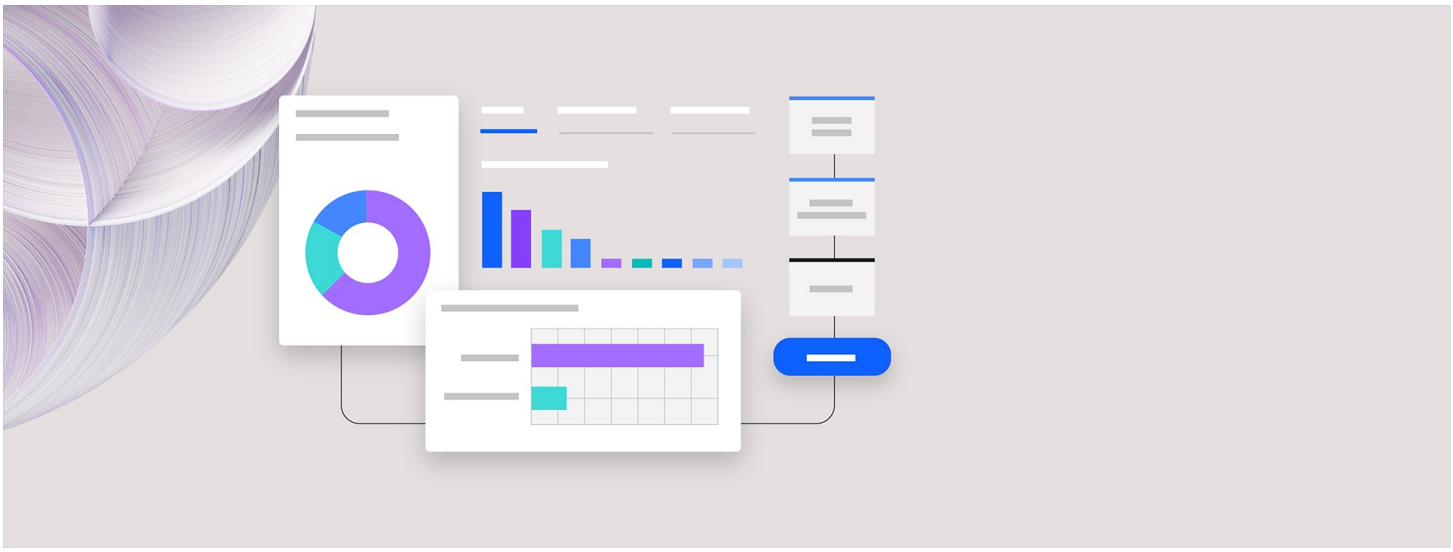
Anuncios

IBM presenta el primer software del mercado que unifica la gobernanza y la seguridad de la IA agéntica

• Las nuevas integraciones de IBM ayudan a las empresas a mantener su IA agéntica, y otros sistemas de IA generativa, seguros y responsables a escala

• Las empresas podrán realizar 'red teaming' de agentes, auditarlos, detectar shadow agents y mucho más



ARMONK, N.Y., 18 de junio de 2025 /PRNewswire/.— A medida que las empresas extienden el uso de agentes de IA en sus organizaciones, IBM anuncia hoy el primer software del sector que unifica los equipos de seguridad y gobernanza de la IA, ofreciendo una visión unificada del perfil de riesgo de las organizaciones.

> *"Los agentes de IA están llamados a revolucionar la productividad empresarial, pero sus beneficios también pueden plantear un desafío. Cuando estos sistemas autónomos no se gobiernan o aseguran adecuadamente, pueden acarrear riesgos importantes."*

Estas nuevas capacidades mejoran e integran watsonx.governance y Guardium AI Security para ayudar a los clientes a mantener sus sistemas de IA, incluidos los agentes, seguros y responsables a escala. IBM watsonx.governance es la herramienta integral de gobernanza de IA de IBM, y Guardium AI Security es la herramienta de la compañía para proteger los modelos, datos y uso de IA.

"Los agentes de IA están llamados a revolucionar la productividad empresarial, pero sus beneficios también pueden plantear un desafío", afirma Ritika Gunnar, General Manager, Data and AI de IBM. "Cuando estos sistemas autónomos no se gobiernan o aseguran adecuadamente, pueden acarrear riesgos importantes".

Entre las funcionalidades anunciadas hoy, se incluyen:

Integración y automatización de la seguridad de la IA agéntica

IBM está mejorando la integración de IBM Guardium AI Security y watsonx.governance, proporcionando a las empresas la primera solución unificada para gestionar los riesgos de seguridad y gobierno asociados a los casos de uso de IA. La integración respalda los procesos de los usuarios para validar estándares de cumplimiento frente a 12 marcos diferentes,

incluida la ley de IA de la UE y la ISO 42001.

IBM también introduce nuevas capacidades en Guardium AI Security gracias a una colaboración conAllTrue.ai, incluida la capacidad de detectar nuevos casos de uso de IA en entornos de nube, repositorios de código y sistemas integrados, proporcionando así una visibilidad y protección amplias en un ecosistema de IA cada vez más descentralizado. Una vez identificados, IBM Guardium AI Security puede activar automáticamente los flujos de trabajo de gobierno apropiados desde watsonx.governance.

Las actualizaciones recientes de IBM Guardium AI Security también incluyen la automatización de*red teaming*, que ayuda a las empresas a detectar y corregir vulnerabilidades y errores de configuración en distintos casos de uso de IA. Además, para mitigar riesgos como la inyección de código, la exposición de datos confidenciales y las fugas de datos, la herramienta permite a los usuarios definir políticas de seguridad personalizadas que analizan tanto las instrucciones de entrada como las respuestas de salida. Estas funcionalidades ya están disponibles en IBM Guardium AI Security, y su integración con watsonx.governance se llevará a cabo a lo largo de este año.

“El futuro de la IA depende de lo bien que la aseguremos hoy. Incorporar la seguridad desde el principio es fundamental para proteger los datos, cumplir con las obligaciones normativas y consolidar una confianza a largo plazo”, ha afirmado Suja Viswesan, Vice President, Security and Runtime Products de IBM.

“Uno de los mayores retos para los equipos de seguridad es traducir los incidentes y violaciones de cumplimiento en riesgos empresariales cuantificables. La rápida adopción de la IA y la IA agéntica amplifica este problema”, ha dicho Jennifer Glenn, Research Director de IDC Security and Trust Group. “Unificar la gobernanza de IA con la seguridad de IA proporciona a las organizaciones el contexto necesario para identificar y priorizar riesgos, así como la información para comunicar claramente las consecuencias de no abordarlos”.

Gobernanza mejorada de la evaluación y ciclo de vida de la IA agéntica

IBM watsonx.governance ahora puede supervisar y gestionar agentes de IA a lo largo de todo su ciclo de vida, desde el desarrollo hasta el despliegue. Se pueden integrar nodos de evaluación directamente en los agentes, lo que permite a los usuarios supervisar cuidadósamente métricas como la relevancia de las respuestas, la pertinencia del contexto y la fidelidad, y ayudar así a identificar la raíz de un rendimiento deficiente. Entre las futuras funciones previstas también se incluyen la evaluación de riesgos en la incorporación de agentes, los registros de auditoría de agentes y un catálogo de herramientas para agentes, cuya disponibilidad está prevista para el 27 de junio.

Funciones de cumplimiento normativo listas para usar

IBM watsonx.governance Compliance Accelerators ofrece una selección de regulaciones, normas y marcos preconfigurados de todo el mundo, lo que permite a los usuarios identificar las obligaciones relevantes y asignarlas a sus propios casos de uso de IA. El contenido cubre normativas clave como el la Ley de IA de la UE, la SR 11-7 de la Reserva Federal de EEUU y la Ley Local 144 de la ciudad de Nueva York, junto con normas globales como ISO/IEC 42001 y marcos como el NIST AI RMF. IBM watsonx.governance Compliance Accelerators está disponible ahora como complemento.

Para proporcionar a los clientes de AWS mayor valor y comodidad, watsonx.governance también está disponible ahora en el centro de datos de AWS en India, con capacidades mejoradas de supervisión de modelos.

Las nuevas capacidades e integraciones que se presentan hoy ofrecen a las empresas el gobierno y la seguridad integrales que necesitan para prosperar en la era de la IA agéntica. Estas innovaciones también se alinean con la gama más amplia de soluciones de IA de IBM watsonx, diseñadas para ayudar a las empresas a acelerar el impacto de la IA generativa, de forma responsable y segura.

Acerca de IBM

IBM es un proveedor líder de nube híbrida global e inteligencia artificial, así como experiencia en consultoría. Ayudamos a clientes en más de 175 países a capitalizar los conocimientos de sus datos, optimizar los procesos comerciales, reducir costos y obtener una ventaja competitiva en sus industrias. Miles de entidades gubernamentales y corporativas en áreas de infraestructura crítica, como servicios financieros, telecomunicaciones y atención médica, confían en la plataforma de nube híbrida de IBM y Red Hat OpenShift para llevar a cabo sus transformaciones digitales de manera rápida, eficiente y segura. Las innovaciones revolucionarias de IBM en IA, computación cuántica, soluciones en la nube específicas de la industria y consultoría ofrecen opciones abiertas y flexibles a nuestros clientes. Todo esto está respaldado por el compromiso de larga data de IBM con la confianza, la transparencia, la responsabilidad, la inclusión y el servicio. Visite http://www.ibm.com/ para obtener más información.

For further information: Alfonso Mateos Cadenas. Dpto. Comunicación IBM España, Portugal, Grecia e Israel.
alfonso.mateos@ibm.com