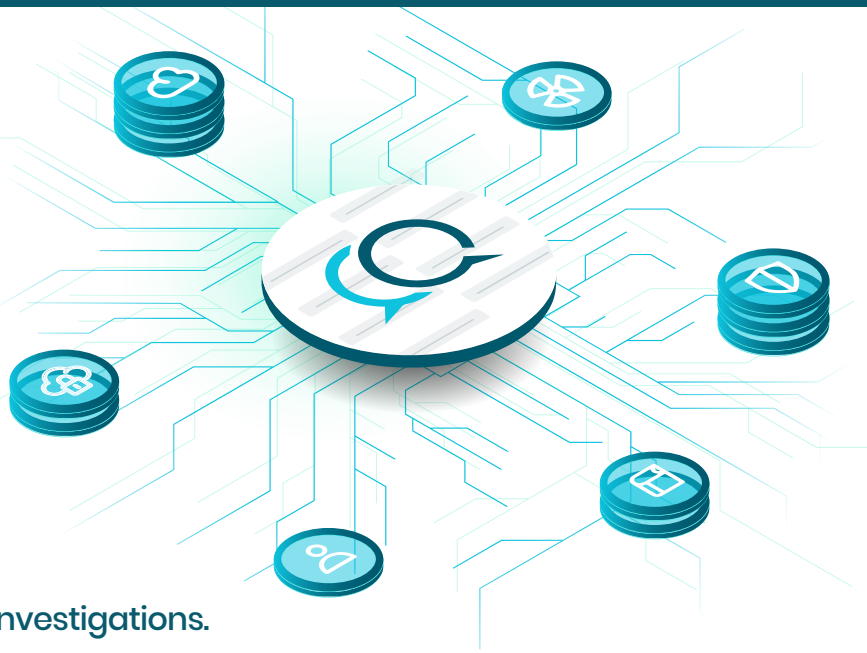
Query.ai

Datasheet

# Security Investigations Control Plane



## Access your data where it lives. Accelerate investigations. Gain high-confidence outcomes.

Legacy approaches for security investigations require enterprises to attempt to centralize all of their siloed security data in one location and format. With growing data volumes across an enterprise's on-premise, multi-cloud, and SaaS environments, combined with security solutions charging by data ingestion, this approach has proven cost prohibitive and consumes valuable staff resources.

The other problem: investigation processes are burdened with time consuming pivots across multiple tools to obtain the needed information. With 45% of organizations using more than 20 disconnected tools for investigations, the reality today is complex investigations and long mean time to respond (MTTR).

**Query.AI alleviates these challenges with a modern approach to security investigations. One that empowers companies to centrally access and efficiently analyze their data, wherever it lives, to enable fast, high-confidence outcomes.**

> "Query.AI vastly reduces the time and effort required for my security investigations by making it easy to access the data I need, when I need it."
> - F1000 Financial Services

## Product overview

Query.AI provides the market's only security investigations control plane for modern enterprises. Our patented browser-based platform delivers real-time access and centralized insights to data across your on-premises, multi-cloud, and SaaS applications, without duplicating it from its native locations.

Query.AI gives you access to all your data, where and when you need it, providing a simple and effective way to meet your security investigation and response goals while simultaneously reducing costs.

Our control plane platform serves as the connective tissue for your investigations to gather the data in real-time from across your systems, eliminating time consuming investigation processes that have traditionally required pivoting across 10 or more tools. The platform then automatically normalizes and enriches the data, delivering meaningful insights in a single aggregated view. This unique approach enables accelerated, consistent security investigations, without the complexity.

## Key benefits

**Access data where it lives**
Delivers real-time access and centralized insights to data across your on-premises, multi-cloud, and SaaS applications, without duplicating it from its native locations.

**Privacy by design**
Alleviates privacy and governance concerns about your enterprise data with a platform architecture that doesn't store, process, or require vendor access to your data.

**Accelerate investigations**
Simultaneously normalizes and enriches alert data across platforms, enabling consistent security investigations with high confidence outcomes and without the complexity.

**Save money**
Provides a highly affordable approach with a security investigations control plane platform that gives you the flexibility to determine where to store your data, who has access, and how to pay for it based on the intended use.

**Amplify your human potential**
Provides guided data exploration and supports natural language processing so security analysts don't need to be experts in individual systems—simply ask questions and get answers.


## Access data where it lives

**Browser-based control plane**
Our control plane platform serves as your connective tissue giving you access to data where it lives. With our lightweight architecture, your browser serves as the data hub that connects your disparate security solutions, making it easy to deploy while eliminating any equipment overhead and management costs.

**Federated search**
Investigate alerts and potential threats across multiple siloed solutions, from a single interface. The platform provides guided data exploration and supports a unified query language (UQL) along with natural language processing so security analysts don't need to be experts in individual systems—they simply ask questions and get answers.

## Investigate in minutes

**Automated data normalization and enrichment**
Eliminating the need to pivot your investigations across multiple security tools, Query.AI simultaneously triages and normalizes the alert data across platforms, delivering meaningful insights with context in a single aggregated view. This streamlined approach enables fast, efficient security investigations with high confidence outcomes.

**Automated data visualizations and analysis**
Query.AI automatically creates intelligent dashboards and visualizations of your data to gain insights and easily view outliers or anomalous events. This makes it simple to gain the context and spot issues that may not be apparent in tabular results alone.

## Respond with one click

**One-click response actions**
Initiate investigation response actions directly from your browser, such as password resets, lock, block, or isolate a user, IP, or host.

**Streamlined annotation**
The platform makes documenting your activity a turnkey process. You can update a ticket in your service management tool and send enriched data to your SOAR and SIEM.

## Experience the advantages

**Accelerate threat response**
Point your browser to your data, where it lives, to conduct federated search against all your data. This unique approach makes fast, high-confidence investigation outcomes a reality.

**Reduce security cost and complexity**
Eliminate expensive data duplication and storage requirements, enhance data sets, and improve the ROI of your current security budget.

**Proactively identify risks**
Our comprehensive integrations allow you to aggregate and correlate data from all your sources, making it fast and effective to proactively identify high-priority risks and reduce your MTTR.

Query.ai

**Learn more**
Visit **www.query.ai**

"The structure of Query.AI's approach is very clever. I love the simplicity with user-friendly queries, quick setup, and no required data duplication."
- Global Retailer

"When developing sustainable security monitoring programs, vendors must strive to make them easy to use and simple to integrate with existing tools. I believe Query.AI sets the standard."
- Chris Borkenhagen, CIO, Docker, Inc.