

La sécurité de l'IA, les services financiers et le Zero Trust

Une approche stratégique de la cybersécurité à l'ère de l'IA

Descriptif de la solution

© 2024 Zscaler, Inc. Tous droits réservés.

Synthèse : naviguer à vue parmi les menaces

À l'ère de l'IA, les services financiers sont confrontés à une litanie de menaces furtives et d'incertitudes, où chaque interaction peut présenter un risque. Tout comme nous ferions preuve d'une extrême prudence dans un environnement dangereux et versatile, les services financiers doivent aborder la sécurité de l'IA avec vigilance. Ce document décrit les mesures que ces entreprises peuvent prendre pour se protéger dans un environnement résolument orienté IA.

Nous allons explorer la manière dont l'IA change l'univers des menaces, donnant lieu à des fraudes optimisées par l'IA et des cyberattaques automatisées. De plus, nous mettrons en évidence les principales tendances et prévisions, afin d'aider les entreprises à anticiper l'impact de l'IA et à y répondre de manière stratégique.

Dans cet environnement à risque, où aucune entité, interne ou externe, n'est digne de confiance, le Zero Trust est une arme redoutable. Ce document propose aux financiers un cap clair pour migrer vers le Zero Trust, via des étapes concrètes qui garantiront un avenir sûr et résilient pour l'IA.

L'IA et l'évolution des menaces

L'IA transforme rapidement les menaces, introduisant des risques complexes qui remettent en question les modèles de sécurité traditionnels. Les attaques ont évolué et sont devenues plus efficaces à grande échelle, permettant aux victimes de poursuivre leurs activités tandis que les hackers menacent d'exposer leurs données.
Bien qu'il existe de nombreuses tendances et prédictions en matière d'IA, nous allons nous pencher sur trois tendances pour 2024–2025 qui évoluent rapidement.

Trois tendances à surveiller sur 2024–2025

Développement de l'IA

Les grands modèles de langage (LLM) de l'IA ont transformé notre façon d'aborder une IA générative qui va désormais au–delà des résultats restreints et spécifiques à une tâche pour donner vie à des solutions plus dynamiques et contextuelles. Mais comme dans le monde physique, tout, y compris l'IA, continuera d'évoluer.

La notion de mystère fait référence au sentiment déstabilisant qu'éprouvent les gens lorsque l'IA devient presque – mais pas tout à fait – indiscernable des humains, créant un sentiment de malaise en raison d'une imitation presque parfaite.

L'IA générative, et ChatGPT en particulier, ont gagné leurs lettres de noblesse après avoir atteint 100 millions d'utilisateurs en deux mois, ce qui est remarquable. Maintenant qu'ils ont franchi ce cap, d'autres évolutions à venir pourraient présenter un impact plus important sur le plan neurologique et cognitif que la seule IA générative.

Attaques de ransomware sans chiffrement

Historiquement, le chiffrement était au cœur de la stratégie des ransomwares : détourner vos données, demander une rançon, et si vous ne payez pas, vos données deviennent inaccessibles et votre activité est à l'arrêt.

© 2024 Zscaler, Inc. Tous droits réservés.

Cependant, au fil du temps, les opérateurs de ransomware ont compris qu'en réduisant le montant de la rançon demandée et en n'obérant pas l'activité de la victime, ils obtiendraient sans doute de meilleurs résultats. Supposons par exemple qu'ils réduisent la rançon de 10 à 2 millions de dollars et que les chances de se faire payer passent de 5 % à 70–80 %. C'est ce qu'on peut nommer un bon business model pour les ransomwares, non ? Et c'est précisément ce principe qui sous-tend le ransomware sans chiffrement.

Ces ransomwares s'emparent des données, vous menacent et, dans de nombreux cas, vous laissent poursuivre vos activités.

En ne mettant pas votre entreprise à l'arrêt, les dommages à votre réputation sont moindres. Les hackers peuvent également essayer de convaincre les victimes de ne pas divulguer la rançon aux instances de réglementation puisque son montant n'est pas si élevé au final.

Attaques de ransomware optimisées par l'IA

Les attaques de ransomware optimisées par l'IA sont plus efficaces pour améliorer la rentabilité, l'impact et l'automatisation des attaques. Dans ce cas, les hackers exploitent l'IA pour automatiser et améliorer la sophistication des cyberattaques, les rendant plus rapides, mieux ciblées et plus difficiles à détecter.

Les services financiers : quatre façons de survivre et de prospérer à l'ère de l'IA

L'utilisation de l'IA en entreprise est en plein essor, tout comme les risques qu'elle comporte. Quatre niveaux de réflexion stratégique peuvent guider les services financiers dans les méandres complexes d'un monde en constante évolution axé sur l'IA.

En 2024, l'utilisation des outils d'IA/AA a bondi de 594 % et l'utilisation de ChatGPT s'est amplifiée de 634 % (Rapport 2024 de Zscaler ThreatLabz sur la sécurité de l'IA).

Politique et éthique

Les services financiers doivent élaborer des politiques globales qui encadrent l'utilisation éthique de l'IA, pour garantir le respect de la réglementation et renforcer la confiance des clients. Ceci implique d'élaborer un cadre pour la confidentialité des données, la transparence des algorithmes et la maîtrise des biais, en mettant l'accent sur des pratiques responsables en matière d'IA.

Cœur de métier

Quel est l'impact de l'IA sur le cœur de métier des entreprises ? Harvard Business Review a réalisé une étude qui révèle une différence statistiquement significative de la performance des entreprises qui utilisent l'IA par rapport à celles qui ne l'utilisent pas dans un secteur donné, et que cet écart continue de se creuser.

Alors, comment comptez-vous intégrer l'IA dans votre entreprise ? Allez-vous le faire avec un partenaire ou de manière autonome ? Serez-vous propriétaire de vos propres modèles ? Serez-vous partie prenante dans des modèles plus vastes ? Et quel est le cas d'utilisation concerné ?

Les entreprises doivent évaluer en quoi l'IA peut enrichir leurs opérations, qu'il s'agisse d'améliorer le service client, d'optimiser les processus métier ou de prendre des décisions basées sur les données.

© 2024 Zscaler, Inc. Tous droits réservés.

Les entreprises doivent évaluer en quoi l'IA peut enrichir leurs opérations, qu'il s'agisse d'améliorer le service client, d'optimiser les processus métier ou de prendre des décisions sur la base de données. En identifiant les domaines essentiels où l'IA apporte une valeur ajoutée, les services financiers peuvent s'octroyer des avantages concurrentiels et stimuler l'innovation dans le droit fil de leurs objectifs stratégiques.

R&D et infrastructure

Comment gérer l'arrivée des outils d'IA dans les entreprises ? Investir dans une infrastructure robuste et adaptée aux capacités d'IA, telles que le cloud computing, le traitement analytique du big data et l'apprentissage automatique, permettra aux entreprises d'exploiter les technologies émergentes et de développer de nouvelles solutions pour répondre à l'évolution des besoins des clients.

Avantages en matière de cybersécurité

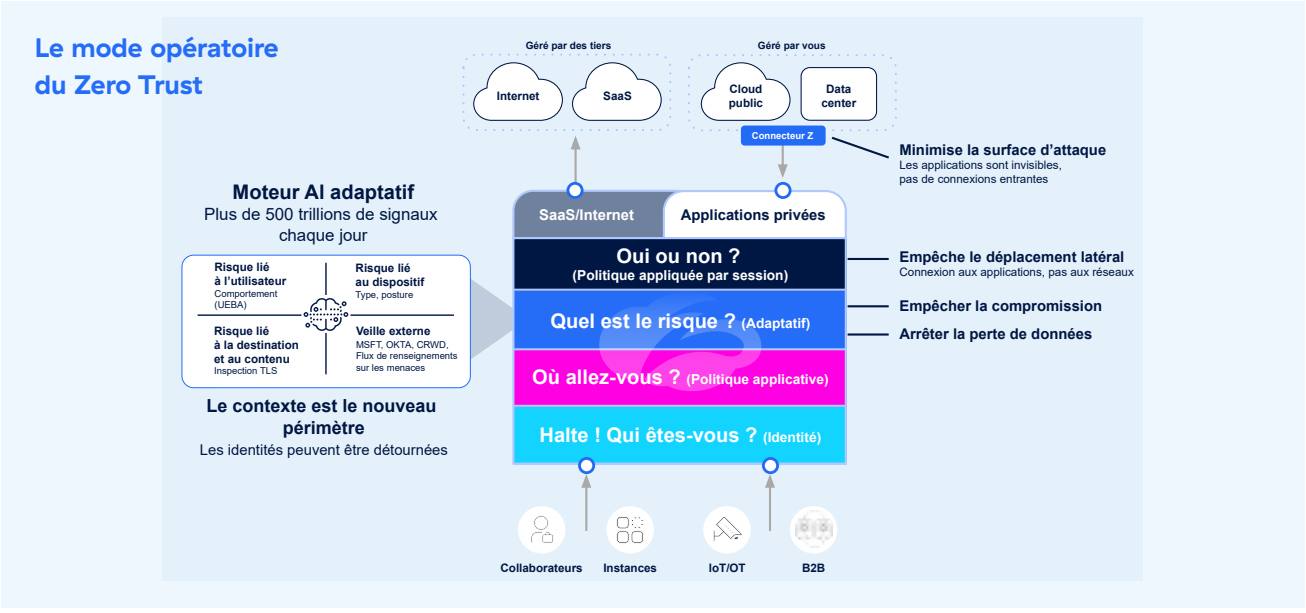
Les institutions financières peuvent améliorer leur posture de cybersécurité en faisant appel à des solutions de sécurité qui exploitent l'IA pour identifier les menaces et y répondre en temps réel.

Posez-vous ces questions : quels sont les avantages — ou les menaces potentielles — pour l'IA et la cybersécurité ? Comment va-t-elle être utilisée contre vous ? Comment vous y préparer ? En déployant des mesures de sécurité optimisées par l'IA, les entreprises peuvent mieux protéger leurs données et ressources sensibles et assurer leur résilience face à des menaces sophistiquées.

Le Zero Trust et la gestion des cyber-risques

Même si l'utilisation de l'IA en entreprise s'accélère, les entreprises bloquent **18,5 %** de toutes les transactions d'IA, soit un bond**de 577 %,** ce qui témoigne de préoccupations croissantes en matière de sécurité (Rapport Zscaler ThreatLabz 2024 sur la sécurité de l'IA). Le Zero Trust est la meilleure défense dans cet environnement à risque, où aucune entité, à l'intérieur ou à l'extérieur de l'entreprise, ne peut être considérée comme fiable.

Le Zero Trust est la stratégie qui nous aide à discerner les menaces en n'autorisant que ce dont l'entreprise a besoin, quand elle en a besoin. Déployer une approche Zero Trust qui ne fait confiance à rien ni personne (utilisateur, instance, appareil ou une autre société) permet de réduire considérablement les cyber-risques :



© 2024 Zscaler, Inc. Tous droits réservés.

1. Authentifier l'identité : Stop ! Qui êtes-vous ?

a. Qui se connecte ?

b. Quels sont les attributs ?

c. Où va la connexion ?

2. Contrôle de la politique de l'application : où comptez-vous aller ?

a. Quelle est votre destination ? À cette étape, le Zero Trust évalue le risque en fonction d'éléments de contexte, ce qui permet d'éviter les compromissions et les pertes de données.

3. Risque contextuel adaptatif : Quel est le risque ?

a. Quel est le risque ? Prévenir les compromissions et les pertes de données en évaluant le risque lié à l'utilisateur, au dispositif, à la destination et au contenu, ainsi que les informations de veille fournies par des tiers (Okta, CrowdStrike, etc.).

4. Appliquer la politique

a. Empêcher les déplacements latéraux afin de se connecter aux applications et non aux réseaux.

b. Appliquer une politique pour les connexions SaaS/Internet sur la base des sessions et des utilisateurs. Applications privées — Minimiser la surface d'attaque afin que les applications soient invisibles et qu'aucune connexion entrante ne soit possible.

Migrer vers le Zero Trust

Pour protéger votre entreprise contre le nombre croissant de cybermenaces optimisées par l'IA, il est essentiel de s'engager dans une démarche Zero Trust. Déployer le Zero Trust s'inscrit dans un processus progressif, décomposé en étapes qui s'alignent sur les priorités de l'entreprise et les objectifs de sécurité. Votre sécurité progressera d'une manière qui est à la fois évolutive et résiliente.

1. Sécuriser les effectifs

a. Phase 1A — pas de changement de réseau

i. Cybersécurité et protection des données, expérience numérique et quantification des risques

b. Phase 1B — simplification du réseau

i. Zero Trust pour les sites distants/café internet, stratégie avancée de cybersécurité et de protection des données, et obtention de perspectives business

2. Sécuriser les instances

a. Cybersécurité et protection des instances

b. Segmentation des instances avec le Zero Trust

3. Accès de tiers

a. Accès Zero Trust aux applications tierces

b. Connectivité Zero Trust vers les sites tiers

4. Sécuriser les dispositifs (IoT/OT)

a. Cybersécurité et protection des données pour l'IoT/OT

b. Connectivité Zero Trust pour l'IoT/OT

© 2024 Zscaler, Inc. Tous droits réservés.

Conclusion

Le Zero Trust offre la meilleure ligne de défense dans un contexte actuel en évolution rapide, où aucune entité, à l'intérieur ou à l'extérieur de l'entreprise, ne peut être intrinsèquement digne de confiance. Alors que la technologie et l'IA continuent d'évoluer et finissent par converger, l'adoption d'une stratégie Zero Trust garantit que seuls les utilisateurs et processus légitimes accèdent à ce qui est nécessaire, et quand c'est nécessaire. Vous gagnez ainsi en résilience et pérennisez votre activité métier.

Maîtrisez vos risques cyber et faites vos premiers pas vers le Zero Trust en consultant zscaler.com/fr.

À propos de l'auteur



Avec plus de trente ans d'expérience en tant qu'entrepreneur, expert en sécurité de l'information et cadre dans des sociétés telles que RSA, Arbor Networks, CA, McAfee, Cybereason et bien d'autres, Sam Curry se consacre à accompagner les organisations pour qu'elles déjouent les cybermenaces, concrétisent la promesse d'une sécurité robuste, et contribuent à un monde protégé, fiable et connecté. Sam Curry est actuellement vice-président et RSSI chez Zscaler. Pendant son temps libre, il donne des conférences, anime un podcast (On the Hook), siège à divers conseils d'administration et publications et est un mentor InfoSec. Suivez-le sur LinkedIn.

zscaler™ | Experience your world, secured.™

À propos de Zscaler
Zscaler (NASDAQ : ZS) accélère la transformation numérique pour améliorer l'agilité, l'efficacité, la résilience et la sécurité de ses clients. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et les pertes des données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Adossé à plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur un SSE, constitue la plus vaste plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **zscaler.com/fr** ou suivez-nous sur Twitter **@zscaler**.

©2024 Zscaler, Inc. Tous droits réservés. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ et les autres marques commerciales répertoriées sur **zscaler.com/fr/legal/trademarks** sont soit 1) des marques déposées ou marques de service, soit 2) des marques commerciales ou marques de service de Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs.

+1 408 533 0288 Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134 zscaler.com/fr