[Datasheet]

Unleash TruOps’ Full GRC Potential With Generative AI

TruOps
Cyber Risk Management

Clark by TruOps is a generative AI module that integrates with your organization’s data to provide unified visibility, reporting, and recommendations on your security, risk, and compliance posture.

INTRODUCTION

Clark is an intelligent, conversational assistant that extends far beyond traditional chatbots or compliance operations to deliver real-time, meaningful insight to data analytic questions posed in plain, natural language. Clark spans across your entire integrated technology stack to extract, interpret, and provide you with clear answers to your most pressing security, risk, and compliance questions.

CLARK FLAWLESSLY DELIVERS:

- A unified view, understanding, and approach to internal, third party, and regulatory risks.
- Data-driven, risk-based dashboards and analysis to support accurate decision-making.
- Quick, precise, and verified answers and insights for assessments by simply uploading a file.
- A faster way to view, report, predict, and ultimately respond to risk.

HOW DOES CLARK WORK?

High level Architecture

Clark provides a seamless and secure user experience, robust data management, and intelligent, real-time analytic responses to complex queries.

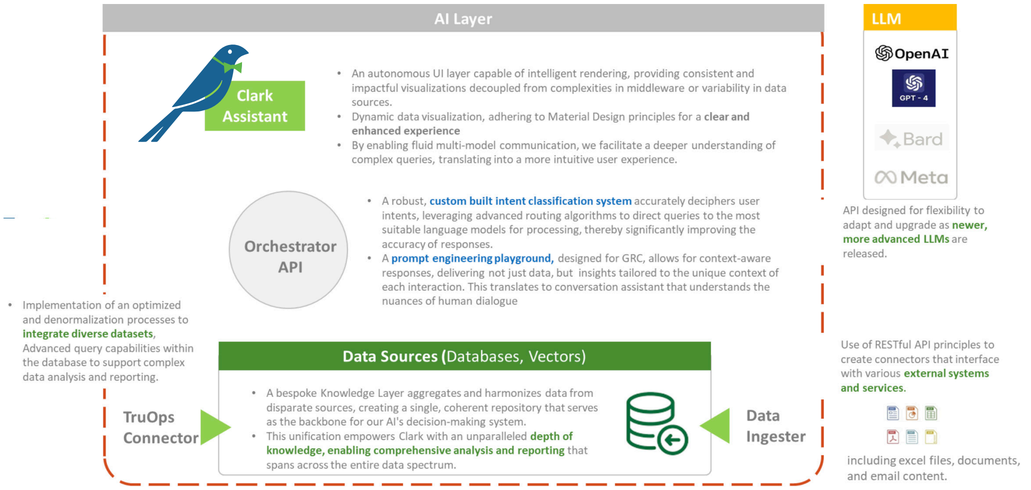
Clark’s modern and **intuitive UI** is designed for ease of use and accessibility. It is intentionally simple to ensure users can easily navigate and make the most out of Clark’s capabilities.

Clark’s AI optimized database is designed to handle large volumes of TruOps data which supports segregation through logical partitioning with Row Level Security (RLS) and Module Level Security (MLS) ensuring data privacy and security.

The vector storage in Clark’s architecture is specialized for managing unstructured data, such as text files, Excel spreadsheets, and PDF documents. It is optimized for high-speed data retrieval and storage, making it highly efficient for processing and analyzing large sets of unstructured data.

The **API layer** acts as a bridge which handles all the requests and responses, ensuring smooth communication between different components of the system, maintaining data privacy and security during these interactions.

At the core of Clark’s analytical capabilities are **Large Language Models (LLMs)** like those provided by OpenAI. They are integrated into the system via the API layer, ensuring that the data used for generating responses is handled securely and in compliance with data privacy standards.



- An autonomous UI layer capable of intelligent rendering, providing consistent and impactful visualizations decoupled from complexities in middleware or variability in data sources.
- Dynamic data visualization, adhering to Material Design principles for a **clear and enhanced experience**
- By enabling fluid multi-model communication, we facilitate a deeper understanding of complex queries, translating into a more intuitive user experience.

- A robust, **custom built intent classification system** accurately deciphers user intents, leveraging advanced routing algorithms to direct queries to the most suitable language models for processing, thereby significantly improving the accuracy of responses.
- A **prompt engineering playground,** designed for GRC, allows for context-aware responses, delivering not just data, but insights tailored to the unique context of each interaction. This translates to conversation assistant that understands the nuances of human dialogue

- Implementation of an optimized and denormalization processes to **integrate diverse datasets**, Advanced query capabilities within the database to support complex data analysis and reporting.

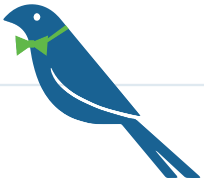
- A bespoke Knowledge Layer aggregates and harmonizes data from disparate sources, creating a single, coherent repository that serves as the backbone for our AI's decision-making system.
- This unification empowers Clark with an unparalleled **depth of knowledge, enabling comprehensive analysis and reporting** that spans across the entire data spectrum.

API designed for flexibility to adapt and upgrade as **newer, more advanced LLMs** are released.

Use of RESTful API principles to create connectors that interface with various **external systems and services.**

including excel files, documents, and email content.

HOW DOES CLARK ENSURE DATA SECURITY AND PRIVACY?



Clark ensures the Security and Privacy of data through several key measures:

Secure Authentication and Authorization:

Clark employs a robust authentication system, using a Single Sign-On (SSO) mechanism integrated with TruOps. This ensures that only authorized users can access the system. Additionally, authorization protocols determine what data each user or role within the organization can access, preventing unauthorized data exposure.

Row Level and Table Level Security Policies:

Clark uses Row Level Security policies to provide fine-grained access control. **Data from different tenants are stored in separate logical partitions**, ensuring isolation of each client's data.

Table level security policy is also leveraged to prevent unnecessary or unauthorized modules from being inadvertently accessed or compromised, thereby **maintaining its confidentiality**. This multipronged approach to data access **greatly enhances data confidentiality** without giving up the goal of presenting a Unified view.

API-Driven Data Handling with OpenAI:

When integrating with external services like OpenAI, Clark uses API routes that are designed to respect data privacy. OpenAI, for instance, has policies in place for data submitted via API, ensuring that it is not used for any other purposes. This minimizes the risk of data leakage or misuse.

Embedding Minimum contextual data while in Processing:

Clark is designed to use only the necessary data required to generate a response. This principle of data minimization reduces the risk of exposing sensitive information and ensures that only relevant data is processed for each query.

Data Encryption:

Data transmitted to and from **Clark is encrypted**, protecting it during transit. This includes using secure protocols including TLS (Transport Layer Security) for data transmission. Additionally, data stored in databases is also **encrypted at rest** using AES-256 encryption, further securing it from unauthorized access or breaches.

HOW TO OPTIMIZE YOUR QUESTIONS AND CREATE EFFECTIVE PROMPTS

To optimize your questions and create effective prompts for Clark, start by clearly defining your objective and using specific, concise language that aligns with the data and functionalities available within the system.

For the Cyber Knowledge base prompts, you can ask as wide or narrow questions as you desire. The system is designed to clearly tell you if it cannot answer your query and can suggest you to change your style for more specific or topic related query.

For TruOps prompts, the more generic your question, the more likely it will be you will not get your desired answer. If you do not get the answer you need, try to be more specific with phrases like, 'Give me the top 5...', 'Show me a count of...', 'What is the highest...' etc. to narrow your focus. Then, slowly build your prompt 'wider' as you go.

Here are few examples of specific, clear and concise prompts that are more likely to get you the desired answers:

Incorrect: Give me some information on top issues last year.

Correct: List top 5 issues in year 2021 by severity.

Incorrect: Show me task planning trend.

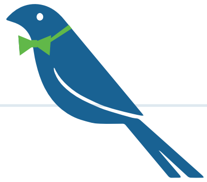
Correct: Show me task planning trend by month over last 5 years.

Incorrect: Show me active Vs inactive issues.

Correct: Show me Active Vs Inactive issues by month in the year 2021.

Incorrect: Provide me information on top 5 vendors from last quarter.

Correct: List top 5 vendors with the severity level as critical in June 2023 quarter.



GENERAL PROMPT CATALOGUE

You can use any question in natural language, however, to make it easier for you, Clark dynamically suggests potential questions, as you type your question.
These suggestions can accelerate your querying process:

- Pick a prompt closely matching your requirements.
- Modify as needed to refine and tailor the query to your exact needs.
- Submit your query.

Below are a few examples of preloaded prompts to pick from. Of course, you are welcome to edit the prompts for custom inquiries.

Module	Clark Demo Prompts	Visual
Asset	Show me Count of critical assets and their criticality score	Yes
Asset	Show me a count of assets by criticality	Yes
Asset	Show me List of 10 Critical assets and associated issues	No
Asset	Show me summary of Orphan assets	No
Risk	Show me a count of Risks by Risk Owner	Yes
Risk	Show me count of Risks by Risk Category	Yes
Issues	Show me a summary of issues by their status for the last 2 months	Yes
Issues	Show me List of 10 issues for issue source Compliance	No
Issues	Show me all issues created in the year 2023 for business unit Commercial Operation	No
Issues	Show me 10 High severity issues	No
Issues	Show me all the issues with Classification value as High and Issue Status as Open	No
Issues	Show me Issue Title, Issue Owner, Issue Description, Business Unit for all the issues with Classification value as High and Issue Status as Open	No
Issues	List critical issues and risks for assets with 100% criticality.	No
Exception	Show Exceptions which are going to expire in next 3 Months	No
Exception	Show List of Exceptions expiring in 2 weeks	No
Exception	Show me count of Exceptions by Exception Type	Yes
Vendor	Show me Count of Vendor Risks, classified by Status.	Yes
Vendor	Show me count of Risks for Vendor service	Yes
Vendor	Show me Risk by Severity for each Vendor service	Yes
Vendor	Show me Risk by Status for each Vendor Business Unit	No

OTHER FREQUENTLY ASKED QUESTIONS

How does Clark differ from traditional chat bots?

Clark goes beyond a traditional conversational assistant by delivering a verified, contextual response to your question in the likeness of a GRC expert. It can do this by combining large language model (LLM) models with GRC knowledge and enterprise data. It seamlessly integrates with your technology stack to extract and interpret data, providing clear answers to complex questions through a sophisticated AI-driven interface.

What types of questions can I ask Clark?

You can ask Clark a variety of questions related to data analytics, security, risk, and compliance. Clark is designed to understand and respond to complex queries in these domains.

How does Clark ensure user authentication and data security?

Clark uses TruOps-based Single Sign-On (SSO) for authentication. Users are redirected to the TruOps login page if they try to access Clark without being logged into TruOps. Each tenant's data is stored in separate logical partitions, secured from unauthorized access using Row Level Security Policy (RLS).

Clark's Module Level Security Policy restricts data access to authorized modules only, ensuring secure and relevant data extraction for responses.

Additional Questions »

How does Clark use OpenAI and LLM?

Clark uses OpenAI's API, which ensures data privacy as OpenAI does not use data submitted via the API in any way. Relevant data is embedded in the prompt only when necessary and is removed after the response is generated.

Once a response is generated, the data used in the prompt is removed from OpenAI, ensuring your information remains private and secure.

How does Clark handle external unstructured data like Excel sheets and PDFs?

External unstructured data is securely stored in our TruOps managed vector database, specially designed and optimized for searching on contextual relevance based on user questions put in natural English language.

Where is the TruOps database hosted, and what security measures are in place?

The TruOps AI database is securely hosted within the SDG managed, cloud environment, leveraging AWS for robust and scalable cloud infrastructure, utilizing Docker containers for secure, isolated runtime environments.

Is there a limit to the number of queries I can ask Clark?

Currently, there is no set limit to the number of queries you can ask. It will be up to a certain token amount allocated for usage. This limit can be set increased based on your requirement. Clark is built to handle a high volume of inquiries efficiently.

How does Clark understand complex queries in natural language?

Clark employs advanced natural language processing (NLP) techniques to interpret and respond to complex queries accurately.

How often is Clark updated?

Clark receives regular updates to enhance its features, security measures, and overall performance. Update schedules are communicated in advance to users.

How secure is the data transmission to and from Clark?

Data transmission to and from Clark is encrypted and secure, adhering to the latest cybersecurity standards and protocols.

What training is required to use Clark effectively?

Clark is designed to be user-friendly and usually no training is necessary to start using it, however, we do offer training materials and sessions to help users maximize its capabilities.

How are external unstructured data like Excel spreadsheets and PDF files handled for privacy?

All external unstructured data uploaded to our system is securely stored in our in-house Chroma DB vector database, ensuring complete data privacy and no external exposure.

How does Clark ensure data privacy and security when using OpenAI?

We utilize OpenAI exclusively through its API, which guarantees data privacy (OpenAI does not utilize API-submitted data for any other purposes.)

We ensure secure communication with OpenAI's API by using a secure API key provided by OpenAI. This key is a unique identifier that authenticates and authorizes our access to the API, ensuring that only authorized requests from TruOps are processed. OpenAI itself is hosted on a secure Azure environment and has built in security measures for its API, including HTTPS encryption for all data in transit and follows industry best practices for securing their infrastructure and services.

Additionally, our architecture uses an embedding mechanism, which ensures that during a chat session, data privacy is maintained by embedding only the necessary data in prompts and removing it after response generation, coupled with our stringent in-house data storage and handling policies.

Where is the TruOps database hosted, and what security measures are in place?

The TruOps database is securely hosted within the SDG managed, containerized cloud environment, leveraging AWS for robust and scalable cloud infrastructure, utilizing Docker containers for secure, isolated runtime environments. All the containers are managed by Kubernetes for automated deployment and scaling, featuring self-healing mechanisms that enhance reliability and security.

We implement stringent security protocols including data encryption, strict access control, advanced network security, and regular security audits to ensure data integrity and confidentiality.

Are there any additional security layers added by TruOps when interfacing with OpenAI's API?

Yes, in addition to OpenAI's inherent security measures, Clark adds extra layers of security, including advanced authentication and authorization checks, through an industry standard Langchain framework, to further safeguard the data being processed through the OpenAI API.

Can Clark be customized to specific organizational needs?

Yes, Clark offers customization options to align with specific organizational requirements in terms of domain specific fine-tuning, data handling, and integration with in-house or third party data sources, and response generation.