EINPRESSWIRE

Query Introduces Federated Detections, Decoupling Detection Logic from Data Ingestion

New capability expands detection coverage across security data that will never be centralized

Query logo

ATLANTA, GA, UNITED STATES, January 28, 2026 /EINPresswire.com/ -- Query today announced Federated Detections, a new capability designed to help security teams run production-grade detections across all of their security data, including sources that traditional SIEM architectures cannot efficiently ingest.

> “
> Federated Detections let you push detection logic to security data in distributed sources and the results aren’t more detections, but higher fidelity detections across the entire environment.”
>
> *Rudy Ristich, CISO and CPO of Avant*

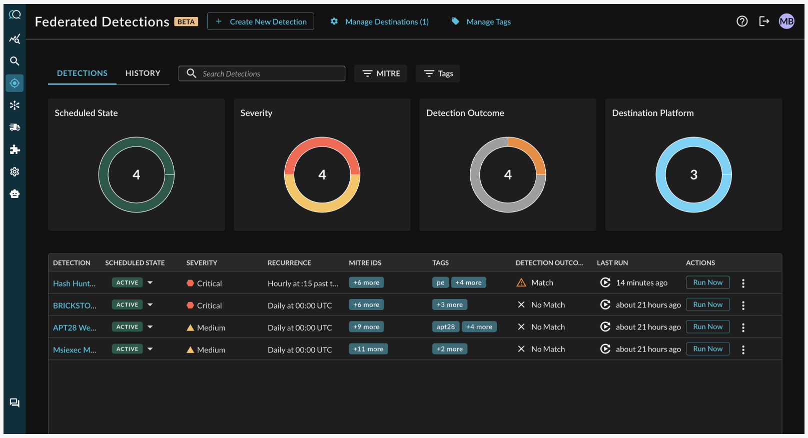
As security data volumes grow and environments sprawl across cloud platforms, SaaS systems, and security tools, detection coverage has become constrained by ingestion-based architectures rather than detection logic. Federated Detections address this challenge by separating detection logic from where data is stored, allowing teams to detect across distributed security data without moving or duplicating it first.

“Detection programs aren’t limited by logic, they’re limited by data availability,” said Mike Bousquet, CPO at Query. “Federated Detections remove the traditional constraints of data centralization. If a data source is connected to Query, customers can run detections against it, regardless of whether it lives in a lake, cloud storage, a security product, or a business platform.”

Detection Coverage Without Ingestion Constraints

“Detection coverage has always been limited by what you could afford to ingest,” said Rudy Ristich, CISO and CPO at Avant. “Federated Detections let you push detection logic to security data in distributed sources without constantly revisiting those tradeoffs, and the results aren’t more detections but higher fidelity detections across the entire environment.”

Federated Detections run as scheduled queries across Query’s Security Data Mesh, executing detection logic directly against connected data sources wherever they live. This allows detection coverage to expand naturally as environments evolve, without requiring teams to re-architect pipelines or centralize data before they can act.



DETECTION	SCHEDULED STATE	SEVERITY	RECURRENCE	MITRE IDS	TAGS	DETECTION OUTCO...	LAST RUN	ACTIONS
Hash Hunt...	ACTIVE	Critical	Hourly at :15 past t...	+6 more	pe +4 more	⚠ Match	14 minutes ago	Run Now
BRICKSTO...	ACTIVE	Critical	Daily at 00:00 UTC	+6 more	+3 more	✕ No Match	about 21 hours ago	Run Now
APT28 We...	ACTIVE	▲ Medium	Daily at 00:00 UTC	+9 more	apt28 +4 more	✕ No Match	about 21 hours ago	Run Now
Msiexec M...	ACTIVE	▲ Medium	Daily at 00:00 UTC	+11 more	+2 more	✕ No Match	about 21 hours ago	Run Now

Query Federated Detections

Detections are defined using structured logic — including aggregation, grouping, and threshold-based conditions — and execute on a predictable cadence with explicit evaluation windows. Each run produces a deterministic outcome that records what data was evaluated and why a detection fired.

This execution model allows security teams to preserve consistent detection logic while reducing long-term operational friction as data volumes and source diversity continue to grow.

Investigation That Starts With Context

When a detection matches, Query generates a finding that includes a replay link to rerun the exact detection logic against the same time window that triggered the result. Analysts can immediately review normalized results across contributing data sources and pivot into related entities and events using federated search.

Federated Detections are designed to hand investigations directly to analysts with the context they need without switching tools or reconstructing activity after the fact. Findings can also be routed into existing chat, ticketing, and incident response workflows.

Flexible Detection Authoring and Migration

Federated Detections support multiple paths for creating and maintaining detection logic. Teams can author detections directly in Federated Search Query Language (FSQL), convert existing SPL, KQL, or Sigma detections, generate FSQL from natural language prompts, or adapt existing detection recipes.

This flexibility reduces the effort required to migrate and scale detection coverage without forcing teams to rewrite existing detection logic on day one.

A New Control Plane for Detection Logic

By decoupling detection logic from ingestion, Federated Detections position Query as a control plane for detection logic across the modern security stack, independent of where data is stored or which tools generate it.

This approach enables broader detection coverage, more sustainable security architectures, and faster, more confident investigations as security environments continue to diversify.

Availability

Federated Detections are available to Query customers today. To learn more or see the capability in action, visit the Query website.

About Query

Query is an AI-powered Security Data Mesh that delivers security teams real-time answers and context from any connected source. Security teams move faster and make better decisions with more data context, while benefiting from federated detections, mission-specific AI agents, and copilots. Query accelerates security operations, working with existing platforms and tools, enabling security teams to access and use data anywhere.

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

This press release can be viewed online at: https://www.einpresswire.com/article/887029930

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.