MicroStrategy
INTELLIGENCE EVERYWHERE

MicroStrategy AI: documento sobre la seguridad

Explore los pasos prácticos para garantizar la integridad de los datos y las implementaciones éticas de la IA.

Publicado: mayo de 2024

Índice

Introducción

La implementación eficaz de la inteligencia artificial (IA) en la inteligencia empresarial (BI) depende en gran medida de la integridad de los datos subyacentes. En el caso de los sistemas de IA que impulsan las decisiones de negocio, la precisión no es meramente beneficiosa: es imperativa. Estos sistemas deben ser dignos de confianza para poder generar una utilidad genuina.

MicroStrategy se destaca como un pilar confiable en este contexto al proporcionar a los usuarios empresariales datos que son a la vez precisos y seguros. El surgimiento de MicroStrategy AI refuerza este compromiso porque ofrece una plataforma en la que el rigor de la BI se encuentra con las capacidades innovadoras de la IA.

Nuestra solución de IA está diseñada para interpretar con precisión las preguntas relacionadas con negocios que se presentan en lenguaje natural, emplean razonamiento lógico y producen resultados relevantes de manera autónoma. Esta síntesis del análisis estructurado de la BI y de la adaptabilidad de la IA garantiza que MicroStrategy AI satisfaga la doble necesidad de contar con integridad de los datos e interacción flexible con los usuarios.

MicroStrategy AI es una evolución de nuestra plataforma establecida que integra sin inconvenientes las capacidades avanzadas de la IA y el aprendizaje automático. Optimiza procesos como la exploración de datos impulsada por IA, la automatización del diseño de paneles y el uso de herramientas especializadas como la generación de lenguaje de consulta estructurada, SQL, y la visualización mejorada por aprendizaje automático para el análisis de datos. Con estas funciones, la plataforma facilita un análisis más profundo de los datos dentro del entorno familiar del ecosistema de MicroStrategy.

La confiabilidad de MicroStrategy AI se apoya en el diseño meticuloso de la capa semántica de MicroStrategy y su marco de seguridad integral. Auto, nuestro asistente de IA, se basa exclusivamente en los datos de MicroStrategy, y todos los análisis se ejecutan mediante nuestro motor analítico establecido. Esto garantiza el procesamiento y la representación de datos coherentes, precisos y seguros, y permite que las empresas tomen decisiones fundamentadas con confianza.

Aislamiento del entorno de MicroStrategy AI

La principal fortaleza de una solución de IA empresarial reside no solo en su capacidad de procesar datos y aportar información estratégica, sino también en la resiliencia de su arquitectura ante las amenazas externas. El entorno MicroStrategy Cloud (MCE) está respaldado por un diseño arquitectónico que pone el mayor énfasis posible en el aislamiento del entorno, el acceso protegido y la ejecución segura de solicitudes en servicios externos o multiempresa.

Diseño para aislamiento:

La arquitectura del MCE se diseñó con el aislamiento del entorno como principio de seguridad central. Al garantizar que los datos de cada cliente operen en un entorno segmentado con seguridad, eliminamos los riesgos de contaminación cruzada y mejoramos la protección de los datos. Cuando el sistema necesita conectarse o enviar una solicitud a un servicio externo, estos flujos de trabajo se ejecutan con estrictas medidas de seguridad y protocolos de comunicación. Esto incluye transmisión de datos cifrados y solicitudes de ejecución sin estado dentro del contexto de seguridad de la instancia del cliente.

MicroStrategy AI dentro del MCE:

La oferta de MicroStrategy Cloud se complementa y mejora con la inclusión del módulo MicroStrategy AI. Al quedar dentro del marco del MCE, nos aseguramos de que MicroStrategy AI beneficie y mantenga constantemente los sólidos estándares de seguridad ambiental intrínsecos al MCE.

Características del aislamiento del MCE:

- **Configuraciones personalizadas:** MicroStrategy puede iniciar recursos en las nubles privadas virtuales (VPC) y modificar los rangos de direcciones del protocolo de Internet (IP), las tablas de ruta, las puertas de enlace de redes y la configuración de seguridad pertinente. Esto garantiza que el entorno de cada cliente esté adaptado a sus necesidades específicas al mismo tiempo que se mantienen los estándares de seguridad.
- **Implementación de un cortafuegos sólido:** Cada empresa de cada cliente está protegida por cortafuegos de nivel hipervisor o grupos de seguridad. Al utilizar software avanzado de virtualización y en la nube, estos cortafuegos dividen aún más las instancias de MCE y crean espacios de procesamiento de cliente completamente separados. Esta segregación resulta fundamental para repeler el acceso no autorizado y garantizar que la información no pública quede protegida.

En esencia, MicroStrategy AI no es simplemente una herramienta de procesamiento de datos inteligente: es un producto integrado profundamente en un entorno en la nube donde cada decisión de arquitectura prioriza la seguridad del usuario. Las estrictas propiedades de seguridad del entorno del MCE resaltan aún más nuestro inquebrantable compromiso de proteger la integridad de los datos de nuestros clientes.

Integración de MicroStrategy con Azure OpenAI

Cómo garantizar la privacidad e integridad de los datos con MicroStrategy AI

MicroStrategy AI

MicroStrategy AI ofrece una serie de funciones de IA que empoderan a usuarios con diversos niveles de habilidades y diferentes roles dentro de una organización. Los usuarios empresariales y los analistas pueden beneficiarse con Auto Answers, una propuesta de chatbot que les permite profundizar el uso de su panel y obtener información y análisis de datos muy detallados. Esto incluye control de calidad avanzado y visualizaciones de IA que aprovechan las capacidades de aprendizaje automático para generar análisis de impulsores clave, pronósticos y tendencias. También pueden usar bots que se enfocan en un caso de uso o personaje específico y admiten personalizaciones adicionales que utilicen campos de activos de conocimientos y de instrucciones personalizadas para proporcionar más contexto empresarial. Otras características disponibles en MicroStrategy AI incluyen Auto Dashboard, que permite a los usuarios diseñar paneles con más eficiencia, y Auto SQL, que ayuda a administradores y arquitectos a agilizar el modelado de datos generando SQL.

Todos los clientes que habilitan la IA en su entorno se benefician con una arquitectura en la que cada entorno de usuario es una empresa separada que se conecta con los servicios de gestión de MicroStrategy AI, que a su vez procesa la solicitud al modelo de lenguaje grande (LLM).

MicroStrategy permite que los usuarios ajusten su bot proporcionando contexto a través de un archivo que usa la funcionalidad de activos de conocimientos. El gestor de conocimientos procesa toda la información cargada mediante un archivo de Excel para aumentar los conocimientos de MicroStrategy AI. Luego, el modelo incrustado procesa esta información y la transforma en definiciones que se guardan en

la tienda de conocimientos. La tienda de conocimientos actúa como una caja fuerte segura para almacenar conocimientos de dominio que se han cifrado utilizando las técnicas de procesamiento cognitivo. Este cifrado no solo preserva la integridad de los datos, sino que también mejora su accesibilidad para las operaciones de búsqueda cognitiva.

Al interactuar con el módulo Gen AI, la tienda de conocimientos desempeña un papel esencial, ya que suministra información relevante para el contexto. Esto garantiza que Gen AI pueda formular consultas precisas y exactas de MicroStrategy. Los avanzados algoritmos de cifrado de la tienda se adaptan para facilitar la recuperación rápida y precisa del conocimiento.

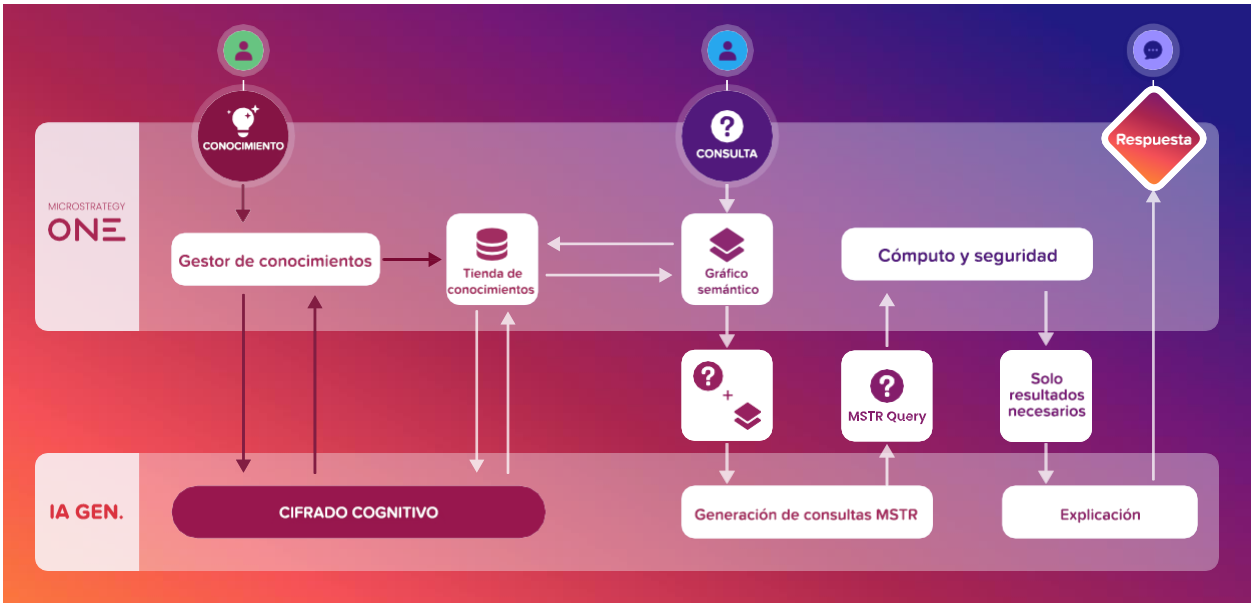
El diseño de la tienda de conocimientos prioriza la seguridad y la gobernanza de datos, garantizando que el conocimiento cifrado esté protegido contra el acceso no autorizado y la manipulación. Al mantener un alto estándar de seguridad de los datos, esta tienda proporciona una base sólida para generar resultados analíticos confiables y reveladores.

Solo los usuarios con privilegios pueden cargar activos de conocimientos para incrementar sus datos. Están protegidos por control de acceso, privilegios y cifrado.

La única información transferida entre MicroStrategy y el modelo de lenguaje grande (LLM) de Azure OpenAI es el esquema del conjunto de datos y los datos de muestra mínima para que el LLM tenga el contexto necesario para procesar la pregunta del usuario. Con la integración de la función de activos de conocimientos y la búsqueda cognitiva, también podemos incluir contexto adicional en el LLM, para lograr una respuesta más precisa. La solicitud se traslada a un plan de ejecución a través del LLM, y posteriormente se realizan cálculos a través del gráfico semántico y el motor analítico de MicroStrategy. De esta manera se garantiza que la información devuelta esté controlada y sea segura y confiable, con lo que se evitan alucinaciones que son problemas comunes con las soluciones que incluyen un LLM. Una vez que se realiza el cómputo, el cálculo se devuelve al LLM para su interpretación, y finalmente se muestra al usuario como lenguaje natural.

MicroStrategy AI utiliza Azure OpenAI de Microsoft, y todas las comunicaciones se realizan estrictamente por canales seguros con TLS 1.2 o superior. Esto garantiza que los datos estén siempre cifrados durante el tránsito y evita el acceso no autorizado o las violaciones de seguridad.

Las funciones de IA trabajan estrictamente dentro de los límites establecidos por los privilegios, las listas de control de acceso y las medidas de seguridad de los datos especificadas por el usuario en la plataforma de MicroStrategy.



Retención de datos

La funcionalidad Auto Answers no retiene historiales de conversaciones después de la sesión de usuario activa.

Los bots de MicroStrategy permiten a los usuarios retener su historial de chat y guardar instantáneas de sus datos. El acceso a este historial de chat y la información de las instantáneas se efectúa por usuario. La información no se comparte entre los usuarios. Además, esta información se aloja en el propio espacio de almacenamiento de la empresa y está completamente cifrada con cifrado AES de 256 bits.

MicroStrategy Platform Analytics reúne datos de telemetría sobre las interacciones de los usuarios con Auto para empoderar a los administradores. Esto incluye la captura de la pregunta del usuario, la interpretación de la pregunta (si se solicitó), la consulta en SQL generada para responder la pregunta y la plantilla de MicroStrategy creada para recuperar y presentar el resultado. El acceso a estos datos se administra limitando la cantidad de usuarios que acceden a los paneles de Auto Adoption y Auto Question Analysis, y sus objetos de esquema dependientes en Platform Analytics. Platform Analytics está alojado en la empresa de cada cliente.

Retención de datos históricos

MicroStrategy AI ofrece sólidas capacidades de retención de datos diseñadas para satisfacer las necesidades de nuestros usuarios al mismo tiempo que se garantizan la seguridad y la privacidad de sus datos. Cada usuario tiene derecho a retener un historial máximo de 30 preguntas y respuestas. Esta función permite a los usuarios acceder a sus interacciones anteriores y revisarlas, lo que mejora su experiencia al facilitar la continuidad y el aprendizaje a partir de consultas pasadas.

Eliminación manual de datos históricos

Con el fin de proporcionar a los usuarios el control sobre sus datos, MicroStrategy AI permite la eliminación manual de preguntas y respuestas de conversaciones pasadas. Los usuarios pueden eliminar las entradas que ya no necesitan a fin de mantener un historial limpio y relevante conforme a sus preferencias.

Instantáneas

Además de los datos históricos, los usuarios pueden crear y guardar instantáneas de preguntas y respuestas específicas. Estas instantáneas se almacenan independientemente del historial estándar y se pueden usar para preservar puntos de datos o información crítica. Cada usuario puede mantener hasta 50 instantáneas, lo que aporta gran flexibilidad en la administración y recuperación de los datos.

Ubicaciones de almacenamiento de datos

Almacenamiento del contenido de texto: El contenido de texto de las preguntas y respuestas se almacena de manera segura en la base de datos MicroStrategy Metadata. Esta base de datos está diseñada para brindar disponibilidad alta y está optimizada para permitir una recuperación eficiente de los datos.

Almacenamiento de datos de visualización: Los puntos de datos que se usan para visualizar cada pregunta se almacenan en MicroStrategy Storage Service. Antes de que los usuarios puedan comenzar a almacenar datos de visualización, deben configurar MicroStrategy Storage Service para asegurar un manejo y seguridad de los datos apropiados.

Text Content Storage y Visualization Data Storage están alojados dentro de la empresa de cada cliente.

Privacidad de los datos de usuario

Las preguntas, respuestas e instantáneas específicas de cada usuario son privadas, y solo el usuario puede acceder a ellas. Este estricto control de acceso es parte de nuestro compromiso con la privacidad de los usuarios y la seguridad de los datos que garantiza que la información sensible siga siendo confidencial y esté protegida.

Esta política de retención de datos es parte de nuestro esfuerzo constante por brindar una experiencia transparente, segura y enfocada en el usuario, que permita el uso efectivo y eficiente de MicroStrategy AI.

Cumplimiento normativo para los componentes de IA en el entorno de MicroStrategy Cloud

MicroStrategy AI, integrado con Azure OpenAI de Microsoft, tiene certificaciones internacionales de protocolos vitales de protección de datos, entre ellas CCPA, GDPR, SOC 2 e ISO 27001. El diseño y los procedimientos operativos de los componentes de MicroStrategy AI dentro del MCE están adaptados a estos estándares de referencia normativos. Nuestro riguroso respeto por la normativa demuestra nuestro compromiso con el cumplimiento y la superación de los estándares establecidos por estas autoridades.

El compromiso de MicroStrategy con la diligencia normativa es sistemático y meticuloso. Contamos con un equipo de cumplimiento normativo interno exclusivo que es responsable de garantizar nuestra adecuación a los estándares de la industria. Este equipo ha diseñado sólidos protocolos de protección y privacidad de los datos que apuntan directamente a cumplir con las disposiciones del Reglamento General de Protección de los Datos (RGPD). MicroStrategy confirma el pleno cumplimiento normativo en todas las jurisdicciones en las opera MicroStrategy Cloud.

El MCE, disponible para AWS, Azure y GCP, cumple con los siguientes marcos de gestión de riesgos y seguridad de la información. Dicho cumplimiento se valida periódicamente y, cuando es necesario, se certifica a través de rigurosas evaluaciones conducidas por profesionales internos y externos:

- Reglamento General de Protección de los Datos
- AICPA SSAE-18, Controles de sistemas y organización – Informe SOC 2 Tipo 2
- ISO/IEC 27001:2013 (ISO 27001:2013) – Certificado número: ISMS-MI-13123
- Marco de Privacidad de los Datos UE-EE. UU. y Suiza-EE. UU.
- Autoevaluación conforme a la Ley de Responsabilidad y Portabilidad del Seguro de Salud de 1996 (HIPAA).

Monitoreo, registro y auditoría del uso de la IA dentro de MicroStrategy

MicroStrategy enfatiza el monitoreo, registro y auditoría del uso de la IA dentro de su plataforma, para garantizar la transparencia y la responsabilidad. Los sistemas de monitoreo implementados ofrecen a los clientes un resumen integral de su uso de la IA. Mediante un panel fácil de usar, los clientes pueden hacer el seguimiento de la cantidad de preguntas que han realizado y obtener información respecto de qué usuarios la utilizan. Esta transparencia empodera a las organizaciones para que optimicen eficazmente su utilización de la IA.

Mecanismos de registro

MicroStrategy ha diseñado meticulosos mecanismos de registro para defender la privacidad y la seguridad de los datos de los usuarios. Dentro de la plataforma de MicroStrategy, se registra determinada información, mientras que se excluye otra información intencionalmente con el propósito de proteger los datos de usuario y cumplir con las leyes que protegen los datos.

Específicamente, el sistema de registro de MicroStrategy captura datos esenciales con fines operativos. Un ejemplo es la cantidad de tokens que se usan para las preguntas que formulan los usuarios, lo que garantiza que se haga el seguimiento de esta información para medir el consumo y el uso. Además, estos datos registrados no se usan para entrenar los modelos de IA o para otros fines que podrían comprometer la privacidad de los datos de los usuarios.

Esta estrategia consciente de la privacidad se corresponde con los estándares y reglamentaciones de protección de datos, y brinda a los usuarios la confianza de interactuar plenamente con las herramientas basadas en IA de MicroStrategy sin tener que preocuparse por la seguridad de su información sensible.

Pistas de auditoría

Las pistas de auditoría son esenciales para garantizar la responsabilidad y la trazabilidad dentro de la plataforma de MicroStrategy. MicroStrategy ha implementado un sólido sistema en Platform Analytics que permite a los clientes realizar pistas de auditoría eficazmente. Un elemento clave de este sistema es preservar un identificador (ID) de pregunta único que permite el seguimiento del uso real asociado con determinados usuarios. Sobre todo, el enfoque de MicroStrategy prioriza la privacidad del usuario al no registrar los resultados generados. En cambio, al enfocarse en el ID de la pregunta, MicroStrategy puede determinar con precisión qué usuario inició una consulta o utilizó funciones de IA específicas. Este enfoque equilibra la responsabilidad y la privacidad de los datos, garantizando que las acciones de los usuarios se puedan trazar y monitorear.

Cumplimiento de las listas de control de acceso y las medidas de seguridad de los datos

A medida que continuamos innovando y expandiendo nuestras ofertas, la protección y seguridad de los datos de los usuarios sigue siendo primordial. El surgimiento de las capacidades de MicroStrategy AI, incluida la notable función Auto, se ha diseñado con sumo cuidado para que estas capacidades se integren sin inconvenientes con el modelo de seguridad integral de la plataforma de MicroStrategy establecida. De esta forma, se garantiza no solo la coherencia en el acceso a los datos, sino también el cumplimiento fiel de los estrictos protocolos de seguridad.

- **Listas de control de acceso (ACL) y permisos coherentes:** Auto, nuestro asistente de IA, está adaptado para garantizar que los usuarios solo reciban respuestas derivadas de los conjuntos de datos para los que tienen autorización de acceso. Cada consulta que se presenta a Auto se somete a una meticulosa verificación contra las ACL configuradas de los objetos subyacentes de la capa semántica. Esto significa que la integridad de los controles de acceso se mantiene incluso mientras los usuarios interactúan con las funcionalidades de IA.
- **Acceso diferenciado a los datos a través de los filtros de seguridad:** Además de las configuraciones básicas de las ACL, nuestra plataforma ofrece control de acceso a los datos detallado mediante filtros de seguridad. Estos filtros actúan como una capa adicional de control que limita el rango de datos que los usuarios pueden consultar. Brinda a los administradores el poder de definir límites precisos para el acceso a los datos, con lo que se garantiza que los usuarios solo puedan interactuar con los segmentos de los datos que les son permitidos.
- **Privilegios configurables para las funciones de IA:** Como reconocemos que cada empresa tiene necesidades y problemas de seguridad únicos, hemos incorporado privilegios configurables para las funcionalidades de IA. Esto permite que los líderes de cada organización decidan qué usuarios pueden aprovechar las funciones avanzadas de IA, ya sea Auto o los análisis y visualizaciones más sofisticados basados en aprendizaje automático. Brinda a las empresas la flexibilidad para equilibrar la innovación con los protocolos de seguridad.

Integridad de los datos y prevención del uso indebido

La principal promesa de MicroStrategy es garantizar la absoluta seguridad de los datos y la prevención de su uso indebido. El panorama digital en expansión intensifica la importancia de la protección de los datos, y aquí mostramos cómo hemos anclado nuestra plataforma:

- **Sólidos protocolos de cifrado:** Nuestra plataforma garantiza la seguridad de los datos tanto en tránsito como en reposo. Las comunicaciones entre nuestra plataforma y los servicios externos, incluido Azure OpenAI de Microsoft, emplea técnicas de cifrado líderes en la industria, como TLS 1.2+, para proteger los datos durante la transmisión y así prevenir la posibilidad de interceptación. Además, implementamos el cifrado de datos en reposo utilizando estándares de cifrado avanzado como AES-256 para proteger los datos almacenados y garantizar que la información confidencial quede protegida contra el acceso no autorizado, incluso cuando no se esté transfiriendo activamente.

- **Configuraciones con Azure OpenAI de Microsoft:** Mediante los parámetros de configuración específicos de nuestra integración con Azure OpenAI de Microsoft, nos hemos asegurado de que los datos enviados a OpenAI no sean retenidos ni utilizados para entrenamiento del modelo. Esta configuración técnica proporciona otra capa de garantía de que los datos de usuario se mantienen intactos en las interacciones externas.
- **Privacidad de la interacción de los usuarios:** Si bien MicroStrategy registra métricas de uso para monitorear la frecuencia y el tipo de preguntas, MicroStrategy nunca accede a los detalles complejos de las conversaciones de los usuarios. Esta meticulosa distinción garantiza que el contenido principal de sus interacciones siga siendo privado, lo que destaca nuestro compromiso con la privacidad de los datos centrados en el usuario.

De conformidad con estos protocolos, MicroStrategy prioriza soluciones avanzadas a la vez que sigue dando gran importancia a la protección de los datos y la confianza de los usuarios. Nuestras prácticas subrayan nuestro énfasis en la excelencia funcional y la rigurosa seguridad de los datos.

Conclusión

El compromiso de MicroStrategy con la seguridad y la integridad de los datos es evidente en su oferta de MicroStrategy AI. En un dominio donde la confiabilidad de los datos impacta directamente sobre la precisión de la IA, MicroStrategy ha desarrollado su plataforma meticulosamente para que cumpla y exceda los rigurosos estándares relacionados con los datos.

La precisión de nuestra BI, combinada con la adaptabilidad de la IA, ofrece a los usuarios la ventaja de un análisis de avanzada sin poner en peligro la seguridad. A través del aislamiento diferenciado del entorno dentro del entorno de MicroStrategy Cloud, la privacidad de los datos se prioriza constantemente para mitigar los riesgos asociados con las violaciones de seguridad. El cumplimiento de las normas internacionales sobre protección de los datos está integrado en el diseño de nuestra plataforma, con lo que se sigue demostrando nuestra dedicación a los estándares globales.

Nuestro cumplimiento de las listas de control de acceso y de las rigurosas medidas de seguridad de los datos garantiza que los usuarios operen siempre dentro de parámetros de acceso a los datos bien definidos. Además, nuestra colaboración con Azure OpenAI de Microsoft está arraigada en las prácticas recomendadas de la industria y garantiza que los datos no sean retenidos más allá de su uso inmediato ni sean aplicados accidentalmente.

En resumen, MicroStrategy AI integra capacidades analíticas avanzadas con rigurosos estándares de protección de los datos. Nuestro enfoque es claro: entregar información de IA confiable y, a la vez, priorizar la seguridad y la protección de los datos. Para obtener más información sobre MicroStrategy AI, visite nuestro sitio web.

Información adicional

Documento sobre la seguridad de MicroStrategy Cloud

MicroStrategy Incorporated, 1850 Towers Crescent Plaza, Tysons Corner, VA 22182

microstrategy.com