DELL Technologies

NVIDIA

Los cinco requisitos de seguridad principales para la IA generativa (GenAI)

Acelere la adopción de una infraestructura segura y ampliable con Dell AI Factory with NVIDIA

El potencial transformador de la IA generativa

La IA generativa tiene el potencial de cambiar el juego de maneras que los visionarios solo están empezando a imaginar.

76 %

de los responsables empresariales y de TI creen que la IA generativa aportará un valor transformador a su organización.[1]

IA

Análisis avanzados y técnicas con base en la lógica para interpretar eventos, y apoyar y automatizar decisiones y acciones.

IA generativa

Tecnologías y técnicas que utilizan grandes cantidades de datos para generar contenido nuevo a partir de lenguaje natural u otras entradas no tradicionales y sin código.

Simulación

- Gemelo digital
- Datos sintéticos
- Marcos de diseño
- Previsión

Creación de contenido

- Codificación
- Matemáticas
- Escritura/discurso
- Imagen/vídeo
- Audio

Descubrimiento de contenido

- Búsqueda de lenguaje natural
- Análisis de grandes conjuntos de datos
- Gestión del conocimiento
- Educación y formación personalizadas

Experiencia de usuario

- Traducciones en tiempo real en más de 70 idiomas
- Interacciones personalizadas utilizando expresiones faciales y lenguaje corporal naturales

1 Estudio "Innovation Catalyst" de Dell Technologies, febrero de 2024.

Mayor potencial, mayor riesgo

Para los líderes empresariales es tentador moverse rápidamente, evitando las implicaciones relacionadas con los datos, el cumplimiento normativo, la gobernanza y otros riesgos. Pero la IA generativa es una espada de doble filo cuando se trata de la seguridad.

Beneficios

- Detección de amenazas mejorada
- Eficiencia operativa mejorada
- Formación personalizada relacionada con la concienciación sobre la seguridad

Inconvenientes

- Mayor sofisticación de los ataques
- Ingeniería social avanzada
- Shadow AI

33 %

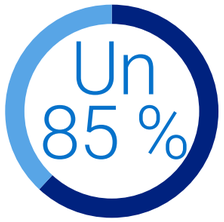
de los encuestados mencionaron la ciberseguridad como el principal riesgo de la IA generativa que sus organizaciones están trabajando para mitigar.[2]

2 McKinsey Global Survey on AI: The state of AI in early, mayo de 2024

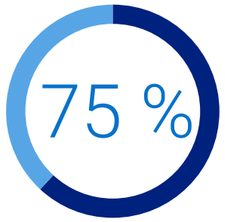
CONSIDERACIÓN 1

El nuevo panorama de amenazas

La promesa de la IA generativa viene con una realidad sombría: los atacantes están creando ataques nuevos y más complejos que pueden superar las defensas convencionales, lo que dificulta que los equipos de ciberseguridad se mantengan al día.



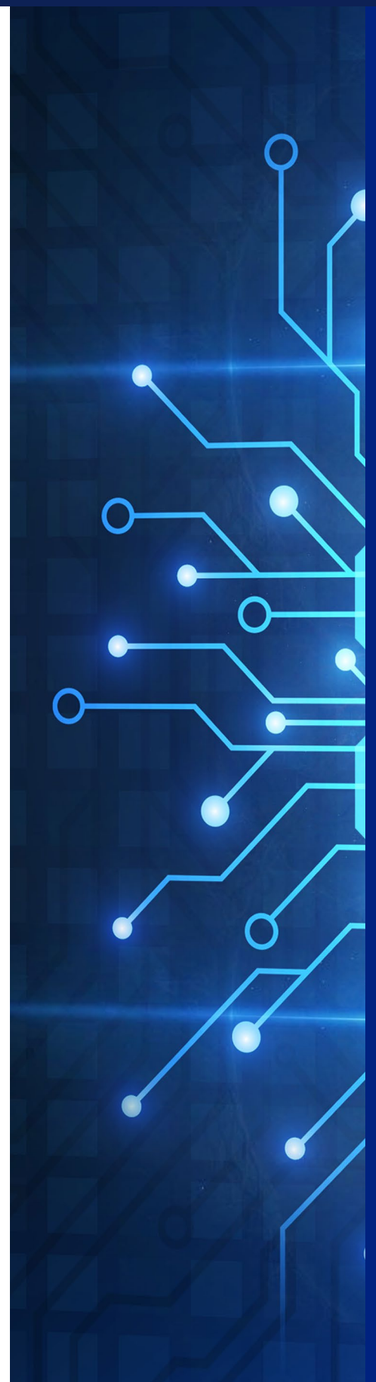
de los encuestados creen que la IA ha aumentado la sofisticación de los ataques a la ciberseguridad.[3]



de los profesionales de la seguridad han observado un incremento en los ataques durante los últimos 12 meses.[4]

Para protegerse frente a estas amenazas emergentes, las empresas deben centrarse en minimizar la superficie de ataque mediante pruebas de penetración, supervisión y auditorías, por ejemplo.

3 2024 Human Risk in Cybersecurity Survey, EY, mayo de 2024
4 Voice of SecOps Report "Generative AI and Cybersecurity: Bright Future or Business Battleground?" 2023



Vectores de ataque emergentes

Malware avanzado
Malware cada vez más sofisticado que utiliza la IA generativa para "evolucionar por sí mismo", modificando continuamente su código para que la seguridad existente, como la detección basada en firmas, no la identifique.

Correos electrónicos y campañas de phishing altamente personalizados
Aumento de la frecuencia de correos electrónicos maliciosos que parecen auténticos y carecen de los signos de estafa habituales.

Datos falsos muy convincentes
El robo de identidades, el fraude financiero y la desinformación resultan más fáciles gracias a la capacidad de imitar las acciones humanas, como la escritura, el discurso, las imágenes o el vídeo.

Reconocimiento automatizado
Recopilación de información que identifica vulnerabilidades y debilidades en la red o el sistema de un objetivo potencial para facilitar ataques más dirigidos.

CONSIDERACIÓN 2

Riesgos de despliegue e implementación

Las organizaciones que quieren aprovechar los beneficios potenciales de la IA generativa necesitan grandes cantidades de datos de alta calidad, que los modelos pueden utilizar para producir los mejores resultados. Pero los datos y el riesgo van de la mano. Antes de utilizar cualquier información, las empresas deben evaluar cuidadosamente y tener en cuenta sus requisitos, datos y riesgos únicos.

Vulnerabilidades de los modelos grandes de lenguaje (LLM)

Los servicios de IA generativa son vulnerables a ataques de inyección rápida, en los que los atacantes manipulan los resultados para eludir las barreras de seguridad u obtener acceso no autorizado a archivos que puedan haberse utilizado para perfeccionar el modelo.

Envenenamiento de datos

Los atacantes pueden introducir deliberadamente datos alterados en un LLM durante la fase de entrenamiento. Esto puede hacer que el modelo sea vulnerable a los ataques a través de puertas traseras integradas en los datos. Un ejemplo real es atacar y explotar los filtros de spam entrenándolos con correos electrónicos de spam.

Complejidad normativa

Las autoridades normativas de todo el mundo se afanan en comprender, controlar y garantizar la seguridad de la IA generativa. Si bien los modelos de IA generativa están sujetos a las reglas actuales de soberanía de datos que dictan cómo se almacenan, procesan y utilizan los datos, los organismos de gobernanza siguen definiendo la supervisión de la información con derechos de propiedad intelectual y derechos de autor. El cumplimiento de las normativas puede ser costoso, pero el incumplimiento de las normativas establecidas y emergentes podría derivar en multas y otras sanciones.

CONSIDERACIÓN 3

Shadow AI

En la actualidad, muchos empleados ya utilizan generadores públicos de texto, imágenes y vídeo como ChatGPT para aumentar sus flujos de trabajo diarios. Sin embargo, cuando estas herramientas se utilizan sin una gobernanza adecuada, representan una amenaza crítica para las organizaciones que intentan proteger la propiedad intelectual y los datos corporativos. Este uso no autorizado de la IA generativa se conoce como IA oculta.

Pérdida de propiedad intelectual

Las empresas ya están lidiando con la pérdida de propiedad intelectual por parte de los empleados que comparten información confidencial en herramientas públicas de IA generativa.

Filtración de datos del código fuente

Los desarrolladores que intentan optimizar el código fuente mediante ChatGPT han provocado fugas de datos.

Para abordar los retos de la IA oculta, las empresas deben implementar un consejo o una junta en toda la empresa con autoridad para tomar decisiones que impliquen una gobernanza segura de la IA.

¿Dónde residen sus datos? ¿Dónde deben ubicarse las cargas de trabajo?

La IA funciona mejor cuando se combina con sus datos, dondequiera que residan. Con un control total de la infraestructura y los LLM, no hay riesgo de pérdida de propiedad intelectual ni de pérdida de datos del código fuente.

Costes

El aprovechamiento de las implementaciones en las instalaciones puede reducir el TCO hasta en un 75 % en 3 años.[5]

Seguridad y privacidad

Desarrolle entornos seguros de IA e IA generativa en toda su organización, utilizando flujos de trabajo y operaciones en las instalaciones. Ejerza un control estricto sobre la seguridad de los datos y el cumplimiento de las normativas, especialmente para los sectores que gestionan datos confidenciales.

5 Según un estudio de Enterprise Strategy Group encargado por Dell, en el que se compara la infraestructura en las instalaciones de Dell con la infraestructura nativa de cloud pública como servicio, abril de 2024. Los modelos analizados muestran que un LLM con 7000 millones de parámetros que utiliza RAG en una organización de 5000 usuarios es hasta un 38 % más rentable; y que un LLM de 70 000 millones de parámetros que utiliza RAG en una organización de 50 000 usuarios es hasta un 75 % más rentable. Los resultados reales pueden variar. Resumen económico

CONSIDERACIÓN 4

Criterios de evaluación

Durante el último año, la comunidad de IA se ha centrado cada vez más en tres cuestiones clave: desarrollo e implementación responsables, evaluación del impacto y mitigación de riesgos. A medida que las empresas evalúan los modelos de IA generativa, deben tener en cuenta algunas advertencias importantes:

Ausencia de requisitos de informes coherentes

Los desarrolladores líderes prueban principalmente sus modelos con diferentes parámetros de referencia de IA responsables. Debido a esta falta significativa de estandarización en la elaboración de informes, es difícil comparar metódicamente los riesgos y las limitaciones de los principales modelos de IA.

Material con derechos de autor en los resultados

Los resultados de los LLM populares pueden contener material con derechos de autor, lo que puede infringir la ley y poner a las empresas que utilizan el material en riesgo de sanciones.

Las vulnerabilidades son cada vez más complejas

Los investigadores están encontrando estrategias menos obvias que hacen que los LLM muestren un comportamiento perjudicial, como pedir a los modelos que repitan palabras aleatorias infinitamente.

Los desarrolladores carecen de transparencia

En muchos casos, los desarrolladores de IA no son transparentes acerca de sus datos y metodologías de entrenamiento. Esto obstaculiza los esfuerzos para comprender mejor la solidez y la seguridad de los sistemas de IA.

CONSIDERACIÓN 5

Beneficios para la seguridad

Junto con los riesgos para la seguridad de la IA generativa, están sus posibles beneficios para la seguridad. La IA generativa se está convirtiendo en un aliado crucial en ciberseguridad que abre nuevas vías de protección.

Ahora puede comenzar a crear operaciones de seguridad ampliables con un acceso más rápido a información más completa y detección automática de amenazas, lo que ofrece eficiencia y complementa a los equipos de seguridad con poco personal.

de Secureworks

AI analizar datos históricos e identificar patrones y anomalías, la IA generativa puede reconocer amenazas nuevas y en desarrollo en tiempo real. Permite supervisar continuamente el tráfico de red, los registros del sistema y el comportamiento de los usuarios, e identificar rápidamente actividades irregulares que pueden suponer amenazas para la seguridad.

El resultado es una potente detección de amenazas adaptable, que permite responder rápidamente a los vectores de ataque cambiantes y proporciona un mecanismo de defensa proactivo contra las ciberamenazas emergentes.

Entrenamiento y simulación de amenazas

Con la IA generativa, las empresas pueden simular una amplia variedad de amenazas de ciberseguridad y escenarios de ataque en un entorno controlado. Como resultado, los equipos están mejor preparados para identificar y mitigar las ciberamenazas, además de responder a ellas, cuando el tiempo es esencial.

Análisis y resumen en profundidad

La IA generativa permite a los equipos investigar datos de diferentes fuentes o módulos, con lo que pueden realizar análisis de datos tediosos y que tradicionalmente llevan mucho tiempo con mayor rapidez y precisión. Los equipos también pueden crear resúmenes en lenguaje natural de evaluaciones de incidentes y amenazas, lo que mejora la eficiencia y aumenta el rendimiento de los equipos.

Formación personalizada relacionada con la concienciación sobre la seguridad

AI incluir la IA conversacional además de la IA generativa e incorporar un avatar de IA en la interfaz de usuario, las organizaciones pueden ofrecer interacciones personalizadas (disponibles a escala, las 24 horas del día, los 7 días de la semana) utilizando expresiones faciales y lenguaje corporal naturales. Esto se puede utilizar para formación y educación en seguridad, lo que proporciona una experiencia de aprendizaje más natural, personalizada e interactiva, evaluaciones automatizadas y mucho más.

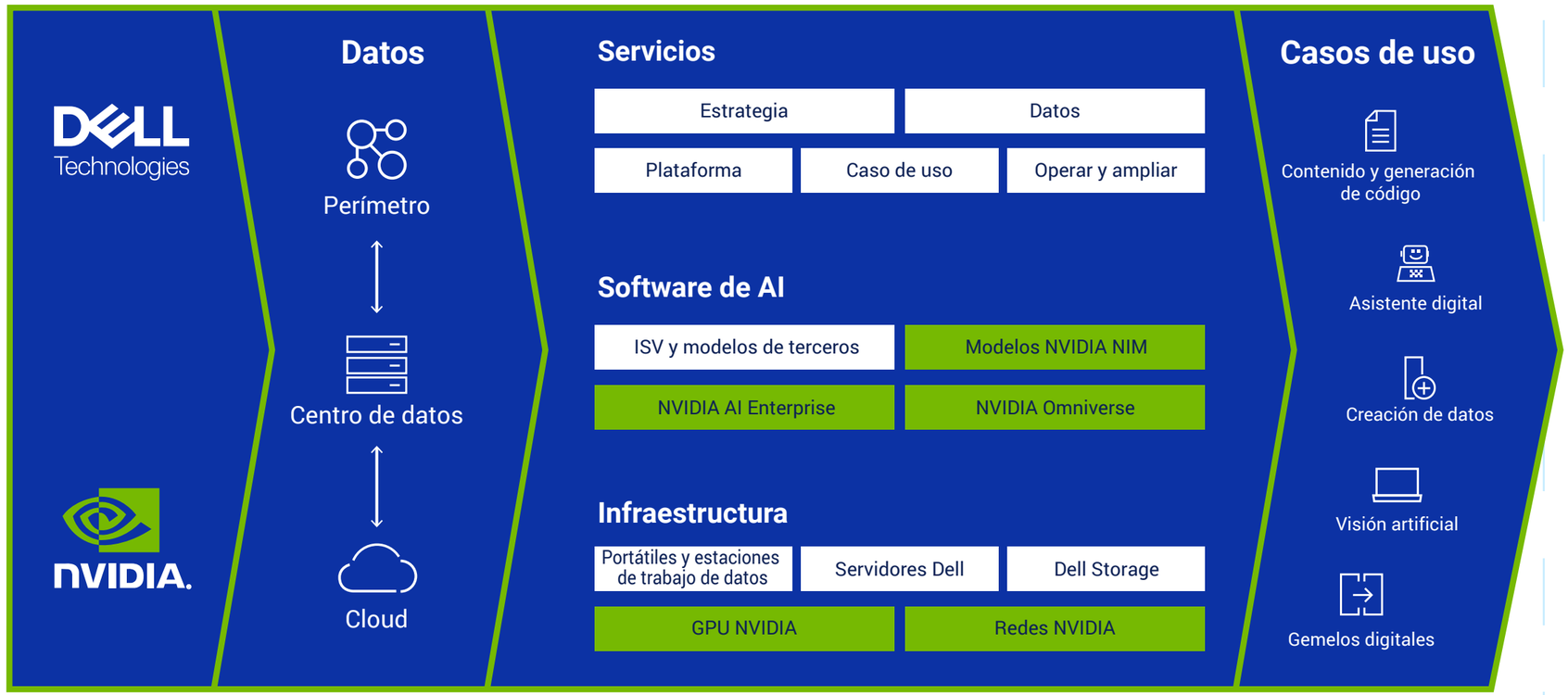
Dell AI Factory with NVIDIA

Agilice la adopción de la IA y transforme sus datos en información de forma segura con la primera solución de IA completa y lista para usar del sector. Dell AI Factory with NVIDIA aborda las complejas necesidades de las empresas que buscan aprovechar la IA y la IA generativa. Con una infraestructura y unos servicios líderes, junto con el software de IA de NVIDIA, podrá aumentar el tiempo de rentabilización de sus proyectos simplificando el desarrollo y la implementación.

- Reduzca el riesgo de comprometer los datos con una infraestructura que cuenta con seguridad intrínseca, incluida la raíz de confianza y otras características clave.
- Proteja sus datos frente a fugas que podrían provocar la pérdida de propiedad intelectual con una solución de IA en las instalaciones que puede controlar.
- Cumpla con los estrictos requisitos de cumplimiento normativo y soberanía de los datos con la incorporación de la IA a sus datos con acceso seguro.
- Proteja la privacidad de las partes interesadas controlando dónde y quién tiene acceso a sus datos.

Dell AI Factory with NVIDIA

La primera solución integral de IA empresarial del sector



Los datos impulsan AI Factory y sus casos de uso

Los datos más valiosos se encuentran en el entorno local y el perimetral. Dell Technologies le ayuda a incorporar IA a sus datos más valiosos y es líder en el almacenamiento, la protección y la gestión de estos datos.

Casos de uso para obtener resultados

AI Factory genera resultados empresariales que se basan en nuestros casos prácticos más prioritarios. Dell Technologies simplifica la implementación de sus casos de uso de IA más importantes con soluciones validadas y servicios personalizados.

No permita que los riesgos de seguridad obstaculicen la innovación

Deje que le guiemos en su viaje hacia el mundo de la IA y la IA generativa, para que pueda aprovechar sus recompensas.

PLANIFICACIÓN ESTRATÉGICA

Accelerator Workshop gratuito para la IA generativa

- Comience su viaje para desarrollar una estrategia ganadora
- Aborde los retos y las carencias, priorice los objetivos e identifique oportunidades
- Obtenga una evaluación de preparación para profundizar en los requisitos de la infraestructura, los modelos de IA, las integraciones operativas y mucho más

PREPARACIÓN TÉCNICA

Un laboratorio móvil listo para usar

Inicie su viaje hacia el éxito. Incluye una estación de trabajo móvil Dell Precision 5690/7780 con GPU NVIDIA y dos días de servicios de consultoría para ayudarle a empezar.

- Entorno aislado portátil para pruebas y demostraciones de IA generativa
- Validación previa con la plataforma NVIDIA AI Workbench, preparada para desarrolladores
- Caso de uso inicial de chatbot implementado con sus datos
- Enfoque rentable y de bajo riesgo para experimentar y desarrollar habilidades de IA generativa

ESTACIÓN DE TRABAJO MÓVIL DELL PRECISION 5690/7780 CON GPU NVIDIA

EMPIECE HOY MISMO

DELL Technologies AI Factory WITH NVIDIA