Cuatro aspectos clave para la implementación de la tecnología de inteligencia artificial

Los líderes empresariales que desean comenzar a implementar la tecnología de inteligencia artificial o quieren ampliar su uso tienen preguntas y preocupaciones en común, como la manera de utilizarla para mejorar la eficiencia operativa y expandir su empresa mientras se mantiene la estabilidad y se reducen los riesgos. A continuación, analizamos cuatro aspectos que se deben tener en cuenta, independientemente de la etapa del proceso de implementación de la inteligencia artificial en la que se encuentre.

1 Elija una plataforma flexible

Ya sea que recién esté comenzando a utilizar la inteligencia artificial o desee ampliar sus casos prácticos actuales para implementarla en más ámbitos, es importante elegir una plataforma flexible y con capacidad de ajuste para respaldar la consolidación del uso de esta tecnología.

Si se encuentra en las primeras etapas de adopción de la inteligencia artificial, necesita una infraestructura estable, flexible y abierta que permita que sus equipos diseñen y ejecuten cargas de trabajo pequeñas. La plataforma que utilice debe admitir el entrenamiento de modelos según sea necesario a medida que aumente el uso de la inteligencia artificial y crezcan las cargas de trabajo.

La plataforma también debe ser estable para que los analistas de datos y los desarrolladores puedan diseñar modelos que proporcionen valor real a los clientes, quienes tienen que estar seguros de que la plataforma que utilizan es confiable y está centrada en la seguridad.

Si su empresa cuenta con funciones de inteligencia artificial más avanzadas, necesita tecnologías de soporte que le permitan alcanzar todo el potencial, lo cual puede requerir una importante inversión en unidades de procesamiento gráfico (GPU) y otros aceleradores de hardware.

Una plataforma abierta y con capacidad de ajuste le permite:

- Proporcionar a su empresa una buena base para diseñar y modernizar las aplicaciones impulsadas por la inteligencia artificial en menos tiempo
- Agilizar la implementación de las aplicaciones impulsadas por la inteligencia artificial
- Obtener una ventaja competitiva en un panorama de la inteligencia artificial que cambia rápidamente

Con la infraestructura adecuada, su empresa estará lista para adoptar todas las innovaciones de la inteligencia artificial que surjan en el futuro.

2 Prepárese para la inteligencia artificial híbrida

La inteligencia artificial generativa ha aumentado la necesidad de los recursos informáticos y ha llevado los procesamientos al extremo de la red. Los casos prácticos de esta tecnología se benefician de una combinación de recursos de las instalaciones y de la nube; sin embargo, algunas cargas de trabajo, en especial las que se influencian por los problemas de cumplimiento normativo o la gravedad de los datos, solo deben ejecutarse en las instalaciones. Con la inteligencia artificial híbrida, los equipos pueden ejecutar las cargas donde sea más conveniente, como la ubicación más cercana al origen de los datos.

Además, ofrece varias ventajas:

- **Flexibilidad:** las cargas de trabajo de producción y de prueba que se ejecutan en el entorno más apto pueden reducir los costos.
- **Distribución agilizada:** la inferencia de las cargas de trabajo pequeñas en el extremo de la red agiliza la distribución de la información a los usuarios.
- **Disminución de los riesgos:** las aplicaciones de inteligencia artificial que se ejecutan en el extremo de la red disminuyen la necesidad de transferir grandes cantidades de información al núcleo, lo cual da como resultado una mejor protección de los datos.

Con la inteligencia artificial híbrida, los equipos de TI entrenan el modelo en un centro de datos principal o en la nube pública y lo distribuyen a los extremos, donde puede inferir y ofrecer información útil de manera con mayor velocidad. Las cargas de trabajo que utilizan muchos recursos pueden encontrarse en la nube central y en el extremo de la red, lo cual equilibra la necesidad de la capacidad de procesamiento con la demanda de recomendaciones rápidas y precisas.

3 No piense solo en el primer modelo

Es posible que los equipos de TI puedan llevar un único modelo de inteligencia artificial a la etapa de producción con mínimo esfuerzo, pero el éxito suele depender de la capacidad de ajuste. Para aprovechar al máximo el valor empresarial, deben poder implementar varias versiones de ese modelo, tal vez cientos de veces al día.

La aplicación de los procesos de operaciones de machine learning (MLOps) permite ajustar las implementaciones de manera sencilla. Al igual que DevOps, MLOps reúne a los desarrolladores, los gerentes de operaciones y los analistas de datos para agilizar el desarrollo y la implementación exitosa de las aplicaciones que se basan en la inteligencia artificial. Con este enfoque, su empresa puede ajustar la creación de las aplicaciones de manera más sencilla, lo cual le permite ofrecer más servicios para los clientes en menos tiempo.

MLOps es un medio de desarrollo eficiente y rentable. Los equipos trabajan en conjunto en una plataforma común y mejoran las eficiencias, lo que puede disminuir el tiempo y los costos que influyen directamente en los resultados finales de la empresa.

4 Priorice la seguridad

Frente a los ciberataques que ocasionan grandes costos, los ejecutivos buscan cada vez más formas de proteger los datos confidenciales y disminuir los riesgos. La inteligencia artificial generativa aumenta la urgencia, ya que su uso incrementa el riesgo de que se exponga la información confidencial.

Es fundamental mantener una estrategia de seguridad sólida para evitar las amenazas, como:

- **Envenenamiento de datos:** se insertan datos incorrectos o maliciosos en los modelos de inteligencia artificial, lo que da como resultado información poco precisa o recomendaciones fraudulentas.
- **Robo de modelo:** se aplica el proceso de ingeniería inversa de un modelo de machine learning (aprendizaje automático) y se extraen los datos con la copia.
- **Ataques de puerta trasera:** el código malicioso se oculta en un modelo de inteligencia artificial, por lo que el agente malintencionado puede robar la información.

Estas y otras tácticas representan una gran amenaza para su empresa y pueden exponerla a riesgos financieros y legales. Disminuya los puntos vulnerables que se relacionan con la inteligencia artificial con la ayuda de un proveedor de plataformas de aplicaciones de confianza que cuente con un historial comprobado y procesos establecidos para gestionar los parches de seguridad y las versiones.

Más información

Agilice su estrategia de inteligencia artificial. Conozca las soluciones de Red Hat.

ARGENTINA
+54 11 4329 7300

CHILE
+562 2597 7000

COLOMBIA
+571 508 8631
+52 55 8851 6400

MÉXICO
+52 55 8851 6400

ESPAÑA
+34 914 148 800

facebook.com/redhatinc
@RedHatLA
@RedHatIberia
linkedin.com/company/red-hat

es.redhat.com