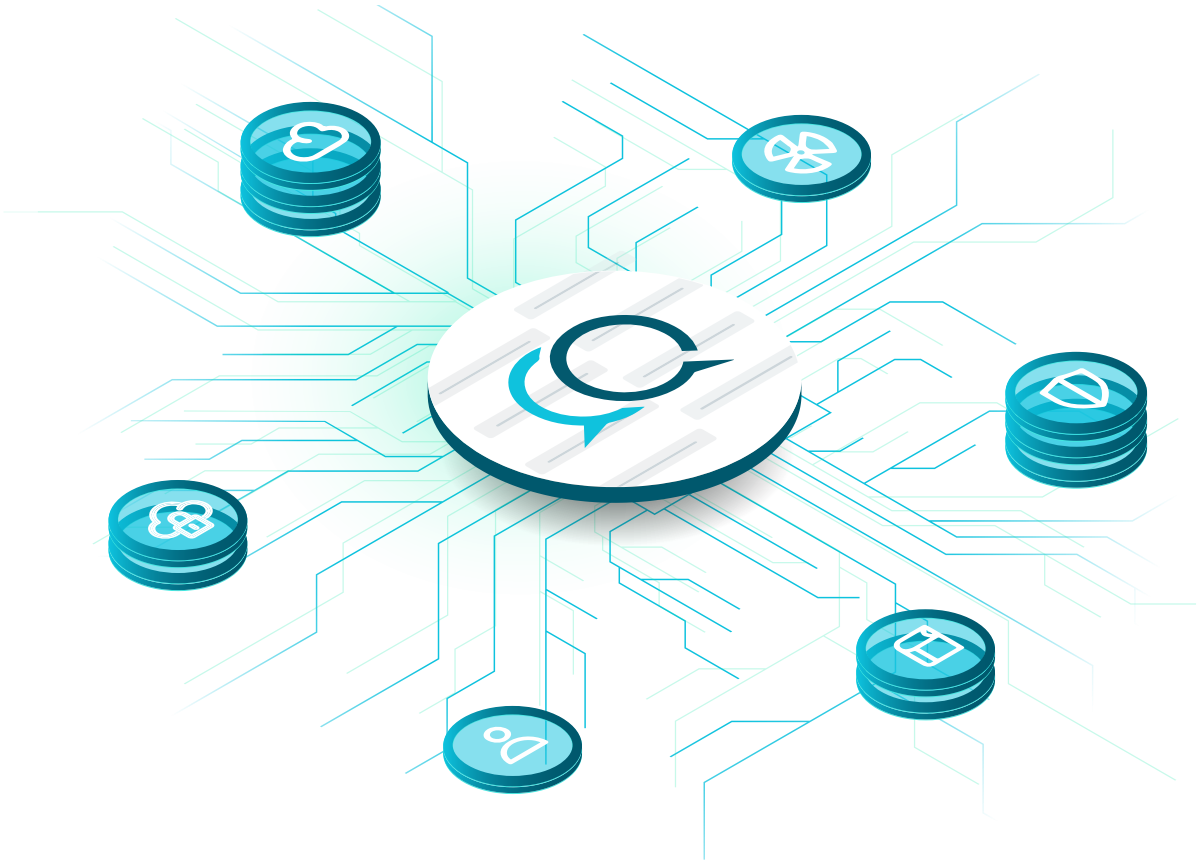
Query.ai

Customer Success

Let's take a closer look at some customer successes and concrete outcomes to see what you can achieve with the Query.AI platform.



Accelerate and increase confidence in the outcomes of your investigations

Most organizations have decentralized data in silos across their cloud, on-premises, and SaaS environments. Our security investigations control plane serves as the data plane to all of your data silos, accessing and analyzing the data in real-time from across your systems.

Instead of manually pivoting from one data silo to the next to conduct a single investigation, with Query.AI, you ask a single question and get meaningful insights from all your data silos. Our customers are transforming investigations from what was a tedious, error-prone process taking up to an hour to search across 50+ tools to a modern process that delivers accurate investigation results in minutes.

Mass Media Company

9,000 employees

Challenge:

Each investigation required 30 minutes; 10+ steps

- Running 6 instances of EDR solution across regions and business units
- Investigation required authenticated login to each EDR tenant to identify the host instance where the issue resided
- Required additional queries on the identified host tenant to pull telemetry data

Outcome with Query.AI:

Reduced investigation time to 1 minute and 1 step

- Gained ability to simultaneously query across all EDR tenants and instantly identify the desired host tenant
- Gained a single console covering their environment to quickly probe further to reach a decision on an alert
- Equipped with capabilities that make it simple to initiate the appropriate response action

Securities Brokerage Company

4,100 employees

Challenge:

Complex triage across 10+ tools; hours per investigation

- Triage for employee phishing email submissions required login and search across 10+ tools
- Required hours to collect, compile, aggregate, and analyze data
- Results took hours and were inconclusive

Outcome with Query.AI:

Reduced mean-time-to-respond (MTTR) to minutes

- Streamlined query and investigation across all tools
- Achieved response in minutes with high confidence outcomes

> "Query.AI eliminates the multiple searches across individual tools and lets us quickly gain the context to determine which alerts are high-fidelity by letting us easily assess what each system says about it. Our team now has greater accuracy with less clicks and time required to reach an outcome. By eliminating the search pivots across tools, we now have confidence in our incident response decisions and have improved our security posture."
>
> - Joe Oney, Security Operations Manager, Hogan Lovells

Amplify your team's potential and make it easier to onboard new analysts

One of the biggest challenges for security team members is learning the ins and outs of every solution in the organization's security stack, each of which require their own search syntax for conducting triage and even the most basic investigation. This burden makes it hard for security analysts to maximize their support of the security processes and inhibits the ability to onboard and train new analysts.

Query.AI lets you cut through this complexity. The platform provides guided data exploration and supports a unified query language (UQL) along with natural language processing, so your security analysts don't need to be experts in individual systems—they simply ask questions and get answers. With Query.AI, your team can fully leverage even the most complex tools in your environment for their investigations.

Regional Healthcare System

7,500 employees

Challenge:

Limited analyst skills and resources

- Expanding analyst proficiency in managing security investigations, which required mastering numerous, complex systems
- Improving the analysts skill set, without massive time investment for training

Outcome with Query.AI:

Increased analyst skills; job satisfaction

- Removed busy work of manual data collection and aggregation and need for analysts to master multiple systems in order to manage investigations
- Dramatically increased analyst productivity and time to alert resolution, reducing MTTR
- Provided a better work environment for existing analysts, reducing turnover

Managed Security Services Provider (MSSP)

250 employees

Challenge:

Time-intensive effort required to train and increase skills of new security staff

- Time to onboard a new analyst was 18-24 months, on average

Outcome with Query.AI:

Reduced cost, time to ramp up analysts

- Reduced onboarding time to days
- Made analysts productive without requiring the learning curve of all the platforms

> "Query.AI provides a strong use case as I only have three security analysts who work 8 to 5. Nothing ever goes bump in the middle of the day. With the native query language and workflows, my junior staff can now initiate an investigation and follow the workflow. Query.AI expands the reach of my existing security staff."
>
> - SOC Manager, Regional Bank

Learn more

Visit: query.ai