MicroStrategy

MicroStrategy AI: Security Whitepaper

Explore practical steps to ensure data integrity and ethical AI implementations.

Published: August 2024

Table of Contents

Introduction

The effective deployment of artificial intelligence (AI) in business intelligence (BI) significantly depends on the integrity of the underlying data. For AI systems driving business decisions, accuracy isn't merely beneficial; it's imperative. These systems need to be trustworthy to be of genuine utility.

MicroStrategy stands out as a reliable pillar in this context, providing business users with data that is both precise and secure. The introduction of MicroStrategy AI reinforces this commitment, offering a platform where the rigor of BI meets the innovative capabilities of AI.

Our AI solution is engineered to accurately interpret business questions presented in natural language, employ logical reasoning, and produce relevant results autonomously. This synthesis of BI's structured analysis and AI's adaptability ensures that MicroStrategy AI meets the dual needs of data integrity and flexible user engagement.

MicroStrategy AI is an evolution of our established platform, seamlessly integrating advanced AI and machine learning capabilities. It streamlines processes such as AI-driven data exploration, dashboard design automation, and the use of specialized tools like SQL generation and machine learning-enhanced visualization for data analysis. With these features, the platform facilitates more profound data insights within the familiar environment of the MicroStrategy ecosystem.

The reliability of MicroStrategy AI is anchored in the meticulous design of the MicroStrategy semantic layer and its comprehensive security framework. Auto, our AI assistant, exclusively relies on data from MicroStrategy, with all analytics executed by our established analytical engine. This ensures consistent, accurate, and secure data processing and representation, allowing businesses to make informed decisions with confidence.

MicroStrategy AI Environment Isolation

The core strength of an enterprise AI solution lies not only in its ability to process data and deliver insights but also in its architecture's resilience to external threats. The MicroStrategy Cloud Environment (MCE) is underpinned by an architectural design that places the utmost emphasis on environment isolation, secure access, and safe execution of requests on external or multi-tenant services.

Designing for Isolation:

The MCE was strategically architected with environment isolation as a central security tenet. By ensuring that each customer's data operates in a securely segmented environment, we eliminate cross-contamination risks and enhance data protection. When the system needs to connect or submit a request to an external service, these workflows are executed with strict security measures and communication protocols. This includes encrypted data transmission and stateless execution requests within the security context of the customer's instance.

MicroStrategy AI within MCE:

The MicroStrategy Cloud offering is complemented and enhanced by including the MicroStrategy AI module. By anchoring it within the MCE framework, we ensure that MicroStrategy AI consistently benefits from and upholds the robust environment security standards intrinsic to MCE.

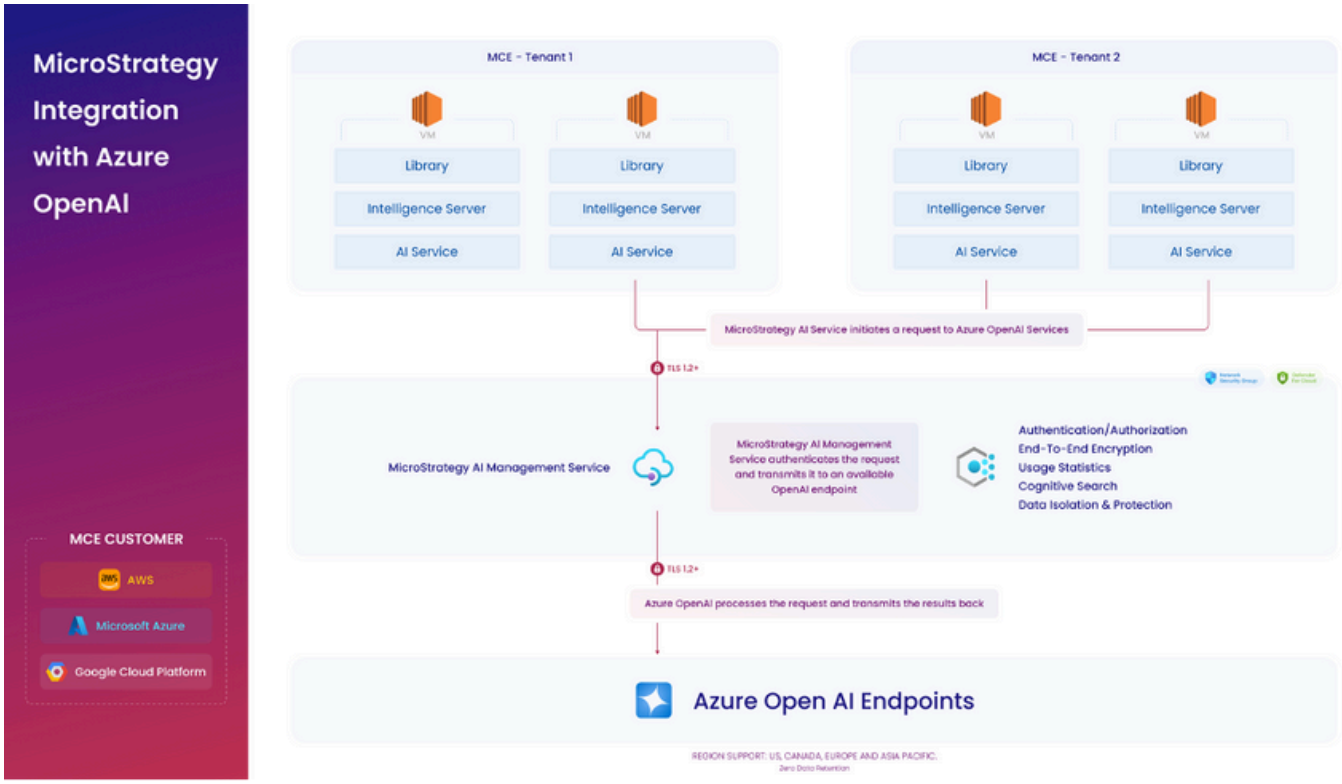
Characteristics of the MCE's Isolation:

- **Custom Configurations:** MicroStrategy can initiate resources into the Virtual Private Clouds (VPCs) and modify internet protocol (IP) address ranges, route tables, network gateways, and pertinent security settings. This ensures that every customer's environment is tailored to their specific needs while upholding security standards.

- **Robust Firewall Implementation:** Each customer's tenant is fortified by hypervisor-level firewalls or security groups. Utilizing advanced cloud and virtualization software, these firewalls further split MCE instances, creating entirely separated client processing spaces. This segregation is instrumental in warding off unauthorized access and ensuring that non-public information remains protected.

In essence, MicroStrategy AI is not merely an intelligent data processing tool; it is a product deeply integrated into a cloud environment where every architectural decision prioritizes user security. The stringent environment security properties of the MCE further highlight our unwavering commitment to safeguarding the integrity of our customers' data.

MicroStrategy Integration with Azure OpenAI



Ensuring Data Privacy and Integrity with MicroStrategy AI

MicroStrategy AI

MicroStrategy AI provides an array of AI features to empower users with varying skill levels and different roles within an organization. Business users and analysts can take advantage of Auto Answers, a chatbot experience that allows them to dig deeper into their dashboard by providing insights and in-depth data analysis. This includes advanced Q&A and AI visualizations that leverage machine learning capabilities to generate key driver analysis, forecasts, and trends. They can also use bots that are focused on a specific use case or persona and allow for additional customizations leveraging Knowledge Asset and Custom Instructions fields to provide more business context. Other features available in MicroStrategy AI include Auto Dashboard, which enables users to design dashboards more efficiently, and Auto SQL, which helps administrators and architects to expedite data modeling by generating SQL.

Every customer that enables AI in their environment leverages an architecture where each customer environment is a separate tenant that connects to MicroStrategy AI Management Services, which processes the request to the LLM.

MicroStrategy now enable users to fine-tune their bot by providing context through a file using the Knowledge Assets functionality. The Knowledge Manager processes all the information uploaded through an Excel file to augment the knowledge of MicroStrategy AI. The embedding model then processes this information, transforming it into definitions saved on the Knowledge Store. The Knowledge Store acts as a secure vault for storing domain knowledge that has been encoded using cognitive processing techniques. This encoding not only preserves the integrity of the data but also enhances its accessibility for cognitive search operations.

When interacting with the Gen AI module, the Knowledge Store plays a critical role by supplying contextually relevant information. This ensures that the Gen AI can formulate precise and accurate MicroStrategy queries. The store's advanced encoding algorithms are tailored to facilitate the swift and accurate retrieval of knowledge.

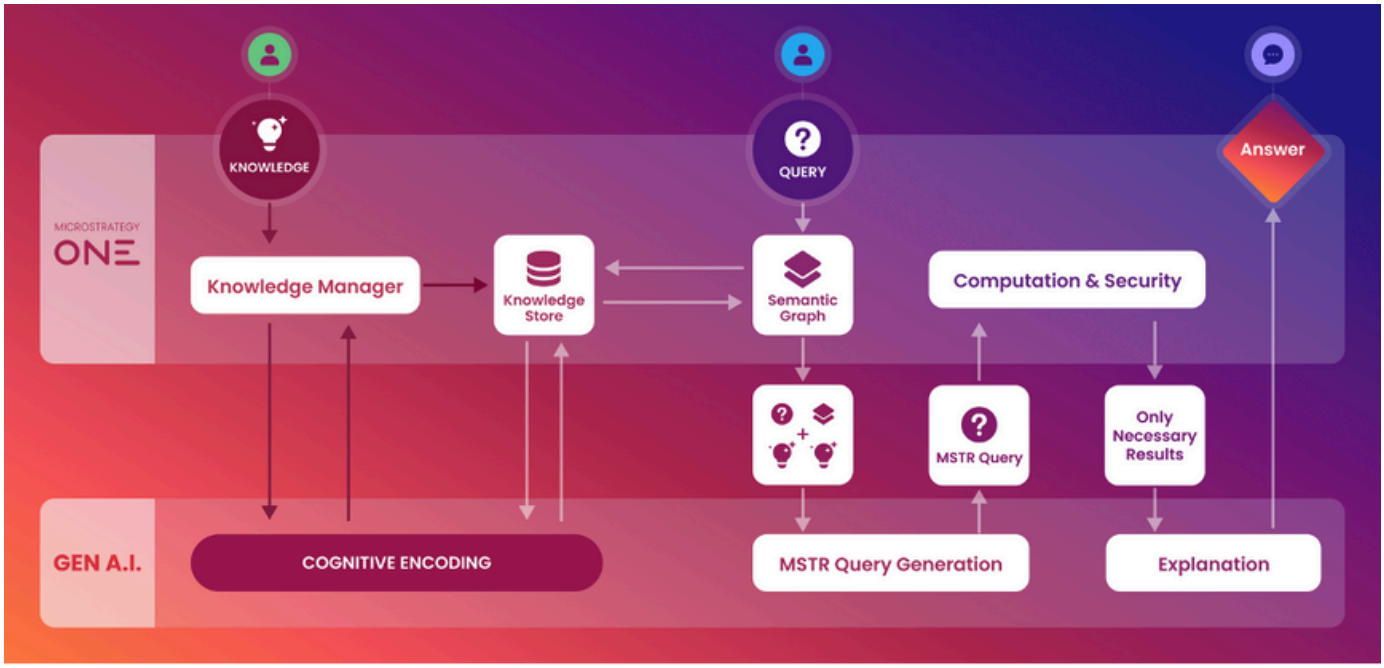
The design of the Knowledge Store emphasizes security and data governance, ensuring that the encoded knowledge is protected against unauthorized access and manipulation. By maintaining a high standard of data security, this store provides a robust foundation to generate reliable and insightful analytical results.

Only privileged users can upload knowledge assets to augment their data. They are protected through access control, privileges, and encryption.

The only information transferred between MicroStrategy, and the Azure OpenAI LLM is the dataset's schema and minimal sample data so that the LLM has necessary context to process the user question. With the integration of the Knowledge Asset function and cognitive search, we can also include additional context to the LLM for a more precise response. The request is translated into an execution plan through the LLM and subsequent calculations are performed through the MicroStrategy's Semantic Graph and analytical engine. This guarantees that the information returned will be governed, secure, and trusted, avoiding hallucinations that are common concerns with LLM solutions. Once the computation is done, the calculation is returned to the LLM for interpretation, and it is finally displayed to the user as natural language.

MicroStrategy AI uses Microsoft Azure OpenAI, and all communication is strictly over secure channels with TLS 1.2 or higher. This ensures that data is always encrypted during transit, preventing unauthorized access or breaches.

The AI Features work strictly within the boundaries set by Privileges, ACLs, and data security measures specified for the user in the MicroStrategy platform.



Data Retention

The Auto Answers functionality does not retain conversation histories after the active user session.

MicroStrategy Auto Bots enable users to persist their chat history and save snapshots of their data. Access to this chat history and the snapshot information is on a per-user basis. The information is not shared between users. Further, this information is stored in tenant's own storage space and is fully encrypted using AES-256 bit encryption.

MicroStrategy Platform Analytics gathers telemetry data on user interactions with Auto to empower administrators. This includes capturing the user's question, the interpretation of the question (if requested), the SQL query generated to address the question, and the MicroStrategy Template created to retrieve and present the result. Access to this data is managed by limiting the number of users accessing the Auto Adoption and Auto Question Analysis dashboards and their dependent schema objects in Platform Analytics. Platform Analytics is hosted under each customer's tenant.

Historical Data Retention

MicroStrategy AI offers robust data retention capabilities designed to meet the needs of our users while ensuring the security and privacy of their data. Each user is entitled to retain a maximum of 30 historical questions and answers. This feature allows users to access and review their previous interactions, enhancing their experience by facilitating continuity and learning from past inquiries.

Manual Deletion of Historical Data

To provide users with control over their data, MicroStrategy AI enables the manual deletion of questions and answers from past conversations. Users can remove entries they no longer need, maintaining a clean and relevant history according to their preferences.

Snapshots

In addition to historical data, users can create and save snapshots of specific questions and answers. These snapshots are stored independently of the standard history and can be used to preserve critical data points or insights. Each user can maintain up to 50 snapshots, allowing for significant flexibility in data management and retrieval.

Data Storage Locations

Text Content Storage: The text content of questions and answers are securely stored in the MicroStrategy Metadata database. This database is designed for high availability and is optimized for efficient data retrieval.

Visualization Data Storage: Data points used to visualize each answer are stored in the MicroStrategy Storage Service. Before users can begin storing visualization data, they must configure the MicroStrategy Storage Service to ensure proper data handling and security.

The Text Content Storage and Visualization Data Storage reside inside each customer's tenant.

User Data Privacy

User-specific questions, answers, and snapshots are private and accessible only to the individual user. This strict access control is part of our commitment to user privacy and data security, ensuring that sensitive information remains confidential and protected.

This data retention policy is part of our ongoing effort to provide a transparent, secure, and user-focused experience, enabling effective and efficient use of MicroStrategy AI.

Regulatory Compliance for the AI Components in the MicroStrategy Cloud Environment

MicroStrategy AI, integrated with Microsoft Azure OpenAI, has certifications for vital international data protection protocols, including CCPA, GDPR, SOC 2, and ISO 27001. The design and operational procedures of the MicroStrategy AI components within the MCE are tailored around these regulatory benchmarks. Our stringent approach to adherence demonstrates our commitment to meeting and surpassing the standards set by these authorities.

MicroStrategy's commitment to regulatory diligence is systematic and meticulous. We maintain a dedicated internal compliance team responsible for ensuring alignment with industry standards. This team has architected robust data protection and privacy protocols, directly aiming to meet the rigors of the General Data Protection Regulation (GDPR). MicroStrategy confirms full regulatory adherence across all jurisdictions where the MicroStrategy Cloud operates

The MCE, available for AWS, Azure, and GCP is compliant with the following risk management and information security frameworks. Such compliance is regularly validated, and when necessary, certified through rigorous evaluations conducted by both internal and third-party professionals:

- General Data Protection Regulation
- AICPA SSAE-18, System and Organization Controls – SOC 2 Type 2 Report
- ISO/IEC 27001:2013 (ISO 27001:2013) – Certificate Number: ISMS-MI-13123
- Data Privacy Framework EU-U.S. and Swiss-U.S.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Self-Assessment.

MicroStrategy AI Compliance with the EU AI Act

MicroStrategy AI is committed to complying with the EU AI Act, which aims to ensure the safe and ethical use of AI technologies in Europe. MicroStrategy AI, which incorporates a General Purpose AI (GPAI) large language model, Azure OpenAI, in order to provide AI capabilities to our customers, is a limited-risk AI system based on its base-level capabilities. MicroStrategy AI's capabilities, including Auto Answers, Auto Bots, and Auto Dashboard, are chat-based and always serve a user rather than make automated decisions. In addition, as a deployer of a limited-risk AI system, MicroStrategy AI is purposefully transparent, and MicroStrategy has implemented quality management practices surrounding our MicroStrategy AI product, including:

- Robust safety measures.
- Transparency in decision-making.
- Clear user information about AI interaction.
- Regular assessments and improvements of the AI system.

Finally, MicroStrategy AI and all of its intelligent features exclusively rely on MicroStrategy's own trusted calculation engine. MicroStrategy AI does not utilize user inputs, chat history, or other communications to train any LLM, GPAI, or other third-party artificial intelligence models.

Monitoring, Logging, and Auditing AI Use within MicroStrategy

MicroStrategy places a significant emphasis on monitoring, logging, and auditing the usage of AI within its platform to ensure transparency and accountability. The monitoring systems in place offer customers a comprehensive overview of their AI usage. Through a user-friendly dashboard, customers can track the number of questions they have made and gain insights into which users use them. This transparency empowers organizations to optimize their AI utilization effectively

Logging Mechanisms

MicroStrategy has designed meticulous logging mechanisms to uphold user data privacy and security. Within the MicroStrategy platform, certain information is logged while others are intentionally left out, with the purpose of safeguarding user data and meeting data compliance laws.

Specifically, MicroStrategy's logging system captures essential data for operational purposes. One example is the number of tokens used for the questions posed by users, ensuring that this information is tracked to measure consumption and usage. Furthermore, this logged data is not used to train AI models or for other purposes that might compromise user data privacy.

This privacy-conscious strategy aligns with contemporary data protection standards and regulations, providing users with the confidence to fully engage with MicroStrategy's AI-powered tools without worrying about the security of their sensitive information.

Audit Trails

Audit trails are crucial in ensuring accountability and traceability within the MicroStrategy platform. MicroStrategy has implemented a robust system in Platform Analytics that allows customers to perform audit trails effectively. One key element of this system is preserving a unique question ID, which enables tracking of actual usage associated with individual users. Importantly, MicroStrategy's approach prioritizes user privacy by not recording the outcomes generated. Instead, by focusing on the question ID, MicroStrategy can precisely determine which user initiated a query or utilized specific AI features. This approach balances accountability and data privacy, ensuring user actions can be traced and monitored.

Adhering to Access Control Lists and Data Security Measures

As we continue to innovate and expand our offerings, the safety and security of user data remain paramount. The introduction of the MicroStrategy AI capabilities, including the notable Auto feature, has been carefully architected to seamlessly integrate with the comprehensive security model of the established MicroStrategy platform. This ensures not only consistency in data access but also steadfast adherence to stringent security protocols.

- **ConsistentAccess Control Lists(ACLs) and Permissions:** Auto, our AI assistant, is tailored to ensure users only receive answers derived from datasets they're authorized to access. Every query posed to Auto undergoes meticulous verification against the configured ACLs of the semantic layer's underlying objects. This meansthat even as users engagewith the AI functionalities, the integrity of access controls remains uncompromised.

- **Granular Data Accessthrough Security Filters:** Beyond the basic ACL configurations, our platform offers fine-graineddata access controlusing security filters.These filters act as an additional layerof control, narrowing down the data scope that users can query. It provides administrators the power to define precise boundaries on data access, ensuring users can only interact with permitted segments of the data.

- **Configurable Privileges for AI Features:** Recognizing that every enterprise has its unique needs and security concerns, we've incorporated configurable privileges for AI functionalities. This allows organizational leaders to decidewhich users can leverage advancedAI features, be it Auto or the more sophisticated ML-driven analyticsand visualizations. It provides businesses with the flexibility to balance innovation with security protocols.

Data Integrity and Preventing Misuse

MicroStrategy's core promise revolves around ensuring absolute data security and prevention of misuse. The expanding digital landscape intensifies the importance of data protection, and here's how we've anchored our platform:

- **Robust Encryption Protocols:** Our platform ensures the security of data both in transit and at rest. Any communication between our platform and external services, including Microsoft Azure OpenAI, employs industry-leading encryption techniques, such as TLS 1.2+, to protect data during transmission, preventing potential interception. Additionally, we implement data-at-rest encryption by utilizing advanced encryption standards like AES-256 to secure stored data, ensuring that sensitive information remains protected against unauthorized access even when not actively being transferred.

- **Configurations with Microsoft Azure OpenAI:** Through the specific configuration settings in our integration with Microsoft Azure OpenAI, we've ensured that data sent to OpenAI is not retained or used for model training. This technical configuration provides another layer of assurance that user data remains untouched in external interactions.

- **User Interaction Privacy:** While MicroStrategy does record usage metrics for monitoring the frequency and type of questions, the intricate details of user conversations are never accessed by MicroStrategy. This meticulous distinction ensures the core content of your interactions remains private, emphasizing our commitment to user-centric data privacy.

In line with these protocols, MicroStrategy prioritizes advanced solutions while maintaining a strong emphasis on data protection and user trust. Our practices underscore the importance we place on both functional excellence and stringent data security.

Conclusion

MicroStrategy's commitment to data security and integrity is evident in its MicroStrategy AI offering. In a domain where the trustworthiness of data directly impacts the accuracy of AI, MicroStrategy has meticulously constructed its platform to meet and exceed rigorous data standards.

The precision of our BI, combined with AI's adaptability, offers users the advantage of cutting-edge analysis without compromising security. Through the distinct environment isolation within the MicroStrategy Cloud Environment, data privacy is consistently prioritized, mitigating risks associated with breaches. Compliance with international data protection regulations is integral to our platform's design, further demonstrating our dedication to global standards.

Our adherence to Access Control Lists and stringent data security measures guarantee users always operate within defined data access parameters. Furthermore, our collaboration with Microsoft Azure OpenAI is rooted in industry best practices, ensuring data is not retained beyond its immediate use or applied unintendedly.

In summary, MicroStrategy AI integrates advanced analytical capabilities with rigorous data protection standards. Our focus is clear: delivering dependable AI insights while prioritizing data security and protection. To learn more about MicroStrategy AI, please visit our website.

Additional Information

MicroStrategy Cloud Security White Paper