

# Query Workers Are Now Generally Available: AI Agents That Investigate Across Every Security Tool Without Moving the Data

*Built on the Query Security Data Mesh, Workers run across 60+ integrations, show every query, and manage findings from triage to close, with full transcripts.*



Query logo

ATLANTA, GA, UNITED STATES, July 30, 2026 /EINPresswire.com/ -- Query,

known for pioneering Federated Search, today made Query Workers generally available. Query Workers are AI agents that investigate a threat the way a senior analyst would, across every connected security tool, in place, without copying data into one more platform first. The agents work alongside security operators, using the Query Security Data Mesh to access data anywhere, through a patented federated search engine that improves reach, reasoning, and AI decision making.

“

Issues that used to take hours of pivoting across consoles come back in minutes, with evidence and every query shown. My analysts still make the call, starting from answers instead of a blank console.”

*Rudy Ristich, CISO and CPO of  
Avant*

The launch lands in a week when the whole industry is saying the same thing Query has said since it was founded. An AI agent is only as good as the data it can reach, and in a real enterprise data does not all live in one place. The difference in the Query architecture shows in the outcomes. Query built the data layer first and has proved it in production. The Workers run on top of it.

That data layer is the Security Data Mesh, and it is where the hard engineering went. Reaching data where it lives is

the mission. Making an agent reason across dozens of disconnected sources is years of work, in three parts.

The first is a common language. Query translates every source into the open OCSF schema at the moment a query runs. Without a shared schema, federation is a set of separate searches, all producing different data sets that cost the operator or the agent time and effort to reconcile.

The second is search that runs in place. Query runs the query against CrowdStrike, Databricks,

Splunk, Microsoft Sentinel, Cribl, Okta, cloud data lakes, and dozens of other tools, reading the data where it lives instead of copying it to one more platform first. The mesh spans more than sixty integrations today, with over a thousand detection recipes behind Federated Detections, and Workers that can write a new detection when your team needs one, ready for a human to review and deploy.

The third is evidence a human can check. Every investigation produces a report, the full log of every query the Worker ran, a ledger of the indicators it found, and, on high-severity findings, an automated nine-point senior-analyst review. Nothing is a black box. Query Workers recommend and humans decide. Workers do not take actions on their own.

"The whole market now agrees that agents need to reach data wherever it lives. I agree with the goal," said Matt Eberhart, CEO of Query. "We spent years building the layer that makes it real, and that layer turned out to be the hard part. We built the mesh first, proved it across more than sixty sources in production, and put the Workers on top. The intelligence was never going to come from the model alone. It comes from what the model can see."

Since the preview at RSAC 2026, Query Workers have grown from autonomous investigation into how a team runs its day, in a form analysts can put to work now. Trust, but verify: every run leaves a complete record, down to the questions the Worker could not answer.

Findings flow into a case workspace that manages the agents and their output, built like the ticketing tools analysts already use: triage, investigate, act, escalate, close, with fast filtering and views a teammate can open from a link, or a push straight into the enterprise ticketing platform. Workers can run on a schedule, so a team starts the morning with one briefing instead of a queue nobody watched overnight: what is new, what recurred, what resolved itself, and the things that need a human review. Pricing is credit-based, with no per-gigabyte ingest fees and no data-volume charges.

Query's [Demo Center](#) publishes real Query Worker investigations as step-by-step replays, every federated query included. The invitation is the same one Query makes to the whole category: do not take our word for it. Watch the runs.

In its own testing, Query gave AI agents raw access to a large set of security tools and watched what happened as the environment grew. The agents quietly stopped consulting sources, then reported their conclusions with full confidence, built on a fraction of the data that was there. Agents working through the mesh kept looking across the whole estate. An agent that cannot reach everything will still sound certain about the little it saw.

Work that took analysts hours now finishes in about fifteen minutes, with a single Worker running dozens of federated queries on a complex case, across tools an analyst used to open one browser tab at a time.

"Issues that used to take my team hours of pivoting between separate consoles come back in minutes, with the evidence attached and every query shown," said Rudy Ristich, CISO and Chief Privacy Officer at Avant. "My analysts still make the call. They just start from an answer instead of a blank console."

"A Query Worker runs the investigation across every connected source and hands back a recommendation with the evidence shown," said Mike Bousquet, Chief Product Officer at Query. "It recommends, your team decides, and that split is deliberate. It only works because the layer underneath can reach every source and read them all in one schema."

Query Workers are generally available now. Query will be at Black Hat USA 2026. Request a demo and see live investigation replays [here](#).

### About Query

The Query security data mesh platform makes your data operational, wherever it's stored. No ingestion. No migration. No centralization required. Give your team and agents (yours or ours) the data foundation they need to search, investigate, hunt and detect across every source, while the data stays where it lives. Query is headquartered in Atlanta, Georgia. Learn more at [query.ai](https://query.ai).

Mike Bousquet

Query.AI, Inc.

[press@query.ai](mailto:press@query.ai)

Visit us on social media:

[LinkedIn](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/930580420>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.