Livre blanc 2024

# Préserver l'avenir de votre entreprise en utilisant l'IA

## Comment les dirigeants doivent se préparer à utiliser et à sécuriser l'IA ainsi que les technologies connectées

kaspersky bring on the future

EN SAVOIR PLUS : KASPERSKY.FR

# Le prochain grand défi pour les entreprises : utiliser et sécuriser l'IA

Les chefs d'entreprise doivent s'assurer qu'ils font les bons investissements technologiques au bon moment. Ils doivent mettre en place les personnes et les systèmes qui peuvent leur assurer la réussite.

Parmi tous les investissements actuels, l'intelligence artificielle (IA) transforme les entreprises, leur permettant d'améliorer leurs services, d'automatiser leurs processus et de prendre de meilleures décisions.

Si l'IA est appelée à bouleverser toutes les industries, elle entraîne également de nouveaux risques et défis en matière de protection des entreprises et de leur clientèle.

**Notre étude vise à aider les entreprises à garder une longueur d'avance sur les changements qu'apporte l'IA, en posant des questions fondamentales sur la façon dont la cybersécurité doit s'adapter à l'IA.**

## À propos de notre étude

Nous avons interrogé 560 responsables de la sécurité informatique dans six zones géographiques : Amérique du Nord (US), Amérique latine (LATAM : Brésil, Chili, Colombie et Mexique), Europe (Autriche, France, Allemagne et Suisse), Moyen-Orient et Afrique (META : Arabie saoudite, Afrique du Sud, Turquie et Émirats arabes unis), Russie et Asie-Pacifique (APAC : Chine, Inde, Indonésie).

Nous leur avons demandé comment ils mettent en place et sécurisent l'IA et d'autres technologies interconnectées comme la 6G, le web 3.0, les espaces de données, les jumeaux numériques, la réalité augmentée (RA) la réalité virtuelle (RV) et l'Internet des objets (IdO).

« Ces nouvelles technologies sont le fruit d'une évolution qui a commencé avec l'intelligence économique et s'est poursuivie avec la science des données. Nous trouvons sans cesse de nouveaux moyens de tirer des renseignements à partir des données, et l'IA générative en est un exemple. »

Responsable de la cybersécurité d'une grande banque brésilienne

# L'IA est l'objectif principal des organisations pour les deux prochaines années

L'IA devient une pierre angulaire pour les organisations qui s'efforcent de rester en tête grâce à sa capacité à favoriser l'innovation. Dans le domaine de la cybersécurité, l'IA offre des analyses prédictives et une plus grande adaptabilité. Goldman Sachs affirme que l'investissement mondial dans l'IA atteindra **200 milliards de dollars** d'ici 2025.

L'IA est plus qu'une technologie. Il s'agit d'une stratégie qui permet aux organisations de naviguer dans l'environnement commercial complexe d'aujourd'hui.

## 9 sur 10

des organisations interrogées ont déjà adopté l'IA ou prévoient de le faire dans les deux années à venir.

### Adoption de l'IA

**54 %**

utilisent déjà l'IA

**33 %**

prévoient d'utiliser l'IA dans les deux prochaines années

**13 %**

prévoient d'utiliser l'IA dans deux ans ou plus

« Aucune vague technologique antérieure n'a capté l'attention des dirigeants et du grand public aussi rapidement que la GenAI [...] Les entreprises devront réinventer leur mode de fonctionnement en plaçant l'IA au centre de leurs préoccupations. »

Julie Sweet, directrice générale,

Les personnes interrogées considèrent que l'IA générative (GenAI) est utile pour améliorer les performances des technologies de sécurité. Joseph Briggs et Devesh Kodnani, économistes chez Goldman Sachs, affirment que la GenAI pourrait stimuler la productivité mondiale du travail de plus d'un point de pourcentage par an une fois que son utilisation se sera généralisée.

Les entreprises informatiques du monde entier améliorent les compétences de leur personnel et lancent des projets pilotes de GenAI pour éviter de se laisser distancer. Le géant de l'informatique Accenture s'est engagé à investir trois milliards de dollars dans les données et l'IA, tandis que l'entreprise technologique française Capgemini consacrera deux milliards d'euros à la GenAI au cours des trois prochaines années.

## Alors que l'IA est de plus en plus adoptée, la plupart des organisations ne sont pas suffisamment préparées à la protéger

**50 %**

ont déclaré que l'IA est peu ou pas du tout difficile à sécuriser

**16 %**

ont déclaré que l'IA est difficile ou très difficile à sécuriser

« Nous nous efforçons d'être encore mieux préparés à répondre aux défis en matière de sécurité. Nous devons mettre en œuvre de meilleures solutions et former les employés afin qu'ils renforcent leurs compétences. »

Responsable de la cybersécurité, Nemak

# L'IA rend indispensables la confiance numérique et la conformité des données

L'IA pose de nouveaux défis et complique la protection des données sensibles ainsi que le maintien de la confiance numérique.

La confiance numérique est un aspect de la confiance des clients. Dans le podcast Kaspersky Insight Story, Malek Ben Salem, expert en sécurité des technologies émergentes, décrit la confiance numérique comme « notre confiance dans la protection et la sécurité de notre vie privée, la fiabilité des transactions numériques et la certitude que nous avons de l'identité des personnes avec lesquelles nous interagissons ».

Selon le rapport 2022 Digital Trust du cabinet d'études McKinsey, 70 % des personnes font confiance aux entreprises pour protéger leur vie privée, mais la plupart d'entre elles ne répondent pas à leurs attentes.

Les violations de données, les accès non autorisés et les atteintes à la vie privée peuvent éroder la confiance numérique et entraîner une atteinte à la réputation, une perte d'activité ainsi que des conséquences réglementaires. L'instauration de la confiance numérique prend du temps, mais elle est essentielle pour que les utilisateurs puissent se fier l'IA.

## L'impact de l'IA sur la confiance numérique

**Davantage de collecte de données :** l'IA permet aux organisations de collecter et de stocker davantage de données sur les clients, les opérations et les interactions. Cette masse de données favorise les analyses, mais accroît également le risque d'atteinte à la sécurité.

**Davantage de partage de données :** l'IA facilite le partage de données entre les appareils, les réseaux et les organisations. Le partage des données favorise la collaboration, l'efficacité et l'innovation, mais il multiplie également les possibilités d'accès non autorisé.

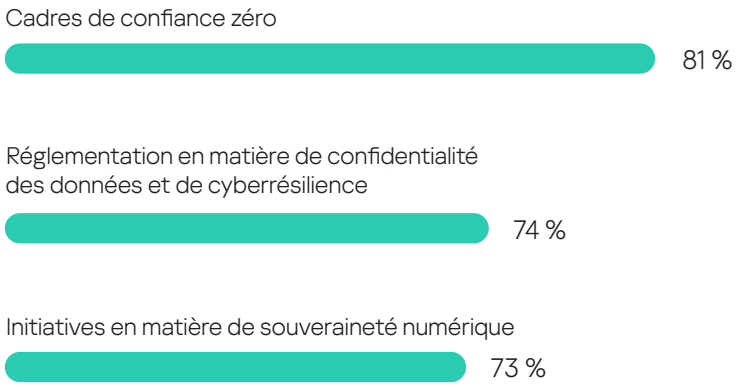
**Manque de transparence :** comme il s'agit d'un phénomène relativement nouveau, les organisations peuvent avoir du mal à expliquer clairement leurs pratiques et leur sécurité autour de l'IA. Sans une communication claire, la confiance peut être rompue.

« Les utilisateurs de la GenAI qui souhaitent obtenir des recommandations d'investissement peuvent se demander si l'envoi de leurs données ou de leur portefeuille ne risque pas d'exposer leur stratégie. Les entreprises devraient répondre à cette préoccupation de manière transparente afin d'apaiser les inquiétudes et d'instaurer la confiance. »

Responsable de la cybersécurité d'une grande banque brésilienne

Lesquels de ces moyens votre organisation met-elle en pratique ou prévoit-elle d'adopter dans les deux ans pour améliorer la confiance des clients et le respect des normes ?

## Les principaux moyens mis en œuvre par les entreprises pour améliorer la confiance et la conformité numériques




Notre recherche a révélé que les entreprises qui optent pour des environnements de confiance zéro sont mieux préparées à sécuriser l'IA et d'autres technologies interconnectées : 51 % des premières entreprises à avoir adopté cette approche se sont déclarées extrêmement bien préparées ou bien préparées à sécuriser ces technologies, contre seulement 27 % des autres.

# Le canevas de la confiance zéro : dessiner l'avenir de la cybersécurité

Les approches traditionnelles en matière de cybersécurité reposent souvent sur la confiance accordée à ceux qui se trouvent à l'intérieur du périmètre d'un réseau et sur la méfiance à l'égard de ceux qui se trouvent à l'extérieur. Ce modèle s'est révélé vulnérable aux attaques d'initiés. Les structures de confiance zéro vérifient rigoureusement chaque personne.

## Les principes de la confiance zéro

Ne jamais faire confiance, toujours vérifier :chaque utilisateur et chaque appareil doivent être soumis à une authentification et à une autorisation permanentes, quel que soit leur niveau de confiance.

Accès au moindre privilège : les utilisateurs et les appareils reçoivent l'accès minimum nécessaire à leurs tâches.

Surveillance continue : surveillance constante de l'activité des utilisateurs, du comportement des appareils et du trafic réseau afin de détecter les menaces et d'y répondre en temps réel.

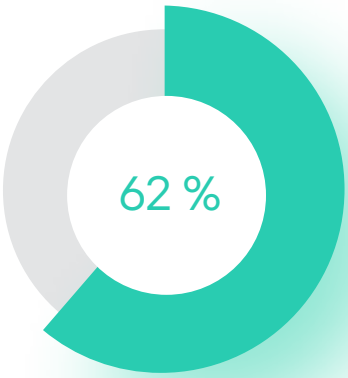
Authentification à plusieurs facteurs : vérification supplémentaire au-delà des mots de passe, ce qui rend l'accès plus difficile pour les personnes non autorisées.

« Le modèle de sécurité à confiance zéro est la seule structure qui fonctionne. Le modèle de sécurité traditionnel ne suffit pas, en particulier pour les technologies interconnectées. Chaque organisation devrait mettre en place une structure de confiance zéro. »

Directeur du service informatique, Searce

## Réglementation et conformité

Étant donné que chaque territoire dispose d'une législation différente en matière de protection des données et de la vie privée, les organisations internationales éprouvent des difficultés à mettre en place des normes cohérentes en matière d'IA.




62 % des dirigeants estiment que le processus de certification de la conformité est difficile. Ils souhaitent que les processus de conformité soient normalisés pour l'ensemble des réglementations et estiment que la mise en place de lignes directrices claires pour les outils et les plateformes en ligne simplifierait davantage le processus de certification.

# Comment les dirigeants peuvent-ils relever les défis croissants et être mieux préparés à sécuriser l'IA ?

Compte tenu de l'ampleur des changements que l'IA est susceptible d'entraîner, les organisations doivent élaborer une stratégie pour se préparer à adopter et à sécuriser l'IA.

**L'étude de Kaspersky a mis en évidence quatre stratégies efficaces pour être prêt à sécuriser l'IA et d'autres technologies interconnectées.**

**Les quatre stratégies**

1. Adopter les principes de la sécurité dès la conception

2. Former les salariés et leur permettre de se perfectionner

3. Moderniser les solutions de cybersécurité

4. Respecter les réglementations et les normes

**Pour en savoir plus, téléchargez le rapport complet :** Un avenir connecté pour les entreprises : comment les dirigeants doivent se préparer à utiliser et à sécuriser l'IA ainsi que les technologies interconnectées

**kaspersky.fr**

kaspersky

Actualitéssur les cybermenaces: securelist.com
Actualités sur la sécurité informatique : business.kaspersky.fr
Revue destinée aux chefs d'entreprise : kaspersky.com/blog/secure-futures-magazine
Solutions de cybersécurité pour les entreprises : kaspersky.fr/enterprise-security