. En intégrant l'IA à l'ensemble du cycle de vie de la sécurité, les entreprises peuvent transformer leurs programmes de sécurité en systèmes cohérents capables d'assurer une défense continue et autonome.

Cette approche consiste à exploiter l'IA pour analyser les expositions, appliquer les politiques et coordonner la détection et le confinement avec une intervention humaine minimale, afin de réduire les fenêtres d'exposition et d'accélérer le confinement des attaques à haute vélocité. En adoptant ces mesures de sécurité pilotées par l'IA, les entreprises peuvent renforcer leur résilience, rationaliser leur conformité et s'assurer qu'elles sont bien équipées pour réagir rapidement face aux menaces dopées à l'IA.

Faire évoluer la sécurité des identités vers une vérification continue à l'exécution

La sécurité des identités reste sous-financée malgré les preuves croissantes de son importance critique. Parmi les entreprises ayant subi des violations liées à l'IA dans l'étude de cette année, 92 % ne disposaient pas de contrôles d'accès appropriés.
Ce constat révèle une défaillance systémique : l'identité n'est pas traitée comme une infrastructure critique. Dans la course au déploiement d'agents d'IA pour automatiser les processus métier (y compris les opérations de sécurité chargées de défendre les organisations contre les modèles d'IA de pointe), les équipes doivent transformer en profondeur leurs systèmes d'identité afin de sécuriser non seulement les humains, mais aussi les identités non humaines.

Cette transformation de l'identité nécessitera :
- La découverte et l'intégration des agents
- La délégation de l'authentification et l'autorisation
- La détection des anomalies et la résolution des risques
- Les contrôles de gouvernance et de cycle de vie

Cette transformation remplacera les approches héritées par des principes modernes de confiance zéro. Les systèmes d'identité pourront alors contribuer à garantir que les agents d'IA opèrent en toute sécurité dans les garde-fous prévus, grâce à des accès juste-à-temps, des approbations limitées dans le temps et des contrôles continus à l'exécution fondés sur le risque, appliqués aux appareils, utilisateurs et workloads. La sécurité des identités, qui peut être renforcée par des outils et services de sécurité autonomes, doit fonctionner sans friction et à la vitesse de la machine. Les entreprises qui opèrent cette transition peuvent adopter l'IA à grande échelle en toute sécurité, répondre aux exigences réglementaires et obtenir des avantages concurrentiels significatifs.

Renforcer le contrôle de l'IA grâce à la souveraineté de l'IA

Alors que les entreprises déploient l'IA à grande échelle sur des plateformes, dans le cloud et au sein d'écosystèmes, elles peuvent perdre le contrôle de la manière dont les modèles fonctionnent, ainsi que de la façon dont les données sont transformées et consultées. Ce défi accroît le risque de violations et complique les réponses à y apporter. C'est pourquoi la souveraineté de l'IA, c'est-à-dire le maintien du contrôle sur l'endroit où les systèmes d'IA s'exécutent, la manière dont les données sont traitées et les personnes ou entités qui y ont accès, est désormais un impératif de sécurité critique.

La souveraineté de l'IA doit inclure une posture de sécurité couvrant les données, les applications, les identités et les environnements cloud dans lesquels l'IA s'exécute et est utilisée. Cette sécurité doit être globale, et non fragmentaire. Elle doit inclure trois dimensions : renforcer la sécurité des applications et des API, appliquer des contrôles d'identité fiables pour les utilisateurs, les données et les agents machine, et s'assurer que les workloads cloud sont correctement configurés et surveillés.

Surveiller la manière dont les données entrent dans les systèmes d'IA, s'y transforment et en sortent peut aider les entreprises à identifier de manière proactive les risques d'exposition des données sensibles, à renforcer la gouvernance et la conformité de l'IA, et à déployer l'IA à grande échelle en toute sécurité.

En unifiant ces couches (au moyen d'approches intégrées), les entreprises peuvent mieux réduire le risque systémique et renforcer la confiance dans le déploiement de l'IA à l'échelle. Établir le contrôle implique de limiter les mouvements de données inutiles, de sécuriser les intégrations avec des outils et modèles externes, et de maintenir une visibilité claire sur les workloads. Cela signifie renforcer la sécurité des applications et des API, et s'assurer que les workloads cloud sont configurés et surveillés avec rigueur.

Se préparer aux menaces de sécurité post-quantiques

Les lacunes fondamentales en matière de chiffrement et de gestion de la cryptographie exposent les entreprises, alors même que les investissements dans la sécurité résistante au quantique commencent à augmenter. Par exemple, seules 37 % des entreprises victimes d'une violation ont déclaré chiffrer les données sensibles au moment de la violation. Dans le même temps, seules 34 % ont déclaré disposer de contrôles permettant de surveiller et de sécuriser les actifs cryptographiques, tels que les clés et les certificats, dans l'ensemble de leurs environnements.

La cryptographie touche tous les aspects du monde numérique, des protocoles Internet aux applications d'entreprise, en passant par les infrastructures critiques et les systèmes financiers. Pour gérer efficacement la cryptographie à l'ère quantique, les entreprises devraient commencer à passer à des algorithmes de chiffrement post-quantiques et à moderniser leurs pratiques de cybersécurité.

Pour accélérer la transition vers la cryptographie post-quantique, instaurer la crypto-agilité et sécuriser les données dans les environnements hybrides et l'IA, les entreprises doivent commencer à bâtir une posture de sécurité robuste. Cette posture leur permettra de découvrir la cryptographie présente dans leur environnement, d'analyser les vulnérabilités et de remédier aux risques. Cette transition peut être complexe et dépendre des besoins propres à chaque entreprise. Il peut donc être utile de s'appuyer sur des experts capables de comprendre les besoins et processus uniques de l'entreprise et de guider sa migration vers une sécurité résistante au quantique.

Lire le rapport complet →

À propos

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. Ponemon a pour mission 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 de données personnelles (PII) 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

IBM

En tant que l'un des principaux fournisseurs 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 sur ibm.com/fr-fr/security.

Participez à la conversation dans la communauté IBM Security.

1. Frontier AI's Impact on the Cybersecurity Landscape, UC Berkeley, 27 novembre 2025.