Kong

Powering the API world

Sécurité des API Perspectives 2025

Menaces renforcées par l'IA et sécurité des API

Résumé exécutif

83 % des développeurs et des chefs d'entreprise ont déclaré que les investissements dans l'IA avaient déjà créé l'opportunité de nouveaux produits ou services, selon le rapport d'impact des API 2024 de Kong.

Mais de quoi s'inquiètent les dirigeants informatiques ? Qu'ont-ils observé jusqu'à présent en ce qui concerne les incidents de sécurité des API et les menaces renforcées par l'IA ?

Notre dernière enquête menée auprès de 700 responsables informatiques révèle un point d'inflexion critique dans la sécurité des API alors que les organisations font face au risque croissant de menaces renforcées par l'IA et à l'adoption d'outils d'IA et de grands modèles linguistiques (LLM).

Près de 75 % des personnes interrogées expriment de sérieuses inquiétudes concernant l'IA améliorée attaques, mais un décalage notable est apparu. Alors que 55 % des organisations ont connu un incident de sécurité des API au cours de l'année écoulée, 85 % d'entre elles déclarent avoir confiance dans les capacités de sécurité de leur organisation.

Cette confiance est peut-être mal placée, étant donné que 77 % reconnaissent le potentiel de risques de sécurité importants liés à l'intégration de l'IA et du LLM dans leur écosystème API.

De plus, le coût des incidents de sécurité des API est substantiel, 20 % d'entre eux signalant des coûts de correction supérieurs à 500 000 $ au cours des 12 derniers mois.

D'autres conclusions clés incluent :

- 40 % ne sont pas sûrs que leurs investissements actuels en matière de sécurité soient suffisants pour faire face risques émergents liés à l'IA
- Les cyberattaques renforcées par l'IA sont classées comme la principale menace pour la sécurité
- 92 % prennent des mesures pour lutter contre Menaces renforcées par l'IA
- Les API fantômes peuvent constituer un angle mort dangereux pour la majorité des organisations

Bien que les organisations reconnaissent l'évolution du paysage des menaces, beaucoup d'entre elles ne disposent pas des mesures de sécurité complètes nécessaires pour protéger leur infrastructure API dans l'IA.
ère.

L'écart entre la perception et la réalité nécessite une attention particulière, en particulier dans la mesure où les attaques d'API devraient augmenter – et les violations d'API entraînent davantage de fuites de données que la réalité.
violation de sécurité moyenne, rapporte Gartner.

Menaces renforcées par l'IA et incidents de sécurité des API

Kong a interrogé 700 responsables informatiques sur la sécurité des API et le risque croissant de menaces renforcées par l'IA.

88%

rapporte que la sécurité des API est une priorité absolue

Les responsables informatiques affirment que la sécurité des API est une préoccupation majeure en matière de sécurité

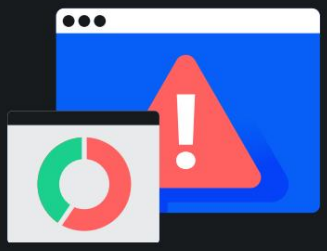
97 % considèrent que la sécurité des API est supérieure ou égale à d'autres préoccupations en matière de cybersécurité, comme la sécurité du réseau et la sécurité des terminaux.

Les incidents de sécurité des API sont

commun — et cher 8% 55%

Plus de la moitié ont vécu un Incident de sécurité des API au cours des 12 derniers mois ; 27 % manquent de confiance dans leurs mesures de sécurité des API.

expérimenté une API incident de sécurité dans l'année dernière



Près de la moitié des personnes ayant vécu un incident ont passé plus de

100 000 $

en remédiation

47 % des personnes ayant subi un incident de sécurité des API au cours des 12 derniers mois ont signalé des coûts de correction supérieurs à 100 000 $; 20 % ont signalé des coûts supérieurs à 500 000 $.

Les dirigeants manquent de confiance dans leur capacité à stopper les menaces renforcées par l'IA

Les attaques renforcées par l'IA arrivent en tête de liste des plus grandes menaces perçues pour la sécurité des API aujourd'hui, suivies par les accès/violations non autorisés et la protection/le cryptage insuffisant des données.

74%

sont très préoccupés par Attaques renforcées par l'IA

92%

prennent des mesures pour contrer les attaques renforcées par l'IA

40%

ne sont pas confiants dans leur investissements de sécurité actuels

Kong Inc., un développeur leader de technologies d'API cloud, a pour mission de permettre aux entreprises du monde entier de devenir « API-first » et d'accélérer en toute sécurité l'adoption de l'IA. Kong aide les organisations du monde entier, des startups aux entreprises Fortune 500, à optimiser la productivité des développeurs, à créer en toute sécurité et à accélérer la mise sur le marché. Pour plus d'informations, visitez www.konghq.com.

Sécurité des API et risque croissant de menaces renforcées par l'IA

Les API (interfaces de programmation d'applications) rendent notre monde numérique possible. Il n'y a pas d'IA sans API, mais même les interactions en ligne les plus basiques, comme la commande de pizza ou la planification d'itinéraires de transports en commun, sont alimentées par des API.

Cependant, sans une gestion, une visibilité et des processus appropriés, les API peuvent constituer une faille potentielle dans votre sécurité.

Rapports de Gartner la violation moyenne d'API entraîne au moins 10 fois plus de fuites de données que la violation de sécurité moyenne. Et Kong prévoit Les attaques API sont en augmentation, avec une croissance prévue de 548 % du nombre d'attaques d'ici 2030.

L'adoption rapide de la technologie de l'IA et des grands modèles linguistiques (LLM) conduit à des innovations jusqu'alors insondables, mais a également entraîné une refonte totale du paysage des menaces de cybersécurité.

Comment ces nouveaux outils et menaces améliorés par l'IA impactent-ils la sécurité des API ? Et quelles sont les préoccupations des dirigeants informatiques pour l'année à venir ?

Pour le savoir, nous avons interrogé 700 responsables informatiques aux États-Unis et au Royaume-Uni sur le rôle de l'IA dans le paysage actuel de la sécurité des API.

Les menaces renforcées par l'IA figurent en tête de liste des menaces potentielles pour la sécurité

L'IA peut réduire la barrière à l'entrée des cyberattaques et fournit un autre vecteur d'attaque pour potentiellement percer les défenses organisationnelles autour de la sécurité des API. Et comme de nombreuses technologies s'appuient sur les API, les attaques API peuvent avoir un impact croissant sur la sécurité des données.

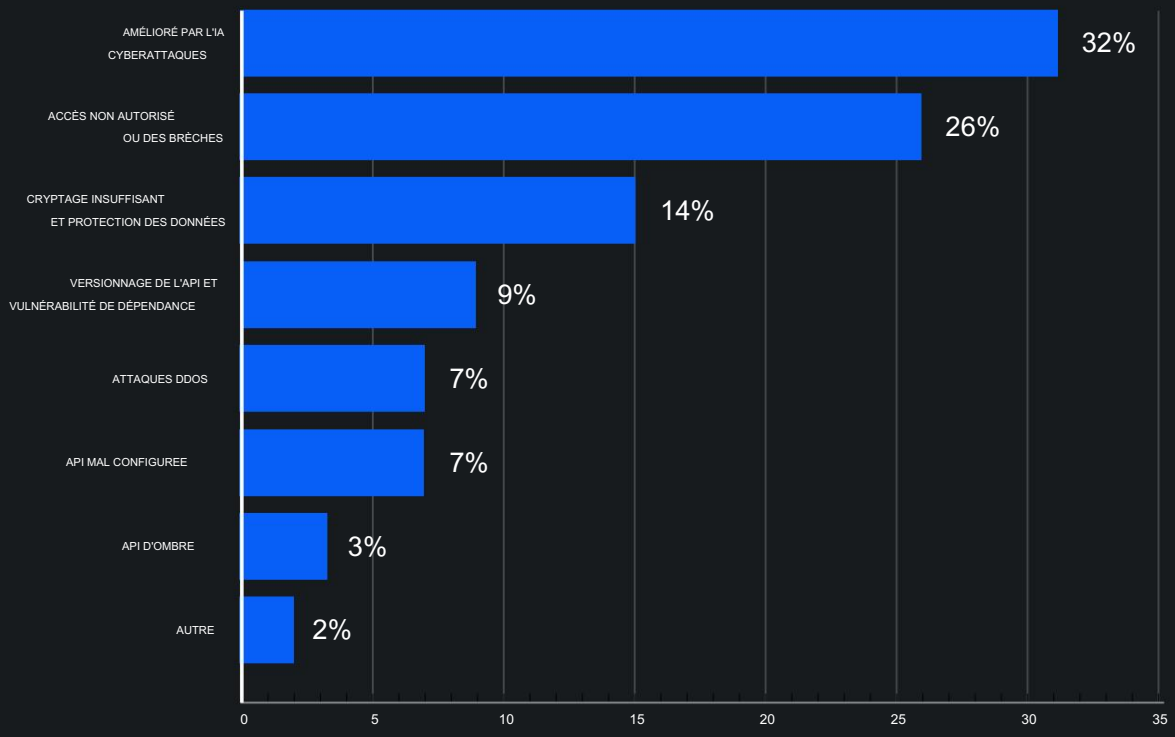
Les professionnels du secteur technologique sont clairement conscients du risque : 74 % d'entre eux se disent extrêmement ou très préoccupés par les attaques renforcées par l'IA, et 32 % affirment qu'elles constituent la plus grande menace pour la sécurité des organisations aujourd'hui. Ces types d'attaques arrivent en tête de liste des menaces les plus importantes pour la sécurité des API aujourd'hui, suivies par les accès non autorisés ou les violations.

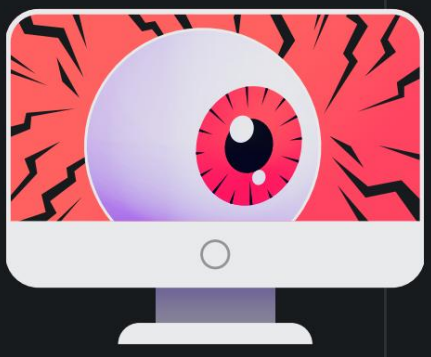
74%

sont extrêmement ou très préoccupés par

Attaques renforcées par l'IA

Quelle est la plus grande menace de sécurité pour votre organisation aujourd'hui ?





Mettre en lumière le risque des API fantômes

Même si les API fantômes sont moins bien perçues comme des menaces, ces API non découvertes et non gérées peuvent représenter des risques de sécurité considérables dans les organisations qui ne disposent pas d'un système d'enregistrement des services et des API à jour. Comme le rapporte Gartner dans le Market Guide for API Protection 2024, « les API, en particulier celles qui sont fantômes et dormantes, provoquent des violations de données au sein des organisations qui, en moyenne, dépassent l'ampleur des autres violations ».

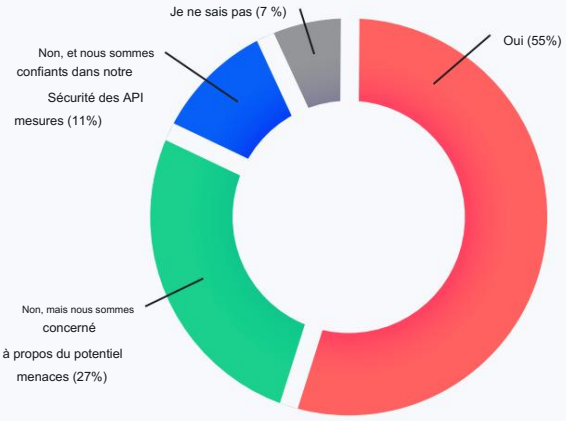
Il est essentiel d'avoir une visibilité sur les services et les API. Parmi les dizaines de milliers de points de terminaison d'API qui peuvent s'exécuter dans l'infrastructure d'une organisation, chacun peut être considéré comme un vecteur d'attaque unique, en particulier s'il n'est pas protégé, sans authentification, autorisation et limitation de débit.

En savoir plus sur la façon de mettre en lumière les API fantômes se cache dans votre infrastructure informatique.

La moitié d'entre eux ont connu un incident de sécurité API au cours des 12 derniers mois

55 % des entreprises interrogées ont signalé un incident de sécurité des API au cours des 12 derniers mois, et un tiers d'entre elles ont déclaré qu'il était « grave ». Seuls 11 % n'ont pas connu d'incident, mais continuent de faire confiance à leurs mesures de sécurité des API.

Avez-vous rencontré un problème de sécurité API incident au cours des 12 derniers mois ?



32%

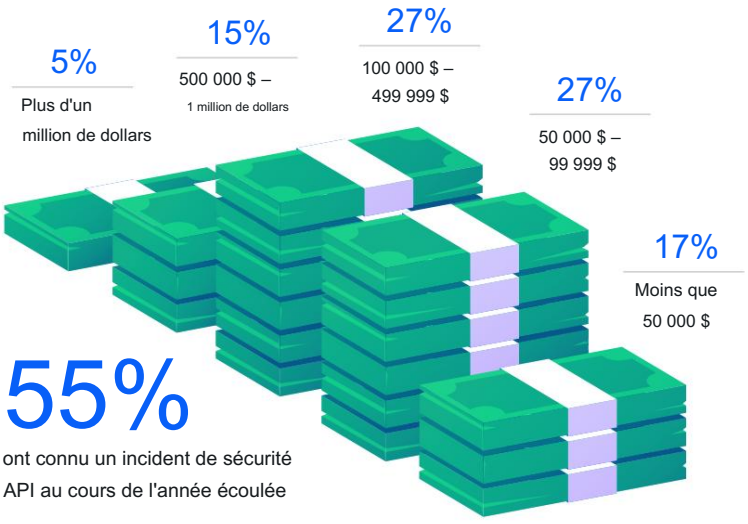
ceux qui ont vécu un incident API disent que c'était « grave »

1 personne sur 5 signale un incident de sécurité API coûtant plus de 500 000 $

47 % des personnes ayant subi un incident au cours des 12 derniers mois ont déclaré des coûts de réparation supérieurs à 100 000 $; 20 % déclarent que leur organisation a payé plus de 500 000 $.

Ces coûts prennent en compte les ressources internes, telles que les heures travaillées, et les ressources externes, comme le conseil, les outils de sécurité et les frais juridiques.

Coût de la résolution d'un incident de sécurité API au cours des 12 derniers mois



55%

ont connu un incident de sécurité API au cours de l'année écoulée

9 % n'étaient pas sûrs ou préféraient ne pas le dire

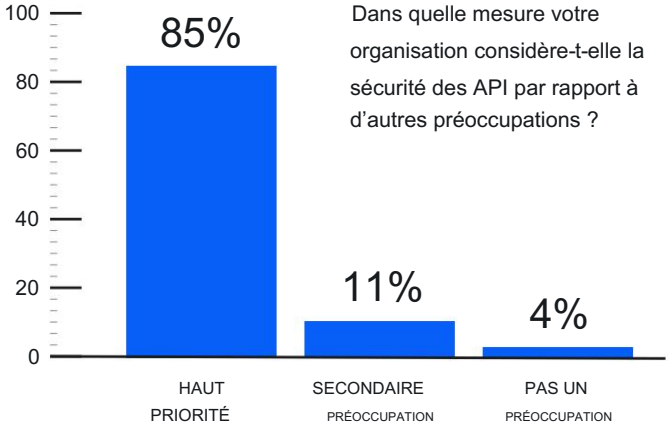
Il existe un décalage surprenant entre la confiance et le nombre d'incidents de sécurité

Malgré le nombre de personnes qui ont récemment été victimes d'une attaque et qui ont dû faire face aux coûts qui en découlent, la plupart d'entre elles sont confiantes dans leur capacité à sécuriser les API contre les menaces actuelles et émergentes. S'agit-il d'un faux sentiment de sécurité ou les organisations ont-elles redoublé d'efforts après les incidents précédents ? Seul le temps nous le dira.

85%

ont confiance en leur leur capacité à sécuriser les API

4% ne sont pas confiants ; 11% sont neutres



Dans quelle mesure votre organisation considère-t-elle la sécurité des API par rapport à d'autres préoccupations ?

La plupart considèrent la sécurité des API comme une priorité absolue en matière de cybersécurité.

préoccupation

97 % considèrent la sécurité des API comme une préoccupation de cybersécurité supérieure ou relative à d'autres, telles que la sécurité du réseau et la sécurité des terminaux.

40 % ne sont pas sûrs que l'investissement de leur organisation c'est suffisant

45 % des personnes déclarent que plus de 20 % de leur budget de cybersécurité est consacré à la sécurité des API, et 40 % ne sont pas sûres ou doutent que l'investissement de leur organisation soit suffisant pour couvrir les risques de sécurité des API, en particulier à la lumière des nouveaux projets d'IA et des menaces renforcées par l'IA.

40%

ne sont pas sûrs que l'investissement de leur organisation soit suffisant pour couvrir les risques de sécurité des API

Les organisations s'appuient sur la surveillance et les passerelles API pour maintenir le contrôle

En ce qui concerne les mesures préventives prises par les organisations pour atténuer les risques de sécurité des API, les outils de surveillance des API et de détection des anomalies arrivent en tête de liste. En comparant le Royaume-Uni et les États-Unis, les répondants britanniques sont plus susceptibles de déclarer avoir mis en œuvre une passerelle API : 71 % au Royaume-Uni contre 50 % aux États-Unis. Cette différence peut être due à des exigences réglementaires et de conformité plus strictes au Royaume-Uni.

Quelles mesures prenez-vous pour atténuer les risques de sécurité des API ?

1. OUTILS DE SURVEILLANCE API ET DE DÉTECTION D'ANOMALIES (63%)
2. MISE EN ŒUVRE DE SOLUTIONS DE PASSERELLE API (61 %)
3. CRYPTAGE ET TOKENISATION API (58%)
4. TESTS DE PÉNÉTRATION ET AUDITS RÉGULIERS (57 %)
5. ADOPTER UNE ARCHITECTURE ZERO-TRUST (35 %)
6. NE PAS PRENDRE DE MESURES SPÉCIFIQUES (6 %)

Seuls 35 % déclarent adopter une architecture Zero Trust, ce qui est surprenant étant donné à quel point cette approche globale de la sécurité des API est établie et généralement acceptée comme une bonne pratique.

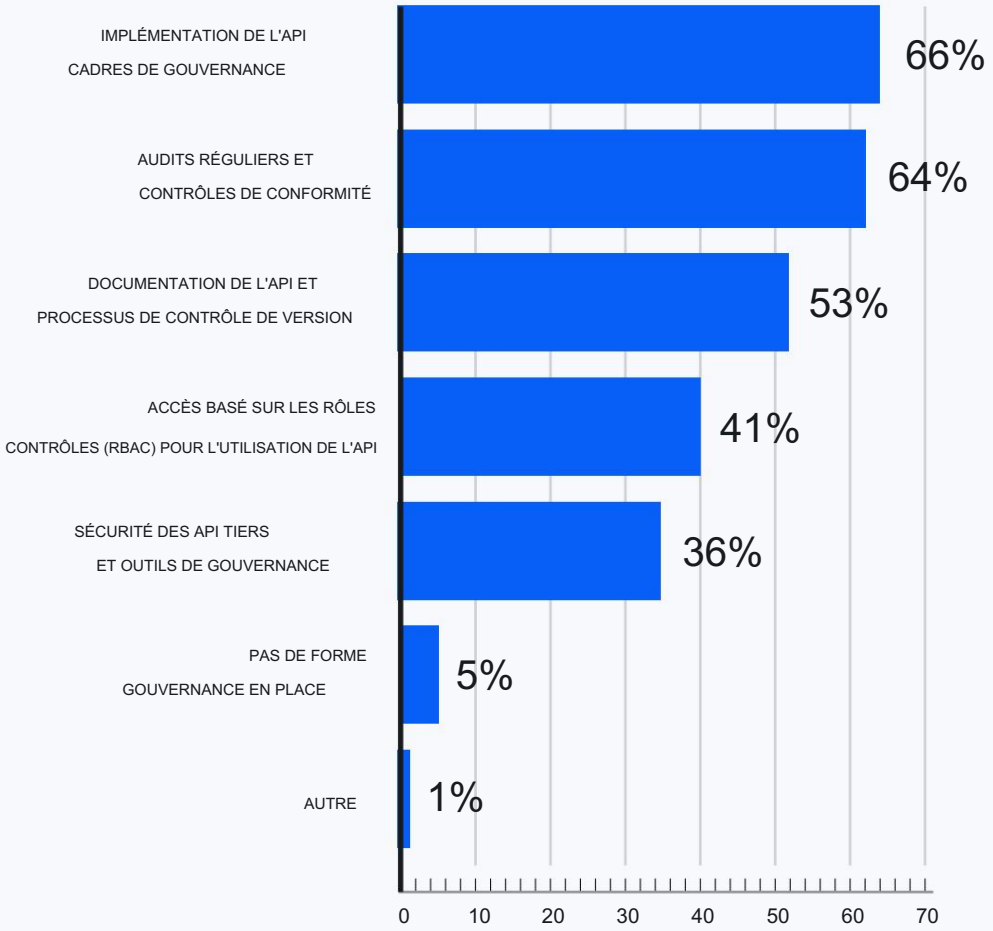
92 % prennent des mesures pour sécuriser les API contre Menaces renforcées par l'IA

L'amélioration de la surveillance et de l'analyse du trafic figure en tête de liste des mesures prises par les organisations pour sécuriser les API contre les menaces renforcées par l'IA. Il existe une différence notable entre le sérieux avec lequel les organisations au Royaume-Uni et aux États-Unis semblent considérer les menaces renforcées par l'IA : 13 % aux États-Unis déclarent ne prendre aucune mesure spécifique contre les menaces renforcées par l'IA, contre seulement 4 % au Royaume-Uni.

Quelles mesures prenez-vous pour sécuriser les API contre les menaces renforcées par l'IA ?

1. SURVEILLANCE ACCRUE ET ANALYSE DU TRAFIC (66%)
2. PERSONNEL ÉDUCATIF (60%)
3. DÉTECTION DES MENACES PAR L'IA SYSTÈMES (51%)
4. EXPLOITER LES SOLUTIONS DE SÉCURITÉ API AVEC CAPACITÉS IA/ML (44 %)
5. PARTENARIAT AVEC DES SERVICES DE SÉCURITÉ TIERS ENTREPRISES DE DÉTECTION ET D'ATTÉNUATION DES MENACES (40 %)
6. AUCUN (8%)

Comment gérez-vous la sécurité des API pour garantir la conformité avec les politiques internes et les réglementations externes ?



Cadres de gouvernance des API, audit des principaux efforts axés sur la conformité

Pour gérer la sécurité des API afin de garantir la conformité avec les politiques internes et les réglementations externes (par exemple, RGPD, HIPAA), les organisations s'appuient sur des cadres de gouvernance des API, des audits et des contrôles réguliers, ainsi que sur des processus de documentation et de contrôle des versions des API.

Les modèles d'IA et les LLM compliquent la sécurité et introduisent des vulnérabilités

77 % affirment qu'il existe un risque important que les modèles d'IA tels que les LLM puissent introduire des vulnérabilités de sécurité lorsqu'ils sont intégrés à leur écosystème API.

25%

ont rencontré

Menaces de sécurité renforcées par l'IA liées aux API ou aux LLM

65%

élaborent une stratégie ou se préparent à faire face aux menaces de sécurité renforcées par l'IA

84%

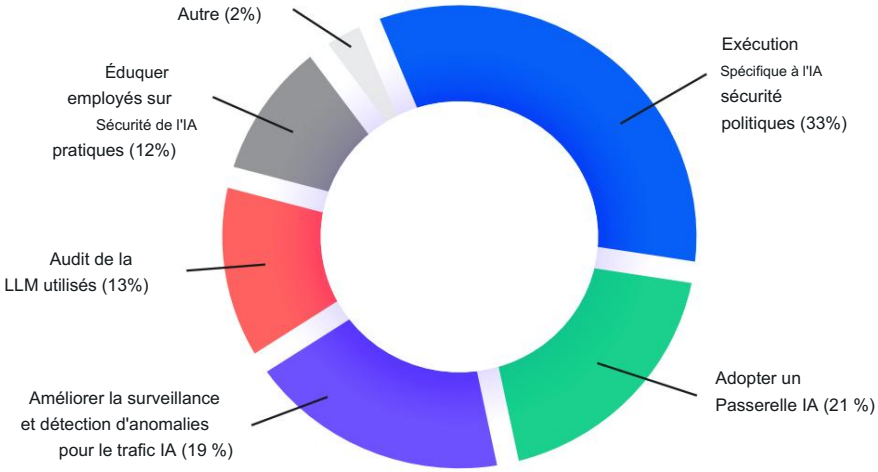
disent que l'IA et les LLM vont augmenter complexité de la sécurisation des API

au cours des 2 à 3 prochaines années

À mesure que l'utilisation de l'IA augmente au sein des organisations, il sera crucial de bloquer les attaques externes renforcées par l'IA et de gérer et sécuriser correctement le trafic généré par l'IA résultant de nouvelles initiatives. Pour atténuer ces risques, les responsables informatiques déclarent mettre en œuvre des politiques de sécurité spécifiques à l'IA, adopter une passerelle IA, et améliorer la surveillance et la détection des anomalies pour le trafic IA.

Une passerelle IA est un endroit central pour gérer la consommation d'IA qui peut être utilisée pour accélérer l'adoption de l'IA sans compromettre l'observabilité, la sécurité et gouvernance.

Comment votre organisation planifie-t-elle pour atténuer les risques liés à l'IA ?



Mise en œuvre sécurisée L'IA et le maillon faible

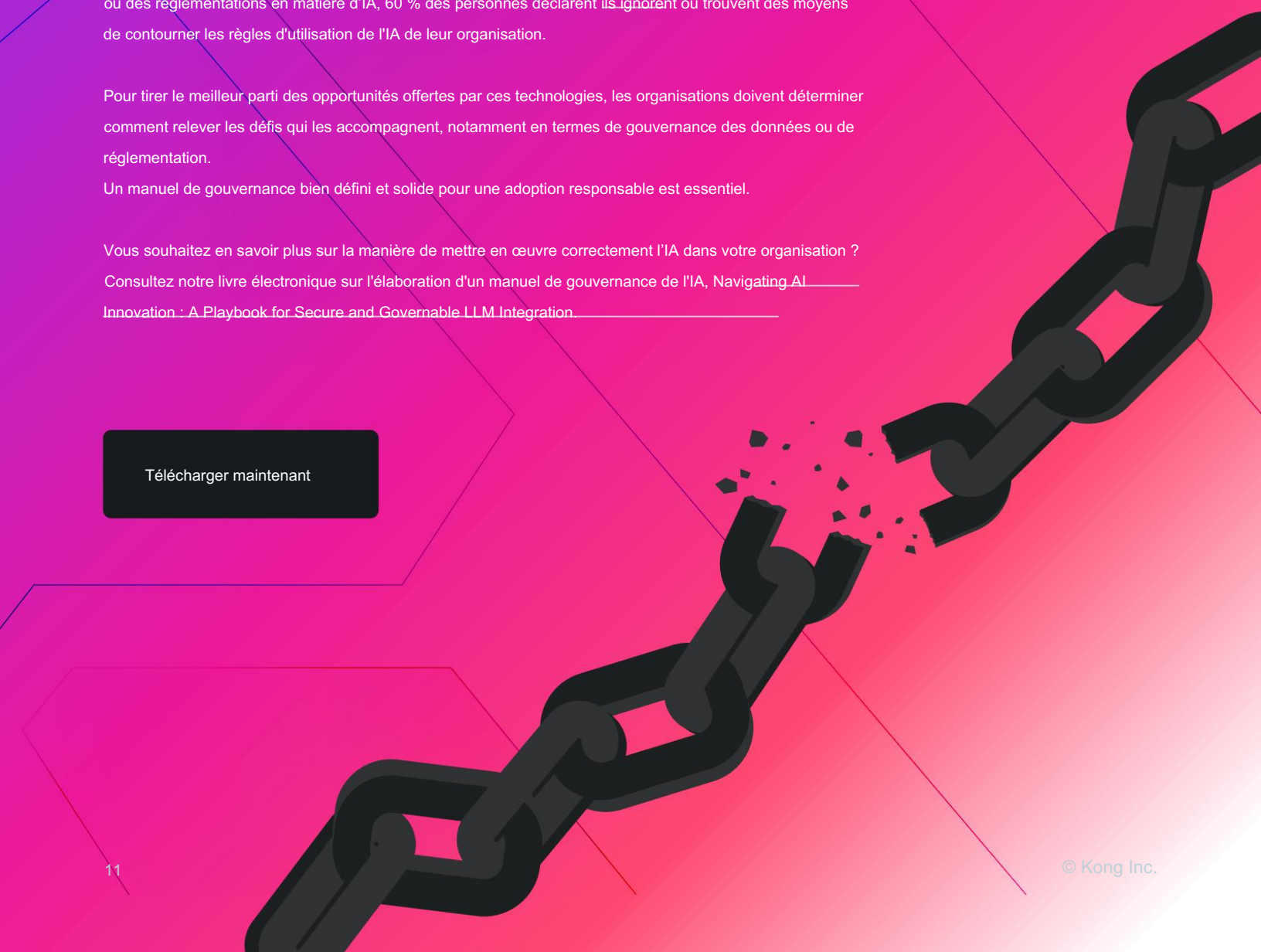
Les humains restent l'un des points faibles de la cybersécurité, il est donc judicieux d'investir de l'énergie dans l'éducation aux meilleures pratiques autour de GenAI et des LLM.

Mais l'éducation seule ne suffit pas. Bien que la plupart des organisations aient mis en place des directives ou des réglementations en matière d'IA, 60 % des personnes déclarent ils ignorent ou trouvent des moyens de contourner les règles d'utilisation de l'IA de leur organisation.

Pour tirer le meilleur parti des opportunités offertes par ces technologies, les organisations doivent déterminer comment relever les défis qui les accompagnent, notamment en termes de gouvernance des données ou de réglementation.
Un manuel de gouvernance bien défini et solide pour une adoption responsable est essentiel.

Vous souhaitez en savoir plus sur la manière de mettre en œuvre correctement l'IA dans votre organisation ? Consultez notre livre électronique sur l'élaboration d'un manuel de gouvernance de l'IA, Navigating AI Innovation : A Playbook for Secure and Governable LLM Integration.

Télécharger maintenant



CONCLUSION

La sécurité des API est plus cruciale que jamais à l'ère de l'IA

La convergence de l'IA et des API présente à la fois des opportunités et des risques sans précédent. Si la plupart des entreprises se disent extrêmement préoccupées par les attaques renforcées par l'IA, 40 % d'entre elles ne sont toujours pas sûres que leurs investissements actuels en matière de sécurité soient suffisants. Nombre d'entre elles sous-estiment encore les vulnérabilités critiques telles que les API fantômes, et jusqu'à 13 % des entreprises aux États-Unis déclarent ne prendre aucune mesure spécifique contre les menaces renforcées par l'IA.

Les attaques d'API devraient augmenter de 548 % d'ici 2030. Il est donc temps d'agir. La plateforme API unifiée de Kong aide les entreprises à relever ces défis en offrant une sécurité robuste, une visibilité complète et une gestion simplifiée sur l'ensemble de votre écosystème API.

Visitez konghq.com pour en savoir plus sur la manière dont Kong peut aider votre organisation à simplifier la gestion des API et à libérer l'innovation en matière d'IA.

Méthodologie

Ce rapport examine l'évolution du paysage de la sécurité des API en analysant les opinions des experts sur les tendances et la dynamique actuelles. Pour recueillir ces informations, une enquête complète a été commandée à un cabinet de sondage professionnel au quatrième trimestre 2024. L'enquête a porté sur 700 professionnels de l'informatique et chefs d'entreprise sur deux marchés clés : les États-Unis et le Royaume-Uni.

À propos de Kong

Kong Inc., un développeur leader de technologies API cloud, a pour mission de permettre aux entreprises du monde entier de devenir « API-first ».
Kong aide les organisations du monde entier, des startups aux entreprises Fortune 500, à libérer la productivité des développeurs, à créer en toute sécurité et à accélérer la mise sur le marché.

Pour plus d'informations sur Kong, veuillez visiter www.konghq.com ou
Suivez-nous sur X @thekonginc.

Apprendre encore plus

Kong

Powering the API world

Konghq.com

Kong Inc.
contact@konghq.com

77, rue Geary, bureau 630
San Francisco, Californie 94108
USA