IA et cybersécurité : pour 50% des PME françaises, l'IA est une menace plutôt qu'une opportunité

Une étude IDC pour Sage révèle le paradoxe français de l'Intelligence Artificielle : alors que cette technologie s'impose comme un levier de compétitivité, les PME françaises l'abordent avec défiance, freinant son adoption stratégique.

Paris, le 19 mai 2026 – Sage, un leader des technologies de comptabilité, de finance, de ressources humaines et de paie pour les petites et moyennes entreprises (PME), dévoile aujourd'hui un rapport réalisé par IDC auprès de 2 210 entreprises de moins de 500 salariés dans 8 pays.

Ce rapport nous apprend que 50% des PME françaises estiment que l'IA a créé plus de risques en matière de cybersécurité et de confidentialité que d'opportunités business. Cette donnée place la France 9 points au-dessus de la moyenne mondiale (41%) et contraste avec une perception plus optimiste dans d'autres marchés. À l'inverse, seules 33% des PME françaises considèrent que l'IA génère plus d'opportunités que de risques, contre 37% au niveau mondial.

Cette méfiance a des conséquences directes sur l'adoption de la technologie : seules 27% des PME françaises font du développement à grande échelle de l'IA une priorité business pour les 12 prochains mois, contre 33% en moyenne mondiale. La France adopte ainsi une posture défensive face à une technologie pourtant stratégique pour la compétitivité.

Une préparation aux menaces IA quasi inexistante

Derrière cette perception se cache une réalité opérationnelle préoccupante. Seulement 2% des PME françaises se déclarent totalement prêtes à répondre aux menaces cyber liées à l'IA, soit quatre fois moins que la moyenne mondiale de 8%. Cette fragilité se traduit également par une maturité quasi nulle des dispositifs de sécurité spécifiques : 1% seulement des PME françaises disposent d'une sécurité IA mature, proactive et intégrée à leurs processus cyber, contre 6% au niveau mondial. À l'opposé, 24% n'ont déployé aucune mesure de sécurité spécifique pour leurs applications IA, contre 22% globalement.

Des incidents de cybersécurité aux conséquences plus lourdes qu'ailleurs

Cette prudence se justifie par une exposition accrue aux cyberattaques. En 2025, 15% des PME françaises ont subi un incident causant une perturbation ou une perte significative, contre 11% au niveau mondial, soit 36% d'incidents majeurs en plus. Seules 51% des PME françaises n'ont connu aucun incident sur les 12 derniers mois, contre 54% en moyenne globale.

Ces résultats s'expliquent en partie par des lacunes sur les fondamentaux de la cybersécurité. Seulement 60% des PME françaises appliquent une maintenance système régulière (mises à jour logicielles, patchs de sécurité, sauvegardes), contre 71% au niveau mondial, soit un écart de 11 points, le plus important observé sur les mesures de base. Si la protection des emails (77% vs 79% global) et des endpoints (69% vs 67% global) reste correcte, les failles sur la maintenance créent des brèches exploitables par les attaquants.

Trois défis structurels freinent les PME françaises

Pour sécuriser leurs applications IA, les PME françaises se heurtent à trois obstacles majeurs. Le manque d'expertise interne en sécurité IA arrive en tête, cité par 48% des répondants contre 45% en moyenne mondiale. La difficulté à mettre en œuvre une gouvernance des données robuste suit de près (43% contre 41% global). Enfin, 35% des PME françaises souffrent d'une visibilité limitée sur les outils IA déployés dans l'organisation, un phénomène de shadow AI spécifiquement français. À titre de comparaison, les autres pays citent davantage la difficulté à suivre le rythme des menaces émergentes comme troisième défi (36% global).

Pour **Pascal Bénard**, Business Information Security Officer chez Sage, *« Près de la moitié des PME françaises manquent d'expertise interne pour sécuriser leurs usages IA. Notre rôle d'éditeur responsable est de leur simplifier cette complexité : via des fonctionnalités IA sécurisées by design, des politiques d'usage claires, et un accompagnement continu. Les PME n'ont pas besoin de devenir expertes en sécurité IA, elles ont besoin de partenaires technologiques de confiance qui le sont déjà pour elles. »*

L'étude IDC souligne que pour transformer cette méfiance en confiance, les PME doivent franchir plusieurs paliers : renforcer leur expertise interne ou s'appuyer sur des partenaires de confiance, adopter une gouvernance des données claire, et intégrer la sécurité IA dès la conception de leurs projets, et non après coup.

A propos de l'étude

Cette étude a été menée par IDC en janvier 2026 auprès de 2 210 décideurs et influenceurs en matière de cybersécurité au sein de PME de moins de 500 employés, répartis dans 8 pays : France (330 répondants), Allemagne, Royaume-Uni, États-Unis, Canada, Espagne, Portugal et Afrique du Sud. Les répondants représentent 16 secteurs d'activité, du manufacturing aux services financiers, en passant par le retail et l'éducation.

A propos de Sage

Sage a pour ambition d'éliminer les barrières afin que tout le monde puisse s'épanouir, à commencer par les millions de petites et moyennes entreprises, les ETI et les experts-comptables que nous accompagnons avec nos partenaires. Nos clients ont confiance en nos logiciels de gestion de finances, de ressources humaines et de paie pour que leurs activités se déroulent en toute sérénité.

En numérisant les processus métier et les échanges avec les clients, les fournisseurs, les employés, les banques et les administrations, notre plateforme intégrant l'IA connecte les PME, réduit les frictions et leur apporte des informations essentielles. Éliminer les barrières signifie aussi consacrer notre temps, notre technologie et notre expérience à lutter contre la fracture numérique, les inégalités économiques et contre la crise climatique.