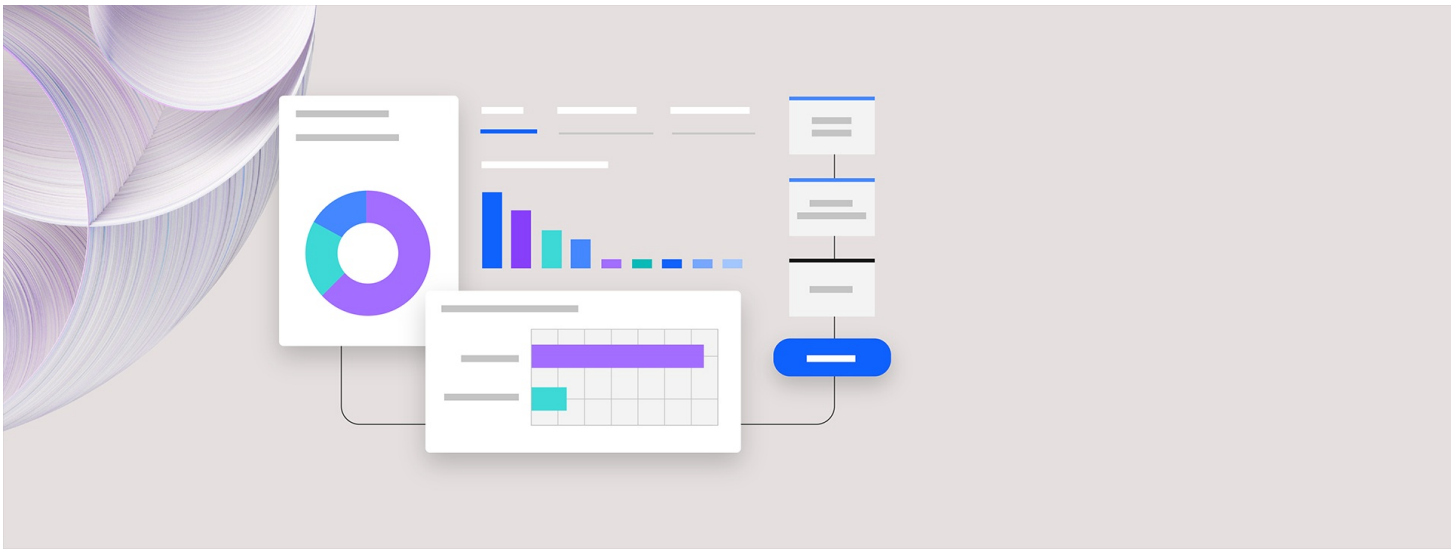
Communiqués de presse

IBM présente un logiciel inédit pour unifier la gouvernance et la sécurité agentiques

Nouvelles intégrations IBM pour aider les entreprises à maintenir leur IA agentique - et autres systèmes d'IA générative - sécurisés et responsables, à grande échelle.

Les entreprises peuvent utiliser des méthodes de « Red Teaming » sur les agents, auditer les agents, détecter des agents non-déclarés, et bien plus encore.



ARMONK, N.Y., le 18 juin 2025 - Aujourd'hui, alors que les entreprises mettent à l'échelle les agents d'IA dans leurs organisations, IBM annonce le premier logiciel du secteur à réunir les équipes de sécurité et de gouvernance de l'IA et à fournir une vue unifiée de la posture de risque des entreprises.

Ces nouvelles fonctionnalités améliorent et intègrent watsonx.governance et Guardium AI Security pour aider les clients à maintenir leurs systèmes d'IA, y compris les agents, sécurisés et responsables, à grande échelle. watsonx.governance est l'outil de gouvernance de l'IA de bout en bout d'IBM et Guardium AI Security est l'outil d'IBM pour sécuriser les modèles, les données et l'utilisation de l'IA.

« Les agents d'IA sont sur le point de révolutionner la productivité des entreprises, mais leurs avantages peuvent également représenter un défi », a déclaré **Ritika Gunnar, General Manager, Data and AI, IBM** *« Lorsque ces systèmes autonomes ne sont pas correctement gouvernés ou sécurisés, ils peuvent avoir de lourdes conséquences. »*

Les nouvelles offres annoncées aujourd'hui comprennent :

L’intégration et l’automatisation de la sécurité de l'IA agentique

IBM améliore l'intégration d'IBM Guardium AI Security et de watsonx.governance, offrant ainsi aux entreprises la première solution unifiée pour gérer les risques de sécurité et de gouvernance associés aux cas d'usage de l'IA. Cette intégration prend en charge les processus des utilisateurs pour valider les normes de conformité par rapport à 12 référentiels différents, dont l’EU AI Act et la norme ISO 42001.

IBM intègre également de nouvelles fonctionnalités à Guardium AI Security, dans le cadre d'une collaboration avecAllTrue.ai, notamment la capacité de détecter de nouveaux cas d'usage de l'IA dans les environnements Cloud, les référentiels de code et les systèmes embarqués, offrant ainsi une visibilité et une protection étendues dans un écosystème de l'IA de plus en plus décentralisé. Une fois identifié, IBM Guardium AI Security peut déclencher automatiquement les processus de gouvernance appropriés depuis watsonx.governance.

Les récentes mises à jour d'IBM Guardium AI Security incluent également une fonction de « red teaming » automatisée pour aider les entreprises à détecter et à corriger les vulnérabilités et les mauvaises configurations dans les cas d'usage de l'IA. Et pour aider à atténuer les risques tels que l'injection de code, l'exposition de données sensibles et la fuite de données, l'outil permet aux utilisateurs de définir des politiques de sécurité personnalisées qui analysent à la fois les prompts d'entrée et de sortie. Ces fonctionnalités sont disponibles dès à présent dans IBM Guardium AI Security et leur intégration avec watsonx.governance sera déployée tout au long de l'année.

« L'avenir de l'IA dépend de la façon dont nous la sécurisons aujourd'hui. Intégrer la sécurité dès le départ est essentiel pour protéger les données, respecter les obligations de conformité et instaurer une confiance durable », a **déclaré Suja Viswesan, Vice President, Security and Runtime Products, IBM.**

« L'un des plus grands défis pour les équipes de sécurité est de traduire les incidents et les violations de conformité en risques commerciaux quantifiables. L'adoption rapide de l'IA et de l'IA agentique amplifie ce problème », a déclaré **Jennifer Glenn, Research Director for the IDC Security and Trust Group**. *« L'unification de la gouvernance de l'IA avec la sécurité de l'IA donne aux organisations le contexte nécessaire pour identifier et hiérarchiser les risques, ainsi que les informations pour communiquer clairement les conséquences de ne pas les traiter. »*

L’évaluation améliorée de l'IA agentique et la gouvernance du cycle de vie

IBM watsonx.governance peut désormais surveiller et gérer les agents d'IA tout au long de leur cycle de vie, du développement au déploiement. Des nœuds d'évaluation peuvent être intégrés directement aux agents, ce qui permet aux utilisateurs de

surveiller attentivement des paramètres tels que la pertinence de la réponse, la pertinence du contexte et la fidélité - et d'aider à identifier la cause d'une mauvaise performance. Les fonctionnalités futures prévues comprennent également l'évaluation des risques liés à l'intégration des agents, une formalisation d'audit des agents et un catalogue d'outils agentiques, qui devraient être disponibles le 27 juin.

Les capacités de mise en conformité prêtes à l'emploi

Les accélérateurs de conformité IBM watsonx.governance (IBM watsonx.governance Compliance Accelerators) proposent une sélection de réglementations, de normes et de cadres préchargés provenant du monde entier, permettant aux utilisateurs d'identifier les obligations pertinentes et de les adapter à leurs propres cas d'usage d'IA. Le contenu couvre des réglementations clés telles que l'EU AI ACT, la SR 11-7 de la Réserve fédérale américaine et la loi locale 144 de la ville de New York, ainsi que des normes mondiales telles que l'ISO/IEC 42001 et des cadres tels que l'AI RMF du NIST. Les accélérateurs de conformité watsonx.governance sont disponibles dès maintenant en tant que module additionnel.

Pour offrir aux clients d'AWS davantage de valeur et de simplicité, watsonx.governance est désormais également disponible sur le datacenter d'AWS en Inde avec des capacités de surveillance des modèles accrues.

Les nouvelles fonctionnalités et intégrations présentées aujourd'hui offrent aux entreprises la gouvernance et la sécurité complètes dont elles ont besoin pour prospérer à l'ère de l'IA agentique. Ces innovations s'inscrivent également dans la suite plus large de solutions d'IA IBM watsonx, conçues pour aider les entreprises à accélérer l'impact de l'IA générative, de manière responsable et sécurisée.

À propos d'IBM

IBM est l'un des principaux fournisseurs mondiaux de Cloud hybride et d'IA, ainsi que d'expertise en matière de conseil. Nous aidons nos clients dans plus de 175 pays à capitaliser sur les connaissances issues de leurs données, à rationaliser leurs processus métier, à réduire leurs coûts et à acquérir un avantage concurrentiel dans leurs secteurs d'activité. Des milliers d'entités gouvernementales et entreprises dans des domaines d'infrastructures critiques tels que les services financiers, les télécommunications et les soins de santé font confiance à la plateforme Cloud hybride d'IBM et à Red Hat OpenShift pour impacter leurs transformations numériques rapidement, efficacement et en toute sécurité. Les innovations révolutionnaires d'IBM en matière d'IA, d'informatique quantique, de solutions Cloud spécifiques à certains secteurs et de conseil offrent des options ouvertes et flexibles à nos clients. Tout cela est soutenu par l'engagement de longue date d'IBM en matière de confiance, de transparence, de responsabilité, d'inclusivité et de service.

Pour en savoir plus : www.ibm.com/fr-fr

Les déclarations d'IBM concernant ses orientations et intentions futures sont sujettes à modification ou retrait sans préavis et ne représentent que des buts et des objectifs.

Contacts Presse :

IBM
Gaëlle Dussutour
Tél. : + 33 (0)6 74 98 26 92
dusga@fr.ibm.com

Weber Shandwick pour IBM

Louise Weber

Tél. : + 33 (0)6 89 59 12 54

ibmfrance@webershandwick.com