safetica

FAQ: Safetica's Use of AI

JULY 28, 2025

Safetica's Use of AI

The following document details how Safetica interacts with and utilizes AI to enhance the capabilities of Intelligent Data Security. This document will be updated periodically as our technology is enhanced.

Safetica uses AI technologies for the following key scenarios:

1. Summarization (Cloud version only)
2. Risk assessment (Cloud version only)
3. Behavior analysis
4. Data flow control

There are three architectures to manage customer data by AI technologies:

1. **Internal pretrained models:** These are expert systems and models trained on external or arbitrary created datasets built into the product platform to solve cases like classification detection, user activity classification, web categorization (Zvelo), application behavior heuristics or similar.
2. **External pretrained models:** Safetica utilizes enterprise grade, third-party services that guarantee customer data will not be included in AI model training. These models must meet all key compliance regulations, and the data is used for transparent scenarios only. Currently, Microsoft Azure OpenAI is the only external model utilized by Safetica within this category.
3. **Dynamically trained internal models:** These models are generated from each individual customer's data within their tenant, to ensure there are no instances of cross-customer data mixing. They are used in cases where pretrained models are insufficient, such as dynamic DLP, user behavior analysis, and operational risk, and are part of the customer tenant, in our on-premises version or cloud based on the product deployment version.

What third-party AI service does Safetica's Intelligent Data Security use?

Currently, Safetica exclusively uses Microsoft Azure OpenAI as an external AI service. No other third-party AI services are used. Click here for a list of all third-party licenses.

How does Safetica ensure the privacy of its customer's data when utilizing AI?

All Microsoft AI services operate under an enterprise agreement with enhanced privacy and compliance settings. No data is used for learning purposes.

How does Safetica utilize AI in practice?

Safetica's AI service and core are specifically designed to not share customer data. The service learns only for the individual customer based on their own data and stores all final models internally in the customer's production tenant. Our service learns from metadata generated from user activity and file activity, as well as outputs (metadata) from data classification. It does not learn from our individual customers' internal documents. When we can, we use anonymization in the process.

Is any data sent externally or to third-party AI providers?

Data is only shared with the third-party providers in the above-listed link. This means that only Azure OpenAI uses customer data when necessary, with no training or saving on the Microsoft side, which is ensured by their Enterprise agreement.

How does Safetica AI ensure data security and compliance?

Safetica maintains strict standards for all external technologies and services, to ensure technology readiness for enterprise organizations, wide compliance and no training on customer data. The requirements are ensured by contract with our suppliers (e.g. Microsoft Enterprise Agreement), and the technology is then managed by Safetica's supply chain security and management processes.

For dynamically trained internal models, we use the Software Security Development Life Cycle process to ensure the proper architecture, quality assurance and cloud provisioning. We ensure that the technology is fully operated within the Safetica product, in the customer tenant (cloud or on-premises, based on the product version being used by the customer). The selection of this technology stack meets the best practices of enterprise development.

When is it expected that Safetica's current AI utilization will change?

Safetica's AI utilization is continuously evolving as part of our ongoing development initiatives. However, it's important to note that any significant changes to the high-level architecture will continue to uphold the established standards for data security, privacy, and compliance.

Should there be any modifications involving third-party technologies or providers, customers will be informed promptly through release notes and third-party notice documents. Customer trust in the Safetica AI stack is very important to us and we regard transparency as a fundamental value.

Where can I learn more?

1. Please review Safetica's Knowledge Base periodically for access to our release notes.

Who can I contact for more information?

If you have additional questions, please email support@safetica.com .