

Le secteur de la finance demeure le plus engagé dans l'adoption de l'intelligence artificielle



L'ESSENTIEL

Principales conclusions du rapport 2026 de ThreatLabz sur la sécurité de l'IA

L'intelligence artificielle n'est plus une technologie émergente ni un ensemble d'outils distincts. Il s'agit d'une infrastructure toujours active, qui traite les données, soutient la prise de décision et accélère les opérations. En 2025, Zscaler ThreatLabz a analysé 989,3 milliards de transactions d'IA/AA au sein du Zscaler Zero Trust Exchange™, offrant une visibilité précise sur la manière dont les entreprises utilisent et restreignent l'IA à grande échelle. Le secteur des services financiers se situe au cœur de cette transformation.

Pour la deuxième année consécutive, le secteur Finance et Assurance a représenté la plus grande part du trafic IA en entreprise, soit **23,3 % du trafic IA/AA mondial**, avec **230 milliards de transactions pour la seule année 2025**. Les institutions financières se trouvent ainsi en première ligne, tant en matière d'adoption de l'IA que d'exposition aux risques associés.

230 milliards de transactions : L'IA à l'échelle opérationnelle

Le secteur Finance et Assurance a généré près de 40 milliards de transactions d'IA/AA de plus que le deuxième secteur le plus actif, consolidant sa position de principal utilisateur de l'IA en entreprise.

Une grande partie de cette activité provient d'applications de productivité largement utilisées. L'analyse de ThreatLabz a identifié Grammarly, ChatGPT et Microsoft Copilot comme les applications d'IA les plus utilisées au sein des organismes financiers. Leur adoption reflète l'intégration naturelle de l'IA dans des environnements où les opérations reposent sur de grands volumes de données et une analyse continue.

C'est pourquoi l'IA fait désormais partie intégrante des workflows financiers essentiels. Les cas d'utilisation les plus courants sont la synthèse de recherches et d'analyses financières, la rédaction et la révision de documents de conformité, ainsi que la détection des fraudes et l'analyse des anomalies.

À mesure que l'IA s'étend au sein de processus qui structurent les risques, la conformité et les résultats opérationnels, elle introduit de nouvelles exigences de contrôle.

39 % des transactions bloquées liées au secteur Finance et Assurance

Le secteur Finance et Assurance a également représenté la plus grande part des transactions d'IA/AA bloquées parmi tous les secteurs dans le cloud de Zscaler. Au total, le secteur a concentré 39,1 % de l'ensemble des activités IA/AA bloquées, ce qui met en évidence les risques en jeu, notamment :

- Sensibilité des données financières des clients
- Obligations réglementaires (SOX, GLBA, réglementations financières régionales, etc.)
- Risque interne et exfiltration potentielle de données
- Application incohérente ou évolutive des mesures de prévention de la perte de données (DLP)

L'ampleur des activités bloquées et des risques associés témoigne d'un changement structurel : l'IA redéfinit déjà la surface d'attaque des services financiers.

Garder une longueur d'avance
sur les risques liés à l'IA

Téléchargez

L'IA fait désormais partie intégrante de la **surface d'attaque des services financiers.**

Pour les institutions financières, l'IA n'est plus seulement un élément périphérique des systèmes centraux, elle fait partie de la surface d'attaque et doit être sécurisée en conséquence.

- Un nombre croissant de workflows financiers impliquent des interactions directes avec des applications d'IA telles que ChatGPT et Microsoft Copilot
- Un nombre croissant d'applications d'entreprise intègrent des capacités d'IA embarquées, souvent « invisibles », connectées aux données financières et aux plateformes internes
- Un nombre croissant de processus opérationnels s'appuient sur des contenus générés par l'IA pour soutenir les décisions métier et les décisions liées aux risques

Cette expansion de l'empreinte IA accroît le risque de fuite de données involontaire via les prompts et les réponses, introduit des usages de l'IA non maîtrisés ou non autorisés, et crée de nouveaux vecteurs pour les acteurs malveillants qui exploitent l'IA. La protection de la surface d'attaque liée à l'IA exige une approche de la sécurité repensée pour l'ère de l'IA.

Zscaler combine red teaming automatisé, évaluation dynamique des risques et garde-fous avancés pour valider en continu les contrôles, réduire les risques liés à l'IA et permettre une adoption sécurisée et conforme de l'IA à l'échelle de l'entreprise.



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 la perte de 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 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 X (ex-Twitter) @zscaler.

© 2026 Zscaler, Inc. Tous droits réservés. Zscaler™ et les autres marques commerciales répertoriées sur zscaler.com/fr/legal/trademarks sont soit 1) des marques déposées ou des marques de service, soit 2) des marques commerciales ou des marques de service de Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques sont la propriété de leurs détenteurs respectifs.

+1 408 533 0288

Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134

zscaler.com/fr

L'**impératif de sécurité de l'IA** pour les services financiers

Le secteur des services financiers doit sécuriser les systèmes, les applications et les interactions liés à l'IA avec le même niveau d'exigence que les autres infrastructures critiques, en garantissant une visibilité complète, une application cohérente des politiques et des protections en temps réel. **La plateforme unifiée de Zscaler pour la sécurité de l'IA** aide les institutions financières à protéger l'intégralité du cycle de vie de l'IA au sein de l'entreprise :

Identifier l'IA et les risques : recenser, cartographier et obtenir une visibilité complète sur l'ensemble de votre écosystème IA, de l'AI fantôme aux applications, modèles et pipelines à risque.

Renforcer les systèmes d'IA : protéger les modèles et réduire l'exposition aux injections de prompts, aux fuites de données et aux usages abusifs grâce à des protections à l'exécution et à des garde-fous appliqués aux systèmes critiques.

Sécuriser l'accès à l'IA : garantir un usage sûr, conforme et maîtrisé des applications d'IA via des contrôles d'accès au moindre privilège et des politiques de protection des données en ligne.

Simplifier la gouvernance de l'IA : assurer la conformité et la traçabilité grâce à une supervision continue des déploiements et des usages de l'IA.

Consultez le rapport complet pour approfondir les tendances d'adoption de l'IA, les menaces renforcées par l'IA et les recommandations de sécurité destinées aux institutions financières.

[Téléchargez](#)



**Act Fast.
Stay Secure.**