Rapport des Tendances 2024

Alors que le monde de la technologie continue de se développer à un rythme accéléré, il est essentiel pour les entreprises de rester à jour avec ces changements.

Dans cet esprit, nous avons compilé notre tout premier **Rapport des Tendances pour 2024**.

Ce rapport offre des informations pertinentes sur le paysage des Technologies de l'Information en abordant des sujets tels que la pénurie de main-d'œuvre en TI, la sécurité du nuage, le ZTNA et l'impact de l'intelligence artificielle (IA)

Pénurie de main-d'œuvre en TI :

Avec une demande mondiale croissante pour les professionnels en TI, des pays comme les États-Unis, l'Inde et la Chine sont à la tête de la pénurie de main-d'œuvre. Les rôles particulièrement difficiles à combler comprennent ceux au tour de la sécurité du nuage.
Pour résoudre ce problème, il faut développer des ressources et des compétences internes, avec une emphase sur l'équilibre vie professionnelle-vie privée pour retenir les talents.

Sécurité du Nuage :

Alors que de plus en plus d'organisations adoptent les technologies cloud, des inquiétudes concernant une bonne configuration et la sécurité s'intensifient. Le manque de compétences en matière de gestion de sécurité du nuage ralentit le taux d'adoption.
Les stratégies clés pour l'amélioration comprennent la formation, la sélection de la bonne architecture et les bons contrôles de sécurité à appliquer.

ZTNA (Zero Trust Network Access) :

Pratiquement tous les leaders TI mettent en œuvre, ou prévoient d'adopter le ZTNA comme moyen d'améliorer les mesures de cybersécurité. Stimulée par le travail à distance et des menaces en constante évolution, l'adoption du ZTNA n'est pas sans ses défis.
Avec un personnel limité et des limitations au niveau des budgets, une approche stratégique comprenant un déploiement par phases, est recommandée.

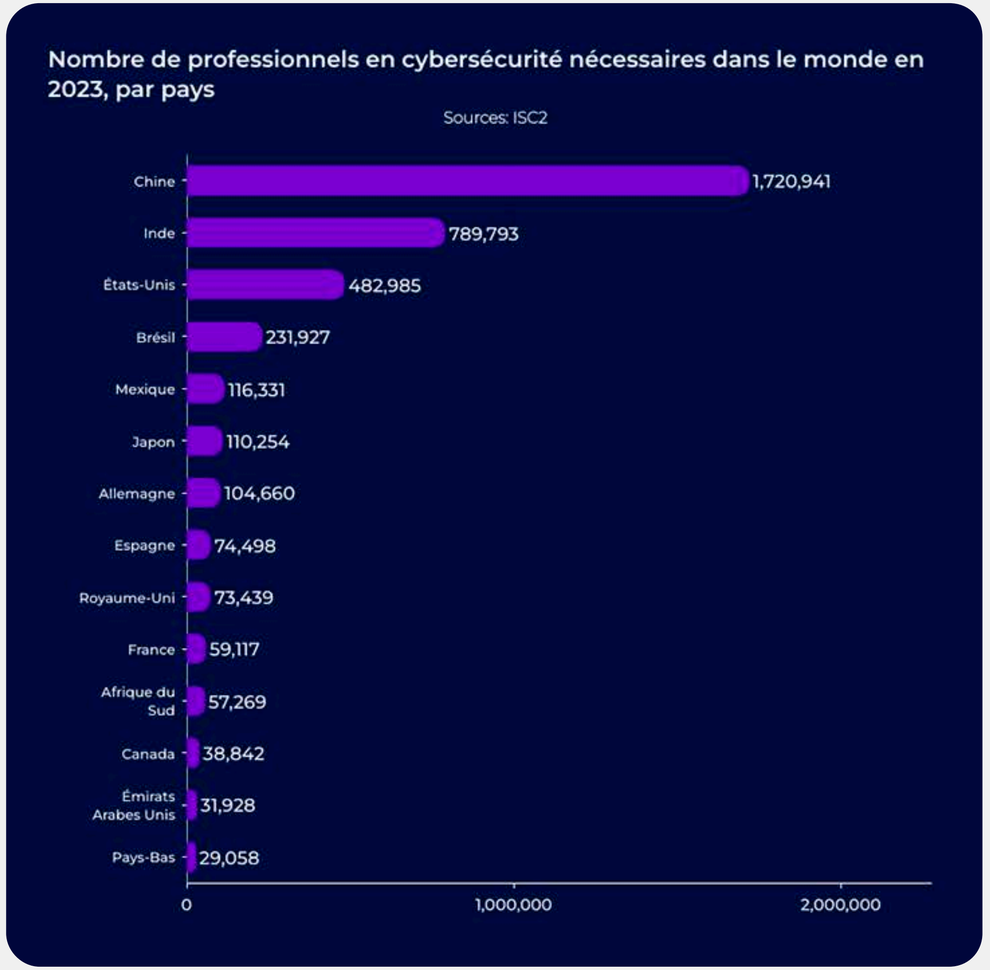
Intelligence artificielle (IA) :

Les progrès rapides de l'IA offrent des opportunités dans plusieurs secteurs, particulièrement dans le secteur de la santé, du marketing et de la vente. Cependant, la forte demande et le manque de personnel qualifié ainsi que des préoccupations éthiques sont des barrières qui peuvent ralentir l'adoption de ces technologies. Les entreprises doivent donc équilibrer la valeur et le risque qui accompagnent l'IA, tout en explorant les opportunités pour ne pas rester derrière.

Pénurie de main-d'œuvre en IT

Résumé

Environ 60% des entreprises affirment avoir une main-d'œuvre en cybersécurité sous-staffée selon une enquête de l'ISACA. Cette charge de travail rend évident que le stress et les déséquilibres entre la vie professionnelle et la vie privée dans le domaine sont significatifs. Au-delà des connaissances techniques, les employeurs recherchent des compétences en résolution de problèmes, travail d'équipe et communication. Les certifications comme le CISSP sont populaires parmi les professionnels de la sécurité. Parmi les postes les plus difficiles a combler on retrouve; la Sécurité du Nuage, Security Opérations et Sécurité du réseau.



Facteurs

- Les postes en TI augmentent plus rapidement que le taux de candidats compétents qui embarquent sur le marché du travail.
- La tendance est également influencée par une baisse d'inscriptions dans les programmes informatiques.

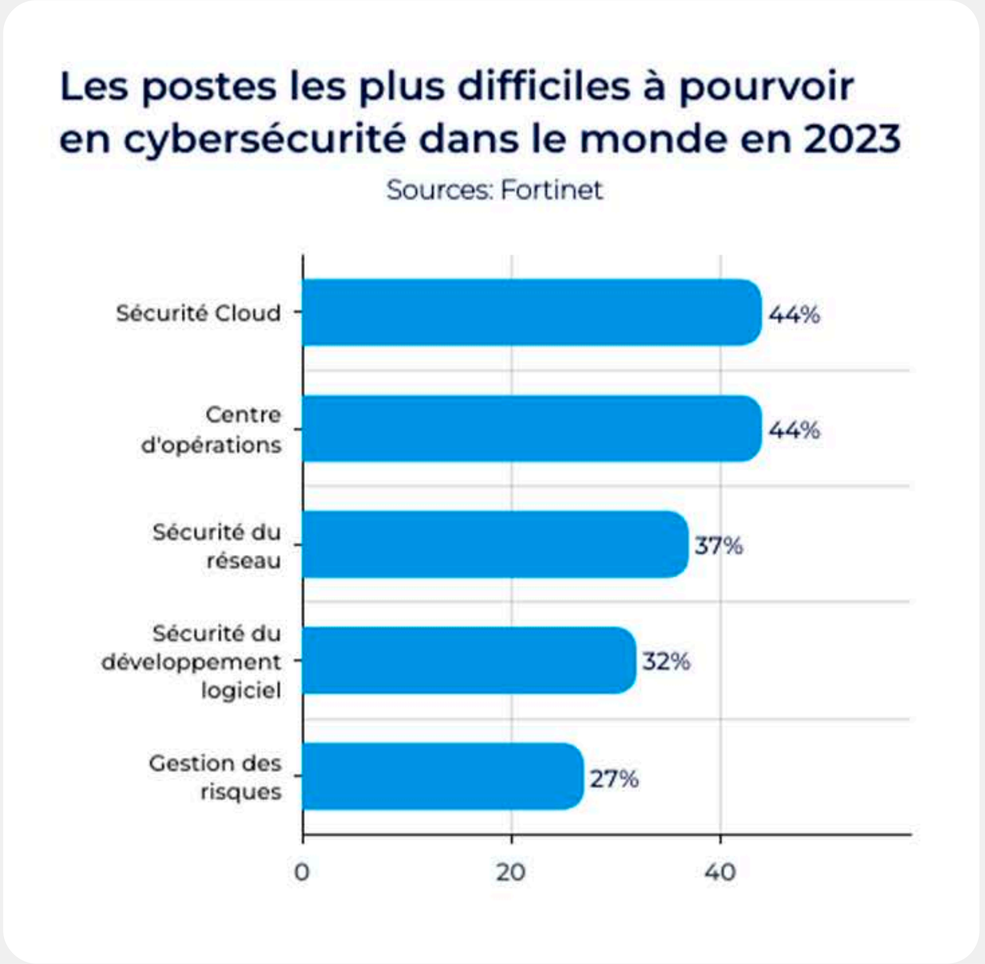
Défis

- Selon une enquête de Gartner, 20% des candidats potentiels sont activement à la recherche d'un emploi, avec plus de la moitié étant des chercheurs d'emploi passifs.
- Il y a un déficit de talents dans le marché du travail en TI, qui peine à répondre aux demandes de compétences avancées.
- Une enquête de PWC révèle que 59% des entreprises sentent un manque de personnel en cybersécurité.
- Les principales raisons pour lesquelles les professionnels de la cybersécurité quittent leurs postes comprennent : les chasseurs de têtes, des compensations financières insuffisantes, des opportunités limitées de promotion ou de développement, des niveaux de stress élevés et un manque de soutien de la part des équipes de direction

- Les rôles les plus difficiles à combler sont souvent ceux impliquant des compétences en sécurité du nuage et en gestion des identités/accès.
- Le temps requis pour pourvoir un poste en cybersécurité est souvent long, s'étendant sur plusieurs mois.

Recommandations

- Transformer les descriptions des postes en offres captivantes qui non seulement décrivent les compétences nécessaires, mais inspirent également les candidats à faire partie de votre équipe.
- Assurer un équilibre sain entre la vie professionnelle et la vie privée dans votre équipe.
- Lors de l'évaluation des candidats, considérer aussi leur capacité à travailler en équipe, à ressourdre des problèmes et communiquer afin de s'assurer qu'ils s'adapteront bien à votre équipe.
- Effectuer régulièrement des analyses de benchmarking pour les salaires et intégrer de la flexibilité dans votre stratégie de rémunération.
- Investir dans les certifications dans le cadre de vos programmes de formation et de développement.
- Fournir des conditions de travail flexibles et encourager les initiatives de diversité, d'équité et d'inclusion pour attirer un plus large bassin de candidats.
- Automatiser certains aspects du travail en utilisant la technologie pour réduire les tâches répétitives et améliorer la satisfaction au travail.
- Être plus ouvert à l'embauche de candidats avec moins d'expérience qui peuvent évoluer avec votre équipe.



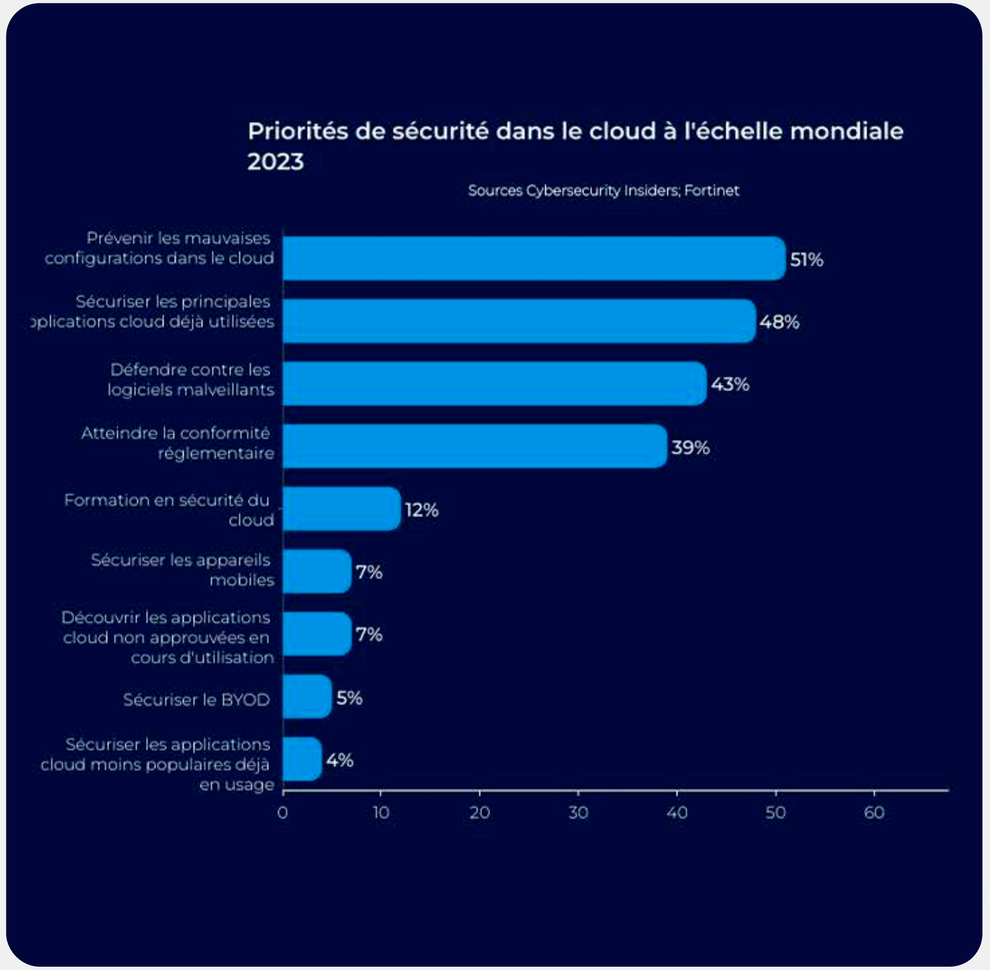
Sécurité du Nuage

Résumé

Malgré l'adoption continue du nuage, plusieurs facteurs comme le manque de connaissances et manque de personnel posent des préoccupations importantes parmi les professionnels des TI.

Facteurs

- Les mesures de protection des données varient entre les environnements cloud et les environnements sur site.
- Les sauvegardes sont courantes dans les deux types d'environnement, en revanche l'authentification à plusieurs facteurs est plus répandue dans le nuage. Pour les environnements sur site, les entreprises mettent moins d'importance sur la prévention de la perte de données (DLP) comparativement au nuage.
- Les incidents de sécurité les plus courants dans le nuage sont l'hameçonnage, les attaques ciblées sur l'infrastructure, et les comptes d'utilisateur compromis.

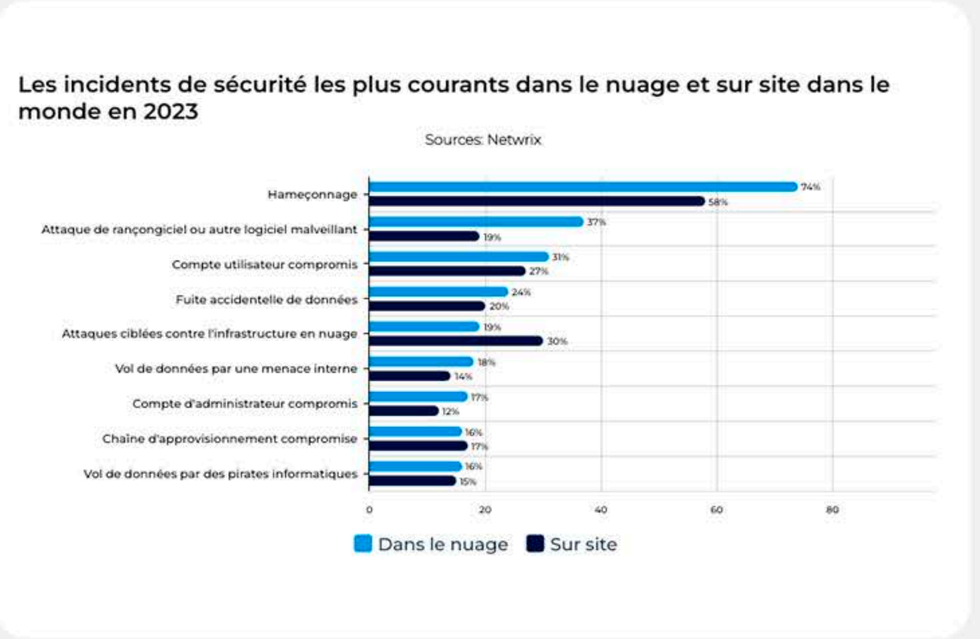


Défis

- La capacité à sécuriser les environnements cloud est exacerbée par le manque de professionnels formés.
- Les rôles en cybersécurité du nuage sont très recherchés par les entreprises, mais difficiles à pourvoir.
- Une mauvaise configuration du nuage est la cause la plus courante de brèches.
- Les principales priorités pour les entreprises en matière de sécurité nuage sont : sécuriser leurs environnements et se défendre contre les maliciels.
- Les environnements multi-cloud posent des défis. Il faut premièrement s'assurer d'avoir les bonnes ressources pour la gestion et deuxièmement pour assurer la protection et la confidentialité des données.

Recommandations

- Assurez-vous que votre équipe est équipée des connaissances nécessaires pour prendre des décisions éclairées sur le type de nuage et les contrôles appropriés à employer.
- Au niveau des affaires, définissez des objectifs de sécurité clairs pour protéger les personnes, les données et la réputation de votre marque.
- Identifiez et atténuez les risques techniques associés aux objectifs commerciaux souhaités.
- Une fois que l'architecture optimale a été définie, déterminez les contrôles de sécurité à appliquer.
- Offrez des opportunités de formation et de certification pour rester à jour avec les avancements et les exigences de cybersécurité.
- Envisagez d'employer des contrôles tiers si vous avez des environnements multi-cloud pour obtenir une interface utilisateur homogène, l'unification des politiques et une gestion simplifiée.



- Mettez en œuvre des mesures de sécurité phase par phase, sécurisant d'abord les applications sensibles en élargissant progressivement le champ d'application de ces mesures.
- Envisagez d'utiliser un accès réseau Zero Trust (ZTNA) sans client pour remplacer le VPN et incorporer le ZTNA basé sur des agents dans un cadre plus large de Secure Access Service Edge (SASE).

Zero Trust Network Access (ZTNA)

Sommaire

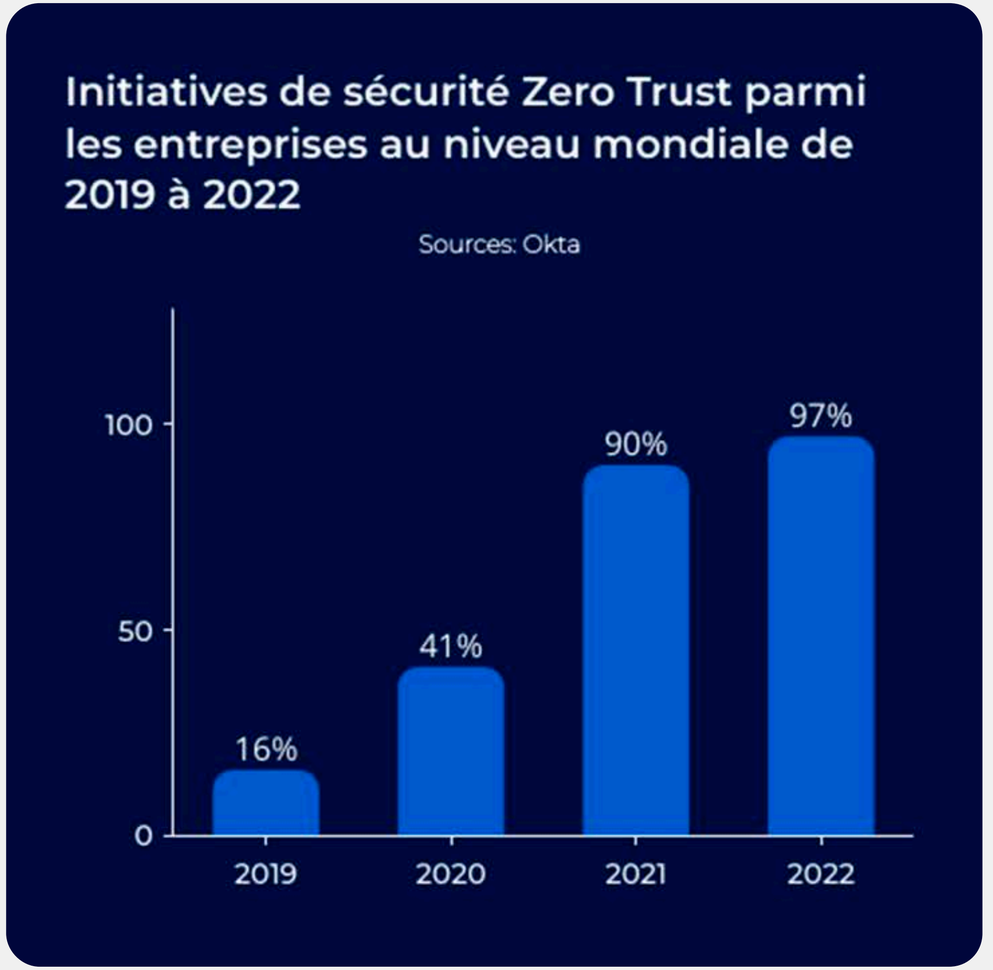
L'approche de sécurité Zero Trust Network Access (ZTNA) est largement acceptée par les dirigeants informatiques comme une méthode viable pour améliorer la cybersécurité. La consolidation des produits chez les fournisseurs intègre de plus en plus le ZTNA dans leurs solutions d'architecture SASE et SSE

Facteurs

- L'essor du travail à distance et des environnements de travail flexibles
- L'évolution des menaces
- Les changements dans les limites des réseaux
- L'intérêt croissant pour le marché du ZTNA est motivé par les organisations ayant besoin de sécuriser leurs end-points et l'adoption du nuage.

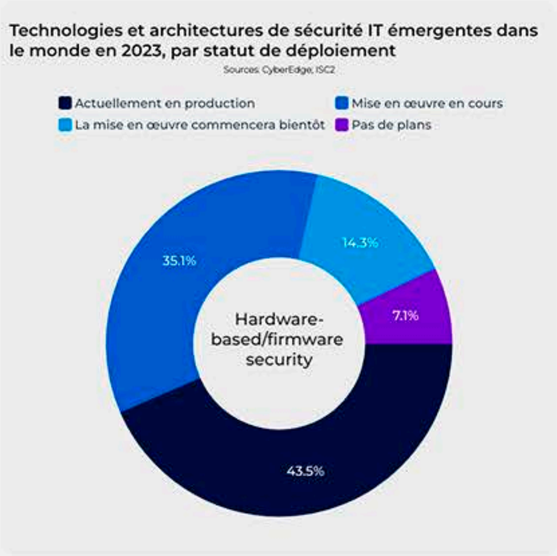
Défis

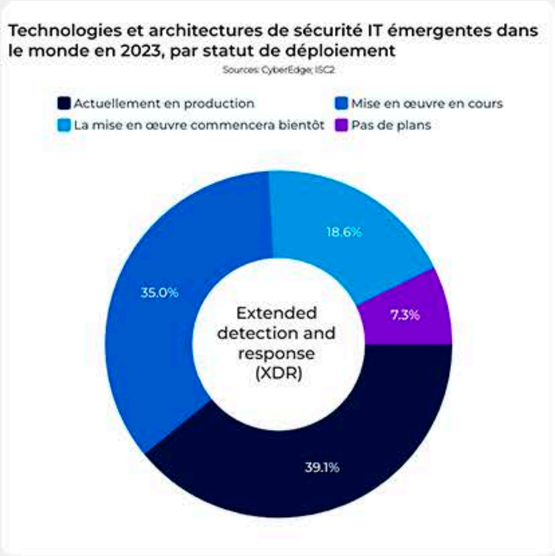
- Le manque de ressources qualifiées représente un obstacle majeur à l'adoption du ZTNA.
- Les organisations sont confrontées à des obstacles au niveau du leadership, des technologiques obsolètes et des contraintes budgétaires.
- Le manque de compréhension et de sensibilisation à propos du ZTNA parmi les professionnels de l'informatique pose un défi à sa mise en œuvre.

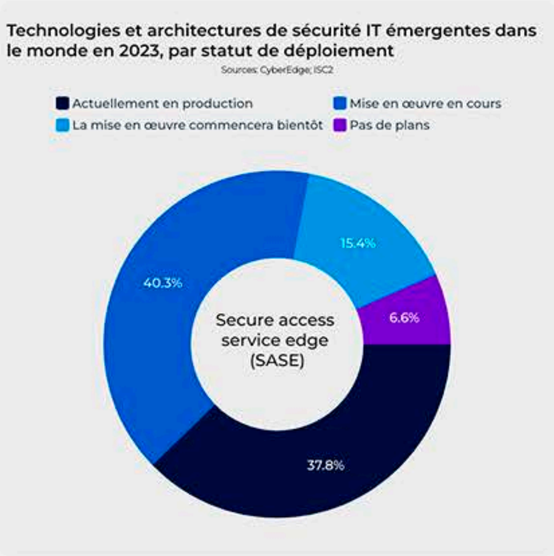


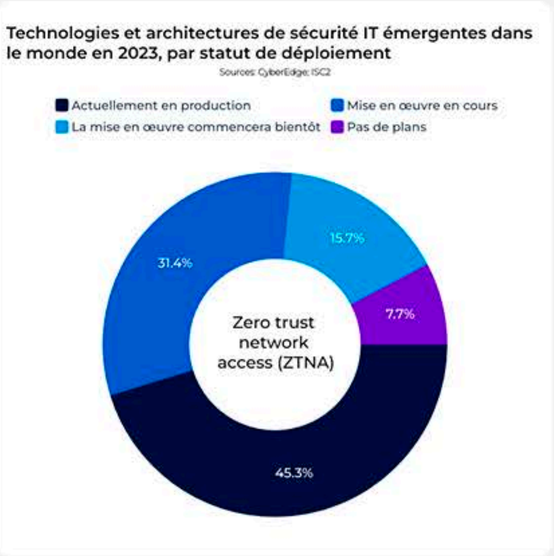
Recommandations

- Formulez une stratégie Zero Trust complète en mettant l'accent sur l'atténuation des risques et une gestion solide et avancé de l'identité et des accès avant d'opter pour les solutions ZTNA.
- Déployez le Zero Trust de manière graduelle, sécurisant d'abord les applications sensibles, puis élargissant le champ d'application par la suite.
- Priorisez le remplacement du VPN par le ZTNA sans client et intégrez le ZTNA basé sur des agents dans un cadre plus large du Secure Access Service Edge (SASE).
- Choisissez des fournisseurs qui répondent aux prérequis de sécurité, minimisent les points d'attaque et soutiennent des politiques de contrôle d'accès dynamiques conformes aux normes du zero trust.
- Expliquez à l'équipe de direction qu'une approche Zero Trust est un concept de sécurité plutôt qu'un produit.





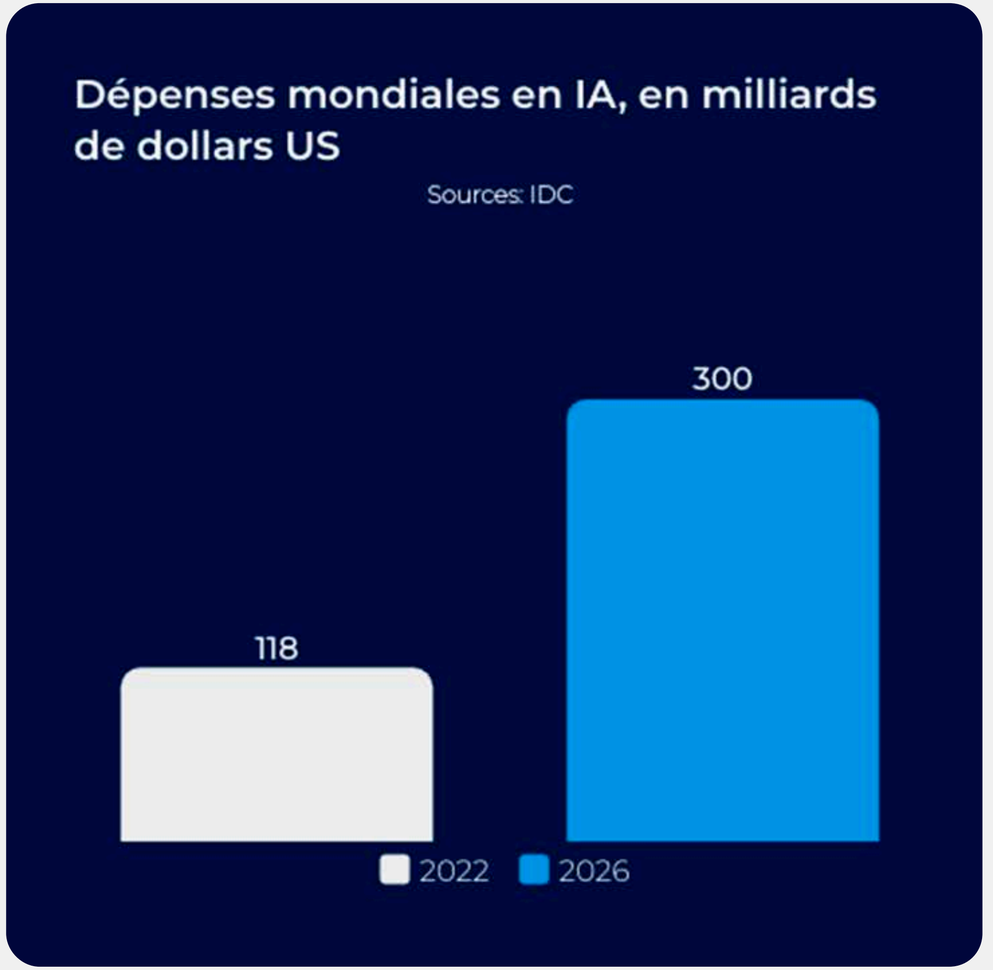




Intelligence Artificielle (IA)

Résumé

L'Intelligence artificielle (IA) est actuellement composée de l'apprentissage automatique, de la robotique, des Réseaux de Neurones Artificiels (RNA) et du Traitement du Langage Naturel (TLN). Le progrès rapide des techniques d'IA, avec l'IA générative prévue pour se développer davantage en 2024, laisse souvent les entreprises qui n'ont pas la capacité d'explorer et d'intégrer ces technologies derrière. Pour gérer efficacement de telles innovations, les organisations font des investissements stratégiques dans des actifs d'IA essentiels tels que l'acquisition de talents, le développement d'une culture qui encourage l'innovation expérimentale et une gestion structurée des données et de la gouvernance.



Facteurs

- La portée croissante de l'IA et son potentiel pour révolutionner les industries poussent les organisations à investir dans cette technologie innovante.
- La disponibilité croissante de données et les progrès en matière de puissance de calcul permettent le développement et l'application de techniques d'IA avancées.
- Les organisations sont également motivées par le potentiel de réduction des couts , d'une augmentation dans l'efficacité et les avantages concurrentiels que peut fournir l'IA.
- Le nombre croissant et la complexité des cybermenaces nécessitent des solutions avancées et automatisées telles que l'IA.
- Les économies potentielles et les gains d'efficacité de la mise en œuvre de l'IA favorisent son adoption dans le domaine de la cybersécurité.
- Les outils alimentés par l'IA peuvent traiter et analyser de vastes quantités de données rapidement et précisément, fournissant des informations pertinentes pour la détection des menaces.

Défis

- Trouver des professionnels qualifiés, pour combler des rôles tels qu'ingénieur ou architecte de données, est un défi majeur.
- L'émergence d'applications d'IA non éthiques.

Recommandations

L'Intelligence artificielle (IA) a déjà eu un impact significatif sur le paysage des affaires, et sa puissance transformatrice continuera de façonner l'avenir. Pour rester en tête de la concurrence et maximiser l'efficacité grâce à l'intégration de l'IA, nous proposons la mise en œuvre des stratégies suivantes :

- Intégrer les informations de l'entreprise avec l'IA pour un avantage concurrentiel ; utiliser l'IA générative pour l'analyse de données.
- Adoptez une approche systématique de l'IA, intégrant les modèles, le code et les données au sein de grands écosystèmes ; et anticiper la rationalisation des applications.
- Combler l'écart de compétences en améliorant les compétences des parties prenantes et du personnel informatique pour une gestion efficace des systèmes d'IA.
- Équilibrez les avantages et les risques de l'IA en poursuivant une valeur à l'échelle de l'écosystème, en créant divers cas d'utilisation et en adoptant des approches itératives pour faciliter l'évolution de votre stratégie.

Conclusion

Nous espérons que vous avez trouvé ces informations utiles.

Merci pour votre temps et votre intérêt pour notre rapport des Tendances 2024.

Nous continuerons à surveiller ces sujets et à les développer dans les mois à venir afin de vous aider à suivre ces tendances.

Des suggestions? Vos commentaires sont importants pour améliorer la qualité du contenu que nous fournissons.

Sources :

- 5 Best Practices for CIOs to Effectively Attract and Hire Top IT Talent - Gartner
- Artificial Intelligence Primer for 2024
- Market Guide for Zero Trust Network Access, 14 August 2023 - Gartner.
- Digital & Trends - Artificial intelligence: in depth market analysis
- Digital Trends – Cloud Security - Statista Report.
- Digital trends – ZTNA – Statista Report
- Digital trends – IT Skills
- Industries & Markets - Artificial Intelligence (AI) In business
- https://www.govtech.com/
- Ethical concerns mount as AI takes bigger decision-making role — Harvard Gazette