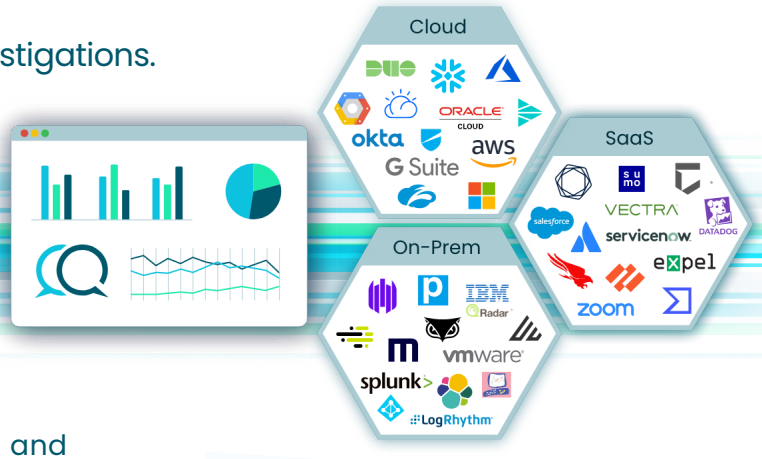
Query.ai

Datasheet

Security Investigations Platform

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



In a simpler time, data volumes were initially small and easily centralized, which enabled organizations to house all data on-prem and tuck it behind a cozy perimeter. Today, data volumes are enormous and highly distributed across cloud, third-party SaaS, and on-prem environments. This makes the universal centralization approach for security investigations entirely impractical.

Companies need to be able to unlock access to and value from cybersecurity data wherever it is stored, regardless of vendor or technology, without requiring centralization.

The Query.AI Security Investigations Platform alleviates these challenges with a modern approach that drives efficiencies in your security investigations so you can more quickly, accurately, and cost-effectively address cybersecurity threats.

Product overview

The Query.AI Security Investigations Platform serves as a connective tissue that delivers federated search to conduct cybersecurity investigations across data silos and eliminates the ineffective universal data centralization approach.

The platform provides companies with a unified browser interface, which plugs into security architectures quickly and easily using APIs. It gives security teams the flexibility to query across cybersecurity systems and contextual information stores with the simplicity of a single query.

Key Benefits

Easily investigate across data silos

Gain real-time access and centralized insights to data across your disparate environments, without centralizing it.

Enjoy privacy by design

Eliminate any added risk or concern about the privacy and security of enterprise data with an architecture that doesn't store or process your company's data.

Expedite investigations

Achieve complete visibility and context to quickly address your high volume of phishing, malware, IOCs, and other investigations.

Amplify your human potential

Enable your senior and junior analysts, alike, to efficiently conduct investigations across toolsets without having to become expert in each, individual system.

Query.ai

Access data where it lives	Investigate in minutes	Respond with one click
Browser-based architecture With our lightweight architecture, your browser serves as the data hub that connects your disparate technologies. The Query.AI platform uses an API-driven approach that removes the hassle and cost of transferring data traditionally required to achieve visibility. There are no infrastructure or duplication costs and getting started is as simple as pointing a browser to your data, wherever it lives.	**Single query language** The platform increases your team's potential by eliminating the need for analysts to learn the syntax of each individual cybersecurity system. Simply ask a question via unified query language, natural language, or text and get contextual results back from your infrastructure.	**Initiate response actions** Right from the platform, you can easily initiate your desired investigation response actions, such as password resets, lock, block, or isolate a user, IP, or host. It can leverage any API system call that's supported by your integrated solutions.
Federated search Our federated search empowers you to simultaneously ask investigative questions across your data silos. For example, you can do a single search on a suspicious IP address and get real-time insights on that IP from across your entire infrastructure and toolsets.	**Automated data normalization and enrichment** Instead of manually correlating the pieces of your investigation across tools, the platform automatically enriches and normalizes the related elements of an investigation so you can understand the context. Your team can rapidly see what's relevant, the potential impact, and priority—all in a single dashboard. This streamlines your investigation and provides everything at your fingertips to efficiently identify and respond to security risk.	**Streamline ticket management** Documenting and closing out your investigations is a turnkey process. From the dashboard, you can initiate or update a ticket in your service management tool. You can also easily attach the relevant investigation information, as well as add annotations so everything is documented and available for future forensic and audit needs

Gartner
COOL VENDOR 2021™

"Query.AI is our solution-of-choice for centralized observability and incident management. The broad-based ability to access, investigate, and respond to what's happening in every one of our core environments through a single console gives us speed and efficiency. Our ability to identify, react, and quarantine is significantly faster, and as a result, more cost effective."

Chris Borkenhagen
Chief Operating Officer and Chief Information Security Officer
AuthenticID

Learn More
Visit: www.query.ai