Benchmark Gensuite Services:

Security and Privacy Overview for AI Usage

Benchmark Digital Partners LLC

DATE: 05-SEPTEMBER-2024

REVISION CONTROL PAGE

Version	Date	Author	Change Reference	Reason for Change
1.0	09/05/2024	Jason Krueger Lucas Read	Initial document creation	AI Security review

SECURITY AND PRIVACY OVERVIEW FOR AI USAGE

Introduction

Benchmark Gensuite has prioritized the delivery of cutting-edge AI solutions within our digital risk management solutions platform that are secure and data privacy-compliant. As a SaaS provider, we understand the importance of protecting our customers' data and ensuring compliance with the highest industry standards. This document details the security and data privacy measures implemented in our integrated AI capabilities to assure that all established data privacy agreements (DPAs) and contractual obligations to data security and privacy are upheld, providing a secure foundation for AI usage in the platform.

Background

Following a comprehensive assessment and field trials of available proprietary Generative AI platforms, Benchmark Gensuite has implemented Amazon Bedrock as our exclusive solution for platform-integrated GenAI capabilities. Amazon Bedrock allows us to assure compliance with established contractual data security and privacy obligations. We have also strategically incorporated Amazon Bedrock in our regional AWS hosting platforms to support the US, EU, and IN regions, leveraging its regional infrastructure to enhance security, scalability, and data privacy compliance.

Regional Deployment and Scalability

Amazon Bedrock forms the backbone of our AI operations, deployable in US, EU, and IN regions; our infrastructure is designed to scale to other AWS regions as required, ensuring robust and flexible AI solutions for our customers.

Isolated and Secure Environments

Amazon Bedrock is deployed within our dedicated Virtual Private Cloud (VPC), creating isolated network environments that enhance security. We manage access to resources securely through AWS Identity and Access Management (IAM), and data in transit and at rest is encrypted using AWS Key Management Service (KMS). No additional sub-processors will be involved in the processing of your data, risk is reduced by avoiding additional third parties.

Network Security and Monitoring

We implement comprehensive network security measures, including security groups, network ACLs, and private subnets to prevent unauthorized access. Continuous monitoring and logging are performed using AWS CloudTrail and Amazon CloudWatch, ensuring any suspicious activities are promptly detected and addressed.

Secure Integration

Our integration with Amazon Bedrock is designed to ensure the highest levels of security. By using API endpoints for all AI-related activities, we maintain a secure environment for data processing and management. Each interaction with the API, which refers to any request or response exchanged between our systems and the API, is authenticated and authorized through the use of API keys. Data in transit is encrypted using Transport Layer Security (TLS).

Stringent Access Controls

We enforce strict access controls to manage and restrict access to sensitive data following the least privilege model. Only authorized Benchmark Gensuite personnel have access to your data, ensuring it remains protected at all times. Amazon Bedrock has committed not to use customer data for training their models, reinforcing our commitment to your data's privacy and integrity.

Comprehensive Privacy Measures

Your privacy is paramount. AWS Bedrock integrates robust guardrails to monitor and filter AI-generated responses, ensuring that sensitive or proprietary information is not inadvertently disclosed. These guardrails utilize AWS's in-built policies, which allow us to manage responses safely without storing or using customer-specific data in a way that could compromise privacy or intellectual property rights. Documentation on these guardrails is maintained by AWS. Importantly, no logging of user data interactions occurs within this environment, ensuring a secure and privacy-centric approach to data handling. This setup aligns with AWS's policies, where logging of AI-generated content can be controlled, and data retention complies with our customer agreements to maintain high standards of privacy and security. You retain full ownership and control over your data, with the assurance that we do not train on your business data. You also have the right to determine how long your data is retained. Data retention is determined by the LSA contract. Data would be purged from our system 30 days after the end of contract obligations.

Robust Security Framework

Benchmark Gensuite security framework includes SOC 2 Type 2 audits. We ensure data encryption both at rest (AES-256) and in transit (TLS 1.2+), adhering to the highest data protection standards.

Compliance and Certifications

Our compliance framework aligns with AWS programs, ensuring adherence to SOC 1/2/3, ISO 27001 standards, and GDPR. Benchmark Gensuite holds SOC 1/2/3 reports and ISO 27001 certification, leveraging AWS certifications to maintain superior data protection standards.

Benchmark Gensuite is dedicated to providing the highest standards of compliance and privacy for your intellectual property. To ensure our AI operates responsibly, we focus on three main areas: compliance and protection, your data rights, and transparency and support.

Our AI solutions are designed with your legal and proprietary rights in mind. We strictly adhere to all relevant laws and regulations, including the EU AI Act and applicable data protection laws. Our AI does not infringe on any third-party intellectual property rights, such as patents, copyrights, trademarks, trade secrets, or other proprietary rights. Additionally, the output generated by our AI is crafted to avoid any violations of third-party rights or legal regulations.

Your data, your rights. When you input data into our AI tools, you retain full ownership of that data. Benchmark Gensuite, or any third party, will never claim any rights or licenses over your data. We will not use your data for training or improving our AI. You have a perpetual, royalty-free, and global right to use and benefit from the AI output for your business needs, in accordance with all applicable laws. We will not use your AI output for training or enhancement purposes and claim no rights to it.

We are committed to transparency and providing you with the information you need. Upon request, we will supply you with details about the AI's decision-making processes, particularly if they involve high-risk systems or sensitive decisions. This includes explanations and documentation of the underlying decision models to help you understand how our AI operates.

The Path Forward

As we innovate and enhance our AI capabilities, our strategic vision includes continually optimizing use of Amazon Bedrock's infrastructure to provide even more secure, scalable, and compliant AI solutions. We are committed to this transition and will keep our customers informed about the progress and timelines, ensuring a seamless and transparent migration.

Conclusion

At Benchmark Gensuite, protecting the security and privacy of our customers' data is the top our AI operations. By leveraging the capabilities of Amazon Bedrock, we uphold the highest standards of data protection and regulatory compliance. For more detailed information or specific inquiries, please reach out to our security and privacy team by submitting a HelpMe request.

References

Benchmark Gensuite Template Data Processing Agreement

**Please note DPAs (when applicable) are executed on a subscriber-specific basis.*

Benchmark Gensuite ISO 27001:2022 Certification

Benchmark Gensuite SOC 3 Type 2 Report

AWS Bedrock Guardrails