Query.AI Decentralized Data Access & Analysis

Access your data where it lives

For years, the legacy approach to achieve centralized insights has seen companies attempt to centralize their data in one place and in one format so the SOC could run queries and gain full context of what's happening. But this poses a big challenge.

"Centralization is unrealistic."

Organizations are unable to store all of their security data in a single, centralized data repository. Data lives everywhere on-prem, in cloud, and in third-party SaaS applications. Security teams need a way to easily access and analyze data with context that is distributed in multiple repositories across platforms, locations, and cloud providers to gain centralized insights without centralizing the data.

"Query.AI has created a revolutionary capability for decentralized data access and analysis ."

Product Overview

Query.AI is a decentralized data access and analysis technology that simplifies security investigations across disparate platforms without data duplication. Our technology runs directly from the analyst's browser and makes human investigations more efficient.

Only Query.AI gives you consistent access to all your data regardless of where it is stored without first moving it to a central location, delivering significant cost savings over legacy approaches that require spending precious security budget to duplicate data to achieve centralized processing.

Key Benefits

Easy to Implement: Get started in minutes, no installations or infrastructure needed

Effortless to Use: We handle the access, translation, aggregation, and normalization

Private by Design: Data, results & credentials stay private

How it Works

The solution's browser-based architecture means you don't need to transfer any data or make any infrastructure investments. Getting started is as simple as pointing your browser to your data, wherever it lives.

Business Value

Gain Efficiencies

Leverage existing tool investments, through a unified interface with easy access to data and faster MTTD and MTTR for security investigations.

Reduce Cost

Get centralized insights without data centralization, and empowering junior resources through the use of assistive AI.

Reduce Risk

Achieve situational awareness with enterprise visibility across data silos and leverage workflows to ensure consistency in security investigations.

Query.ai

Use Cases

Virtual SIEM

Gain centralized insight through dashboards, searching, correlation, and reporting all without data centralization.

Investigation support (IR and Threat Hunting)

Accelerate investigations with real-time access to data and context across all tools and platforms, without the need to access each repository individually.

Empower your team with Assistive-AI

Leverage natural language processing, guided data exploration, and a curated knowledge base of security questions

About Query.AI

Query.AI is a decentralized data access and analysis technology that simplifies security investigations across disparate platforms without data duplication. Our technology runs directly from the analyst's browser and makes human investigations more efficient, while reducing SIEM costs.

Based in Brookings South Dakota, Query.AI is in the heart of the Silicon Prairie and is proof that innovation and talent can sprout and grow anywhere. Our founding team has decades of experience as both security practitioners and as developers of security solutions.

Key Features

Experience the best in simplified and uniform security analysis that gives you full visibility, without moving or centralizing your data:

Query your data in plain English

NLP-powered Assistive-AI technology makes it easy to use plain English to query your data.

Powerful search

Simultaneously query across multiple data platforms, results are returned in a single aggregated view for investigations and analysis.

Correlate across multiple data stores

Create and schedule workflows leveraging data from multiple platforms to provide you with relevant insights you need.

> "This is a really novel approach, I like the simplicity of user-friendly queries, lightweight deployment, and flexibility to reduce data duplication. Query.AI has vastly increased efficiency and provided a level of consistency that was previously out of reach."
>
> Chris Borkenhagen
> CIO/CISO at Docker

Adaptive visualizations

Advanced machine learning enables intelligent visualizations based on your data identifying outliers and anomalies to further explore.

Robust questions library

A curated knowledgebase of investigative queries and workflows that can be applied by your users that cover a wide range of use cases.

Internal and external collaboration

You can easily share your insights and analysis processes with other teams, departments, partners, and industry communities.