Query.ai Launches Agents and Data Pipelines to Cut Through Security Data Chaos

Mission-specific AI Agents and automated Pipelines help security teams turn distributed data into answers, fast

Query logo

ATLANTA, GA, UNITED STATES, August 4, 2025 /EINPresswire.com/ -- FOR IMMEDIATE RELEASE

Query.ai, Inc., an early pioneer in federated search for cybersecurity, today announced two new features, Query Agents and Query Security Data Pipelines to help security teams turn raw telemetry into real answers, without the usual data engineering pain. Both are available now in preview.

> Query's approach is refreshingly different, they understand that smaller, purpose-built agents using normalized data deliver the precision and context that security operations teams actually need."
>
> *Rudy Ristich, CISO and CPO of Avant*

- Query Agents automate triage, threat research, and investigations with high-context AI.
- Security Data Pipelines deliver OCSF-aligned data directly to Amazon S3, Azure Blob, Google Cloud Storage, and Splunk with no ETL required.

These new capabilities are powered by the OCSF-normalized data mesh that Query creates, enabling customers to access, understand, and act on distributed security data.

"In my time as a CISO, I've watched how the industry's rush to apply general-purpose LLMs to security operations can create more noise than signal," said Query customer Rudy Ristich, CISO and CPO of Avant. "Query.ai's approach is refreshingly different, they understand that smaller, purpose-built agents using high-quality, normalized data deliver the precision and context that security operations teams actually need to save time and arrive at answers rather than struggling to ask the right question."

The Query Federated Search Platform creates a normalized OCSF data mesh at search time, allowing purpose-built agents to operate with high context from real-time reach into distributed

customer environments, using just the data they need, when they need it. These agents can automate common investigation and triage tasks, vulnerability assessments, threat research, and many other mission-specific actions, using the full context of the data mesh. Query agents are not confined to centralized data in a SIEM or single platform, like many solutions. Because each action uses only the data required for the task, sourced from the Query Data Mesh and normalized to the Open Cybersecurity Schema Framework (OCSF), they are fast and less prone to hallucinations, errors, or gaps in data context.

Alongside the agents, Query Security Data Pipelines makes it effortless to write high-quality, OCSF-aligned "gold" datasets into a customer's chosen cloud storage platform or into their Splunk SIEM. There is no ETL or schema mapping to maintain, and no data engineering required.

"Our mission is to enable security teams to turn their data into an advantage, getting the data-driven answers they need quickly, so they can protect and defend their environments," said Matt Eberhart, CEO of Query.ai. "Security teams have the data they need, but wrangling and using it is far too difficult. We built these new solutions with our customers to solve the data problems they face, using the latest advances in AI and data best practices so they can stop focusing on plumbing and focus on their missions."

At launch, Security Data Pipelines support storing data from sources connected to the Query Security Data Mesh in customer owned data stores, including: Amazon S3, Azure Blob Storage (Azure Data Lake Service V2), Google Cloud Storage, and Splunk. Support for Snowflake, Databricks, and Amazon Security Lake support is coming soon.

"I've worked with some of the best data-forward security teams in the world," said Jonathan Rau, Distinguished Engineer at Query.ai. "We are taking our collective experience and enabling teams to write data the right way and unlock answers from it immediately. We're helping security teams work smarter, not harder, with better data. Stay dangerous."

These launches continue the history of breaking norms at Query and decades of inertia around requirements to centralize data, while removing the high barriers of data engineering work. Security teams run on data. Query works with the best data forward teams that want to simplify the path to using as much of their data as possible to get the answers they need, faster.

Preview now available. Learn more at www.query.ai or get in touch at press@query.ai.

Mike Bousquet
Query.ai, Inc.
press@query.ai
Visit us on social media:
LinkedIn