Strategy₿

ARTIGO TÉCNICO

Segurança de IA

Explore etapas práticas para garantir a integridade dos dados e implementações éticas da IA

Sumário

Introdução

A implantação eficiente da inteligência artificial (IA) na business intelligence (BI) depende significativamente da integridade dos dados subjacentes. Para os sistemas de IA que conduzem as decisões de negócios, a precisão não é meramente benéfica, ela é imperativa. Esses sistemas precisam ser confiáveis para terem utilidade genuína.

A Strategy se destaca como um pilar confiável nesse contexto, fornecendo dados precisos e seguros para os usuários de negócios. A introdução do Strategy AI reforça esse compromisso, com uma plataforma na qual o rigor do BI se une às capacidades inovadoras da IA.

Nossa solução de IA foi projetada para interpretar com precisão as questões de negócios apresentadas em linguagem natural, empregar raciocínio lógico e gerar resultados relevantes de maneira autônoma. Essa síntese da análise estruturada do BI e da adaptabilidade da IA garante que o Strategy AI atenda às necessidades de integridade dos dados e interação flexível dos usuários.

O Strategy AI é uma evolução da nossa plataforma estabelecida e integra perfeitamente recursos avançados de IA e machine learning. Ele simplifica processos como a exploração de dados orientada por IA, a automação do design de painéis e o uso de ferramentas especializadas, tais como a geração de SQL e visualização aprimorada por machine learning para análises de dados. Com esses recursos, a plataforma facilita a obtenção de insights de dados mais profundos dentro do ecossistema familiar do Strategy.

A confiabilidade do Strategy AI está ancorada no meticuloso design da camada semântica da Strategy e em sua estrutura abrangente de segurança. O Auto, nosso assistente de IA, usa exclusivamente os dados da Strategy, e todas as análises são executadas pelo nosso mecanismo analítico estabelecido. Isso garante o processamento e a representação de dados consistentes, precisos e seguros, permitindo que as empresas tomem decisões embasadas com confiança.

Isolamento do ambiente no Strategy AI

A principal força de uma solução de IA empresarial não está apenas na sua capacidade de processar dados e fornecer insights, mas também na resistência da arquitetura a ameaças externas. O Strategy Cloud Environment (MCE) é sustentado por um design que dá a máxima ênfase ao isolamento do ambiente, ao acesso seguro e à execução protegida de solicitações em serviços externos ou multilocatários.

Design com foco no isolamento:

O MCE foi projetado estrategicamente tendo o isolamento do ambiente como um dos pilares centrais de segurança. Ao garantir que os dados de cada cliente operem em um ambiente segmentado com segurança, eliminamos riscos de contaminação cruzada e reforçamos a proteção dos dados. Quando o sistema precisa se conectar ou enviar uma solicitação a um serviço externo, esses fluxos de trabalho são executados com rigorosas medidas de segurança e protocolos de comunicação. Isso inclui transmissão de dados criptografados e solicitações de execução sem reconhecimento de estado dentro do contexto de segurança da instância do cliente.

Strategy AI no MCE:

A oferta do Strategy Cloud é complementada e aprimorada com a inclusão do módulo Strategy AI. Ao ancorá-lo na estrutura do MCE, garantimos que o Strategy AI mantenha consistentemente os robustos padrões de segurança do ambiente que são intrínsecos ao MCE.

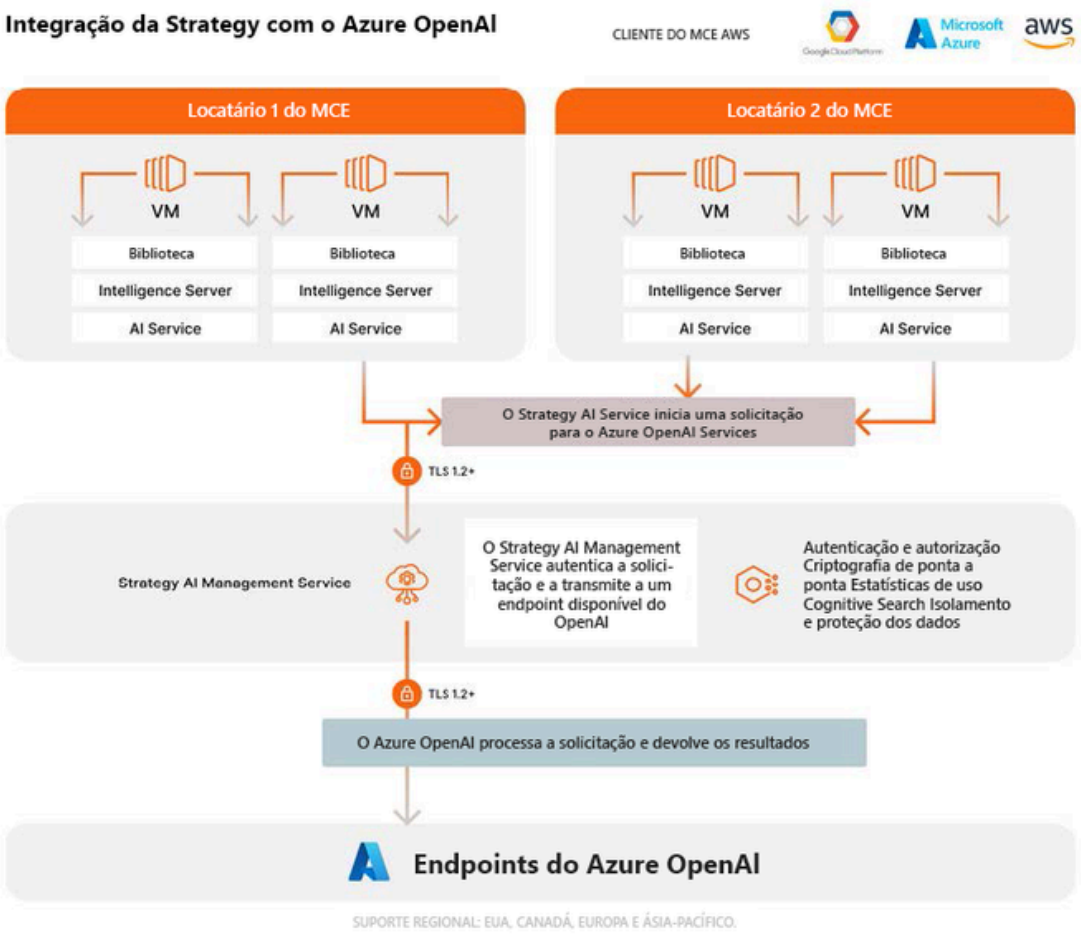
Características do isolamento do MCE:

- **Configurações personalizadas:** A Strategy pode iniciar recursos em nuvens virtuais privadas (VPCs) e modificar intervalos de endereços de protocolo Internet (IP), tabelas de rotas, gateways de rede e configurações de segurança pertinentes. Isso garante que o ambiente de cada cliente seja adaptado às necessidades específicas deles e, ao mesmo tempo, mantenha os padrões
- de segurança.

- **Implementação robusta de firewall:** o locatário de cada cliente é fortalecido por firewalls ou
- grupos de segurança em nível de hipervisor. Utilizando softwares avançados de nuvem e virtualização, esses firewalls dividem ainda mais as instâncias do MCE, criando espaços de processamento de clientes totalmente separados. Essa segregação é fundamental para evitar
- o acesso não autorizado e assegurar que informações não públicas permaneçam protegidas.

Em essência, o Strategy AI não é uma mera ferramenta inteligente de processamento de dados; ele é um produto profundamente integrado a um ambiente de nuvem em que cada decisão de design prioriza a segurança dos usuários. As rigorosas propriedades de segurança do ambiente do MCE destacam ainda mais nosso compromisso inabalável de proteger a integridade dos dados dos nossos clientes.

Integração da Strategy com o Azure OpenAI



Garantia da privacidade e da integridade dos dados com o Strategy AI

Strategy AI

O Strategy AI oferece uma série de recursos de IA para capacitar usuários com diferentes níveis de habilidade e diferentes funções dentro de uma organização. Analistas e usuários de negócios podem aproveitar as vantagens do Auto Answers, uma experiência de chatbot que permite que se aprofundar nos painéis e fornece insights e análises detalhadas de dados. Isso inclui visualizações avançadas de IA e perguntas e repostas que usam recursos de machine learning para gerar análises, previsões e tendências dos principais fatores. Eles também podem usar bots que se concentram em um caso de uso ou persona específicos e permitem personalizações adicionais, com o apoio dos campos "Ativo de conhecimento" e "Instruções personalizadas" para fornecer mais contexto comercial. Outros recursos disponíveis no Strategy AI incluem o Auto Dashboard, que permite aos usuários criar painéis de maneira mais eficiente, e o Auto SQL, que ajuda os administradores e arquitetos a agilizar a modelagem de dados com geração de SQL.

Cada cliente que adota a IA em seu ambiente utiliza uma arquitetura em que cada ambiente de cliente é um locatário separado que se conecta ao Strategy AI Management Services, que processa a solicitação para o LLM.

Agora a Strategy permite que os usuários ajustem seus bots fornecendo contexto através de um arquivo com a funcionalidade de ativos de conhecimento. O gerenciador de conhecimento processa todas as informações carregadas por um arquivo do Excel para ampliar o conhecimento do Strategy AI. Em seguida, o modelo de incorporação processa essas informações, transformando-as em definições salvas no repositório de conhecimento. O repositório de conhecimento funciona como um cofre seguro para armazenar o conhecimento do domínio que foi codificado usando técnicas de processamento cognitivo. Essa codificação preserva a integridade dos dados e melhora sua acessibilidade para operações de pesquisa cognitiva.

Ao interagir com o módulo de IA generativa, o repositório de conhecimento desempenha um papel fundamental, fornecendo informações contextualmente relevantes. Isso garante que a IA generativa possa formular consultas precisas e exatas da Strategy. Os algoritmos avançados de codificação do repositório são adaptados para facilitar a recuperação rápida e precisa do conhecimento.

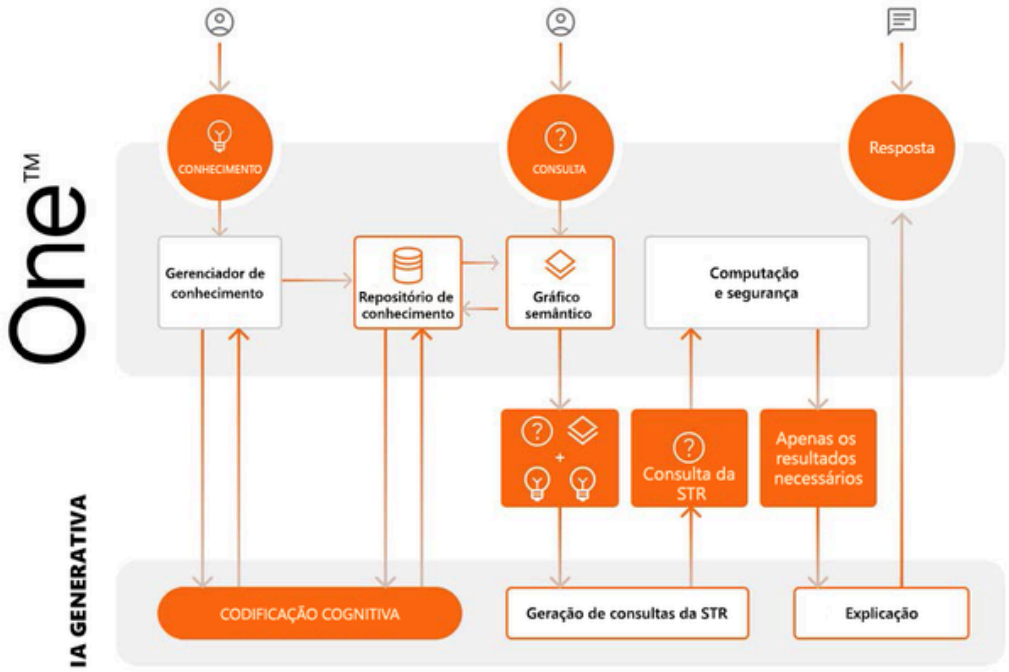
O design do repositório de conhecimento enfatiza a segurança e a governança de dados, de modo que o conhecimento codificado seja protegido contra acesso e manipulação não autorizados. Ao manter um alto padrão de segurança de dados, esse repositório fornece uma base sólida para gerar resultados analíticos confiáveis e relevantes.

Somente usuários privilegiados podem carregar ativos de conhecimento para ampliar seus dados. Esses ativos são protegidos por controle de acesso, privilégios e criptografia.

As únicas informações transferidas entre a Strategy e o LLM do Azure OpenAI são o esquema do conjunto de dados e dados de amostra mínimos, para que o LLM tenha o contexto necessário para processar a pergunta do usuário. Com a integração dos ativos de conhecimento e da pesquisa cognitiva, também podemos incluir contexto adicional ao LLM para obter uma resposta mais precisa. A solicitação é convertida em um plano de execução no LLM, e cálculos subsequentes são realizados com o gráfico semântico e o mecanismo analítico da Strategy. Isso assegura que as informações fornecidas sejam regulamentadas, seguras e confiáveis, evitando erros comuns em soluções com LLM. Depois de pronto, o cálculo é retornado ao LLM para interpretação e, por fim, exibido ao usuário como linguagem natural.

O Strategy AI usa o Microsoft Azure OpenAI, e toda a comunicação é feita estritamente por canais seguros via TLS 1.2 ou superior. Isso garante que os dados sejam sempre criptografados durante o trânsito, impedindo violações ou acesso não autorizado.

Os recursos de IA funcionam estritamente dentro dos limites estabelecidos pelos privilégios, ACLs e medidas de segurança de dados especificadas para o usuário na plataforma Strategy.



Retenção de dados

A funcionalidade Auto Answers não retém históricos de conversas após a sessão do usuário ativo.

Os Auto Bots da Strategy permitem que os usuários mantenham seu histórico de chat e salvem snapshots dos dados. O acesso a esse histórico de chat e às informações de snapshots é feito com base em cada usuário. As informações não são compartilhadas entre os usuários. Além disso, elas ficam salvas no espaço de armazenamento do próprio locatário e são totalmente criptografadas com AES de 256 bits.

O Strategy Platform Analytics reúne dados de telemetria sobre as interações dos usuários com o Auto para capacitar os administradores. Isso inclui a captura da pergunta do usuário, a interpretação da pergunta (se solicitada), a consulta SQL gerada para responder à pergunta e o Modelo Strategy criado para recuperar e apresentar o resultado. Para gerenciar o acesso a esses dados, é possível limitar o número de usuários que podem acessar os painéis Auto Adoption e Auto Question Analysis e seus objetos de esquema dependentes no Platform Analytics. O Platform Analytics é hospedado no locatário de cada cliente.

Retenção de dados históricos

O **Strategy** AI oferece recursos robustos de retenção, projetados para atender às necessidades dos nossos usuários e, ao mesmo tempo, garantir a segurança e a privacidade de seus dados. Cada usuário tem o direito de reter um máximo de 30 perguntas e respostas históricas. Esse recurso permite que os usuários acessem e avaliem suas interações anteriores, aprimorando a experiência ao facilitar a continuidade e o aprendizado com consultas passadas.

Exclusão manual de dados históricos

Para fornecer aos usuários o controle sobre seus dados, o Strategy AI permite a exclusão manual de perguntas e respostas de conversas anteriores. Os usuários podem remover entradas não mais necessárias, mantendo um histórico limpo e relevante de acordo com suas preferências.

Snapshots

Além dos dados históricos, os usuários podem criar e salvar snapshots de perguntas e respostas específicas. Esses snapshots são armazenados independentemente do histórico padrão e podem ser usados para preservar insights ou pontos de dados críticos. Cada usuário pode manter até 50 snapshots, o que permite uma flexibilidade significativa no gerenciamento e na recuperação dos dados.

Locais de armazenamento de dados

Armazenamento do conteúdo de texto: O conteúdo de texto das perguntas e respostas é armazenado com segurança no banco de dados de metadados da Strategy. Esse banco de dados foi projetado com foco em disponibilidade e otimização para a recuperação eficiente de dados.

Armazenamento de dados de visualizações: Os pontos de dados usados para visualizar cada resposta são armazenados no Strategy Storage Service. Antes de começar a armazenar dados de visualizações, os usuários devem configurar o Strategy Storage Service para garantir o manuseio correto e a devida segurança dos dados.

O armazenamento de conteúdo de texto e o armazenamento de dados de visualizações residem no locatário de cada cliente.

Privacidade dos dados dos usuários

Perguntas, respostas e snapshots específicos do usuário são privados e acessíveis apenas pelo usuário individual. Esse rigoroso controle de acesso faz parte do nosso compromisso com a privacidade dos usuários e com a segurança dos dados, garantindo que informações sensíveis permaneçam confidenciais e protegidas.

A política de retenção de dados representa o nosso esforço contínuo para fornecer uma experiência transparente, segura e focada no usuário, o que termina por possibilitar o uso eficaz do Strategy AI.

Conformidade regulatória para os componentes de IA no Strategy Cloud Environment

O Strategy AI, integrado ao Microsoft Azure OpenAI, tem certificações para protocolos internacionais essenciais de proteção dos dados, incluindo CCPA, GDPR, SOC 2 e ISO 27001. O design e os procedimentos operacionais dos componentes do Strategy AI no MCE são adaptados em torno dessas referências regulatórias. Nossa abordagem rigorosa de aderência demonstra nosso compromisso em cumprir os padrões estabelecidos por essas autoridades e também em superá-los.

O compromisso da Strategy com a diligência regulatória é sistemático e meticuloso. Mantemos uma equipe de conformidade interna dedicada e responsável por garantir o alinhamento com os padrões do setor. Essa equipe projetou protocolos robustos de proteção de dados e privacidade, com o objetivo direto de atender aos rigores do Regulamento Geral sobre a Proteção de Dados (GDPR). A Strategy confirma total aderência regulatória em todas as jurisdições de operação do Strategy Cloud

O MCE, disponível para AWS, Azure e GCP, está em conformidade com as estruturas de gerenciamento de riscos e segurança da informação listadas a seguir. A conformidade é validada regularmente e, quando necessário, certificada por avaliações rigorosas conduzidas por profissionais internos e terceirizados:

- Regulamento Geral de Proteção de Dados
- AICPA SSAE-18, Controles de Sistemas e Organizações – Relatório SOC 2 Tipo 2
- ISO/IEC 27001:2013 (ISO 27001:2013) – Número do certificado: ISMS-MI-13123
- Estrutura de Privacidade dos Dados da UE/EUA e Suíça/EUA.
- Autoavaliação nos termos da HIPAA (Health Insurance Portability and Accountability Act) de 1996.

Conformidade do Strategy AI com a Lei da UE sobre IA

O Strategy AI está comprometido em cumprir a Lei da UE sobre IA, que tem como objetivo garantir o uso seguro e ético das tecnologias de IA na Europa. O Strategy AI incorpora um modelo de linguagem grande de IA de Propósito Geral (GPAI), o Azure OpenAI, para fornecer recursos de IA aos nossos clientes. É um sistema de risco limitado orientado por recursos de nível básico. Os recursos do Strategy AI, incluindo Auto Answers, Auto Bots e Auto Dashboard, são baseados em chat e sempre atendem a um usuário em vez de tomarem decisões automatizadas. Além disso, por se tratar de um sistema de IA de risco limitado, o Strategy AI é propositalmente transparente, e a Strategy implementou práticas de gestão de qualidade em torno do produto Strategy AI, como:

- Medidas de segurança robustas.
- Transparência na tomada de decisões.
- Informações claras sobre as interações do usuário com a IA.
- Avaliações e melhorias regulares do sistema da IA.

Por fim, o Strategy AI e todos os seus recursos inteligentes se baseiam exclusivamente no mecanismo confiável e proprietário da Strategy. O Strategy AI não utiliza entradas do usuário, histórico de chat ou outras comunicações para treinar qualquer LLM, GPAI ou outros modelos de inteligência artificial.

Monitoramento, registro em log e auditoria do uso da IA na Strategy

A Strategy enfatiza significativamente o monitoramento, o registro em log e a auditoria do uso da IA na sua plataforma para garantir transparência e responsabilidade. Os sistemas de monitoramento em vigor oferecem aos clientes uma visão abrangente de como usam a IA. Em um painel prático, os clientes podem acompanhar o número de perguntas feitas e obter insights sobre quais usuários as utilizam. Essa transparência permite que as organizações otimizem a utilização da IA de maneira eficaz.

Mecanismos de registro em log

A **Strategy** projetou mecanismos de registro meticulosos para manter a privacidade e a segurança dos dados dos usuários. Na plataforma Strategy, certas informações são registradas enquanto outras são intencionalmente omitidas, com o objetivo de proteger os dados dos usuários e cumprir as leis de conformidade de dados.

Em específico, o sistema de registro em log da plataforma Strategy captura dados essenciais para fins operacionais. Um exemplo é o número de tokens usados para as perguntas feitas pelos usuários, garantindo que essas informações sejam rastreadas para avaliar o consumo e o uso. Além disso, esses dados registrados não são usados para treinar modelos de IA nem para outros fins que possam comprometer a privacidade dos dados dos usuários.

Essa estratégia centrada na privacidade se alinha aos padrões e regulamentos contemporâneos de proteção de dados, proporcionando aos usuários a confiança necessária para uma interação total com as ferramentas do Strategy AI, sem que eles se preocupem com a segurança de suas informações confidenciais.

Trilhas de auditoria

Trilhas de auditoria são essenciais para garantir a responsabilidade e a capacidade de rastreamento dentro da plataforma Strategy. A Strategy implementou um sistema robusto no Platform Analytics que permite aos clientes realizar trilhas de auditoria de maneira eficaz. Um elemento fundamental desse sistema é a preservação de um ID de pergunta exclusivo, que viabiliza o rastreamento do uso real associado a usuários individuais. Acima de tudo, a abordagem da Strategy prioriza a privacidade do usuário por não registrar os resultados gerados. Em vez disso, ao se concentrar no ID da pergunta, a Strategy é capaz de determinar com precisão qual usuário iniciou uma consulta ou utilizou recursos específicos de IA. Essa abordagem traz um equilíbrio entre responsabilidade e privacidade dos dados, garantindo que as ações dos usuários possam ser rastreadas e monitoradas.

Aderência a listas de controle de acesso e medidas de segurança dos dados

À medida que continuamos buscando a inovação e a expansão das nossas ofertas, a segurança e a proteção dos dados dos usuários continuam sendo fundamentais. A introdução dos recursos do Strategy AI, om destaque para a funcionalidade Auto, foi cuidadosamente arquitetada para integrar-se ao modelo de segurança abrangente da plataforma Strategy estabelecida. Isso garante a consistência no acesso aos dados e o cumprimento constante de rigorosos protocolos de segurança.

- **Listas de controle de acesso (ACLs) e permissões consistentes:** o Auto, nosso assistente de IA, é adaptado para assegurar que os usuários recebam apenas respostas derivadas dos conjuntos de dados que estão autorizados a acessar. Todas as consultas feitas ao Auto passam por uma verificação meticulosa em relação às ACLs configuradas dos objetos subjacentes da camada semântica. Isso significa que, mesmo que os usuários se envolvam com as funcionalidades de IA, a integridade dos controles de acesso não será comprometida.

- **Acesso granular aos dados com filtros de segurança:** Além das configurações básicas, nossa plataforma oferece controle granular de acesso aos dados usando filtros de segurança. Eles atuam como uma camada adicional de controle, pois restringem o escopo dos dados que os usuários podem consultar. Com eles, os administradores podem definir limites precisos para o acesso aos dados e ter a certeza de que os usuários só podem interagir com segmentos de dados autorizados.

- **Privilégios configuráveis para recursos de IA:** sabemos que cada empresa tem suas necessidades e preocupações de segurança, então incorporamos privilégios configuráveis para as funcionalidades de IA. Isso permite que os líderes organizacionais decidam quais usuários podem usar os recursos avançados de IA, como o Auto ou as análises e visualizações mais sofisticadas orientadas por ML. Desse modo, as empresas têm a flexibilidade necessária para equilibrar a inovação e os protocolos de segurança.

Integridade de dados e prevenção de uso indevido

A principal promessa da Strategy gira em torno de garantir a segurança absoluta dos dados e a prevenção de uso indevido. O cenário digital em constante expansão intensifica a importância da proteção dos dados, e é assim que ancoramos nossa plataforma:

- **Protocolos de criptografia robustos:** nossa plataforma garante a segurança dos dados em trânsito e em repouso. Qualquer comunicação entre nossa plataforma e serviços externos, incluindo o Microsoft Azure OpenAI, emprega técnicas de criptografia líderes do setor, como TLS 1.2+, para proteger os dados durante a transmissão e evitar possíveis interceptações. Além disso, implementamos a criptografia de dados em repouso com padrões avançados de criptografia, como AES-256, para proteger os dados armazenados e garantir que as informações confidenciais permaneçam protegidas contra acesso não autorizado, mesmo quando não estiverem sendo ativamente transferidas.

- **Configurações com o Microsoft Azure OpenAI:** por meio das definições de configuração específicas na nossa integração com o Microsoft Azure OpenAI, garantimos que os dados enviados ao OpenAI não sejam retidos nem usados para o treinamento de modelos. Essa configuração técnica fornece outra camada de garantia para que os dados do usuário permaneçam intactos nas interações externas.

- **Privacidade na interação com os usuários:** Embora a Strategy registre métricas de uso para monitorar a frequência e os tipos de perguntas, os detalhes intrincados das conversas dos usuários nunca são acessados pela Strategy. Essa distinção meticulosa faz com que o conteúdo principal de suas interações permaneça privado, enfatizando nosso compromisso com a privacidade dos dados centrada no usuário.

Em linha com esses protocolos, a Strategy prioriza soluções avançadas e mantém uma forte ênfase na proteção dos dados e na confiança dos usuários. Nossas práticas ressaltam a importância que damos tanto à excelência funcional quanto à proteção rigorosa dos dados.

Conclusão

O compromisso da Strategy com a segurança e a integridade dos dados é evidente no produto Strategy AI. Em um domínio em que a confiabilidade dos dados afeta diretamente a precisão da IA, a Strategy desenvolveu sua plataforma meticulosamente para cumprir e exceder rigorosos padrões de dados.

A precisão da nossa BI, combinada com a adaptabilidade da IA, oferece aos usuários a vantagem das análises de alto nível sem comprometer a segurança. Com o isolamento de ambientes no Strategy Cloud Environment, a privacidade dos dados é priorizada de maneira consistente, mitigando os riscos associados a violações. A conformidade com as normas internacionais de proteção de dados é fundamental no design da nossa plataforma e comprova nossa dedicação no cumprimento dos padrões globais.

Nossa adesão a listas de controle de acesso e rigorosas medidas de segurança de dados garantem que os usuários sempre operem dentro dos parâmetros definidos de acesso aos dados. Ademais, nossa colaboração com o Microsoft Azure OpenAI está enraizada nas práticas recomendadas do setor e assegura que os dados não sejam retidos além de seu uso imediato ou aplicados de maneira não intencional.

Em resumo, o Strategy AI integra recursos analíticos avançados com padrões rigorosos de proteção de dados. Nosso foco é claro: fornecer insights de IA confiáveis e, ao mesmo tempo, priorizar a segurança e a proteção dos dados. Para saber mais sobre o Strategy AI, acesse nosso site.

Strategy Incorporated, 1850 Towers Crescent Plaza, Tysons Corner, VA 22182.

strategysoftware.com