Rapport 2024

# 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 bring on the future

EN SAVOIR PLUS : KASPERSKY.FR

# Les contributions de plus de 500 responsables de la sécurité informatique au sein d'entreprises du monde entier

## À qui s'adresse cette recherche ?

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.

De tous les investissements actuels, les technologies interconnectées, c'est-à-dire le réseau croissant d'appareils, de systèmes et d'applications connectés à Internet et les uns aux autres, sont les plus importants et les plus difficiles à mettre en œuvre. De l'intelligence artificielle (IA) aux espaces de données en passant par l'Internet des objets (IoT), les technologies interconnectées transforment les entreprises, leur permettant de recueillir davantage de données, d'automatiser les processus et de prendre de meilleures décisions.

Alors que cette « quatrième révolution industrielle » pousse au changement dans toutes les industries, les environnements hyperconnectés entraînent de nouveaux risques et défis en matière de sécurisation des entreprises et de protection des clients.

Cette recherche vise à aider les entreprises à garder une longueur d'avance sur les changements qu'apportent les technologies interconnectées, en posant des questions fondamentales sur la façon dont la cybersécurité doit s'adapter aux technologies interconnectées.

« 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. »

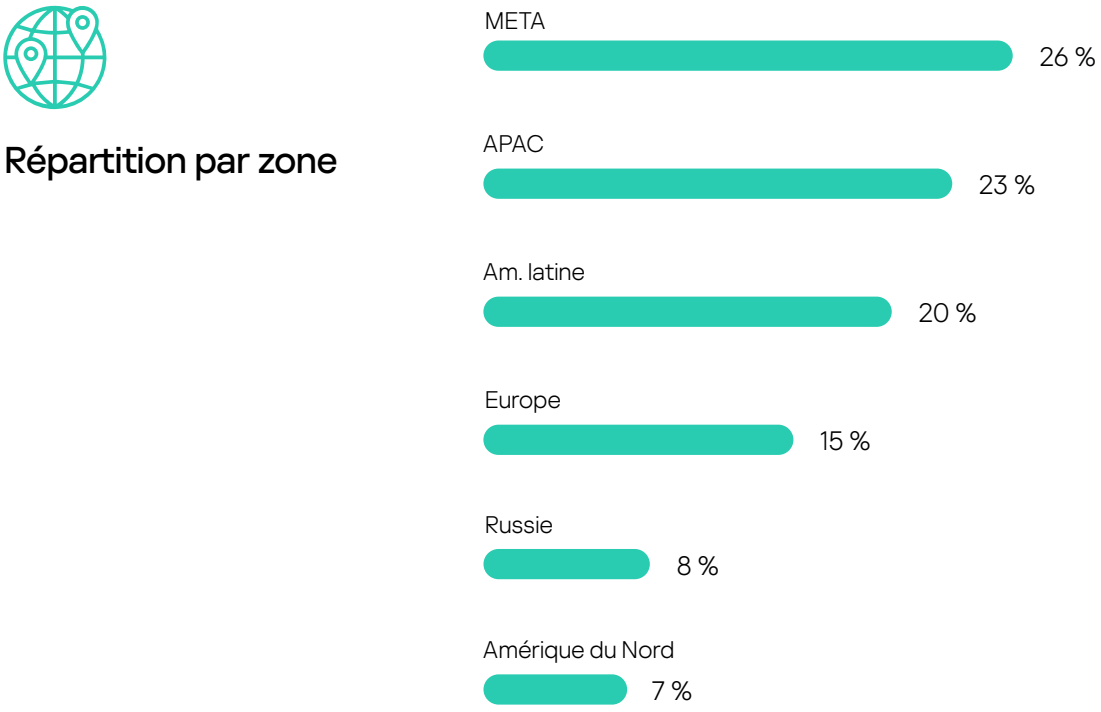
Responsable de la cybersécurité d'une grande banque brésilienne

# Participants

Kaspersky a interrogé 560 responsables de la sécurité informatique dans six zones géographiques : Amérique du Nord (US), Amérique latine (LATAM : Brésil, Chili, Colombie, Mexique), Europe (Autriche, France, Allemagne, Suisse), Moyen-Orient et Afrique (META : Arabie saoudite, Afrique du Sud, Turquie, Émirats arabes unis), Russie et Asie-Pacifique (APAC : Chine, Inde, Indonésie) pour comprendre comment ils mettent en place et sécurisent les technologies interconnectées.

Les participants provenaient d'entreprises comptant au moins 1 000 employés dans de nombreux secteurs d'activité. Chacun d'entre eux était au courant des décisions prises dans le domaine de la cybersécurité pour les technologies interconnectées ou y participait.

## Répartition par zone




## Taille des entreprises

47 % 1 001 – 5 000 employés

24 % 5 001 – 10 000 employés

12 % 10 001 – 15 000 employés

7 % 15 001 – 20 000 employés

10 % Plus de 20 001 collaborateurs

## Technologies interconnectées examinées

### Intelligence artificielle (IA)

Les systèmes d'IA imitent l'intelligence humaine dans des domaines tels que l'apprentissage, la résolution de problèmes et la prise de décision.

Son rôle : transformer les soins de santé, la finance, les véhicules et plus encore, en analysant les données, en prédisant les résultats et en automatisant les tâches, afin d'améliorer la prise de décision et l'efficacité.

### Web 3.0

Le Web 3.0 offre des applications décentralisées (DApps), des contrats intelligents (blockchain) et des données gérées par l'utilisateur, ce qui favorise l'efficacité et la confiance dans les écosystèmes numériques.

Son rôle : Assurer un contrôle décentralisé des données, des transactions transparentes et une sécurité accrue, en redéfinissant les modèles avec la finance décentralisée (DeFi), la vérification de l'identité et la gestion de la chaîne d'approvisionnement.

### Espaces de données

Les espaces de données offrent un partage transparent des données dans un cadre collaboratif, favorisant ainsi la prise de décision en temps réel, l'innovation et l'interopérabilité.

Son rôle : Favoriser la collaboration et permettre l'utilisation des données à des fins d'innovation, afin d'améliorer la flexibilité et la compétitivité des organisations.

### Jumeaux numériques, réalité augmentée et réalité virtuelle

Les jumeaux numériques reproduisent numériquement des objets physiques. La réalité augmentée (RA) ajoute des superpositions numériques au monde réel. La réalité virtuelle (RV) crée des environnements immersifs.

Son rôle : optimiser les processus de fabrication, en offrant une assistance et une formation à distance. Simuler des environnements réels.

### 6G

La 6G est la prochaine génération de communication sans fil avec des vitesses ultra-rapides, une faible latence et de nouvelles capacités de connexion.

Son rôle : améliorer la connectivité dans tous les secteurs, y compris la chirurgie à distance dans les soins de santé, les expériences de réalité augmentée transparentes et l'alimentation des véhicules autonomes.

### Internet des objets (IoT)

Les réseaux IoT sont composés d'appareils « intelligents » interconnectés permettant le contrôle à distance et le partage de données.

Son rôle : connecter les appareils et permettre l'échange de données, optimiser l'efficacité et le confort, de la domotique à la surveillance industrielle.

# Quels sont les facteurs de croissance des technologies interconnectées ?

### 1. Convergence technologique

On parle de convergence technologique lorsque les technologies s'intègrent et fusionnent, perturbant les anciens modes de pensée, favorisant l'innovation et créant de nouveaux marchés.

### 2. Plus grande accessibilité financière

Les appareils sont devenus plus rentables tandis que leurs applications sont devenues plus puissantes.

### 3. Plus grande disponibilité du réseau Internet à haut débit

La disponibilité et la fiabilité croissantes du réseau Internet à haut débit dans toutes les régions du monde ont permis à un plus grand nombre d'entreprises de s'interconnecter.

## Vitesse d'adoption

### Adoption actuelle

**54 %**
AI

**51 %**
Internet des objets (IoT)

### Projets d'adoption au cours des deux prochaines années

**50 %**
Web 3.0

**46 %**
Jumeaux numériques, réalité augmentée et réalité virtuelle

**43 %**
6G

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

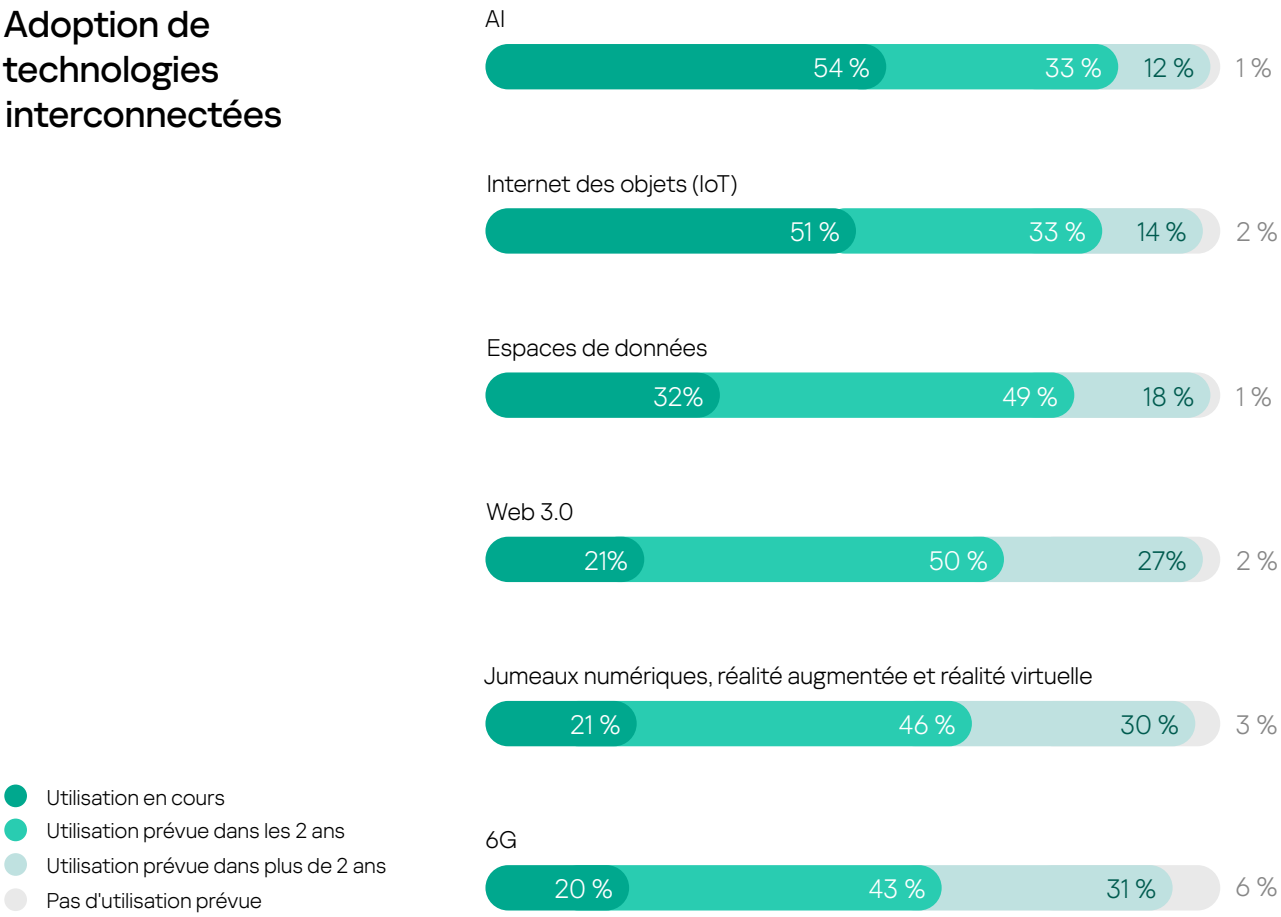
**9 sur 10**

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

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.

## Adoption de technologies interconnectées



« 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, Accenture

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.

« L'IA se développe rapidement. Beaucoup de technologies utilisent l'IA, que ce soit au niveau du front-end (comme ChatGPT et les bots) ou du back-end. »

Directeur du service informatique, Searce

# 32 %

des organisations sont extrêmement ou bien préparées à sécuriser les technologies interconnectées

## Alors que les technologies interconnectées sont de plus en plus adoptées, la plupart des organisations ne sont pas suffisamment préparées à les protéger

La plupart des technologies interconnectées ne sont pas suffisamment mûres pour être correctement sécurisées. Certains dirigeants affirment que leur entreprise se concentre sur l'essentiel plutôt que sur la sécurisation des technologies émergentes.

### Niveau de préparation par technologie

**Dans quelle mesure votre organisation est-elle prête à sécuriser les technologies interconnectées ?**

(Les participants qui ont répondu **extrêmement bienpréparé** et **bien préparé**.)


Internet des objets (IoT)
59 %

AI
49 %


6G
38 %

Espaces de données
35 %

Web 3.0
32 %

Jumeaux numériques, réalité augmentée et réalité virtuelle
30 %

« 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. »

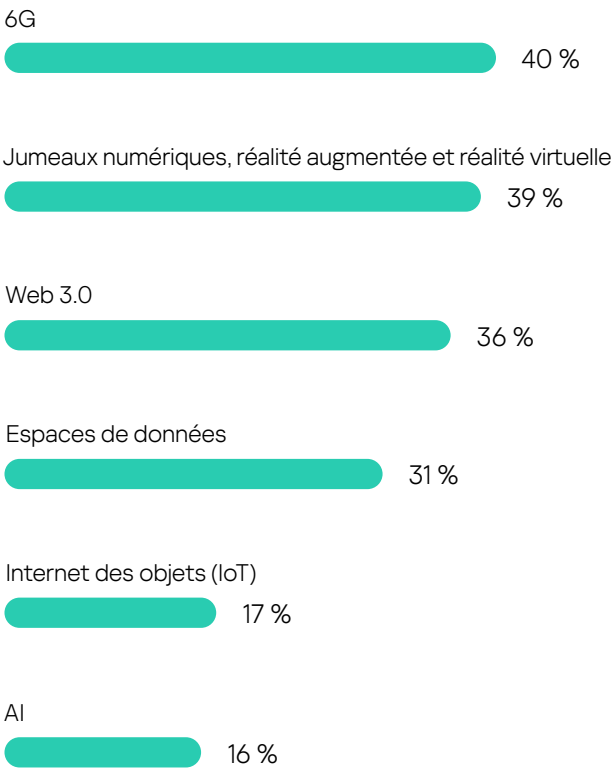
Responsable de la cybersécurité, Nemak

La plupart des dirigeants affirment qu'ils sont confrontés à des problèmes d'infrastructure pour sécuriser la réalité augmentée et la réalité virtuelle, en particulier en ce qui concerne les données. Un responsable de la sécurité des systèmes d'information (RSSI) d'une entreprise médicale de premier plan en Arabie saoudite a expliqué que l'infrastructure et la conformité du Web 3.0 n'étaient pas en place, ce qui rendait complexe la préparation à leur sécurisation. Près de la moitié des organisations pensent que l'IA et l'IoT sont peu ou pas du tout difficiles à sécuriser.

## Difficulté à sécuriser les technologies

**Dans quelle mesure est-il difficile de sécuriser ces technologies interconnectées au sein de votre organisation ?**

(Les participants qui ont répondu **très difficile** et **extrêmement difficile**.)




« La plupart du temps, je ne trouve pas de problèmes de sécurité avec GenAI. Nous savons déjà comment la faire fonctionner et l'entraîner.»

Responsable de la cybersécurité d'une grande banque brésilienne

# Pour sécuriser les technologies interconnectées, les organisations sont confrontées à des défis internes et externes

## Les cinq principaux défis liés à l'introduction et à la sécurisation des technologies interconnectées

1  47 % Cyberincidents les plus courants et les plus graves

2  45 % Solutions insuffisantes

3  45 % Difficultés liées à l'utilisation des nouvelles technologies

4  42 % Difficulté d'engager ou de former des experts

5  42 % Dépendance à l'égard des anciennes technologies

La nature et l'importance des défis varient en fonction du degré de préparation. Les organisations insuffisamment préparées considèrent que les problèmes internes et d'infrastructure sont les plus difficiles, tandis que les organisations mieux préparées considèrent que les facteurs externes sont plus difficiles.

## Quelle est l'influence du niveau de préparation sur les défis à relever ?

### Organisations insuffisamment préparées

- Difficulté d'embaucher ou de former des experts pour soutenir les technologies interconnectées
- Dépendance à l'égard d'une technologie plus ancienne et plus vulnérable
- Ressources financières limitées pour l'acquisition de nouvelles technologies

### Comment la préparation a une incidence sur les difficultés rencontrées

- Des solutions de cybersécurité inadaptées sur le marché
- Les technologies interconnectées entraînent des incidents plus fréquents et plus graves
- Absence de demande de sécurité de la part des clients

# Les technologies interconnectées rendent indispensables la confiance numérique et la conformité des données

Les technologies interconnectées posent de nouveaux défis et compliquent 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 KasperskyInsight 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 aux technologies émergentes.

## L'impact de l'interconnexion des technologies sur la confiance numérique

**Davantage de collecte de données :** les technologies interconnectées permettent 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 :** les technologies interconnectées facilitent 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 des technologies interconnectées. 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. »

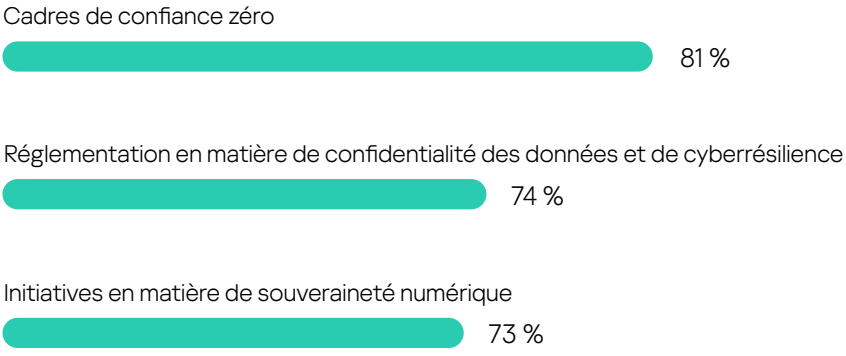
Responsable de la cybersécurité d'une grande banque brésilienne

## Cinq étapes pour protéger les informations sensibles

1. Développez et mettez en œuvre des politiques claires en matière de collecte, d'utilisation et de protection des données des clients.
2. Communiquez ouvertement avec vos clients au sujet de vos politiques d'utilisation des données.
3. Mettez en place une protection solide des données afin d'empêcher tout accès non autorisé.
4. Formez vos employés aux bonnes pratiques en matière de confidentialité et de sécurité des données.
5. Respectez les réglementations et les normes en matière de protection de la vie privée.

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

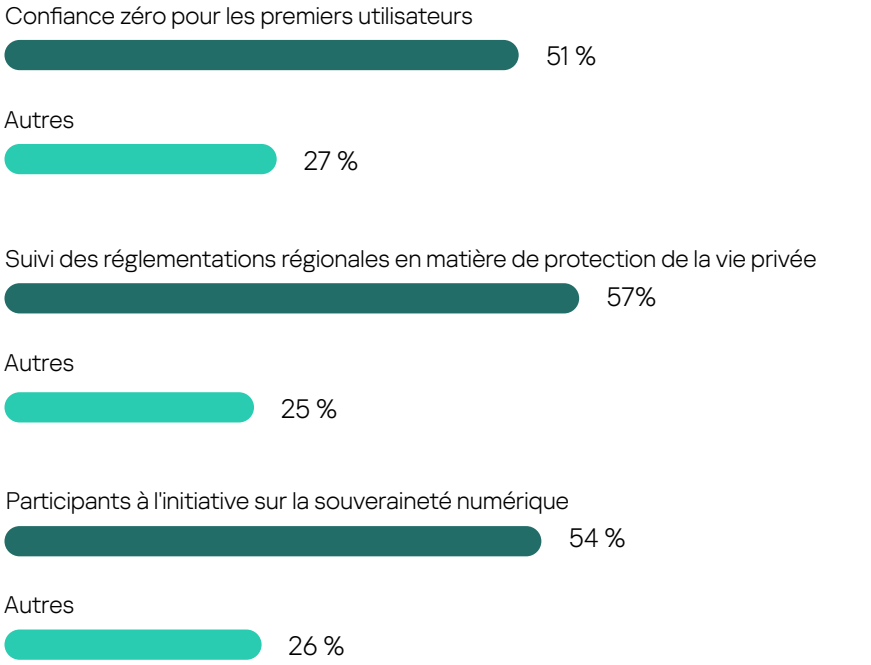
Lesquels de ces moyens votre organisation met-elle en pratique ou prévoit-elle d'adopter dans les deux ans pour améliorer la confiance des clients et le respect des normes ?



Notre étude a révélé que les entreprises qui appliquent des principes de confiance zéro, des réglementations en matière de confidentialité des données et de cyberrésilience, ainsi que des initiatives de souveraineté des données, sont mieux préparées que les autres à sécuriser les technologies interconnectées.

## Dans quelle mesure votre organisation est-elle prête à sécuriser les technologies interconnectées ?

(Les participants qui ont répondu **extrêmement bien préparé** et **bien préparé**.)




# 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.

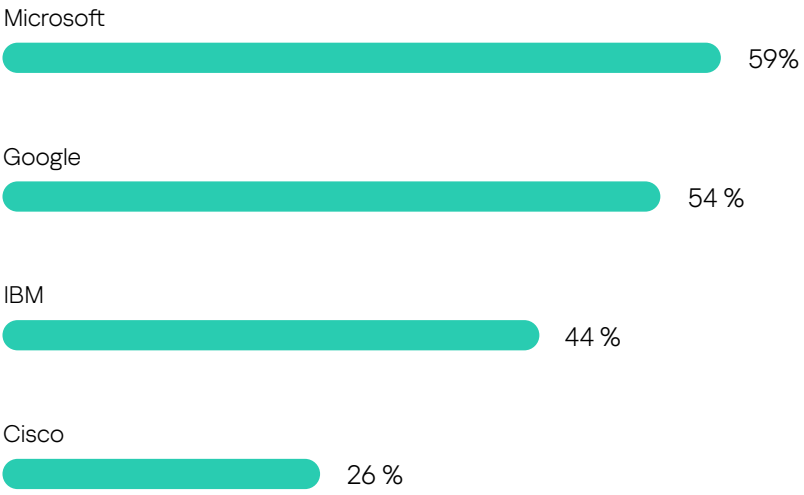
Surveillance continue : surveillance constante de l'activité des utilisateurs, du comportement des appareils et du trafic réseau afin de détecter les menaces et d'y répondre en temps réel.

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. »

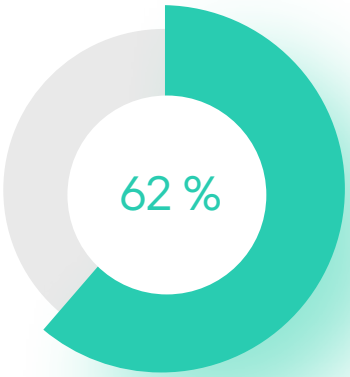
Directeur du service informatique, Searce

## Modèles de confiance zéro les plus utilisés par les participants




## 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.




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 que les outils et plateformes en ligne soient assortis de directives claires afin de simplifier davantage la certification.

# Comment les dirigeants peuvent-ils relever les défis croissants et être mieux préparés à sécuriser les technologies interconnectées ?

Compte tenu de l'ampleur des changements que ces nouvelles technologies sont susceptibles d'entraîner, les organisations doivent élaborer une stratégie pour se préparer à adopter et à sécuriser les technologies interconnectées.

**L'étude de Kaspersky a mis en évidence quatre stratégies efficaces pour être prêt à sécuriser les 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

Stratégie 1

# Adopter les principes de la sécurité dès la conception

L'intégration de la cybersécurité à chaque étape du cycle de développement des logiciels permet aux logiciels et aux matériels sécurisés dès leur conception de mieux résister aux cyberattaques, ce qui contribue à la sécurité globale des systèmes numériques.

L'étude de Kaspersky a révélé que les dirigeants qui se concentrent sur l'intégration de la cybersécurité dans les processus de développement, c'est-à-dire les promoteurs de la sécurité dès la conception, sont mieux préparés à sécuriser les technologies interconnectées.

**80 %**

des organisations donneront la priorité à l'intégration de la cybersécurité dans le développement de logiciels au cours des deux prochaines années.

**30 %**

des dirigeants se concentrent déjà sur l'intégration de la cybersécurité dans le développement de logiciels. Ce groupe de promoteurs de la sécurité dès la conception est mieux préparé à sécuriser les technologies interconnectées.

« Les modes de développement des technologies vont changer – la sécurité dès la conception prendra de plus en plus d'importance. Lorsque nous aurons un produit en main, nous examinerons la sécurité de sa conception. »

Directeur de la cybersécurité, Aselsan

## Niveau de préparation général pour sécuriser les technologies interconnectées

**50 %**

des promoteurs de la sécurité dès la conception

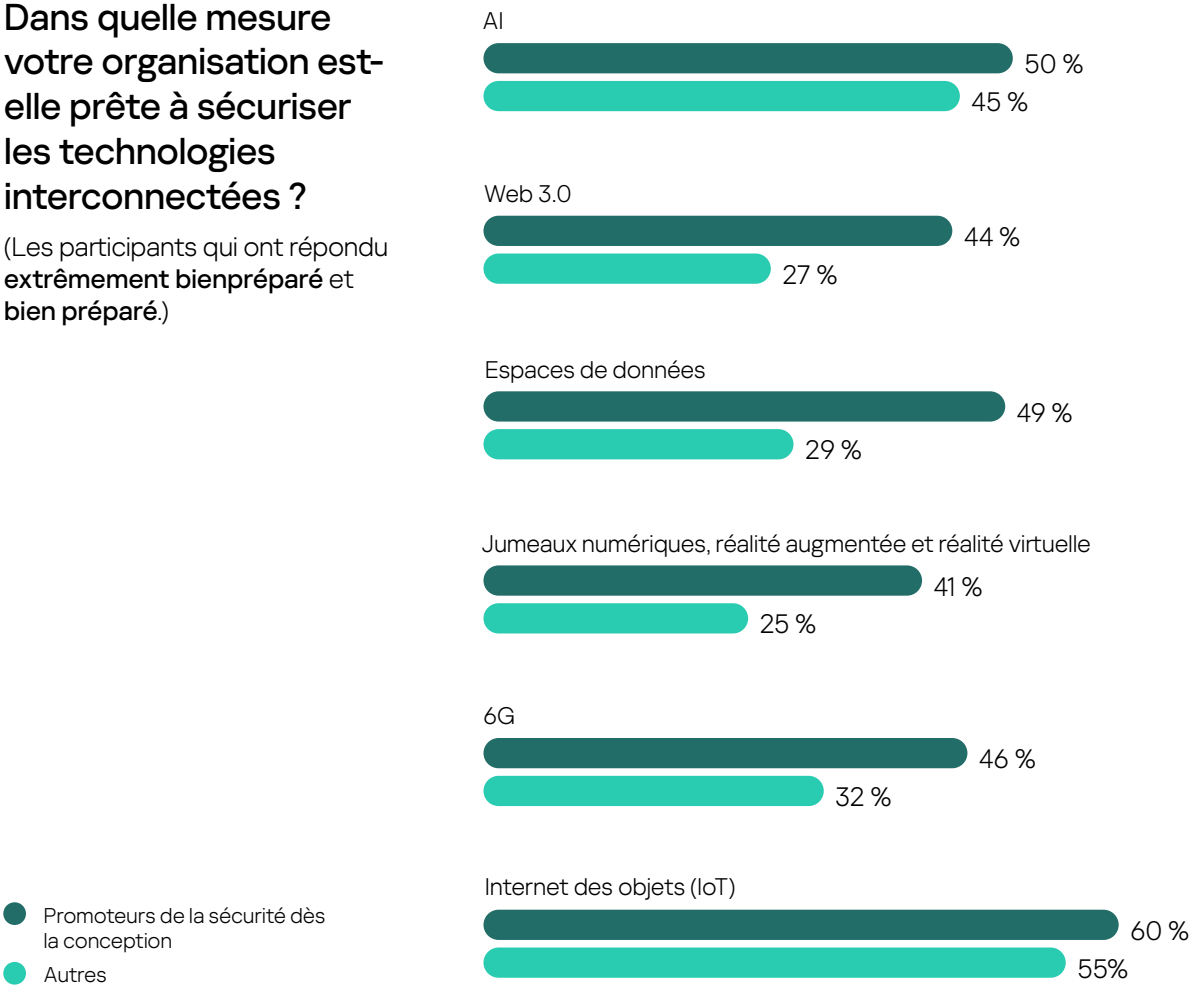
**26 %**

des entreprises qui n'accordent pas la priorité à la sécurité dès la conception

## Dans quelle mesure votre organisation est-elle prête à sécuriser les technologies interconnectées ?

(Les participants qui ont répondu **extrêmement bienpréparé** et **bien préparé**.)

## Niveau de préparation par technologie : les promoteurs de la sécurité dès la conception par rapport aux autres




## Trois questions pour l'équipe de direction

1. À quel moment de nos processus de conception l'expertise en cybersécurité intervient-elle pour la première fois ?
2. Planifions-nous et budgétisons-nous les tests de sécurité pendant les phases de conception ?
3. Comment garantir la sécurité dès la conception tout en restant flexible et souple ?

Stratégie 2

# Former les salariés et leur permettre de se perfectionner

Le personnel qui comprend les cyberattaques et les moyens de les prévenir constitue une formidable ligne de défense. L'instauration d'une culture de la cyberconscience exige une stratégie globale qui permette aux employés d'acquérir des connaissances et de les mettre en pratique.

L'étude de Kaspersky révèle que les promoteurs de formation et de perfectionnement, c'est-à-dire les organisations qui accordent la priorité à la formation et au perfectionnement de leur personnel, sont mieux préparés à sécuriser les technologies interconnectées.

**75 %**

des organisations donneront la priorité à la formation et à l'amélioration des compétences de leur personnel en ce qui concerne les défis de sécurité technologique interconnectés au cours des deux prochaines années.

**32 %**

des dirigeants forment leurs salariés et leur permettent déjà de se perfectionner pour relever les défis de la sécurité des technologies interconnectées. L'étude de Kaspersky révèle que ces promoteurs de formation et de perfectionnement sont mieux préparés à sécuriser les technologies interconnectées.

« Mon personnel n'est pas encore prêt pour les technologies interconnectées. Il y parviendra avec le temps – c'est un processus d'apprentissage continu. Il faut un plan de formation adéquat pour que les employés soient prêts. »

RSSI d'une entreprise médicale de premier plan en Arabie saoudite

## Niveau de préparation général pour sécuriser les technologies interconnectées

**55 %**

des promoteurs de formation et de perfectionnement

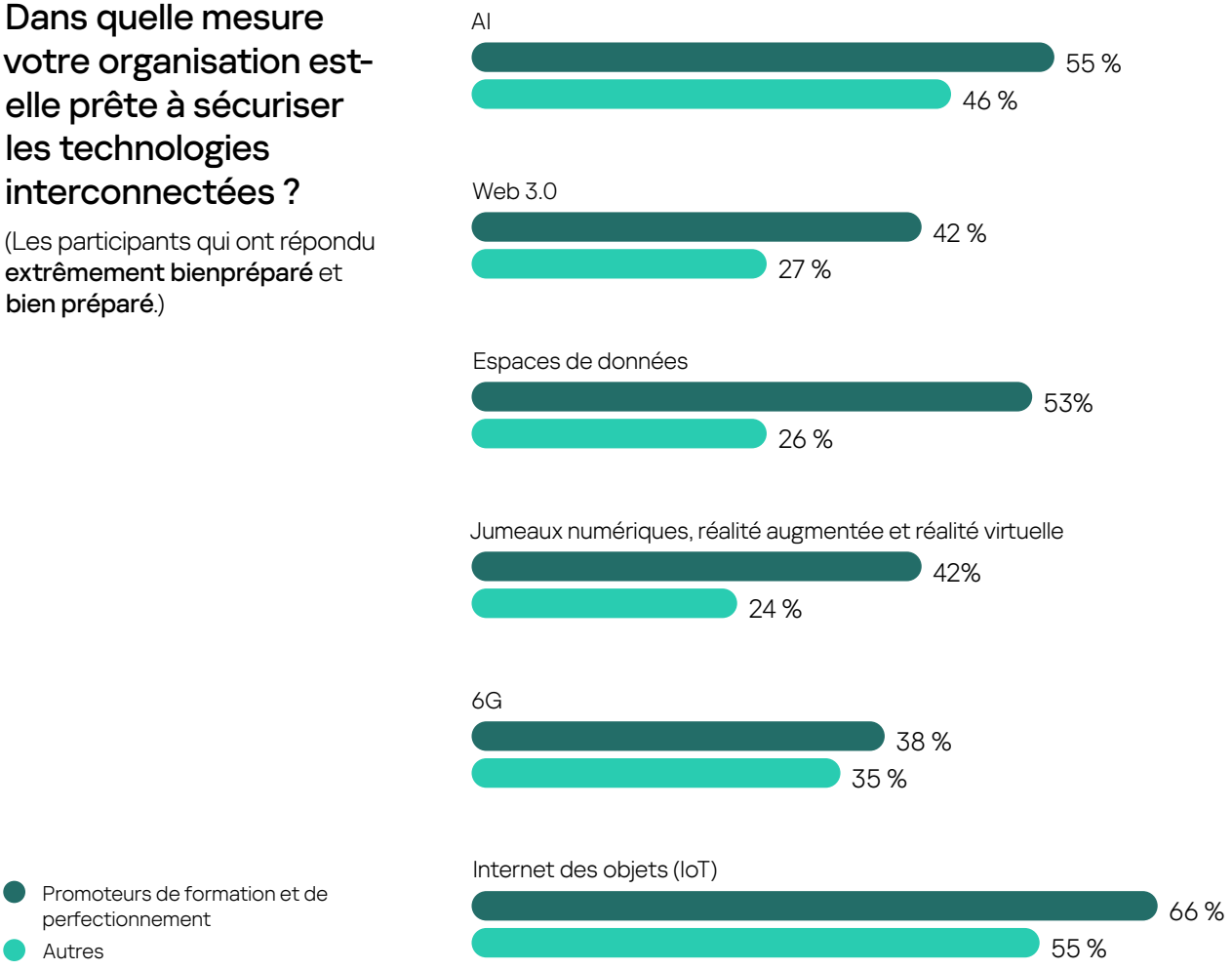
**25 %**

de ceux qui n'investissent pas encore dans la formation et l'amélioration des compétences

## Niveau de préparation par technologie : les promoteurs de formation et de perfectionnement par rapport aux autres

### Dans quelle mesure votre organisation est-elle prête à sécuriser les technologies interconnectées ?

(Les participants qui ont répondu **extrêmement bienpréparé** et **bien préparé**.)



## Comment combler les lacunes en matière de compétences : ce que les dirigeants recommandent

Dans l'étude de Kaspersky, les dirigeants ont recommandé les moyens suivants pour améliorer les compétences des employés et les former.

Programmes d'éducation et de formation : des programmes réguliers couvrant des sujets tels que vos politiques de cybersécurité, les cybermenaces les plus courantes et les bonnes pratiques en matière de sécurité.

Simulation de phishing : aider les employés à reconnaître les emails de phishing et à y répondre. Les résultats donnent des informations sur les besoins en matière de formation continue.

Campagnes de communication et de sensibilisation : partagez les mises à jour, les actualités et les bonnes pratiques en matière de cybersécurité par le biais de plusieurs canaux. Utilisez des exemples concrets pour montrer l'impact des incidents de cybersécurité et l'importance de la contribution de chacun.

Politiques de sécurité conviviales : les employés sont plus enclins à suivre les politiques si elles sont claires, concises et faciles d'accès.

Collaboration avec les équipes informatiques et de sécurité : des liens plus étroits entre l'entreprise au sens large et les équipes chargées des technologies de l'information et de la sécurité encouragent le signalement des problèmes de sécurité.

Implication des dirigeants : montrez aux dirigeants qui participent à des initiatives de cybersécurité un message clair sur l'importance de cette dernière.

### Trois questions pour l'équipe de direction

1. À quelle fréquence faut-il former les employés à la cybersécurité ?
2. Comment savoir si les employés comprennent la cybersécurité ?
3. Comment favoriser une culture de sensibilisation à la cybersécurité au sein de notre organisation ?

Stratégie 3

# Moderniser les solutions de cybersécurité

Plus le nombre d'appareils connectés à Internet est élevé, plus les possibilités d'attaque sont nombreuses. Au fur et à mesure que vous adoptez ces technologies, vous pouvez être amené à utiliser des fonctions plus avancées dans les solutions de cybersécurité, telles que des contrôles d'accès renforcés, le chiffrement et la conformité aux réglementations.

L'étude de Kaspersky révèle que les utilisateurs avancés de la cybersécurité, c'est-à-dire les entreprises qui adoptent des solutions de cybersécurité avancées, sont mieux préparés à sécuriser les technologies interconnectées.

**86 %**

des organisations mettront à niveau leurs solutions de cybersécurité pour sécuriser les technologies interconnectées au cours des deux prochaines années.

**31 %**

des dirigeants se concentrent déjà sur la mise à niveau des solutions de cybersécurité. L'étude de Kaspersky révèle que ce groupe – les utilisateurs avancés de la cybersécurité – est mieux préparé à sécuriser les technologies interconnectées.

« Les failles de sécurité coûtent très cher, et la question n'est pas « si », mais « quand » elle arriveront. Au lieu de dépenser de l'argent pour nettoyer les dégâts, il faut le dépenser à se préparer. »

Directeur de la cybersécurité, Aselsan

## Niveau de préparation général pour sécuriser les technologies interconnectées

**55 %**

des utilisateurs avancés de la cybersécurité

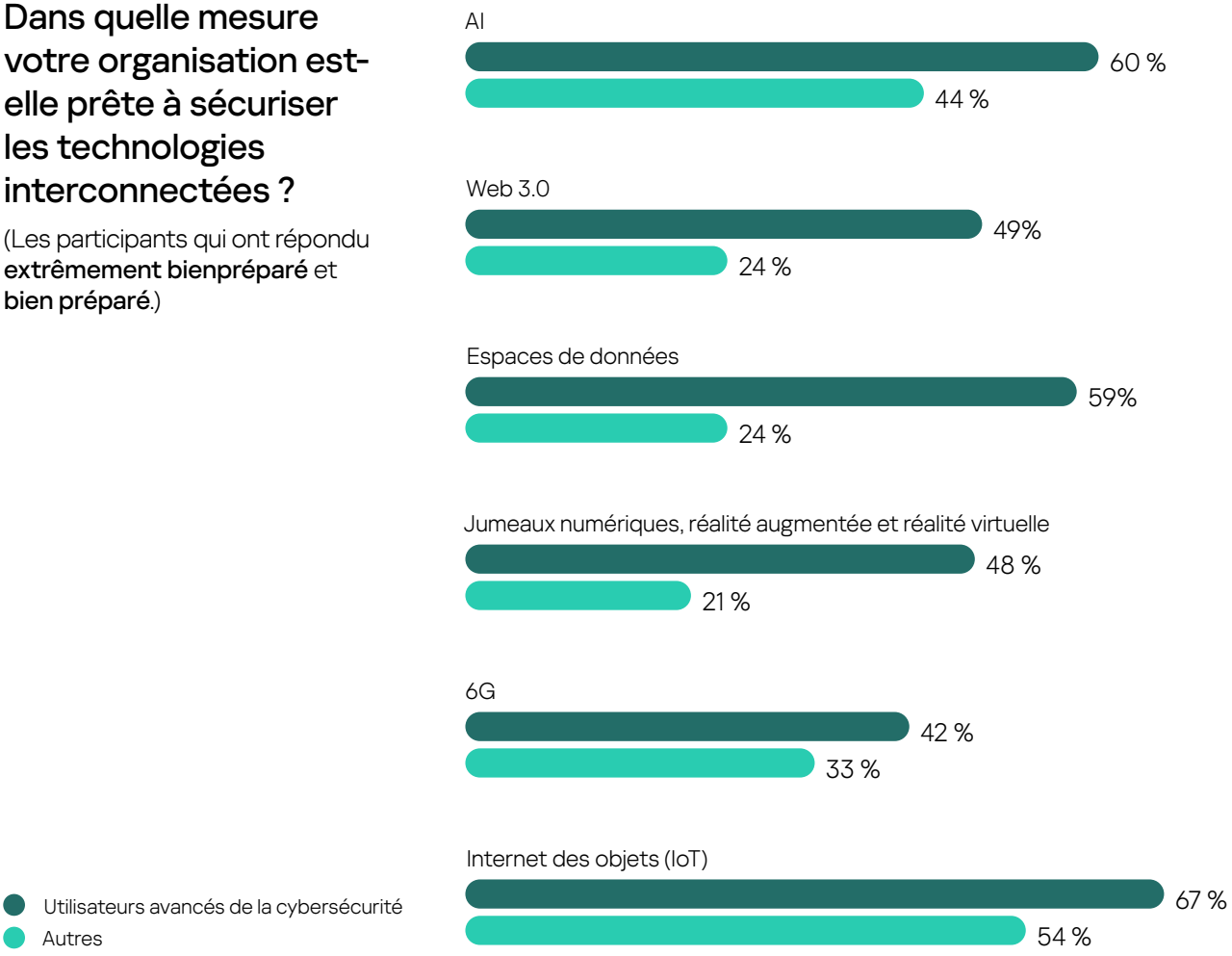
**22 %**

des entreprises qui n'ont pas encore adopté des mesures de cybersécurité avancées

## Niveau de préparation par technologie : les utilisateurs avancés de la cybersécurité par rapport aux autres

### Dans quelle mesure votre organisation est-elle prête à sécuriser les technologies interconnectées ?

(Les participants qui ont répondu **extrêmement bienpréparé** et **bien préparé**.)



## Avantages de l'investissement dans des solutions de cybersécurité avancées

S'adapter à un paysage changeant : la cybersécurité doit s'adapter à des menaces en constante évolution. La mise à jour des solutions de cybersécurité permet aux entreprises de garder une longueur d'avance sur les nouvelles menaces.

Respecter les normes réglementaires : la modernisation de la cybersécurité aide les entreprises à répondre aux exigences des nouvelles réglementations et normes, réduisant ainsi le risque de problèmes juridiques et d'atteinte à la réputation.

Mieux protéger les données stratégiques : le passage à des solutions de cybersécurité dotées de fonctionnalités telles que le chiffrement avancé, les contrôles d'accès et la détection améliorée des menaces permet de mieux protéger les informations de l'entreprise.

## Trois questions pour l'équipe de direction

1. Que savons-nous des menaces et des vulnérabilités qui nous incitent à moderniser nos solutions de cybersécurité ?
2. Comment minimiser l'impact de la mise à niveau des solutions sur les flux de travail ?
3. Comment s'assurer que les employés peuvent utiliser efficacement nos outils de cybersécurité améliorés ?

Stratégie 4

# Respecter les réglementations et les normes

Pour éviter les problèmes juridiques ou les atteintes à la réputation, veillez à ce que vos pratiques en matière de cybersécurité soient conformes à l'évolution des normes et des exigences légales.

L'étude de Kaspersky a révélé que les organisations qui accordent la priorité au respect des nouvelles réglementations et normes, c'est-à-dire les promoteurs de réglementations, sont mieux préparées à sécuriser les technologies interconnectées.

**81 %**

des organisations donneront la priorité au respect des nouvelles réglementations et normes pour sécuriser les technologies interconnectées au cours des deux prochaines années.

**40 %**

des dirigeants accordent déjà la priorité au respect des nouvelles réglementations et normes. L'étude de Kaspersky révèle que ce groupe – promoteurs de réglementations – est mieux préparé à sécuriser les technologies interconnectées.

« Lorsque les entreprises adoptent ces technologies [IA], elles doivent également prendre en compte les lois et les perspectives d'audit qui peuvent permettre d'identifier les causes des cyberattaques et des failles de sécurité. »

Responsable de la cybersécurité d'une grande banque brésilienne

## Niveau de préparation général pour sécuriser les technologies interconnectées

**40 %**

des promoteurs de réglementations

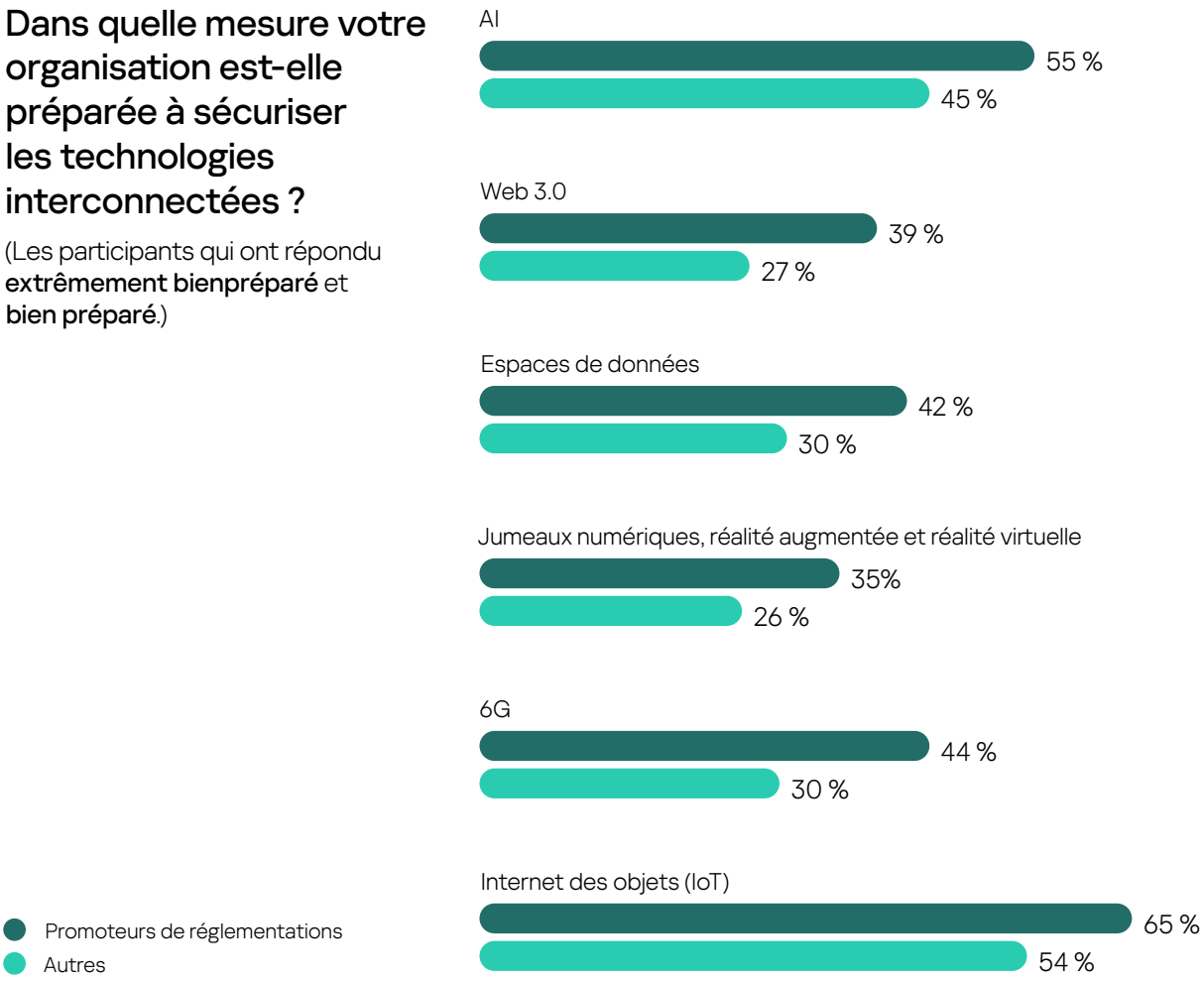
**27 %**

de ceux qui ne respectent pas encore les réglementations et les normes en matière de sécurité

## Dans quelle mesure votre organisation est-elle préparée à sécuriser les technologies interconnectées ?

(Les participants qui ont répondu **extrêmement bienpréparé** et **bien préparé**.)

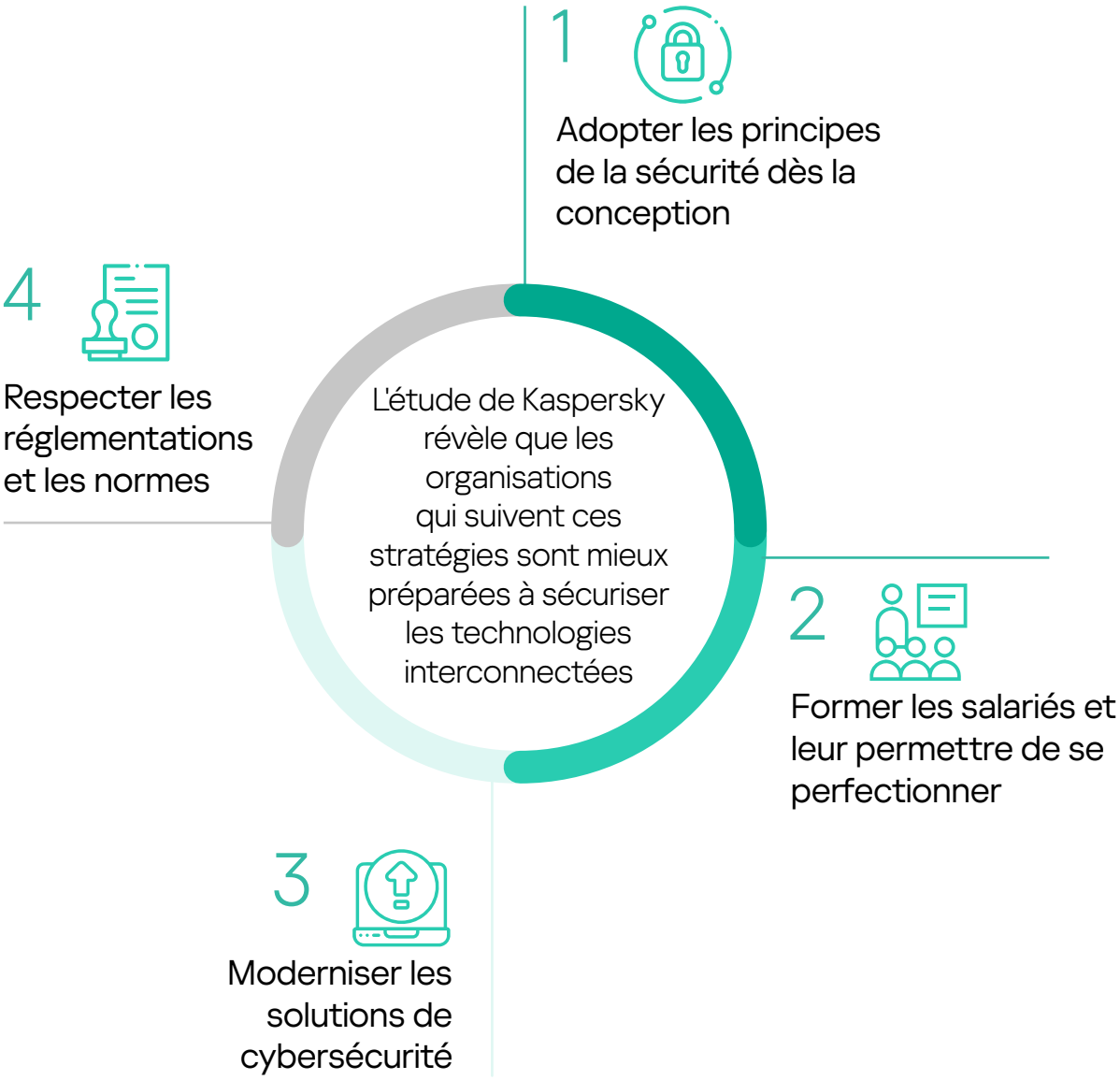
## Niveau de préparation par technologie : les promoteurs de réglementations par rapport aux autres




## Trois questions pour l'équipe de direction

1. Respectons-nous toutes les normes et réglementations en matière de sécurité ?
2. Devons-nous respecter toutes les normes et réglementations en matière de sécurité ? Comment les classer par ordre de priorité ?
3. Comment instaurer la confiance numérique par le biais de nos processus de conformité en matière de cybersécurité ?

# Quatre façons de maximiser le succès des technologies interconnectées tout en minimisant les risques




Les technologies interconnectées offrent d'immenses possibilités commerciales, mais elles ouvrent également la voie à une nouvelle ère de vulnérabilité face à de graves cybermenaces. Avec la multiplication des données collectées et transmises, les mesures de cybersécurité doivent être renforcées. Les entreprises devraient utiliser les quatre stratégies présentées dans ce rapport pour protéger leurs ressources critiques et renforcer la confiance de leurs clients dans un contexte où les appareils sont de plus en plus interconnectés. Les dirigeants doivent veiller à ce que leurs ressources en matière de cybersécurité soient suffisantes pour leur permettre d'utiliser de nouvelles solutions de cybersécurité capables de relever les défis à venir de la technologie interconnectée.

**kaspersky.fr**

kaspersky

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