BLACK KITE

UNIQUE™ PARSER

FAQ

Data

How is data treated?

- The Black Kite parsing engine (UniQuE™ Parser) and Black Kite as a platform does not store or write uploaded data to disk when consuming any security documentation, artifacts, or questionnaires. Once the parsing engine has reviewed, parsed, scored and mapped the security artifacts and/or questionnaires to the 15 frameworks and/or the Enterprise framework, the contents and data of the security artifacts and/or questionnaires are deleted to protect the privacy of the data and to protect the NDAs in place between our customers and their vendors. If you choose to save the results, Black Kite only retains the mapped confidence and completeness scores for future reference and for our customers to have historical compliance trend analysis capabilities. Black Kite is not a security artifact or document repository; we rely on GRCs or VRMs to fill that function. Black Kite built the natural language model that powers our parsing engine in-house and does not use any open-source software or publicly available AI services like ChatGPT. It is also important to note that Black Kite does not use any of the uploaded documentation to further train our parsing engine.

Is customer data used to train algorithms and/or provided results to your customers?

- No.

Do you encrypt tenant data at rest (on disk/storage) within your environment?

- Yes, using Advanced Encryption Standard (AES) 256.

BLACK KITE

UNIQUE™ PARSER FAQ

AI Use

Do you leverage Artificial Intelligence (AI) for the product we are considering and if so, is the AI homegrown or managed by a third-party?

- Yes, we leverage a homegrown AI that's based on Google's cloud compute capabilities. It's used to make suggestions, calculations, and more based off our data lake (this is what enables our Cyber Risk Quantification (CRQ) using Open FAIR™ methodology, Ransomware Susceptibility Index® (RSI™), Data Breach Index (DBI), and other intelligence). It is also used to map uploaded artifacts to the various compliance frameworks we support. Customer uploaded artifacts are NOT stored when used to feed the machine learning engine. They are kept in memory while the parsing/matching takes place, then only the matches themselves and document metadata (timestamp, name, uploader) are kept for customer reference. The rest is released/deleted from memory.

What is your governance process around AI within your organization and your AI types used (e.g., deep learning, machine learning, AI, generative AI)?

- We use machine learning (ML) for the purposes stated above. The typical governance processes you would see around AI (most involving correction/opting out for individuals whose data is collected) don't apply to our use case, which is all processing public information such as open ports, unpatched front end code, leaked credentials, etc. For what it's worth, we do have the means to correct errors here. Users can manually map/unmap findings in the parser and mark findings as false positives for the vulnerability aspect of the platform. It is worth noting we are not using AI to process the information of individuals, like their names, emails, or phone numbers. We are also not using generative AI.