MicroStrategy
INTELLIGENCE EVERYWHERE

MicroStrategy AI: Security Whitepaper

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

Published: October 2023

Table of Contents

Introduction

The effective deployment of artificial intelligence (AI) in business intelligence (BI) significantly depends on the integrity of the underlying data. The foundational understanding is clear: the accuracy of AI models and their subsequent results directly correlate with the quality of the input 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.

Ensuring Data Privacy and Integrity with MicroStrategy AI

MicroStrategy AI employs stringent data security measures to maintain the privacy and integrity of your data.

Data Transmission & Encryption:

- MicroStrategy AI uses encryption protocols TLS 1.2 or higher, during data transmission.
- Communication with Microsoft Azure OpenAI is strictly over secure channels, ensuring that data is always encrypted during transit, preventing unauthorized access or breaches.

Data Retention Principles:

- MicroStrategy AI does not retain conversation histories post the active user session.
- This design eliminates the potential risk of storing sensitive information or specific content shared during interactions.

User Interaction & Anonymization:

- MicroStrategy logs usage data, such as question consumption, for internal analysis and service improvement.
- Specific user interactions and conversation content are exempt from these logs, ensuring user-specific details remain confidential.

Role of Microsoft Azure OpenAI in Upholding Security:

- Collaborative configurations with Microsoft Azure OpenAI are designed to prioritize data security.
- Azure OpenAI operates under parameters set by MicroStrategy, which prohibit unwarranted data retention or use to train their models.

Continuous Review and Enhancements:

- MicroStrategy AI's security protocols undergo continuous reviews and are aligned with industry best practices.
- Feedback mechanisms ensure practices remain updated against evolving security threats.
- By adhering to these principles and protocols, MicroStrategy AI offers an enhanced user experience while ensuring uncompromised data privacy and security.

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 when needed.

Designing for Isolation:

The MCE was strategically architected with environment isolation as a dedicated 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. This includes encrypted data transmission and stateless execution requests within the security context of the customer's instance.

MicroStrategy AI within MCE:

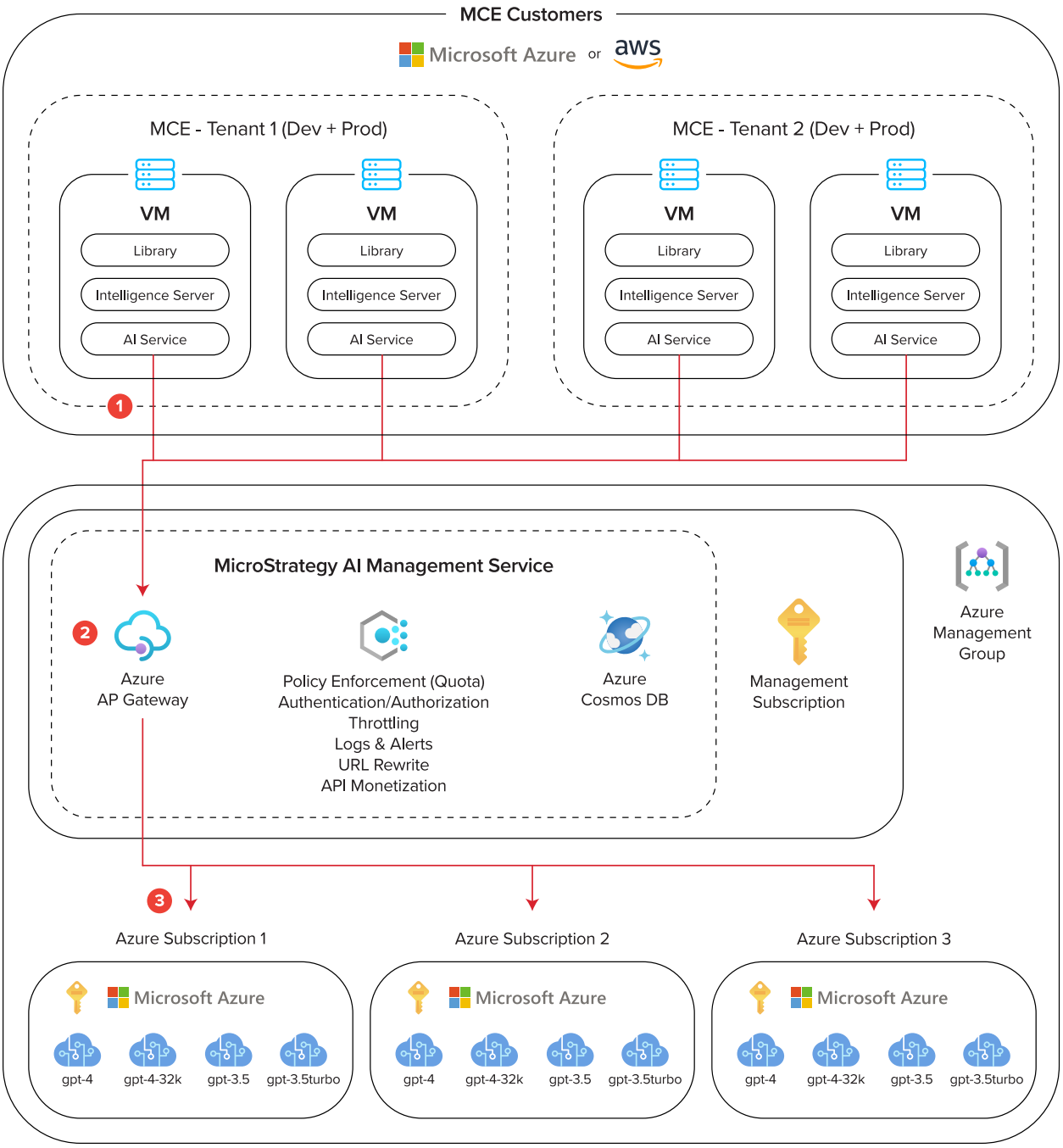
The MicroStrategy Cloud offering is complemented and enhanced by the inclusion of the MicroStrategy AI module. By anchoring it within the MCE framework, we ensure that MicroStrategy AI consistently benefits from and upholds the robust environment security standards intrinsic to MCE.

Characteristics of the MCE's Isolation:

- **Unique Virtual Private Cloud (VPC) Instances:** Every customer of the MicroStrategy Cloud receives a unique VPC. This is a dedicated virtual network and computing environment that remains logically separated from other customers' deployments, guaranteeing data exclusivity and protection.
- **Custom Configurations:** MicroStrategy can both initiate resources into these 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 deployment 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 our customers' data integrity.

MicroStrategy Integration with Azure OpenAI



(Region Support: US, Canada, Europe, and Asia Pacific)

1. MicroStrategy AI Service initiates a request to Azure OpenAI Service.
2. MicroStrategy AI Management Service authenticates the request and transmits it to available Azure OpenAI endpoint.
3. Azure OpenAI processes the request and transmits the request back.

Figure 1. High-level architecture of the integration between the MicroStrategy Cloud Environment and the Azure OpenAI service.

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 SOC 3. 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). Collaborating with the legal department, they confirm full regulatory adherence across all jurisdictions where the MicroStrategy Cloud operates.

The MCE, available for both AWS and Azure, 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.

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 a purpose to safeguarding user data and meeting data compliance laws.

Specifically, MicroStrategy's logging system captures essential data for operational purposes. It records the number of tokens used for the questions posed by users, ensuring that this information is tracked for measuring consumption and usage. However, the logs do not store sensitive data elements such as the content of the questions asked, or the outcomes generated by these queries. Furthermore, this logged data is not used to train AI models, or for any 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 that allows customers to perform audit trails effectively. One key element of this system is the preservation of 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 specific content of the questions asked or 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 without compromising sensitive information.

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.

- **Consistent Access 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 means that even as users engage with the AI functionalities, the integrity of access controls remains uncompromised.

- **Granular Data Access through Security Filters:** Beyond the basic ACL configurations, our platform offers fine-grained data access control using security filters. These filters act as an additional layer of 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 decide which users can leverage advanced AI features, be it Auto or the more sophisticated ML-driven analytics and visualizations. It provides businesses with the flexibility to balance innovation with security protocols.

The MicroStrategy AI suite, while bringing cutting-edge capabilities to the forefront, remains steadfast in its commitment to uphold the rigorous security measures synonymous with the MicroStrategy brand.

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:

- **Session-Limited Data Retention:** User data is transient, meaning it is not stored beyond the duration of an active session. This minimizes data vulnerability and aligns with the best practices of data handling.
- **Robust Encryption Protocols:** Any communication between our platform and external services, including Microsoft Azure OpenAI, employs industry-leading encryption techniques. This guarantees the security of data during transmission, preventing potential interception.
- **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 stored. 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 on 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 guarantees 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 in unintended ways.

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 at www.microstrategy.com/ai.

Additional Information

MicroStrategy Cloud Security White Paper. MicroStrategy 2023

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

microstrategy.com