Query.ai

Tech Brief

Security Investigations Control Plane

A modern approach to security investigations for accelerated, high confidence outcomes

Successful security operations require real-time access to data across your on-premises, multi-cloud, and SaaS applications. Investigation processes are also time consuming, requiring you to pivot across multiple tools to obtain the needed information. This high number of siloled tools creates complex security investigations that lead to long mean time to respond (MTTR) and increased costs in the event of a successful breach.

Enterprises need a modern approach to security investigations. One that empowers you to centrally access and efficiently analyze your data, wherever it lives, to enable fast investigations with high confidence outcomes.

Query.AI empowers you to do just that.

Platform 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 environments, without duplicating it from its native locations.

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

How it works

Query.AI eliminates the burdens of universal data centralization for your security investigations. Our platform enables complete control of your security investigations, providing:

- Seamless access to data where it lives
- Simultaneous search across multiple systems with a single Unified Query Language (UQL)
- Automated alert enrichment to understand context, impact, and severity for accelerated, high confidence investigations
- Closed loop, human-driven response actions and incident annotation to case management

All within a single, unified interface: your security investigations control plane.

Access data where it lives

With our lightweight architecture, your browser serves as the data hub that connects your disparate security platforms. Our modern, API-driven approach removes the burden to transfer or duplicate data in an effort to centralize. No infrastructure or data duplication costs; getting started is as simple as pointing your browser to your data, wherever it lives.

Providing privacy-by-design, our platform doesn't store or process your data, eliminating any added risk or concern about the privacy and security of your enterprise data.

Investigate in minutes, without swivel-chair analysis

When you have activity to investigate, our control plane platform serves as your connective tissue, providing real-time, federated search for data collection from across your systems. This eliminates the time consuming process of pivoting from one security tool to the next. Query.AI then automatically normalizes and enriches the data, delivering meaningful insights in a single aggregated view. This unique approach to federate investigations reduces response times from hours to minutes, enabling you to optimize your MTTR.

Respond with one-click orchestration

Query.AI makes it simple to gain the context required to initiate the appropriate response actions on your investigations—all directly from your browser. The platform can initiate or update tickets in your service management tool, as well as initiate a password reset, lock, block, or isolate a user, IP, or host. Any response action your tools and infrastructure can support is at your fingertips.

Capabilities

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.

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 understand the context and spot issues that may not be apparent in tabular results alone.

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.

Use case: Unified incident response

Security investigations are plagued with pivoting from tool to tool spread across the on-premise, multi-cloud, and SaaS infrastructure. A single investigation requires time consuming logins and custom search across more than 10 tools.

Impact of legacy approach

- Swivel chair pivots across 10+ tools
- Analyst time consumption: accessing investigation data, manual normalization, lengthy analysis to identify relationship and context
- Average MTTR is days to weeks[1]

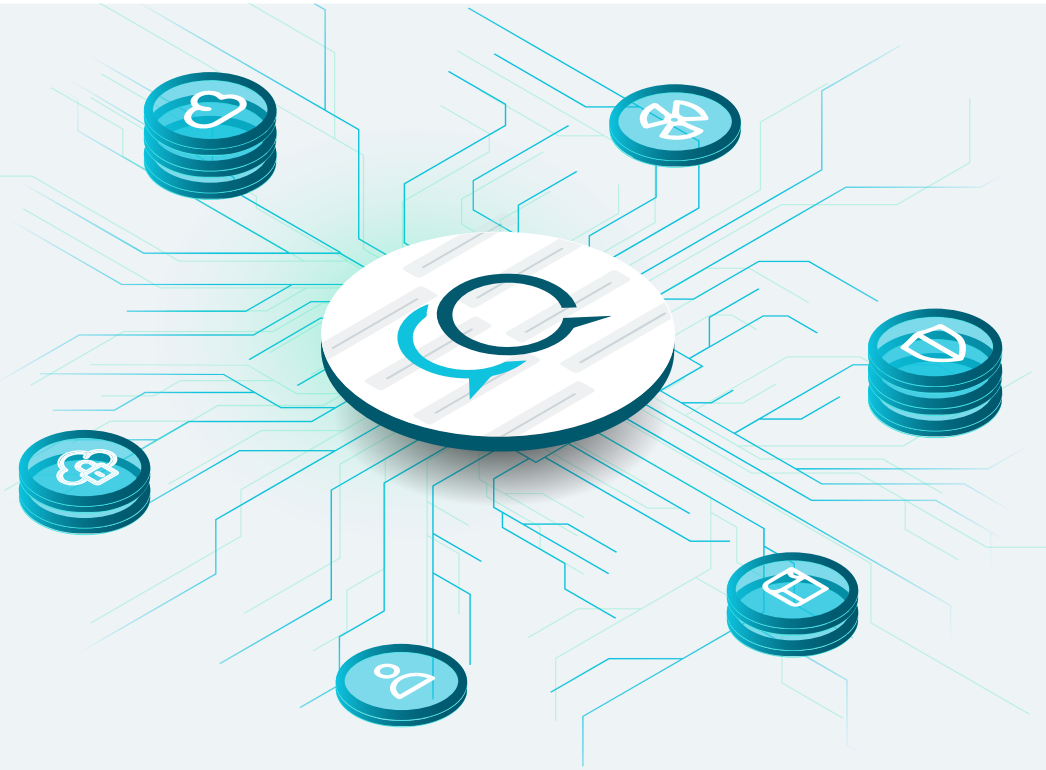
With Query.ai, security operations teams gain a new approach that cuts through legacy complexity. Your security investigations control plane will simultaneously normalize and enrich your alert data across platforms, enabling consistent security investigations with high confidence outcomes in minutes.

Impact of modern approach with Query.ai

- Eliminates swivel chair with federated search across your tools
- Automates data normalization and enrichment, enabling analysts to quickly gain meaningful insights in a single aggregated view
- Reduces response times from hours to minutes

Request a demo.

Ready to get started?
Visit **info.query.ai/demo-request**



Query.ai

[1] Computing Research. Best practice makes perfect: malware response in the new normal. August 2020.